Kommunikator GET – Installations- und Bedienungsanleitung

Installations- und Bedienungsanleitung für den Trikdis-Kommunikator GET mit Ethernet und 4G: Anschluss an die Alarmzentrale, LAN- und SIM-Einstellung in TrikdisConfig, Übertragung an die Leitstelle, die App Protegus 2.



Ausgabe: 2026-11-17
Immer aktuelle Webversion: https://trikdis.at/get-anleitung

Inhalt

1. Überblick

1.1 Wozu er dient, wie er funktioniert
1.2 Varianten: GET, GT und GT+
1.3 Kompatible Alarmzentralen
1.4 Die Teile des Kommunikators
1.5 Klemmen
1.6 LED-Anzeigen
1.7 Technische Daten

2. Schnelle Inbetriebnahme

2.1 Vorbereitung
2.2 Verbindung mit der App Protegus 2
2.3 Verbindung mit der Leitstelle

3. Montage und Anschluss

3.1 Schritte der Montage
3.2 Unterbringung im Gehäuse der Zentrale, Antenne
3.3 Anschluss an die Alarmzentrale
3.3.1 DSC – Datenbus (Keybus)
3.3.2 Paradox – serielle Schnittstelle
3.3.3 Paradox SP/MG – Keybus und TIP/RING
3.3.4 UTC Interlogix (Caddx) – Datenbus
3.3.5 Texecom – serielle Schnittstelle
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – Datenbus
3.3.9 Jede Zentrale – TIP/RING
3.4 Anschluss einer Schlüsselschalterzone
3.5 Anschluss der Eingänge
3.6 Anschluss eines Ausgangs mit Relais
3.7 Einschalten und erste Prüfung
A TRIKDIS átjelző elindítása

4. Programmierung der Alarmzentrale

4.1 Anschluss an Datenbus oder serielle Schnittstelle
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Anschluss an die Telefonleitung (TIP/RING)
4.2.1 Programmierung des Wählgeräts der Honeywell Vista
4.2.2 Das Wählgerät der UTC Interlogix (Caddx) NX

5. Fernsteuerung mit der App Protegus 2

5.1 Gerät hinzufügen
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Scharf- und Unscharfschalten mit einem Ausgang

5.3 Scharf- und Unscharfschalten aus der App

6. Die Einstellungen im Detail

6.1 Verbindung mit dem Kommunikator

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Empfängerkanäle (CMS settings)

6.4.2 Test, PING und die Reihenfolge der Verbindungen

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 und SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Wiederherstellen der Werkseinstellungen

7. Fernprogrammierung

8. Funktionsprüfung des Kommunikators

9. Firmware-Aktualisierung

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

Der GET ist der **Ethernet- und 4G-Kommunikator** von Trikdis: Er überträgt die Ereignisse der Alarmzentrale über das kabelgebundene lokale Netzwerk (LAN) oder über das Mobilfunknetz an die Leitstelle und in die App Protegus 2. Er lässt sich auf zwei Arten mit der Zentrale verbinden: **direkt**, an den Datenbus oder die serielle Schnittstelle der Zentrale (bei Zentralen von DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange und Honeywell), oder an das **Telefonwählgerät (TIP/RING) jeder Zentrale**, die ihre Ereignisse im Format Contact ID mit DTMF-Tönen sendet. Der Kommunikator überträgt die vollständige Ereignisinformation (Code, Bereich, Zone oder Benutzer) an die Leitstelle. Mit der App Protegus 2 steuert der Benutzer die Anlage aus der Ferne und erhält Benachrichtigungen über die Ereignisse; die App arbeitet mit jeder Zentrale, die der Kommunikator unterstützt, unabhängig vom Hersteller der Zentrale. Die Übertragung an die Leitstelle und Protegus 2 lassen sich gleichzeitig nutzen. Diese Anleitung wurde für den GET-Kommunikator mit LTE-Modem (4G) erstellt; die Unterschiede zwischen GET, GT und GT+ fasst Abschnitt 1.2 zusammen.

1.1 Wozu er dient, wie er funktioniert

- **Er meldet an die Leitstelle.** Die Ereignisse sendet er über eine IP-Verbindung, über das kabelgebundene Netzwerk oder das Mobilfunknetz, an den Software- oder Hardware-Empfänger von Trikdis (Protokoll TRK8) – diese arbeiten mit jeder Leitstellensoftware zusammen –, an einen SIA-DC-09-Empfänger oder an einen SUR-GARD-Empfänger (TL150). Gegenüber einem SUR-GARD-Empfänger wandelt er die von der Zentrale empfangenen Contact-ID-Codes in SIA-Codes um; die Umwandlungstabelle steht im Anhang der englischsprachigen Dokumentation auf docs.trikdis.com. Die Verbindung zum Empfänger prüft er alle 30 Sekunden (oder im eingestellten Intervall) mit einer PING-Nachricht; fällt der primäre Kanal aus, wechselt er auf den Ersatzkanal. Mit einem parallelen Kanal gehen die Ereignisse gleichzeitig an zwei Empfänger. Die Verbindungswege – LAN, SIM1, SIM2 – können Sie in eine Reihenfolge bringen: Funktioniert der Hauptweg nicht, wechselt der Kommunikator auf den Ersatzweg (Abschnitt 6.4.2). Ist auch der Protegus-Dienst eingeschaltet, erhält zuerst die Leitstelle das Ereignis und erst danach die App der Benutzer.
- **Er benachrichtigt den Benutzer.** Die App Protegus 2 meldet die Ereignisse als Push-Nachricht mit eigenem Signalton; der Benutzer kann aus der App scharf und unscharf schalten und die angeschlossenen Geräte schalten (Beleuchtung, Tor, Lüftung, Heizung, Bewässerung usw.). In der App haben Administrator, Errichter und Benutzer unterschiedliche Rechte. Der GET sendet keine SMS- und keine Anrufbenachrichtigungen: Die Benachrichtigung kommt über die App Protegus 2.
- **Er steuert die Zentrale direkt.** Am Datenbus oder an der seriellen Schnittstelle angeschlossen, sieht der Kommunikator auch die Bereichs- und Zonenzustände der Zentrale, und der Benutzer schaltet mit seinem eigenen Bedienteilcode aus Protegus 2 scharf und unscharf – dafür ist keine Schlüsselschalterzone nötig.
- **Er hat eigene Ein- und Ausgänge.** Zwei I/O-Klemmen mit Doppelfunktion lassen sich als Eingang (IN) oder als steuerbarer Ausgang (OUT) verwenden; werkseitig sind beide Ausgänge. Die Ausgänge lassen sich aus der App Protegus 2 schalten. Die Klemmen **A 485** und **B 485** werden beim GET nicht verwendet; ein RS485-Erweiterungsmodul kann an den GET nicht angeschlossen werden.
- **Er lässt sich mit zwei Werkzeugen einrichten.** Die Einstellungen können mit dem unter Windows laufenden Programm TrikdisConfig (über ein USB-C-Kabel oder aus der Ferne) und – mit Firmware 1.08 oder neuer – auch aus der App Protegus 2 (Settings → Advanced settings) vorgenommen werden. Die Einstellungen lassen sich in einer Datei speichern und in andere Kommunikatoren schreiben. Es gibt

zwei Zugriffsebenen: die des Administrators der Leitstelle und die des Errichters. Der Kommunikator lässt sich auch aus der Ferne einrichten, und auch seine Firmware kann aus der Ferne aktualisiert werden.

Den Aufbau des Systems zeigt die folgende Abbildung: Die Alarmzentrale ist an den Kommunikator angeschlossen, der Kommunikator erreicht das Internet auf zwei Wegen – über das Mobilfunknetz (LTE) oder über den Router (LAN) –, von dort den Empfänger der Leitstelle (und dessen Software) und den Protegus-Server; der Benutzer sieht die Anlage in der App Protegus 2.

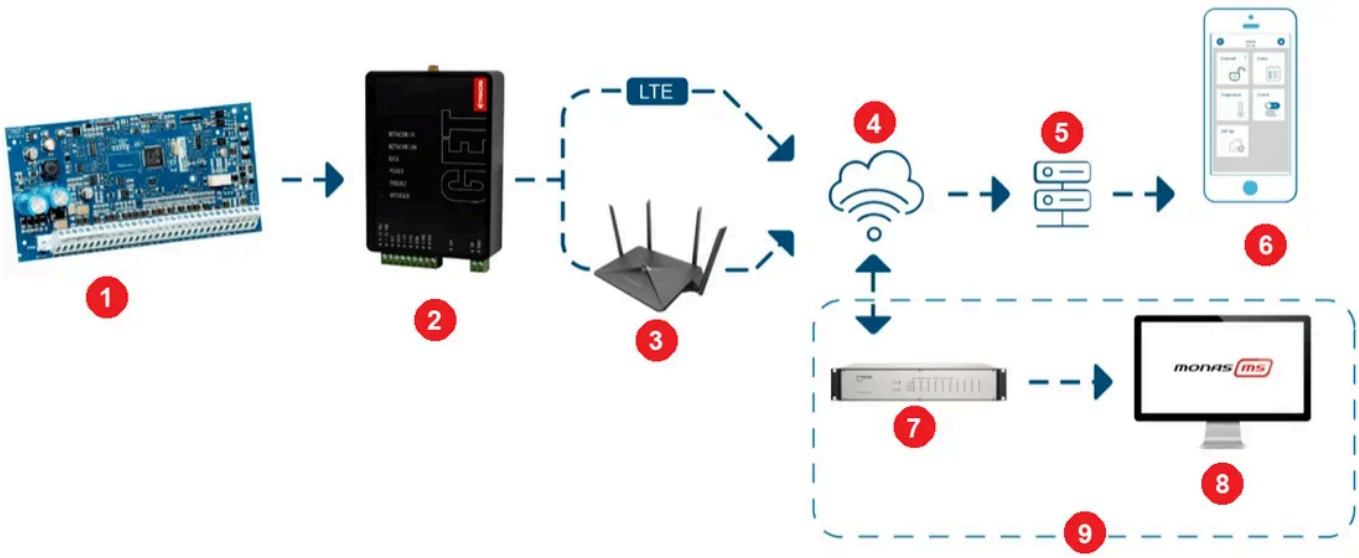


Abbildung 1. Die Stellung des Kommunikators im System: Alarmzentrale → GET → Mobilfunknetz (LTE) oder Router (LAN) → Internet → Empfänger der Leitstelle und Protegus-Server → App Protegus 2.

- 1 Alarmzentrale („Alarm panel“)
- 2 LTE-Kommunikator GET („LTE communicator“)
- 3 Router („Router“)
- 4 Internet („Internet“)
- 5 Protegus-Server („Protegus server“)
- 6 Telefon mit der App Protegus („Phone with Protegus software“)
- 7 Empfänger der Leitstelle („Receiver“)
- 8 Leitstellensoftware („Monitoring software“)
- 9 die Leitstelle des Sicherheitsunternehmens („Monitoring station in security company“) – im gestrichelten Rahmen

1.2 Varianten: GET, GT und GT+

Der GET ist das Geschwistermodell der Kommunikatoren GT und GT+ mit Ethernet-Anschluss: Anschluss und Programmierung der Alarmzentrale, die Liste der kompatiblen Zentralen, das Modem, die Übertragungsprotokolle und die Nutzung von Protegus 2 sind gleich, deshalb ist auch die Kapitelfolge der Anleitungen der drei Kommunikatoren dieselbe. Die Unterschiede fasst die folgende Tabelle zusammen.

	GET	GT	GT+
Netzwerkverbindung	**LTE (4G) und Ethernet (LAN, RJ45)**; die Reihenfolge der Verbindungswege ist einstellbar (Main / Backup / Backup 2: LAN, SIM1, SIM2; Abschnitt 6.4.2)	LTE (4G)	LTE (4G)

	GET	GT	GT+
SIM-Karte	**2 Nano-SIM-Halter** (SIM1, SIM2); eine oder zwei Karten können eingesetzt werden	1 Nano-SIM	1 Nano-SIM
Versorgungsspannung	10–18 V DC	10–18 V DC	10–32 V DC
Stromaufnahme	höchstens 100 mA im Ruhezustand, 300 mA beim Senden von Daten	höchstens 100 / 200 mA	höchstens 100 / 200 mA
Abmessungen, Gewicht	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g
Klemmen	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; separate **LAN**-Buchse (RJ45) sowie TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Werkseinstellung der I/O-Klemmen	Ausgang (OUT)	Eingang (IN, NO)	Eingang (IN, NO)
RS485-Bus, Erweiterungsmodul iO-8	die Klemmen A 485 / B 485 werden **nicht verwendet**; kein Erweiterungsmodul anschließbar	bis zu 4 iO-8	bis zu 4 iO-8
LEDs	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (nicht verwendet)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Blinksignale der LED TROUBLE	1 = physische LAN-Verbindung (Kabel), 2 = SIM1-Fehler, 3 = SIM2-Fehler, 7 = Zentrale	1–8 (SIM, PIN, APN, Netz, Empfänger, Zentrale, ICCID)	1–8
SMS und Anruf	keine SMS-Benachrichtigung, keine SMS-Befehle und kein Anruf: Benachrichtigung und Steuerung erfolgen über Protegus 2	SMS- und Anrufbenachrichtigung, SMS-Befehle	SMS- und Anrufbenachrichtigung, SMS-Befehle
DSC-Zentrale gleichzeitig am Datenbus und an den Klemmen TIP/RING	nein	nein	ja
Einstellung für den TIP/RING-Anschluss (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (auch **3. MANUAL** wählbar)
Einrichtung aus der App Protegus 2	ja (Advanced settings, ab Firmware 1.08)	TrikdisConfig	TrikdisConfig
Ereignisspeicher	60 Ereignisse	keine Angabe	keine Angabe

	GET	GT	GT+
Interne Meldungen (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	wie beim GT
Modem, Übertragungsprotokolle (TRK8, DC-09, TL150), Verschlüsselung, kompatible Zentralen, Anschlusspläne, Protegus 2	gleich	gleich	gleich

Alle drei Kommunikatoren werden mit denselben drei Modemtypen gefertigt; für den europäischen Markt ist die europäische Variante (EU) die richtige. Den Modemtyp und die Hardwarevariante finden Sie in der Statusleiste von TrikdisConfig (**Device**, **HW**) und auf dem Etikett des Geräts.

Modem	Netz und Frequenzbänder
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (Lateinamerika)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Kompatible Alarmzentralen

Die folgenden Zentralen lassen sich direkt, über den Datenbus oder die serielle Schnittstelle, an den Kommunikator anschließen. Die Spalte „Direkte Steuerung“ zeigt, ob der Benutzer aus Protegus 2 ohne weitere Verdrahtung mit seinem eigenen Bedienteilcode scharf und unscharf schalten kann; wo das nicht möglich ist, liest der Kommunikator die Ereignisse vom Bus, und für die Steuerung ist eine Schlüsselschalterzone nötig (Abschnitt 3.4).

Hersteller	Typ	Anschluss	Direkte Steuerung
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	Datenbus (Keybus)	ja
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	serielle Schnittstelle (Kabel EX-CRP2.4) oder Keybus + TIP/RING	ja
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	serielle Schnittstelle (Kabel EX-CRP2.4) oder Keybus + TIP/RING	ja
Paradox	Digiplex EVO192, EVOHD, EVOHD+	serielle Schnittstelle (Kabel EX-CRP2.4)	ja
Paradox	Digiplex EVO48	serielle Schnittstelle (Kabel EX-CRP2.4)	nein
Paradox	Spectra 1727, 1728, 1738; Esprit E55	serielle Schnittstelle (Kabel EX-CRP2.4)	nein
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	Datenbus	ja

Hersteller	Typ	Anschluss	Direkte Steuerung
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	serielle Schnittstelle (Kabel EX-CRP4)	ja
InnerRange	Inception, Integriti	serielle Schnittstelle (mit dem Kabel des Zentralenherstellers)	nein
Honeywell	Ademco Vista-15, Vista-20, Vista-48	Datenbus	ja

- Die Firmware direkt gesteuerter **Paradox**-Zentralen muss mindestens **V.4** sein. Bei den neueren Paradox-Zentralen (SP+, MG+, EVOHD+) kann die serielle Schnittstelle werkseitig gesperrt sein; die Freischaltung behandelt Abschnitt 4.1.2. Die Zentralen Spectra SP / SP+ und Magellan MG / MG+ lassen sich statt an die serielle Schnittstelle auch gleichzeitig an den Datenbus (Keybus) und an die Klemmen TIP/RING anschließen – dafür ist die kostenpflichtige Freischaltung nicht nötig, aber die Firmware des Kommunikators muss mindestens 1.21 sein (Abschnitt 3.3.3).
- Die Zentralen **aller anderen Hersteller** werden über ihr Telefonwählgerät (TIP/RING) angeschlossen, wenn dieses die Ereignisse im Format Contact ID mit DTMF-Wahl sendet; in diesem Fall ist für die Steuerung eine Schlüsselschalterzone nötig.
- Welcher Trikdis-Kommunikator und welcher Anschluss zu Ihrer Zentrale passt, können Sie in der Kompatibilitätssuche nachsehen.

1.4 Die Teile des Kommunikators

Die Leiterplatte des Kommunikators sitzt in einem schwarzen Kunststoffgehäuse; die Frontabdeckung lässt sich abnehmen (sie ist eingerastet), die Klemmleiste lässt sich abziehen. Die LAN-Buchse und die Klemmen TIP/RING sind an der Seite des Gehäuses durch eine eigene Öffnung zugänglich.

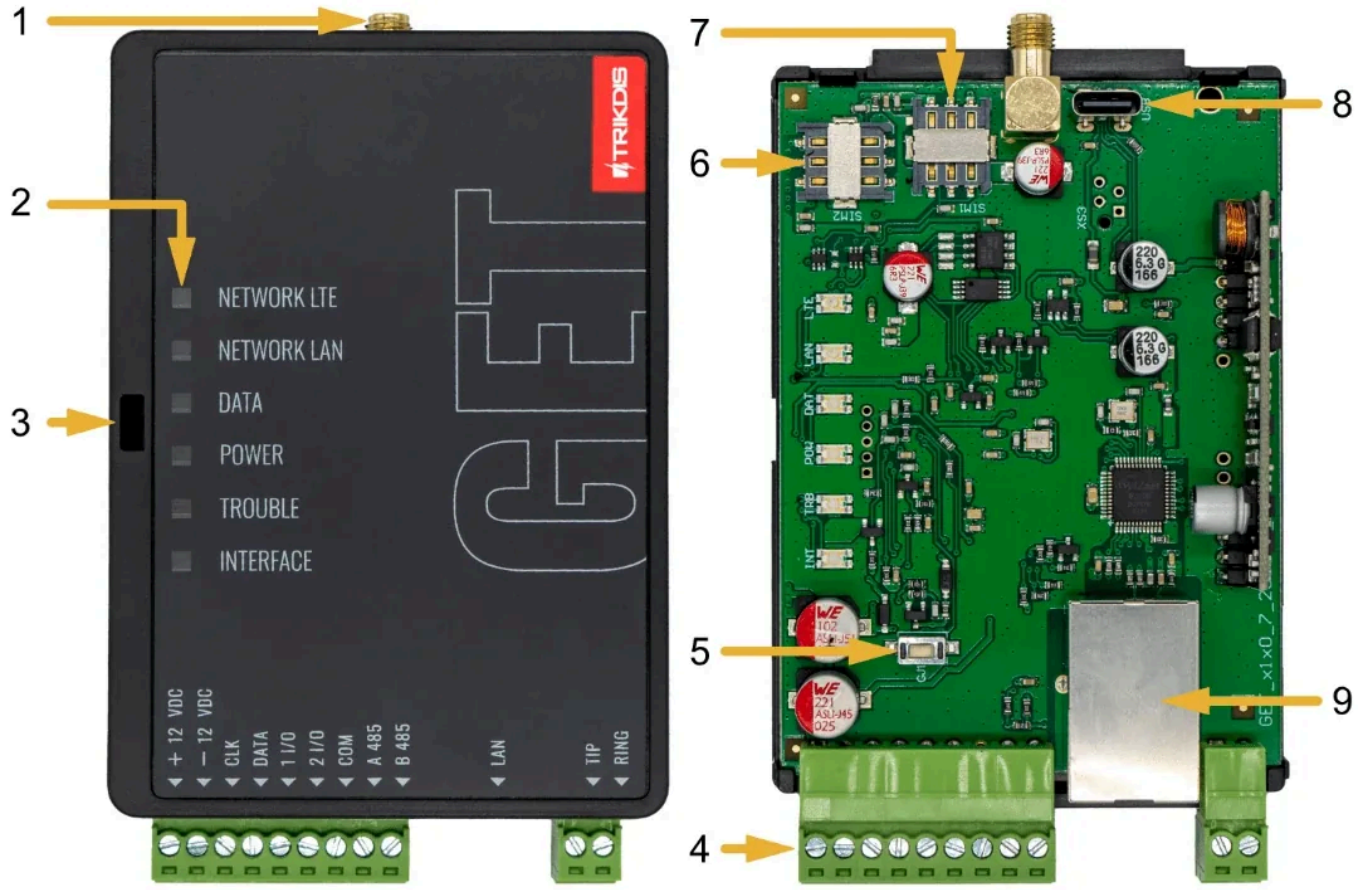


Abbildung 2. Die Teile des Kommunikators von vorn (links) und bei geöffnetem Gehäuse (rechts).

- 1 SMA-Anschluss der Mobilfunkantenne
- 2 LED-Anzeigen (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Öffnung zum Abnehmen der Frontabdeckung
- 4 Abnehmbare Klemmleiste für die externen Anschlüsse
- 5 Taste RESET
- 6 Halter der SIM2-Karte
- 7 Halter der SIM1-Karte
- 8 USB-C-Buchse zum Programmieren
- 9 Ethernet-Buchse (LAN, RJ45)

Die Klemmleiste lässt sich abziehen: So kann das Gerät mit einem Handgriff stromlos gemacht oder neu gestartet werden, es ist beim Verdrahten leichter zu handhaben, und zum Programmieren über USB kann es zum Computer gebracht werden.

1.5 Klemmen

Klemme	Funktion
+12 VDC	Versorgung, positiv: +10–18 V DC
–12 VDC	Versorgung, 0 V
CLK	Serieller Bus oder Datenbus (Takt) für den direkten Anschluss der Zentrale
DATA	Serieller Bus oder Datenbus (Daten) für den direkten Anschluss der Zentrale
1 I/O	Ein-/Ausgang 1 (Werkseinstellung: Ausgang, OUT)
2 I/O	Ein-/Ausgang 2 (Werkseinstellung: Ausgang, OUT)
COM	Gemeinsamer (negativer) Punkt für die Ein- und Ausgänge

Klemme	Funktion
A 485	Nicht verwendet
B 485	Nicht verwendet (das Gegenstück zu A 485)
LAN	Ethernet-Buchse (lokales Netzwerk, RJ45)
TIP	Klemme TIP des Telefonwählgeräts der Alarmzentrale
RING	Klemme RING des Telefonwählgeräts der Alarmzentrale

In den Anschlussplänen sind die Versorgungsklemmen mit **+DC** und **–DC** bezeichnet (am Gerät +12 VDC / –12 VDC), die RS485-Klemmen mit **A RS485** / **B RS485** (am Gerät A 485 / B 485). Die Beschriftung der Klemmleiste steht auch auf der Frontabdeckung.

1.6 LED-Anzeigen

Die LEDs auf der Frontabdeckung sind die wichtigsten Hilfsmittel bei der Inbetriebnahme und der Fehlersuche. Lesen Sie sie zusammen: POWER zeigt die Versorgung, NETWORK LTE das Mobilfunknetz, NETWORK LAN das kabelgebundene Netzwerk, TROUBLE einen Fehler; die LED INTERFACE hat beim GET keine Funktion.

NETWORK LTE – Verbindung zum Mobilfunknetz

Anzeige	Bedeutung
aus	Keine Verbindung zum Mobilfunknetz
blinkt gelb	Verbindung mit dem Mobilfunknetz wird aufgebaut
leuchtet grün, blinkt gelb	Mit dem Mobilfunknetz verbunden; die Anzahl der gelben Blinkimpulse ist der **Signalpegel**: bei 4G bedeuten 3 Blinkimpulse ein ausreichendes Signal

NETWORK LAN – Verbindung zum kabelgebundenen Netzwerk

Anzeige	Bedeutung
aus	Keine Verbindung zum Computernetzwerk
leuchtet grün	Mit dem Computernetzwerk verbunden

DATA – Datenverkehr

Anzeige	Bedeutung
aus	Keine Ereignisse warten auf das Senden
leuchtet grün	Im Speicher warten Ereignisse auf das Senden
blinkt grün	Datenübertragung zwischen Kommunikator und Computer (während der Programmierung)

Schnellprüfung

Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im

Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

POWER – Versorgungsspannung

Anzeige	Bedeutung
aus	Keine Versorgung, oder die Versorgung ist getrennt
leuchtet grün	Eingeschaltet, die Versorgungsspannung ist in Ordnung
leuchtet gelb	Unzureichende Versorgungsspannung (11,5 V oder weniger)
leuchtet grün, blinkt gelb	Bereit zum Programmieren (während der Programmierung)
leuchtet gelb (während der Programmierung)	Keine Verbindung zum Computer

TROUBLE – Fehler

Anzeige	Bedeutung
aus	Kein Fehler
1 roter Blinkimpuls	Fehler in der physischen Verbindung des kabelgebundenen Netzwerks (PHY Link) – prüfen Sie das LAN-Kabel
2 rote Blinkimpulse	Fehler der SIM1-Karte
3 rote Blinkimpulse	Fehler der SIM2-Karte
7 rote Blinkimpulse	Die Verbindung zur Alarmzentrale ist unterbrochen (serieller Bus)

INTERFACE – beim GET nicht verwendet.

1.7 Technische Daten

Parameter	Wert
Netzwerkverbindung	LTE (4G) und Ethernet (LAN)
Verbindung zur Alarmzentrale	serieller Bus, Datenbus (Keybus) oder Telefonleitung (TIP/RING, Contact ID, DTMF)
Ein-/Ausgänge	2 I/O mit Doppelfunktion: als Eingang NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (Abschlusswiderstand 2,2 kΩ); als Ausgang Open Collector (OC), max. 0,15 A / 30 V DC
Modem	EG915U-EU (Europa), EG915U-LA (Lateinamerika) oder BG95-M5 (LTE Cat M1) – die Frequenzbänder listet die Tabelle in Abschnitt 1.2 auf
SIM-Karte	2 Nano-SIM-Halter (SIM1, SIM2)
Versorgungsspannung	10–18 V DC
Stromaufnahme	höchstens 100 mA im Ruhezustand; höchstens 300 mA beim Senden von Daten
Übertragungsprotokolle	TRK8, DC-09_2007, DC-09_2012, TL150
Verschlüsselung	AES-128
Ereignisspeicher	60 Ereignisse

Parameter	Wert
Programmierung	TrikdisConfig (Windows) über ein USB-C-Kabel oder aus der Ferne; App Protegus 2 (ab Firmware 1.08)
Betriebsumgebung	−10 … +50 °C, max. 80 % relative Luftfeuchtigkeit (bei +20 °C)
Abmessungen	113 × 70 × 25 mm
Gewicht	110 g

2. Schnelle Inbetriebnahme

Die Einstellungen des Kommunikators lassen sich mit zwei Werkzeugen vornehmen: mit dem unter Windows laufenden Programm **TrikdisConfig** – über ein USB-C-Kabel oder aus der Ferne – und **aus der App Protegus 2** (Settings → Advanced settings). In diesem Kapitel beschreiben wir den kürzesten Weg: welche Einstellungen nötig sind, damit der Kommunikator Ereignisse an die Leitstelle sendet und die Anlage aus der App Protegus 2 steuerbar ist. Zu jedem Schritt geben wir den Pfad in der App und in TrikdisConfig an; die ausführliche Erklärung der Einstellungen enthält Kapitel 6.

2.1 Vorbereitung

Was Sie benötigen

USB-C-Kabel zum Programmieren · mindestens 4-adriges Kabel zwischen Kommunikator und Zentrale · für die serielle Schnittstelle von Paradox das Kabel CRP2.4 · flacher Schraubendreher 2,5 mm · eine Mobilfunkantenne mit passendem Gewinn, wenn die Netzabdeckung am Standort schwach ist · aktive SIM-Karte (eine oder zwei; die PIN-Abfrage lässt sich ausschalten), wenn Sie das Mobilfunknetz nutzen · Ethernet-Kabel bis zum Router oder Switch, wenn Sie das kabelgebundene Netzwerk nutzen · die Errichteranleitung der Alarmzentrale.

Das nötige Zubehör bestellen Sie separat beim Händler.

Einrichtung mit TrikdisConfig. Sie richten das Gerät auf dem Tisch ein, vor dem Anschließen; vor Ort muss es danach nur noch angeschlossen werden.

1. Laden Sie die Software TrikdisConfig herunter und installieren Sie sie. Geben Sie auf der Website des Herstellers (www.trikdis.com) in das Suchfeld „TrikdisConfig“ ein.

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. Öffnen Sie das Gehäuse des Kommunikators mit einem flachen Schraubendreher: Stecken Sie den Schraubendreher oben in den Spalt neben der Antenne und hebeln Sie nach außen, danach unten an der Öffnung nach unten. Die Abbildung zeigt auch die Lage der USB-C-Buchse am Rand der Leiterplatte.

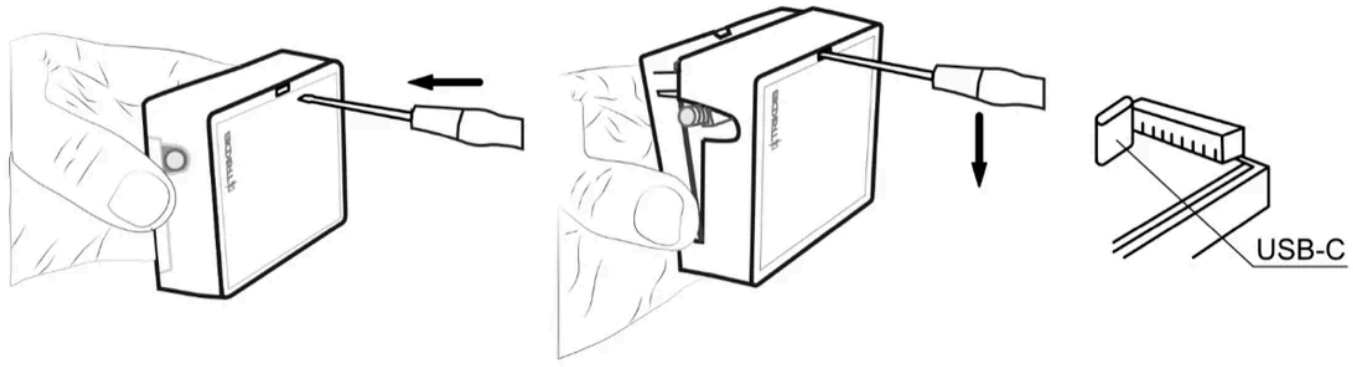


Abbildung 3. Abnehmen der Frontabdeckung mit einem flachen Schraubendreher; der vergrößerte Ausschnitt zeigt die Lage der USB-C-Buchse.

3. Setzen Sie die Nano-SIM-Karte (oder die Karten) in den Halter ein, in der in der Abbildung gezeigten Richtung: Der Halter SIM1 liegt in der Mitte der Leiterplatte, SIM2 am Rand. Die Karte muss aktiv sein und einen mobilen Datendienst haben; schalten Sie nach Möglichkeit die PIN-Abfrage in einem Telefon aus (dann muss keine PIN in das Gerät eingetragen werden). Wenn Sie den Kommunikator nur über das kabelgebundene Netzwerk nutzen, ist keine SIM-Karte nötig.

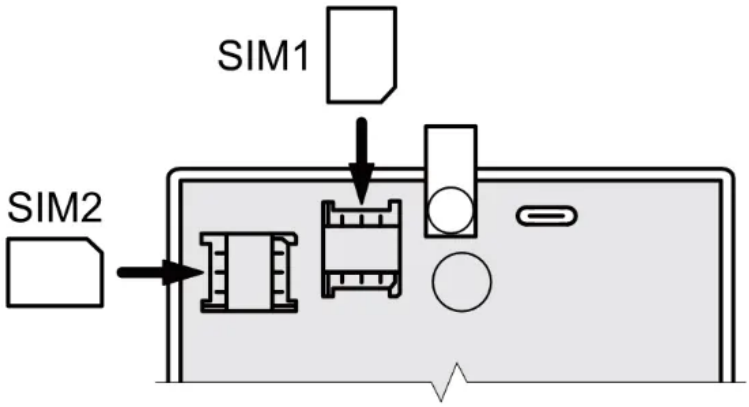


Abbildung 4. Die Lage der Halter SIM1 und SIM2 auf der Leiterplatte; die Pfeile zeigen die Einsteckrichtung der Karte.

4. Verbinden Sie den Kommunikator mit einem USB-C-Kabel mit dem Computer.

Warnung

Solange das Gerät per USB-Kabel mit dem Computer verbunden ist, befindet es sich im Programmiermodus: Der Normalbetrieb ist unterbrochen, es überwacht nicht, meldet nicht, lässt sich nicht steuern, wird über USB versorgt und startet nach dem Abziehen des Kabels neu. Das Gerät darf daher nicht frei zugänglich sein: Es gehört in ein verschlossenes Metallgehäuse mit Sabotageschutz (Tamper) oder mit einem Bewegungsmelder, der das Gehäuse überwacht. Details in den FAQ

5. Starten Sie TrikdisConfig. Das Programm erkennt das Gerät und öffnet das Programmierfenster. Klicken Sie auf die Schaltfläche **Read [F4]** (Lesen): Das Programm liest die aktuellen Einstellungen des Geräts aus. Fragt es nach einem Passwort, geben Sie den 6-stelligen Administratorcode (werkseitig `123456`) oder Errichtercode (werkseitig `654321`) ein.

Einrichtung aus der App Protegus 2. Aus der App können Sie die Einstellungen vornehmen, wenn der Kommunikator bereits online ist und Sie ihn Ihrem Protegus-Konto hinzugefügt haben (Abschnitt 5.1). Kann sich der Kommunikator noch nicht verbinden – zum Beispiel weil die SIM-Karte eine PIN verlangt oder der Anbieter einen anderen APN benötigt –, nehmen Sie die erste Einrichtung mit TrikdisConfig vor.

1. Öffnen Sie in der App die Anlage und gehen Sie in das Menü **Settings** → **Advanced settings**.
2. Beim ersten Mal warnt die App (**Proceed with Caution**): Diese Einstellungen sind für Fachleute gedacht. Tippen Sie auf **Accept the risk and continue**; mit dem Häkchen **Do not show this again** erscheint die Warnung beim nächsten Mal nicht.
3. Die App liest die Einstellungen des Kommunikators aus. Verlangt sie einen **Service Access code**, geben Sie den Protegus-Cloud-Zugangscode des Kommunikators ein (werkseitig `123456`).
4. Nehmen Sie die unten beschriebenen Einstellungen vor und tippen Sie dann auf **Write**: Die App schreibt sie in den Kommunikator.

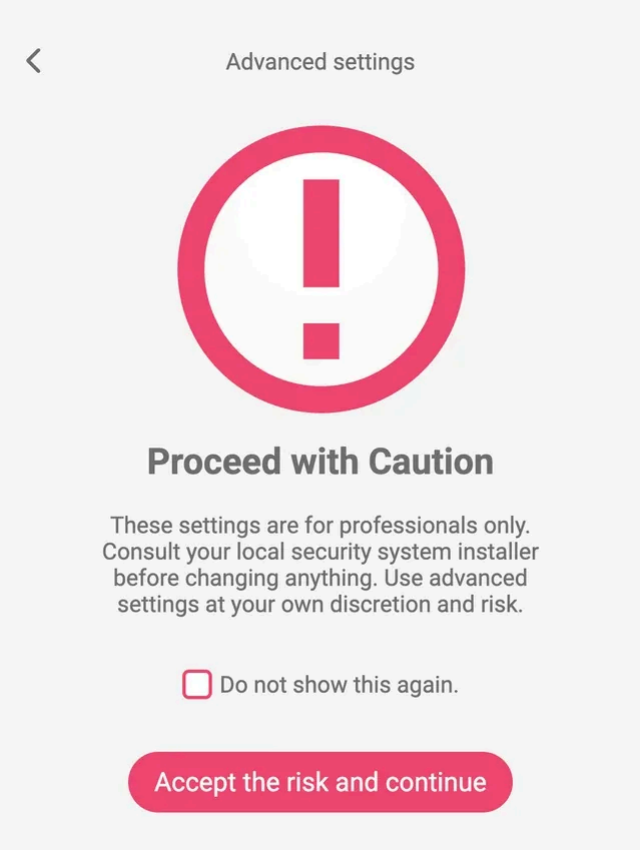


Abbildung 5. Protegus 2 – die Warnung beim ersten Öffnen von Advanced settings (Proceed with Caution) und die Schaltfläche Accept the risk and continue.

Aus der App Protegus 2 lässt sich der GET **mit Firmware 1.08 oder neuer** einrichten (die Aktualisierung beschreibt Kapitel 9).

2.2 Verbindung mit der App Protegus 2

In der App (Settings → Advanced settings):

1. **Panel settings** → **TLF** – wenn der Kommunikator an den Klemmen TIP/RING der Zentrale angeschlossen ist: **Security panel model** muss **AUTO** sein.
2. **Panel settings** → **Serial Bus** – wenn der Kommunikator am Datenbus oder an der seriellen Schnittstelle der Zentrale angeschlossen ist: Wählen Sie im Feld **Security panel model** den Typ der angeschlossenen Zentrale.
3. Schalten Sie an derselben Stelle die Option **Remote Arm/Disarm** ein, wenn die Benutzer die Zentrale aus Protegus 2 mit ihrem eigenen Bedienteilcode steuern möchten. Sie erscheint nur bei direkt steuerbaren Zentralen.

4. Für die direkte Steuerung einer Paradox-Zentrale geben Sie das **PC download password** ein, bei einer Texecom-Zentrale den **UDL passcode**; er muss mit dem in der Zentrale eingestellten Passwort übereinstimmen.
5. **User reporting** → **Cloud**: Schalten Sie die Option **Enabled** ein und ändern Sie den **Cloud access code**, wenn der Benutzer ihn beim Hinzufügen der Anlage zur App eingeben soll (werkseitig `123456`).
6. **Network settings** → **LAN** – wenn der Kommunikator am kabelgebundenen Netzwerk angeschlossen ist: Schalten Sie die Option **Use DHCP** ein.
7. **Network settings** → **SIM** und **SIM2** – für jede eingesetzte SIM-Karte: Geben Sie **SIM card PIN** und **APN** ein und prüfen Sie, ob **DNS1** und **DNS2** bei Ihrem Anbieter funktionieren.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: Legen Sie in den Feldern **Main type**, **Backup type** und **Backup type 2** fest, in welcher Reihenfolge der Kommunikator die Verbindungen **LAN**, **SIM** (SIM1) und **SIM2** nutzt.
9. Tippen Sie auf **Write**.

In TrikdisConfig. Legen Sie zuerst auf der Seite **Panel settings** fest, wie der Kommunikator an die Zentrale angeschlossen ist.

Wenn Sie ihn an den Telefonleitungsausgang (TIP/RING) der Zentrale anschließen: Wählen Sie im Feld **Communication protocol** den Wert **AUTO**.

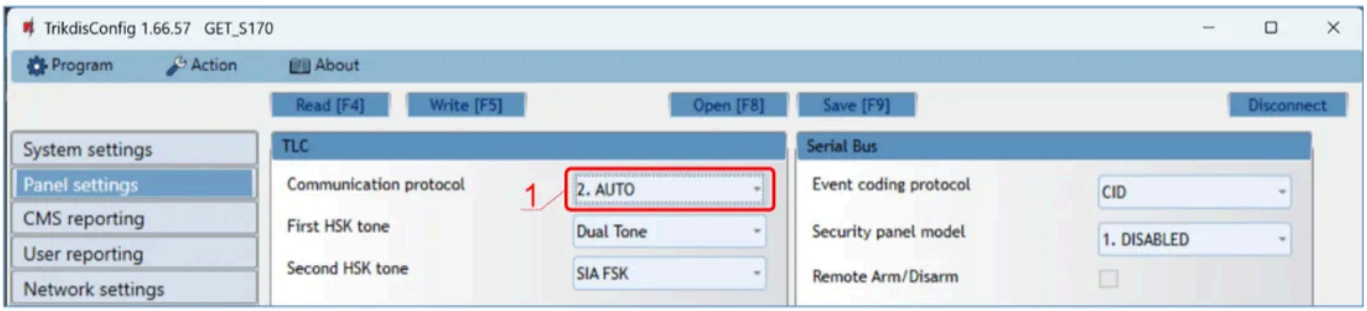


Abbildung 6. TrikdisConfig – Panel settings, Gruppe TLC.

- 1 **Communication protocol** – beim TIP/RING-Anschluss **2. AUTO**.

Wenn Sie ihn an den Datenbus oder die serielle Schnittstelle der Zentrale anschließen: Stellen Sie in der Gruppe **Serial bus** die Zentrale ein.



Abbildung 7. TrikdisConfig – Panel settings, Gruppe Serial bus.

- 2 **Security panel model** – der Typ der angeschlossenen Zentrale.
- 3 **Remote Arm/Disarm** – setzen Sie das Häkchen, wenn die Benutzer die Zentrale aus Protegus 2 mit ihrem eigenen Bedienteilcode steuern möchten. Erscheint nur bei direkt steuerbaren Zentralen.
- 4 **Security panel PC download password** – für die direkte Steuerung einer Paradox- bzw. Texecom-Zentrale das in der Zentrale eingestellte PC- bzw. UDL-Passwort; beide müssen übereinstimmen.

Für die direkte Steuerung muss auch die Alarmzentrale eingerichtet werden – das beschreibt Kapitel 4; dort finden Sie auch, wie das PC- bzw. UDL-Passwort eingegeben wird.

Aktivieren Sie danach auf der Seite **User reporting**, im Reiter **PROTEGUS Cloud**, die Cloud-Verbindung.

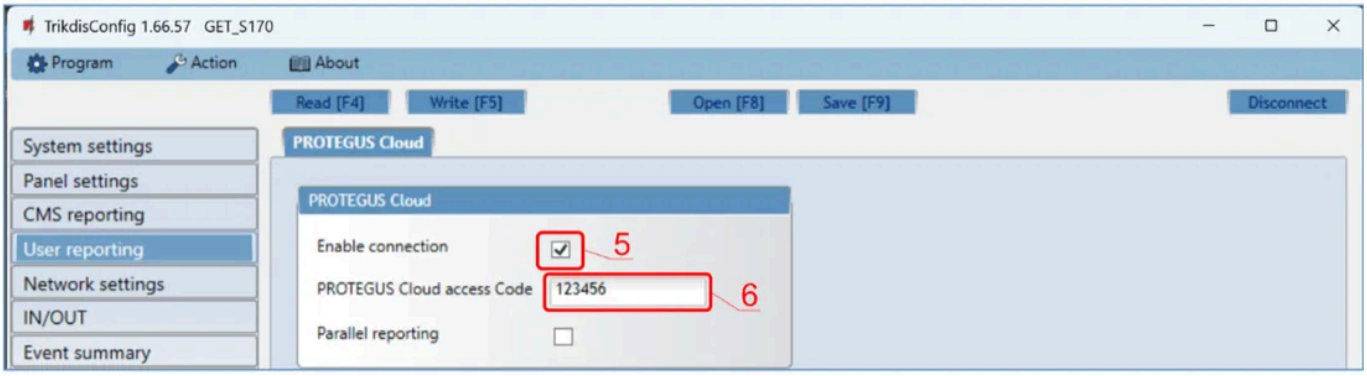


Abbildung 8. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- 5 **Enable connection** – setzen Sie das Häkchen: Es aktiviert die Verbindung mit der Protegus Cloud.
- 6 **PROTEGUS Cloud access Code** – der Zugangscode für Protegus 2 (werkseitig `123456`). Ändern Sie ihn, wenn der Benutzer ihn beim Hinzufügen der Anlage zur App eingeben soll. Wenn Sie den Code später ändern, muss er auch in der App Protegus 2 geändert werden.

Ist der Kommunikator am kabelgebundenen Netzwerk angeschlossen, setzen Sie auf der Seite **Network settings**, im Reiter **LAN**, das Häkchen bei **Use DHCP**: Der Kommunikator erhält die Netzwerkeinstellungen (Subnetzmaske, Gateway) automatisch und bekommt eine IP-Adresse.

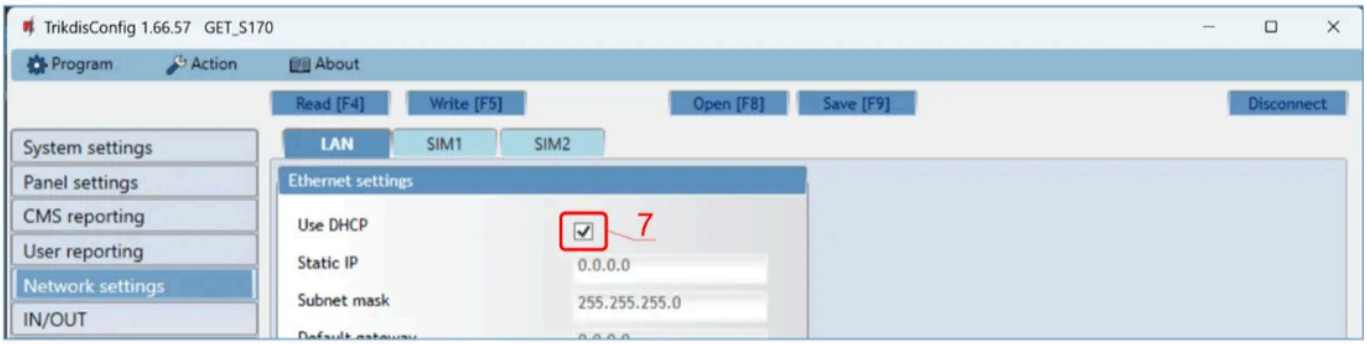


Abbildung 9. TrikdisConfig – Network settings, Reiter LAN (Ethernet settings).

- 7 **Use DHCP** – mit Häkchen erhält der Kommunikator IP-Adresse und Netzwerkeinstellungen automatisch vom Router.

Steckt eine SIM-Karte (eine oder zwei Karten) im Kommunikator, geben Sie im Reiter **SIM1** (und **SIM2**) die Daten der Karte ein.

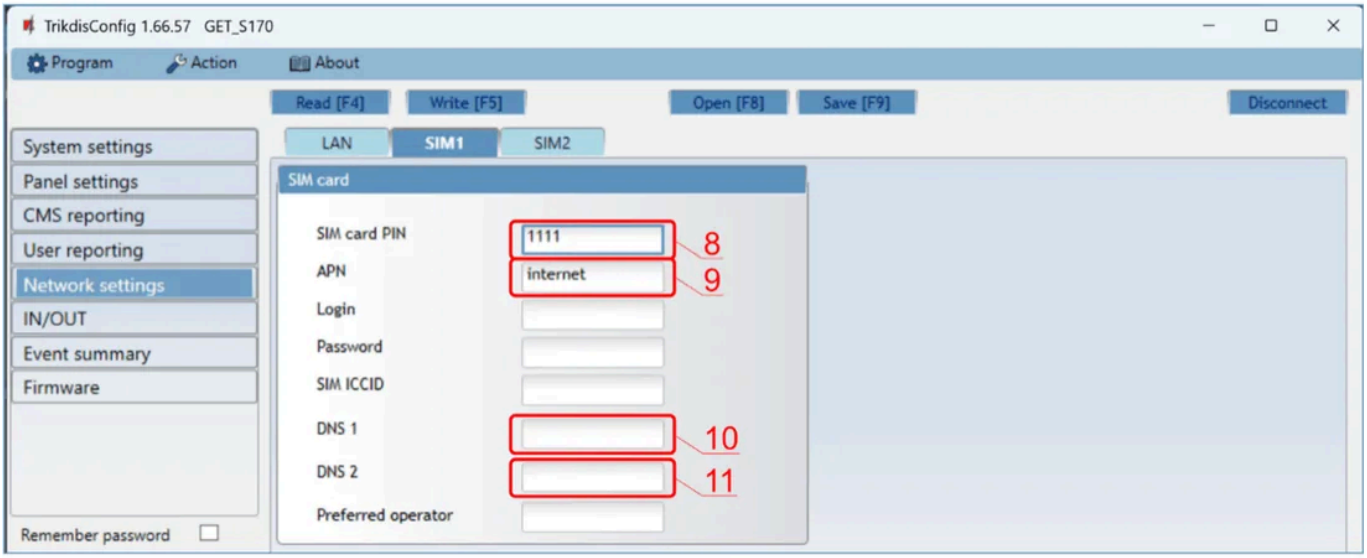


Abbildung 10. TrikdisConfig – Network settings, Reiter SIM1.

- 8 **SIM card PIN** – die PIN der Karte (ist die PIN-Abfrage ausgeschaltet, kann der Werkswert bleiben).
- 9 **APN** – der Zugangspunkt für die Datenverbindung des Anbieters (siehe unten).
- 10 **DNS 1** – primärer Nameserver; werkseitig der DNS von Google. Prüfen Sie unabhängig von den IP-Einstellungen, ob die DNS-Adressen bei Ihrem Anbieter funktionieren.
- 11 **DNS 2** – sekundärer Nameserver (werkseitig ebenfalls von Google).

Der APN (Access Point Name) ist der Zugangspunkt für die Datenverbindung des Mobilfunkanbieters; ohne ihn kann sich das Gerät über das Mobilfunknetz nicht mit dem Internet verbinden. Den genauen Wert finden Sie auf der Website des Anbieters der SIM-Karte. Die bekannten APNs europäischer Anbieter führen wir in einem eigenen Artikel: APN-Einstellung – Liste europäischer Mobilfunkanbieter. Wenn Sie vom Anbieter keine anderen Angaben haben, probieren Sie den APN `internet`: Er ist allgemein gültig und funktioniert in den Netzen vieler Anbieter.

Für IoT- / M2M-Datenkarten (Maschine-zu-Maschine) gibt der Anbieter in der Regel **einen anderen APN als für Privatkundenkarten** an – mit dem Privatkunden-APN verbindet sich das Gerät nicht. Auch diesen Wert finden Sie im APN-Artikel, oder fragen Sie den Anbieter; wenn der Anbieter auch einen Benutzernamen und ein Passwort angibt, tragen Sie diese ebenfalls ein.

Legen Sie zum Schluss auf der Seite **CMS reporting**, im Reiter **Settings**, in der Gruppe **Reporting mode** die Reihenfolge der Verbindungen fest: Auf diesem Weg sendet der Kommunikator die Meldungen an die Leitstelle und an Protegus 2.

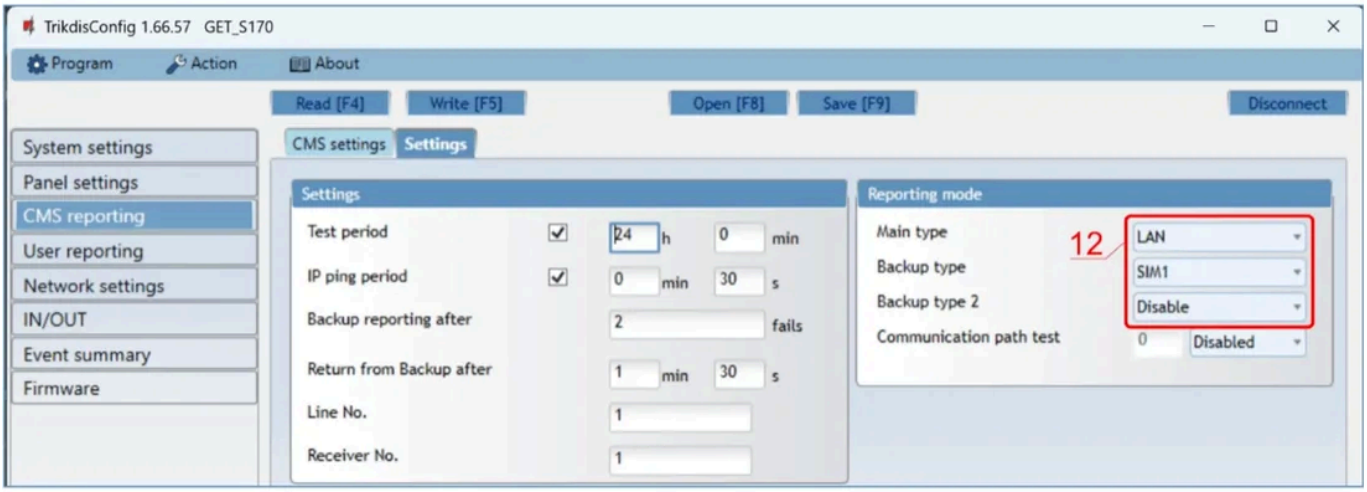


Abbildung 11. TrikdisConfig – CMS reporting, Reiter Settings, Gruppe Reporting mode (werkseitig Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type**: die Hauptverbindung (LAN, SIM1 oder SIM2); **Backup type**: die Ersatzverbindung; **Backup type 2**: die zweite Ersatzverbindung.

Die Verbindungsarten geben Sie in einer Reihenfolge an. Kann sich der Kommunikator über die Verbindung **Main type** nicht verbinden, wechselt er auf **Backup type** und so weiter. Hat die Ersatzverbindung die Meldung erfolgreich an die Leitstelle übertragen, versucht der Kommunikator nach Ablauf der eingestellten Zeit, zur Hauptverbindung zurückzukehren (Abschnitt 6.4.2).

Meldet das Gerät nicht an eine Leitstelle, ist die Einrichtung damit abgeschlossen: Drücken Sie die Schaltfläche **Write [F5]** (Schreiben), warten Sie die Bestätigung ab und ziehen Sie das USB-Kabel ab.

Vergessen Sie beim Telefonleitungsanschluss (TIP/RING) nicht, das Wählgerät der Alarmzentrale einzuschalten und einzurichten, sonst sendet die Zentrale keine Ereignisse; für die direkte Steuerung müssen auch die Zentralen von Paradox, Texecom, Caddx, InnerRange und Honeywell eingerichtet werden. Die Einrichtung der Zentrale beschreibt Kapitel 4.

2.3 Verbindung mit der Leitstelle

In der App (Settings → Advanced settings):

1. **System options** → **System general**: Geben Sie die von der Leitstelle erhaltene Objektkennung ein (**Account No.**; 0–9, A–F; `FFFE` und `FFFF` sind nicht verwendbar). Bei der Hardwarevariante **x1x1** mit Firmware **1.31** oder neuer geben Sie die Objektkennung je Kanal ein: **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** Sie erkennen es am Bildschirm: Zeigt System general nur das Feld **Time set**, verwenden Sie die Einstellung am Kanal.
2. **Panel settings** → **TLF** (TIP/RING-Anschluss): **Security panel model** muss **AUTO** sein; oder **Panel settings** → **Serial Bus** (Anschluss an Datenbus oder serielle Schnittstelle): Wählen Sie das **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel**: Schalten Sie die Option **Enabled** ein und geben Sie dann ein: **Communication type**: **IP**; Adresse (**Domain or IP**) und **Port** des Empfängers; **TCP or UDP**; **Protocol**: **TRK8** für einen Trikdis-Empfänger, **DC-09_2007** oder **DC-09_2012** für einen universellen Empfänger, **TL150** für einen SUR-GARD-Empfänger; sowie den im Empfänger eingestellten Verschlüsselungsschlüssel: beim TRK-Protokoll im Feld **TRK encryption key**, bei DC-09 schalten Sie die Option **Enable encryption key** ein und geben den **DC-09 encryption key** ein.
4. (Empfohlen) Richten Sie den **Backup channel** (Ersatzkanal) auf dieselbe Weise ein.
5. **Reporting to CMS** → **CMS settings** → **Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.

6. **Network settings** → **LAN** (kabelgebundenes Netzwerk): Schalten Sie die Option **Use DHCP** ein. **Network settings** → **SIM** und **SIM2** (für jede SIM-Karte): **SIM card PIN**, **APN**, und prüfen Sie die Felder **DNS1**, **DNS2**.
7. Tippen Sie auf **Write**.

In TrikdisConfig. Geben Sie zuerst auf der Seite **System settings** die Objektkennung ein.



Abbildung 12. TrikdisConfig – Seite System settings, Gruppe General.

- 1 **Object ID** – die von der Leitstelle erhaltene Objektkennung (6 hexadezimale Zeichen, 0–9, A–F). `FFFE` und `FFFF` sind nicht verwendbar.

Legen Sie auf der Seite **Panel settings** den Anschluss der Zentrale fest, wenn Sie das in Abschnitt 2.2 noch nicht getan haben: Beim TIP/RING-Anschluss muss **Communication protocol** auf **AUTO** stehen; beim Anschluss an Datenbus oder serielle Schnittstelle wählen Sie im Feld **Security panel model** den Typ der angeschlossenen Zentrale (Abbildungen in Abschnitt 2.2).

Stellen Sie danach auf der Seite **CMS reporting**, im Reiter **CMS settings**, im Teil **Primary channel** (primärer Kanal) die Daten des Empfängers ein. Das Bild zeigt das Fenster vor der Einrichtung: Das Feld **Communication type** des primären Kanals steht noch auf **Disable**.

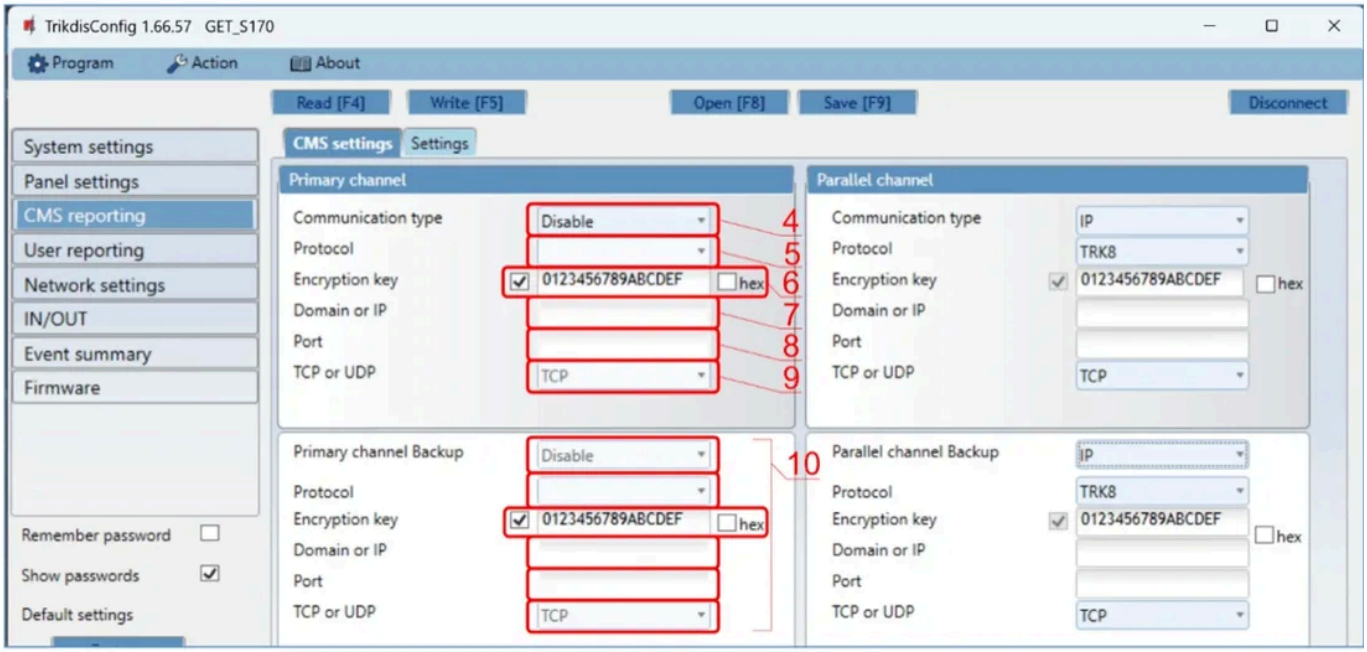


Abbildung 13. TrikdisConfig – CMS reporting, Reiter CMS settings.

- 4 **Communication type** – wählen Sie die Verbindung **IP**.
- 5 **Protocol** – **TRK8** für einen Trikdis-Empfänger, **DC-09_2007** oder **DC-09_2012** für einen universellen Empfänger, **TL150** für einen SUR-GARD-Empfänger.
- 6 **Encryption key** – der im Empfänger eingestellte Verschlüsselungsschlüssel.
- 7 **Domain or IP** – Domainname oder IP-Adresse des Empfängers.
- 8 **Port** – die Portnummer des Empfängers.
- 9 **TCP or UDP** – das Übertragungsprotokoll; richtet sich nach der Einstellung des Empfängers.
- 10 **Primary channel Backup** – Ersatzkanal für den Ausfall des primären Kanals; füllen Sie ihn genauso aus, die Angabe wird empfohlen.

Legen Sie im Reiter **Settings**, in der Gruppe **Reporting mode**, die Reihenfolge der Verbindungen fest (**Main type**, **Backup type**, **Backup type 2**), wenn Sie das in Abschnitt 2.2 noch nicht getan haben – dort finden Sie auch die Abbildung und die Beschreibung der Funktionsweise.

Geben Sie zum Schluss auf der Seite **Network settings** die Netzwerkdaten ein, wenn Sie das in Abschnitt 2.2 noch nicht getan haben: im Reiter **LAN** das Häkchen **Use DHCP**, im Reiter **SIM1** (und **SIM2**) die Daten der Karte (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Beim Protokoll **DC-09** geben Sie im Reiter **Settings** auch die Linien- und Empfängernummer ein (**Line No.**, **Receiver No.**, Abschnitt 6.4.2). Der GET meldet an die Leitstelle nur über eine IP-Verbindung – über das kabelgebundene Netzwerk oder das mobile Internet –, einen SMS-Ersatzkanal hat er nicht.

Drücken Sie am Ende der Einstellungen die Schaltfläche **Write [F5]** (Schreiben), warten Sie die Bestätigung ab und ziehen Sie das USB-Kabel ab. Damit ist das Gerät bereit zum Anschließen. Beim Telefonleitungsanschluss muss auch hier das Wählgerät der Alarmzentrale eingeschaltet und eingerichtet werden, sonst sendet die Zentrale keine Ereignisse (Kapitel 4).

3. Montage und Anschluss

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 Schritte der Montage

1. Nehmen Sie die Frontabdeckung ab (siehe Abschnitt 2.1) und ziehen Sie die Klemmleiste ab.
2. Setzen Sie die Nano-SIM-Karte – oder beide – in ihren Halter ein, falls Sie das bei der Inbetriebnahme noch nicht getan haben.
3. Nehmen Sie die Leiterplatte aus dem Gehäuseboden: Öffnen Sie die Verriegelung neben dem Antennenanschluss und heben Sie die Platine heraus (siehe Abbildung).
4. Befestigen Sie den Gehäuseboden mit Schrauben an der gewählten Stelle (in der Abbildung sind die Schraubenlöcher eingekreist) oder gemäß Abschnitt 3.2 mit dem mitgelieferten doppelseitigen Klebeband.
5. Setzen Sie die Leiterplatte wieder in den Gehäuseboden ein und stecken Sie die Klemmleiste wieder auf.
6. Schrauben Sie die Mobilfunkantenne an.
7. Setzen Sie die Frontabdeckung wieder auf.
8. Wenn Sie die Ereignisse auch über das kabelgebundene Netzwerk (LAN) an die Leitstelle senden, stecken Sie das Netzwerkkabel in die LAN-Buchse des Kommunikators.

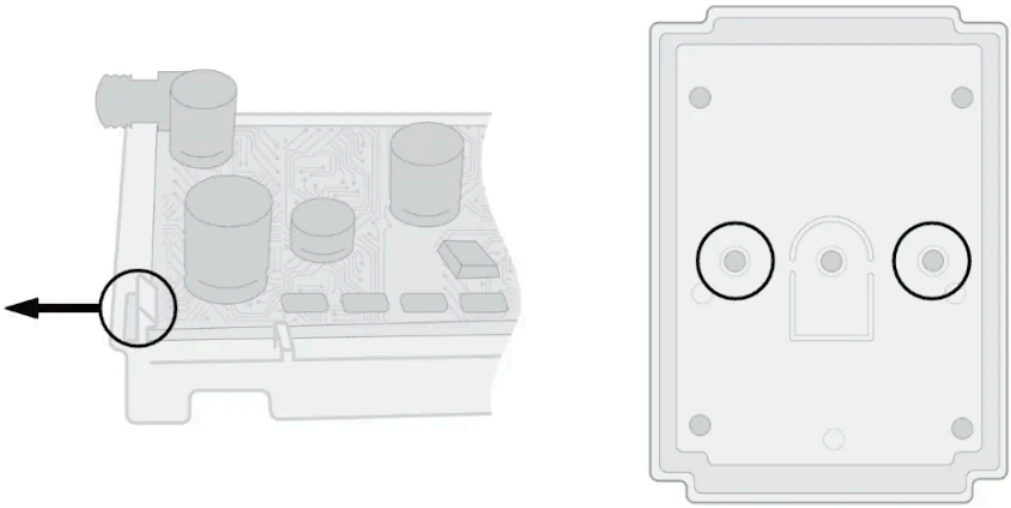


Abbildung 14. Herausnehmen der Leiterplatte aus dem Gehäuseboden (links: die Verriegelung und die Richtung zum Herausheben) und die Schraubenlöcher des Gehäusebodens (rechts).

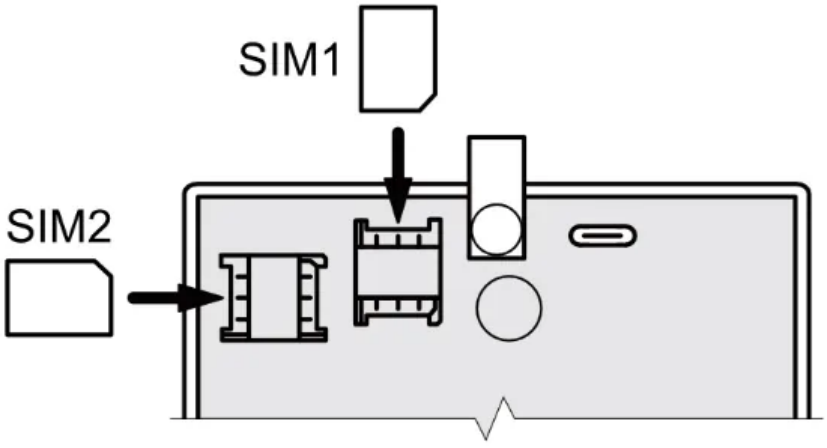


Abbildung 15. Die Lage der beiden SIM-Halter auf der Leiterplatte: SIM1 in der Mitte der Platine, SIM2 am linken Rand; die Pfeile zeigen die Einsteckrichtung der Karte.

In den Kommunikator können eine oder zwei SIM-Karten eingesetzt werden. Die Karte muss aktiv sein, und für die IP-basierte Nutzung muss die mobile Datenverbindung auf ihr funktionieren. Wenn TrikdisConfig keine PIN abfragen soll, setzen Sie die Karte in ein Mobiltelefon ein und schalten Sie dort die PIN-Abfrage aus.

3.2 Unterbringung im Gehäuse der Zentrale, Antenne

Der Kommunikator muss im **durch einen Deckelsabotagekontakt geschützten Gehäuse** der Alarmzentrale untergebracht werden. Befestigen Sie ihn mit dem mitgelieferten doppelseitigen Acryl-Schaumklebeband in Industriequalität an der inneren Rückwand des Gehäuses: Kleben Sie das Band auf eine saubere, trockene Fläche und drücken Sie es kräftig an, damit es sicher hält. Lässt das Gehäuse der Zentrale diese sichere Befestigung nicht zu, kann der Kommunikator auch in ein eigenes, sabotagegeschütztes Gehäuse montiert werden.

- **In einem Metallgehäuse** wird das Mobilfunksignal stark gedämpft. Kommt der Kommunikator in das Metallgehäuse der Zentrale, führen Sie die Antenne aus dem Gehäuse heraus oder verwenden Sie eine Antenne mit längerem Kabel.
- **Prüfen Sie vor der endgültigen Befestigung den Signalpegel**: Die Anzahl der gelben Blinkimpulse der LED NETWORK LTE muss bei 4G mindestens 3 sein (Abschnitt 1.6). Sind es weniger, suchen Sie einen besseren Platz für die Antenne oder wechseln Sie zu einer empfindlicheren, weiter entfernt platzierbaren Antenne.
- Halten Sie Antenne und Kommunikator vom Transformator der Zentrale und von Netzleitungen fern.
- Führen Sie das LAN-Kabel durch die Kabeleinführung des Gehäuses zur RJ45-Buchse an der Seite des Kommunikators; das Kabel darf nicht an den Klemmen ziehen.



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 Anschluss an die Alarmzentrale

Folgen Sie dem Plan, der zu Ihrer Zentrale passt. In den Plänen sind **+DC** und **–DC** die Versorgungsklemmen **+12 VDC** / **–12 VDC** des Kommunikators, **A RS485** / **B RS485** die Klemmen **A 485** / **B 485** (diese müssen beim GET nicht angeschlossen werden). Der Kommunikator wird über den Hilfsspannungsausgang (AUX) der

Zentrale versorgt, so dass bei einem Stromausfall der Akku der Zentrale auch den Kommunikator versorgt.

3.3.1 DSC – Datenbus (Keybus)

Schließen Sie den Keybus der DSC-Zentrale mit vier Adern an den Kommunikator an: **RED → +DC**, **BLK → –DC**, **YEL → CLK**, **GRN → DATA**.

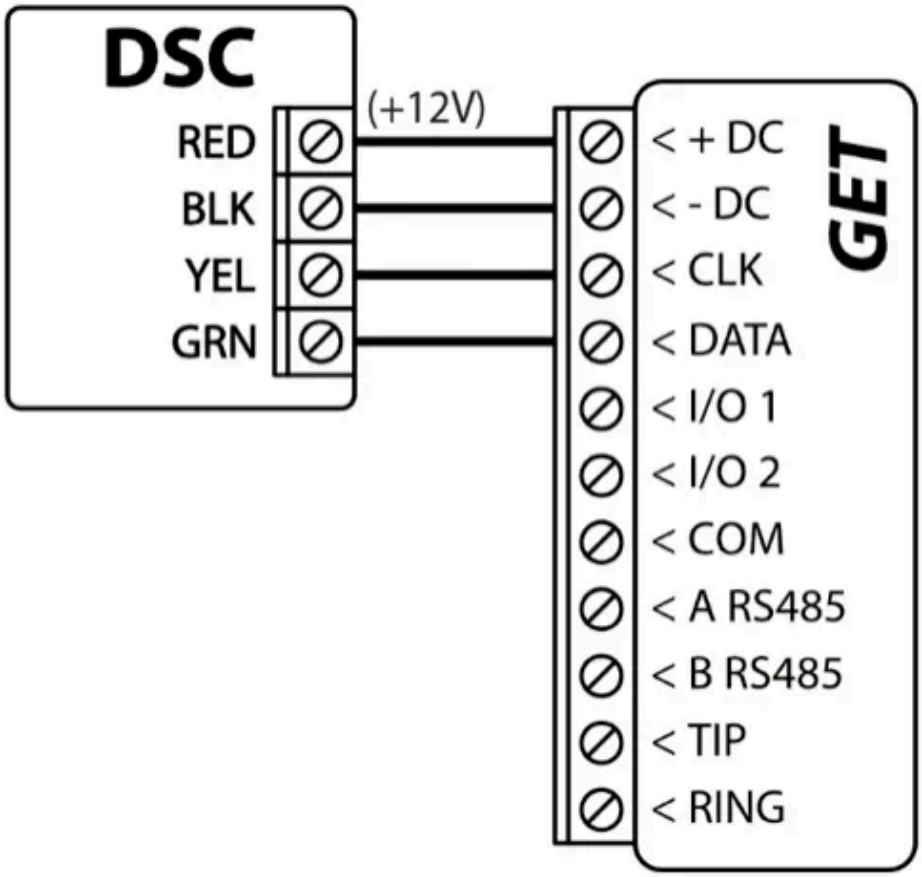


Abbildung 16. Anschluss einer DSC-Zentrale am Datenbus (Keybus, „Keypad bus"): RED → +DC, BLK → –DC, YEL → CLK, GRN → DATA.

Der GET bedient die DSC-Zentrale nur über den Datenbus; der gleichzeitige Anschluss an Keybus und Klemmen TIP/RING ist nur beim Kommunikator GT+ möglich. Nur am Keybus angeschlossen erhält der Kommunikator von der Zentrale den allgemeinen Zustand der Zonen, nicht aber den Zonentyp (Feuer, Einbruch, Wasserleck usw.), deshalb meldet er jeden Alarm **als allgemeinen Alarm mit dem Contact-ID-Code E130**. Benötigt die Leitstelle die eigenen Codes der Zentrale (zum Beispiel Feueralarm: E110), können Sie die Ereignisse über das Telefonwählgerät der Zentrale mit TIP/RING-Anschluss senden (Abschnitte 3.3.9 und 4.2); dann gibt es keine direkte Steuerung.

3.3.2 Paradox – serielle Schnittstelle

An die serielle Schnittstelle der Paradox-Zentrale wird der Kommunikator mit dem separat bestellbaren Kabel **EX-CRP2.4** angeschlossen: **rot → +DC**, **schwarz → –DC**, **gelb → CLK**, **grün → DATA**.

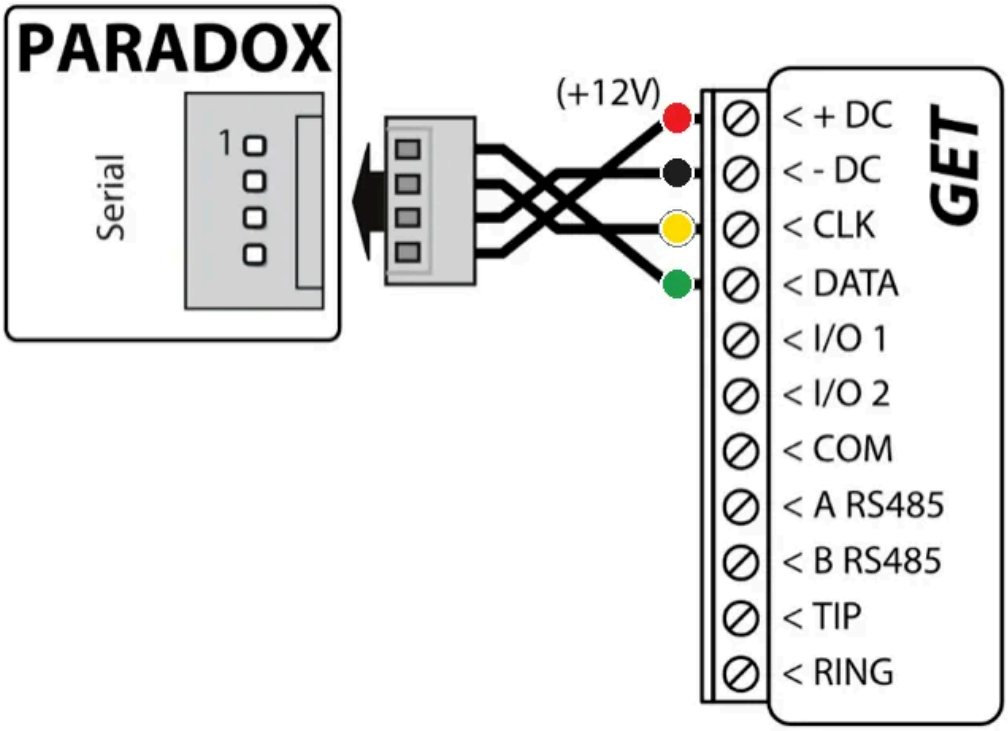


Abbildung 17. Anschluss einer Paradox-Zentrale an der seriellen Schnittstelle mit dem Kabel EX-CRP2.4 (separat zu bestellen; „Use the EX-CRP2.4 cable (ordered separately)"): rot → +DC, schwarz → −DC, gelb → CLK, grün → DATA.

- rote Ader („R - red")
- schwarze Ader („B - black")
- gelbe Ader („Y - yellow")
- grüne Ader („G - green")

Bei den neueren Paradox-Zentralen (SP+, MG+, EVOHD+) kann die serielle Schnittstelle werkseitig gesperrt sein; die Freischaltung behandelt Abschnitt 4.1.2. Bei den Zentralen Spectra SP / SP+ und Magellan MG / MG+ kann statt der seriellen Schnittstelle auch der Anschluss nach dem folgenden Abschnitt verwendet werden.

3.3.3 Paradox SP/MG – Keybus und TIP/RING

Die Zentralen Paradox Spectra SP, SP+ und Magellan MG, MG+ lassen sich statt an der seriellen Schnittstelle auch gleichzeitig an ihrem Datenbus (Keybus) und an ihren Klemmen TIP/RING anschließen: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK** sowie **TIP** → **TIP**, **RING** → **RING**. Dieser Anschluss nutzt den Keybus der Zentrale statt der seriellen Schnittstelle, deshalb ist die kostenpflichtige Freischaltung der seriellen Schnittstelle von Paradox nicht nötig.

Für diesen Anschluss muss die Firmware des Kommunikators mindestens **1.21** sein (die Aktualisierung beschreibt Kapitel 9).

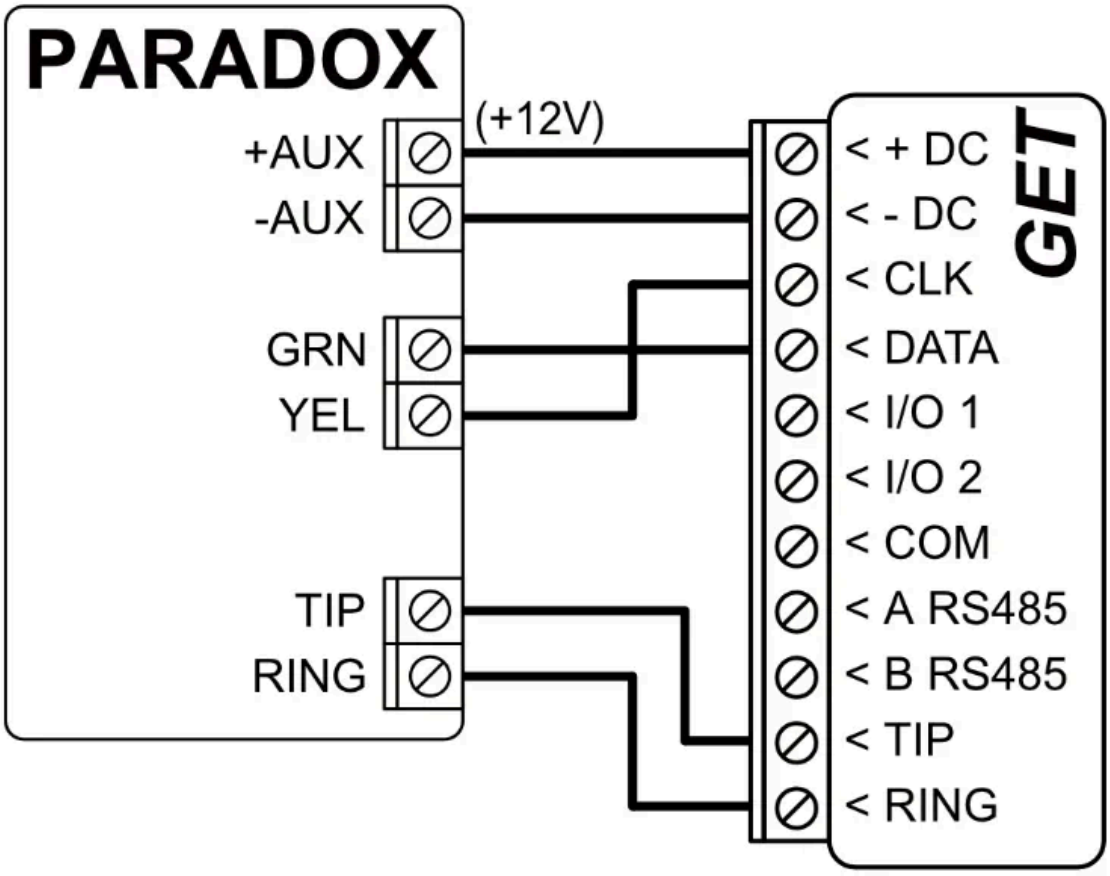


Abbildung 18. Anschluss einer Paradox-Zentrale SP / SP+ / MG / MG+ gleichzeitig am Keybus (Datenbus, „Keypad bus") und an den Klemmen TIP/RING: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Für diesen Anschluss stellen Sie auf der Seite **Panel settings** in TrikdisConfig Folgendes ein:

1. **Communication protocol**: **2. AUTO**.
2. **Security panel model**: Wählen Sie aus der Liste den Eintrag **Paradox SP+/MG+ series KeyBus** (im Bild 7. PARADOX SP+/MG+).
3. **Remote Arm/Disarm**: Setzen Sie das Häkchen, wenn die Benutzer die Zentrale aus der App Protegus 2 mit ihrem eigenen Bedienteilcode steuern möchten.
4. **Security panel PC download password**: Geben Sie für die direkte Steuerung das in der Zentrale eingestellte PC-Passwort ein; beide müssen übereinstimmen.

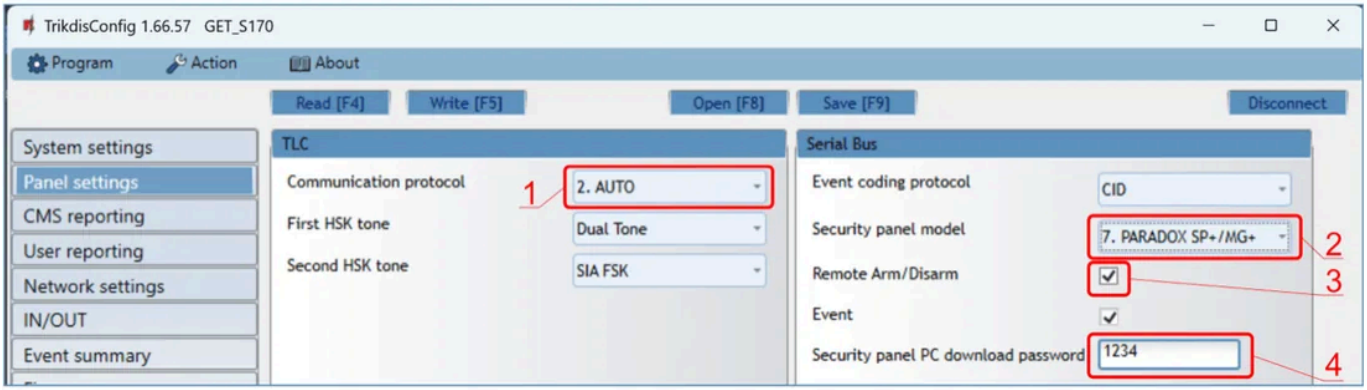


Abbildung 19. TrikdisConfig – Panel settings für den Anschluss Keybus + TIP/RING: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm mit Häkchen (3), Security panel PC download password eingegeben (4).

In der App Protegus 2 finden Sie dieselben Einstellungen auf den Seiten **Panel settings** → **TLF** (Security panel model = Communication protocol) und **Panel settings** → **Serial Bus** (Abschnitt 6.3).

Auch die Paradox-Zentrale muss programmiert werden, damit sie die Ereignisse an die Leitstelle sendet und aus Protegus 2 steuerbar ist – stellen Sie am an die Zentrale angeschlossenen Bedienteil die folgenden Speicherplätze ein:

Speicherplatz	Wert	Speicherplatz	Wert
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

Das im Speicherplatz **911** eingetragene PC-Passwort muss mit dem Feld **Security panel PC download password** des Kommunikators übereinstimmen (Abschnitt 4.1.2).

3.3.4 UTC Interlogix (Caddx) – Datenbus

Schließen Sie den Datenbus der Caddx-NetworX-Zentrale mit drei Adern an den Kommunikator an: **POS** → **+DC**, **COM** → **–DC**, **DATA** → **DATA**. Die Klemmen CLK, TIP und RING werden nicht benötigt.

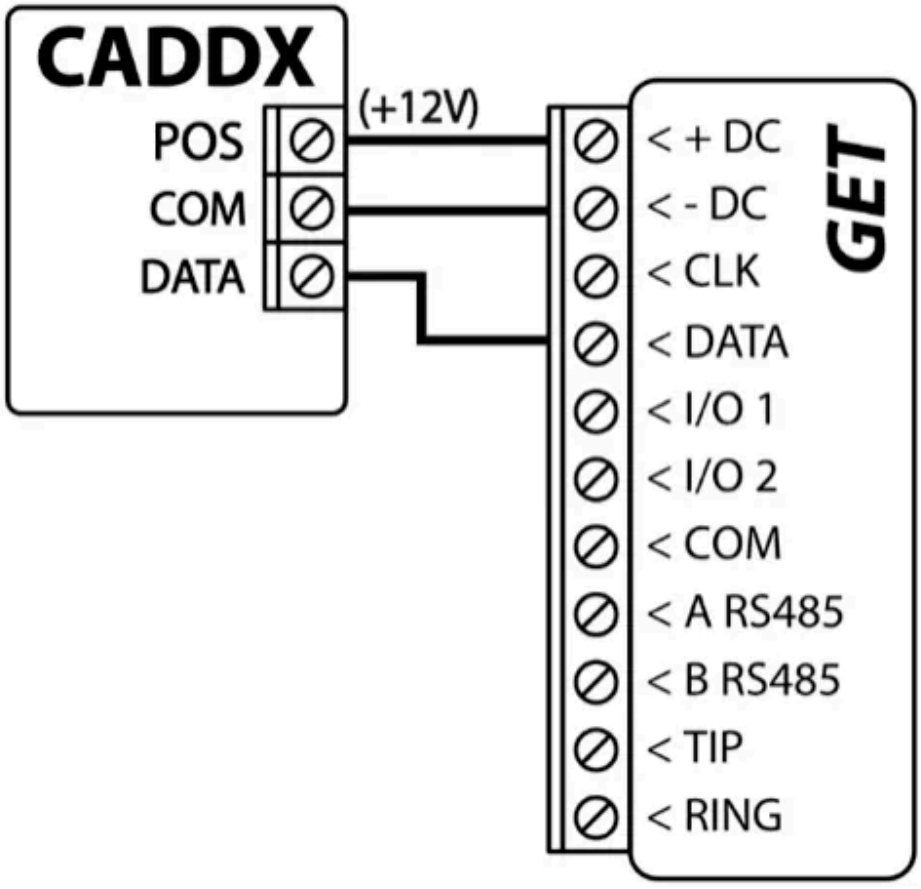


Abbildung 20. Anschluss einer UTC-Interlogix-Zentrale (Caddx) NetworX am Datenbus („Keypad bus“): POS → +DC, COM → –DC, DATA → DATA.

3.3.5 Texecom – serielle Schnittstelle

An die serielle Schnittstelle der Zentrale Texecom Premier / Premier Elite wird der Kommunikator mit dem separat bestellbaren Kabel **EX-CRP4** angeschlossen: **rot → +DC**, **schwarz → –DC**, **blau → CLK**, **weiß → DATA**.

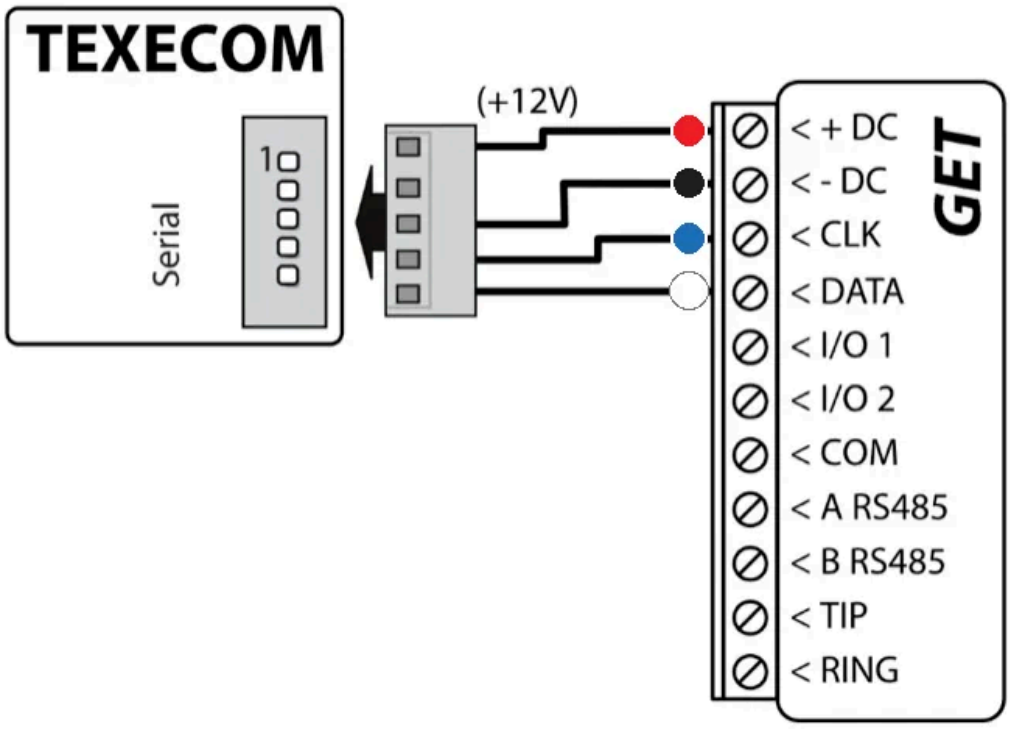


Abbildung 21. Anschluss einer Texecom-Zentrale an der seriellen Schnittstelle mit dem Kabel EX-CRP4 (separat zu bestellen; „Use the EX-CRP4 cable (ordered separately)“): rot → +DC, schwarz → –DC, blau → CLK, weiß → DATA.

- rote Ader („R - red“)
- schwarze Ader („B - black“)
- blaue Ader („BL - blue“)
- weiße Ader („W - white“)

3.3.6 InnerRange Inception

Der Kommunikator wird über den Versorgungsausgang der Zentrale Inception versorgt (**VOUT + → +DC**, **VOUT 0V → –DC**), die Datenverbindung kommt vom USB-Anschluss der Zentrale über das Kabel **993030USB** von Inner Range: **schwarz → 0V / –DC**, **grün → CLK**, **weiß → DATA**.

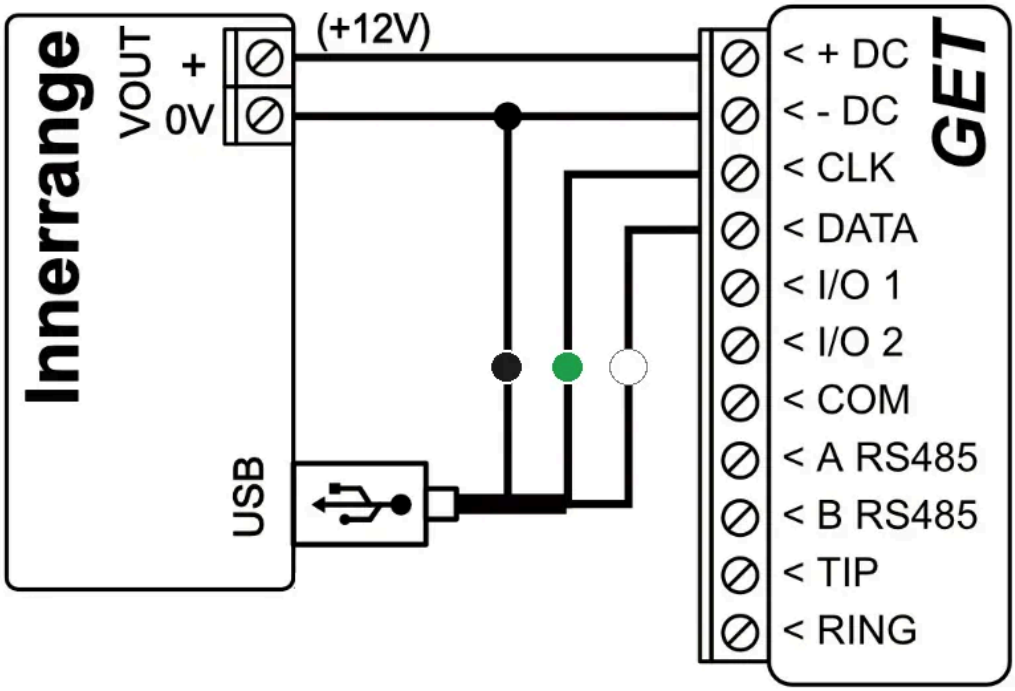


Abbildung 22. Anschluss einer InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; vom USB-Anschluss mit dem Kabel 993030USB („Cable, Inner Range part number 993030USB") schwarz → −DC, grün → CLK, weiß → DATA.

- schwarze Ader („Black wire")
- grüne Ader („Green wire")
- weiße Ader („White wire")

3.3.7 InnerRange Integriti

An die serielle Schnittstelle **Port 0** der Zentrale Integriti wird der Kommunikator mit dem Kabel **INTG-996795** von Inner Range angeschlossen: **+DET (+13 V)** → **+DC**, **GND (5)** → **−DC**, **Rx (3)** → **CLK**, **Tx (2)** → **DATA**.

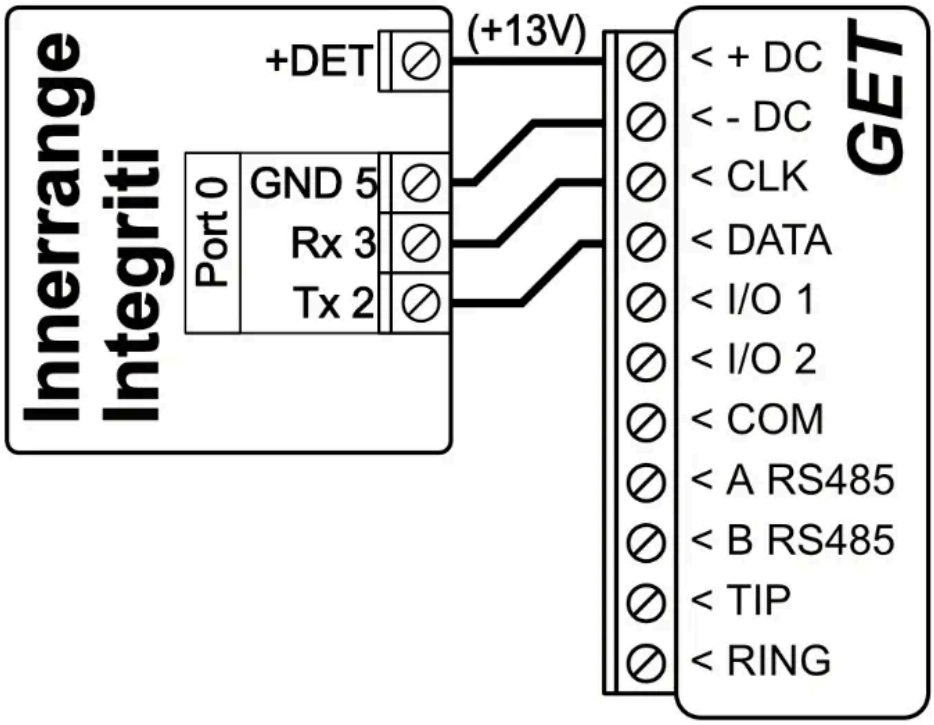


Abbildung 23. Anschluss einer InnerRange Integriti an Port 0 mit dem Kabel INTG-996795 („Cable, Inner Range part number INTG-996795"): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – Datenbus

Schließen Sie den Bedienteilbus der Zentralen Honeywell Ademco Vista-15, Vista-20 und Vista-48 von den Klemmen der Zentrale an den Kommunikator an: **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.

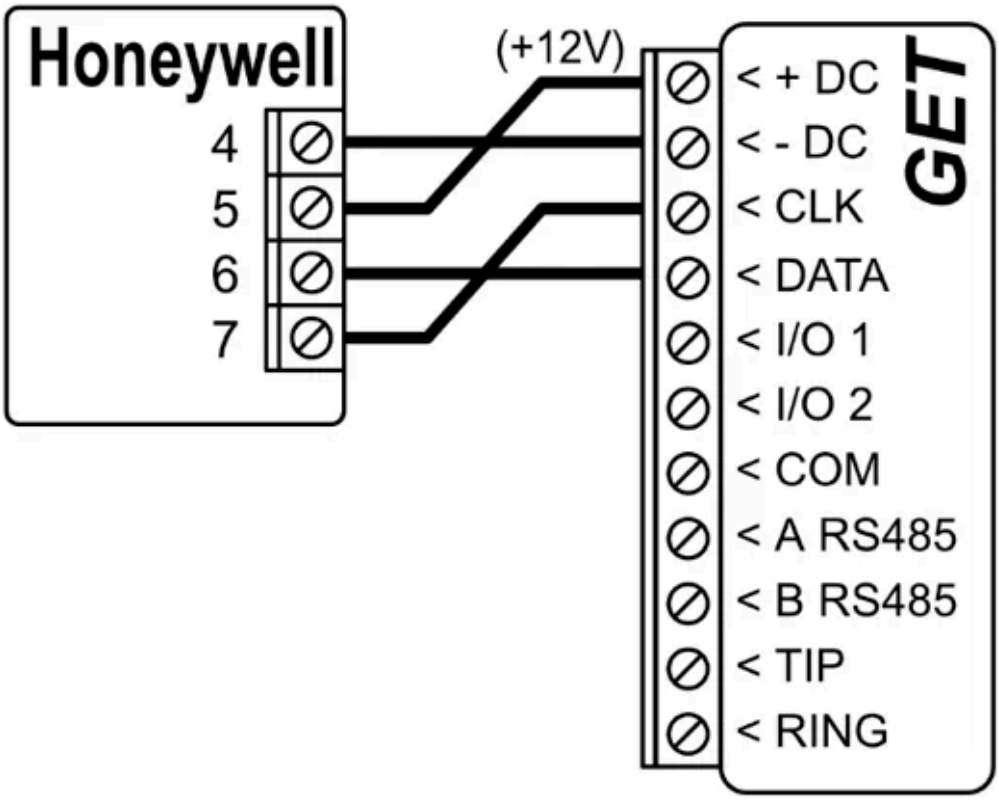


Abbildung 24. Anschluss einer Honeywell-Zentrale Vista-15 / -20 / -48 am Datenbus („Keypad bus"): Klemme 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Jede Zentrale – TIP/RING

Jede andere Zentrale lässt sich über ihr Telefonwählgerät anschließen: die Versorgung vom Hilfsspannungsausgang der Zentrale (**+AUX** → **+DC**, **–AUX** → **–DC**), der Telefonleitungsausgang an die Klemmen **TIP** und **RING** des Kommunikators (**TIP** → **TIP**, **RING** → **RING**). Das Wählgerät der Zentrale muss eingerichtet werden (Abschnitt 4.2).

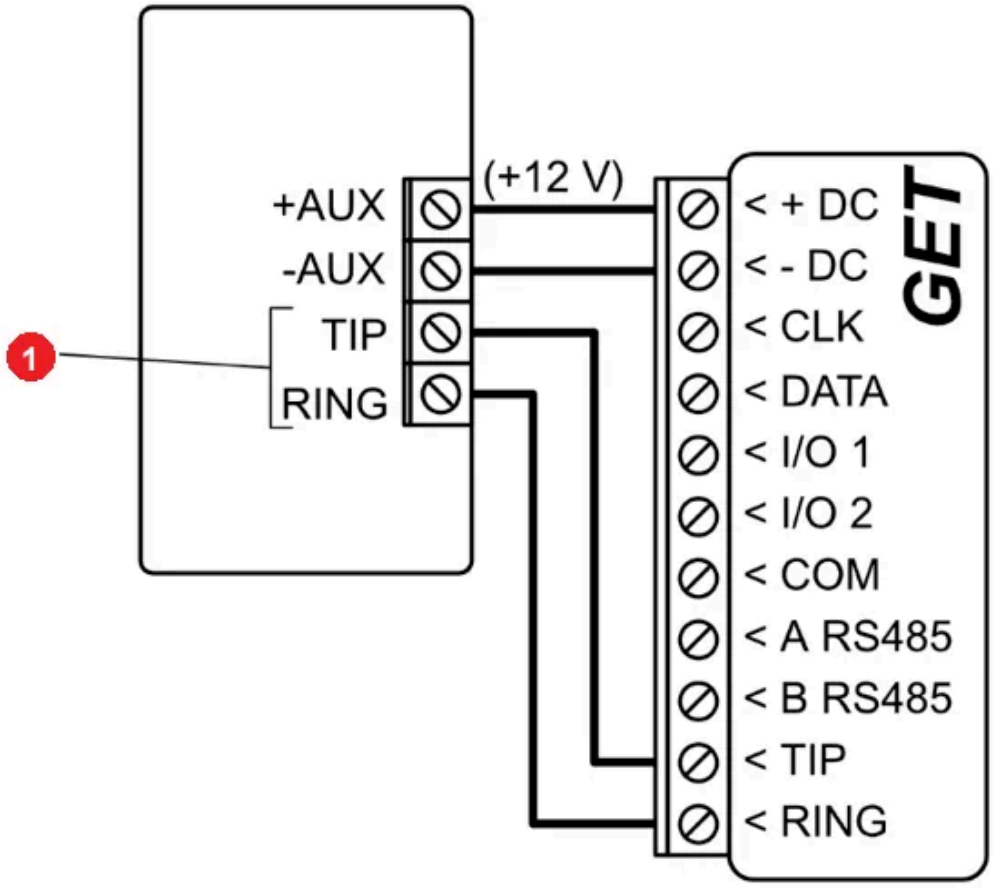


Abbildung 25. Anschluss an das Telefonwählgerät der Zentrale („Control panel"): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 die Klemmen des Telefonwählgeräts der Zentrale („Telephone line communicator terminals")

3.4 Anschluss einer Schlüsselschalterzone

Wenn Sie die Zentrale aus der App Protegus 2 so scharf und unscharf schalten möchten, dass der Ausgang (PGM) des Kommunikators die **Schlüsselschalterzone** der Zentrale schaltet, folgen Sie diesem Anschluss. Die beiden I/O-Klemmen mit Doppelfunktion des Kommunikators arbeiten als Ausgang (OUT, PGM) – beim GET sind werkseitig beide Ausgänge –, so dass die beiden Ausgänge zwei Bereiche der Anlage steuern können: Schließen Sie die Schlüsselschalterzone von Bereich 1 an die Klemme **1 I/O** an, die von Bereich 2 an die Klemme **2 I/O**. Bei diesem Anschluss entfernen Sie auf der Seite **Panel settings** in TrikdisConfig das Häkchen bei **Remote Arm/Disarm**, die Klemmen müssen auf der Seite **IN/OUT** auf die Funktion **OUT** gestellt sein (Abschnitt 6.7), und in der App Protegus 2 ordnen Sie die Ausgänge gemäß Abschnitt 5.2 den Bereichen zu.

Beim Anschluss an Datenbus oder serielle Schnittstelle bleibt die Datenverbindung zwischen Zentrale und Kommunikator bestehen (der Kommunikator liest die Ereignisse vom Bus), das Scharf- und Unscharfschalten erfolgt über die Schlüsselschalterzone:

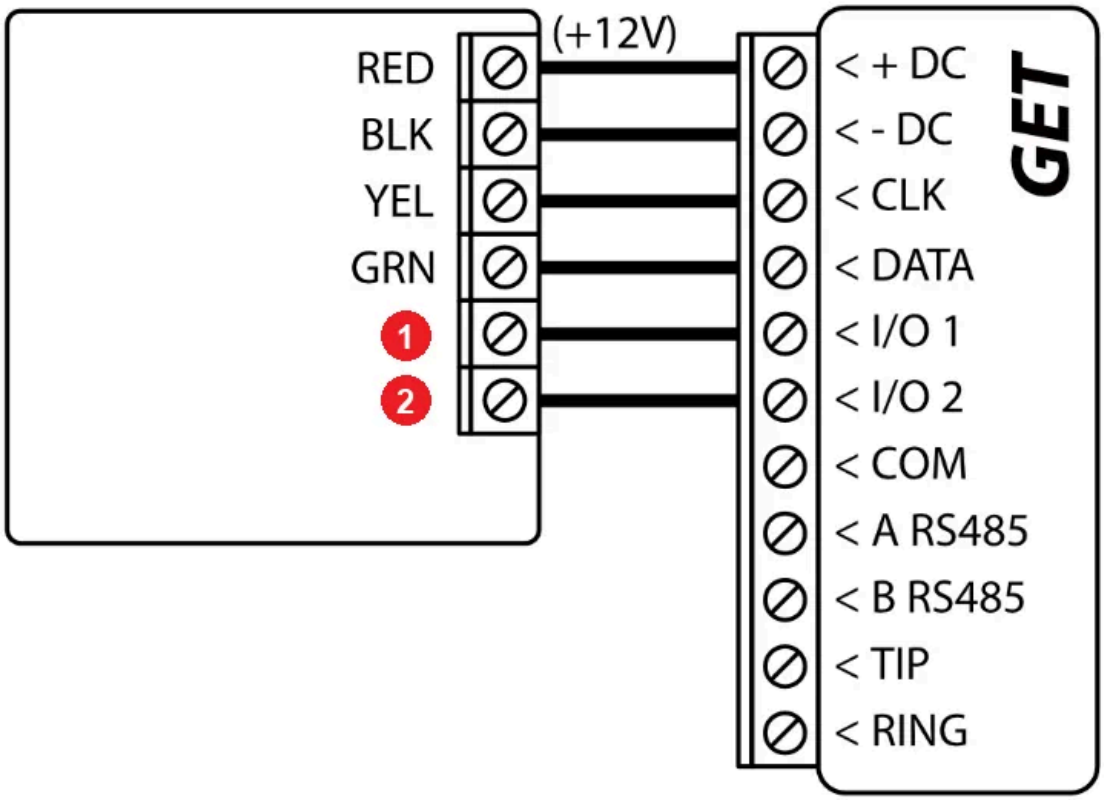


Abbildung 26. Scharf- und Unscharfschalten mit einer Schlüsselschalterzone („Zone (keyswitch)“) beim Anschluss an Datenbus oder serielle Schnittstelle („Keypad bus or Serial port“): Klemme RED der Alarmzentrale („Control panel“) → +DC, BLK → −DC, YEL → CLK, GRN → DATA; die Zone von Bereich 1 → 1 I/O, die von Bereich 2 → 2 I/O.

- 1 Schlüsselschalterzone von Bereich 1 („1-st Area“)
- 2 Schlüsselschalterzone von Bereich 2 („2-nd Area“)

Beim Telefonleitungsanschluss (TIP/RING) sendet die Zentrale die Ereignisse über ihr Wählgerät, das Scharf- und Unscharfschalten erfolgt ebenso über die Schlüsselschalterzone:

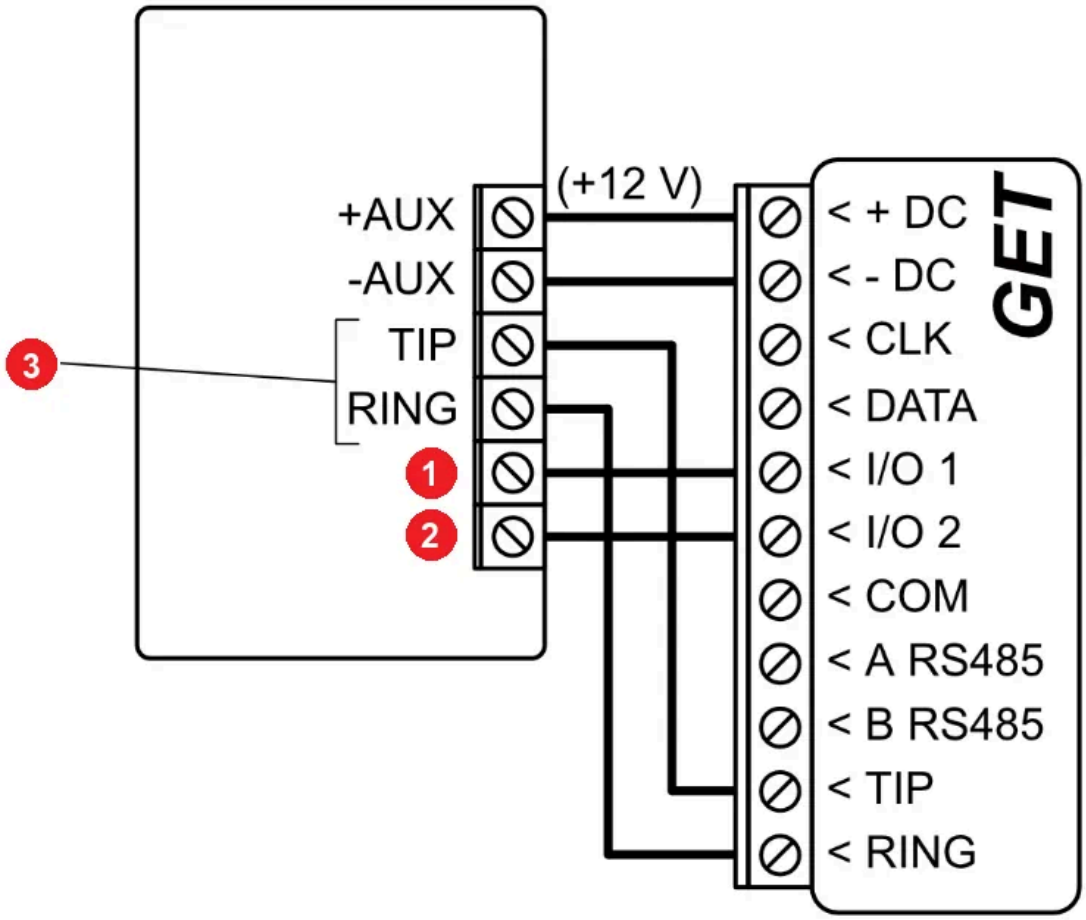


Abbildung 27. Scharf- und Unscharfschalten mit einer Schlüsselschalterzone („Zone (keyswitch)“) beim Telefonleitungsanschluss: Klemme +AUX der Alarmzentrale („Control panel“) → +DC, −AUX → −DC, TIP → TIP, RING → RING; die Zone von Bereich 1 → 1 I/O, die von Bereich 2 → 2 I/O.

- 1 Schlüsselschalterzone von Bereich 1 („1-st Area“)
- 2 Schlüsselschalterzone von Bereich 2 („2-nd Area“)
- 3 die Klemmen des Telefonwählgeräts der Zentrale („Telephone line communicator terminals“)

Die Schlüsselschalterzone kann impulsgesteuert oder zweistellig (rastend) sein – in der App Protegus 2 muss derselbe Modus eingestellt werden (Abschnitt 5.2). Details und Fallstricke des Scharfschaltens per Schlüsselschalter behandelt ein eigener Artikel: Scharfschalten aus der Ferne per Schlüsselschalter aus der App Protegus 2.

3.5 Anschluss der Eingänge

Die beiden I/O-Klemmen mit Doppelfunktion des Kommunikators lassen sich als Eingang (IN) auch zum Anschluss weiterer Melder (z. B. Sabotagekontakt, Paniktaster) verwenden, unabhängig von der Alarmzentrale. An den Eingang lässt sich ein Stromkreis NO, NC, NO/EOL, NC/EOL, NO/DEOL oder NC/DEOL anschließen. Beim GET sind die Klemmen werkseitig Ausgänge: Stellen Sie die verwendete Klemme auf der Seite **IN/OUT** in TrikdisConfig auf die Funktion **IN** und geben Sie im Feld **Type** den Typ des angeschlossenen Stromkreises an; in der App Protegus 2 finden Sie dasselbe auf der Seite **Advanced settings** → **IN/OUT**, im Feld **Type** der Klemme 1 oder 2 (Abschnitt 6.7). Der Eingang wird zwischen der gewählten I/O-Klemme und der Klemme **COM** angeschlossen, entsprechend dem gewählten Typ.

Die Eingänge akzeptieren die folgenden Schleifentypen: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Der Abschlusswiderstand beträgt **2,2 kΩ**. Beim einfachen Abschluss (EOL) gelten Kurzschluss und Unterbrechung gleichermaßen als Alarm; der doppelte Abschluss (DEOL) mit zwei Widerständen erkennt

Alarm und Sabotage (Kurzschluss oder Unterbrechung) getrennt. Die Werkseinstellung ist NO (im Ruhezustand offen); den Eingangstyp stellen Sie in TrikdisConfig auf der Seite **IN/OUT** entsprechend der Verdrahtung ein.

Typ	Ruhezustand	Alarm	Sabotage
NC	geschlossen	offen	–
NO	offen	geschlossen	–
NC/EOL	2,2 kΩ	Unterbrechung oder Kurzschluss	–
NO/EOL	2,2 kΩ	Kurzschluss oder Unterbrechung	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	Unterbrechung oder Kurzschluss
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	Unterbrechung oder Kurzschluss

Wird der Eingang ausgelöst, sendet der Kommunikator ein eigenes Ereignis an die Leitstelle und an Protegus 2; Contact-ID-Code, Bereichs- und Zonennummer des Ereignisses können Sie auf der Seite **IN/OUT** angeben.

Anschluss der Eingangsstromkreise zwischen COM und dem Punkt INx: NO, NC, NC/EOL, NO/EOL sowie mit Sabotageerkennung NO/DEOL und NC/DEOL, mit Abschlusswiderständen von 2,2 kΩ; die einzelnen Zustände (Kurzschluss, Unterbrechung, 2,2 kΩ, 3,3–5,5 kΩ) erklärt die Tabelle in Abschnitt 3.5.

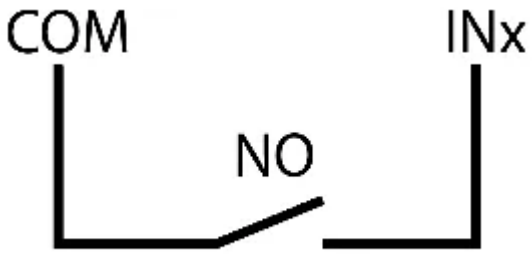


Abbildung 28. NO – im Ruhezustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

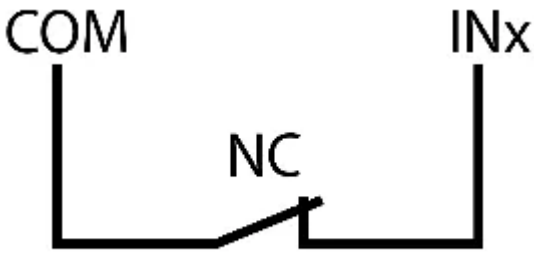


Abbildung 29. NC – im Ruhezustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

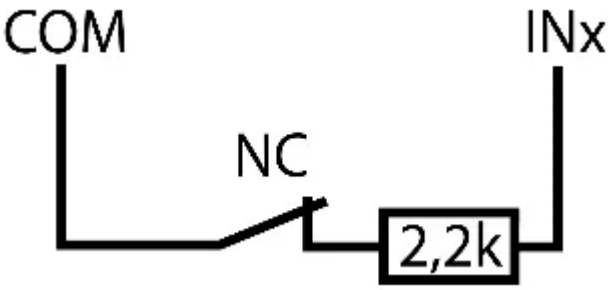


Abbildung 30. NC/EOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

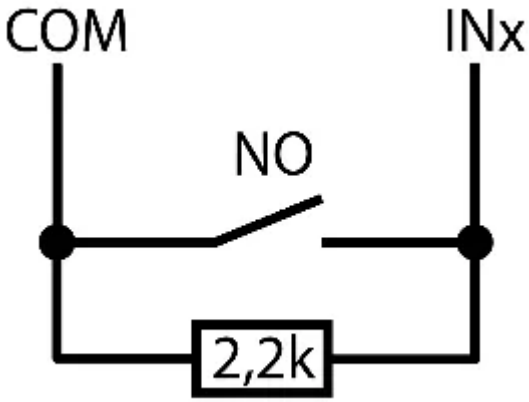


Abbildung 31. NO/EOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

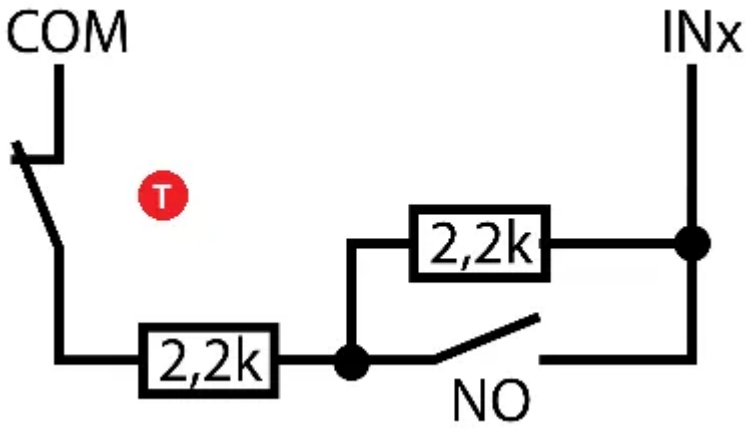


Abbildung 32. NO/DEOL – im Ruhezustand offener Kreis mit Abschlusswiderständen 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

- T Sabotagekontakt („Tamper“), meldet das Öffnen des Meldergehäuses

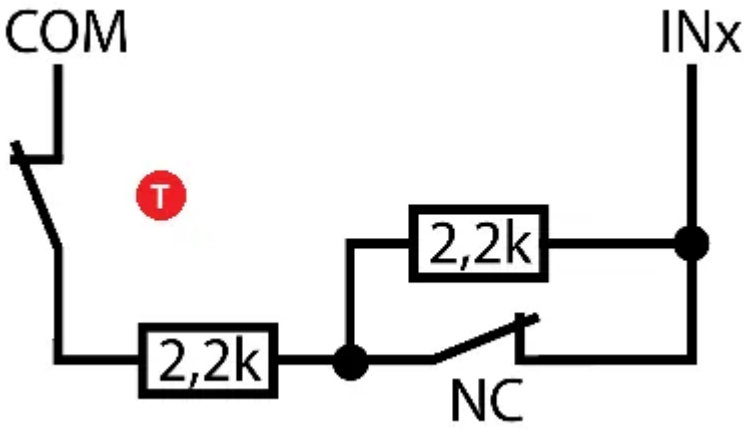


Abbildung 33. NC/DEOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderständen 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

- T Sabotagekontakt („Tamper"), meldet das Öffnen des Meldergehäuses

3.6 Anschluss eines Ausgangs mit Relais

Als Ausgang sind die I/O-Klemmen Open-Collector-Ausgänge (OC): Im aktiven Zustand ziehen sie die angeschlossene Last auf Minus, mit höchstens 0,15 A, bis 30 V DC. Mit den Kontakten eines Relais können Sie verschiedene elektrische Geräte ein- und ausschalten: Ein Ende der Relaisspule kommt an **+DC**, das andere an die Klemme **x I/O**, den Verbraucher schalten die Kontakte des Relais (NC, C, NO). Die verwendete I/O-Klemme muss auf der Seite **IN/OUT** in TrikdisConfig (oder auf der Seite IN/OUT der App) ein Ausgang (**OUT**) sein – beim GET ist das die Werkseinstellung.

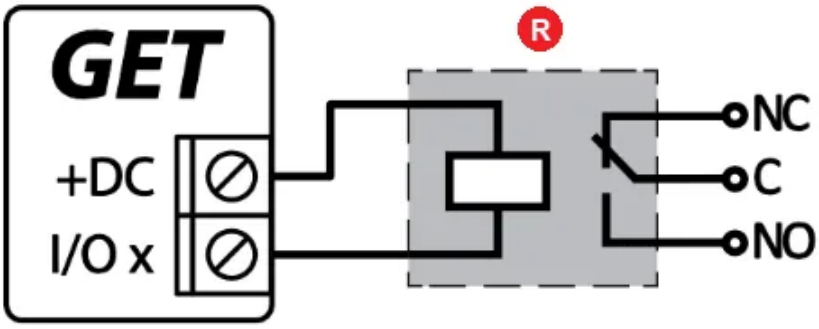


Abbildung 34. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule liegt zwischen +DC und der Klemme x I/O, die Kontakte (NC, C, NO) schalten den Verbraucher.

- R Relais („Relay")

Die Ausgänge können Sie aus der App Protegus 2 schalten (Kapitel 5).

3.7 Einschalten und erste Prüfung

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.

Nach dem Anschließen startet mit dem Einschalten der Versorgung der Alarmzentrale auch der Kommunikator. Auf der Frontabdeckung sollten Sie Folgendes sehen:

- **POWER** leuchtet grün – die Versorgung ist in Ordnung;
- **NETWORK LTE** leuchtet grün und blinkt gelb – mit dem Mobilfunknetz verbunden; die Anzahl der gelben Blinkimpulse ist der Signalpegel: bei 4G sind 3 Blinkimpulse ausreichend; zählen Sie weniger, ist das Signal schwach: Suchen Sie für den Kommunikator oder die Antenne einen anderen Platz oder verwenden Sie eine empfindlichere Antenne (Abschnitt 3.2);
- **NETWORK LAN** leuchtet grün, wenn Sie auch ein Netzwerkkabel eingesteckt haben – mit dem kabelgebundenen Netzwerk verbunden;
- **TROUBLE** leuchtet nicht.

Blinkt TROUBLE, gibt die Anzahl der Blinkimpulse die Ursache an (Abschnitt 1.6); auch jede andere abweichende LED-Anzeige weist auf einen Fehler hin, dessen Ursache Sie anhand der Tabellen in Abschnitt 1.6 finden. Leuchtet keine LED, prüfen Sie Versorgung und Anschluss.

4. Programmierung der Alarmzentrale

Die Einrichtung der Zentrale hängt davon ab, wie Sie sie angeschlossen haben: über Datenbus oder serielle Schnittstelle (Abschnitt 4.1) oder über ihr Telefonwählgerät, an den Klemmen TIP/RING (Abschnitt 4.2). Beim Anschluss Keybus + TIP/RING einer Paradox SP / SP+ / MG / MG+ gibt die Tabelle in Abschnitt 3.3.3 die Einstellung der Speicherplätze der Zentrale an.

4.1 Anschluss an Datenbus oder serielle Schnittstelle

Hier beschreiben wir, wie die Zentrale einzurichten ist, damit der Kommunikator ihre Ereignisse liest und sie aus der Ferne steuern kann. Für die Fernsteuerung muss auf der Seite **Panel settings** in TrikdisConfig (in der App: **Panel settings** → **Serial Bus**) die Option **Remote Arm/Disarm** angehakt sein (Abschnitte 2.2 und 6.3).

4.1.1 DSC

Die Zentralen **DSC PowerSeries** (Liste der unterstützten Typen in Punkt 1.2) erfordern keinerlei besondere Einstellung: Der am Keybus angeschlossene Kommunikator liest die Ereignisse sofort, und nach dem Setzen des Häkchens bei **Remote Arm/Disarm** schaltet der Benutzer mit seinem eigenen Bedienteilcode aus der App scharf und unscharf. Die Details der direkten Steuerung – Zonenzustände, Zonensperrung, automatische Erkennung der Bereiche – behandelt ein eigener Artikel: Direkte Steuerung für DSC-PowerSeries-Alarmzentralen.

Mit den Zentralen **DSC PowerSeries NEO** funktioniert der Kommunikator nicht: Am Bus der NEO lässt der Hersteller keine externen Geräte zu. Für die NEO eignet sich ein Telefonleitungs-Kommunikator (TIP/RING) – siehe DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen.

4.1.2 Paradox

Die **Paradox**-Zentralen müssen nur für die direkte Steuerung programmiert werden; zum Lesen der Ereignisse ist nichts einzustellen. Die Firmware der Zentrale muss mindestens **V.4** sein.

Bei neueren Paradox-Zentralen (zum Beispiel der Serien SP+, MG+ und EVOHD+) kann die serielle Schnittstelle **werkseitig gesperrt** sein: Der Kommunikator erhält keine Daten, bis Sie die Schnittstelle freischalten. So funktioniert die Freischaltung: Freischaltung der gesperrten seriellen Schnittstelle bei Paradox-Alarmzentralen.

Für die Steuerung muss das **PC-Passwort** (PC password) der Zentrale eingestellt und dasselbe in TrikdisConfig im Feld **System settings → Security panel PC download password** eingetragen werden – beide müssen übereinstimmen.

1. Öffnen Sie am Bedienteil die Installateur-Programmierung der Zentrale.
2. Öffnen Sie die Sektion des PC-Passworts: bei den Serien **MAGELLAN und SPECTRA** die Sektion **911**, bei der Serie **DIGIPLEX EVO** die Sektion **3012**.
3. Geben Sie ein **4-stelliges** Passwort ein. Das Passwort darf nicht 0000 sein und **nicht mit einer Null beginnen**.
4. Verlassen Sie die Programmierung und **starten Sie die Zentrale neu** – die Änderung des PC-Passworts wird erst nach einem Neustart wirksam. Tragen Sie anschließend dasselbe Passwort in TrikdisConfig ein.

Typische Fehler und ihre Lösung

- Der dem Bereich zugewiesene **Bedienteilcode darf nicht der Mastercode sein**: Geben Sie dem Benutzer einen anderen Code, damit funktioniert das Scharf-/Unscharfschalten aus Protegus 2.
- **Starten Sie den Kommunikator nach jeder Änderung eines Bedienteilcodes neu** (Spannung trennen oder SMS-Befehl `RESET`): Er liest die Codes beim Start aus, spätere Änderungen sieht er nicht.

Beim GET-Kommunikator befindet sich das Feld **Security panel PC download password** auf der Seite **Panel settings** in TrikdisConfig, in der Gruppe **Serial bus**; in der App Protegus 2 unter **Panel settings → Serial Bus → PC download password** (Abschnitte 2.2 und 6.3).

Anschluss Keybus und TIP/RING (SP / SP+ / MG / MG+, Abschnitt 3.3.3): Die Zentrale muss zusätzlich so programmiert werden, dass sie die Ereignisse an die Leitstelle sendet und aus Protegus 2 steuerbar ist – die Werte der Speicherplätze (801, 811, 812, 815, 911) gibt die Tabelle in Abschnitt 3.3.3 an.

4.1.3 Texecom

Die Zentralen **Texecom Premier / Premier Elite** müssen sowohl zum Lesen der Ereignisse als auch für die Steuerung programmiert werden: Das 4-stellige Passwort der Zentrale mit dem Namen **UDL passcode** muss eingestellt und dasselbe in TrikdisConfig im Feld **System settings → Security panel PC download password** eingetragen werden – beide müssen übereinstimmen.

Mit der Texecom-Software Wintex: Der UDL passcode befindet sich im Fenster **Communication Options** auf der Registerkarte **Options**.

Am Bedienteil:

1. Geben Sie den 4-stelligen Installateurcode ein und drücken Sie die Taste **[Menu]**, um ins Programmiermenü zu gelangen.
2. Drücken Sie gleich danach die Taste **[9]**.

3. Drücken Sie **[7][6]**, dann die Taste **[2]**, und geben Sie den 4-stelligen UDL passcode ein.
4. Drücken Sie die Taste **[Yes]** und verlassen Sie die Programmierung mit der Taste **[Menu]**.

Beim GET-Kommunikator befindet sich das Feld **Security panel PC download password** auf der Seite **Panel settings** in TrikdisConfig, in der Gruppe **Serial bus** (in der App **Panel settings → Serial Bus → PC download password**); der UDL passcode muss damit übereinstimmen.

4.1.4 UTC Interlogix (Caddx)

Die Firmware der Zentrale **UTC Interlogix (Caddx) NetworX** muss mindestens **V2** sein. Am Bedienteil der Zentrale ist Folgendes einzustellen:

1. Drücken Sie die Tasten **[*][8]** und geben Sie den Installateurcode ein (werkseitig **9713**).
2. Geben Sie die dem Kommunikator zugewiesene **Gerätenummer** ein (device address; werkseitig **0**).
3. Programmieren Sie die Zeilen der folgenden Tabelle nacheinander: Geben Sie die Adresse (location), die Segmentnummer und dann die Einstellung ein. Mit der Taste **[*]** gelangen Sie zurück ins vorherige Feld. `12345678` bedeutet, dass alle acht Schalter des Segments eingeschaltet sind (auf der Anzeige sind alle Ziffern zu sehen).

Adresse (location)	Segment	Einstellung
23	3	12345678
37 (nicht unbedingt erforderlich)	3	12345678
37 (nicht unbedingt erforderlich)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Wenn Sie alle Zeilen programmiert haben, drücken Sie zweimal die Taste **[Exit]**, um die Programmierung zu verlassen.

4.1.5 InnerRange

Die Firmware der Zentrale **InnerRange Inception** muss mindestens **2.3.0.3507-r0** sein, und die Zentrale benötigt eine Internetverbindung. Die Einstellung nehmen Sie in der Weboberfläche der Zentrale vor:

1. Öffnen Sie im Browser die Adresse `https://skytunnel.com.au/inception/SERIENNUMMER`, wobei SERIENNUMMER die Seriennummer auf dem Gehäuse der Zentrale ist. Melden Sie sich mit dem Installateurkonto an.
2. Öffnen Sie die Seite **Configuration → General → Alarm Reporting**.
3. In der Gruppe **3rd Party Device Configuration**: - setzen Sie das Häkchen bei **Enable 3rd Party Device Reporting**; - wählen Sie im Feld **3rd Party Device Type** den Wert **Trikdis**; - wählen Sie im Feld **Serial Port** den Wert **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Speichern Sie die Einstellungen und verlassen Sie die Oberfläche.

Die Firmware der Zentrale **InnerRange Integriti** muss mindestens **19.1.0.36608**, ihre Programmiersoftware (Integriti Professional) mindestens **19.1.0.15396** sein. Die Einstellung nehmen Sie in der Programmiersoftware der Zentrale vor:

1. Wählen Sie für die serielle Schnittstelle (**TTL Port-0**), an die der Kommunikator angeschlossen ist, das Kommunikationsprotokoll **Trikdis**.
2. Das Datenformat muss **Contact ID** sein.
3. Einstellung der Schnittstelle: **19200, 8, N, 1**.
4. Speichern Sie die Einstellungen und beenden Sie das Programm.

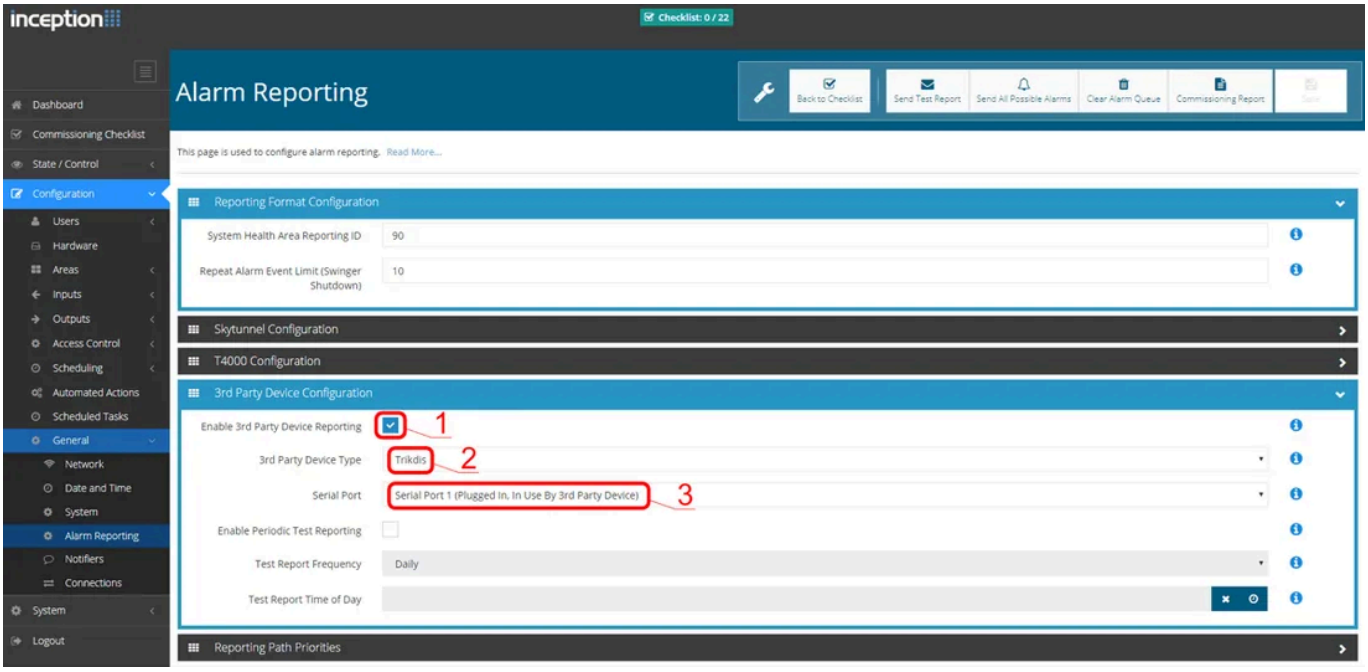


Abbildung 35. InnerRange Inception – Configuration → General → Alarm Reporting, Gruppe 3rd Party Device Configuration: Enable 3rd Party Device Reporting angehakt, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

Die Firmware der Zentralen **Honeywell Ademco Vista-20** und **Vista-48** muss mindestens **V5.3** sein. Die Einstellung nehmen Sie am Bedienteil der Zentrale vor.

Einstieg in die Programmierung – auf zwei Arten:

- Geben Sie den Installateurcode ein (werkseitig **4112**), dann die Tasten **[8][0][0]**; oder
- schalten Sie die Versorgung der Zentrale ein und drücken Sie **innerhalb von 50 Sekunden** gleichzeitig die Tasten **[*]** und **[#]** (das funktioniert nur, wenn die Programmierung zuvor mit den Tasten [*][9][8] verlassen wurde).

Einstellungen:

1. Aktivieren Sie das Senden von Contact-ID-Ereignissen am Ausgang für Langstreckenfunk (LRR): Drücken Sie die Tasten **[*][2][9][1][#]**.
2. Für die Fernsteuerung aktivieren Sie die Verwendung der **2. AUI-Adresse** (2nd AUI address): Drücken Sie die Tasten **[*][1][8][9][1][1][#]**.

Verlassen der Programmierung: Drücken Sie die Tasten **[*][9][9]**.

4.2 Anschluss an die Telefonleitung (TIP/RING)

Damit die Alarmzentrale die Ereignisse über ihren Telefonleitungsausgang sendet, muss das Wählgerät der Zentrale aktiviert und eingestellt werden. Die genauen Programmadressen finden Sie in der Installationsanleitung der Zentrale; das Wesentliche der Einstellung ist bei allen Herstellern gleich:

1. **Aktivieren Sie den Telefonleitungs-Kommunikator (PSTN)** in der Zentrale.
2. **Geben Sie als Telefonnummer `1234` an** beim Leitstellenempfänger – egal ob der Kommunikator an die RING/TIP-Klemmen der Zentrale oder an die Telefonleitung angeschlossen ist. Mit einer anderen Nummer kann es vorkommen, dass die Zentrale wählt, der Kommunikator die Ereignisse aber trotzdem nicht erhält: Auch bei einer DSC PowerSeries NEO startete die Übertragung erst nach der Änderung auf `1234`.
3. **Wählverfahren:** DTMF (tone), nicht Impulswahl.
4. **Protokoll:** Contact ID.

Wenn Sie die Zentrale aus der Ferne über den Ausgang des Kommunikators scharf- und unscharfschalten möchten, muss die an den Ausgang angeschlossene Zone in der Zentrale als **Schlüsselschalterzone** eingestellt werden.

Die Schlüsselschalterzone kann impulsgesteuert oder bistabil sein. Der Ausgang des Kommunikators gibt standardmäßig einen Impuls von 3 Sekunden aus; die Impulslänge oder den bistabilen Modus können Sie in den Einstellungen der Protegus-2-App ändern.

Die Zentralen von DSC, Paradox, Caddx, Texecom, InnerRange und Honeywell lassen sich auch über ihren Telefonleitungsausgang an den Kommunikator anschließen (Abschnitt 3.3.9) – dann ist auch bei ihnen das Wählgerät einzurichten, und die direkte Steuerung ist nicht verfügbar.

4.2.1 Programmierung des Wählgeräts der Honeywell Vista

Wechseln Sie am Bedienteil in den Programmiermodus und stellen Sie diese Programmadressen ein:

Programmadresse	Einstellung
`*41`	Telefonnummer des Leitstellenempfängers: `1234`
`*43`	Objektkennung der Zentrale
`*47`	Tone dial = `1` und die Anzahl der Wählversuche
`*48`	`7` (Standard)
`*49`	`5` (Split/Dual-Meldung)
`*50`	Verzögerung beim Senden des Einbruchalarms – Standard `2,0` (30 s); für sofortiges Senden `0,0`

Bei der Zentrale **Honeywell Vista 48** stellen Sie zusätzlich die folgenden Programmadressen ein:

Programmadresse	Wert	Programmadresse	Wert	Programmadresse	Wert
`*41`	1234 (Telefonnummer des Empfängers)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (Objektkennung)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1

Programmadresse	Wert	Programmadresse	Wert	Programmadresse	Wert
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

Verlassen Sie am Ende der Programmierung den Programmiermodus mit dem Befehl `*99`.

4.2.2 Das Wählgerät der UTC Interlogix (Caddx) NX

Programmierung der Zentrale Interlogix NX-4V2 (NX-6V2, NX-8V2), wenn der Kommunikator an den Klemmen TIP/RING der Zentrale angeschlossen ist. Geben Sie am Bedienteil nacheinander Folgendes ein:

Adresse (location)	Tasten	Bemerkung
	`*89713`	Einstieg in die Programmierung (`9713` ist der werkseitige Errichtercode)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Alle Zonen-LEDs leuchten (Segment 1)
Location 4	`12345678*`	Alle Zonen-LEDs leuchten (Segment 2)
Location 4	`12345678*#`	
Location 23	`23#`	Alle Zonen-LEDs leuchten (Segment 3)
Location 23	`**`	Alle Zonen-LEDs leuchten (Segment 3)
Location 23	`12345678*#`	Alle Zonen-LEDs leuchten (Segment 3)
Location 37	`37#`	Alle Zonen-LEDs leuchten (Segment 3)
Location 37	`**`	Alle Zonen-LEDs leuchten (Segment 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT EXIT`	Verlassen der Programmierung

5. Fernsteuerung mit der App Protegus 2

Mit der mobilen und Web-App Protegus 2 sieht der Benutzer den Zustand der Anlage aus der Ferne, erhält Benachrichtigungen über Ereignisse, kann scharf- und unscharfschalten und die Ausgänge des Kommunikators schalten. Die App lässt sich für Android und iOS herunterladen (Google Play, App Store) oder im Browser verwenden: web.protegus.app. Melden Sie sich mit Ihrem Benutzernamen und Passwort an oder registrieren Sie ein neues Konto. Der GET benachrichtigt nicht per SMS oder Telefonanruf und nimmt auch keine SMS-Befehle an: Fernsteuerung und Benachrichtigung erfolgen über die App; auch die Einstellungen des Kommunikators sind aus der App erreichbar (**Settings** → **Advanced settings**, Kapitel 6).

5.1 Gerät hinzufügen

Prüfen Sie vor dem Hinzufügen des Geräts:

1. Die SIM-Karte ist aktiv, und ihre PIN ist im Gerät eingetragen oder die PIN-Abfrage ist ausgeschaltet – **oder** der Kommunikator ist mit einem Netzwerkkabel (LAN) am lokalen Netzwerk angeschlossen.
2. Auf der Seite **User reporting** → **PROTEGUS Cloud** in TrikdisConfig ist **Enable connection** angehakt (Abschnitt 6.5).
3. Die LED **POWER** leuchtet grün.
4. Die LED **NETWORK LTE** leuchtet grün und blinkt gelb (das Gerät ist im Mobilfunknetz); bei rein kabelgebundener Verbindung leuchtet die LED **NETWORK LAN** grün.

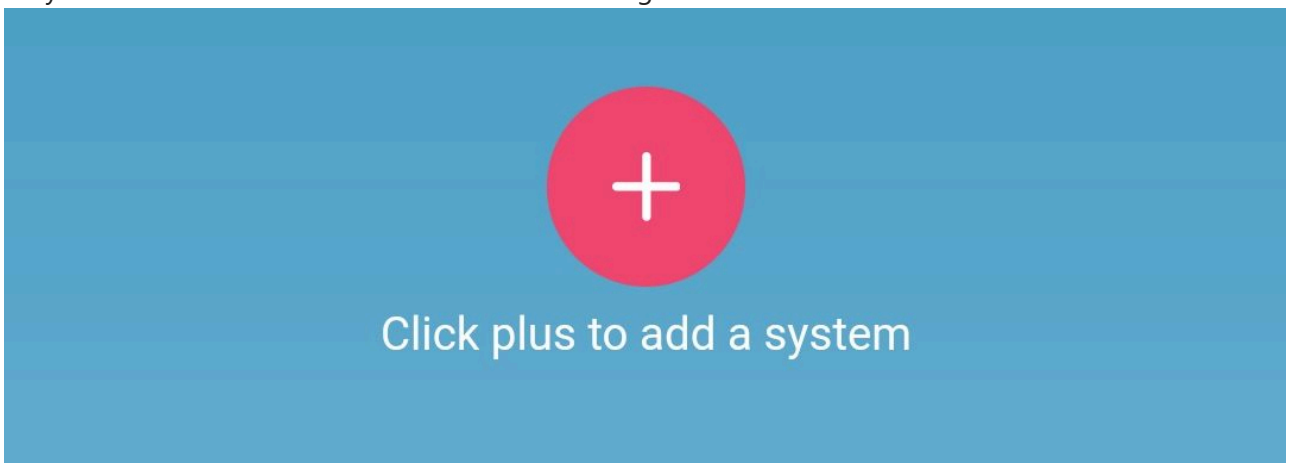
Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



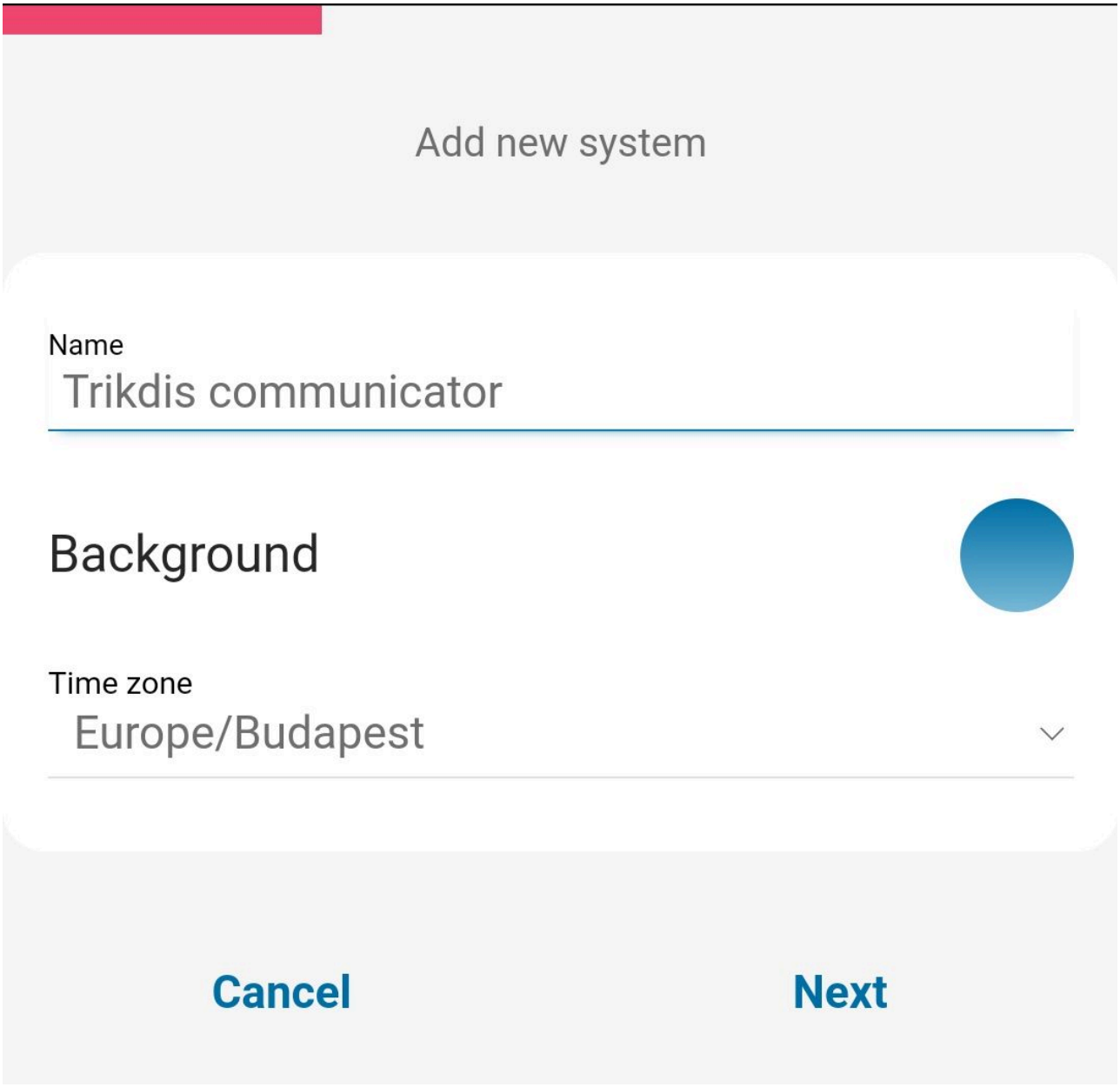
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



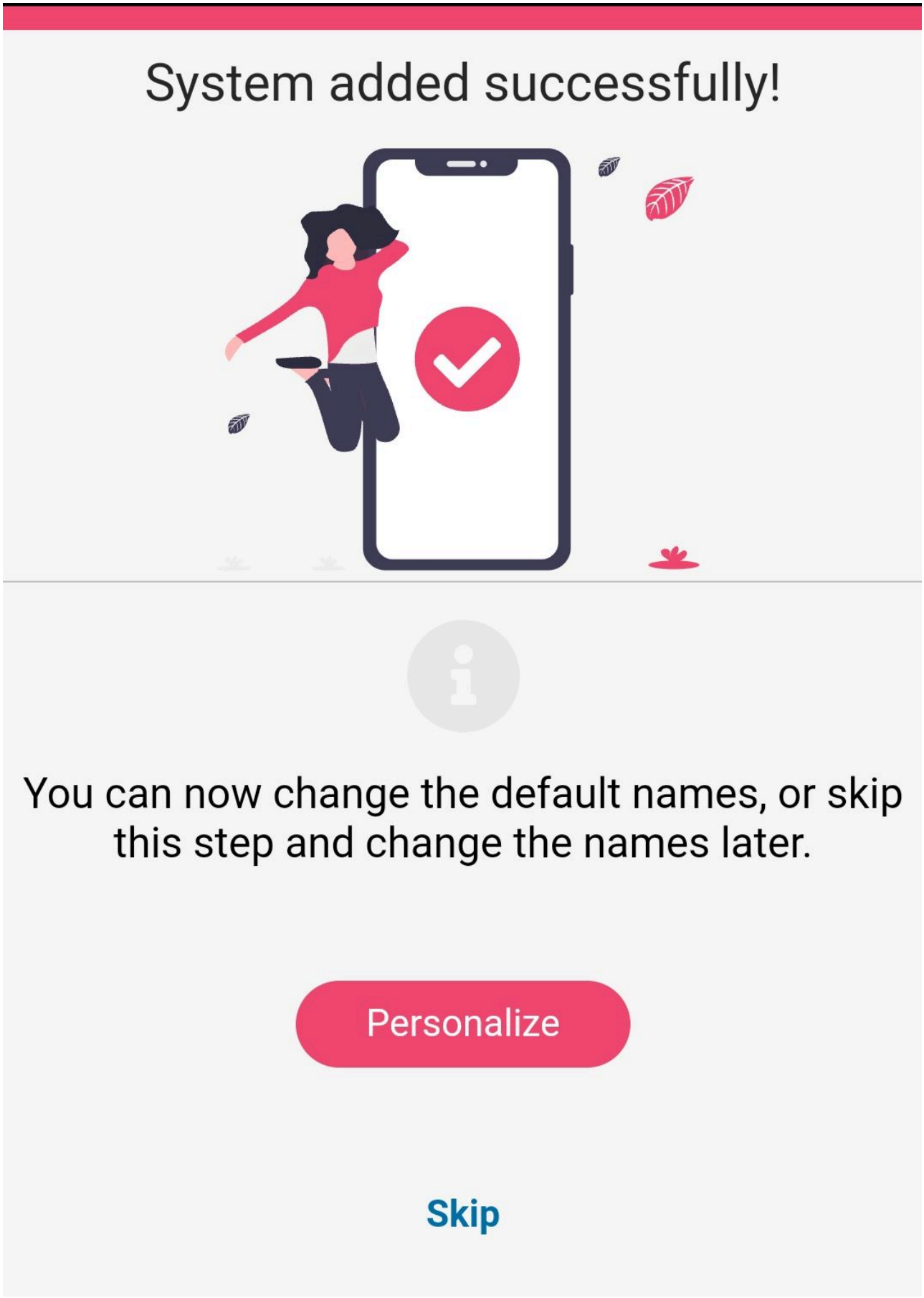
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



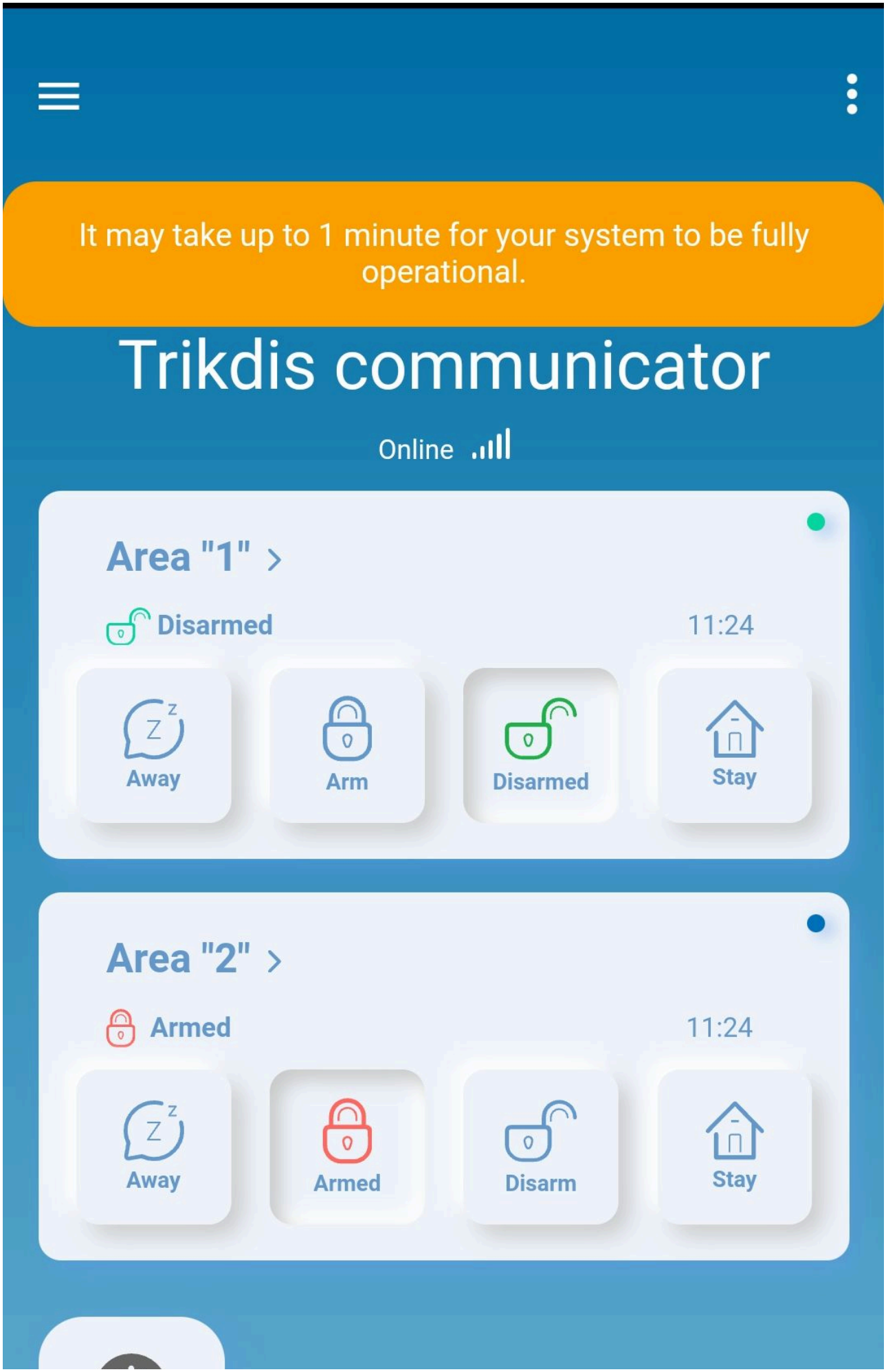
6. Add meg a rendszer nevét és válassz idozónát



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



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


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

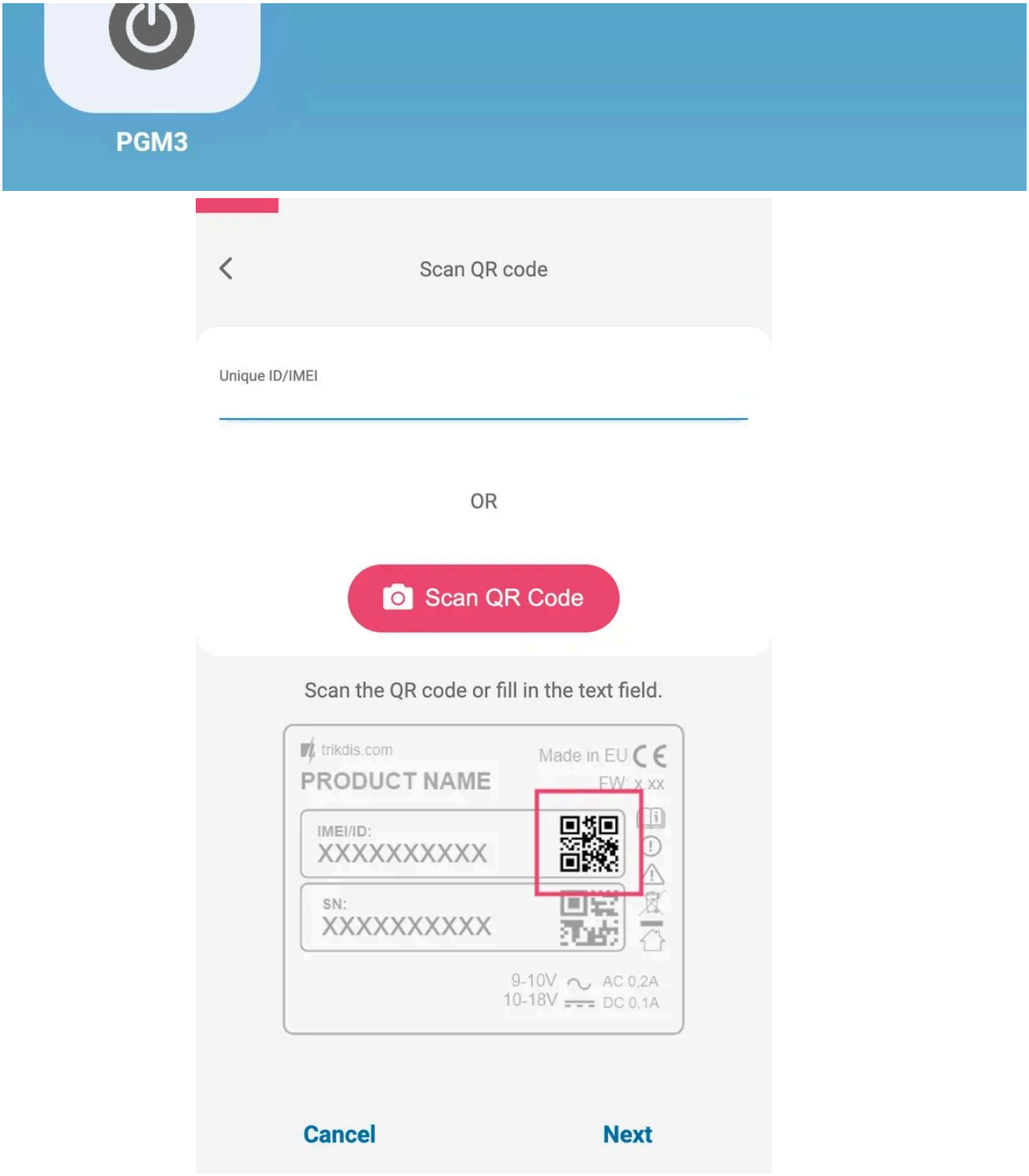


Abbildung 36. Protegus 2 – neue Anlage hinzufügen: IMEI / Unique ID eingeben oder den QR-Code des Etiketts scannen, dann Next.

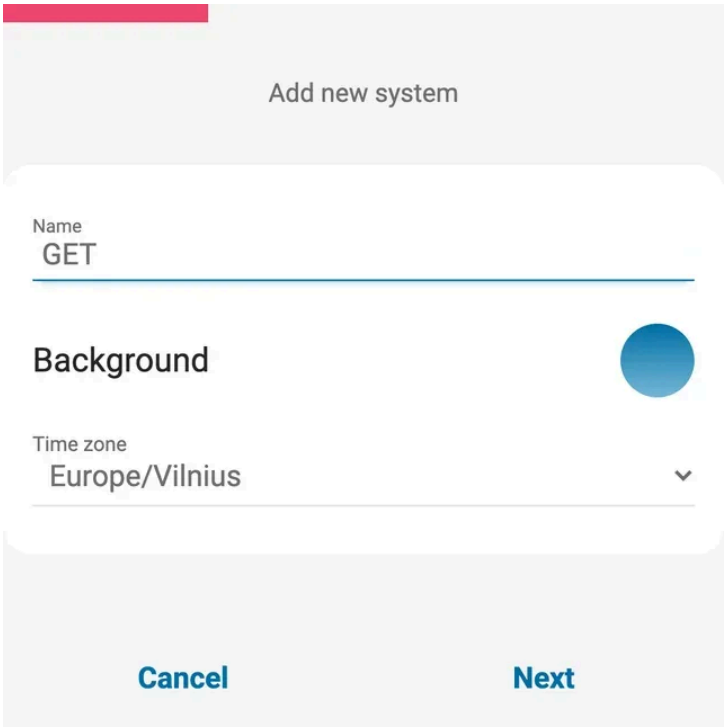


Abbildung 37. Protegus 2 – Name der Anlage (Name) eingeben, dann Next.

Die eindeutige Kennung des Geräts (**IMEI / Unique ID**) steht auf dem Etikett des Geräts und auf dem Aufkleber der Verpackung, und auch die Statusleiste von TrikdisConfig zeigt sie an. Ist der **PROTEGUS Cloud access Code** im Gerät nicht der werkseitige, fragt die App beim Hinzufügen danach.

5.2 Scharf- und Unscharfschalten mit einem Ausgang

Wenn Sie die Alarmzentrale über den Ausgang des Kommunikators und die Schlüsselschalterzone der Zentrale scharf- und unscharfschalten möchten, geben Sie in der Protegus-2-App beim Bereich an, welcher Ausgang ihn steuert.

Die Zone der Zentrale, an die der Ausgang des Kommunikators angeschlossen ist, muss in der Zentrale als **Schlüsselschalterzone** programmiert sein, und die Zentrale muss die Scharf- und Unscharfschaltereignisse melden – daraus zeigt Protegus 2 den Zustand des Bereichs an.

Die Einstellung können Sie beim Anlegen des Systems, beim Hinzufügen der Bereiche, oder nachträglich in den Systemeinstellungen beim Bearbeiten des Bereichs vornehmen. Beim Anlegen des Systems führt Sie der Assistent von Protegus 2 durch die Schritte: Klicken Sie auf **Continue** (Weiter), geben Sie den Namen des Bereichs ein (**Area name**) und erlauben Sie die Steuerung des PGM-Ausgangs aus der Protegus-2-App – das geschieht mit den folgenden Schritten:

1. Wählen Sie den Bereich aus (oder legen Sie ihn an), den Sie steuern möchten. Die Bereichsnummer muss mit der übereinstimmen, die die Zentrale in den Ereignissen sendet (Bereich 1 ist 1, Bereich 2 ist 2).
2. Aktivieren Sie die Option **Steuerung mit PGM** (Control with Protegus2) und wählen Sie im Feld **Ausgang** (Assigned Output) den Ausgang des Kommunikators (PGM1, PGM2 …). Ein Ausgang kann nur einen Bereich steuern.
3. Wählen Sie die Betriebsart: **Impuls** (Pulse) oder **bistabil** (Level) – dieselbe, die Sie in der Zentrale bei der Schlüsselschalterzone eingestellt haben. Üblicherweise verwenden wir den Impulsbetrieb; auch die Impulslänge kann angegeben werden (Standard 3 s).

4. Speichern Sie die Einstellung (**Save**). Bei mehreren Bereichen wiederholen Sie dies für jeden, mit seinem eigenen Ausgang: Im Assistenten legen Sie den weiteren Bereich mit der Schaltfläche **Click to add an area** an und stellen seinen PGM-Ausgang auf die gleiche Weise ein. Wenn Sie alle Bereiche eingestellt haben, gehen Sie im Assistenten mit der Schaltfläche **Skip** weiter.

Protegus 2 kann den Zustand der Bereiche nur dann richtig anzeigen, wenn die Zentrale die Scharf- und Unscharfschaltereignisse mit der richtigen Bereichsnummer sendet. Die Details und Fallstricke der Scharfschaltung über Schlüsselschalter behandelt ein eigener Artikel: Fern-Scharfschaltung über Schlüsselschalter aus der Protegus-2-App.



Abbildung 38. Protegus 2 – die Seite „Die Anlage wird nicht direkt aus der Ferne gesteuert“ beim Anlegen der Anlage: Mit der Schaltfläche Continue gelangen Sie zur Einrichtung von Bereich und PGM-Ausgang.

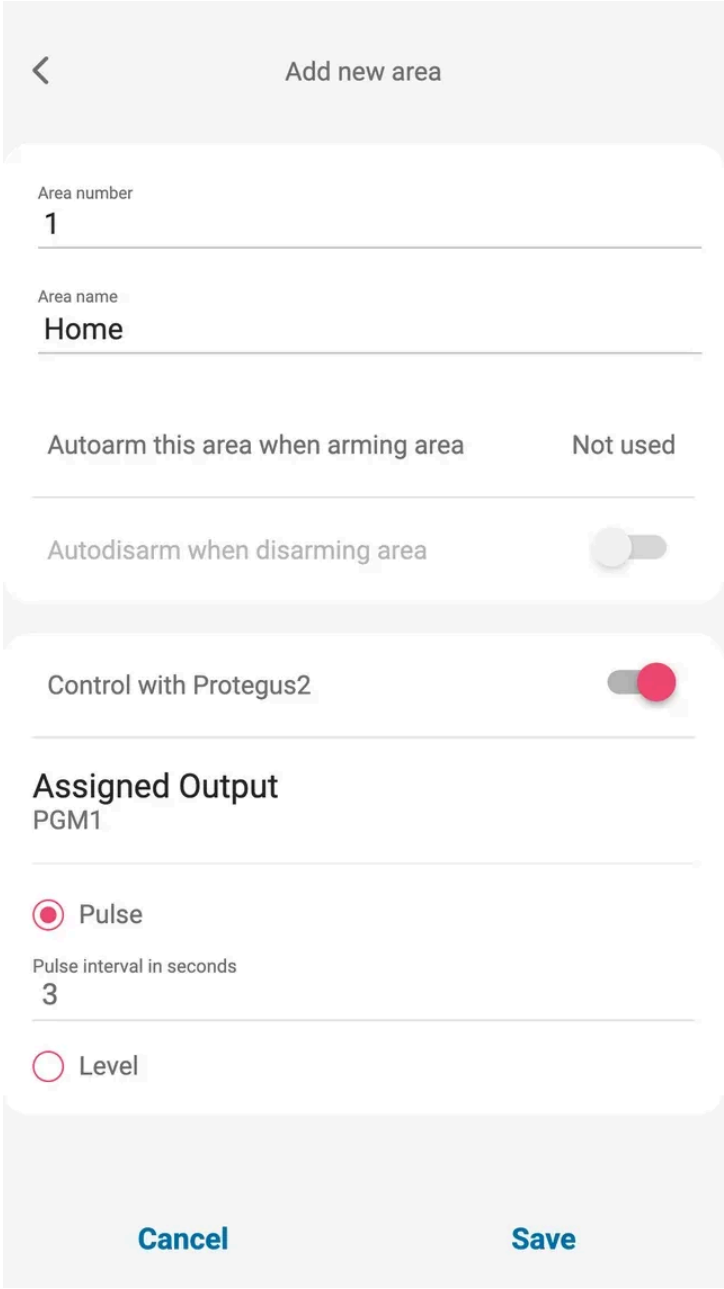


Abbildung 39. Protegus 2 – Bereich anlegen (Add new area): Area number, Area name, Control with Protegus2 eingeschaltet, Assigned Output PGM1, Pulse (3 s) oder Level, dann Save.

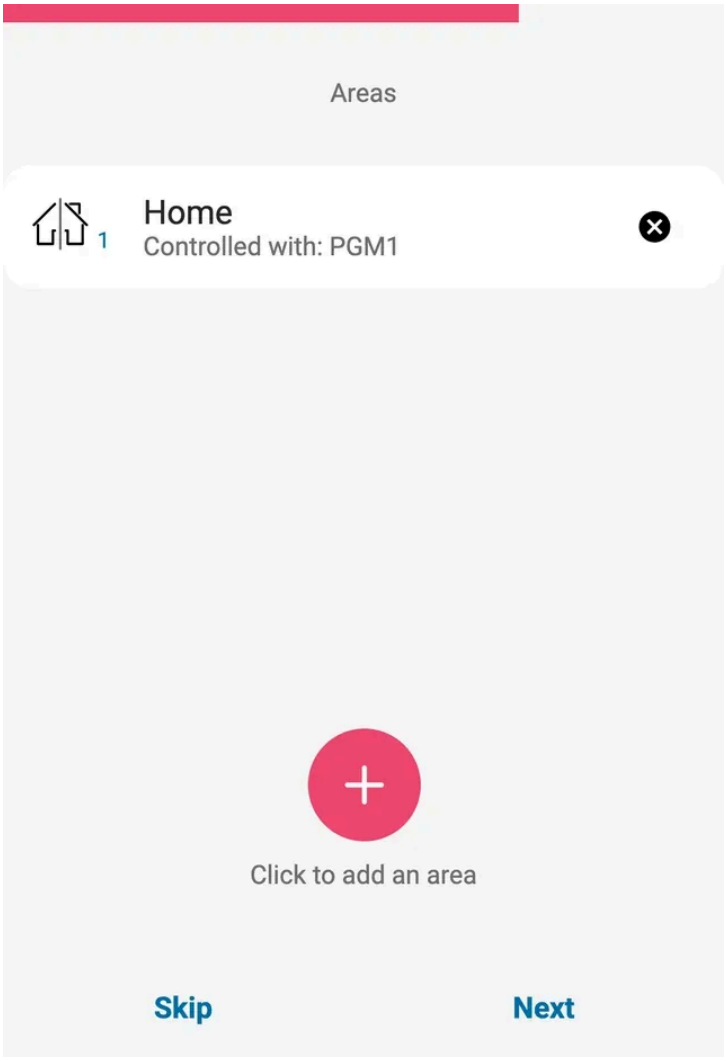


Abbildung 40. Protegus 2 – die Liste der Bereiche (Areas): Der Bereich Home wird von PGM1 gesteuert; weitere Bereiche mit der Schaltfläche Click to add an area, der Assistent lässt sich mit Skip beenden.

5.3 Scharf- und Unscharfschalten aus der App

1. Öffnen Sie das System in der Protegus-2-App. Auf dem Startbildschirm hat jeder Bereich eine eigene Karte und ein eigenes Schloss: Das **geschlossene, rote Schloss** steht für einen scharfgeschalteten, das **offene, grüne Schloss** für einen unscharfgeschalteten Bereich.
2. Tippen Sie auf das Schloss des Bereichs und wählen Sie die gewünschte Aktion: Scharfschalten oder Unscharfschalten.
3. Wenn die App danach fragt, geben Sie den PIN-Code ein.

Das Schloss nimmt den tatsächlichen Zustand aufgrund des von der Alarmzentrale eingehenden Ereignisses an; die App meldet in der Ereignisliste und per Benachrichtigung auch zurück, ob die Zentrale die Aktion ausgeführt hat.

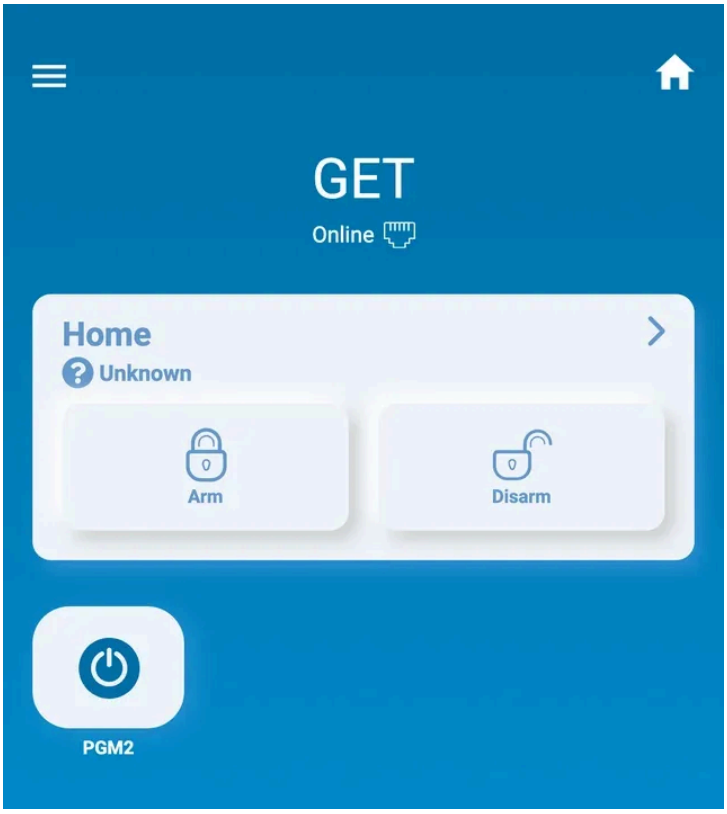


Abbildung 41. Protegus 2 – der Startbildschirm der Anlage: der Zustand des Bereichs, die Schaltflächen Arm und Disarm, darunter der schaltbare PGM-Ausgang.

6. Die Einstellungen im Detail

Die meisten Einstellungen des GET sind sowohl im unter Windows laufenden Programm **TrikdisConfig** als auch in der App **Protegus 2** (**Settings** → **Advanced settings**, Abschnitt 2.2) verfügbar; wo etwas nur in einem der beiden vorhanden ist, weisen wir darauf hin. Jede Einstellung beschreiben wir einmal und geben je Abschnitt an, wo Sie sie in den beiden Werkzeugen finden; in Klammern steht die Beschriftung der App, wenn sie von der in TrikdisConfig abweicht. Im TrikdisConfig-Fenster sehen Sie links die Liste der Seiten (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), oben die Schaltflächenleiste (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), unten die Statusleiste.

6.1 Verbindung mit dem Kommunikator

App Protegus 2. Öffnen Sie die Anlage und gehen Sie in das Menü **Settings** → **Advanced settings**. Oben auf jedem Bildschirm stehen die Daten des verbundenen Geräts: **Unique ID** (IMEI), **Serial** (Seriennummer), Version von **Firmware** und **Boot**. Die Gruppen der Einstellungen im Menü: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** und **System events**. Nach einer Änderung schreiben Sie die Einstellungen mit der Schaltfläche **Write** in das Gerät; **Read** liest die aktuellen Werte erneut aus dem Gerät aus.

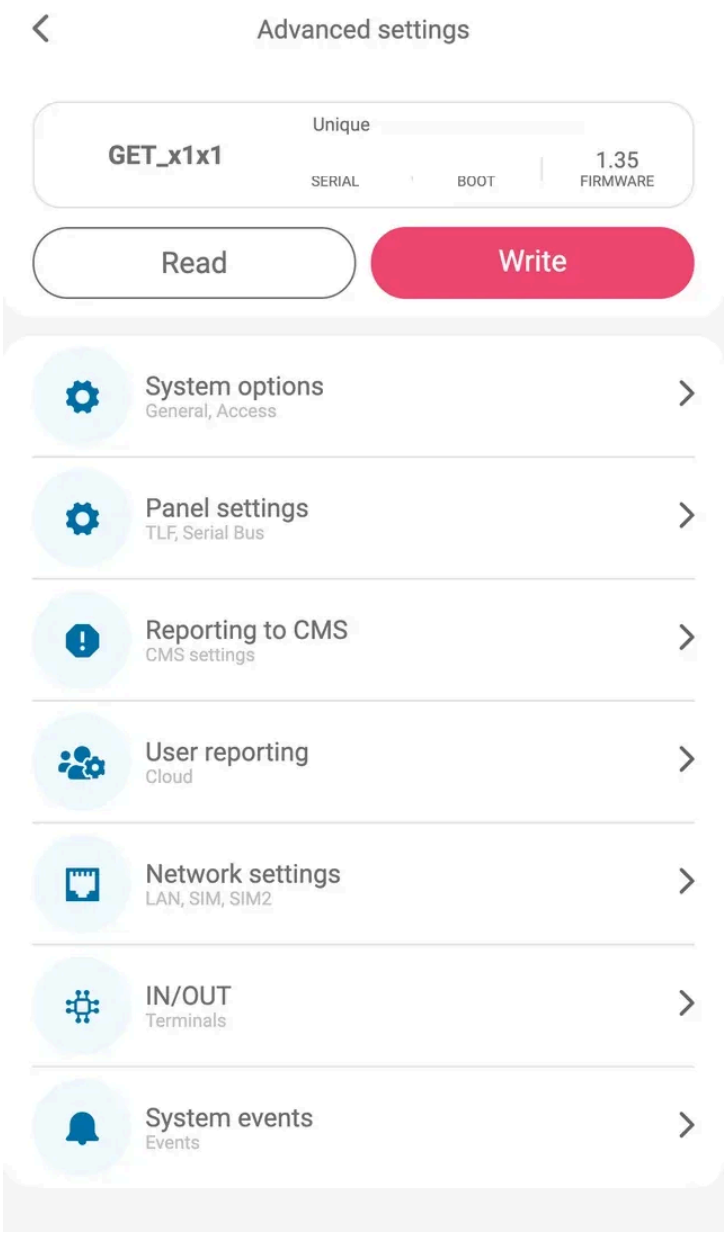


Abbildung 42. Protegus 2 – Menü Advanced settings: oben die Daten des Geräts (Typ, Unique ID, Seriennummer, Boot- und Firmware-Version), die Schaltflächen Read und Write, darunter die Gruppen der Einstellungen.

TrikdisConfig. Nach dem Verbinden des Kommunikators und dem Drücken von **Read [F4]** zeigt das Programm die Daten des Geräts in der Statusleiste an.

Nach dem Anschließen und Auslesen des Geräts (**Read [F4]**) werden unten im Fenster die wichtigsten Daten des Geräts angezeigt:

Beschriftung	Bedeutung
IMEI / Unique ID, bei einem Ethernet-Gerät **MAC / Unique ID**	Die eindeutige Kennung des Geräts: bei einem Gerät mit SIM-Karte die IMEI, bei einem Ethernet-Gerät die MAC-Adresse. Dieselbe steht auf der Verpackung und auf der Rückseite des Geräts.
Status	Der aktuelle Betriebszustand.

Beschriftung	Bedeutung
Device	Der Gerätetyp (Typbezeichnung). Prüfen Sie, ob hier der Typ Ihres eigenen Geräts steht.
SN	Seriennummer.
BL	Die Version des Bootloaders.
FW	Die Version der Firmware.
HW	Die Version der Hardware.
State	Die Verbindungsart: USB oder Fernzugriff (remote).
Administrator / Installer	Die Zugriffsebene der programmierenden Person (nach Eingabe des Passworts).

Nach Abschluss der Einstellungen schreiben Sie sie mit der Schaltfläche **Write [F5]** in das Gerät; mit den Schaltflächen **Open [F8]** und **Save [F9]** können Sie den gesamten Einstellungssatz in einer Datei speichern und in ein anderes Gerät laden. **Save [F9]** speichert die Einstellungen in einer Einstellungsdatei, **Open [F8]** öffnet die gespeicherte Datei; die gespeicherten Einstellungen können Sie später auch in andere Geräte laden und so mehrere Geräte schnell mit identischen Einstellungen einrichten.



Abbildung 43. Die Statusleiste von TrikdisConfig mit ausgelesenem GET: Kennung, Zustand, Typ (Device: GET_S170), Seriennummer, Version von BL (Bootloader), FW und HW, Verbindungsart und Zugriffsebene.

Im Feld **Device** muss eine GET-Typbezeichnung stehen (im Bild GET_S170; das Buchstaben-Ziffern-Suffix bezeichnet die Hardwarevariante), **BL** ist die Version des Bootloaders. Nach **Read [F4]** liest das Programm die im Gerät eingestellten Werte aus und zeigt sie an; nehmen Sie die nötigen Einstellungen gemäß den folgenden Seitenbeschreibungen vor.

6.2 System settings (System options)

In der App: Advanced settings → System options → System general (Kennungen, Zeitsynchronisation) und **System options → Access** (Codes und Errichterrechte). Wo sich **Account No.** und **Device account No.** befinden, hängt von Hardwarevariante und Firmware ab: Bei Hardware **x1x1** mit Firmware **1.31** oder neuer finden Sie sie auf der Seite **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.**; beim parallelen Kanal **Parallel Account no.**) und auf der Seite **Reporting to CMS → Settings** (**Device account No.**), auf der Seite System general bleibt nur **Time set**; andernfalls befinden sich beide auf der Seite System general.

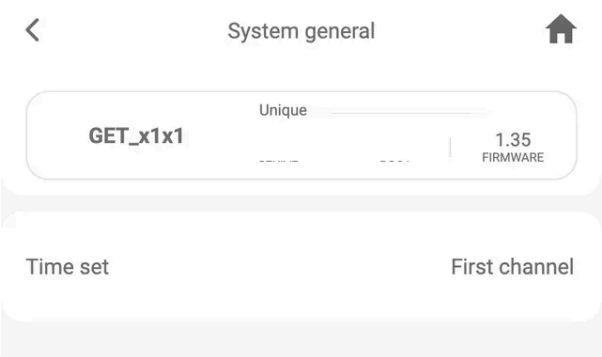


Abbildung 44. Protegus 2 – System options → System general bei Hardware x1x1 (Firmware 1.35): Nur Time set ist sichtbar, die Kennungen befinden sich bei den CMS-Einstellungen.

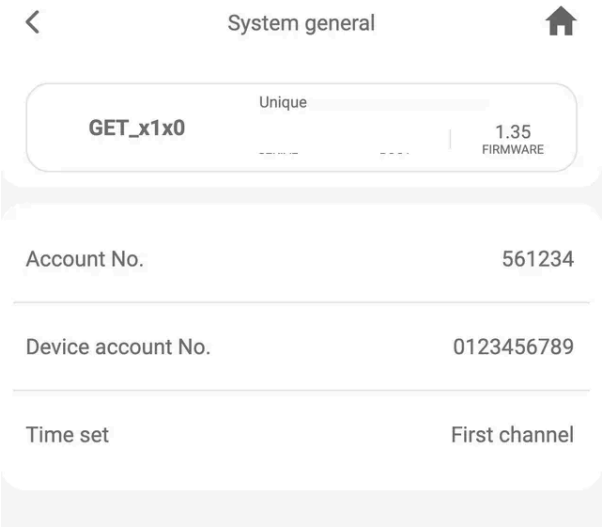


Abbildung 45. Protegus 2 – System options → System general bei Hardware x1x0: Account No., Device account No. und Time set.

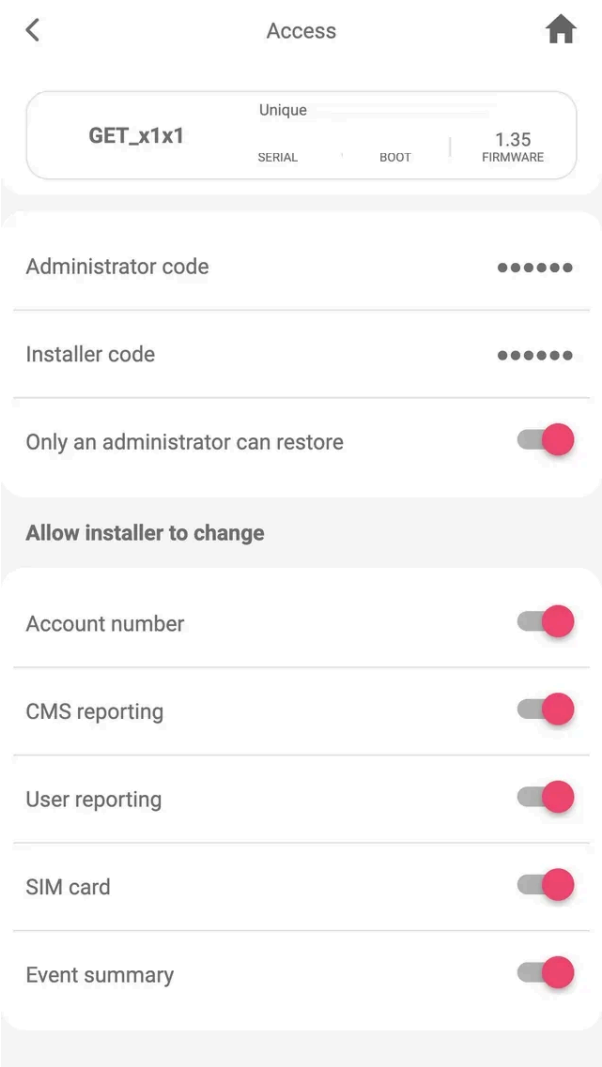


Abbildung 46. Protegus 2 – System options → Access: Administrator code, Installer code, Only an administrator can restore und die Liste Allow installer to change (Account number, CMS reporting, User reporting, SIM card, Event summary).

In TrikdisConfig: Die Seite **System settings** besteht aus zwei Gruppen: In der Gruppe **General** stellen Sie die Kennungen des Geräts ein, in der Gruppe **Access** die Zugriffsebenen.

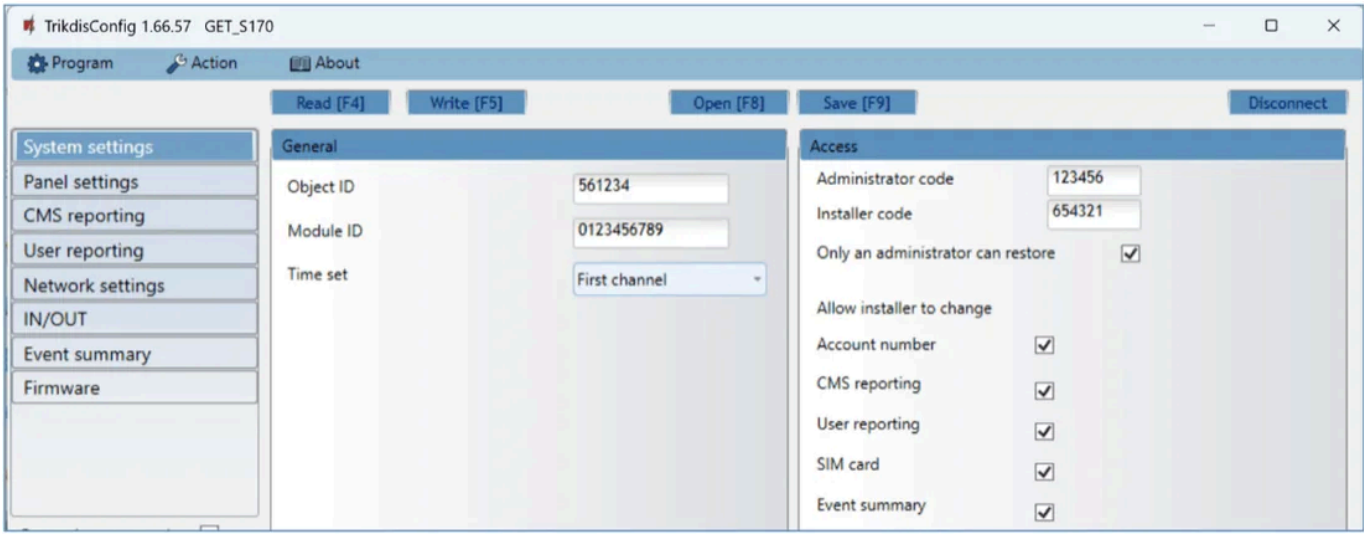


Abbildung 47. TrikdisConfig – Seite System settings: Gruppe General (Object ID, Module ID, Time set) und Gruppe Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – die von der Leitstelle erhaltene Objektkennung (6 hexadezimale Zeichen: 0–9, A–F; `FFFE` und `FFFF` sind nicht verwendbar). Pflichtangabe, wenn das Gerät auch an eine Leitstelle meldet.
- **Module ID** (Device account No.) – die Kennnummer des Moduls.
- **Time set** – von welchem Server das Gerät seine Uhr synchronisiert.

In der Gruppe **Access** verwalten Sie die Zugriffsebenen und Passwörter.

Für die Einstellungen des Geräts gibt es zwei Zugriffsebenen: **Administrator** und **Installateur**.

- **Administrator code** – Zugriff auf alle Einstellungen (Werkspasswort: `123456`; das Passwort hat 6 Zeichen: Ziffern oder lateinische Buchstaben).
- **Installer code** – einschränkbarer Zugriff (Werkspasswort: `654321`).
- **Only an administrator can restore** – mit Häkchen kann nur der Administrator die Wiederherstellung der Werkseinstellungen starten.
- **Allow installer to change** – hier legen Sie fest, welche Einstellungsgruppen der Installateur ändern darf: **Account number** (Objektkennung), **CMS reporting**, **User reporting**, **SIM card** (bei einem Mobilfunkgerät) oder **Ethernet settings** (bei einem Ethernet-Gerät), **Event summary**.

Lassen Sie keine Werkspasswörter im Gerät!

Ändern Sie bei der Inbetriebnahme mindestens das Administrator-Passwort und notieren Sie es an einem sicheren Ort. Ein vergessenes Passwort lässt sich auch durch die Wiederherstellung der Werkseinstellungen nicht löschen, denn auch dafür ist ein Passwort nötig: Dann kann nur der Hersteller oder der Händler das Gerät zurücksetzen, nachdem Sie es ihm geschickt haben. Ausnahme ist ein Gerät mit Hardware-RESET-Taste: Wird die Taste 10 Sekunden gedrückt gehalten, werden die Werkseinstellungen ohne Passwort wiederhergestellt.

Errichterzugang in der App. Öffnen Sie den Kommunikator mit dem Errichtercode, blendet Protegus 2 die Felder **Administrator code** und **Only an administrator can restore** aus und zeigt die vom Administrator nicht freigegebenen Einstellungen nur lesbar an. In der App gilt das Recht **SIM card** auch für die LAN-Einstellungen; wo sich die Kennungen bei den CMS-Einstellungen befinden (siehe oben), gilt für sie das Recht **CMS reporting**.

6.3 Panel settings

Auf dieser Seite legen Sie fest, wie der Kommunikator an die Alarmzentrale angeschlossen ist: Die Gruppe **TLC** (in der App **TLF**) enthält die Einstellungen für den Telefonleitungsanschluss (TIP/RING), die Gruppe **Serial bus** (**Serial Bus**) die für den Anschluss an Datenbus oder serielle Schnittstelle. In der App: **Advanced settings** → **Panel settings** → **TLF** bzw. **Panel settings** → **Serial Bus**.

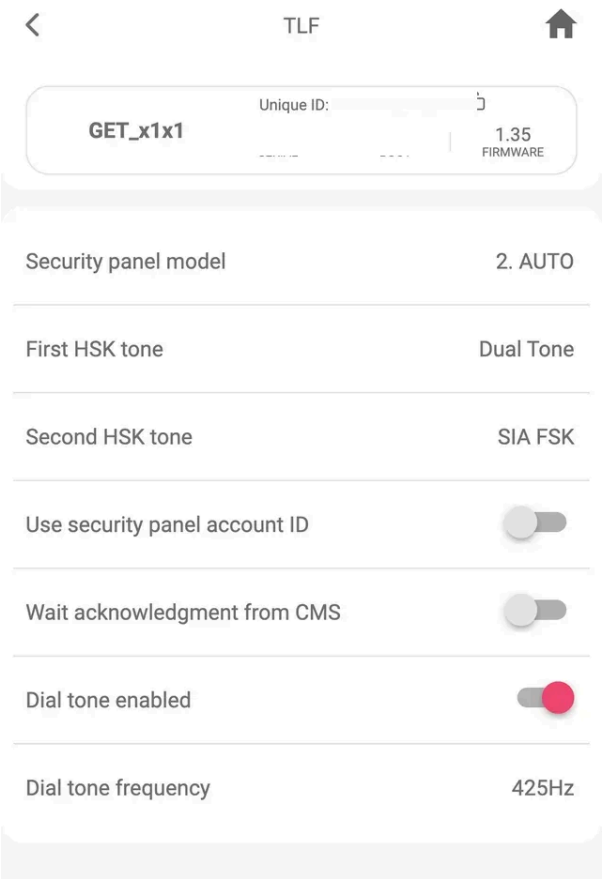


Abbildung 48. Protegus 2 – Panel settings → TLF: Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.

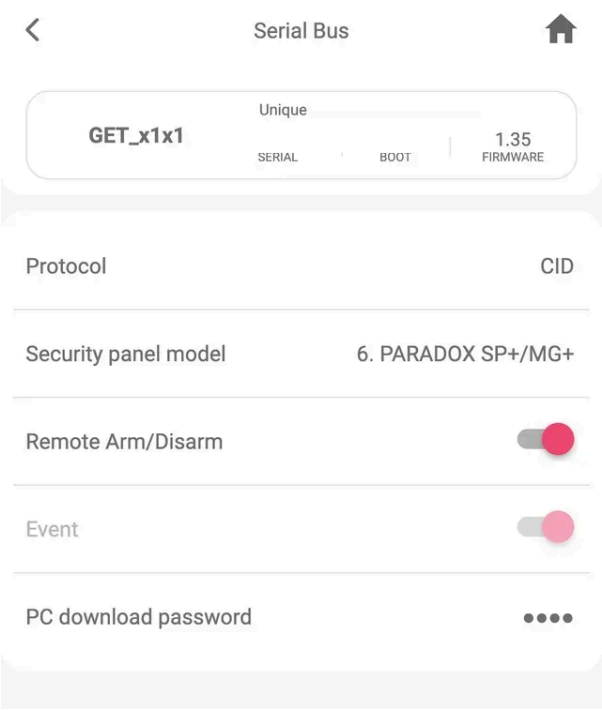


Abbildung 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm eingeschaltet, Event (nur lesbar), PC download password.

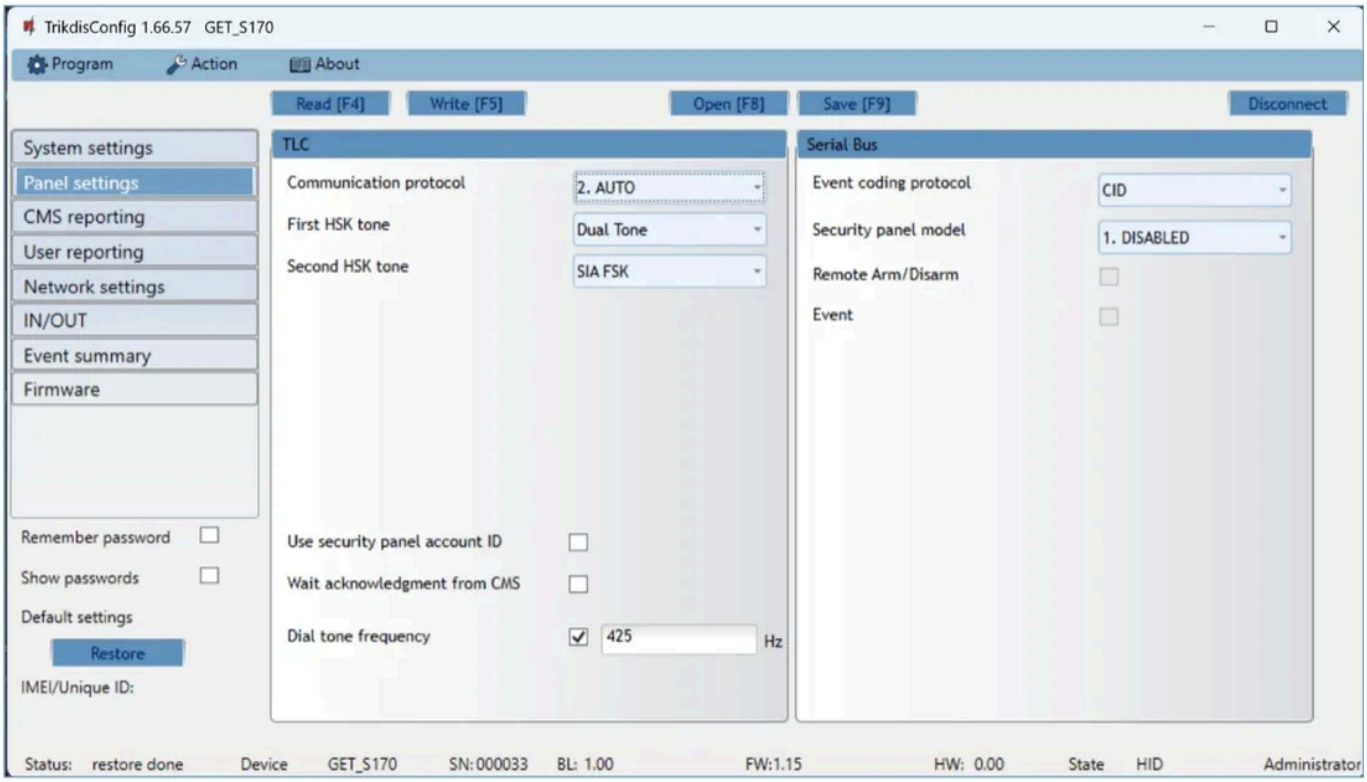


Abbildung 50. TrikdisConfig – Panel settings beim TIP/RING-Anschluss: in der Gruppe TLC Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; die Gruppe Serial bus ist in diesem Fall grau.

Gruppe TLC – wenn der Kommunikator an den Klemmen TIP/RING des Telefonwählgeräts der Zentrale angeschlossen ist:

- **Communication protocol** (Security panel model) – Einschalten (**2. AUTO**) bzw. Sperren (**1. DISABLED**) der DTMF-Telefonleitungsschnittstelle des Kommunikators. Beim TIP/RING-Anschluss wählen Sie AUTO.
- **First HSK tone**, **Second HSK tone** – der Quittungston (Handshake) der Zentrale, mit dem der Kommunikator das Wählgerät der Zentrale annimmt (im Bild Dual Tone und SIA FSK).
- **Use security panel account ID** – mit Häkchen sendet der Kommunikator nicht den Wert seines eigenen Feldes **Object ID**, sondern die in der Zentrale eingestellte und von der Zentrale gesendete Objektkennung.
- **Wait acknowledgment from CMS** – mit Häkchen wartet der Kommunikator nach dem Senden jedes Ereignisses auf die Quittung des IP-Empfängers, dass die Meldung angekommen ist; kommt keine Quittung, gibt er der Zentrale kein „Kiss-off"-Signal, und das Telefonwählgerät der Zentrale wiederholt die Meldung.
- **Dial tone frequency** – die Frequenz des Wähltons, mit dem der Kommunikator mit dem Wählgerät der Zentrale kommuniziert (Standard 425 Hz, der in den meisten europäischen Ländern übliche Wählton). Auf der Seite TLF der App gibt es zusätzlich den Schalter **Dial tone enabled**: Er schaltet den Wählton ein oder aus; die Frequenz lässt sich nur bei eingeschaltetem Wählton ändern.

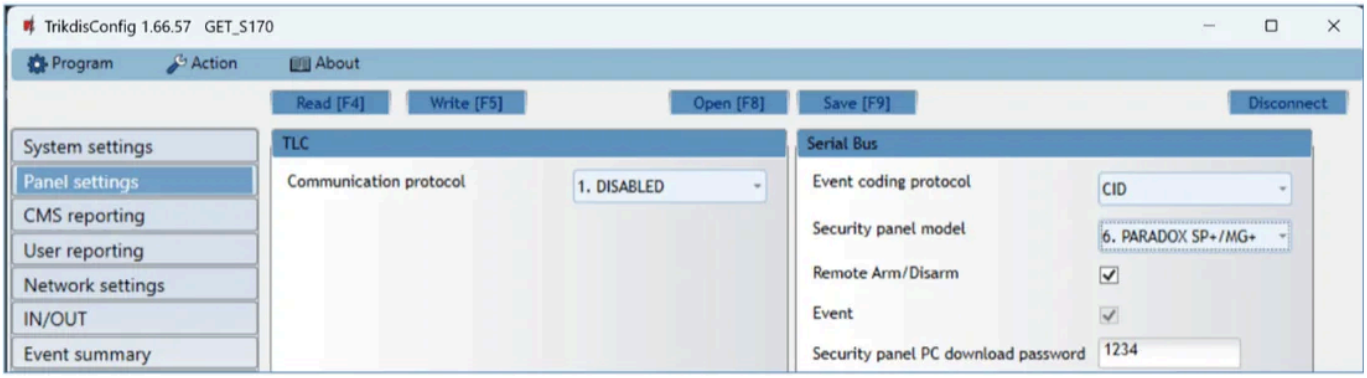


Abbildung 51. TrikdisConfig – Panel settings beim Anschluss an Datenbus oder serielle Schnittstelle: Communication protocol 1. DISABLED; in der Gruppe Serial bus Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm und Event angehakt, Security panel PC download password eingegeben.

Gruppe Serial bus – wenn der Kommunikator am Datenbus oder an der seriellen Schnittstelle der Zentrale angeschlossen ist:

- **Event coding protocol** (Protocol) – das Protokoll der Ereignismeldung: **CID** oder **SIA**.
- **Security panel model** – der Typ der angeschlossenen Alarmzentrale aus der Liste (für den Anschluss Keybus + TIP/RING der Paradox SP / SP+ / MG / MG+ wählen Sie den Eintrag **Paradox SP+/MG+ series KeyBus**, Abschnitt 3.3.3).
- **Remote Arm/Disarm** – mit Häkchen steuert der Kommunikator die Zentrale direkt (Scharf- und Unscharfschalten aus Protegus 2). Nur bei direkt steuerbaren Zentralen sichtbar. Für die direkte Steuerung muss auch die Zentrale gemäß Abschnitt 4.1 eingerichtet werden.
- **Event** – mit Häkchen sendet der Kommunikator die Ereignisse der Zentrale an die Leitstelle und an Protegus 2. Die App zeigt diesen Schalter an, dort lässt er sich aber nicht ändern.
- **Security panel PC download password** (PC download password; bei Texecom der UDL passcode) – für die direkte Steuerung einer Paradox- bzw. Texecom-Zentrale das PC- bzw. UDL-Passwort; es muss mit dem in der Zentrale eingestellten Passwort übereinstimmen, dessen Eingabe Abschnitt 4.1 beschreibt.

6.4 CMS reporting (Reporting to CMS)

Der Kommunikator sendet die Ereignisse über eine IP-Verbindung an die Leitstelle – über das kabelgebundene Netzwerk (LAN) oder das Mobilfunknetz (SIM1, SIM2), in der in Abschnitt 6.4.2 eingestellten Reihenfolge. Die Ereignisse können über mehrere Kanäle gehen: Der **primäre** und der **parallele** Kanal arbeiten gleichzeitig (an zwei Empfänger gleichzeitig), und zu beiden gehört ein **Ersatzkanal**, der in Kraft tritt, wenn der jeweilige Kanal ausfällt. Die Kommunikation ist verschlüsselt und passwortgeschützt. Für die TRK-Protokolle ist ein Trikdis-Empfänger nötig, der die Ereignisse empfängt und an die Leitstellensoftware weitergibt: für die IP-Verbindung der Software-Empfänger IPcom (Windows oder Linux), der IP/SMS-Empfänger RL14 oder der Mehrkanalempfänger RM14; die Protokolle DC-09 und TL150 sind für universelle bzw. SUR-GARD-Empfänger gedacht (siehe unten, **Protocol**).

6.4.1 Empfängerkanäle (CMS settings)

In der App: Advanced settings → Reporting to CMS → CMS settings, dann **Primary channel**, **Backup channel** oder **Parallel channel** (darin **Parallel primary channel** und **Parallel backup channel**). Mit dem Einschalten des Schalters **Enabled** erscheinen die Einstellungen des Kanals.

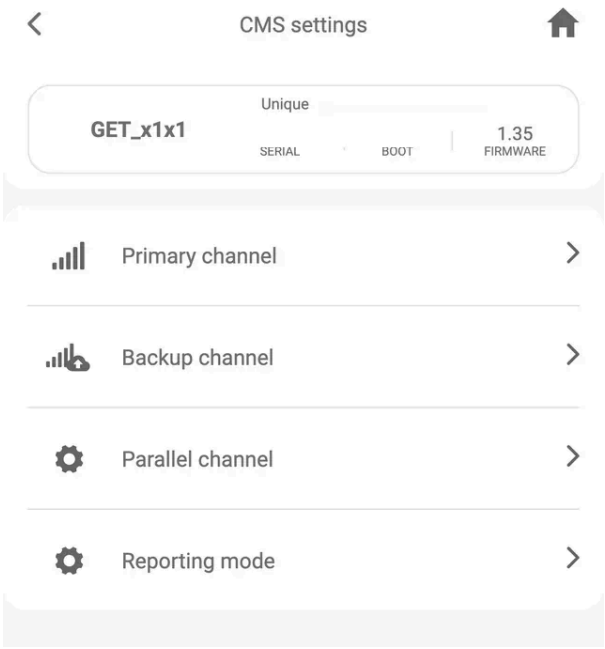


Abbildung 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel und Reporting mode.

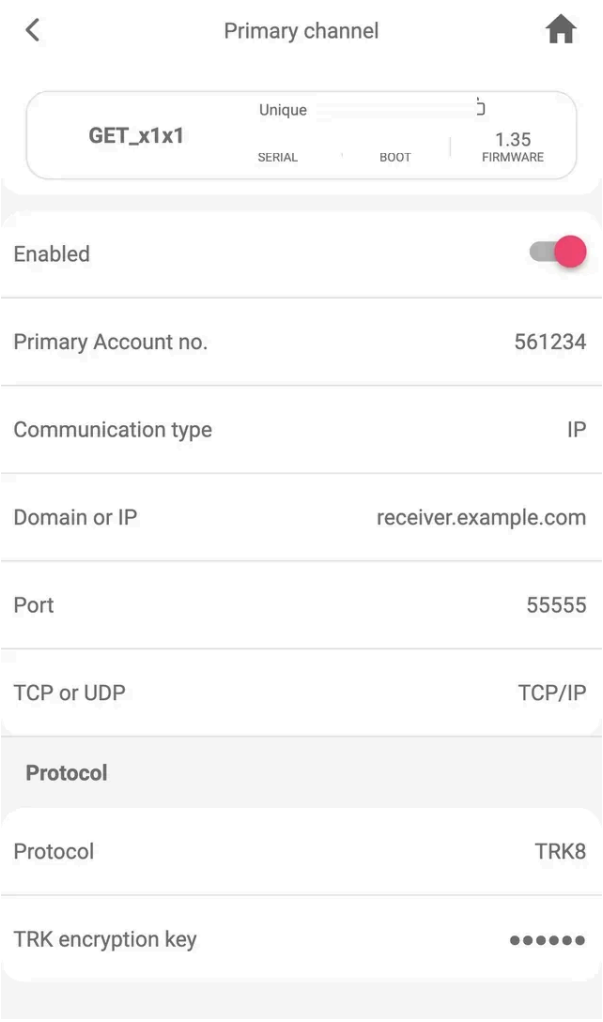


Abbildung 53. Protegus 2 – Primary channel bei Hardware x1x1: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 und der TRK encryption key.

In TrikdisConfig: der Reiter **CMS settings** der Seite **CMS reporting**.

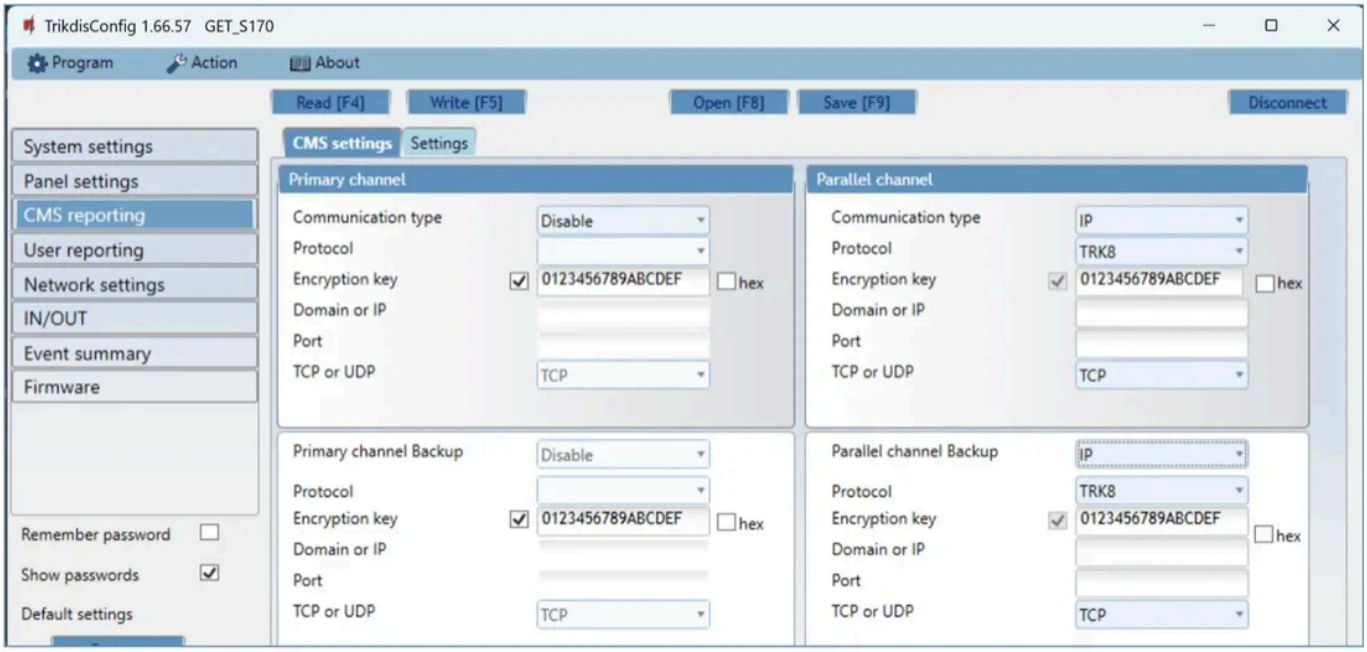


Abbildung 54. TrikdisConfig – CMS reporting, Reiter CMS settings: primärer Kanal und sein Ersatzkanal, paralleler Kanal und sein Ersatzkanal (im Bild der parallele Kanal mit der Einstellung IP / TRK8 / TCP).

Primary channel – primärer Kanal

- **Communication type** – die Art der Verbindung mit dem Empfänger: **IP**.
- **Protocol** – **TRK8** (Trikdis-Empfänger), **DC-09_2007** oder **DC-09_2012** (universelle Empfänger), **TL150** (SUR-GARD-Empfänger).
- **Encryption key** (TRK encryption key; bei den DC-09-Protokollen **Enable encryption key** und **DC-09 encryption key**, mit dem Schalter **HEX** für einen hexadezimalen Schlüssel) – der Verschlüsselungsschlüssel der Meldungen; er muss im Kommunikator und im Empfänger derselbe sein. In der App hat der TRK encryption key höchstens 6, der DC-09 encryption key höchstens 16 Zeichen (in HEX 32).
- **Domain or IP**, **Port** – Domainname oder IP-Adresse und Netzwerkport des Empfängers.
- **TCP or UDP** – das Übertragungsprotokoll.

Primary channel Backup – Ersatzkanal. Eingeschaltet übernimmt er die Kommunikation, wenn der primäre Kanal nicht funktioniert; seine Einstellungen entsprechen den obigen.

Parallel channel – paralleler Kanal. Er sendet neben dem primären Kanal gleichzeitig an einen zweiten Empfänger (zum Beispiel an die örtliche und an die zentrale Leitstelle). Seine Einstellungen sind dieselben wie beim primären Kanal.

6.4.2 Test, PING und die Reihenfolge der Verbindungen

In der App: Advanced settings → Reporting to CMS → Settings (Test, PING, Zeiten des Ersatzkanals, Empfänger- und Liniennummer) und **Reporting to CMS → CMS settings → Reporting mode** (Reihenfolge der Verbindungswege). In der App gibt es neben jedem Intervall einen Schalter: **Enable test** für Test period, **Enable ping** für IP ping period und **Test enabled** für Communication path test; auf der Seite Reporting mode heißen die Verbindungsarten **LAN**, **SIM** (die SIM1) und **SIM2**.

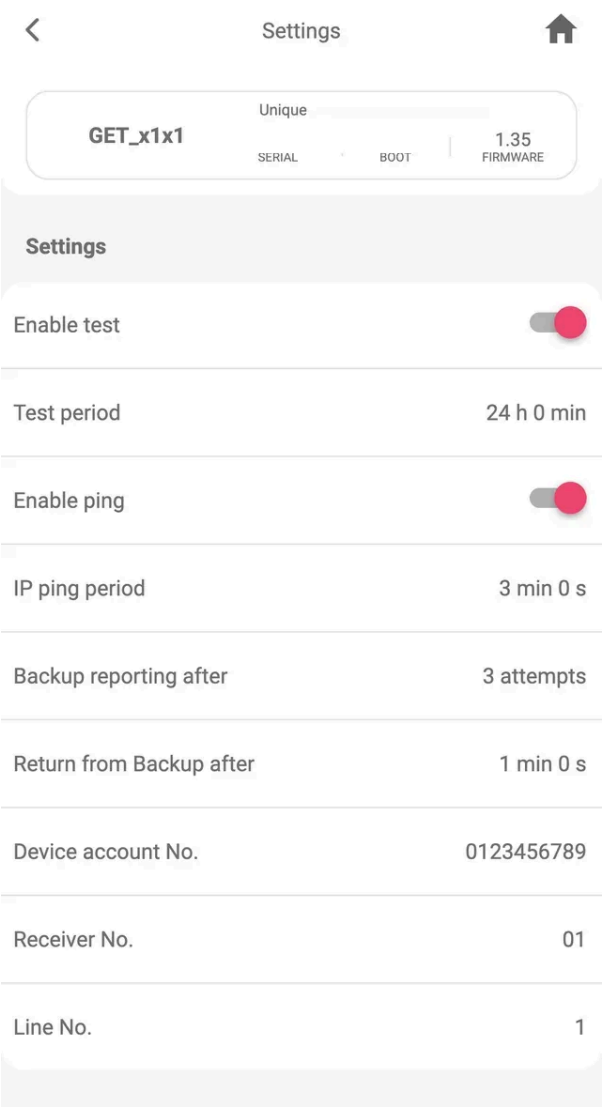


Abbildung 55. Protegus 2 – Reporting to CMS → Settings bei Hardware x1x1: Enable test und Test period, Enable ping und IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.

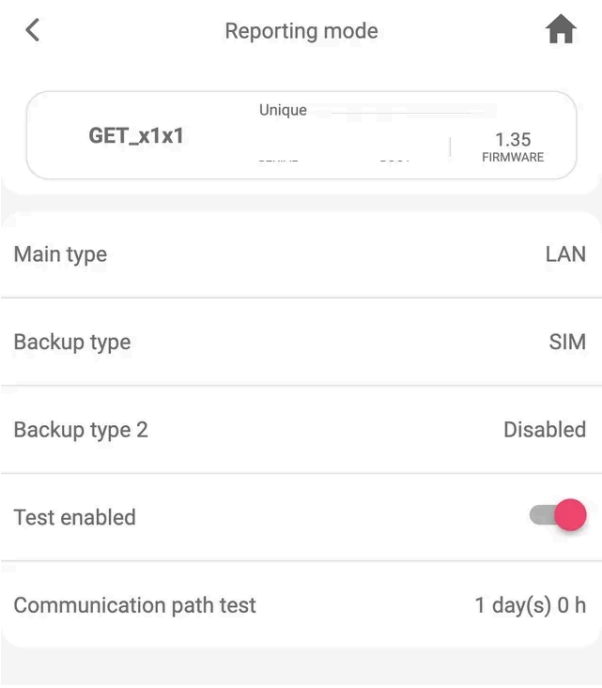


Abbildung 56. Protegus 2 – CMS settings → Reporting mode: Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled und Communication path test.

In TrikdisConfig: der Reiter **Settings** der Seite **CMS reporting**.

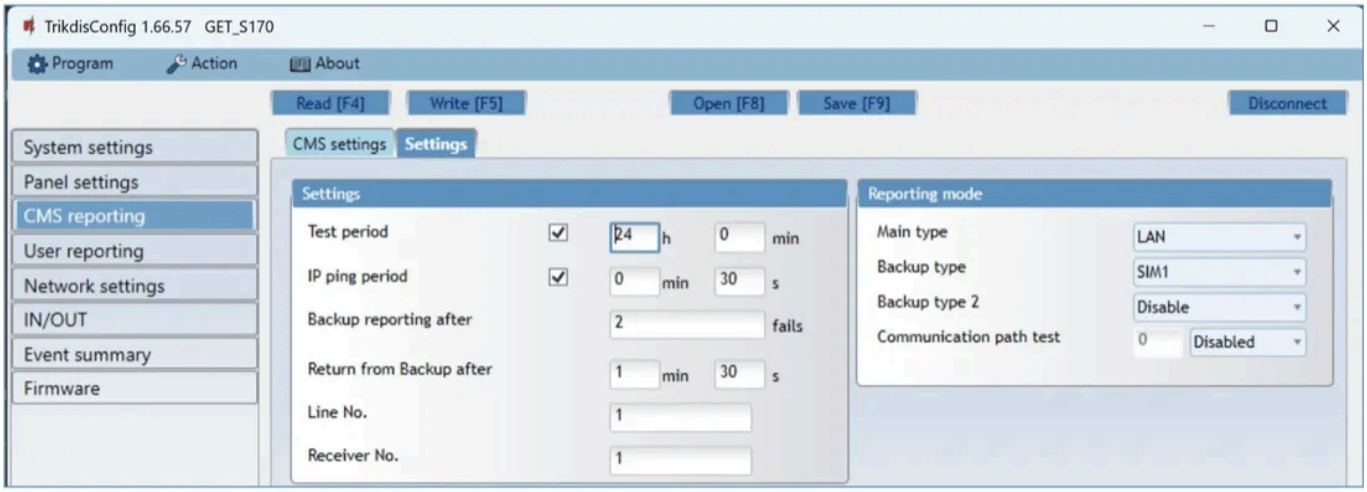


Abbildung 57. TrikdisConfig – CMS reporting, Reiter Settings: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; in der Gruppe Reporting mode Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **Test period** – Intervall des periodischen Testberichts (Standard 24 Stunden). Der Testbericht wird als Contact-ID-Meldung an die Leitstelle und an Protegus 2 gesendet.
- **IP ping period** – Intervall des Lebenszeichens (PING) auf dem IP-Kanal (Standard 30 s). Sie aktivieren es mit dem Häkchen und geben die Zeit in den Feldern für Minuten (**min**) und Sekunden (**s**) ein; es ist für die Überwachung der Verbindung erforderlich. Der Empfänger leitet die PINGs nicht an die Leitstellensoftware weiter, um sie nicht zu überlasten; die Software erhält nur dann eine Meldung, wenn der Empfänger innerhalb des Dreifachen der eingestellten Zeit keinen PING erhält. Beträgt die PING-Periode zum Beispiel 3 Minuten, wird der Verbindungsverlust nach der 9. Minute gemeldet.
- **Backup reporting after** – nach so vielen erfolglosen Sendeversuchen wechselt das Gerät auf den Reservekanal (Standard 2).

- **Return from Backup after** – nach dieser Zeit kehrt es auf den primären Kanal zurück (Standard 1 Minute 30 s).

Der PING hält die aktive Verbindung zwischen Gerät und Empfänger aufrecht; davon hängen auch Fernzugriff, Fernsteuerung und Fernprogrammierung ab. Deshalb **empfehlen wir keine PING-Periode von mehr als 5 Minuten**.

DC-09 Settings (rechts auf der Registerkarte) – nur auszufüllen, wenn Sie auf einem Kanal mit dem Protokoll DC-09_2007 oder DC-09_2012 senden; die Gruppe erscheint, wenn im Feld **Protocol** eines Kanals DC-09_2007 oder DC-09_2012 ausgewählt ist:

- **Object ID in DC-09** – 3–16-stellige hexadezimale Kennung, wird von der Leitstelle vergeben.
- **DC-09 line No** – die Liniennummer.
- **DC-09 receiver No.** – die Empfängernummer.

Auf dem Reiter Settings des GET befinden sich auch die Felder **Line No.** (Liniennummer des Empfängers) und **Receiver No.** (Empfängernummer); ein eigenes Feld „Object ID in DC-09“ gibt es beim GET nicht.

Gruppe Reporting mode – hier legen Sie fest, auf welchem Weg der Kommunikator mit den Leitstellenkanälen und mit Protegus 2 kommuniziert. Die Verbindungsarten geben Sie in einer Reihenfolge an: Kommt die Verbindung nach **Main type** nicht zustande, wechselt der Kommunikator auf die nach **Backup type** und so weiter; ist die Meldung über den Ersatzweg gesendet worden, versucht er nach Ablauf der eingestellten Zeit (Return from backup after) erneut den Hauptweg.

- **Main type** – die Art der Hauptverbindung mit dem Empfänger und mit Protegus 2: **LAN**, **SIM1** oder **SIM2**.
- **Backup type** – die Art der Ersatzverbindung (LAN, SIM1, SIM2).
- **Backup type 2** – die Art der zweiten Ersatzverbindung (LAN, SIM1, SIM2).
- **Communication path test** – in welchem Intervall der Kommunikator die gewählten Verbindungsarten (LAN, SIM1, SIM2) ausprobiert.

6.5 User reporting (Protegus Cloud)

Mit dem Dienst Protegus 2 überwacht und steuert der Benutzer den Kommunikator und die daran angeschlossene Anlage aus der Ferne; Details: web.protegus.app. In der App: **Advanced settings** → **User reporting** → **Cloud**; in TrikdisConfig der Reiter **PROTEGUS Cloud** der Seite **User reporting**.

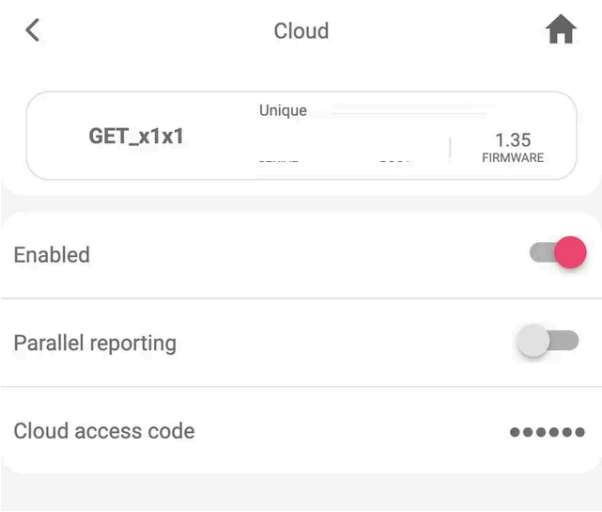


Abbildung 58. Protegus 2 – User reporting → Cloud: Enabled, Parallel reporting, Cloud access code.

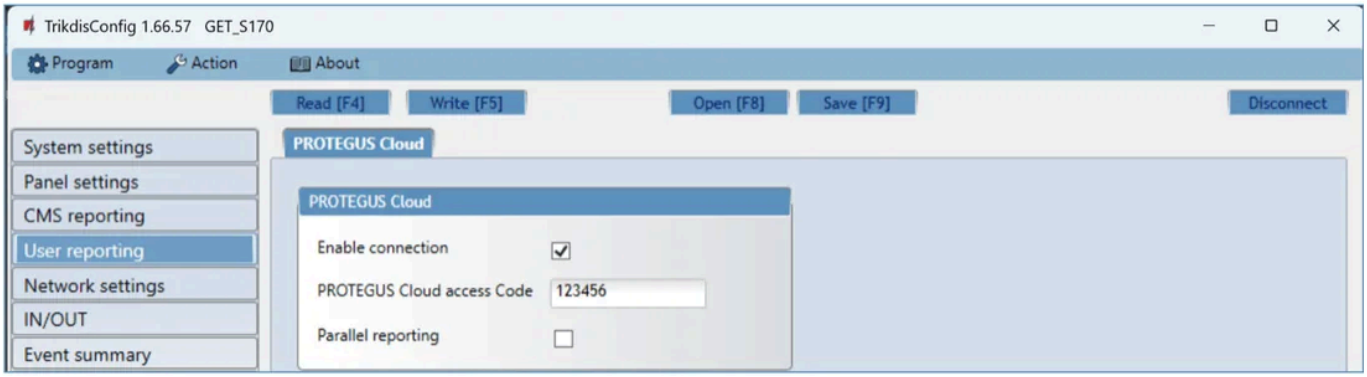


Abbildung 59. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – aktiviert den Dienst Protegus 2: Das Gerät tauscht Daten mit der App Protegus 2 aus, und TrikdisConfig erreicht es auch aus der Ferne.
- **PROTEGUS Cloud access Code** (Cloud access code) – 6-stelliger Code für die Verbindung mit Protegus 2 (werkseitig `123456`). Wenn Sie ihn in TrikdisConfig ändern, muss er auch in der App Protegus 2 geändert werden.
- **Parallel reporting** (in der App nur sichtbar, wenn die Firmware es unterstützt) – mit Häkchen gehen die Meldungen gleichzeitig über den primären Kanal (an die Leitstelle) und an Protegus 2; Protegus 2 und die Benutzer erhalten die Meldung erst, nachdem sie an die Leitstelle gegangen ist.

6.6 Network settings

6.6.1 LAN (Ethernet)

Diese Einstellungen sind nötig, wenn der Kommunikator am kabelgebundenen lokalen Netzwerk (LAN) angeschlossen ist. In der App: **Advanced settings** → **Network settings** → **LAN**; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** und **DNS2** lassen sich nur bei ausgeschaltetem **Use DHCP** ändern. In TrikdisConfig der Reiter **LAN** der Seite **Network settings**, Gruppe **Ethernet settings**.

Was muss das Netzwerk bieten? Der Kommunikator baut die ausgehende Verbindung zum Leitstellenempfänger und zur Protegus-Cloud selbst auf, deshalb müssen am Router **keine Ports geöffnet oder weitergeleitet werden**, und weder eine öffentliche feste IP-Adresse noch dynamisches DNS ist nötig. Erforderlich sind:

- ein freier Ethernet-Port am Router oder Switch;
- DHCP (Werkseinstellung) oder eine vom Netzwerkadministrator vergebene feste IP-Adresse, Subnetzmaske, Gateway und DNS;
- die Freigabe des ausgehenden Datenverkehrs zur Adresse und zum Port des Empfängers (TCP oder UDP, je nach Einstellung des Empfängers) sowie zur Protegus-Cloud.

In gefilterten Netzwerken – in Unternehmen und Institutionen – stimmen Sie dies vorab mit dem Netzwerkadministrator ab: Bei Heimroutern sind standardmäßig alle ausgehenden Verbindungen erlaubt, in einem durch eine Firewall geschützten Netzwerk kann jedoch eine eigene Regel nötig sein.

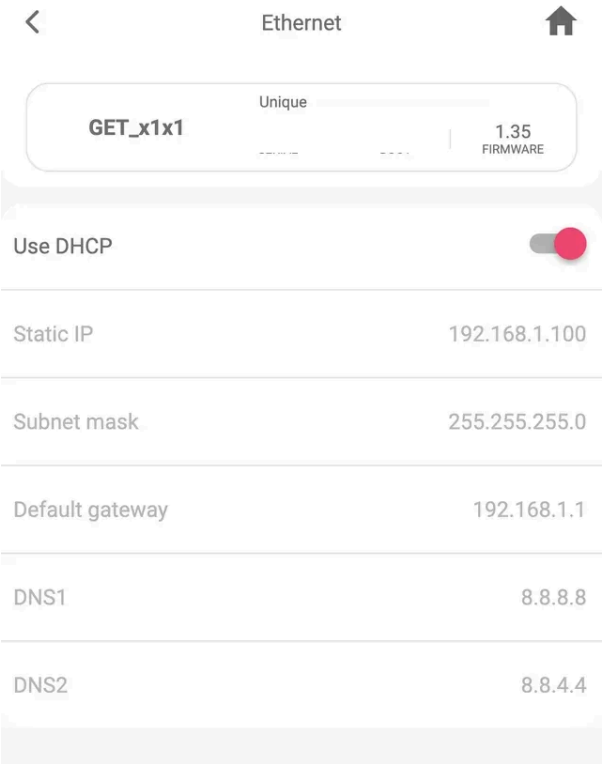


Abbildung 60. Protegus 2 – Network settings → LAN: Use DHCP eingeschaltet; die Felder Static IP, Subnet mask, Default gateway, DNS1 und DNS2 sind in diesem Fall grau.



Abbildung 61. TrikdisConfig – Network settings, Reiter LAN, Gruppe Ethernet settings: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

- **Use DHCP** – mit Häkchen meldet sich der Kommunikator automatisch im Netzwerk an (er erhält seine Adresse vom DHCP-Server des Routers). Gelingt die automatische Anmeldung nicht, müssen die Adressen von Hand eingegeben werden:
- **Static IP** – die feste IP-Adresse des Kommunikators bei manueller Einstellung.
- **Subnet mask** – Subnetzmaske bei manueller Einstellung.
- **Default gateway** – die Adresse des Gateways (Routers) bei manueller Einstellung.
- **DNS1, DNS2** – Nameserver (DNS, Domain Name System: liefert die zum Domainnamen gehörende IP-Adresse); sie sind nötig, wenn Sie den Empfänger im Feld **Domain or IP** des Kanals mit einem Domainnamen und nicht mit einer IP-Adresse angegeben haben. Standard ist der öffentliche DNS von Google. Prüfen Sie unabhängig von den IP-Einstellungen, ob die DNS-Adressen bei Ihrem Internetanbieter funktionieren.

6.6.2 SIM1 und SIM2

Diese Einstellungen sind für jede eingesetzte SIM-Karte separat vorzunehmen; die Einstellungen der Halter SIM1 und SIM2 sind gleich.

Vergewissern Sie sich vor der Verwendung, dass die SIM-Karte aktiv ist und funktioniert und dass auf der Karte auch der mobile Datendienst freigeschaltet ist.

In der App: **Advanced settings** → **Network settings** → **SIM** (die SIM1) oder **SIM2**. In TrikdisConfig der Reiter **SIM1** bzw. **SIM2** der Seite **Network settings**, Gruppe **SIM card**.

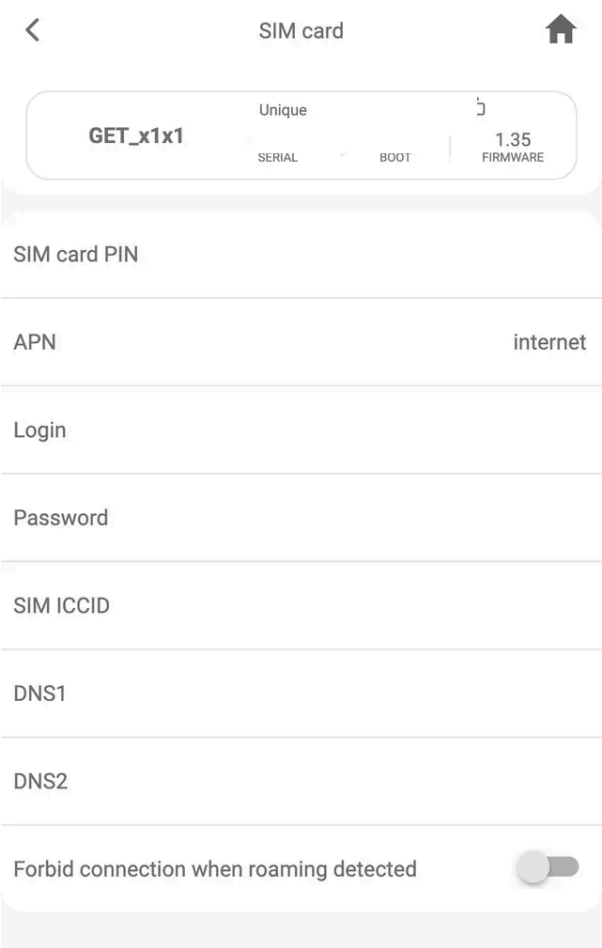


Abbildung 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 und der Schalter Forbid connection when roaming detected.

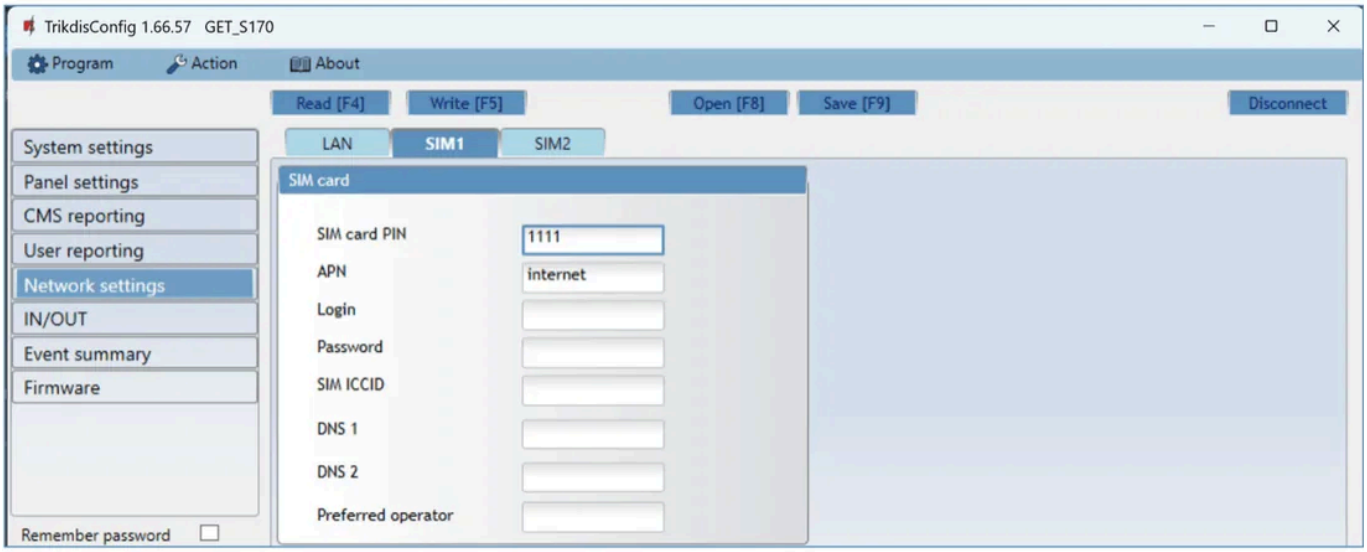


Abbildung 63. TrikdisConfig – Network settings, Reiter SIM1, Gruppe SIM card: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (der Reiter SIM2 ist genauso aufgebaut).

- **SIM card PIN** – die PIN der Karte. Die PIN-Abfrage schalten Sie aus, indem Sie die Karte in ein Mobiltelefon einsetzen und sie dort deaktivieren; dann kann der Werkswert des Feldes bleiben.

- **APN** – der Zugangspunkt des Anbieters (Access Point Name); ohne ihn verbindet sich das Gerät nicht mit dem Internet. Den Wert finden Sie auf der Website des Anbieters der SIM-Karte; `internet` ist allgemein gültig und funktioniert in den Netzen vieler Anbieter. Die bekannten APNs der Anbieter listet der APN-Artikel auf (bei einer IoT- / M2M-Karte gibt der Anbieter einen eigenen APN an, siehe Abschnitt 2.3).
- **Login, Password** – Benutzername und Passwort für die Internetverbindung, wenn der Anbieter sie verlangt.
- **SIM ICCID** – die ICCID-Nummer der SIM-Karte, wenn das Gerät nur mit dieser Karte arbeiten soll.
- **DNS1, DNS2** – Nameserver; sie sind nötig, wenn Sie den Empfänger im Feld **Domain or IP** des Kanals mit einem Domainnamen angegeben haben. Standard ist der öffentliche DNS von Google; prüfen Sie, ob die DNS-Adressen bei Ihrem Anbieter funktionieren.
- **Preferred operator** – der Code des Mobilfunkanbieters (MCC + MNC); wenn Sie ihn angeben, verbindet sich das Gerät nur mit dem Netz des gewählten Anbieters. Gibt es **nur in TrikdisConfig**.

Auf der Seite SIM der App gibt es statt Preferred operator den Schalter **Forbid connection when roaming detected**: Eingeschaltet verbindet sich der Kommunikator nicht, wenn er Roaming erkennt. Bei der Hardwarevariante **M15** mit Firmware **1.17** oder neuer erscheinen auf der Seite SIM auch die Einstellungen **Generation** und **Bands**: Damit können Sie einschränken, welche Mobilfunktechnologie und welche Frequenzbänder der Kommunikator verwendet.

6.7 IN/OUT

Hier legen Sie die Rolle der beiden I/O-Klemmen mit Doppelfunktion des Kommunikators fest: **Disabled** (nicht verwendet), **IN** (Eingang) oder **OUT** (Ausgang; beim GET die Werkseinstellung). Bei einem Eingang muss im Feld **Type** auch der Typ des angeschlossenen Stromkreises angegeben werden (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). An die Eingänge lassen sich weitere Melder anschließen: Wird der Melder ausgelöst, sendet der Kommunikator ein eigenes Ereignis mit dem dem Eingang zugeordneten Contact-ID-Code (SIA-Code) an die Leitstelle und an Protegus 2.

In der App: **Advanced settings** → **IN/OUT**, dann Klemme **1** oder **2**: **Function** (Disabled, IN, OUT) und bei einem Eingang **Type**; in den Teilen **Alarm** und **Tamper** die beim Auslösen des Eingangs gesendeten Ereignis- und Wiederherstellungsmeldungen. In TrikdisConfig die Seite **IN/OUT**.

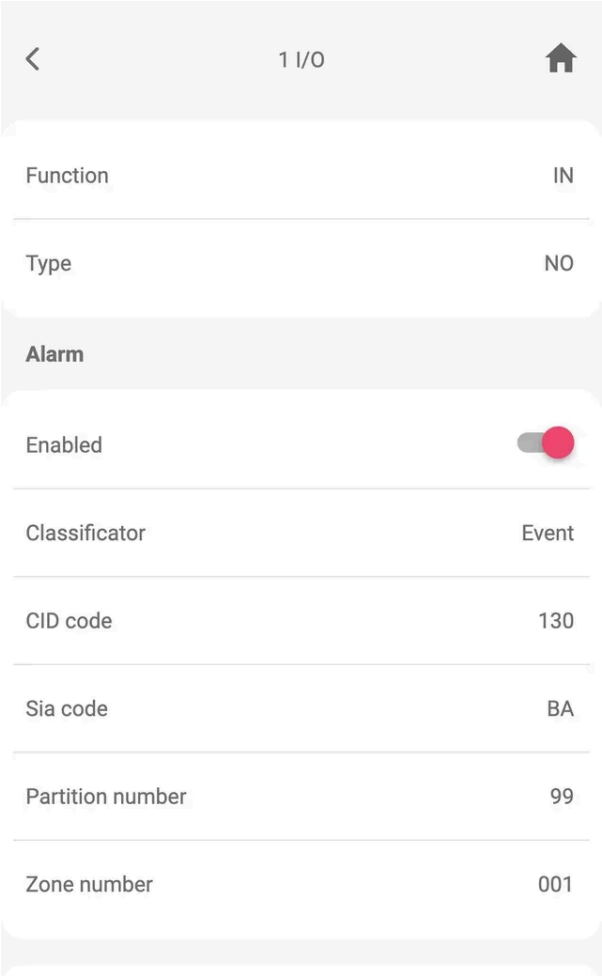


Abbildung 64. Protegus 2 – IN/OUT, Klemme 1: Function IN, Type NO; das Ereignis Alarm Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.

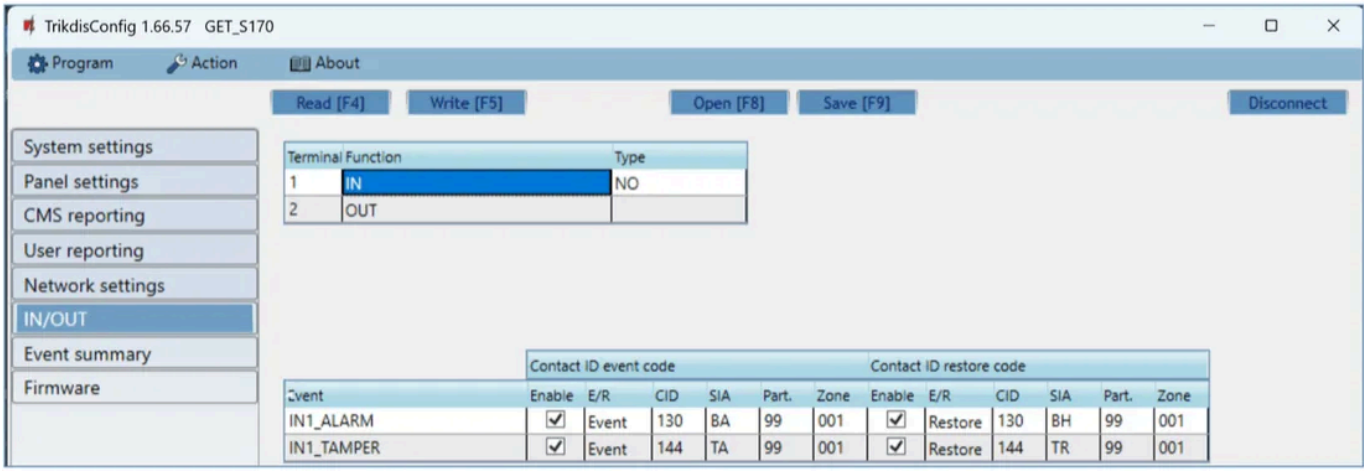


Abbildung 65. TrikdisConfig – Seite IN/OUT: Klemme 1 Eingang (IN, NO), Klemme 2 Ausgang (OUT); darunter die Alarm- und Sabotageereignisse von Eingang 1 mit CID- und SIA-Code.

Wird der am Eingang angeschlossene Melder ausgelöst, sendet der Kommunikator einen Alarm (**INx_ALARM**, Contact ID 130, SIA BA; Wiederherstellung BH), wird der Sabotagekreis verletzt, ein Sabotageereignis (**INx_TAMPER**, 144, SIA TA; Wiederherstellung TR); in der Tabelle erscheinen die Ereignisse jeder als Eingang eingestellten Klemme. Die Spalten der Tabelle:

- **Enable** (Enabled) – aktiviert das Senden der Meldung an die Leitstelle und an Protegus 2.

- **E/R** (Classificator) – der Typ der Meldung: Event (Ereignis) oder Restore (Wiederherstellung).
- **CID** (CID code) – der Contact-ID-Code (änderbar, oder der Werkswert bleibt); beim Auslösen des Eingangs geht die Meldung mit diesem Code an Protegus 2 und an die Leitstelle.
- **SIA** (Sia code) – der SIA-Code (änderbar, oder der Werkswert bleibt).
- **Part.** (Partition number) – die Nummer des Bereichs in der Meldung (beim Ereignis und bei der Wiederherstellung).
- **Zone** (Zone number) – die Nummer der Zone in der Meldung.

6.8 Event summary (System events)

Hier können Sie die eigenen, internen Meldungen des Geräts aktivieren, sperren und ändern. Eine hier gesperrte Meldung wird unabhängig von allen anderen Einstellungen nicht gesendet. In der App: **Advanced settings** → **System events**, die Meldungen stehen in den Listen **Event** und **Restore**; zum Ändern wählen Sie die Meldung aus. In TrikdisConfig die Seite **Event summary**.

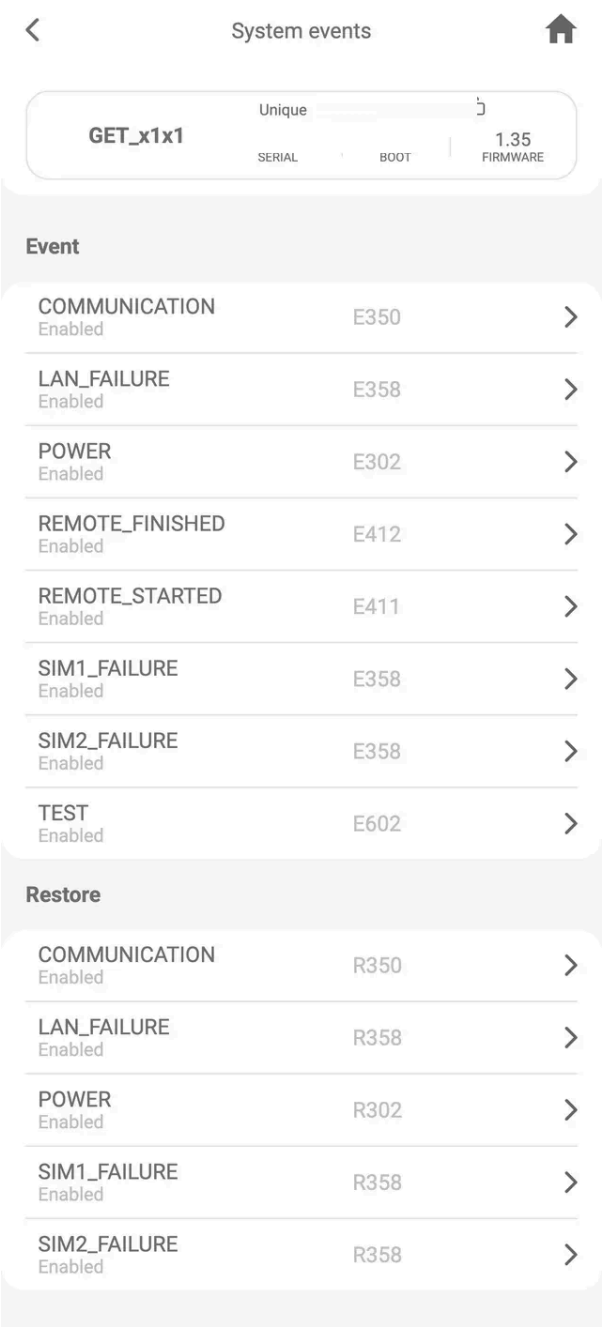


Abbildung 66. Protegus 2 – System events: die Liste Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) und die Liste Restore.

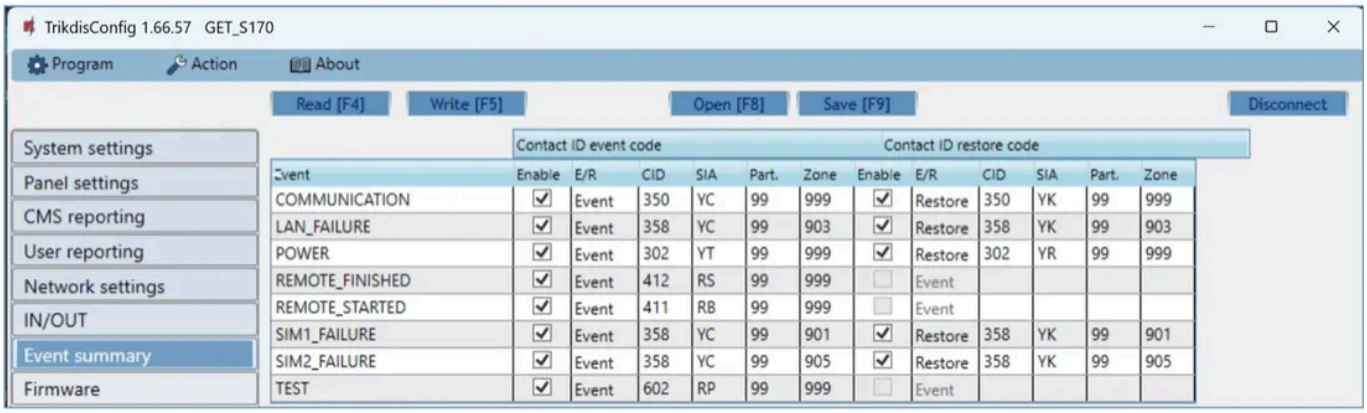


Abbildung 67. TrikdisConfig – Seite Event summary: die internen Meldungen des Geräts mit CID- und SIA-Code, mit Bereich 99.

Die internen Meldungen des GET (in Klammern der werkseitige Contact-ID-Code und die Zone):

- **COMMUNICATION** (350, Zone 999) – Fehler der Verbindung zwischen Zentrale und Kommunikator; ihre Wiederherstellung ist eine eigene Meldung.
- **LAN_FAILURE** (358, Zone 903) – Fehler der kabelgebundenen Netzwerkverbindung (LAN); ihre Wiederherstellung ist eine eigene Meldung.
- **POWER** (302, Zone 999) – niedrige Versorgungsspannung; ihre Wiederherstellung ist eine eigene Meldung.
- **REMOTE_FINISHED** (412) – Ende der Fernprogrammierung mit TrikdisConfig (Trennung).
- **REMOTE_STARTED** (411) – Fernverbindung zur Programmierung des GET mit TrikdisConfig.
- **SIM1_FAILURE** (358, Zone 901) – Fehler der Mobilfunkverbindung über SIM1; ihre Wiederherstellung ist eine eigene Meldung.
- **SIM2_FAILURE** (358, Zone 905) – Fehler der Mobilfunkverbindung über SIM2; ihre Wiederherstellung ist eine eigene Meldung.
- **TEST** (602) – periodische Testmeldung.

Das Einschalten und das Intervall der periodischen Meldung TEST stellen Sie im Feld **Test period** ein (Abschnitt 6.4.2).

- **Enable** (Enabled) – mit Häkchen ist das Senden der Meldung aktiviert.
- Bei jeder Meldung lassen sich der Contact-ID-Code (SIA-Code) sowie die Nummer von Zone und Bereich ändern.

6.9 Wiederherstellen der Werkseinstellungen

Aus der App Protegus 2 lassen sich die Werkseinstellungen **nicht** wiederherstellen: Dafür ist die Schaltfläche **Restore** in TrikdisConfig oder die Taste **RESET** am Gerät nötig.

Um die Werkseinstellungen wiederherzustellen, klicken Sie unten links im TrikdisConfig-Fenster in der Gruppe **Default settings** auf die Schaltfläche **Restore**. Die Wiederherstellung löscht alle Einstellungen – auch die Passwörter –, deshalb sollten Sie die Einstellungen vorher in einer Datei speichern (**Save [F9]**).

Mit dem Installateur-Passwort ist dies nur möglich, wenn der Administrator es auf der Seite **System settings** → **Access** nicht gesperrt hat.



Abbildung 68. TrikdisConfig – die Schaltfläche Restore der Gruppe Default settings.

Die Werkseinstellungen lassen sich auch am Gerät wiederherstellen, ohne Computer: Drücken Sie bei eingeschalteter Versorgung die Taste **RESET** auf der Leiterplatte (Abschnitt 1.4) und halten Sie sie **10 Sekunden** gedrückt, bis die LEDs NETWORK, POWER und TROUBLE erlöschen und danach die LED POWER aufleuchtet. Lassen Sie dann die Taste los: Die Werkseinstellungen sind wiederhergestellt.

7. Fernprogrammierung

TrikdisConfig erreicht die Trikdis-Geräte nicht nur über das USB-Kabel, sondern auch **aus der Ferne, über die Protegus-Cloud**. So können Sie die Einstellungen eines bereits montierten Geräts ändern, ohne zum Einsatzort fahren zu müssen.

Für den Fernzugriff erforderlich:

1. Das Gerät muss eingeschaltet sein und eine Netzwerkverbindung haben (die LEDs **POWER** und **NETWORK** leuchten grün; bei einem Mobilfunkgerät blinkt NETWORK auch gelb). Bei einem Mobilfunkgerät muss die eingelegte SIM-Karte aktiv sein und ihr PIN-Code im Gerät eingetragen oder die PIN-Abfrage deaktiviert sein; bei einem Ethernet-Gerät muss das Netzwerkkabel (LAN) eingesteckt sein, und das Gerät muss das Internet erreichen.
2. In TrikdisConfig muss auf der Seite **User reporting** → **PROTEGUS Cloud** das Häkchen bei **Enable connection** gesetzt sein (stellen Sie dies über USB bei der ersten Inbetriebnahme ein).
3. Sie müssen die **eindeutige Kennung** des Geräts (IMEI oder MAC – auf der Verpackung und auf der Rückseite des Geräts zu lesen) und das Administrator- oder Installateur-Passwort kennen.

Schritte:

1. Starten Sie die Software TrikdisConfig.
2. Geben Sie im Bereich **Remote access** im Feld **Unique ID** die eindeutige Kennung des Geräts (IMEI oder MAC) ein.
3. Geben Sie dem System nach Belieben einen Namen im Feld **System name** – das Programm merkt ihn sich, und beim nächsten Mal können Sie ihn aus der Dropdown-Liste wählen.
4. Drücken Sie die Schaltfläche **Configure**.
5. Klicken Sie im sich öffnenden Fenster auf **Read [F4]** (Lesen) und geben Sie das Passwort ein. Mit dem Häkchen **Remember password** merkt sich das Programm es für diese Sitzung.
6. Nehmen Sie die Änderungen vor und senden Sie sie dann mit der Schaltfläche **Write [F5]** (Schreiben) an das Gerät.

Früher aus der Ferne programmierte, mit Namen versehene Systeme speichert das Programm; mit dem Pfeil neben dem Feld **System name** können Sie sie auflisten. Zum Löschen markieren Sie die Kennung in der Liste, drücken Sie die Taste **Delete** und bestätigen Sie.

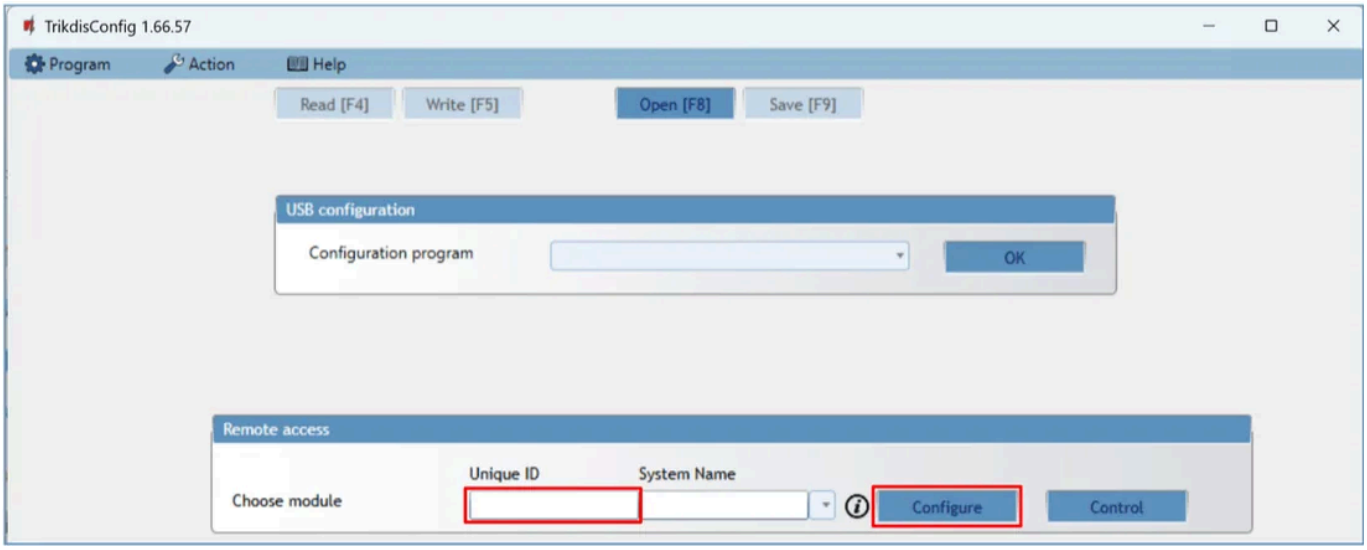


Abbildung 69. TrikdisConfig – die Gruppe Remote access: das Feld Unique ID, die Liste System name und die Schaltfläche Configure.

Die eindeutige Kennung des GET ist die **IMEI / Unique ID**; sie steht auf dem Etikett des Geräts und auf dem Aufkleber der Verpackung. Der Fernzugriff funktioniert nur, wenn die SIM-Karte aktiv ist und ihre PIN eingetragen oder die PIN-Abfrage ausgeschaltet ist – **oder** der Kommunikator mit einem Netzwerkkabel (LAN) angeschlossen ist –; auf der Seite **User reporting** → **PROTEGUS Cloud** ist **Enable connection** angehakt (Abschnitt 6.5); die LED **POWER** leuchtet grün; die LED **NETWORK LTE** leuchtet grün und blinkt gelb (bei rein kabelgebundener Verbindung leuchtet die LED **NETWORK LAN** grün). Beginn und Ende der Fernprogrammierung meldet der Kommunikator mit den Meldungen REMOTE_STARTED und REMOTE_FINISHED (Abschnitt 6.8).

8. Funktionsprüfung des Kommunikators

Prüfen Sie nach Programmierung und Anschluss immer die gesamte Kette: Alarmzentrale → Kommunikator → Leitstelle und/oder Protegus 2.

Prüfen Sie vorher, ob Spannung anliegt (die **POWER**-LED leuchtet grün) und ob eine Netzwerkverbindung besteht (die **NETWORK**-LED leuchtet grün).

1. **Lösen Sie ein Ereignis aus.** Scharf- und unscharfschalten Sie das System am Bedienteil, oder verletzen Sie bei scharfgeschaltetem System eine Zone, damit ein Alarm entsteht.
2. **Prüfen Sie den Eingang.** Sehen Sie nach, ob das Ereignis in der Leitstellensoftware und/oder in der Ereignisliste der Protegus-2-App erschienen ist – mit der richtigen Bereichs- und Zonennummer.
3. **Eingänge.** Lösen Sie den Melder aus, der an einen eigenen Eingang des Kommunikators angeschlossen ist, und prüfen Sie das zugehörige Ereignis.
4. **Ausgänge.** Schalten Sie den Ausgang aus der Protegus-2-App und prüfen Sie, ob das angeschlossene Gerät (Relais, Schlüsselschalterzone) tatsächlich anspricht.
5. **Fern-Scharfschaltung.** Wenn die Zentrale fernsteuerbar ist, schalten Sie sie auch aus der Protegus-2-App scharf und unscharf.

Meldet der Kommunikator sowohl über das kabelgebundene Netzwerk als auch über das Mobilfunknetz (Abschnitt 6.4.2, Reporting mode), lohnt es sich, den Test auf beiden Wegen durchzuführen: Ziehen Sie das LAN-Kabel ab, lösen Sie ein Ereignis aus und prüfen Sie, ob es auch über die SIM-Karte bei der Leitstelle ankommt; stecken Sie das Kabel danach wieder ein.

9. Firmware-Aktualisierung

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

Sie können die Firmware auch selbst aktualisieren – auf eine neuere und bei Bedarf auch auf eine ältere Version. Nach der Aktualisierung bleiben alle Einstellungen des Geräts unverändert.

1. Starten Sie die Software TrikdisConfig und verbinden Sie das Gerät per USB-Kabel, oder öffnen Sie seine Programmierung aus der Ferne.
2. Wenn es eine neuere Firmware gibt, bietet das Programm deren Download an – nehmen Sie ihn an.
3. Wählen Sie die Seite **Firmware** und klicken Sie auf die Schaltfläche **Open firmware**. Wählen Sie die Firmware-Datei aus.
4. Drücken Sie die Schaltfläche **Update [F12]**, warten Sie das Ende der Aktualisierung ab, und klicken Sie dann im Popup-Fenster auf **OK**. Ziehen Sie währenddessen nicht das Kabel ab und unterbrechen Sie die Verbindung nicht.

Die Firmware-Dateien befinden sich im Installationsordner von TrikdisConfig, im Unterordner **Firmwares**, in dem mit dem Gerätenamen bezeichneten Ordner. Gibt es diesen Ordner nicht, dann gibt es entweder keine Aktualisierung dafür, oder die Software TrikdisConfig selbst muss aktualisiert werden. Die neuesten Dateien können Sie als registrierter Benutzer auch von der Website des Herstellers, auf der Seite des Geräts, herunterladen.

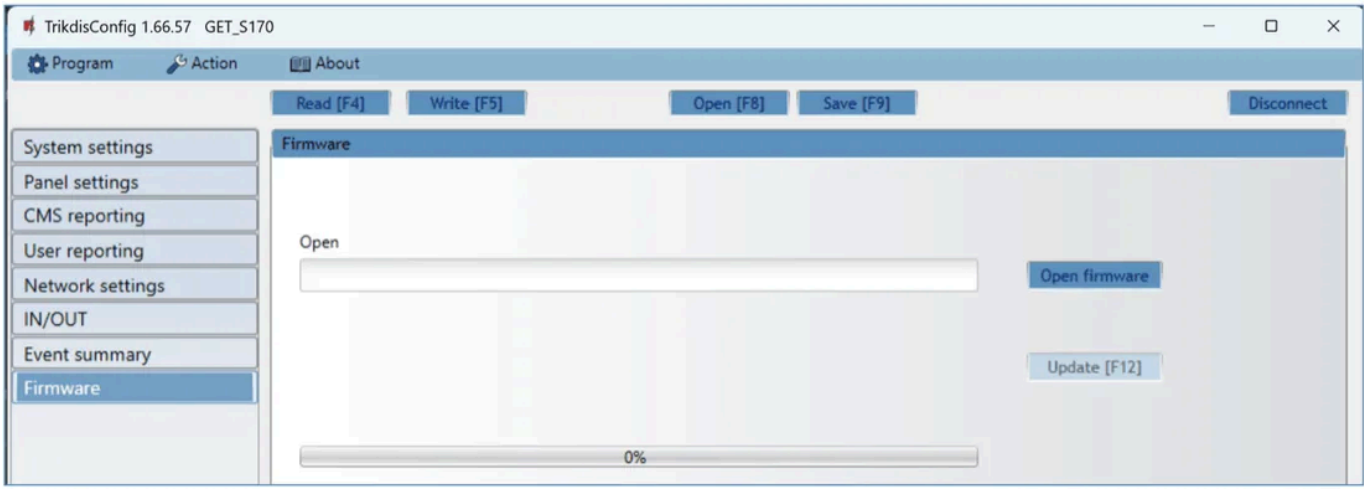


Abbildung 70. TrikdisConfig – Seite Firmware: Schaltfläche Open firmware, Schaltfläche Update [F12] und die Fortschrittsanzeige.

Für die Aktualisierung ist eine Internetverbindung nötig. Virenschutz, Firewall oder strenge Einstellungen für den Internetzugang können die automatische Firmware-Aktualisierung verhindern; in diesem Fall müssen die Einstellungen des Virenschutzes geändert werden.

Einzelne Funktionen des GET erfordern eine bestimmte Firmware-Version:

- **1.08** oder neuer: Einrichtung aus der App Protegus 2 (Advanced settings, Abschnitt 2.2 und Kapitel 6);
- **1.17** oder neuer, bei der Hardwarevariante **M15**: die Einstellungen **Generation** und **Bands** auf der Seite SIM der App (Abschnitt 6.6.2);
- **1.21** oder neuer: der Anschluss Keybus + TIP/RING der Paradox SP / SP+ / MG / MG+ (Abschnitt 3.3.3);
- **1.31** oder neuer, bei der Hardwarevariante **x1x1**: Die Kennungen (Account No., Device account No.) befinden sich in der App bei den CMS-Einstellungen (Abschnitt 6.2).

10. Fehlersuche und häufige Fragen

Die häufigsten Fragen und Fehler, ausgehend von den LED-Anzeigen. Verweist die Antwort auf das ausführliche Kapitel, finden Sie dort die genaue Stelle der Einstellung.

Die LED NETWORK LTE leuchtet nicht – kein Mobilfunknetz

1. Beachten Sie die Blinkimpulse der LED **TROUBLE**: 2 = Fehler der SIM1-Karte, 3 = Fehler der SIM2-Karte (Abschnitt 1.6).
2. Prüfen Sie, ob die SIM-Karte aktiv ist, einen Datendienst hat und richtig im Halter sitzt (SIM1 in der Mitte der Platine, SIM2 am linken Rand; Abschnitt 3.1).
3. Ist die PIN-Abfrage auf der Karte eingeschaltet, geben Sie die PIN im Reiter **Network settings** → **SIM1** (oder **SIM2**) ein oder schalten Sie die PIN-Abfrage in einem Telefon aus.
4. Prüfen Sie den APN (Abschnitt 2.3): Bei einer IoT- / M2M-Karte gibt der Anbieter einen eigenen APN an.
5. Prüfen Sie die Antenne: Sie ist angeschraubt, befindet sich nicht in einem Metallgehäuse, und der Signalpegel ist ausreichend (die LED NETWORK LTE blinkt mindestens 3-mal gelb; Abschnitte 1.6 und 3.2).
6. Meldet der Kommunikator über das kabelgebundene Netzwerk, hält ihn das fehlende Mobilfunknetz allein nicht auf: Er sendet gemäß der Reihenfolge in **Reporting mode** (Abschnitt 6.4.2) über den nächsten verfügbaren Weg – allerdings fehlt dann der Ersatzweg, es lohnt sich, das in Ordnung zu bringen.

Die LED NETWORK LAN leuchtet nicht – kein kabelgebundenes Netzwerk

1. 1 Blinkimpuls der LED **TROUBLE** zeigt einen Fehler in der physischen Verbindung des kabelgebundenen Netzwerks an: Prüfen Sie das LAN-Kabel an beiden Enden und ob der Port des Routers oder Switches aktiv ist (Abschnitt 1.6).
2. Ist das Kabel in Ordnung, sehen Sie sich den Reiter **Network settings** → **LAN** an: Bei DHCP muss der Router eine Adresse vergeben; bei fester Adresse müssen Static IP, Subnet mask und Default gateway zum lokalen Netzwerk passen (Abschnitt 6.6.1).
3. Haben Sie den Empfänger mit einem Domainnamen angegeben, müssen auch die DNS-Adressen im Netzwerk funktionieren (DNS1, DNS2).

Es gibt ein Netz, aber die Leitstelle erhält keine Ereignisse

Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

1. Prüfen Sie Adresse, Port, TCP/UDP-Einstellung, Protokoll und Verschlüsselungsschlüssel des Empfängers (**CMS reporting** → **CMS settings**, Abschnitt 6.4.1); der Schlüssel muss im Kommunikator und im Empfänger derselbe sein.

2. Sehen Sie sich die Einstellung **Reporting mode** an (Abschnitt 6.4.2): **Main type** muss ein Weg sein, der vor Ort tatsächlich verfügbar ist (ein LAN-Kabel ist vorhanden bzw. im angegebenen Halter steckt eine SIM-Karte), und es sollte auch einen Ersatzweg geben.
3. Ist der Empfänger mit einem Domainnamen angegeben, prüfen Sie die DNS-Einstellung auf dem Weg, über den der Kommunikator meldet (**Network settings** → **LAN** bzw. **SIM1 / SIM2** → **DNS1, DNS2**).
4. Prüfen Sie im Mobilfunknetz, ob der Datentarif der SIM-Karte den benötigten Port nicht sperrt (manche M2M-Karten lassen nur bestimmte Adressen zu); im kabelgebundenen Netzwerk muss die örtliche Firewall den Port des Empfängers nach außen zulassen.
5. Sendet die Zentrale keine Ereignisse (die LED DATA leuchtet nicht auf), liegt die Ursache auf der Seite der Zentrale: siehe den nächsten Punkt.

Die LED TROUBLE blinkt 7-mal – keine Verbindung zur Zentrale

1. Prüfen Sie beim Anschluss an Datenbus oder serielle Schnittstelle die Adern CLK und DATA und ob im Feld **Panel settings** → **Security panel model** der Typ der angeschlossenen Zentrale ausgewählt ist (Abschnitt 6.3).
2. Prüfen Sie bei einer Paradox-Zentrale, ob die serielle Schnittstelle nicht gesperrt ist (Abschnitt 4.1.2); bei Texecom- und Paradox-Zentralen muss das **Security panel PC download password** mit dem in der Zentrale eingestellten übereinstimmen.
3. Beim Telefonleitungsanschluss muss das Wählgerät der Zentrale eingeschaltet sein, im DTMF-Modus, mit dem Format Contact ID und mit eingetragener Telefonnummer (Abschnitt 4.2), und **Communication protocol** muss auf **2. AUTO** stehen (Abschnitt 6.3).

Über welchen Weg geht das Ereignis: über LAN oder über SIM?

Über den, den die Reihenfolge in **Reporting mode** (Abschnitt 6.4.2) vorgibt: über den Weg nach **Main type**; funktioniert dieser nicht, über den nach **Backup type**, dann nach **Backup type 2**. Ist die Meldung über den Ersatzweg gegangen, versucht der Kommunikator nach Ablauf der Zeit **Return from backup after** erneut den Hauptweg, und **Communication path test** probiert in Intervallen jeden Weg aus. Auch die Verbindung zu Protegus 2 nutzt denselben Weg. Im kabelgebundenen Netzwerk wird kein mobiles Datenvolumen verbraucht.

Wozu dienen die beiden SIM-Halter?

Mit Karten zweier verschiedener Anbieter wird auch das Mobilfunknetz zweiwegig: In Reporting mode sind SIM1 und SIM2 eigene Verbindungsarten, jede kann Haupt- oder Ersatzweg sein (Abschnitt 6.4.2). Die beiden Karten müssen separat eingerichtet werden (**Network settings** → **SIM1**, **SIM2**: PIN, APN; Abschnitt 6.6.2); einen Fehler der SIM2 zeigen 3 Blinkimpulse der LED TROUBLE und die Meldung SIM2_FAILURE an (Abschnitte 1.6 und 6.8). Der Kommunikator funktioniert auch mit einer Karte.

DSC: Jeder Alarm kommt als allgemeiner Alarm E130

Nur am Keybus angeschlossen erhält der Kommunikator von der Zentrale den Zustand der Zonen, nicht aber den Zonentyp, deshalb meldet er jeden Alarm mit dem Code E130 (Abschnitt 3.3.1). Den gleichzeitigen Anschluss an Keybus und TIP/RING gibt es beim GET nicht (das ist eine Funktion des GT+). Erwartet die Leitstelle den dem Zonentyp entsprechenden Code (zum Beispiel Feuer: E110), schließen Sie den GET nur an die Klemmen TIP/RING der Zentrale an und programmieren Sie das Wählgerät (Abschnitte 3.3.9 und 4.2): So gehen die eigenen Contact-ID-Codes der Zentrale hinaus, aber es gibt keine direkte Steuerung – zum Scharfschalten ist eine Schlüsselschalterzone nötig (Abschnitt 3.4).

Paradox: Die serielle Schnittstelle ist gesperrt, oder es gibt keine Verbindung

Bei den neueren Paradox-Zentralen (SP+, MG+, EVOHD+) kann die serielle Schnittstelle werkseitig gesperrt sein; die Freischaltung behandeln Abschnitt 4.1.2 und der Artikel Freischalten der gesperrten seriellen Schnittstelle bei Paradox-Alarmzentralen. Bei den Zentralen Spectra SP / SP+ und Magellan MG / MG+ kann statt der seriellen Schnittstelle auch der Anschluss Keybus + TIP/RING verwendet werden (Abschnitt 3.3.3); dafür ist keine Freischaltung nötig, aber die Firmware des Kommunikators muss mindestens 1.21 sein (Kapitel 9).

Ich kann aus Protegus 2 nicht scharfschalten

1. Bei direkter Steuerung muss **Panel settings** → **Remote Arm/Disarm** angehakt und die Zentrale gemäß Abschnitt 4.1 eingerichtet sein (Paradox: PC-Passwort, Firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: die beschriebenen Einstellungen). Sehen Sie in der Tabelle in Abschnitt 1.3 nach, ob die Zentrale überhaupt direkt steuerbar ist.
2. Beim Scharfschalten per Schlüsselschalter (Abschnitt 3.4) muss die Klemme auf der Seite **IN/OUT** auf **OUT** stehen (Werkseinstellung des GET), die Zone der Zentrale muss eine Schlüsselschalterzone sein, und in Protegus 2 muss der Ausgang dem Bereich zugeordnet sein, im selben Modus wie in der Zentrale (impulsgesteuert oder zweistellig; Abschnitt 5.2).
3. Protegus 2 zeigt den Zustand des Bereichs anhand der Scharf- und Unscharfschaltereignisse der Zentrale: Die Zentrale muss diese melden (Opening/Closing).

Protegus 2 sieht das Gerät nicht

1. Auf der Seite **User reporting** → **PROTEGUS Cloud** muss **Enable connection** angehakt sein (Abschnitt 6.5).
2. Beim Hinzufügen muss der im Gerät eingestellte **PROTEGUS Cloud access Code** eingegeben werden; haben Sie den Code in TrikdisConfig geändert, ändern Sie ihn auch in der App.
3. Geben Sie die IMEI genau vom Etikett des Geräts oder vom Aufkleber der Verpackung ein (oder scannen Sie den QR-Code).
4. Auf mindestens einem Weg muss funktionierendes Internet vorhanden sein: Die LED NETWORK LTE leuchtet grün und blinkt gelb (SIM-Karte mit Datendienst und richtigem APN), oder die LED NETWORK LAN leuchtet grün (LAN-Kabel). Die LED DATA muss nach einem Ereignis erlöschen.

Ich kann mich mit TrikdisConfig nicht aus der Ferne verbinden

1. Das Gerät muss online sein (NETWORK LTE grün, blinkt gelb, oder NETWORK LAN grün), und die Protegus-Verbindung muss aktiviert sein (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** darf nicht länger als 5 Minuten sein: Der PING hält die für den Fernzugriff nötige Verbindung aufrecht.
3. Prüfen Sie das Administrator- oder Errichterpasswort.

Kann ich den Kommunikator aus der App einrichten?

Ja: Mit Firmware 1.08 oder neuer sind im Menü **Settings** → **Advanced settings** von Protegus 2 die meisten Einstellungen verfügbar (Abschnitt 2.2 und Kapitel 6). Nur in TrikdisConfig gibt es: das Wiederherstellen der Werkseinstellungen (Abschnitt 6.9), **Preferred operator** (Abschnitt 6.6.2) und die manuelle Firmware-Aktualisierung (Kapitel 9); den Schalter **Event** von Serial bus zeigt die App an, ändert ihn aber nicht. Mit dem Errichtercode angemeldet, können Sie nur die Gruppen ändern, die der Administrator freigegeben hat (Abschnitt 6.2).

Ich habe das Passwort vergessen

Mit TrikdisConfig ist das nicht möglich, denn auch die Wiederherstellung erfordert ein Passwort. Mit der Taste **RESET** des Geräts geht es jedoch (Punkt 6.9): bei eingeschalteter Versorgung 10 Sekunden gedrückt halten. Alle Einstellungen werden gelöscht. Aus der App lässt sich die Wiederherstellung nicht starten.

Wie viel Datenvolumen verbraucht das Gerät?

Die Ereignismeldungen und die PINGs sind sehr klein; das Datenvolumen hängt überwiegend vom PING-Intervall und von der Häufigkeit der Testmeldungen ab. Bei einer durchschnittlichen Haushaltsanlage bleibt das monatliche Volumen in der Regel unter 10 MB. Der genaue Wert hängt von den Einstellungen und von der Abrechnungseinheit des Anbieters ab, deshalb lohnt es sich bei einer Karte mit Datenlimit, das Volumen des ersten Monats zu prüfen. Solange der Kommunikator über das kabelgebundene Netzwerk meldet, wird kein Datenvolumen der SIM-Karte verbraucht.

11. Sicherheitshinweise

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.

- Montage und Wartung sicherheitstechnischer Anlagen dürfen nur von einer qualifizierten Fachkraft durchgeführt werden.
- Lesen Sie vor der Installation die Anleitung; die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen oder zu einem Defekt der Anlage führen.
- Trennen Sie die Anlage vor dem Anschließen, bei jedem elektrischen Anschließen und vor Servicearbeiten von der Versorgung.
- Vom Hersteller nicht genehmigte Änderungen, Umbauten und Reparaturen führen zum Verlust der Garantie.
- Beachten Sie die örtlichen Vorschriften zur Abfallentsorgung: Entsorgen Sie das unbrauchbar gewordene Gerät und seine Teile nicht mit dem Hausmüll. Das Symbol der durchgestrichenen Mülltonne (WEEE) auf dem Gerät zeigt an, dass es als Elektronikschrott getrennt abzugeben ist.

Siehe auch

- Kompatibilitätssuche – welcher Trikdis-Kommunikator und welcher Anschluss zu Ihrer Alarmzentrale passt.
- Trikdis-Kommunikator + DSC-Alarmzentrale: Kurzanleitung für Errichter – die Schritte des DSC-Anschlusses in Kürze.
- Trikdis-Kommunikator + Paradox-Alarmzentrale: Kurzanleitung für Errichter – die Schritte des Paradox-Anschlusses in Kürze.
- DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen – warum die NEO nicht an den Datenbus angeschlossen werden kann und was die Lösung ist.

- Freischalten der gesperrten seriellen Schnittstelle bei Paradox-Alarmzentralen – Freischalten der seriellen Schnittstelle der Zentralen SP+, MG+ und EVOHD+.
- Scharfschalten aus der Ferne per Schlüsselschalter aus der App Protegus 2 – Details und Fallstricke des Scharfschaltens per Schlüsselschalter.
- APN-Einstellung – Liste europäischer Mobilfunkanbieter – die APNs der Anbieter, auch für IoT- / M2M-Karten.
- Englischsprachige Dokumentation: docs.trikdis.com – GET – hier finden Sie auch die Umwandlungstabelle Contact ID → SIA (Anhang).

Die Anleitungen auf docs.trikdis.com sind in englischer Sprache.

Passende Produkte

Trikdis GET Ethernet + 4G Kommunikationsmodul

Trikdis CRP2 Seriell-Port-Verbindungskabel für Paradox-Alarmpulte

Trikdis Ant04 GSM Stick-On-Antenne mit 2,5 m Draht

Trikdis ME301M Magnetantenne mit 2,5 m Draht

Urheberrecht

Diese Anleitung wurde von trikdis.hu und mobilamb.eu erstellt. Text, Aufbau, eigene Abbildungen und Ergänzungen sind unser geistiges Eigentum und urheberrechtlich geschützt. Ohne unsere Erlaubnis darf sie weder ganz noch teilweise kopiert, verbreitet oder auf einer anderen Website veröffentlicht werden. Für die Installation und Nutzung des Produkts darfst du sie frei herunterladen und ausdrucken.

Die Namen und Logos Trikdis und Protegus sind Marken der UAB Trikdis.

Immer aktuelle Version dieser Anleitung: https://trikdis.at/get-anleitung