Kommunikator GT und GT+ – Errichter- und Benutzeranleitung

Errichter- und Benutzeranleitung für die Trikdis-Kommunikatoren GT und GT+: Anschluss an den Datenbus, die serielle Schnittstelle oder den Telefonleitungsausgang der Alarmzentrale, Programmierung der Zentrale, Einrichtung in TrikdisConfig, Übertragung an die Leitstelle, die App Protegus 2.



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

Inhalt

1. Überblick

1.1 Wofür er gedacht ist und wie er funktioniert
1.2 Varianten: 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 mit TrikdisConfig

2.1 Vorbereitung
2.2 Verbindung zur App Protegus 2
2.3 Verbindung zur Leitstelle

3. Montage und Anschluss

3.1 Schritte der Montage
3.2 Platzierung und Antenne
3.3 Anschluss an die Alarmzentrale
3.3.1 DSC – Datenbus (Keybus)
3.3.2 DSC – Keybus und TIP/RING (nur GT+)
3.3.3 Paradox – serielle Schnittstelle
3.3.4 Paradox SP/MG – Keybus und TIP/RING
3.3.5 UTC Interlogix (Caddx) – Datenbus
3.3.6 Texecom – serielle Schnittstelle
3.3.7 InnerRange Inception
3.3.8 InnerRange Integriti
3.3.9 Honeywell Vista – Datenbus
3.3.10 Jede Zentrale – TIP/RING
3.4 Anschluss einer Schlüsselschalter-Zone
3.5 Anschluss der Eingänge
3.6 Anschluss eines Ausgangs mit Relais
3.7 Anschluss des Erweiterungsmoduls iO-8
3.8 Einschalten und erste Prüfung
A TRIKDIS átjelző elindítása

4. Programmierung der Alarmzentrale

4.1 Anschluss über 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 Wählgerät der UTC Interlogix (Caddx) NX

5. Fernsteuerung mit der App Protegus 2

5.1 Das 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
5.4 Steuerung mit SMS-Nachrichten

6. TrikdisConfig – die Einstellungen im Detail

6.1 Die Statusleiste
6.2 System settings
6.3 Panel settings
6.4 CMS reporting
6.5 User reporting
6.6 Network settings
6.7 IN/OUT
6.8 RS485 modules
6.9 Event summary
6.10 Werkseinstellungen wiederherstellen

7. Fernprogrammierung

8. Prüfung der Funktion des Kommunikators

9. Firmware-Aktualisierung

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

GT und GT+ sind die **4G-Mobilfunk-Kommunikatoren** von Trikdis, die die Ereignisse der Alarmzentrale an die Leitstelle und in die App Protegus 2 übertragen. Sie können auf zwei Arten an die Zentrale angeschlossen werden: **direkt**, an den Datenbus oder die serielle Schnittstelle der Zentrale (bei Zentralen von DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange und Honeywell), oder **an den Telefonleitungs-Kommunikator jeder beliebigen Zentrale** (TIP/RING), die die 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 das System aus der Ferne und wird über die Ereignisse benachrichtigt; die App funktioniert mit allen Zentralen, die der Kommunikator unterstützt, unabhängig vom Hersteller der Zentrale. Die Meldung an die Leitstelle und Protegus 2 können gleichzeitig genutzt werden. Diese Anleitung gilt für die 4G-Kommunikatoren GT und GT+; die Unterschiede der beiden Varianten fasst Punkt 1.2 zusammen.

1.1 Wofür er gedacht ist und wie er funktioniert

- **Meldet an die Leitstelle.** Er sendet die Ereignisse über IP 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). An einen SUR-GARD-Empfänger gibt er die von der Zentrale erhaltenen Contact-ID-Codes in SIA-Codes umgewandelt weiter; die Umwandlungstabelle steht im Anhang der englischen Herstellerdokumentation. Die Verbindung zum Empfänger prüft er alle 30 Sekunden (oder im eingestellten Intervall) mit einer PING-Nachricht; fällt der Hauptkanal aus, wechselt er auf den Ersatzkanal. Mit einem parallelen Kanal gehen die Ereignisse gleichzeitig an zwei Empfänger. Ist auch der Protegus-Dienst eingeschaltet, erhält zuerst die Leitstelle das Ereignis und erst danach die App der Benutzer.
- **Benachrichtigt den Benutzer.** Die App Protegus 2 meldet die Ereignisse als Push-Nachricht mit eigenem Signalton; der Benutzer kann in der App scharf- und unscharfschalten und die angeschlossenen Geräte schalten (Beleuchtung, Tor, Lüftung, Heizung, Bewässerung usw.). In der App haben Administrator, Errichter und Benutzer unterschiedliche Rechte. Neben Protegus 2 kann die Benachrichtigung auch per SMS und per Anruf erfolgen.
- **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 schärft und entschärft in Protegus 2 mit seinem eigenen Bedienteilcode – dafür ist keine Schlüsselschalter-Zone nötig. Der GT+ kann an DSC-Zentralen gleichzeitig an den Datenbus (Keybus) und an die Klemmen TIP/RING angeschlossen werden: Der Bus dient der Steuerung und den Zuständen, die Ereignisse gehen mit den eigenen Contact-ID-Codes der Zentrale (Punkt 3.3.2).
- **Eigene Ein- und Ausgänge.** Zwei Klemmen mit Doppelfunktion (I/O) sind als Eingang (IN) oder als steuerbarer Ausgang (OUT) nutzbar. Die Ausgänge können in der App Protegus 2 und per SMS-Befehl geschaltet werden. Mit Erweiterungsmodulen iO-8 am RS485-Bus lassen sich weitere Ein- und Ausgänge hinzufügen.
- **Einstellung.** 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 kann auch aus der Ferne eingestellt und seine Firmware aus der Ferne aktualisiert werden.

Den Aufbau des Systems zeigt die folgende Abbildung: Die Alarmzentrale ist mit dem Kommunikator verbunden, der Kommunikator erreicht über das Mobilfunknetz (LTE) das Internet und von dort den Empfänger der Leitstelle (und dessen Software) sowie den Protegus-Server; der Benutzer sieht das System in der App Protegus 2 und kann über das Mobilfunknetz auch SMS und Anrufe erhalten.

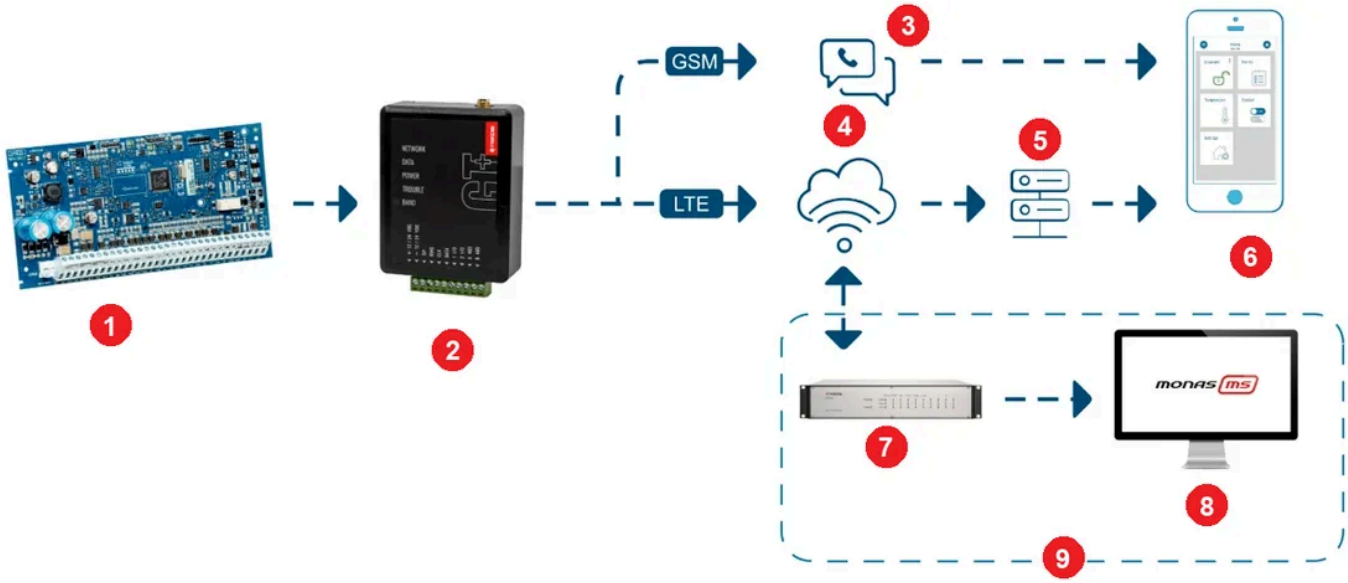


Abbildung 1. Die Stellung des Kommunikators im System: Alarmzentrale → GT / GT+ → Mobilfunknetz → Internet → Empfänger der Leitstelle und Protegus-Server → App Protegus 2; SMS und Anruf direkt über das Mobilfunknetz.

- 1 Alarmzentrale („Alarm panel“)
- 2 LTE-Kommunikator GT / GT+ („LTE communicator“)
- 3 Anruf und SMS („Call/SMS“)
- 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 Leitstelle des Sicherheitsdienstleisters („Monitoring station in security company“) – im gestrichelten Rahmen

1.2 Varianten: GT und GT+

GT und GT+ sind dasselbe Gerät in zwei Varianten: Anschluss, Einstellung und Funktion sind nahezu gleich, daher beschreiben wir sie in einer Anleitung. Die Unterschiede fasst die folgende Tabelle zusammen; wo der Text den Wert des GT+ angibt, beachten Sie beim GT diesen Wert.

	GT	**GT+**
Versorgungsspannung	10–18 V DC	10–32 V DC
Beschriftung der Versorgungsklemmen	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Anschluss einer DSC-Zentrale	nur an den Datenbus (Keybus)	an den Datenbus oder an den Datenbus und die Klemmen TIP/RING zusammen – so gehen die Ereignisse mit den eigenen Contact-ID-Codes der Zentrale (z. B. Feuer: E110), nicht als allgemeiner Alarm (E130)
Einstellung des Telefonleitungs-Anschlusses (TIP/RING) in TrikdisConfig (**Panel settings** → **Communication protocol**)	**2. Dual tone**	**2. AUTO** (in der Liste ist auch **3. MANUAL** wählbar)

	GT	GT+
Prüfung bei DSC mit Anschluss Bus + TIP/RING (Kapitel 8)	–	Alarm einer Feuerzone muss als E110 ankommen
Alles andere: Ein-/Ausgänge, RS485-Bus, Modem, LEDs, Abmessungen, Protokolle, Protegus 2, SMS-Befehle	gleich	gleich

Beide Varianten werden mit drei Modemtypen hergestellt; für den europäischen Markt ist die europäische Variante (EU) geeignet. Den Modemtyp und die Hardwareversion 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 können direkt, über Datenbus oder serielle Schnittstelle, an den Kommunikator angeschlossen werden. Die Spalte „Direkte Steuerung“ zeigt, ob der Benutzer in Protegus 2 mit seinem eigenen Bedienteilcode ohne weiteren Anschluss scharf- und unscharfschalten kann; wo das nicht möglich ist, liest der Kommunikator die Ereignisse vom Bus, und für die Steuerung ist eine Schlüsselschalter-Zone nötig (Punkt 3.4).

Hersteller	Typ	Anschluss	Direkte Steuerung
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	Datenbus (Keybus); GT+: auch Keybus + TIP/RING	ja
DSC	PC5020	Datenbus (Keybus)	nein
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
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 Herstellers)	nein
Honeywell	Ademco Vista-15, Vista-20, Vista-48	Datenbus	ja

- Die Firmware der direkt gesteuerten **Paradox**-Zentralen muss mindestens **V.4** sein. Bei den neueren Paradox-Zentralen (SP+, MG+, EVOHD+) kann die serielle Schnittstelle ab Werk gesperrt sein; zur Freischaltung siehe Punkt 4.1.2. Die Zentralen Spectra SP / SP+ und Magellan MG / MG+ können statt an die serielle Schnittstelle auch an den Datenbus (Keybus) und die Klemmen TIP/RING zusammen angeschlossen werden – dafür ist die kostenpflichtige Freischaltung nicht nötig (Punkt 3.3.4).
- Die Zentrale **jedes anderen Herstellers** wird über ihren Telefonleitungs-Kommunikator (TIP/RING) angeschlossen, wenn sie die Ereignisse im Format Contact ID mit DTMF-Wahl sendet; dann ist für die Steuerung eine Schlüsselschalter-Zone 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, die Klemmleiste abziehen. Das folgende Bild zeigt den GT+; der GT sieht genauso aus, nur steht auf dem Gehäuse GT, und die Versorgungsklemmen sind mit +12 VDC / −12 VDC beschriftet.

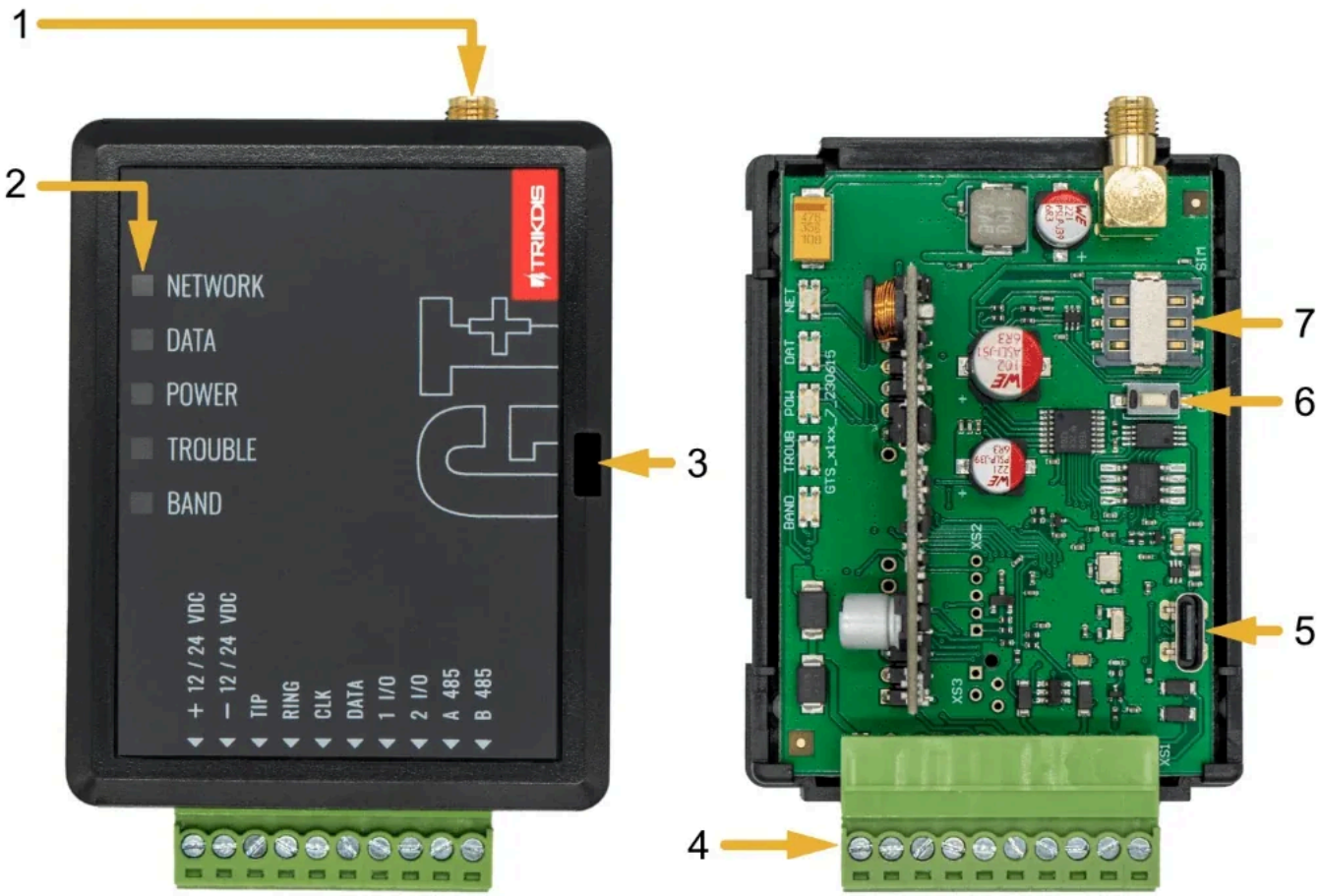


Abbildung 2. Die Teile des Kommunikators von vorn (links) und mit geöffnetem Gehäuse (rechts).

- 1 SMA-Anschluss der Mobilfunkantenne
- 2 LED-Anzeigen (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Öffnung zum Abnehmen der Frontabdeckung
- 4 Abnehmbare Klemmleiste für die externen Anschlüsse
- 5 USB-C-Buchse für die Programmierung
- 6 Taste RESET
- 7 Halter für die Nano-SIM-Karte

Die Klemmleiste ist abziehbar: So kann das Gerät mit einem Handgriff stromlos gemacht oder neu gestartet werden, beim Anschließen ist sie leichter zu handhaben, und für die Programmierung über USB kann das Gerät zum Computer gebracht werden.

1.5 Klemmen

Klemme (GT)	Klemme (GT+)	Funktion
+12 VDC	**+12 / 24 VDC**	Versorgung, positiv: +10–18 V DC (GT), +10–32 V DC (GT+)
–12 VDC	**–12 / 24 VDC**	Versorgung, 0 V
TIP	**TIP**	Klemme TIP des Telefonleitungs-Kommunikators der Alarmzentrale
RING	**RING**	Klemme RING des Telefonleitungs-Kommunikators der Alarmzentrale
CLK	**CLK**	Serieller Bus oder Datenbus (Takt) für den direkten Anschluss der Zentrale
DATA	**DATA**	Serieller Bus oder Datenbus (Daten) für den direkten Anschluss der Zentrale
1 I/O	**1 I/O**	Ein-/Ausgang 1 (Werkseinstellung: Eingang, NO)
2 I/O	**2 I/O**	Ein-/Ausgang 2 (Werkseinstellung: Eingang, NO)
A 485	**A 485**	Leitung A des RS485-Busses
B 485	**B 485**	Leitung B des RS485-Busses

Auf den Anschlussplänen sind die Versorgungsklemmen einheitlich mit **+DC** und **–DC** bezeichnet (beim GT die Klemmen +12 VDC / –12 VDC, beim GT+ die Klemmen +12 / 24 VDC / –12 / 24 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 Frontseite sind die wichtigsten Hilfsmittel bei Inbetriebnahme und Fehlersuche. Lesen Sie sie zusammen: POWER zeigt die Versorgung, NETWORK das Netz, TROUBLE den Fehler, BAND die Art des Netzes.

NETWORK – Netzverbindung

Anzeige	Bedeutung
leuchtet nicht	Keine Verbindung zum Mobilfunknetz
blinkt gelb	Verbindung zum Mobilfunknetz wird aufgebaut
leuchtet grün, blinkt gelb	Mit dem Mobilfunknetz verbunden; die Zahl der gelben Blinkimpulse ist die **Signalstärke**: Bei 4G sind 3 Blinkimpulse ein gutes Signal

DATA – Datenverkehr

Anzeige	Bedeutung
leuchtet nicht	Kein Ereignis wartet 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
leuchtet nicht	Keine Versorgung, oder die Versorgung ist getrennt
leuchtet grün	Eingeschaltet, die Versorgungsspannung ist in Ordnung
leuchtet gelb	Unzureichende Versorgungsspannung (höchstens 11,5 V)
leuchtet grün, blinkt gelb	Bereit zur Programmierung (während der Programmierung)
leuchtet gelb (während der Programmierung)	Keine Verbindung zum Computer

TROUBLE – Fehler

Anzeige	Bedeutung
leuchtet nicht	Kein Fehler
1 roter Blinkimpuls	Keine SIM-Karte
2 rote Blinkimpulse	SIM-PIN-Fehler (falscher PIN-Code)
3 rote Blinkimpulse	Programmierfehler (kein APN)
4 rote Blinkimpulse	Anmeldung im Mobilfunknetz nicht möglich (Registrierungsfehler)
5 rote Blinkimpulse	Anmeldung im Datennetz (GPRS/UMTS) nicht möglich
6 rote Blinkimpulse	Keine Verbindung zum Empfänger der Leitstelle
7 rote Blinkimpulse	Die Verbindung zur Alarmzentrale ist unterbrochen
8 rote Blinkimpulse	Die eingestellte ICCID stimmt nicht mit der ICCID der SIM-Karte überein (Punkt 6.6)
blinkt rot (während der Programmierung)	Speicherfehler
leuchtet rot (während der Programmierung)	Beschädigte Firmware

BAND – Art des Netzes

Grüne Blinkimpulse	Netz
1	keines
2	GSM
3	GPRS

Grüne Blinkimpulse	Netz
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.7 Technische Daten

Parameter	Wert
Verbindung mit der 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. Mit Erweiterungsmodulen iO-8 erweiterbar
Modem	EG915U-EU (Europa), EG915U-LA (Lateinamerika) oder BG95-M5 (LTE Cat M1) – die Frequenzbänder listet die Tabelle in Punkt 1.2 auf
Versorgungsspannung	GT: 10–18 V DC; GT+: 10–32 V DC
Stromaufnahme	höchstens 100 mA im Ruhezustand; höchstens 200 mA beim Senden von Daten
Übertragungsprotokolle	TRK8, DC-09_2007, DC-09_2012, TL150
Verschlüsselung	AES-128
Programmierung	TrikdisConfig (Windows) über USB-C-Kabel oder aus der Ferne
Betriebsumgebung	−10 … +50 °C, max. 80 % relative Luftfeuchtigkeit (bei +20 °C)
Abmessungen	92 × 62 × 26 mm
Gewicht	80 g

2. Schnelle Inbetriebnahme mit TrikdisConfig

Alle Einstellungen des Kommunikators erfolgen mit dem Windows-Programm **TrikdisConfig** – über USB-C-Kabel oder aus der Ferne. In diesem Kapitel beschreiben wir den kürzesten Weg: Sie stellen das Gerät auf dem Tisch ein, vor dem Anschließen, und vor Ort muss es dann nur noch angeschlossen werden. Wir beschreiben, welche Einstellungen nötig sind, damit der Kommunikator Ereignisse an die Leitstelle sendet und das System aus der App Protegus 2 steuerbar ist; die ausführliche Erklärung der Einstellungen enthält Kapitel 6.

2.1 Vorbereitung

Was Sie brauchen

USB-C-Kabel für die Programmierung · Kabel mit mindestens 4 Adern zwischen Kommunikator und Zentrale · für die serielle Schnittstelle von Paradox das Kabel CRP2.4 · flacher Schraubendreher 2,5 mm · Mobilfunkantenne mit passender Verstärkung, wenn die Netzabdeckung vor Ort schwach ist · aktive SIM-Karte (die PIN-Abfrage kann abgeschaltet werden) · die Errichteranleitung der Alarmzentrale.

Das benötigte Zubehör bestellen Sie separat beim Händler.

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 Schlitz neben der Antenne und hebeln Sie nach außen, dann unten an der Öffnung nach unten. Die Abbildung zeigt auch die Lage der USB-C-Buchse am Rand der Leiterplatte.

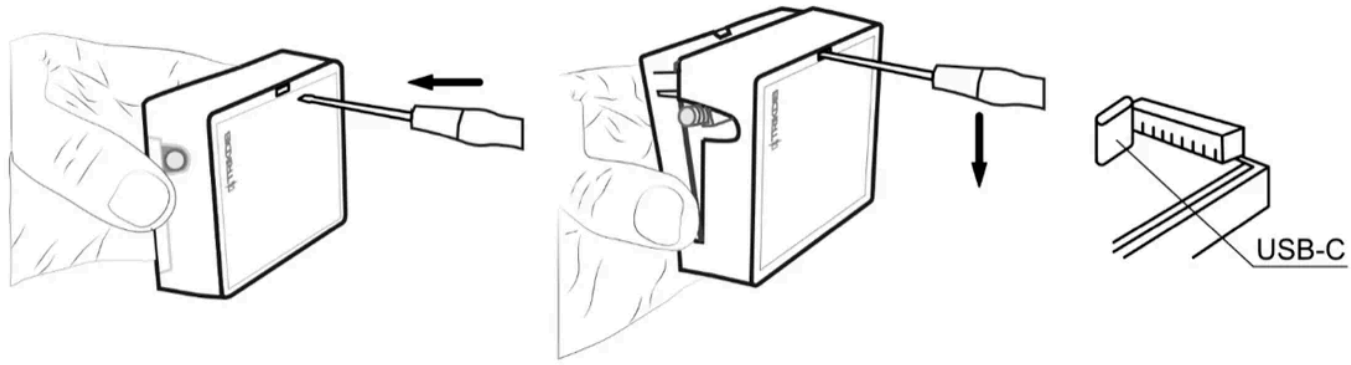


Abbildung 3. Abnehmen der Frontabdeckung mit einem flachen Schraubendreher; der vergrößerte Ausschnitt zeigt die Lage der USB-C-Buchse.

3. Setzen Sie die Nano-SIM-Karte in den Halter ein, in der auf der Abbildung gezeigten Richtung. Die Karte muss aktiv sein und einen mobilen Datendienst haben; schalten Sie, wenn möglich, die PIN-Abfrage in einem Telefon ab (dann muss keine PIN in das Gerät eingetragen werden).

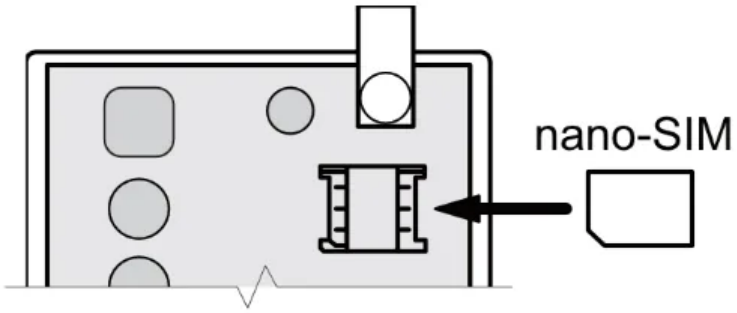


Abbildung 4. Die Lage der Nano-SIM-Karte auf der Leiterplatte.

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

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. Wenn es ein Passwort verlangt, geben Sie den 6-stelligen Administratorcode (ab Werk `123456`) oder

Errichtercode (ab Werk `654321`) ein.

2.2 Verbindung zur App Protegus 2

Geben Sie zuerst auf der Seite **Panel settings** an, wie der Kommunikator mit der Zentrale verbunden ist.

Wenn Sie ihn an den Telefonleitungsausgang der Zentrale (TIP/RING) anschließen: Wählen Sie im Feld **Communication protocol** den Wert **AUTO** (beim GT ist das zweite Element der Liste **Dual tone** – dort diesen).

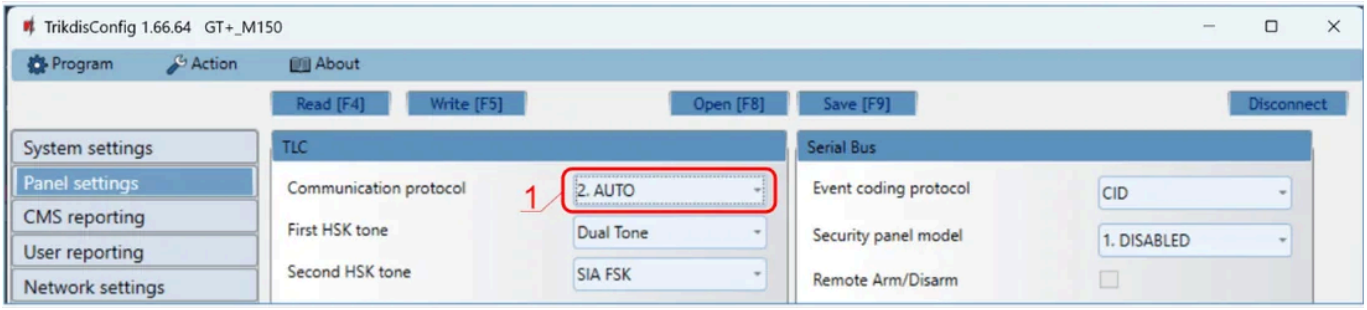


Abbildung 5. TrikdisConfig – Panel settings, Gruppe TLC (im Bild die Einstellung des GT+).

- 1 **Communication protocol** – beim Anschluss an TIP/RING **2. AUTO** (GT: **2. Dual tone**).

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



Abbildung 6. 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 in Protegus 2 mit ihrem eigenen Bedienteilcode steuern möchten. Erscheint nur bei direkt steuerbaren Zentralen.
- 4 **Security panel PC download password** – für die direkte Steuerung von Paradox- und Texecom-Zentralen das in der Zentrale eingestellte PC- bzw. UDL-Passwort; beide müssen übereinstimmen.

GT+, DSC-Zentrale am Datenbus und an den Klemmen TIP/RING zusammen: Communication protocol muss **AUTO** sein, **Security panel model** der DSC-Typ, und setzen Sie das Häkchen bei **Remote Arm/Disarm**, wenn die Zentrale aus Protegus 2 gesteuert werden soll (Punkt 3.3.2).

Für die direkte Steuerung muss auch die Alarmzentrale eingestellt 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.

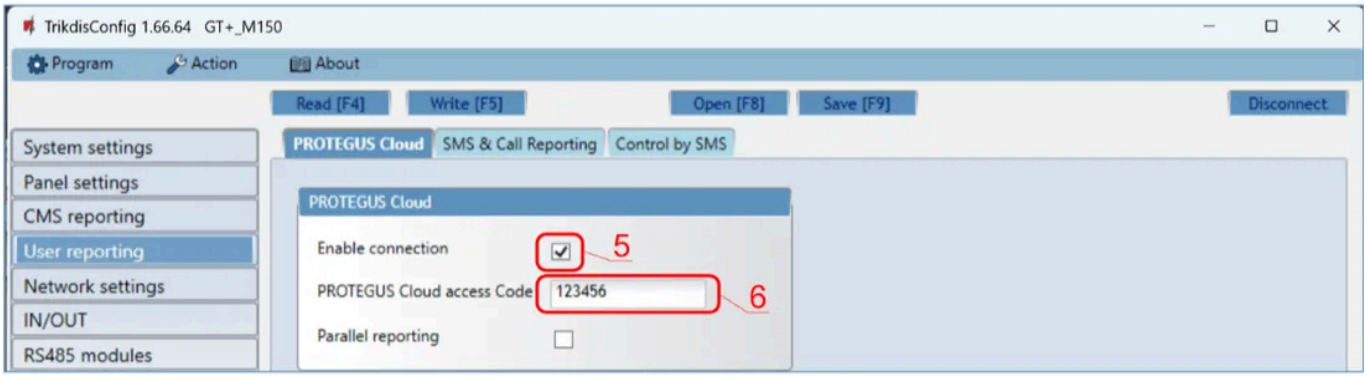


Abbildung 7. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- 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 (ab Werk `123456`). Ändern Sie ihn, wenn der Benutzer ihn beim Hinzufügen des Systems in die App eingeben soll. Wichtig: Wenn Sie den Code später in TrikdisConfig ändern, muss er auch in der App Protegus 2 geändert werden.

Geben Sie zum Schluss auf der Seite **Network settings**, im Reiter **SIM1**, die Daten der Karte ein.

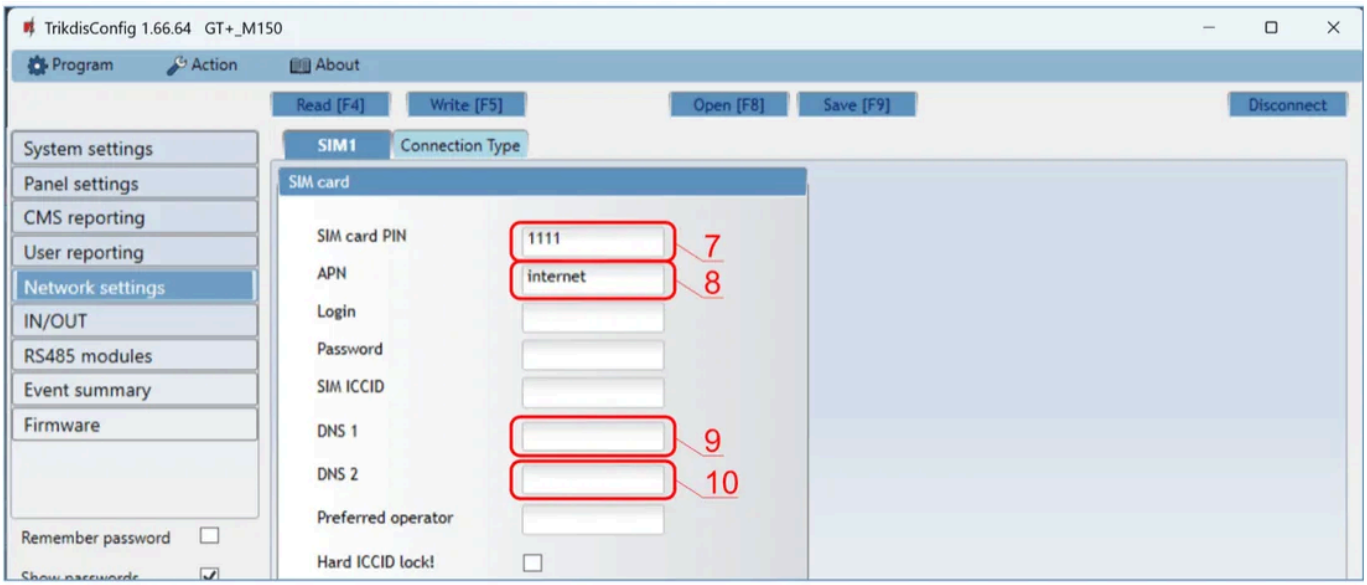


Abbildung 8. TrikdisConfig – Network settings, Reiter SIM1.

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

Der APN (Access Point Name) ist der Zugangspunkt für die Datenverbindung des Mobilfunkanbieters; ohne ihn kann sich das Gerät 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.

Wenn das Gerät nicht an eine Leitstelle meldet, ist die Einstellung damit fertig: Drücken Sie die Schaltfläche **Write [F5]** (Schreiben), warten Sie auf die Rückmeldung und ziehen Sie das USB-Kabel ab.

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

2.3 Verbindung zur Leitstelle

Wenn das Gerät auch an einen Empfänger der Leitstelle meldet, geben Sie zuerst auf der Seite **System settings** die Objektkennung ein.

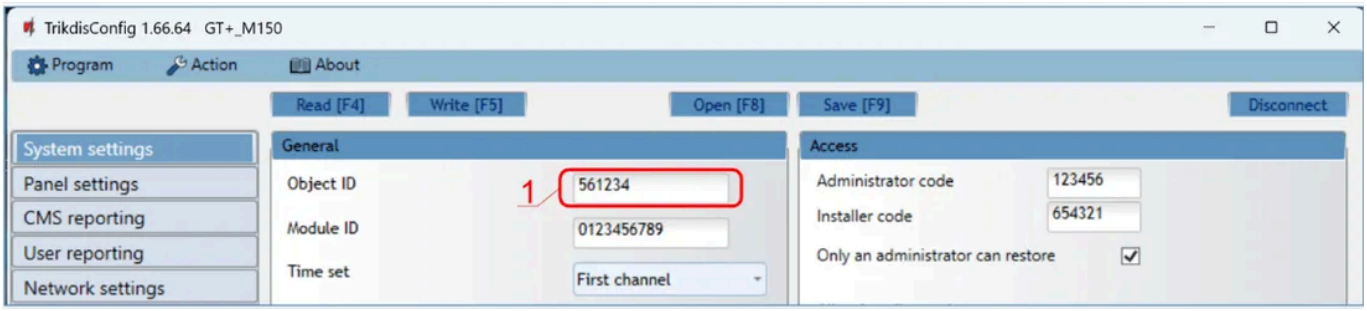


Abbildung 9. TrikdisConfig – Seite System settings, Gruppe General.

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

Geben Sie auf der Seite **Panel settings** den Anschluss der Zentrale an, falls Sie das in Punkt 2.2 noch nicht getan haben: Beim Anschluss an TIP/RING muss **Communication protocol** auf **AUTO** stehen (GT: **Dual tone**); beim Anschluss an Datenbus oder serielle Schnittstelle wählen Sie im Feld **Security panel model** den Typ der angeschlossenen Zentrale (die Abbildungen in Punkt 2.2).

Stellen Sie danach auf der Seite **CMS reporting**, im Teil **Primary channel** (Hauptkanal), die Daten des Empfängers ein.

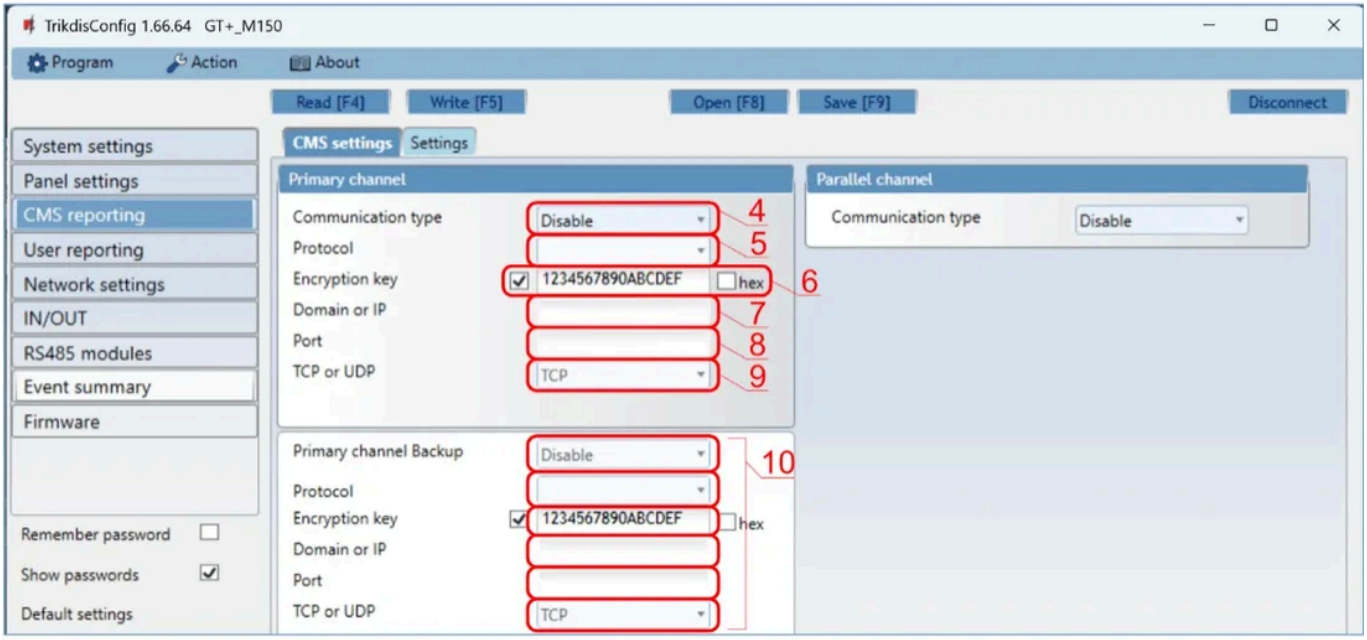


Abbildung 10. TrikdisConfig – CMS reporting, Reiter CMS settings.

- 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** – der Domainname oder die 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 bei einem Fehler des Hauptkanals; füllen Sie ihn genauso aus, die Angabe wird empfohlen.

Geben Sie zum Schluss auf der Seite **Network settings**, im Reiter **SIM1**, die Daten der Karte ein (**SIM card PIN**, **APN**, **DNS 1, DNS 2**), falls Sie das in Punkt 2.2 noch nicht getan haben.

Beim Protokoll **DC-09** geben Sie im Reiter **Settings** auch die Linien- und Empfängernummer ein (**Line No.**, **Receiver No.**, Punkt 6.4). GT und GT+ melden an die Leitstelle nur über IP, einen SMS-Ersatzkanal haben sie nicht.

Drücken Sie am Ende der Einstellungen die Schaltfläche **Write [F5]** (Schreiben), warten Sie auf die Rückmeldung und ziehen Sie das USB-Kabel ab. Das Gerät ist damit bereit zum Anschließen. Beim Anschluss an die Telefonleitung muss auch hier das Wählgerät der Alarmzentrale eingeschaltet und eingestellt 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 Punkt 2.1) und ziehen Sie die Klemmleiste ab.
2. Setzen Sie die Nano-SIM-Karte in den 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).
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.

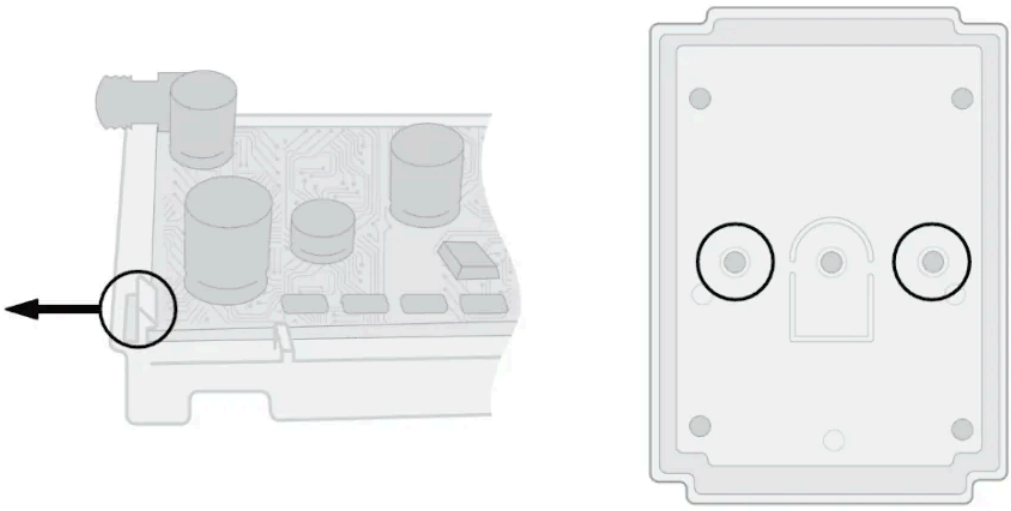


Abbildung 11. Herausnehmen der Leiterplatte aus dem Gehäuseboden (links: die Verriegelung und die Richtung des Herausnehmens) und die Schraubenlöcher des Gehäusebodens (rechts).

Die SIM-Karte muss aktiv sein, und für die IP-basierte Nutzung muss die mobile Datenverbindung auf ihr funktionieren. Wenn TrikdisConfig keinen PIN-Code verlangen soll, setzen Sie die Karte in ein Mobiltelefon ein und schalten Sie dort die PIN-Abfrage ab.

3.2 Platzierung und Antenne

- Montieren Sie den Kommunikator an einem **trockenen Ort in Innenräumen**, möglichst in der Nähe des Gehäuses der Alarmzentrale, damit die Verkabelung kurz bleibt.
- **In einem Metallgehäuse** wird das Mobilfunksignal stark abgeschwächt. 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 die Signalstärke**: Die Zahl der gelben Blinkimpulse der LED NETWORK muss bei 4G mindestens 3 sein (Punkt 1.6). Sind es weniger, suchen Sie einen besseren Ort, oder wechseln Sie zu einer empfindlicheren Antenne, die weiter entfernt platziert werden kann.
- Halten Sie Antenne und Kommunikator vom Transformator der Zentrale und von Netzleitungen fern.



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 Anschlussplan, der zu Ihrer Zentrale passt. Auf den Plänen sind **+DC** und **–DC** die Versorgungsklemmen des Kommunikators (GT: +12 VDC / −12 VDC, GT+: +12 / 24 VDC / −12 / 24 VDC), **A RS485** / **B RS485** die Klemmen A 485 / B 485. Der Kommunikator wird über den Hilfsspannungsausgang (AUX) der Zentrale versorgt, sodass bei einem Stromausfall der Akku der Zentrale auch den Kommunikator versorgt. Die Pläne zeigen den GT+; der Anschluss des GT ist derselbe.

3.3.1 DSC – Datenbus (Keybus)

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

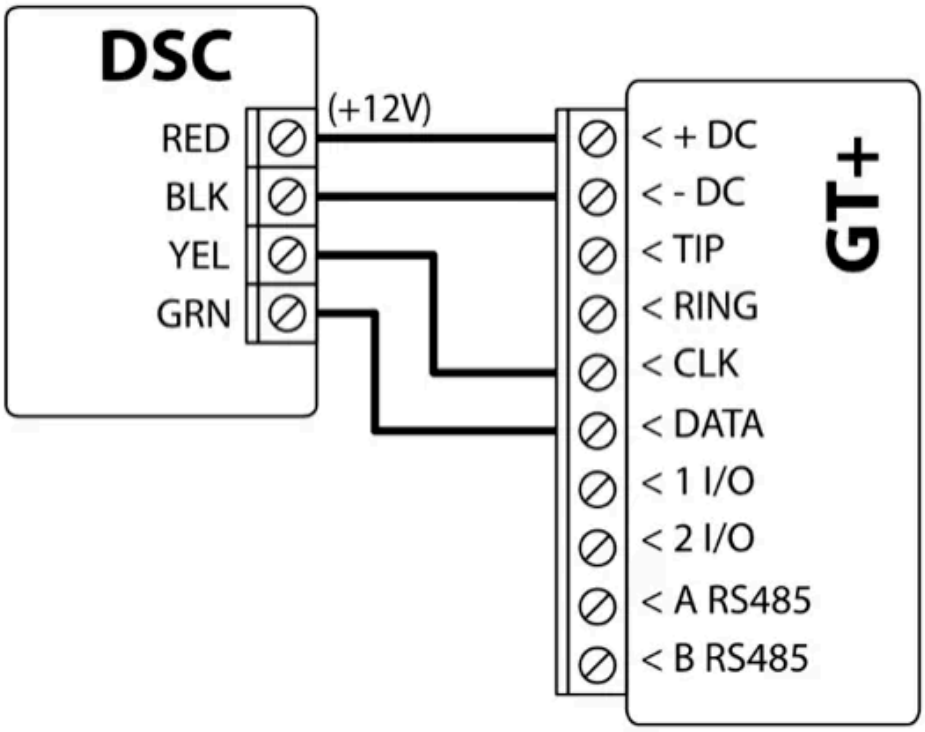


Abbildung 12. Anschluss einer DSC-Zentrale über den Datenbus (Keybus, „Keypad bus"): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Nur am Keybus angeschlossen, erhält der Kommunikator von der Zentrale den allgemeinen Zustand der Zonen, den Zonentyp (Feuer, Einbruch, Wasserleck usw.) kennt er nicht. Daher meldet er jeden Alarm **als allgemeinen Alarm, mit dem Contact-ID-Code E130**, und manche Leitstellen behandeln diesen anders als den tatsächlich ausgelösten Zonentyp. Wenn die Ereignisse mit den eigenen Contact-ID-Codes der Zentrale gesendet werden sollen (zum Beispiel Feueralarm: E110), schließen Sie beim GT+ auch die Klemmen TIP/RING an (Punkt 3.3.2).

3.3.2 DSC – Keybus und TIP/RING (nur GT+)

Der GT+ kann an eine DSC-Zentrale gleichzeitig über den Datenbus und den Telefonleitungsausgang angeschlossen werden: Verbinden Sie neben den Keybus-Leitungen auch die Klemmen **TIP** → **TIP** und **RING** → **RING** der Zentrale mit denen des Kommunikators.

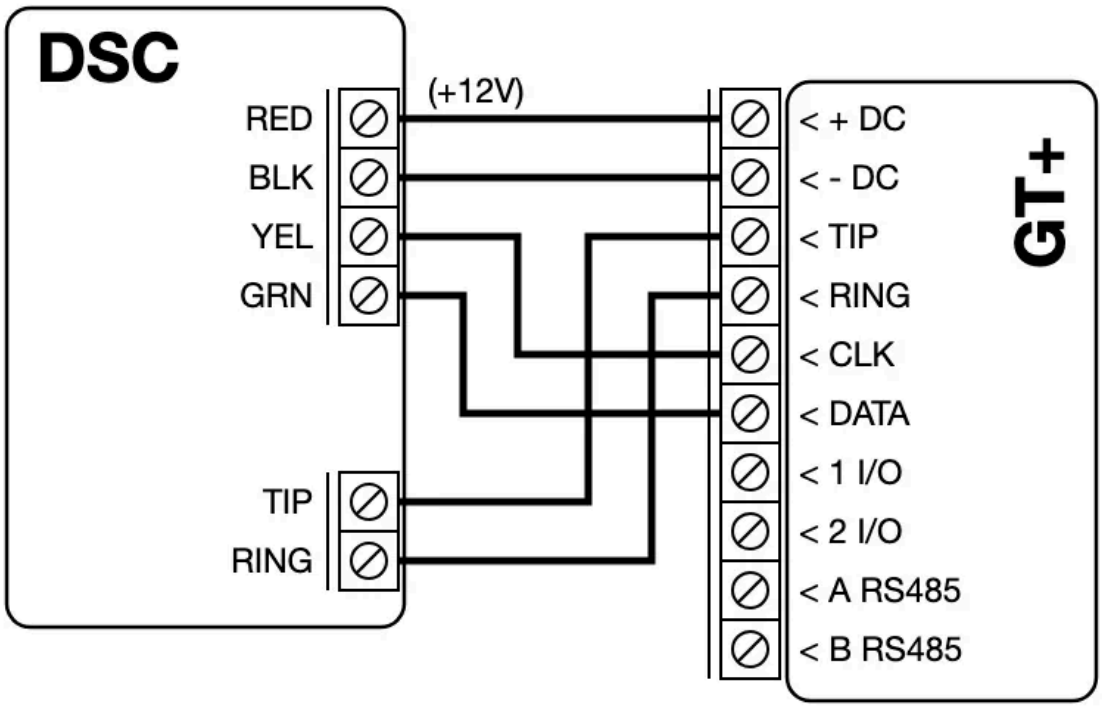


Abbildung 13. Anschluss einer DSC-Zentrale über den Datenbus („Keypad bus“) und die Klemmen TIP/RING zusammen (GT+): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA sowie TIP → TIP, RING → RING.

In diesem Fall dient der Keybus der Steuerung und den Zuständen (Fern-Scharf- und -Unscharfschaltung, Bereichs- und Zonenzustände), die Ereignisse sendet dagegen das Telefon-Wählgerät der Zentrale über die Klemmen TIP/RING, sie gehen also mit den eigenen Contact-ID-Codes der Zentrale. Solange der TIP/RING-Anschluss funktioniert, sendet der Kommunikator die vom Keybus kommenden Ereignisse nicht ein zweites Mal.

Stellen Sie für diesen Anschluss auf der Seite **Panel settings** von TrikdisConfig Folgendes ein:

1. **Communication protocol**: **AUTO**.
2. **Security panel model**: der Typ der DSC-Zentrale.
3. **Remote Arm/Disarm**: Setzen Sie das Häkchen, wenn die Benutzer die Zentrale aus der App Protegus 2 steuern möchten.

Auch das Telefon-Wählgerät der DSC-Zentrale muss programmiert werden, damit es die Ereignisse sendet – das beschreibt Punkt 4.1.1.

3.3.3 Paradox – serielle Schnittstelle

An die serielle Schnittstelle der Paradox-Zentrale wird der Kommunikator mit dem separat erhältlichen Kabel **EX-CRP2.4** angeschlossen: **Rot → +DC**, **Schwarz → −DC**, **Gelb → CLK**, **Grün → DATA**.

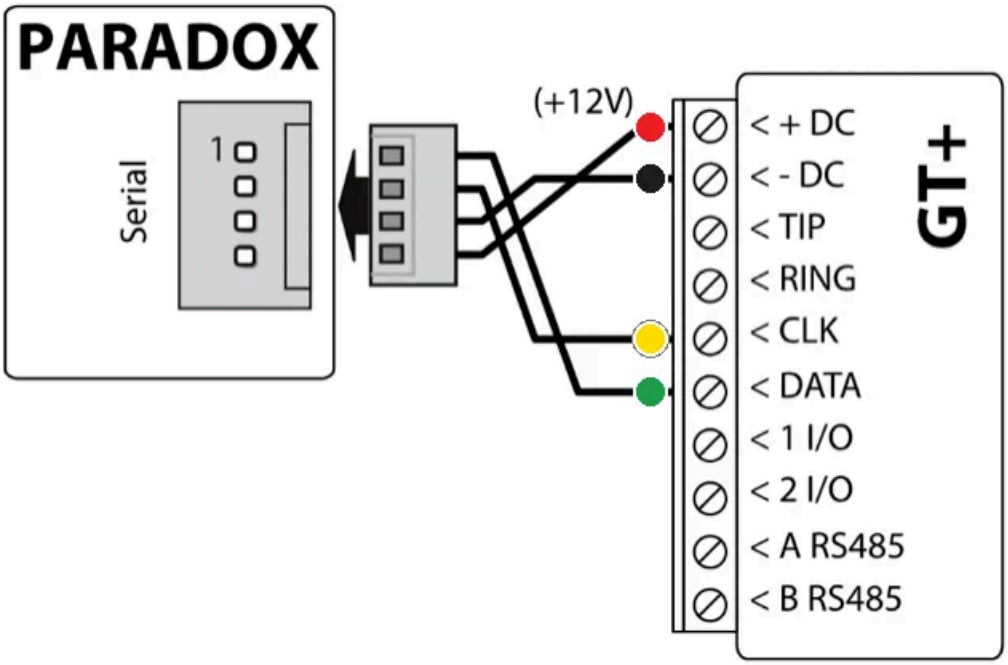


Abbildung 14. Anschluss einer Paradox-Zentrale über die serielle Schnittstelle mit dem Kabel EX-CRP2.4 (separat zu bestellen; „Use the EX-CRP2.4 cable (ordered separately)"): Rot → +DC, Schwarz → −DC, Gelb → CLK, Grün → DATA.

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

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

3.3.4 Paradox SP/MG – Keybus und TIP/RING

Die Paradox-Zentralen Spectra SP, SP+ und Magellan MG, MG+ können statt über die serielle Schnittstelle auch über ihren Datenbus (Keybus) und ihre Klemmen TIP/RING zusammen angeschlossen werden: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK** sowie **TIP** → **TIP**, **RING** → **RING**. Dieser Anschluss nutzt den Keybus der Zentrale statt der seriellen Schnittstelle, daher ist die kostenpflichtige Freischaltung der seriellen Schnittstelle von Paradox nicht nötig.

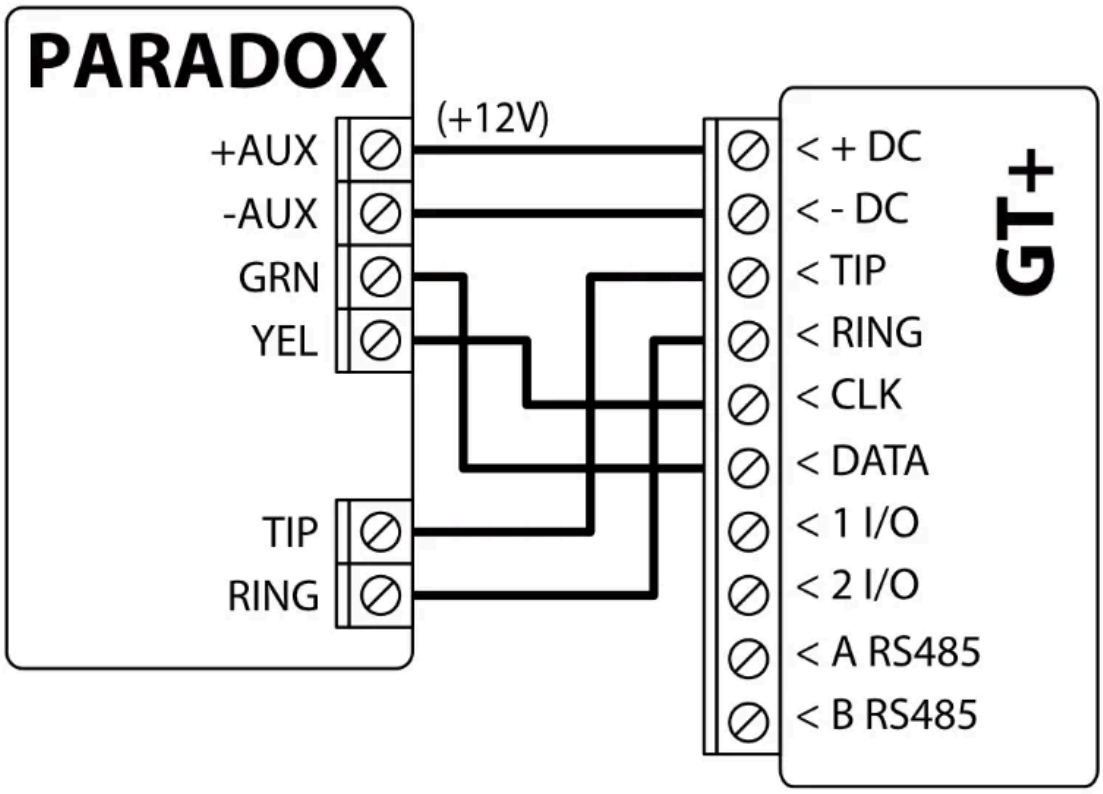


Abbildung 15. Anschluss einer Paradox-Zentrale SP / SP+ / MG / MG+ über den Keybus (Datenbus, „Keypad bus“) und die Klemmen TIP/RING zusammen: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

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

Stellen Sie für diesen Anschluss auf der Seite **Panel settings** von TrikdisConfig Folgendes ein:

1. **Communication protocol**: **AUTO** (GT: **Dual tone**).
2. **Security panel model**: **7. Paradox SP+/MG+ series KeyBus**.
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 16. TrikdisConfig – Panel settings für den Anschluss Keybus + TIP/RING: Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm angehakt, PC download password eingegeben.

Auch die Paradox-Zentrale muss programmiert werden, damit sie die Ereignisse an die Leitstelle sendet und aus Protegus 2 steuerbar ist – das beschreibt Punkt 4.1.2.

3.3.5 UTC Interlogix (Caddx) – Datenbus

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

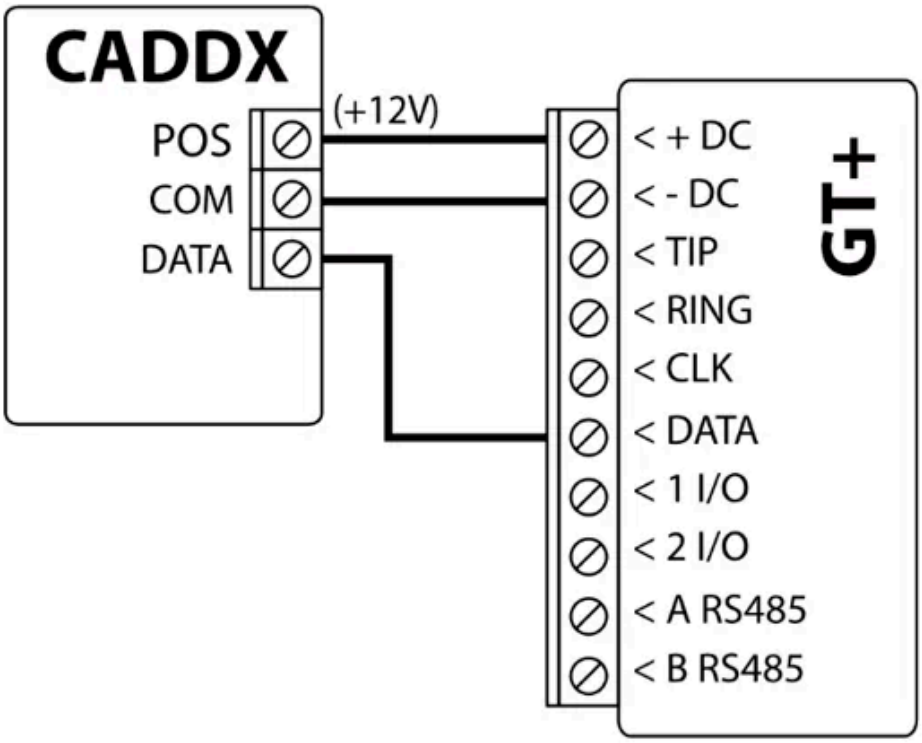


Abbildung 17. Anschluss einer UTC-Interlogix-Zentrale (Caddx) NetworX über den Datenbus („Keypad bus"): POS → +DC, COM → –DC, DATA → DATA.

3.3.6 Texecom – serielle Schnittstelle

An die serielle Schnittstelle der Texecom-Zentrale Premier / Premier Elite wird der Kommunikator mit dem separat erhältlichen Kabel **EX-CRP4** angeschlossen: **Rot → +DC**, **Schwarz → –DC**, **Blau → CLK**, **Weiß → DATA**.

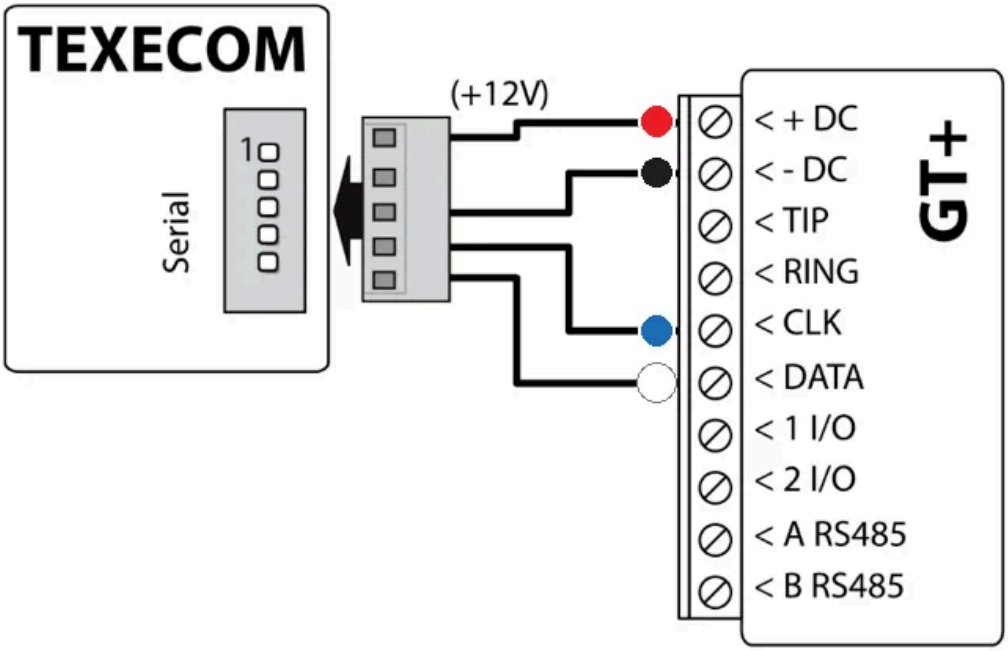


Abbildung 18. Anschluss einer Texecom-Zentrale über die serielle Schnittstelle mit dem Kabel EX-CRP4 (separat zu bestellen; „Use the EX-CRP4 cable (ordered separately)“): Rot → +DC, Schwarz → −DC, Blau → CLK, Weiß → DATA.

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

3.3.7 InnerRange Inception

Der Kommunikator wird über den Versorgungsausgang der Inception-Zentrale versorgt (**VOUT +** → **+DC**, **VOUT 0V** → **−DC**), die Datenverbindung kommt vom USB-Port der Zentrale, mit dem Kabel **993030USB** von Inner Range: **Schwarz** → **0V / −DC**, **Grün** → **CLK**, **Weiß** → **DATA**.

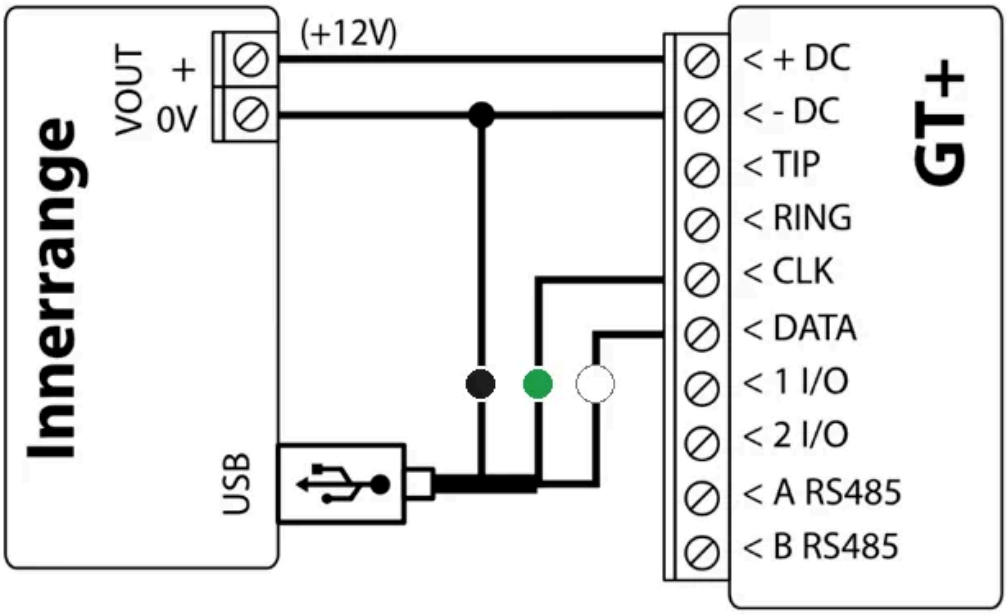


Abbildung 19. Anschluss der InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; vom USB-Port mit dem Kabel 993030USB („Cable, Inner Range part number 993030USB“) Schwarz → −DC, Grün → CLK, Weiß → DATA.

- schwarze Leitung („Black wire“)
- grüne Leitung („Green wire“)
- weiße Leitung („White wire“)

3.3.8 InnerRange Integriti

An die serielle Schnittstelle **Port 0** der Integriti-Zentrale 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**.

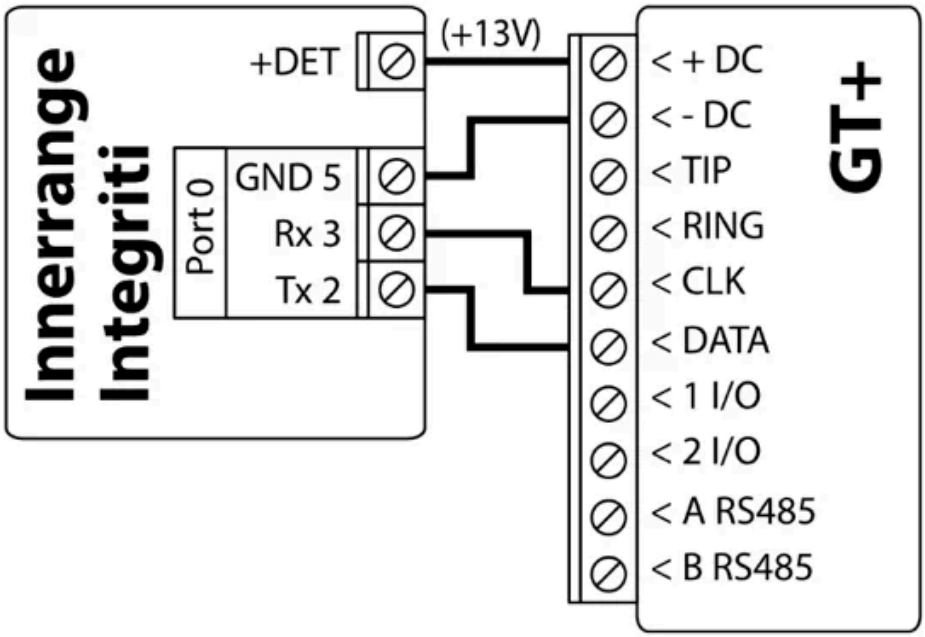


Abbildung 20. Anschluss der InnerRange Integriti an Port 0 mit dem Kabel INTG-996795 („Cable, Inner Range part number INTG-996795“): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – Datenbus

Schließen Sie den Bedienteilbus der Honeywell-Zentralen 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**.

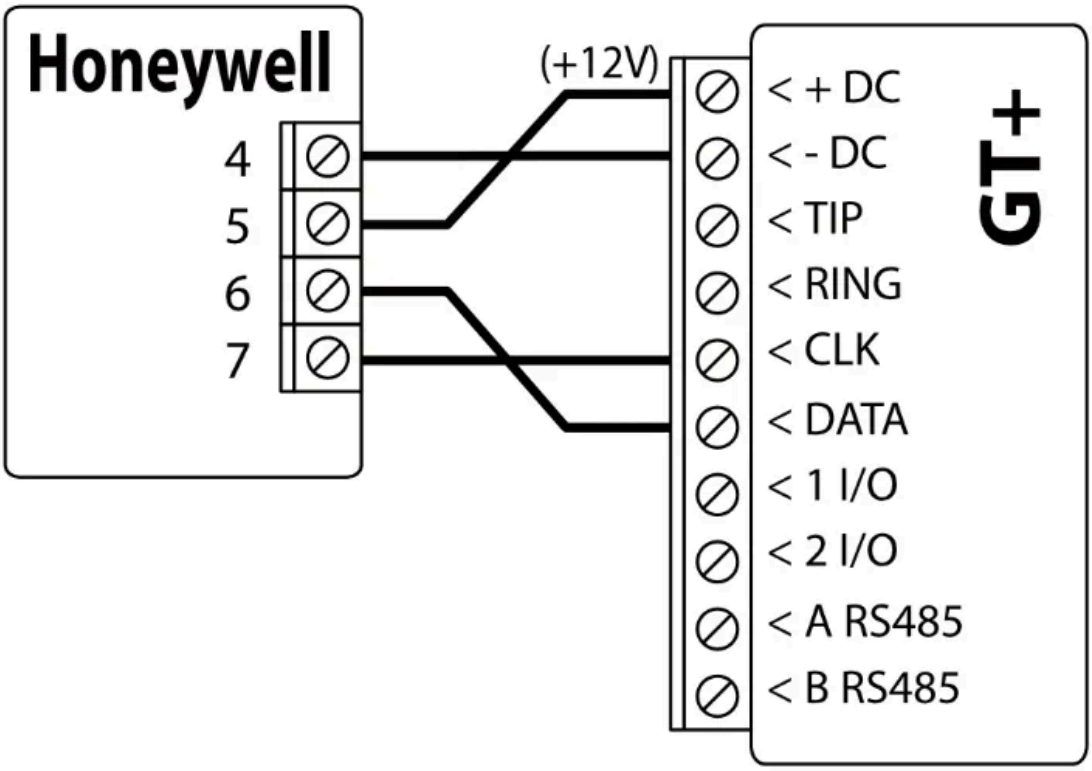


Abbildung 21. Anschluss einer Honeywell-Zentrale Vista-15 / -20 / -48 über den Datenbus („Keypad bus"): Klemme 5 → +DC, 4 → –DC, 7 → CLK, 6 → DATA.

3.3.10 Jede Zentrale – TIP/RING

Jede andere Zentrale kann über ihren Telefonleitungs-Kommunikator angeschlossen werden: 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 eingestellt werden (Punkt 4.2).

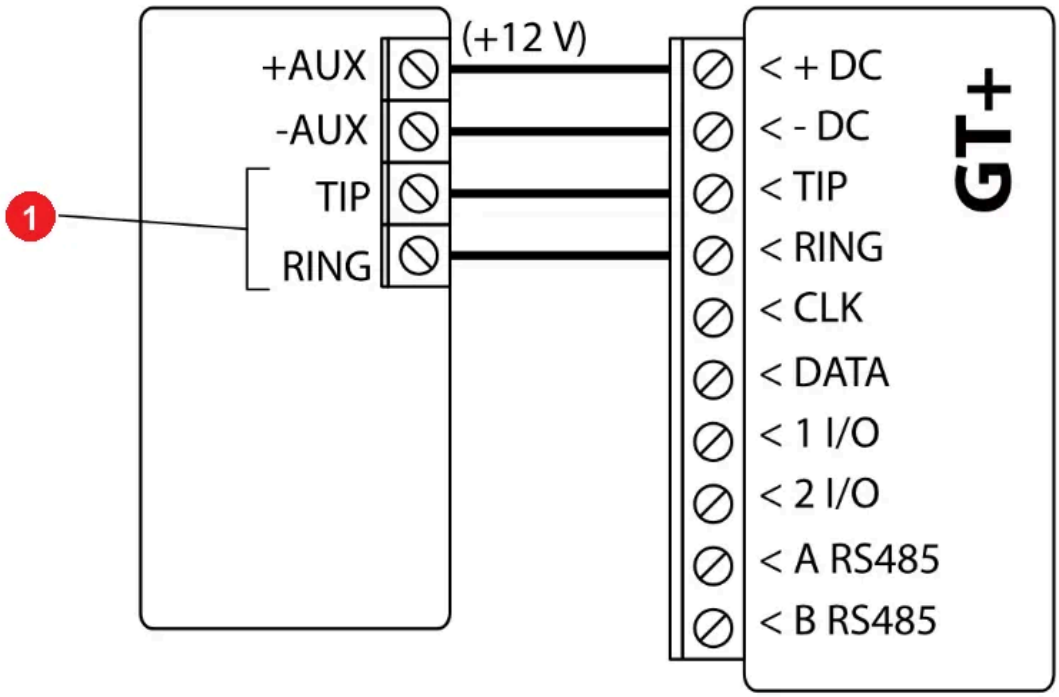


Abbildung 22. Anschluss an den Telefonleitungs-Kommunikator der Zentrale („Control panel"): +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

- 1 Klemmen des Telefonleitungs-Kommunikators der Zentrale („Telephone line communicator terminals")

3.4 Anschluss einer Schlüsselschalter-Zone

Wenn Sie die Zentrale aus der App Protegus 2 so scharf- und unscharfschalten möchten, dass der Ausgang (PGM) des Kommunikators die **Schlüsselschalter-Zone** der Zentrale schaltet, folgen Sie diesem Anschluss. Die zwei I/O-Klemmen mit Doppelfunktion des Kommunikators lassen sich als Ausgang (OUT, PGM) einstellen, sodass die zwei Ausgänge zwei Bereiche des Systems steuern können: Schließen Sie die Schlüsselschalter-Zone 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** von TrikdisConfig das Häkchen bei **Remote Arm/Disarm**, stellen die Klemmen auf der Seite **IN/OUT** auf die Funktion **OUT** (Punkt 6.7) und ordnen in der App Protegus 2 die Ausgänge nach Punkt 5.2 den Bereichen zu.

Beim Anschluss über 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 Schlüsselschalter-Zone:

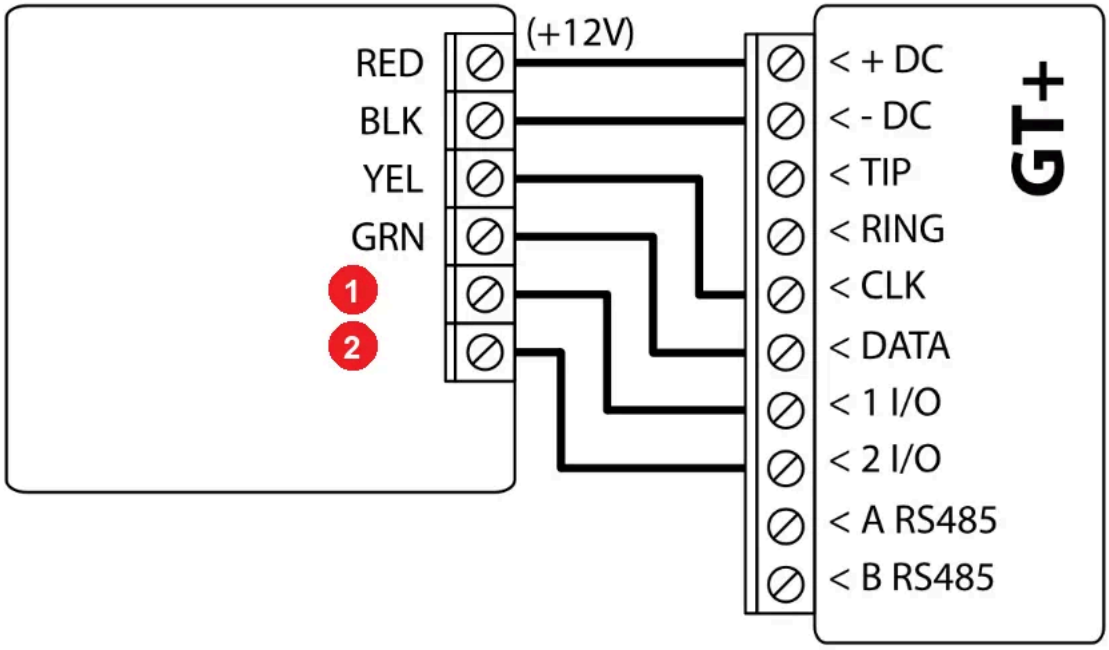


Abbildung 23. Scharf- und Unscharfschalten mit Schlüsselschalter-Zone („Zones (keyswitch)“), beim Anschluss über Datenbus oder serielle Schnittstelle („Keypad bus or serial“): Klemme RED der Alarmzentrale („Control panel terminals“) → +DC, BLK → −DC, YEL → CLK, GRN → DATA; die Zone von Bereich 1 → 1 I/O, die von Bereich 2 → 2 I/O.

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

Beim Anschluss an die Telefonleitung (TIP/RING) sendet die Zentrale die Ereignisse über ihr Wählgerät, das Scharf- und Unscharfschalten erfolgt ebenso über die Schlüsselschalter-Zone:

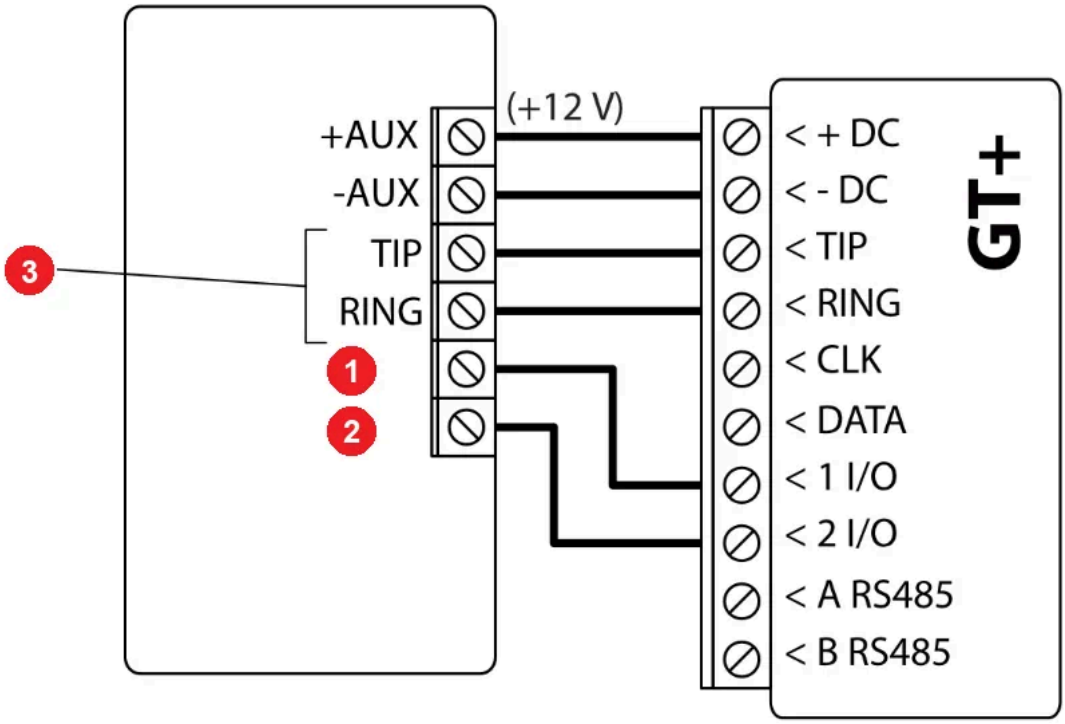


Abbildung 24. Scharf- und Unscharfschalten mit Schlüsselschalter-Zone („Zone (keyswitch)“), beim Anschluss an die Telefonleitung: Klemme +AUX der Alarmzentrale („Control panel“) → +DC, −AUX → −DC, TIP → TIP, RING → RING; die Zone von Bereich 1 → 1 I/O, die von Bereich 2 → 2 I/O.

- 1 Schlüsselschalter-Zone von Bereich 1 („1-st Area“)
- 2 Schlüsselschalter-Zone von Bereich 2 („2-nd Area“)
- 3 Klemmen des Telefonleitungs-Kommunikators der Zentrale („Telephone line communicator terminals“)

Die Schlüsselschalter-Zone kann impulsgesteuert oder bistabil (zwei Stellungen) sein – in der App Protegus 2 muss derselbe Modus eingestellt werden (Punkt 5.2). Über die Einzelheiten und Fallstricke des Scharfschaltens mit Schlüsselschalter gibt es einen eigenen Artikel: Fern-Scharfschaltung mit Schlüsselschalter aus der App Protegus 2.

3.5 Anschluss der Eingänge

Die zwei I/O-Klemmen mit Doppelfunktion des Kommunikators können als Eingang (IN) auch weitere Melder aufnehmen (z. B. Sabotagekontakt, Paniktaster), unabhängig von der Alarmzentrale. An den Eingang kann ein Kreis NO, NC, NO/EOL, NC/EOL, NO/DEOL oder NC/DEOL angeschlossen werden; ab Werk sind beide Klemmen Eingang, NO. Den Eingangstyp stellen Sie auf der Seite **IN/OUT** von TrikdisConfig im Feld **Type** ein. Der Eingang wird zwischen der gewählten I/O-Klemme und der Klemme **−DC** (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	–

Typ	Ruhezustand	Alarm	Sabotage
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 Eingangskreise zwischen COM und dem Punkt INx: NO, NC, NC/EOL, NO/EOL sowie mit Sabotageerkennung NO/DEOL und NC/DEOL, mit Abschlusswiderständen 2,2 kΩ; die einzelnen Zustände (Kurzschluss, Unterbrechung, 2,2 kΩ, 3,3–5,5 kΩ) erklärt die Tabelle in Punkt 3.5.

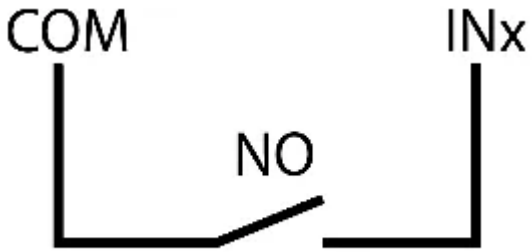


Abbildung 25. NO – im Ruhezustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

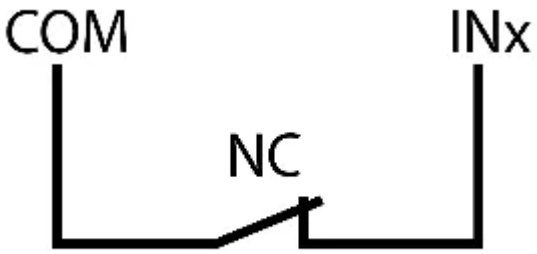


Abbildung 26. NC – im Ruhezustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

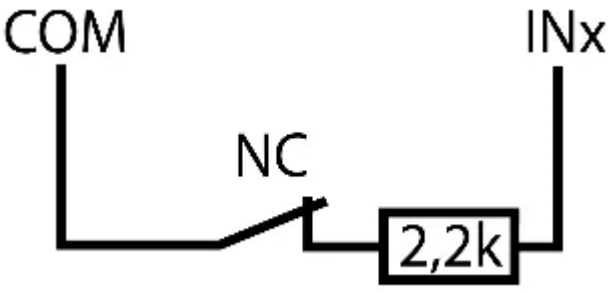


Abbildung 27. NC/EOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

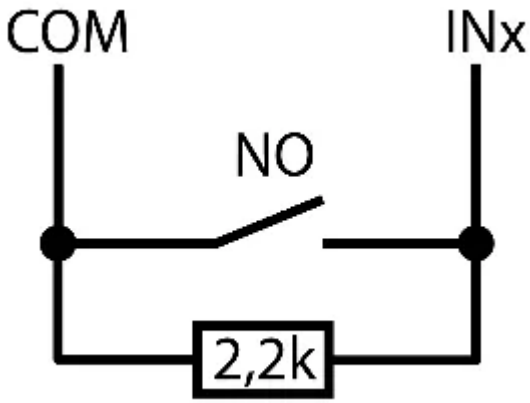


Abbildung 28. NO/EOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

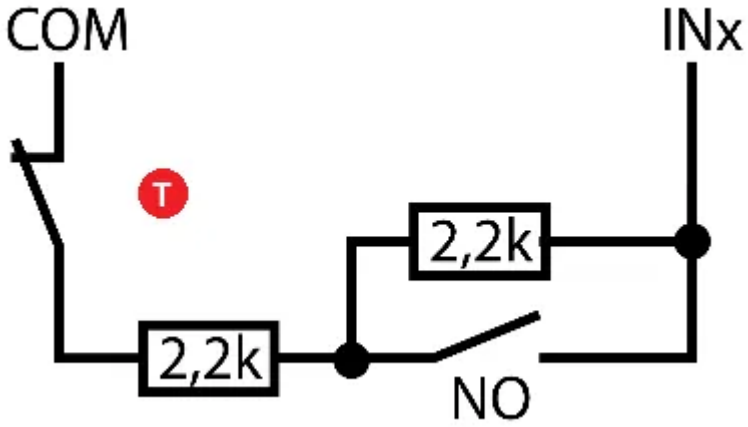


Abbildung 29. NO/DEOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

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

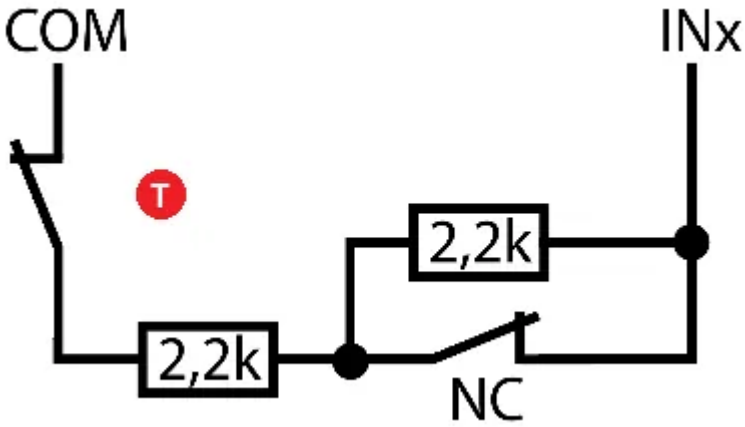


Abbildung 30. NC/DEOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

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

Wenn mehr Ein- oder Ausgänge nötig sind, schließen Sie an den Kommunikator ein Trikdis-Erweiterungsmodul **iO-8** an (Punkt 3.7); seinen Anschluss beschreibt auch die Anleitung des iO-8.

3.6 Anschluss eines Ausgangs mit Relais

Als Ausgänge 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 Relaiskontakte (NC, C, NO). Die verwendete I/O-Klemme muss auf der Seite **IN/OUT** von TrikdisConfig auf Ausgang (**OUT**) gestellt werden.

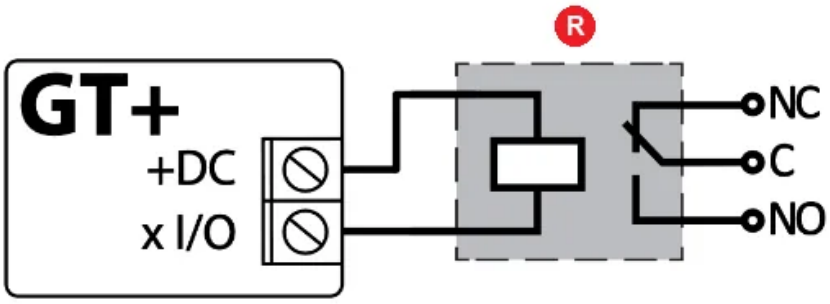


Abbildung 31. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule kommt zwischen +DC und die Klemme x I/O, die Kontakte (NC, C, NO) schalten den Verbraucher.

- R Relais („Relay“)

Die Ausgänge können Sie aus der App Protegus 2 oder per SMS-Befehl schalten (Kapitel 5).

3.7 Anschluss des Erweiterungsmoduls iO-8

Wenn mehr Ein- oder Ausgänge nötig sind, können an den RS485-Bus des Kommunikators bis zu vier Erweiterungsmodule **iO-8** angeschlossen werden; jedes liefert 8 weitere I/O mit Doppelfunktion. Verbinden Sie die Klemmen **A 485** und **B 485** mit den Klemmen **A (RS485)** und **B (RS485)** des Moduls; Kommunikator und Erweiterungsmodul werden beide über den Hilfsspannungsausgang der Zentrale versorgt (**+AUX** → **+DC**, **–AUX** → **–DC** an beiden Geräten). Das Erweiterungsmodul muss auf der Seite **RS485 modules** von TrikdisConfig hinzugefügt und eingestellt werden (Punkt 6.8).

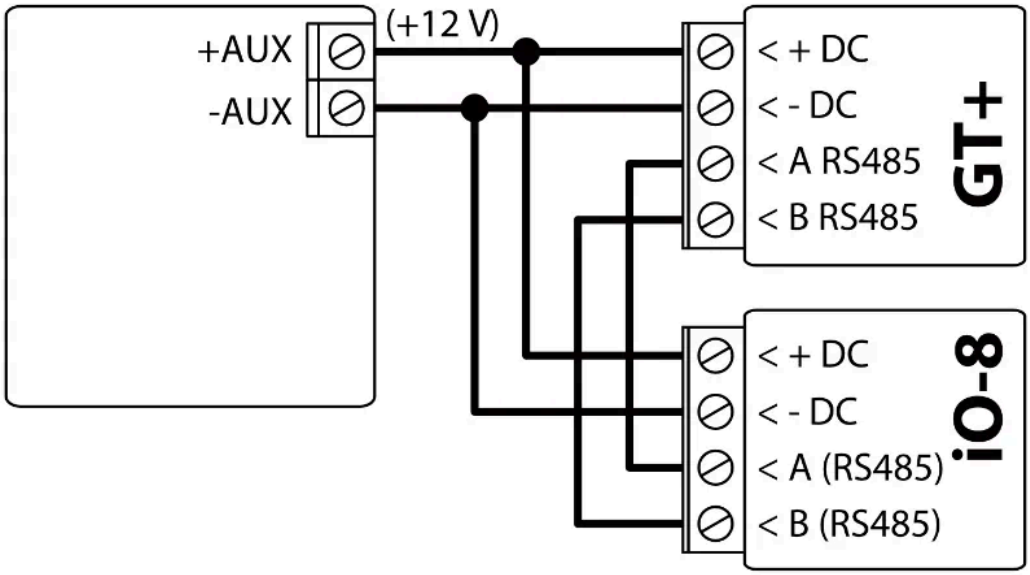


Abbildung 32. Anschluss des Erweiterungsmoduls iO-8 an den RS485-Bus des Kommunikators; die Versorgung kommt vom AUX-Ausgang der Alarmzentrale („Control panel"), für beide Geräte.

3.8 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** leuchtet grün und blinkt gelb – mit dem Netz verbunden; die Zahl der gelben Blinkimpulse ist die Signalstärke: Bei 4G sind 3 Blinkimpulse gut; zählen Sie weniger, ist das Signal schwach: Suchen Sie für den Kommunikator einen anderen Ort, oder verwenden Sie eine empfindlichere Antenne (Punkt 3.2);
- **TROUBLE** leuchtet nicht.

Wenn TROUBLE blinkt, nennt die Zahl der Blinkimpulse die Ursache (Punkt 1.6); jede andere abweichende LED-Anzeige weist ebenfalls auf einen Fehler hin, die Ursache finden Sie anhand der Tabellen in Punkt 1.6. Leuchtet keine LED, prüfen Sie die Versorgung und den Anschluss.

4. Programmierung der Alarmzentrale

Die Einstellung der Zentrale hängt davon ab, wie Sie sie angeschlossen haben: über Datenbus oder serielle Schnittstelle (Punkt 4.1) oder über ihren Telefonleitungs-Kommunikator, an den Klemmen TIP/RING (Punkt 4.2). Beim GT+ sind für den Anschluss DSC Keybus + TIP/RING beide nötig: die Einstellungen für den Keybus-Anschluss und die Programmierung des Wählgeräts der Zentrale (Punkt 4.1.1).

4.1 Anschluss über Datenbus oder serielle Schnittstelle

Hier beschreiben wir, wie die Zentrale eingestellt werden muss, damit der Kommunikator ihre Ereignisse liest und sie aus der Ferne steuern kann. Für die Fernsteuerung muss auf der Seite **Panel settings** von TrikdisConfig die Option **Remote Arm/Disarm** angehakt sein (Punkt 2.2).

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.

GT+, Anschluss Keybus und TIP/RING (Punkt 3.3.2): Das Telefon-Wählgerät der Zentrale muss programmiert werden, damit es die Ereignisse sendet. Die folgende Tabelle gilt für die Zentrale DSC PowerSeries PC1616 (PC1832, PC1864). Gehen Sie am an die Zentrale angeschlossenen Bedienteil in die Programmierung: **[*][8][Errichtercode]**, und geben Sie dann die Nummer der Sektion ein.

Sektion	Wert
[301] Erste Telefonnummer	Eine beliebige Nummer mit mehr als vier Ziffern, am Anfang **ohne D** (zum Beispiel `5555555`). Das D bedeutet Warten auf den Wählton; ohne es wählt die Zentrale schneller. Der Kommunikator nimmt jeden Anruf an
[310] Objektkennung des Systems	Die 4-stellige Objektkennung, danach `FF` (zum Beispiel `1234FF`). Verwenden Sie statt der Ziffer 0 das HEX-`A`
[311] Objektkennung von Bereich 1	Die 4-stellige Objektkennung; statt 0 das HEX-`A`
[350] Format des Kommunikators	`03` (Contact ID) für Telefonnummer 1
[351]–[376] Anrufrichtungen	Aktivieren Sie für Telefonnummer 1 die benötigten Ereignisgruppen: Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Prüfen Sie die Gruppe Opening/Closing gesondert: Bei manchen DSC-Zentralen ist sie ab Werk ausgeschaltet

Sektion	Wert
[380] Kommunikator-Option 1	Option 1 **EIN** (Kommunikator aktiviert); Option 3 **AUS** (DTMF-Wahl)
[381] Kommunikator-Option 2	Option 7 **AUS** (die Contact-ID-Meldecodes bildet die Zentrale automatisch)
[320]–[349] Meldecodes	Bei den zu meldenden Ereignissen ein beliebiger Wert, nur nicht `00`
[015] Systemoption 3	Option 7 **AUS** (Telefonleitungsüberwachung, TLM, ausgeschaltet)

Schalten Sie die Telefonleitungsüberwachung (TLM) ab: Bleibt sie eingeschaltet, kann die Zentrale einen Telefonleitungsfehler melden. Die Verzögerung des TLM-Fehlers stellen Sie in Sektion **[377]** ein.

Die obigen Sektionsnummern gelten für die Zentralen PC1616, PC1832 und PC1864 (Installationsanleitung v4.x). Bei anderen DSC-Typen können die Sektionsnummern abweichen – sehen Sie in der Programmieranleitung der Zentrale nach.

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.

Bei den Kommunikatoren GT und GT+ befindet sich das Feld **Security panel PC download password** auf der Seite **Panel settings** von TrikdisConfig, in der Gruppe **Serial bus** (Punkte 2.2 und 6.3).

Anschluss Keybus und TIP/RING (SP / SP+ / MG / MG+, Punkt 3.3.4): Die Zentrale muss zusätzlich so programmiert werden, dass sie die Ereignisse an die Leitstelle sendet und aus Protegus 2 steuerbar ist:

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

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]**.

Bei den Kommunikatoren GT und GT+ befindet sich das Feld **Security panel PC download password** auf der Seite **Panel settings** von TrikdisConfig, in der Gruppe **Serial bus**; 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

Adresse (location)	Segment	Einstellung
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.

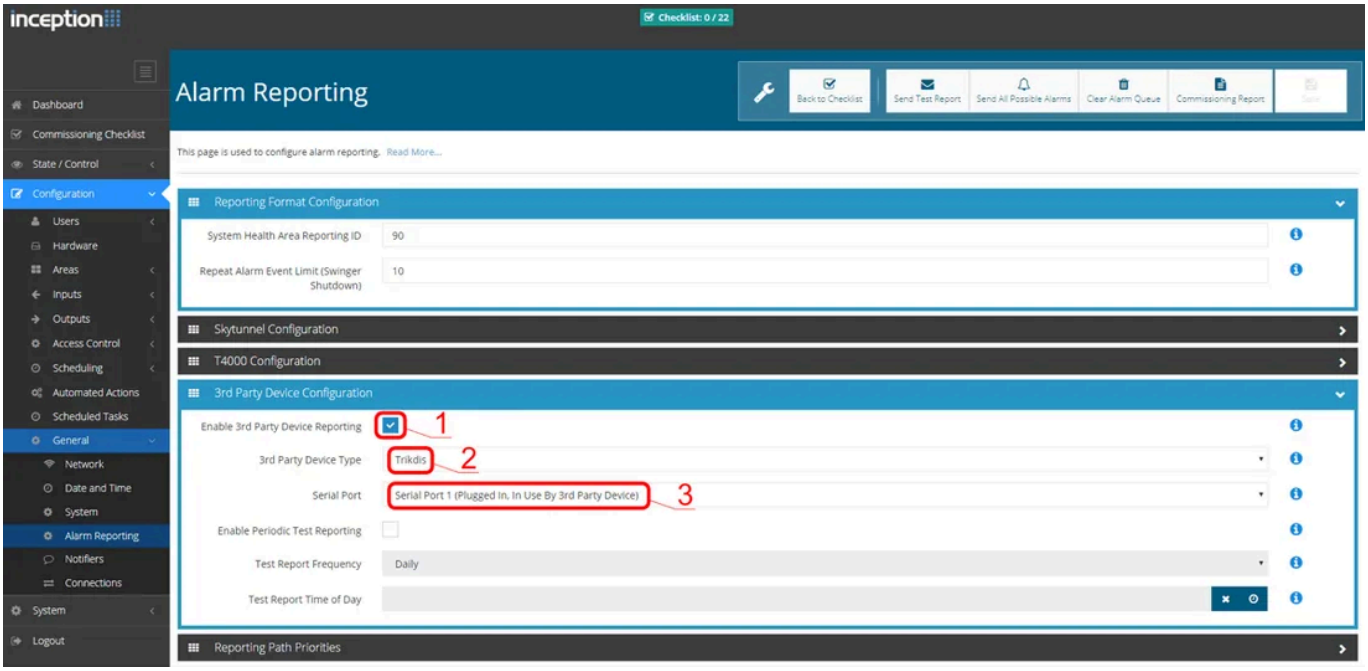


Abbildung 33. InnerRange Inception – Configuration → General → Alarm Reporting, Gruppe 3rd Party Device Configuration: Enable 3rd Party Device Reporting angehakt, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

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 können auch über ihren Telefonleitungsausgang an den Kommunikator angeschlossen werden (Punkt 3.3.10) – dann muss auch bei ihnen das Wählgerät eingestellt werden, 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
`*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 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:

Stelle (location)	Tasten	Bemerkung
	`*89713`	Eintritt 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 Mobil- und Web-App Protegus 2 sieht der Benutzer aus der Ferne den Zustand des Systems, wird über die Ereignisse benachrichtigt, kann scharf- und unscharfschalten und die Ausgänge des Kommunikators schalten. Die App kann für Android und iOS heruntergeladen werden (Google Play, App Store) oder im Browser genutzt werden: web.protegus.app. Melden Sie sich mit Ihrem Benutzernamen und Passwort an, oder registrieren Sie ein neues Konto.

5.1 Das Gerät hinzufügen

Prüfen Sie vor dem Hinzufügen des Geräts:

1. Die SIM-Karte ist aktiv, und die mobile Datenverbindung funktioniert auf ihr; ihr PIN-Code ist im Gerät eingetragen, oder die PIN-Abfrage ist abgeschaltet.

2. Auf der Seite **User reporting** → **PROTEGUS Cloud** von TrikdisConfig ist **Enable connection** angehakt (Punkt 6.5).
3. Die LED **POWER** leuchtet grün.
4. Die LED **NETWORK** leuchtet grün und blinkt gelb (das Gerät ist im Netz).

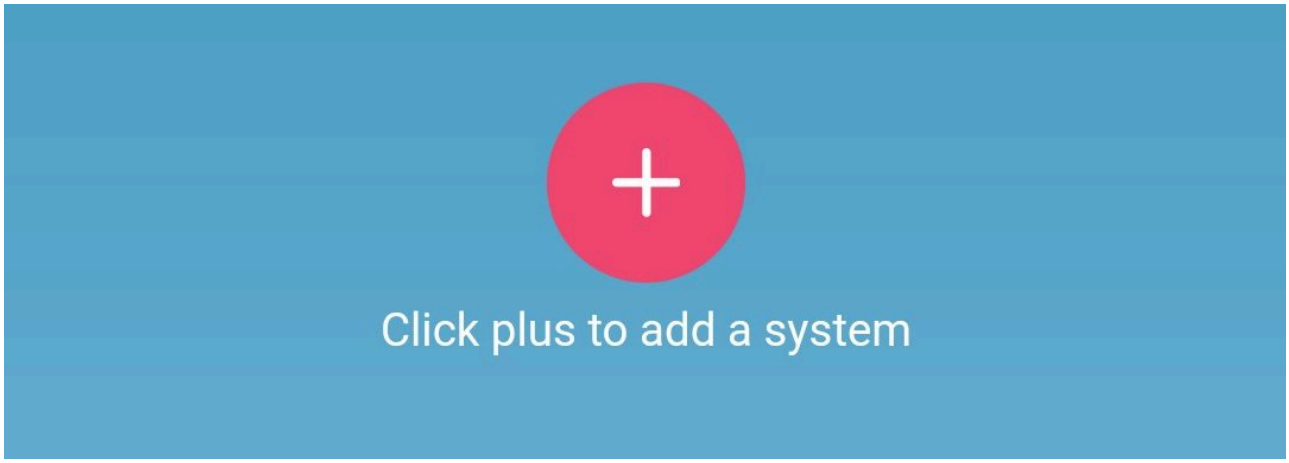
Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, 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



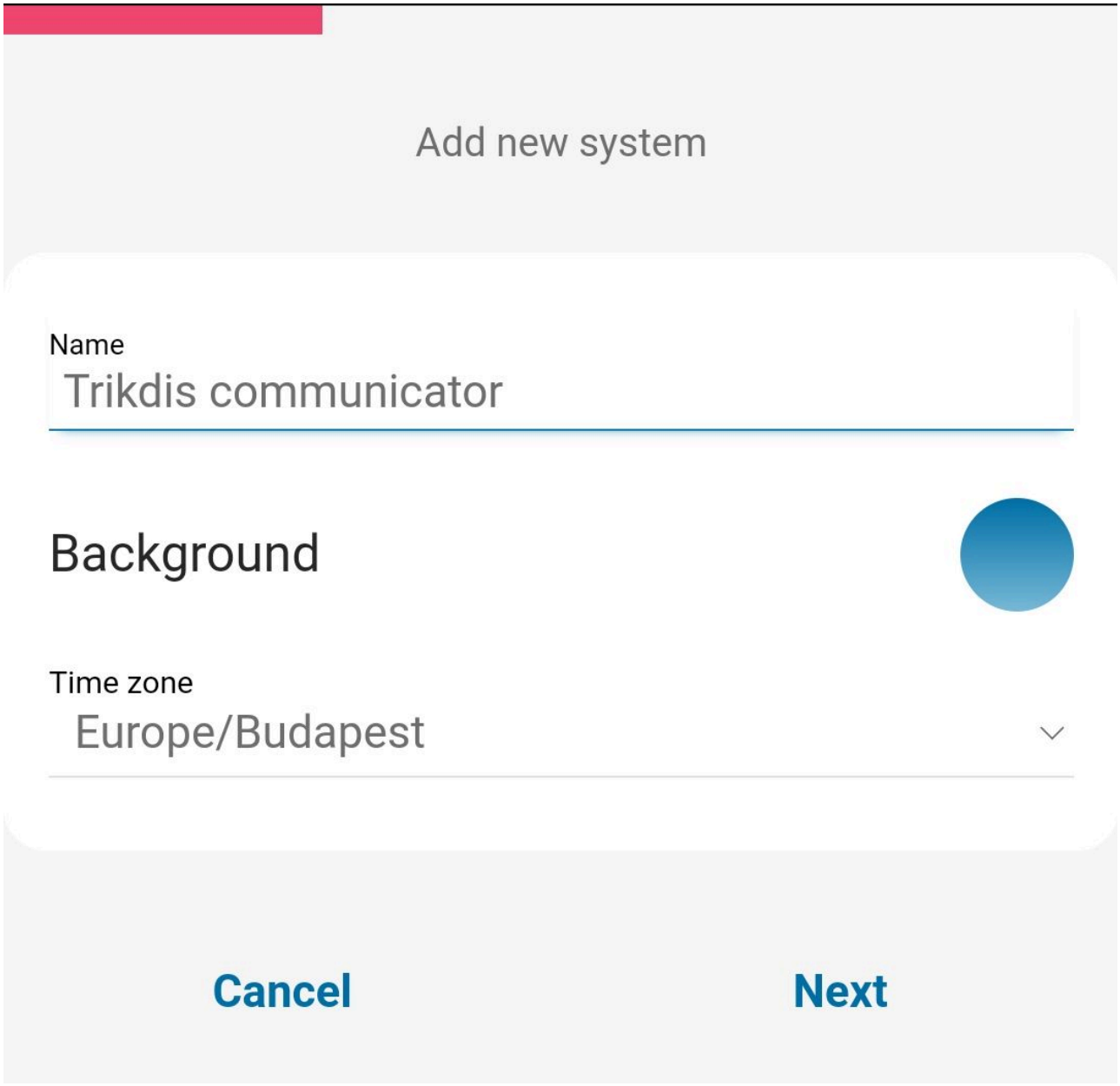
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



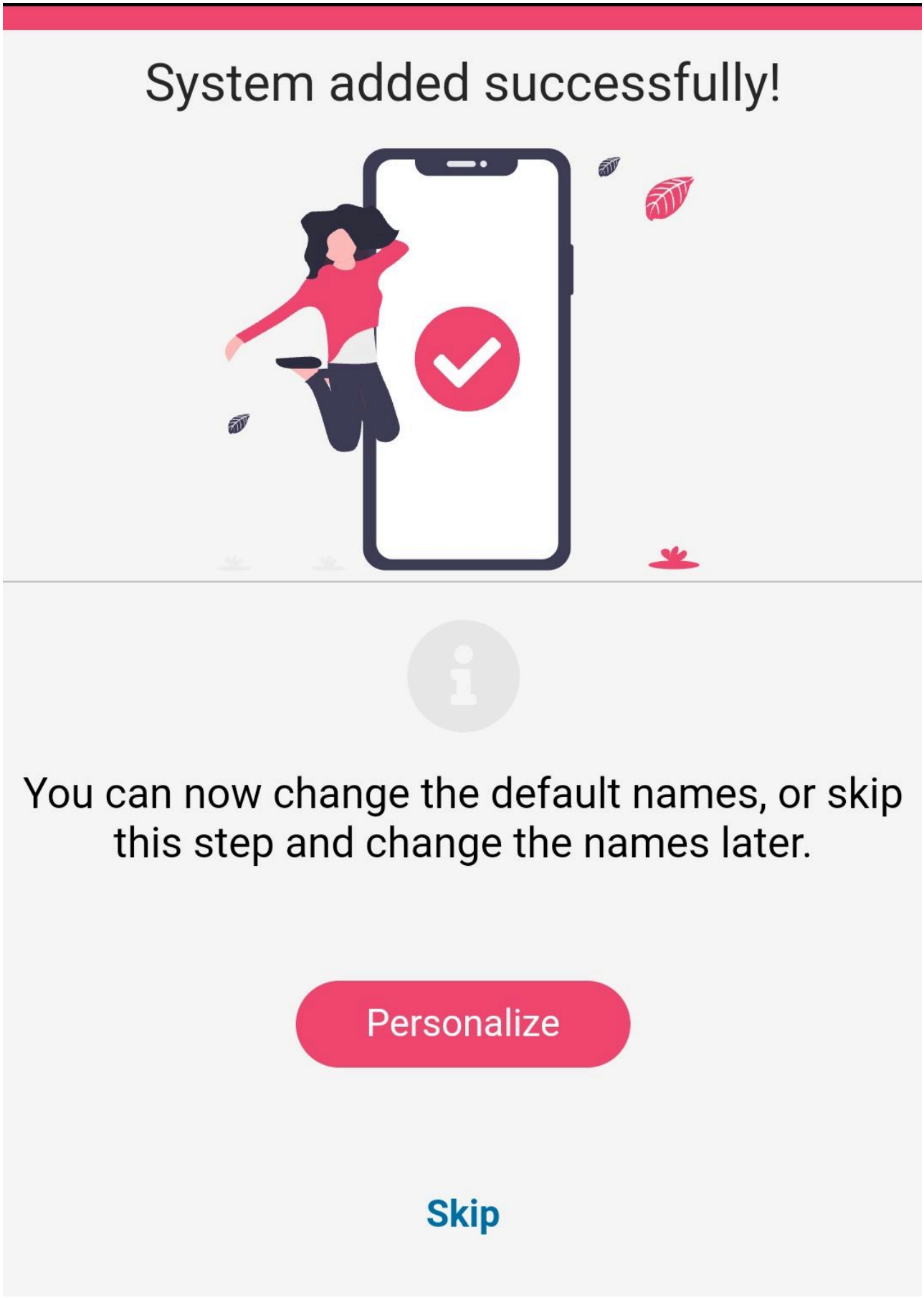
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



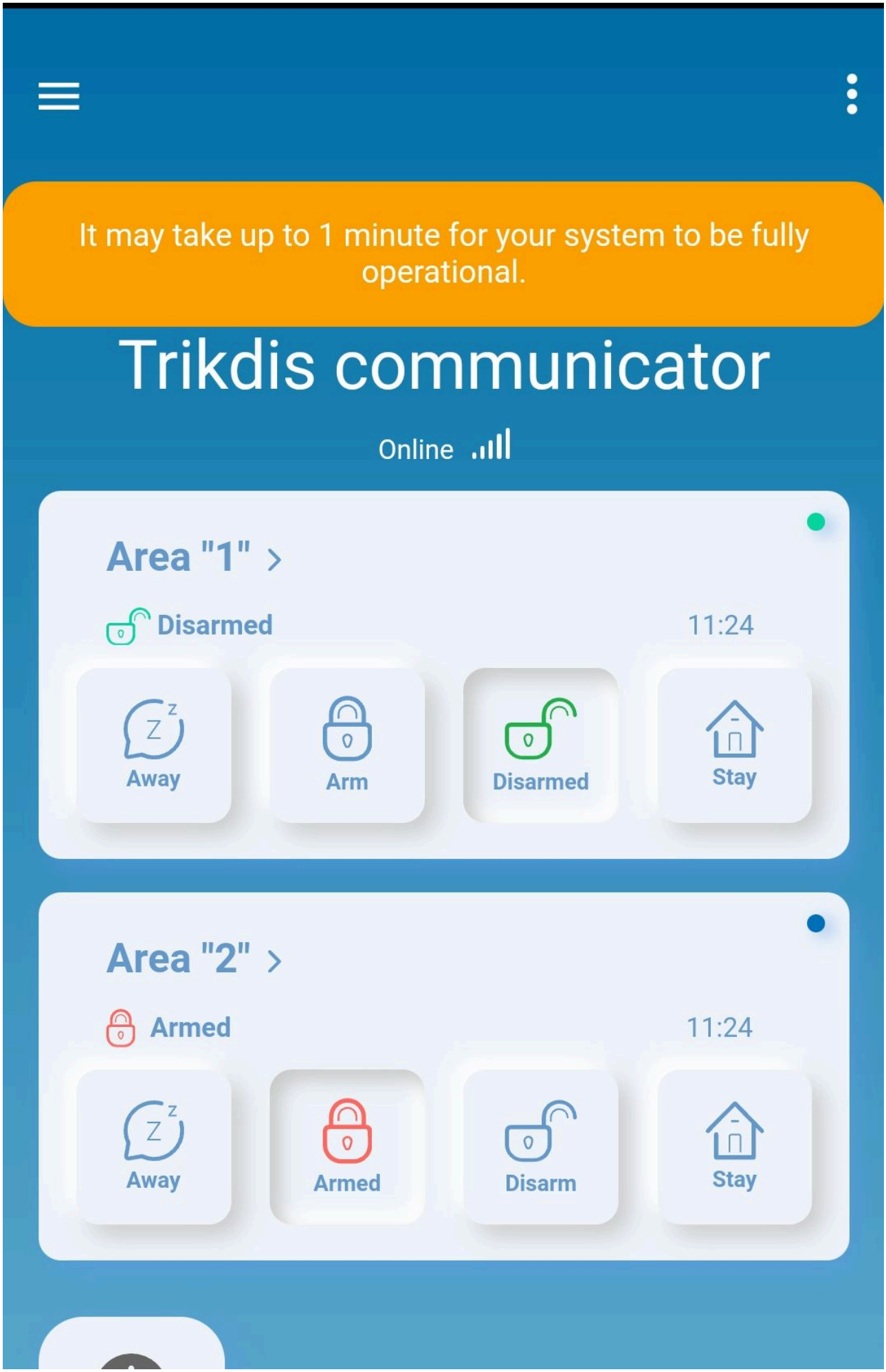
6. Add meg a rendszer nevét és válassz idozónát



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

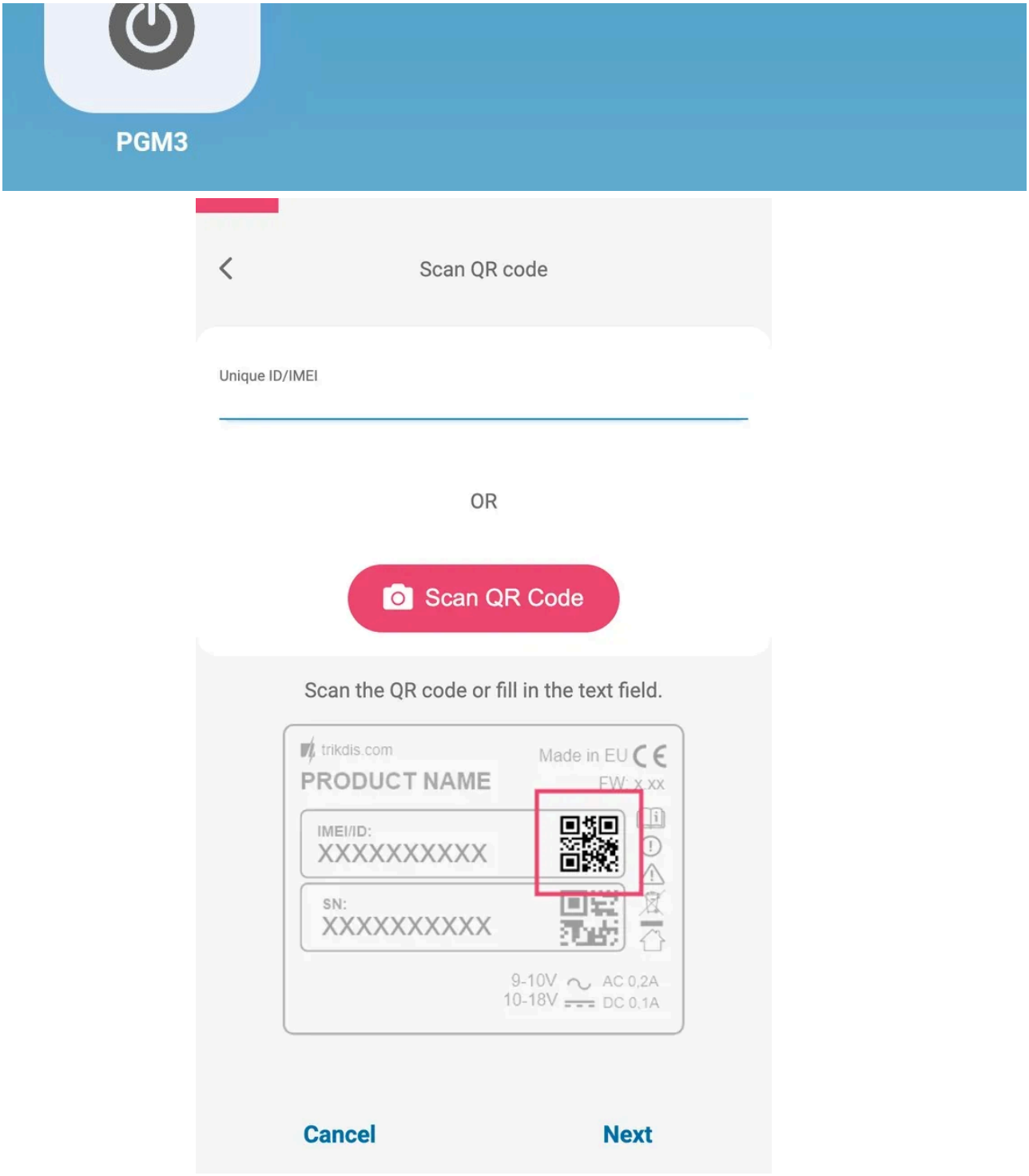


Abbildung 34. Protegus 2 – neues System hinzufügen: IMEI / Unique ID eingeben oder den QR-Code des Etiketts einlesen, dann Next.

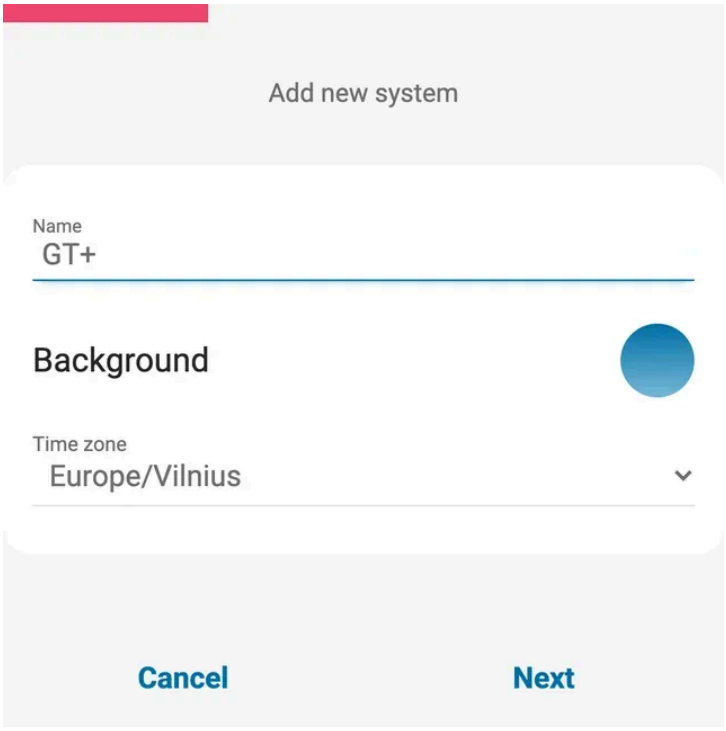


Abbildung 35. Protegus 2 – den Namen des Systems (Name) eingeben, dann Next.

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. Wenn der **PROTEGUS Cloud access Code** im Gerät nicht der Werkscode ist, 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 36. Protegus 2 – die Seite „Das System wird nicht aus der Ferne gesteuert“ beim Anlegen des Systems: Mit der Schaltfläche Continue gelangen Sie zur Einstellung des Bereichs und des PGM-Ausgangs.

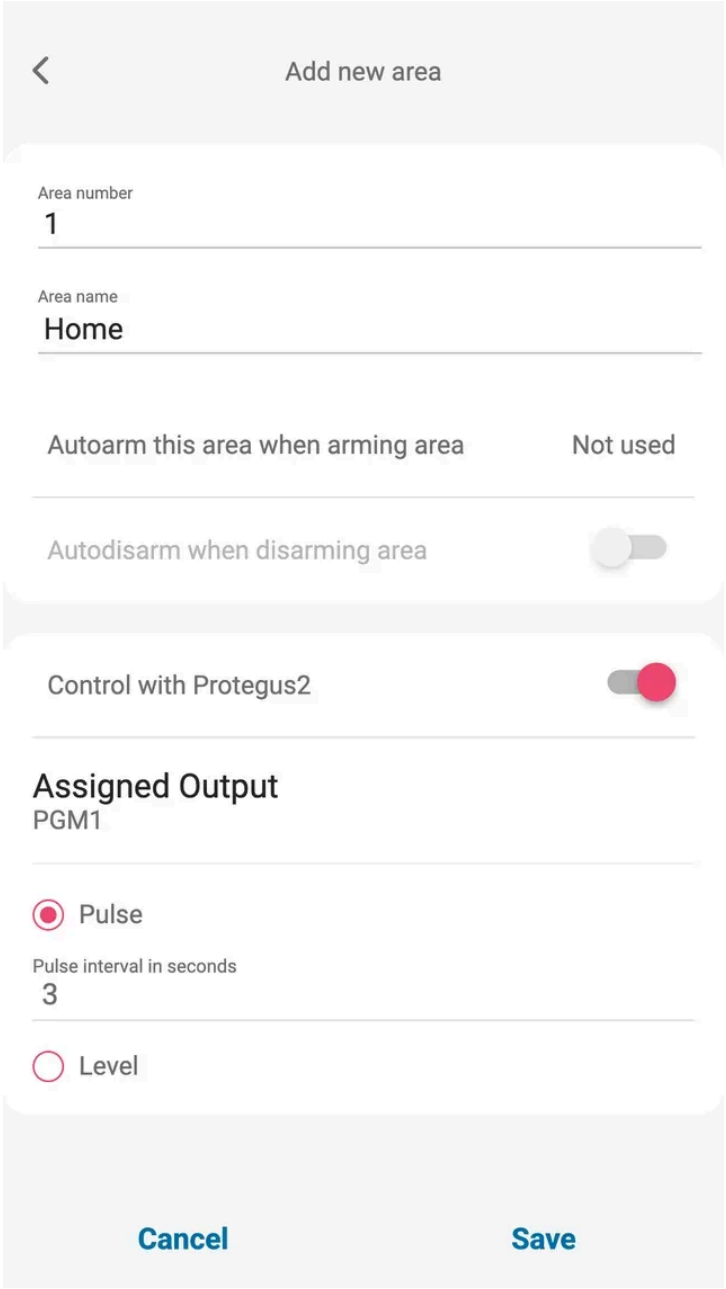


Abbildung 37. Protegus 2 – Bereich hinzufügen (Add new area): Area number, Area name, Control with Protegus2 eingeschaltet, Assigned Output PGM1, Pulse (3 s) oder Level, dann Save.

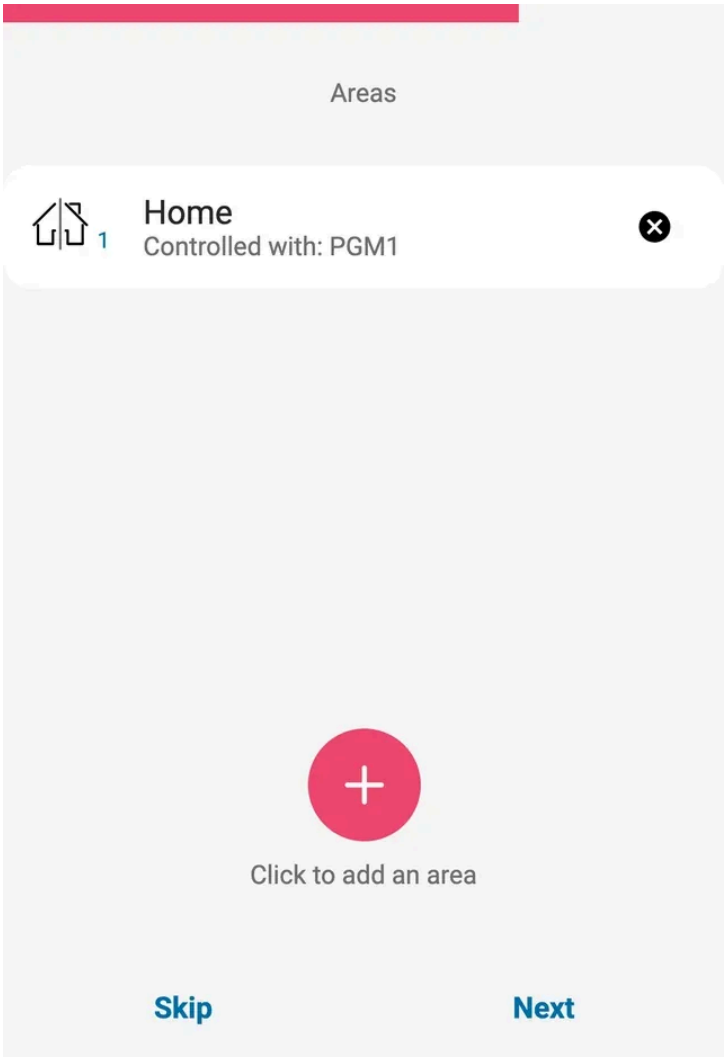


Abbildung 38. Protegus 2 – die Liste der Bereiche (Areas): Den Bereich Home steuert PGM1; einen weiteren Bereich fügen Sie mit der Schaltfläche Click to add an area hinzu, der Assistent lässt sich mit der Schaltfläche Skip beenden.

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.

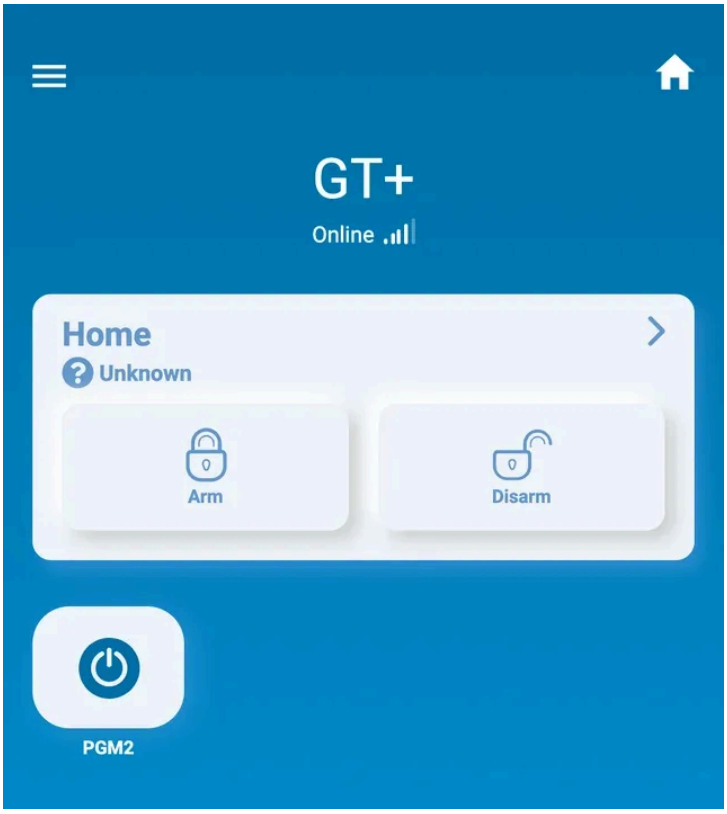


Abbildung 39. Protegus 2 – der Startbildschirm des Systems: der Zustand des Bereichs, die Schaltflächen Arm und Disarm, darunter der schaltbare PGM-Ausgang.

5.4 Steuerung mit SMS-Nachrichten

Der Kommunikator lässt sich auch mit SMS-Befehlen steuern. Aufbau der Nachricht: `Passwort Befehl Daten` (durch Leerzeichen getrennt). Als Passwort können Sie den **Administratorcode** (ab Werk `123456`) für die Befehle `INFO`, `RESET` und `OUTPUTx` verwenden, den **Errichtercode** (ab Werk `654321`) für die Befehle `INFO` und `OUTPUTx`.

Befehl	Daten	Was er tut	Beispiel
`INFO`	–	Fordert Informationen über das Gerät an. Die Antwort: Gerätetyp, IMEI-Nummer, Seriennummer und Firmwareversion.	`123456 INFO`
`RESET`	–	Startet das Gerät neu (nur mit dem Administratorcode).	`123456 RESET`
`OUTPUTx`	`ON`	Schaltet den Ausgang x ein (x = 1 oder 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Schaltet den Ausgang x aus.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Schaltet den Ausgang im Impulsmodus für die angegebene Zeit ein; `tttt` ist die Impulsdauer in Sekunden, vierstellig.	`123456 OUTPUT2 PULSE=0002`

Der Ausgang kann nur geschaltet werden, wenn die betreffende I/O-Klemme auf der Seite **IN/OUT** von TrikdisConfig auf Ausgang (**OUT**) gestellt ist. Von welchen Telefonnummern das Gerät Befehle annimmt, können Sie im Reiter **User reporting** → **Control by SMS** einschränken (Punkt 6.5).

6. TrikdisConfig – die Einstellungen im Detail

Im Fenster von TrikdisConfig sehen Sie links die Liste der Seiten (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, RS485 modules, Event summary, Firmware), oben die Schaltflächenleiste (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) und unten die Statusleiste. Dieses Kapitel geht die Einstellungen von GT und GT+ Seite für Seite durch; wo sich die beiden Varianten unterscheiden, weisen wir gesondert darauf hin.

6.1 Die Statusleiste

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.
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 40. Die Statusleiste von TrikdisConfig mit ausgelesenem GT+: Kennung, Zustand, Typ (Device: GT+_M150), Seriennummer, Versionen, Verbindungsart und Zugriffsebene.

Im Feld **Device** muss beim GT die Typbezeichnung GT stehen, beim GT+ die Typbezeichnung GT+ (im Bild GT+_M150; das Buchstaben-Zahlen-Suffix bezeichnet die Hardwareversion). Nach **Read [F4]** liest das Programm die im Gerät eingestellten Werte aus und zeigt sie an; nehmen Sie die nötigen Einstellungen nach den folgenden Seitenbeschreibungen vor.

6.2 System settings

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

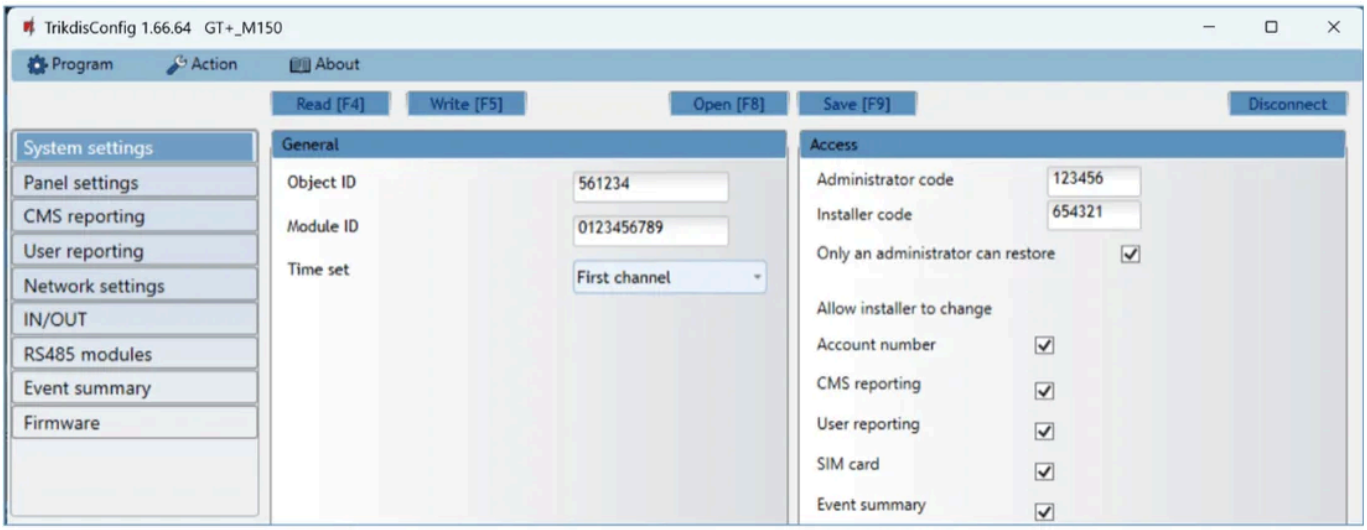


Abbildung 41. TrikdisConfig – Seite System settings: Gruppen General und Access.

- **Object ID** – die von der Leitstelle erhaltene Objektkennung (6 hexadezimale Zeichen: 0–9, A–F; `FFFE` und `FFFF` sind nicht zulässig). Pflicht, wenn das Gerät auch an eine Leitstelle meldet.
- **Module ID** – 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.

6.3 Panel settings

Auf dieser Seite geben Sie an, wie der Kommunikator mit der Alarmzentrale verbunden ist: Die Gruppe **TLC** enthält die Einstellungen für den Anschluss an die Telefonleitung (TIP/RING), die Gruppe **Serial bus** die für den Anschluss über Datenbus oder serielle Schnittstelle. Hier befinden sich auch die gemeinsamen Einstellungen zur Behandlung der Ereignisse der Zentrale.

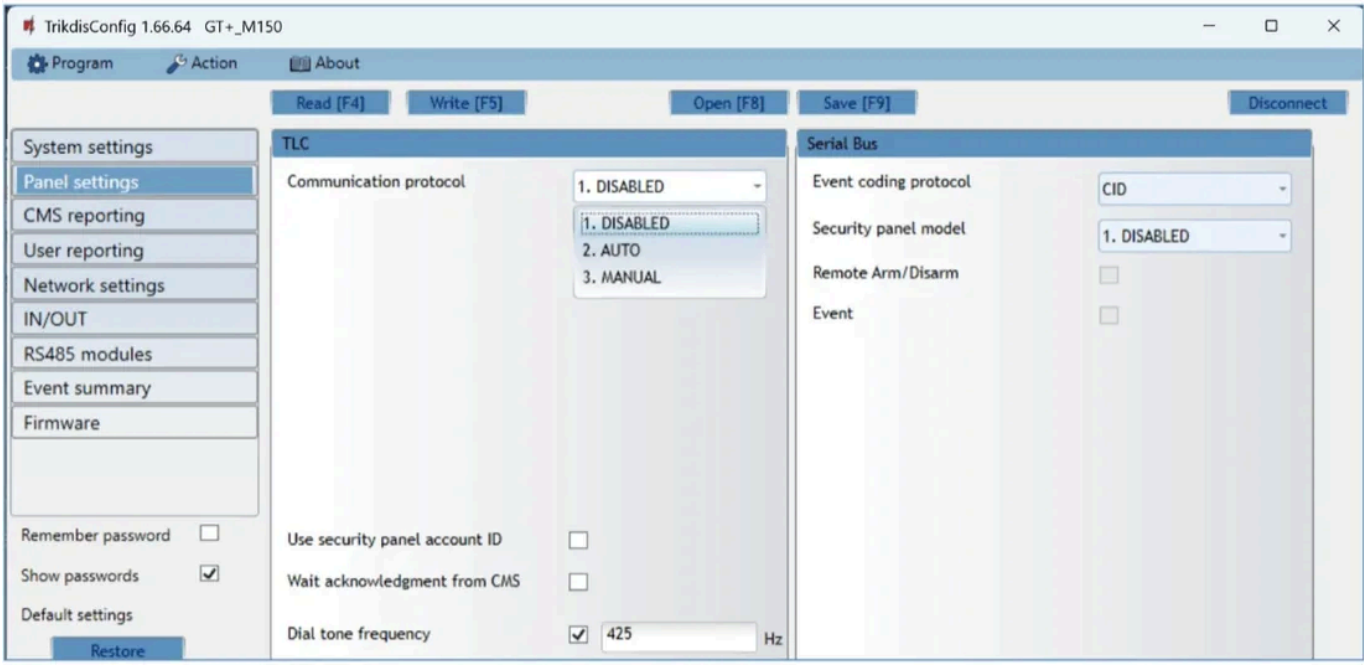


Abbildung 42. TrikdisConfig – Panel settings beim GT+: die Liste Communication protocol der Gruppe TLC (1. DISABLED, 2. AUTO, 3. MANUAL), darunter die Gruppe Serial bus und die gemeinsamen Einstellungen.

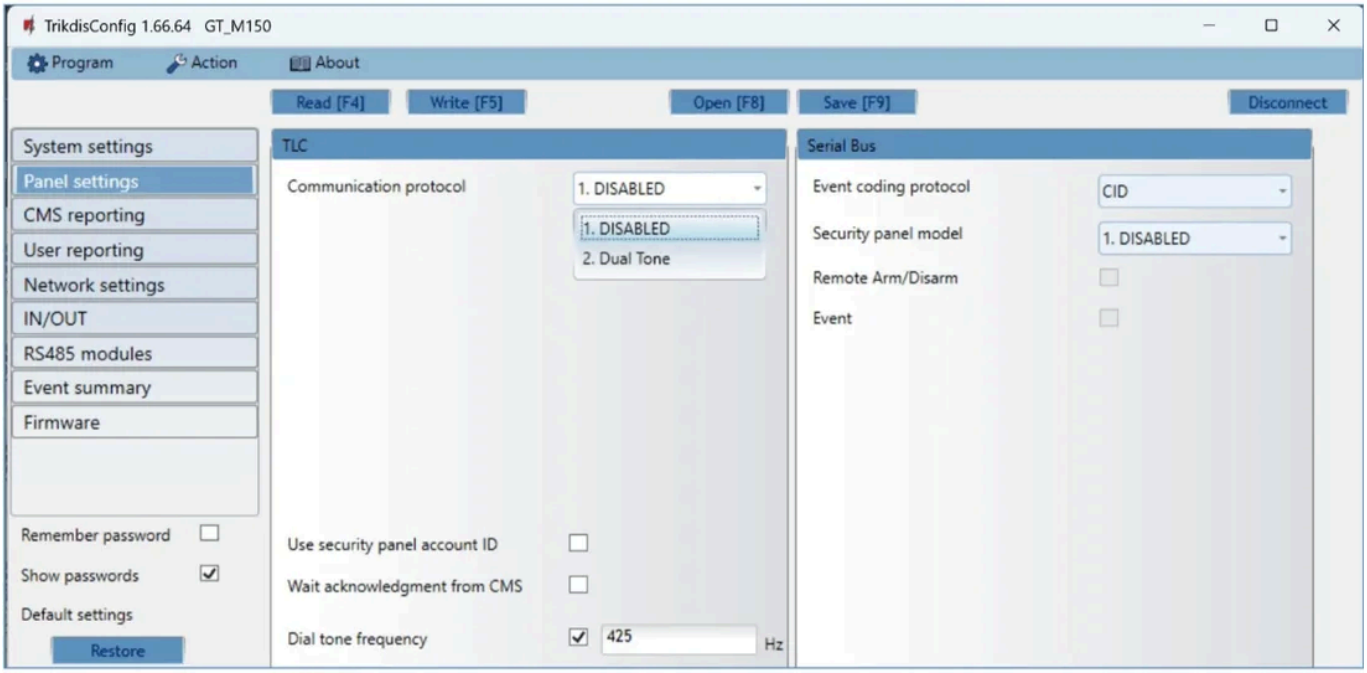


Abbildung 43. TrikdisConfig – Panel settings beim GT: Die Liste Communication protocol enthält hier 1. DISABLED und 2. Dual tone.

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

- **Communication protocol** – Einschalten bzw. Sperren der DTMF-Telefonleitungsschnittstelle des Kommunikators. GT+: **1. DISABLED** (ausgeschaltet), **2. AUTO**, **3. MANUAL**; GT: **1. DISABLED**, **2. Dual tone**. Wählen Sie beim Anschluss an TIP/RING den Wert AUTO (GT: Dual tone).

Die Einstellungen unter der Gruppe, die für beide Anschlussarten gelten:

- **Use security panel account ID** – angehakt verwendet der Kommunikator nicht seine eigene Object ID, sondern die in der Zentrale eingestellte und von der Zentrale gesendete Objektkennung.
- **Wait acknowledgment from CMS** – angehakt wartet der Kommunikator nach jedem Ereignis auf die Quittung des Empfängers (Kiss-off) und quittiert erst danach gegenüber der Zentrale; kommt die Quittung nicht rechtzeitig, sendet er die Nachricht erneut. Wenn das Gerät nicht an eine Leitstelle meldet, lassen Sie die Option ausgeschaltet.
- **Dial tone frequency** – die Frequenz des Wähltons, mit der der Kommunikator mit dem Wählgerät der Zentrale kommuniziert (Standard 425 Hz, der in den meisten europäischen Ländern übliche Wählton).



Abbildung 44. TrikdisConfig – Panel settings, Gruppe Serial bus: Event coding protocol CID, Security panel model (im Bild 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** – das Protokoll der Ereigniscodierung (CID).
- **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 das Element **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – angehakt 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 nach Kapitel 4 eingestellt werden.
- **Security panel PC download password** – für die direkte Steuerung von Paradox- und Texecom-Zentralen das PC- bzw. UDL-Passwort; es muss mit dem in der Zentrale eingestellten Passwort übereinstimmen, dessen Eingabe Kapitel 4 beschreibt.

6.4 CMS reporting

Der Kommunikator sendet die Ereignisse über die mobile Datenverbindung (IP) an die Leitstelle. Die Ereignisse können über mehrere Kanäle gehen: Der **Hauptkanal** und der **parallele** Kanal arbeiten gleichzeitig (an zwei Empfänger zugleich), und zu beiden gehört ein **Ersatzkanal**, der greift, wenn der betreffende Kanal ausfällt. Die Kommunikation ist verschlüsselt und passwortgeschützt; für den Empfang und die Weiterleitung der Ereignisse an die Leitstellensoftware ist ein Trikdis-Empfänger (Software-Empfänger IPcom – Windows oder

Linux –, IP/SMS-Empfänger RL14 oder Mehrkanal-Empfänger RM14) oder ein universeller Empfänger nötig, der das Protokoll DC-09 / TL150 beherrscht. GT und GT+ melden an die Leitstelle nur über einen IP-Kanal, einen SMS-Kanal haben sie nicht.

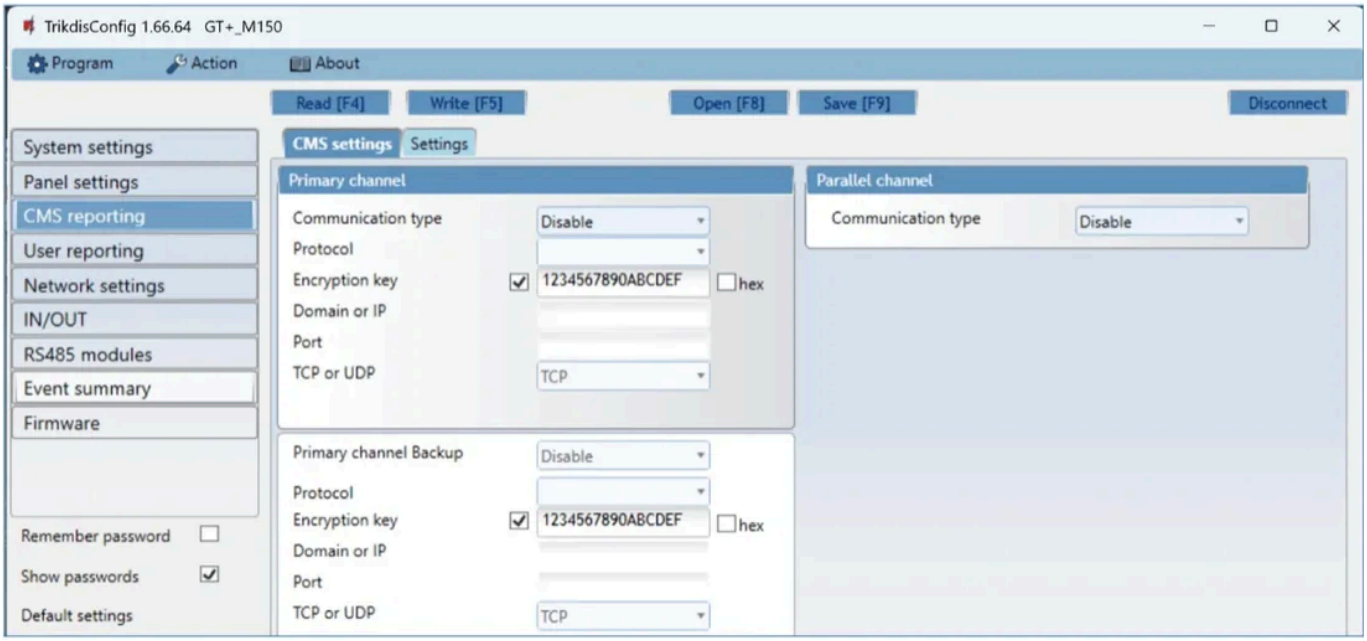


Abbildung 45. TrikdisConfig – CMS reporting, Reiter CMS settings: Haupt-, Ersatz- und paralleler Kanal.

Primary channel – Hauptkanal

- **Communication type** – die Verbindungsart mit dem Empfänger: **IP**.
- **Protocol** – **TRK8** (Trikdis-Empfänger), **DC-09_2007** oder **DC-09_2012** (universelle Empfänger), **TL150** (SUR-GARD-Empfänger).
- **Encryption key** – der Verschlüsselungsschlüssel der Nachrichten; im Kommunikator und im Empfänger muss derselbe stehen.
- **Domain or IP**, **Port** – Domainname oder IP-Adresse und Port des Empfängers.
- **TCP or UDP** – das Übertragungsprotokoll.

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

Primary channel Backup – Ersatzkanal. Er übernimmt die Kommunikation, wenn der Hauptkanal nicht funktioniert; seine Einstellungen stimmen mit den obigen überein.

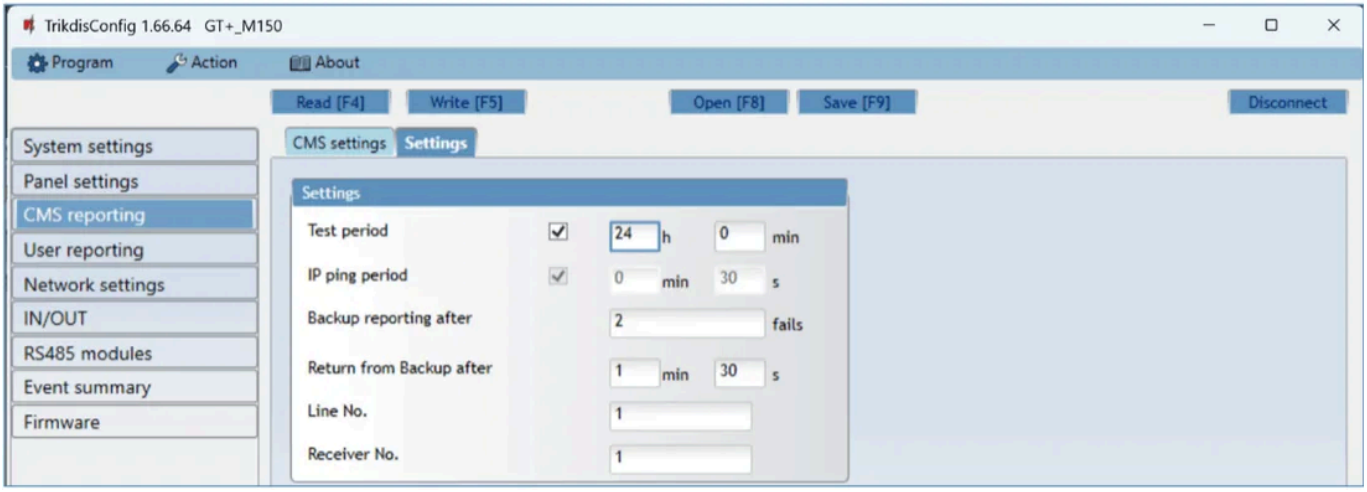


Abbildung 46. TrikdisConfig – CMS reporting, Reiter Settings: Testmeldung, PING, die Zeiten des Ersatzkanals und die DC-09-Daten.

Im Reiter **Settings** stellen Sie die Zeiten und die DC-09-Daten ein.

- **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.

Im Reiter Settings von GT und GT+ stehen in der Gruppe DC-09 die Felder **Line No.** (Liniennummer) und **Receiver No.** (Empfängernummer); die Gruppe erscheint, wenn im Feld **Protocol** eines Kanals DC-09_2007 oder DC-09_2012 ausgewählt ist.

6.5 User reporting

Im Reiter **PROTEGUS Cloud** aktivieren Sie den Protegus-Dienst, mit dem der Benutzer den Kommunikator und das daran angeschlossene System aus der Ferne überwacht und steuert; Einzelheiten: www.protegus.app.

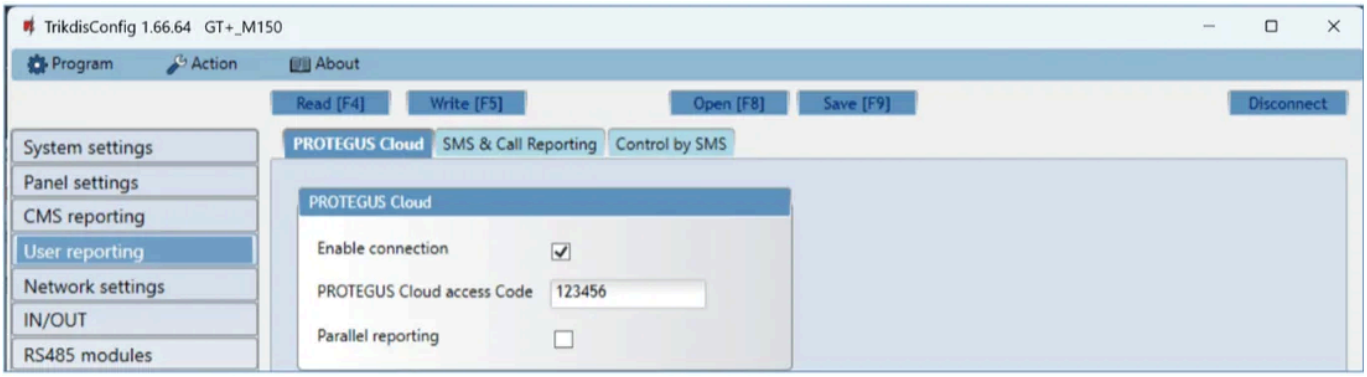


Abbildung 47. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- **Enable connection** – aktiviert den Protegus-Dienst: Das Gerät tauscht Daten mit der App Protegus 2 aus, und TrikdisConfig erreicht es auch aus der Ferne.
- **PROTEGUS Cloud access Code** – 6-stelliger Code für die Verbindung mit Protegus 2 (ab Werk `123456`). Wenn Sie ihn in TrikdisConfig ändern, muss er auch in der App Protegus 2 geändert werden.
- **Parallel reporting** – angehakt gehen die Nachrichten gleichzeitig über den Hauptkanal (an die Leitstelle) und an Protegus 2.

Im Reiter **SMS & Call Reporting** kann der Benutzer auch per SMS oder Telefonanruf über die Ereignisse benachrichtigt werden.

Bei einem Alarm sendet das Gerät zuerst die SMS an alle eingetragenen Telefonnummern und ruft die Nummern dann nacheinander von Tel 1 bis Tel 4 an. Jede Nummer wird einmal angerufen und klingelt 20 Sekunden lang; ein Anruf gilt als erfolgreich, wenn die Nummer klingelt (Annehmen oder Abweisen genügt ebenfalls). Das Modem baut den Anruf über 2G oder VoLTE auf. Wo der Netzbetreiber 2G abgeschaltet und das Modem nicht für VoLTE freigegeben hat, kommt die SMS an, das Telefon klingelt aber nicht. Das ist kein Konfigurationsfehler. Verwenden Sie dort SMS und die Protegus-2-App.

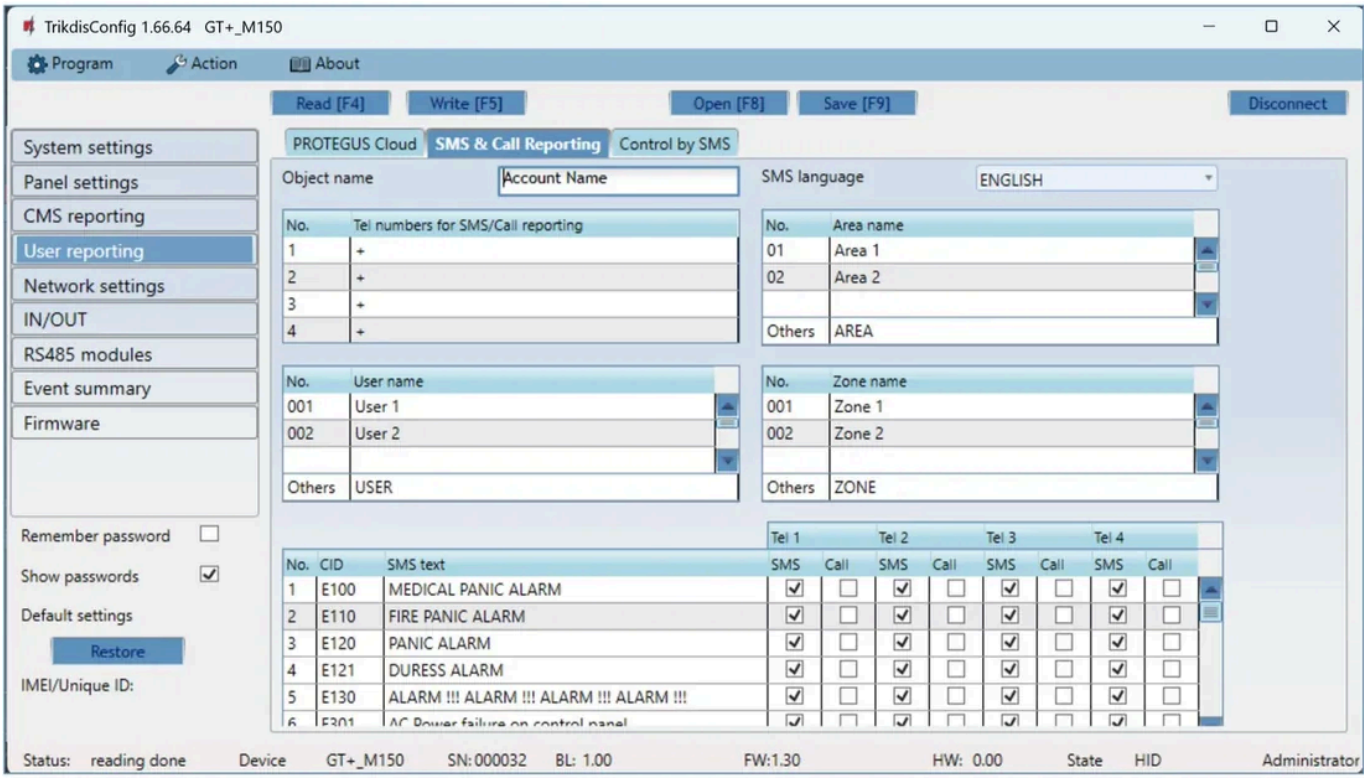


Abbildung 48. TrikdisConfig – User reporting, Reiter SMS & Call Reporting.

- **Object name** – der Name des Systems; er steht in jeder SMS.
- **SMS language** – die Sprache der SMS (die Nachrichten können auch mit den eigenen Zeichen der Sprache gesendet werden).
- **Tel numbers for SMS/Call reporting** – bis zu 4 Telefonnummern, die über die Ereignisse eine SMS oder einen Anruf erhalten; geben Sie sie mit Ländervorwahl ein (z. B. `+43…`, `0043…` oder `43…`).
- **Area name, User name, Zone name** – die Namen der Bereiche, Benutzer und Zonen; diese verwendet das Gerät im Text der SMS. Tragen Sie in die passende Tabelle die Nummer des Bereichs, des Benutzers oder der Zone ein und daneben den Namen.
- **CID event table** – pro Ereignis einstellbar, welche Nummer eine SMS oder einen Anruf erhält. SMS-Text und Contact-ID-Code der Standardereignisse sind änderbar, und es kann auch ein neues Ereignis mit Beschreibung hinzugefügt werden.

Im Reiter **Control by SMS** stellen Sie den Empfang von SMS-Befehlen ein: Mit den Befehlen lassen sich die Ausgänge schalten und Informationen über das Gerät abfragen (die Befehle beschreibt Punkt 5.4).

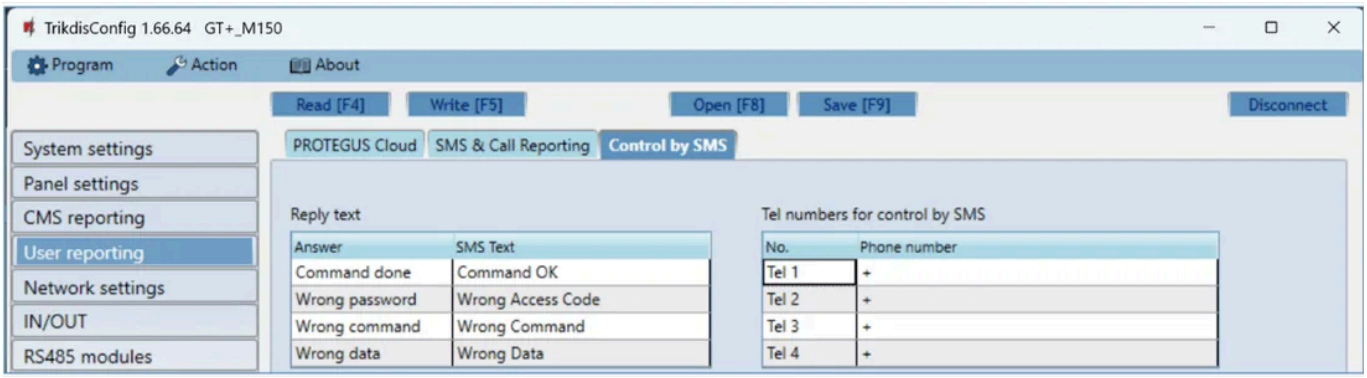


Abbildung 49. TrikdisConfig – User reporting, Reiter Control by SMS.

- **Reply text** – der Text der Antwortnachrichten auf einen SMS-Befehl: erfolgreicher Befehl (Command done), falsches Passwort (Wrong password), falscher Befehl (Wrong command), falsche Daten (Wrong data). Die Texte sind bearbeitbar.
- **Tel numbers for control by SMS** – die Telefonnummern, von denen das Gerät Befehle annimmt.

Ist hier keine Telefonnummer angegeben, nimmt das Gerät Befehle von jeder Nummer an. Die Sicherheit ergibt sich dann daraus, dass im Befehl das Administrator- oder Errichterpasswort Pflicht ist.

6.6 Network settings

Vergewissern Sie sich vor der Nutzung, dass die SIM-Karte aktiv ist und funktioniert. Wenn Sie die Ereignisse über einen IP-Kanal oder über das mobile Internet an Protegus 2 senden, muss auf der Karte auch der mobile Datendienst freigeschaltet sein.

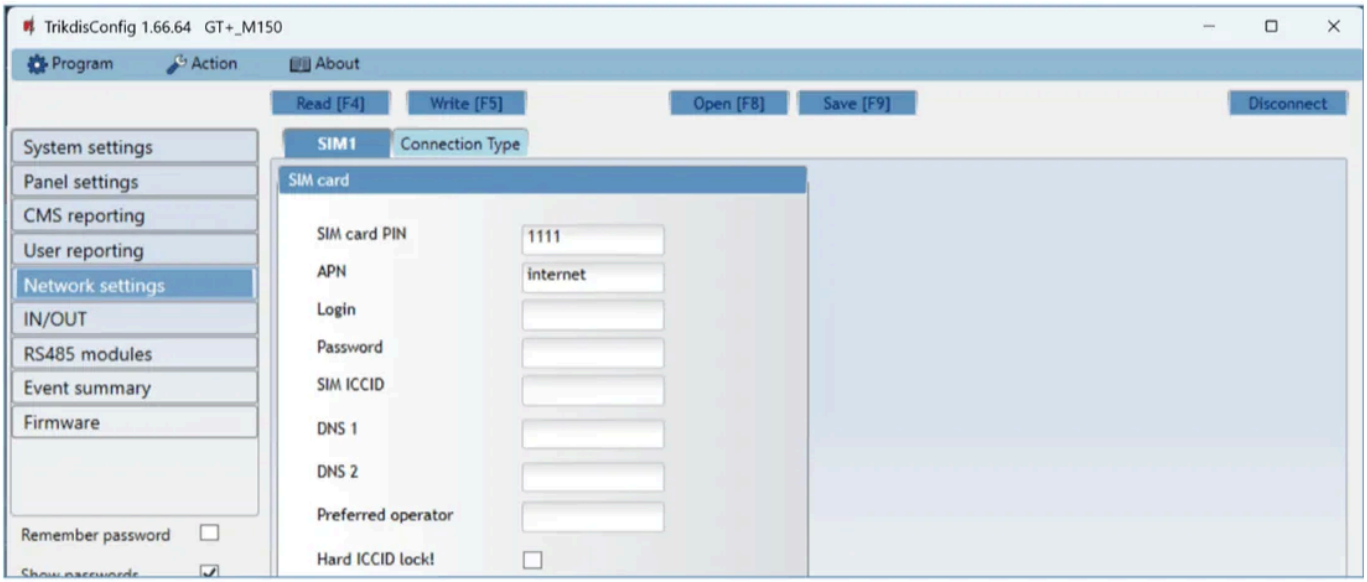


Abbildung 50. TrikdisConfig – Network settings, Reiter SIM1: die Daten der SIM-Karte.

Reiter SIM1, Gruppe SIM card

- **SIM card PIN** – der PIN-Code der Karte. Die PIN-Abfrage schalten Sie ab, indem Sie die Karte in ein Mobiltelefon einsetzen und sie dort deaktivieren; dann kann der Werkswert des Felds 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 Punkt 2.2).
- **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 funktionieren soll. Stimmt die ICCID der eingesetzten Karte nicht überein, blinkt die LED TROUBLE 8-mal (Punkt 1.6).
- **DNS 1, DNS 2** – Nameserver (DNS, Domain Name System: liefert die zum Domainnamen gehörende IP-Adresse); sie werden benötigt, wenn Sie den Empfänger im Feld **Domain or IP** 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 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.
- **Hard ICCID lock** – angehakt und nach einem Neustart des Geräts ist der Kommunikator strikt an die SIM-Karte mit der angegebenen ICCID-Nummer gebunden.

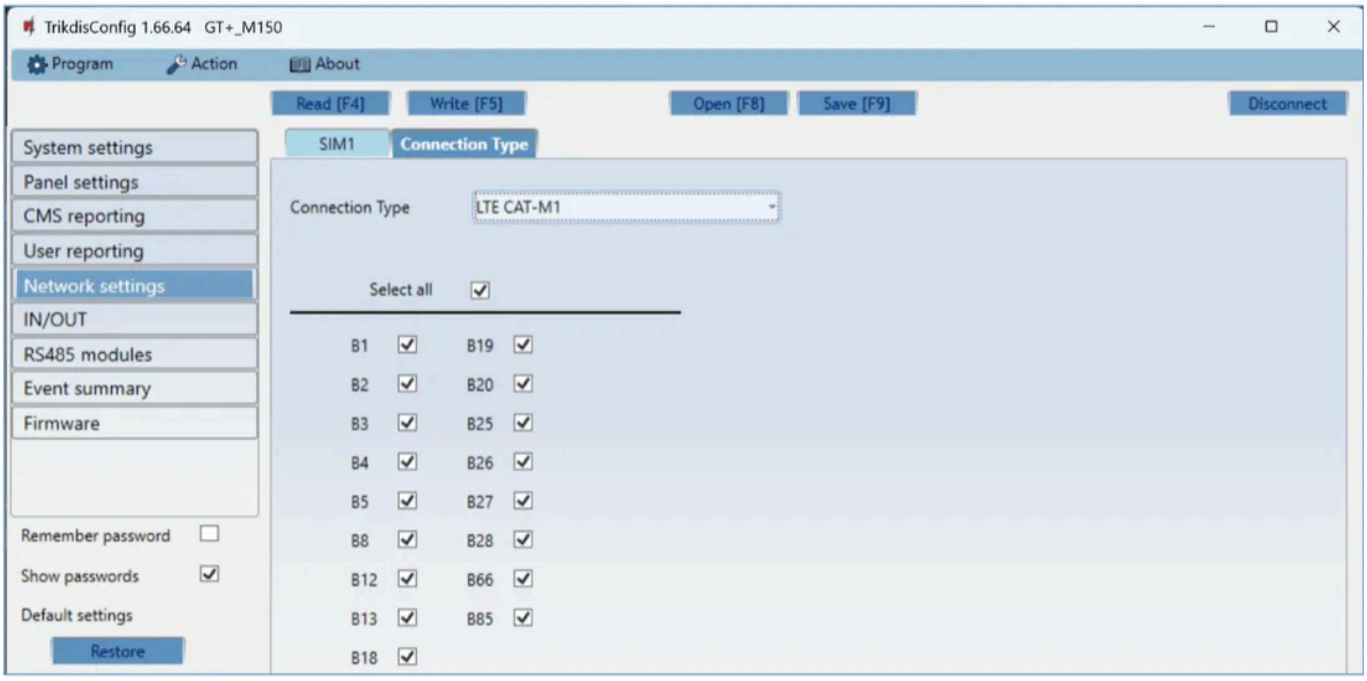


Abbildung 51. TrikdisConfig – Network settings, Reiter Connection Type: Auswahl der LTE-Bänder bei der Variante mit CAT-M1-Modem.

Reiter Connection Type – gilt nur für die Variante mit CAT-M1-Modem (BG95-M5): Hier können Sie angeben, auf welchen LTE-Frequenzbändern das Modem des Geräts arbeiten soll (**Select all** = alle).

6.7 IN/OUT

Hier legen Sie die Rolle der zwei I/O-Klemmen mit Doppelfunktion des Kommunikators fest: **Off** (nicht verwendet), **IN** (Eingang) oder **OUT** (Ausgang). Bei einem Eingang muss im Feld **Type** auch der Typ des angeschlossenen Kreises angegeben werden (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

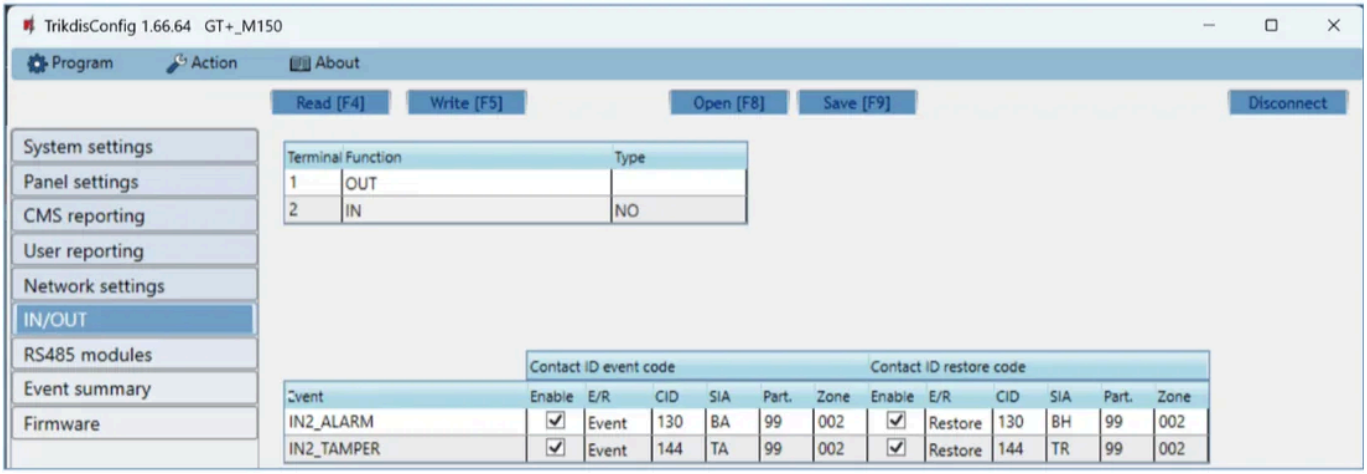


Abbildung 52. TrikdisConfig – Seite IN/OUT: Klemme 1 Ausgang (OUT), Klemme 2 Eingang (IN, NO); darunter die Alarm- und Sabotageereignisse von Eingang 2 mit CID- und SIA-Code.

Bei Auslösung des am Eingang angeschlossenen Melders sendet der Kommunikator ein eigenes Ereignis (**INx_ALARM**, Contact ID 130, SIA BA; Wiederherstellung BH), bei Verletzung des Sabotagekreises ein Sabotageereignis (**INx_TAMPER**, 144, SIA TA; Wiederherstellung TR) an die Leitstelle und an Protegus 2; in der Tabelle erscheinen die Ereignisse jeder als Eingang eingestellten Klemme. Die Spalten der Tabelle:

- **Enable** – aktiviert das Senden der Nachricht an die Leitstelle und an Protegus 2.
- **E/R** – der Typ der Nachricht: Event (Ereignis) oder Restore (Wiederherstellung).

- **CID** – der Contact-ID-Code (änderbar, oder er kann der Werkscode bleiben).
- **SIA** – der SIA-Code (änderbar, oder er kann der Werkscode bleiben).
- **Part.** – die Nummer des Bereichs in der Nachricht.
- **Zone** – die Nummer der Zone in der Nachricht.

6.8 RS485 modules

Mit den am RS485-Bus angeschlossenen Erweiterungsmodulen **iO-8** lassen sich dem Kommunikator weitere Eingänge und Ausgänge hinzufügen. Die angeschlossenen Erweiterungsmodule müssen im Reiter **Modules list** hinzugefügt werden.

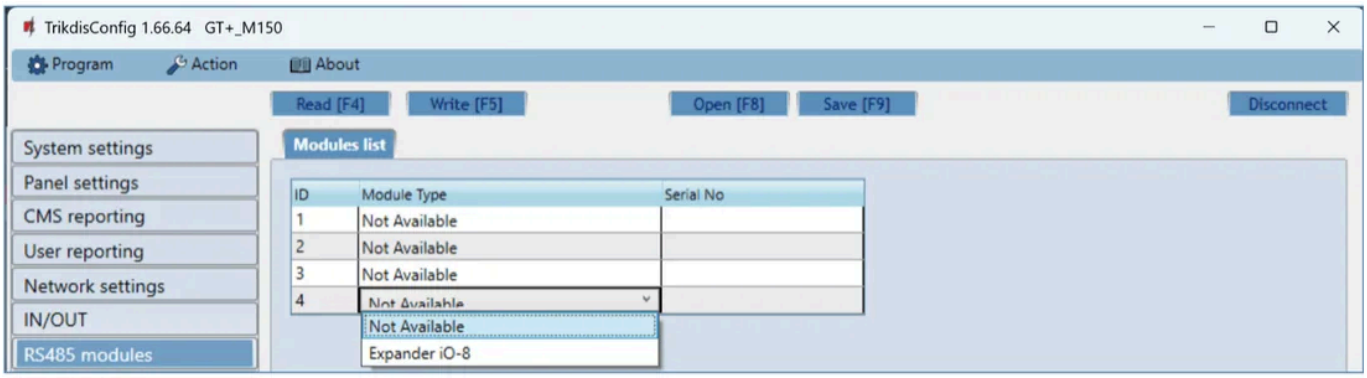


Abbildung 53. TrikdisConfig – RS485 modules, Reiter Modules list: an Stelle 4 die Liste Module type (Not Available, Expander iO-8).

- **Module type** – der Typ des am Bus angeschlossenen Moduls aus der Liste (**Expander iO-8**).
- **Serial No** – die 6-stellige Seriennummer des Moduls (auf dem Gehäuse des Moduls und auf dem Aufkleber der Verpackung).

Wechseln Sie nach der Auswahl des Moduls und der Eingabe der Seriennummer in den Reiter **RS485 modules** → **Module**: Für das hinzugefügte Modul erscheint ein eigener, nummerierter Reiter (Module 1 …) mit seinen Einstellungen.

Erweiterungsmodul iO-8 – 8 I/O-Klemmen mit Doppelfunktion; an den Kommunikator können bis zu vier iO-8 angeschlossen werden.

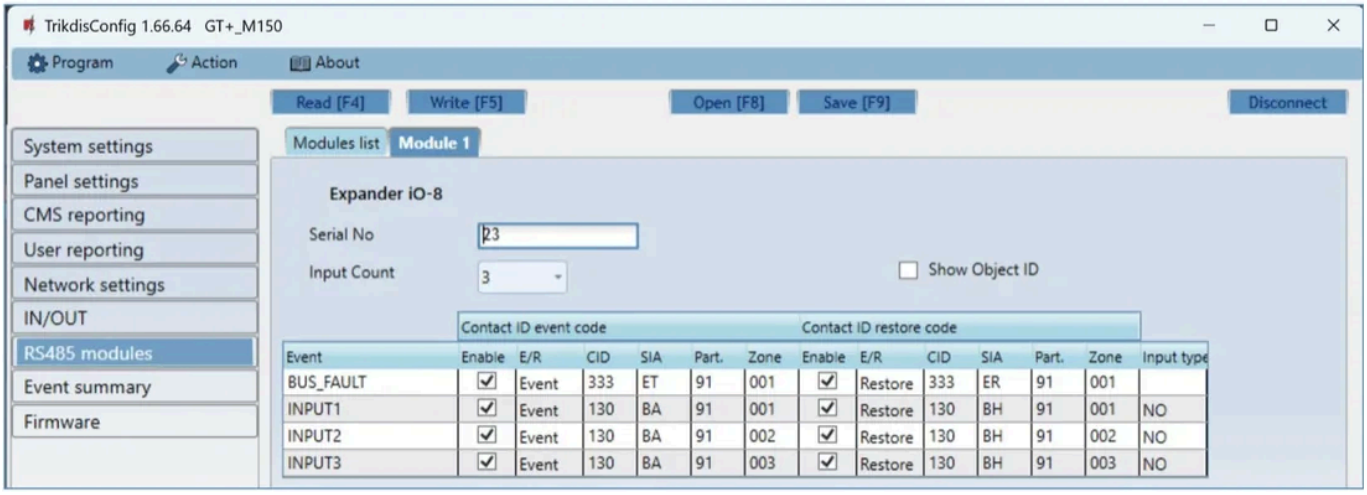


Abbildung 54. TrikdisConfig – RS485 modules, Reiter Module 1 (iO-8): Input Count, Show Object ID und die Ereignisse BUS_FAULT, INPUT1–INPUT3 mit CID- und SIA-Code, mit Bereich 91.

- **Input Count** – wie viele Klemmen Eingang (IN) sein sollen; die übrigen werden Ausgang (OUT). Die Rolle der Ausgänge (Scharf- / Unscharfschalten oder Schalten eines Geräts) stellen Sie direkt in der App Protegus 2 ein.
- In der Tabelle können Sie dem Busfehler (**BUS_FAULT**, Contact ID 333) und den Eingängen (**INPUTx**, 130) einen Ereignis- und Wiederherstellungscode zuordnen; bei Auslösung des Eingangs sendet der Kommunikator mit dem eingestellten Code ein Ereignis an den Empfänger der Leitstelle und an Protegus 2. Die Spalten der Zeilen für Ereignis (Contact ID event code) und Wiederherstellung (Contact ID restore code): **Enable** (Aktivierung), **E/R** (Event oder Restore), **CID** (Contact-ID-Code), **SIA** (SIA-Code), **Part.** (der Bereich – hängt automatisch von der Nummer des Moduls ab: beim Modul 1 ist es 91, beim Modul 4 ist es 94), **Zone** (die Nummer der Zone).
- **Object ID** – für den Eingang kann auch eine von der des Kommunikators abweichende Objektkennung angegeben werden (die Spalte erscheint durch Anhaken von **Show Object ID**).
- **Input type** – der Typ des Eingangs: NO, NC oder EOL.

6.9 Event summary

Auf dieser Seite können Sie die **eigenen, internen Meldungen** des Geräts ein- oder ausschalten und ihren Contact-ID-Code sowie ihre Bereichs- und Zonennummer ändern. Eine hier deaktivierte Meldung sendet das Gerät über keinen Kanal. Werkseitig werden die Meldungen mit Bereich 99 und Zone 999 gesendet.

Meldung	Contact ID	Wann sie entsteht
COMMUNICATION	350	Die Kommunikation zwischen Kommunikator und Alarmzentrale ist unterbrochen (werkseitig deaktiviert). Ein am Bus oder an der seriellen Schnittstelle angeschlossener Kommunikator erkennt dies direkt; ein Telefonleitungs-Kommunikator nur bei aktivierter **Line supervision**.
POWER	302	Unzureichende (niedrige) Versorgungsspannung; ihre Wiederherstellung ist eine eigene Meldung.
REMOTE_STARTED	411	Die Fernprogrammierung mit TrikdisConfig hat begonnen.
REMOTE_FINISHED	412	Die Fernprogrammierung ist beendet.
START	700	Das Gerät hat sich mit dem Netzwerk verbunden (Start).
TEST	602	Periodischer Testbericht.
PING	760	Die PING-Lebenszeichenmeldung. Sie steht nicht in der Liste jedes Geräts: Auf dem Bildschirm der früheren Hardwareversion ja, auf der Seite Event summary der neueren Versionen gibt es keine solche Zeile. Ihr Intervall stellen Sie im Feld **CMS reporting → Settings → IP ping period** ein.

- **Enable** – erlaubt das Senden der Meldung an die Leitstelle und an Protegus 2.
- **E/R** – der Typ der Meldung: Event (Ereignis) oder Restore (Wiederherstellung) – die jeweilige Zeile steht für das Eintreten des Ereignisses oder für dessen Wiederherstellung.
- **Part.** – die Nummer des Bereichs, die das Gerät beim internen Ereignis und bei der Wiederherstellung sendet.
- **Zone** – die Nummer der Zone, die das Gerät beim internen Ereignis und bei der Wiederherstellung sendet.
- Der **CID**-Code, der **Bereich** und die **Zone** können bei jedem Ereignis geändert werden; wo es eine Wiederherstellung (Restore) gibt, kann deren Code separat angegeben werden.

Die Ereignisse der eigenen Eingänge (**INx_ALARM**, **INx_TAMPER**) werden auf der Seite **IN/OUT** eingestellt, die Ereignisse der Erweiterungsmodule (**BUS_FAULT**, **INPUTx**) auf der Seite **RS485 modules** auf der Registerkarte des Moduls. Aktivierung und Intervall des Testberichts stellen Sie im Feld **CMS reporting** → **Settings** → **Test period** ein.

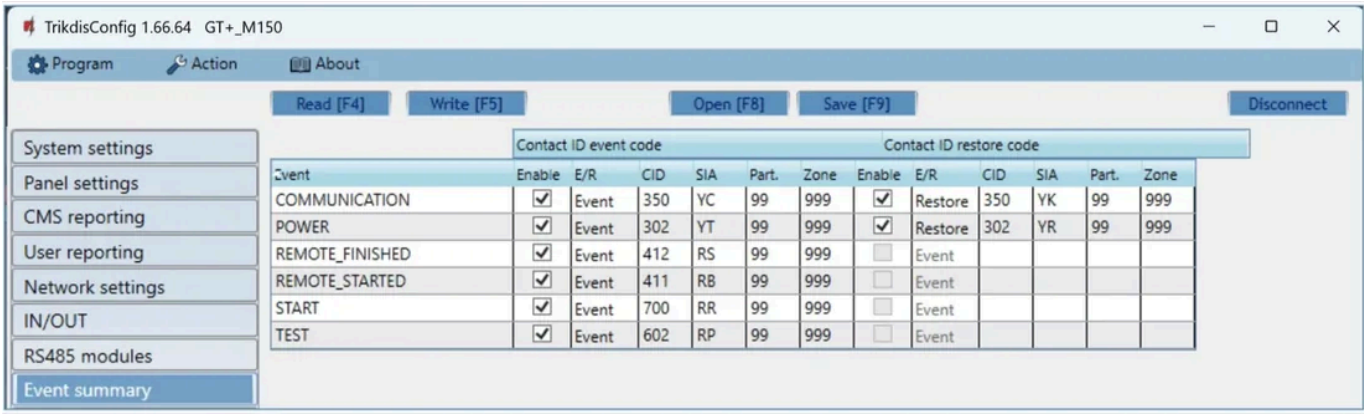


Abbildung 55. TrikdisConfig – Seite Event summary: die internen Nachrichten des Geräts mit CID- und SIA-Code (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

In der Liste von GT und GT+ stehen die Nachrichten **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** und **TEST**, jeweils auch mit dem SIA-Code. Die Nachricht COMMUNICATION meldet einen Fehler der Verbindung zwischen Zentrale und Kommunikator: Beim Anschluss über Datenbus oder serielle Schnittstelle erkennt der Kommunikator diesen direkt (die LED TROUBLE blinkt 7-mal).

6.10 Werkseinstellungen wiederherstellen

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 56. 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 (Punkt 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.

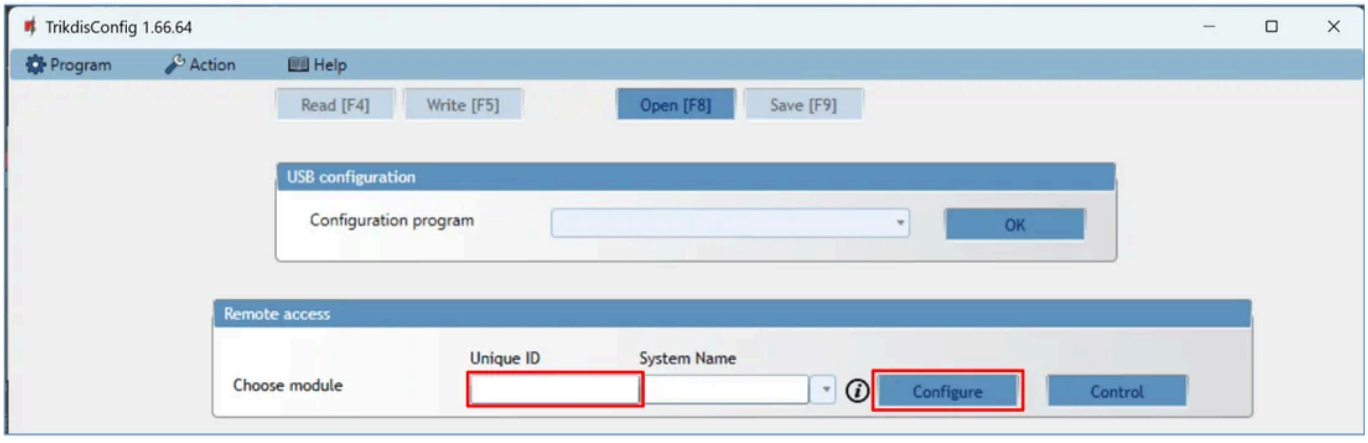


Abbildung 57. TrikdisConfig – die Gruppe Remote access: das Feld Unique ID, die Liste System name und die Schaltfläche Configure.

Die eindeutige Kennung von GT und GT+ ist die **IMEI**; sie steht auf dem Etikett des Geräts und auf dem Aufkleber der Verpackung. Für den Fernzugriff muss die SIM-Karte aktiv sein, ihr PIN-Code eingetragen oder die PIN-Abfrage abgeschaltet; auf der Seite **User reporting** → **PROTEGUS Cloud** muss **Enable connection** angehakt sein (Punkt 6.5); die LED **POWER** muss grün leuchten, die LED **NETWORK** grün leuchten und gelb blinken.

8. Prüfung der Funktion 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.

6. **DSC-Zentrale mit Anschluss Keybus + TIP/RING (GT+).** Schärfen Sie das System und lösen Sie einen Alarm einer Feuerzone aus. Die Leitstelle muss das Ereignis mit dem zum Zonentyp passenden Contact-ID-Code erhalten (zum Beispiel E110 – Feueralarm), nicht als allgemeinen Alarm (E130).

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.

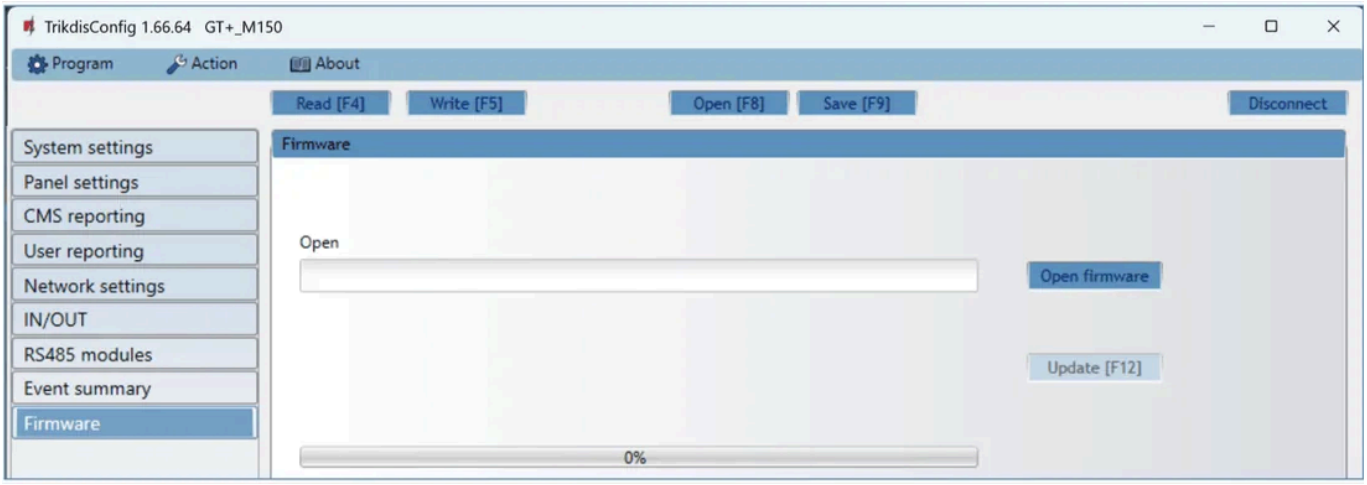


Abbildung 58. TrikdisConfig – Seite Firmware: Schaltfläche Open firmware, Schaltfläche Update [F12] und die Fortschrittsanzeige.

Für die Aktualisierung ist eine Internetverbindung nötig. Virenschutz, Firewall oder strenge Einstellungen für den Internetzugang können die automatische Firmware-Aktualisierung verhindern; dann müssen die Einstellungen des Virenschutzes geändert werden. Für den Anschluss Keybus + TIP/RING der Paradox SP / SP+ / MG / MG+ (Punkt 3.3.4) ist mindestens die Firmware 1.21 nötig.

10. Fehlersuche und häufige Fragen

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

Die LED NETWORK leuchtet nicht – kein Netz

1. Sehen Sie sich die Blinkimpulse der LED **TROUBLE** an: 1 = keine SIM, 2 = falsche PIN, 3 = kein APN, 4 = Anmeldung im Mobilfunknetz nicht möglich, 5 = Anmeldung im Datennetz nicht möglich (Punkt 1.6).
2. Prüfen Sie, ob die SIM-Karte aktiv ist, einen Datendienst hat und richtig im Halter sitzt.
3. Wenn die PIN-Abfrage auf der Karte eingeschaltet ist, geben Sie die PIN im Reiter **Network settings** → **SIM1** ein, oder schalten Sie die PIN-Abfrage in einem Telefon ab.
4. Prüfen Sie den APN (Punkt 2.2): Bei einer IoT- / M2M-Karte gibt der Anbieter einen eigenen APN an.
5. Prüfen Sie die Antenne: Sie ist angeschraubt, nicht in einem Metallgehäuse, und die Signalstärke ist ausreichend (die LED NETWORK blinkt mindestens 3-mal gelb; Punkte 1.6 und 3.2).

Es gibt 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. 6 Blinkimpulse der LED **TROUBLE** zeigen, dass keine Verbindung zum Empfänger besteht: Prüfen Sie Adresse und Port des Empfängers, die Einstellung TCP/UDP, das Protokoll und den Verschlüsselungsschlüssel (**CMS reporting**).
2. Wenn der Empfänger mit einem Domainnamen angegeben ist, prüfen Sie die DNS-Einstellung (**Network settings** → **SIM1** → **DNS 1, DNS 2**).
3. Prüfen Sie, ob das Datenpaket der SIM-Karte den nötigen Port nicht sperrt (manche M2M-Karten lassen nur bestimmte Adressen zu).

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

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

Die LED TROUBLE blinkt 8-mal – ICCID-Abweichung

Die im Feld **Network settings** → **SIM1** → **SIM ICCID** angegebene Nummer stimmt nicht mit der ICCID der eingesetzten SIM-Karte überein: Das Gerät funktioniert nur mit der angegebenen Karte. Setzen Sie die ursprüngliche Karte wieder ein, oder ändern (löschen) Sie die ICCID; bei **Hard ICCID lock** starten Sie das Gerät nach der Änderung neu (Punkt 6.6).

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, daher meldet er jeden Alarm mit dem Code E130 (Punkt 3.3.1). Wenn die Leitstelle den zum Zonentyp passenden Code erwartet (zum Beispiel Feuer: E110): Schließen Sie den **GT+** neben dem Keybus auch an die Klemmen TIP/RING an und programmieren Sie das Wählgerät der Zentrale (Punkte 3.3.2 und 4.1.1). Beim GT gibt es diesen doppelten Anschluss nicht; dort gehen die eigenen Codes der Zentrale über das Wählgerät der Zentrale nur beim reinen Anschluss an TIP/RING, dann gibt es aber keine direkte Steuerung, und zum Scharfschalten ist eine Schlüsselschalter-Zone nötig (Punkt 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 ab Werk gesperrt sein; zur Freischaltung siehe Punkt 4.1.2 und den 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 (Punkt 3.3.4), für den keine Freischaltung nötig ist, die Firmware des Kommunikators muss aber 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 nach Punkt 4.1 eingestellt sein (Paradox: PC-Passwort, Firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: die beschriebenen Einstellungen). Sehen Sie in der Tabelle in Punkt 1.3 nach, ob die Zentrale überhaupt direkt steuerbar ist.

2. Beim Scharfschalten mit Schlüsselschalter (Punkt 3.4) muss die Klemme auf der Seite **IN/OUT** auf **OUT** stehen, die Zone der Zentrale muss eine Schlüsselschalter-Zone sein, und in Protegus 2 muss dem Bereich der Ausgang zugeordnet sein, im gleichen Modus wie in der Zentrale (impulsgesteuert oder bistabil; Punkt 5.2).
3. Protegus 2 zeigt den Zustand des Bereichs anhand der Scharf- und Unscharfschalt-Ereignisse 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.
2. Beim Hinzufügen muss der im Gerät eingestellte **PROTEGUS Cloud access Code** eingegeben werden; wenn Sie den Code in TrikdisConfig geändert haben, ändern Sie ihn auch in der App.
3. Geben Sie die IMEI genau ein, vom Etikett des Geräts oder vom Aufkleber der Verpackung (oder lesen Sie den QR-Code ein).
4. Datendienst der SIM-Karte und APN müssen in Ordnung sein (die LED NETWORK ist grün, und die LED DATA erlischt nach einem Ereignis).

Ich kann mich mit TrikdisConfig nicht aus der Ferne verbinden

1. Das Gerät muss online sein (LED NETWORK grün, blinkt gelb), 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.

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 6.10): bei eingeschalteter Versorgung 10 Sekunden gedrückt halten. Alle Einstellungen werden gelöscht.

GT oder GT+ – welcher wird gebraucht?

Anschluss, Einstellung und Funktion der beiden Varianten sind gleich; die Unterschiede fasst die Tabelle in Punkt 1.2 zusammen. Der GT+ arbeitet auch mit einer Versorgung von 10–32 V DC (auch in 24-V-Systemen) und beherrscht an DSC-Zentralen auch den Anschluss Keybus + TIP/RING, sodass die Ereignisse mit den eigenen Contact-ID-Codes der Zentrale gehen. Wenn Sie das nicht brauchen, kann der GT dasselbe.

Wie viel Datenverkehr verbraucht das Gerät?

Die Ereignisnachrichten und PINGs sind sehr klein; der Verkehr hängt überwiegend von der PING-Periode und der Häufigkeit der Testmeldungen ab. Bei einem durchschnittlichen Haushaltssystem bleibt der monatliche Verkehr typischerweise unter 10 MB. Der genaue Wert hängt von den Einstellungen und der Abrechnungseinheit des Anbieters ab, daher lohnt es sich bei einer Karte mit Datenlimit, den Verkehr des ersten Monats zu prüfen.

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 Anschluss 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 getrennt als Elektronikschrott abzugeben ist.

Siehe auch

- Kompatibilitätssuche – welcher Trikdis-Kommunikator und welcher Anschluss zu Ihrer Alarmzentrale passt.
- Trikdis-Kommunikator + DSC-Alarmzentrale: kurze Errichteranleitung – die Schritte des DSC-Anschlusses in Kürze.
- Trikdis-Kommunikator + Paradox-Alarmzentrale: kurze Errichteranleitung – 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+.
- Fern-Scharfschaltung mit Schlüsselschalter aus der App Protegus 2 – Einzelheiten und Fallstricke des Scharfschaltens mit Schlüsselschalter.
- APN-Einstellung – Liste europäischer Mobilfunkanbieter – die APNs der Anbieter, auch für IoT- / M2M-Karten.
- Englischsprachige Dokumentation: docs.trikdis.com – auf der Seite von GT und GT+ steht auch die Umwandlungstabelle der Codes Contact ID → SIA (Anhang).

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

Passende Produkte

Trikdis GT 4G Kommunikationsmodul **Trikdis GT+ 4G Kommunikationsmodul**

Trikdis IO8 Wired Expander Modul

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/gt-anleitung