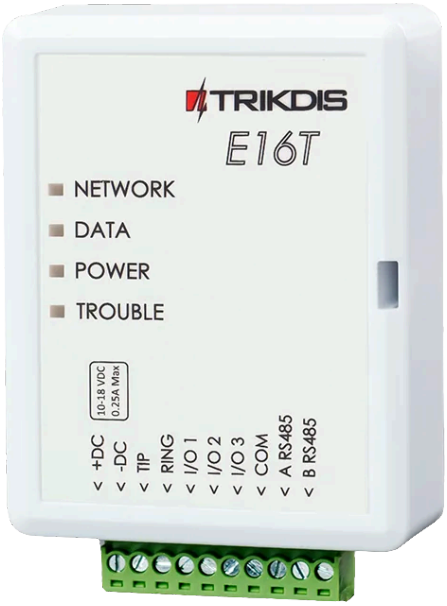
Komunikator E16T – instrukcja dla instalatora i użytkownika

Instrukcja instalatora i użytkownika komunikatora Ethernet Trikdis E16T: podłączenie do centrali alarmowej, konfiguracja sieci w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2, sprawdzanie i rozwiązywanie problemów.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-e16t

Spis treści

1. Przegląd

1.1 Do czego służy i jak działa
1.2 Wersje
1.3 Główne cechy
1.4 Elementy komunikatora
1.5 Zaciski
1.6 Sygnalizacja diod
1.7 Dane techniczne

2. Szybkie uruchomienie z TrikdisConfig

2.1 Przygotowanie
2.2 Połączenie z aplikacją Protegus 2
2.3 Połączenie ze stacją monitorowania

3. Instalacja i podłączenie

3.1 Kroki instalacji
3.2 Miejsce montażu i sieć
3.3 Podłączenie do centrali alarmowej
3.3.1 W uzasadnionych przypadkach: nadzór linii
3.4 Podłączenie strefy przełącznika kluczowego
3.5 Podłączenie wejść
3.6 Podłączenie kabla Ethernet
3.7 Podłączenie wyjścia z przekaźnikiem
3.8 Podłączenie ekspandera iO-8
3.9 Włączenie i pierwsze sprawdzenie
A TRIKDIS átjelző elindítása

4. Programowanie centrali alarmowej

4.1 Programowanie dialera Honeywell Vista
4.2 Centrale innych producentów

5. Zdalne sterowanie aplikacją Protegus 2

5.1 Dodawanie urządzenia
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Uzbrajanie i rozbrajanie wyjściem
5.3 Uzbrajanie i rozbrajanie z aplikacji

6. TrikdisConfig – szczegółowe ustawienia

6.1 Pasek stanu
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 Przywracanie ustawień fabrycznych

7. Zdalne programowanie

8. Sprawdzenie działania komunikatora

9. Aktualizacja firmware

10. Rozwiązywanie problemów i częste pytania

11. Zasady bezpieczeństwa

Zobacz też

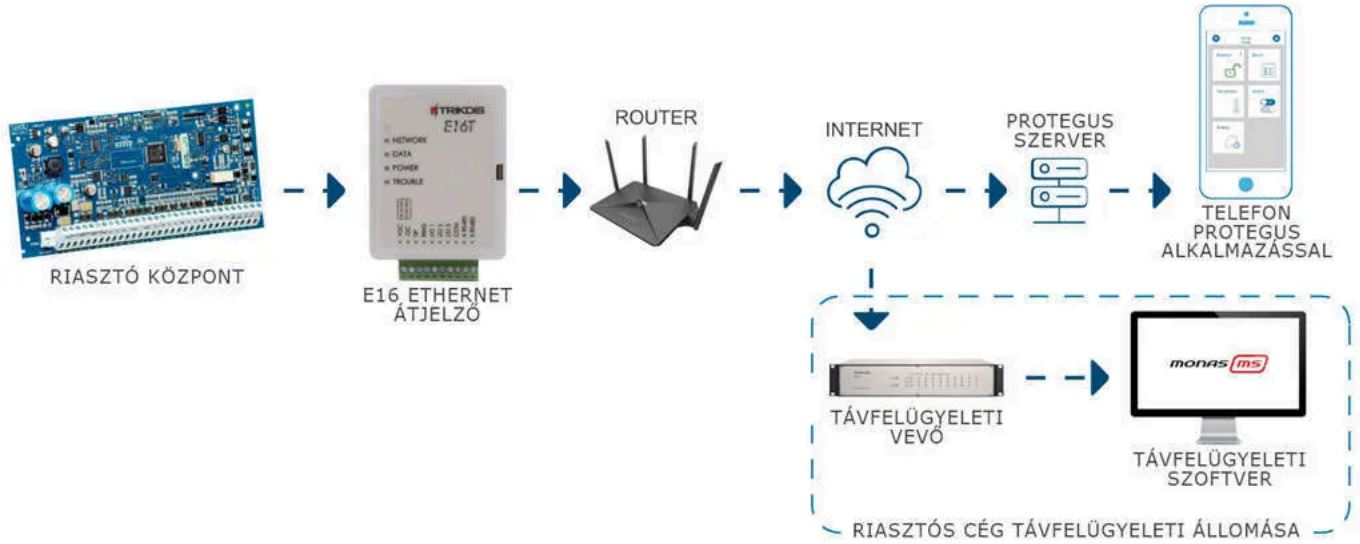
1. Przegląd

E16T to **uniwersalny komunikator Ethernet** Trikdis: łączy się z wyjściem linii telefonicznej centrali alarmowej (TIP/RING) i zachowuje się jak centrala telefoniczna. Centrala alarmowa „wybiera numer" i tonami DTMF wysyła komunikat Contact ID, a E16T podnosi linię, dekoduje komunikat i przez sieć lokalną oraz przewodowe łącze internetowe przekazuje go do odbiornika stacji monitorowania, a także do chmury Protegus, czyli do aplikacji użytkownika. Dzięki temu można go używać z **centralą dowolnego producenta**, która ma dialer Contact ID – centrali nie trzeba wymieniać, wystarczy ustawić jej dialer. E16T działa przez przewodowy internet, bez karty SIM i bez abonamentu.

1.1 Do czego służy i jak działa

- **Raportuje do stacji monitorowania.** Wysyła zdarzenia przez połączenie IP do programowego lub sprzętowego odbiornika Trikdis (protokół TRK; odbiorniki te współpracują z dowolnym oprogramowaniem stacji monitorowania) albo do dowolnego odbiornika uniwersalnego (SIA DC-09 2007/2012, SUR-GARD TL150). Połączenie jest domyślnie sprawdzane co 30 sekund (komunikator wysyła do odbiornika sygnał życia, PING; odstęp można zmienić), a w razie awarii komunikator przełącza się na kanał zapasowy.
- **Powiadamia użytkownika.** Aplikacja Protegus 2 pokazuje, co się stało, w powiadomieniu push (z osobnym sygnałem dźwiękowym) i na liście zdarzeń; użytkownik może z aplikacji uzbrajać i rozbrajać system oraz włączać i wyłączać podłączone urządzenia (oświetlenie, bramę, wentylację, ogrzewanie, system nawadniania itp.). Aplikacja działa z centralą alarmową dowolnego producenta, do której podłączony jest E16T.
- **Działa ze stacją monitorowania i z użytkownikiem jednocześnie lub osobno:** można go używać tylko z Protegus 2 (bez stacji monitorowania), tylko ze stacją monitorowania albo z obiema. Jeśli ustawione są obie, zdarzenie trafia najpierw do stacji monitorowania, a potem do użytkownika.
- **Ma własne wejścia i wyjścia.** Trzy zaciski I/O o podwójnej funkcji mogą pracować jako wejście (czujka, sabotaż) lub jako sterowane wyjście (strefa przełącznika kluczowego, przekaźnik). Ekspanderem iO-8 podłączonym do magistrali RS485 można dodać do systemu kolejne 8 I/O.
- **Bez abonamentu.** E16T korzysta z istniejącego łącza internetowego w obiekcie: nie jest potrzebna karta SIM, abonament komórkowy ani antena, a siła sygnału komórkowego nie ma znaczenia.

Budowę systemu pokazuje poniższy rysunek: wyjście linii telefonicznej centrali alarmowej łączy się z E16T, E16T przez lokalny router łączy się z internetem, a stamtąd z odbiornikiem stacji monitorowania i chmurą Protegus, natomiast użytkownik widzi system w aplikacji Protegus 2.



Rysunek 1. Miejsce E16T w systemie: centrala alarmowa → E16T → router → internet → odbiornik stacji monitorowania i chmura Protegus → aplikacja Protegus 2.

1.2 Wersje

Ta instrukcja dotyczy **obecnej wersji sprzętowej E16T oznaczonej v2** (TrikdisConfig pokazuje ją jako **E16T_2000**), ale **można jej używać również do wcześniejszego E16T**: podłączenie, konfiguracja i działanie są w dużej mierze takie same. Różnice zestawia poniższa tabela; tam, gdzie tekst podaje dane v2, przy wcześniejszej wersji uwzględnij te z tabeli.

	Wcześniejszy E16T	**E16T v2 (obecny)**
Wejścia/wyjścia	2 wejścia z wybieralnym typem (T-1/IN1, R-1/IN2 – NC, NO, EOL; można ich też używać do nadzoru linii telefonicznej) + 1 wyjście typu otwarty kolektor (OUT, maks. 0,15 A, do 30 V; sterowane z aplikacji Protegus)	3 zaciski I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3), każdy do użycia jako wejście (typy NC, NO, EOL, DEOL) lub jako wyjście typu otwarty kolektor (maks. 0,15 A)
Pobór prądu	najwyżej 0,5 A	100 mA nominalnie, najwyżej 250 mA podczas wysyłania
Diody	NETWORK, DATA, POWER, TROUBLE, LINE (LINE świeci na zielono, dopóki centrala „podniosła słuchawkę", czyli wybiera numer; odmienną sygnalizację pozostałych diod wymienia uwaga na końcu punktu 1.6)	NETWORK, DATA, POWER, TROUBLE
Bufor zdarzeń	100 komunikatów	60 komunikatów
Wymiary	88 × 62 × 25 mm	88 × 65 × 26 mm

Wersję sprzętową znajdziesz na pasku stanu TrikdisConfig (**HW**) i na etykiecie z tyłu urządzenia.

1.3 Główne cechy

Połączenie z centralą alarmową

- Standardowe podłączenie do wyjścia linii telefonicznej centrali: DC+, DC−, TIP i RING. W uzasadnionych przypadkach można go podłączyć także z nadzorem linii (przewodami T-1 i R-1): wtedy połączenie między centralą a komunikatorem jest **nadzorowane**, przerwanie przewodu komunikator sygnalizuje.
- Centrala wysyła zdarzenia w formacie Contact ID, wybieraniem DTMF; E16T przekazuje pełną informację o zdarzeniu (kod, partycja, strefa lub użytkownik).

Komunikacja ze stacją monitorowania

- Połączenie IP z odbiornikami Trikdis (odbiornik programowy IPcom, RL14, RM14) i odbiornikami uniwersalnymi (SIA DC-09, TL150).
- Kanał główny, zapasowy i równoległy: może wysyłać jednocześnie do dwóch odbiorników, do każdego z osobnym kanałem zapasowym.
- Szyfrowana, chroniona hasłem komunikacja; bufor zdarzeń 60 komunikatów.

Funkcje dla użytkownika

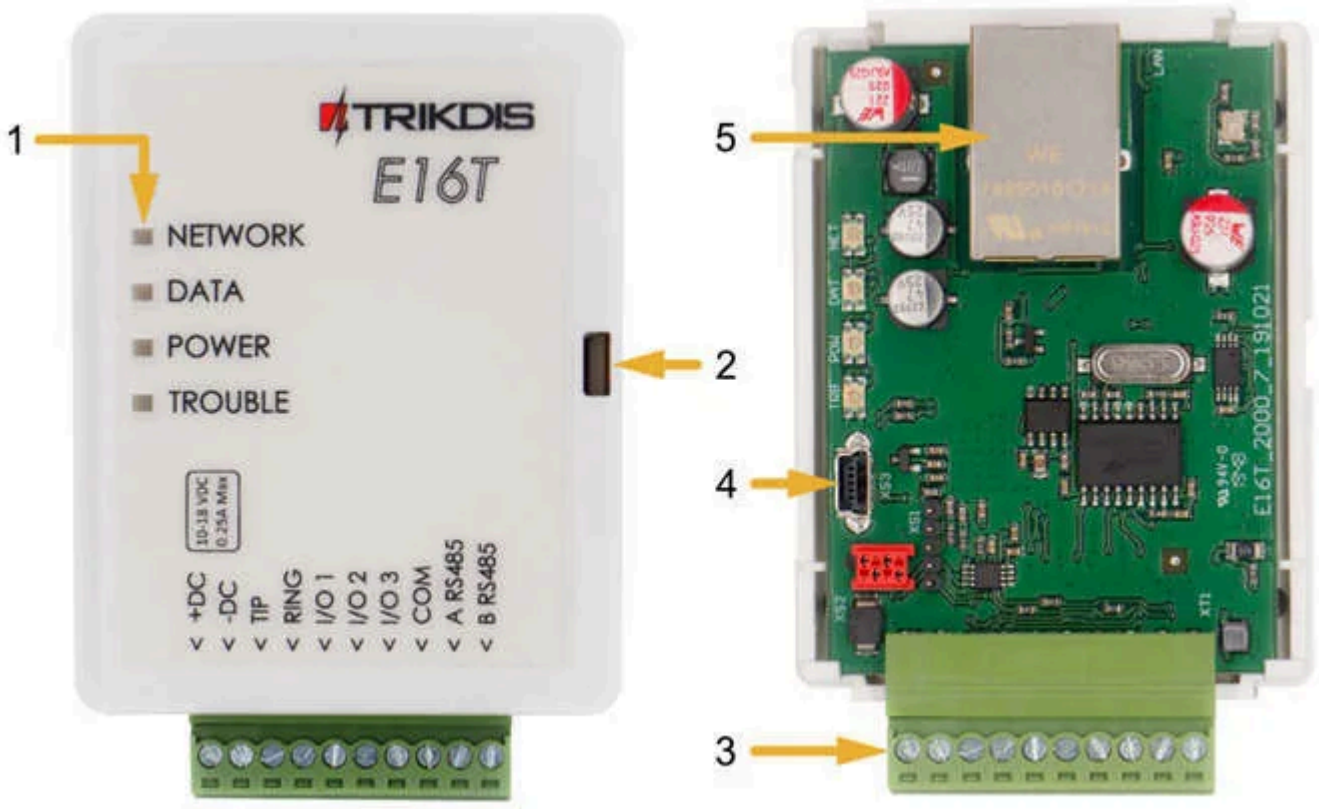
- Aplikacja mobilna i webowa Protegus 2: powiadomienia, lista zdarzeń, uzbrajanie i rozbrajanie, sterowanie wyjściami.
- Wielopoziomowe uprawnienia użytkowników w aplikacji (administrator, instalator, użytkownik).

Instalacja i konfiguracja

- Ustawienia można zapisać do pliku i wczytać do innego komunikatora.
- Dwa poziomy dostępu: administrator i instalator – do konfiguracji urządzenia, dla administratora stacji monitorowania i dla instalatora.
- Zdalna konfiguracja i aktualizacja programem TrikdisConfig.

1.4 Elementy komunikatora

Płytka drukowana E16T jest umieszczona w białej obudowie z tworzywa; przednią pokrywę można zdjąć, a listwę zaciskową – wyciągnąć. Złącze sieciowe (RJ45) znajduje się przy górnej krawędzi płytki drukowanej i jest dostępne przez otwór w obudowie.



Rysunek 2. Elementy E16T od przodu i przy otwartej obudowie.

- 1 Diody sygnalizacyjne (NETWORK, DATA, POWER, TROUBLE)
- 2 Otwór ułatwiający zdjęcie przedniej pokrywy (na górnej krawędzi pokrywy)
- 3 Wyjmowana listwa zaciskowa
- 4 Gniazdo USB Mini-B do programowania
- 5 Złącze Ethernet (RJ45)

Listwę zaciskową można wyciągnąć: dzięki temu urządzenie jednym ruchem odłączysz od zasilania lub uruchomisz ponownie, łatwiej się ją podłącza, a do programowania przez USB urządzenie można zanieść do komputera.

1.5 Zaciski

Zacisk	Funkcja
+DC	Zasilanie, +10–18 V DC
–DC	Zasilanie, minus
TIP	Zacisk TIP centrali alarmowej
RING	Zacisk RING centrali alarmowej
I/O 1 (T-1)	1. wejście/wyjście lub punkt T-1 nadzoru linii telefonicznej
I/O 2 (R-1)	2. wejście/wyjście lub punkt R-1 nadzoru linii telefonicznej
I/O 3	3. wejście/wyjście
COM	Wspólny punkt (minus) wejść i wyjść
A 485	Przewód A magistrali RS485 (iO-8 i inne ekspandery serii iO)
B 485	Przewód B magistrali RS485

Opis listwy zaciskowej jest też na przedniej pokrywie, więc przy podłączaniu nie trzeba jej zdejmować.

1.6 Sygnalizacja diod

Diody na przedniej pokrywie to najważniejsze narzędzie przy uruchamianiu i rozwiązywaniu problemów. Odczytuj je razem: POWER pokazuje zasilanie, NETWORK połączenie z siecią, DATA komunikaty oczekujące na wysłanie, a TROUBLE usterkę.

NETWORK – połączenie z siecią

Sygnał	Znaczenie
nie świeci	Brak połączenia z siecią (brakuje kabla, port nie działa lub urządzenie nie otrzymało adresu IP)
świeci na zielono	Połączono z siecią lokalną – połączenie działa aż do routera. Czy dostępny jest też internet, pokaże dioda DATA (zobacz niżej).

DATA – ruch danych

Sygnał	Znaczenie
nie świeci	Brak komunikatów oczekujących na wysłanie
świeci na zielono	W buforze są komunikaty oczekujące na wysłanie
miga na zielono	Trwa wysyłanie lub odbieranie danych (podczas programowania)

Szybkie sprawdzenie

Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie działa do routera – ale nie to, że urządzenie ma też dostęp do internetu. Jeśli dioda NETWORK jest zielona, a dioda DATA świeci ciągle także po zdarzeniu lub raporcie testowym, połączenie z internetem nie działa: komunikat nie może zostać wysłany. W sieci komórkowej najczęściej winny jest APN albo usługa transmisji danych karty SIM, przy Ethernecie router, zapora sieciowa (firewall) lub DNS. Jeśli dioda DATA zgaśnie, komunikat został wysłany, a połączenie danych działa prawidłowo.

POWER – napięcie zasilania

Sygnał	Znaczenie
nie świeci	Brak zasilania lub zasilanie jest odłączone
świeci na zielono	Włączony, napięcie zasilania prawidłowe
świeci na żółto	Nieprawidłowe napięcie zasilania (najwyżej 11,5 V)
świeci na zielono, miga na żółto	Gotowy do programowania (kabel USB podłączony)
świeci na żółto (podczas programowania)	Brak połączenia z komputerem

TROUBLE – usterka

Sygnał	Znaczenie
nie świeci	Brak usterki
1 czerwone mignięcie	Brak fizycznego połączenia z siecią (PHY link): kabel, wtyk albo port routera / switcha

Sygnał	Znaczenie
2 czerwone mignięcia	Błąd DHCP: urządzenie nie otrzymało adresu IP
3 czerwone mignięcia	Błąd DNS: rozwiązywanie nazw nie działa
6 czerwonych mignięć	Brak połączenia z odbiornikiem stacji monitorowania
7 czerwonych mignięć	Zerwane połączenie z centralą alarmową
miga na czerwono (podczas programowania)	Błąd pamięci
świeci na czerwono (podczas programowania)	Uszkodzony firmware

Wcześniejszy E16T

Diody wcześniejszego E16T sygnalizują częściowo co innego: **DATA** świeci na żółto, jeśli w buforze jest zdarzenie oczekujące na wysłanie, i miga na zielono, dopóki centrala alarmowa przekazuje komunikat do komunikatora; **POWER** miga na zielono, jeśli zasilanie jest włączone, a napięcie prawidłowe, i miga na żółto, jeśli napięcie zasilania jest niewystarczające (najwyżej 11,5 V); ciągłe czerwone światło **TROUBLE** oznacza błąd połączenia z siecią (LAN), a zgaszona dioda – brak usterki; **LINE** świeci na zielono, dopóki centrala „podniosła słuchawkę" (punkt 1.2).

1.7 Dane techniczne

Parametr	Wartość
Połączenie z centralą alarmową	przewodowa linia telefoniczna (TIP/RING), Contact ID, DTMF
Wejścia/wyjścia	3 I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3): jako wejście NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (rezystor końcowy 2,2 kΩ); jako wyjście typu otwarty kolektor (OC), maks. 0,15 A / 30 V DC
Rozbudowa	na magistrali RS485: ekspander iO-8 (+8 I/O) i inne ekspandery serii iO, najwyżej 4 moduły
Złącze sieciowe	Ethernet, IEEE 802.3, 10Base-T, gniazdo RJ45
Ustawienia sieci	DHCP (fabrycznie) lub stały adres IP
Napięcie zasilania	10–18 V DC
Pobór prądu	100 mA nominalnie; najwyżej 250 mA podczas wysyłania
Protokoły transmisji	TRK, DC-09_2007, DC-09_2012, TL150
Bufor zdarzeń	60 komunikatów
Programowanie	TrikdisConfig (Windows) przez kabel USB Mini-B lub zdalnie
Warunki pracy	−10 … +50 °C, maks. 80 % wilgotności względnej (przy +20 °C)
Wymiary	88 × 65 × 26 mm
Masa	80 g

2. Szybkie uruchomienie z TrikdisConfig

Wszystkie ustawienia E16T wprowadza się programem **TrikdisConfig** działającym w systemie Windows – przez kabel USB lub zdalnie. W tym rozdziale opisujemy najkrótszą drogę: urządzenie konfigurujesz na biurku, przed podłączeniem, a w obiekcie trzeba je już tylko podłączyć. Szczegółowe objaśnienie ustawień zawiera rozdział 6.

2.1 Przygotowanie

Czego będziesz potrzebować

kabel USB Mini-B (do konfiguracji) · co najmniej 4-żyłowy przewód do centrali · płaski śrubokręt 2,5 mm · kabel Ethernet (CAT-5 lub lepszy, najwyżej 100 m) do routera lub switcha · wolny port sieciowy · jeśli w sieci nie ma DHCP: stały adres IP, maska, brama i DNS otrzymane od administratora sieci · instrukcja instalatora centrali alarmowej. To, czego brakuje, można zamówić osobno u lokalnego dystrybutora.

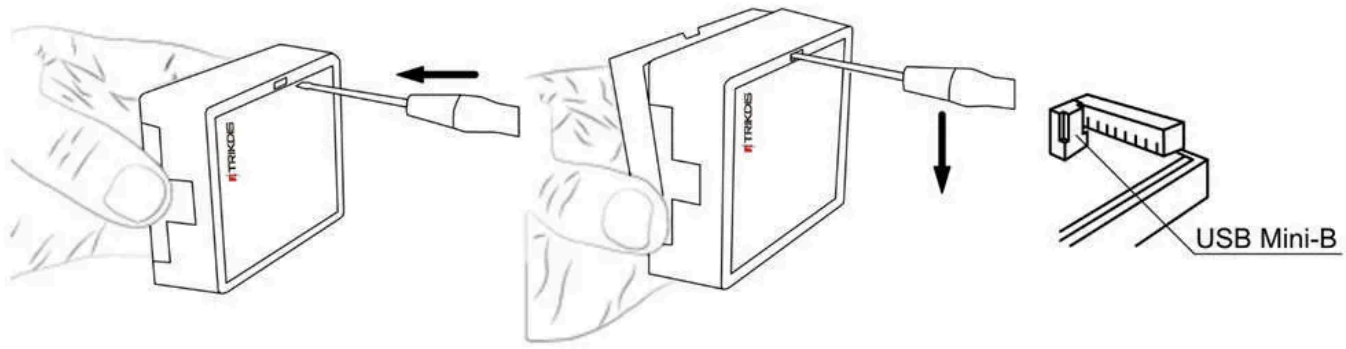
1. Pobierz i zainstaluj program TrikdisConfig. Na stronie www.trikdis.com wpisz w pole wyszukiwania „TrikdisConfig".

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. Otwórz przednią pokrywę E16T i połącz go z komputerem. Włóż płaski śrubokręt w otwór na górnej krawędzi pokrywy i, podważając w dół, delikatnie zdejmij przednią pokrywę z zatrzasków, a następnie podłącz kabel USB Mini-B. USB daje wystarczające zasilanie do programowania, osobne zasilanie nie jest potrzebne.



Rysunek 3. Zdejmowanie przedniej pokrywy i połączenie z komputerem kablem USB Mini-B.

Ostrzeżenie

Dopóki urządzenie jest podłączone kablem USB do komputera, pracuje w trybie programowania: przestaje normalnie działać, nie dozoruje, nie wysyła zdarzeń, nie da się nim sterować, jest zasilane z USB, a po odłączeniu kabla uruchamia się ponownie. Dlatego urządzenie nie może być swobodnie dostępne: musi być w zamkniętej metalowej obudowie z ochroną antysabotażową (tamper) albo z czujką ruchu dozorującą obudowę. Szczegóły w FAQ

3. Uruchom TrikdisConfig. Program rozpozna urządzenie i otworzy okno programowania. Kliknij przycisk **Read [F4]** (odczyt): program odczyta bieżące ustawienia urządzenia. Jeśli poprosi o hasło, podaj 6-cyfrowy kod administratora (fabrycznie `123456`) lub instalatora (fabrycznie `654321`).

Kolejne dwa punkty opisują, co trzeba ustawić, aby centralą alarmową można było sterować z aplikacji Protegus 2 (2.2) i aby komunikator wysyłał zdarzenia do stacji monitorowania (2.3).

2.2 Połączenie z aplikacją Protegus 2

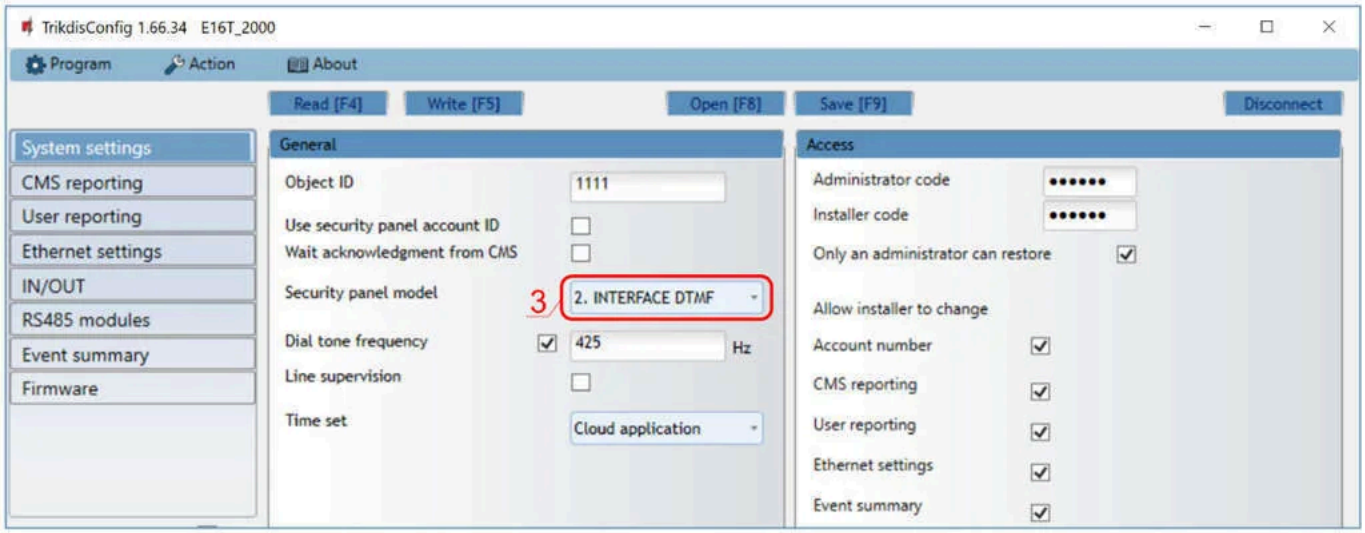
Jeśli użytkownik chce widzieć system i sterować nim z aplikacji Protegus 2, na stronie **User reporting**, w zakładce **PROTEGUS Cloud** ustaw następujące pola.



Rysunek 4. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

- 1 **Enable connection** – zaznacz: włącza połączenie z chmurą Protegus.
- 2 **Protegus Cloud access code** – zmień fabryczne hasło `123456`. To hasło trzeba będzie podać w aplikacji przy tworzeniu systemu; **po utworzeniu systemu nie można go już zmienić.**

Następnie na stronie **System settings** sprawdź typ interfejsu centrali alarmowej.



Rysunek 5. TrikdisConfig – strona System settings, grupa General.

- 3 **Security panel model** – pozostaw **2. INTERFACE DTMF** (połączenie przez linię telefoniczną z wybieraniem DTMF).

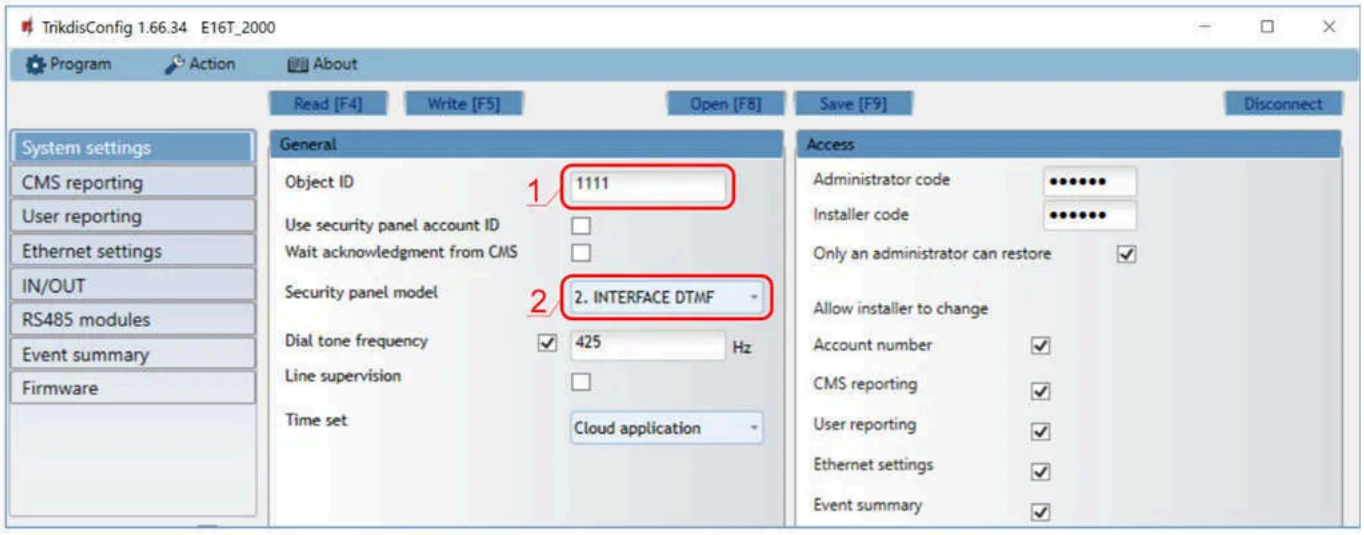
Jeśli chodzi o ustawienia sieci, na stronie **Ethernet settings** fabrycznie zaznaczone jest **Use DHCP**: urządzenie automatycznie otrzymuje adres IP od routera i w większości miejsc nie trzeba nic więcej robić. Jeśli w sieci nie ma DHCP albo trzeba użyć stałego adresu, wprowadź tu ustawienia ręczne (punkt 6.5).

Jeśli używasz urządzenia tylko z Protegus 2, bez stacji monitorowania, konfiguracja jest gotowa: naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB.

Nie zapomnij włączyć i ustawić dialera linii telefonicznej centrali alarmowej, w przeciwnym razie centrala nie wyśle zdarzeń. Ustawienia centrali opisuje rozdział 4.

2.3 Połączenie ze stacją monitorowania

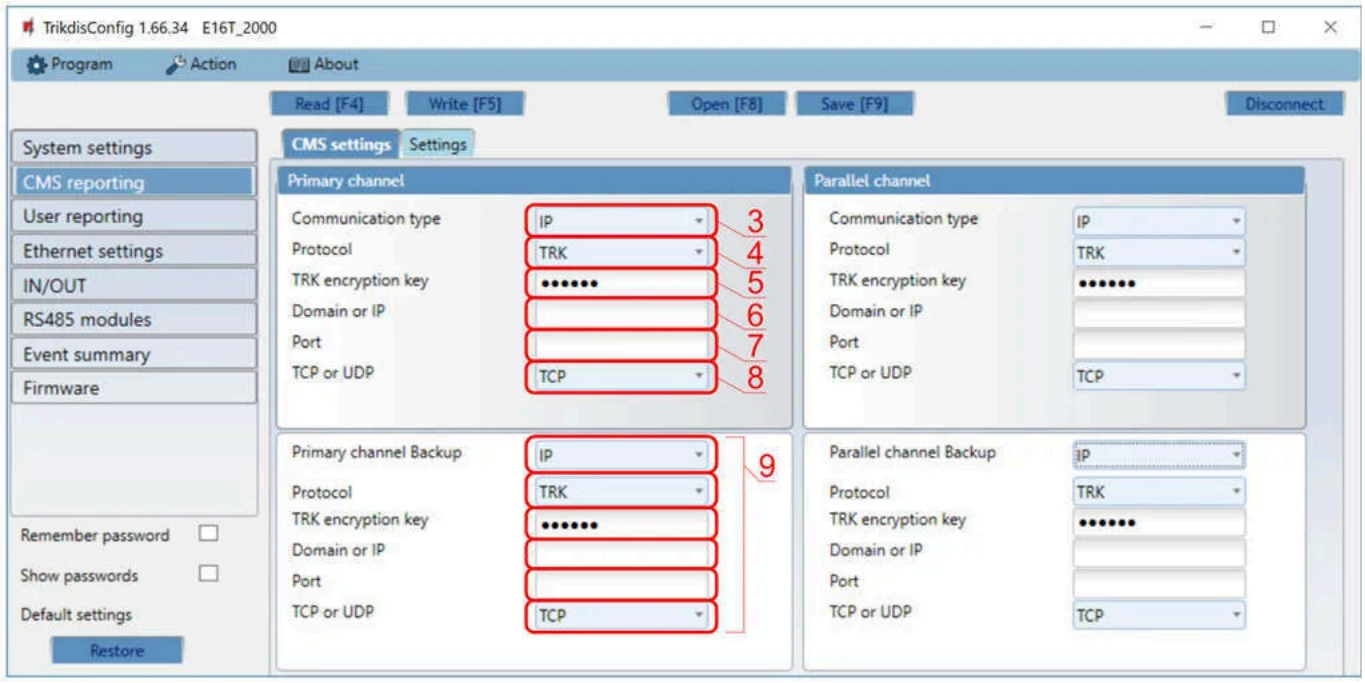
Jeśli urządzenie raportuje też do odbiornika stacji monitorowania, najpierw na stronie **System settings** wpisz identyfikator obiektu.



Rysunek 6. TrikdisConfig – strona System settings, grupa General.

- 1 **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe, 0–9, A–F). Nie można używać `FFFE` i `FFFF`.
- 2 **Security panel model** – pozostaw **2. INTERFACE DTMF**.

Następnie na stronie **CMS reporting**, w części **Primary channel** (kanał główny) ustaw dane odbiornika.



Rysunek 7. TrikdisConfig – CMS reporting, zakładka CMS settings.

- 3 **Communication type** – **IP** (w E16T dostępna jest tylko ta opcja).
- 4 **Protocol** – **TRK** dla odbiornika Trikdis, **DC-09_2007** lub **DC-09_2012** dla odbiornika uniwersalnego, **TL150** dla odbiornika SUR-GARD.
- 5 **TRK encryption key** – 6-cyfrowy klucz szyfrowania ustawiony w odbiorniku.
- 6 **Domain or IP** – nazwa domeny lub adres IP odbiornika.
- 7 **Port** – numer portu odbiornika.
- 8 **TCP or UDP** – protokół transmisji; dopasuj go do ustawień odbiornika.
- 9 **Primary channel Backup** – kanał zapasowy na wypadek awarii kanału głównego; wypełnij go tak samo, zalecamy go ustawić.

Przy protokole **DC-09** w zakładce **Settings** podaj też numer obiektu, linii i odbiornika DC-09 (punkt 6.3); przy DC-09_2012 można włączyć szyfrowanie kluczem DC-09 ustawionym w odbiorniku (uwaga w punkcie 6.3). Do sprawdzania połączenia odstęp sygnału życia (PING) ustawiasz w tej samej zakładce **Settings** (**IP ping period**, fabrycznie 30 s). Jeśli odbiornik podałeś nazwą domeny, do rozwiązywania nazw potrzebne jest też ustawienie DNS na stronie **Ethernet settings** (fabrycznie wpisany jest publiczny DNS Google). We wcześniejszym E16T pola nazywają się inaczej (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**); ich odpowiedniki podaje uwaga w punkcie 6.3.

Jeśli użytkownik korzysta też z aplikacji Protegus 2, wprowadź również ustawienia z punktu 2.2 (**User reporting → PROTEGUS Cloud**). Na koniec naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB. Urządzenie jest gotowe do podłączenia.

3. Instalacja i podłączenie

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 Kroki instalacji

1. Zdejmij przednią pokrywę (zobacz punkt 2.1) i wyciągnij listwę zaciskową.

2. Wyjmij płytkę drukowaną z tylnej części obudowy: otwórz zatrzask w rogu.
3. Przymocuj tylną część obudowy wkrętami w wybranym miejscu.
4. Włóż płytkę drukowaną z powrotem do tylnej części obudowy i wsuń z powrotem listwę zaciskową.
5. Podłącz kabel Ethernet do gniazda RJ45 (punkt 3.6).
6. Załóż z powrotem przednią pokrywę.

3.2 Miejsce montażu i sieć

- Komunikator umieść w **suchym miejscu wewnątrz budynku**, najlepiej w pobliżu obudowy centrali alarmowej, aby okablowanie było krótkie. Metalowa obudowa nie przeszkadza: E16T nie ma anteny.
- Kabel Ethernet (CAT-5 lub lepszy) do routera lub switcha może mieć **najwyżej 100 m**.
- Komunikator i kable trzymaj z dala od transformatora centrali i od przewodów sieci elektrycznej.

Odległości „do … m” to teoretyczne maksima osiągalne w idealnych warunkach. W praktyce jakość i przebieg kabla, źródła zakłóceń, a przy łączach radiowych także ściany i ukształtowanie terenu dają znacznie mniejszy zasięg. Planuj z zapasem, a przy długich odcinkach sprawdź połączenie podczas uruchomienia.

Czego wymaga sieć? Komunikator sam nawiązuje połączenie wychodzące do odbiornika stacji monitorowania i do chmury Protegus, dlatego na routerze **nie trzeba otwierać ani przekierowywać portów**, nie jest też potrzebny publiczny stały adres IP ani dynamiczny DNS. Potrzebne są:

- wolny port Ethernet na routerze lub switchu;
- DHCP (ustawienie fabryczne) albo stały adres IP, maska podsieci, brama i DNS otrzymane od administratora sieci;
- zezwolenie na ruch wychodzący na adres i port odbiornika (TCP lub UDP, zgodnie z ustawieniem odbiornika) oraz do chmury Protegus.

W sieci filtrowanej – firmowej, instytucjonalnej – uzgodnij to wcześniej z administratorem sieci: na domowych routerach wszystkie połączenia wychodzące są domyślnie dozwolone, ale w sieci chronionej zaporą może być potrzebna osobna reguła.

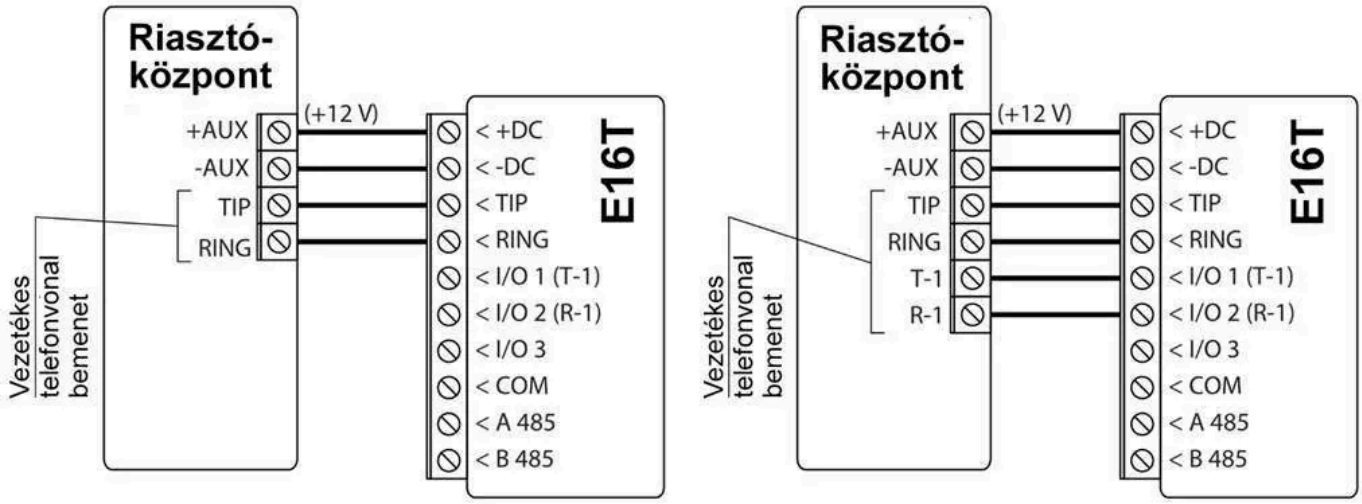
Przerwa w zasilaniu

E16T jest zasilany z centrali alarmowej, więc podczas przerwy w zasilaniu działa dalej z akumulatora centrali – router i modem zazwyczaj jednak nie, a bez nich nie ma internetu. Jeśli w tym systemie jest to nie do przyjęcia, zasilaj także urządzenia sieciowe z zasilacza bezprzerwowego (UPS) albo wybierz komunikator komórkowy (G16T).

3.3 Podłączenie do centrali alarmowej

E16T łączy się z wyjściem linii telefonicznej centrali (TIP/RING), a zasilanie otrzymuje z wyjścia zasilania pomocniczego 12 V (AUX) centrali.

Zalecane, standardowe podłączenie: DC+, DC−, TIP i RING. Wtedy komunikator nie wykryje przerwania przewodu.



Rysunek 8. Podłączenie do wyjścia linii telefonicznej centrali: po lewej podłączenie standardowe, po prawej podłączenie z nadzorem linii.

E16T pobiera podczas wysyłania najwyżej 250 mA. Sprawdź, czy wyjście AUX centrali to wytrzyma razem z pozostałymi podłączonymi urządzeniami. Ponieważ zasilanie zapewnia centrala, podczas przerwy w zasilaniu akumulator centrali zasila również komunikator.

3.3.1 W uzasadnionych przypadkach: nadzór linii

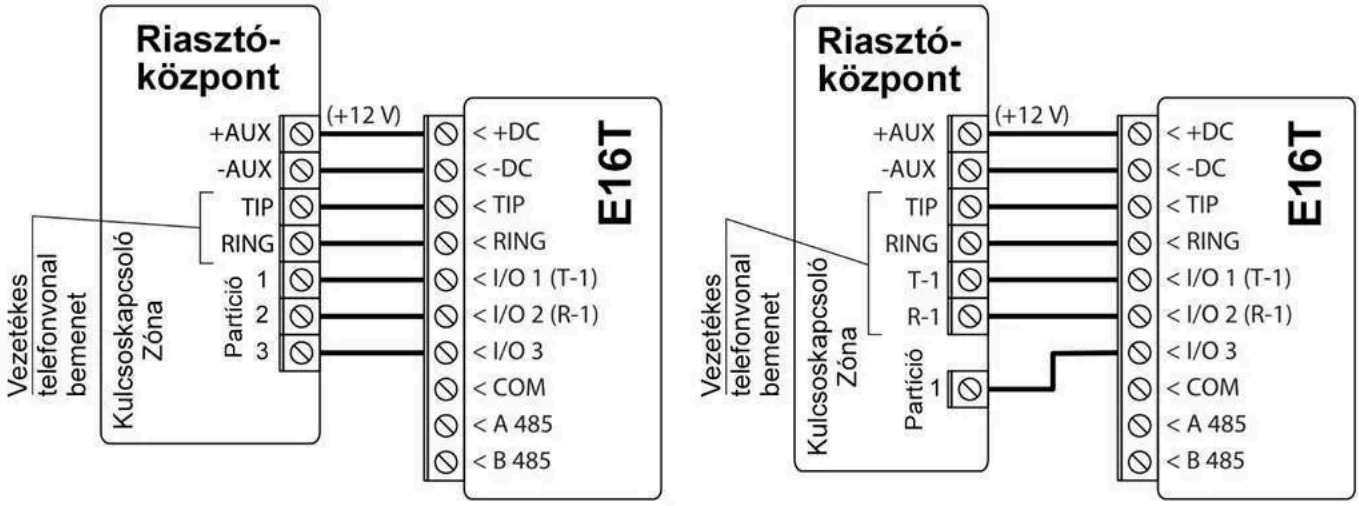
Potrzebny tylko wtedy, gdy wymagany jest nadzór linii: komunikator sygnalizuje wtedy przerwanie połączenia między nim a centralą alarmową.

1. Oprócz standardowego podłączenia podłącz też te dwa przewody: zacisk **T-1** centrali do zacisku **I/O 1 (T-1)** komunikatora, a zacisk **R-1** centrali do zacisku **I/O 2 (R-1)**.
2. Na stronie **System settings** w TrikdisConfig włącz opcję **Line supervision**.
3. Potrzebne ustawienia po stronie centrali alarmowej sprawdź w instrukcji instalacji centrali.

Wtedy I/O 1 i I/O 2 nie można używać do innych celów.

3.4 Podłączenie strefy przełącznika kluczowego

Jeśli chcesz zdalnie uzbrajać i rozbrajać centralę z aplikacji Protegus 2, ustaw jeden z zacisków I/O komunikatora jako **wyjście** i podłącz go do **strefy przełącznika kluczowego** centrali. Po aktywacji wyjście zwiera strefę do COM (minusa); rezystor końcowy strefy podłącz zgodnie z typem strefy centrali. Ponieważ E16T ma trzy zaciski I/O, można obsługiwać nawet trzy partycje, każdą osobnym wyjściem.



Rysunek 9. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego: po lewej podłączenie standardowe, po prawej podłączenie z nadzorem linii (wtedy do przełącznika kluczowego pozostaje I/O 3).

Strefa przełącznika kluczowego może być impulsowa lub dwustanowa – w aplikacji Protegus 2 trzeba ustawić ten sam tryb (punkt 5.2). Szczegóły i pułapki uzbrajania przełącznikiem kluczowym opisuje osobny artykuł: Zdalne uzbrajanie przełącznikiem kluczowym z aplikacji Protegus 2.

Wcześniejszy E16T

We wcześniejszym E16T (2 wejścia + OUT) typ i tryb wyjścia ustawia się w grupie **System settings** → **Output** w TrikdisConfig: do uzbrajania przełącznikiem kluczowym **OUT type** ustaw na **Remote Control**, a **OUT mode** na **Pulse** (z długością impulsu) lub **Level** – zgodnie z typem strefy centrali.

3.5 Podłączenie wejść

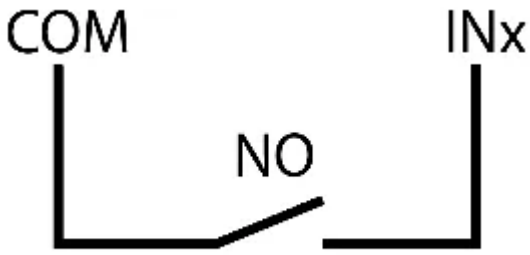
Zaciski I/O komunikatora mogą jako wejścia przyjmować też dodatkowe czujki (np. styk sabotażowy, przycisk napadowy, termostat), niezależnie od centrali alarmowej. Wejście podłącza się między wybrany zacisk I/O a zacisk COM.

Wejścia obsługują następujące typy obwodów: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Rezystor końca linii ma wartość **2,2 kΩ**. Przy pojedynczej parametryzacji (EOL) zarówno zwarcie, jak i przerwa są traktowane jako alarm; podwójna parametryzacja (DEOL) z dwoma rezystorami rozróżnia alarm i sabotaż (zwarcie lub przerwa). Ustawienie fabryczne to NO (normalnie otwarte); typ wejścia ustawiasz na stronie **IN/OUT** programu TrikdisConfig, zgodnie z podłączeniem.

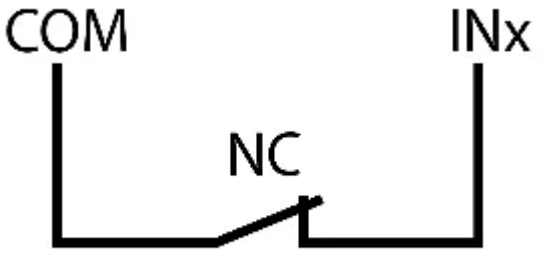
Typ	Stan spoczynkowy	Alarm	Sabotaż
NC	zamknięty	otwarty	–
NO	otwarty	zamknięty	–
NC/EOL	2,2 kΩ	przerwa lub zwarcie	–
NO/EOL	2,2 kΩ	zwarcie lub przerwa	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	przerwa lub zwarcie
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	przerwa lub zwarcie

Po naruszeniu wejścia komunikator wysyła własne zdarzenie do stacji monitorowania i do Protegus 2; kod Contact ID zdarzenia, numer partycji i strefy możesz podać na stronie **IN/OUT**.

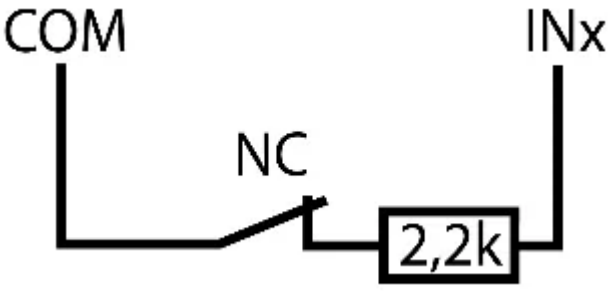
Podłączenie obwodów wejściowych: typy NC, NO, EOL i DEOL z rezystorem końcowym 2,2 kΩ, przy typach DEOL z obwodem sabotażowym.



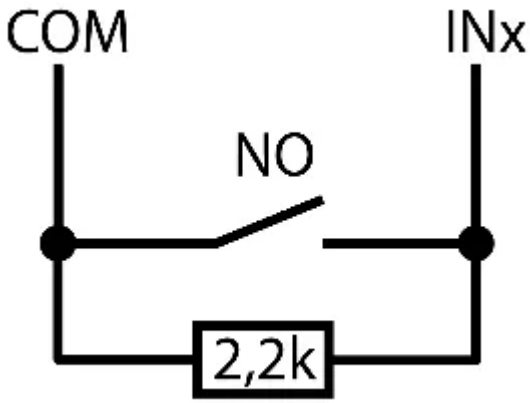
Rysunek 10. NO – obwód normalnie otwarty: zamknięty – alarm, otwarty – stan spoczynkowy.



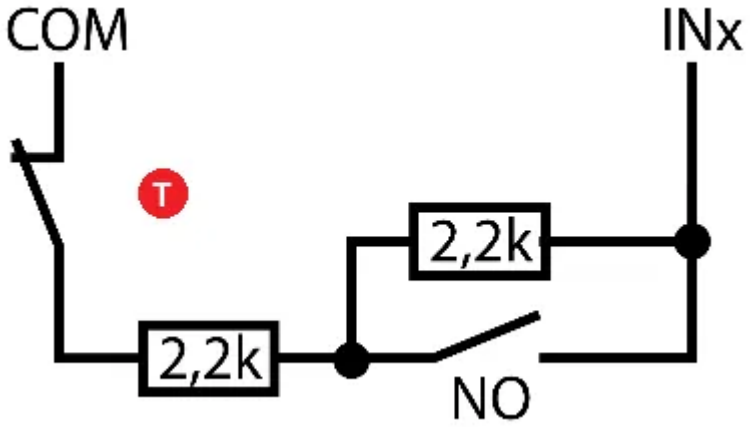
Rysunek 11. NC – obwód normalnie zamknięty: otwarty – alarm, zamknięty – stan spoczynkowy.



Rysunek 12. NC/EOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.

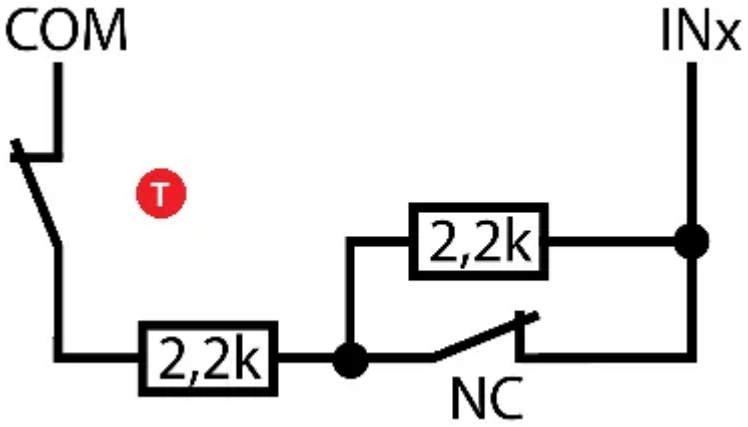


Rysunek 13. NO/EOL – obwód normalnie otwarty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.



Rysunek 14. NO/DEOL – obwód normalnie otwarty z rezystorem końcowym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – alarm, 3,3–5,5 kΩ – stan spoczynkowy.

- T styk sabotażowy („Tamper"), sygnalizuje otwarcie obudowy czujki



Rysunek 15. NC/DEOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – stan spoczynkowy, 3,3–5,5 kΩ – alarm.

- T styk sabotażowy („Tamper"), sygnalizuje otwarcie obudowy czujki

Wcześniejszy E16T

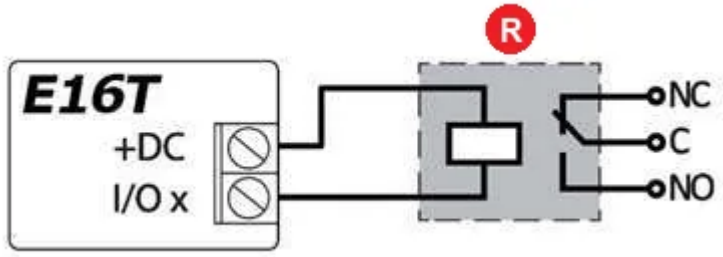
Dwa wejścia (IN1, IN2) wcześniejszego E16T (2 wejścia + OUT) przyjmują obwody typu NO, NC lub EOL; ustawienie fabryczne to NO. Typ wejścia ustawia się tam nie na stronie IN/OUT, lecz na stronie **Event summary** w TrikdisConfig (uwaga w punkcie 6.6). Podłączenie jest takie samo: wejście podłącz zgodnie z wybranym typem (NO, NC, EOL).

3.6 Podłączenie kabla Ethernet

Jeden koniec kabla Ethernet podłącz do gniazda RJ45 na płytce drukowanej E16T, a drugi do wolnego portu routera lub switcha. Potrzebny jest zwykły kabel prosty (patch); kabel wchodzi przez górny otwór obudowy. Nawiązanie połączenia z siecią po włączeniu pokazuje zielone światło diody **NETWORK**.

3.7 Podłączenie wyjścia z przekaźnikiem

Zaciski I/O jako wyjścia są wyjściami typu otwarty kolektor (OC): w stanie aktywnym zwierają podłączone obciążenie do minusa, z prądem najwyżej 0,15 A, do 30 V DC. Większe odbiorniki lub urządzenia zasilane napięciem sieciowym przełączaj **przez przekaźnik**: jeden koniec cewki przekaźnika podłącz do +DC, drugi do zacisku I/O. Diodę sygnalizacyjną można podłączyć do wyjścia bezpośrednio: z +DC przez szeregowy rezystor 2,2 kΩ do diody, a drugą nóżkę diody do zacisku I/O (we wcześniejszym E16T do zacisku OUT).



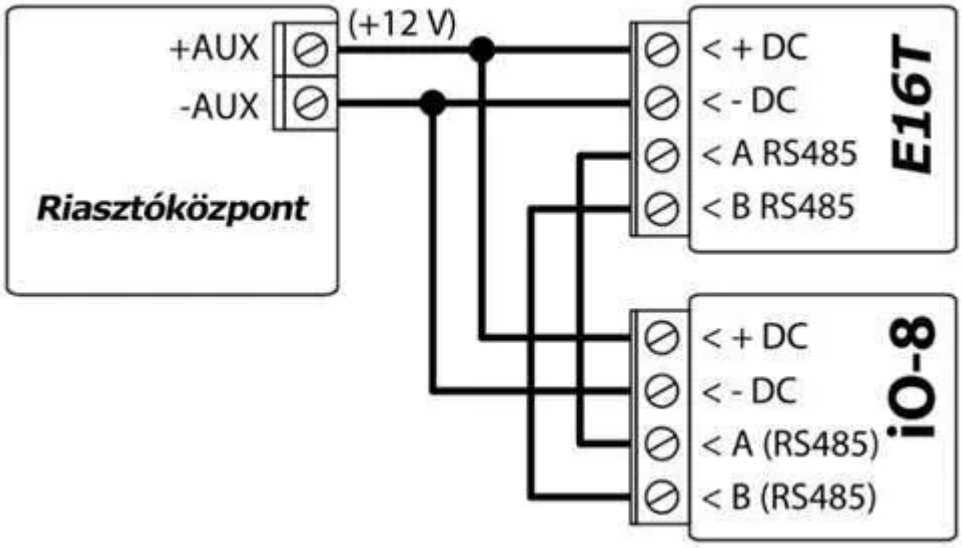
Rysunek 16. Podłączenie przekaźnika do wyjścia komunikatora: cewka jest między +DC a zaciskiem I/O x, a styki (NC, C, NO) przełączają odbiornik.

- R przekaźnik („Relay")

Wyjściami możesz sterować z aplikacji Protegus 2 (rozdział 5).

3.8 Podłączenie ekspandera iO-8

Jeśli potrzeba więcej wejść lub wyjść, do magistrali RS485 E16T można podłączyć najwyżej cztery ekspandery **iO-8**; każdy daje 8 kolejnych I/O o podwójnej funkcji. Zaciski A 485 i B 485 połącz z zaciskami A i B modułu, a zasilanie modułu weź z 12 V centrali. Magistrala RS485 może mieć najwyżej 100 m – to teoretyczne maksimum, zobacz uwagę w punkcie 3.2. Moduł trzeba dodać na stronie **RS485 modules** w TrikdisConfig (punkt 6.7). Tu można też podłączyć pozostałe urządzenia serii iO (iO, iO-WL, iO-LO, LO-MOD); moduły W485 i E485 nie są przeznaczone do E16T, bo sam E16T jest urządzeniem z przewodowym internetem.



Rysunek 17. Podłączenie ekspandera iO-8 do magistrali RS485 E16T; zasilanie z wyjścia AUX centrali alarmowej.

3.9 Włączenie i pierwsze sprawdzenie

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.

Po podłączeniu komunikator uruchamia się razem z włączeniem centrali alarmowej. Na przedniej pokrywie powinieneś zobaczyć:

- **POWER** świeci na zielono – zasilanie prawidłowe;
- **NETWORK** świeci na zielono – połączono z siecią lokalną;
- **TROUBLE** nie świeci.

Jeśli TROUBLE miga, liczba mignięć wskazuje przyczynę (punkt 1.6): 1 = brak fizycznego połączenia (kabel, port), 2 = brak adresu IP (DHCP), 3 = błąd DNS, 6 = brak połączenia z odbiornikiem. Jeśli żadna dioda nie świeci, sprawdź zasilanie i okablowanie.

4. Programowanie centrali alarmowej

Aby centrala alarmowa wysyłała zdarzenia przez swoje wyjście linii telefonicznej, trzeba włączyć i skonfigurować jej dialer (komunikator telefoniczny). Dokładne adresy programowe znajdziesz w instrukcji instalatora centrali; istota ustawień jest u wszystkich producentów taka sama:

1. **Włącz komunikator telefoniczny (PSTN)** w centrali.
2. **Jako numer telefonu podaj** `1234` dla odbiornika stacji monitorowania – niezależnie od tego, czy komunikator jest podłączony do zacisków RING/TIP centrali, czy do linii telefonicznej. Z innym numerem zdarza się, że centrala wybiera numer, a komunikator mimo to nie otrzymuje zdarzeń: także w przypadku centrali DSC PowerSeries NEO transmisja ruszyła dopiero po zmianie numeru na `1234`.
3. **Tryb wybierania:** DTMF (tonowy), nie impulsowy.
4. **Protokół:** Contact ID.

Jeśli chcesz uzbrajać i rozbrajać centralę zdalnie za pomocą wyjścia komunikatora, strefę podłączoną do tego wyjścia trzeba ustawić w centrali jako **strefę typu klucz**.

Strefa typu klucz może być impulsowa lub bistabilna. Wyjście komunikatora domyślnie podaje impuls o długości 3 sekund; długość impulsu lub tryb bistabilny możesz zmienić w ustawieniach aplikacji Protegus 2.

4.1 Programowanie dialera Honeywell Vista

Na manipulatorze wejdź w tryb programowania instalatora i ustaw następujące pola programowe:

Pole programowe	Ustawienie
`*41`	numer telefonu odbiornika stacji monitorowania: `1234`
`*43`	identyfikator obiektu centrali
`*47`	Tone dial = `1` oraz liczba prób wybierania
`*48`	`7` (domyślnie)
`*49`	`5` (komunikat Split/Dual)
`*50`	opóźnienie wysłania alarmu włamaniowego – domyślnie `2,0` (30 s); do natychmiastowego wysłania `0,0`

W centrali **Honeywell Vista 48** ustaw dodatkowo następujące pola programowe:

Pole programowe	Wartość	Pole programowe	Wartość	Pole programowe	Wartość
`*41`	1234 (numer telefonu odbiornika)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (identyfikator obiektu)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

Na końcu programowania wyjdź z trybu programowania poleceniem `*99`.

4.2 Centrale innych producentów

W instrukcji instalatora każdej centrali szukaj tych samych czterech ustawień: włączenie komunikatora linii telefonicznej, numer telefonu odbiornika, tryb wybierania (DTMF) i format komunikacji (Contact ID). Jeśli centrala przed wybieraniem oczekuje sygnału zgłoszenia (dial tone), zapewnia go E16T; jeśli połączenie mimo to się nie rozpoczyna, wyłącz w centrali wykrywanie sygnału zgłoszenia (opcja „wybieranie bez sygnału zgłoszenia" lub podobna).

Jeśli centrala na końcu połączenia sygnalizuje błąd, choć zdarzenie dotarło, sprawdź ustawienie **Wait acknowledgment from CMS** na stronie **System settings** w TrikdisConfig: gdy jest włączone, komunikator kończy połączenie dopiero po potwierdzeniu odbiornika stacji monitorowania (kiss-off). W systemie bez stacji monitorowania, tylko z Protegus 2, pozostaw je wyłączone (to ustawienie fabryczne), bo nie ma odbiornika, który mógłby potwierdzić.

5. Zdalne sterowanie aplikacją Protegus 2

Dzięki aplikacji mobilnej i webowej Protegus 2 użytkownik zdalnie widzi stan systemu, otrzymuje powiadomienia o zdarzeniach, może uzbrajać i rozbrajać system oraz sterować wyjściami komunikatora.

5.1 Dodawanie urządzenia

Przed dodaniem urządzenia sprawdź:

1. E16T jest podłączony do sieci i ma dostęp do internetu: dioda **NETWORK** świeci na zielono, a dioda **DATA** gaśnie po zdarzeniu lub raporcie testowym.
2. Na stronie **User reporting** → **PROTEGUS Cloud** w TrikdisConfig (punkt 6.4) zaznaczone jest **Enable connection** – czyli chmura Protegus jest włączona – i ustawiony jest **Protegus Cloud access code** (po utworzeniu systemu nie można go już zmienić).
3. Dioda **POWER** świeci na zielono.

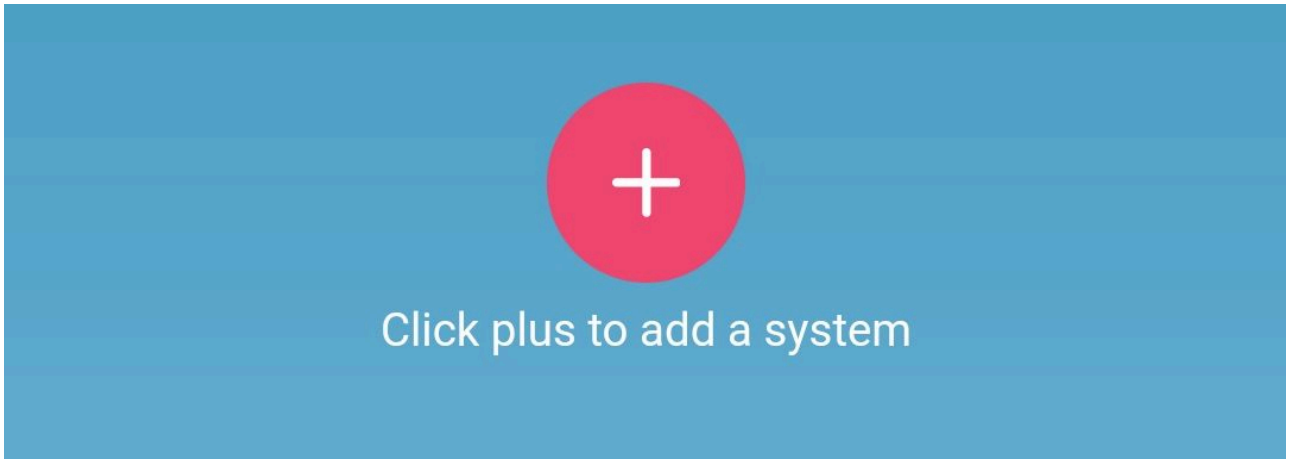
Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie działa do routera – ale nie to, że urządzenie ma też dostęp do internetu. Jeśli dioda NETWORK jest zielona, a dioda DATA świeci ciągle także po zdarzeniu lub raporcie testowym, połączenie z internetem nie działa: komunikat nie może zostać wysłany. W sieci komórkowej najczęściej winny jest APN albo usługa transmisji danych karty SIM, przy Ethernecie router, zapora sieciowa (firewall) lub DNS. Jeśli dioda DATA zgaśnie, komunikat został wysłany, a połączenie danych działa prawidłowo.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



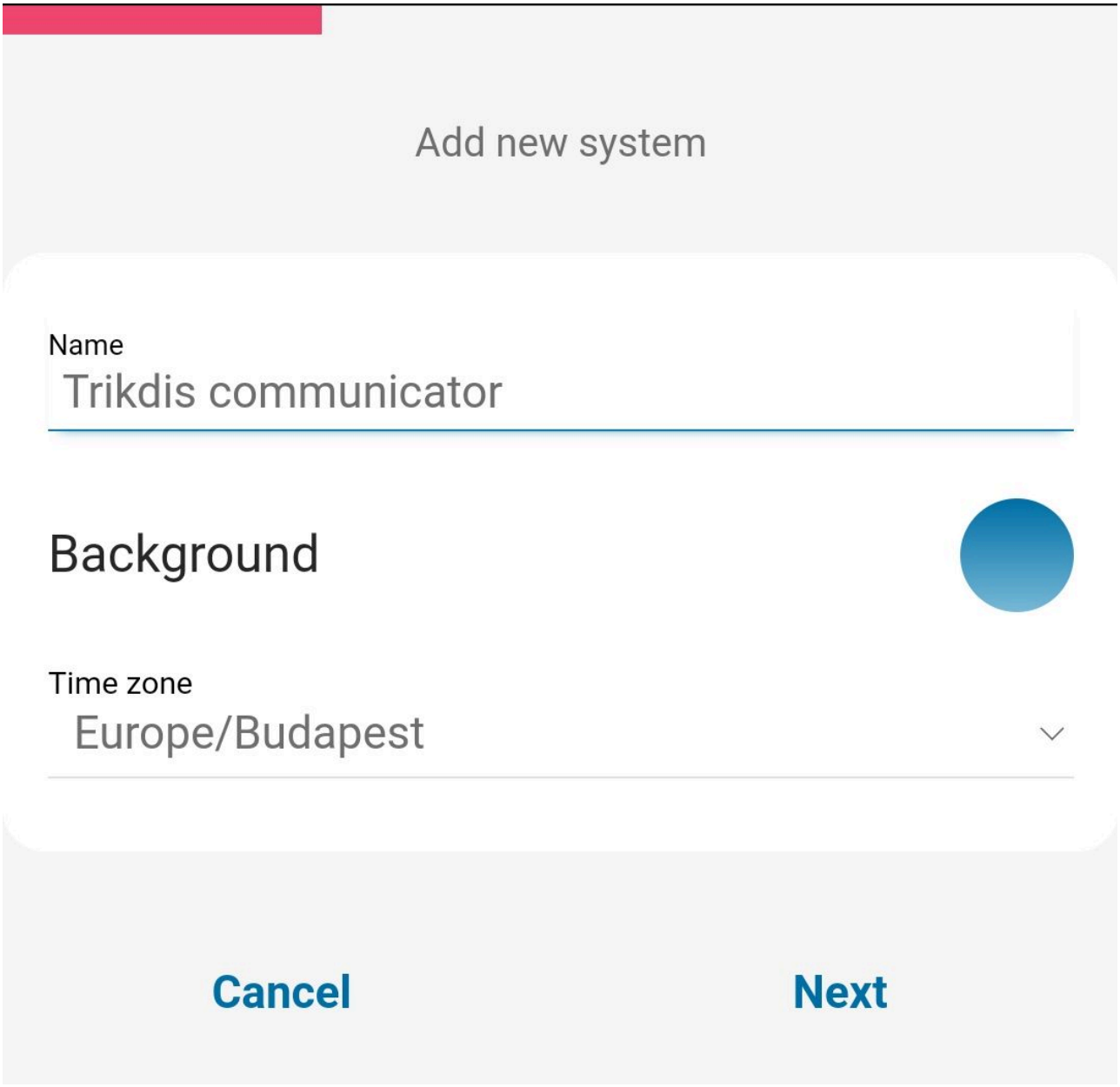
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



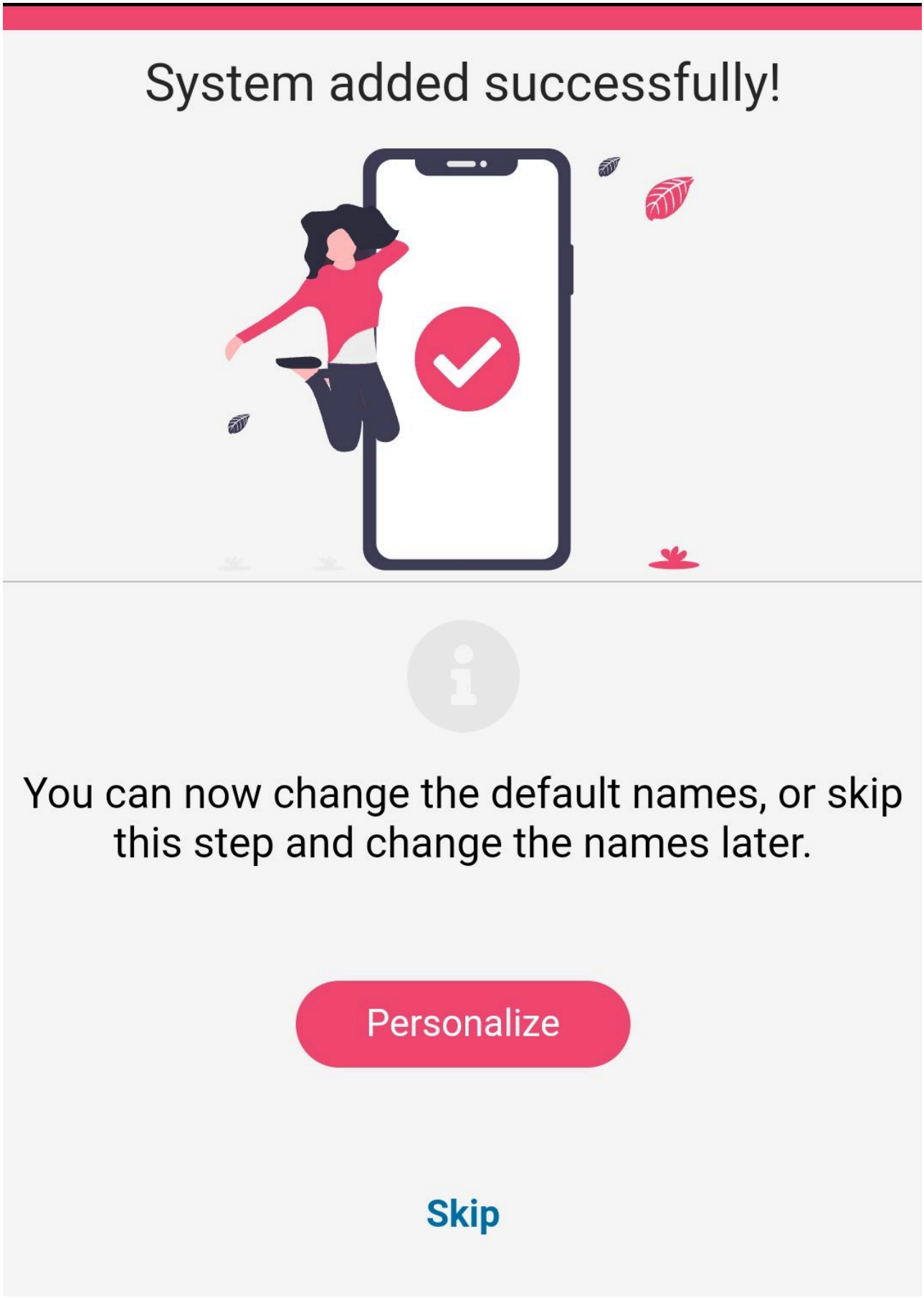
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



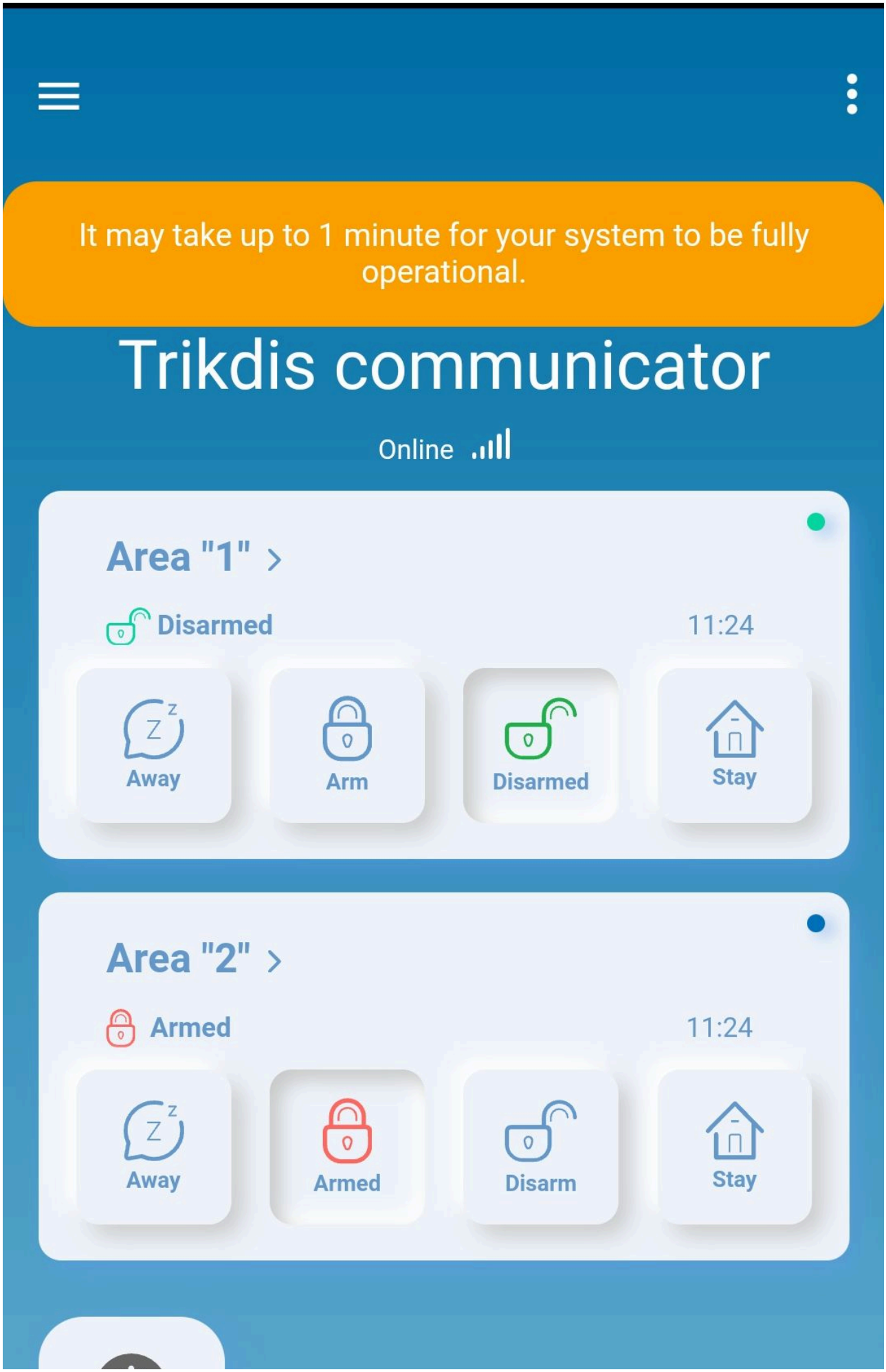
6. Add meg a rendszer nevét és válassz idozónát



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



Unikalnym identyfikatorem urządzenia w E16T jest **adres MAC**: znajdziesz go na pudełku i z tyłu urządzenia, pokazuje go też TrikdisConfig (**MAC / Unique ID**).

5.2 Uzbrajanie i rozbrajanie wyjściem

Jeśli chcesz uzbrajać i rozbrajać centralę alarmową za pomocą wyjścia komunikatora, przez strefę typu klucz centrali, w aplikacji Protegus 2 podaj przy partycji, które wyjście nią steruje.

Strefa centrali, do której podłączone jest wyjście komunikatora, musi być zaprogramowana w centrali jako **strefa typu klucz**, a centrala musi raportować zdarzenia uzbrojenia i rozbrojenia – na ich podstawie Protegus 2 pokazuje stan partycji.

Ustawienie możesz wprowadzić podczas tworzenia systemu, przy dodawaniu partycji, albo później w ustawieniach systemu, przy edycji partycji. Podczas tworzenia systemu prowadzi cię kreator Protegus 2: kliknij przycisk **Continue** (Dalej), podaj nazwę partycji (**Area name**) i włącz sterowanie wyjściem PGM z aplikacji Protegus 2 – odbywa się to w poniższych krokach:

1. Wybierz (lub dodaj) partycję, którą chcesz sterować. Numer partycji musi być zgodny z tym, który centrala wysyła w zdarzeniach (partycja 1 to 1, partycja 2 to 2).
2. Włącz opcję **Control with Protegus2** (sterowanie przez PGM) i w polu **Assigned Output** (wyjście) wybierz wyjście komunikatora (PGM1, PGM2 …). Jedno wyjście może sterować tylko jedną partycją.
3. Wybierz tryb działania: **Pulse** (impulsowy) lub **Level** (bistabilny) – ten sam, który ustawiłeś w centrali dla strefy typu klucz. Zwykle używamy trybu impulsowego; można też podać długość impulsu (domyślnie 3 s).
4. Zapisz ustawienie (**Save**). Przy kilku partycjach powtórz to dla każdej, z jej własnym wyjściem: w kreatorze kolejną partycję dodajesz przyciskiem **Click to add an area** i tak samo ustawiasz jej wyjście PGM. Gdy ustawisz wszystkie partycje, przejdź dalej w kreatorze przyciskiem **Skip**.

Protegus 2 może poprawnie pokazywać stan partycji tylko wtedy, gdy centrala wysyła zdarzenia uzbrojenia i rozbrojenia z właściwym numerem partycji. Szczegółom i pułapkom uzbrajania przez strefę typu klucz poświęcony jest osobny artykuł: Zdalne uzbrajanie przez strefę typu klucz z aplikacji Protegus 2.

5.3 Uzbrajanie i rozbrajanie z aplikacji

1. Otwórz system w aplikacji Protegus 2. Na ekranie startowym każda partycja ma własną kartę i kłódkę: **zamknięta, czerwona kłódka** oznacza partycję uzbrojoną, **otwarta, zielona kłódka** – rozbrojoną.
2. Stuknij kłódkę partycji i wybierz żądaną operację: uzbrojenie lub rozbrojenie.
3. Jeśli aplikacja o to poprosi, wprowadź kod PIN.

Kłódka przyjmuje rzeczywisty stan na podstawie zdarzenia odebranego z centrali alarmowej; aplikacja potwierdza też na liście zdarzeń i w powiadomieniu, czy centrala wykonała operację.

6. TrikdisConfig – szczegółowe ustawienia

Po lewej stronie okna TrikdisConfig widać listę stron (System settings, CMS reporting, User reporting, Ethernet settings, IN/OUT, RS485 modules, Event summary, Firmware), u góry pasek przycisków (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), a na dole pasek stanu. Ten rozdział omawia ustawienia E16T strona po stronie.

6.1 Pasek stanu

Po podłączeniu urządzenia i odczytaniu go (**Read [F4]**) na dole okna widać najważniejsze dane urządzenia:

Etykieta	Znaczenie
IMEI / Unique ID, w urządzeniu z Ethernetem **MAC / Unique ID**	Unikalny identyfikator urządzenia: w urządzeniu z kartą SIM numer IMEI, w urządzeniu z Ethernetem adres MAC. Ten sam identyfikator jest podany na pudełku i na tylnej ściance urządzenia.
Status	Bieżący stan pracy.
Device	Typ urządzenia (oznaczenie modelu). Sprawdź, czy widnieje tu typ twojego urządzenia.
SN	Numer seryjny.
BL	Wersja bootloadera.
FW	Wersja firmware.
HW	Wersja sprzętu.
State	Sposób połączenia: USB lub zdalne (remote).
Administrator / Installer	Poziom dostępu osoby programującej (po wprowadzeniu hasła).

Po wprowadzeniu ustawień zapisujesz je w urządzeniu przyciskiem **Write [F5]**; przyciskami **Open [F8]** i **Save [F9]** możesz zapisać cały zestaw ustawień do pliku i wczytać go do innego urządzenia. **Save [F9]** zapisuje ustawienia do pliku konfiguracyjnego, a **Open [F8]** otwiera zapisany plik; zapisane ustawienia możesz później wczytać także do innych urządzeń, dzięki czemu szybko skonfigurujesz wiele urządzeń z identycznymi ustawieniami.

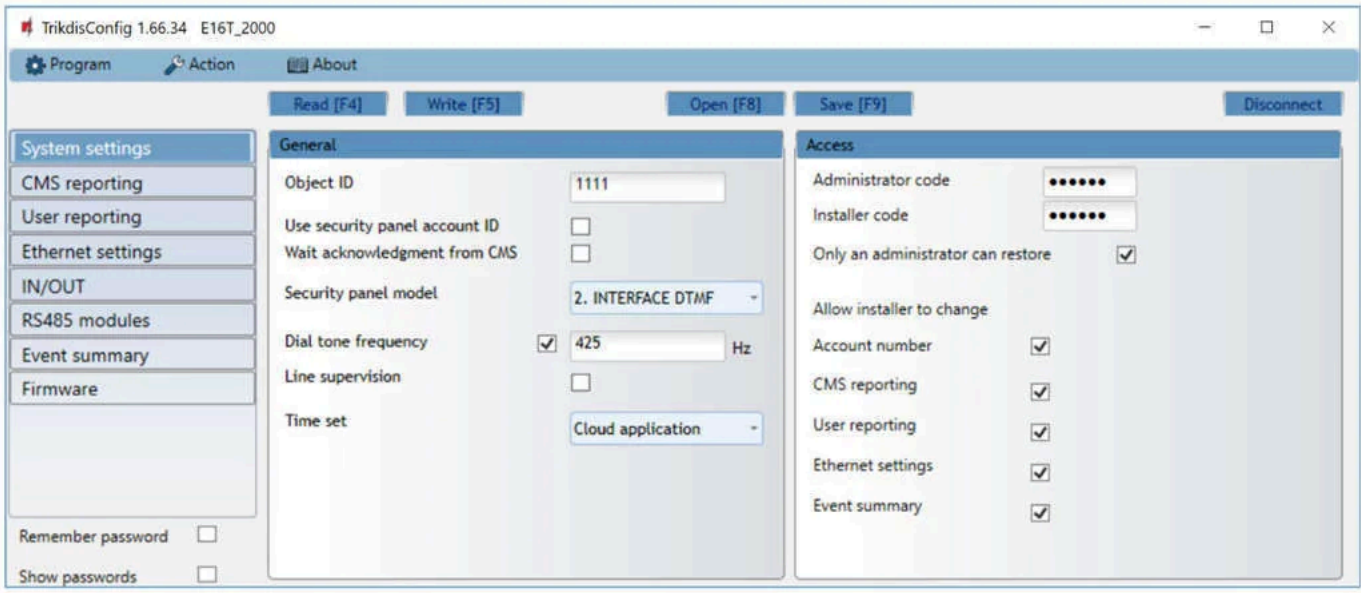


Rysunek 18. Pasek stanu TrikdisConfig z odczytanym E16T: po lewej przycisk przywracania ustawień fabrycznych i MAC / Unique ID, na dole stan, typ, numer seryjny, wersje, sposób połączenia i poziom dostępu.

Po **Read [F4]** program odczytuje i pokazuje ustawienia zapisane w urządzeniu; w polu **Device** powinien być widoczny typ urządzenia (E16T; przy v2 **E16T_2000**). Ustawienia wprowadź zgodnie z poniższymi opisami stron.

6.2 System settings

Strona składa się z dwóch grup: w grupie **General** ustawiasz podstawowe działanie urządzenia, w grupie **Access** – poziomy dostępu.



Rysunek 19. TrikdisConfig – strona System settings: grupy General i Access.

- **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe: 0–9, A–F; nie można używać `FFFE` i `FFFF`). Obowiązkowy, jeśli urządzenie raportuje też do stacji monitorowania.
- **Use security panel account ID** – po zaznaczeniu komunikator używa nie własnego Object ID, lecz identyfikatora wysłanego przez centralę w komunikacie Contact ID. Przydatne, gdy kilka partycji raportuje z osobnymi identyfikatorami.
- **Wait acknowledgment from CMS** – po zaznaczeniu komunikator po każdym zdarzeniu czeka na potwierdzenie odbiornika i dopiero potem wysyła do centrali sygnał zakończenia (kiss-off). Jeśli potwierdzenia nie ma, centrala wysyła zdarzenie ponownie. W systemie bez stacji monitorowania, tylko z Protegus 2, pozostaw wyłączone (ustawienie fabryczne).
- **Security panel model** – typ interfejsu linii telefonicznej; domyślnie **2. INTERFACE DTMF**. Tym ustawieniem włączasz lub wyłączasz interfejs linii telefonicznej DTMF komunikatora.
- **Dial tone frequency** – częstotliwość sygnału zgłoszenia, który E16T podaje centrali (domyślnie 425 Hz, standardowy sygnał zgłoszenia w Polsce i w większości krajów europejskich).
- **Line supervision** – nadzór przewodów między centralą a komunikatorem; wymaga także podłączenia przewodów T-1 i R-1 (punkt 3.3.1).
- **Time set** – źródło czasu zegara urządzenia (domyślnie **Cloud application**, chmura Protegus).

Wcześniejszy E16T

We wcześniejszym E16T strona System settings ma też dodatkowe grupy:

- **General** → **Test period** – okresowy raport testowy jest wysyłany w podanych tu odstępach (w v2 jest to na zakładce **CMS reporting** → **Settings**).
- Grupa **Ethernet settings** (w v2 osobna strona, punkt 6.5): **Internal MAC** – unikalny identyfikator urządzenia, adres MAC; **Use DHCP** – po zaznaczeniu urządzenie automatycznie rejestruje się w sieci; jeśli automatyczna rejestracja się nie powiedzie, wypełnij ręcznie pola **Internal IP address**, **Mask** (maska podsieci), **Gateway** (brama) i **DNS**.
- Grupa **Output** (w v2 strona IN/OUT, punkt 6.6): **OUT type** – działanie wyjścia wybrane z listy: Disabled (wyłączone), LAN OK (sieć w porządku), Communication Trouble (błąd komunikacji), Remote Control (zdalne sterowanie z aplikacji Protegus); **Inverted** – po zaznaczeniu wyjście działa odwrotnie; **OUT mode**: **Pulse** – wyjście pozostaje w nowym stanie przez czas (w sekundach) podany w polu **Pulse Time**, **Level** – stan utrzymuje się do następnego polecenia; **Pulse time** – długość impulsu w sekundach; w trybie Pulse wyjście przełącza się na ten czas.

W grupie **Access** zarządzasz poziomami dostępu i hasłami.

Do ustawień urządzenia istnieją dwa poziomy dostępu: **administrator** i **instalator**.

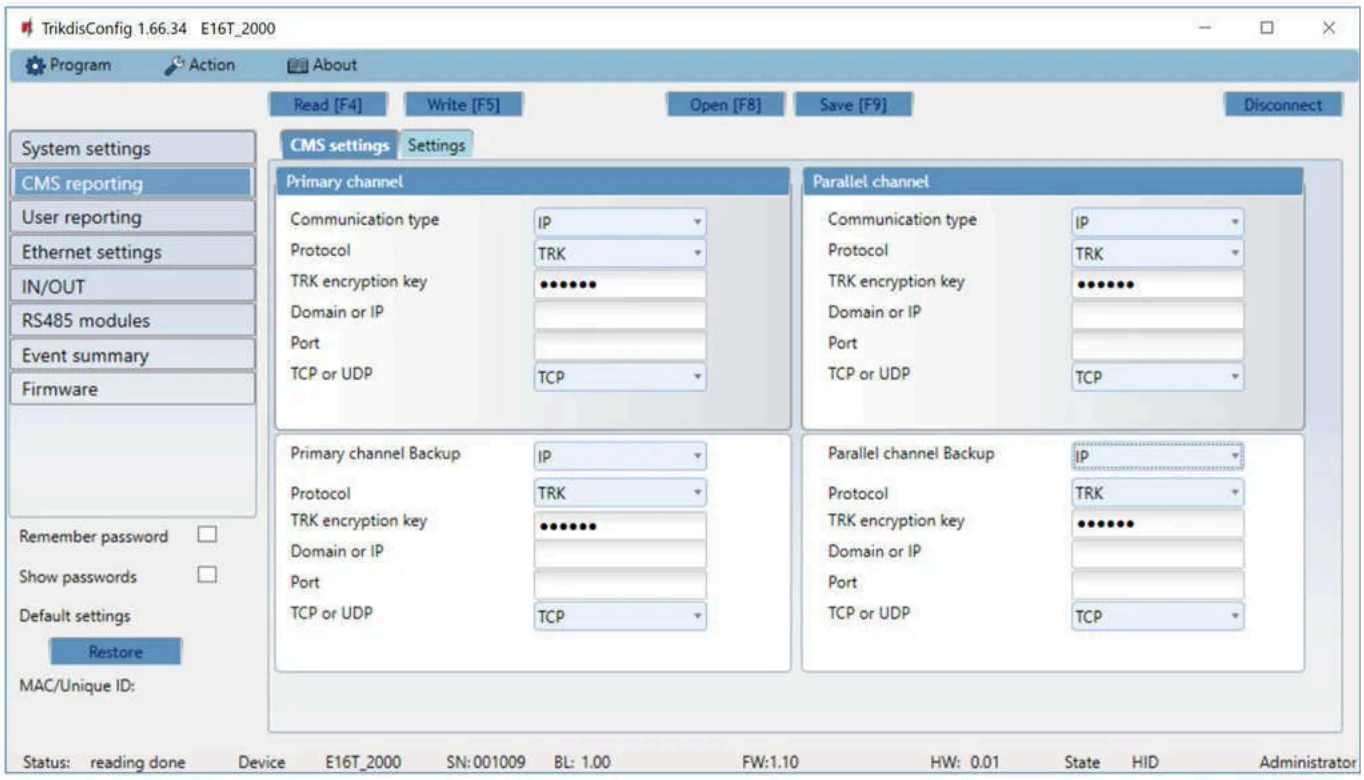
- **Administrator code** – dostęp do wszystkich ustawień (hasło fabryczne: `123456`; hasło ma 6 znaków: cyfry lub litery łacińskie).
- **Installer code** – dostęp, który można ograniczyć (hasło fabryczne: `654321`).
- **Only an administrator can restore** – po zaznaczeniu przywrócenie ustawień fabrycznych może uruchomić tylko administrator.
- **Allow installer to change** – tutaj wskazujesz, które grupy ustawień może zmieniać instalator: **Account number** (identyfikator obiektu), **CMS reporting**, **User reporting**, **SIM card** (w urządzeniu z siecią komórkową) lub **Ethernet settings** (w urządzeniu z Ethernetem), **Event summary**.

Nie zostawiaj w urządzeniu haseł fabrycznych!

Przy uruchomieniu zmień co najmniej hasło administratora i zapisz je w bezpiecznym miejscu. Zapomnianego hasła nie da się usunąć nawet przywróceniem ustawień fabrycznych, bo do tego także potrzebne jest hasło: wtedy zresetować je może tylko producent lub dystrybutor, po dostarczeniu mu urządzenia. Wyjątkiem jest urządzenie ze sprzętowym przyciskiem RESET: przytrzymanie przycisku przez 10 sekund przywraca ustawienia fabryczne bez hasła.

6.3 CMS reporting

Komunikator wysyła zdarzenia do stacji monitorowania przez połączenie IP. Zdarzenia mogą iść kilkoma kanałami: kanał **główny** i **równoległy** działają jednocześnie (do dwóch odbiorników naraz), a do każdego z nich należy kanał **zapasowy**, który włącza się, gdy dany kanał zostanie przerwany. Komunikacja jest szyfrowana i chroniona hasłem; do odbioru i przekazywania do oprogramowania stacji monitorowania potrzebny jest odbiornik Trikdis (programowy odbiornik IPcom dla Windows lub Linux, sprzętowy odbiornik IP/SMS RL14, wielokanałowy odbiornik RM14) albo odbiornik uniwersalny obsługujący protokół DC-09 / TL150.



Rysunek 20. TrikdisConfig – CMS reporting, zakładka CMS settings: kanał główny, zapasowy i równoległy.

Primary channel – kanał główny

- **Communication type** – w E16T dostępne jest tylko **IP**.
- **Protocol** – TRK (odbiorniki Trikdis), DC-09_2007 lub DC-09_2012 (odbiorniki uniwersalne), TL150 (SUR-GARD).
- **TRK encryption key** – 6-cyfrowy klucz szyfrowania; w komunikatorze i w odbiorniku musi być taki sam.
- **Domain or IP**, **Port** – adres odbiornika (nazwa domeny lub adres IP) i jego numer portu sieciowego.
- **TCP or UDP** – protokół transmisji, w którym wysyłane są zdarzenia (zgodnie z ustawieniem odbiornika).

Primary channel Backup – kanał zapasowy. Przejmuje komunikację, gdy kanał główny nie działa; ustawienia są takie same jak powyżej. Warto go ustawić także w urządzeniu przewodowym – na przykład drugi adres lub port odbiornika – bo kanał zapasowy obejdzie też awarię po stronie odbiornika.

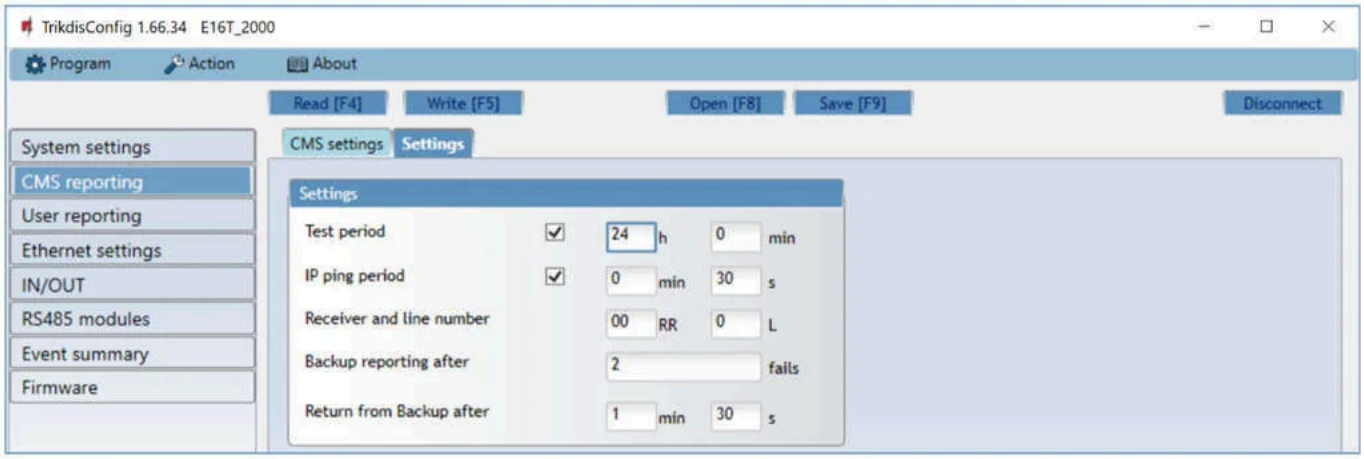
Parallel channel – kanał równoległy. Oprócz kanału głównego wysyła jednocześnie do drugiego odbiornika (na przykład do lokalnej i centralnej stacji monitorowania). Ma własny kanał zapasowy.

Wcześniejszy E16T

We wcześniejszym E16T TrikdisConfig pokazuje to samo na zakładce **CMS Reporting** okna **Reporting**, z innymi nazwami pól:

- Grupa **Primary**: **Enable** – po zaznaczeniu kanał główny do stacji monitorowania jest aktywny; **Remote Host** – nazwa domeny lub adres IP odbiornika; **Remote Port** – numer portu sieciowego odbiornika; **TCP or UDP** – protokół transmisji; **PING Time** – włącz i podaj odstęp między sygnałami życia (wartość fabryczna 30) – potrzebne do nadzoru połączenia; **Encryption key** – 6-cyfrowy klucz szyfrowania, taki sam w komunikatorze i w odbiorniku.
- Grupa **Backup**: **Enable** – włącza kanał zapasowy, który wysyła, gdy połączenie główne zostanie przerwane; pozostałe pola są takie same jak przy kanale głównym.

- Grupa **Settings**: **TCP protocol** – kodowanie wysyłki: TRK (do odbiornika Trikdis), DC-09_2007 lub DC-09_2012 (do odbiornika uniwersalnego).
- Grupa **SIA IP parameter** – można ją zmieniać tylko wtedy, gdy w polu **TCP protocol** jest DC-09_2007 lub DC-09_2012: **Encryption enabled** – przy DC-09_2012 można włączyć szyfrowanie; **DC09-2012 encryption key** – klucz szyfrowania ustawiony w odbiorniku; **DC09-2012 receiver No.** – numer odbiornika; **DC-09 line No.** – numer linii odbiornika; **Use time stamp** – po zaznaczeniu komunikat zawiera też czas (znacznik czasu).



Rysunek 21. TrikdisConfig – CMS reporting, zakładka Settings: raport testowy, PING, numer odbiornika i linii (Receiver and line number: RR = numer odbiornika, L = numer linii) oraz czasy kanału zapasowego.

Na zakładce **Settings** ustawiasz czasy oraz numer odbiornika i linii; grupa DC-09 jest potrzebna tylko wtedy, gdy wysyłasz protokołem DC-09 (na zrzucie ekranu z 2022 roku jeszcze jej nie widać).

- **Test period** – odstęp czasu między okresowymi raportami testowymi (domyślnie 24 godziny). Raport testowy trafia jako komunikat Contact ID do stacji monitorowania i do Protegus 2.
- **IP ping period** – odstęp czasu między sygnałami życia (PING) na kanale IP (domyślnie 30 s). Włączasz go zaznaczeniem pola wyboru, a czas podajesz w polach minut (**min**) i sekund (**s**); jest niezbędny do nadzoru połączenia. Odbiornik nie przekazuje sygnałów PING do oprogramowania stacji monitorowania, aby go nie przeciążać; oprogramowanie dostaje komunikat dopiero wtedy, gdy odbiornik nie otrzyma sygnału PING przez trzykrotność ustawionego czasu. Jeśli na przykład okres PING wynosi 3 minuty, utrata połączenia zostanie zgłoszona po 9. minucie.
- **Backup reporting after** – po tylu nieudanych próbach wysłania urządzenie przełącza się na kanał zapasowy (domyślnie 2).
- **Return from Backup after** – po takim czasie urządzenie wraca na kanał główny (domyślnie 1 min 30 s).

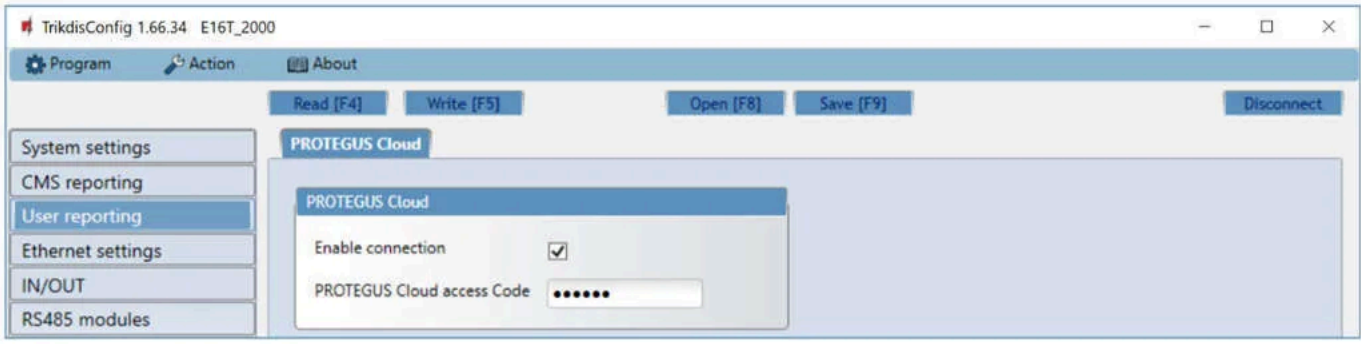
PING utrzymuje aktywne połączenie między urządzeniem a odbiornikiem i od niego zależy również zdalny dostęp, sterowanie i programowanie. Dlatego **nie zalecamy okresu PING dłuższego niż 5 minut**.

DC-09 Settings (po prawej stronie karty) – wypełniasz tylko wtedy, gdy na którymś kanale wysyłasz protokołem DC-09_2007 lub DC-09_2012; grupa pojawia się, gdy w polu **Protocol** któregoś kanału wybrano DC-09_2007 lub DC-09_2012:

- **Object ID in DC-09** – szesnastkowy identyfikator o długości 3–16 znaków, nadaje go stacja monitorowania.
- **DC-09 line No** – numer linii.
- **DC-09 receiver No.** – numer odbiornika.

6.4 User reporting

Na zakładce **PROTEGUS Cloud** włączasz usługę Protegus. E16T nie ma powiadomień SMS ani sterowania SMS, dlatego na tej stronie jest tylko ta jedna zakładka.



Rysunek 22. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

- **Enable connection** – włącza połączenie z chmurą Protegus i zdalny dostęp TrikdisConfig.
- **Protegus Cloud access code** – 6-cyfrowy kod do połączenia z Protegus (fabrycznie `123456`). Jeśli go zmieniłeś, ten kod trzeba podać przy dodawaniu systemu w Protegus 2. Można go ustawić tylko przed utworzeniem systemu w Protegus 2, później nie można go zmienić.

6.5 Ethernet settings

Tu ustalasz, jak E16T ma łączyć się z siecią lokalną.



Rysunek 23. TrikdisConfig – strona Ethernet settings; fabrycznie włączone jest DHCP.

- **Use DHCP** – po zaznaczeniu urządzenie automatycznie otrzymuje adres IP, maskę podsieci i bramę z serwera DHCP routera. To ustawienie fabryczne i w większości miejsc nie trzeba nic więcej robić. Jeśli w sieci nie ma DHCP, jeśli automatyczne logowanie do sieci się nie udaje albo administrator sieci wymaga stałego adresu, odznacz pole i wypełnij ręcznie poniższe pola oraz serwery nazw:
- **Static IP** – stały adres IP urządzenia w sieci lokalnej (adres, którego nie używa inne urządzenie i który leży poza zakresem DHCP).
- **Subnet mask** – maska podsieci.
- **Default gateway** – brama domyślna, zwykle adres routera. Przy błędnej bramie urządzenie ma dostęp do sieci lokalnej, ale nie do internetu.
- **DNS 1, DNS 2** – serwery nazw; za ich pomocą urządzenie odnajduje chmurę Protegus i odbiornik podany nazwą domeny. Fabrycznie wpisany jest publiczny DNS Google; jeśli sieć pozwala na ruch na zewnątrz tylko do własnego serwera nazw, wpisz tutaj adres lokalnego DNS. 3 błyski diody TROUBLE oznaczają błąd DNS.

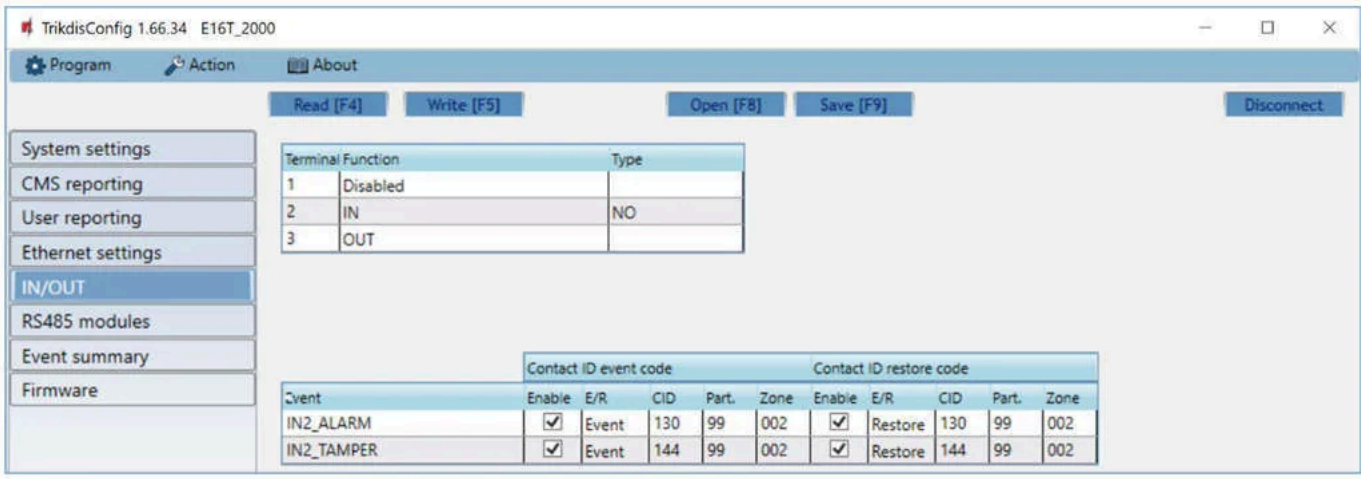
Unikalny identyfikator urządzenia, adres MAC (w programie **Internal MAC**), w nowszym oknie TrikdisConfig nie jest widoczny na tej stronie, lecz na dole okna, w polu **MAC / Unique ID** paska stanu.

Urządzenie nawiązuje tylko połączenia **wychodzące** do odbiornika i do chmury Protegus, dlatego na routerze nie trzeba otwierać ani przekierowywać portów i nie jest potrzebny publiczny stały adres IP.

We wcześniejszym E16T adres MAC pokazuje pole **Internal MAC** w grupie Ethernet settings na stronie **System settings** (uwaga w punkcie 6.2).

6.6 IN/OUT

Tu ustalasz rolę trzech zacisków I/O o podwójnej funkcji: **Disabled** (nieużywany), **IN** (wejście) lub **OUT** (wyjście). Przy wejściu trzeba też podać typ (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).



Rysunek 24. TrikdisConfig – strona IN/OUT: funkcja zacisków I/O i zdarzenia wejść.

Po naruszeniu czujki podłączonej do wejścia komunikator wysyła własne zdarzenie (**INx_ALARM**, Contact ID 130), a po naruszeniu obwodu sabotażowego – zdarzenie sabotażu (**INx_TAMPER**, 144) do stacji monitorowania i do Protegus 2; w tabeli pojawiają się zdarzenia każdego zacisku ustawionego jako wejście. Kolumny tabeli:

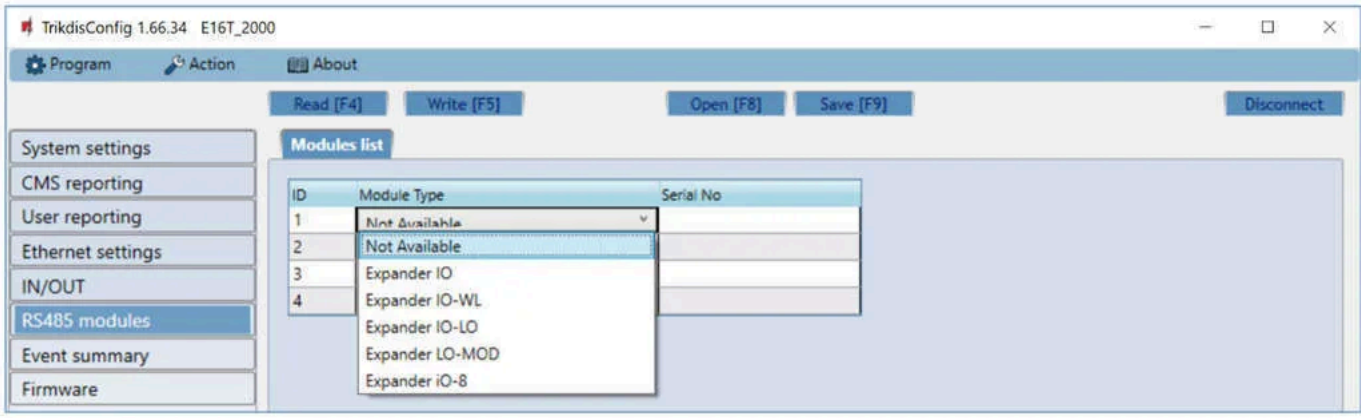
- **Enable** – włącza wysyłanie komunikatu.
- **E/R** – typ zdarzenia: Event (alarm) lub Restore (powrót do normy).
- **CID** – kod Contact ID.
- **Part.** – numer partycji w komunikacie.
- **Zone** – numer strefy w komunikacie.

Wcześniejszy E16T

We wcześniejszym E16T nie ma strony IN/OUT: typ i zdarzenia dwóch wejść ustawiasz w grupie **Input description** na stronie **Event summary**. **Partition** – numer partycji; **Contact ID** – kod zdarzenia (może pozostać wartość fabryczna), przy naruszeniu wejścia ten kod jest wysyłany do Protegus i do stacji monitorowania; **Zone No.** – numer strefy, który trafia do komunikatów; **Type** – typ wejścia (NO, NC, EOL); **Enable / Alarm** – po zaznaczeniu raportuje naruszenie wejścia (zdarzenie); **Enable / Restore** – po zaznaczeniu raportuje powrót wejścia do normy. Ustawienie wyjścia jest w grupie **System settings** → **Output** (uwaga w punkcie 6.2).

6.7 RS485 modules

Ekspandery iO-8 i inne ekspandery serii iO podłączone do magistrali RS485 trzeba dodać na zakładce **Modules list**.

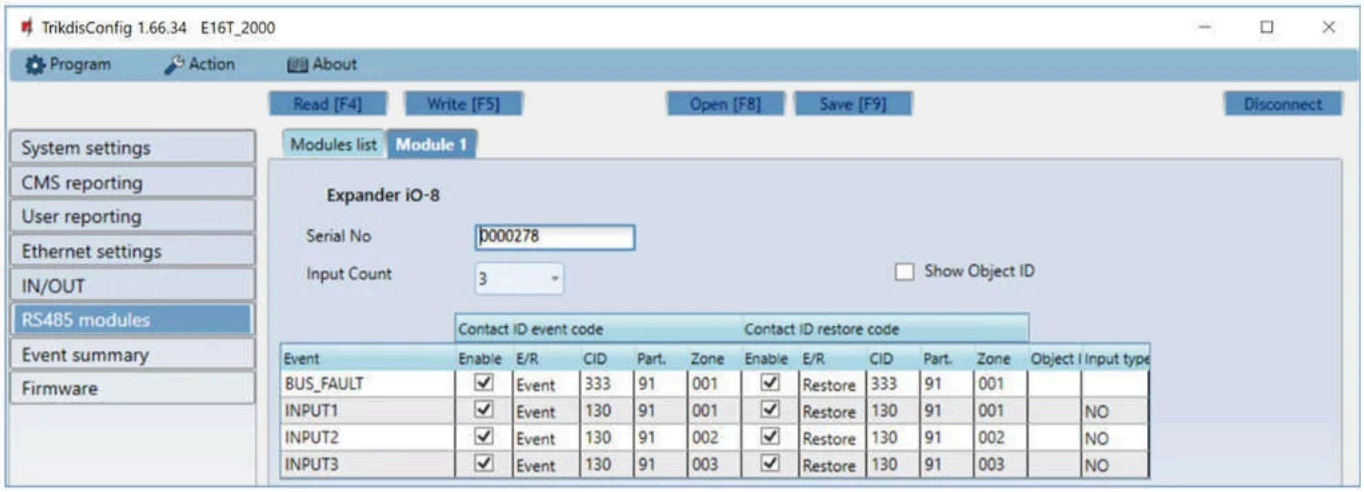


Rysunek 25. TrikdisConfig – RS485 modules, zakładka Modules list: dostępne typy modułów.

- **Module Type** – typ podłączonego modułu z listy (Expander iO-8, IO, IO-WL, IO-LO, LO-MOD).
- **Serial No** – 6-cyfrowy numer seryjny modułu (na module i na jego pudełku, SN).

Po wybraniu modułu i podaniu numeru seryjnego naciśnij przycisk **Write [F5]**, odłącz kabel USB i odczekaj minutę, aż komunikator zarejestruje moduł. Następnie podłącz kabel z powrotem, odczytaj urządzenie (**Read [F4]**), a na stronie RS485 modules pojawi się własna, numerowana zakładka modułu.

Ekspander iO-8 – 8 I/O o podwójnej funkcji; do komunikatora można podłączyć najwyżej 4 moduły.



Rysunek 26. TrikdisConfig – RS485 modules, zakładka modułu iO-8.

- **Input Count** – ile zacisków ma być wejściami; pozostałe będą wyjściami. Typ wejścia (**Input type**: NO lub NC) można podać w tabeli. Rolę wyjść (uzbrajanie / rozbrajanie lub przełączanie urządzenia) ustawiasz w aplikacji Protegus 2.
- W tabeli możesz przypisać kody Contact ID do usterki magistrali (**BUS_FAULT**, Contact ID 333) oraz do zdarzeń naruszenia i powrotu do normy wejść (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Domyślnie 1. moduł raportuje z partycją 91, a 4. moduł z partycją 94. Po zaznaczeniu **Show Object ID** można dla wejść podać identyfikator obiektu inny niż komunikatora.

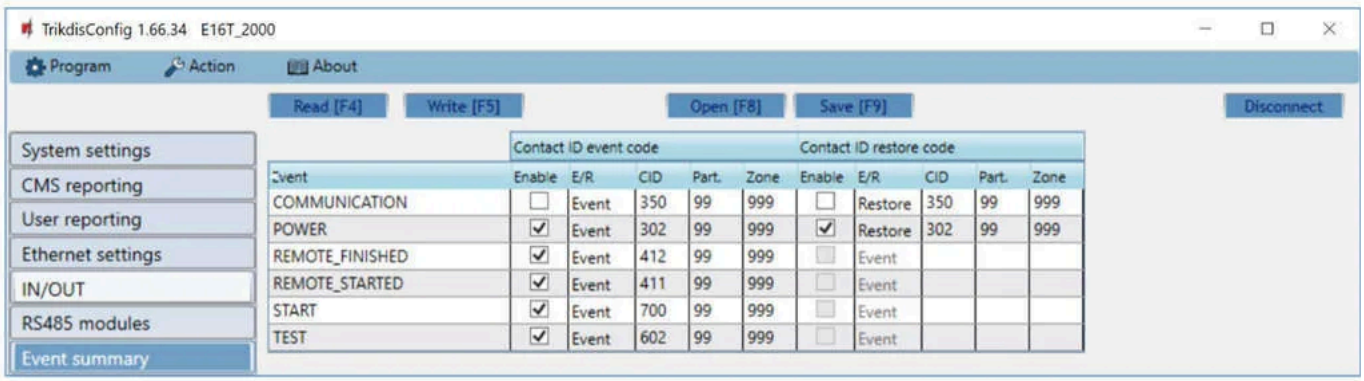
6.8 Event summary

Na tej stronie włączasz lub wyłączasz **własne, wewnętrzne komunikaty** urządzenia oraz zmieniasz ich kod Contact ID, numer partycji i strefy. Komunikatu wyłączonego tutaj urządzenie nie wysyła żadnym kanałem. Fabrycznie komunikaty są wysyłane z partycją 99 i strefą 999.

Komunikat	Contact ID	Kiedy powstaje
COMMUNICATION	350	Przerwana komunikacja między komunikatorem a centralą alarmową (fabrycznie wyłączony). Komunikator podłączony do magistrali lub portu szeregowego wykrywa ją bezpośrednio; komunikator podłączony do linii telefonicznej – tylko przy włączonym **Line supervision**.
POWER	302	Nieprawidłowe (niskie) napięcie zasilania; jego powrót to osobny komunikat.
REMOTE_STARTED	411	Rozpoczęło się zdalne programowanie za pomocą TrikdisConfig.
REMOTE_FINISHED	412	Zdalne programowanie zostało zakończone.
START	700	Urządzenie połączyło się z siecią (uruchomienie).
TEST	602	Okresowy raport testowy.
PING	760	Komunikat życia PING. Nie występuje na liście każdego urządzenia: na ekranie wcześniejszej wersji sprzętowej tak, na stronie Event summary nowszych wersji nie ma takiego wiersza. Jego odstęp ustawiasz w polu **CMS reporting** → **Settings** → **IP ping period**.

- **Enable** – zezwala na wysyłanie komunikatu do stacji monitorowania i do Protegus 2.
- **E/R** – typ komunikatu: Event (zdarzenie) lub Restore (przywrócenie) – dany wiersz oznacza wystąpienie zdarzenia lub jego przywrócenie.
- **Part.** – numer partycji (obszaru), który urządzenie wysyła przy zdarzeniu wewnętrznym i przy przywróceniu.
- **Zone** – numer strefy, który urządzenie wysyła przy zdarzeniu wewnętrznym i przy przywróceniu.
- Kod **CID**, **partycję** i **strefę** można zmienić przy każdym zdarzeniu; tam, gdzie istnieje przywrócenie (Restore), jego kod można podać osobno.

Zdarzenia własnych wejść (**INx_ALARM**, **INx_TAMPER**) ustawia się na stronie **IN/OUT**, a zdarzenia modułów rozszerzeń (**BUS_FAULT**, **INPUTx**) na stronie **RS485 modules**, na karcie danego modułu. Włączenie raportu testowego i jego odstęp ustawia się w polu **CMS reporting** → **Settings** → **Test period**.



Rysunek 27. TrikdisConfig – strona Event summary: komunikaty wewnętrzne urządzenia.

We wcześniejszym E16T na tej stronie są też ustawienia wejść (uwaga w punkcie 6.6).

6.9 Przywracanie ustawień fabrycznych

Aby przywrócić ustawienia fabryczne, kliknij przycisk **Restore** w grupie **Default settings**, w lewej dolnej części okna TrikdisConfig. Przywrócenie usuwa wszystkie ustawienia – także hasła – dlatego warto wcześniej zapisać ustawienia do pliku (**Save [F9]**).

Z hasłem instalatora jest to możliwe tylko wtedy, gdy administrator nie zablokował tego na stronie **System settings → Access**.

7. Zdalne programowanie

TrikdisConfig łączy się z urządzeniami Trikdis nie tylko kablem USB, ale także **zdalnie, przez chmurę Protegus**. Dzięki temu możesz zmieniać ustawienia już zamontowanego urządzenia bez wyjazdu na miejsce.

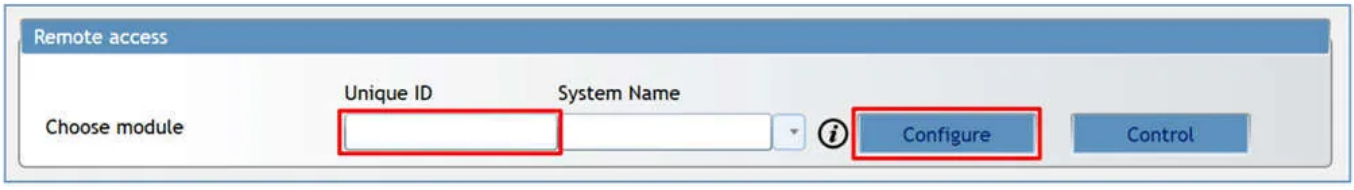
Do zdalnego dostępu potrzebne jest:

1. Urządzenie musi być włączone i mieć połączenie z siecią (diody **POWER** i **NETWORK** świecą na zielono; w urządzeniu z siecią komórkową dioda NETWORK miga też na żółto). W urządzeniu z siecią komórkową włożona karta SIM musi być aktywna, a jej kod PIN musi być wpisany w urządzeniu albo żądanie kodu PIN musi być wyłączone; w urządzeniu z Ethernetem kabel sieciowy (LAN) musi być podłączony, a urządzenie musi mieć dostęp do internetu.
2. Na stronie **User reporting → PROTEGUS Cloud** programu TrikdisConfig musi być zaznaczone **Enable connection** (ustaw to przez USB, przy pierwszym uruchomieniu).
3. Musisz znać **unikalny identyfikator** urządzenia (IMEI lub MAC – podany na pudełku i na tylnej ściance urządzenia) oraz hasło administratora lub instalatora.

Kroki:

1. Uruchom program TrikdisConfig.
2. W części **Remote access**, w polu **Unique ID** wpisz unikalny identyfikator urządzenia (IMEI lub MAC).
3. Opcjonalnie nadaj systemowi nazwę w polu **System name** – program ją zapamięta i następnym razem wybierzesz ją z listy rozwijanej.
4. Naciśnij przycisk **Configure**.
5. W otwartym oknie kliknij przycisk **Read [F4]** (odczyt) i podaj hasło. Po zaznaczeniu **Remember password** program zapamięta je na czas tej sesji.
6. Wprowadź zmiany, a następnie przyciskiem **Write [F5]** (zapis) wyślij je do urządzenia.

Systemy wcześniej programowane zdalnie i opatrzone nazwą program zapisuje; możesz je wyświetlić strzałką obok pola **System name**. Aby usunąć wpis, zaznacz identyfikator na liście, naciśnij klawisz **Delete** i potwierdź.



Rysunek 28. TrikdisConfig – Remote access: identyfikator urządzenia (w E16T adres MAC), nazwa systemu i przycisk Configure.

Włączenie usługi Protegus opisuje punkt 6.4, a pobieranie TrikdisConfig – punkt 2.1.

8. Sprawdzenie działania komunikatora

Po zaprogramowaniu i podłączeniu zawsze sprawdź cały łańcuch: centrala alarmowa → komunikator → stacja monitorowania i/lub Protegus 2.

Wcześniej sprawdź, czy jest zasilanie (dioda **POWER** świeci na zielono) i czy jest połączenie z siecią (dioda **NETWORK** świeci na zielono).

1. **Wywołaj zdarzenie.** Uzbrój, a następnie rozbrój system z manipulatora albo przy uzbrojonym systemie narusz strefę, aby powstał alarm.
2. **Sprawdź, czy zdarzenie dotarło.** Zobacz, czy zdarzenie pojawiło się w oprogramowaniu stacji monitorowania i/lub na liście zdarzeń aplikacji Protegus 2 – z właściwym numerem partycji i strefy.
3. **Wejścia.** Narusz czujkę podłączoną do własnego wejścia komunikatora i sprawdź odpowiadające jej zdarzenie.
4. **Wyjścia.** Przełącz wyjście z aplikacji Protegus 2 i sprawdź, czy podłączone do niego urządzenie (przekaźnik, strefa typu klucz) rzeczywiście zadziała.
5. **Zdalne uzbrajanie.** Jeśli centralą można sterować zdalnie, uzbrój ją i rozbrój także z aplikacji Protegus 2.

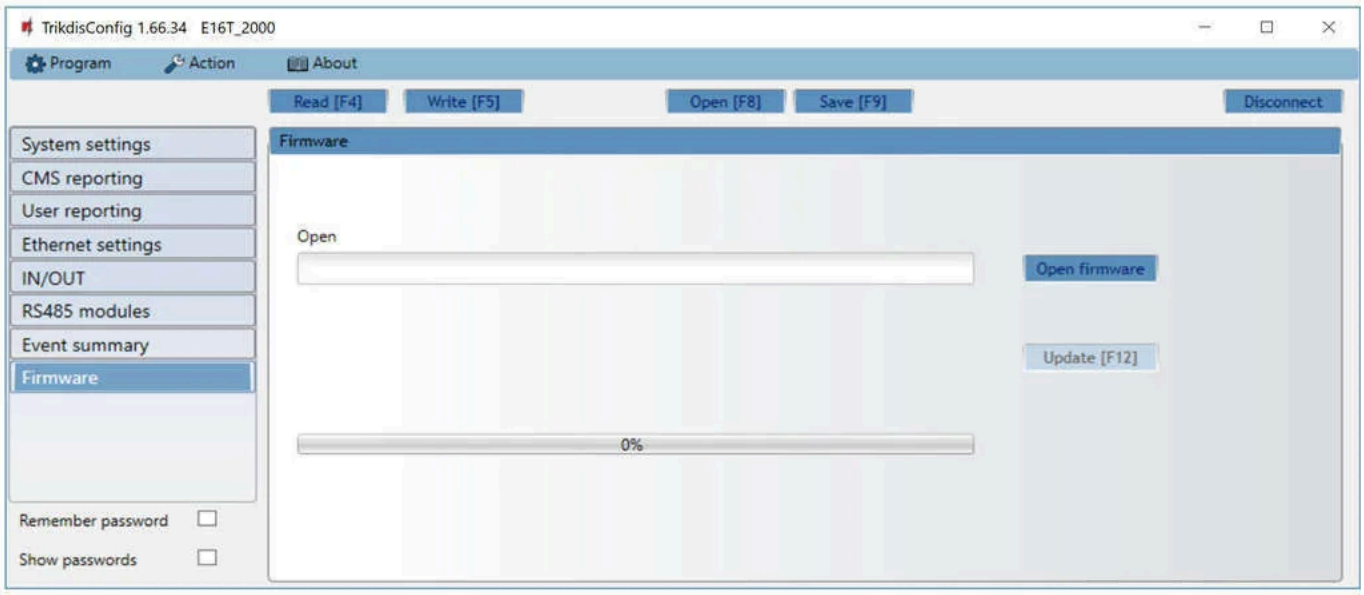
9. Aktualizacja firmware

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

Firmware możesz zaktualizować samodzielnie – do nowszej wersji, a w razie potrzeby także do starszej. Po aktualizacji wszystkie ustawienia urządzenia pozostają bez zmian.

1. Uruchom program TrikdisConfig i podłącz urządzenie kablem USB albo połącz się z nim zdalnie w trybie programowania.
2. Jeśli jest dostępny nowszy firmware, program zaproponuje jego pobranie – zaakceptuj.
3. Wybierz stronę **Firmware** i kliknij przycisk **Open firmware**. Wybierz plik firmware.
4. Naciśnij przycisk **Update [F12]**, poczekaj na zakończenie aktualizacji, a następnie w wyskakującym oknie kliknij **OK**. W tym czasie nie odłączaj kabla i nie przerywaj połączenia.

Pliki firmware znajdują się w folderze instalacyjnym TrikdisConfig, w podfolderze **Firmwares**, w folderze oznaczonym nazwą urządzenia. Jeśli takiego folderu nie ma, to albo nie ma dla niego aktualizacji, albo trzeba zaktualizować sam program TrikdisConfig. Najnowsze pliki może też pobrać zarejestrowany użytkownik ze strony internetowej producenta, ze strony danego urządzenia.



Rysunek 29. TrikdisConfig – strona Firmware: Open firmware i Update [F12].

Do aktualizacji potrzebne jest połączenie z internetem. Program antywirusowy, zapora sieciowa lub restrykcyjne ustawienia sieci mogą uniemożliwić automatyczne pobranie firmware; wtedy pobierz plik ręcznie i otwórz go na stronie Firmware.

10. Rozwiązywanie problemów i częste pytania

Najczęstsze pytania i usterki, wychodząc od sygnalizacji diod. Jeśli odpowiedź odsyła do szczegółowego rozdziału, znajdziesz tam dokładne miejsce ustawienia.

Dioda NETWORK nie świeci – brak sieci

1. Sprawdź mignięcia diody **TROUBLE**: 1 = brak fizycznego połączenia, 2 = brak adresu IP (DHCP), 3 = błąd DNS.
2. **Przy 1 mignięciu** sprawdź kabel i wtyki (czy RJ45 jest wsunięty do kliknięcia), port routera lub switcha (czy działa, czy nie jest wyłączony) i spróbuj innego kabla lub portu.
3. **Przy 2 mignięciach** w sieci nie ma serwera DHCP albo nie odpowiada: włącz go na routerze lub nadaj urządzeniu stały adres IP, maskę i bramę na stronie **Ethernet settings** (punkt 6.5).
4. **Przy 3 mignięciach** nie działa rozwiązywanie nazw: sprawdź pola DNS 1 / DNS 2 (fabrycznie publiczny DNS Google) i czy sieć przepuszcza wychodzący ruch DNS.

Sieć jest, ale stacja monitorowania nie otrzymuje zdarzeń

Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie działa do routera – ale nie to, że urządzenie ma też dostęp do internetu. Jeśli dioda NETWORK jest zielona, a dioda DATA świeci ciągle także po zdarzeniu lub raporcie testowym, połączenie z internetem nie działa: komunikat nie może zostać wysłany. W sieci komórkowej najczęściej winny jest APN albo usługa transmisji danych karty SIM, przy Ethernecie router, zapora sieciowa (firewall) lub DNS. Jeśli dioda DATA zgaśnie, komunikat został wysłany, a połączenie danych działa prawidłowo.

1. 6 mignięć diody **TROUBLE** oznacza brak połączenia z odbiornikiem: sprawdź adres odbiornika, port, ustawienie TCP/UDP i klucz szyfrowania (**CMS reporting**).

2. Jeśli odbiornik jest podany nazwą domeny, sprawdź ustawienie DNS (**Ethernet settings**).
3. Przy stałym adresie IP sprawdź bramę (**Default gateway**): z niewłaściwą bramą urządzenie osiąga sieć lokalną, ale nie internet.
4. W sieci firmowej lub filtrowanej zapora może blokować połączenie wychodzące na port odbiornika – uzgodnij to z administratorem sieci (punkt 3.2).

Centrala nie wysyła zdarzeń do komunikatora

1. Dialer centrali musi być włączony, w trybie DTMF, z formatem Contact ID i wpisanym numerem telefonu (rozdział 4).
2. Sprawdź podłączenie TIP/RING; 7 mignięć diody **TROUBLE** oznacza brak połączenia z centralą (przy podłączeniu z nadzorem linii).
3. Jeśli centrala oczekuje sygnału zgłoszenia i nie rozpoczyna połączenia, wyłącz w niej wykrywanie sygnału zgłoszenia.
4. Jeśli centrala sygnalizuje „błąd komunikacji", choć zdarzenie dotarło, sprawdź ustawienie **Wait acknowledgment from CMS** (punkt 6.2).

Protegus 2 nie widzi urządzenia

1. Na stronie **User reporting** → **PROTEGUS Cloud** musi być zaznaczone **Enable connection**.
2. Przy tworzeniu systemu trzeba podać **Protegus Cloud access code** ustawiony w urządzeniu; po utworzeniu systemu nie można go już zmienić w urządzeniu.
3. Adres MAC wpisz dokładnie, z pudełka lub z tyłu urządzenia – albo zeskanuj aplikacją kod QR z etykiety, wtedy nie można się pomylić.
4. Połączenie z internetem musi działać: dioda NETWORK świeci na zielono, a dioda DATA gaśnie po zdarzeniu. Do połączenia z chmurą Protegus potrzebny jest też działający DNS (**Ethernet settings**).

Nie mogę połączyć się zdalnie przez TrikdisConfig

1. Urządzenie musi być online (dioda NETWORK zielona, dioda DATA gaśnie po zdarzeniu), a połączenie z Protegus musi być włączone.
2. **CMS reporting** → **Settings** → **IP ping period** nie może być dłuższy niż 5 minut: PING podtrzymuje połączenie potrzebne do zdalnego dostępu.
3. Sprawdź hasło administratora lub instalatora.

Zapomniałem hasła

Zapomnianego hasła nie można odczytać ani usunąć przywróceniem ustawień fabrycznych, bo do tego także potrzebne jest hasło. Wtedy zresetować je może tylko producent lub dystrybutor: urządzenie trzeba mu dostarczyć. Dlatego zapisz ustawione hasła w bezpiecznym miejscu.

Czy potrzebny jest stały adres IP lub przekierowanie portów na routerze?

Nie. E16T sam nawiązuje połączenie wychodzące do odbiornika i do chmury Protegus, dlatego nie jest potrzebny ani publiczny stały adres IP, ani dynamiczny DNS, ani przekierowanie portów. W sieci lokalnej wystarczy adres otrzymany przez DHCP; stały adres lokalny nadaj tylko wtedy, gdy w sieci nie ma DHCP albo prosi o to administrator sieci (punkt 6.5).

Czy działa przez Wi-Fi?

Nie: E16T obsługuje tylko przewodowe (RJ45) połączenie sieciowe. Jeśli w pobliżu centrali nie ma kabla sieciowego, można zbudować most Wi-Fi do routera albo wybrać komunikator komórkowy G16T.

Co się dzieje podczas przerwy w zasilaniu?

Komunikator jest zasilany z akumulatora centrali, ale jeśli router i modem zostaną bez prądu, nie ma internetu, a zdarzenia czekają w buforze (dioda DATA świeci). Po powrocie internetu urządzenie je wyśle. Jeśli taka przerwa jest nie do przyjęcia, rozwiązaniem jest zasilacz bezprzerwowy (UPS) dla urządzeń sieciowych albo komunikator komórkowy (punkt 3.2).

11. Zasady bezpieczeństwa

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.

- Montaż i konserwację urządzeń systemów zabezpieczeń może wykonywać wyłącznie wykwalifikowany instalator.
- Przed instalacją uważnie przeczytaj instrukcję; nieprzestrzeganie wskazówek może prowadzić do nieprawidłowego działania lub uszkodzenia.
- Przed podłączaniem, przy każdym podłączaniu elektrycznym i przed serwisem odłącz urządzenie od zasilania.
- Usterki wynikające z nieprawidłowej instalacji lub użytkowania oraz zmiany i naprawy niezatwierdzone przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów dotyczących odpadów: nie wyrzucaj uszkodzonego urządzenia ani jego części razem z odpadami komunalnymi.

Zobacz też

- Zdalne uzbrajanie przełącznikiem kluczowym z aplikacji Protegus 2 – szczegóły i pułapki uzbrajania przełącznikiem kluczowym.
- Dokumentacja Trikdis: docs.trikdis.com.

Instrukcje w serwisie docs.trikdis.com są w języku angielskim.

Powiązane produkty

Trikdis E16T Ethernet Universal Communicator - Moduł IP

Trikdis IO8 PRZEWIDY MODUŁ EXPADER

Prawa autorskie

Tę instrukcję przygotowały trikdis.hu i mobilamb.eu. Jej tekst, struktura, nasze własne ilustracje i uzupełnienia są naszą własnością intelektualną i podlegają ochronie prawa autorskiego. Bez naszej zgody nie wolno jej kopiować, rozpowszechniać ani publikować na innej stronie internetowej, ani w całości, ani we fragmentach. Do instalacji i użytkowania produktu możesz ją swobodnie pobrać i wydrukować.

Nazwy i logo Trikdis oraz Protegus są znakami towarowymi UAB Trikdis.

Zawsze aktualna wersja tej instrukcji: https://pl.mobilamb.eu/instrukcja-e16t