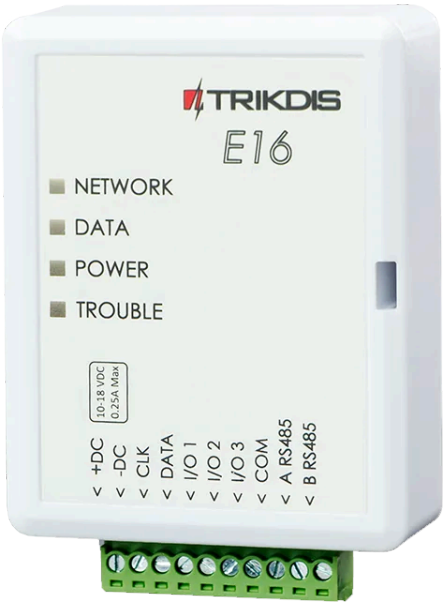
mobilamb
TRIKDIS Official Distributor

Kommunikator E16 – Errichter- und Benutzeranleitung

Errichter- und Benutzeranleitung für den Trikdis-Ethernet-Kommunikator E16: Anschluss an den Datenbus oder die serielle Schnittstelle der Alarmzentrale, Programmierung der Zentrale, Netzwerkeinstellung in TrikdisConfig, Übertragung an die Leitstelle, App Protegus 2.



Ausgabe: 2026-11-17
Immer aktuelle Webversion: https://trikdis.at/e16-anleitung

Inhalt

1. Überblick

- 1.1 Wozu er dient, wie er funktioniert
- 1.2 Kompatible Alarmzentralen
- 1.3 Hauptmerkmale
- 1.4 Teile des Kommunikators
- 1.5 Klemmen
- 1.6 LED-Anzeigen
- 1.7 Technische Daten

2. Schnelle Inbetriebnahme mit TrikdisConfig

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

3. Installation und Anschluss

- 3.1 Schritte der Installation
- 3.2 Montageort und Netzwerk
- 3.3 Anschluss an die Alarmzentrale
  - 3.3.1 DSC PowerSeries
  - 3.3.2 Paradox
  - 3.3.3 UTC Interlogix (Caddx) NetworX
  - 3.3.4 Texecom Premier / Premier Elite
  - 3.3.5 Crow Runner
  - 3.3.6 Pyronix
  - 3.3.7 Honeywell Ademco Vista
  - 3.3.8 InnerRange Inception und Integriti
- 3.4 Anschluss einer Schlüsselschalterzone
- 3.5 Anschluss von Eingängen
- 3.6 Anschluss eines Ausgangs mit Relais
- 3.7 Anschluss des Erweiterungsmoduls iO-8
- 3.8 Anschluss des Ethernet-Kabels
- 3.9 Einschalten und erste Prüfung
- A TRIKDIS átjelző elindítása

4. Programmierung der Alarmzentrale

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

5. Fernsteuerung mit der App Protegus 2

- 5.1 Gerät hinzufügen
- A rendszer létrehozása a Protegus 2 alkalmazásban
- 5.2 Direkte Steuerung mit dem Bedienteilcode

5.3 Scharfschalten über eine Schlüsselschalterzone
5.4 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 Zurücksetzen auf Werkseinstellungen

7. Fernprogrammierung

8. Prüfung der Funktion des Kommunikators

9. Firmware-Update

10. Fehlersuche und häufige Fragen

11. Sicherheitshinweise

Siehe auch

1. Überblick

Der E16 ist der **direkt angeschlossene Ethernet-Kommunikator** von Trikdis: Er wird nicht an den Telefonleitungsausgang der Alarmzentrale angeschlossen, sondern an den **Bedienteilbus oder die serielle Schnittstelle** der Zentrale. Er liest die Ereignisse direkt aus der Zentrale – zusammen mit Zonen-, Bereichs- und Benutzernummer – 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. Er arbeitet mit den unterstützten Zentralen von DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell und Crow; bei den **direkt steuerbaren** Typen schaltet der Benutzer aus der App Protegus 2 mit seinem eigenen Bedienteilcode scharf und unscharf, ohne separate Schlüsselschalterzone. Für Zentralen anderer Hersteller, die nur einen Telefonleitungsausgang haben, ist der Ethernet-Kommunikator E16T (TIP/RING) gedacht; wo es kein kabelgebundenes Internet gibt, der Mobilfunk-Kommunikator G16.

1.1 Wozu er dient, wie er funktioniert

- **Er liest die Zentrale direkt.** Über den Bus der Zentrale kommt jedes Ereignis sofort und mit der eigenen Nummerierung der Zentrale beim Kommunikator an; das Wählgerät der Zentrale muss nicht eingerichtet werden, und es gibt auch keine Contact-ID-Wahl.
- **Er meldet an die Leitstelle.** Die Ereignisse sendet er über IP an den Software- oder Hardware-Empfänger von Trikdis (Protokoll TRK; die Trikdis-Empfänger arbeiten mit jeder Leitstellensoftware zusammen) bzw. an jeden universellen Empfänger (SIA DC-09 2007/2012, SUR-GARD TL150). Bei einem SUR-GARD-Empfänger wandelt der Kommunikator die von der Zentrale erhaltenen Contact-ID-Codes in SIA-Codes um; die Umrechnungstabelle steht im Anhang der englischsprachigen Herstellerdokumentation. Die Verbindung prüft er standardmäßig alle 30 Sekunden (das Intervall ist änderbar, Abschnitt 6.3) und wechselt bei einem Fehler auf einen Ersatzkanal; mit einem Parallelkanal lassen sich die Ereignisse gleichzeitig an zwei Empfänger senden.
- **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, Heizung, Lüftung, Bewässerungsanlage usw.). Protegus 2 arbeitet mit den Zentralen aller vom E16 unterstützten Hersteller.
- **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.
- **Keine SIM-Karte und kein Mobilfunkvertrag nötig.** Das Gerät nutzt die vorhandene Internetverbindung des Objekts: Es wird mit einem Ethernet-Kabel an den Router oder Switch angeschlossen, bezieht ab Werk seine Adresse per DHCP und baut nur ausgehende Verbindungen auf, deshalb muss am Router kein Port geöffnet werden.
- **Er hat eigene Ein- und Ausgänge.** Drei Klemmen mit Doppelfunktion (I/O) 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.

Den Aufbau des Systems zeigt die folgende Abbildung: Der Bus der Alarmzentrale ist an den E16 angeschlossen, der E16 erreicht über den Router das Internet, von dort die Protegus Cloud und den Empfänger der Leitstelle, und der Benutzer sieht das System in der App Protegus 2.

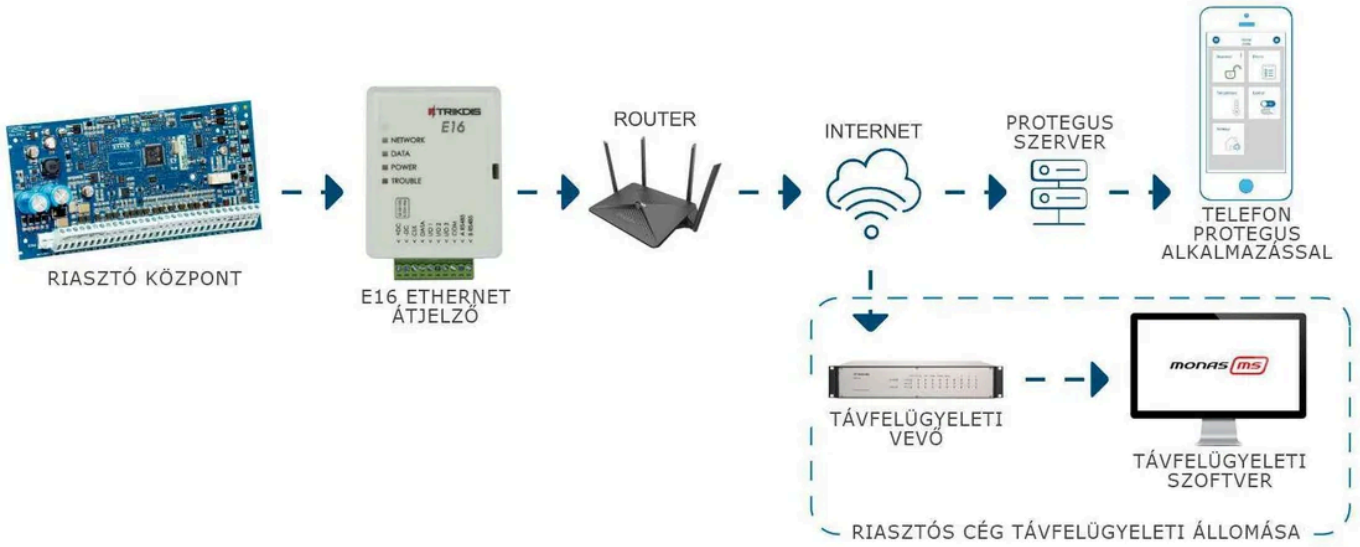


Abbildung 1. Die Stellung des E16 im System: Alarmzentrale (Bedienteilbus oder serielle Schnittstelle) → Ethernet-Kommunikator E16 → Router → Internet → Protegus Cloud und Empfänger der Leitstelle → Telefon des Benutzers mit der App Protegus 2 bzw. die Leitstellensoftware des Sicherheitsunternehmens.

1.2 Kompatible Alarmzentralen

Der E16 kann an die folgenden Zentralen angeschlossen werden. Bei den **direkt steuerbaren** Typen erfolgt das Scharf- und Unscharfschalten aus der App mit dem Bedienteilcode; bei den übrigen über eine Schlüsselschalterzone (Abschnitt 3.4). Für die direkte Steuerung von Paradox-Zentralen muss die Firmware der Zentrale mindestens **V.4** sein; bei den neueren Paradox-Typen (SP+, MG5050+, EVOHD+) ist die serielle Schnittstelle ab Werk gesperrt und muss vor der Verwendung freigeschaltet werden.

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

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

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

Soros port feloldás útmutató

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

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

Darüber hinaus ist er auch mit den Zentralen **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 und MATRIX 816** sowie **Paradox DIGIPLEX NE96 und EVO96** verwendbar.

Die Liste ändert sich von Zeit zu Zeit; den aktuellen Stand finden Sie in der Kompatibilitätssuche. Mit den Zentralen **DSC PowerSeries NEO** funktioniert der E16 nicht: Der Hersteller lässt am NEO-Bus kein externes Gerät zu, siehe DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen.

1.3 Hauptmerkmale

Verbindung zur Alarmzentrale

- Mit höchstens 4 Adern (+DC, −DC, CLK, DATA) an den Bedienteilbus (DSC, Caddx, Crow, Pyronix, Honeywell) oder die serielle Schnittstelle (Paradox, Texecom, InnerRange) der Zentrale anschließbar; für die serielle Schnittstelle gibt es ein Originalkabel (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Er überträgt jedes Ereignis der Zentrale mit der vollständigen Ereignisinformation (Code, Bereich, Zone oder Benutzer); eine Unterbrechung der Verbindung meldet er (LED TROUBLE, Ereignis COMMUNICATION).
- Die direkt steuerbaren Zentralen lassen sich aus der App mit dem Bedienteilcode scharf und unscharf schalten; Protegus 2 zeigt auch den Zustand der Zonen.

Netzwerkverbindung

- Ethernet-Anschluss (IEEE 802.3, 10Base-T, RJ45) an das lokale Netzwerk; die Adresse bezieht er ab Werk per DHCP, eine feste IP-Adresse ist ebenfalls einstellbar.
- Er baut nur ausgehende Verbindungen zum Empfänger und zur Protegus Cloud auf: Es muss kein Port geöffnet werden, eine öffentliche IP-Adresse und eine SIM-Karte sind nicht nötig.

Kommunikation mit der Leitstelle

- IP-Verbindung mit Trikdis-Empfängern (Software-Empfänger IPcom, RL14, RM14) und universellen Empfängern (SIA DC-09, TL150).
- Primärer, Ersatz- und Parallelkanal, jeweils mit eigenem Ersatzempfänger; mit dem Parallelkanal gehen die Ereignisse gleichzeitig an zwei Empfänger.
- Verschlüsselte Nachrichten (AES-128); Ereignisspeicher 60 Nachrichten.

Benutzerfunktionen

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

Installation und Einrichtung

- Die Einstellungen lassen sich in einer Datei speichern und in einen anderen Kommunikator laden.
- Zwei Zugriffsebenen: Administrator und Errichter.
- Fernkonfiguration und Fern-Update mit der Software TrikdisConfig.

1.4 Teile des Kommunikators

Der E16 trägt die Leiterplatte in einem weißen Kunststoffgehäuse; die Frontabdeckung ist abnehmbar, die Klemmleiste steckbar. Der Ethernet-Anschluss sitzt auf der Leiterplatte, das Kabel wird durch die Öffnung des Gehäuses eingeführt.

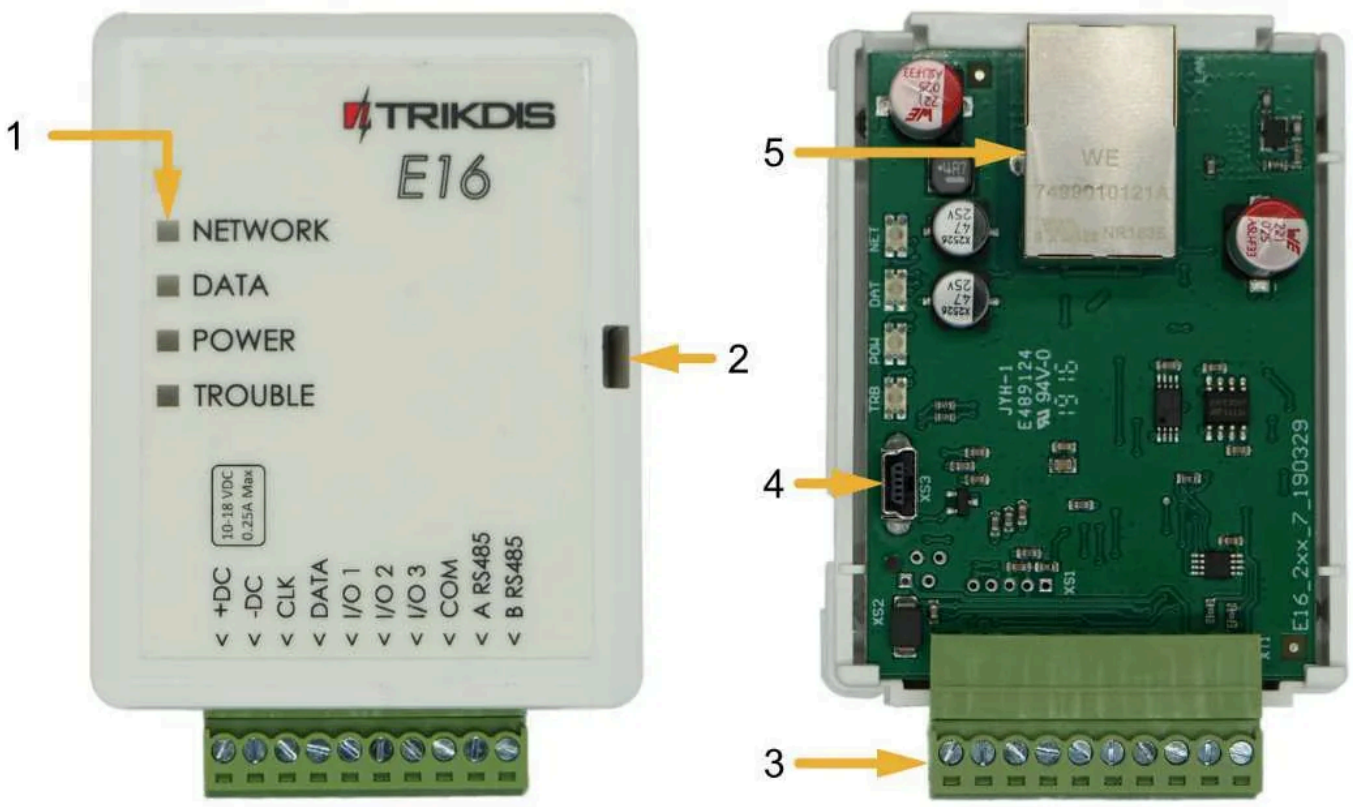


Abbildung 2. Die Teile des E16 von vorne und bei geöffnetem Gehäuse.

- 1 LED-Anzeigen (NETWORK, DATA, POWER, TROUBLE)
- 2 Öffnung zum Abnehmen der Frontabdeckung
- 3 Abnehmbare Klemmleiste
- 4 USB-Mini-B-Buchse zur 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 Klemmen

Klemme	Funktion
+DC	Versorgung, +10–18 V DC
–DC	Versorgung, negativ
CLK	Takt- / serielle Leitung des Busses der Zentrale

Klemme	Funktion
DATA	Datenleitung des Busses der Zentrale
I/O 1	1. Aus-/Eingang (Werkseinstellung: Eingang, NO)
I/O 2	2. Aus-/Eingang (Werkseinstellung: Eingang, NO)
I/O 3	3. Aus-/Eingang (Werkseinstellung: Ausgang)
COM	Gemeinsamer (negativer) Punkt für die Ein- und Ausgänge
A RS485	Ader A des RS485-Busses
B RS485	Ader B des RS485-Busses

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

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 die Netzwerkverbindung, DATA den Datenverkehr, TROUBLE den Fehler.

NETWORK – Netzwerkverbindung

Anzeige	Bedeutung
leuchtet nicht	Keine Verbindung zum Netzwerk (Kabel, Router oder IP-Adresse fehlt – welches davon, sagt die LED TROUBLE)
leuchtet grün	Mit dem Netzwerk verbunden

DATA – Datenverkehr

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

Schnellprüfung

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

POWER – Versorgungsspannung

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

TROUBLE – Fehler

Anzeige	Bedeutung
leuchtet nicht	Kein Fehler
1 rotes Blinken	Keine physische Verbindung zum Netzwerk (PHY link): Das Kabel ist nicht eingesteckt, oder der Port des Routers / Switches ist nicht aktiv
2 rote Blinksignale	DHCP-Fehler: Das Gerät hat keine IP-Adresse erhalten
3 rote Blinksignale	DNS-Fehler: Der Domainname des Empfängers oder der Protegus Cloud lässt sich nicht auflösen
6 rote Blinksignale	Keine Verbindung zum Empfänger der Leitstelle und/oder zum Protegus-Server (die Ursache kann auch die Internetverbindung oder die Firewall sein)
7 rote Blinksignale	Die Verbindung zur Alarmzentrale ist unterbrochen (Bus- oder serielle Verbindung)
blinkt rot (während der Programmierung)	Speicherfehler
leuchtet rot (während der Programmierung)	Beschädigte Firmware

1.7 Technische Daten

Parameter	Wert
Verbindung zur Alarmzentrale	Bedienteilbus oder serielle Schnittstelle, je nach Typ der Zentrale (4 Adern: +DC, −DC, CLK, DATA)
Netzwerkanschluss	Ethernet, IEEE 802.3, 10Base-T, RJ45-Buchse
Netzwerkeinstellung	DHCP (ab Werk) oder feste IP-Adresse, Subnetzmaske, Gateway, DNS
Ein-/Ausgänge	3 I/O mit Doppelfunktion: als Eingang NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (Abschlusswiderstand 2,2 kΩ); als Ausgang Open Collector (OC), max. 0,15 A / 30 V DC
Erweiterung	Am RS485-Bus höchstens 4 Erweiterungsmodule iO-8 (je Modul +8 I/O)
Versorgungsspannung	10–18 V DC
Stromaufnahme	100 mA nominal (im Ruhezustand); höchstens 250 mA beim Senden
Übertragungsprotokolle	TRK, DC-09_2007, DC-09_2012, TL150
Nachrichtenverschlüsselung	AES-128
Ereignisspeicher	60 Nachrichten
Programmierung	TrikdisConfig (Windows) über USB-Mini-B-Kabel oder per Fernzugriff

Parameter	Wert
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 E16 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 · Kabel mit mindestens 4 Adern für den Bus der Zentrale – für die serielle Schnittstelle von Paradox das Kabel **CRP2** oder **CRP2B**, für die serielle Schnittstelle von Texecom das Kabel **CRP4** · flacher Schraubendreher 2,5 mm · Ethernet-Kabel (CAT-5 oder besser, höchstens 100 m) bis zum Router oder Switch · die Errichteranleitung der Alarmzentrale. Kabel und Zubehör sind separat beim Händler zu beschaffen.

1. Laden Sie die Software TrikdisConfig herunter und installieren Sie sie.

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 E16. Stecken Sie einen flachen Schraubendreher in die Öffnung an der Oberkante des Deckels und hebeln Sie die Frontabdeckung nach unten vorsichtig ab. Die folgende Abbildung zeigt das Öffnen und die Lage der USB-Buchse.

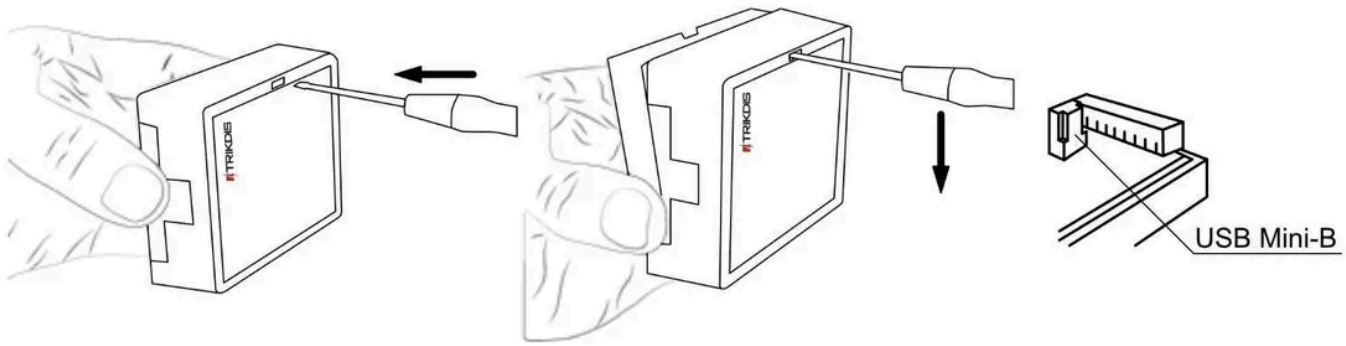


Abbildung 3. Abhebeln der Frontabdeckung mit einem flachen Schraubendreher (links, Mitte) und Lage der USB-Mini-B-Buchse auf der Leiterplatte (rechts).

3. Verbinden Sie den E16 mit dem Computer über ein USB-Mini-B-Kabel. USB liefert genügend Strom für die Programmierung, eine separate Versorgung ist nicht nötig.

Warnung

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

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

2.2 Typ der Zentrale und direkte Steuerung

Welche Betriebsart Sie auch verwenden, geben Sie zuerst auf der Seite **System settings** an, an welche Zentrale der Kommunikator kommt.

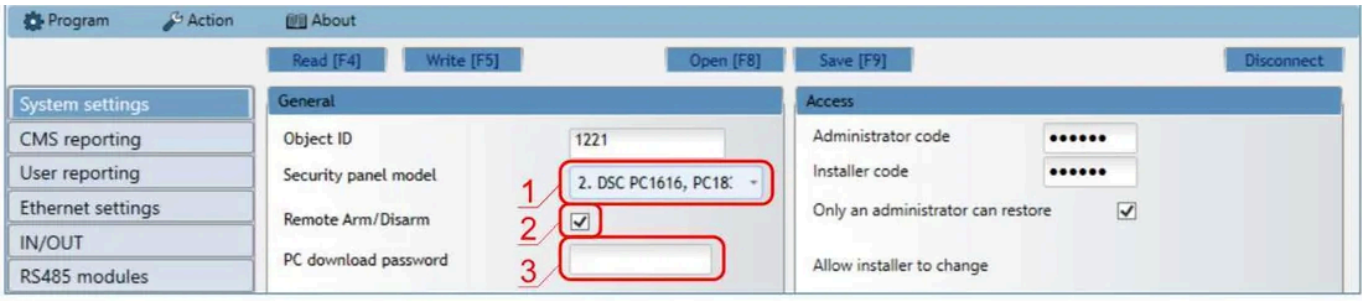


Abbildung 4. TrikdisConfig – Seite System settings, Gruppe General.

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

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

2.3 Verbindung zur App Protegus 2

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



Abbildung 5. TrikdisConfig – User reporting, Registerkarte PROTEGUS Cloud.

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

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).

Der E16 baut nur **ausgehende** Verbindungen zur Protegus Cloud und zum Empfänger auf, deshalb muss am Router kein Port geöffnet oder weitergeleitet werden. In einem durch eine Firewall gefilterten Firmennetz stimmen Sie den ausgehenden Datenverkehr mit dem Systemadministrator ab (Abschnitt 3.2).

Wenn das Gerät nur mit Protegus 2 arbeitet, 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. Wenn es auch an eine Leitstelle meldet, fahren Sie mit Abschnitt 2.4 fort.

2.4 Verbindung zur Leitstelle

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

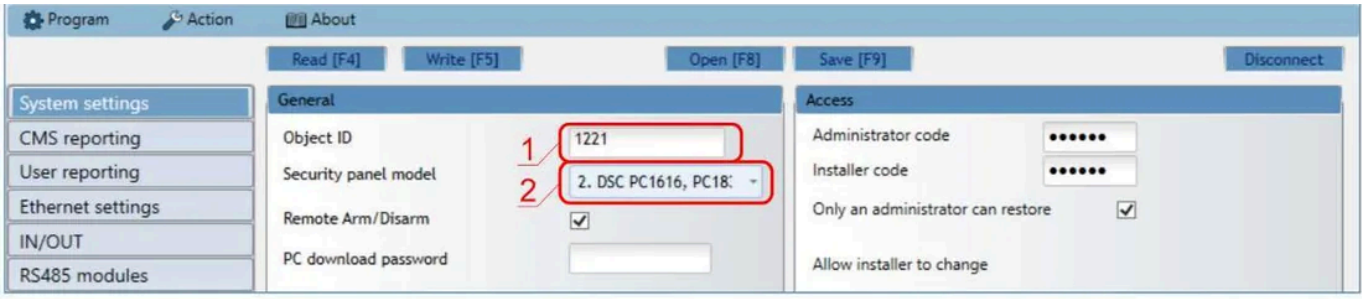


Abbildung 6. TrikdisConfig – Seite System settings, Gruppe General.

- 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** – der Typ der angeschlossenen Alarmzentrale (falls Sie ihn in Abschnitt 2.2 noch nicht eingestellt haben).

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

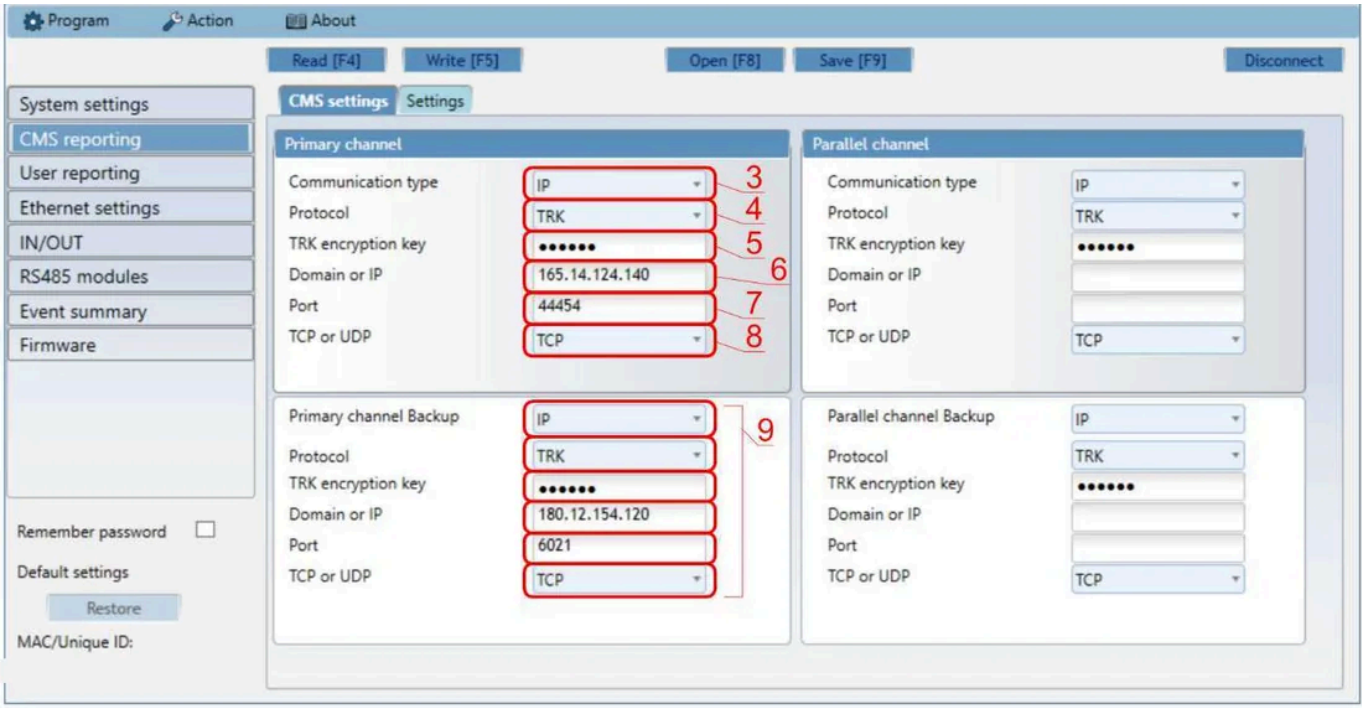


Abbildung 7. TrikdisConfig – CMS reporting, Registerkarte CMS settings.

- 3 **Communication type** – **IP** (beim E16 die einzige Möglichkeit).
- 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** – Übertragungsprotokoll; richtet sich nach der Einstellung des Empfängers.
- 9 **Primary channel Backup** – Ersatzkanal für den Ausfall des primären Kanals; füllen Sie ihn genauso aus, die Angabe wird empfohlen.

Empfohlen wird auch die Einrichtung des **Parallel channel** (Parallelkanal) und des zugehörigen Ersatzkanals, wenn zwei Empfänger die Ereignisse erhalten müssen.

Beim Protokoll **DC-09** geben Sie auf der Registerkarte **Settings** auch die DC-09-Objekt-, Linien- und Empfängernummer ein. Wenn Sie den Empfänger mit Domainnamen angeben, muss auf der Seite **Ethernet settings** eine funktionierende DNS-Adresse stehen (ab Werk der öffentliche Nameserver von Google).

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 die Frontabdeckung 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 3.8).
6. Setzen Sie die Frontabdeckung wieder auf.

3.2 Montageort und Netzwerk

- Montieren Sie den Kommunikator an einem **trockenen Ort im Innenbereich**, möglichst in der Nähe des Gehäuses der Alarmzentrale, damit die Busleitung kurz bleibt. Ein Metallgehäuse stört nicht: Der E16 hat keine Antenne.
- Das Ethernet-Kabel (CAT-5 oder besser) bis zum Router oder Switch darf **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 E16 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 (G16).

3.3 Anschluss an die Alarmzentrale

Der E16 wird mit **höchstens vier Adern** an die Zentrale angeschlossen (am Bus von Caddx und Pyronix wird CLK nicht verwendet): An die Klemmen **+DC** und **–DC** kommt die 12-V-Hilfsversorgung (AUX) der Zentrale, an die Klemmen **CLK** und **DATA** die beiden Datenleitungen des Bedienteilbusses oder der seriellen Schnittstelle der Zentrale. Welche Klemme der Zentrale welche ist, ist je nach Hersteller verschieden – schließen Sie nach den folgenden Plänen an. Für Zentralen mit serieller Schnittstelle (Paradox, Texecom) gibt es ein Originalkabel, dessen eines Ende in den Steckverbinder der Zentrale passt und dessen anderes Ende an die Klemmleiste des E16 angeschlossen wird.

Der E16 kann beim Senden bis zu 250 mA aufnehmen. Prüfen Sie, ob der AUX-Ausgang der Zentrale das zusammen mit den übrigen angeschlossenen Geräten verkraftet. Da die Versorgung von der Zentrale kommt, versorgt der Akku der Zentrale bei Stromausfall auch den Kommunikator. Bei den meisten Zentralen schaden vertauschte Adern eines am Bus angeschlossenen Geräts nicht, aber das Vertauschen von **+DC und −DC** kann den Kommunikator zerstören – prüfen Sie vor dem Anschließen die Polarität.

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

3.3.1 DSC PowerSeries

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

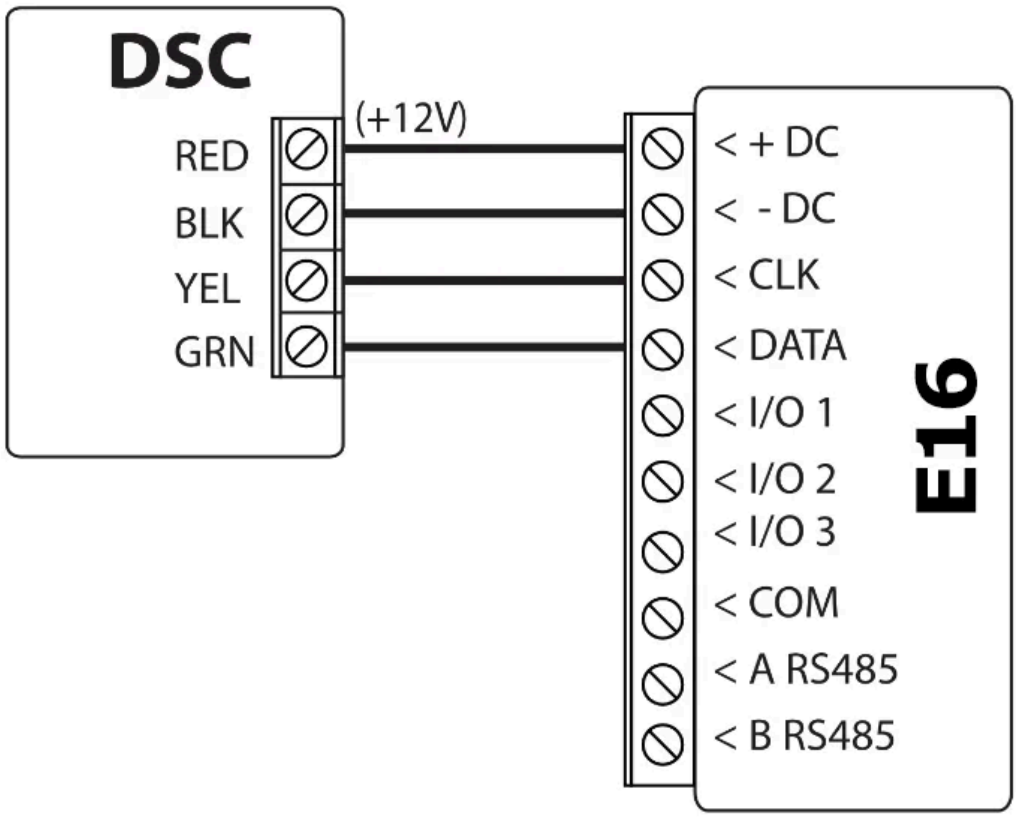


Abbildung 8. Anschluss an den Keybus einer DSC-PowerSeries-Zentrale (Bedienteilbus, „Keypad bus"): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

An die **serielle Schnittstelle** (SERIAL) der Paradox-Zentralen wird der Kommunikator mit dem Originalkabel **CRP2** oder **CRP2B** angeschlossen; das zentralenseitige Ende des Kabels passt in den seriellen Steckverbinder, das andere Ende schließen Sie an die Klemmleiste des E16 an. Die 4 Pins des Steckverbinders: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Die Aderfarben der beiden Kabel unterscheiden sich – der Plan zeigt die Farbbelegung beider Kabel. Die Bezeichnung des seriellen Steckverbinders bei Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

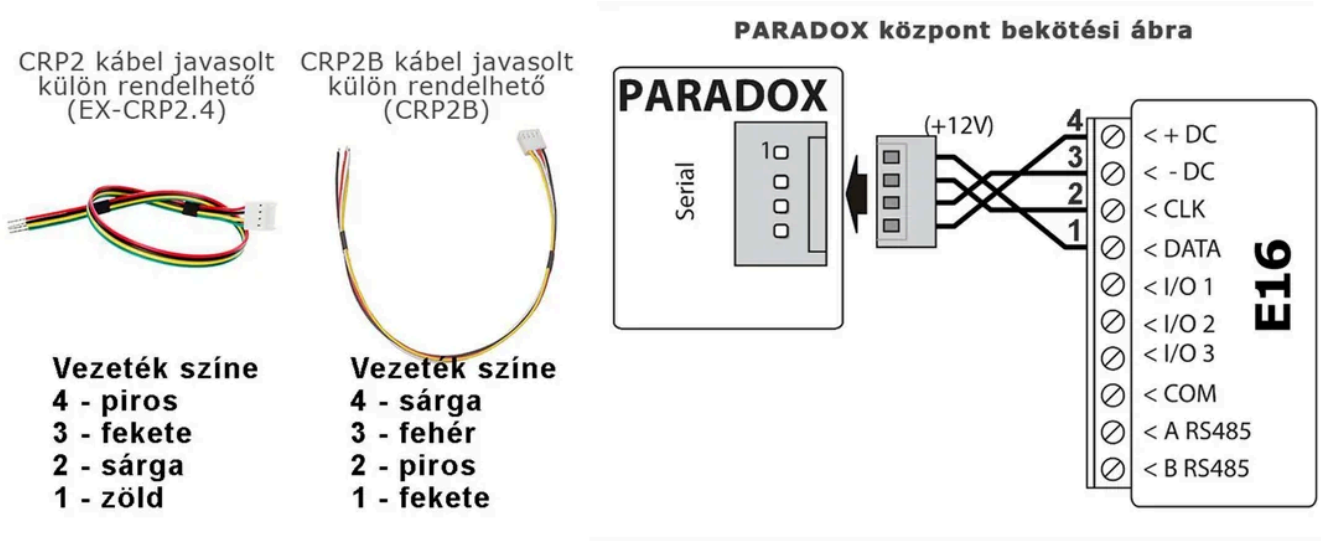


Abbildung 9. Anschluss an die serielle Schnittstelle einer Paradox-Zentrale mit dem Kabel CRP2 (EX-CRP2.4) bzw. CRP2B. CRP2: 4 rot → +DC, 3 schwarz → −DC, 2 gelb → CLK, 1 grün → DATA. CRP2B: 4 gelb → +DC, 3 weiß → −DC, 2 rot → CLK, 1 schwarz → DATA.

Bei den neueren Paradox-Zentralen kann die serielle Schnittstelle ab Werk gesperrt sein – das Vorgehen zur Freischaltung steht in Abschnitt 4.2 und im Artikel Freischaltung der gesperrten seriellen Schnittstelle an Paradox-Alarmzentralen.

3.3.3 UTC Interlogix (Caddx) NetworX

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

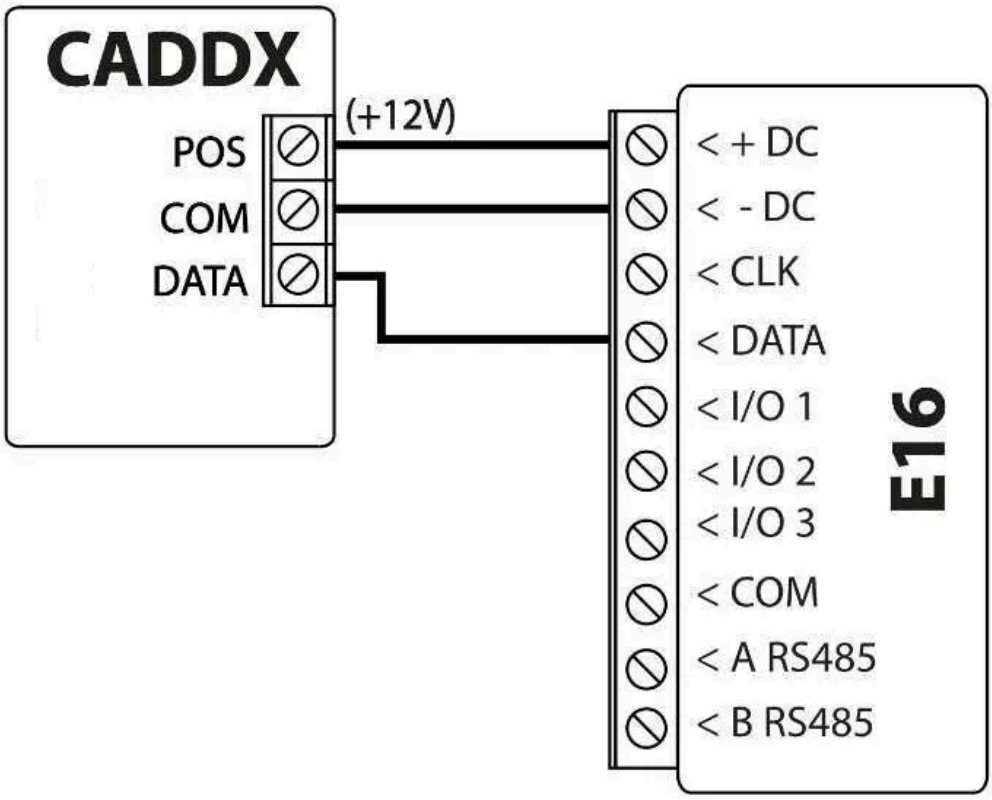


Abbildung 10. Anschluss an den Bedienteilbus („Keypad bus“) einer Caddx-NetworX-Zentrale: POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK bleibt frei.

3.3.4 Texecom Premier / Premier Elite

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

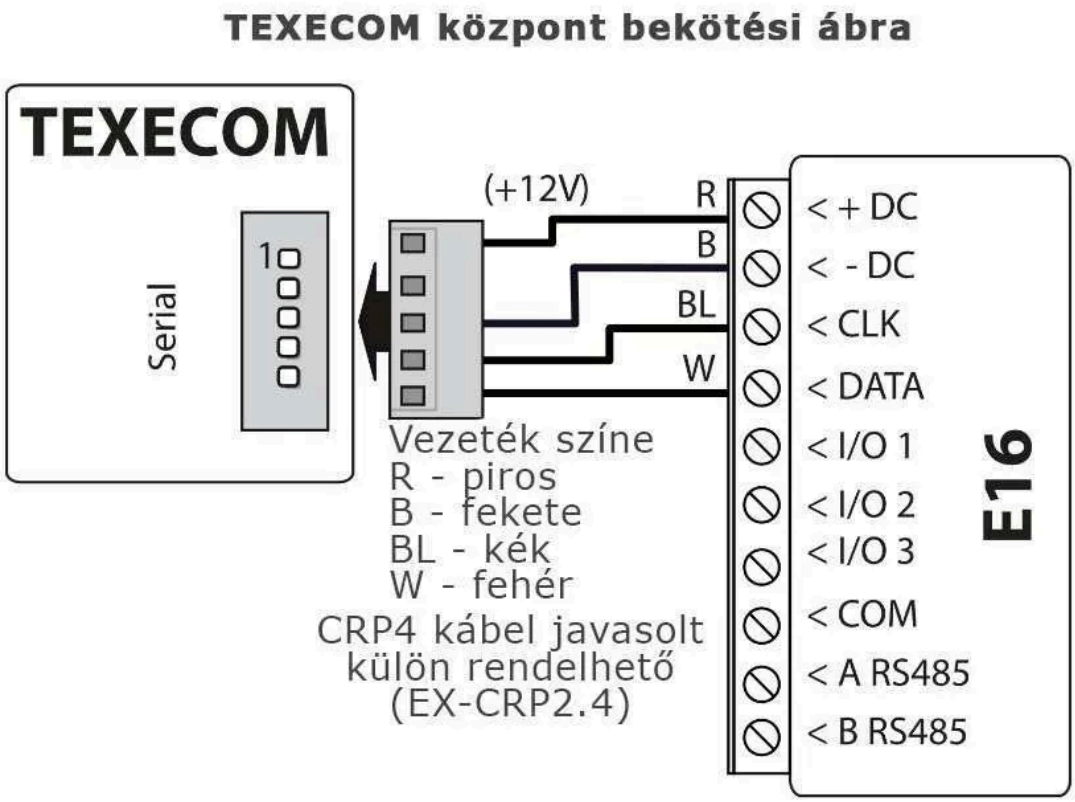


Abbildung 11. Anschluss an die serielle Schnittstelle einer Texecom-Zentrale mit dem Kabel CRP4: rot → +DC, schwarz → −DC, blau → CLK, weiß → DATA.

3.3.5 Crow Runner

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

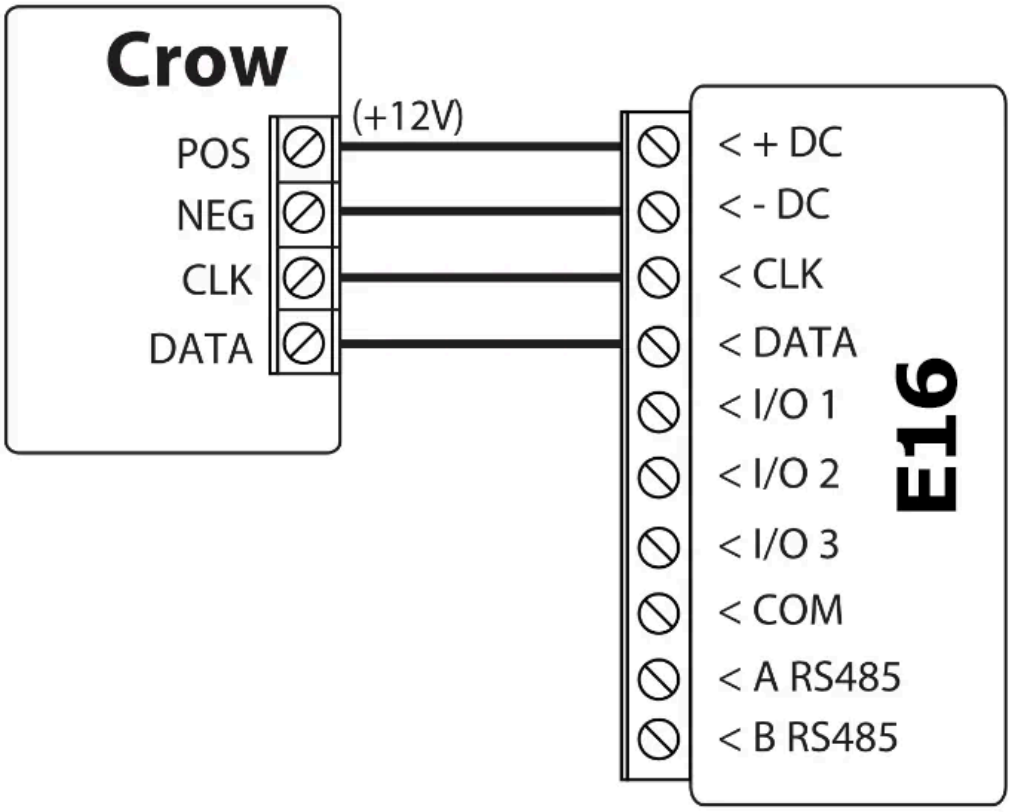


Abbildung 12. Anschluss an den Bedienteilbus („Keypad bus") einer Zentrale Crow Runner 4/8 und Runner 8/16: POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Der Bedienteilbus der Pyronix-Zentralen: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. Die Klemme **CLK** wird nicht verwendet. Nach dem Anschluss und der Einrichtung des Kommunikators machen Sie die Zentrale stromlos und starten sie neu, damit sie den Kommunikator akzeptiert (Abschnitt 4.5).

3.3.7 Honeywell Ademco Vista

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

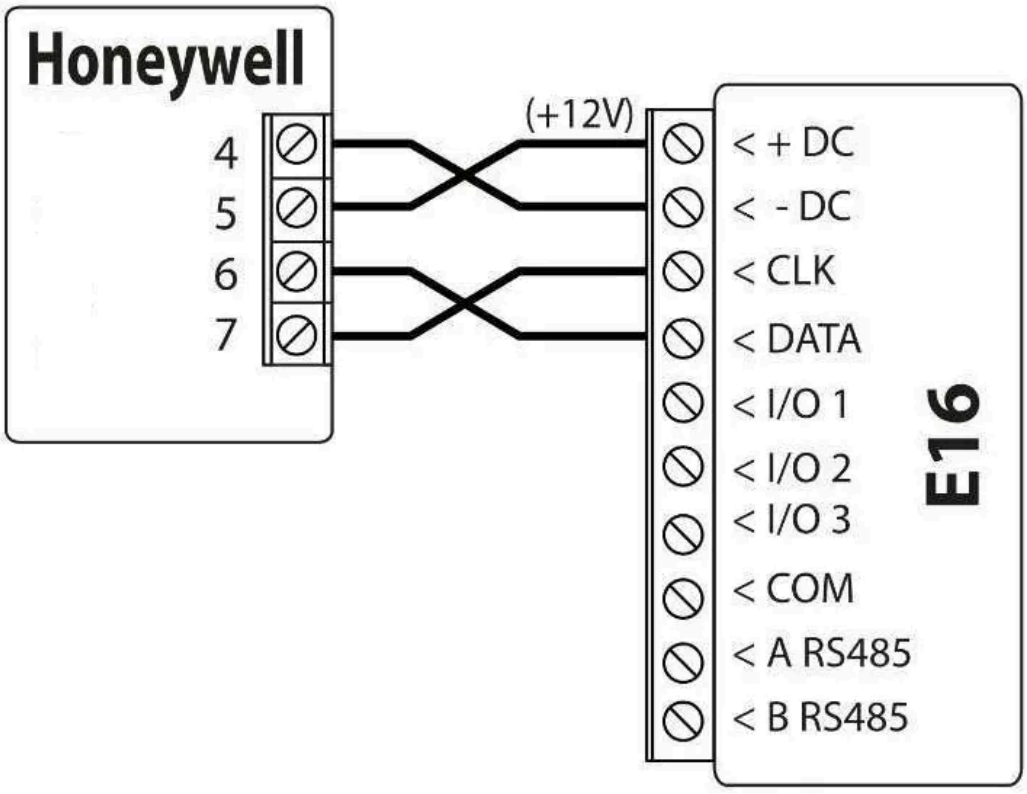


Abbildung 13. Anschluss an den Bedienteilbus („Keypad bus") einer Zentrale Honeywell Vista-20 / Vista-48: 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception und Integriti

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

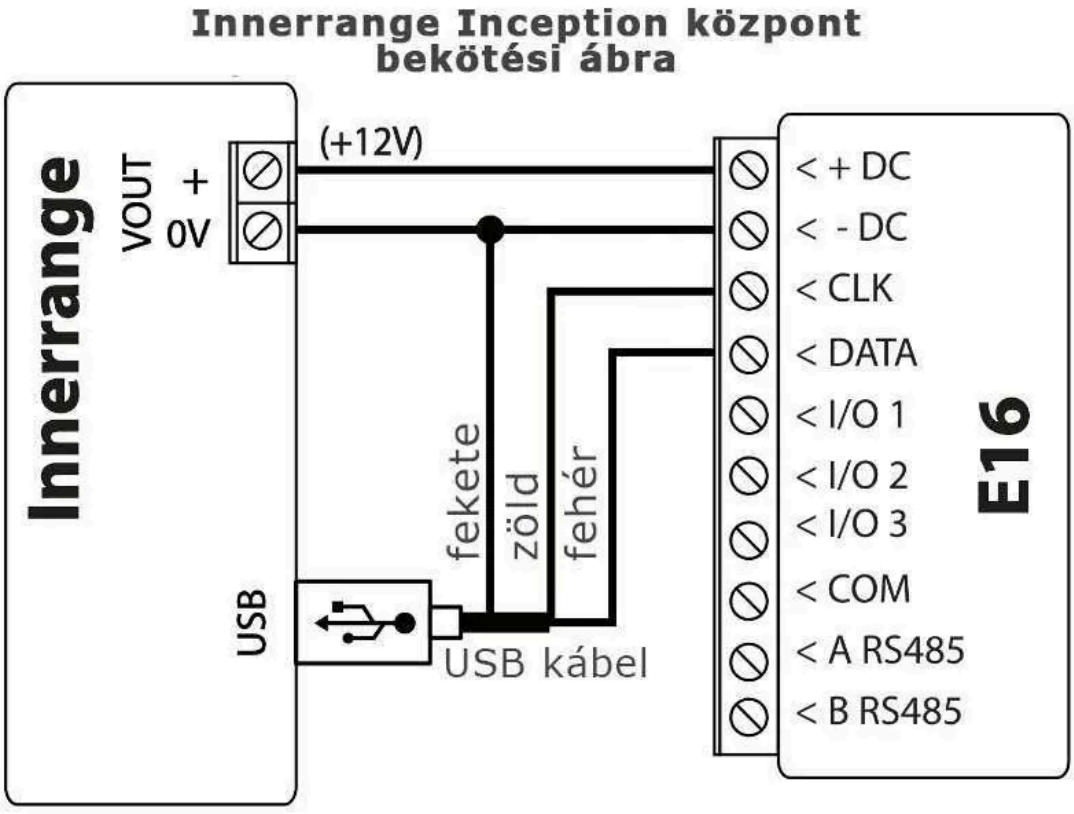


Abbildung 14. Anschluss an die Zentrale InnerRange Inception: Versorgung von den Klemmen VOUT + und 0V, Daten über den USB-Port mit dem Kabel 993030USB (schwarz → 0V, grün → CLK, weiß → DATA).

An Port 0 der Zentrale **Integriti** wird mit dem Kabel INTG-996795 angeschlossen: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA. Die serielle Schnittstelle der Zentrale muss auf das Trikdis-Protokoll eingestellt werden (Abschnitt 4.7).

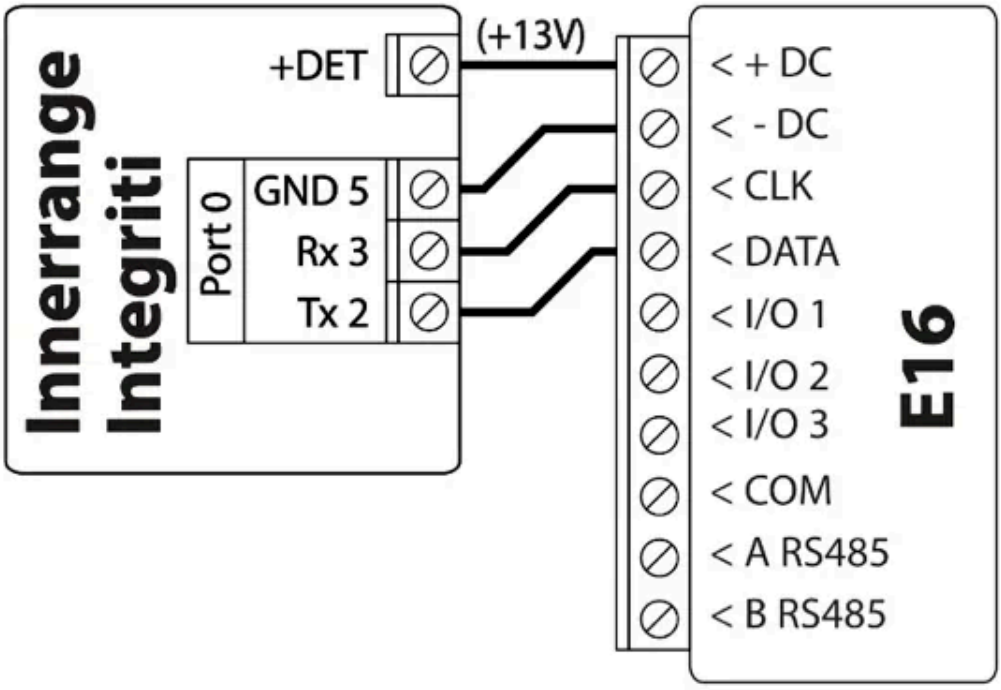


Abbildung 15. Anschluss an die Zentrale InnerRange Integriti mit dem Kabel Inner Range Artikelnummer INTG-996795: +DET (+13 V) → +DC, Port 0 GND (5) → −DC, Rx (3) → CLK, Tx (2) → DATA.

3.4 Anschluss einer Schlüsselschalterzone

Wenn die Zentrale nicht zu den direkt steuerbaren Typen gehört oder Sie die direkte Steuerung nicht verwenden möchten, lässt sich das Scharf- und Unscharfschalten aus der Ferne über eine **Schlüsselschalterzone** lösen: Sie stellen eine I/O-Klemme des Kommunikators als **Ausgang** ein (Seite IN/OUT, Abschnitt 6.6) und schließen 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 E16 drei I/O-Klemmen hat, lassen sich bis zu drei Bereiche mit je einem eigenen Ausgang bedienen.

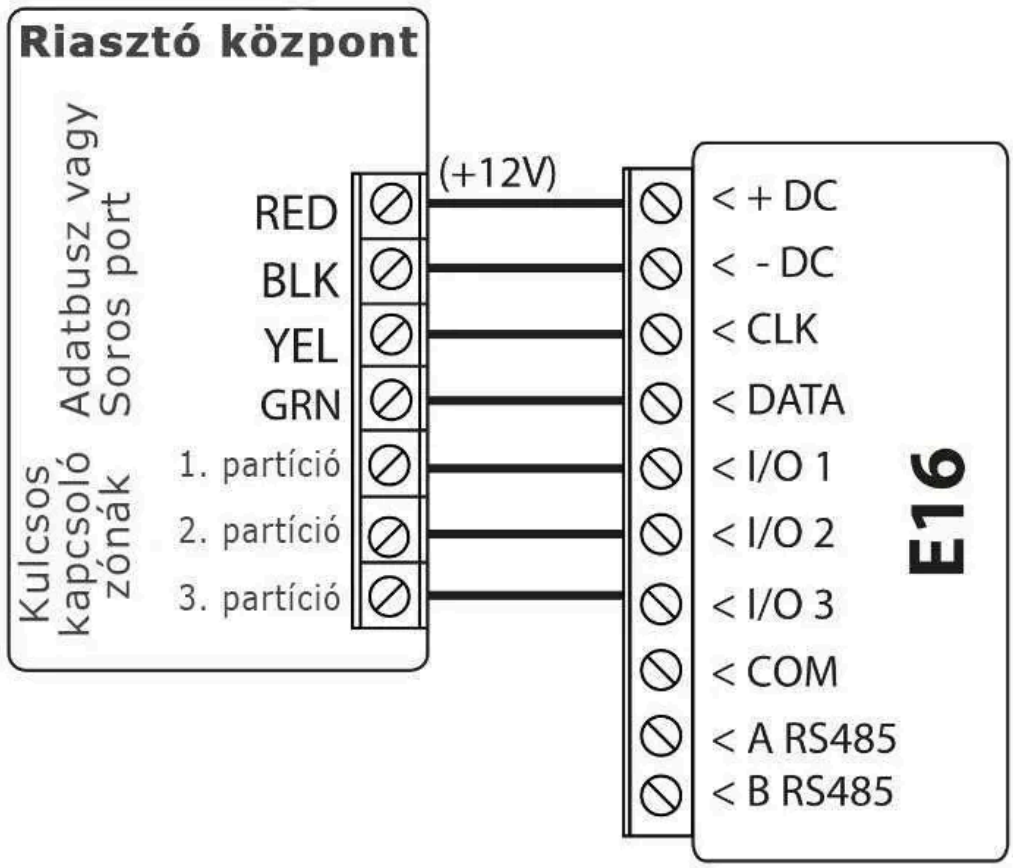


Abbildung 16. Scharf- und Unscharfschalten über eine Schlüsselschalterzone: Der Kommunikator liest die Ereignisse vom Bus der Zentrale, die Ausgänge I/O 1–3 schalten die Schlüsselschalterzone der Bereiche 1–3 der Zentrale.

- Auf der Seite **System settings** von TrikdisConfig muss **Remote Arm/Disarm leer** bleiben – beides kann nicht gleichzeitig verwendet werden.
- Die Schlüsselschalterzone kann impulsgesteuert oder zweistufig (bistabil) sein; in der App Protegus 2 muss derselbe Modus eingestellt werden (Abschnitt 5.3).

Über Details und Fallstricke des Scharfschaltens per Schlüsselschalter gibt es einen eigenen Artikel: Scharfschalten aus der Ferne per Schlüsselschalter aus der App Protegus 2.

3.5 Anschluss von Eingängen

Die I/O-Klemmen des Kommunikators lassen sich als Eingänge auch zur Aufnahme weiterer Melder verwenden (z. B. Sabotagekontakt, Paniktaster, Temperaturschalter), unabhängig von der Alarmzentrale. Der Eingang wird zwischen die gewählte I/O-Klemme und die Klemme COM angeschlossen.

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

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

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

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

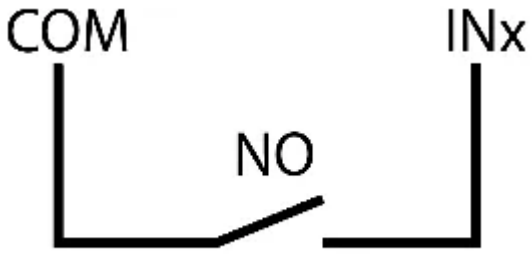


Abbildung 17. NO – im Grundzustand offener Kreis: geschlossen – Alarm, offen – Ruhezustand.

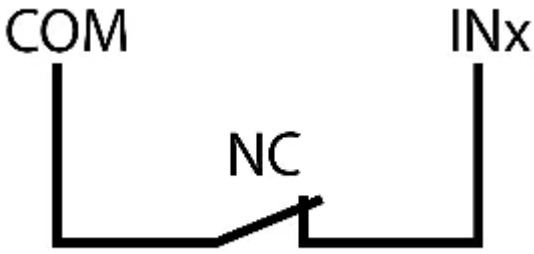


Abbildung 18. NC – im Grundzustand geschlossener Kreis: offen – Alarm, geschlossen – Ruhezustand.

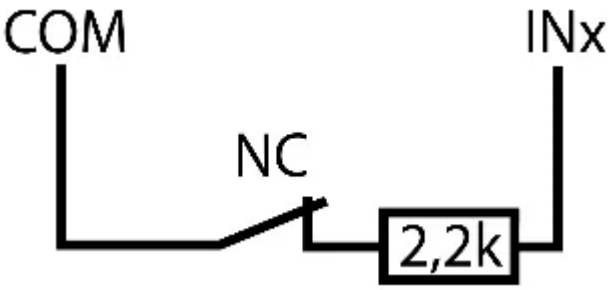


Abbildung 19. NC/EOL – im Grundzustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

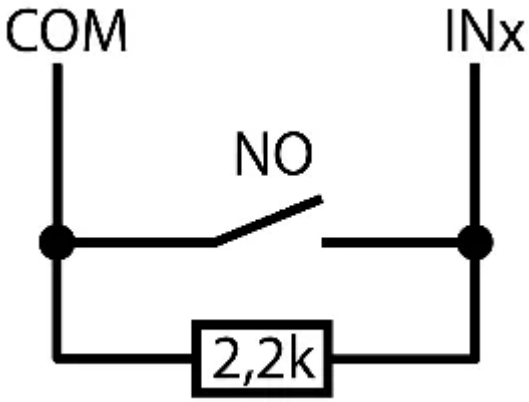


Abbildung 20. NO/EOL – im Grundzustand offener Kreis mit Abschlusswiderstand 2,2 kΩ: Kurzschluss oder Unterbrechung – Alarm, 2,2 kΩ – Ruhezustand.

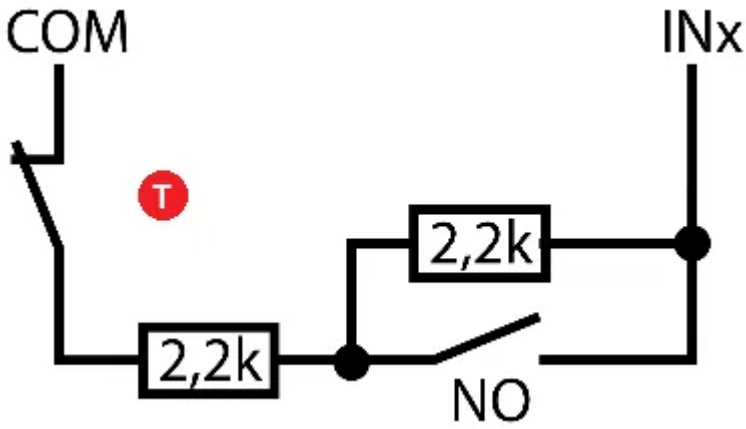


Abbildung 21. NO/DEOL – im Grundzustand offener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Alarm, 3,3–5,5 kΩ – Ruhezustand.

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

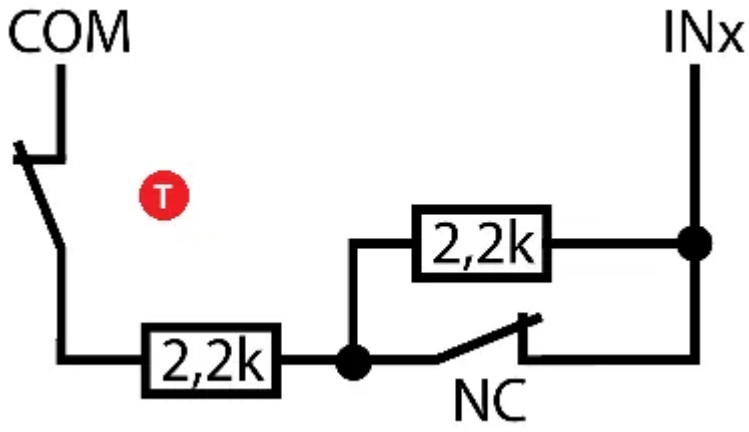


Abbildung 22. NC/DEOL – im Grundzustand geschlossener Kreis mit Abschlusswiderstand 2,2 kΩ und Sabotageerkennung: Kurzschluss oder Unterbrechung – Sabotage, 2,2 kΩ – Ruhezustand, 3,3–5,5 kΩ – Alarm.

- 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. Mit den Kontakten eines Relais können Sie verschiedene elektrische Geräte ein- und ausschalten. 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. Die verwendete I/O-Klemme muss auf der Seite **IN/OUT** von TrikdisConfig als Ausgang (**OUT**) eingestellt werden (Abschnitt 6.6).

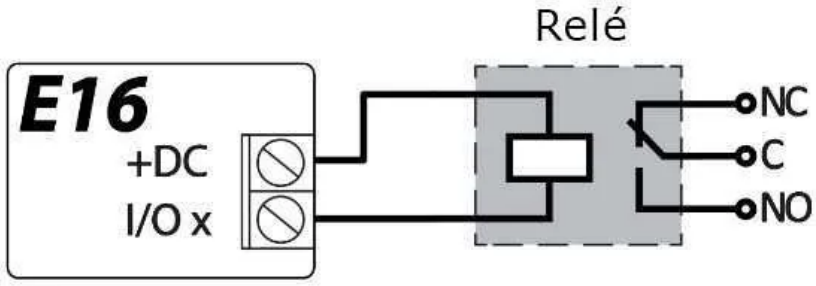


Abbildung 23. Anschluss eines Relais an den Ausgang des Kommunikators: Die Spule liegt zwischen den Klemmen +DC und I/O x, die Kontakte (NC, C, NO) schalten den Verbraucher.

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

3.7 Anschluss des Erweiterungsmoduls iO-8

Wenn mehr Ein- oder Ausgänge benötigt werden, kann an den RS485-Bus des E16 ein Erweiterungsmodul **iO-8** angeschlossen werden; jedes liefert 8 weitere I/O mit Doppelfunktion. Verbinden Sie die Klemmen A RS485 und B RS485 mit den Klemmen A und B des Moduls, die Versorgung des Moduls nehmen Sie vom 12-V-AUX-Ausgang der Zentrale. Das Modul muss auf der Seite **RS485 modules** von TrikdisConfig hinzugefügt werden (Abschnitt 6.7); die Ereignisse der Eingänge gehen an die Leitstelle und in Protegus 2, die Ausgänge lassen sich aus der App schalten.

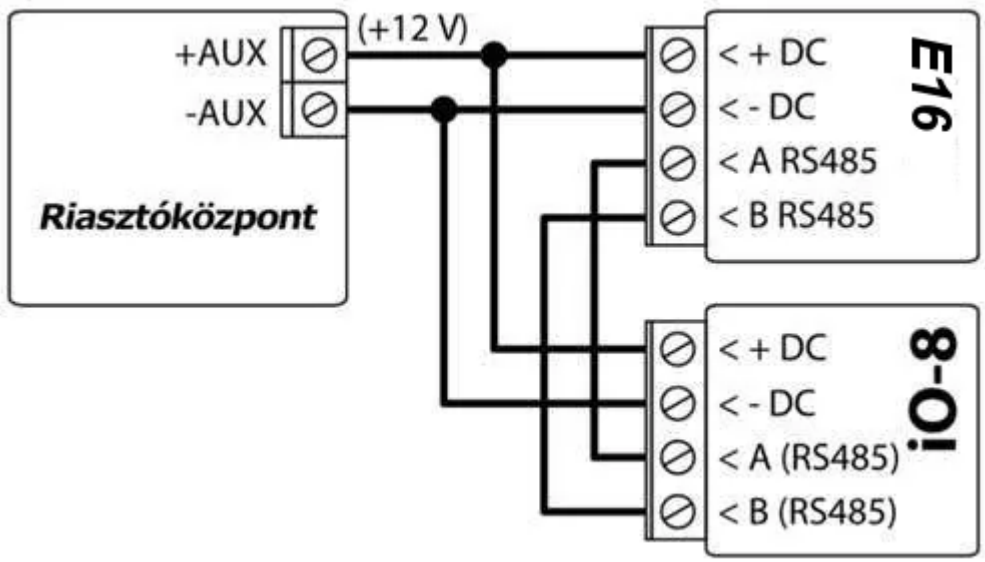


Abbildung 24. Anschluss des Erweiterungsmoduls iO-8 an den RS485-Bus des E16 (A RS485 → A, B RS485 → B); beide Geräte werden vom AUX-Ausgang der Alarmzentrale (+12 V) versorgt.

3.8 Anschluss des Ethernet-Kabels

Stecken Sie ein Ende des Ethernet-Kabels in die RJ45-Buchse auf der Leiterplatte des E16, das andere in einen freien Port des Routers oder Switches. Es wird ein herkömmliches, gerade beschaltetes Kabel (Patchkabel) benötigt; das Kabel wird durch die Öffnung des Gehäuses eingeführt. Das Zustandekommen der Netzwerkverbindung zeigt nach dem Einschalten das grüne Licht der LED **NETWORK**.

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 Anschluss 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 – mit dem Netzwerk verbunden;
- **TROUBLE** leuchtet nicht.

Jedes davon abweichende LED-Bild zeigt einen Fehler an; bestimmen Sie die Ursache anhand der LED-Tabelle in Abschnitt 1.6. Wenn TROUBLE blinkt, nennt die Anzahl der Blinksignale die Ursache (Abschnitt 1.6): 1 = keine physische Verbindung (Kabel, Port), 2 = keine IP-Adresse erhalten (DHCP), 3 = DNS-Fehler, 6 =

Empfänger oder Protegus Cloud nicht erreichbar. **7 Blinksignale** zeigen eine fehlende Verbindung zur Zentrale an: Prüfen Sie die Adern CLK und DATA, den ausgewählten Typ der Zentrale und – wo nötig – die Programmierung der Zentrale (Kapitel 4). Wenn keine LED leuchtet, prüfen Sie die Versorgung und die Verdrahtung.

4. Programmierung der Alarmzentrale

Dieses Kapitel beschreibt je Hersteller, was in der Alarmzentrale eingestellt werden muss, damit der E16 die Ereignisse liest und – wo möglich – die Zentrale aus der Ferne steuert. Bei den meisten Zentralen muss für das Lesen der Ereignisse nichts programmiert werden; für die **direkte Steuerung** setzen Sie auf der Seite **System settings** von TrikdisConfig das Häkchen bei **Remote Arm/Disarm**, und bei Paradox- bzw. Texecom-Zentralen geben Sie im Feld **Security panel PC download password** auch das PC- bzw. UDL-Passwort der Zentrale ein (Abschnitte 2.2 und 6.2).

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

4.1 DSC

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

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

4.2 Paradox

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

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

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

1. Öffnen Sie am Bedienteil die Installateur-Programmierung der Zentrale.
2. Öffnen Sie die Sektion des PC-Passworts: bei den Serien **MAGELLAN und SPECTRA** die Sektion **911**, bei der Serie **DIGIPLEX EVO** die Sektion **3012**.
3. Geben Sie ein **4-stelliges** Passwort ein. Das Passwort darf nicht 0000 sein und **nicht mit einer Null beginnen**.

4. Verlassen Sie die Programmierung und **starten Sie die Zentrale neu** – die Änderung des PC-Passworts wird erst nach einem Neustart wirksam. Tragen Sie anschließend dasselbe Passwort in TrikdisConfig ein.

Typische Fehler und ihre Lösung

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

4.3 Texecom

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

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

Am Bedienteil:

1. Geben Sie den 4-stelligen Installateurcode ein und drücken Sie die Taste **[Menu]**, um ins Programmiermenü zu gelangen.
2. Drücken Sie gleich danach die Taste **[9]**.
3. Drücken Sie **[7][6]**, dann die Taste **[2]**, und geben Sie den 4-stelligen UDL passcode ein.
4. Drücken Sie die Taste **[Yes]** und verlassen Sie die Programmierung mit der Taste **[Menu]**.

4.4 UTC Interlogix (Caddx)

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

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

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

Adresse (location)	Segment	Einstellung
102	3	12345678
105	3	12345678
108	3	12345678

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

4.5 Crow und Pyronix

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

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

4.6 Honeywell Ademco Vista

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

Einstieg in die Programmierung – auf zwei Arten:

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

Einstellungen:

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

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

4.7 InnerRange Inception und Integriti

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

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

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

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

Inception und Integriti übergeben die Ereignisse an den Kommunikator; für das Scharf- und Unscharfschalten ist eine Schlüsselschalterzone nötig (Abschnitte 1.2 und 3.4).

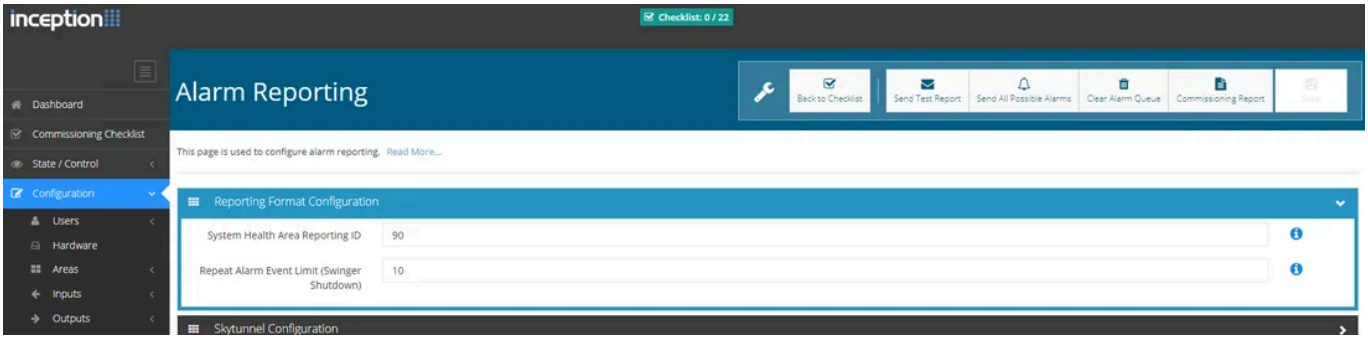


Abbildung 25. Weboberfläche der Inception – Configuration → General → Alarm Reporting.



Abbildung 26. Inception – 3rd Party Device Configuration.

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

5. Fernsteuerung mit der App Protegus 2

Mit der mobilen und Web-App Protegus 2 sieht der Benutzer den Zustand des Systems aus der Ferne, erhält Benachrichtigungen über Ereignisse, kann scharf und unscharf schalten und die Ausgänge des Kommunikators schalten. Beim E16 kann das Scharfschalten auf zwei Arten erfolgen: bei den **direkt steuerbaren** Zentralen mit dem eigenen **Bedienteilcode** des Benutzers, bei den über eine Schlüsselschalterzone angeschlossenen Zentralen mit einem **Ausgang** des Kommunikators.

5.1 Gerät hinzufügen

Prüfen Sie vor dem Hinzufügen des Geräts:

1. Der E16 ist mit dem Netzwerk verbunden und erreicht das Internet: Die LED **NETWORK** leuchtet grün, die LED **TROUBLE** blinkt nicht.
2. Auf der Seite **User reporting** → **PROTEGUS Cloud** von TrikdisConfig ist **Enable connection** angehakt, und der **Protegus Cloud access code** ist eingestellt (nach dem Anlegen des Systems nicht mehr änderbar).
3. Die LED **POWER** leuchtet grün.

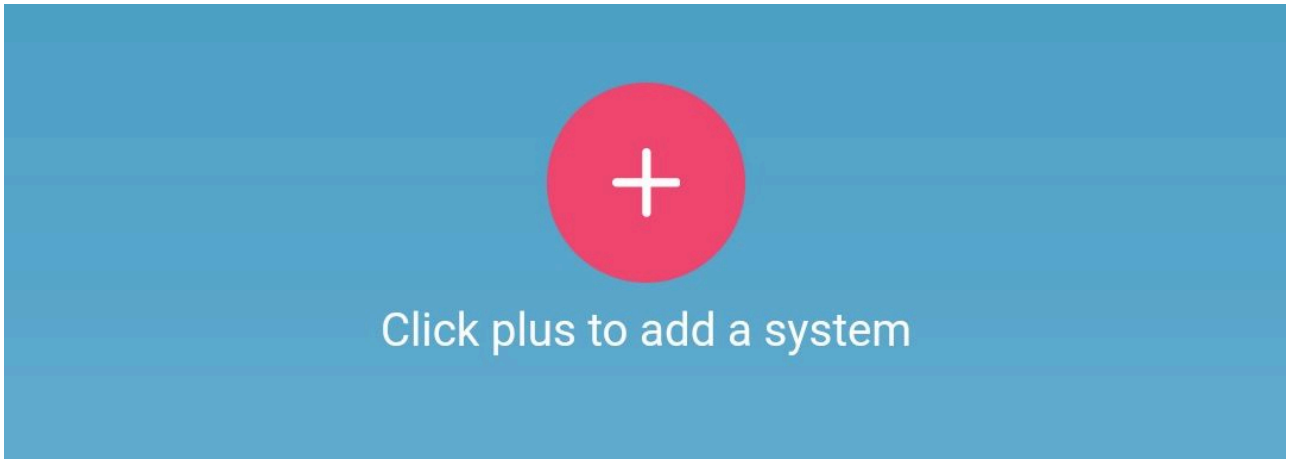
Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet,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



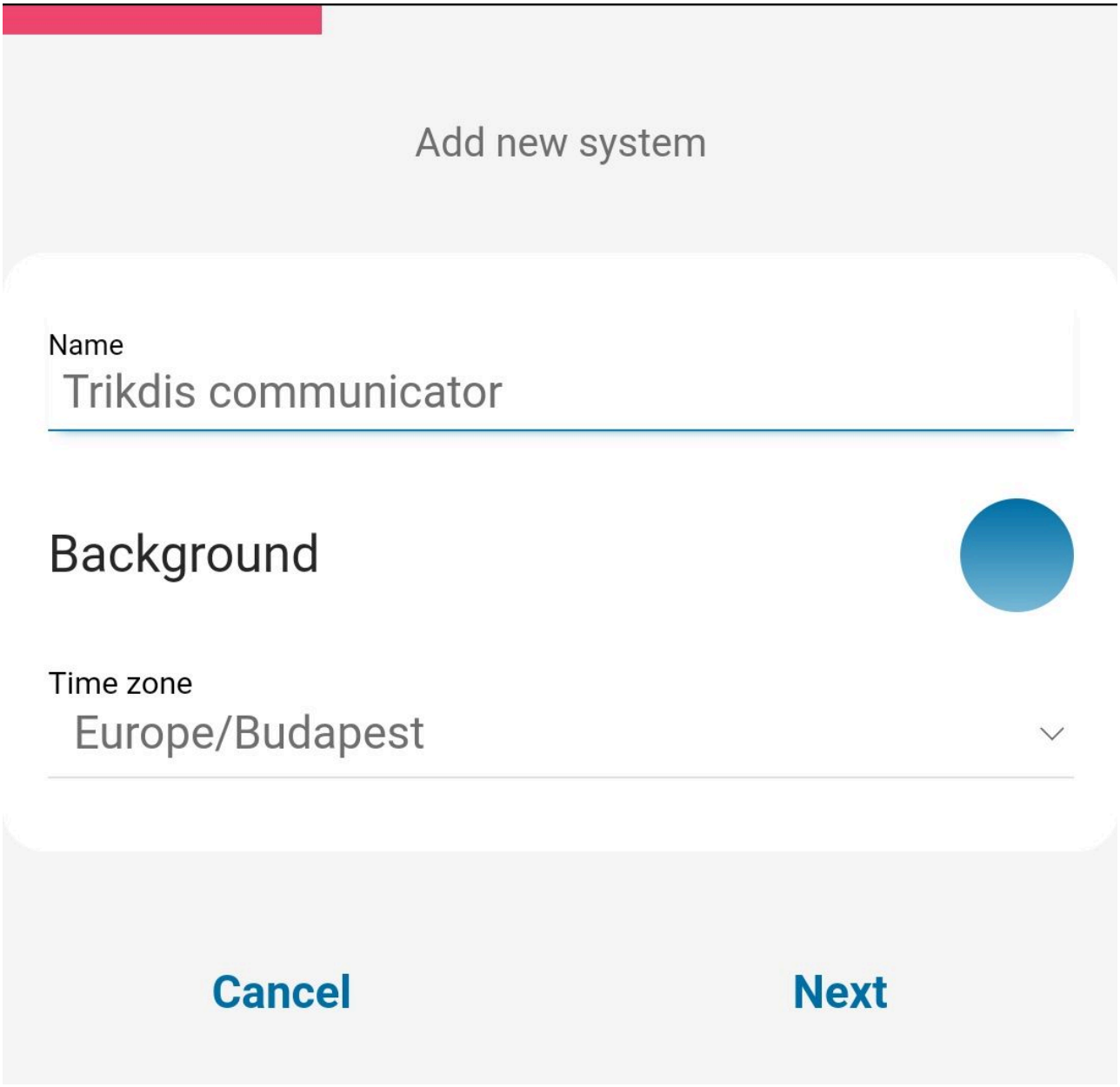
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



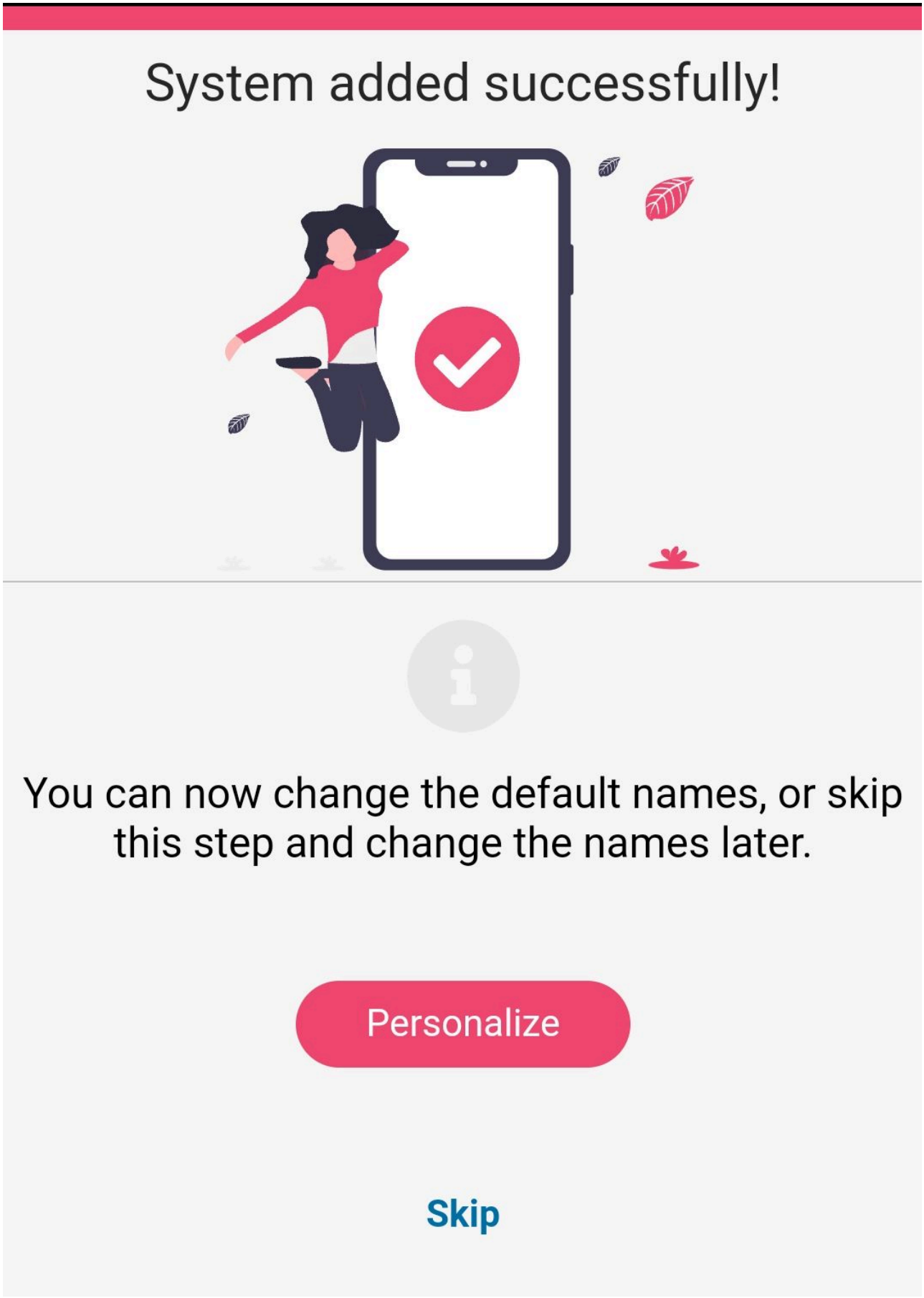
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



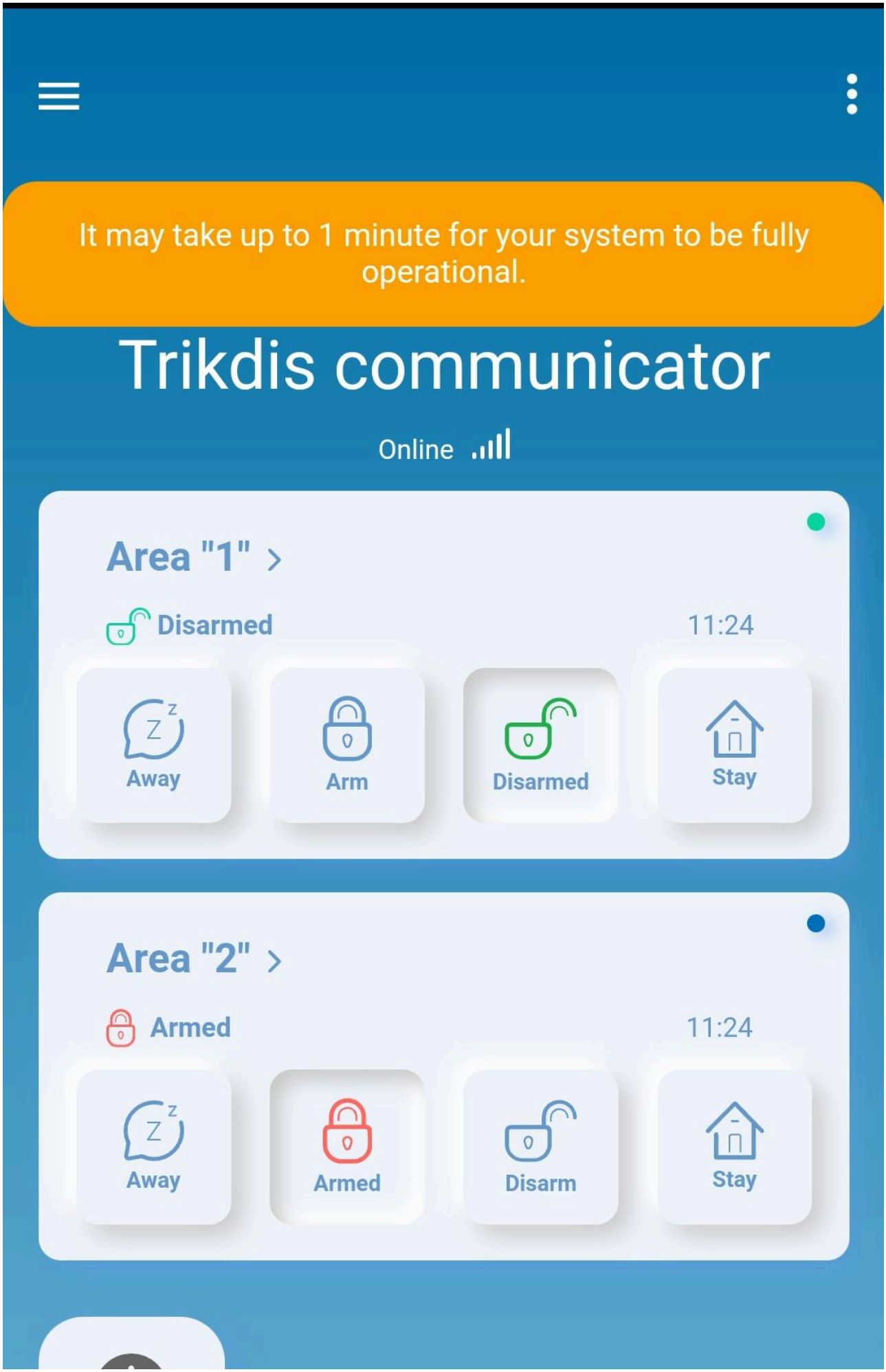
6. Add meg a rendszer nevét és válassz idozónát



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 E16 die **MAC-Adresse (Unique ID)**: Sie steht auf der Verpackung und auf der Rückseite des Geräts, und auch die Statusleiste von TrikdisConfig zeigt sie an (Abschnitt 6.1). In der App muss beim Anlegen des Systems diese als Kennung des Geräts eingegeben werden.

5.2 Direkte Steuerung mit dem Bedienteilcode

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

- In der Zentrale ist dafür je nach Hersteller eine Einstellung nötig (Paradox: PC-Passwort, Texecom: UDL-Passwort; bei Caddx-, Honeywell- und InnerRange-Zentralen die Freigabe des Busses bzw. der seriellen Schnittstelle schon für das Lesen der Ereignisse) – siehe Kapitel 4.
- Den Bedienteilcode prüft die Zentrale, und auch das Ereignisprotokoll der Zentrale verzeichnet den Benutzer, nicht den Kommunikator.
- Bei einer Paradox-Zentrale darf der Code des Benutzers **nicht der Mastercode** sein; starten Sie nach einer Codeänderung den Kommunikator neu (Abschnitt 4.2).
- Bei einer DSC-PowerSeries-Zentrale zeigt die App auch den Zustand der Zonen, und auch das Sperren von Zonen ist möglich – Details im Artikel über die direkte Steuerung von DSC (der Artikel behandelt den G16, gilt aber genauso für den E16).

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

5.3 Scharfschalten über eine Schlüsselschalterzone

Wenn die Zentrale nicht direkt steuerbar ist oder Sie sie nicht so verwenden möchten, schließen Sie einen Ausgang des Kommunikators an die Schlüsselschalterzone der Zentrale an (Abschnitt 3.4), in TrikdisConfig bleibt **Remote Arm/Disarm** leer, und in Protegus 2 ordnen Sie dem Bereich den Ausgang zu.

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

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

Die Einstellung können Sie beim Anlegen des Systems, beim Hinzufügen der Bereiche, oder nachträglich in den Systemeinstellungen beim Bearbeiten des Bereichs vornehmen. Beim Anlegen des Systems führt Sie der Assistent von Protegus 2 durch die Schritte: Klicken Sie auf **Continue** (Weiter), geben Sie den Namen des

Bereichs ein (**Area name**) und erlauben Sie die Steuerung des PGM-Ausgangs aus der Protegus-2-App – das geschieht mit den folgenden Schritten:

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

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

5.4 Scharf- und Unscharfschalten 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.

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

Der E16 hat keine SMS-Steuerung und keine SMS-Benachrichtigung: Das Scharf- und Unscharfschalten und das Schalten der Ausgänge erfolgen aus der App Protegus 2, die Benachrichtigung kommt als Push-Nachricht.

6. TrikdisConfig – die Einstellungen im Detail

Links im Fenster von TrikdisConfig 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 E16 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 27. Die Statusleiste von TrikdisConfig mit ausgelesenem E16: MAC-Adresse (Unique ID, im Bild leer gelassen), Zustand, Typ (E16_1100), Seriennummer, Versionen, Verbindungsart und Zugriffsebene.

Beim E16 ist die eindeutige Kennung des Geräts die **MAC-Adresse**: Diese verlangt Protegus 2 beim Anlegen des Systems und TrikdisConfig für den Fernzugriff (Unique ID). Dieselbe Adresse steht auch auf der Verpackung und auf der Rückseite des Geräts.

6.2 System settings

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

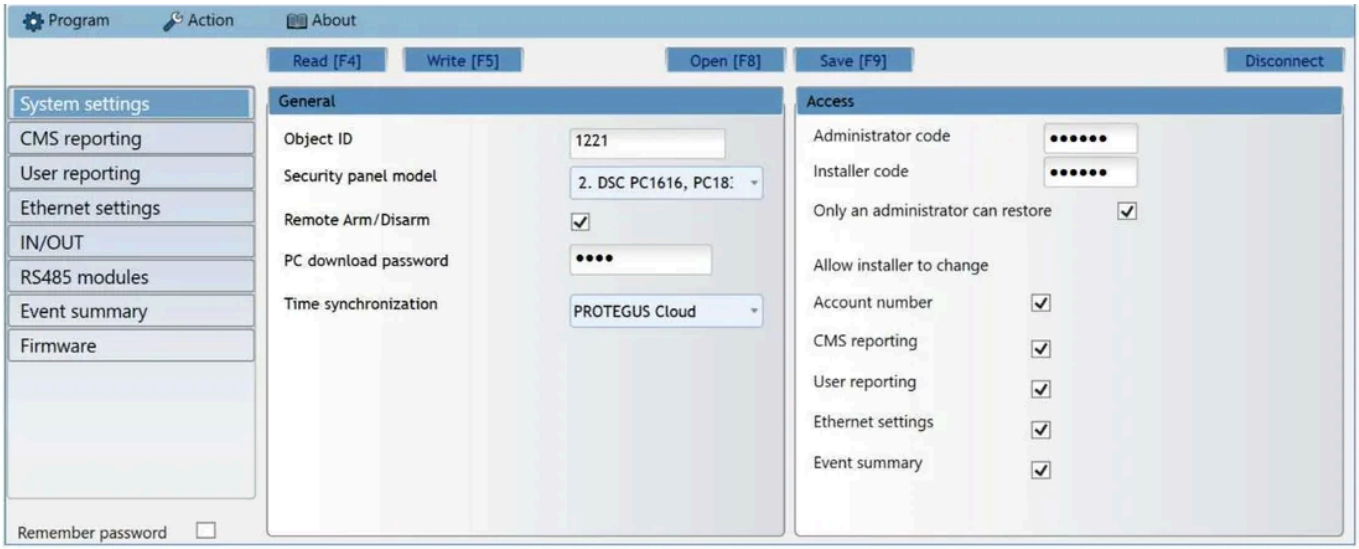


Abbildung 28. TrikdisConfig – Seite System settings: Gruppen General und Access.

- **Object ID** – die von der Leitstelle erhaltene Objektkennung (4 hexadezimale Zeichen, 0–9, A–F). Pflichtangabe, wenn das Gerät auch an eine Leitstelle meldet; `FFFE` und `FFFF` sind nicht verwendbar.
- **Security panel model** – der Typ der angeschlossenen Alarmzentrale aus der Liste. Davon hängt ab, wie der Kommunikator den Bus liest, wählen Sie deshalb den genauen Typ der angeschlossenen Zentrale.
- **Remote Arm/Disarm** – angehakt steuert der Kommunikator die Zentrale direkt: Der Benutzer schaltet aus Protegus 2 mit seinem Bedienteilcode scharf und unscharf. Erscheint nur bei den direkt steuerbaren Zentralentypen; in der Zentrale ist dafür je nach Hersteller eine Einstellung nötig (Kapitel 4). Beim Scharfschalten über eine Schlüsselschalterzone lassen Sie das Feld leer.
- **Security panel PC download password** – für die direkte Steuerung einer Paradox- bzw. Texecom-Zentrale das PC- bzw. UDL-Passwort der Zentrale (4 Zeichen); es muss mit dem in der Zentrale eingestellten übereinstimmen (Abschnitte 4.2 und 4.3).
- **Time synchronization** – die Quelle für die Uhr des Geräts (Standard **PROTEGUS Cloud**, 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 eine IP-Verbindung an die Leitstelle. Die Ereignisse können über mehrere Kanäle gehen: Der **primäre** und der **parallele** Kanal arbeiten gleichzeitig (an zwei Empfänger zugleich), und zu beiden gehört ein **Ersatzkanal**, der in Kraft tritt, wenn der jeweilige Kanal unterbrochen ist. Die Kommunikation ist verschlüsselt und passwortgeschützt; für den Empfang und die Weitergabe an die Leitstellensoftware ist ein Trikdis-Empfänger (Software-Empfänger IPcom für Windows oder Linux, Hardware-IP/SMS-Empfänger RL14, Mehrkanal-Empfänger RM14) oder ein universeller Empfänger nötig, der das Protokoll DC-09 / TL150 beherrscht.

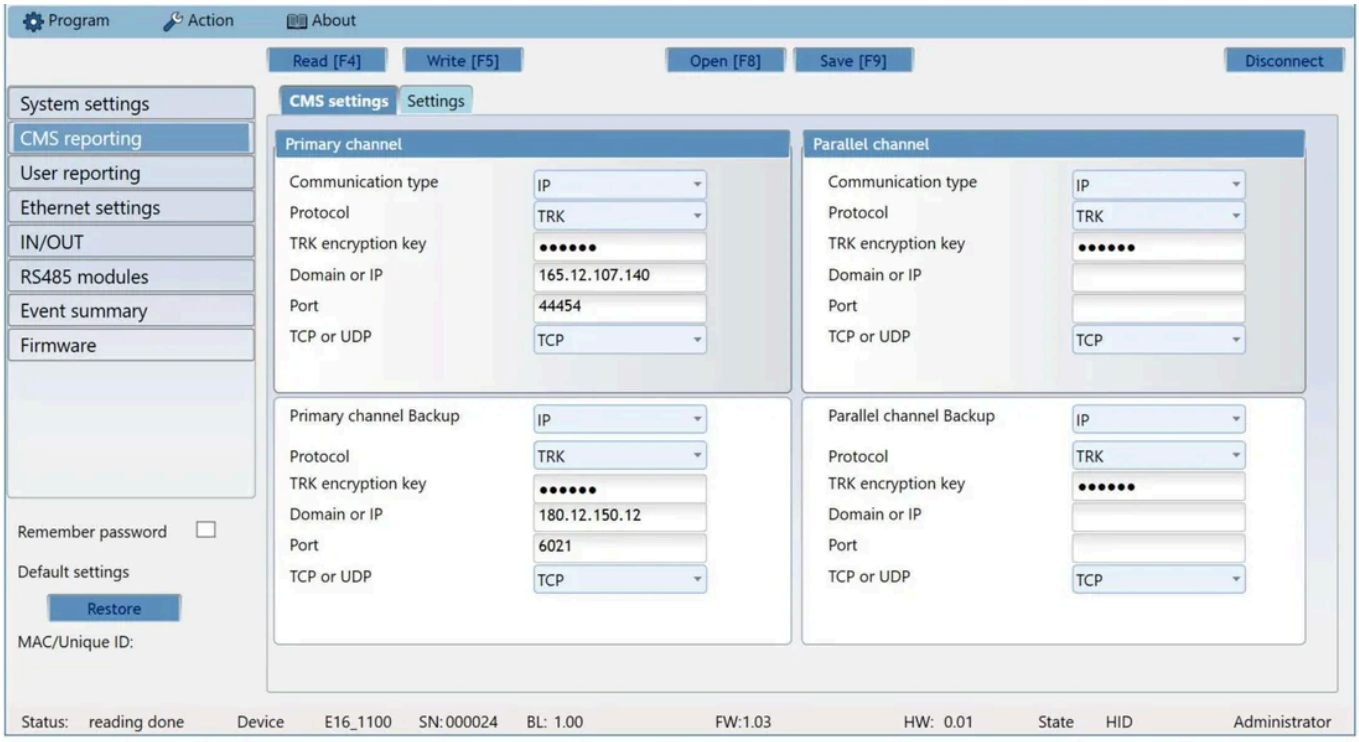


Abbildung 29. TrikdisConfig – CMS reporting, Registerkarte CMS settings: primärer und paralleler Kanal (oben), die zugehörigen Ersatzkanäle (unten).

Primary channel – primärer Kanal

- **Communication type** – **IP**; mit dem Wert **Disable** lässt sich der Kanal ausschalten (zum Beispiel, wenn das Gerät nur mit Protegus 2 arbeitet, ohne Leitstelle).
- **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.

Primary channel Backup – Ersatzkanal. Übernimmt die Kommunikation, wenn der primäre Kanal nicht funktioniert; seine Einstellungen entsprechen den obigen. Da der E16 über einen einzigen Netzwerkweg (das lokale Netzwerk) kommuniziert, ist der Ersatzkanal eine zweite Empfängeradresse auf demselben Weg: Er überbrückt einen Fehler auf der Empfängerseite, nicht aber den Ausfall der Internetverbindung.

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

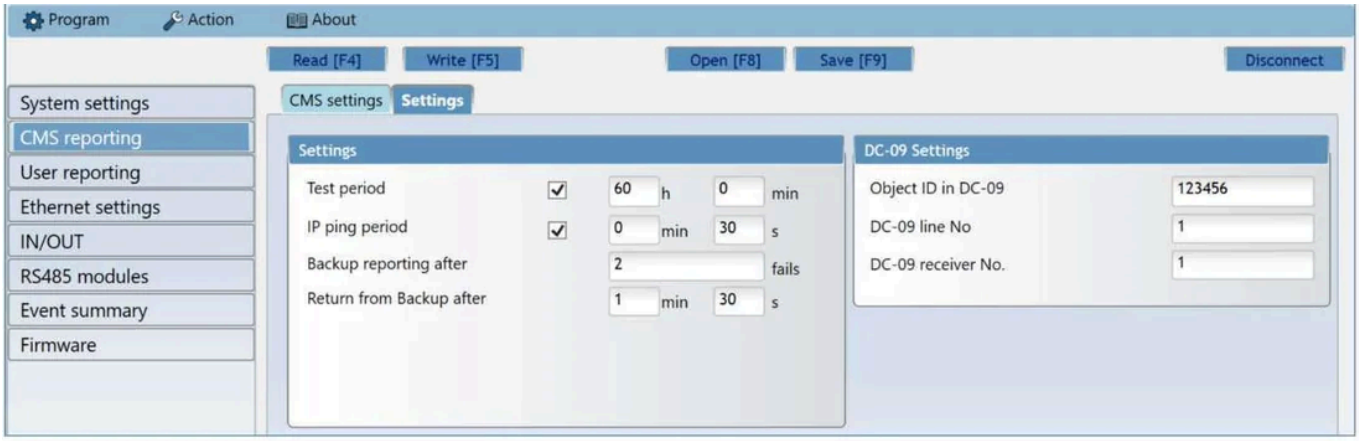


Abbildung 30. TrikdisConfig – CMS reporting, Registerkarte Settings: Testmeldung, PING, die Zeiten des Ersatzkanals und die DC-09-Daten.

Auf der Registerkarte **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.

Die Gruppe **DC-09 settings** ist nur sichtbar, wenn auf einem Kanal das Protokoll DC-09 eingestellt ist. Die Nameserver (DNS) geben Sie beim E16 nicht hier, sondern auf der Seite **Ethernet settings** ein (Abschnitt 6.5).

6.4 User reporting

Auf der Registerkarte **PROTEGUS Cloud** geben Sie den Protegus-Dienst frei, mit dem der Benutzer den Kommunikator aus der Ferne überwachen und steuern kann; mehr über den Dienst: www.protegus.app. Der E16 hat keine SMS-Benachrichtigung und keine SMS-Steuerung, deshalb gibt es auf dieser Seite nur diese eine Registerkarte.

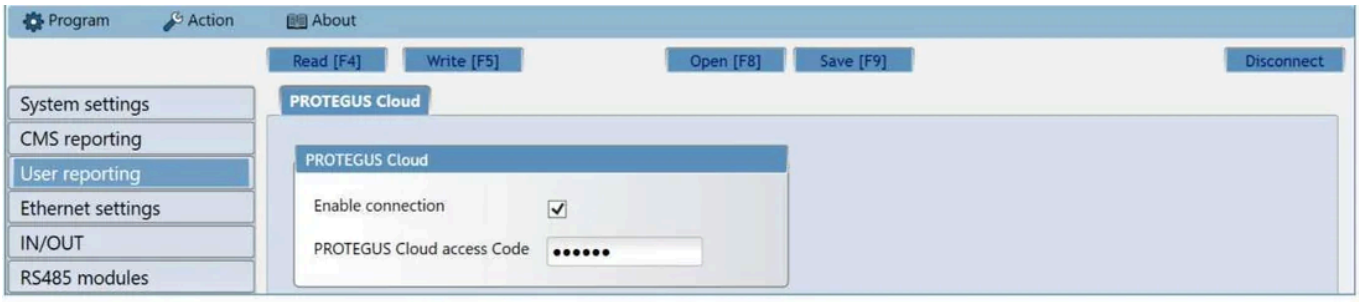


Abbildung 31. TrikdisConfig – User reporting, Registerkarte PROTEGUS Cloud.

- **Enable connection** – gibt die Verbindung zur Protegus Cloud und den Fernzugriff von TrikdisConfig frei.
- **Protegus Cloud access code** – 6-stelliger Code für die Protegus-Verbindung (ab Werk `123456`). Nur vor dem Anlegen des Systems in Protegus 2 einstellbar, nachträglich nicht änderbar.

6.5 Ethernet settings

Hier stellen Sie ein, wie sich der E16 mit dem lokalen Netzwerk verbindet. Ab Werk ist **Use DHCP** angehakt: Das Gerät erhält Adresse, Gateway und Nameserver automatisch vom Router, und an den meisten Orten ist damit nichts zu tun.



Abbildung 32. TrikdisConfig – Seite Ethernet settings: DHCP oder manuelle Netzwerkeinstellung, Nameserver.

- **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.

6.6 IN/OUT

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

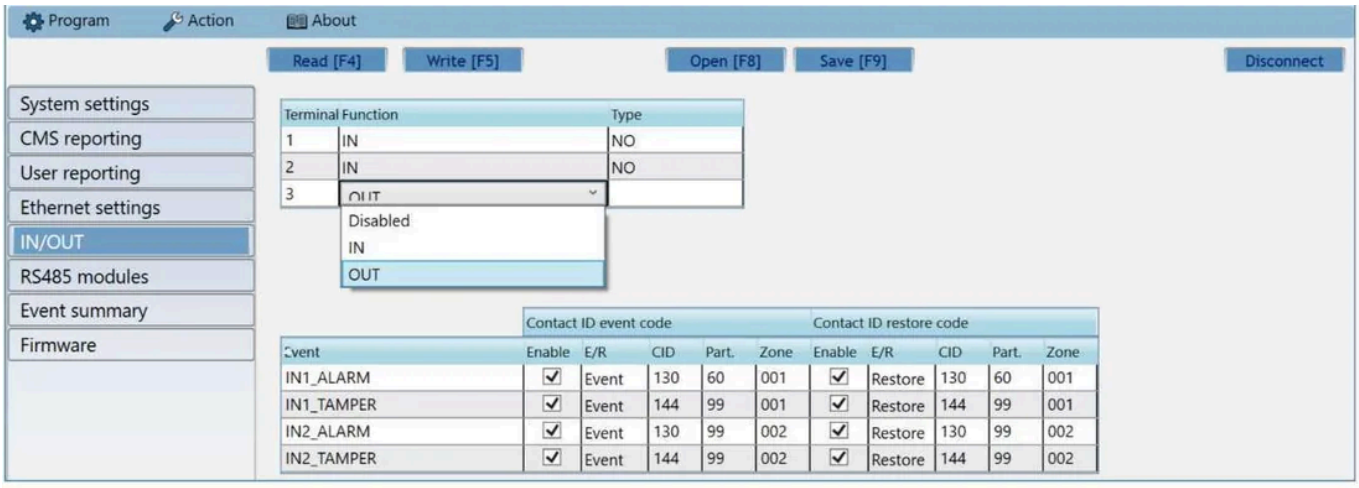


Abbildung 33. TrikdisConfig – Seite IN/OUT: Funktion der I/O-Klemmen und Ereignisse der Eingänge.

Bei Auslösung des am Eingang angeschlossenen Melders 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** – gibt das Senden der Nachricht frei.
- **E/R** – Typ des Ereignisses: Event (Alarm) oder Restore (Wiederherstellung).
- **CID** – der Contact-ID-Code; Sie können ihn angeben oder den Standardwert belassen. Das Ereignis geht mit diesem Code an Protegus 2 und an die Leitstelle.
- **Part.** – die Nummer des Bereichs in der Nachricht.
- **Zone** – die Nummer der Zone in der Nachricht.

6.7 RS485 modules

Die an den RS485-Bus angeschlossenen Erweiterungsmodule iO-8 müssen auf der Registerkarte **Modules list** hinzugefügt werden.

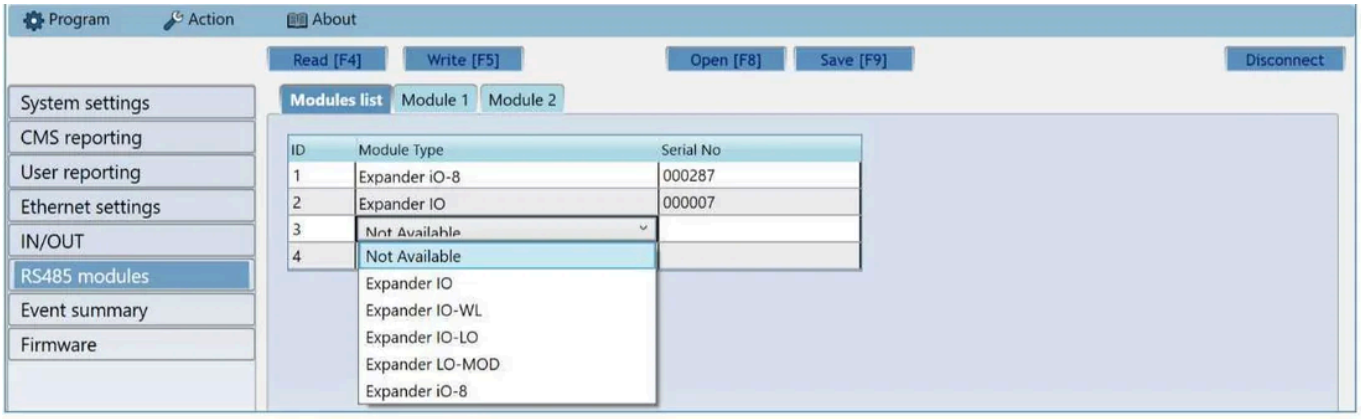


Abbildung 34. TrikdisConfig – RS485 modules, Registerkarte Modules list: Typ des Moduls (Expander iO-8) und Seriennummer.

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

Nach Auswahl des Moduls und Eingabe der Seriennummer drücken Sie die Schaltfläche **Write [F5]**, ziehen das USB-Kabel ab und warten eine Minute, bis der Kommunikator das Modul registriert hat. Danach stecken Sie das Kabel wieder ein, lesen das Gerät aus (**Read [F4]**), und auf der Seite RS485 modules erscheint die eigene, nummerierte Registerkarte des Moduls.

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

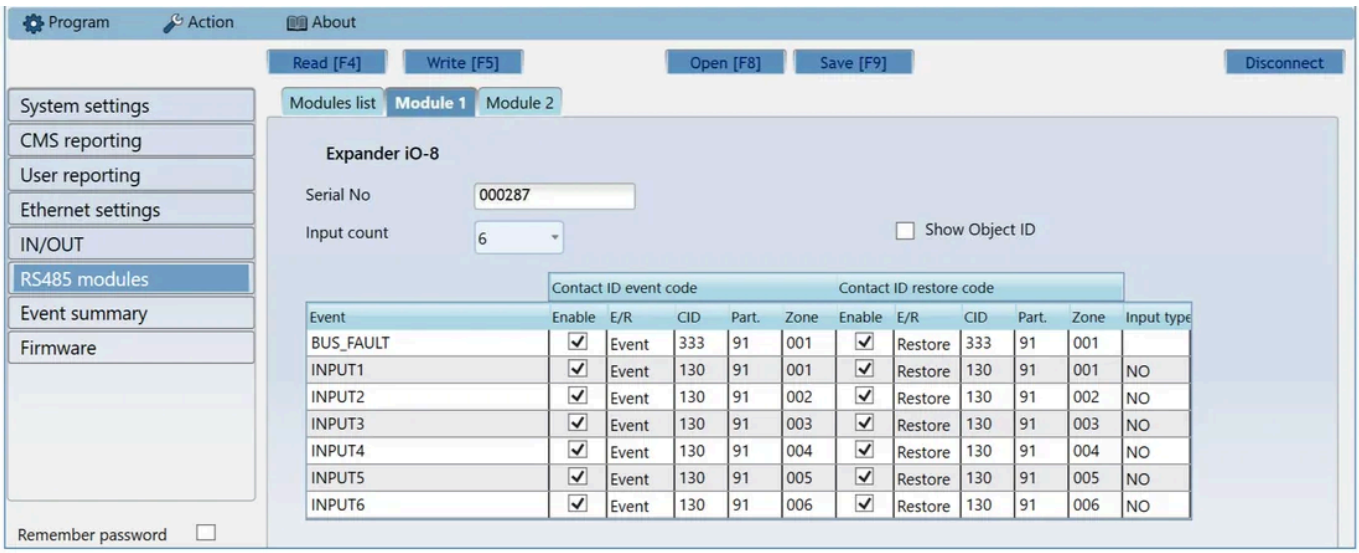


Abbildung 35. TrikdisConfig – RS485 modules, Registerkarte des Moduls iO-8 (oben) und Ereignistabelle des Erweiterungsmoduls (unten).

- **Input Count** – wie viele Klemmen Eingänge sein sollen; die übrigen werden Ausgänge. Der Typ des Eingangs (**Input type**: NO oder NC) lässt sich in der Tabelle angeben. Die Rolle der Ausgänge (Scharf- / Unscharfschalten über eine Schlüsselschalterzone 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**). Standardmäßig meldet Modul 1 mit Bereich 91, Modul 4 mit Bereich 94. Mit dem Häkchen bei **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.

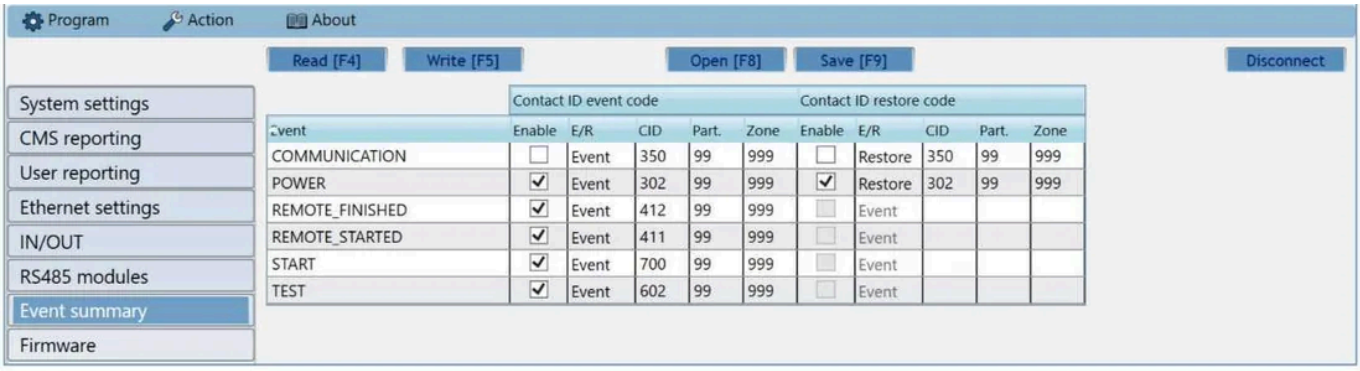


Abbildung 36. TrikdisConfig – Seite Event summary: die internen Nachrichten des Geräts (COMMUNICATION, POWER, REMOTE_FINISHED, REMOTE_STARTED, START, TEST) und die zugehörigen Contact-ID-Codes.

6.9 Zurücksetzen auf Werkseinstellungen

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

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

7. Fernprogrammierung

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

Für den Fernzugriff erforderlich:

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

Schritte:

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

6. Nehmen Sie die Änderungen vor und senden Sie sie dann mit der Schaltfläche **Write [F5]** (Schreiben) an das Gerät.

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

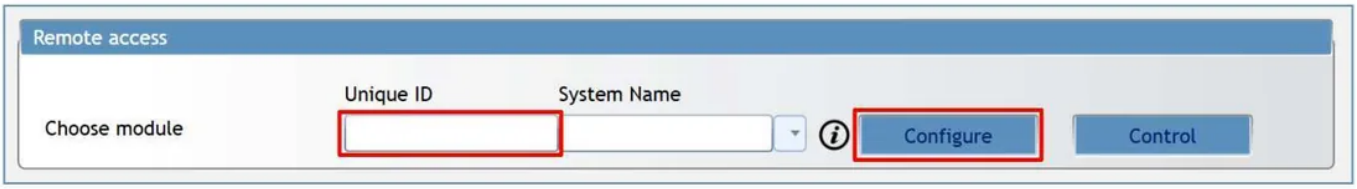


Abbildung 37. TrikdisConfig – Remote access: die Kennung des Geräts (Unique ID – beim E16 die MAC-Adresse), der Name des Systems und die Schaltfläche Configure.

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.

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

Prüfen Sie auch das Verhalten bei Netzwerkausfall: Ziehen Sie das Ethernet-Kabel ab und sehen Sie nach, ob die LED TROUBLE den Ausfall mit 1 Blinksignal meldet, ob nach dem Wiedereinstecken die LED NETWORK wieder grün leuchtet und ob die gespeicherten Ereignisse bei der Leitstelle bzw. in der App ankommen.

9. Firmware-Update

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

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

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

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

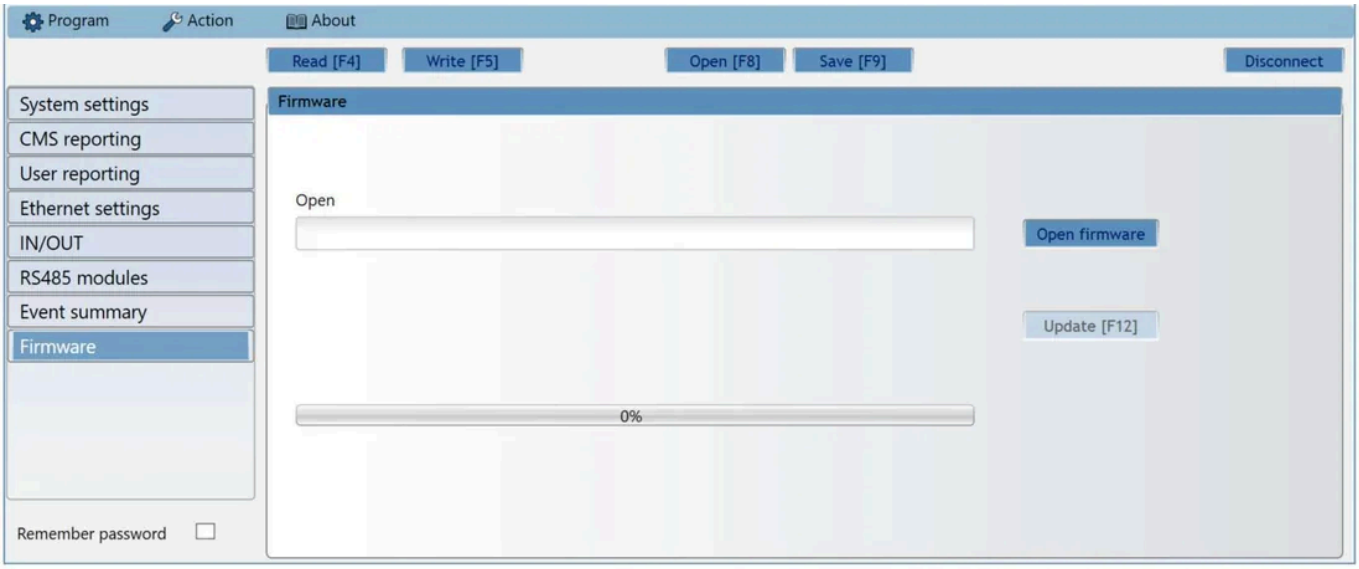


Abbildung 38. TrikdisConfig – Seite Firmware: Open firmware und Update [F12] (oben), Fortschrittsanzeige des Updates (unten).

Für das Update ist eine Internetverbindung nötig. Virenscanner, Firewall oder strenge Netzwerkeinstellungen können den automatischen Download der Firmware verhindern; ändern Sie in diesem Fall die Einstellungen des Virenscanners, oder laden Sie die Datei manuell herunter und öffnen Sie sie auf der Seite Firmware.

10. Fehlersuche und häufige Fragen

Die häufigsten Fragen und Fehler, ausgehend von den LED-Anzeigen. 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 Blinksignale der LED **TROUBLE** an: 1 = keine physische Verbindung (Kabel, Port), 2 = keine IP-Adresse erhalten (DHCP), 3 = der Name des Empfängers oder der Protegus Cloud lässt sich nicht auflösen (DNS).

2. **1 Blinksignal:** Prüfen Sie das Ethernet-Kabel an beiden Enden und ob der Port des Routers oder Switches aktiv ist (die LED des Ports leuchtet); versuchen Sie einen anderen Port oder ein anderes Kabel.
3. **2 Blinksignale:** Am Router muss DHCP eingeschaltet sein, oder geben Sie dem Gerät auf der Seite **Ethernet settings** eine feste IP-Adresse (Abschnitt 6.5). In einem Firmennetz kann der Systemadministrator das Gerät anhand der MAC-Adresse freigeben.
4. **3 Blinksignale:** Der Nameserver ist nicht erreichbar. Ab Werk ist das öffentliche DNS von Google eingestellt; wenn das Netzwerk externes DNS sperrt, geben Sie auf der Seite **Ethernet settings** den lokalen Nameserver ein.

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 Blinksignale der LED **TROUBLE** zeigen an, dass keine Verbindung zum Empfänger besteht: Prüfen Sie Adresse und Port des Empfängers, die TCP/UDP-Einstellung und den Verschlüsselungsschlüssel (**CMS reporting**).
2. Wenn der Empfänger mit Domainnamen angegeben ist, prüfen Sie die DNS-Einstellung (**Ethernet settings**).
3. In einem durch eine Firewall gefilterten Netzwerk muss der ausgehende TCP/UDP-Verkehr zum Port des Empfängers freigegeben werden; am Router muss kein Port (eingehend) geöffnet werden.

Die LED TROUBLE blinkt sieben Mal – der Kommunikator sieht die Zentrale nicht

1. Prüfen Sie den Anschluss nach der Abbildung in Abschnitt 3.3: Der häufigste Fehler sind vertauschte Adern **CLK** und **DATA** oder eine an die falsche Klemme der Zentrale angeschlossene Datenleitung.
2. Im Feld **System settings** → **Security panel model** von TrikdisConfig muss der genaue Typ der angeschlossenen Zentrale ausgewählt sein.
3. Bei Texecom-, Caddx-, Honeywell- und InnerRange-Zentralen ist auch in der Zentrale eine Einstellung nötig (Kapitel 4) – ohne sie gibt die Zentrale keine Daten auf den Bus.
4. Bei einer Paradox-Zentrale kann die serielle Schnittstelle ab Werk gesperrt sein – so schalten Sie sie frei.
5. Machen Sie eine Pyronix-Zentrale nach dem Anschluss stromlos und starten Sie sie neu, damit sie den Kommunikator akzeptiert.
6. Mit einer DSC-PowerSeries-Zentrale **NEO** funktioniert der E16 nicht (der NEO-Bus lässt kein externes Gerät zu) – hier ist ein Kommunikator für die Telefonleitung (E16T) nötig.

Die Ereignisse kommen an, aber ich kann aus der App nicht scharf schalten

Bei direkter Steuerung:

1. Auf der Seite **System settings** muss **Remote Arm/Disarm** angehakt sein.
2. Bei Paradox- und Texecom-Zentralen muss das **Security panel PC download password** mit dem PC- bzw. UDL-Passwort der Zentrale übereinstimmen (Abschnitte 4.2 und 4.3).

3. Bei einer Paradox-Zentrale muss die Firmware der Zentrale mindestens **V.4** sein; der Code des Benutzers darf nicht der Mastercode sein; starten Sie nach einer Codeänderung den Kommunikator neu.
4. Bei einer Honeywell-Vista-Zentrale muss die 2. AUI-Adresse freigegeben sein (Abschnitt 4.6).
5. In Protegus 2 darf dem Bereich **kein** Ausgang zugeordnet sein (Control with Protegus2 ausgeschaltet).

Mit einer Schlüsselschalterzone:

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

Protegus 2 sieht das Gerät nicht

1. Auf der Seite **User reporting → PROTEGUS Cloud** muss **Enable connection** angehakt sein.
2. Beim Anlegen des Systems muss der im Gerät eingestellte **Protegus Cloud access code** eingegeben werden; dieser ist nach dem Anlegen des Systems im Gerät nicht mehr änderbar.
3. Geben Sie die **MAC-Adresse (Unique ID)** genau ein, von der Verpackung oder von der Rückseite.
4. Das Gerät muss online sein: Die LED NETWORK ist grün, TROUBLE blinkt nicht, und die LED DATA erlischt nach einem Ereignis. In einem Netzwerk mit Firewall muss die ausgehende Verbindung zur Protegus Cloud freigegeben werden.

Ich kann mich mit TrikdisConfig nicht aus der Ferne verbinden

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

Muss am Router ein Port geöffnet oder weitergeleitet werden?

Nein. Der E16 baut nur **ausgehende** Verbindungen zum Empfänger und zur Protegus Cloud auf, deshalb sind weder Portweiterleitung noch eine öffentliche IP-Adresse nötig; auch die Fernprogrammierung läuft über diese ausgehende Verbindung. Achten Sie nur darauf, dass die Firewall den ausgehenden Verkehr zum Port des Empfängers und zur Protegus Cloud nicht sperrt.

Funktioniert er über WLAN oder Mobilfunk?

Nein: Der E16 hat nur einen kabelgebundenen Ethernet-Anschluss. Wenn die Stromversorgung des Routers nicht zuverlässig ist, betreiben Sie die Netzwerkgeräte an einer unterbrechungsfreien Stromversorgung.

Was passiert bei einem Stromausfall?

Der E16 wird von der Alarmzentrale versorgt und arbeitet daher über den Akku der Zentrale weiter, Router und Modem fallen jedoch in der Regel aus, und damit ist auch das Internet weg. Solange keine Verbindung besteht, meldet die LED TROUBLE mit 1 oder 6 Blinksignalen, das Gerät speichert die Ereignisse (höchstens 60

Nachrichten) und sendet sie bei Wiederkehr des Internets der Reihe nach. Wenn ein Ausfall des Internets für das System nicht zulässig ist, betreiben Sie auch die Netzwerkgeräte an einer unterbrechungsfreien Stromversorgung.

11. Sicherheitshinweise

Figyelem!

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- Montage und Wartung sicherheitstechnischer Anlagen dürfen nur von einer qualifizierten Fachkraft durchgeführt werden.
- Lesen Sie vor der Installation die Anleitung; die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen oder 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

- Kompatibilitätssuche – welcher Kommunikator zu welcher Alarmzentrale passt.
- G16 – direkte Steuerung für DSC-PowerSeries-Alarmzentralen – Scharfschalten mit dem Bedienteilcode, Zonenzustände, Sperren von Zonen; gilt genauso für den E16.
- DSC Power Series NEO und Trikdis-Kommunikatoren: Kompatibilität und Lösungen – warum der E16 nicht an die NEO angeschlossen werden kann und was die Lösung ist.
- Freischaltung der gesperrten seriellen Schnittstelle an Paradox-Alarmzentralen – Freischaltung der seriellen Schnittstelle neuerer Paradox-Zentralen.
- 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 E16 Ethernet Communicator - IP -Modul

Trikdis CRP2 Seriell-Port-Verbindungskabel für Paradox-Alarmpulte

Trikdis CRP2B Seriell-Port-Verbindungskabel für Paradox-Alarmpulte

Trikdis CRP4 Serienkabel für Texcom -Steuerplatten **Trikdis IO8 Wired Expander Modul**

Urheberrecht

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

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

Immer aktuelle Version dieser Anleitung: https://trikdis.at/e16-anleitung