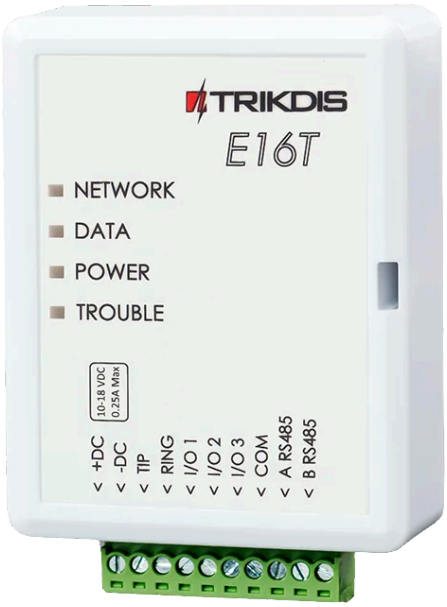
Kommunikator E16T – Errichter- und Benutzeranleitung

Errichter- und Benutzeranleitung für den Trikdis-Ethernet-Kommunikator E16T: Anschluss an die Alarmzentrale, Netzwerkeinstellung in TrikdisConfig, Übertragung an die Leitstelle, App Protegus 2, Prüfung und Fehlersuche.



Ausgabe: 2026-11-17
Immer aktuelle Webversion: https://trikdis.at/e16t-anleitung

Inhalt

1. Überblick

1.1 Wozu er dient, wie er funktioniert
1.2 Varianten
1.3 Hauptmerkmale
1.4 Bestandteile des Kommunikators
1.5 Anschlussklemmen
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 Schritte der Installation
3.2 Montageort und Netzwerk
3.3 Anschluss an die Alarmzentrale
3.3.1 Bei Bedarf: Leitungsüberwachung
3.4 Anschluss einer Schlüsselschalterzone
3.5 Anschluss von Eingängen
3.6 Anschluss des Ethernet-Kabels
3.7 Anschluss eines Ausgangs mit Relais
3.8 Anschluss des Erweiterungsmoduls iO-8
3.9 Einschalten und erste Prüfung
A TRIKDIS átjelző elindítása

4. Programmierung der Alarmzentrale

4.1 Programmierung des Wählgeräts der Honeywell Vista
4.2 Zentralen anderer Hersteller

5. Fernsteuerung mit der App Protegus 2

5.1 Hinzufügen des Geräts
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Scharf- und Unscharfschalten mit einem Ausgang
5.3 Scharf- und Unscharfschalten aus der App

6. TrikdisConfig – die Einstellungen im Detail

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

7. Fernprogrammierung

8. Prüfung der Funktion des Kommunikators

9. Firmware-Aktualisierung

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

Der E16T ist der **universelle Ethernet-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 E16T nimmt die Leitung ab, decodiert die Meldung und überträgt sie über das lokale Netzwerk und die kabelgebundene Internetverbindung an den Empfänger der Leitstelle sowie in die Protegus Cloud, in die App des Benutzers. So lässt sich **eine Zentrale jedes Herstellers** mit ihm verwenden, die ein Contact-ID-Wählgerät hat – die Zentrale muss nicht ausgetauscht werden, nur ihr Wählgerät ist einzurichten. Der E16T arbeitet über kabelgebundenes Internet, ohne SIM-Karte und ohne Vertrag.

1.1 Wozu er dient, wie er funktioniert

- **Er meldet an die Leitstelle.** Die Ereignisse sendet er über IP an den Software- oder Hardware-Empfänger von Trikdis (Protokoll TRK; diese Empfänger arbeiten mit jeder Leitstellensoftware zusammen) bzw. an jeden universellen Empfänger (SIA DC-09 2007/2012, SUR-GARD TL150). Die Verbindung prüft er standardmäßig alle 30 Sekunden (er sendet ein Lebenszeichen, einen PING, an den Empfänger; das Intervall ist einstellbar) und wechselt bei einem Fehler auf einen Ersatzkanal.
- **Er benachrichtigt den Benutzer.** Die App Protegus 2 zeigt das Geschehen als Push-Nachricht (mit eigenem Signalton) und in der Ereignisliste; der Benutzer kann aus der App scharf und unscharf schalten und die angeschlossenen Geräte schalten (Beleuchtung, Tor, Lüftung, Heizung, Bewässerung usw.). Die App arbeitet mit der Alarmzentrale jedes Herstellers, an die der E16T angeschlossen ist.
- **Gemeinsam oder getrennt** arbeitet er mit der Leitstelle und dem Benutzer: Er kann nur mit Protegus 2 (ohne Leitstelle), nur mit der Leitstelle oder mit beiden verwendet werden. Sind beide eingerichtet, sendet er das Ereignis zuerst an die Leitstelle, danach an den Benutzer.
- **Er hat eigene Ein- und Ausgänge.** Drei I/O-Klemmen mit Doppelfunktion lassen sich als Eingang (Melder, Sabotage) oder als steuerbarer Ausgang (Schlüsselschalterzone, Relais) verwenden. Mit dem an den RS485-Bus angeschlossenen Erweiterungsmodul iO-8 lassen sich dem System weitere 8 I/O hinzufügen.
- **Kein Vertrag nötig.** Der E16T nutzt die vorhandene Internetverbindung des Objekts: Es sind keine SIM-Karte, kein Mobilfunkvertrag und keine Antenne nötig, und auch die Stärke des Mobilfunksignals spielt keine Rolle.

Den Aufbau des Systems zeigt die folgende Abbildung: Der Telefonleitungsausgang der Alarmzentrale ist an den E16T angeschlossen, der E16T erreicht über den lokalen Router das Internet, von dort den Empfänger der Leitstelle und die Protegus Cloud, und der Benutzer sieht das System in der App Protegus 2.

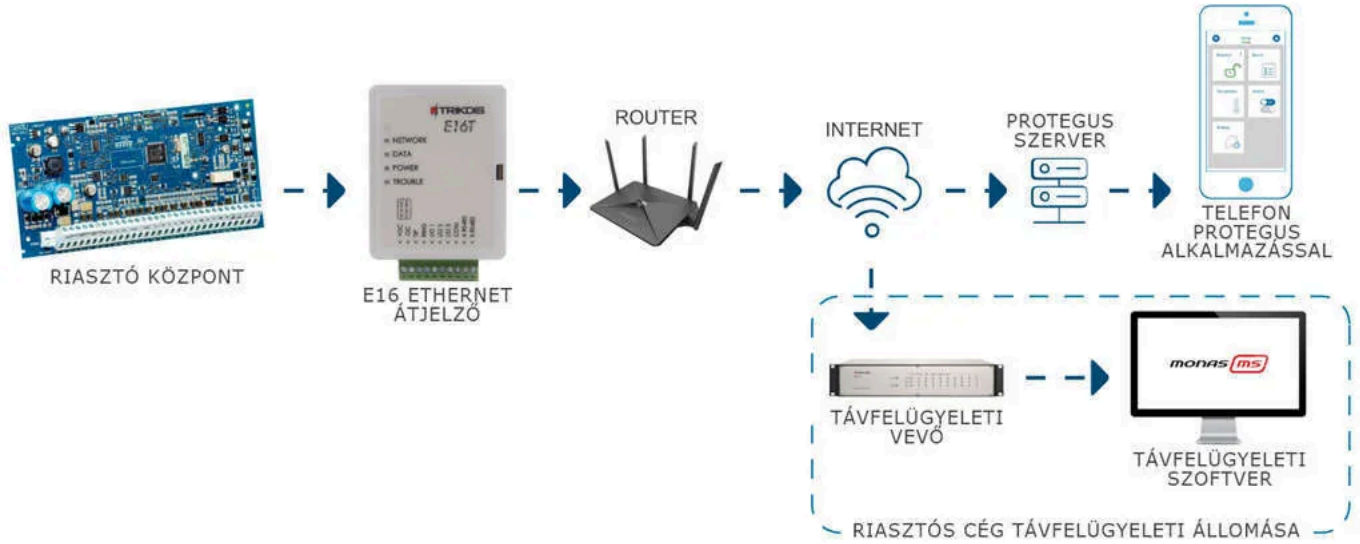


Abbildung 1. Die Stellung des E16T im System: Alarmzentrale → E16T → Router → Internet → Empfänger der Leitstelle und Protegus Cloud → App Protegus 2.

1.2 Varianten

Diese Anleitung wurde für die **aktuelle Hardwarevariante v2** des E16T erstellt (TrikdisConfig zeigt sie als **E16T_2000** an), sie ist aber **auch für den früheren E16T verwendbar**: Anschluss, Einstellung und Funktion sind weitgehend gleich. Die Unterschiede fasst die folgende Tabelle zusammen; wo der Text den Wert der v2 angibt, beachten Sie bei der früheren Variante diesen.

	Früherer E16T	**E16T v2 (aktuell)**
Ein-/Ausgänge	2 Eingänge mit wählbarem Typ (T-1/IN1, R-1/IN2 – NC, NO, EOL; auch zur Überwachung der Telefonleitung verwendbar) + 1 Open-Collector-Ausgang (OUT, max. 0,15 A, bis 30 V; aus der App Protegus steuerbar)	3 I/O-Klemmen mit Doppelfunktion (I/O 1, I/O 2, I/O 3), jede als Eingang (Typen NC, NO, EOL, DEOL) oder als Open-Collector-Ausgang (max. 0,15 A) verwendbar
Stromaufnahme	höchstens 0,5 A	100 mA nominal, höchstens 250 mA beim Senden
LEDs	NETWORK, DATA, POWER, TROUBLE, LINE (LINE leuchtet grün, solange die Zentrale „den Hörer abgenommen hat", also wählt; die abweichenden Anzeigen der übrigen LEDs listet der Hinweis am Ende von Abschnitt 1.6 auf)	NETWORK, DATA, POWER, TROUBLE
Ereignisspeicher	100 Meldungen	60 Meldungen
Abmessungen	88 × 62 × 25 mm	88 × 65 × 26 mm

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

1.3 Hauptmerkmale

Verbindung mit der 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 per DTMF-Wahl; der E16T überträgt die vollständige Ereignisinformation (Code, Bereich, Zone oder Benutzer).

Kommunikation mit der Leitstelle

- IP-Verbindung mit den Trikdis-Empfängern (Software-Empfänger IPcom, RL14, RM14) und mit universellen Empfängern (SIA DC-09, TL150).
- Primär-, Ersatz- und Parallelkanal: Er kann gleichzeitig an zwei Empfänger senden, für jeden mit eigenem Ersatzkanal.
- Verschlüsselte, passwortgeschützte Kommunikation; Ereignisspeicher 60 Meldungen.

Benutzerfunktionen

- Mobil- und Web-App Protegus 2: Benachrichtigung, Ereignisliste, Scharf- und Unscharfschalten, Schalten der Ausgänge.
- Mehrstufige Benutzerrechte in der App (Administrator, Errichter, Benutzer).

Installation und Einstellung

- Die Einstellungen lassen sich in eine Datei speichern und in einen anderen Kommunikator laden.
- Zwei Zugriffsebenen: Administrator und Errichter – für die Einstellung des Geräts, für den Administrator der Leitstelle und für den Errichter.
- Fernkonfiguration und Fernaktualisierung mit der Software TrikdisConfig.

1.4 Bestandteile des Kommunikators

Die Leiterplatte des E16T sitzt in einem weißen Kunststoffgehäuse; der Frontdeckel ist abnehmbar, die Klemmleiste abziehbar. Der Netzwerkanschluss (RJ45) befindet sich am oberen Rand der Leiterplatte und ist durch die Öffnung des Gehäuses zugänglich.

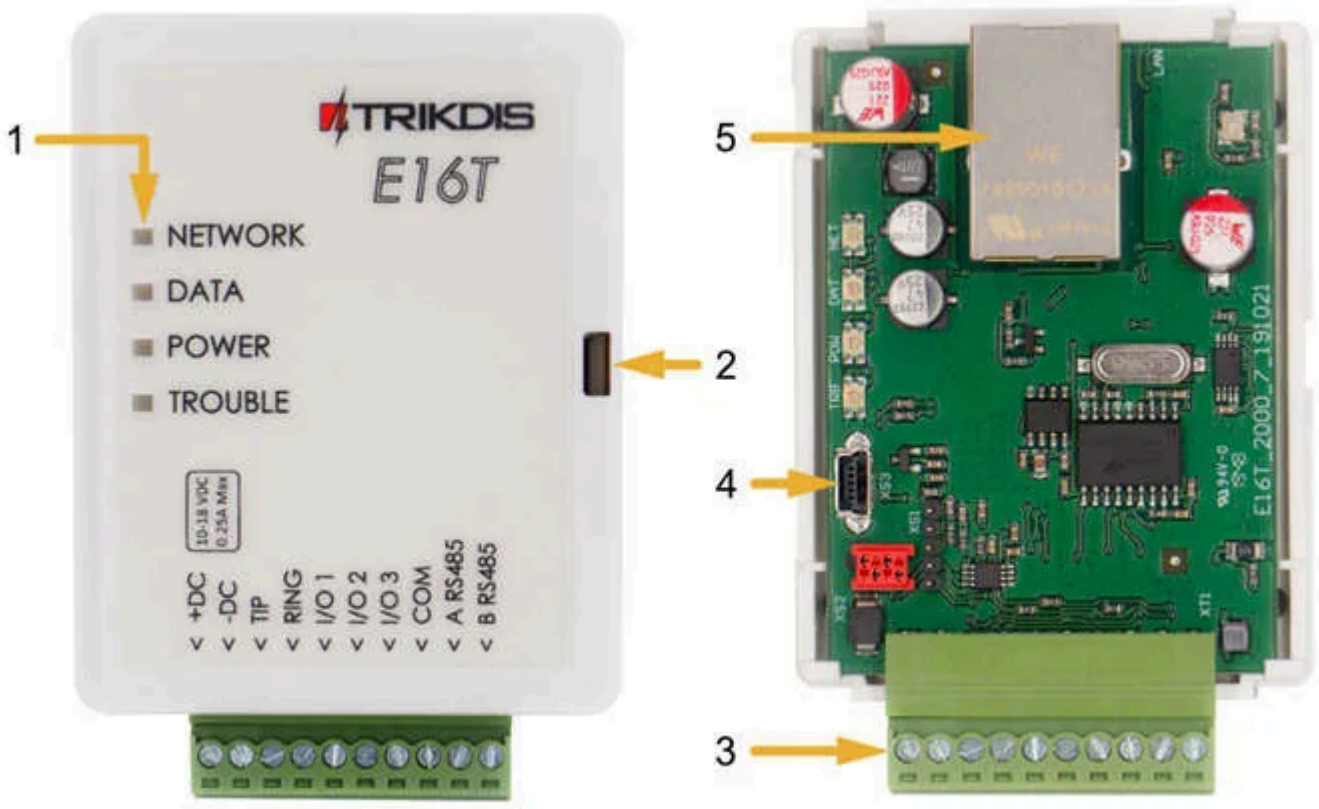


Abbildung 2. Die Bestandteile des E16T von vorn und bei geöffnetem Gehäuse.

- 1 LED-Anzeigen (NETWORK, DATA, POWER, TROUBLE)
- 2 Öffnung zum Abnehmen des Frontdeckels (an der Oberkante des Deckels)
- 3 Abziehbare Klemmleiste
- 4 USB-Mini-B-Buchse für die Programmierung
- 5 Ethernet-Anschluss (RJ45)

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

1.5 Anschlussklemmen

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)	1. Ein-/Ausgang oder Punkt T-1 der Telefonleitungsüberwachung
I/O 2 (R-1)	2. Ein-/Ausgang oder Punkt R-1 der Telefonleitungsüberwachung
I/O 3	3. Ein-/Ausgang
COM	Gemeinsamer (negativer) Punkt für die Ein- und Ausgänge
A 485	Ader A des RS485-Busses (iO-8 und andere Erweiterungsmodule der iO-Serie)
B 485	Ader B des RS485-Busses

Die Beschriftung der Klemmleiste steht auch auf dem Frontdeckel, deshalb muss der Deckel beim Anschließen nicht abgenommen werden.

1.6 LED-Anzeigen

Die LEDs auf dem Frontdeckel sind die wichtigsten Hilfsmittel bei Inbetriebnahme und Fehlersuche. Lesen Sie sie zusammen: POWER zeigt die Versorgung, NETWORK die Netzwerkverbindung, DATA die zum Senden wartenden Meldungen, TROUBLE den Fehler.

NETWORK – Netzwerkverbindung

Anzeige	Bedeutung
aus	Keine Netzwerkverbindung (kein Kabel, Port nicht aktiv oder keine IP-Adresse erhalten)
leuchtet grün	Mit dem lokalen Netzwerk verbunden – die Verbindung steht bis zum Router. Ob auch das Internet erreichbar ist, zeigt die LED DATA (siehe unten).

DATA – Datenverkehr

Anzeige	Bedeutung
aus	Keine zum Senden wartende Meldung
leuchtet grün	Im Speicher warten Meldungen auf das Senden
blinkt grün	Daten werden gesendet oder empfangen (beim Programmieren)

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	Ungeeignete Versorgungsspannung (höchstens 11,5 V)
leuchtet grün, blinkt gelb	Bereit zur Programmierung (USB-Kabel eingesteckt)
leuchtet gelb (beim Programmieren)	Keine Verbindung mit dem Computer

TROUBLE – Fehler

Anzeige	Bedeutung
aus	Kein Fehler
1 rotes Blinken	Keine physische Netzwerkverbindung (PHY-Link): Kabel, Stecker oder Port des Routers/Switches
2 rote Blinkzeichen	DHCP-Fehler: Das Gerät hat keine IP-Adresse erhalten
3 rote Blinkzeichen	DNS-Fehler: Die Namensauflösung funktioniert nicht
6 rote Blinkzeichen	Keine Verbindung mit dem Empfänger der Leitstelle
7 rote Blinkzeichen	Die Verbindung mit der Alarmzentrale ist unterbrochen
blinkt rot (beim Programmieren)	Speicherfehler
leuchtet rot (beim Programmieren)	Beschädigte Firmware

Früherer E16T

Die LEDs des früheren E16T zeigen teilweise etwas anderes: **DATA** leuchtet gelb, wenn im Speicher ein Ereignis auf das Senden wartet, und blinkt grün, solange die Alarmzentrale eine Meldung an den Kommunikator übergibt; **POWER** blinkt grün, wenn die Versorgung eingeschaltet und die Spannung in Ordnung ist, und blinkt gelb, wenn die Versorgungsspannung nicht ausreicht (höchstens 11,5 V); ein dauerhaftes rotes Licht von **TROUBLE** zeigt einen Fehler der Netzwerkverbindung (LAN), erloschen bedeutet kein Fehler; **LINE** leuchtet grün, solange die Zentrale „den Hörer abgenommen hat“ (Abschnitt 1.2).

1.7 Technische Daten

Parameter	Wert
Verbindung mit der Alarmzentrale	kabelgebundene Telefonleitung (TIP/RING), Contact ID, DTMF
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: Erweiterungsmodul iO-8 (+8 I/O) und andere Erweiterungsmodule der iO-Serie, höchstens 4 Module
Netzwerkanschluss	Ethernet, IEEE 802.3, 10Base-T, RJ45-Buchse
Netzwerkeinstellung	DHCP (Werkseinstellung) oder feste IP-Adresse
Versorgungsspannung	10–18 V DC
Stromaufnahme	100 mA nominal; höchstens 250 mA beim Senden
Übertragungsprotokolle	TRK, DC-09_2007, DC-09_2012, TL150
Ereignisspeicher	60 Meldungen
Programmierung	TrikdisConfig (Windows) über USB-Mini-B-Kabel oder aus der Ferne
Betriebsumgebung	−10 … +50 °C, max. 80 % relative Luftfeuchtigkeit (bei +20 °C)
Abmessungen	88 × 65 × 26 mm
Gewicht	80 g

2. Schnelle Inbetriebnahme mit TrikdisConfig

Alle Einstellungen des E16T erfolgen mit dem Windows-Programm **TrikdisConfig** – über USB-Kabel oder per Fernzugriff. In diesem Kapitel beschreiben wir den kürzesten Weg: Sie richten das Gerät auf dem Tisch vor dem Anschließen ein, danach muss es vor Ort nur noch angeschlossen werden. Die ausführliche Erklärung der Einstellungen enthält Kapitel 6.

2.1 Vorbereitung

Was Sie brauchen

USB-Mini-B-Kabel (für die Einstellung) · Kabel mit mindestens 4 Adern zur Zentrale · flacher Schraubendreher 2,5 mm · Ethernet-Kabel (CAT-5 oder besser, höchstens 100 m) bis zum Router oder Switch · ein freier Netzwerkport · wenn es im Netzwerk kein DHCP gibt: die vom Netzwerkadministrator erhaltene feste IP-Adresse, Maske, Gateway und DNS · die Errichteranleitung der Alarmzentrale. Was fehlt, ist separat beim Händler vor Ort erhältlich.

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 E16T und verbinden Sie ihn mit dem Computer. Stecken Sie einen flachen Schraubendreher in die Öffnung an der Oberkante des Deckels, hebeln Sie die Frontabdeckung nach unten vorsichtig ab und stecken Sie dann das USB-Mini-B-Kabel ein. USB liefert genügend Strom für die Programmierung, eine separate Versorgung ist nicht nötig.

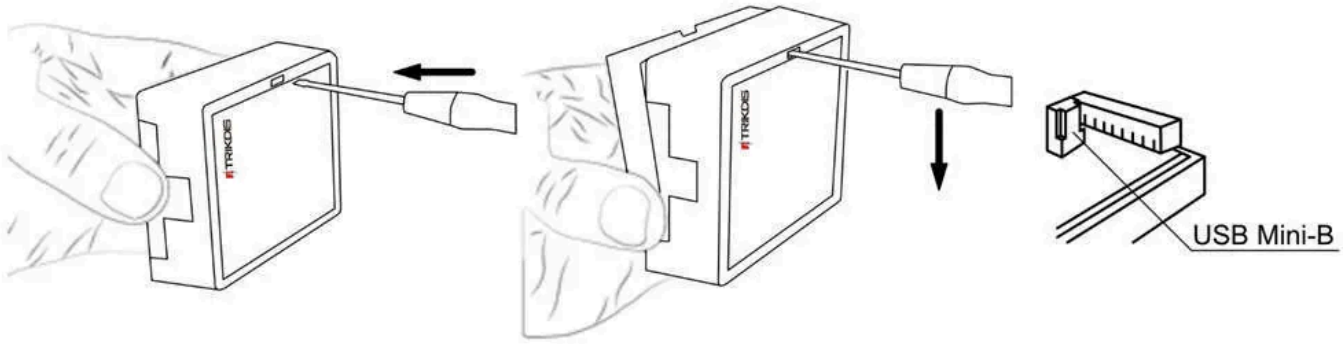


Abbildung 3. Abhebeln der Frontabdeckung und Verbindung mit dem Computer über ein USB-Mini-B-Kabel.

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

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

Die nächsten beiden Abschnitte beschreiben, was einzustellen ist, damit die Alarmzentrale aus der App Protegus 2 gesteuert werden kann (2.2) und damit der Kommunikator Ereignisse an die Leitstelle sendet (2.3).

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 4. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- 1 **Enable connection** – anhaken: erlaubt die Verbindung mit der Protegus Cloud.
- 2 **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 ist es nicht mehr änderbar.**

Prüfen Sie danach auf der Seite **System settings** den Schnittstellentyp der Alarmzentrale.

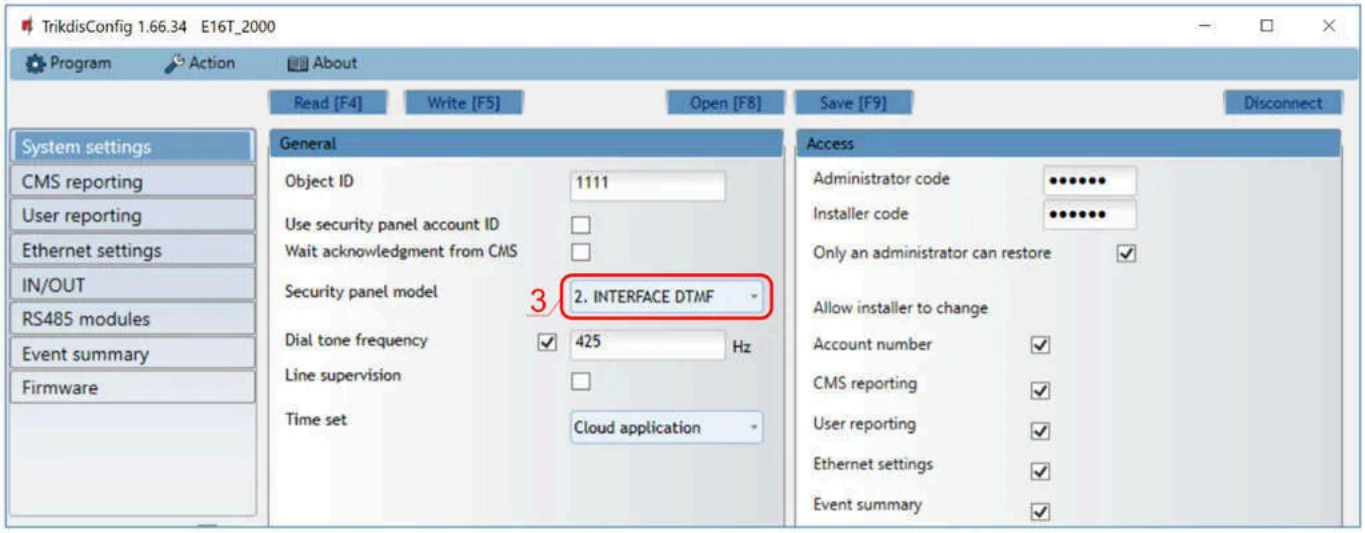


Abbildung 5. TrikdisConfig – Seite System settings, Gruppe General.

- 3 **Security panel model** – bleibt **2. INTERFACE DTMF** (die Verbindung über die Telefonleitung mit DTMF-Wahl).

Für die Netzwerkeinstellungen ist auf der Seite **Ethernet settings** ab Werk **Use DHCP** angehakt: Das Gerät erhält vom Router automatisch eine IP-Adresse, und an den meisten Orten ist damit nichts weiter zu tun. Wenn es im Netzwerk kein DHCP gibt oder eine feste Adresse verwendet werden muss, geben Sie hier die manuellen Einstellungen ein (Abschnitt 6.5).

Wenn Sie das Gerät nur mit Protegus 2 verwenden, ohne Leitstelle, ist die Einrichtung damit fertig: Drücken Sie die Schaltfläche **Write [F5]** (Schreiben), warten Sie die Rückmeldung ab und ziehen Sie das USB-Kabel ab.

Vergessen Sie nicht, das Telefonwählgerät der Alarmzentrale einzuschalten und einzurichten, sonst sendet die Zentrale keine Ereignisse. Die Einstellung der Zentrale beschreibt Kapitel 4.

2.3 Verbindung zur Leitstelle

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

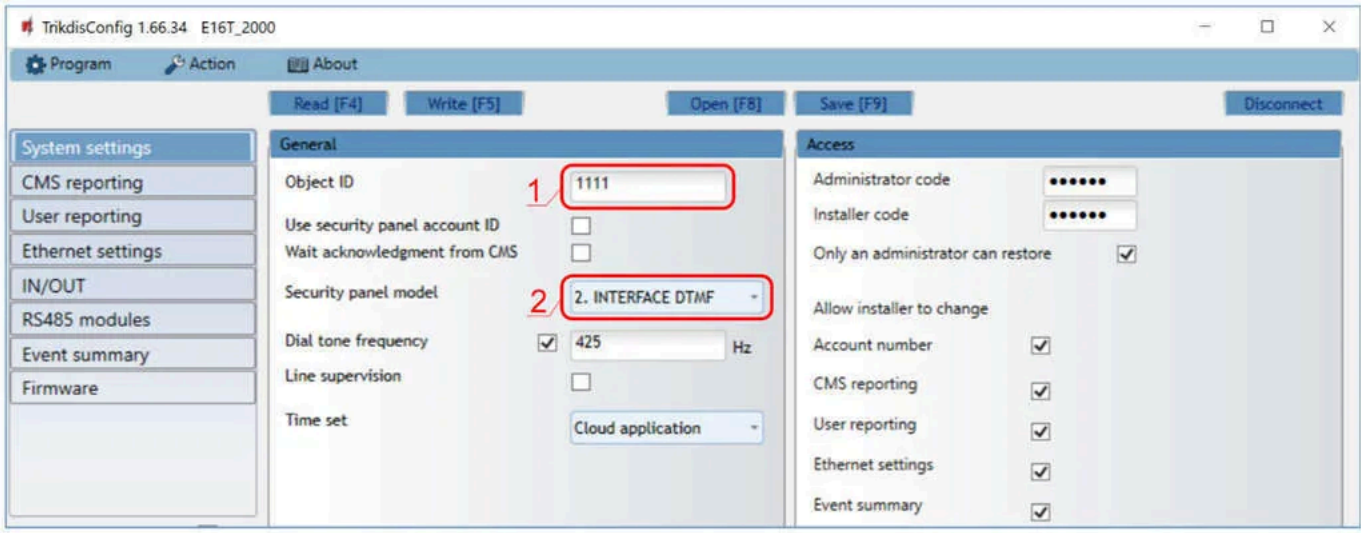


Abbildung 6. TrikdisConfig – Seite System settings, Gruppe General.

- 1 **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen, 0–9, A–F). `FFFE` und `FFFF` sind nicht verwendbar.
- 2 **Security panel model** – bleibt **2. INTERFACE DTMF**.

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

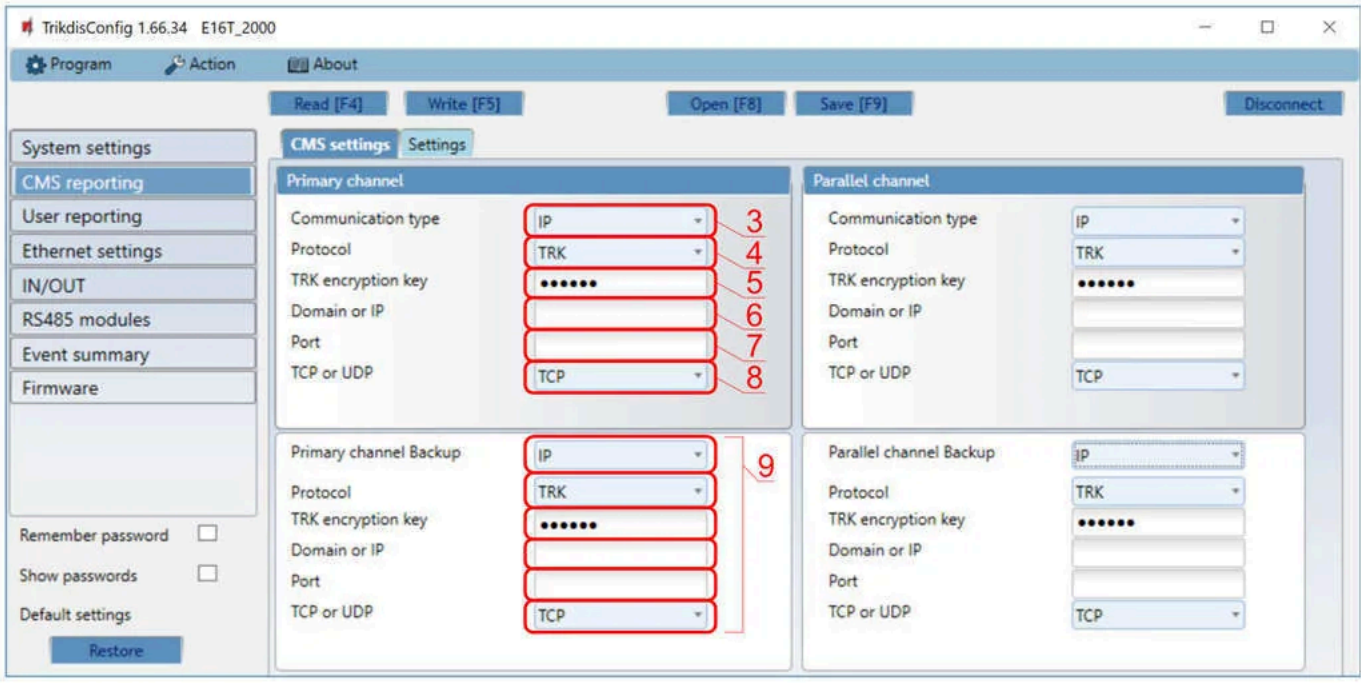


Abbildung 7. TrikdisConfig – CMS reporting, Reiter CMS settings.

- 3 **Communication type** – **IP** (beim E16T ist nur dies wählbar).
- 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** – Portnummer des Empfängers.
- 8 **TCP or UDP** – das Übertragungsprotokoll; richtet sich nach der Einstellung des Empfängers.
- 9 **Primary channel Backup** – Ersatzkanal bei einem Fehler des Primärkanals; genauso ausfüllen, die Angabe wird empfohlen.

Beim Protokoll **DC-09** geben Sie im Reiter **Settings** auch die DC-09-Objekt-, Linien- und Empfängernummer ein (Abschnitt 6.3); bei DC-09_2012 lässt sich auch die Verschlüsselung mit dem im Empfänger eingestellten DC-09-Schlüssel einschalten (Hinweis in Abschnitt 6.3). Für die Verbindungsprüfung stellen Sie das Intervall des Lebenszeichens (PING) im selben Reiter **Settings** ein (**IP ping period**, ab Werk 30 s). Wenn Sie den Empfänger mit einem Domainnamen angegeben haben, ist für die Namensauflösung auch die DNS-Einstellung auf der Seite **Ethernet settings** nötig (ab Werk ist der öffentliche DNS von Google eingetragen). Beim früheren E16T heißen die Felder anders (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**); die Zuordnung gibt der Hinweis in Abschnitt 6.3.

Wenn der Benutzer auch die App Protegus 2 verwendet, nehmen Sie auch die Einstellungen aus Abschnitt 2.2 vor (**User reporting** → **PROTEGUS Cloud**). Am Ende der Einstellungen drücken Sie die Schaltfläche **Write [F5]** (Schreiben), warten die Rückmeldung ab und ziehen 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 Schritte der Installation

1. Nehmen Sie den Frontdeckel ab (siehe Abschnitt 2.1) und ziehen Sie die Klemmleiste ab.
2. Nehmen Sie die Leiterplatte aus dem Gehäuseboden: Öffnen Sie die Verriegelung in der Ecke.
3. Befestigen Sie den Gehäuseboden mit Schrauben an der gewählten Stelle.
4. Setzen Sie die Leiterplatte wieder in den Gehäuseboden ein und stecken Sie die Klemmleiste wieder auf.
5. Stecken Sie das Ethernet-Kabel in die RJ45-Buchse (Abschnitt 3.6).
6. Setzen Sie den Frontdeckel wieder auf.

3.2 Montageort und Netzwerk

- Setzen Sie den Kommunikator an einen **trockenen Ort im Innenbereich**, möglichst in die Nähe des Gehäuses der Alarmzentrale, damit die Verkabelung kurz bleibt. Ein Metallgehäuse stört nicht: Der E16T hat keine Antenne.
- Das Ethernet-Kabel (CAT-5 oder besser) darf bis zum Router oder Switch **höchstens 100 m** lang sein.
- Halten Sie den Kommunikator und die Kabel vom Transformator der Zentrale und von Netzleitungen fern.

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.

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

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

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

Stromausfall

Der E16T wird von der Alarmzentrale versorgt und arbeitet daher bei einem Stromausfall über den Akku der Zentrale weiter – Router und Modem in der Regel jedoch nicht, und ohne sie gibt es kein Internet. Wenn das für das System nicht akzeptabel ist, betreiben Sie auch die Netzwerkgeräte an einer unterbrechungsfreien Stromversorgung, oder wählen Sie einen Mobilfunk-Kommunikator (G16T).

3.3 Anschluss an die Alarmzentrale

Der E16T wird an den Telefonleitungsausgang (TIP/RING) der Zentrale angeschlossen, die Versorgung erhält er vom 12-V-Hilfsspannungsausgang (AUX) der Zentrale.

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

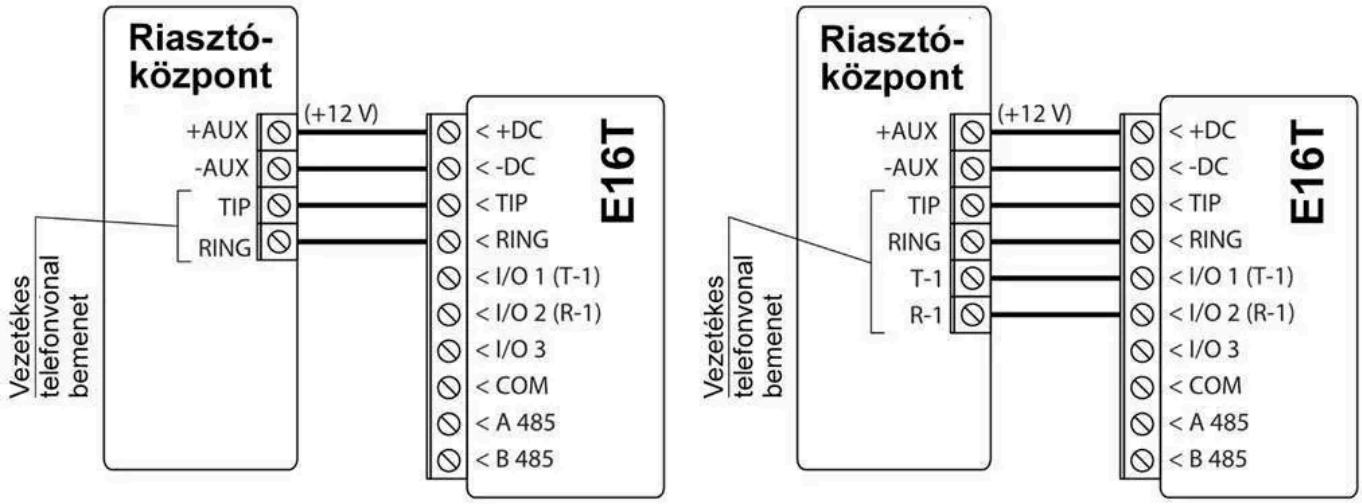


Abbildung 8. Anschluss an den Telefonleitungsausgang der Zentrale: links der normale Anschluss, rechts der Anschluss mit Leitungsüberwachung.

Der E16T nimmt beim Senden höchstens 250 mA auf. Prüfen Sie, ob der AUX-Ausgang der Zentrale dies zusammen mit den übrigen angeschlossenen Geräten verkraftet. Da die Versorgung von der Zentrale kommt, versorgt der Akku der Zentrale bei einem Stromausfall 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 Schlüsselschalterzone

Wenn Sie die Zentrale aus der Ferne, aus der App Protegus 2, scharf- und unscharfschalten möchten, stellen Sie eine I/O-Klemme des Kommunikators als **Ausgang** ein und schließen Sie sie an eine **Schlüsselschalterzone** der Zentrale an. Der Ausgang zieht die Zone beim Aktivieren auf COM (negativ); den Abschlusswiderstand der Zone schließen Sie entsprechend dem Zonentyp der Zentrale an. Da der E16T drei I/O-Klemmen hat, lassen sich sogar drei Bereiche mit je einem eigenen Ausgang bedienen.

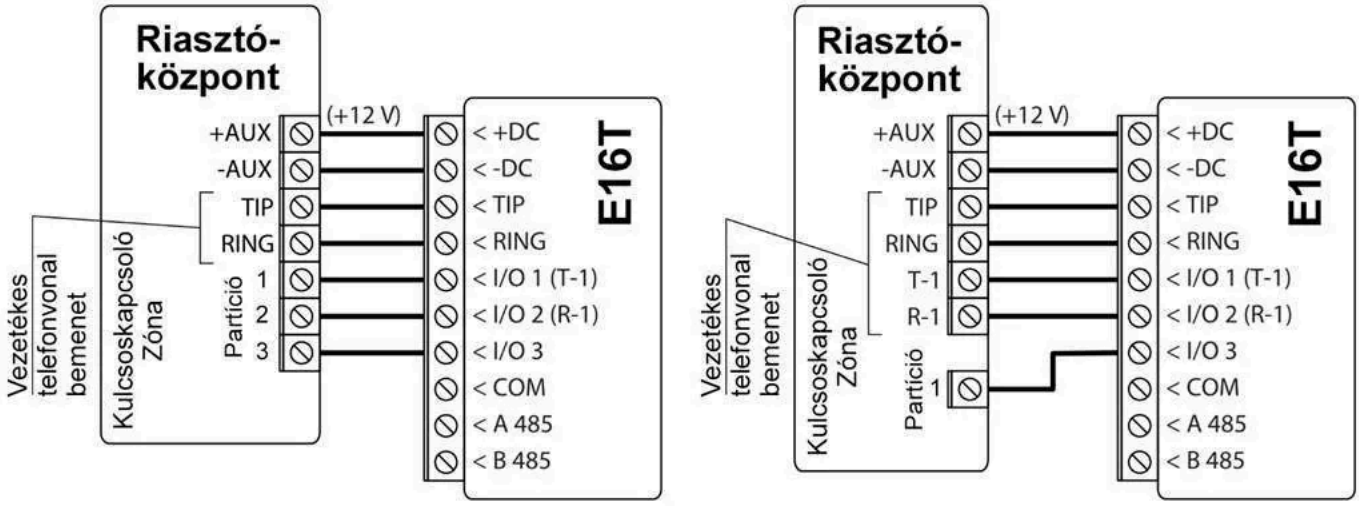


Abbildung 9. Scharf- und Unscharfschalten mit einer Schlüsselschalterzone: links der normale Anschluss, rechts der Anschluss mit Leitungsüberwachung (dann bleibt I/O 3 für den Schlüsselschalter).

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

Früherer E16T

Beim früheren E16T (2 Eingänge + OUT) werden Typ und Modus des Ausgangs in TrikdisConfig in der Gruppe **System settings** → **Output** eingestellt: Für das Scharfschalten per Schlüsselschalter muss **OUT type** auf **Remote Control** und **OUT mode** auf **Pulse** (mit Impulslänge) oder **Level** stehen – entsprechend dem Zonentyp der Zentrale.

3.5 Anschluss von Eingängen

Die I/O-Klemmen des Kommunikators lassen sich als Eingänge auch für weitere Melder verwenden (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 2,2-kΩ-Abschlusswiderstand, bei den DEOL-Typen mit Sabotagekreis.

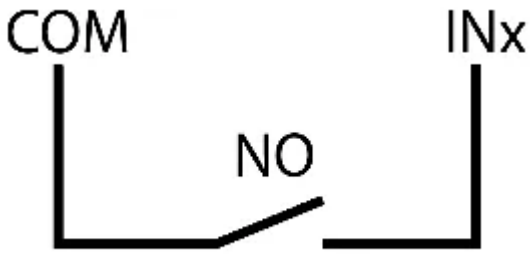


Abbildung 10. NO – im Ruhezustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

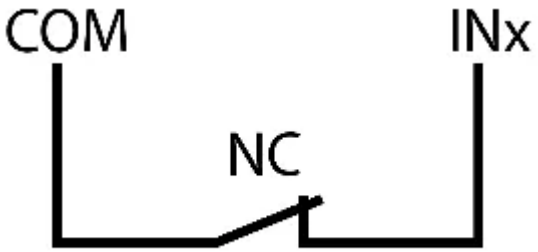


Abbildung 11. NC – im Ruhezustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

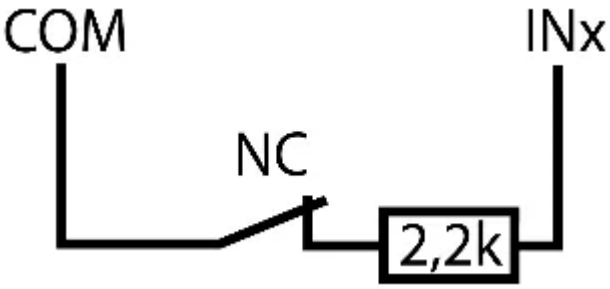


Abbildung 12. NC/EOL – im Ruhezustand geschlossener Kreis mit 2,2-kΩ-Abschlusswiderstand: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

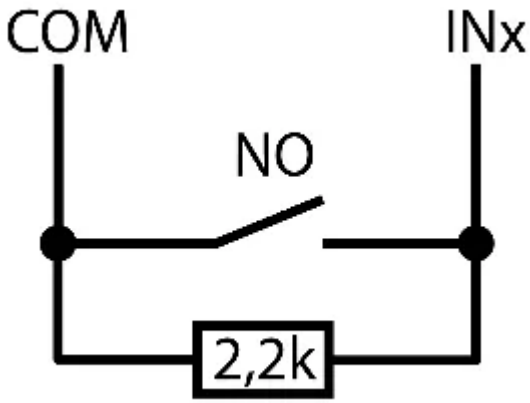


Abbildung 13. NO/EOL – im Ruhezustand offener Kreis mit 2,2-kΩ-Abschlusswiderstand: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

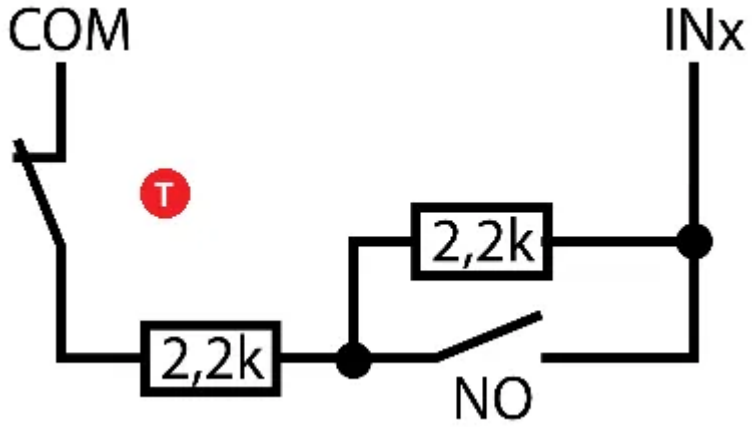


Abbildung 14. NO/DEOL – im Ruhezustand offener Kreis mit 2,2-kΩ-Abschlusswiderstand und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

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

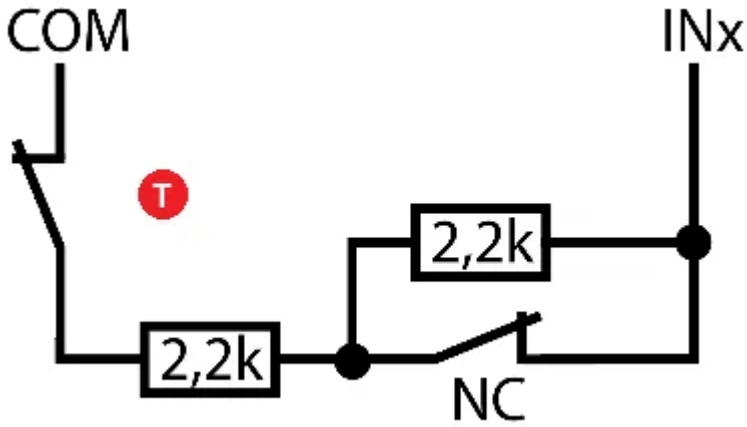


Abbildung 15. NC/DEOL – im Ruhezustand geschlossener Kreis mit 2,2-kΩ-Abschlusswiderstand und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

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

Früherer E16T

Die beiden Eingänge (IN1, IN2) des früheren E16T (2 Eingänge + OUT) nehmen Kreise vom Typ NO, NC oder EOL auf; die Werkseinstellung ist NO. Den Eingangstyp stellen Sie dort nicht auf der Seite IN/OUT, sondern auf der Seite **Event summary** von TrikdisConfig ein (Hinweis in Abschnitt 6.6). Der Anschluss ist derselbe: Schließen Sie den Eingang entsprechend dem gewählten Typ (NO, NC, EOL) an.

3.6 Anschluss des Ethernet-Kabels

Stecken Sie ein Ende des Ethernet-Kabels in die RJ45-Buchse auf der Leiterplatte des E16T, das andere in einen freien Port des Routers oder Switches. Nötig ist ein herkömmliches, 1:1 belegtes Kabel (Patchkabel); das Kabel wird durch die obere Öffnung des Gehäuses eingeführt. Dass die Netzwerkverbindung zustande gekommen ist, zeigt nach dem Einschalten das grüne Licht der LED **NETWORK**.

3.7 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. Einen größeren Verbraucher oder ein Gerät mit Netzspannung schalten Sie **über ein Relais**: Ein Ende der Relaisspule kommt an +DC, das andere an die I/O-Klemme. Eine Anzeige-LED lässt sich auch direkt an den Ausgang anschließen: von +DC über einen 2,2-kΩ-Vorwiderstand an die LED, das andere Bein der LED an die I/O-Klemme (beim früheren E16T an die Klemme OUT).

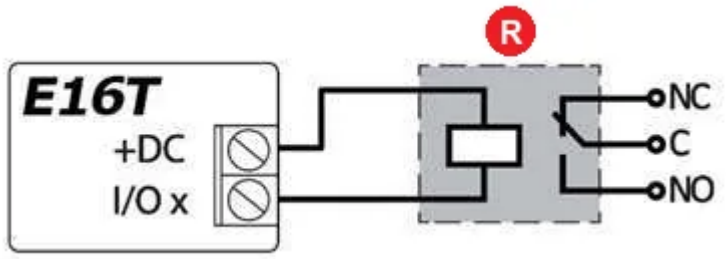


Abbildung 16. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule kommt zwischen +DC und die Klemme I/O x, die Kontakte (NC, C, NO) schalten den Verbraucher.

- R Relais („Relay“)

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

3.8 Anschluss des Erweiterungsmoduls iO-8

Wenn mehr Ein- oder Ausgänge nötig sind, lassen sich an den RS485-Bus des E16T höchstens vier Erweiterungsmodule **iO-8** anschließen; jedes bringt 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 von den 12 V der Zentrale. Der RS485-Bus darf höchstens 100 m lang sein – das ist ein theoretisches Maximum, siehe den Hinweis in Abschnitt 3.2. Das Modul muss in TrikdisConfig auf der Seite **RS485 modules** hinzugefügt werden (Abschnitt 6.7). Hier lassen sich auch die anderen Mitglieder der iO-Serie anschließen (iO, iO-WL, iO-LO, LO-MOD); die Module W485 und E485 gehören nicht zum E16T, denn der E16T ist selbst ein Gerät für kabelgebundenes Internet.

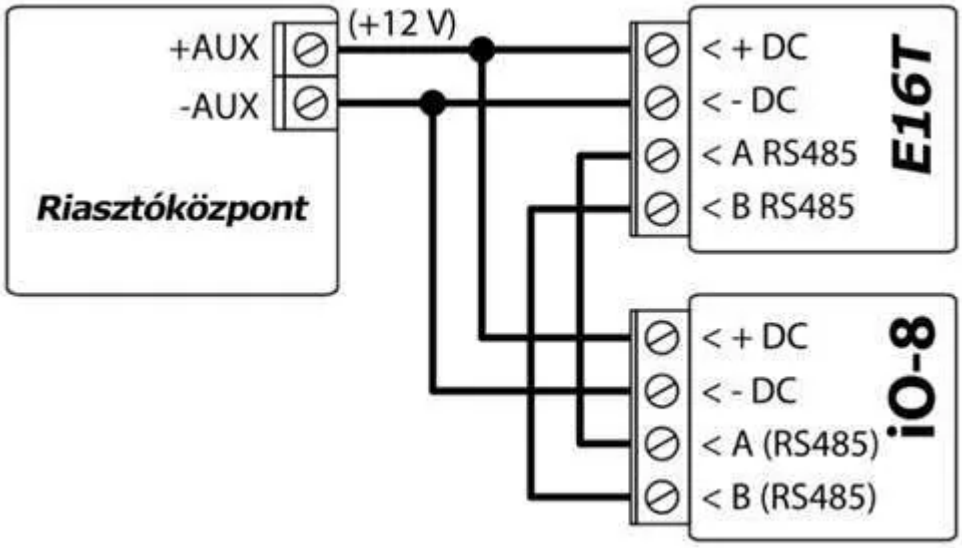


Abbildung 17. Anschluss des Erweiterungsmoduls iO-8 an den RS485-Bus des E16T; die Versorgung kommt vom AUX-Ausgang der Alarmzentrale.

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 dem Frontdeckel sollten Sie Folgendes sehen:

- **POWER** leuchtet grün – die Versorgung ist in Ordnung;
- **NETWORK** leuchtet grün – mit dem lokalen Netzwerk verbunden;
- **TROUBLE** leuchtet nicht.

Wenn TROUBLE blinkt, verrät die Zahl der Blinkzeichen die Ursache (Abschnitt 1.6): 1 = keine physische Verbindung (Kabel, Port), 2 = keine IP-Adresse erhalten (DHCP), 3 = DNS-Fehler, 6 = Empfänger nicht erreichbar. Wenn keine LED leuchtet, prüfen Sie die Versorgung und die Verkabelung.

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 Wählgeräts der Honeywell Vista

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

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

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

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

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

4.2 Zentralen anderer Hersteller

Suchen Sie in der Errichteranleitung jeder Zentrale dieselben vier Einstellungen: Freigabe des Telefonleitungs-Kommunikators, Telefonnummer des Empfängers, Wählverfahren (DTMF) und Übertragungsformat (Contact ID). Wenn die Zentrale vor dem Wählen einen Wählton (dial tone) erwartet, liefert ihn der E16T; startet der Anruf trotzdem nicht, schalten Sie in der Zentrale die Wähltonerkennung aus („Wählen ohne Wählton" oder eine ähnliche Option).

Wenn die Zentrale am Ende des Anrufs einen Fehler meldet, obwohl das Ereignis angekommen ist, prüfen Sie auf der Seite **System settings** von TrikdisConfig die Einstellung **Wait acknowledgment from CMS**: 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 die Ereignisse, kann scharf- und unscharfschalten und die Ausgänge des Kommunikators schalten.

5.1 Hinzufügen des Geräts

Prüfen Sie vor dem Hinzufügen des Geräts:

1. Der E16T ist mit dem Netzwerk verbunden und erreicht das Internet: Die LED **NETWORK** leuchtet grün, und die LED **DATA** erlischt nach einem Ereignis oder einer Testmeldung.
2. Auf der Seite **User reporting** → **PROTEGUS Cloud** von TrikdisConfig (Abschnitt 6.4) ist **Enable connection** angehakt – die Protegus Cloud ist also freigegeben –, und der **Protegus Cloud access code** ist eingestellt (nach dem Anlegen des Systems ist er nicht mehr änderbar).
3. Die LED **POWER** leuchtet grün.

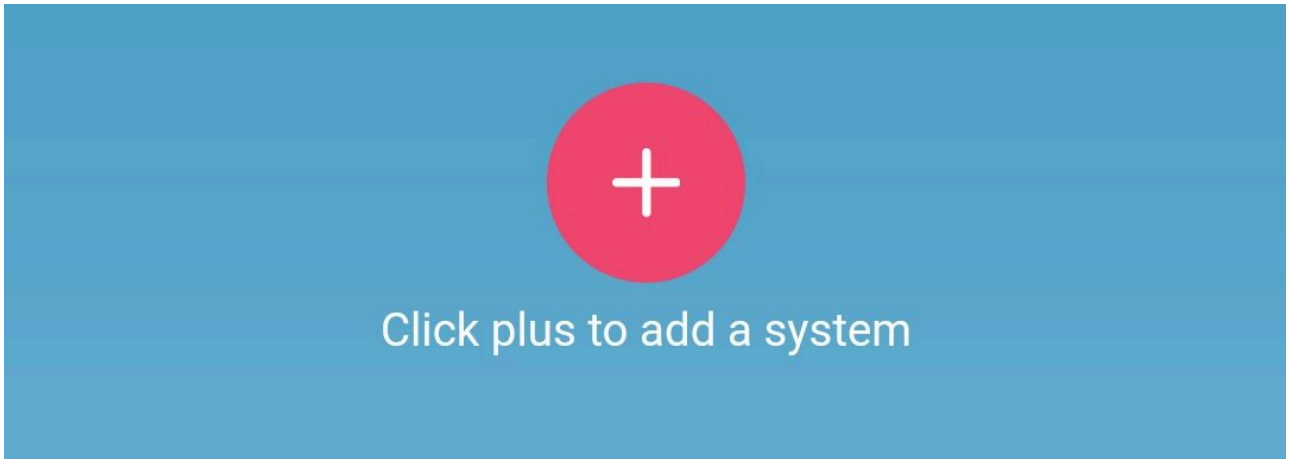
Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet,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

A rendszer létrehozása a Protegus 2 alkalmazásban

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



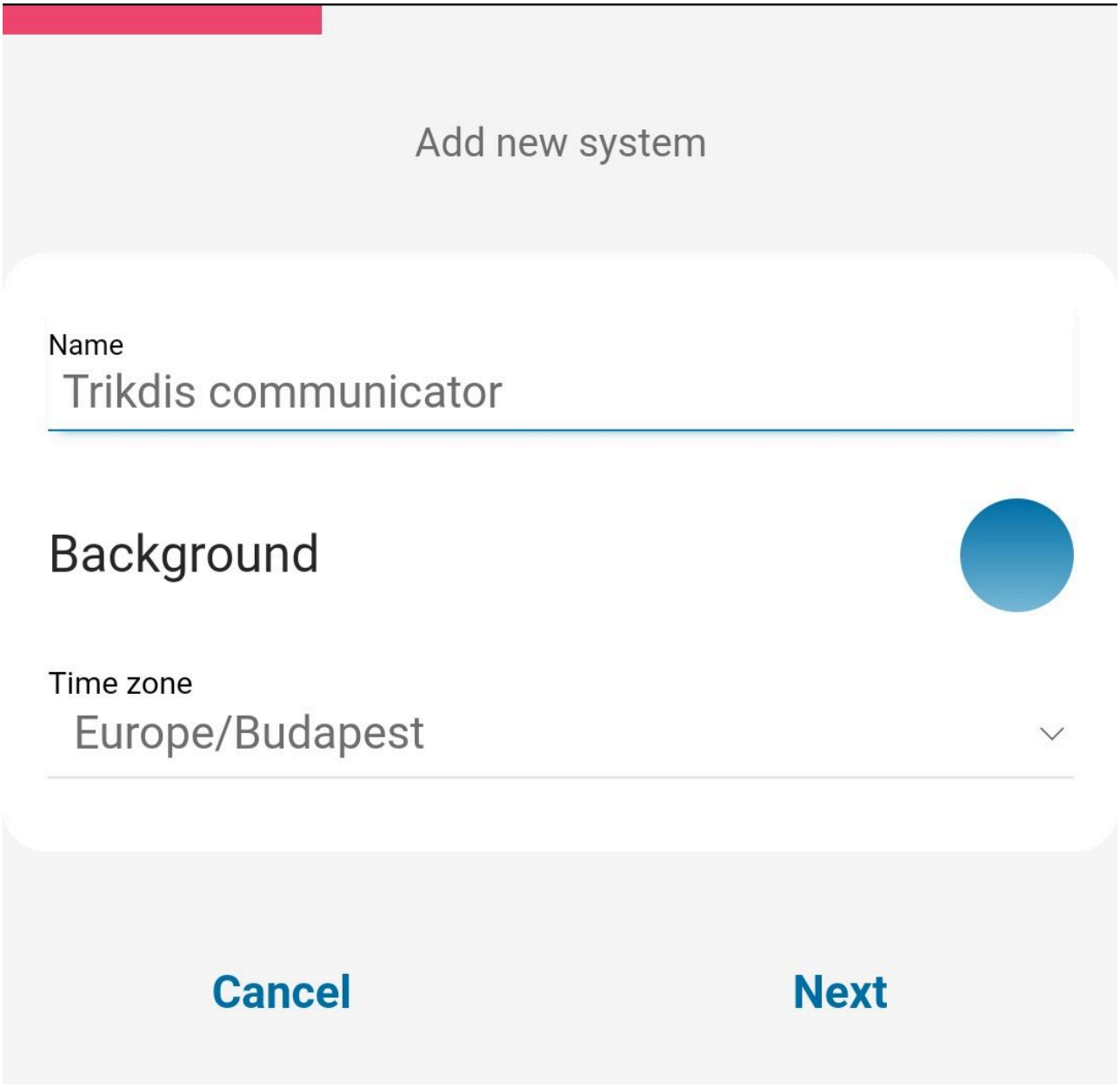
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



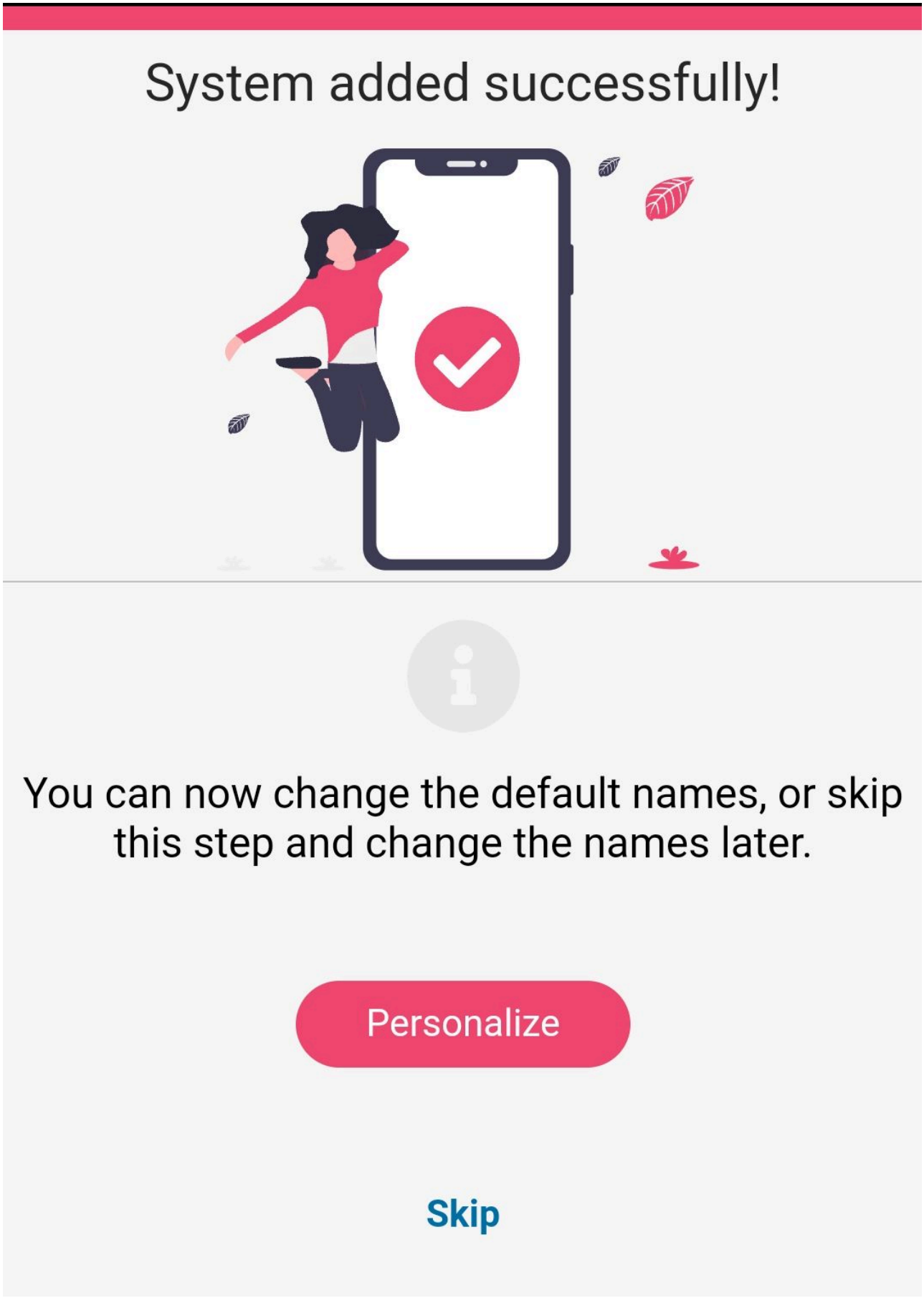
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



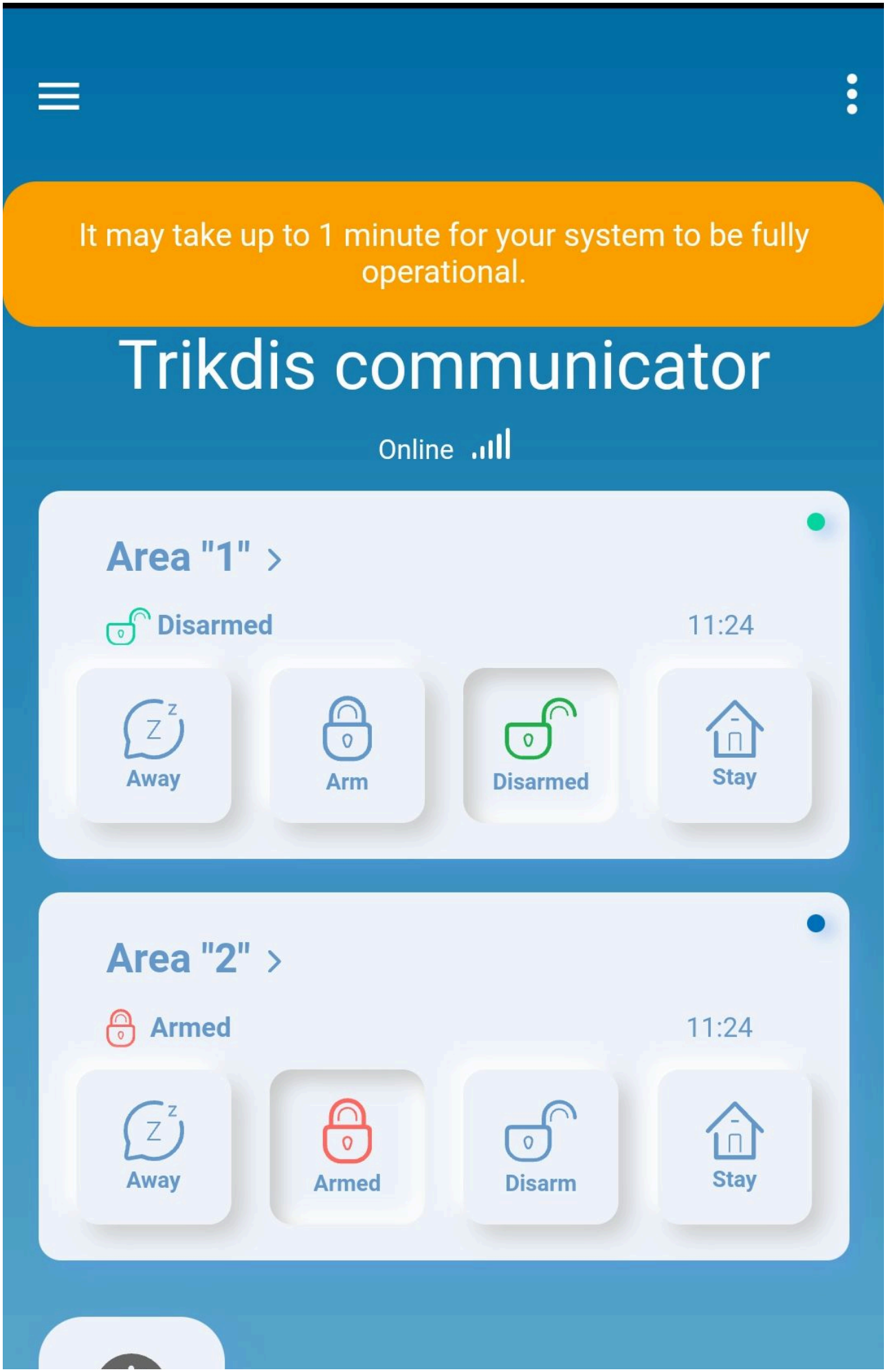
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Die eindeutige Kennung des Geräts ist beim E16T die **MAC-Adresse**: Sie steht auf der Verpackung und auf der Rückseite des Geräts, und auch TrikdisConfig zeigt sie an (**MAC / Unique ID**).

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.

6. TrikdisConfig – die Einstellungen im Detail

Auf der linken Seite des TrikdisConfig-Fensters steht die Liste der Seiten (System settings, CMS reporting, User reporting, Ethernet settings, 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 E16T 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 18. Die Statusleiste von TrikdisConfig mit ausgelesenem E16T: links die Schaltfläche für die Rücksetzung auf Werkseinstellungen und MAC / Unique ID, unten Status, Typ, Seriennummer, Versionen, Verbindungsart und Zugriffsebene.

Nach **Read [F4]** liest das Programm die im Gerät gespeicherten Einstellungen aus und zeigt sie an; im Feld **Device** muss der Gerätetyp zu sehen sein (E16T; bei der v2 **E16T_2000**). Nehmen Sie die 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.

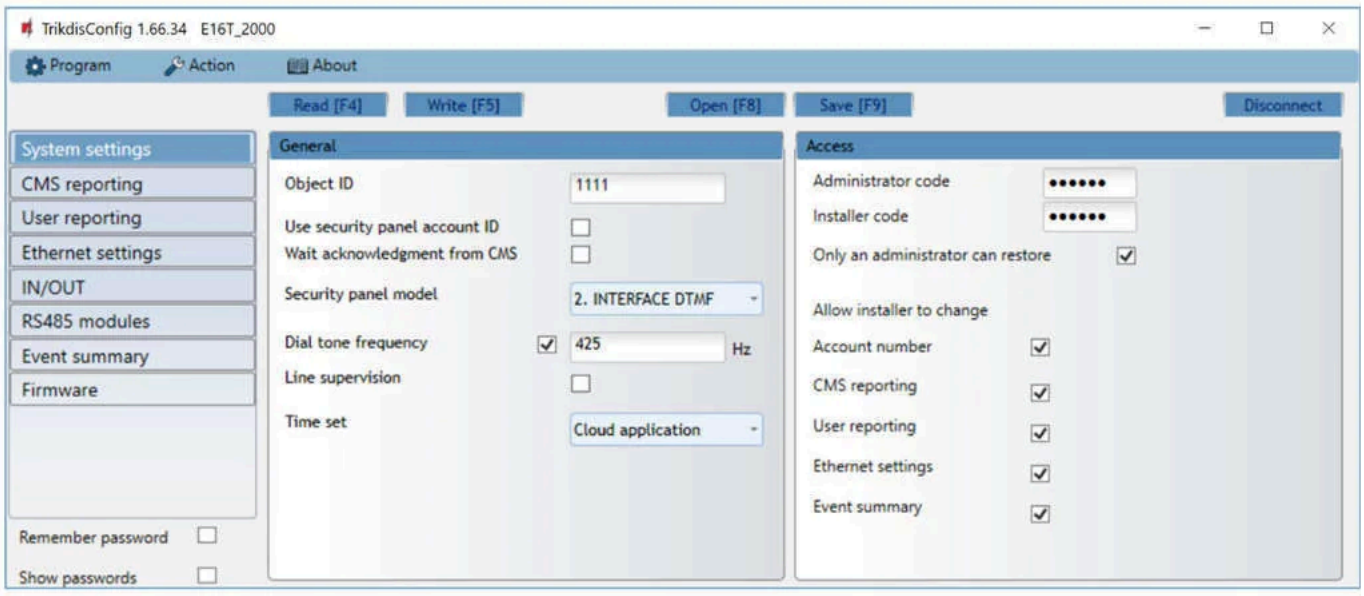


Abbildung 19. TrikdisConfig – Seite System settings: Gruppen General und Access.

- **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen: 0–9, A–F; `FFFE` und `FFFF` sind nicht verwendbar). 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 die Quittung des Empfängers ab und sendet erst danach das Abschlusssignal (Kiss-off) an die Zentrale. Bleibt die Quittung aus, sendet die Zentrale das Ereignis erneut. In einem System ohne Leitstelle, nur mit Protegus 2, lassen Sie es ausgeschaltet (Werkseinstellung).
- **Security panel model** – der Typ der Telefonleitungsschnittstelle; Standard **2. INTERFACE DTMF**. Damit schalten Sie die DTMF-Telefonleitungsschnittstelle des Kommunikators ein oder aus.
- **Dial tone frequency** – die Frequenz des Wähltons, den der E16T der Zentrale 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).
- **Time set** – die Quelle für die Uhr des Geräts (Standard **Cloud application**, die Protegus Cloud).

Früherer E16T

Beim früheren E16T gibt es auf der Seite System settings weitere Gruppen:

- **General → Test period** – die periodische Testmeldung wird in dem hier angegebenen Intervall gesendet (bei der v2 befindet sich dies im Reiter **CMS reporting → Settings**).

- Gruppe **Ethernet settings** (bei der v2 eine eigene Seite, Abschnitt 6.5): **Internal MAC** – die eindeutige Kennung des Geräts, die MAC-Adresse; **Use DHCP** – angehakt meldet sich das Gerät automatisch im Netzwerk an; gelingt die automatische Anmeldung nicht, füllen Sie die Felder **Internal IP address**, **Mask** (Subnetzmaske), **Gateway** und **DNS** manuell aus.
- Gruppe **Output** (bei der v2 die Seite IN/OUT, Abschnitt 6.6): **OUT type** – die Funktion des Ausgangs aus der Liste: Disabled (ausgeschaltet), LAN OK (das Netzwerk ist in Ordnung), Communication Trouble (Kommunikationsfehler), Remote Control (Fernsteuerung aus der App Protegus); **Inverted** – angehakt arbeitet der Ausgang umgekehrt; **OUT mode**: **Pulse** – der Ausgang bleibt für die im Feld **Pulse Time** angegebene Zeit (Sekunden) im neuen Zustand, **Level** – der Zustand bleibt bis zum nächsten Befehl erhalten; **Pulse time** – die Impulslänge in Sekunden; im Modus Pulse schaltet der Ausgang für diese Zeit.

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 IP an die Leitstelle. Die Ereignisse können über mehrere Kanäle gehen: Der **Primärkanal** und der **Parallelkanal** arbeiten gleichzeitig (an zwei Empfänger zugleich), und zu jedem gehört ein **Ersatzkanal**, der in Kraft tritt, wenn der jeweilige Kanal unterbrochen ist. Die Kommunikation ist verschlüsselt und passwortgeschützt; für den Empfang und die Weiterleitung an die Leitstellensoftware ist ein Trikdis-Empfänger (Software-Empfänger IPcom für Windows oder Linux, Hardware-IP/SMS-Empfänger RL14, Mehrkanalempfänger RM14) oder ein universeller Empfänger nötig, der die Protokolle DC-09 / TL150 beherrscht.

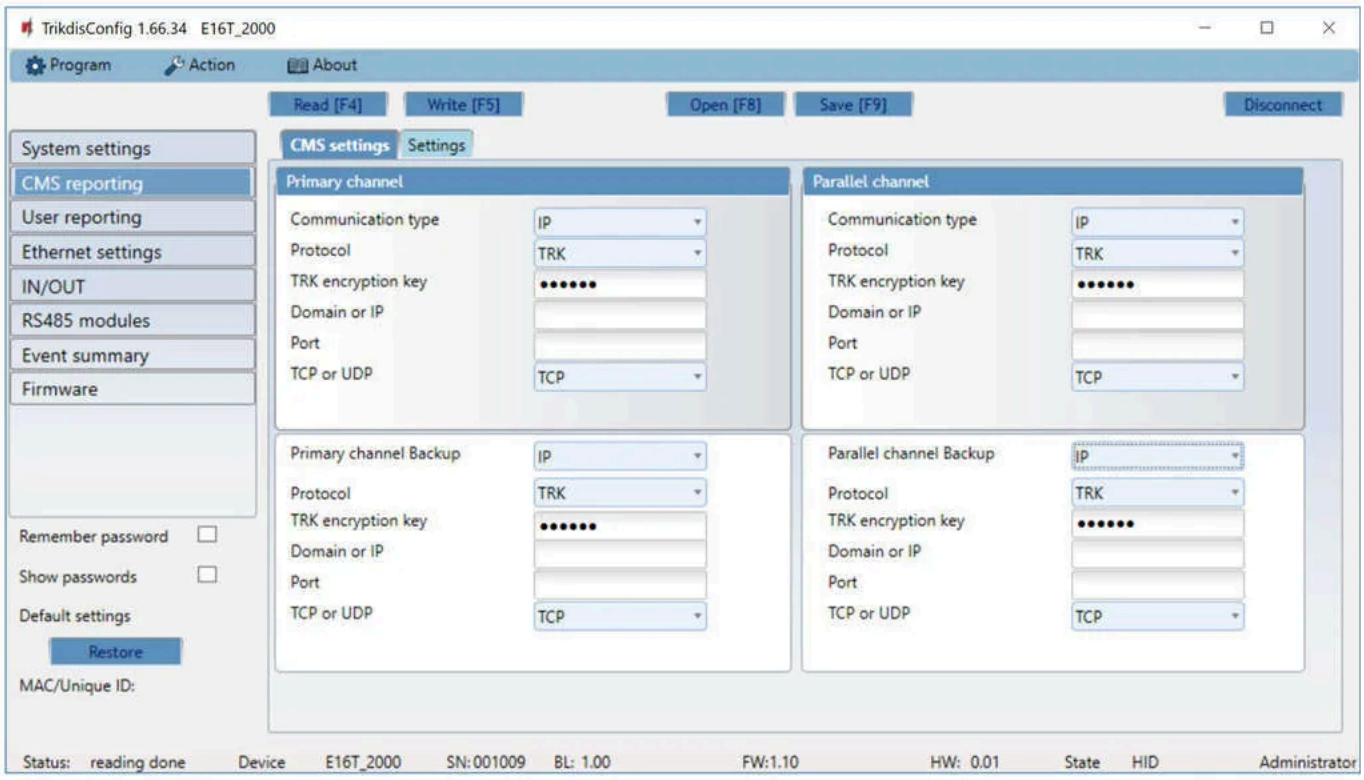


Abbildung 20. TrikdisConfig – CMS reporting, Reiter CMS settings: Primär-, Ersatz- und Parallelkanal.

Primary channel – Primärkanal

- **Communication type** – beim E16T ist nur **IP** wählbar.
- **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** – die Adresse des Empfängers (Domainname oder IP-Adresse) und seine Netzwerk-Portnummer.
- **TCP or UDP** – das Übertragungsprotokoll: damit sendet er die Ereignisse (gemäß der Einstellung des Empfängers).

Primary channel Backup – Ersatzkanal. Übernimmt die Kommunikation, wenn der Primärkanal nicht funktioniert; die Einstellungen sind dieselben wie oben. Auch bei einem kabelgebundenen Gerät lohnt sich die Angabe – zum Beispiel einer zweiten Adresse oder eines zweiten Ports des Empfängers –, denn der Ersatzkanal überbrückt auch einen Fehler auf der Seite des Empfängers.

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.

Früherer E16T

Beim früheren E16T zeigt TrikdisConfig dasselbe im Fenster **Reporting** im Reiter **CMS Reporting**, mit anderen Feldnamen:

- Gruppe **Primary**: **Enable** – angehakt ist der Primärkanal zur Leitstelle aktiv; **Remote Host** – Domainname oder IP-Adresse des Empfängers; **Remote Port** – Netzwerk-Portnummer des Empfängers; **TCP or UDP** – das Übertragungsprotokoll; **PING Time** – einschalten und die Zeit

zwischen den Lebenszeichen angeben (Werkswert 30) – nötig für die Überwachung der Verbindung; **Encryption key** – 6-stelliger Verschlüsselungsschlüssel, im Kommunikator und im Empfänger derselbe.

- Gruppe **Backup**: **Enable** – schaltet den Ersatzkanal ein, der sendet, wenn die Primärverbindung unterbrochen ist; die übrigen Felder sind dieselben wie beim Primärkanal.
- Gruppe **Settings**: **TCP protocol** – die Codierung der Übertragung: TRK (für einen Trikdis-Empfänger), DC-09_2007 oder DC-09_2012 (für einen universellen Empfänger).
- Gruppe **SIA IP parameter** – nur änderbar, wenn im Feld **TCP protocol** DC-09_2007 oder DC-09_2012 steht: **Encryption enabled** – bei DC-09_2012 lässt sich die Verschlüsselung einschalten; **DC09-2012 encryption key** – der im Empfänger eingestellte Verschlüsselungsschlüssel; **DC09-2012 receiver No.** – die Nummer des Empfängers; **DC-09 line No.** – die Nummer der Empfängerlinie; **Use time stamp** – angehakt enthält die Meldung auch die Zeit (Zeitstempel).

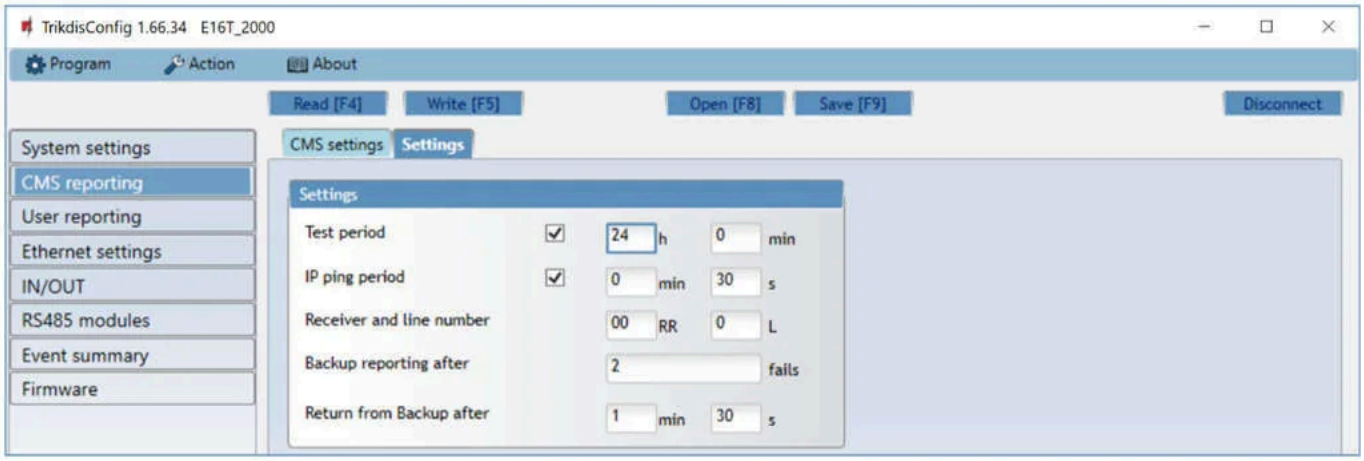


Abbildung 21. TrikdisConfig – CMS reporting, Reiter Settings: Testmeldung, PING, Empfänger- und Liniennummer (Receiver and line number: RR = Empfängernummer, L = Liniennummer) und die Zeiten des Ersatzkanals.

Im Reiter **Settings** stellen Sie die Zeiten sowie die Empfänger- und Liniennummer ein; die Gruppe DC-09 ist nur nötig, wenn Sie mit dem Protokoll DC-09 senden (auf dem Bildschirmfoto von 2022 ist sie noch nicht zu sehen).

- **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.

6.4 User reporting

Im Reiter **PROTEGUS Cloud** geben Sie den Protegus-Dienst frei. Der E16T hat keine SMS-Benachrichtigung und keine SMS-Steuerung, deshalb gibt es auf dieser Seite nur diesen einen Reiter.

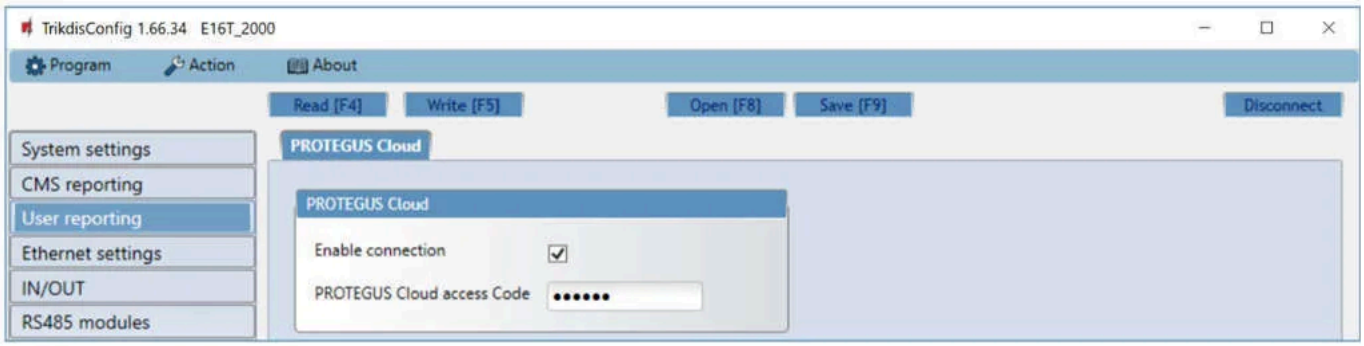


Abbildung 22. TrikdisConfig – User reporting, Reiter PROTEGUS Cloud.

- **Enable connection** – erlaubt die Verbindung mit der Protegus Cloud und den Fernzugriff von TrikdisConfig.
- **Protegus Cloud access code** – 6-stelliger Code für die Protegus-Verbindung (ab Werk `123456`). Wenn Sie ihn geändert haben, muss beim Hinzufügen des Systems in Protegus 2 dieser eingegeben werden. Er lässt sich nur vor dem Anlegen des Systems in Protegus 2 einstellen, nachträglich ist er nicht änderbar.

6.5 Ethernet settings

Hier legen Sie fest, wie sich der E16T mit dem lokalen Netzwerk verbindet.



Abbildung 23. TrikdisConfig – Seite Ethernet settings; ab Werk ist DHCP eingeschaltet.

- **Use DHCP** – mit Häkchen erhält das Gerät IP-Adresse, Subnetzmaske und Gateway automatisch vom DHCP-Server des Routers. Das ist die Werkseinstellung, und an den meisten Orten ist damit nichts weiter zu tun. Wenn es im Netzwerk kein DHCP gibt, die automatische Anmeldung im Netzwerk nicht gelingt oder der Netzwerkadministrator eine feste Adresse verlangt, entfernen Sie das Häkchen und füllen Sie die folgenden Felder und die Nameserver von Hand aus:
- **Static IP** – die feste IP-Adresse des Geräts im lokalen Netzwerk (eine Adresse, die kein anderes Gerät verwendet und die außerhalb des DHCP-Bereichs liegt).

- **Subnet mask** – die Subnetzmaske des Netzwerks.
- **Default gateway** – das Standard-Gateway, meist die Adresse des Routers. Mit einem falschen Gateway erreicht das Gerät das lokale Netzwerk, aber nicht das Internet.
- **DNS 1, DNS 2** – Nameserver; über sie findet das Gerät die Protegus-Cloud und einen mit Domainnamen angegebenen Empfänger. Werkseitig ist der öffentliche DNS von Google eingetragen; wenn das Netzwerk nach außen nur den eigenen Nameserver zulässt, tragen Sie hier die Adresse des lokalen DNS ein. 3 Blinkimpulse der TROUBLE-LED zeigen einen DNS-Fehler an.

Die eindeutige Kennung des Geräts, die MAC-Adresse (im Programm **Internal MAC**), ist im neueren TrikdisConfig-Fenster nicht auf dieser Seite, sondern unten im Fenster im Feld **MAC / Unique ID** der Statusleiste zu sehen.

Das Gerät baut nur **ausgehende** Verbindungen zum Empfänger und zur Protegus-Cloud auf, deshalb müssen am Router keine Ports geöffnet oder weitergeleitet werden, und eine öffentliche feste IP-Adresse ist nicht nötig.

Beim früheren E16T zeigt das Feld **Internal MAC** der Gruppe Ethernet settings auf der Seite **System settings** die MAC-Adresse an (Hinweis in Abschnitt 6.2).

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 ist auch der Typ anzugeben (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

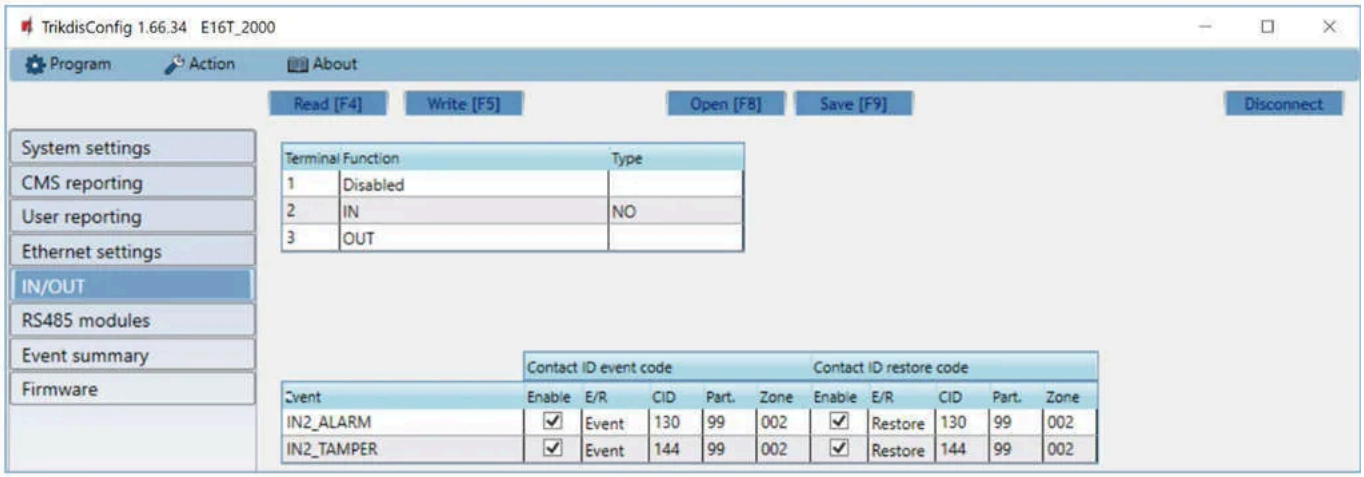


Abbildung 24. TrikdisConfig – Seite IN/OUT: Funktion der I/O-Klemmen und Ereignisse der Eingänge.

Wird der an einen 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 jeder als Eingang eingestellten Klemme. Die Spalten der Tabelle:

- **Enable** – erlaubt das Senden der Meldung.
- **E/R** – der Ereignistyp: Event (Alarm) oder Restore (Wiederherstellung).
- **CID** – der Contact-ID-Code.
- **Part.** – die Bereichsnummer in der Meldung.
- **Zone** – die Zonennummer in der Meldung.

Früherer E16T

Beim früheren E16T gibt es keine Seite IN/OUT: Typ und Ereignisse der beiden Eingänge stellen Sie in der Gruppe **Input description** der Seite **Event summary** ein. **Partition** – die Bereichsnummer; **Contact ID** – der Ereigniscode (der Werkswert kann bleiben), bei Auslösung des Eingangs sendet er diesen Code an Protegus und an die Leitstelle; **Zone No.** – die Zonennummer, sie geht in die Meldungen; **Type** – der Eingangstyp (NO, NC, EOL); **Enable / Alarm** – angehakt meldet er, wenn der Eingang ausgelöst wird (Ereignis); **Enable / Restore** – angehakt meldet er, wenn der Eingang wiederhergestellt ist. Die Einstellung des Ausgangs befindet sich in der Gruppe **System settings → Output** (Hinweis in Abschnitt 6.2).

6.7 RS485 modules

Die an den RS485-Bus angeschlossenen Erweiterungsmodule iO-8 und andere Module der iO-Serie müssen im Reiter **Modules list** hinzugefügt werden.

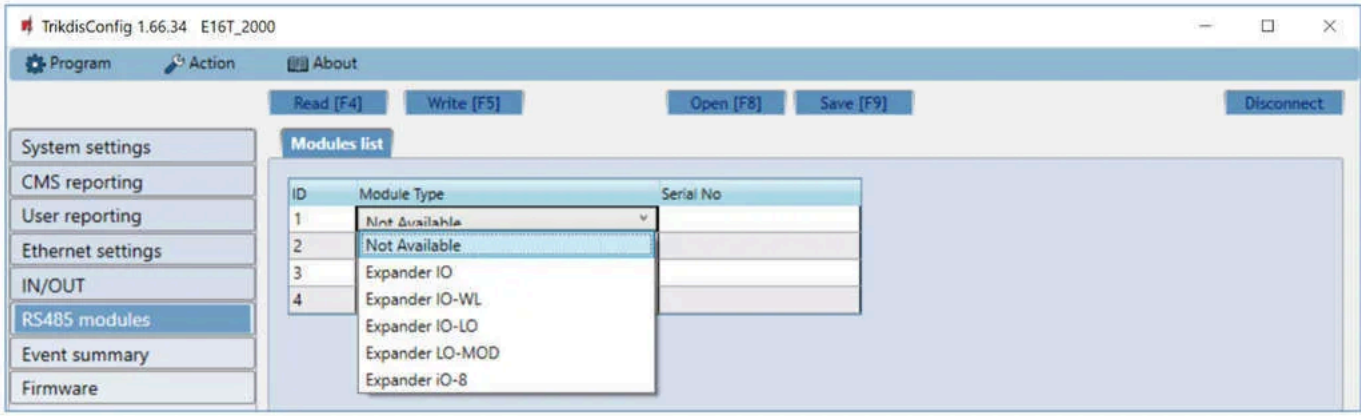


Abbildung 25. TrikdisConfig – RS485 modules, Reiter Modules list: die wählbaren Modultypen.

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

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

Erweiterungsmodul iO-8 – 8 I/O mit Doppelfunktion; an den Kommunikator lassen sich höchstens 4 Module anschließen.

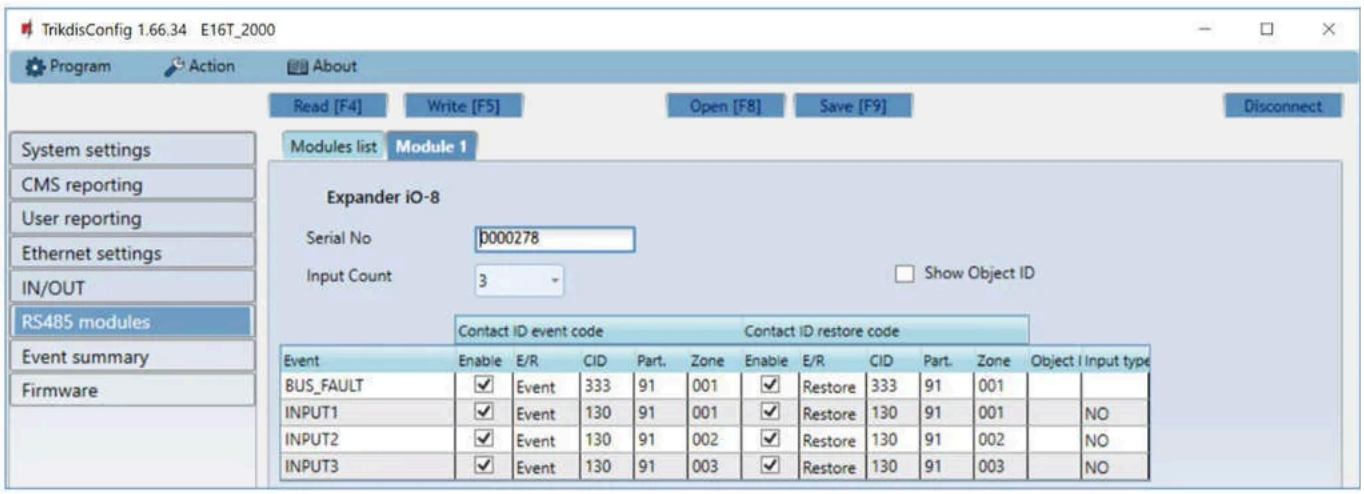


Abbildung 26. TrikdisConfig – RS485 modules, Reiter des Moduls iO-8.

- **Input Count** – wie viele Klemmen Eingänge sein sollen; die übrigen werden Ausgänge. Der Eingangstyp (**Input type**: NO oder NC) lässt sich in der Tabelle angeben. 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) Contact-ID-Codes zuordnen (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Standardmäßig meldet das 1. Modul mit Bereich 91, das 4. Modul mit Bereich 94. Durch Anhaken von **Show Object ID** lässt sich für die Eingänge auch eine vom Kommunikator abweichende Objektkennung angeben.

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.

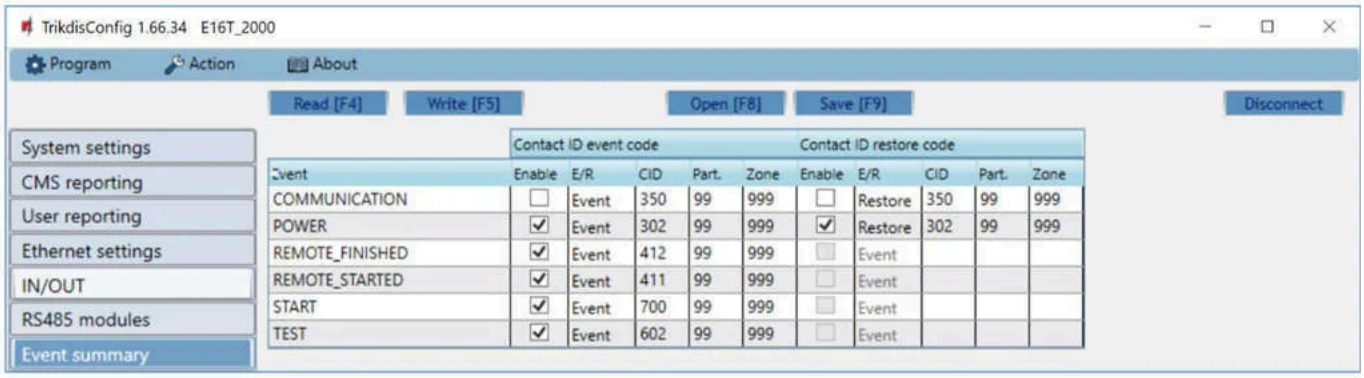


Abbildung 27. TrikdisConfig – Seite Event summary: die internen Meldungen des Geräts.

Beim früheren E16T befindet sich auf dieser Seite auch die Einstellung der Eingänge (Hinweis in Abschnitt 6.6).

6.9 Rücksetzung 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.

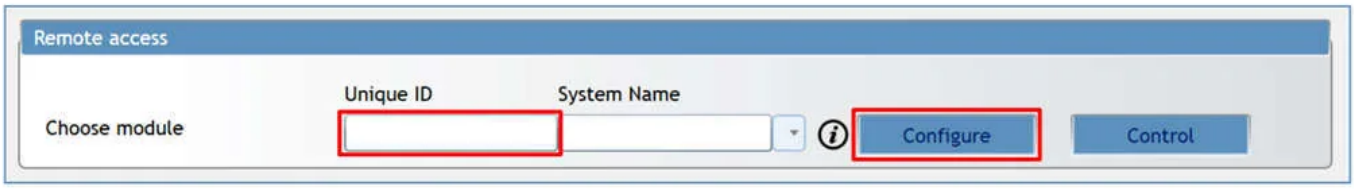


Abbildung 28. TrikdisConfig – Remote access: die Kennung des Geräts (beim E16T die MAC-Adresse), der Name des Systems und die Schaltfläche Configure.

Die Freigabe des Protegus-Dienstes beschreibt Abschnitt 6.4, das Herunterladen von TrikdisConfig Abschnitt 2.1.

8. Prüfung der Funktion des Kommunikators

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

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

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

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.

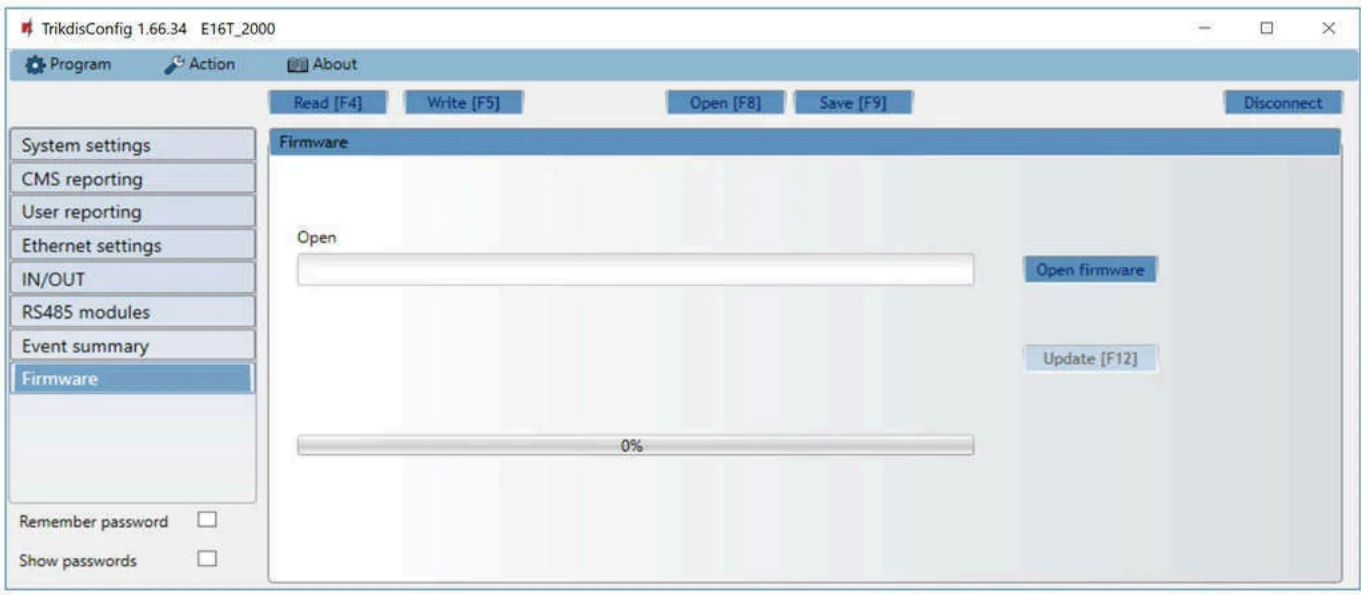


Abbildung 29. TrikdisConfig – Seite Firmware: Open firmware und Update [F12].

Für die Aktualisierung ist eine Internetverbindung nötig. Ein Virenscanner, eine Firewall oder strenge Netzwerkeinstellungen können den automatischen Firmware-Download verhindern; laden Sie die Datei in diesem Fall 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. Wenn die Antwort auf das ausführliche Kapitel verweist, finden Sie dort die genaue Stelle der Einstellung.

Die LED NETWORK leuchtet nicht – kein Netzwerk

1. Sehen Sie sich die Blinkzeichen der LED **TROUBLE** an: 1 = keine physische Verbindung, 2 = keine IP-Adresse erhalten (DHCP), 3 = DNS-Fehler.
2. **Bei 1 Blinkzeichen** prüfen Sie das Kabel und die Stecker (ob der RJ45-Stecker bis zum Einrasten eingesteckt ist), den Port des Routers oder Switches (ob er aktiv und nicht gesperrt ist), und versuchen Sie ein anderes Kabel oder einen anderen Port.
3. **Bei 2 Blinkzeichen** gibt es im Netzwerk keinen DHCP-Server oder er antwortet nicht: Schalten Sie ihn am Router ein, oder geben Sie dem Gerät auf der Seite **Ethernet settings** eine feste IP-Adresse, Maske und Gateway (Abschnitt 6.5).

4. **Bei 3 Blinkzeichen** funktioniert die Namensauflösung nicht: Prüfen Sie die Felder DNS 1 / DNS 2 (ab Werk der öffentliche DNS von Google) und ob das Netzwerk ausgehenden DNS-Verkehr erlaubt.

Es gibt Netzwerk, 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 LED **TROUBLE** zeigen, dass keine Verbindung mit dem Empfänger besteht: Prüfen Sie Adresse und Port des Empfängers, die Einstellung TCP/UDP und den Verschlüsselungsschlüssel (**CMS reporting**).
2. Wenn der Empfänger mit einem Domainnamen angegeben ist, prüfen Sie die DNS-Einstellung (**Ethernet settings**).
3. Prüfen Sie bei einer festen IP-Adresse das Gateway (**Default gateway**): Mit einem falschen Gateway erreicht das Gerät das lokale Netzwerk, aber nicht das Internet.
4. In einem Firmennetz oder gefilterten Netzwerk kann die Firewall die ausgehende Verbindung zum Port des Empfängers sperren – stimmen Sie sich mit dem Netzwerkadministrator ab (Abschnitt 3.2).

Die Zentrale sendet die Ereignisse nicht an den Kommunikator

1. Das Wählgerät 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 einen Wählton erwartet und den Anruf nicht startet, schalten Sie in ihr die Wähltonerkennung aus.
4. Wenn die Zentrale einen „Kommunikationsfehler" meldet, 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** eingegeben werden; nach dem Anlegen des Systems ist er im Gerät nicht mehr änderbar.
3. Geben Sie die MAC-Adresse genau ein, von der Verpackung oder von der Rückseite – oder scannen Sie den QR-Code des Etiketts mit der App, so sind Tippfehler ausgeschlossen.
4. Die Internetverbindung muss in Ordnung sein: Die LED NETWORK leuchtet grün, und die LED DATA erlischt nach einem Ereignis. Für den Zugriff auf die Protegus Cloud ist auch ein funktionierender DNS nötig (**Ethernet settings**).

Ich komme mit TrikdisConfig nicht aus der Ferne auf das Gerät

1. Das Gerät muss online sein (LED NETWORK grün, die LED DATA erlischt nach einem Ereignis), 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 Errichterpasswort.

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.

Brauche ich eine feste IP-Adresse oder eine Portweiterleitung am Router?

Nein. Der E16T baut die ausgehende Verbindung zum Empfänger und zur Protegus Cloud selbst auf, deshalb sind weder eine öffentliche feste IP-Adresse noch dynamisches DNS noch eine Portweiterleitung nötig. Im lokalen Netzwerk ist auch die per DHCP erhaltene Adresse geeignet; eine feste lokale Adresse vergeben Sie nur, wenn es im Netzwerk kein DHCP gibt oder der Netzwerkadministrator es verlangt (Abschnitt 6.5).

Funktioniert er über WLAN?

Nein: Der E16T kennt nur eine kabelgebundene (RJ45-)Netzwerkverbindung. Wenn es in der Nähe der Zentrale kein Netzwerkkabel gibt, lässt sich eine WLAN-Brücke bis zum Router einrichten, oder Sie wählen den Mobilfunk-Kommunikator G16T.

Was passiert bei einem Stromausfall?

Der Kommunikator wird vom Akku der Zentrale versorgt, aber wenn Router und Modem ohne Strom bleiben, gibt es kein Internet, und die Ereignisse warten im Speicher (die LED DATA leuchtet). Das Gerät sendet sie, sobald das Internet zurück ist. Wenn der Ausfall nicht akzeptabel ist, sind eine unterbrechungsfreie Stromversorgung der Netzwerkgeräte oder ein Mobilfunk-Kommunikator die Lösung (Abschnitt 3.2).

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 sorgfältig; die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen oder Defekten führen.
- Trennen Sie die Anlage vor dem Anschließen, bei jedem elektrischen Anschließen und vor Servicearbeiten von der Versorgung.

- Fehler durch unsachgemäße Installation oder Verwendung 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

- Scharfschalten aus der Ferne per Schlüsselschalter aus der App Protegus 2 – Details und Fallstricke des Scharfschaltens per Schlüsselschalter.
- Englischsprachige Dokumentation: docs.trikdis.com.

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

Passende Produkte

Trikdis E16T Ethernet Universal Communicator - IP -Modul

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/e16t-anleitung