Kommunikator G16 – Errichter- und Benutzeranleitung

Errichter- und Benutzeranleitung für den Trikdis-Kommunikator G16: Anschluss an den Datenbus oder die serielle Schnittstelle der Alarmzentrale, Programmierung der Zentrale, SIM und Einrichtung in TrikdisConfig, Übertragung an die Leitstelle, die App Protegus 2.



Ausgabe: 2026-11-17
Immer aktuelle Webversion: https://trikdis.at/g16-anleitung

Inhalt

1. Überblick

1.1 Wofür er gedacht ist und wie er funktioniert
1.2 Kompatible Alarmzentralen
1.3 Varianten
1.4 Hauptmerkmale
1.5 Bestandteile des Kommunikators
1.6 Klemmen
1.7 LED-Anzeigen
1.8 Technische Daten

2. Schnelle Inbetriebnahme mit TrikdisConfig

2.1 Vorbereitung
2.2 Typ der Zentrale und direkte Steuerung
2.3 Verbindung zur App Protegus 2
2.4 Verbindung zur Leitstelle

3. Installation und Anschluss

3.1 Installationsschritte
3.2 Montageort und Antenne
3.3 Anschluss an die Alarmzentrale
3.3.1 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception und Integriti
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 Anschluss der Module W485 und E485
3.9 Einschalten und erste Prüfung
A TRIKDIS átjelző elindítása

4. Programmierung der Alarmzentrale

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

5. Fernsteuerung mit der App Protegus 2

5.1 Gerät hinzufügen
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Direkte Steuerung mit dem Bedienteilcode
5.3 Scharfschalten über eine Schlüsselschalter-Zone
5.4 Scharf- und Unscharfschalten in der App
5.5 Steuerung per SMS

6. TrikdisConfig – die Einstellungen im Detail

6.1 Die Statusleiste
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 SIM card
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Zurücksetzen auf Werkseinstellungen

7. Fernprogrammierung

8. Funktionsprüfung des Kommunikators

9. Firmware-Update

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

Der G16 ist ein **direkt angeschlossener Mobilfunk-Kommunikator** von Trikdis: Er wird nicht an den Telefonleitungsausgang der Alarmzentrale angeschlossen, sondern an den **Bedienteilbus oder die serielle Schnittstelle** der Zentrale. Er liest die Ereignisse direkt aus der Zentrale – mit Zonen-, Bereichs- und Benutzernummer – und überträgt sie über die mobile Datenverbindung an den Empfänger der Leitstelle sowie in die Protegus-Cloud, in die App des Benutzers. Er arbeitet mit den unterstützten Zentralen von DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell und Crow; bei den **direkt steuerbaren** Typen schärft und entschärft der Benutzer in der App Protegus 2 mit seinem eigenen Bedienteilcode, ohne eigene Schlüsselschalter-Zone. Die App Protegus 2 ist mit allen vom G16 unterstützten Alarmzentralen nutzbar, unabhängig vom Hersteller. Für Zentralen anderer Hersteller, die nur einen Telefonleitungsausgang haben, ist der Kommunikator G16T (TIP/RING) gedacht.

1.1 Wofür er gedacht ist und wie er funktioniert

- **Liest die Zentrale direkt.** Über den Bus der Zentrale kommt jedes Ereignis sofort und mit der eigenen Nummerierung der Zentrale beim Kommunikator an; der Wählgerät-Teil der Zentrale muss nicht eingerichtet werden, und es gibt auch keine Contact-ID-Wahl.
- **Meldet an die Leitstelle.** Er sendet die Ereignisse über IP an den Software- oder Hardware-Empfänger von Trikdis (Protokoll TRK) – diese arbeiten mit jeder Leitstellensoftware zusammen – oder an jeden universellen Empfänger (SIA DC-09 2007/2012, SUR-GARD TL150). An einen SUR-GARD-Empfänger gibt er die von der Zentrale kommenden Contact-ID-Codes in SIA-Codes umgewandelt weiter. Die Verbindung prüft er standardmäßig alle 30 Sekunden (oder in dem von Ihnen eingestellten Intervall) und wechselt bei einem Fehler auf den Ersatzkanal.
- **Benachrichtigt den Benutzer.** Die App Protegus 2 zeigt die Geschehnisse als Push-Nachricht – mit einem zum Ereignis passenden, eigenen Signalton – und in der Ereignisliste; der Benutzer kann in der App scharf- und unscharfschalten und die angeschlossenen Geräte schalten (Beleuchtung, Tor, Lüftung, Heizung, Bewässerung usw.). Er kann auch per SMS und Anruf benachrichtigt werden.
- **Gleichzeitig oder getrennt** arbeitet er mit der Leitstelle und dem Benutzer: Er ist nur mit Protegus 2 (ohne Leitstelle), nur mit der Leitstelle oder mit beiden nutzbar. Sind beide eingerichtet, sendet er das Ereignis zuerst an die Leitstelle, danach an den Benutzer.
- **SMS-Reserve.** Er benachrichtigt die Leitstelle auch per SMS, wenn die Datenverbindung im Netz des Anbieters nicht funktioniert; er kann parallel an zwei Empfänger senden, jeweils mit eigenem Ersatzkanal.
- **Eigene Ein- und Ausgänge.** Drei Klemmen mit Doppelfunktion (I/O) sind als Eingang (Melder, Sabotage) oder als steuerbarer Ausgang (Schlüsselschalter-Zone, Relais) nutzbar; die Ausgänge können Sie in der App Protegus 2 und per SMS-Befehl schalten. Die 4G-Variante kann über ihren RS485-Bus mit dem Erweiterungsmodul iO-8 weitere 8 I/O erhalten und mit dem Modul W485 oder E485 auch über WLAN bzw. kabelgebundenes Internet kommunizieren – dann ist das Mobilfunknetz der Ersatzweg.

Den Aufbau des Systems zeigt die folgende Abbildung: Der Bus der Alarmzentrale ist mit dem G16 verbunden, der G16 erreicht über das Mobilfunknetz das Internet, von dort den Empfänger der Leitstelle und die Protegus-Cloud, und der Benutzer sieht das System in der App Protegus 2.

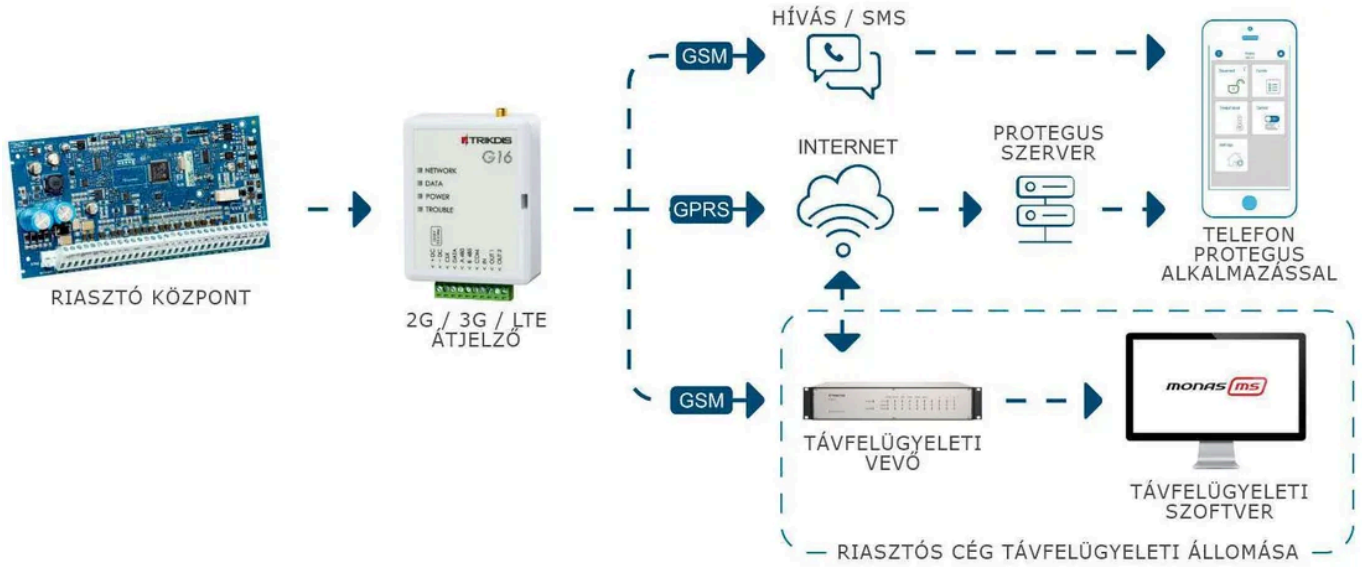


Abbildung 1. Die Stellung des G16 im System: Alarmzentrale → G16 → Mobilfunknetz → Empfänger der Leitstelle und Protegus-Cloud → App Protegus 2. Der Benutzer kann auch SMS und Anrufe erhalten (GSM), der Empfänger der Leitstelle als Reserve SMS.

- 1 Alarmzentrale (Bedienteilbus oder serielle Schnittstelle)
- 2 Kommunikator G16 (2G / 4G)
- 3 Anruf und SMS an den Benutzer
- 4 Mobile Datenverbindung → Internet → Protegus-Cloud
- 5 Telefon mit der App Protegus 2
- 6 Empfänger der Leitstelle
- 7 Leitstellensoftware (Leitstelle des Sicherheitsdienstleisters)

1.2 Kompatible Alarmzentralen

Der G16 kann an die folgenden Zentralen angeschlossen werden. Bei den **direkt steuerbaren** Typen erfolgt das Scharf- und Unscharfschalten in der App mit dem Bedienteilcode; bei den übrigen über eine Schlüsselschalter-Zone (Punkt 3.4). Für die direkte Steuerung von Paradox-Zentralen muss die Firmware der Zentrale mindestens **V.4** sein; bei den neueren Paradox-Typen (SP+, MG5050+, EVOHD+) ist die serielle Schnittstelle ab Werk gesperrt und muss vor der Nutzung freigeschaltet werden.

Direkt steuerbare Zentralen – der Kommunikator erhält die Ereignisse über den Datenbus oder die serielle Schnittstelle, und das Scharf-/Unscharfschalten funktioniert ohne zusätzliche Verkabelung:

Hersteller	Anschluss	Typen
Paradox	serielle Schnittstelle	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* ab Firmware 7.50)
DSC	Datenbus	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	Datenbus	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	serielle Schnittstelle	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	Datenbus	Ademco Vista-15, Vista-20, Vista-48

Bei den mit * gekennzeichneten neueren Paradox-Zentralen ist die serielle Schnittstelle werkseitig gesperrt; ein externes Gerät kommuniziert erst nach der Freischaltung mit ihr.

Soros port feloldás útmutató

Über Schlüsselschalter steuerbare Zentralen – der Kommunikator erhält die Ereignisse über den Datenbus oder die serielle Schnittstelle, für die Steuerung sind ein Schlüsselschalter-Anschluss und dessen Programmierung erforderlich (Punkt 3.4):

Hersteller	Anschluss	Typen
Paradox	serielle Schnittstelle	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	Datenbus	PC1404, PC5020
Texecom	serielle Schnittstelle	Premier 412, 816, 832, 832+
Inner Range	Datenbus	Inception, Integriti
Crow	Datenbus	Runner 4/8, 8/16

Die Liste ändert sich von Zeit zu Zeit; den aktuellen Stand finden Sie in der Kompatibilitätssuche. Darüber hinaus ist er auch mit den Zentralen **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 und MATRIX 816**, **DSC PC5015** sowie **Paradox DIGIPLEX EVO96 und NE96** nutzbar. Mit den Zentralen **DSC PowerSeries NEO** funktioniert der G16 nicht: Am Bus der NEO lässt der Hersteller kein externes Gerät zu, siehe DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen.

1.3 Varianten

Diese Anleitung wurde für die **Hardware-Version 4** des G16 erstellt, ist aber **auch für die Hardware-Version 3 nutzbar**: Anschluss, Einrichtung und Funktion der beiden Versionen sind weitgehend gleich. Die Anleitung gilt gleichermaßen für die Variante mit 2G-, 3G- und 4G-Modem. Die Unterschiede fasst die folgende Tabelle zusammen; wo der Text einen Wert der Version 4 nennt, beachten Sie bei der Version 3 diesen.

	Hardware 3 (v3)	Hardware 4 (v4)
Typen (in TrikdisConfig)	z. B. G16_3210 (2G); es gab auch Varianten mit 3G- und 4G-Modem	G16_G410 (2G), G16_54E0 (4G)
Ein-/Ausgänge	1 Eingang mit wählbarem Typ (IN) + 2 Open-Collector-Ausgänge (OUT1, OUT2, max. 0,15 A)	3 Klemmen mit Doppelfunktion (I/O 1, I/O 2, I/O 3), jede als Eingang oder als Open-Collector-Ausgang (max. 0,15 A) nutzbar
Einstellung der Ein-/Ausgänge	Seite System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	Seite **IN/OUT** (Punkt 6.6)
Stromaufnahme	100 mA; beim Senden höchstens 250 mA	60–100 mA; beim Senden höchstens 500 mA
RS485-Bus (iO-8, W485, E485)	nur bei der 3G- und 4G-Variante	nur bei der 4G-Variante (G16_54E0)

Die Hardware-Version 4 wird mit zwei Modems gefertigt:

Typ	Modem	Frequenzen	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	nein
G16_54E0	4G (LTE)	regionsabhängige LTE-Bänder	ja

Die Hardware-Version finden Sie in der Statusleiste von TrikdisConfig (**HW**) und auf dem Etikett auf der Rückseite des Geräts. Über die Einführung der Version 4 berichtet ein eigener Artikel: Die Hardware-Version v4 der GSM-Kommunikatoren G16 und G16T ist da.

1.4 Hauptmerkmale

Verbindung mit der Alarmzentrale

- Mit höchstens 4 Leitungen (+DC, −DC, CLK, DATA) an den Bedienteilbus (DSC, Caddx, Crow, Pyronix, Honeywell) oder die serielle Schnittstelle (Paradox, Texecom, InnerRange) der Zentrale anschließbar; für die serielle Schnittstelle gibt es ein Originalkabel (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Überträgt jedes Ereignis der Zentrale mit der vollständigen Ereignisinformation (Code, Bereich, Zone oder Benutzer); meldet die Unterbrechung der Verbindung (LED TROUBLE, Ereignis COMMUNICATION).
- Direkt steuerbare Zentralen können in der App mit dem Bedienteilcode scharf- und unscharfgeschaltet werden; Protegus 2 zeigt auch den Zustand der Zonen.

Kommunikation mit der Leitstelle

- IP-Verbindung mit den Trikdis-Empfängern (Software-Empfänger IPcom, RL14, RM14) und mit universellen Empfängern (SIA DC-09, TL150).
- Primärer, Ersatz- und paralleler Kanal; SMS-Ersatzbenachrichtigung an den Trikdis-SMS-Empfänger (RL14, RM14, GM14).
- Nachrichtenverschlüsselung AES-128; Ereignisspeicher 60 Nachrichten.

Benutzerfunktionen

- Mobile und Web-App Protegus 2: Benachrichtigung, Ereignisliste, Scharf- und Unscharfschalten, Schalten der Ausgänge.
- Steuerung und Grundeinstellung auch per SMS-Befehl.
- Benachrichtigung auch per SMS und Anruf an bis zu 4 Telefonnummern.
- Mehrstufige Benutzerrechte in der App (Administrator, Errichter, Benutzer).

Installation und Einrichtung

- Die Einstellungen können in einer Datei gespeichert und in einen anderen Kommunikator geladen werden.
- Zwei Zugriffsebenen: Administrator und Errichter.
- Fernkonfiguration und Fern-Update mit der Software TrikdisConfig.

1.5 Bestandteile des Kommunikators

Die Leiterplatte des G16 sitzt in einem weißen Kunststoffgehäuse; die Frontabdeckung ist abnehmbar, die Klemmleiste steckbar. Das folgende Bild zeigt die 4G-Variante; die 2G-Variante hat keine LED BAND und keine Klemmen A 485 / B 485.

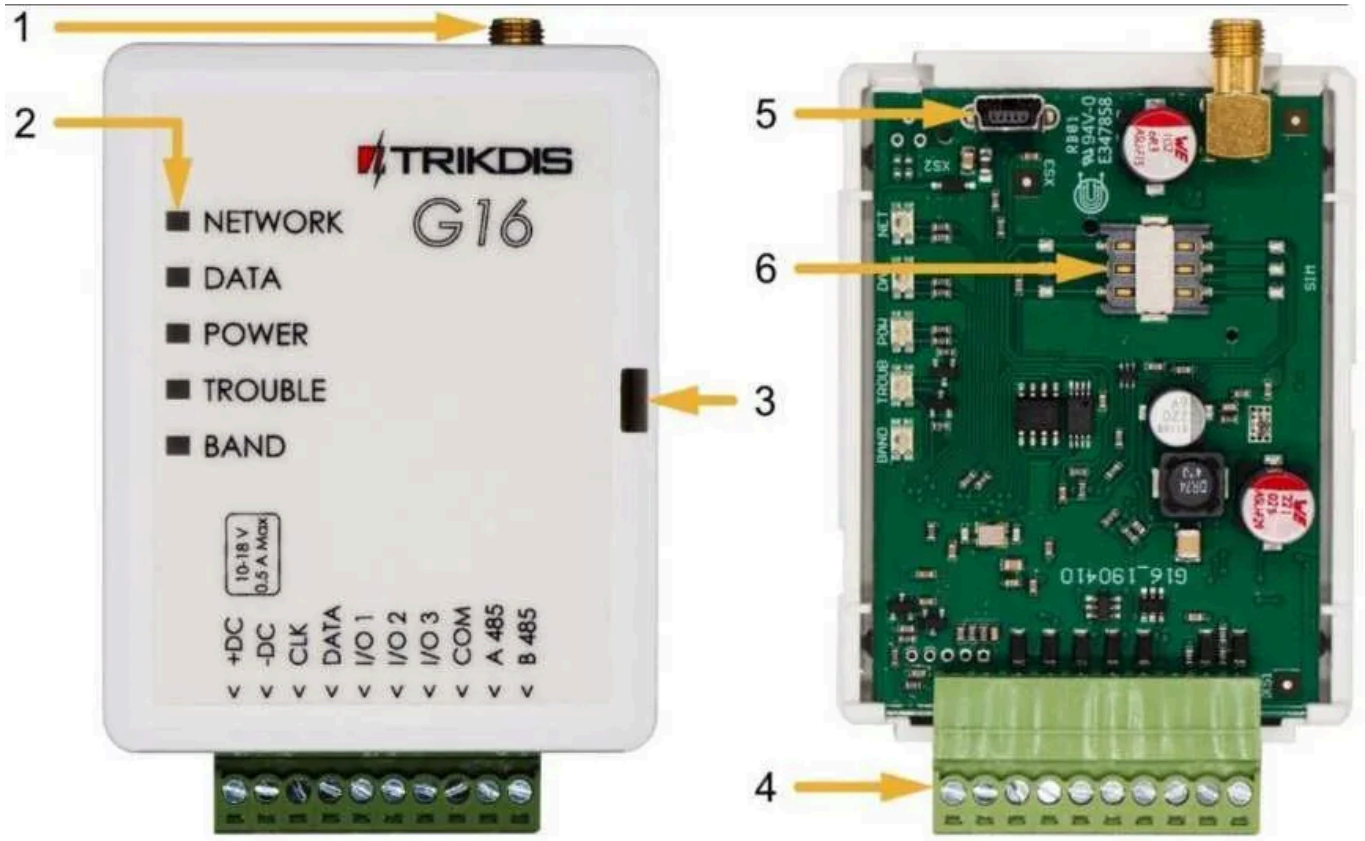


Abbildung 2. Die Bestandteile des G16 (4G-Variante) von vorn und mit geöffnetem Gehäuse.

- 1 SMA-Anschluss der GSM-Antenne
- 2 LED-Anzeigen (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Öffnung zum Abnehmen der Frontabdeckung
- 4 Abnehmbare Klemmleiste
- 5 USB-Mini-B-Buchse für die Programmierung
- 6 Halter für die Nano-SIM-Karte

Die Klemmleiste ist steckbar: So lässt sich das Gerät mit einem Handgriff spannungsfrei machen oder neu starten, sie ist beim Anschließen leichter zu handhaben, und zur Programmierung über USB kann das Gerät zum Computer gebracht werden.

1.6 Klemmen

Klemme	Funktion
+DC	Versorgung, +10–18 V DC
−DC	Versorgung, negativ
CLK	Takt- / serielle Leitung des Busses der Zentrale
DATA	Datenleitung des Busses der Zentrale
I/O 1	Ein-/Ausgang 1 (Werkseinstellung: nicht verwendet)
I/O 2	Ein-/Ausgang 2 (Werkseinstellung: Eingang, NO)
I/O 3	Ein-/Ausgang 3 (Werkseinstellung: Ausgang)
COM	Gemeinsamer (negativer) Punkt für Ein- und Ausgänge
A 485	Leitung A des RS485-Busses (nur 4G-Variante)
B 485	Leitung B des RS485-Busses (nur 4G-Variante)

Die Beschriftung der Klemmleiste steht auch auf der Frontabdeckung, daher muss der Deckel beim Anschließen nicht abgenommen werden. An welche Klemme der Zentrale CLK und DATA gehen, ist je nach Hersteller unterschiedlich – die Anschlusspläne enthält Punkt 3.3.

1.7 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 (nur 4G) die Art des Netzes.

NETWORK – Netzverbindung

Anzeige	Bedeutung
aus	Keine Verbindung zum Mobilfunknetz
blinkt gelb	Verbindung zum Mobilfunknetz wird aufgebaut
leuchtet grün	Mit dem Mobilfunknetz verbunden
leuchtet grün, blinkt gelb	Verbunden; die Zahl der gelben Blinkimpulse ist die **Signalstärke**: Bei 2G sind 5, bei 4G 3 Blinkimpulse ein gutes Signal

DATA – Datenverkehr

Anzeige	Bedeutung
aus	Keine Nachricht wartet auf das Senden
leuchtet grün	Im Speicher warten Nachrichten auf das Senden
blinkt grün	Daten werden gesendet oder empfangen (während der Programmierung)

Schnelle Prüfung

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

POWER – Versorgungsspannung

Anzeige	Bedeutung
aus	Keine Versorgung, oder die Versorgung ist getrennt
leuchtet grün	Eingeschaltet, die Versorgungsspannung ist in Ordnung
leuchtet gelb	Unzureichende Versorgungsspannung (höchstens 11,5 V)
leuchtet grün, blinkt gelb	Bereit zur Programmierung (USB-Kabel eingesteckt)
leuchtet gelb (während der Programmierung)	Keine Verbindung zum Computer

TROUBLE – Fehler

Anzeige	Bedeutung
aus	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	Kann sich nicht im Mobilfunknetz anmelden (Registrierungsfehler)
5 rote Blinkimpulse	Kann keine Verbindung zum Datennetz (GPRS/UMTS/LTE) herstellen
6 rote Blinkimpulse	Keine Verbindung zum Empfänger der Leitstelle und/oder zum Protegus-Server (die Ursache kann auch ein Fehler der Internetverbindung sein)
7 rote Blinkimpulse	Die Verbindung zur Alarmzentrale ist unterbrochen (Bus- oder serielle Verbindung)
blinkt rot (während der Programmierung)	Speicherfehler
leuchtet rot (während der Programmierung)	Beschädigte Firmware

BAND – Art des Netzes (nur 4G-Variante)

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

1.8 Technische Daten

Parameter	Wert
Verbindung mit der Alarmzentrale	Bedienteilbus oder serielle Schnittstelle, je nach Typ der Zentrale (höchstens 4 Leitungen: +DC, −DC, CLK, DATA; am Bus von Caddx und Pyronix wird CLK nicht verwendet)
Ein-/Ausgänge	3 I/O mit Doppelfunktion (I/O 1, I/O 2, I/O 3): 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
Erweiterung	Über den RS485-Bus (nur 4G-Variante): Erweiterungsmodul iO-8 (+8 I/O) und andere Erweiterungsmodule der iO-Serie; WiFi-Modul W485, Ethernet-Modul E485
2G-Modem	850 / 900 / 1800 / 1900 MHz
4G-Modem	regionsabhängige LTE-Bänder
Versorgungsspannung	10–18 V DC
Stromaufnahme	60–100 mA nominal; höchstens 500 mA beim Senden
Übertragungsprotokolle	TRK, DC-09_2007, DC-09_2012, TL150

Parameter	Wert
Ereignisspeicher	60 Nachrichten
Verschlüsselung	AES-128
Programmierung	TrikdisConfig (Windows) über USB-Mini-B-Kabel oder aus der Ferne; SMS-Befehle
Betriebsumgebung	−10 … +50 °C, max. 80 % relative Luftfeuchtigkeit (bei +20 °C)
Abmessungen	92 × 65 × 26 mm
Gewicht	80 g

2. Schnelle Inbetriebnahme mit TrikdisConfig

Alle Einstellungen des G16 werden mit dem Windows-Programm **TrikdisConfig** vorgenommen – über USB-Kabel oder aus der Ferne. In diesem Kapitel beschreiben wir den kürzesten Weg: Sie richten das Gerät auf dem Tisch ein, vor dem Anschließen, danach muss es vor Ort nur noch angeschlossen werden. Die ausführliche Erklärung der Einstellungen enthält Kapitel 6.

2.1 Vorbereitung

Was Sie benötigen

USB-Mini-B-Kabel · mindestens 4-adriges Kabel für den Bus der Zentrale – für die serielle Schnittstelle von Paradox das Kabel **CRP2** oder **CRP2B**, für die serielle Schnittstelle von Texecom das Kabel **CRP4** · flacher Schraubendreher 2,5 mm · Mobilfunkantenne mit passendem Gewinn (an Orten mit schwacher Netzabdeckung eine Antenne mit höherem Gewinn) · aktive Nano-SIM-Karte mit mobilem Datendienst (die PIN-Abfrage kann ausgeschaltet werden) · die Errichteranleitung der Alarmzentrale. Das benötigte Zubehör muss separat beim Händler bestellt werden.

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

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Öffnen Sie die Frontabdeckung des G16. Stecken Sie einen flachen Schraubendreher in die Öffnung an der Oberkante des Deckels und hebeln Sie die Frontabdeckung durch Druck nach unten vorsichtig ab. Die folgende Abbildung zeigt das Öffnen und die Lage der USB-Buchse.

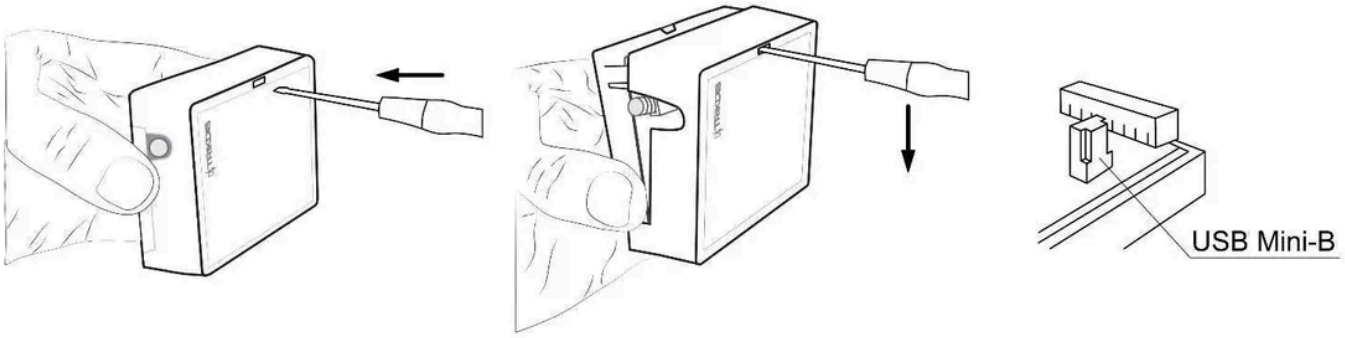


Abbildung 3. Abhebeln der Frontabdeckung mit einem flachen Schraubendreher (links, Mitte) und die Lage der USB-Mini-B-Buchse auf der Leiterplatte (rechts).

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

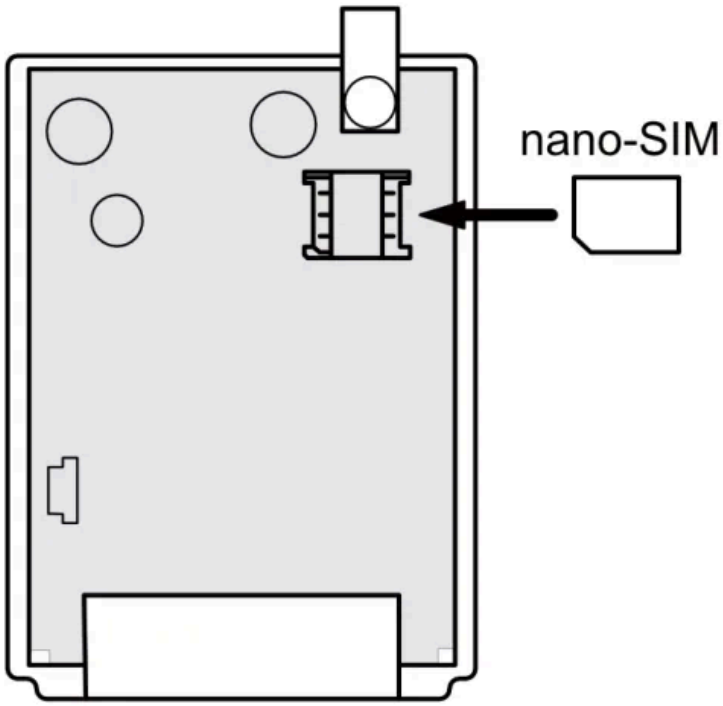


Abbildung 4. Die Lage der Nano-SIM-Karte auf der Leiterplatte.

4. Verbinden Sie den G16 mit dem Computer über ein USB-Mini-B-Kabel. USB liefert genügend Strom für die Programmierung, eine eigene Versorgung ist nicht nötig.

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 **Read [F4]** (Lesen): Das Programm liest die aktuellen Einstellungen des Geräts aus. Wenn es ein Passwort verlangt, geben Sie den 6-stelligen Administrator-Code (ab Werk `123456`) oder Errichter-Code (ab

Werk `654321`) ein.

2.2 Typ der Zentrale und direkte Steuerung

Welche Betriebsart Sie auch nutzen: Geben Sie zuerst auf der Seite **System settings** an, an welche Zentrale der Kommunikator angeschlossen wird.

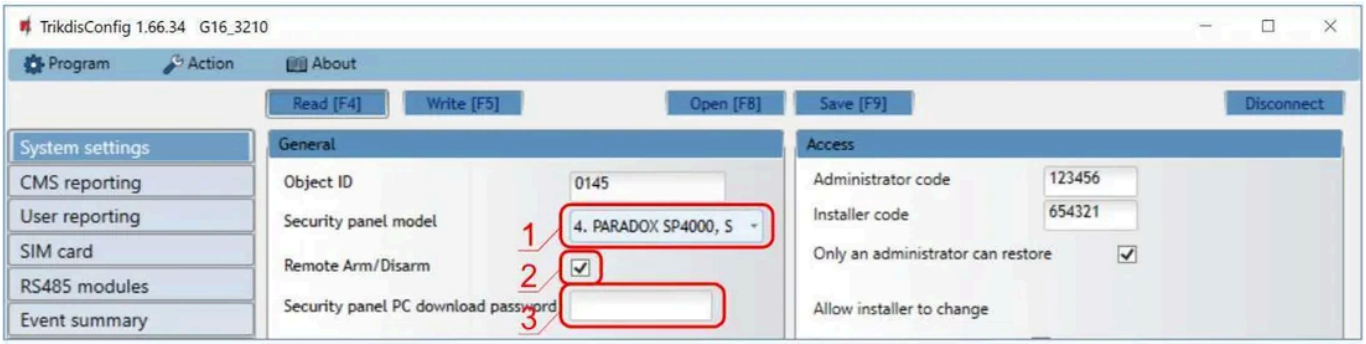


Abbildung 5. TrikdisConfig – Seite System settings, Gruppe General.

- 1 **Security panel model** – der Typ der angeschlossenen Alarmzentrale aus der Liste; davon hängt ab, wie der Kommunikator den Bus liest.
- 2 **Remote Arm/Disarm** – aktivieren Sie das Häkchen, wenn der Benutzer die Zentrale in der App Protegus 2 mit seinem eigenen Bedienteilcode scharf- und unscharfschalten möchte. Erscheint nur bei den direkt steuerbaren Typen; bei den übrigen Zentralen lässt sich das Scharfschalten über eine Schlüsselschalter-Zone lösen (Punkt 3.4) – lassen Sie es dann leer.
- 3 **Security panel PC download password** – bei Paradox- und Texecom-Zentralen das PC- bzw. UDL-Passwort der Zentrale (4 Zeichen); es muss mit dem in der Zentrale eingestellten übereinstimmen. Das Feld erscheint, nachdem Remote Arm/Disarm angehakt wurde.

Bei mehreren Zentralen ist auch in der Zentrale eine Einstellung nötig: bei Caddx-, Honeywell- und InnerRange-Zentralen schon für das Lesen der Ereignisse (Freigabe des Busses bzw. der seriellen Schnittstelle), bei Paradox- und Texecom-Zentralen für die direkte Steuerung (PC- bzw. UDL-Passwort) – Kapitel 4 beschreibt dies je Hersteller, zusammen mit dem Ändern des Passworts.

2.3 Verbindung zur App Protegus 2

Wenn der Benutzer das System in der App Protegus 2 sehen und steuern möchte, stellen Sie auf der Seite **User reporting**, Reiter **PROTEGUS Cloud**, Folgendes ein.



Abbildung 6. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- 4 **Enable connection** – aktivieren Sie das Häkchen: Es gibt die Verbindung mit der Protegus-Cloud frei.
- 5 **Protegus Cloud access code** – ändern Sie das werkseitige Passwort `123456`. Dieses muss später in der App beim Anlegen des Systems eingegeben werden; **nach dem Anlegen des Systems kann es nicht mehr geändert werden.**

Geben Sie danach auf der Seite **SIM card** die Daten der Karte ein.

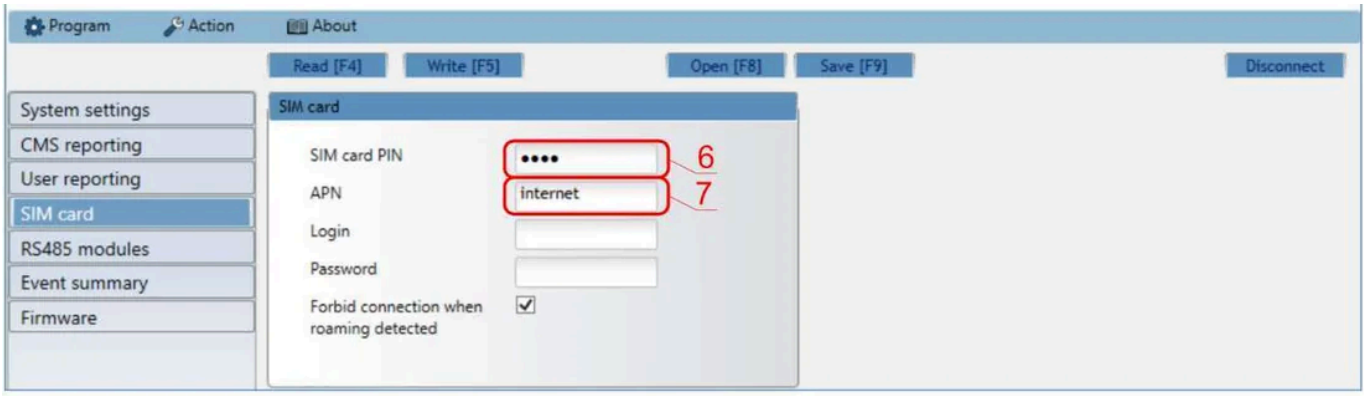


Abbildung 7. TrikdisConfig – Seite SIM card.

- 6 **SIM card PIN** – der PIN-Code der Karte (wenn die PIN-Abfrage ausgeschaltet ist, kann der Werkswert bleiben).
- 7 **APN** – der Zugangspunkt für die Datenverbindung des Anbieters (siehe unten).

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 erhalten Sie vom Anbieter der SIM-Karte, und Sie finden ihn auch auf dessen Website; der APN „internet“ ist allgemein und funktioniert in den Netzen vieler Anbieter. Die bekannten APNs europäischer Anbieter führen wir in einem eigenen Artikel: APN-Einstellung – Liste europäischer Mobilfunkanbieter.

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.

2.4 Verbindung zur Leitstelle

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

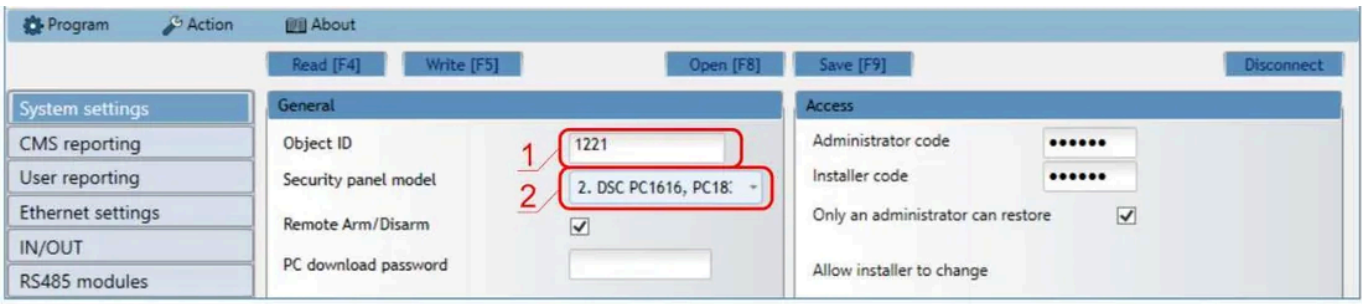


Abbildung 8. TrikdisConfig – Seite System settings, Gruppe General.

- 1 **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen, 0–9, A–F). `FFFE` und `FFFF` sind nicht zulässig.
- 2 **Security panel model** – der Typ der angeschlossenen Alarmzentrale (falls Sie ihn in Punkt 2.2 noch nicht eingestellt haben).

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

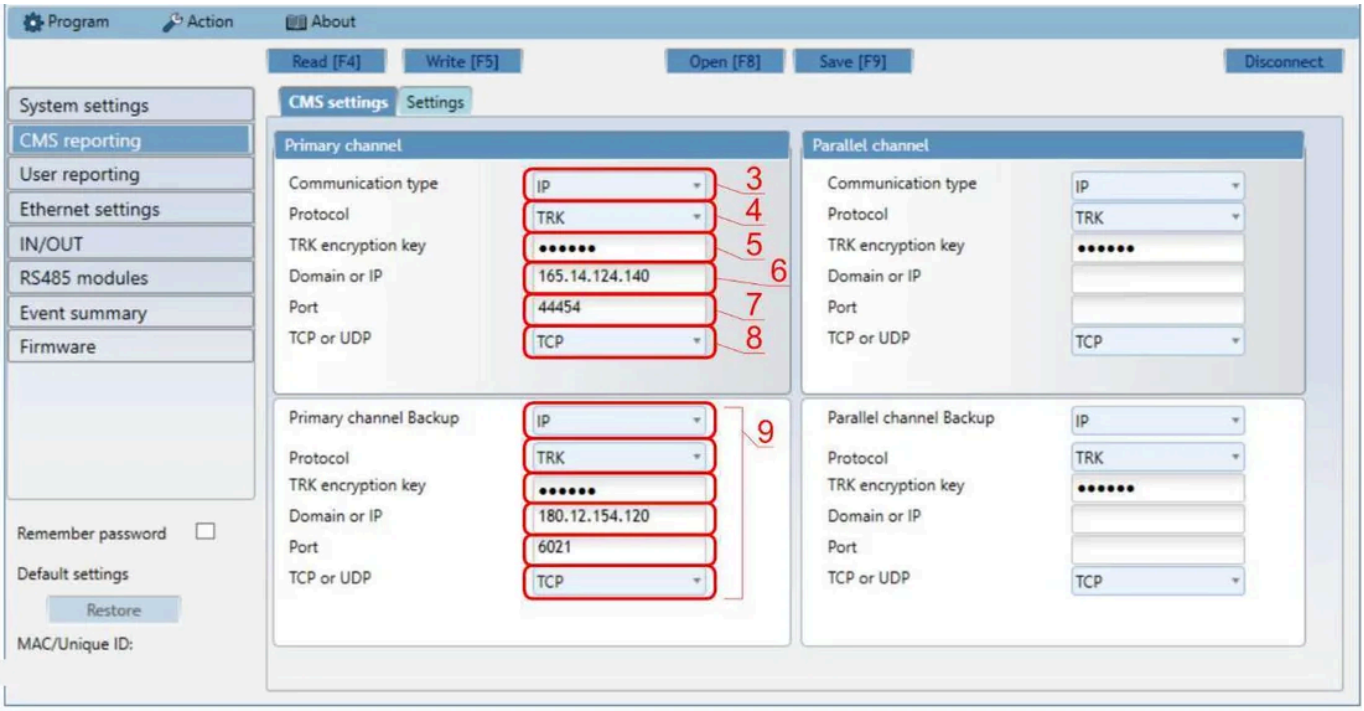


Abbildung 9. TrikdisConfig – CMS reporting, Reiter CMS settings.

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

Empfohlen wird auch die Einstellung des **Parallel channel** (paralleler Kanal) und des zugehörigen Ersatzkanals, wenn die Ereignisse zwei Empfänger erhalten müssen; in das Feld **Backup SMS reporting number** können Sie – auch das wird empfohlen – die Telefonnummer des Trikdis-SMS-Empfängers eintragen: Das Gerät sendet nach dem ersten Start sofort eine SMS dorthin und meldet danach per SMS, wenn keiner der IP-Kanäle funktioniert.

Geben Sie zum Schluss auf der Seite **SIM card** die Daten der Karte ein, falls Sie das in Punkt 2.3 noch nicht getan haben.

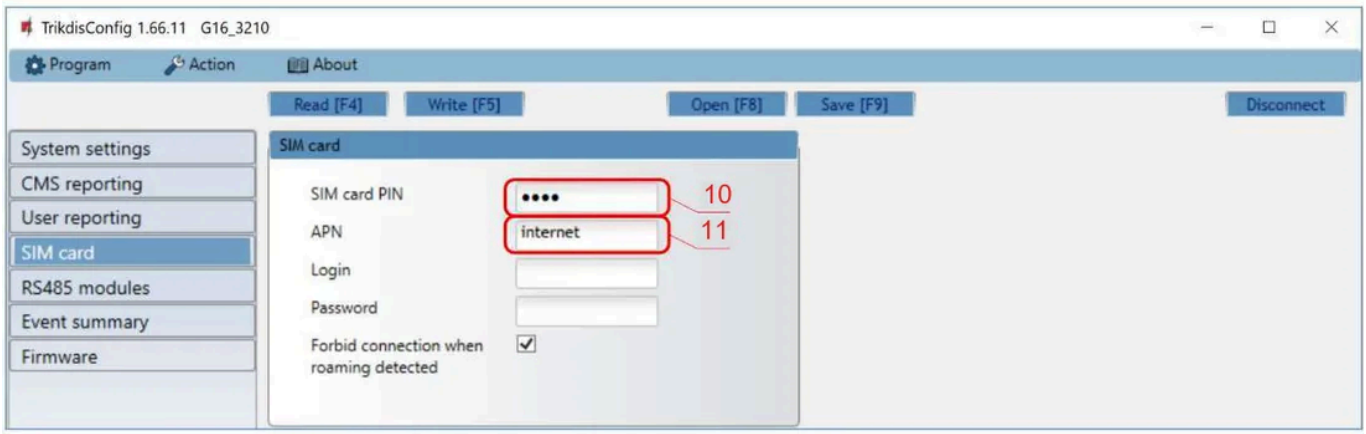


Abbildung 10. TrikdisConfig – Seite SIM card.

- 10 **SIM card PIN** – der PIN-Code der Karte.
- 11 **APN** – der Zugangspunkt des Anbieters (siehe Punkt 2.3).

Meldung per SMS an die Leitstelle funktioniert nur mit einem Trikdis-Empfänger (IP/SMS-Empfänger RL14, Mehrkanal-Empfänger RM14 oder SMS-Empfänger GM14); dann sind nur der Verschlüsselungsschlüssel und die Telefonnummer nötig. Beim Protokoll **DC-09** geben Sie im Reiter **Settings** auch die DC-09-Objekt-, Linien- und Empfängernummer ein.

Drücken Sie am Ende der Einstellungen die Taste **Write [F5]** (Schreiben), warten Sie die Rückmeldung ab und ziehen Sie das USB-Kabel ab. Das Gerät ist damit bereit zum Anschließen.

3. Installation 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 Installationsschritte

1. Nehmen Sie die Frontabdeckung ab (siehe Punkt 2.1) und ziehen Sie die Klemmleiste ab.
2. Setzen Sie die Nano-SIM-Karte ein, falls Sie das bei der Inbetriebnahme noch nicht getan haben.
3. Nehmen Sie die Leiterplatte aus der Rückwand: Öffnen Sie die Verriegelung in der Ecke (siehe Abbildung).
4. Befestigen Sie die Rückwand mit Schrauben am gewählten Ort.
5. Setzen Sie die Leiterplatte wieder in die Rückwand ein und stecken Sie die Klemmleiste wieder auf.
6. Schrauben Sie die GSM-Antenne an.
7. Setzen Sie die Frontabdeckung wieder auf.

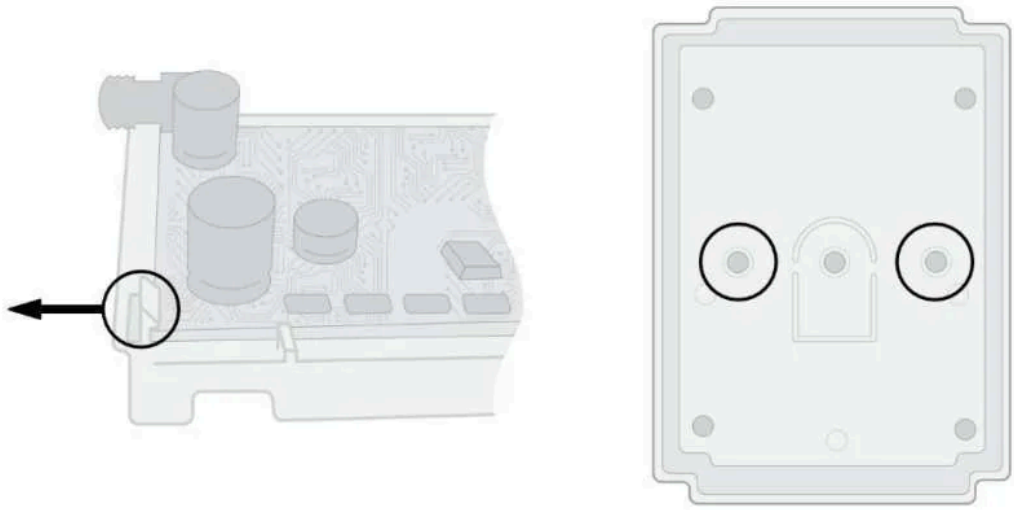


Abbildung 11. Herausnehmen der Leiterplatte: Öffnen der Verriegelung in der Ecke (links) und die Befestigungslöcher der Rückwand (rechts, eingekreist).

Die SIM-Karte muss aktiv sein, und für die IP-basierte Nutzung muss darauf die mobile Datenverbindung funktionieren. Wenn Sie nicht möchten, dass TrikdisConfig einen PIN-Code verlangt, schalten Sie die PIN-Abfrage der Karte in einem Telefon aus.

3.2 Montageort und Antenne

- Setzen Sie den Kommunikator an einen **trockenen Ort im Innenbereich**, möglichst in die Nähe des Gehäuses der Alarmzentrale, damit die Busleitung kurz bleibt.
- In einem **Metallgehäuse** wird das Mobilfunksignal stark gedämpft. Wenn der Kommunikator in das Metallgehäuse der Zentrale kommt, 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 2G mindestens 5, bei 4G mindestens 3 betragen (siehe Punkt 1.7). Sind es weniger, suchen Sie einen besseren Ort oder wechseln Sie zu einer empfindlicheren, weiter entfernt platzierbaren Antenne.
- 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

Der G16 wird mit **höchstens vier Leitungen** an die Zentrale angeschlossen (am Bus von Caddx und Pyronix wird CLK nicht verwendet): An die Klemmen **+DC** und **–DC** kommt die 12-V-Hilfsversorgung (AUX) der Zentrale, an die Klemmen **CLK** und **DATA** die beiden Datenleitungen des Bedienteilbusses oder der seriellen Schnittstelle der Zentrale. Welche Klemme der Zentrale welche ist, unterscheidet sich je nach Hersteller – schließen Sie nach den folgenden Plänen an. Für die Zentralen mit serieller Schnittstelle (Paradox, Texecom) gibt es ein Originalkabel, dessen eines Ende in den Steckverbinder der Zentrale passt und dessen anderes Ende an die Klemmleiste des G16 angeschlossen werden kann.

Der G16 kann beim Senden bis zu 500 mA aufnehmen. Prüfen Sie, ob der AUX-Ausgang der Zentrale dies zusammen mit den übrigen angeschlossenen Geräten verkraftet. Da die Versorgung von der Zentrale kommt, versorgt bei Stromausfall der Akku der Zentrale auch den Kommunikator. Die meisten Zentralen nehmen durch vertauschte Leitungen eines am Bus angeschlossenen Geräts keinen Schaden, das Vertauschen von **+DC und –DC** kann den Kommunikator jedoch zerstören – prüfen Sie vor dem Anschließen die Polarität.

Nach dem Anschließen muss in TrikdisConfig im Feld **System settings** → **Security panel model** der Typ der angeschlossenen Zentrale ausgewählt werden (Punkt 2.2); bei einigen Herstellern ist auch in der Zentrale eine Einstellung nötig (Kapitel 4).

3.3.1 DSC PowerSeries

Die vier Klemmen des Keybus: **RED** → +DC, **BLK** → –DC, **YEL** → CLK, **GRN** → DATA.

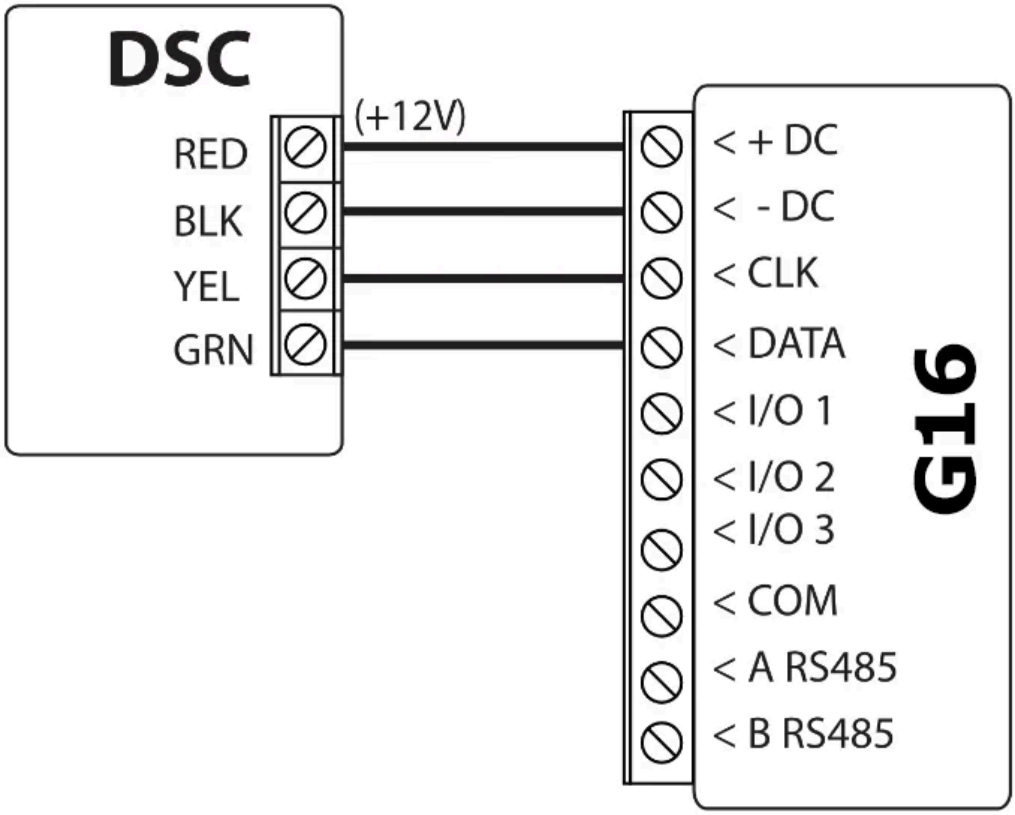


Abbildung 12. Anschluss an den Keybus einer DSC-PowerSeries-Zentrale (Bedienteilbus, „Keypad bus"): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

An die **serielle Schnittstelle** (SERIAL) der Paradox-Zentralen wird der Kommunikator mit dem Originalkabel **CRP2** oder **CRP2B** angeschlossen; das zentralenseitige Ende des Kabels passt in den seriellen Steckverbinder, das andere Ende schließen Sie an die Klemmleiste des G16 an. Die 4 Pins des Steckverbinders: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Die Aderfarben der beiden Kabel unterscheiden sich – der Plan zeigt die Farbbelegung beider Kabel. Die Bezeichnung des seriellen Steckverbinders von Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

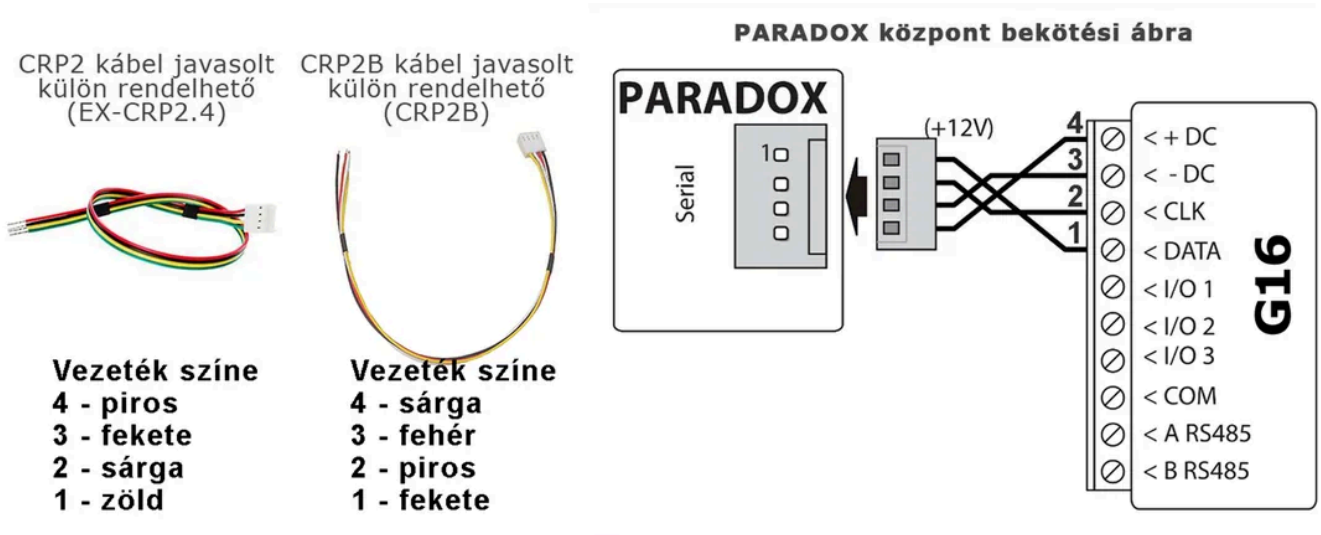


Abbildung 13. Anschluss an die serielle Schnittstelle einer Paradox-Zentrale mit dem Kabel CRP2 (EX-CRP2.4) bzw. CRP2B. CRP2: 4 rot → +DC, 3 schwarz → −DC, 2 gelb → CLK, 1 grün → DATA. CRP2B: 4 gelb → +DC, 3 weiß → −DC, 2 rot → CLK, 1 schwarz → DATA.

Bei den neueren Paradox-Zentralen kann die serielle Schnittstelle ab Werk gesperrt sein – das Freischalten beschreiben Punkt 4.2 und der Artikel Freischalten der gesperrten seriellen Schnittstelle bei Paradox-Alarmzentralen.

3.3.3 UTC Interlogix (Caddx) NetworX

Die drei Klemmen des Bedienteilbusses: **POS** → +DC, **COM** → −DC, **DATA** → DATA. Die Klemme **CLK** wird nicht verwendet.

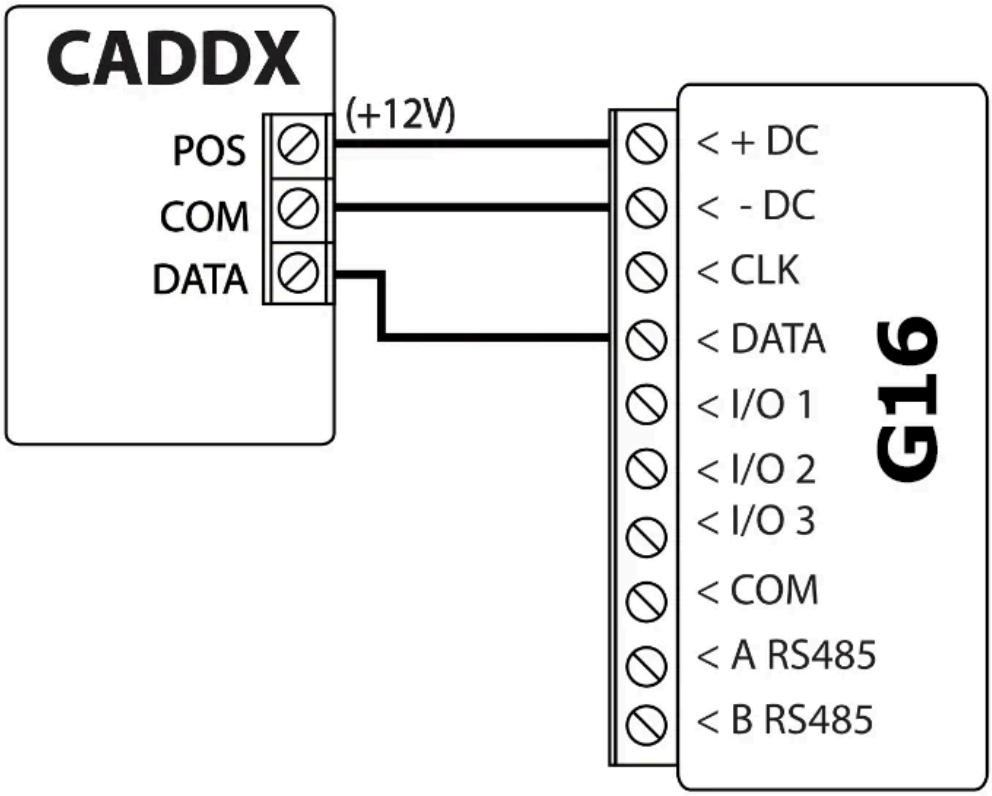


Abbildung 14. Anschluss an den Bedienteilbus („Keypad bus“) einer Caddx-NetworX-Zentrale: POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK bleibt frei.

3.3.4 Texecom Premier / Premier Elite

An die serielle Schnittstelle der Zentrale wird der Kommunikator mit dem Originalkabel **CRP4** angeschlossen: **rot (R)** → +DC, **schwarz (B)** → −DC, **blau (BL)** → CLK, **weiß (W)** → DATA.

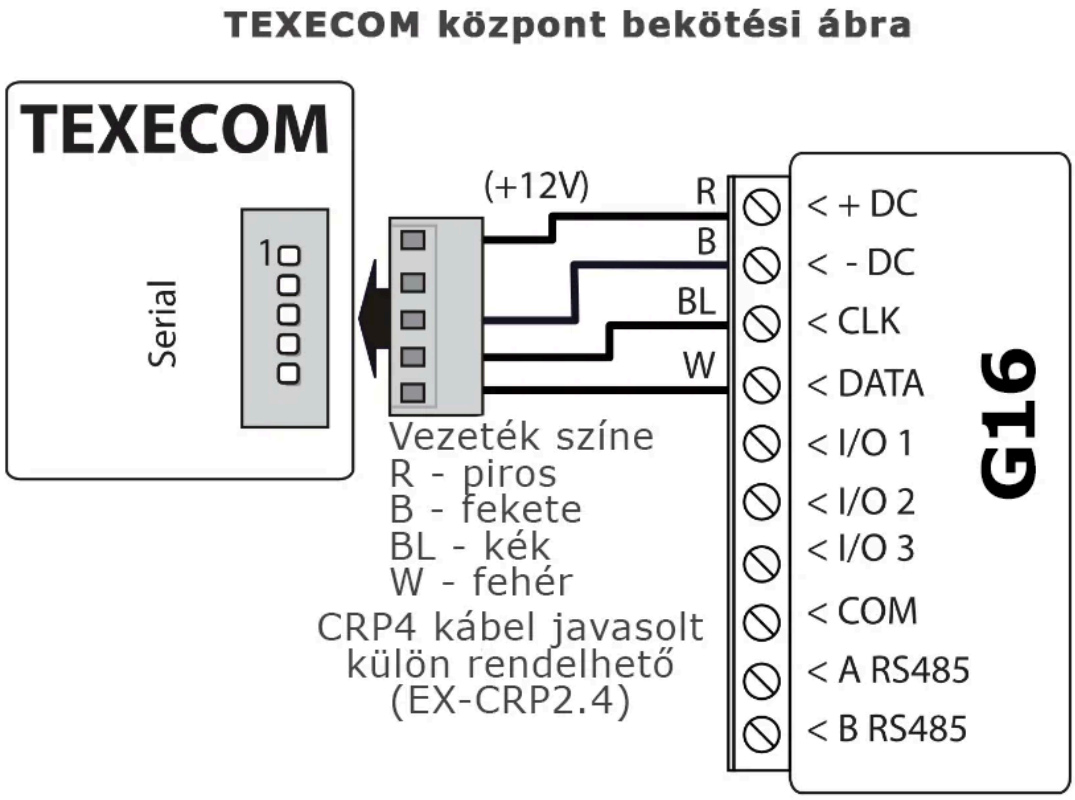


Abbildung 15. Anschluss an die serielle Schnittstelle einer Texecom-Zentrale mit dem Kabel CRP4: rot → +DC, schwarz → −DC, blau → CLK, weiß → DATA.

3.3.5 Crow Runner

Der Bedienteilbus von Crow Runner 4/8 und Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

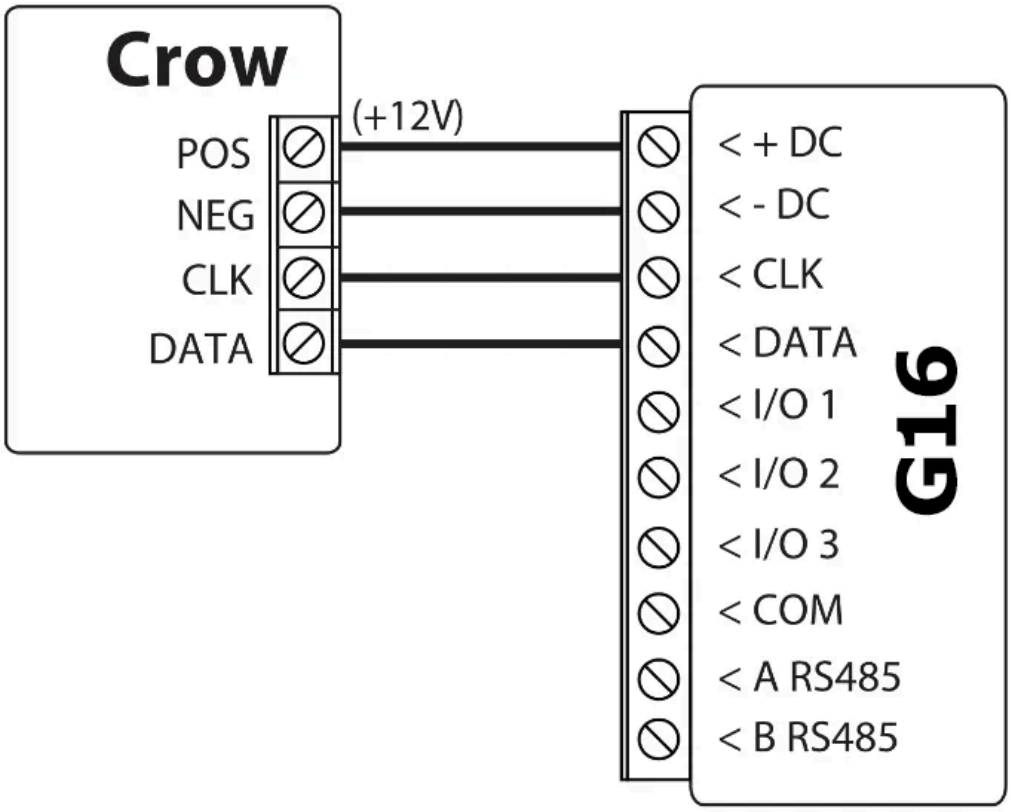


Abbildung 16. Anschluss an den Bedienteilbus („Keypad bus") einer Zentrale Crow Runner 4/8 und Runner 8/16: POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Der Bedienteilbus der Pyronix-Zentralen: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. Die Klemme **CLK** wird nicht verwendet. Machen Sie die Zentrale nach dem Anschließen und dem Einrichten des Kommunikators spannungsfrei und starten Sie sie neu, damit sie den Kommunikator akzeptiert (Punkt 4.5).

3.3.7 Honeywell Ademco Vista

Die nummerierten Klemmen des Bedienteilbusses der Zentralen Vista-15, Vista-20 und Vista-48: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (Datenausgang, gelb) → CLK, **6** (Dateneingang, grün) → DATA.

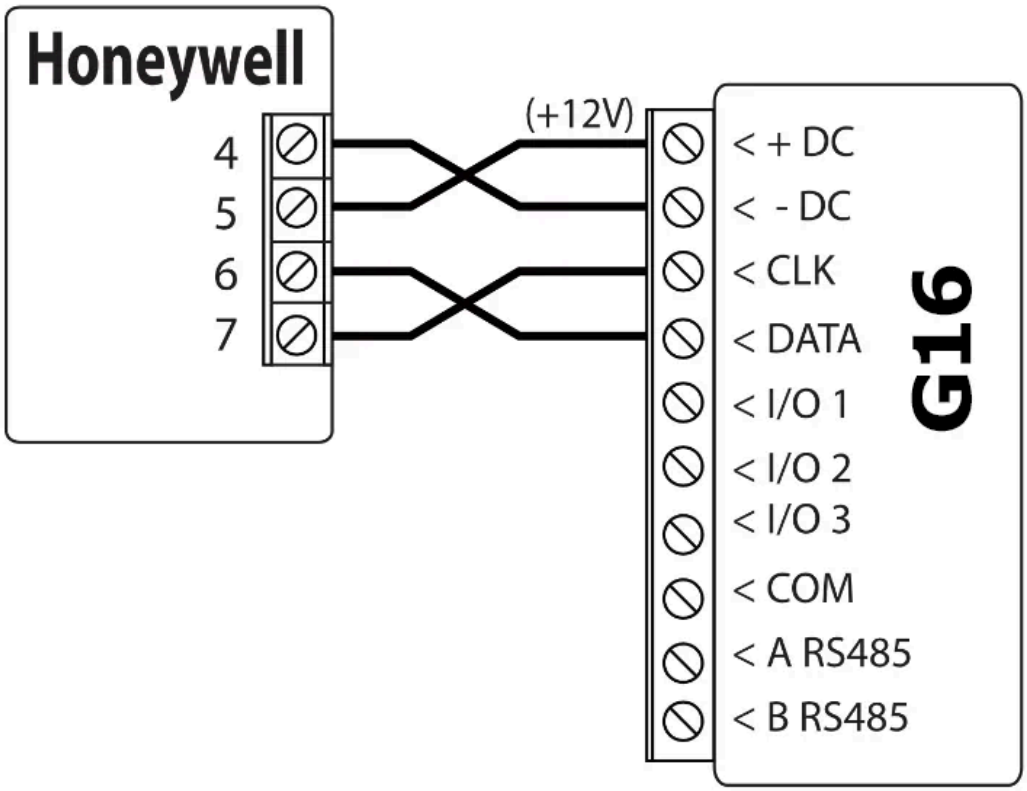


Abbildung 17. Anschluss an den Bedienteilbus („Keypad bus") einer Zentrale Honeywell Vista-20 / Vista-48: 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception und Integriti

Bei der Zentrale **Inception** erhält der Kommunikator die Versorgung von den Versorgungsklemmen der Zentrale (**VOUT +** → +DC, **0V** → −DC), die Datenverbindung entsteht über den USB-Port der Zentrale mit dem Kabel 993030USB von InnerRange: **schwarz** → 0V (−DC), **grün** → CLK, **weiß** → DATA. In der Zentrale muss die Nutzung der seriellen Schnittstelle freigegeben werden (Punkt 4.7).

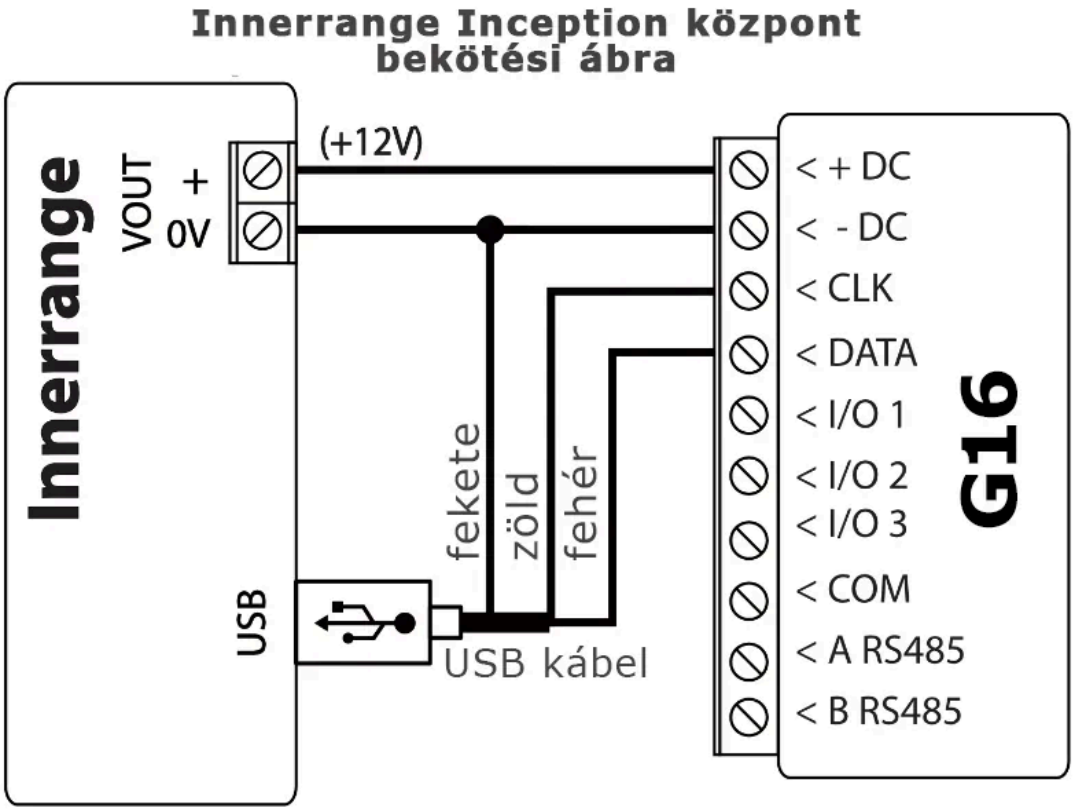


Abbildung 18. Anschluss an eine InnerRange-Inception-Zentrale: Versorgung von den Klemmen VOUT + und 0V, Daten vom USB-Port mit dem Kabel 993030USB (schwarz → 0V, grün → CLK, weiß → DATA).

An den Port 0 (Port 0) der Zentrale **Integriti** kann er mit dem Kabel INTG-996795 angeschlossen werden: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Anschluss einer Schlüsselschalter-Zone

Gehört die Zentrale nicht zu den direkt steuerbaren Typen oder möchten Sie die direkte Steuerung nicht nutzen, lässt sich das Scharf- und Unscharfschalten aus der Ferne über eine **Schlüsselschalter-Zone** lösen: Sie stellen eine I/O-Klemme des Kommunikators als **Ausgang** ein (Seite IN/OUT, Punkt 6.6) und schließen sie an eine Schlüsselschalter-Zone der Zentrale an. Der Ausgang zieht die Zone bei Aktivierung auf COM (negativ); schließen Sie den Abschlusswiderstand der Zone entsprechend dem Zonentyp der Zentrale an. Da der G16 drei I/O-Klemmen hat, können bis zu drei Bereiche mit je einem eigenen Ausgang gesteuert werden.

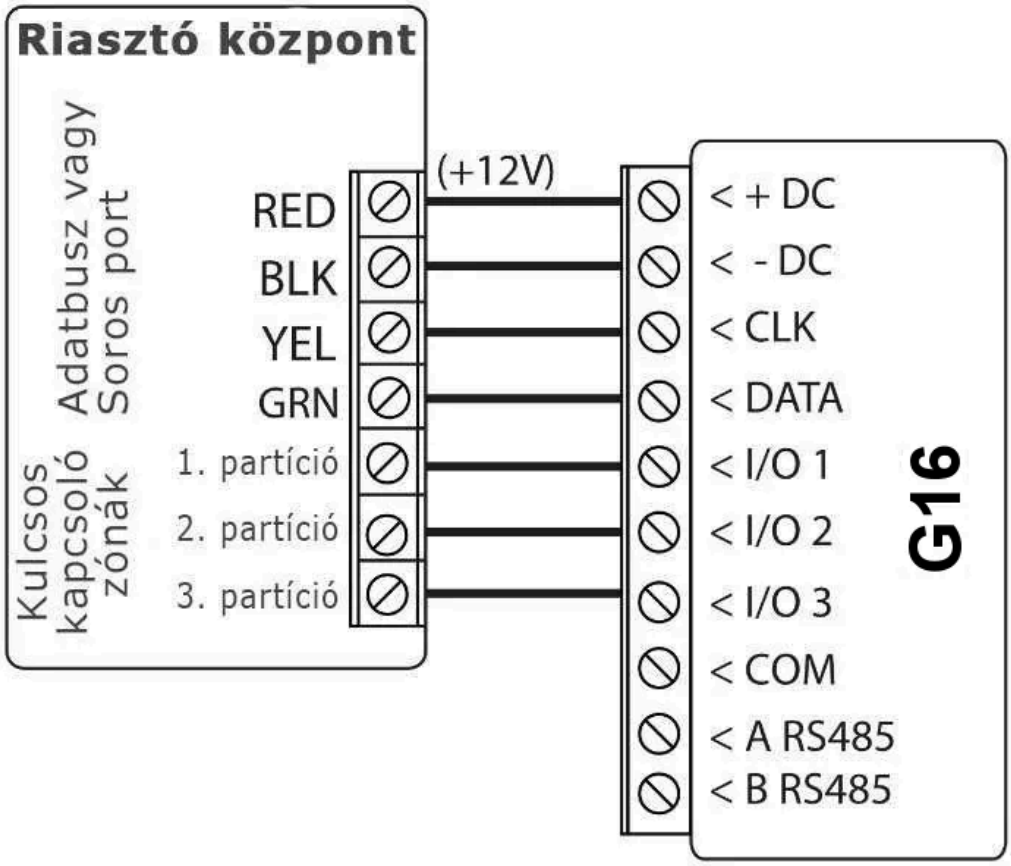


Abbildung 19. Scharf- und Unscharfschalten über eine Schlüsselschalter-Zone: Der Kommunikator liest die Ereignisse vom Bus der Zentrale, die Ausgänge I/O 1–3 schalten die Schlüsselschalter-Zone der Bereiche 1–3 der Zentrale.

- Auf der Seite **System settings** von TrikdisConfig muss **Remote Arm/Disarm leer** bleiben – beides gleichzeitig ist nicht nutzbar.
- Die Schlüsselschalter-Zone kann impulsgesteuert oder zweistellig sein; in der App Protegus 2 muss derselbe Modus eingestellt werden (Punkt 5.3).
- Bei der **Hardware-Version 3** können die zwei Ausgänge (OUT1, OUT2) zwei Bereiche steuern; das Feld **System settings → Output OUT1 & OUT2 mode** muss auf **Remote control** (Werkseinstellung) stehen.

Über die Einzelheiten und Stolperfallen des Scharfschaltens per Schlüsselschalter berichtet ein eigener Artikel: Scharfschalten aus der Ferne per Schlüsselschalter in der App Protegus 2.

3.5 Anschluss der Eingänge

Die I/O-Klemmen des Kommunikators können als Eingänge auch weitere Melder aufnehmen (z. B. Sabotagekontakt, Paniktaster, Temperaturschalter), unabhängig von der Alarmzentrale. Der Eingang wird zwischen der gewählten I/O-Klemme und der Klemme COM angeschlossen.

Die Eingänge akzeptieren die folgenden Schleifentypen: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Der Abschlusswiderstand beträgt **2,2 kΩ**. Beim einfachen Abschluss (EOL) gelten Kurzschluss und Unterbrechung gleichermaßen als Alarm; der doppelte Abschluss (DEOL) mit zwei Widerständen erkennt Alarm und Sabotage (Kurzschluss oder Unterbrechung) getrennt. Die Werkseinstellung ist NO (im Ruhezustand offen); den Eingangstyp stellen Sie in TrikdisConfig auf der Seite **IN/OUT** entsprechend der Verdrahtung ein.

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

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

Anschluss der Eingangskreise: Typen NO, NC, NC/EOL, NO/EOL, NO/DEOL und NC/DEOL mit Abschlusswiderstand 2,2 kΩ; bei den DEOL-Typen ist auch der Sabotagekreis angeschlossen.

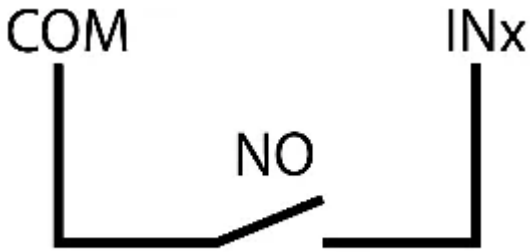


Abbildung 20. NO – im Ruhezustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

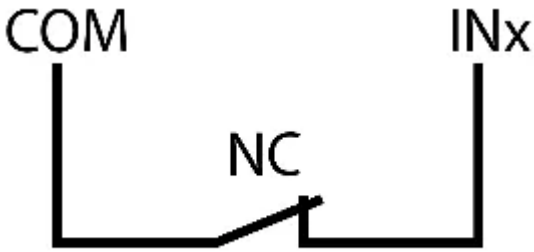


Abbildung 21. NC – im Ruhezustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

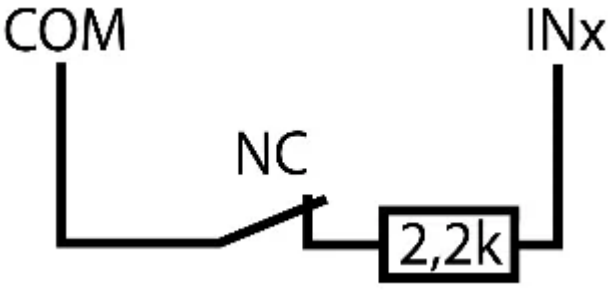


Abbildung 22. NC/EOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

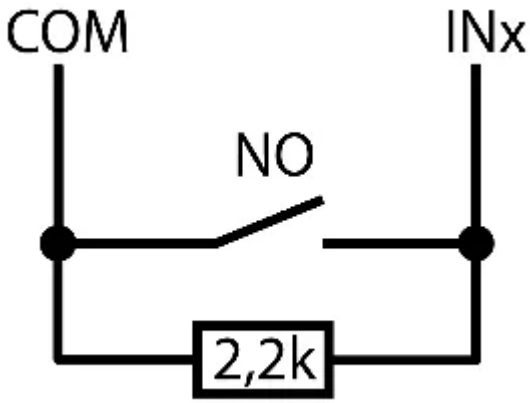


Abbildung 23. NO/EOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

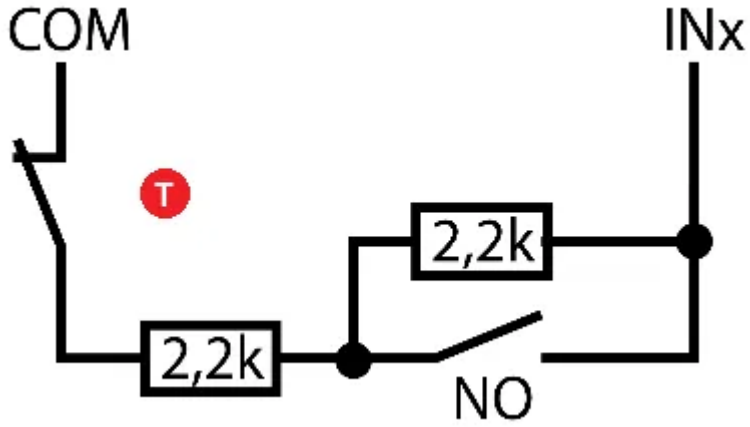


Abbildung 24. NO/DEOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

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

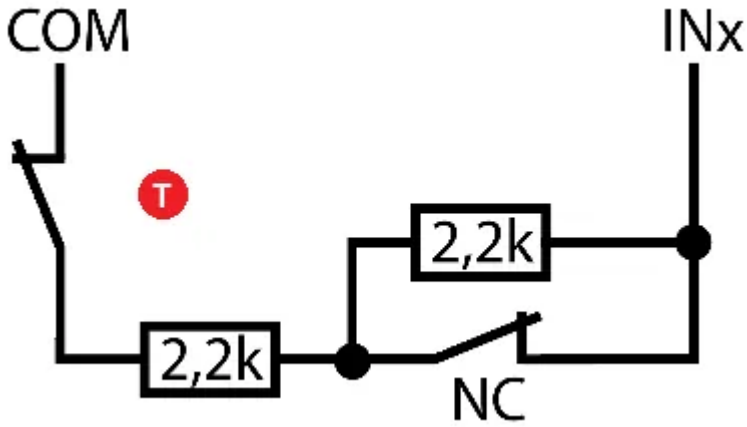


Abbildung 25. NC/DEOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

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

Die **Hardware-Version 3** hat einen Eingang (IN); seinen Typ stellen Sie im Feld **System settings → Input IN type** ein.

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 negativ, mit höchstens 0,15 A, bis 30 V DC. Größere Verbraucher oder Geräte mit Netzspannung schalten Sie **über ein Relais**: Ein Ende der Relaisspule kommt an +DC, das andere an die I/O-Klemme. Mit den Kontakten des Relais lassen sich verschiedene elektrische Geräte ein- und ausschalten. Die I/O-Klemme muss dazu auf der Seite **IN/OUT** von TrikdisConfig als Ausgang (**OUT**) eingestellt werden (Punkt 6.6).

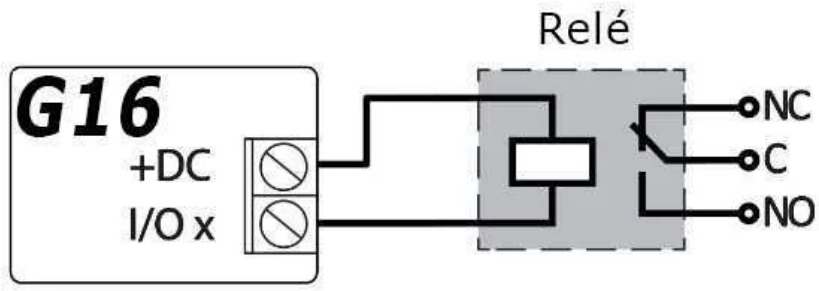


Abbildung 26. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule kommt zwischen +DC und die Klemme I/O x, die Kontakte (NC, C, NO) schalten den Verbraucher.

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

3.7 Anschluss des Erweiterungsmoduls iO-8

Werden mehr Ein- oder Ausgänge benötigt, können an den RS485-Bus der **4G-Variante** 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 und B des Moduls, die Versorgung des Moduls nehmen Sie vom 12-V-AUX-Ausgang der Zentrale. Die Art des Anschlusses beschreibt auch die eigene Anleitung des iO-8. Das Modul muss auf der Seite **RS485 modules** von TrikdisConfig hinzugefügt werden (Punkt 6.7); die Ereignisse der Eingänge gehen an die Leitstelle und an Protegus 2, die Ausgänge sind in der App schaltbar.

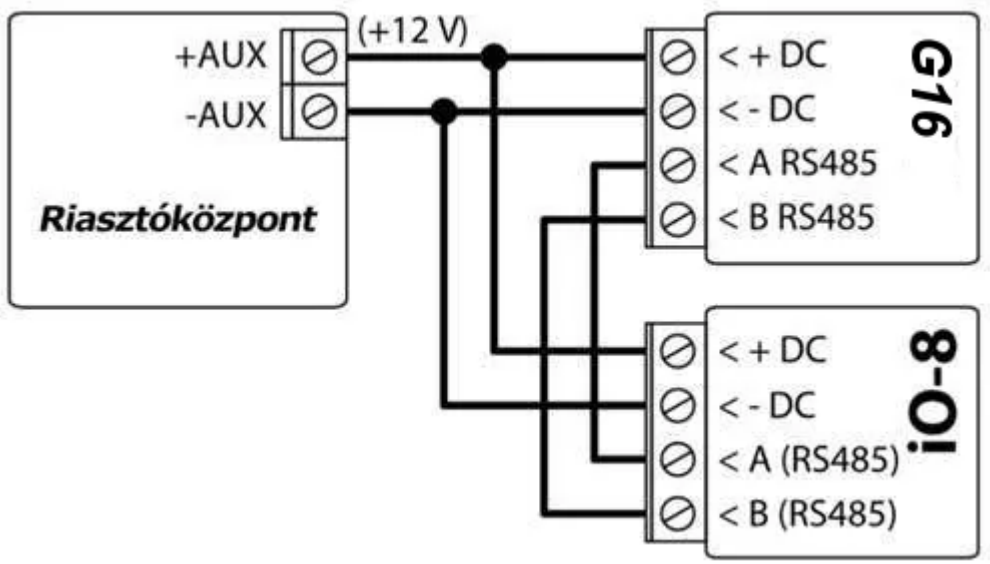


Abbildung 27. Anschluss des Erweiterungsmoduls iO-8 an den RS485-Bus des G16 (A 485 → A, B 485 → B); beide Geräte werden vom AUX-Ausgang der Alarmzentrale (+12 V) versorgt.

Der G16 mit 2G-Modem (G16_G410) hat keinen RS485-Bus, daher können an ihn keine Module iO-8, W485 und E485 angeschlossen werden.

3.8 Anschluss der Module W485 und E485

Ethernet- oder WLAN-Erweiterung – W485 und E485. Der Kommunikator lässt sich mit dem WLAN-Modul W485 oder dem Ethernet-Modul E485 ergänzen: Die Ereignisse gehen dann über kabelgebundenes Internet oder WLAN an die Leitstelle und an die Protegus-2-App.

- **Anschluss:** über den RS485-Bus, aus derselben Versorgung wie der Kommunikator (Versorgungseingang des Moduls 9–28 V DC); ein eigenes Netzteil ist nicht nötig.
- **Das Internet ist der primäre Kanal:** Solange es verfügbar ist, läuft alles darüber. Fällt es aus, wechselt der Kommunikator selbsttätig auf das Mobilfunknetz und kehrt auf IP zurück, sobald das Internet wieder da ist.
- **Nicht nur Alarmübertragung:** Auch die Protegus-2-App (Benachrichtigungen, Fernsteuerung) funktioniert über diesen Kanal.
- **E485** – kabelgebundenes Ethernet (RJ45). **W485** – WLAN 2,4 GHz (WPA / WPA2), wo kein UTP-Kabel verlegt ist.
- Bei Bedarf auch ohne SIM-Karte nutzbar. Einstellung: mit der Software TrikdisConfig, über USB.

Trikdis E485 Ethernet -Modul (RS485) **Trikdis W485 WiFi -Modul (RS485)**

Solange die WLAN- bzw. Ethernet-Verbindung besteht, kommuniziert der G16 darüber und nutzt die mobile Datenverbindung nicht; bricht die Verbindung ab, wechselt er zur mobilen Datenverbindung und kehrt nach Wiederherstellung der Verbindung zum Modul zurück. Damit das Modul funktioniert, **muss im G16 eine SIM-Karte stecken**.

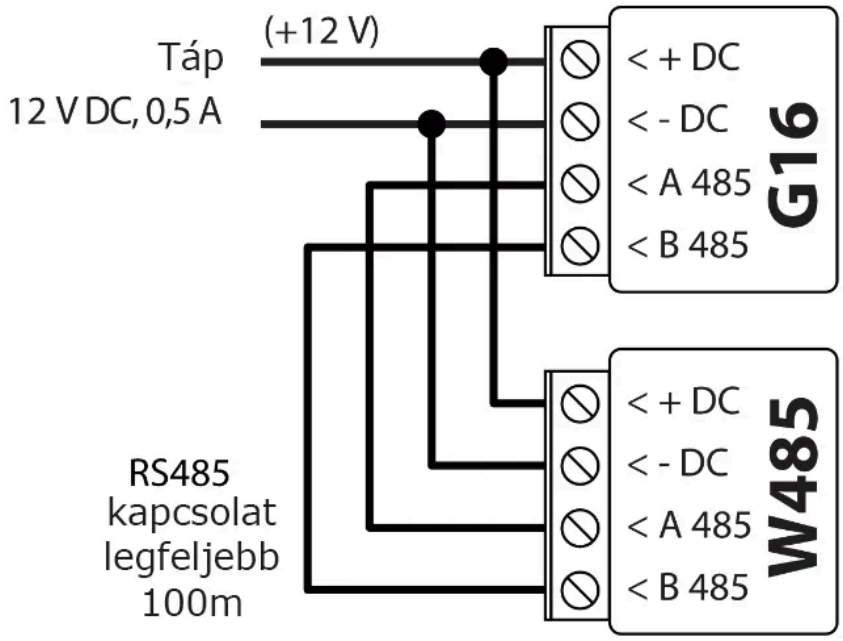


Abbildung 28. Anschluss des WiFi-Moduls W485 an den G16 über den RS485-Bus. Die beiden Geräte laufen an einer gemeinsamen 12-V-DC-Versorgung (mindestens 0,5 A) (Versorgungseingang des Moduls 9–28 V DC); das RS485-Kabel darf höchstens 100 m lang sein.

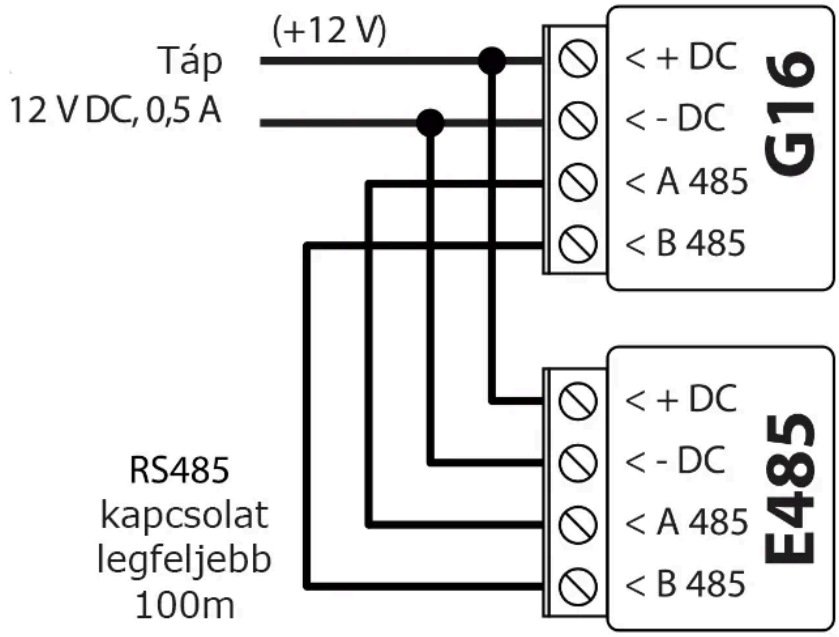


Abbildung 29. Anschluss des Ethernet-Moduls E485 an den G16 über den RS485-Bus. Die beiden Geräte laufen an einer gemeinsamen 12-V-DC-Versorgung (mindestens 0,5 A) (Versorgungseingang des Moduls 9–28 V DC); das RS485-Kabel darf höchstens 100 m lang sein.

Die Entfernungsangaben „bis … m“ sind theoretische Höchstwerte, die unter idealen Bedingungen erreichbar sind. In der Praxis ergeben Qualität und Verlegung des Kabels, Störquellen und bei Funkverbindungen Wände und Gelände eine deutlich geringere Reichweite. Planen Sie mit Reserve, und prüfen Sie bei langen Strecken die Verbindung bei der Inbetriebnahme.

Die Netzwerkeinstellungen der Module nehmen Sie auf der Seite **RS485 modules** von TrikdisConfig vor (Punkt 6.7).

3.9 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 Alarmzentrale auch der Kommunikator. Auf der Frontseite 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 Blinkimpulse ist die Signalstärke (bei 2G sind 5, bei 4G 3 gut);
- **TROUBLE** ist aus.

Gibt die LED NETWORK weniger gelbe Blinkimpulse, ist die Signalstärke nicht ausreichend: Suchen Sie für den Kommunikator einen anderen Ort oder verwenden Sie eine empfindlichere Antenne (Punkt 3.2). Jede davon abweichende LED-Anzeige weist auf einen Fehler hin – bestimmen Sie ihn anhand der Tabellen in Punkt 1.7. Blinkt TROUBLE, nennt die Zahl der Blinkimpulse die Ursache (Punkt 1.7). **7 Blinkimpulse** zeigen eine fehlende Verbindung zur Zentrale an: Prüfen Sie die Leitungen CLK und DATA, den gewählten Zentralentyp und – wo nötig – die Programmierung der Zentrale (Kapitel 4). Leuchtet keine LED, prüfen Sie Versorgung und Verdrahtung.

4. Programmierung der Alarmzentrale

Dieses Kapitel beschreibt je Hersteller, was in der Alarmzentrale eingestellt werden muss, damit der G16 die Ereignisse liest und – wo möglich – die Zentrale aus der Ferne steuert. Bei den meisten Zentralen muss für das Lesen der Ereignisse nichts programmiert werden; für die **direkte Steuerung** aktivieren Sie auf der Seite **System settings** von TrikdisConfig die Option **Remote Arm/Disarm**, und bei Paradox- bzw. Texecom-Zentralen geben Sie im Feld **Security panel PC download password** auch das PC- bzw. UDL-Passwort der Zentrale ein (Punkte 2.2 und 6.2).

Wenn Sie die Zentrale nicht direkt, sondern über eine Schlüsselschalter-Zone steuern (Punkt 3.4), bleibt **Remote Arm/Disarm** leer, und dieses Kapitel betrifft nur die für das Lesen der Ereignisse nötigen Einstellungen.

4.1 DSC

Die Zentralen **DSC PowerSeries** (Liste der unterstützten Typen in Punkt 1.2) erfordern keinerlei besondere Einstellung: Der am Keybus angeschlossene Kommunikator liest die Ereignisse sofort, und nach dem Setzen des Häkchens bei **Remote Arm/Disarm** schaltet der Benutzer mit seinem eigenen Bedienteilcode aus der

App scharf und unscharf. Die Details der direkten Steuerung – Zonenzustände, Zonensperrung, automatische Erkennung der Bereiche – behandelt ein eigener Artikel: Direkte Steuerung für DSC-PowerSeries-Alarmzentralen.

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

4.2 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.

4.3 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]**.

4.4 UTC Interlogix (Caddx)

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

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

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

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

4.5 Crow und Pyronix

Die Zentralen **Crow Runner 4/8** und **Runner 8/16** erfordern keinerlei besondere Einstellung.

Auch die **Pyronix**-Zentralen erfordern keine Programmierung, aber nach Einstellung und Anschluss des Kommunikators **trennen Sie die Zentrale von der Stromversorgung** (Netz und Akku) und starten Sie sie neu: Die Zentrale akzeptiert den an ihren Bus angeschlossenen Kommunikator beim Start.

4.6 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]**.

4.7 InnerRange Inception und Integriti

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.

Inception und Integriti übergeben dem Kommunikator die Ereignisse; für das Scharf- und Unscharfschalten ist eine Schlüsselschalter-Zone nötig (Punkte 1.2 und 3.4).

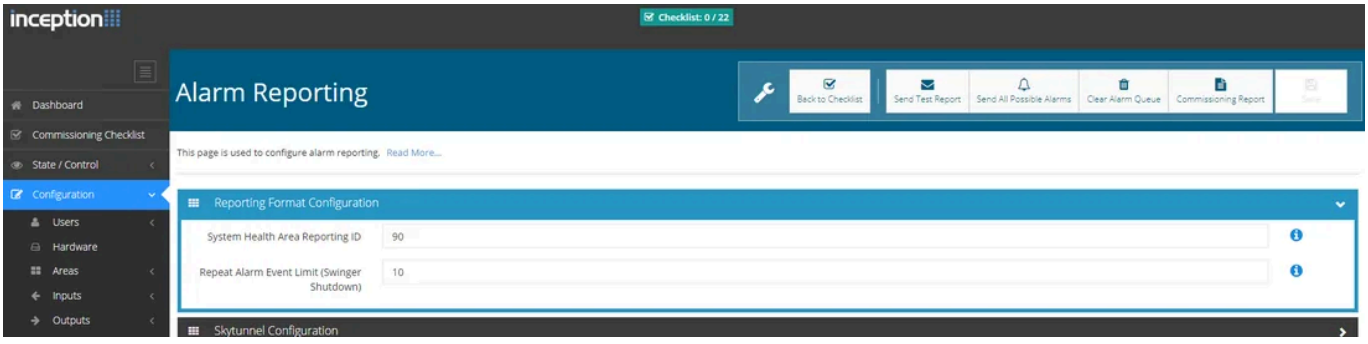


Abbildung 30. Weboberfläche der Inception – Configuration → General → Alarm Reporting.



Abbildung 31. Inception – 3rd Party Device Configuration.

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

5. Fernsteuerung mit der App Protegus 2

Mit der mobilen und Web-App Protegus 2 sieht der Benutzer den Zustand des Systems aus der Ferne, erhält Benachrichtigungen über Ereignisse, kann scharf- und unscharfschalten und die Ausgänge des Kommunikators schalten. Beim G16 kann das Scharfschalten auf zwei Arten erfolgen: bei den **direkt steuerbaren** Zentralen mit dem eigenen **Bedienteilcode** des Benutzers, bei Zentralen mit angeschlossener Schlüsselschalter-Zone mit einem **Ausgang** des Kommunikators.

5.1 Gerät hinzufügen

Prüfen Sie vor dem Hinzufügen des Geräts:

1. Die SIM-Karte ist aktiv, und die mobile Datenverbindung funktioniert darauf; ihr PIN-Code ist im Gerät eingetragen, oder die PIN-Abfrage ist ausgeschaltet.
2. Auf der Seite **User reporting** → **PROTEGUS Cloud** von TrikdisConfig ist **Enable connection** angehakt, und der **Protegus Cloud access code** ist eingestellt (nach dem Anlegen des Systems kann er nicht mehr geändert werden).
3. Die LED **POWER** leuchtet grün, die LED **NETWORK** leuchtet grün und blinkt gelb.

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

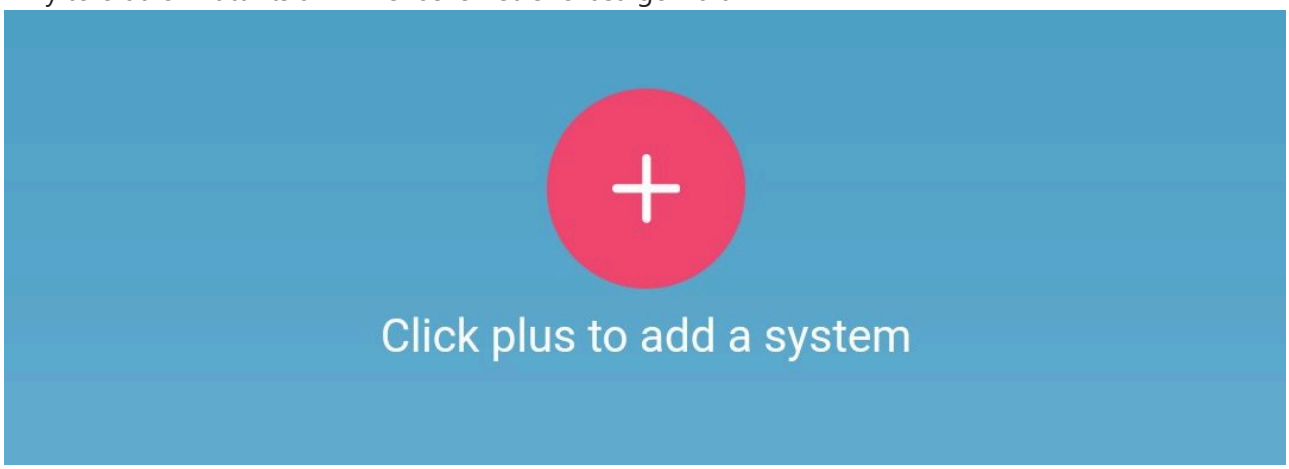
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

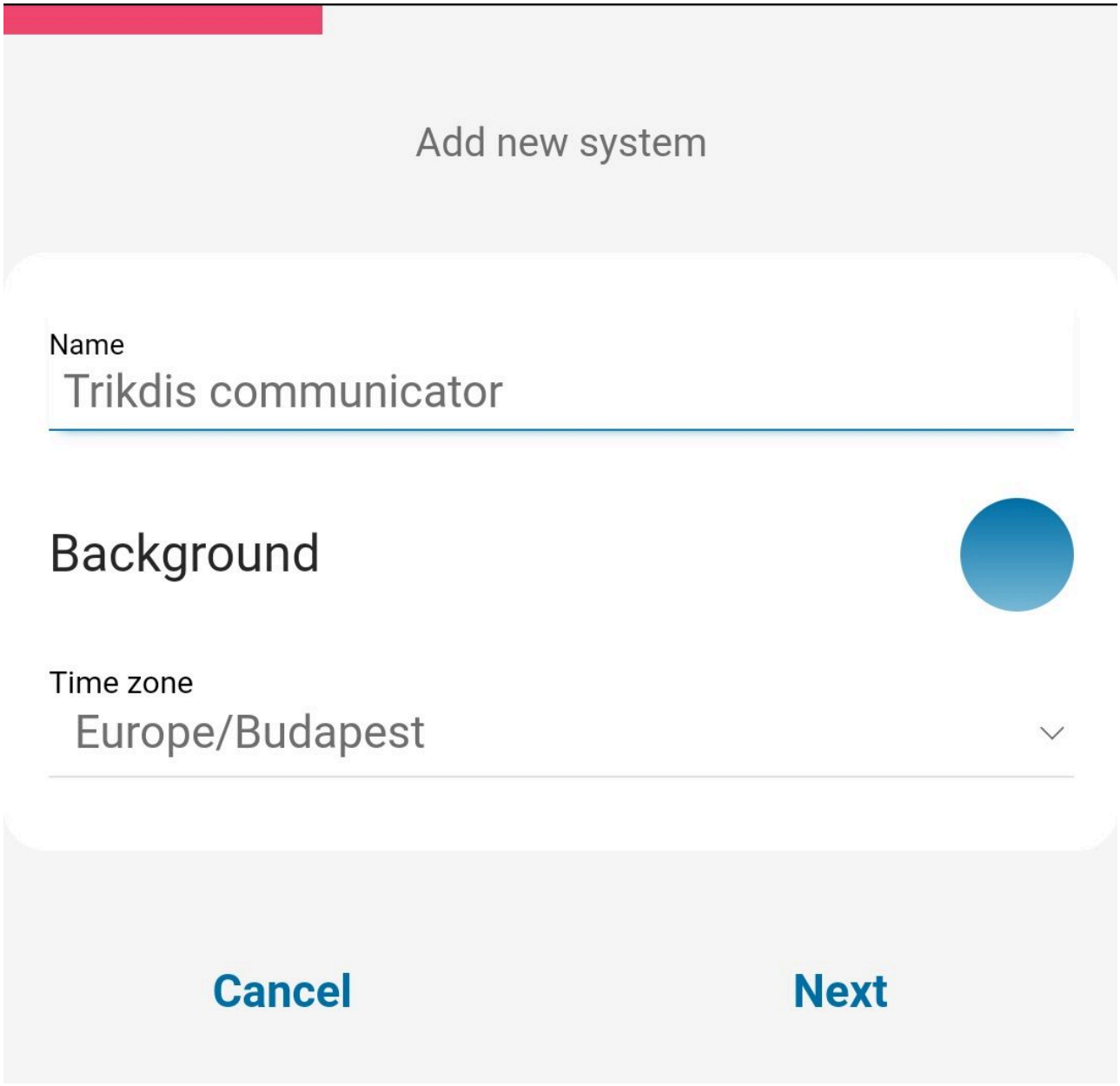
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



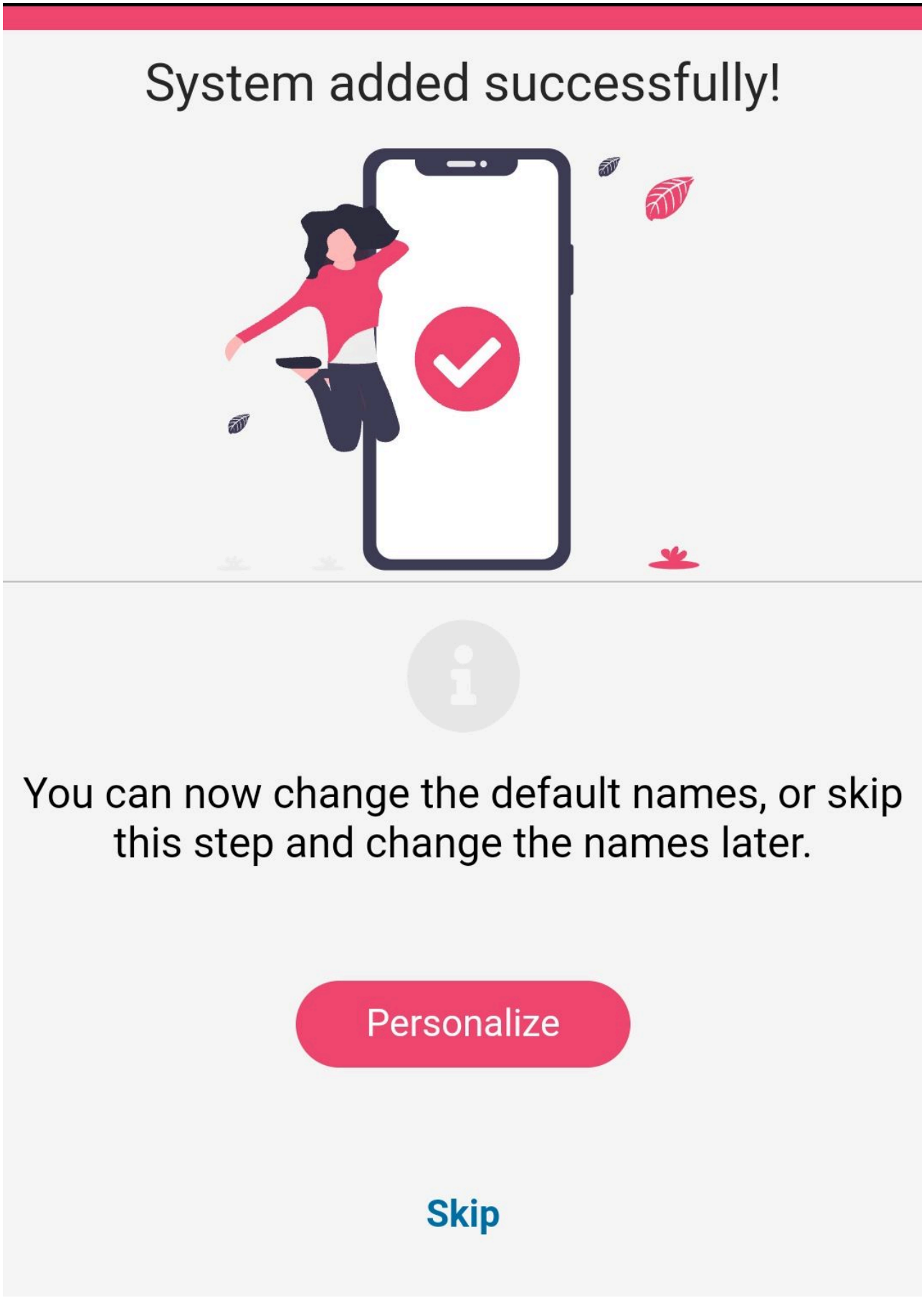
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



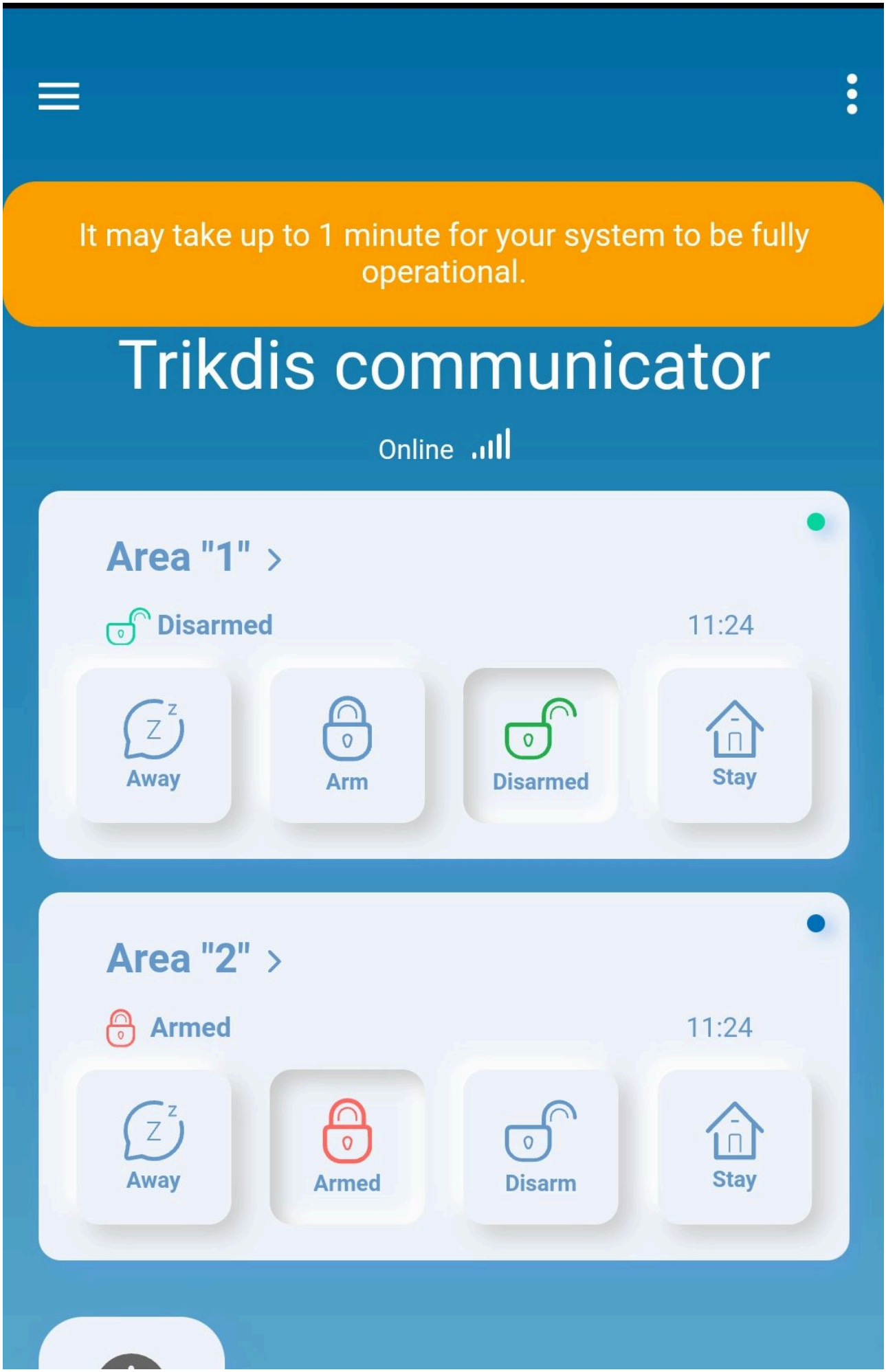
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Die eindeutige Kennung des Geräts (**IMEI**) steht auf der Verpackung und auf der Rückseite des Geräts, und auch die Statusleiste von TrikdisConfig zeigt sie an.

5.2 Direkte Steuerung mit dem Bedienteilcode

Gehört die Zentrale zu den direkt steuerbaren Typen (Punkt 1.2) und ist auf der Seite **System settings** von TrikdisConfig **Remote Arm/Disarm** angehakt, zeigt Protegus 2 die Bereiche der Zentrale mit dem vom Bus gelesenen Zustand, und zum Scharf- / Unscharfschalten gibt der Benutzer in der App **den Bedienteilcode der Zentrale** ein – denselben, den er am Bedienteil verwendet. Ein eigener Ausgang und eine Schlüsselschalter-Zone sind nicht nötig.

- In der Zentrale ist dafür je nach Hersteller eine Einstellung nötig (Paradox: PC-Passwort, Texecom: UDL-Passwort; bei Caddx-, Honeywell- und InnerRange-Zentralen die Freigabe des Busses bzw. der seriellen Schnittstelle bereits für das Lesen der Ereignisse) – siehe Kapitel 4.
- Den Bedienteilcode prüft die Zentrale, und auch das Ereignisprotokoll der Zentrale verzeichnet den Benutzer, nicht den Kommunikator.
- Bei Paradox-Zentralen darf der Code des Benutzers **nicht der Mastercode sein**; starten Sie den Kommunikator nach einer Codeänderung neu (Punkt 4.2).
- Bei DSC-PowerSeries-Zentralen zeigt die App auch den Zustand der Zonen, und auch das Sperren von Zonen ist möglich – Einzelheiten im Artikel über die direkte Steuerung von DSC.

Beim Anlegen des Systems fragt Protegus 2, ob das Scharfschalten von einem Ausgang des Kommunikators gesteuert wird. Bei direkter Steuerung ordnen Sie dem Bereich **keinen** Ausgang zu (**Control with Protegus2** ausgeschaltet): Den Bereich verwaltet die Zentrale, der Zustand kommt vom Bus.

5.3 Scharfschalten über eine Schlüsselschalter-Zone

Ist die Zentrale nicht direkt steuerbar oder möchten Sie sie nicht so nutzen, schließen Sie einen Ausgang des Kommunikators an die Schlüsselschalter-Zone der Zentrale an (Punkt 3.4), in TrikdisConfig bleibt **Remote Arm/Disarm** leer, und in Protegus 2 ordnen Sie dem Bereich den Ausgang zu.

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.

5.4 Scharf- und Unscharfschalten in 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.

Bei direkter Steuerung verlangt die App den Bedienteilcode der Zentrale; beim Scharfschalten per Schlüsselschalter – falls eingeschaltet – das Passwort von Protegus 2.

5.5 Steuerung per SMS

Der Kommunikator kann auch per SMS gesteuert und programmiert werden. Aufbau der Nachricht:

`PASSWORT Leerzeichen BEFEHL Leerzeichen DATEN` – zum Beispiel `123456 OUTPUT1 ON`

Mit dem **Administrator**-Passwort sind alle Befehle verfügbar, mit dem **Installateur**-Passwort die Befehle INFO, RESET und OUTPUTx. `x` ist die Nummer des Ausgangs: die als Ausgang eingestellte I/O-Klemme (1, 2 oder 3), die Sie schalten möchten.

Befehl	Daten	Funktion	Beispiel
`INFO`	–	Fragt Informationen zum Gerät ab: Typ, IMEI, Seriennummer, Firmwareversion	`123456 INFO`
`RESET`	–	Startet das Gerät neu	`123456 RESET`
`OUTPUTx`	`ON`	Schaltet Ausgang x ein	`123456 OUTPUT1 ON`

Befehl	Daten	Funktion	Beispiel
`OUTPUTx`	`OFF`	Schaltet Ausgang x aus	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Gibt an Ausgang x einen Impuls aus; `tttt` = Impulslänge in Sekunden, vierstellig	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Aktiviert bzw. deaktiviert die Protegus-Verbindung	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adresse:port`	IP-Adresse und Port des primären Kanals	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=schlüssel`	Der TRK-Verschlüsselungsschlüssel	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=name`	Der APN der SIM-Karte	`123456 CONNECT APN=internet`
`CONNECT`	`USER=name`	APN-Benutzername (falls vom Anbieter verlangt)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=passwort`	APN-Passwort (falls vom Anbieter verlangt)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Auswahl des Typs der Alarmzentrale über die laufende Nummer in der Liste **Security panel model** von TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=pppp` / `DIR=OFF`	Das 4-stellige Passwort der direkten Steuerung (das PC- bzw. UDL-Passwort der Zentrale); `DIR=OFF` deaktiviert sie	`123456 CONNECT DIR=1122`

Sie können einschränken, von welchen Telefonnummern das Gerät Befehle annimmt: TrikdisConfig → Seite **User reporting** → **Control by SMS**. Ist keine einzige Nummer eingetragen, führt es Befehle mit korrektem Passwort von jeder beliebigen Nummer aus.

6. TrikdisConfig – die Einstellungen im Detail

Im Fenster von TrikdisConfig sehen Sie links die Liste der Seiten (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), oben die Schaltflächenleiste (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), unten die Statusleiste. Dieses Kapitel geht die Einstellungen des G16 Seite für Seite durch.

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.

Beschriftung	Bedeutung
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.

Im Feld **Device** muss beim G16 die Typbezeichnung des G16 stehen (zum Beispiel G16_G410 oder G16_54E0). Nach dem Auslesen zeigt das Programm die im G16 gespeicherten Einstellungen; stellen Sie diese gemäß den folgenden Seitenbeschreibungen ein.



Abbildung 32. Die Statusleiste von TrikdisConfig mit ausgelesenem G16: Kennung, Zustand, Typ, Seriennummer, Versionen, Verbindungsart und Zugriffsebene.

6.2 System settings

Die Seite besteht aus zwei Gruppen: In der Gruppe **General** stellen Sie die grundlegende Funktion des Geräts und seine Verbindung mit der Alarmzentrale ein, in der Gruppe **Access** die Zugriffsebenen.

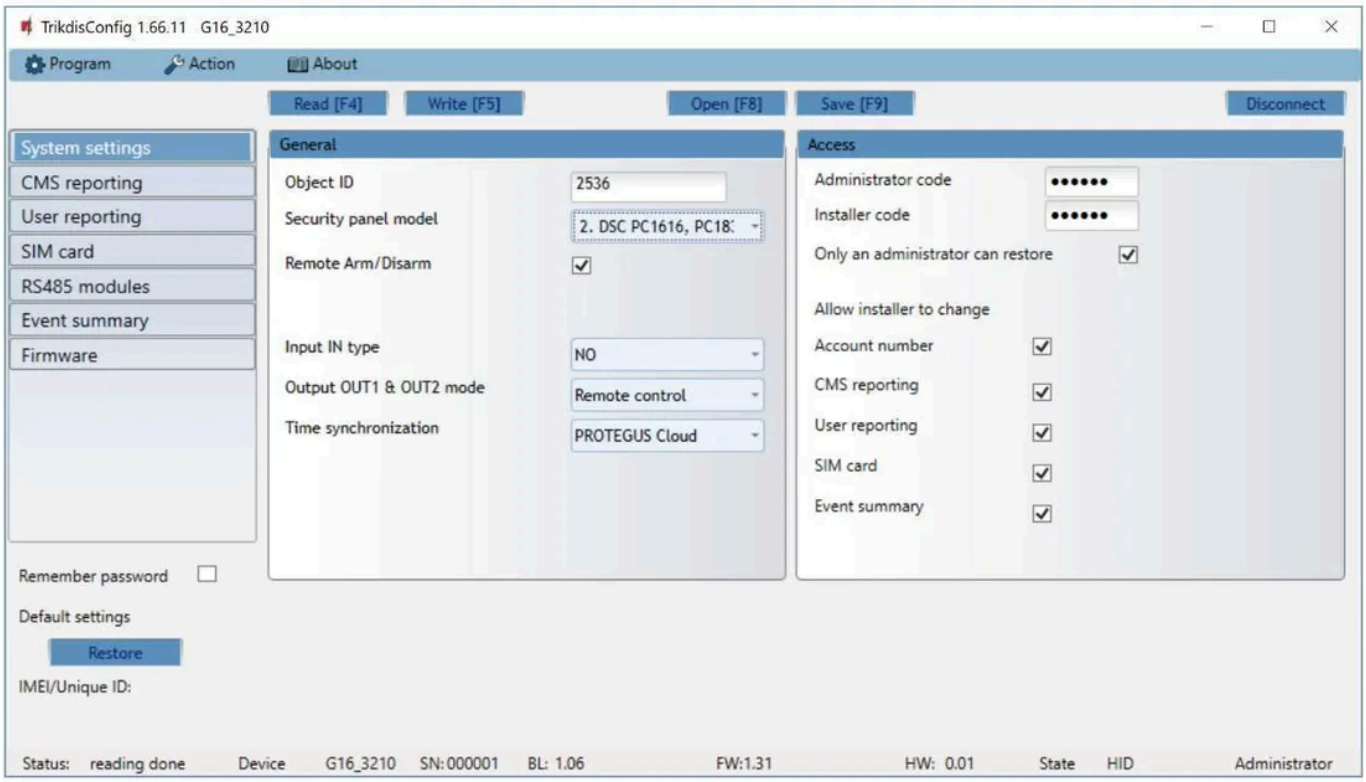


Abbildung 33. TrikdisConfig – Seite System settings: Gruppen General und Access (im Bild die Hardware-Version 3, G16_3210; bei der Version 4 gibt es die Felder Input IN type und Output OUT1 & OUT2 mode nicht, sie sind auf die Seite IN/OUT gewandert).

- **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen, 0–9, A–F). Pflichtfeld, wenn das Gerät auch an eine Leitstelle meldet; `FFFE` und `FFFF` sind nicht zulässig.
- **Security panel model** – der Typ der angeschlossenen Alarmzentrale aus der Liste. Davon hängt ab, wie der Kommunikator den Bus liest, wählen Sie daher den genauen Typ der angeschlossenen Zentrale.
- **Remote Arm/Disarm** – angehakt steuert der Kommunikator die Zentrale direkt: Der Benutzer schaltet in Protegus 2 mit seinem Bedienteilcode scharf und unscharf. Erscheint nur bei den direkt steuerbaren Zentralentypen; in der Zentrale ist dafür je nach Hersteller eine Einstellung nötig (Kapitel 4). Beim Scharfschalten über eine Schlüsselschalter-Zone lassen Sie es leer.
- **Security panel PC download password** – für die direkte Steuerung von Paradox- und Texecom-Zentralen das PC- bzw. UDL-Passwort der Zentrale (4 Zeichen); es muss mit dem in der Zentrale eingestellten übereinstimmen (Punkte 4.2 und 4.3).
- **Time set** – die Quelle der Uhr des Geräts (Standard **Cloud application**, die Protegus-Cloud).
- Bei der **Hardware-Version 3** befinden sich hier außerdem die Felder **Input IN type** (Typ des Eingangs: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) und **Output OUT1 & OUT2 mode** (Modus der beiden Ausgänge; für das Scharfschalten per Schlüsselschalter **Remote control**).

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 CMS reporting

Der Kommunikator sendet die Ereignisse über die mobile Datenverbindung (IP) oder per SMS an die Leitstelle. Die Ereignisse können über mehrere Kanäle gehen: Der **primäre** und der **parallele** Kanal arbeiten gleichzeitig (an zwei Empfänger gleichzeitig), und zu beiden gehört ein **Ersatzkanal**, der in Kraft tritt, wenn der jeweilige Kanal abbricht. Die Kommunikation ist verschlüsselt und passwortgeschützt; für den Empfang ist ein Trikdis-Empfänger (Software-Empfänger IPcom, RL14, RM14) oder ein universeller Empfänger nötig, der das Protokoll DC-09 / TL150 beherrscht. Die Trikdis-Empfänger leiten die Ereignisse an die Leitstellensoftware weiter: über IP der Software-Empfänger **IPcom** (Windows / Linux), der IP/SMS-Empfänger **RL14** oder der Mehrkanal-Empfänger **RM14**; für den Empfang von SMS der RL14, der RM14 oder der SMS-Empfänger **GM14**.

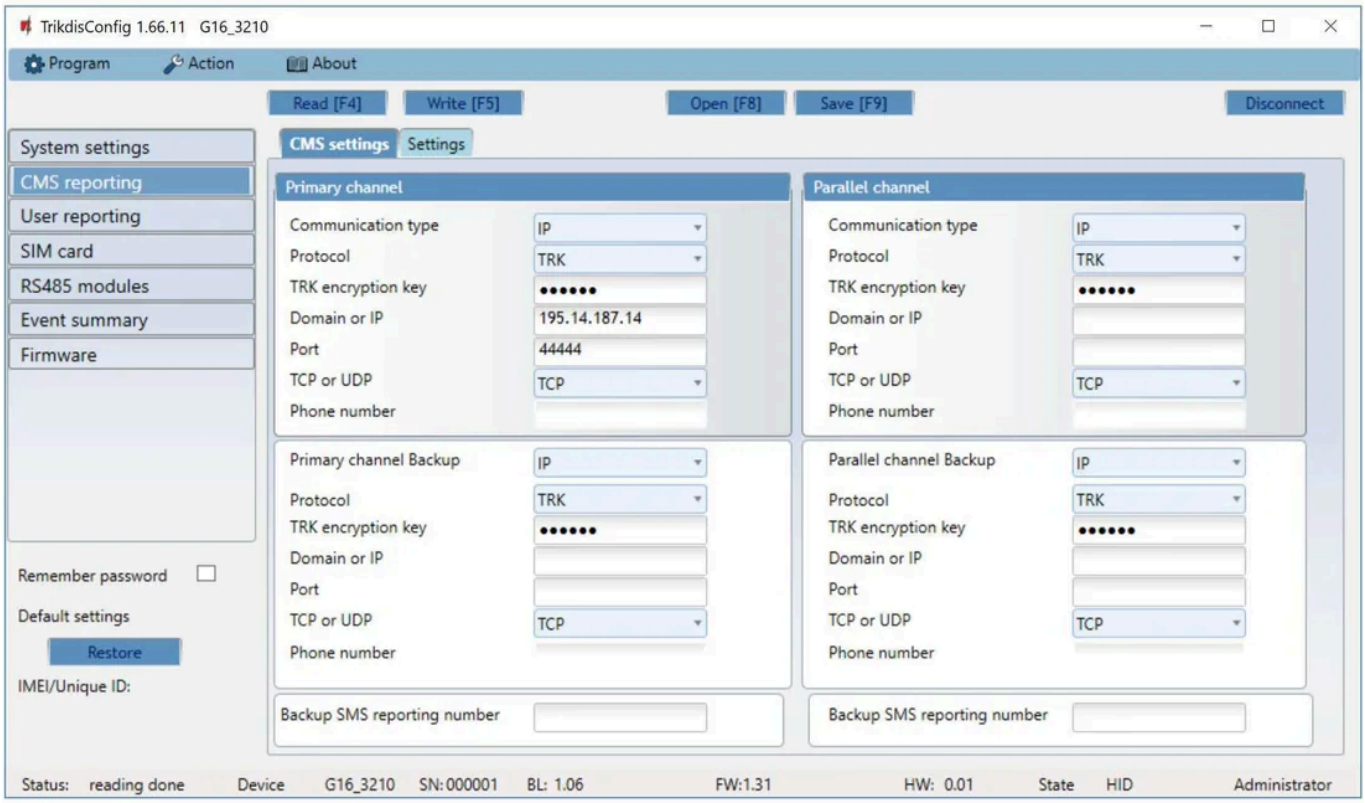


Abbildung 34. TrikdisConfig – CMS reporting, Reiter CMS settings: primärer, Ersatz- und paralleler Kanal.

Primary channel – primärer Kanal

- **Communication type** – IP oder SMS. SMS eignet sich als Reserve – es funktioniert auch ohne mobile Datenverbindung –, als primärer Kanal wird es nicht empfohlen.

- **Protocol** – TRK (Trikdis-Empfänger), DC-09_2007 oder DC-09_2012 (universelle Empfänger), TL150 (SUR-GARD).
- **TRK encryption key** – 6-stelliger Verschlüsselungsschlüssel; im Kommunikator und im Empfänger muss derselbe stehen.
- **Domain or IP**, **Port** – Adresse und Port des Empfängers.
- **TCP or UDP** – das Übertragungsprotokoll.
- **Phone number** – nur bei SMS-Kommunikation: die Telefonnummer des Trikdis-SMS-Empfängers mit Landesvorwahl (z. B. `CCxxxxxxxxx`, wobei CC die Landesvorwahl ist).

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

Parallel channel – paralleler Kanal. Sendet neben dem primären gleichzeitig an einen zweiten Empfänger (zum Beispiel an die örtliche und die zentrale Leitstelle). Er hat einen eigenen Ersatzkanal.

Backup SMS reporting number – Ersatz-SMS-Nummer. Tritt in Kraft, wenn das Senden weder über den primären noch über den parallelen noch über den Ersatzkanal gelingt; sie ist nützlich, weil sie auch ohne IP-Verbindung funktioniert. Sie ist nur aktiv, wenn der primäre und der Ersatzkanal im IP-Modus sind. Das Gerät sendet eine SMS an den SMS-Empfänger der Leitstelle nach dem ersten Start sowie dann, wenn die TCP/IP- oder UDP/IP-Verbindung sowohl auf dem primären Kanal als auch auf dessen Ersatzkanal abbricht. Tragen Sie in das Feld die Telefonnummer des Trikdis-SMS-Empfängers der Leitstelle mit Landesvorwahl ein (z. B. `CCxxxxxxxxx`).

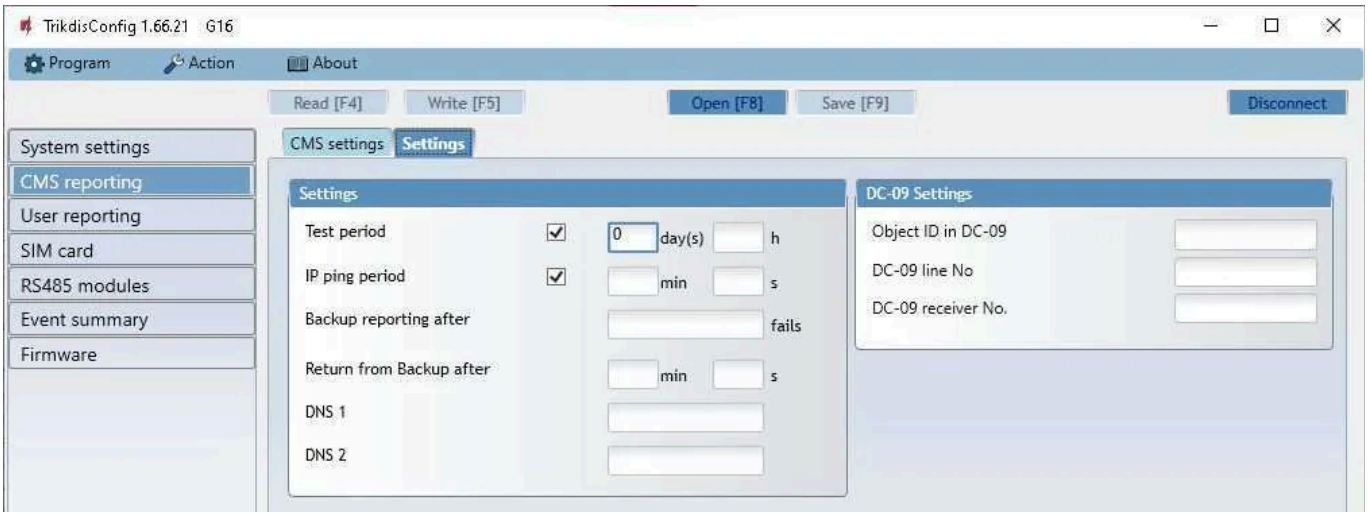


Abbildung 35. TrikdisConfig – CMS reporting, Reiter Settings: Testmeldung, PING, Zeitvorgaben des Ersatzkanals, DNS und die DC-09-Daten.

Im Reiter **Settings** stellen Sie die Zeitvorgaben 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.

Am unteren Rand des Reiters: **DNS 1, DNS 2** – Nameserver; sie werden benötigt, wenn Sie den Empfänger mit einem Domainnamen und nicht mit einer IP-Adresse angegeben haben. Standard ist der öffentliche DNS von Google. Die Gruppe **DC-09 settings** ist nur sichtbar, wenn auf einem Kanal das Protokoll DC-09 eingestellt ist.

6.4 User reporting

Im Reiter **PROTEGUS Cloud** geben Sie den Protegus-Dienst frei. Mit dem Protegus-Dienst kann der Benutzer den Kommunikator und das System aus der Ferne überwachen und steuern; weitere Informationen: www.protegus.app.

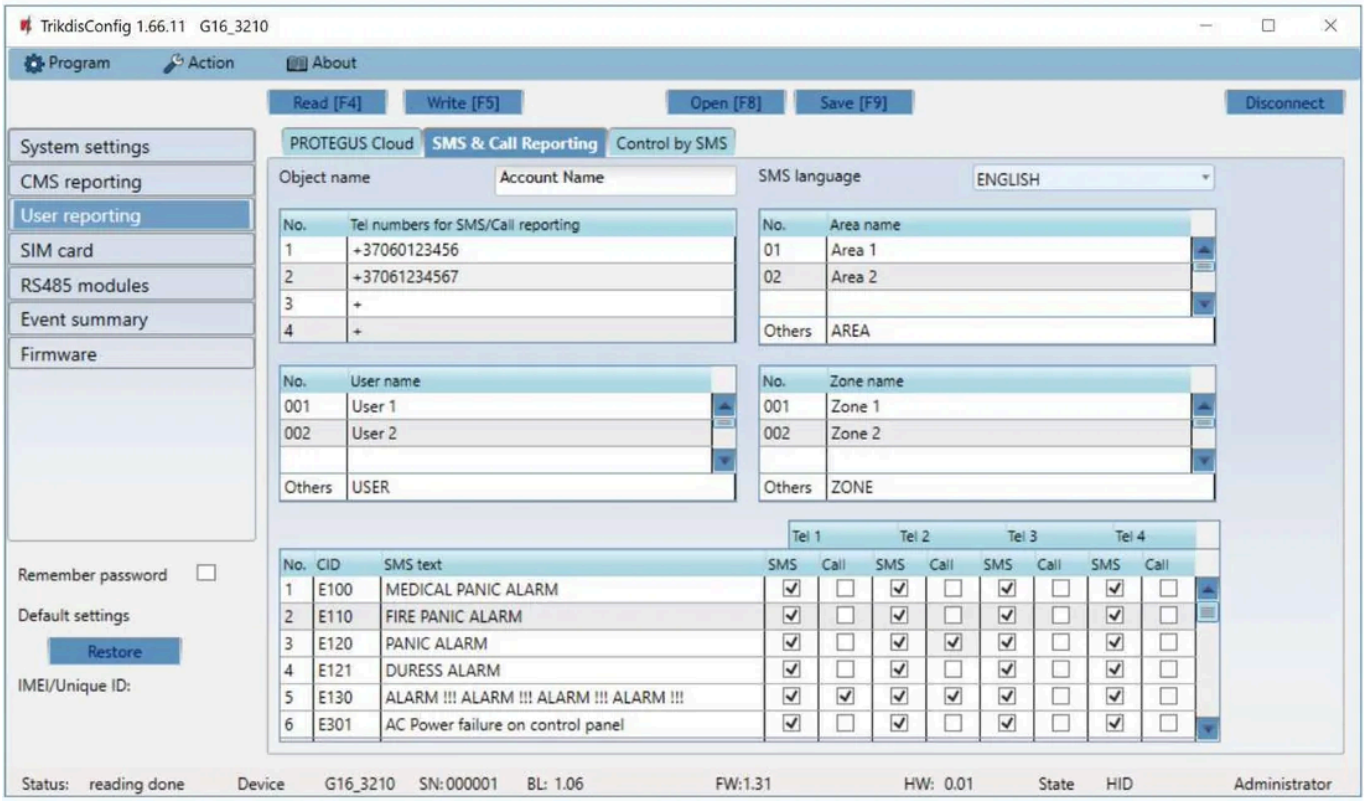


Abbildung 36. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- **Enable connection** – gibt die Verbindung mit der Protegus-Cloud und den Fernzugriff von TrikdisConfig frei.

- **Protegus Cloud access code** – 6-stelliger Code für die Protegus-Verbindung (ab Werk `123456`). Er kann nur vor dem Anlegen des Systems in Protegus 2 eingestellt werden, nachträglich ist er nicht änderbar.

Im Reiter **SMS & Call Reporting** kann der Benutzer auch per SMS oder Anruf 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.

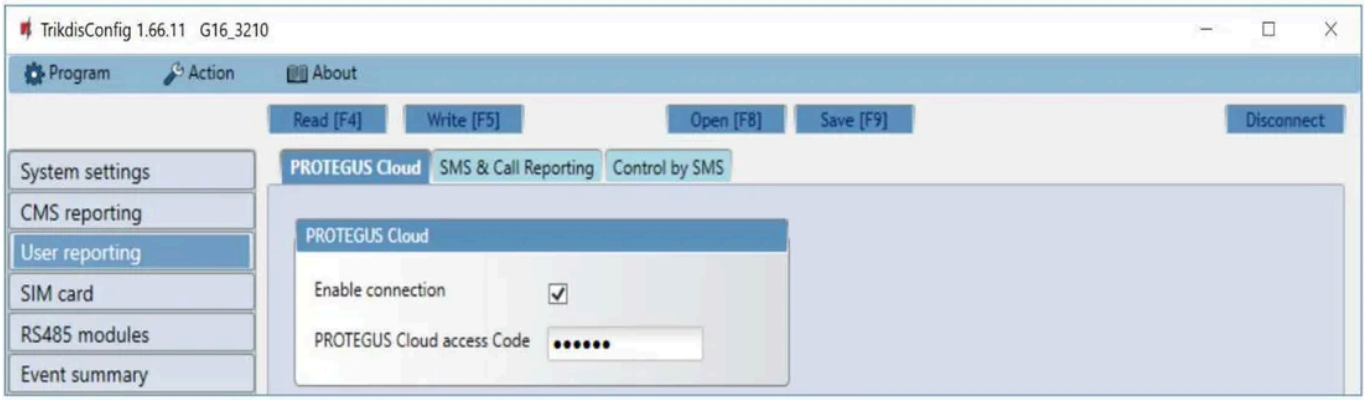


Abbildung 37. TrikdisConfig – User reporting, Reiter SMS & Call Reporting.

- **Object name** – der Name des Systems; er steht in jeder SMS.
- **SMS language** – die Sprache der SMS (für die Sonderzeichen der jeweiligen Sprache).
- **Tel numbers for SMS/Call reporting** – bis zu 4 Telefonnummern mit Landesvorwahl (`+CC…`, `00CC…` oder `CC…`, wobei CC die Landesvorwahl ist).
- **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 entsprechende Tabelle die Nummer des Bereichs, des Benutzers oder der Zone und daneben den Namen ein. Bei einer über den Bus gelesenen Zentrale kommen die eigenen Zonen- und Benutzernummern der Zentrale an; geben Sie für diese die Namen ein.
- **CID event table** – für jedes Ereignis einstellbar, welche Nummer eine SMS oder einen Anruf erhält; Nachrichtentext und Contact-ID-Code sind ebenfalls änderbar, auch ein neues Ereignis kann hinzugefügt werden.

Im Reiter **Control by SMS** stellen Sie den Empfang von SMS-Befehlen ein (die Befehle beschreibt Punkt 5.5).



Abbildung 38. TrikdisConfig – User reporting, Reiter Control by SMS.

- **Reply text** – der Text der vier Antwortnachrichten auf einen SMS-Befehl: erfolgreicher Befehl (Command done), falsches Passwort (Wrong password), falscher Befehl (Wrong command), falsche Daten (Wrong data).
- **Tel numbers for control by SMS** – bis zu 4 Nummern; nur von diesen Nummern nimmt das Gerät Befehle an. Ist das Feld leer, nimmt es einen Befehl mit richtigem Passwort von jeder Nummer an; die Sicherheit gewährleistet auch dann, dass im Befehl das Administrator- oder Errichter-Passwort zwingend ist.

6.5 SIM card

Ohne die Daten der SIM-Karte verbindet sich das Gerät nicht mit dem Datennetz.

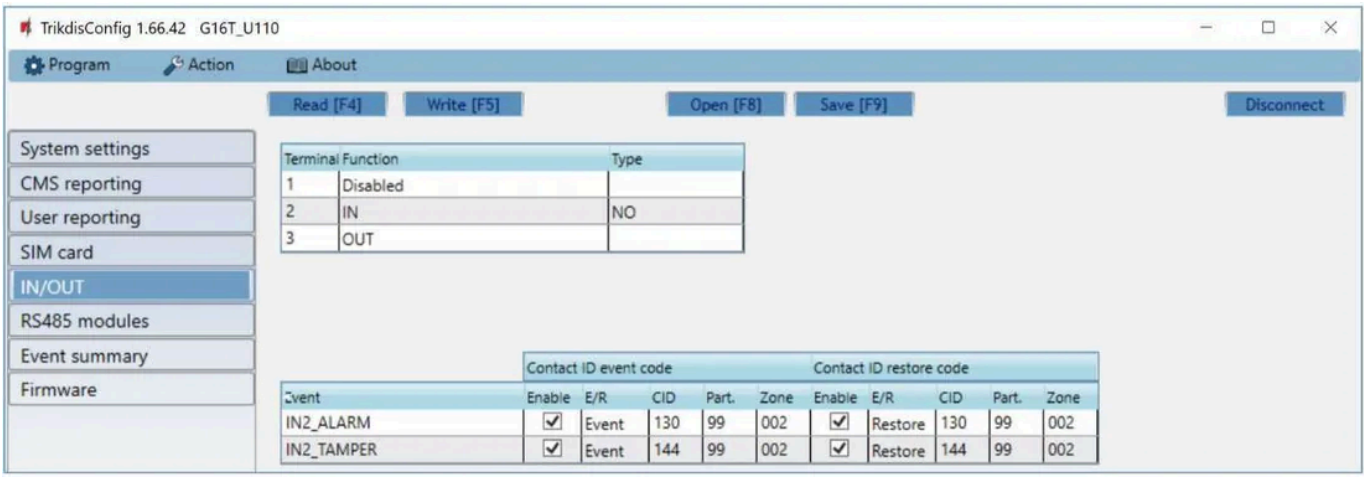


Abbildung 39. TrikdisConfig – Seite SIM card.

- **SIM card PIN** – der PIN-Code der Karte. Die PIN-Abfrage können Sie ausschalten, indem Sie die Karte in ein Mobiltelefon einsetzen und sie dort deaktivieren. Ist die PIN-Abfrage ausgeschaltet, kann der Werkswert des Feldes bleiben.
- **APN** – der Zugangspunkt des Anbieters (Access Point Name); ohne ihn kann sich der Kommunikator nicht mit dem Internet verbinden. Sie finden ihn auch auf der Website des Anbieters; der APN „internet“ ist allgemein und funktioniert in den Netzen vieler Anbieter. Die bekannten APNs der Anbieter listet der APN-Artikel auf (für eine IoT- / M2M-Karte gibt der Anbieter einen eigenen APN an, siehe Punkt 2.3).
- **Login, Password** – APN-Benutzername und -Passwort, falls der Anbieter sie verlangt.
- **Forbid connection when roaming detected** – nützlich in der Nähe einer Landesgrenze: Es verhindert, dass sich das Gerät mit dem Netz des Nachbarlandes verbindet.

Vergewissern Sie sich vor der Nutzung, dass die SIM-Karte aktiv ist und für die IP-Kommunikation der mobile Datendienst darauf freigegeben ist.

6.6 IN/OUT

Hier legen Sie die Rolle der drei I/O-Klemmen mit Doppelfunktion des Kommunikators fest: **Disabled** (nicht verwendet), **IN** (Eingang) oder **OUT** (Ausgang). Bei einem Eingang muss auch der Typ angegeben werden (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Werkseinstellung: I/O 1 nicht verwendet, I/O 2 Eingang (NO), I/O 3 Ausgang.



Abbildung 40. TrikdisConfig – Seite IN/OUT: die Funktion der I/O-Klemmen und die Ereignisse der Eingänge.

Wird der an den Eingang angeschlossene Melder ausgelöst, sendet der Kommunikator ein eigenes Ereignis (**INx_ALARM**, Contact ID 130), wird der Sabotagekreis verletzt, ein Sabotageereignis (**INx_TAMPER**, 144) an die Leitstelle und an Protegus 2; in der Tabelle erscheinen die Ereignisse jeder als Eingang eingestellten Klemme. Die Spalten der Tabelle:

- **Enable** – gibt das Senden der Nachricht frei.
- **E/R** – der Typ des Ereignisses: Event (Alarm) oder Restore (Wiederherstellung).
- **CID** – der Contact-ID-Code.
- **Part.** – die Nummer des Bereichs in der Nachricht.
- **Zone** – die Nummer der Zone in der Nachricht.

Bei der **Hardware-Version 3** gibt es keine Seite IN/OUT: Den Typ des einzigen Eingangs stellen Sie im Feld **System settings** → **Input IN type** ein, den Modus der beiden Ausgänge im Feld **Output OUT1 & OUT2 mode**, und die Ereignisse des Eingangs (IN_ALARM, IN_TAMPER) auf der Seite **Event summary**.

6.7 RS485 modules

Die an den RS485-Bus angeschlossenen Erweiterungsmodule iO-8 und Module W485 / E485 müssen im Reiter **Modules list** hinzugefügt werden.

Beim G16 mit 2G-Modem (G16_G410) ist diese Seite nicht nutzbar: Die 2G-Variante hat keinen RS485-Bus.

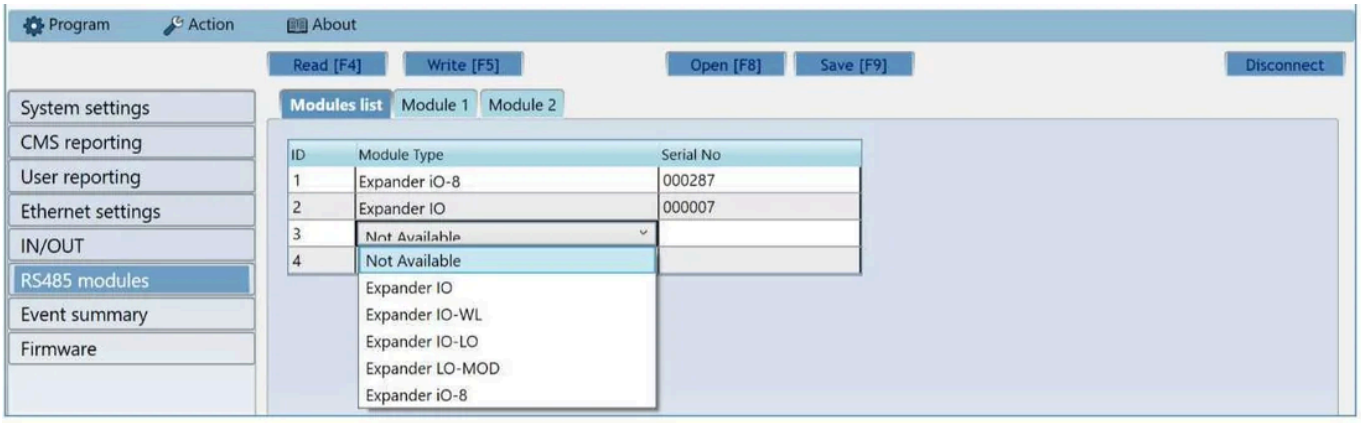


Abbildung 41. TrikdisConfig – RS485 modules, Reiter Modules list: Typ des Moduls (Expander iO-8, W17u/W485, E485) und Seriennummer.

- **Module Type** – der Typ des angeschlossenen Moduls aus der Liste (Expander iO-8, W17u/W485, E485).
- **Serial No** – die 6-stellige Seriennummer des Moduls (auf dem Modul und seiner Verpackung, SN).

Drücken Sie nach der Auswahl des Moduls und der Eingabe der Seriennummer die Taste **Write [F5]**, ziehen Sie das USB-Kabel ab und warten Sie eine Minute, bis der Kommunikator das Modul registriert. Stecken Sie dann das Kabel wieder ein, lesen Sie das Gerät aus (**Read [F4]**), und auf der Seite RS485 modules erscheint der eigene, nummerierte Reiter des Moduls.

Erweiterungsmodul iO-8 – 8 I/O mit Doppelfunktion; bis zu 4 Module können an den Kommunikator angeschlossen werden.

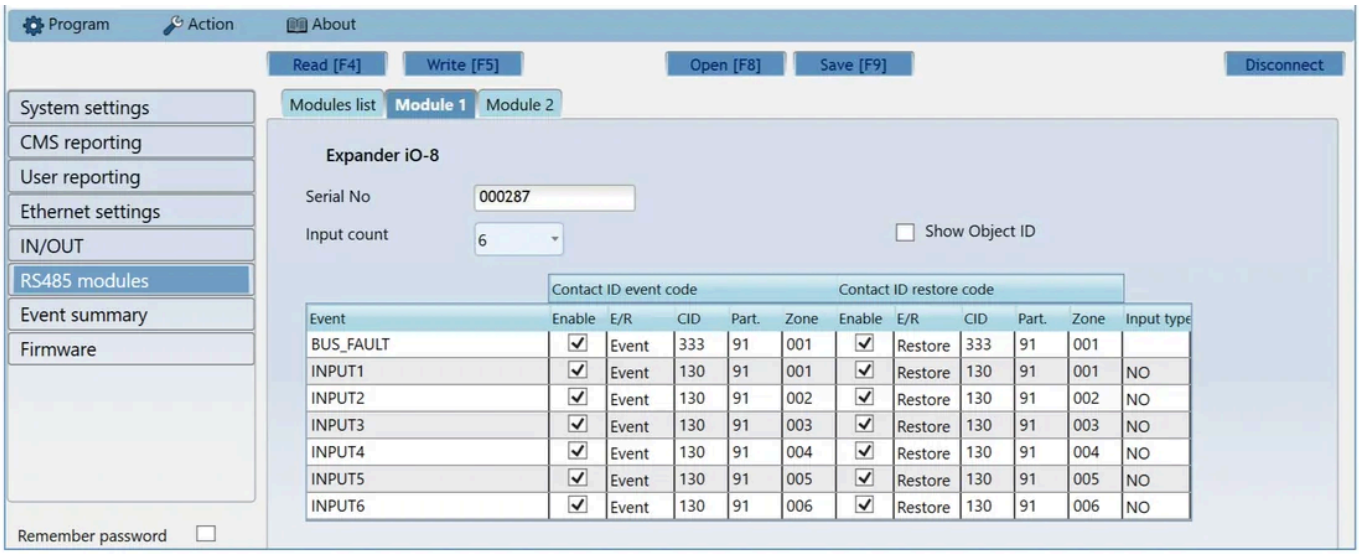


Abbildung 42. TrikdisConfig – RS485 modules, Reiter des Moduls iO-8.

- **Input Count** – wie viele Klemmen Eingänge sein sollen; die übrigen werden Ausgänge. Der Typ des Eingangs (**Input type**: NO oder NC) ist in der Tabelle einstellbar. Die Rolle der Ausgänge (Scharf- / Unscharfschalten über eine Schlüsselschalter-Zone oder Schalten eines Geräts) stellen Sie in der App Protegus 2 ein.
- In der Tabelle können Sie dem Busfehler (**BUS_FAULT**, Contact ID 333) und den Auslöse- und Wiederherstellungsereignissen der Eingänge (**INPUTx**, 130) einen Contact-ID-Code zuordnen (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Bei Auslösung eines Eingangs sendet der Kommunikator mit dem eingestellten Code ein Ereignis an den Empfänger der Leitstelle, an die App Protegus 2 und per SMS an die

Telefonnummer des Benutzers. Standardmäßig meldet das Modul 1 mit dem Bereich 91, das Modul 4 mit dem Bereich 94. Durch Anhaken von **Show Object ID** kann für die Eingänge auch eine von der des Kommunikators abweichende Objektkennung angegeben werden.

- Soll der Benutzer zu den Eingängen des Erweiterungsmoduls auch eine SMS oder einen Anruf erhalten, nehmen Sie den dem Eingang zugeordneten Contact-ID-Code auch in die Ereignistabelle des Reiters **SMS & Call Reporting** auf.

WiFi-Modul W485 (in der Liste W17u/W485) – die Daten des WLAN-Netzes und die Netzwerkeinstellungen.



Abbildung 43. TrikdisConfig – RS485 modules, Reiter des Moduls W485.

- **DHCP mode** – automatische (DHCP) oder manuelle (Static) Netzwerkeinstellung.
- **Static IP**, **Subnet mask**, **Default gateway** – bei manueller Einstellung.
- **Wifi SSID name**, **Wifi SSID password** – Name und Passwort des WLAN-Netzes.
- In der Tabelle können Sie den Fehlern des RS485-Busses (Unterbrechung und Wiederherstellung der Verbindung zwischen Modul und G16) einen Contact-ID-Code zuordnen; das Ereignis erhalten die Leitstelle und auch Protegus 2.

Ethernet-Modul E485 – dieselben Netzwerkeinstellungen ohne WLAN (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); in der Tabelle können Sie auch hier dem Fehler des RS485-Busses (Unterbrechung und Wiederherstellung der Verbindung zwischen E485 und G16) einen Contact-ID-Code zuordnen, den die Leitstelle und auch Protegus 2 erhalten.

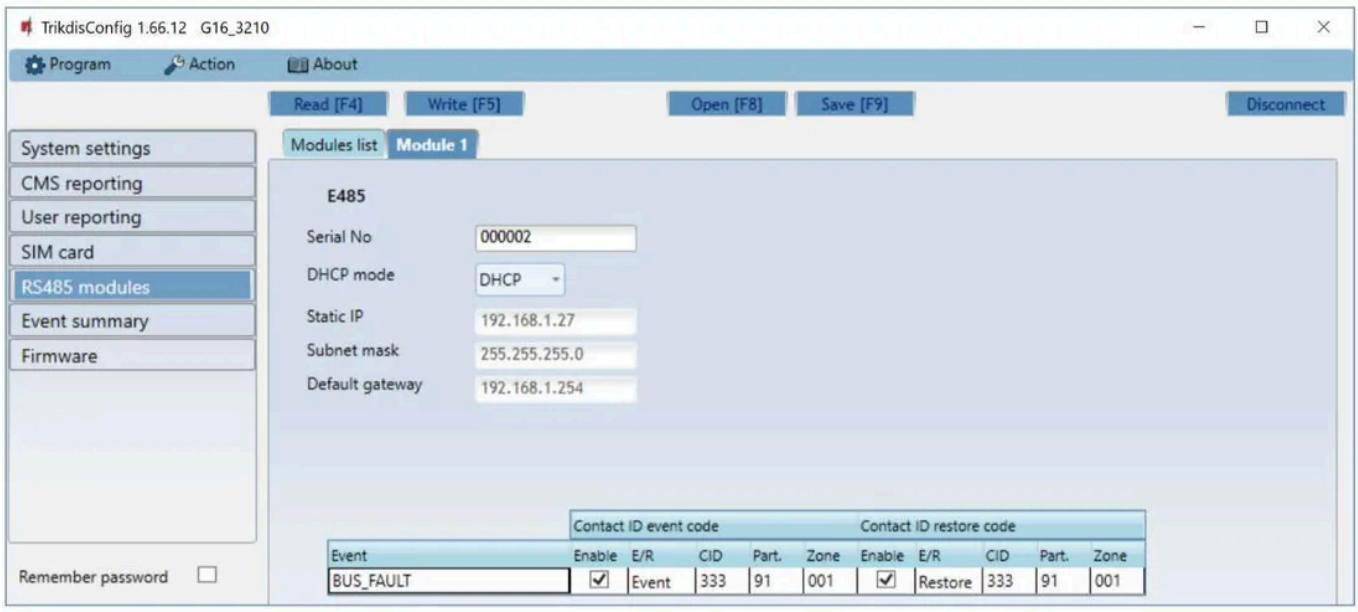


Abbildung 44. TrikdisConfig – RS485 modules, Reiter des Moduls E485.

Damit W485 und E485 funktionieren, muss die Verbindung des G16 zur Leitstelle und/oder zu Protegus eingerichtet sein (Punkte 2.3 und 2.4), und im G16 muss eine SIM-Karte stecken. Solange die kabelgebundene oder WLAN-Verbindung besteht, kommuniziert der Kommunikator darüber und nutzt die mobile Datenverbindung nicht.

6.8 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.

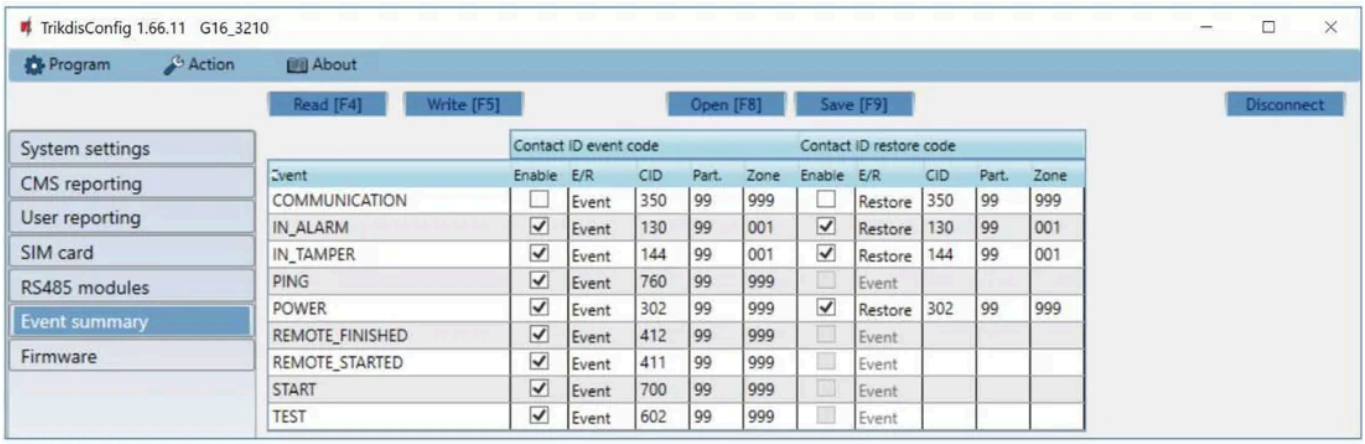


Abbildung 45. TrikdisConfig – Seite Event summary: die internen Meldungen des Geräts (im Bild die Hardware-Version 3, bei der auch das Ereignis IN_ALARM und IN_TAMPER des Eingangs und der PING hier stehen; bei der Version 4 sind die Ereignisse der Eingänge auf der Seite IN/OUT).

6.9 Zurücksetzen auf Werkseinstellungen

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.

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.

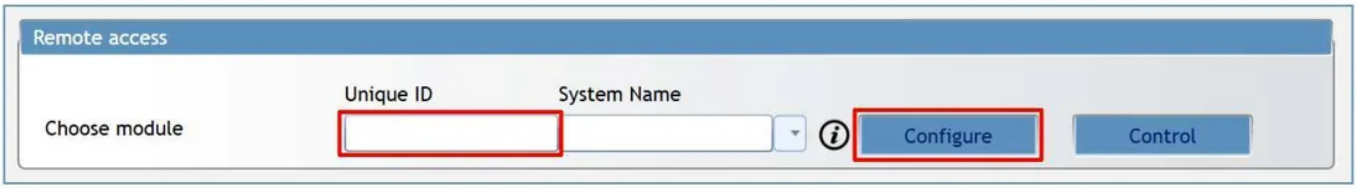


Abbildung 46. TrikdisConfig – Remote access: die Kennung des Geräts, der Name des Systems und die Schaltfläche Configure.

8. Funktionsprüfung des Kommunikators

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

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

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

Prüfen Sie bei einer am Bus angeschlossenen Zentrale auch, ob der Kommunikator tatsächlich aus der Zentrale liest: Schalten Sie die Zentrale am Bedienteil scharf und unscharf und sehen Sie nach, ob das Ereignis in der Ereignisliste von Protegus 2 (und bei der Leitstelle) mit der richtigen Bereichs- und Benutzernummer erscheint. Führen Sie bei direkter Steuerung auch ein Probe-Scharfschalten aus der App durch, mit dem Bedienteilcode des Benutzers.

9. Firmware-Update

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

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.

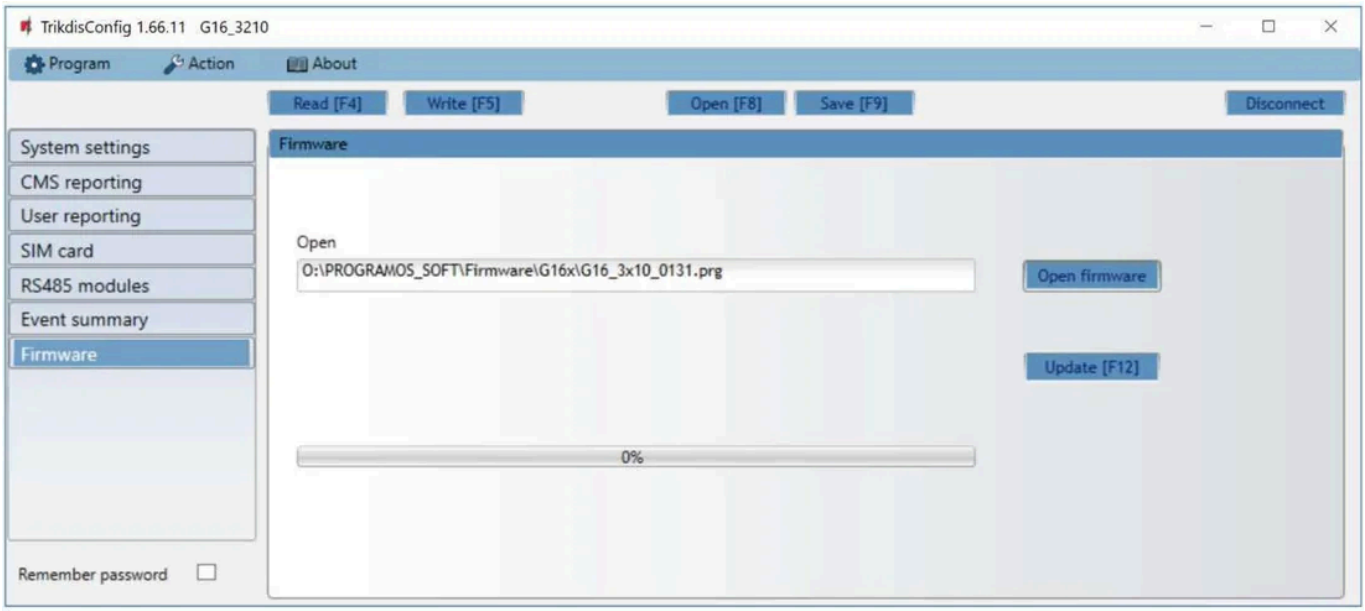


Abbildung 47. TrikdisConfig – Seite Firmware: Open firmware und Update [F12].

Für das Update ist eine Internetverbindung nötig. Virenscanner, Firewall oder strenge Netzwerkeinstellungen können den automatischen Firmware-Download verhindern; stellen Sie in diesem Fall den Virenscanner um (erlauben Sie TrikdisConfig den Internetzugang) oder laden Sie die Datei manuell herunter und öffnen Sie sie

auf der Seite Firmware.

10. Fehlersuche und häufige Fragen

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

Die LED NETWORK leuchtet nicht – kein Netz

1. Sehen Sie sich die Blinkimpulse der LED **TROUBLE** an: 1 = keine SIM, 2 = falsche PIN, 3 = kein APN, 4 = kann sich nicht mit dem Mobilfunknetz verbinden, 5 = kann sich nicht mit dem Datennetz verbinden.
2. Prüfen Sie, ob die SIM-Karte aktiv ist, einen Datendienst hat und richtig im Halter sitzt.
3. Ist auf der Karte die PIN-Abfrage eingeschaltet, geben Sie die PIN auf der Seite **SIM card** ein oder schalten Sie die PIN-Abfrage in einem Telefon aus.
4. Prüfen Sie die Antenne: Sie ist aufgeschraubt, befindet sich nicht in einem Metallgehäuse, die Signalstärke ist ausreichend (Punkte 1.7 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 an, dass keine Verbindung zum Empfänger besteht: Prüfen Sie Adresse, Port, die TCP/UDP-Einstellung und den Verschlüsselungsschlüssel des Empfängers (**CMS reporting**).
2. Ist der Empfänger mit einem Domainnamen angegeben, prüfen Sie die DNS-Einstellung (**CMS reporting** → **Settings**).
3. Prüfen Sie, ob das Datenpaket der SIM-Karte den benötigten Port nicht sperrt (manche M2M-Karten erlauben nur bestimmte Adressen).

Die LED TROUBLE blinkt siebenmal – der Kommunikator sieht die Zentrale nicht

1. Prüfen Sie den Anschluss anhand der Abbildung in Punkt 3.3: Der häufigste Fehler sind vertauschte Leitungen **CLK** und **DATA** oder eine an die falsche Klemme der Zentrale angeschlossene Datenleitung.
2. Im Feld **System settings** → **Security panel model** von TrikdisConfig muss der genaue Typ der angeschlossenen Zentrale ausgewählt sein.
3. Bei Texecom-, Caddx-, Honeywell- und InnerRange-Zentralen ist auch in der Zentrale eine Einstellung nötig (Kapitel 4) – ohne sie gibt die Zentrale keine Daten auf den Bus.
4. Bei Paradox-Zentralen kann die serielle Schnittstelle ab Werk gesperrt sein – so schalten Sie sie frei.
5. Machen Sie eine Pyronix-Zentrale nach dem Anschließen spannungsfrei und starten Sie sie neu, damit sie den Kommunikator akzeptiert.
6. Mit einer Zentrale DSC PowerSeries **NEO** funktioniert der G16 nicht (am Bus der NEO ist kein externes Gerät zugelassen) – hier ist ein Kommunikator für die Telefonleitung nötig.

Die Ereignisse kommen an, aber ich kann in der App nicht scharfschalten

Bei direkter Steuerung:

1. Auf der Seite **System settings** muss **Remote Arm/Disarm** angehakt sein.
2. Bei Paradox- und Texecom-Zentralen muss das **Security panel PC download password** mit dem PC- bzw. UDL-Passwort der Zentrale übereinstimmen (Punkte 4.2 und 4.3).
3. Bei Paradox-Zentralen muss die Firmware der Zentrale mindestens **V.4** sein; der Code des Benutzers darf nicht der Mastercode sein; starten Sie den Kommunikator nach einer Codeänderung neu.
4. Bei einer Honeywell-Vista-Zentrale muss die 2. AUI-Adresse freigegeben sein (Punkt 4.6).
5. In Protegus 2 darf dem Bereich **kein** Ausgang zugeordnet sein (Control with Protegus2 ausgeschaltet).

Mit Schlüsselschalter-Zone:

1. **Remote Arm/Disarm** muss leer sein, die I/O-Klemme muss auf der Seite **IN/OUT** auf **OUT** stehen.
2. Die Zone der Zentrale muss vom Typ Schlüsselschalter sein, und in Protegus 2 muss dem Bereich der passende Ausgang zugeordnet sein, im zur Zone passenden Impuls- oder zweistelligen Modus (Punkt 5.3).

Protegus 2 sieht das Gerät nicht

1. Auf der Seite **User reporting → PROTEGUS Cloud** muss **Enable connection** angehakt sein.
2. Beim Anlegen des Systems muss der im Gerät eingestellte **Protegus Cloud access code** eingegeben werden; nach dem Anlegen des Systems kann er im Gerät nicht mehr geändert werden.
3. Geben Sie die IMEI genau ein, von der Verpackung oder der Rückseite.
4. Datendienst und APN der SIM-Karte 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 anmelden

1. Das Gerät muss online sein (LED NETWORK grün), und die Protegus-Verbindung muss freigegeben sein.
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 Errichter-Passwort.

Ich habe das Passwort vergessen

Ein vergessenes Passwort lässt sich nicht abfragen und 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: Es muss ihm zugeschickt werden. Notieren Sie die gesetzten Passwörter daher an einem sicheren Ort.

Warum sehe ich die Seite RS485 modules nicht, oder warum funktioniert das iO-8 nicht?

Der G16 mit 2G-Modem (G16_G410) hat keinen RS485-Bus; iO-8, W485 und E485 können nur an die 4G-Variante (G16_54E0) angeschlossen werden. Für die Module W485 und E485 muss im G16 außerdem eine SIM-Karte stecken.

Ich habe ein 2G-Gerät – wie lange funktioniert es?

Die Abschaltung der 2G-Netze schreitet je nach Anbieter unterschiedlich schnell voran; für den langfristigen Betrieb empfehlen wir die 4G-Variante, die auch über den RS485-Bus erweiterbar ist.

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 von 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 aufmerksam durch; die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen oder Defekten führen.
- Trennen Sie die Anlage vor dem Anschließen, bei jedem elektrischen Anschluss und vor Servicearbeiten von der Versorgung.
- Fehler aus unsachgemäßer Installation oder Nutzung sowie vom Hersteller nicht genehmigte Änderungen und Reparaturen führen zum Verlust der Garantie.
- Beachten Sie die örtlichen Vorschriften zur Abfallentsorgung: Entsorgen Sie das defekte Gerät und seine Teile nicht mit dem Hausmüll.

Siehe auch

- Kompatibilitätssuche – welcher Kommunikator zu welcher Alarmzentrale passt.
- G16 – direkte Steuerung für DSC-PowerSeries-Alarmzentralen – Scharfschalten mit dem Bedienteilcode, Zonenzustände, Sperren von Zonen.
- DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen – warum der G16 nicht an die NEO angeschlossen werden kann und was die Lösung ist.
- Freischalten der gesperrten seriellen Schnittstelle bei Paradox-Alarmzentralen – Freischalten der seriellen Schnittstelle der neueren Paradox-Zentralen.
- Scharfschalten aus der Ferne per Schlüsselschalter in der App Protegus 2 – Einzelheiten und Stolperfallen des Scharfschaltens per Schlüsselschalter.
- Die Hardware-Version v4 der GSM-Kommunikatoren G16 und G16T ist da – was sich gegenüber der Version 3 geändert hat.
- APN-Einstellung – Liste europäischer Mobilfunkanbieter – der APN der SIM-Karte je Anbieter.
- Englischsprachige Dokumentation: docs.trikdis.com – die Anleitungen auf docs.trikdis.com sind in englischer Sprache.

Passende Produkte

Trikdis G16 4G GSM Kommunikationsmodul | **Trikdis G16 2G GSM Kommunikationsmodul**

Trikdis CRP2 Seriell-Port-Verbindungskabel für Paradox-Alarmpulte

Trikdis CRP2B Seriell-Port-Verbindungskabel für Paradox-Alarmpulte

Trikdis CRP4 Serienkabel für Texcom -Steuerplatten | **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/g16-anleitung