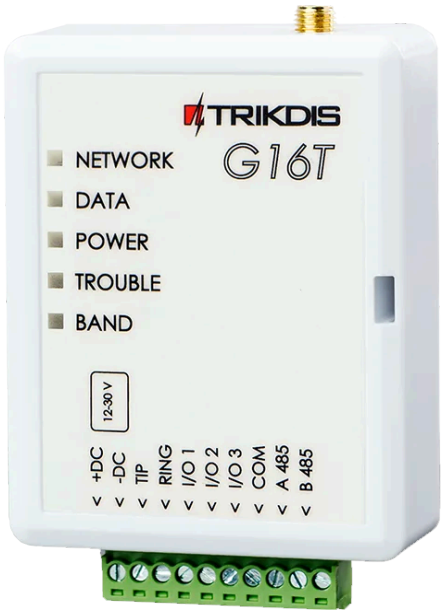
Kommunikator G16T – Installations- und Benutzeranleitung

Installations- und Benutzeranleitung für den Trikdis-Kommunikator G16T: Anschluss an die Alarmzentrale, SIM-Karte und Einrichtung in TrikdisConfig, Übertragung an die Leitstelle, App Protegus 2, Prüfung und Fehlersuche.



Ausgabe: 2026-11-17
Immer aktuelle Webversion: https://trikdis.at/g16t-anleitung

Inhalt

1. Überblick

1.1 Wofür er dient und wie er funktioniert
1.2 Versionen
1.3 Hauptmerkmale
1.4 Bestandteile des Kommunikators
1.5 Klemmen
1.6 LED-Anzeigen
1.7 Technische Daten

2. Schnelle Inbetriebnahme mit TrikdisConfig

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

3. Installation und Anschluss

3.1 Installationsschritte
3.2 Montageort und Antenne
3.3 Anschluss an die Alarmzentrale
3.3.1 Bei Bedarf: Leitungsüberwachung
3.4 Anschluss einer Schlüsselschalter-Zone
3.5 Anschluss von Eingängen
3.6 Anschluss eines Ausgangs mit Relais
3.7 Anschluss der Erweiterung 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 Programmierung des Wählers der Honeywell Vista
4.2 Zentralen anderer Hersteller

5. Fernsteuerung mit der App Protegus 2

5.1 Gerät hinzufügen
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Scharf- und Unscharfschalten mit einem Ausgang
5.3 Scharf- und Unscharfschalten aus der App
5.4 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 Werkseinstellungen wiederherstellen

7. Fernprogrammierung

8. Funktionsprüfung des Kommunikators

9. Firmware-Aktualisierung

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

Der G16T ist der **universelle Mobilfunk-Kommunikator** von Trikdis: Er wird an den Telefonleitungsausgang (TIP/RING) der Alarmzentrale angeschlossen und verhält sich wie eine Telefonvermittlung. Die Alarmzentrale „wählt", sendet die Contact-ID-Meldung mit DTMF-Tönen, und der G16T nimmt die Leitung ab, dekodiert die Meldung und leitet sie über eine mobile Datenverbindung an den Empfänger der Leitstelle sowie an die Protegus-Cloud, in die App des Benutzers, weiter. So kann er mit **einer Zentrale beliebigen Herstellers** verwendet werden, die über einen Contact-ID-Wähler verfügt – die Zentrale muss nicht ausgetauscht werden, nur ihr Wähler muss eingestellt werden. Die G16T-Kommunikatoren sind nach dem höchsten Sicherheitsgrad **EN 50131 Grade 4** zertifiziert.

1.1 Wofür er dient und wie er funktioniert

- **Er meldet an die Leitstelle.** Die Ereignisse sendet er über IP an einen 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). Für einen SUR-GARD-Empfänger wandelt er die von der Zentrale empfangenen Contact-ID-Codes in SIA-Codes um; die Umwandlungstabelle steht im Anhang der englischen Trikdis-Dokumentation. Die Verbindung prüft er standardmäßig alle 30 Sekunden (oder im eingestellten Intervall) und schaltet bei einem Fehler auf den Ersatzkanal um.
- **Er benachrichtigt den Benutzer.** Die App Protegus 2 zeigt das Geschehen per Push-Nachricht mit eigenem Signalton und in der Ereignisliste; aus der App kann der Benutzer scharf- und unscharfschalten sowie die angeschlossenen Geräte schalten (Beleuchtung, Tor, Lüftung, Heizung, Bewässerung usw.). Die App funktioniert mit jeder Alarmzentrale, an die der Kommunikator angeschlossen ist, unabhängig vom Hersteller der Zentrale.
- **Er arbeitet mit Leitstelle und Benutzer gleichzeitig oder getrennt:** Er kann nur mit Protegus 2 (ohne Leitstelle), nur mit einer Leitstelle oder mit beidem verwendet werden. Sind beide eingerichtet, sendet er das Ereignis zuerst an die Leitstelle, danach an den Benutzer.
- **SMS-Ersatzweg.** Er benachrichtigt die Leitstelle auch per SMS, wenn die Datenverbindung im Netz des Mobilfunkanbieters nicht funktioniert; er kann parallel an zwei Empfänger senden, für jeden mit eigenem Ersatzkanal.
- **Er hat eigene Ein- und Ausgänge.** Drei I/O-Klemmen mit Doppelfunktion können als Eingang (Melder, Sabotage) oder als steuerbarer Ausgang (Schlüsselschalter-Zone, Relais) verwendet werden. Am RS485-Bus der 4G-Version bringt ein Erweiterungsmodul iO-8 weitere 8 I/Os (andere drahtgebundene oder drahtlose Erweiterungen der iO-Serie bringen weitere Ein- und Ausgänge, eine iO- oder iO-WL-Erweiterung die Fern-Temperaturüberwachung), und mit einem W485- oder E485-Modul kann er auch über WLAN bzw. kabelgebundenes Internet kommunizieren – dann ist das Mobilfunknetz der Ersatzweg.

Den Aufbau des Systems zeigt die folgende Abbildung: Der Telefonleitungsausgang der Alarmzentrale ist mit dem G16T verbunden, der G16T erreicht über das Mobilfunknetz das Internet und von dort den Empfänger der Leitstelle und die Protegus-Cloud, und der Benutzer sieht das System in der App Protegus 2.

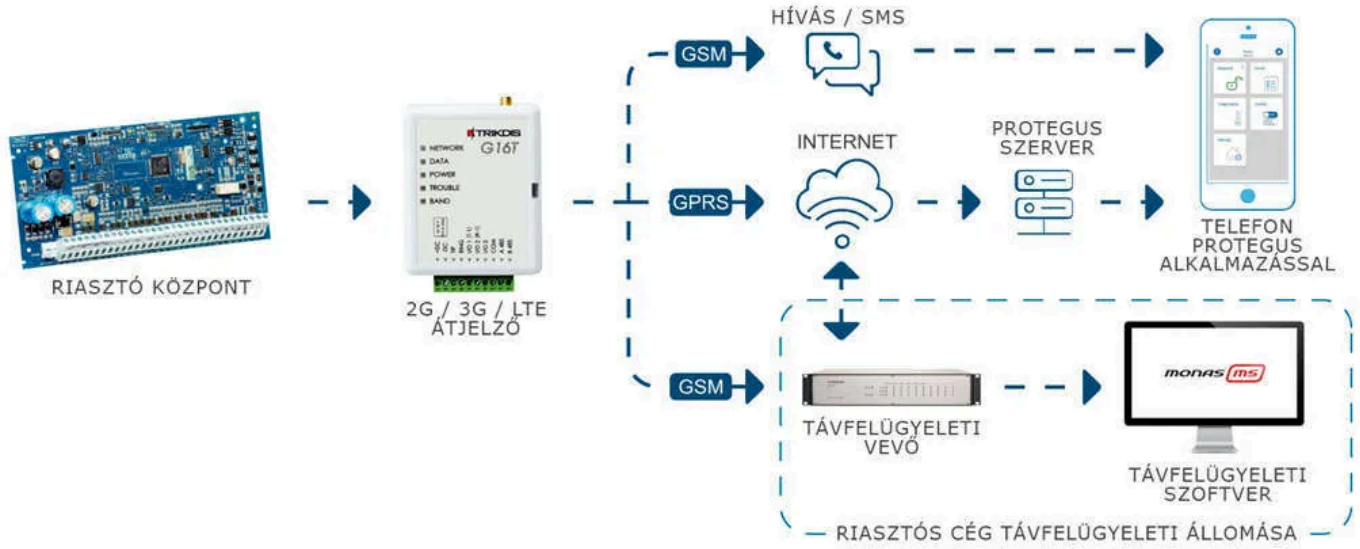


Abbildung 1. Die Stellung des G16T im System: Alarmzentrale → G16T → Mobilfunknetz → Empfänger der Leitstelle und Protegus-Cloud → App Protegus 2.

1.2 Versionen

Diese Anleitung wurde für die **Hardwareversion 4** des G16T erstellt, sie ist aber **auch für die Hardwareversion 3 verwendbar**: Anschluss, Einrichtung und Funktion der beiden Versionen sind weitgehend gleich. Die Unterschiede fasst die folgende Tabelle zusammen; wo der Text einen Wert der Version 4 angibt, beachten Sie bei der Version 3 diese Tabelle.

	Hardware 3 (v3)	**Hardware 4 (v4)**
Typen	G16T_321x (2G), G16T_331x (3G), G16T_341x (4G), G16T_3M10 (LTE Cat-M1 + 2G) – alle mit 1 SIM-Karte	G16T_G410 (2G), G16T_E120 (4G, mit 2G-Rückfall)
Ein-/Ausgänge	2 Eingänge mit wählbarem Typ (T-1/IN1, R-1/IN2 – auch zur Überwachung der Telefonleitung verwendbar) + 1 Open-Collector-Ausgang (OUT, max. 0,15 A)	3 I/O-Klemmen mit Doppelfunktion (I/O 1, I/O 2, I/O 3), jede als Eingang oder als Open-Collector-Ausgang (max. 0,15 A) verwendbar
Stromaufnahme	60–100 mA; beim Senden höchstens 250 mA	60–100 mA; beim Senden höchstens 500 mA
Modemfrequenzen	2G: 850 / 900 / 1800 / 1900 MHz; 3G: 800 / 850 / 900 / 1900 / 2100 MHz; 4G: regionsabhängig	2G: 850 / 900 / 1800 / 1900 MHz; 4G: regionsabhängig
Abmessungen	92 × 62 × 26 mm	92 × 65 × 26 mm
RS485-Bus (iO-8, W485, E485)	ja	nur bei der 4G-Version (G16T_E120)

Die Hardwareversion 4 gibt es mit zwei Modems:

Typ	**Modem**	**Frequenzen**	**RS485 (iO-8, W485, E485)**
G16T_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	nein
G16T_E120	4G (LTE), mit 2G-Rückfall	regionsabhängig	ja

Die Hardwareversion finden Sie in der Statusleiste von TrikdisConfig (**HW**) und auf dem Etikett auf der Rückseite des Geräts.

1.3 Hauptmerkmale

Verbindung zur Alarmzentrale

- Normaler Anschluss an den Telefonleitungsausgang der Zentrale: DC+, DC−, TIP und RING. Bei Bedarf auch mit Leitungsüberwachung anschließbar (mit den Adern T-1 und R-1): Dann ist die Verbindung zwischen Zentrale und Kommunikator **überwacht**, eine Unterbrechung der Leitung meldet der Kommunikator.
- Die Zentrale sendet die Ereignisse im Format Contact ID mit DTMF-Wahl; der G16T leitet die vollständige Ereignisinformation (Code, Bereich, Zone oder Benutzer) weiter.

Kommunikation mit der Leitstelle

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

Benutzerfunktionen

- Mobil- und Web-App Protegus 2: Push-Benachrichtigung mit eigenem Signalton, Ereignisliste, Scharf- und Unscharfschalten, Schalten von Ausgängen.
- Fern-Temperaturüberwachung (mit einer iO- oder iO-WL-Erweiterung).
- Steuerung und Grundeinstellung auch per SMS-Befehl.
- Benachrichtigung auch per SMS und Telefonanruf, 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 andere Kommunikatoren geladen werden.
- Zwei Zugriffsebenen: Administrator (die der Leitstelle) und Errichter.
- Fernkonfiguration und Fernaktualisierung mit der Software TrikdisConfig.

1.4 Bestandteile des Kommunikators

Die Leiterplatte des G16T sitzt in einem weißen Kunststoffgehäuse; die Frontabdeckung ist abnehmbar, der Klemmenblock abziehbar. Die folgende Abbildung zeigt die 4G-Version; die 2G-Version hat keine BAND-LED und keine Klemmen A 485 / B 485.

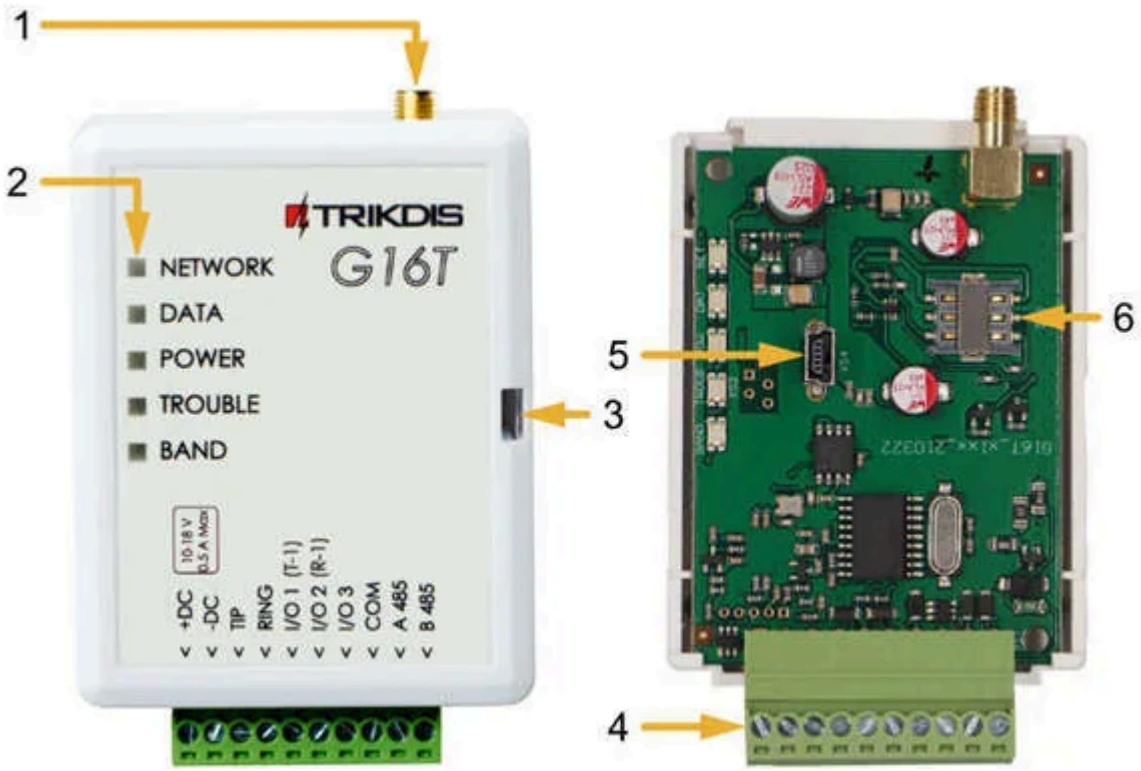


Abbildung 2. Bestandteile des G16T (4G-Version), von vorn und mit geöffnetem Gehäuse.

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

Der Klemmenblock ist abziehbar: So lässt sich das Gerät mit einem Handgriff stromlos machen oder neu starten, beim Anschließen ist es leichter zu handhaben, und für die Programmierung über USB kann das Gerät zum Computer gebracht werden.

1.5 Klemmen

Klemme	Funktion
+DC	Versorgung, +10–18 V DC
–DC	Versorgung, negativ
TIP	Klemme TIP der Alarmzentrale
RING	Klemme RING der Alarmzentrale
I/O 1 (T-1)	Ein-/Ausgang 1 oder Punkt T-1 der Telefonleitungsüberwachung
I/O 2 (R-1)	Ein-/Ausgang 2 oder Punkt R-1 der Telefonleitungsüberwachung
I/O 3	Ein-/Ausgang 3
COM	Gemeinsamer (negativer) Punkt für die Ein- und Ausgänge
A 485	Ader A des RS485-Busses (nur 4G-Version)
B 485	Ader B des RS485-Busses (nur 4G-Version)

Die Klemmenbeschriftung steht auch auf der Frontabdeckung, daher muss die Abdeckung beim Anschließen nicht abgenommen werden.

1.6 LED-Anzeigen

Die LEDs auf der Frontabdeckung sind die wichtigsten Hilfsmittel bei Inbetriebnahme und Fehlersuche. Lesen Sie sie zusammen: POWER zeigt die Versorgung, NETWORK das Netz, TROUBLE den Fehler und BAND (nur 4G) den Netztyp.

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 Anzahl der gelben Blinkzeichen ist der **Signalpegel**: bei 2G sind 5 Blinkzeichen, bei 3G/4G 3 Blinkzeichen ein gutes Signal

DATA – Datenverkehr

Anzeige	Bedeutung
aus	Keine Meldung wartet auf Versand
leuchtet grün	Im Speicher warten Meldungen auf Versand
blinkt grün	Daten werden gesendet oder empfangen (während der Programmierung)

Schnellprüfung

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

POWER – Versorgungsspannung

Anzeige	Bedeutung
aus	Keine Versorgung, oder die Versorgung ist getrennt
leuchtet grün	Eingeschaltet, die Versorgungsspannung ist in Ordnung
leuchtet gelb	Versorgungsspannung ungenügend (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 rotes Blinkzeichen	Keine SIM-Karte
2 rote Blinkzeichen	SIM-PIN-Fehler (falscher PIN-Code)
3 rote Blinkzeichen	Programmierfehler (kein APN)
4 rote Blinkzeichen	Anmeldung am Mobilfunknetz nicht möglich (Registrierungsfehler)
5 rote Blinkzeichen	Verbindung zum Datennetz (GPRS/UMTS/LTE) nicht möglich
6 rote Blinkzeichen	Keine Verbindung zum Empfänger der Leitstelle
7 rote Blinkzeichen	Verbindung zur Alarmzentrale unterbrochen
blinkt rot (während der Programmierung)	Speicherfehler
leuchtet rot (während der Programmierung)	Beschädigte Firmware

BAND – Netztyp (nur 4G-Version)

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

1.7 Technische Daten

Parameter	Wert
Verbindung zur Alarmzentrale	drahtgebundene Telefonleitung (TIP/RING), Contact ID, DTMF
Ein-/Ausgänge	3 I/Os 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	am RS485-Bus (nur 4G-Version): Erweiterung iO-8 (+8 I/O) und andere Erweiterungen der iO-Serie; WLAN-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
Ereignisspeicher	60 Meldungen
Verschlüsselung	AES-128
Programmierung	TrikdisConfig (Windows) über USB-Mini-B-Kabel oder aus der Ferne; SMS-Befehle

Parameter	Wert
Betriebsumgebung	−10 … +50 °C, max. 80 % relative Luftfeuchte (bei +20 °C)
Abmessungen	92 × 65 × 26 mm
Gewicht	80 g

2. Schnelle Inbetriebnahme mit TrikdisConfig

Alle Einstellungen des G16T erfolgen mit dem Windows-Programm **TrikdisConfig** – über USB-Kabel oder aus der Ferne. In diesem Kapitel beschreiben wir den kürzesten Weg: Sie richten das Gerät auf dem Tisch ein, bevor Sie es anschließen, und vor Ort muss es dann nur noch angeschlossen werden. Die ausführliche Erklärung der Einstellungen finden Sie in Kapitel 6.

2.1 Vorbereitung

Was Sie benötigen

USB-Mini-B-Kabel · Kabel mit mindestens 4 Adern zur Zentrale · Schlitzschraubendreher 2,5 mm · Mobilfunkantenne mit ausreichender Verstärkung (wenn die Netzabdeckung vor Ort schwach ist) · aktive Nano-SIM-Karte mit mobilem Datendienst · Installationsanleitung der Alarmzentrale.

Das nötige Zubehör bestellen Sie separat beim Händler.

1. Laden Sie die Software TrikdisConfig herunter und installieren Sie sie. Geben Sie auf der Website 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 G16T. Stecken Sie einen Schlitzschraubendreher in die seitliche Öffnung und hebeln Sie die Abdeckung vorsichtig ab. Die folgende Abbildung zeigt die Stelle der Verriegelung und die Befestigungslöcher der Rückwand.

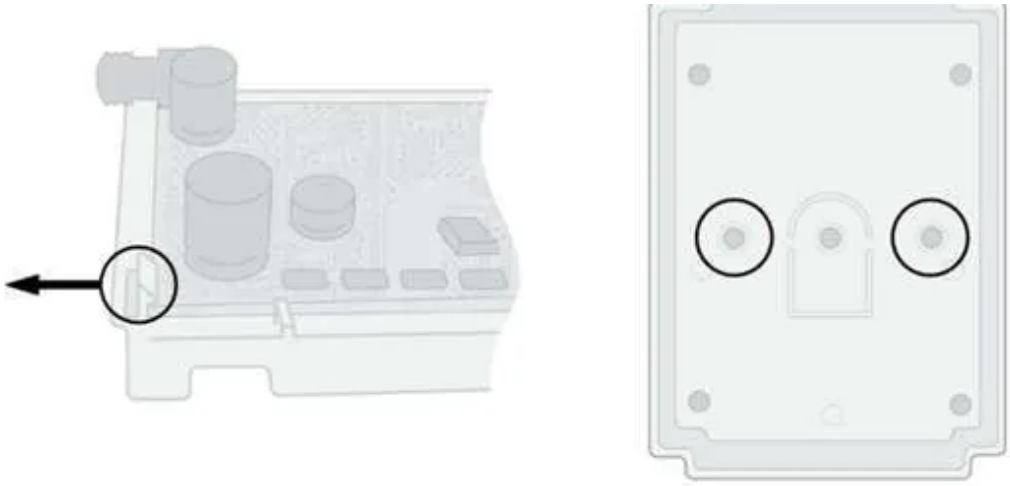


Abbildung 3. Abhebeln der Frontabdeckung (links) und Befestigungslöcher der Rückwand (rechts).

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

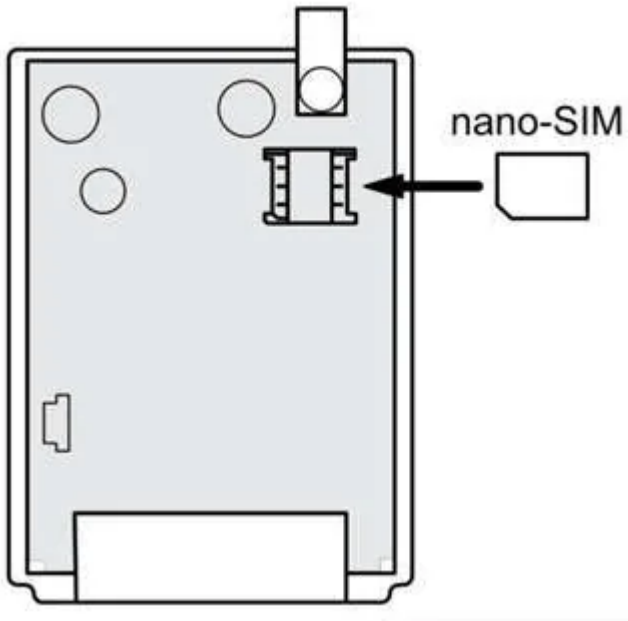


Abbildung 4. Position der Nano-SIM-Karte auf der Leiterplatte.

4. Verbinden Sie den G16T mit dem Computer über ein USB-Mini-B-Kabel. USB liefert genug Strom für die Programmierung, eine separate Versorgung ist nicht nötig.



Abbildung 5. Verbindung zum Computer mit einem USB-Mini-B-Kabel.

Warnung

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

5. Starten Sie TrikdisConfig. Das Programm erkennt das Gerät und öffnet das Programmierfenster. Klicken Sie auf **Read [F4]** (Lesen): Das Programm liest die aktuellen Einstellungen des Geräts aus. Wenn ein Passwort verlangt wird, geben Sie den 6-stelligen Administrator-Code (werkseitig `123456`) oder den Errichter-Code (werkseitig `654321`) ein.

2.2 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**, im Reiter **PROTEGUS Cloud**, Folgendes ein.

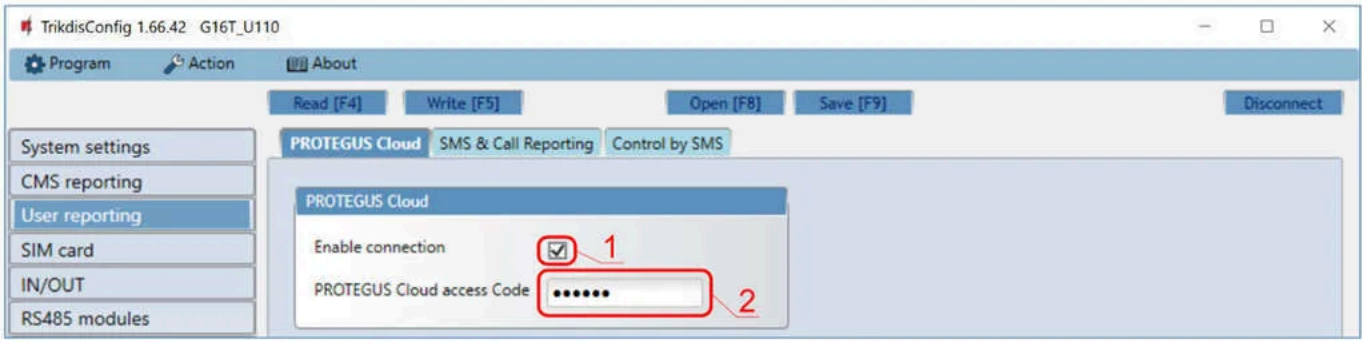


Abbildung 6. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- 1 **Enable connection** – anhaken: aktiviert die Verbindung zur Protegus-Cloud.
- 2 **Protegus Cloud access code** – ändern Sie das werkseitige Passwort `123456`. Dieses müssen Sie später beim Anlegen des Systems in der App eingeben; **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.

- 3 **SIM card PIN** – der PIN-Code der Karte (ist die PIN-Abfrage abgeschaltet, kann der Werkswert bleiben).
- 4 **APN** – der Zugangspunkt für die Datenverbindung des Anbieters (siehe unten).

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

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

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

Vergessen Sie nicht, den Telefonwähler der Alarmzentrale einzuschalten und einzustellen, sonst sendet die Zentrale keine Ereignisse. Die Einstellung der Zentrale beschreibt Kapitel 4.

2.3 Verbindung zur Leitstelle

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

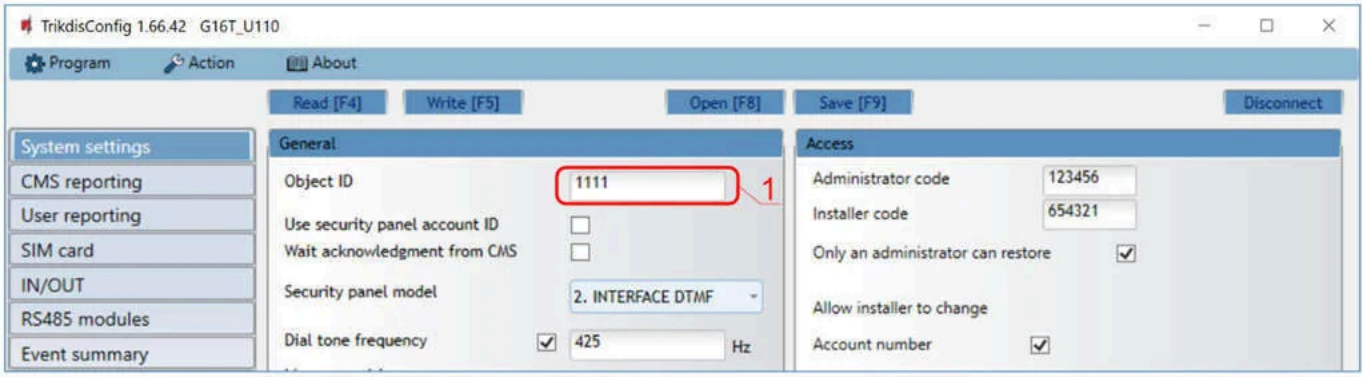


Abbildung 8. TrikdisConfig – Seite System settings, Gruppe General.

- 1 **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen, 0–9, A–F). `FFFE` und `FFFF` sind nicht zulässig.

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

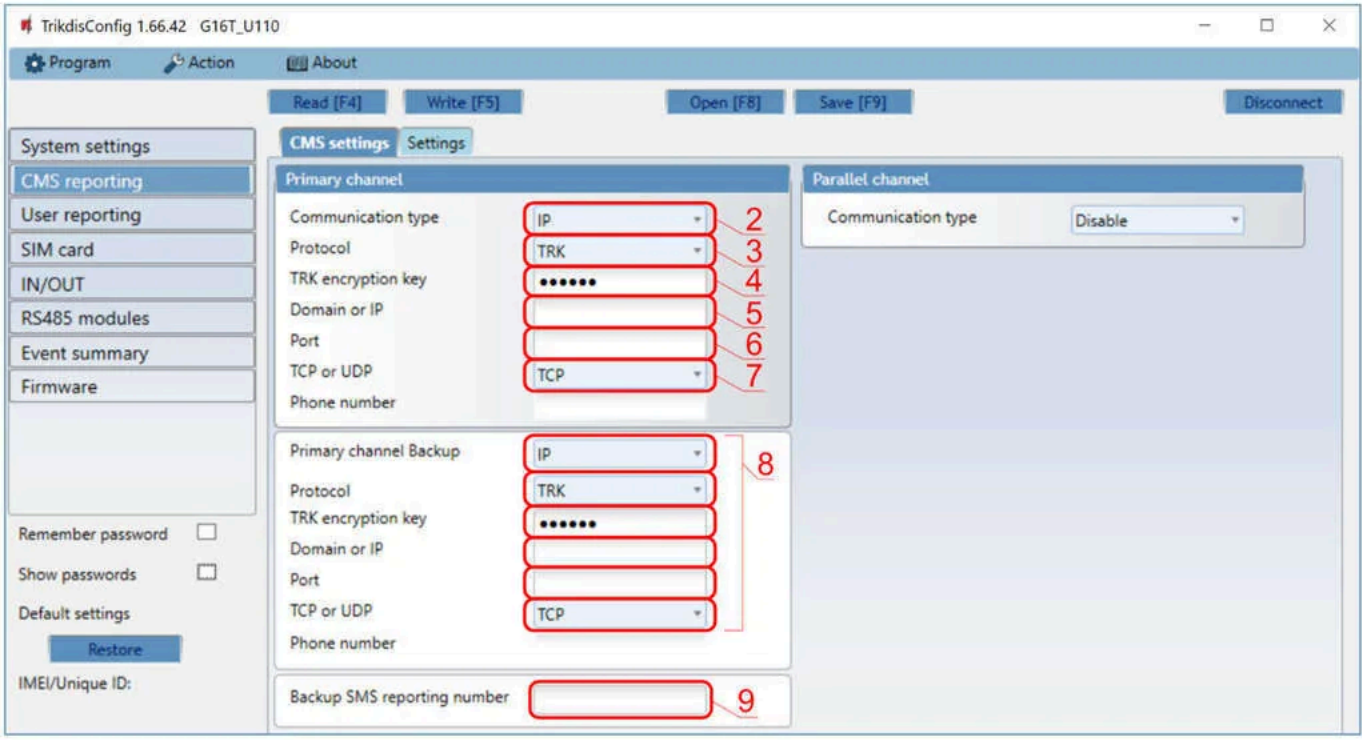


Abbildung 9. TrikdisConfig – CMS reporting, Reiter CMS settings.

- 2 **Communication type** – wählen Sie die Verbindung **IP** (SMS ist als Primärkanal nicht empfohlen).
- 3 **Protocol** – **TRK** für einen Trikdis-Empfänger, **DC-09_2007** oder **DC-09_2012** für einen universellen Empfänger, **TL150** für einen SUR-GARD-Empfänger.
- 4 **TRK encryption key** – der im Empfänger eingestellte 6-stellige Verschlüsselungsschlüssel.
- 5 **Domain or IP** – Domainname oder IP-Adresse des Empfängers.
- 6 **Port** – Portnummer des Empfängers.
- 7 **TCP or UDP** – das Übertragungsprotokoll; richtet sich nach der Einstellung des Empfängers.
- 8 **Primary channel Backup** – Ersatzkanal bei einem Fehler des Primärkanals; genauso ausfüllen, die Angabe wird empfohlen.
- 9 **Backup SMS reporting number** – wenn ein Trikdis-SMS-Empfänger vorhanden ist, tragen Sie hier dessen Telefonnummer ein: Das Gerät sendet direkt nach dem ersten Start 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 Abschnitt 2.2 noch nicht getan haben.

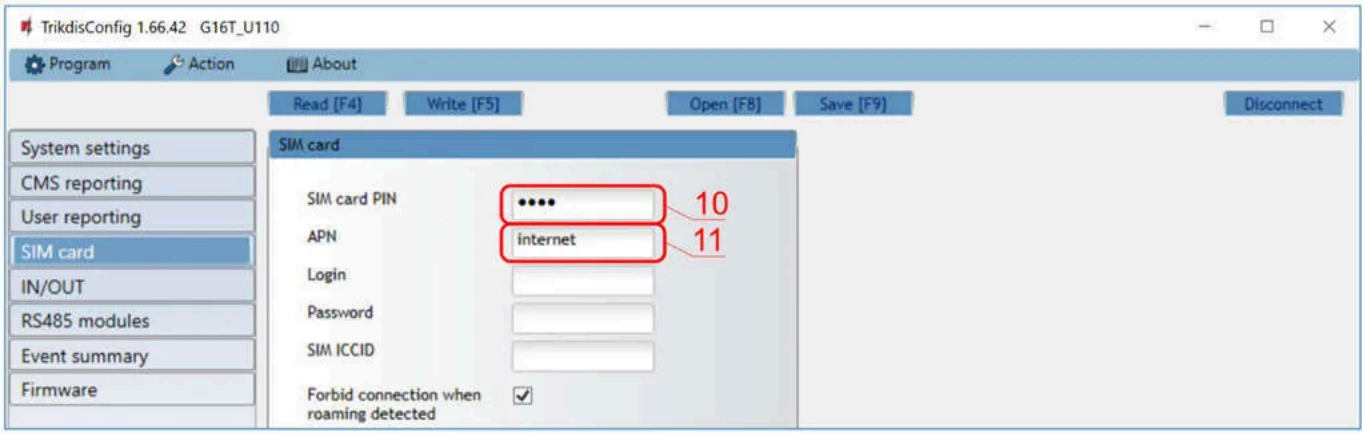


Abbildung 10. TrikdisConfig – Seite SIM card.

- 10 **SIM card PIN** – der PIN-Code der Karte.
- 11 **APN** – der Zugangspunkt des Anbieters (siehe Abschnitt 2.2).

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

Drücken Sie am Ende der Einstellungen **Write [F5]** (Schreiben), warten Sie die Rückmeldung ab und ziehen Sie das USB-Kabel ab. Damit ist das Gerät bereit zum Anschließen. Auch hier muss der Telefonwähler der Alarmzentrale eingeschaltet und eingestellt werden, sonst sendet die Zentrale keine Ereignisse (Kapitel 4).

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 Abschnitt 2.1) und ziehen Sie den Klemmenblock 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 in Abschnitt 2.1).
4. Befestigen Sie die Rückwand mit Schrauben am gewählten Ort.
5. Setzen Sie die Leiterplatte wieder in die Rückwand ein und stecken Sie den Klemmenblock wieder auf.
6. Schrauben Sie die GSM-Antenne an.
7. Setzen Sie die Frontabdeckung wieder auf.

Die SIM-Karte muss aktiv sein, und für den IP-basierten Betrieb muss die mobile Datenverbindung auf ihr funktionieren. Wenn TrikdisConfig keinen PIN-Code abfragen soll, schalten Sie die PIN-Abfrage der Karte in einem Telefon ab.

3.2 Montageort und Antenne

- Montieren Sie den Kommunikator an einem **trockenen Ort im Innenbereich**, möglichst in der Nähe des Gehäuses der Alarmzentrale, damit die Verdrahtung kurz bleibt.
- In einem **Metallgehäuse** wird das Mobilfunksignal stark gedämpft. Kommt der Kommunikator in das Metallgehäuse der Zentrale, führen Sie die Antenne aus dem Gehäuse heraus oder verwenden Sie eine Antenne mit längerem Kabel.
- **Prüfen Sie vor der endgültigen Befestigung den Signalpegel**: Die Anzahl der gelben Blinkzeichen der NETWORK-LED sollte bei 2G mindestens 5, bei 4G mindestens 3 betragen (siehe Abschnitt 1.6). Sind es weniger, suchen Sie einen besseren Ort oder wechseln Sie zu einer empfindlicheren, abgesetzt montierbaren 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 G16T wird an den Telefonleitungsausgang (TIP/RING) der Zentrale angeschlossen, die Versorgung erhält er vom 12-V-Hilfsausgang (AUX) der Zentrale.

Empfohlener, normaler Anschluss: DC+, DC−, TIP und RING. Dabei erkennt der Kommunikator nicht, wenn die Leitung unterbrochen wird.

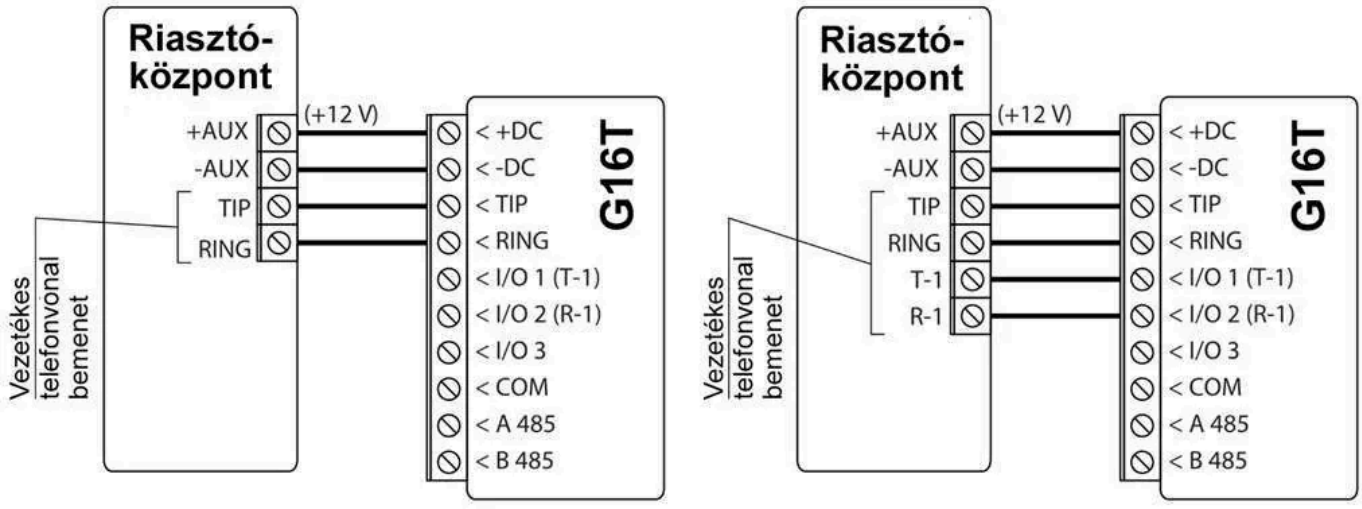


Abbildung 11. Anschluss an den Telefonleitungsausgang der Zentrale: links der normale Anschluss, rechts der Anschluss mit Leitungsüberwachung.

Der G16T 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 einem Stromausfall der Akku der Zentrale auch den Kommunikator.

3.3.1 Bei Bedarf: Leitungsüberwachung

Nur nötig, wenn eine Leitungsüberwachung gebraucht wird: Dann meldet der Kommunikator, wenn die Verbindung zwischen ihm und der Alarmzentrale unterbrochen wird.

1. Schließen Sie zusätzlich zum normalen Anschluss auch diese zwei Adern an: die Klemme **T-1** der Zentrale an die Klemme **I/O 1 (T-1)** des Kommunikators, die Klemme **R-1** der Zentrale an die Klemme **I/O 2 (R-1)**.
2. Schalten Sie auf der Seite **System settings** von TrikdisConfig die Option **Line supervision** ein.
3. Die nötigen Einstellungen auf Seiten der Alarmzentrale prüfen Sie in der Installationsanleitung der Zentrale.

In diesem Fall sind I/O 1 und I/O 2 nicht für andere Zwecke verwendbar.

3.4 Anschluss einer Schlüsselschalter-Zone

Wenn Sie die Zentrale aus der Ferne, aus der App Protegus 2, scharf- und unscharfschalten möchten, stellen Sie eine der I/O-Klemmen des Kommunikators als **Ausgang** ein und verbinden Sie sie mit einer **Schlüsselschalter-Zone** der Zentrale. Der Ausgang zieht die Zone bei Aktivierung auf COM (negativ); schließen Sie den Abschlusswiderstand der Zone passend zum Zonentyp der Zentrale an. Da der G16T drei I/O-Klemmen hat, lassen sich bis zu drei Bereiche mit je einem eigenen Ausgang steuern. Stellen Sie die für den Schlüsselschalter verwendete Klemme in TrikdisConfig auf der Seite **IN/OUT** auf die Funktion **OUT** (Abschnitt 6.6). Die Hardware 3 hat einen programmierbaren Ausgang (OUT), der einen Bereich steuern kann; dort muss auf der Seite **System settings** das Feld **Output OUT1 mode** auf **Remote control** stehen (das ist die Werkseinstellung).

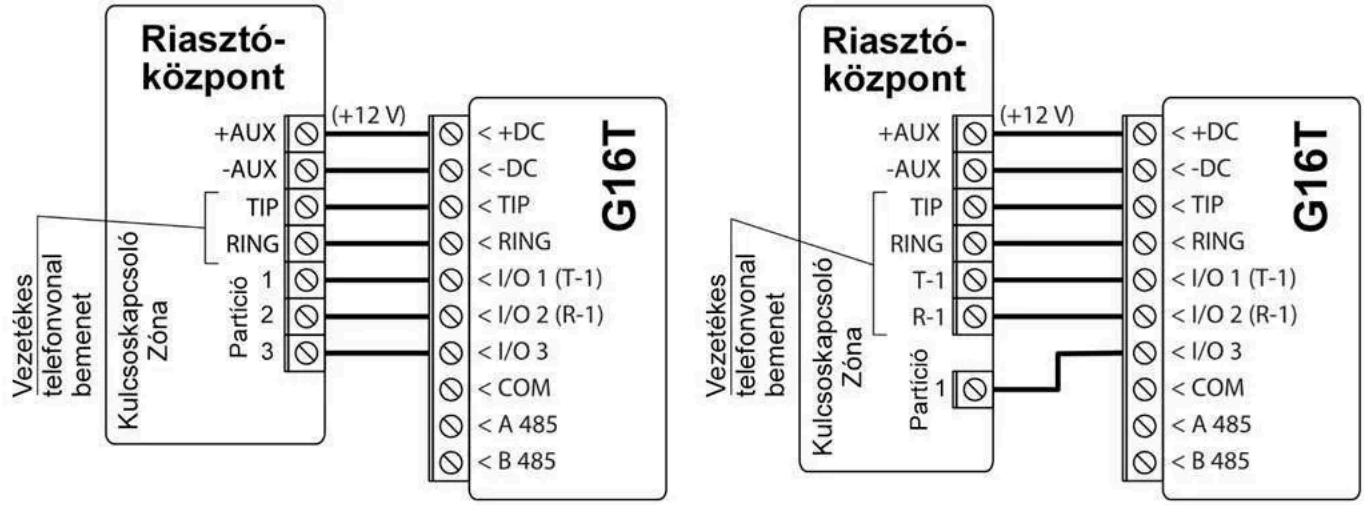


Abbildung 12. Scharf- und Unscharfschalten mit einer Schlüsselschalterzone: links der normale Anschluss, rechts der Anschluss mit Leitungsüberwachung (dann bleibt I/O 3 für den Schlüsselschalter).

Die Schlüsselschalter-Zone kann impulsgesteuert oder bistabil sein – in der App Protegus 2 muss derselbe Modus eingestellt werden (Abschnitt 5.2). Über Details und Fallstricke der Scharfschaltung per Schlüsselschalter gibt es einen eigenen Artikel: Fern-Scharfschaltung mit Schlüsselschalter aus der App Protegus 2.

3.5 Anschluss von Eingängen

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

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 NC, NO, EOL und DEOL mit Abschlusswiderstand 2,2 kΩ, bei den DEOL-Typen mit Sabotagekreis.

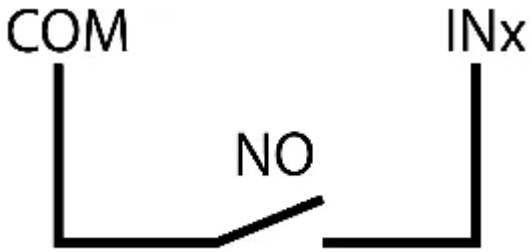


Abbildung 13. NO – im Ruhezustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

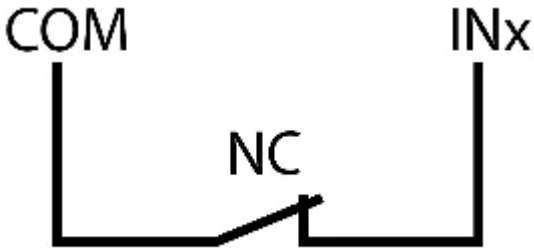


Abbildung 14. NC – im Ruhezustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

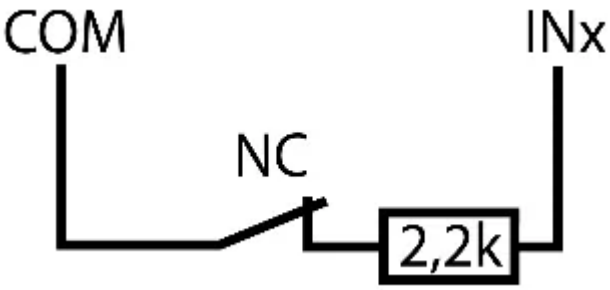


Abbildung 15. NC/EOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

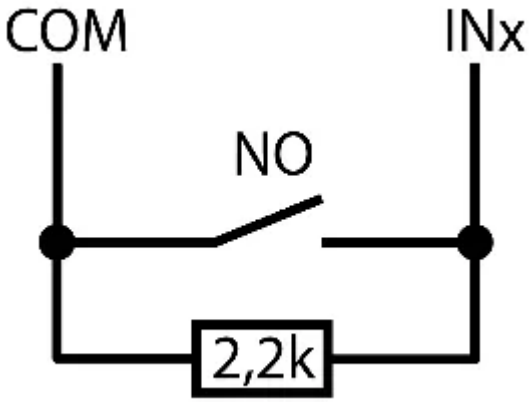


Abbildung 16. NO/EOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

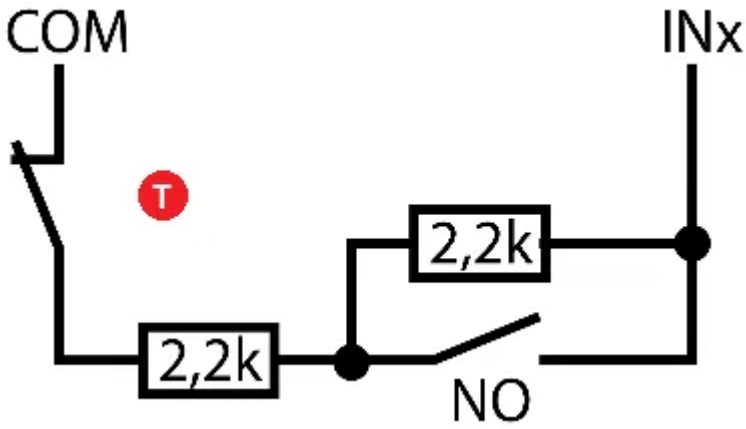


Abbildung 17. NO/DEOL – im Ruhezustand offener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

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

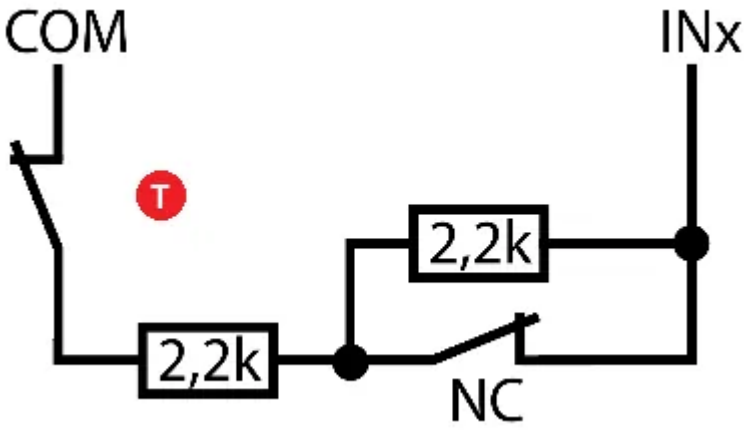


Abbildung 18. NC/DEOL – im Ruhezustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

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

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.

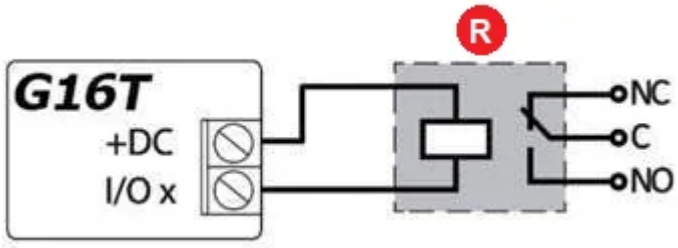


Abbildung 19. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule liegt zwischen +DC und der Klemme I/O x, die Kontakte (NC, C, NO) schalten den Verbraucher.

- R Relais („Relay")

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

3.7 Anschluss der Erweiterung iO-8

Werden mehr Ein- oder Ausgänge benötigt, können an den RS485-Bus der **4G-Version** bis zu vier **iO-8**-Erweiterungen angeschlossen werden; jede bringt 8 weitere I/Os mit Doppelfunktion. An denselben Bus können auch die übrigen drahtgebundenen oder drahtlosen Erweiterungen der Trikdis-iO-Serie angeschlossen werden, zum Beispiel wenn Sie einen Temperatursensor anschließen möchten: Die Erweiterung **iO** hat 1 Eingang, 1 Relaisausgang und einen 1-Wire-Bus für Temperatursensoren (Einstellung in Abschnitt 6.7). Verbinden Sie die Klemmen A 485 und B 485 mit den Klemmen A und B des Moduls und versorgen Sie das Modul aus den 12 V der Zentrale. Das Modul muss in TrikdisConfig auf der Seite **RS485 modules** hinzugefügt werden (Abschnitt 6.7).

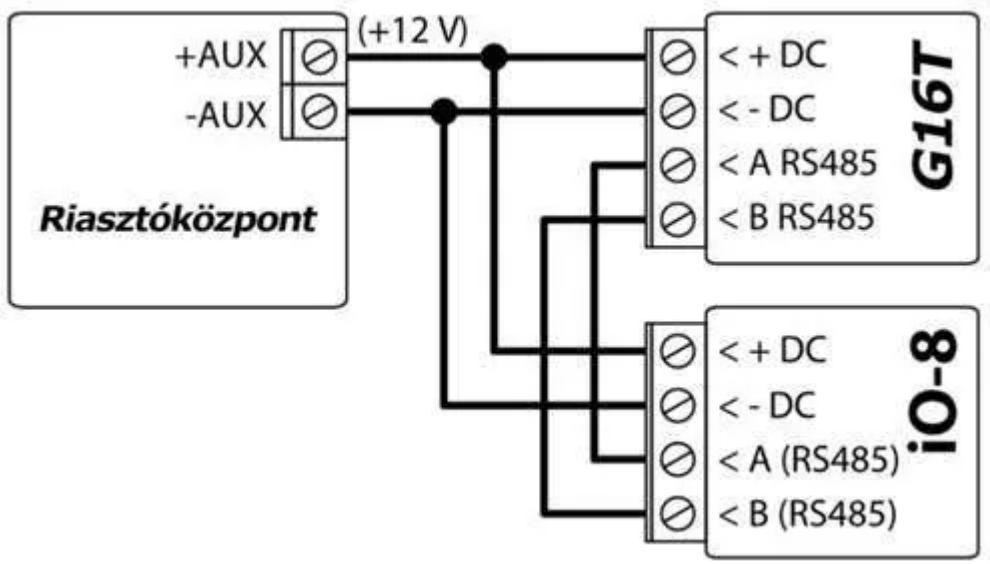


Abbildung 20. Anschluss der Erweiterung iO-8 an den RS485-Bus des G16T; Versorgung vom AUX-Ausgang der Alarmzentrale.

Der G16T mit 2G-Modem (G16T_G410) hat keinen RS485-Bus, daher können an ihn keine iO-8-, W485- oder E485-Module 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 G16T darüber (die Meldungen an die Leitstelle und an Protegus laufen über den WLAN-Router bzw. das kabelgebundene Internet, die mobile Datenverbindung wird dann nicht genutzt); bricht sie ab, wechselt er auf die mobile Datenverbindung und kehrt nach Wiederherstellung der Verbindung zum Modul zurück. Damit das Modul funktioniert, **muss im G16T eine SIM-Karte stecken**.

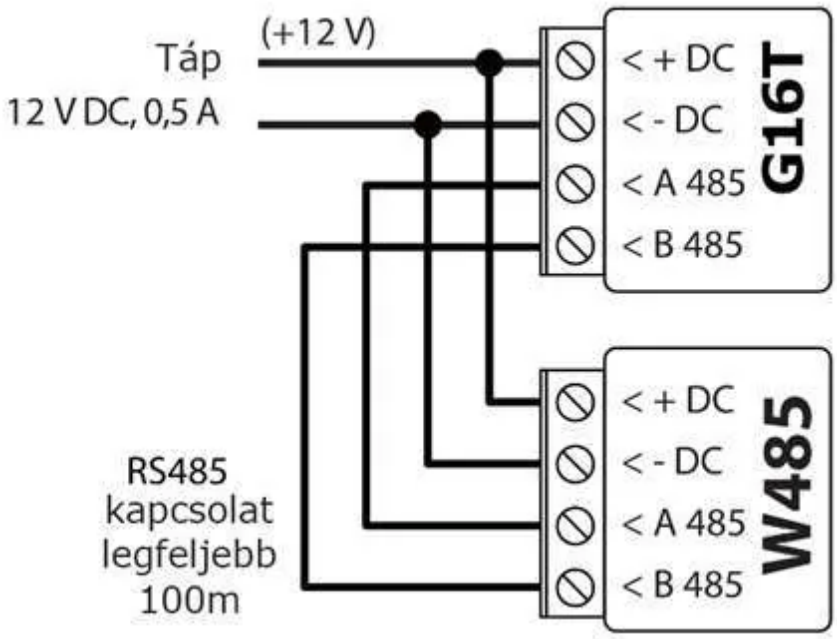


Abbildung 21. Anschluss des WLAN-Moduls W485 an den G16T über den RS485-Bus. Beide Geräte laufen an einer gemeinsamen Versorgung mit 12 V DC (mindestens 0,5 A) (Versorgungseingang des Moduls 9–28 V DC); das RS485-Kabel darf höchstens 100 m lang sein.

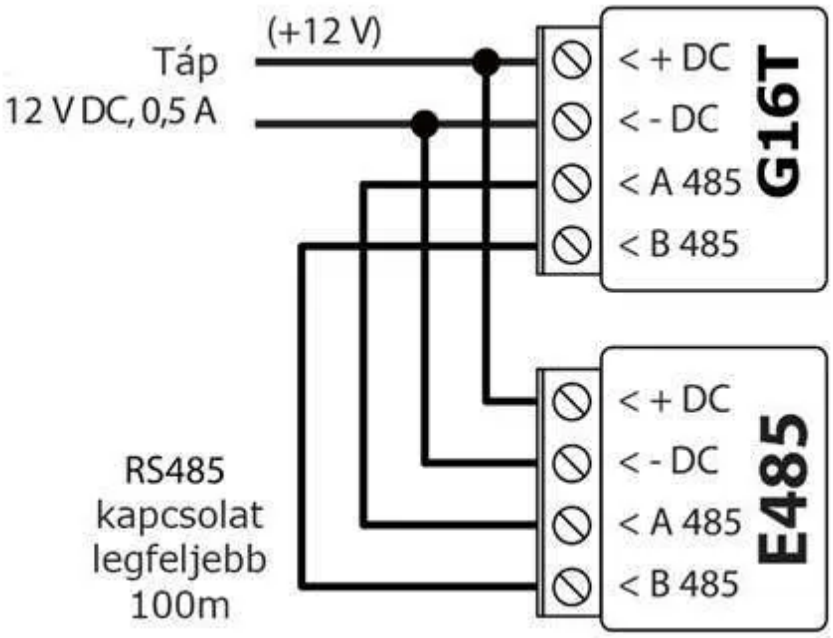


Abbildung 22. Anschluss des Ethernet-Moduls E485 an den G16T über den RS485-Bus. Beide Geräte laufen an einer gemeinsamen Versorgung mit 12 V DC (mindestens 0,5 A) (Versorgungseingang des Moduls 9–28 V DC); das RS485-Kabel darf höchstens 100 m lang sein.

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 in TrikdisConfig auf der Seite **RS485 modules** vor (Abschnitt 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 Frontabdeckung sollten Sie Folgendes sehen:

- **POWER** leuchtet grün – die Versorgung ist in Ordnung;
- **NETWORK** leuchtet grün und blinkt gelb – mit dem Netz verbunden; die Anzahl der Blinkzeichen ist der Signalpegel (bei 2G sind 5, bei 4G 3 gut); zählen Sie weniger, ist das Signal schwach: Suchen Sie einen anderen Ort für den Kommunikator oder verwenden Sie eine empfindlichere Antenne (Abschnitt 3.2);
- **TROUBLE** leuchtet nicht.

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

4. Programmierung der Alarmzentrale

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

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

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

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

4.1 Programmierung des Wählers der Honeywell Vista

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

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

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

Programmadresse	Wert	Programmadresse	Wert	Programmadresse	Wert
`*41`	1234 (Telefonnummer des Empfängers)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (Objektkennung)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

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

4.2 Zentralen anderer Hersteller

Suchen Sie in der Installationsanleitung jeder Zentrale dieselben vier Einstellungen: Aktivierung des Telefonleitungs-Kommunikators, Telefonnummer des Empfängers, Wählverfahren (DTMF) und Übertragungsformat (Contact ID). Wartet die Zentrale vor dem Wählen auf einen Wählton (dial tone), liefert ihn der G16T; startet der Anruf trotzdem nicht, schalten Sie in der Zentrale die Wähltonerkennung ab („Wählen ohne Wählton“ oder eine ähnliche Option).

Wenn die Zentrale am Ende des Anrufs einen Fehler meldet, obwohl das Ereignis angekommen ist, prüfen Sie in TrikdisConfig auf der Seite **System settings** die Einstellung **Wait acknowledgment from CMS**: Ist sie eingeschaltet, beendet der Kommunikator den Anruf erst nach der Quittung des Leitstellenempfängers (Kiss-

off). In einem System ohne Leitstelle, nur mit Protegus 2, lassen Sie sie ausgeschaltet (das ist die Werkseinstellung), denn es gibt keinen Empfänger, der quittieren würde.

5. Fernsteuerung mit der App Protegus 2

Mit der Mobil- 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.

5.1 Gerät hinzufügen

Prüfen Sie vor dem Hinzufügen des Geräts:

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

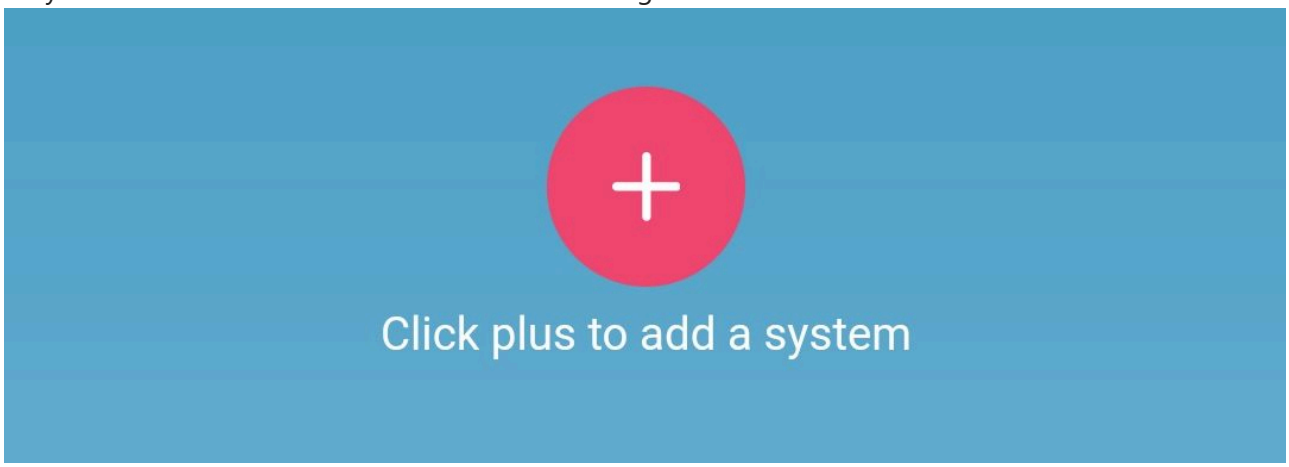
A rendszer létrehozása a Protegus 2 alkalmazásban

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





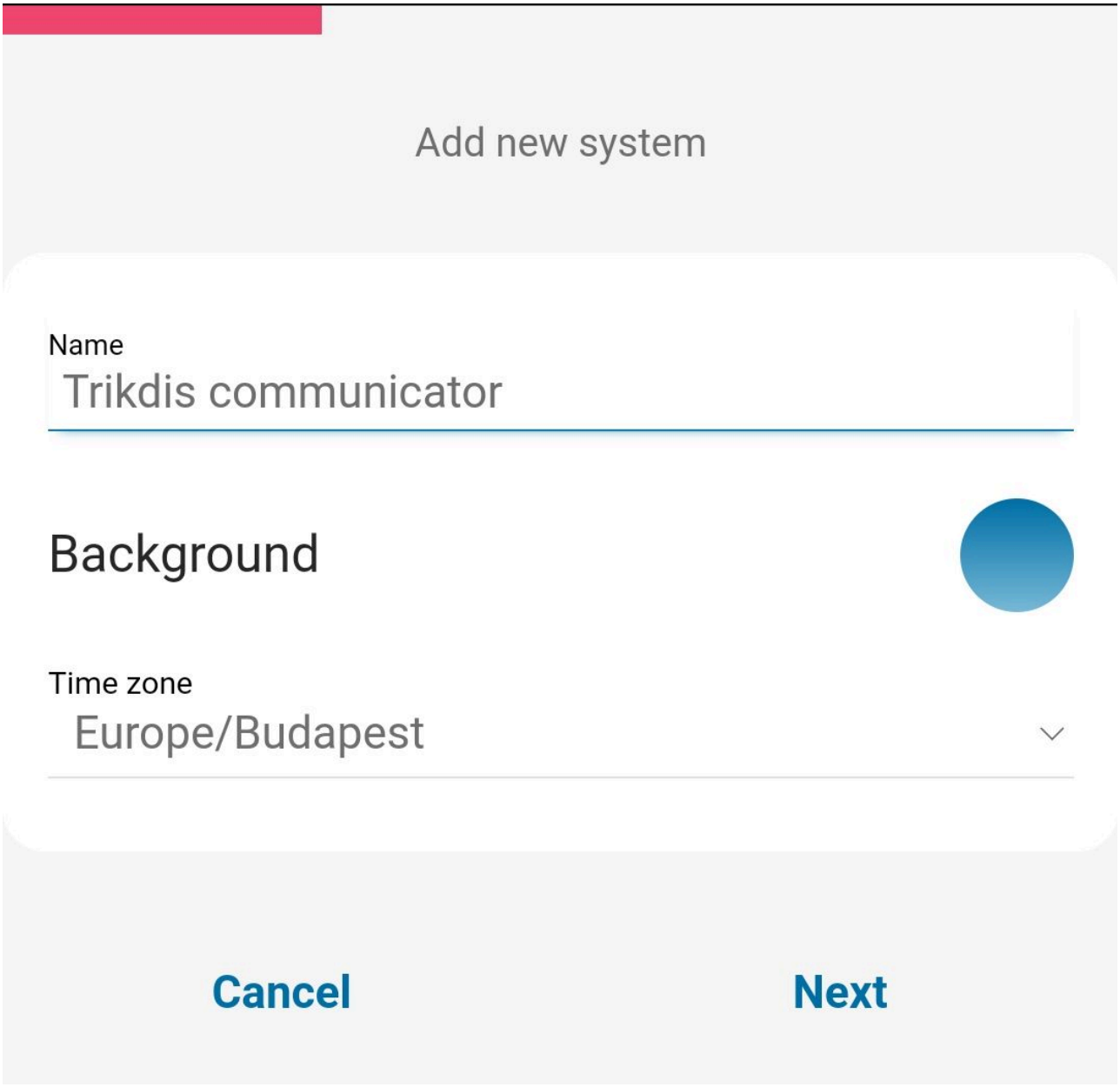
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



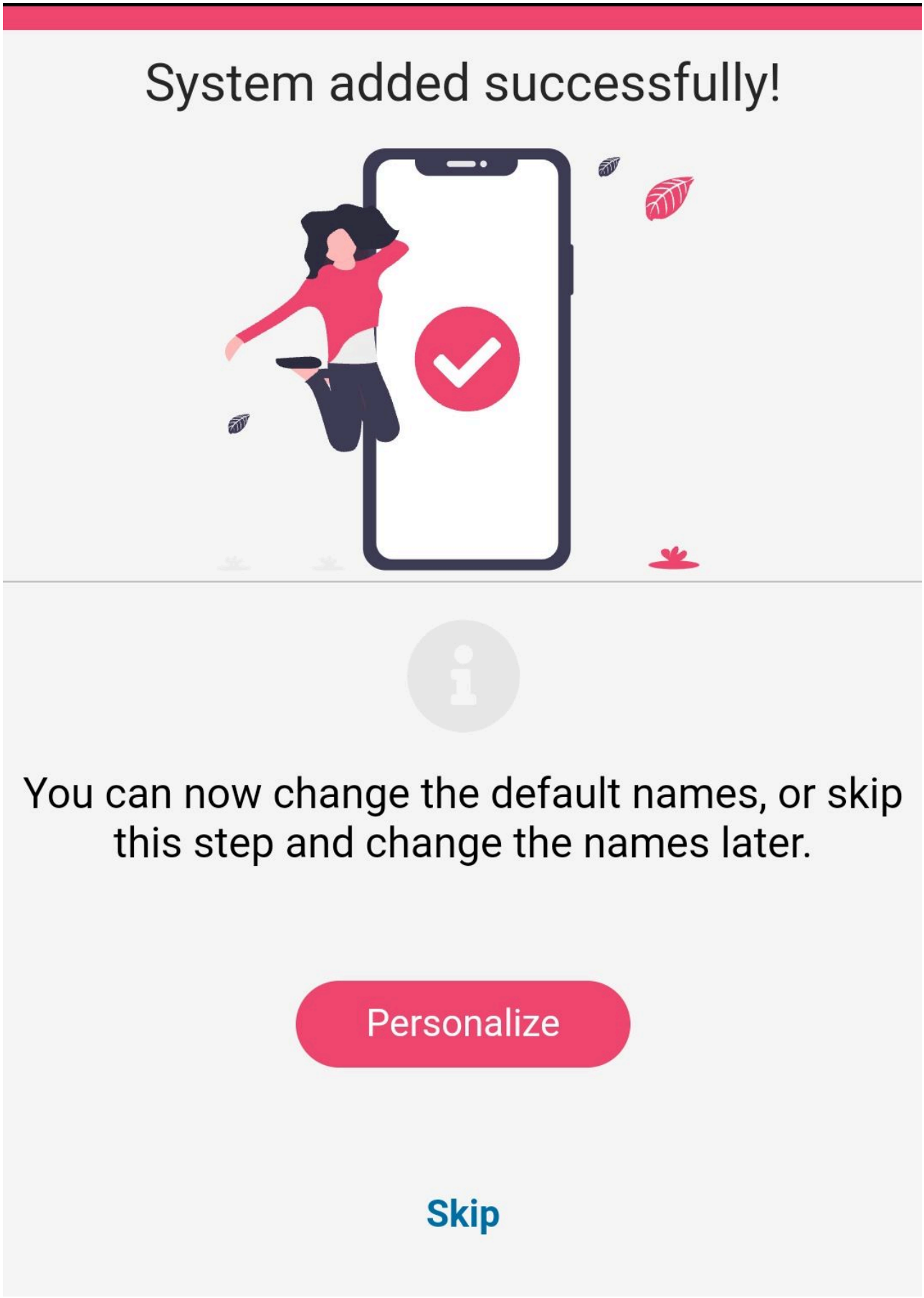
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



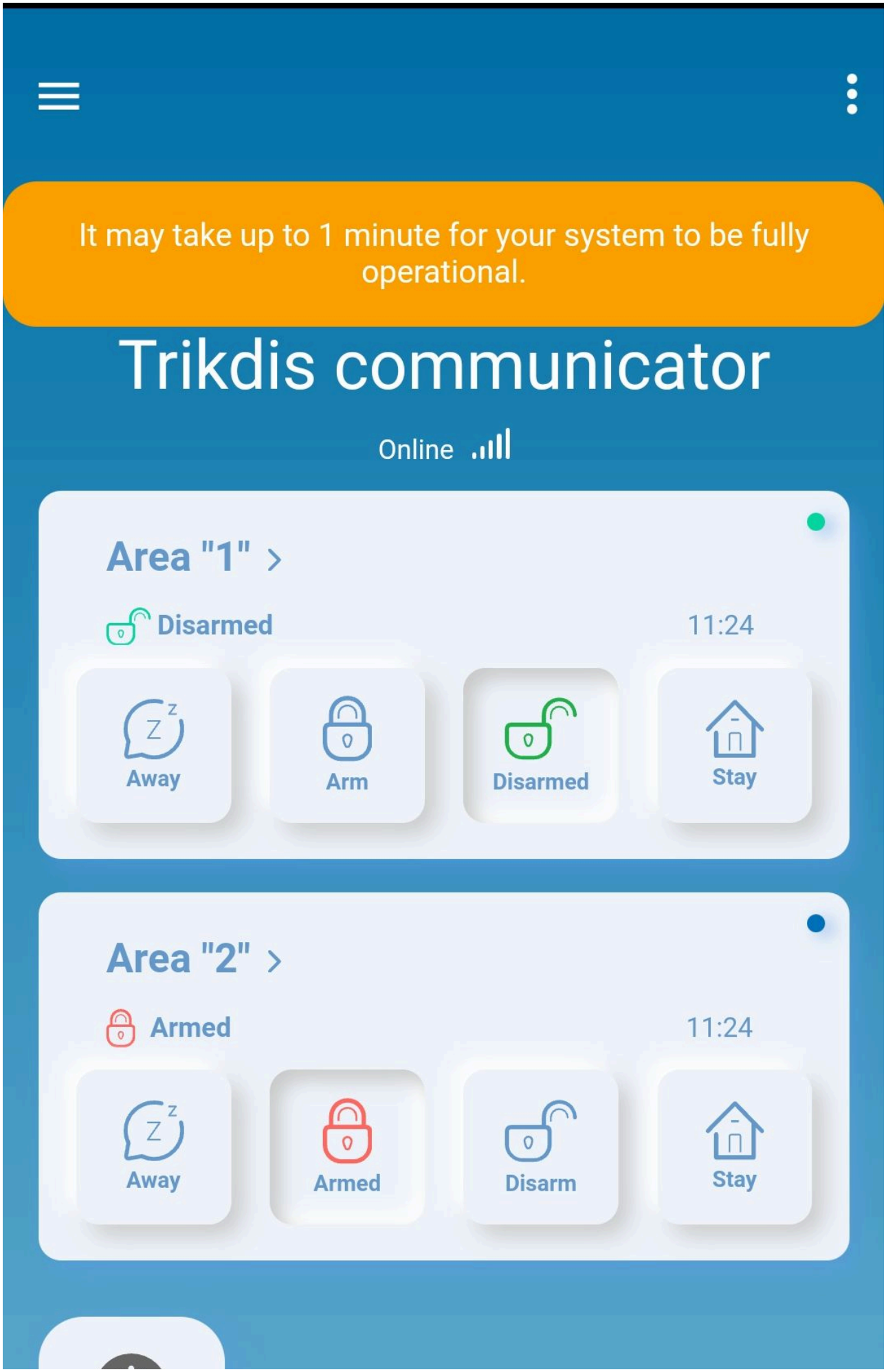
6. Add meg a rendszer nevét és válassz idozónát



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 wird auch in der Statusleiste von TrikdisConfig angezeigt.

5.2 Scharf- und Unscharfschalten mit einem Ausgang

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

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

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

1. Wählen Sie den Bereich aus (oder legen Sie ihn an), den Sie steuern möchten. Die Bereichsnummer muss mit der übereinstimmen, die die Zentrale in den Ereignissen sendet (Bereich 1 ist 1, Bereich 2 ist 2).
2. Aktivieren Sie die Option **Steuerung mit PGM** (Control with Protegus2) und wählen Sie im Feld **Ausgang** (Assigned Output) den Ausgang des Kommunikators (PGM1, PGM2 …). Ein Ausgang kann nur einen Bereich steuern.
3. Wählen Sie die Betriebsart: **Impuls** (Pulse) oder **bistabil** (Level) – dieselbe, die Sie in der Zentrale bei der Schlüsselschalterzone eingestellt haben. Üblicherweise verwenden wir den Impulsbetrieb; auch die Impulslänge kann angegeben werden (Standard 3 s).
4. Speichern Sie die Einstellung (**Save**). Bei mehreren Bereichen wiederholen Sie dies für jeden, mit seinem eigenen Ausgang: Im Assistenten legen Sie den weiteren Bereich mit der Schaltfläche **Click to add an area** an und stellen seinen PGM-Ausgang auf die gleiche Weise ein. Wenn Sie alle Bereiche eingestellt haben, gehen Sie im Assistenten mit der Schaltfläche **Skip** weiter.

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

5.3 Scharf- und Unscharfschalten aus der App

1. Öffnen Sie das System in der Protegus-2-App. Auf dem Startbildschirm hat jeder Bereich eine eigene Karte und ein eigenes Schloss: Das **geschlossene, rote Schloss** steht für einen scharfgeschalteten, das **offene, grüne Schloss** für einen unscharfgeschalteten Bereich.

2. Tippen Sie auf das Schloss des Bereichs und wählen Sie die gewünschte Aktion: Scharfschalten oder Unscharfschalten.
3. Wenn die App danach fragt, geben Sie den PIN-Code ein.

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

5.4 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.

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`
`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`

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.

Beim G16T hat der Befehl `CONNECT` noch einen weiteren Parameter: `CP=1` schaltet die Telefonleitungs-Schnittstelle des Kommunikators aus, `CP=2` schaltet sie ein. Beispiel: `123456 CONNECT CP=2`.

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]**) und unten die Statusleiste. Dieses Kapitel geht die Einstellungen des G16T 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.
SN	Seriennummer.
BL	Die Version des Bootloaders.
FW	Die Version der Firmware.
HW	Die Version der Hardware.
State	Die Verbindungsart: USB oder Fernzugriff (remote).
Administrator / Installer	Die Zugriffsebene der programmierenden Person (nach Eingabe des Passworts).

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



Abbildung 23. Die Statusleiste von TrikdisConfig mit ausgelesenem G16T: Kennung, Zustand, Typ, Seriennummer, Versionen, Verbindungsart und Zugriffsebene.

Nach **Read [F4]** liest das Programm die im Gerät eingestellten Werte aus und zeigt sie an; nehmen Sie die nötigen Einstellungen gemäß den folgenden Seitenbeschreibungen vor.

6.2 System settings

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

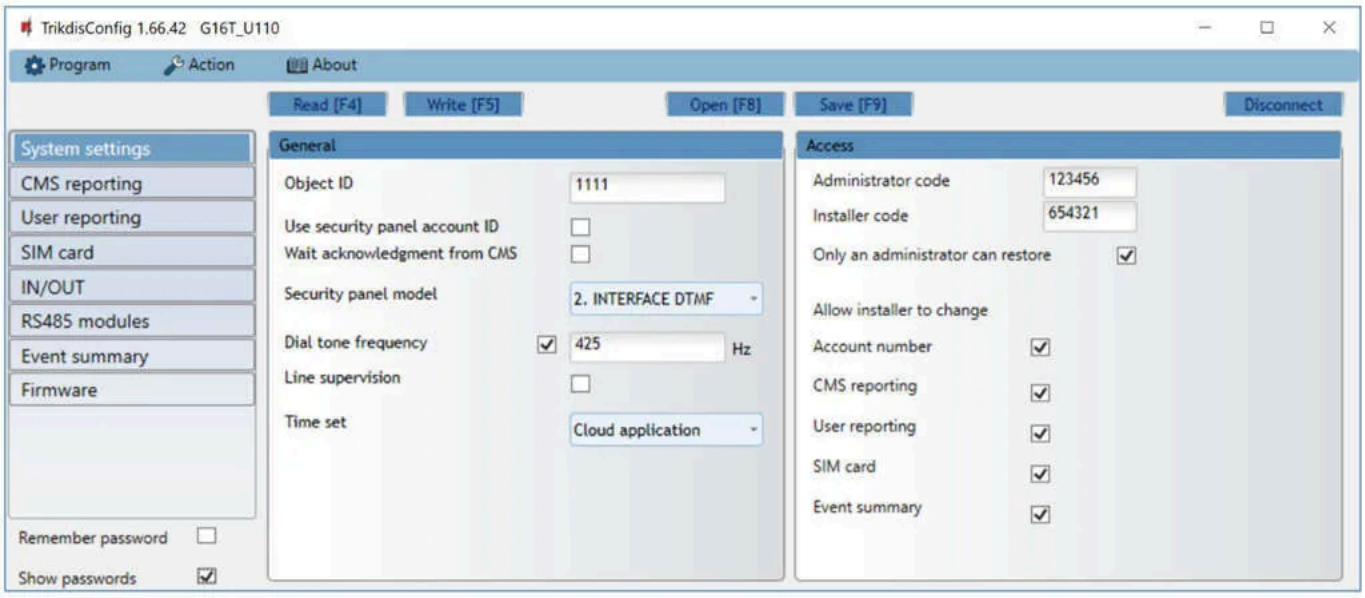


Abbildung 24. TrikdisConfig – Seite System settings: Gruppen General und Access.

- **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen: 0–9, A–F; `FFFE` und `FFFF` sind nicht zulässig). Pflichtangabe, wenn das Gerät auch an eine Leitstelle meldet.
- **Use security panel account ID** – angehakt verwendet der Kommunikator nicht seine eigene Object ID, sondern die Kennung, die die Zentrale in der Contact-ID-Meldung sendet. Nützlich, wenn mehrere Bereiche mit eigener Kennung melden.
- **Wait acknowledgment from CMS** – angehakt wartet der Kommunikator nach jedem Ereignis auf die Quittung des Empfängers und sendet erst danach das Abschlusssignal (Kiss-off) an die Zentrale. Kommt keine Quittung, sendet die Zentrale das Ereignis erneut. In einem System ohne Leitstelle, nur mit Protegus 2, lassen Sie die Option ausgeschaltet (Werkseinstellung).
- **Security panel model** – der Typ der Telefonleitungs-Schnittstelle (damit aktivieren oder deaktivieren Sie die DTMF-Telefonleitungs-Schnittstelle des Kommunikators); Standard ist **2. INTERFACE DTMF**.
- **Dial tone frequency** – die Frequenz des Wähltons, den der G16T zur Zentrale hin liefert (Standard 425 Hz, der in den meisten europäischen Ländern übliche Wählton).
- **Line supervision** – Überwachung der Leitung zwischen Zentrale und Kommunikator; erfordert zusätzlich den Anschluss der Adern T-1 und R-1 (Abschnitt 3.3.1).
- Den Typ der Eingänge und die Rolle der Ausgänge stellen Sie bei der Hardware 4 auf der Seite **IN/OUT** ein (Abschnitt 6.6). Bei der Hardware 3 befinden sich diese beiden Felder hier: **Input IN1-IN2 type** – der Eingangstyp aus der Liste (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL); **Output OUT1 mode** – die Betriebsart des Ausgangs aus der Liste.
- **Time set** – die Quelle für die Uhr des Geräts (Standard **Cloud application**, die Protegus-Cloud).

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 laufen: Der **Primärkanal** und der **Parallelkanal** arbeiten gleichzeitig (an zwei Empfänger zugleich), und zu jedem gehört ein **Ersatzkanal**, der greift, wenn der jeweilige Kanal ausfällt. Die Kommunikation ist verschlüsselt und passwortgeschützt; für den Empfang und die Weiterleitung der Ereignisse an die Leitstellensoftware wird ein Trikdis-Empfänger (Software-Empfänger IPcom – Windows oder Linux –, RL14, RM14; für den SMS-Empfang IP/SMS-Empfänger RL14, Mehrkanal-Empfänger RM14 oder SMS-Empfänger GM14) oder ein universeller Empfänger mit dem Protokoll DC-09 / TL150 benötigt. SMS ist als Ersatzkanal besonders nützlich, weil es ohne mobiles Internet funktioniert; als Primärkanal empfehlen wir es nicht.

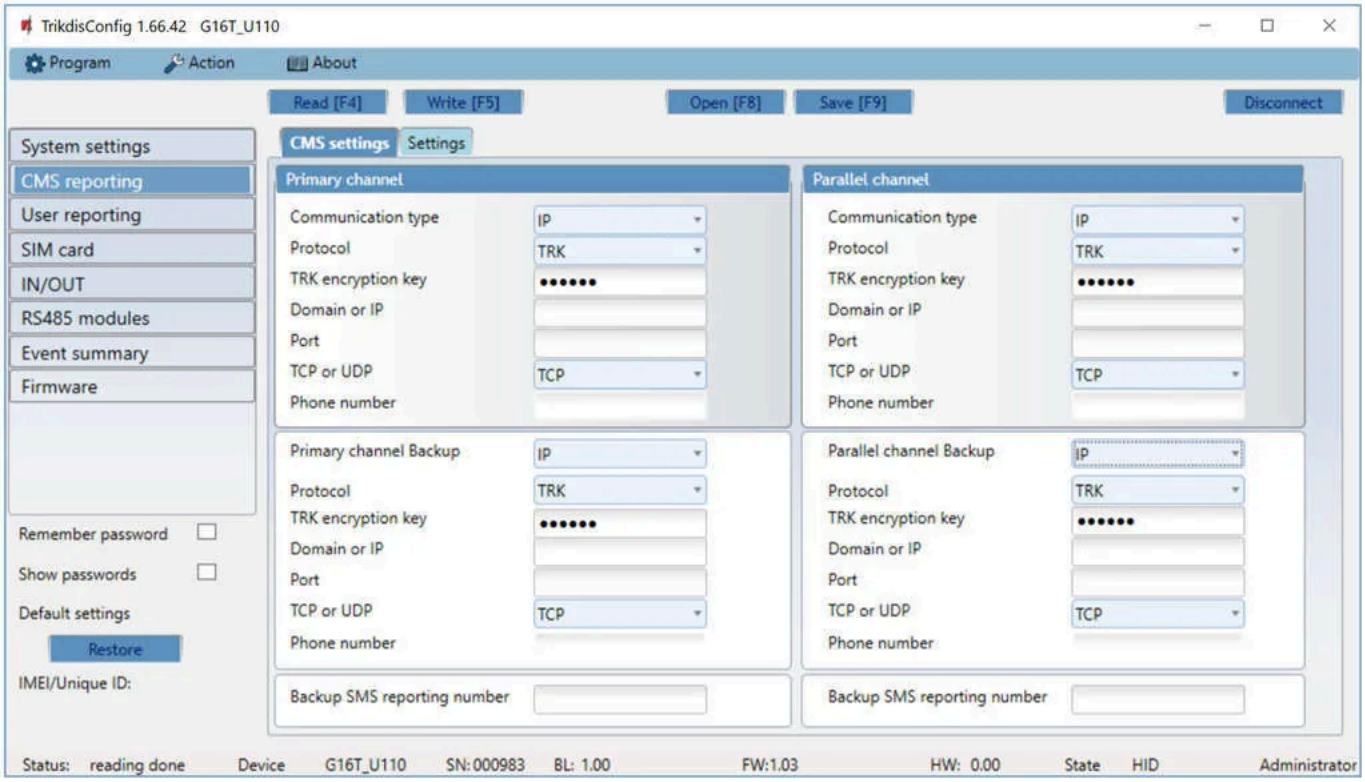


Abbildung 25. TrikdisConfig – CMS reporting, Reiter CMS settings: Primär-, Ersatz- und Parallelkanal.

Primary channel – Primärkanal

- **Communication type** – IP oder SMS.
- **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 Ländervorwahl (z. B. `43xxxxxxxxx` für eine österreichische Nummer).

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

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

Backup SMS reporting number – SMS-Ersatznummer. Greift, wenn weder über den Primär-, noch über den Parallel-, noch über den Ersatzkanal gesendet werden kann; nützlich, weil sie ohne IP-Verbindung funktioniert. Sie ist nur aktiv, wenn Primär- und 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 Primärkanal als auch auf dessen Ersatzkanal abbricht. Geben Sie die Telefonnummer des Trikdis-SMS-Empfängers mit Ländervorwahl ein (z. B. `43xxxxxxxxx` für eine österreichische Nummer).

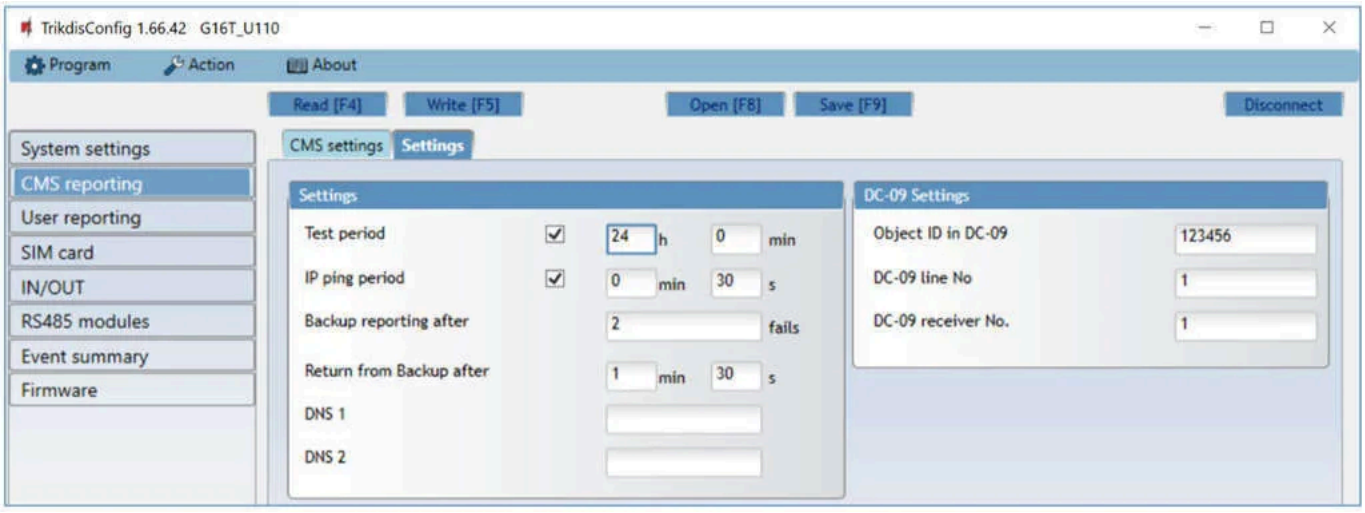


Abbildung 26. TrikdisConfig – CMS reporting, Reiter Settings: Testmeldung, PING, Zeiten des Ersatzkanals, DNS und die DC-09-Daten.

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

- **Test period** – Intervall des periodischen Testberichts (Standard 24 Stunden). Der Testbericht wird als Contact-ID-Meldung an die Leitstelle und an Protegus 2 gesendet.
- **IP ping period** – Intervall des Lebenszeichens (PING) auf dem IP-Kanal (Standard 30 s). Sie aktivieren es mit dem Häkchen und geben die Zeit in den Feldern für Minuten (**min**) und Sekunden (**s**) ein; es ist für die Überwachung der Verbindung erforderlich. Der Empfänger leitet die PINGs nicht an die Leitstellensoftware weiter, um sie nicht zu überlasten; die Software erhält nur dann eine Meldung, wenn der Empfänger innerhalb des Dreifachen der eingestellten Zeit keinen PING erhält. Beträgt die PING-Periode zum Beispiel 3 Minuten, wird der Verbindungsverlust nach der 9. Minute gemeldet.
- **Backup reporting after** – nach so vielen erfolglosen Sendeversuchen wechselt das Gerät auf den Reservekanal (Standard 2).
- **Return from Backup after** – nach dieser Zeit kehrt es auf den primären Kanal zurück (Standard 1 Minute 30 s).

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

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

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

Unten im Reiter: **DNS 1, DNS 2** – Namensserver (DNS, Domain Name System: liefert die zum Domainnamen gehörende IP-Adresse); sie werden benötigt, wenn Sie den Empfänger mit einem Domainnamen und nicht mit einer IP-Adresse angegeben haben. Standard ist das öffentliche DNS von Google.

6.4 User reporting

Im Reiter **PROTEGUS Cloud** aktivieren Sie den Protegus-Dienst. Mit dem Protegus-Dienst kann der Benutzer den Kommunikator und das daran angeschlossene System aus der Ferne überwachen und steuern; Details: www.protegus.app.

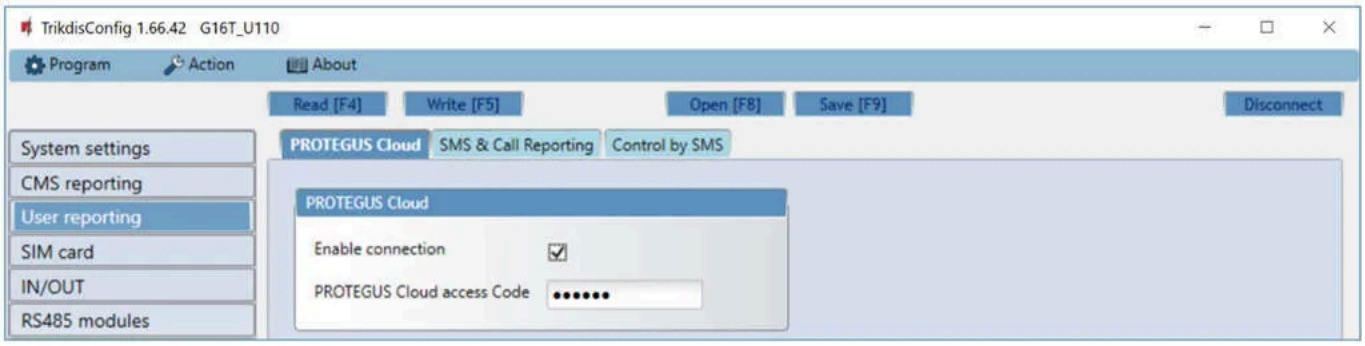


Abbildung 27. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- **Enable connection** – aktiviert die Verbindung zur Protegus-Cloud und den Fernzugriff von TrikdisConfig.
- **Protegus Cloud access code** – 6-stelliger Code für die Protegus-Verbindung (werkseitig `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 Telefonanruf über die Ereignisse benachrichtigt werden.

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

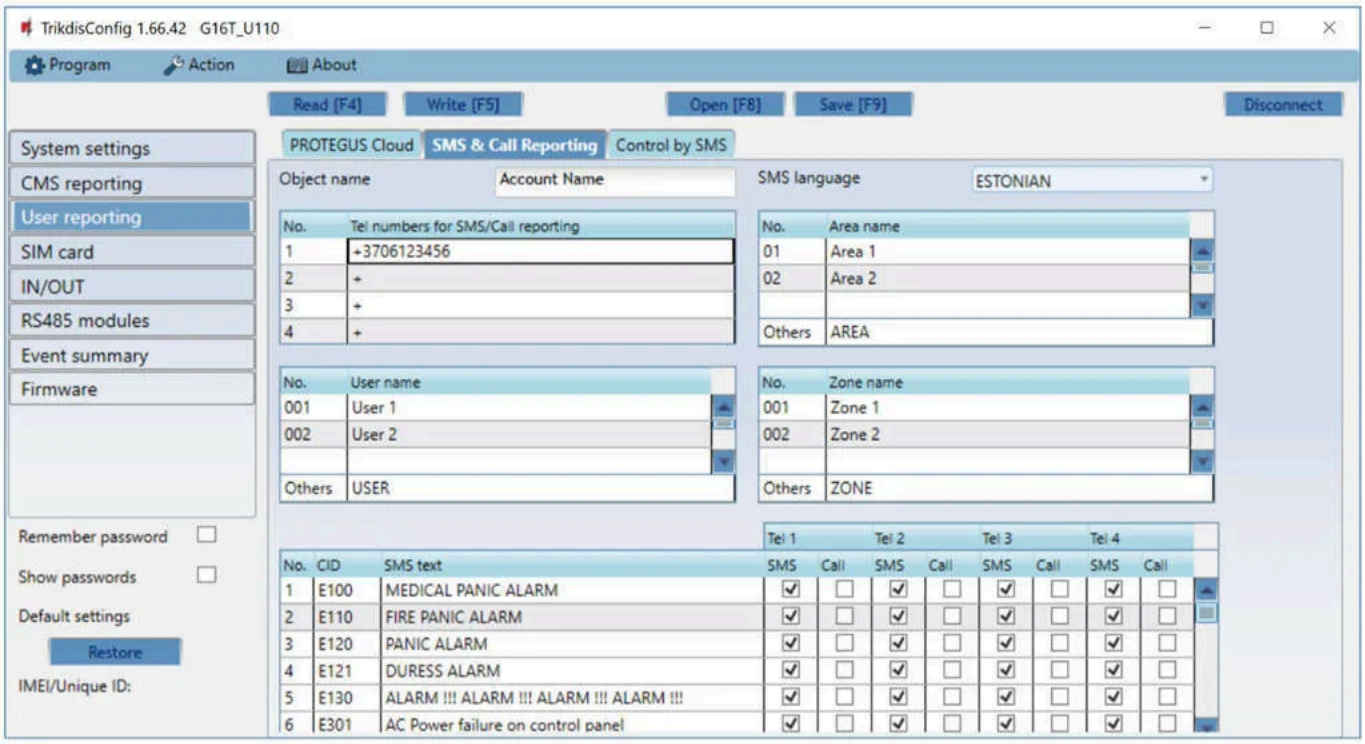


Abbildung 28. TrikdisConfig – User reporting, Reiter SMS & Call Reporting.

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

Im Reiter **Control by SMS** stellen Sie den Empfang von SMS-Befehlen ein (die Befehle beschreibt Abschnitt 5.4).

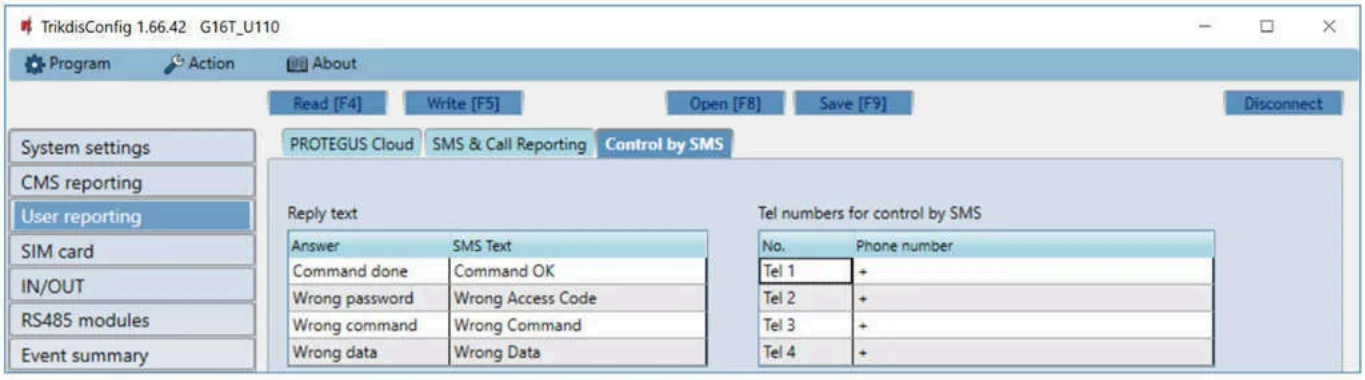


Abbildung 29. TrikdisConfig – User reporting, Reiter Control by SMS.

- **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). Die Antworttexte sind bearbeitbar.

- **Tel numbers for control by SMS** – bis zu 4 Nummern; das Gerät nimmt Befehle nur von diesen Nummern an. Ist das Feld leer, nimmt es einen Befehl mit korrektem Passwort von jeder Nummer an. Die Sicherheit ergibt sich auch dann daraus, 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 30. TrikdisConfig – Seite SIM card.

- **SIM card PIN** – der PIN-Code der Karte. Die PIN-Abfrage schalten Sie ab, indem Sie die Karte in ein Mobiltelefon einlegen und sie dort deaktivieren. Ist die PIN-Abfrage abgeschaltet, kann der Werkswert des Felds bleiben.
- **APN** – der Zugangspunkt des Anbieters; die bekannten APNs der Anbieter listet der APN-Artikel auf (für eine IoT- / M2M-Karte gibt der Anbieter einen eigenen APN an, siehe Abschnitt 2.2). Der APN ist für die Internetverbindung des Geräts nötig; wenn Sie keine anderen Angaben haben, versuchen Sie den APN `internet`, der allgemein gültig ist und in den Netzen vieler Anbieter funktioniert.
- **Login, Password** – APN-Benutzername und -Passwort, falls der Anbieter sie verlangt.
- **Forbid connection when roaming detected** – nützlich in Grenznähe: verhindert, dass sich das Gerät mit dem Netz des Nachbarlands verbindet.

Vergewissern Sie sich vor der Verwendung, dass die SIM-Karte aktiv ist und dass für die IP-Kommunikation der mobile Datendienst auf ihr freigeschaltet ist.

6.6 IN/OUT

Hier legen Sie die Rolle der drei I/O-Klemmen mit Doppelfunktion 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). Bei der Hardware 3 befinden sich diese Einstellungen auf der Seite **System settings** (Abschnitt 6.2).

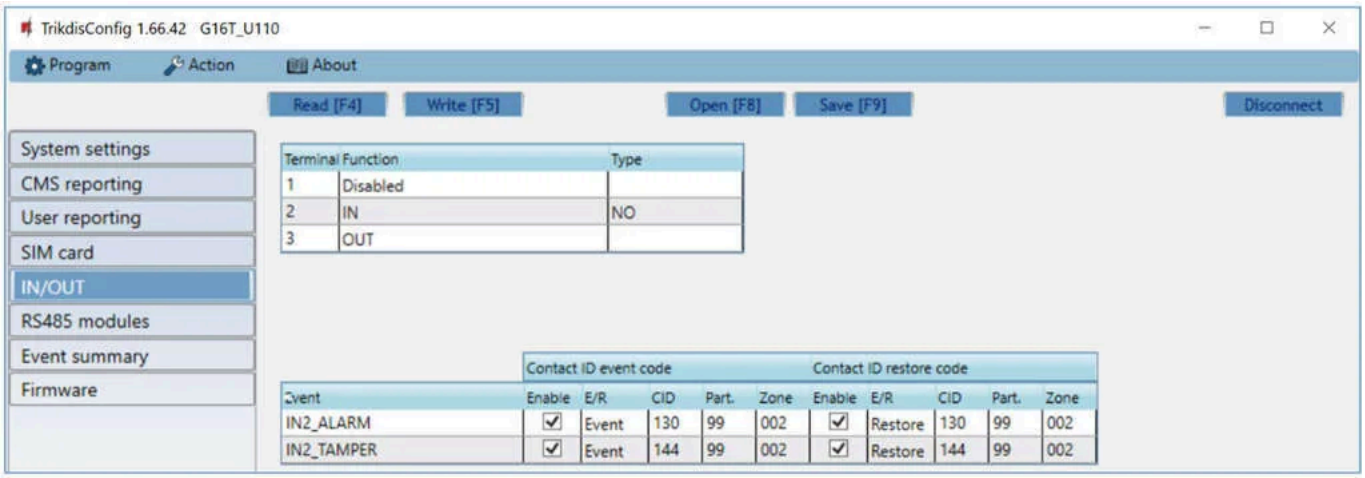


Abbildung 31. TrikdisConfig – Seite IN/OUT: Funktion der I/O-Klemmen und Ereignisse der Eingänge.

Wird der am Eingang angeschlossene Melder ausgelöst, sendet der Kommunikator ein eigenes Ereignis (**INx_ALARM**, Contact ID 130), bei Verletzung des Sabotagekreises ein Sabotageereignis (**INx_TAMPER**, 144) an die Leitstelle und an Protegus 2; in der Tabelle erscheinen die Ereignisse aller als Eingang eingestellten Klemmen. Die Spalten der Tabelle:

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

6.7 RS485 modules

Mit den Erweiterungen der iO-Serie lassen sich dem Kommunikator weitere Eingänge, Ausgänge und ein serieller Bus für Temperatursensoren hinzufügen. Die am RS485-Bus angeschlossenen iO-8-Erweiterungen (und die übrigen Erweiterungen der iO-Serie) sowie W485- / E485-Module müssen im Reiter **Modules list** hinzugefügt werden.

Beim G16T mit 2G-Modem (G16T_G410) ist diese Seite nicht verwendbar: Die 2G-Version hat keinen RS485-Bus.

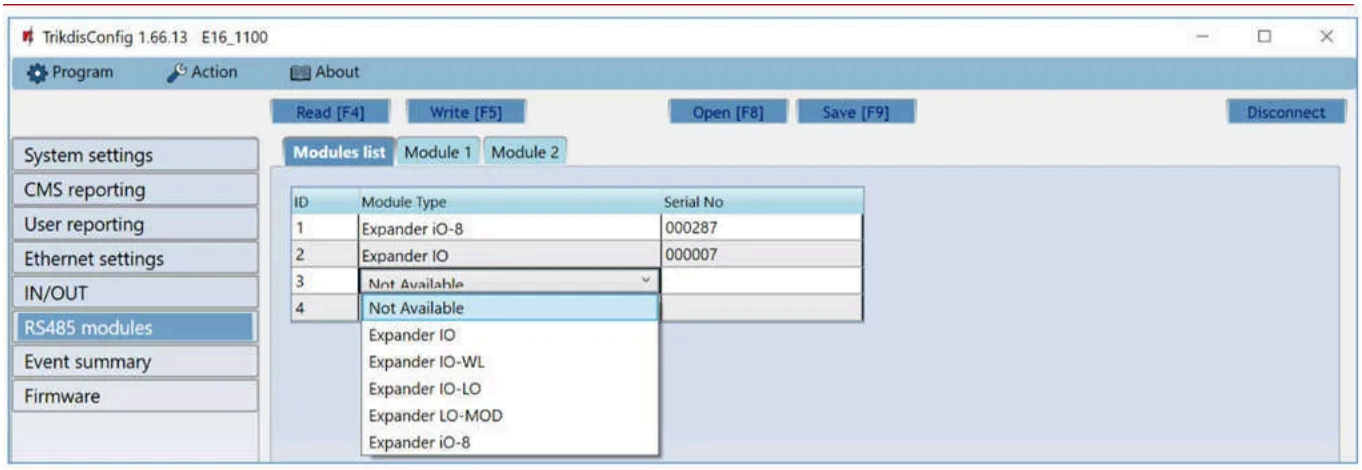


Abbildung 32. TrikdisConfig – RS485 modules, Reiter Modules list.

- **Module Type** – der Typ des angeschlossenen Moduls aus der Liste (iO-8 und andere Erweiterungen der iO-Serie, W485, E485).

- **Serial No** – die 6-stellige Seriennummer des Moduls (auf dem Modul und seiner Verpackung, SN).

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

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

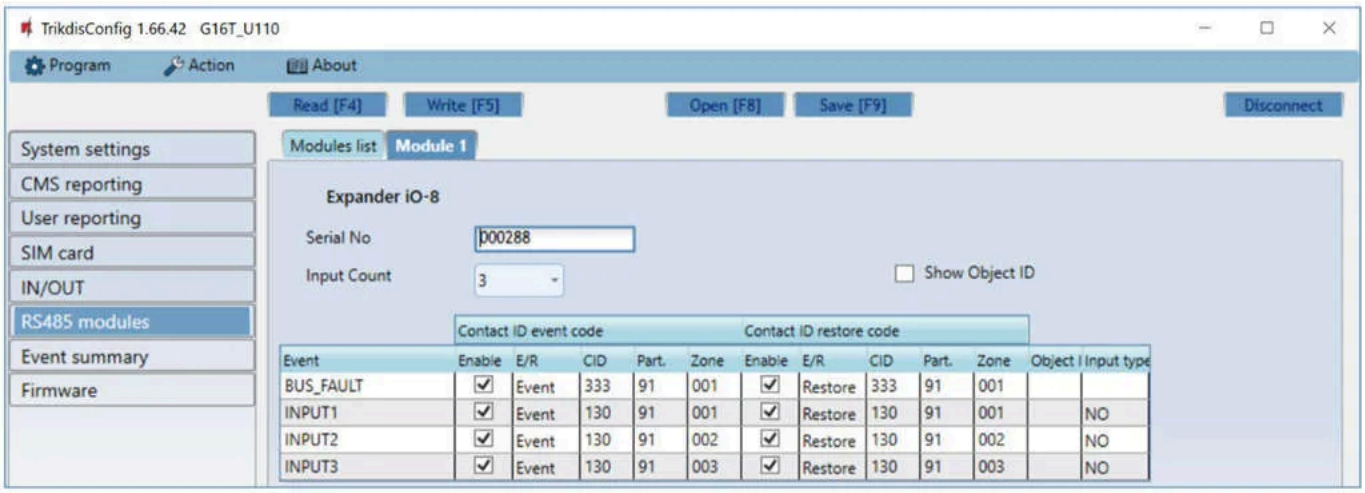


Abbildung 33. TrikdisConfig – RS485 modules, Reiter des Moduls iO-8.

- **Input Count** – wie viele Klemmen Eingänge sein sollen; die übrigen werden Ausgänge. Der Eingangstyp (**Input type**: NO oder NC) wird in der Tabelle angegeben. Die Rolle der Ausgänge (Scharf-/ Unscharfschalten 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 Leitstellenempfänger und an Protegus 2. Standardmäßig meldet das 1. Modul mit Bereich 91, das 4. Modul mit Bereich 94. Mit dem Haken bei **Show Object ID** kann für die Eingänge auch eine vom Kommunikator abweichende Objektkennung angegeben werden.
- Soll der Benutzer bei Auslösung der Eingänge der Erweiterung auch eine SMS oder einen Anruf erhalten, nehmen Sie den dem Eingang zugeordneten Contact-ID-Ereigniscode auch in die Tabelle im Reiter **User reporting** → **SMS & Call Reporting** auf.

Erweiterung iO – 1 Eingang, 1 Relaisausgang (Relaiskontakte) und ein serieller 1-Wire-Bus für Temperatursensoren. Der Relaisausgang kann auch nach logischen Bedingungen (WENN … DANN) gesteuert werden.

- **Input IN1 type** – der Eingangstyp (NO oder NC).
- **Max °C (T1)** – liegt die Temperatur darüber, sendet das Gerät ein Ereignis; dazu muss das Ereignis in der Tabelle aktiviert sein.
- **Min °C (T2)** – liegt die Temperatur darunter, sendet das Gerät ein Ereignis; dazu muss das Ereignis in der Tabelle aktiviert sein.
- In der Tabelle können Sie dem Eingang einen Contact-ID-Ereignis- und Wiederherstellungscode zuordnen, genauso wie bei der Erweiterung iO-8; bei Auslösung des Eingangs sendet der Kommunikator mit dem eingestellten Code ein Ereignis an den Leitstellenempfänger und an Protegus 2.

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

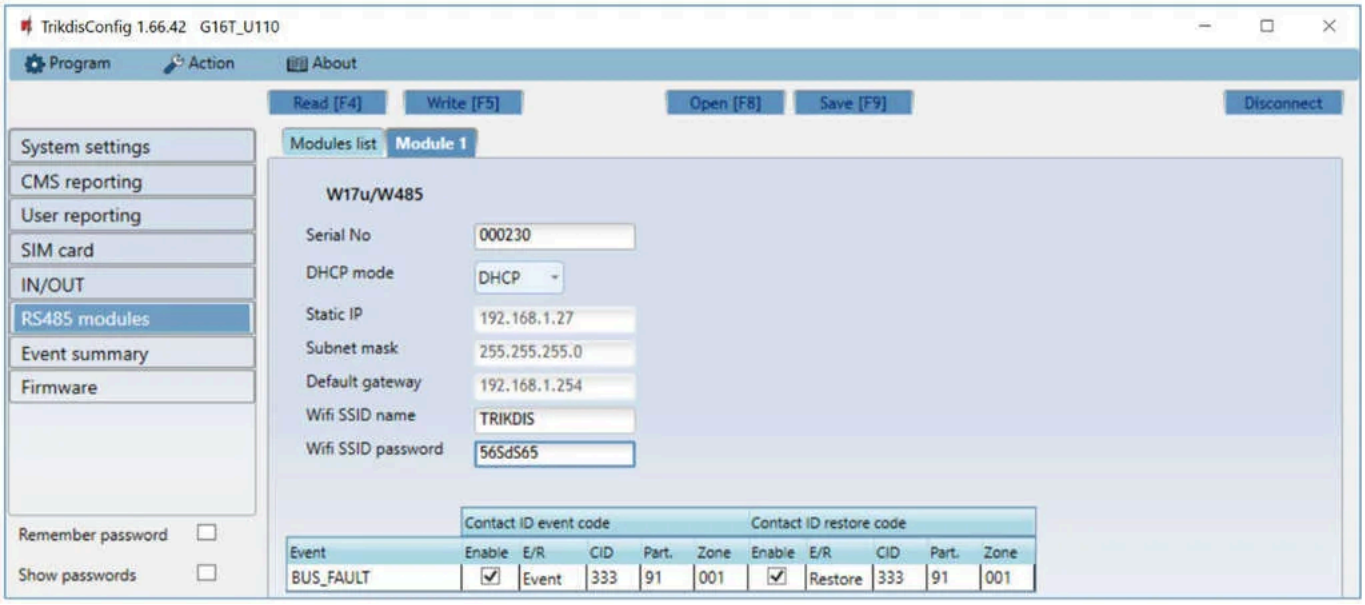


Abbildung 34. TrikdisConfig – RS485 modules, Reiter des Moduls W485.

- **DHCP mode** – automatische oder manuelle 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 (Abbruch und Wiederherstellung der Verbindung zwischen Modul und G16T) einen Contact-ID-Code zuordnen; das Ereignis erhalten sowohl die Leitstelle als auch Protegus 2.

Ethernet-Modul E485 – dieselben Netzwerkeinstellungen ohne WLAN (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**), und ebenso können Sie den Fehlern des RS485-Busses (Abbruch und Wiederherstellung der Verbindung zwischen Modul und G16T) einen Contact-ID-Code zuordnen; das Ereignis erhalten sowohl die Leitstelle als auch Protegus 2.

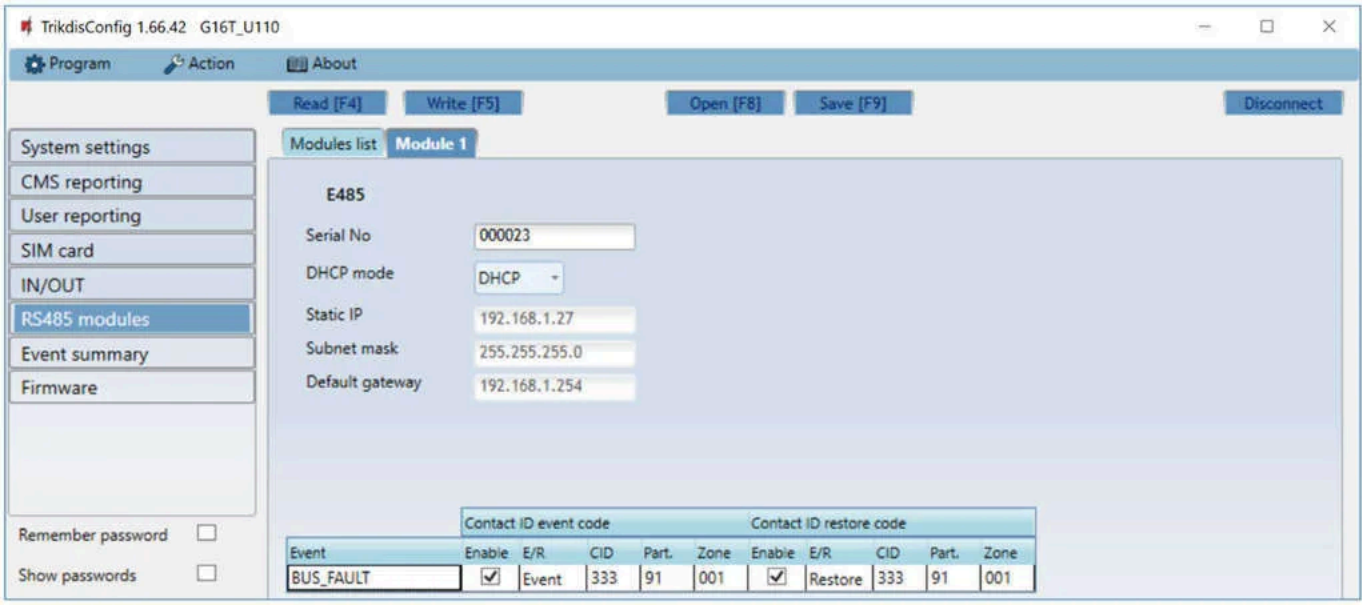


Abbildung 35. TrikdisConfig – RS485 modules, Reiter des Moduls E485.

Damit W485 und E485 funktionieren, muss im G16T die Verbindung zur Leitstelle und/oder zu Protegus eingerichtet sein (Abschnitte 2.2 und 2.3), und im Normalfall muss im G16T auch eine SIM-Karte stecken (bei Bedarf kann er auch ohne SIM-Karte arbeiten: diese Möglichkeit wurde nachträglich auf Anfrage entwickelt).

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.

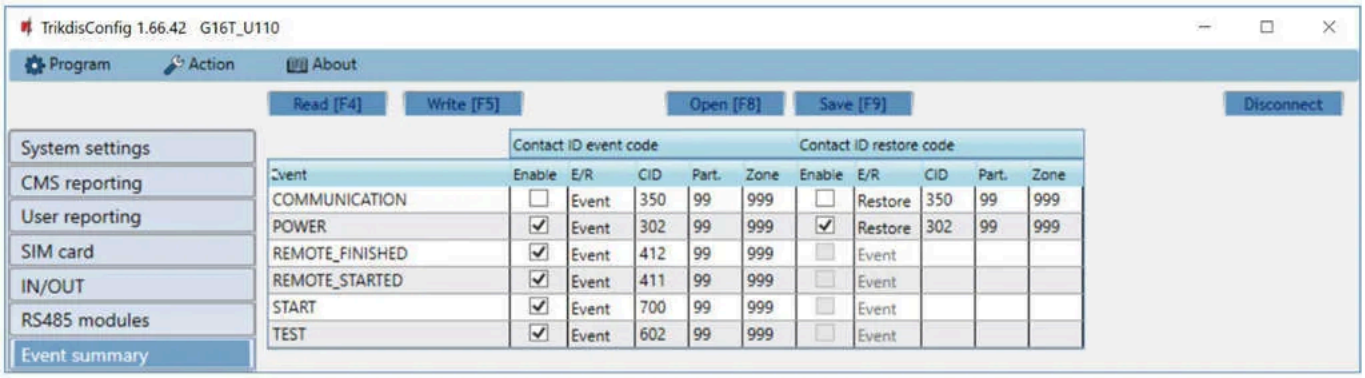


Abbildung 36. TrikdisConfig – Seite Event summary: die internen Meldungen des Geräts.

6.9 Werkseinstellungen wiederherstellen

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

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

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.

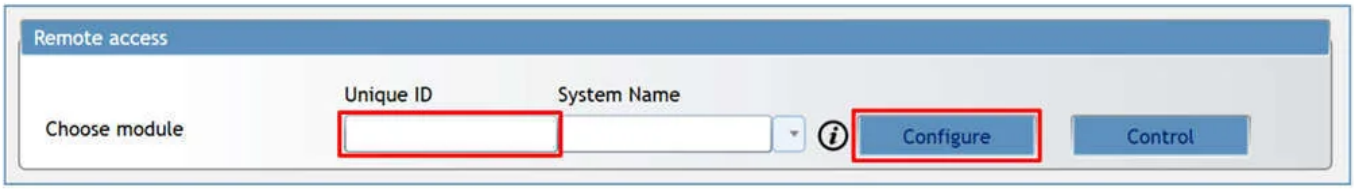


Abbildung 37. TrikdisConfig – Remote access: Kennung des Geräts, Name des Systems und Schaltfläche Configure.

Die Freigabe der Protegus-Cloud beschreibt Abschnitt 6.4.

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.

9. Firmware-Aktualisierung

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

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

1. Starten Sie die Software TrikdisConfig und verbinden Sie das Gerät per USB-Kabel, oder öffnen Sie seine Programmierung aus der Ferne.
2. Wenn es eine neuere Firmware gibt, bietet das Programm deren Download an – nehmen Sie ihn an.
3. Wählen Sie die Seite **Firmware** und klicken Sie auf die Schaltfläche **Open firmware**. Wählen Sie die Firmware-Datei aus.

4. Drücken Sie die Schaltfläche **Update [F12]**, warten Sie das Ende der Aktualisierung ab, und klicken Sie dann im Popup-Fenster auf **OK**. Ziehen Sie währenddessen nicht das Kabel ab und unterbrechen Sie die Verbindung nicht.

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

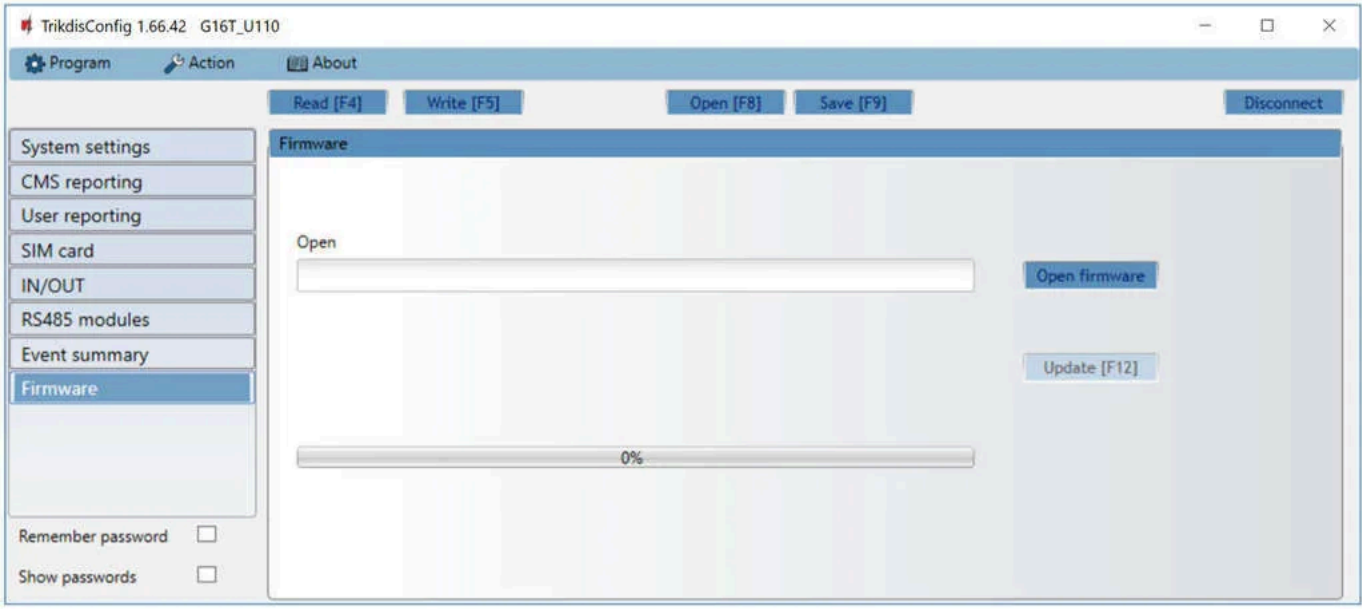


Abbildung 38. TrikdisConfig – Seite Firmware: Open firmware und Update [F12].

Für die Aktualisierung ist eine Internetverbindung nötig. Virenscanner, Firewall oder strenge Netzwerkeinstellungen können das automatische Herunterladen der Firmware verhindern; laden Sie die Datei dann 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 ein ausführliches Kapitel, finden Sie dort die genaue Stelle der Einstellung.

Die NETWORK-LED leuchtet nicht – kein Netz

1. Achten Sie auf die Blinkzeichen der **TROUBLE**-LED: 1 = keine SIM, 2 = falscher PIN, 3 = kein APN, 4 = keine Verbindung zum GSM-Netz möglich, 5 = keine Verbindung zum Datennetz möglich.
2. Prüfen Sie, ob die SIM-Karte aktiv ist, einen Datendienst hat und richtig im Halter sitzt.
3. Ist die PIN-Abfrage auf der Karte eingeschaltet, geben Sie den PIN auf der Seite **SIM card** ein oder schalten Sie die PIN-Abfrage in einem Telefon ab.
4. Prüfen Sie die Antenne: Sie ist angeschraubt, nicht in einem Metallgehäuse, und der Signalpegel ist ausreichend (Abschnitte 1.6 und 3.2).

Netz ist vorhanden, 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 Blinkzeichen der **TROUBLE**-LED zeigen, dass keine Verbindung zum Empfänger besteht: Prüfen Sie Adresse und Port des Empfängers, die TCP/UDP-Einstellung und den Verschlüsselungsschlüssel (**CMS reporting**).
2. Ist der Empfänger mit einem Domainnamen angegeben, prüfen Sie die DNS-Einstellung (**CMS reporting → Settings**).
3. Prüfen Sie, ob der Datentarif der SIM-Karte den benötigten Port nicht sperrt (manche M2M-Karten lassen nur bestimmte Adressen zu).

Die Zentrale sendet die Ereignisse nicht an den Kommunikator

1. Der Wähler der Zentrale muss eingeschaltet sein, im DTMF-Modus, mit dem Format Contact ID und mit eingetragener Telefonnummer (Kapitel 4).
2. Prüfen Sie den Anschluss TIP/RING; 7 Blinkzeichen der LED **TROUBLE** zeigen eine fehlende Verbindung mit der Zentrale an (beim Anschluss mit Leitungsüberwachung).
3. Wenn die Zentrale auf einen Wählton wartet und den Anruf nicht startet, schalten Sie in ihr die Wähltonerkennung ab.
4. Meldet die Zentrale einen „Kommunikationsfehler", obwohl das Ereignis angekommen ist, prüfen Sie die Einstellung **Wait acknowledgment from CMS** (Abschnitt 6.2).

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** angegeben werden; nach dem Anlegen des Systems ist er im Gerät nicht mehr änderbar.
3. Geben Sie die IMEI genau ein, von der Verpackung oder von der Rückseite.
4. Datendienst der SIM-Karte und APN müssen in Ordnung sein (die NETWORK-LED ist grün, und die DATA-LED erlischt nach einem Ereignis).

Ich kann mich mit TrikdisConfig nicht aus der Ferne verbinden

1. Das Gerät muss online sein (NETWORK-LED grün), und die Protegus-Verbindung muss aktiviert 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 G16T mit 2G-Modem (G16T_G410) hat keinen RS485-Bus; iO-8, W485 und E485 können nur an die 4G-Version (G16T_E120) angeschlossen werden. Für die Module W485 und E485 muss im Normalfall auch eine SIM-Karte im G16T stecken; bei Bedarf kann er auch ohne SIM-Karte arbeiten (eine nachträglich auf Anfrage entwickelte Möglichkeit).

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

Die Abschaltung der 2G-Netze schreitet je nach Anbieter unterschiedlich schnell voran; für den langfristigen Betrieb empfehlen wir die 4G-Version, die auch einen 2G-Rückfall hat. Die 4G-Version lässt sich außerdem über den RS485-Bus erweitern.

Wie viel Datenvolumen verbraucht das Gerät?

Ereignismeldungen und PINGs sind sehr klein; das Volumen hängt hauptsächlich vom PING-Intervall und von der Häufigkeit der Testmeldungen ab. Bei einer durchschnittlichen Anlage im Haushalt bleibt das monatliche Volumen typischerweise unter 10 MB. Der genaue Wert hängt von den Einstellungen und von der Abrechnungseinheit des Anbieters ab; bei einer Karte mit Datenlimit lohnt es sich daher, das Volumen 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.

- Sicherheitstechnische Anlagen dürfen nur von einem qualifizierten Errichter installiert und gewartet werden.
- Lesen Sie vor der Installation die Anleitung; die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen oder Schäden führen.
- Trennen Sie das Gerät vor dem Anschließen, bei jeder elektrischen Verbindung und vor der Wartung von der Versorgung.
- Fehler aufgrund unsachgemäßer Installation oder Verwendung sowie nicht vom Hersteller 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

- Fern-Scharfschaltung mit Schlüsselschalter aus der App Protegus 2 – Details und Fallstricke der Scharfschaltung per Schlüsselschalter.

- Die Hardwareversion 4 der GSM-Kommunikatoren G16 und G16T kommt – was sich gegenüber der vorherigen Version geändert hat.
- Neuerungen im Kommunikator G16T v3 – die Produktankündigung.
- Dokumentation in englischer Sprache: docs.trikdis.com.

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

Passende Produkte

Trikdis G16T 4G GSM Smart Communicator (Tipp-Ring)

Trikdis G16T 2G GSM Smart Communicator (Tipp-Ring) **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/g16t-anleitung