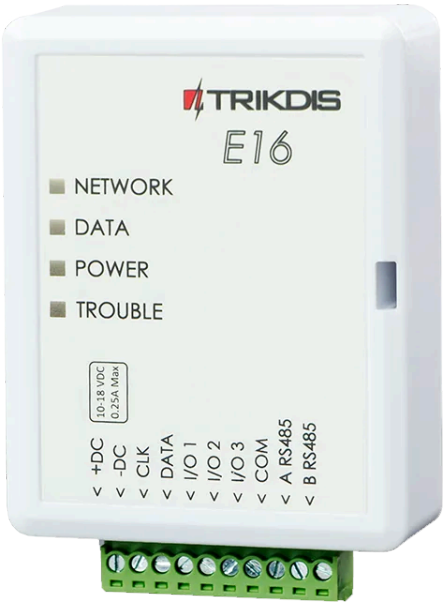
Komunikator E16 – instrukcja dla instalatora i użytkownika

Instrukcja instalatora i użytkownika komunikatora Ethernet Trikdis E16: podłączenie do magistrali danych lub portu szeregowego centrali alarmowej, programowanie centrali, konfiguracja sieci w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-e16

Spis treści

1. Przegląd

1.1 Do czego służy i jak działa
1.2 Zgodne centrale alarmowe
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 Typ centrali i sterowanie bezpośrednie
2.3 Połączenie z aplikacją Protegus 2
2.4 Połączenie ze stacją monitorowania

3. Instalacja i podłączenie

3.1 Kroki instalacji
3.2 Umiejscowienie i sieć
3.3 Podłączenie do centrali alarmowej
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 i Integriti
3.4 Podłączenie strefy przełącznika kluczowego
3.5 Podłączenie wejść
3.6 Podłączenie wyjścia z przekaźnikiem
3.7 Podłączenie ekspandera iO-8
3.8 Podłączenie kabla Ethernet
3.9 Włączenie i pierwsze sprawdzenie
A TRIKDIS átjelző elindítása

4. Programowanie centrali alarmowej

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

5. Zdalne sterowanie aplikacją Protegus 2

5.1 Dodanie urządzenia
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Sterowanie bezpośrednie kodem manipulatora

5.3 Uzbrajanie strefą przełącznika kluczowego
5.4 Uzbrajanie i rozbrajanie z aplikacji

6. TrikdisConfig – ustawienia szczegółowo

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 FAQ

11. Zasady bezpieczeństwa

Zobacz też

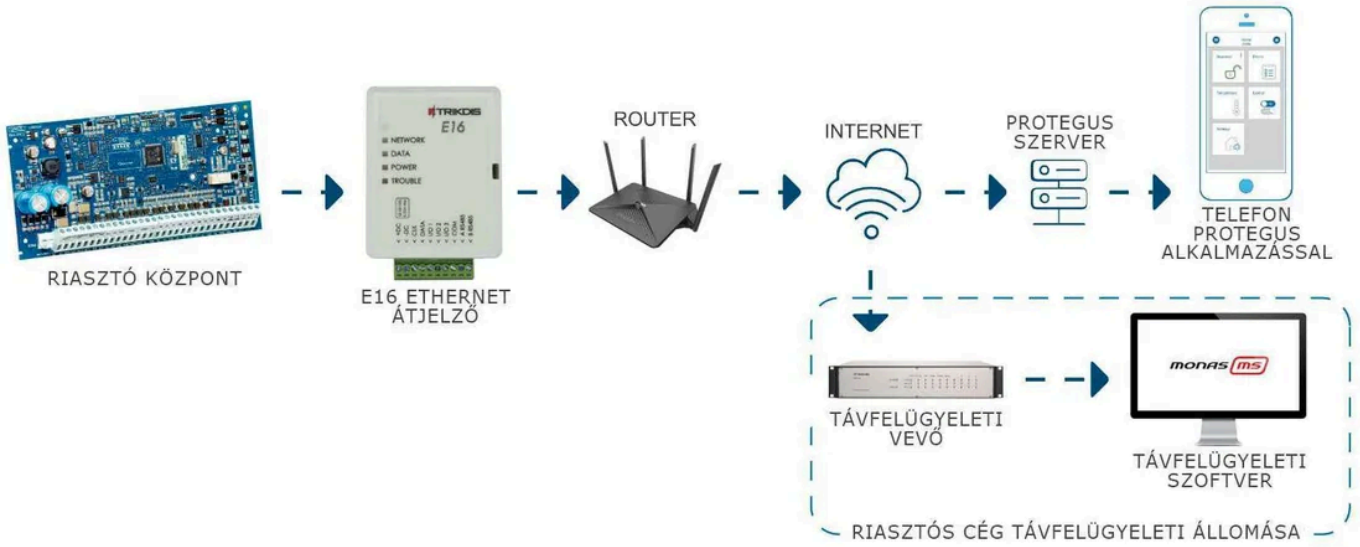
1. Przegląd

E16 to **komunikator Ethernet Trikdis podłączany bezpośrednio**: nie łączy się z wyjściem linii telefonicznej centrali alarmowej, lecz z **magistralą manipulatorów lub portem szeregowym** centrali. Odczytuje zdarzenia bezpośrednio z centrali – razem z numerem strefy, partycji i użytkownika – i przekazuje je przez sieć lokalną i przewodowe łącze internetowe do odbiornika stacji monitorowania oraz do chmury Protegus, czyli do aplikacji użytkownika. Działa z obsługiwanymi centralami DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell i Crow; przy typach **ze sterowaniem bezpośrednim** użytkownik uzbraja i rozbraja system z aplikacji Protegus 2 własnym kodem manipulatora, bez osobnej strefy przełącznika kluczowego. Do central innych producentów, które mają tylko wyjście linii telefonicznej, służy komunikator Ethernet E16T (TIP/RING); tam, gdzie nie ma internetu przewodowego – komunikator komórkowy G16.

1.1 Do czego służy i jak działa

- **Odczytuje centralę bezpośrednio.** Na magistrali centrali każde zdarzenie trafia do komunikatora natychmiast, z własną numeracją centrali; nie trzeba konfigurować dialera centrali i nie ma też wybierania Contact ID.
- **Raportuje do stacji monitorowania.** Wysyła zdarzenia przez połączenie IP do programowego lub sprzętowego odbiornika Trikdis (protokół TRK; odbiorniki Trikdis współpracują z dowolnym oprogramowaniem stacji monitorowania) albo do dowolnego odbiornika uniwersalnego (SIA DC-09 2007/2012, SUR-GARD TL150). Przy odbiorniku SUR-GARD komunikator zamienia kody Contact ID otrzymane z centrali na kody SIA; tabela konwersji znajduje się w załączniku do anglojęzycznej dokumentacji Trikdis. Połączenie jest domyślnie sprawdzane co 30 sekund (odstęp można zmienić, punkt 6.3), a w razie awarii komunikator przełącza się na kanał zapasowy; dzięki kanałowi równoległemu zdarzenia mogą trafiać jednocześnie do dwóch odbiorników.
- **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, ogrzewanie, wentylację, system nawadniania itp.). Protegus 2 działa z centralami wszystkich producentów obsługiwanych przez E16.
- **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.
- **Nie potrzebuje karty SIM ani abonamentu komórkowego.** Urządzenie korzysta z istniejącego łącza internetowego w obiekcie: łączy się z routerem lub switchem jednym kablem Ethernet, fabrycznie pobiera adres przez DHCP i nawiązuje tylko połączenia wychodzące, dlatego na routerze nie trzeba otwierać portów.
- **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.

Budowę systemu pokazuje poniższy rysunek: magistrala centrali alarmowej łączy się z E16, E16 przez router łączy się z internetem, a stamtąd z chmurą Protegus i odbiornikiem stacji monitorowania, natomiast użytkownik widzi system w aplikacji Protegus 2.



Rysunek 1. Miejsce E16 w systemie: centrala alarmowa (magistrala manipulatorów lub port szeregowy) → komunikator Ethernet E16 → router → internet → chmura Protegus i odbiornik stacji monitorowania → telefon użytkownika z aplikacją Protegus 2 oraz oprogramowanie stacji monitorowania firmy ochrony.

1.2 Zgodne centrale alarmowe

E16 można podłączyć do poniższych central. Przy typach **ze sterowaniem bezpośrednim** uzbrajanie i rozbrajanie odbywa się z aplikacji kodem manipulatora; przy pozostałych – strefą przełącznika kluczowego (punkt 3.4). Do bezpośredniego sterowania centralami Paradox firmware centrali musi mieć wersję co najmniej **V.4**; w nowszych typach Paradox (SP+, MG5050+, EVOHD+) port szeregowy jest fabrycznie zablokowany i przed użyciem trzeba go odblokować.

Centrale sterowane bezpośrednio – komunikator odbiera zdarzenia przez magistralę danych lub port szeregowy, a uzbrajanie / rozbrajanie działa bez dodatkowego okablowania:

Producent	Połączenie	Modele
Paradox	port szeregowy	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* firmware powyżej 7.50)
DSC	magistrala danych	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	magistrala danych	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	port szeregowy	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	magistrala danych	Ademco Vista-15, Vista-20, Vista-48

W nowszych centralach Paradox oznaczonych * port szeregowy jest fabrycznie zablokowany; urządzenie zewnętrzne komunikuje się z nim dopiero po odblokowaniu.

Soros port feloldás útmutató

Centrale sterowane przez strefę typu klucz – komunikator odbiera zdarzenia przez magistralę danych lub port szeregowy, a do sterowania potrzebne jest podłączenie i zaprogramowanie strefy typu klucz (punkt 3.4):

Producent	Połączenie	Modele
Paradox	port szeregowy	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	magistrala danych	PC1404, PC5020
Texecom	port szeregowy	Premier 412, 816, 832, 832+
Inner Range	magistrala danych	Inception, Integriti
Crow	magistrala danych	Runner 4/8, 8/16

Oprócz tego komunikator można stosować z centralami **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 i MATRIX 816** oraz **Paradox DIGIPLEX NE96 i EVO96**.

Lista od czasu do czasu się zmienia; najnowszy stan znajdziesz w wyszukiwarce zgodności. Z centralami **DSC PowerSeries NEO** E16 nie działa: do magistrali NEO producent centrali nie dopuszcza urządzeń zewnętrznych, zobacz DSC Power Series NEO i komunikatory Trikdis: zgodność i rozwiązania.

1.3 Główne cechy

Połączenie z centralą alarmową

- Podłączenie najwyżej 4 przewodami (+DC, −DC, CLK, DATA) do magistrali manipulatorów centrali (DSC, Caddx, Crow, Pyronix, Honeywell) lub do jej portu szeregowego (Paradox, Texecom, InnerRange); do portu szeregowego dostępny jest fabryczny kabel (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Przekazuje każde zdarzenie centrali z pełną informacją (kod, partycja, strefa lub użytkownik); sygnalizuje zerwanie połączenia (dioda TROUBLE, zdarzenie COMMUNICATION).
- Centrale ze sterowaniem bezpośrednim można uzbrajać i rozbrajać z aplikacji kodem manipulatora; Protegus 2 pokazuje też stan stref.

Połączenie sieciowe

- Złącze Ethernet (IEEE 802.3, 10Base-T, RJ45) do sieci lokalnej; adres fabrycznie pobierany przez DHCP, można też ustawić stały adres IP.
- Nawiązuje tylko połączenia wychodzące do odbiornika i chmury Protegus: nie trzeba otwierać portów, nie jest potrzebny ani publiczny adres IP, ani karta SIM.

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, każdy z własnym odbiornikiem zapasowym; dzięki kanałowi równoległemu zdarzenia trafiają jednocześnie do dwóch odbiorników.
- Szyfrowane komunikaty (AES-128); bufor zdarzeń 60 komunikatów.

Funkcje dla użytkownika

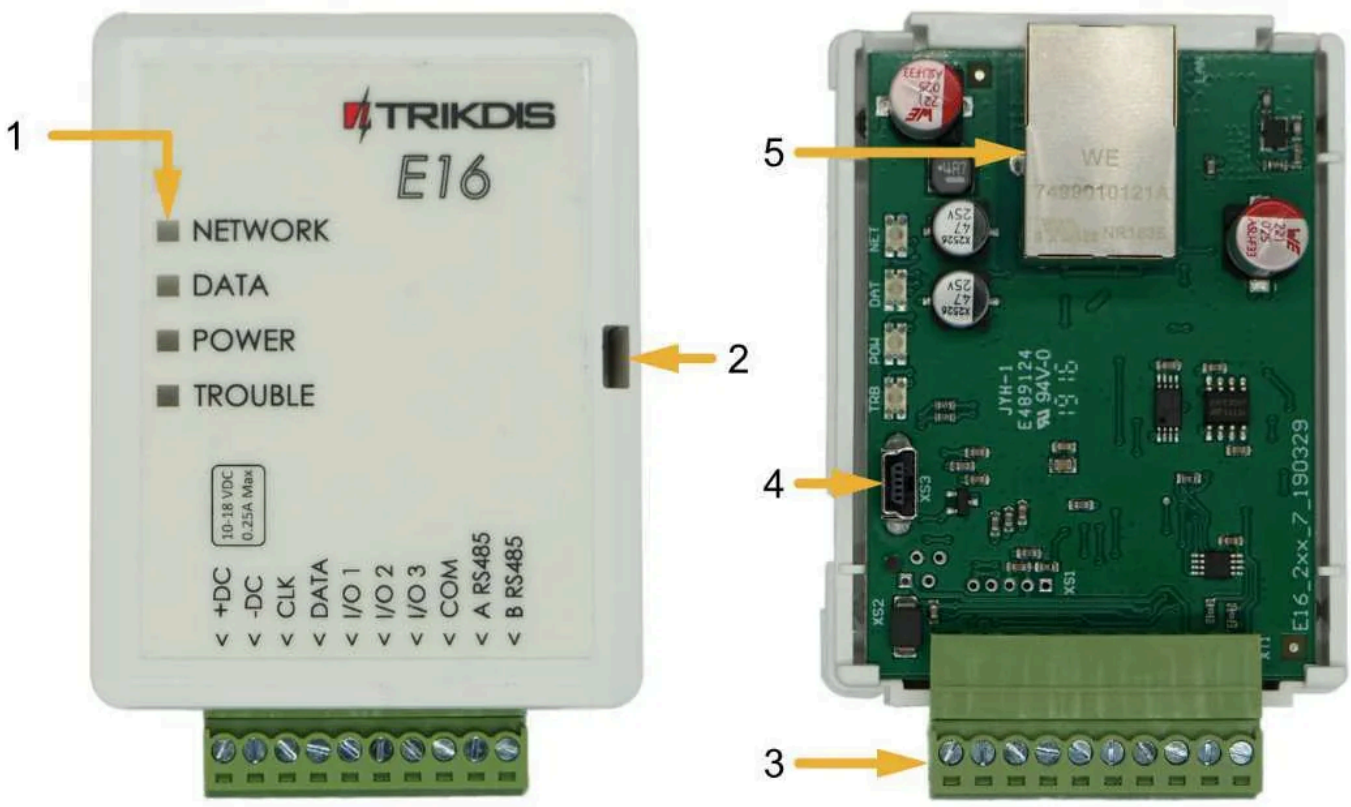
- Aplikacja mobilna i webowa Protegus 2: powiadomienia, lista zdarzeń, uzbrajanie i rozbrajanie, sterowanie wyjściami.
- Wielopoziomowe uprawnienia użytkowników w aplikacji (administrator, instalator, użytkownik).

Instalacja i konfiguracja

- Ustawienia można zapisać do pliku i wczytać do innego komunikatora.
- Dwa poziomy dostępu: administrator i instalator.
- Zdalna konfiguracja i aktualizacja programem TrikdisConfig.

1.4 Elementy komunikatora

Płytka drukowana E16 jest umieszczona w białej obudowie z tworzywa; przednią pokrywę można zdjąć, a listwę zaciskową – wyciągnąć. Złącze Ethernet znajduje się na płytce drukowanej, a kabel wchodzi przez otwór w obudowie.



Rysunek 2. Elementy E16 od przodu i przy otwartej obudowie.

- 1 Diody sygnalizacyjne (NETWORK, DATA, POWER, TROUBLE)
- 2 Otwór ułatwiający zdjęcie przedniej 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
CLK	Linia zegara / linia szeregowa magistrali centrali

Zacisk	Funkcja
DATA	Linia danych magistrali centrali
I/O 1	1. wejście/wyjście (ustawienie fabryczne: wejście, NO)
I/O 2	2. wejście/wyjście (ustawienie fabryczne: wejście, NO)
I/O 3	3. wejście/wyjście (ustawienie fabryczne: wyjście)
COM	Wspólny punkt (minus) wejść i wyjść
A RS485	Przewód A magistrali RS485
B RS485	Przewód B magistrali RS485

Opis listwy zaciskowej jest też na przedniej pokrywie, więc przy podłączaniu nie trzeba jej zdejmować. To, do którego zacisku centrali idą CLK i DATA, zależy od producenta – schematy podłączenia zawiera punkt 3.3.

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 ruch danych, a TROUBLE usterkę.

NETWORK – połączenie z siecią

Sygnał	Znaczenie
nie świeci	Brak połączenia z siecią (brakuje kabla, routera lub adresu IP – czego dokładnie, pokaże dioda TROUBLE)
świeci na zielono	Połączono z siecią

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 nie jest podłączony albo port routera / switcha nie działa
2 czerwone mignięcia	Błąd DHCP: urządzenie nie otrzymało adresu IP
3 czerwone mignięcia	Błąd DNS: nie można rozwiązać nazwy domeny odbiornika lub chmury Protegus
6 czerwonych mignięć	Brak połączenia z odbiornikiem stacji monitorowania i/lub z serwerem Protegus (przyczyną może być też łącze internetowe lub zapora sieciowa)
7 czerwonych mignięć	Zerwane połączenie z centralą alarmową (połączenie przez magistralę lub port szeregowy)
miga na czerwono (podczas programowania)	Błąd pamięci
świeci na czerwono (podczas programowania)	Uszkodzony firmware

1.7 Dane techniczne

Parametr	Wartość
Połączenie z centralą alarmową	magistrala manipulatorów lub port szeregowy, zależnie od typu centrali (4 przewody: +DC, −DC, CLK, DATA)
Złącze sieciowe	Ethernet, IEEE 802.3, 10Base-T, gniazdo RJ45
Ustawienia sieci	DHCP (fabrycznie) lub stały adres IP, maska podsieci, brama, DNS
Wejścia/wyjścia	3 I/O o podwójnej funkcji: 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 najwyżej 4 ekspandery iO-8 (każdy +8 I/O)
Napięcie zasilania	10–18 V DC
Pobór prądu	100 mA nominalnie (w czuwaniu); najwyżej 250 mA podczas wysyłania
Protokoły transmisji	TRK, DC-09_2007, DC-09_2012, TL150
Szyfrowanie komunikatów	AES-128
Bufor zdarzeń	60 komunikatów
Programowanie	TrikdisConfig (Windows) przez kabel USB Mini-B lub zdalnie

Parametr	Wartość
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 E16 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 · co najmniej 4-żyłowy przewód do magistrali centrali – do portu szeregowego Paradox kabel **CRP2** lub **CRP2B**, do portu szeregowego Texecom kabel **CRP4** · płaski śrubokręt 2,5 mm · kabel Ethernet (CAT-5 lub lepszy, najwyżej 100 m) do routera lub switcha · instrukcja instalatora centrali alarmowej. Kable i akcesoria trzeba kupić osobno u dystrybutora.

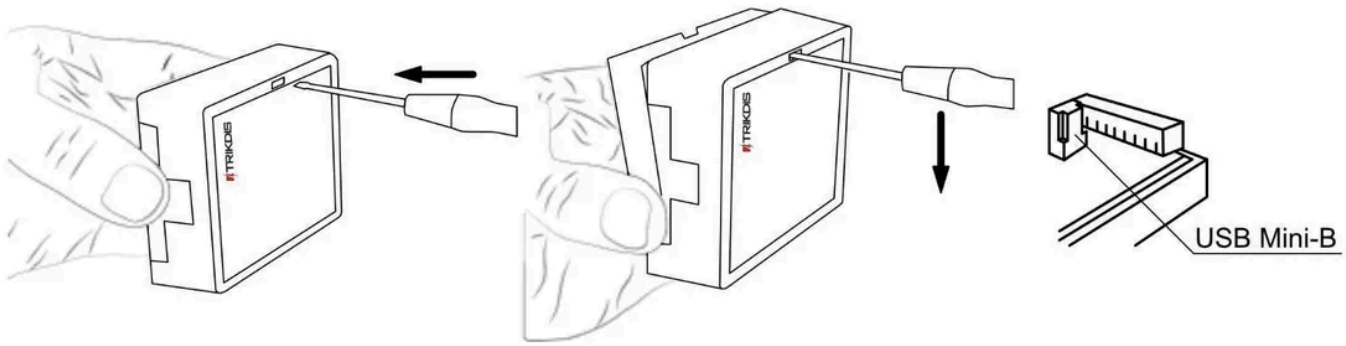
1. Pobierz i zainstaluj program TrikdisConfig.

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 E16. Włóż płaski śrubokręt w otwór na górnej krawędzi pokrywy i, podważając w dół, delikatnie zdejmij przednią pokrywę z zatrzasków. Poniższy rysunek pokazuje otwieranie i położenie gniazda USB.



Rysunek 3. Zdejmowanie przedniej pokrywy płaskim śrubokrętem (po lewej, pośrodku) i położenie gniazda USB Mini-B na płytce drukowanej (po prawej).

3. Połącz E16 z komputerem kablem USB Mini-B. USB daje wystarczające zasilanie do programowania, osobne zasilanie nie jest potrzebne.

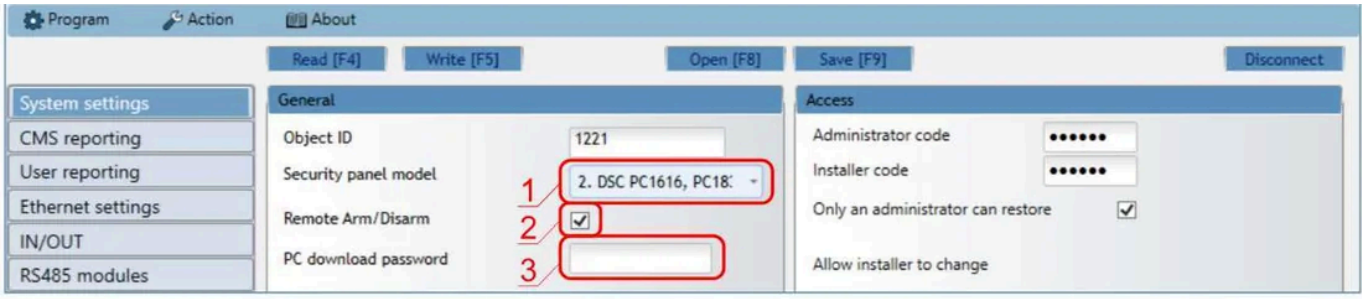
Ostrzeżenie

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

4. 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`).

2.2 Typ centrali i sterowanie bezpośrednie

Niezależnie od trybu pracy najpierw na stronie **System settings** wskaż, do jakiej centrali trafi komunikator.



Rysunek 4. TrikdisConfig – strona System settings, grupa General.

- 1 **Security panel model** – typ podłączonej centrali alarmowej z listy; od niego zależy, jak komunikator odczytuje magistralę.
- 2 **Remote Arm/Disarm** – zaznacz, jeśli użytkownik ma uzbrajać i rozbrajać centralę z aplikacji Protegus 2 własnym kodem manipulatora. Pojawia się tylko przy typach ze sterowaniem bezpośrednim; przy pozostałych centralach uzbrajanie można rozwiązać strefą przełącznika kluczowego (punkt 3.4) – wtedy pozostaw to pole puste.
- 3 **Security panel PC download password** – przy centralach Paradox i Texecom hasło PC lub UDL centrali (4 znaki); musi być takie samo jak ustawione w centrali. Pole pojawia się po zaznaczeniu Remote Arm/Disarm.

W kilku centralach ustawienie jest potrzebne także w centrali: w centralach Caddx, Honeywell i InnerRange już do odczytu zdarzeń (włączenie magistrali lub portu szeregowego), w centralach Paradox i Texecom do sterowania bezpośredniego (hasło PC lub UDL) – rozdział 4 opisuje to dla każdego producenta, razem ze zmianą hasła.

2.3 Połączenie z aplikacją Protegus 2

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



Rysunek 5. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

- 4 **Enable connection** – zaznacz: włącza połączenie z chmurą Protegus.
- 5 **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.**

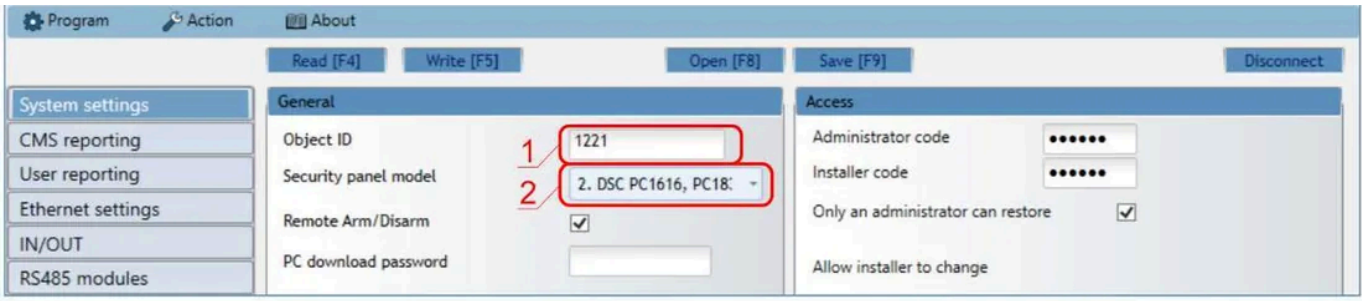
W ustawieniach sieci na stronie **Ethernet settings** fabrycznie zaznaczona jest opcja **Use DHCP**: urządzenie automatycznie otrzymuje adres IP z routera i w większości miejsc nie trzeba nic więcej robić. Jeśli w sieci nie ma DHCP albo trzeba użyć stałego adresu, wprowadź tu ustawienia ręczne (punkt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

E16 nawiązuje tylko **wychodzące** połączenia do chmury Protegus i odbiornika, dlatego na routerze nie trzeba otwierać ani przekierowywać portów. W sieci firmowej filtrowanej zaporą uzgodnij ruch wychodzący z administratorem sieci (punkt 3.2).

Jeśli urządzenie działa tylko z Protegus 2, bez stacji monitorowania, konfiguracja jest gotowa: naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB. Jeśli urządzenie raportuje także do stacji monitorowania, przejdź do punktu 2.4.

2.4 Połączenie ze stacją monitorowania

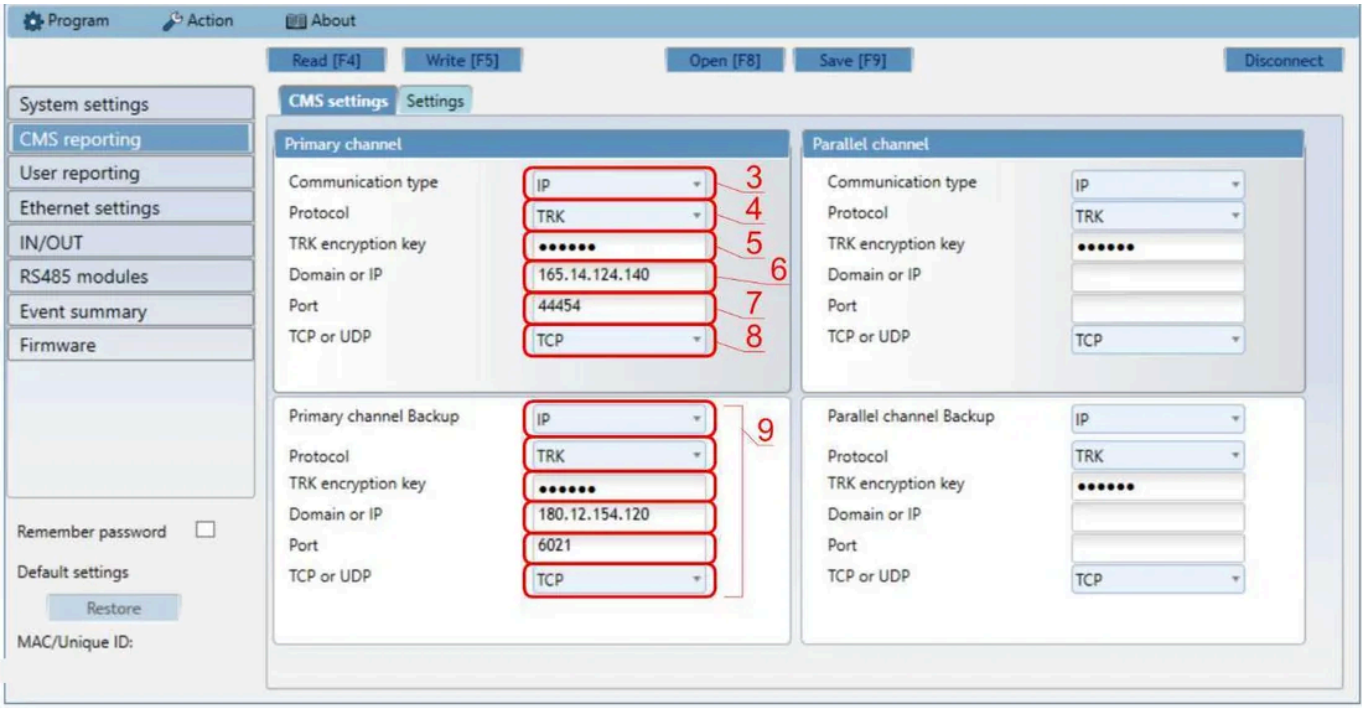
Jeśli urządzenie raportuje także do odbiornika stacji monitorowania, na stronie **System settings** podaj również identyfikator obiektu.



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

- 1 **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe, 0–9, A–F). Wartości `FFFE` i `FFFF` nie można używać.
- 2 **Security panel model** – typ podłączonej centrali alarmowej (jeśli nie ustawiono go jeszcze w punkcie 2.2).

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 E16 to jedyna możliwość).
- 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; dostosuj go do ustawień odbiornika.
- 9 **Primary channel Backup** – kanał zapasowy na wypadek awarii kanału głównego; wypełnij go tak samo, zalecane.

Zalecane jest też ustawienie **Parallel channel** (kanału równoległego) i należącego do niego kanału zapasowego, jeśli zdarzenia mają otrzymywać dwa odbiorniki.

Przy protokole **DC-09** na zakładce **Settings** podaj też numer obiektu, linii i odbiornika DC-09. Jeśli odbiornik podajesz nazwą domeny, na stronie **Ethernet settings** musi być działający adres DNS (fabrycznie publiczny serwer nazw Google).

Na koniec konfiguracji 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. Przykręć tylną część obudowy wkrętami w wybranym miejscu.
4. Włóż płytkę drukowaną z powrotem do tylnej części obudowy i ponownie włóż listwę zaciskową.

5. Podłącz kabel Ethernet do gniazda RJ45 (punkt 3.8).
6. Załóż przednią pokrywę.

3.2 Umiejscowienie i sieć

- Komunikator umieść w **suchym miejscu wewnątrz budynku**, najlepiej w pobliżu obudowy centrali alarmowej, aby przewód magistrali był krótki. Metalowa obudowa nie przeszkadza: E16 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 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.

Zanik zasilania

E16 jest zasilany z centrali alarmowej, więc przy zaniku zasilania sieciowego działa dalej z akumulatora centrali – router i modem zwykle jednak nie, a bez nich nie ma internetu. Jeśli w danym systemie jest to nie do przyjęcia, zasilaj także urządzenia sieciowe z zasilacza awaryjnego (UPS) albo wybierz komunikator komórkowy (G16).

3.3 Podłączenie do centrali alarmowej

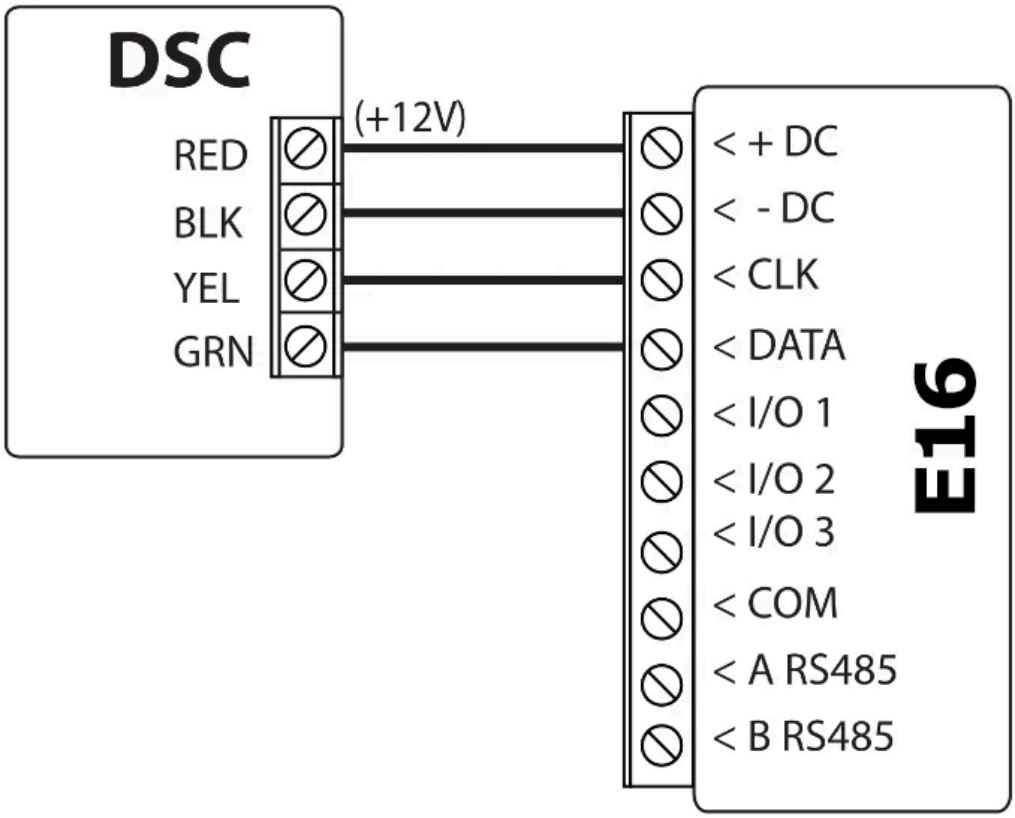
E16 łączy się z centralą **najwyżej czterema przewodami** (na magistrali Caddx i Pyronix CLK nie jest używany): do zacisków **+DC** i **–DC** trafia 12-woltowe zasilanie pomocnicze centrali (AUX), do zacisków **CLK** i **DATA** – dwa przewody danych magistrali manipulatorów lub portu szeregowego centrali. To, który zacisk centrali jest którym, zależy od producenta – podłączaj według poniższych schematów. Do central z portem szeregowym (Paradox, Texecom) dostępny jest fabryczny kabel, którego jeden koniec pasuje do złącza centrali, a drugi podłącza się do listwy zaciskowej E16.

Podczas wysyłania E16 może pobierać nawet 250 mA. Sprawdź, czy wyjście AUX centrali to wytrzyma razem z pozostałymi podłączonymi urządzeniami. Ponieważ zasilanie zapewnia centrala, przy zaniku zasilania sieciowego akumulator centrali zasila także komunikator. Większość central nie ulega uszkodzeniu przy zamienionych przewodach urządzenia podłączonego do magistrali, ale zamiana **+DC i –DC** może zniszczyć komunikator – przed podłączeniem sprawdź biegunowość.

Po podłączeniu w polu **System settings** → **Security panel model** w TrikdisConfig trzeba wybrać typ podłączonej centrali (punkt 2.2); u niektórych producentów potrzebne jest też ustawienie w centrali (rozdział 4).

3.3.1 DSC PowerSeries

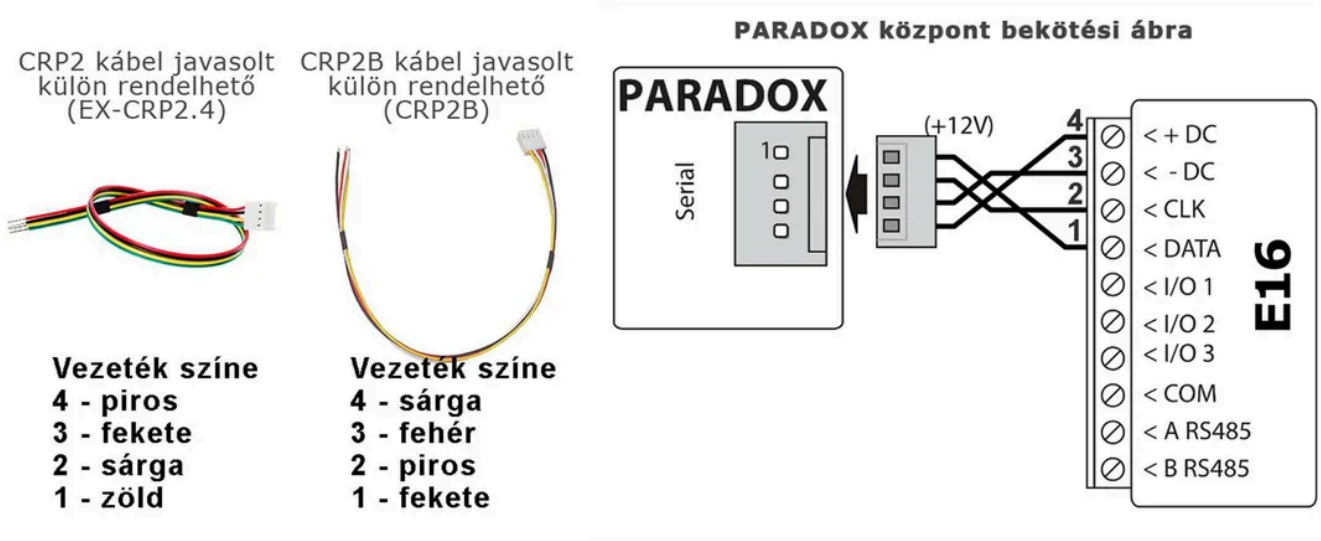
Cztery zaciski Keybus: **RED** → +DC, **BLK** → −DC, **YEL** → CLK, **GRN** → DATA.



Rysunek 8. Podłączenie do magistrali Keybus centrali DSC PowerSeries (magistrala manipulatorów, „Keypad bus"): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Komunikator łączy się z **portem szeregowym** (SERIAL) central Paradox fabrycznym kablem **CRP2** lub **CRP2B**; koniec kabla od strony centrali pasuje do złącza szeregowego, a drugi koniec podłączasz do listwy zaciskowej E16. 4 piny złącza: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Kolory żył obu kabli się różnią – schemat pokazuje przypisanie kolorów dla obu kabli. Oznaczenia złącza szeregowego Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

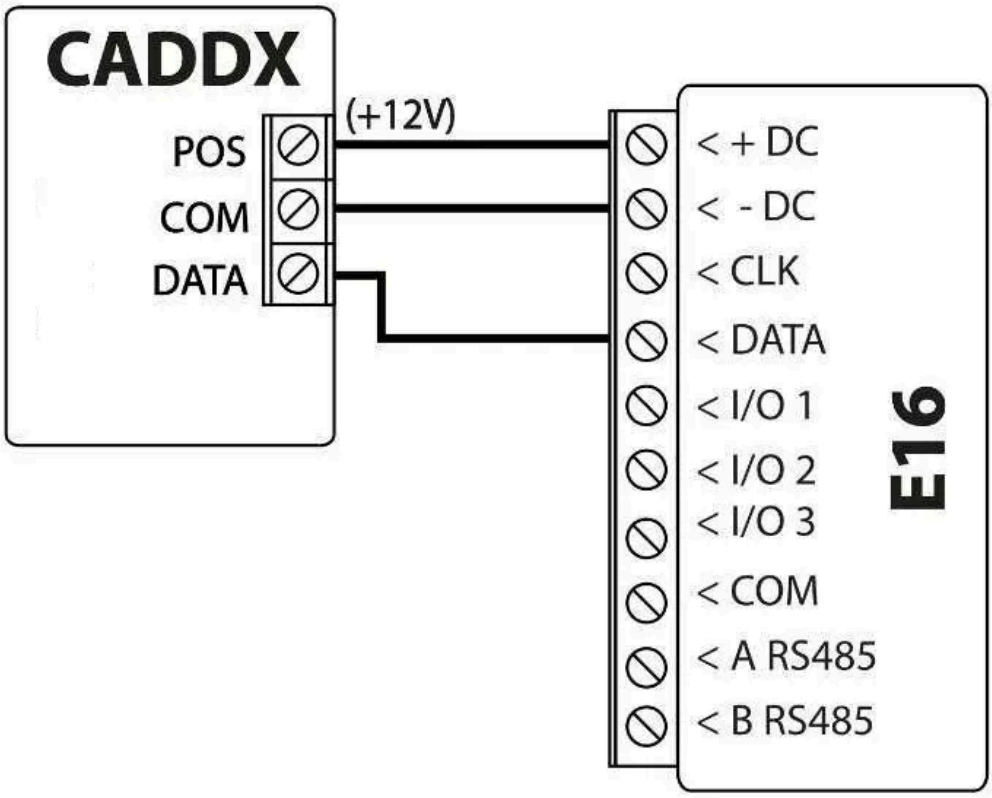


Rysunek 9. Podłączenie do portu szeregowego centrali Paradox kablem CRP2 (EX-CRP2.4) lub CRP2B. CRP2: 4 czerwony → +DC, 3 czarny → −DC, 2 żółty → CLK, 1 zielony → DATA. CRP2B: 4 żółty → +DC, 3 biały → −DC, 2 czerwony → CLK, 1 czarny → DATA.

W nowszych centralach Paradox port szeregowy może być fabrycznie zablokowany – sposób odblokowania opisuje punkt 4.2 i artykuł Odblokowanie zablokowanego portu szeregowego w centralach alarmowych Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

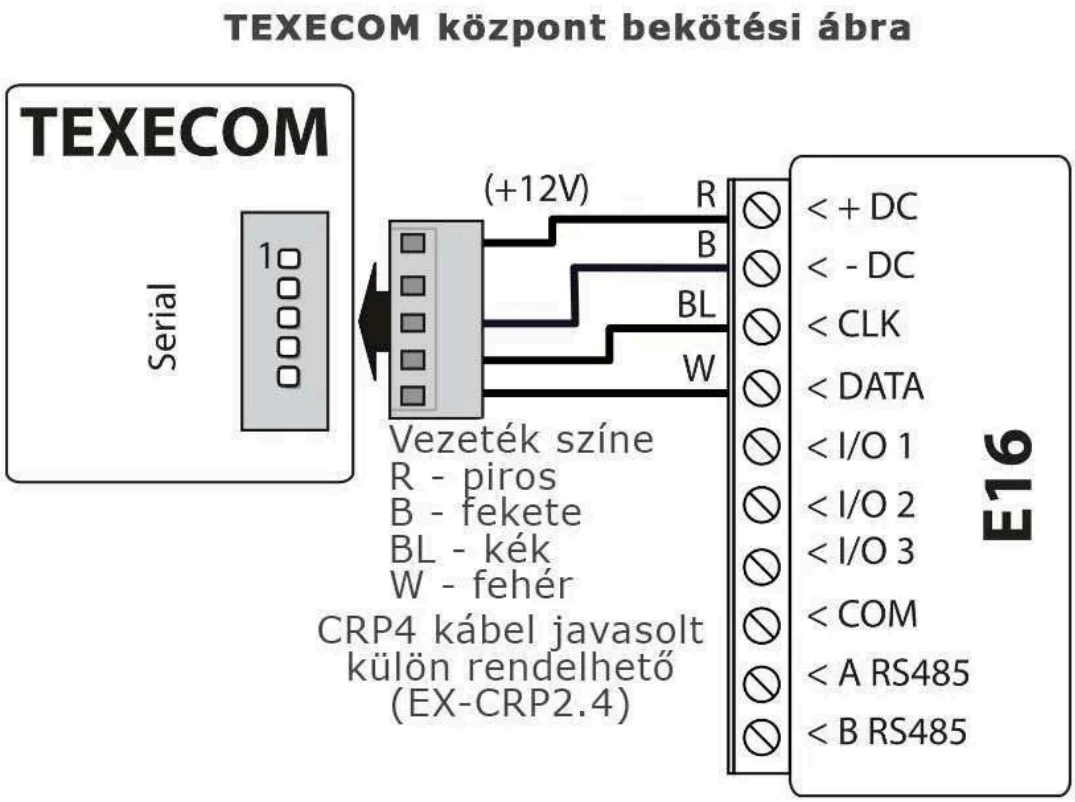
Trzy zaciski magistrali manipulatorów: **POS** → +DC, **COM** → −DC, **DATA** → DATA. Zacisk **CLK** nie jest używany.



Rysunek 10. Podłączenie do magistrali manipulatorów centrali Caddx NetworX („Keypad bus"): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK pozostaje wolny.

3.3.4 Texecom Premier / Premier Elite

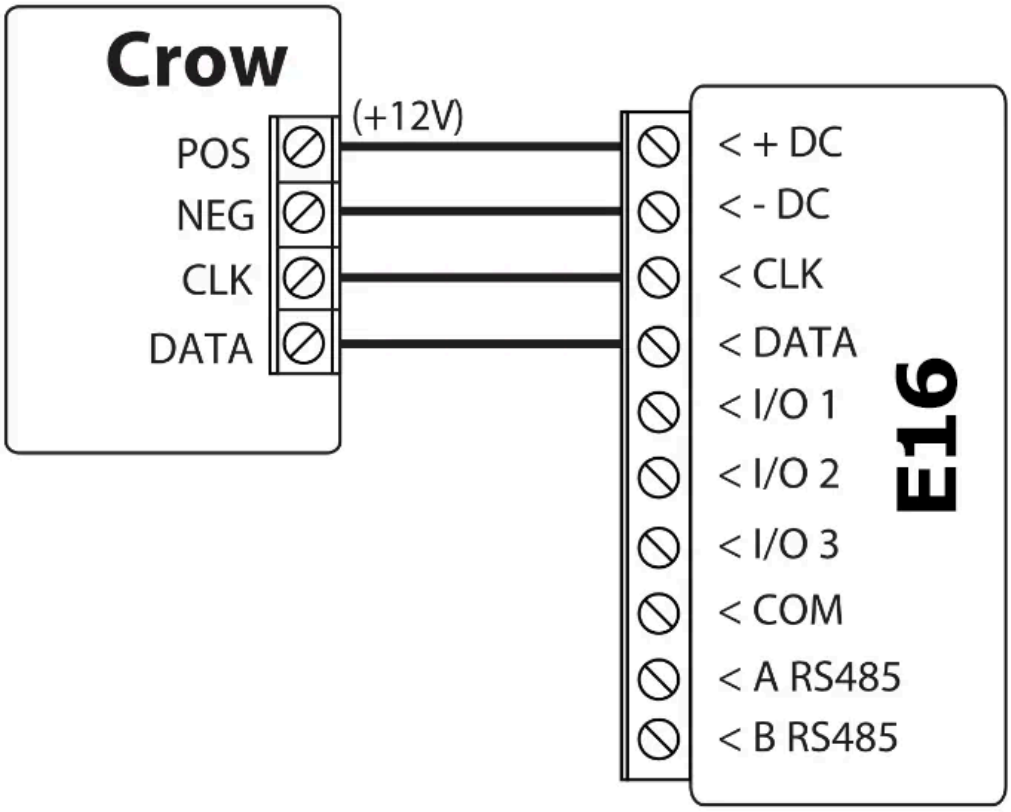
Komunikator łączy się z portem szeregowym centrali fabrycznym kablem **CRP4**: **czerwony (R)** → +DC, **czarny (B)** → −DC, **niebieski (BL)** → CLK, **biały (W)** → DATA.



Rysunek 11. Podłączenie do portu szeregowego centrali Texecom kablem CRP4: czerwony → +DC, czarny → −DC, niebieski → CLK, biały → DATA.

3.3.5 Crow Runner

Magistrala manipulatorów central Crow Runner 4/8 i Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.



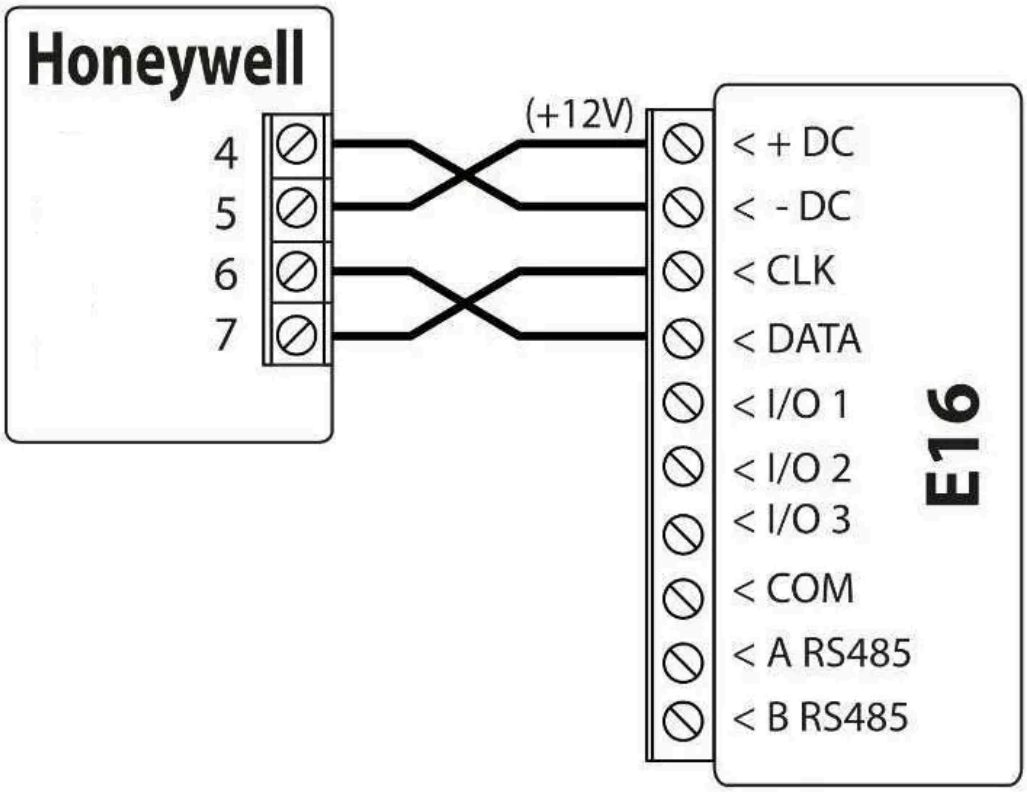
Rysunek 12. Podłączenie do magistrali manipulatorów centrali Crow Runner 4/8 i Runner 8/16 („Keypad bus"): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Magistrala manipulatorów central Pyronix: **+AUX** → +DC, **–AUX** → −DC, **KD** → DATA. Zacisk **CLK** nie jest używany. Po podłączeniu i skonfigurowaniu komunikatora odłącz centralę od zasilania i uruchom ją ponownie, aby zaakceptowała komunikator (punkt 4.5).

3.3.7 Honeywell Ademco Vista

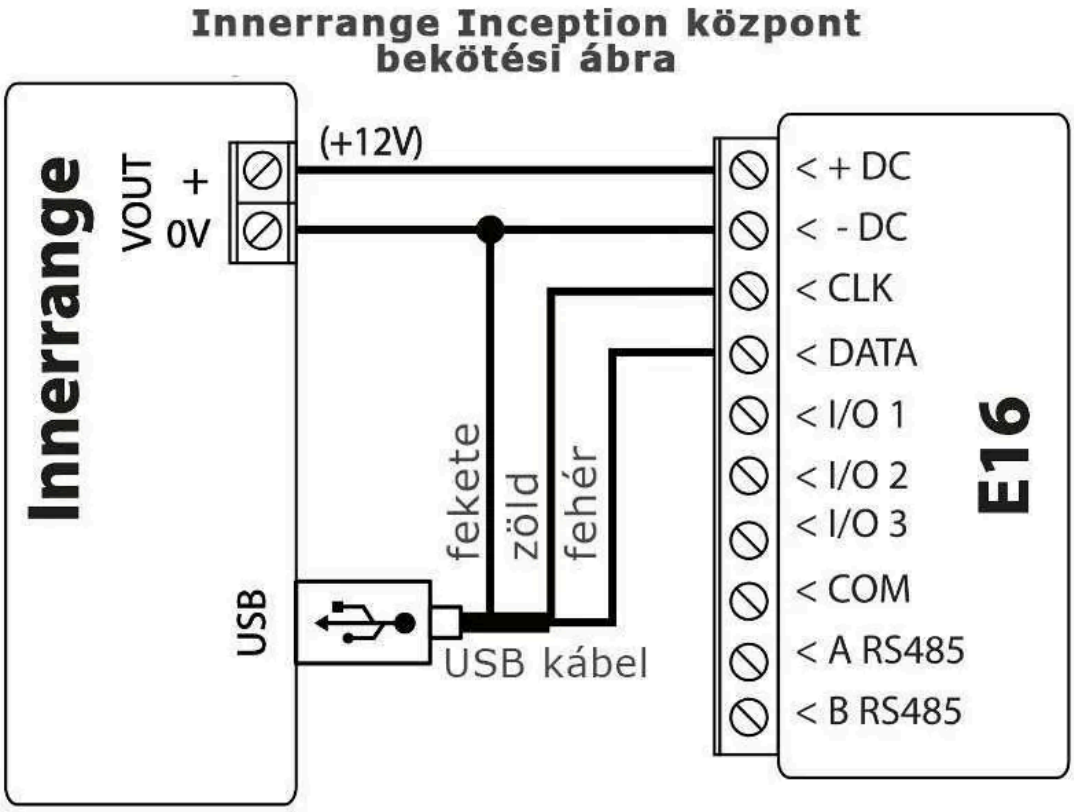
Numerowane zaciski magistrali manipulatorów central Vista-15, Vista-20 i Vista-48: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (wyjście danych, żółty) → CLK, **6** (wejście danych, zielony) → DATA.



Rysunek 13. Podłączenie do magistrali manipulatorów centrali Honeywell Vista-20 / Vista-48 („Keypad bus"): 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

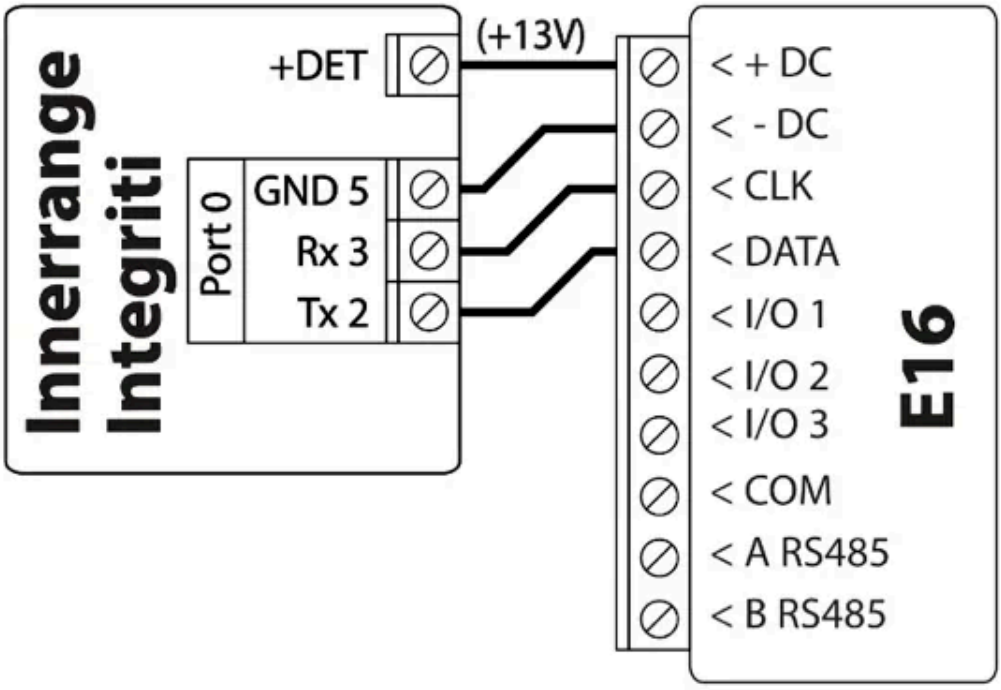
3.3.8 InnerRange Inception i Integriti

Przy centrali **Inception** komunikator pobiera zasilanie z jej zacisków zasilania (**VOUT +** → +DC, **0V** → −DC), a połączenie danych wykonuje się z portu USB centrali kablem InnerRange 993030USB: **czarny** → 0V (−DC), **zielony** → CLK, **biały** → DATA. W centrali trzeba włączyć używanie portu szeregowego (punkt 4.7).



Rysunek 14. Podłączenie do centrali InnerRange Inception: zasilanie z zacisków VOUT + i 0V, dane z portu USB kablem 993030USB (czarny → 0V, zielony → CLK, biały → DATA).

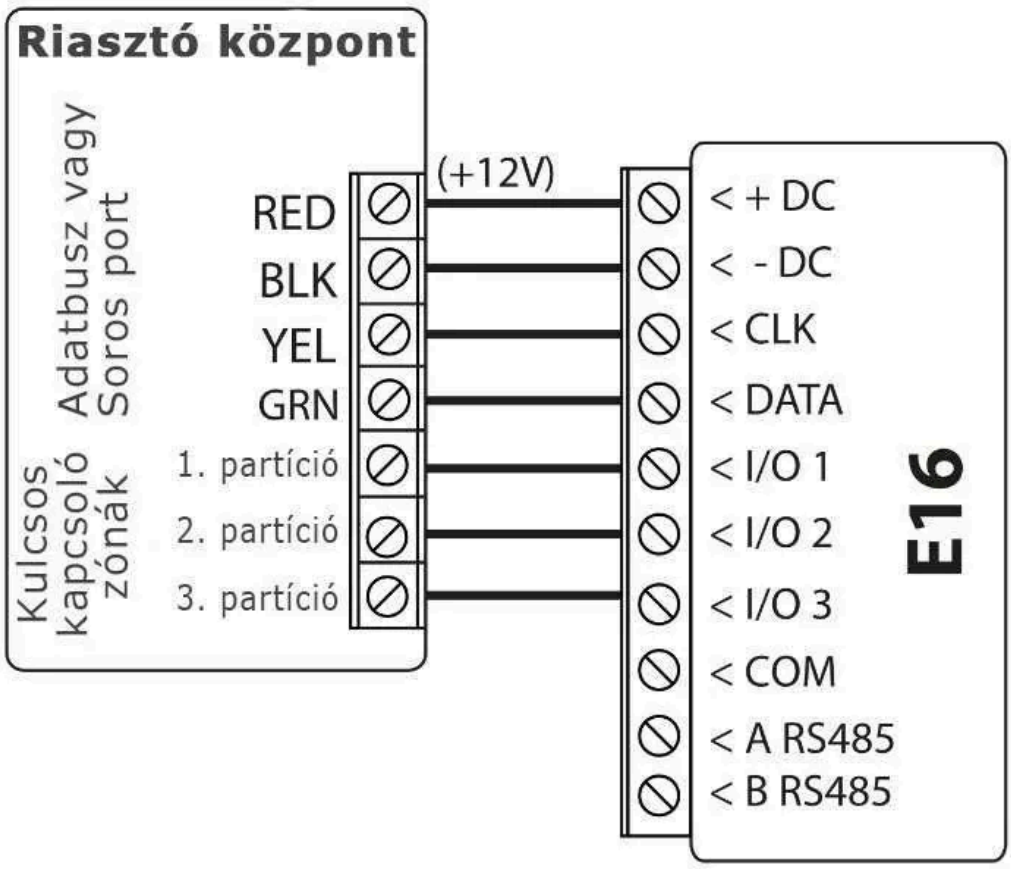
Do portu 0 (Port 0) centrali **Integriti** komunikator podłącza się kablem INTG-996795: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA. Port szeregowy centrali trzeba ustawić na protokół Trikdis (punkt 4.7).



Rysunek 15. Podłączenie do centrali InnerRange Integriti kablem Inner Range o numerze katalogowym INTG-996795: +DET (+13 V) → +DC, Port 0 GND (5) → −DC, Rx (3) → CLK, Tx (2) → DATA.

3.4 Podłączenie strefy przełącznika kluczowego

Jeśli centrala nie należy do typów ze sterowaniem bezpośrednim albo nie chcesz używać sterowania bezpośredniego, zdalne uzbrajanie i rozbrajanie można rozwiązać **strefą przełącznika kluczowego**: jeden z zacisków I/O komunikatora ustawiasz jako **wyjście** (strona IN/OUT, punkt 6.6) i podłączasz do strefy przełącznika kluczowego centrali. Po aktywacji wyjście zwiera strefę do COM (minusa); rezystor końcowy strefy podłącz zgodnie z typem strefy w centrali. Ponieważ E16 ma trzy zaciski I/O, można obsłużyć nawet trzy partycje osobnymi wyjściami.



Rysunek 16. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego: komunikator odczytuje zdarzenia z magistrali centrali, a wyjścia I/O 1–3 przełączają strefy przełącznika kluczowego 1.–3. partycji centrali.

- Na stronie **System settings** w TrikdisConfig pole **Remote Arm/Disarm** pozostaw **puste** – obu sposobów nie można używać jednocześnie.
- Strefa przełącznika kluczowego może być impulsowa lub dwustanowa; w aplikacji Protegus 2 trzeba ustawić ten sam tryb (punkt 5.3).

Szczegóły i pułapki uzbrajania przełącznikiem kluczowym opisuje osobny artykuł: Zdalne uzbrajanie przełącznikiem kluczowym z aplikacji Protegus 2.

3.5 Podłączenie wejść

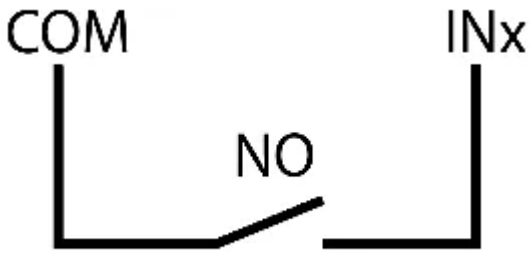
Zaciski I/O komunikatora jako wejścia mogą też przyjmować dodatkowe czujki (np. łącznik sabotażowy, przycisk napadowy, czujnik temperatury), niezależnie od centrali alarmowej. Wejście podłącza się między wybrany zacisk I/O a zacisk COM.

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.

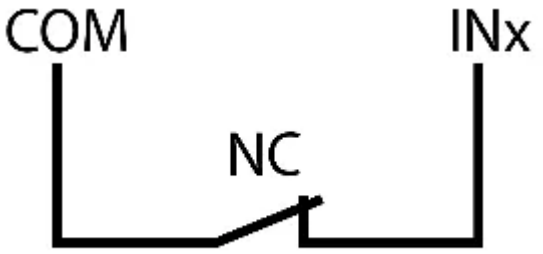
Typ	Stan spoczynkowy	Alarm	Sabotaż
NC	zamknięty	otwarty	–
NO	otwarty	zamknięty	–
NC/EOL	2,2 kΩ	przerwa lub zwarcie	–
NO/EOL	2,2 kΩ	zwarcie lub przerwa	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	przerwa lub zwarcie
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	przerwa lub zwarcie

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**.

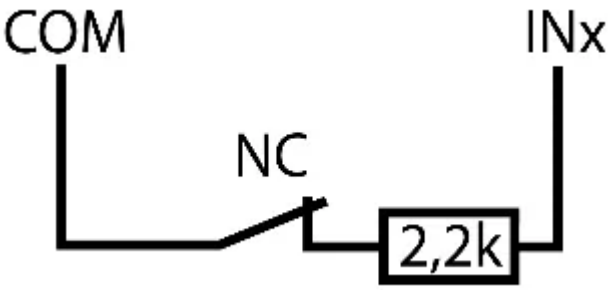
Podłączenie obwodów wejściowych: typy NO, NC, NC/EOL, NO/EOL, NO/DEOL i NC/DEOL z rezystorem końcowym 2,2 kΩ; przy typach DEOL podłączony jest też obwód sabotażowy.



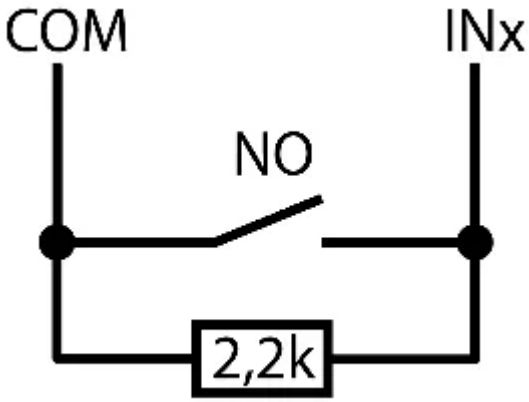
Rysunek 17. NO – obwód normalnie otwarty: zwarty – alarm, otwarty – stan spoczynkowy.



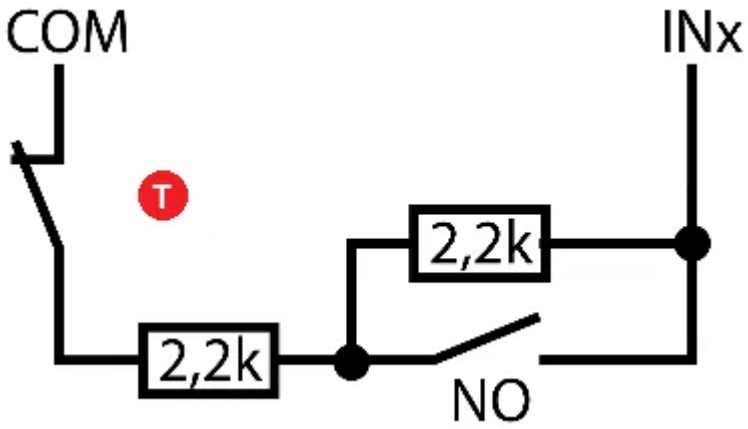
Rysunek 18. NC – obwód normalnie zamknięty: otwarty – alarm, zwarty – stan spoczynkowy.



Rysunek 19. NC/EOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.

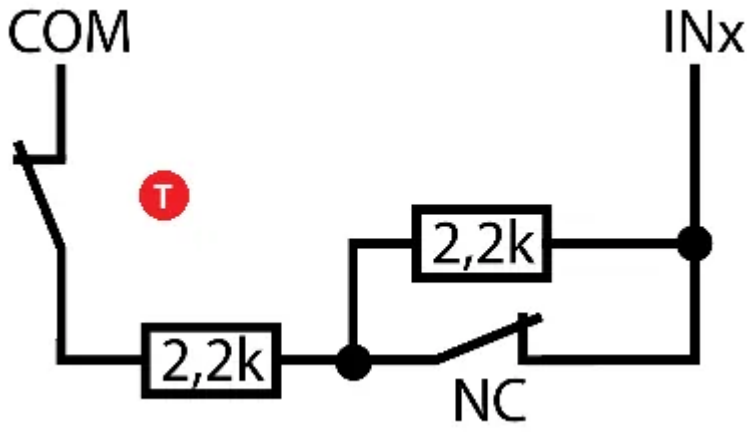


Rysunek 20. NO/EOL – obwód normalnie otwarty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.



Rysunek 21. 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

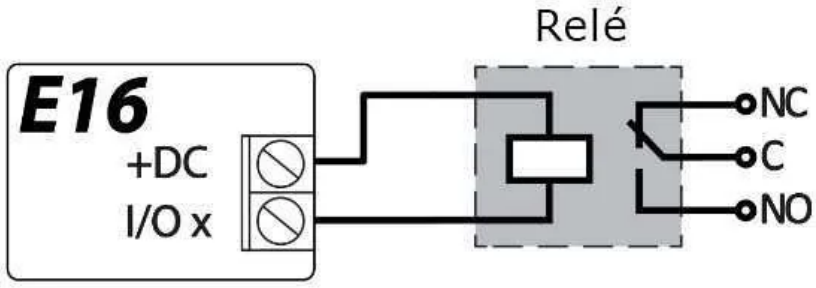


Rysunek 22. NC/DEOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – stan spoczynkowy, 3,3–5,5 kΩ – alarm.

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

3.6 Podłączenie wyjścia z przekaźnikiem

Zaciski I/O jako wyjścia są wyjściami typu otwarty kolektor (OC): w stanie aktywnym zwierają podłączone obciążenie do minusa, najwyżej 0,15 A, do 30 V DC. Stykami przekaźnika możesz włączać i wyłączać różne urządzenia elektryczne. Większe odbiorniki lub urządzenia zasilane z sieci elektrycznej przełączaj **przez przekaźnik**: jeden koniec cewki przekaźnika podłącz do +DC, drugi do zacisku I/O. Używany zacisk I/O trzeba ustawić na stronie **IN/OUT** w TrikdisConfig jako wyjście (**OUT**) (punkt 6.6).

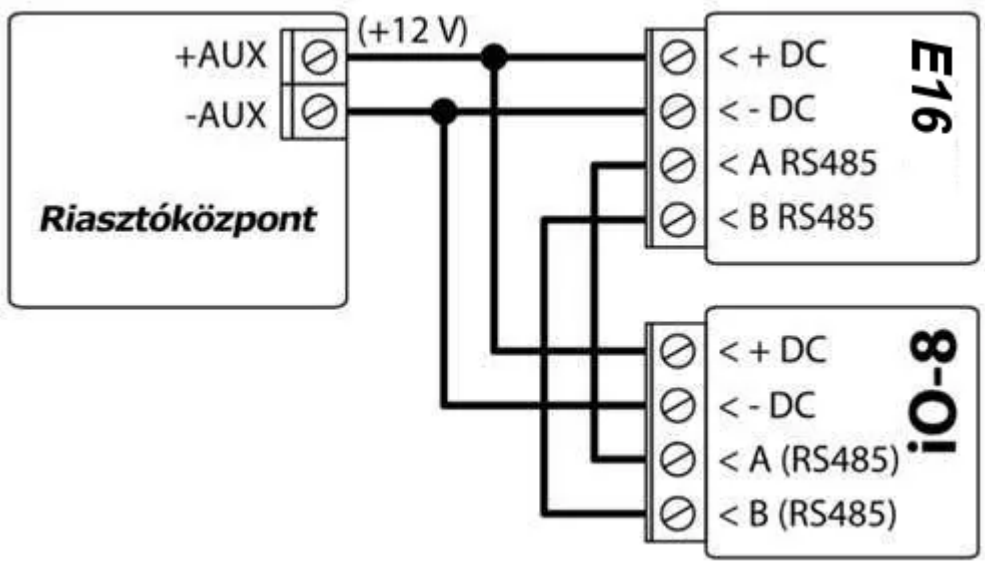


Rysunek 23. Podłączenie przekaźnika do wyjścia komunikatora: cewka między zaciskami +DC i I/O x, styki (NC, C, NO) przełączają odbiornik.

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

3.7 Podłączenie ekspandera iO-8

Jeśli potrzeba więcej wejść lub wyjść, do magistrali RS485 E16 można podłączyć ekspander **iO-8**; każdy daje 8 dodatkowych I/O o podwójnej funkcji. Zaciski A RS485 i B RS485 połącz z zaciskami A i B modułu, a zasilanie modułu weź z 12-woltowego wyjścia AUX centrali. Moduł trzeba dodać na stronie **RS485 modules** w TrikdisConfig (punkt 6.7); zdarzenia z wejść trafiają do stacji monitorowania i do Protegus 2, a wyjściami można sterować z aplikacji.



Rysunek 24. Podłączenie ekspandera iO-8 do magistrali RS485 E16 (A RS485 → A, B RS485 → B); oba urządzenia zasilane z wyjścia AUX centrali alarmowej (+12 V).

3.8 Podłączenie kabla Ethernet

Jeden koniec kabla Ethernet włóż do gniazda RJ45 na płytce drukowanej E16, a drugi do wolnego portu routera lub switcha. Potrzebny jest zwykły kabel prosty (patch); kabel wchodzi przez otwór w obudowie. Nawiązanie połączenia z siecią po włączeniu pokazuje zielone światło diody **NETWORK**.

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;
- **TROUBLE** nie świeci.

Każdy inny obraz diod oznacza jakąś usterkę; jej przyczynę ustal na podstawie tabeli diod w punkcie 1.6. Jeśli TROUBLE miga, liczba mignięć wskazuje przyczynę (punkt 1.6): 1 = brak fizycznego połączenia (kabel, port), 2 = nie otrzymano adresu IP (DHCP), 3 = błąd DNS, 6 = brak połączenia z odbiornikiem lub chmurą Protegus. **7**

mignięć oznacza brak połączenia z centralą: sprawdź przewody CLK i DATA, wybrany typ centrali i – tam, gdzie to potrzebne – programowanie centrali (rozdział 4). Jeśli nie świeci żadna dioda, sprawdź zasilanie i okablowanie.

4. Programowanie centrali alarmowej

Ten rozdział opisuje dla każdego producenta, co trzeba ustawić w centrali alarmowej, aby E16 odczytywał zdarzenia i – tam, gdzie to możliwe – zdalnie sterował centralą. W większości central do odczytu zdarzeń nie trzeba niczego programować; do **sterowania bezpośredniego** zaznacz na stronie **System settings** w TrikdisConfig opcję **Remote Arm/Disarm**, a przy centralach Paradox i Texecom podaj też hasło PC lub UDL centrali w polu **Security panel PC download password** (punkty 2.2 i 6.2).

Jeśli sterujesz centralą nie bezpośrednio, lecz przez strefę przełącznika kluczowego (punkt 3.4), pole **Remote Arm/Disarm** pozostaw puste, a ten rozdział dotyczy tylko ustawień potrzebnych do odczytu zdarzeń.

4.1 DSC

Centrale **DSC PowerSeries** (lista obsługiwanych modeli w punkcie 1.2) nie wymagają żadnych dodatkowych ustawień: komunikator podłączony do magistrali Keybus od razu odczytuje zdarzenia, a po zaznaczeniu **Remote Arm/Disarm** użytkownik uzbraja i rozbraja system z aplikacji własnym kodem manipulatora. Szczegółom sterowania bezpośredniego – stanom stref, blokowaniu stref, automatycznemu rozpoznawaniu partycji – poświęcony jest osobny artykuł: Sterowanie bezpośrednie centralami alarmowymi DSC PowerSeries.

Z centralami **DSC PowerSeries NEO** komunikator nie działa: producent centrali nie dopuszcza do magistrali NEO urządzeń zewnętrznych. Do NEO odpowiedni jest komunikator z wejściem linii telefonicznej (TIP/RING) – zobacz DSC Power Series NEO i komunikatory Trikdis: kompatybilność i rozwiązania.

4.2 Paradox

Centrale **Paradox** trzeba programować tylko do sterowania bezpośredniego; do odczytu zdarzeń nie trzeba niczego ustawiać. Firmware centrali musi mieć wersję co najmniej **V.4**.

W nowszych centralach Paradox (na przykład w seriach SP+, MG+ i EVOHD+) port szeregowy może być **fabrycznie zablokowany**: komunikator nie otrzymuje danych, dopóki nie odblokujesz portu. Sposób odblokowania: Odblokowanie zablokowanego portu szeregowego w centralach alarmowych Paradox.

Do sterowania trzeba ustawić **hasło PC** centrali (PC password) i wpisać to samo hasło w polu **System settings → Security panel PC download password** programu TrikdisConfig – oba muszą być identyczne.

1. Wejdź w programowanie instalatora centrali na manipulatorze.
2. Otwórz sekcję hasła PC: w seriach **MAGELLAN i SPECTRA** sekcję **911**, w serii **DIGIPLEX EVO** sekcję **3012**.
3. Wprowadź **4-znakowe** hasło. Hasło nie może być 0000 i **nie może zaczynać się od zera**.
4. Wyjdź z programowania i **uruchom ponownie centralę** – zmiana hasła PC zaczyna obowiązywać po ponownym uruchomieniu. Następnie wpisz to samo hasło w TrikdisConfig.

Typowe błędy i ich rozwiązanie

- **Kod manipulatora przypisany do partycji nie może być kodem głównym (master)**: nadaj użytkownikowi inny kod, a uzbrajanie / rozbrajanie z Protegus 2 będzie działać.

- **Po każdej zmianie kodu manipulatora uruchom ponownie komunikator** (odłączenie zasilania lub polecenie SMS `RESET`): kody odczytuje przy uruchomieniu, późniejszej zmiany nie widzi.

4.3 Texecom

Centrale **Texecom Premier / Premier Elite** trzeba zaprogramować zarówno do odczytu zdarzeń, jak i do sterowania: należy ustawić 4-znakowe hasło centrali o nazwie **UDL passcode** i wpisać to samo hasło w polu **System settings → Security panel PC download password** programu TrikdisConfig – oba muszą być identyczne.

Za pomocą programu Texecom Wintex: UDL passcode znajduje się na karcie **Options** okna **Communication Options**.

Z manipulatora:

1. Wprowadź 4-cyfrowy kod instalatora i naciśnij przycisk **[Menu]**, aby wejść do menu programowania.
2. Zaraz potem naciśnij przycisk **[9]**.
3. Naciśnij **[7][6]**, a następnie przycisk **[2]** i wprowadź 4-cyfrowy UDL passcode.
4. Naciśnij przycisk **[Yes]**, a następnie wyjdź z programowania przyciskiem **[Menu]**.

4.4 UTC Interlogix (Caddx)

Firmware centrali **UTC Interlogix (Caddx) NetworX** musi mieć wersję co najmniej **V2**. Na manipulatorze centrali trzeba ustawić następujące parametry:

1. Naciśnij przyciski **[*][8]** i wprowadź kod instalatora (fabrycznie **9713**).
2. Wprowadź **numer urządzenia** przypisany komunikatorowi (device address; fabrycznie **0**).
3. Zaprogramuj kolejno wiersze poniższej tabeli: wprowadź lokację (location), numer segmentu, a następnie ustawienie. Przyciskiem **[*]** możesz wrócić do poprzedniego pola. `12345678` oznacza, że wszystkie osiem przełączników segmentu jest włączonych (na wyświetlaczu widać wszystkie cyfry).

Lokacja (location)	Segment	Ustawienie
23	3	12345678
37 (niekoniecznie wymagane)	3	12345678
37 (niekoniecznie wymagane)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Po zaprogramowaniu wszystkich wierszy naciśnij dwukrotnie przycisk **[Exit]**, aby wyjść z programowania.

4.5 Crow i Pyronix

Centrale **Crow Runner 4/8** i **Runner 8/16** nie wymagają żadnych dodatkowych ustawień.

Centrale **Pyronix** również nie wymagają programowania, ale po skonfigurowaniu i podłączeniu komunikatora **odłącz zasilanie centrali** (sieciowe i akumulator) i uruchom ją ponownie: centrala akceptuje komunikator podłączony do swojej magistrali podczas uruchamiania.

4.6 Honeywell Ademco Vista

Firmware centrali **Honeywell Ademco Vista-20** i **Vista-48** musi mieć wersję co najmniej **V5.3**. Ustawienia wprowadzasz na manipulatorze centrali.

Wejście w tryb programowania – na dwa sposoby:

- wprowadź kod instalatora (fabrycznie **4112**), a następnie naciśnij przyciski **[8][0][0]**; albo
- włącz zasilanie centrali i **w ciągu 50 sekund** naciśnij jednocześnie przyciski **[*]** i **[#]** (działa to tylko wtedy, gdy wcześniej wyjście z programowania nastąpiło przyciskami [*][9][8]).

Ustawienia:

1. Włącz wysyłanie zdarzeń Contact ID na wyjściu radiowym dalekiego zasięgu (LRR): naciśnij przyciski **[*][2][9][1][#]**.
2. Do zdalnego sterowania włącz użycie **2. adresu AUI** (2nd AUI address): naciśnij przyciski **[*][1][8][9][1][1][#]**.

Wyjście z programowania: naciśnij przyciski **[*][9][9]**.

4.7 InnerRange Inception i Integriti

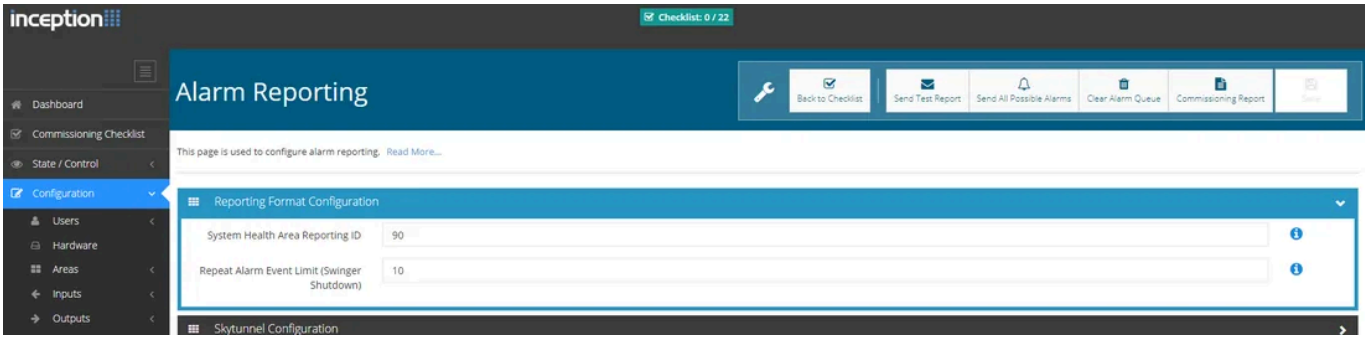
Firmware centrali **InnerRange Inception** musi mieć wersję co najmniej **2.3.0.3507-r0**, a centrala potrzebuje połączenia z internetem. Ustawienia wprowadzasz w interfejsie WWW centrali:

1. Otwórz w przeglądarce adres `https://skytunnel.com.au/inception/NUMER_SERYJNY`, gdzie NUMER_SERYJNY to numer seryjny podany na pudełku centrali. Zaloguj się na konto instalatora.
2. Otwórz stronę **Configuration → General → Alarm Reporting**.
3. W grupie **3rd Party Device Configuration**: - zaznacz opcję **Enable 3rd Party Device Reporting**; - w polu **3rd Party Device Type** wybierz wartość **Trikdis**; - w polu **Serial Port** wybierz wartość **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Zapisz ustawienia i wyjdź z interfejsu.

Firmware centrali **InnerRange Integriti** musi mieć wersję co najmniej **19.1.0.36608**, a jej oprogramowanie do programowania (Integriti Professional) co najmniej **19.1.0.15396**. Ustawienia wprowadzasz w oprogramowaniu do programowania centrali:

1. Dla portu szeregowego (**TTL Port-0**), do którego podłączony jest komunikator, wybierz protokół komunikacyjny **Trikdis**.
2. Format danych musi być **Contact ID**.
3. Ustawienia portu: **19200, 8, N, 1**.
4. Zapisz ustawienia i zamknij program.

Inception i Integriti przekazują komunikatorowi zdarzenia; do uzbrajania i rozbrajania potrzebna jest strefa przełącznika kluczowego (punkty 1.2 i 3.4).



Rysunek 25. Interfejs webowy Inception – Configuration → General → Alarm Reporting.



Rysunek 26. Inception – 3rd Party Device Configuration.

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

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. W E16 uzbrajanie może odbywać się na dwa sposoby: w centralach **ze sterowaniem bezpośrednim** użytkownik używa własnego **kodu manipulatora**, w centralach podłączonych przez strefę przełącznika kluczowego – **wyjścia** komunikatora.

5.1 Dodanie urządzenia

Przed dodaniem urządzenia sprawdź:

1. E16 jest podłączony do sieci i ma dostęp do internetu: dioda **NETWORK** świeci na zielono, dioda **TROUBLE** nie miga.
2. Na stronie **User reporting** → **PROTEGUS Cloud** w TrikdisConfig zaznaczone jest **Enable connection**, a **Protegus Cloud access code** jest ustawiony (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:

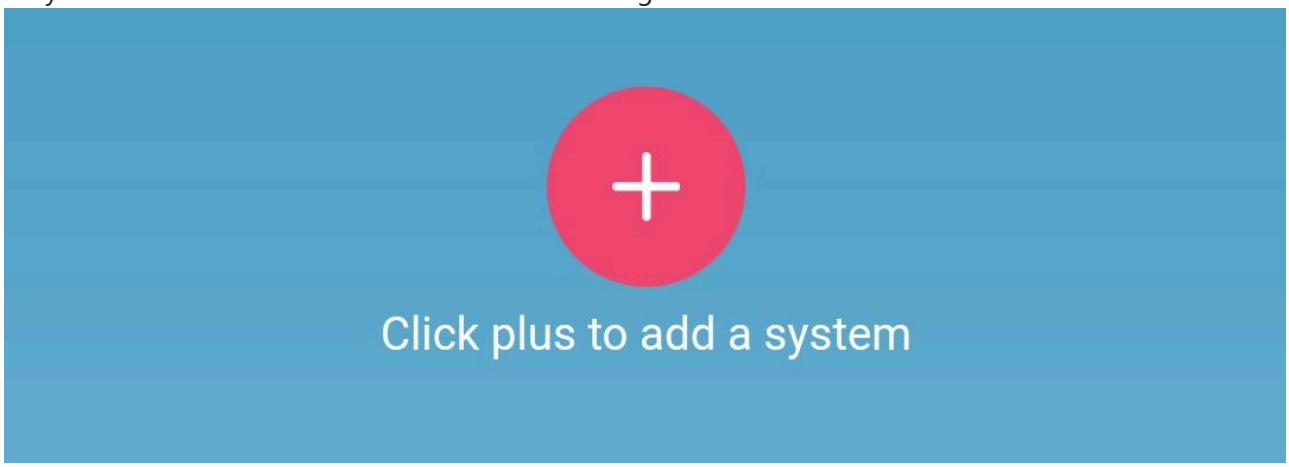
komunikat nie może zostać wysłany. W sieci komórkowej najczęściej winny jest APN albo usługa transmisji danych karty SIM, przy Ethernecie router, zapora sieciowa (firewall) lub DNS. Jeśli dioda DATA zgaśnie, komunikat został wysłany, a połączenie danych działa prawidłowo.

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

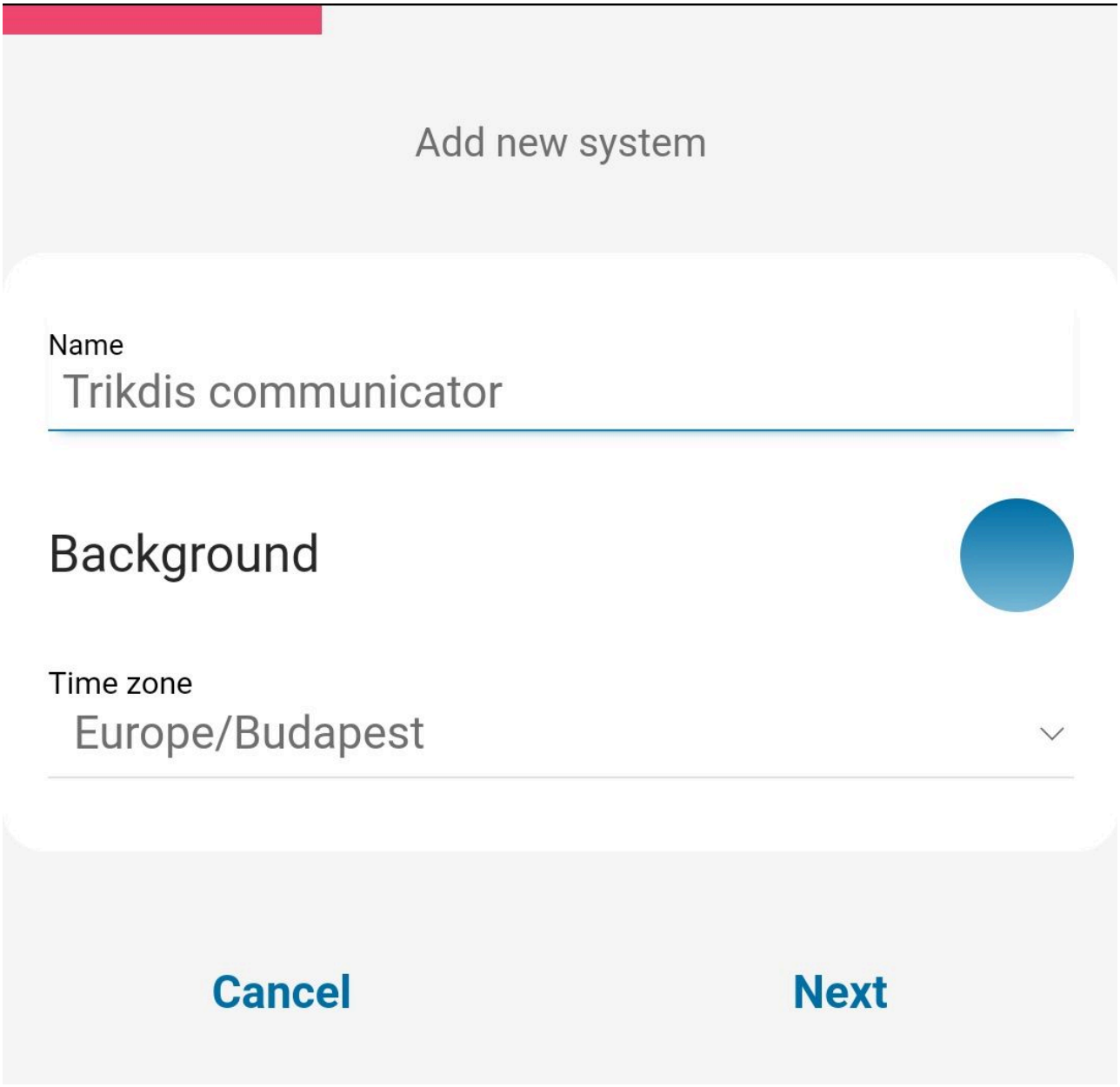


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

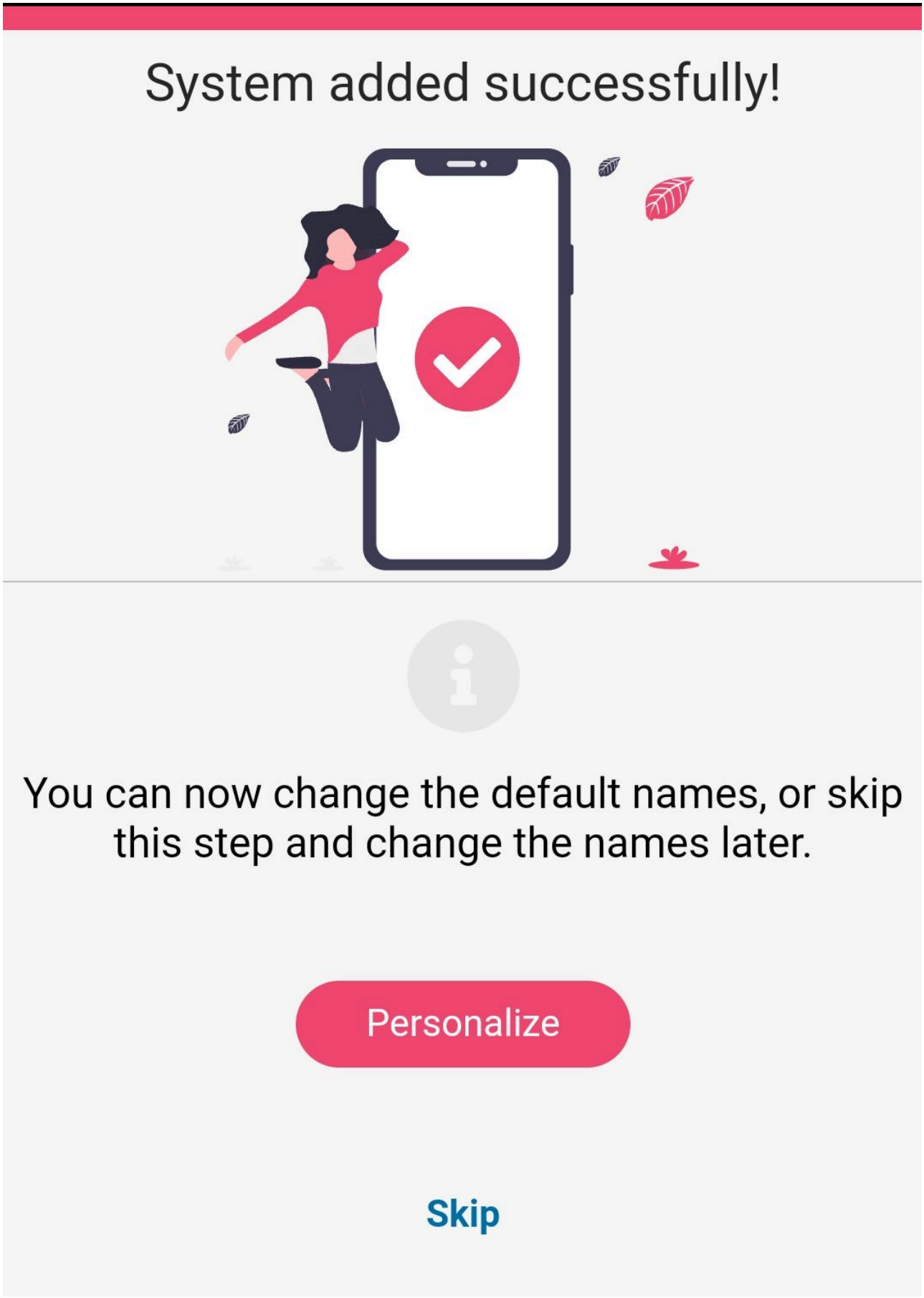
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



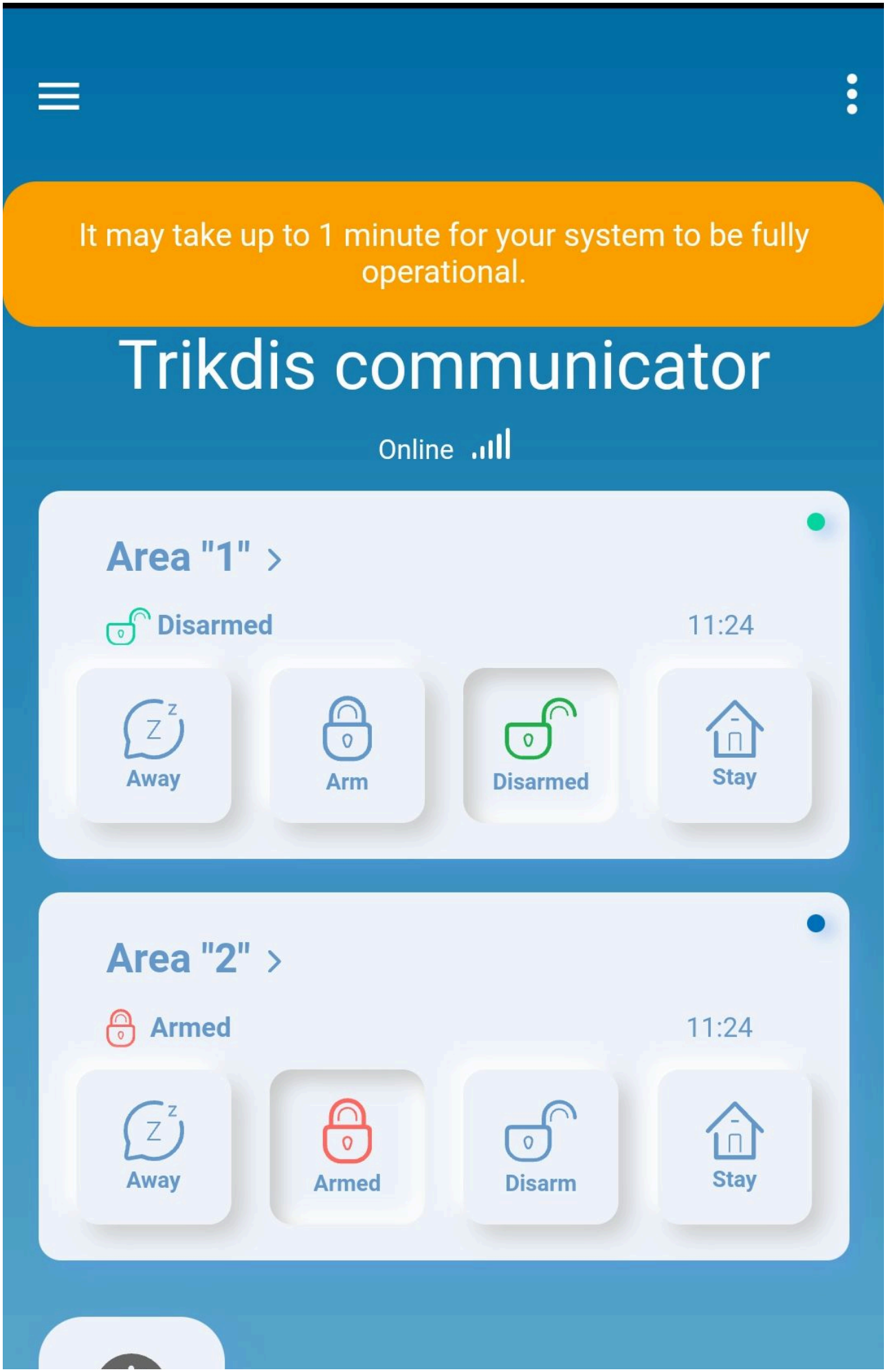
6. Add meg a rendszer nevét és válassz idozónát



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 E16 jest **adres MAC (Unique ID)**: znajduje się na pudełku i na tylnej części urządzenia, pokazuje go też pasek stanu TrikdisConfig (punkt 6.1). Przy tworzeniu systemu w aplikacji trzeba go podać jako identyfikator urządzenia.

5.2 Sterowanie bezpośrednie kodem manipulatora

Jeśli centrala należy do typów ze sterowaniem bezpośrednim (punkt 1.2), a na stronie **System settings** w TrikdisConfig zaznaczone jest **Remote Arm/Disarm**, Protegus 2 pokazuje partycje centrali ze stanem odczytanym z magistrali, a do uzbrojenia / rozbrojenia użytkownik podaje w aplikacji **kod manipulatora centrali** – ten sam, którego używa na manipulatorze. Osobne wyjście i strefa przełącznika kluczowego nie są potrzebne.

- W centrali potrzebne jest do tego ustawienie zależne od producenta (Paradox: hasło PC, Texecom: hasło UDL; w centralach Caddx, Honeywell i InnerRange włączenie magistrali lub portu szeregowego jest potrzebne już do odczytu zdarzeń) – zobacz rozdział 4.
- Kod manipulatora sprawdza centrala, a dziennik zdarzeń centrali też zapisuje użytkownika, nie komunikator.
- W centrali Paradox kod użytkownika **nie może być kodem głównym (master)**; po zmianie kodu uruchom ponownie komunikator (punkt 4.2).
- W centrali DSC PowerSeries aplikacja pokazuje też stan stref i możliwe jest blokowanie stref – szczegóły w artykule o sterowaniu bezpośrednim DSC (artykuł dotyczy G16, ale tak samo odnosi się do E16).

Przy tworzeniu systemu Protegus 2 zapyta, czy uzbrajaniem steruje wyjście komunikatora. Przy sterowaniu bezpośrednim **nie** przypisuj partycji wyjścia (**Control with Protegus2** wyłączone): partycją zarządza centrala, a stan przychodzi z magistrali.

5.3 Uzbrajanie strefą przełącznika kluczowego

Jeśli centralą nie można sterować bezpośrednio albo nie chcesz jej tak używać, jedno z wyjść komunikatora podłączasz do strefy przełącznika kluczowego centrali (punkt 3.4), w TrikdisConfig pole **Remote Arm/Disarm** pozostaje puste, a w Protegus 2 przypisujesz wyjście do partycji.

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.

5.4 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.

Przy sterowaniu bezpośrednim aplikacja prosi o kod manipulatora centrali; przy uzbrajaniu przełącznikiem kluczowym – jeśli jest włączone – o hasło Protegus 2.

E16 nie ma sterowania SMS ani powiadomień SMS: uzbrajanie, rozbrajanie i sterowanie wyjściami odbywa się z aplikacji Protegus 2, a powiadomienia przychodzą jako wiadomości push.

6. TrikdisConfig – ustawienia szczegółowo

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 E16 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.

Etykieta	Znaczenie
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.

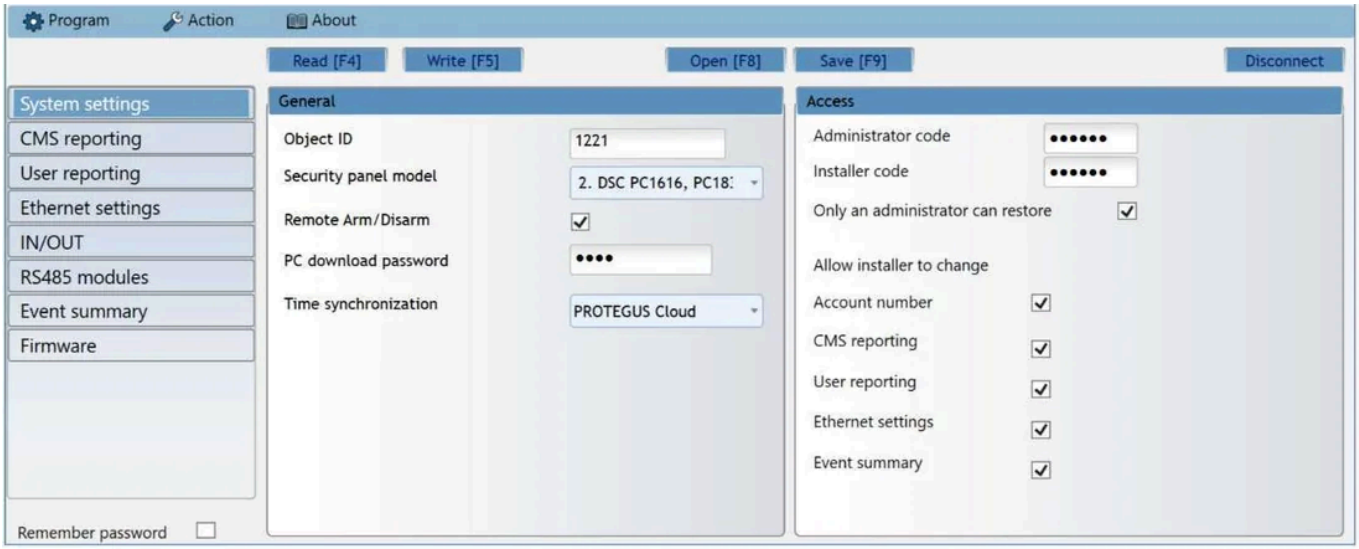


Rysunek 27. Pasek stanu TrikdisConfig po odczycie E16: adres MAC (Unique ID, na ilustracji pozostawiony pusty), stan, typ (E16_1100), numer seryjny, wersje, sposób połączenia i poziom dostępu.

W E16 unikalnym identyfikatorem urządzenia jest **adres MAC**: o niego prosi Protegus 2 przy tworzeniu systemu i TrikdisConfig przy zdalnym dostępie (Unique ID). Ten sam adres znajduje się też na pudełku i na tylnej części urządzenia.

6.2 System settings

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



Rysunek 28. TrikdisConfig – strona System settings: grupy General i Access.

- **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe, 0–9, A–F). Obowiązkowy, jeśli urządzenie raportuje także do stacji monitorowania; wartości `FFFE` i `FFFF` nie można używać.
- **Security panel model** – typ podłączonej centrali alarmowej z listy. Od niego zależy, jak komunikator odczytuje magistralę, dlatego wybierz dokładny typ podłączonej centrali.

- **Remote Arm/Disarm** – po zaznaczeniu komunikator steruje centralą bezpośrednio: użytkownik uzbraja i rozbraja system z Protegus 2 swoim kodem manipulatora. Pojawia się tylko przy typach central ze sterowaniem bezpośrednim; w centrali potrzebne jest do tego ustawienie zależne od producenta (rozdział 4). Przy uzbrajaniu strefą przełącznika kluczowego pozostaw puste.
- **Security panel PC download password** – do bezpośredniego sterowania centralą Paradox i Texecom hasło PC lub UDL centrali (4 znaki); musi być takie samo jak ustawione w centrali (punkty 4.2 i 4.3).
- **Time synchronization** – źródło zegara urządzenia (domyślnie **PROTEGUS Cloud**, chmura Protegus).

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

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

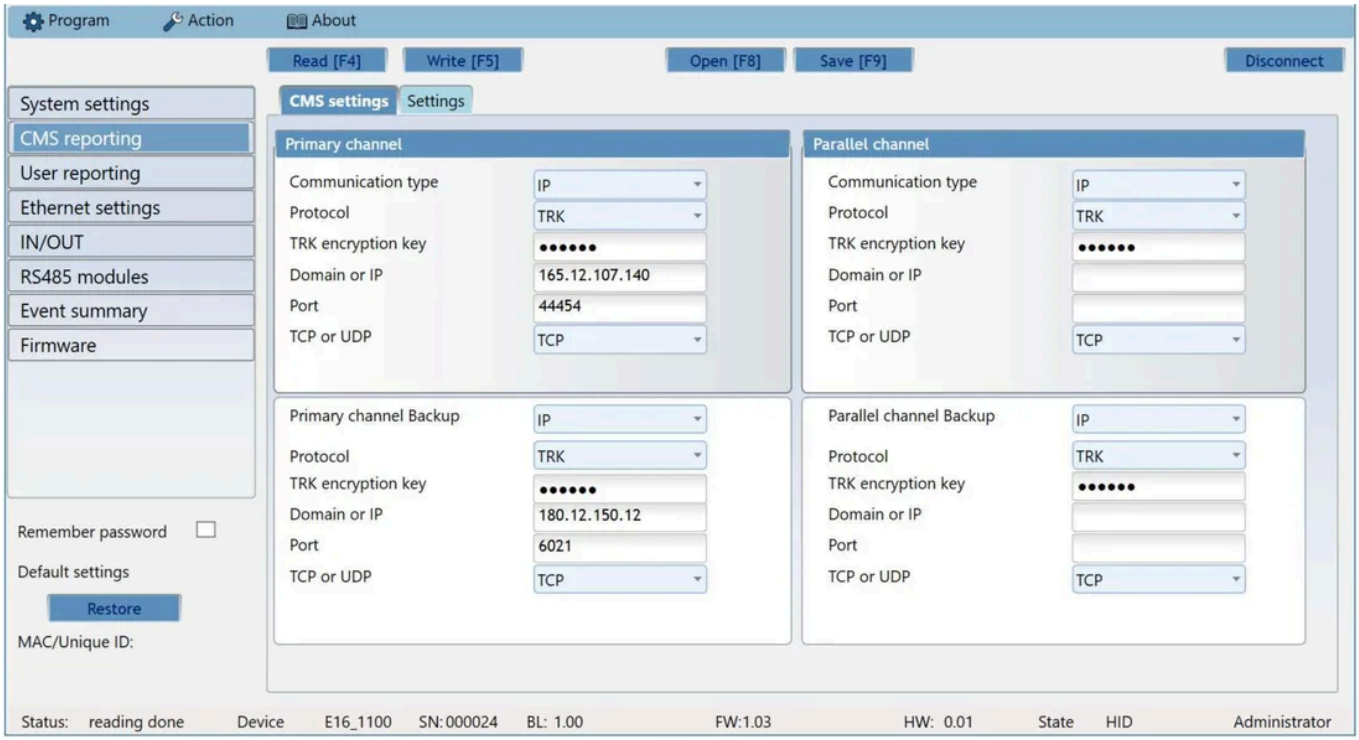
- **Administrator code** – dostęp do wszystkich ustawień (hasło fabryczne: `123456`; hasło ma 6 znaków: cyfry lub litery łacińskie).
- **Installer code** – dostęp, który można ograniczyć (hasło fabryczne: `654321`).
- **Only an administrator can restore** – po zaznaczeniu przywrócenie ustawień fabrycznych 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 przekazania do oprogramowania stacji monitorowania potrzebny jest odbiornik Trikdis (odbiornik programowy IPcom dla Windows lub Linux, sprzętowy odbiornik IP/SMS RL14, odbiornik wielokanałowy RM14) albo odbiornik uniwersalny obsługujący protokół DC-09 / TL150.



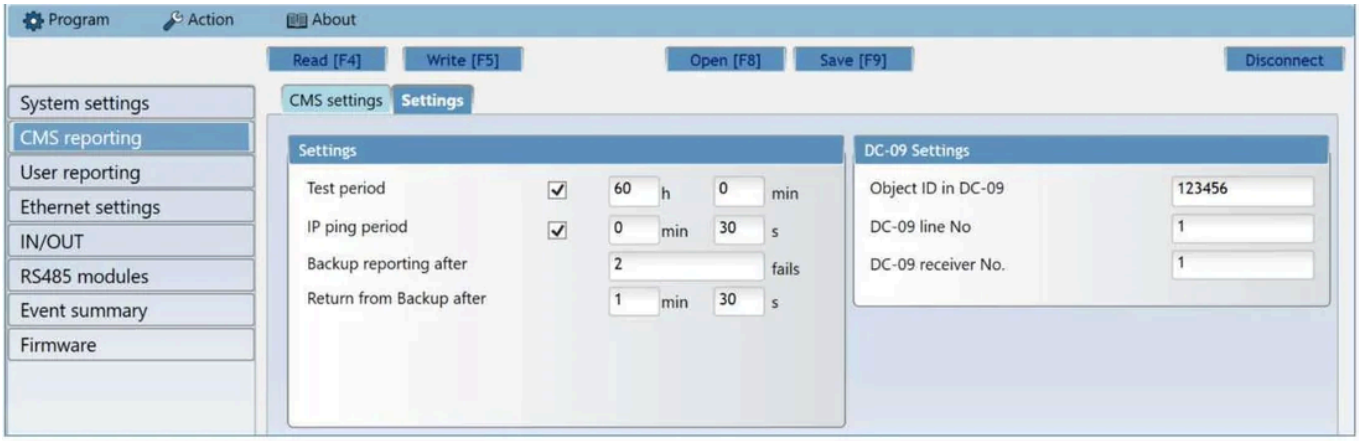
Rysunek 29. TrikdisConfig – CMS reporting, zakładka CMS settings: kanał główny i równoległy (u góry), należące do nich kanały zapasowe (na dole).

Primary channel – kanał główny

- **Communication type** – **IP**; wartością **Disable** kanał można wyłączyć (na przykład gdy urządzenie działa tylko z Protegus 2, bez stacji monitorowania).
- **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 i port odbiornika.
- **TCP or UDP** – protokół transmisji.

Primary channel Backup – kanał zapasowy. Przejmuje komunikację, gdy kanał główny nie działa; jego ustawienia są takie same jak powyżej. Ponieważ E16 komunikuje się jedną drogą sieciową (przez sieć lokalną), kanał zapasowy to drugi adres odbiornika na tej samej drodze: chroni przed awarią po stronie odbiornika, ale nie przed utratą łącza internetowego.

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



Rysunek 30. TrikdisConfig – CMS reporting, zakładka Settings: raport testowy, PING, czasy kanału zapasowego i dane DC-09.

Na zakładce **Settings** ustawiasz czasy i dane DC-09.

- **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.

Grupa **DC-09 settings** jest widoczna tylko wtedy, gdy na którymś kanale ustawiono protokół DC-09. Serwery nazw (DNS) w E16 podajesz nie tutaj, lecz na stronie **Ethernet settings** (punkt 6.5).

6.4 User reporting

Na zakładce **PROTEGUS Cloud** włączasz usługę Protegus, dzięki której użytkownik może zdalnie obserwować komunikator i nim sterować; więcej o usłudze: www.protegus.app. E16 nie ma powiadomień SMS ani sterowania SMS, dlatego na tej stronie jest tylko ta jedna zakładka.



Rysunek 31. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

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

6.5 Ethernet settings

Tutaj ustawiasz, jak E16 łączy się z siecią lokalną. Fabrycznie zaznaczone jest **Use DHCP**: urządzenie automatycznie otrzymuje z routera adres, bramę i serwery nazw, i w większości miejsc nie trzeba nic więcej robić.



Rysunek 32. TrikdisConfig – strona Ethernet settings: DHCP lub ręczne ustawienia sieci, serwery nazw.

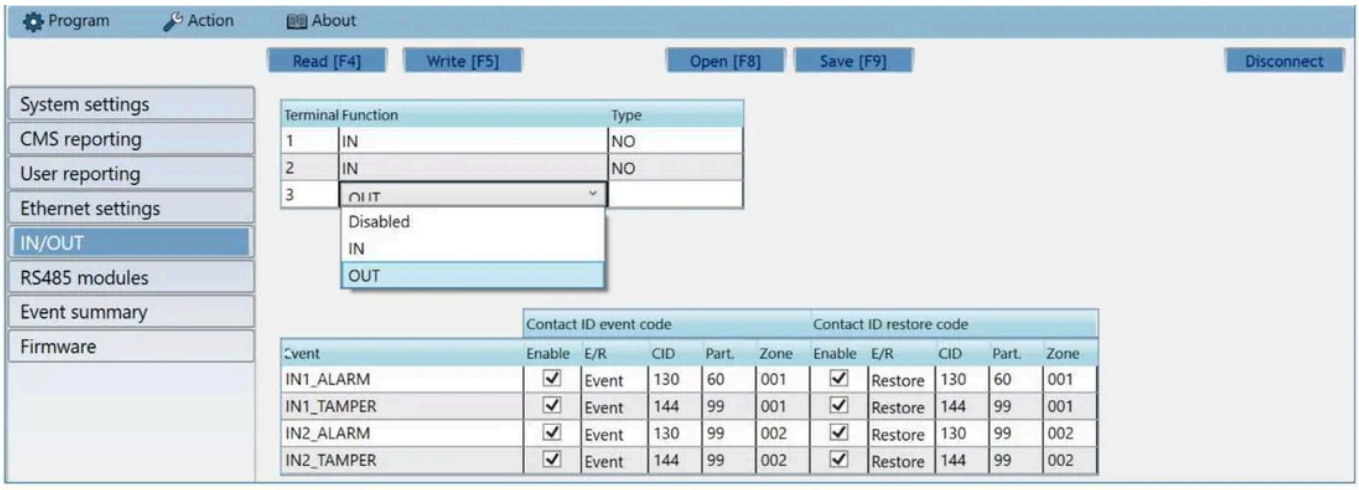
- **Use DHCP** – po zaznaczeniu urządzenie automatycznie otrzymuje adres IP, maskę podsieci i bramę z serwera DHCP routera. To ustawienie fabryczne i w większości miejsc nie trzeba nic więcej robić. Jeśli w sieci nie ma DHCP, jeśli automatyczne logowanie do sieci się nie udaje albo administrator sieci 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.

6.6 IN/OUT

Tutaj określasz rolę trzech zacisków I/O komunikatora 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). Ustawienie fabryczne: I/O 1 i I/O 2 – wejście (NO), I/O 3 – wyjście.



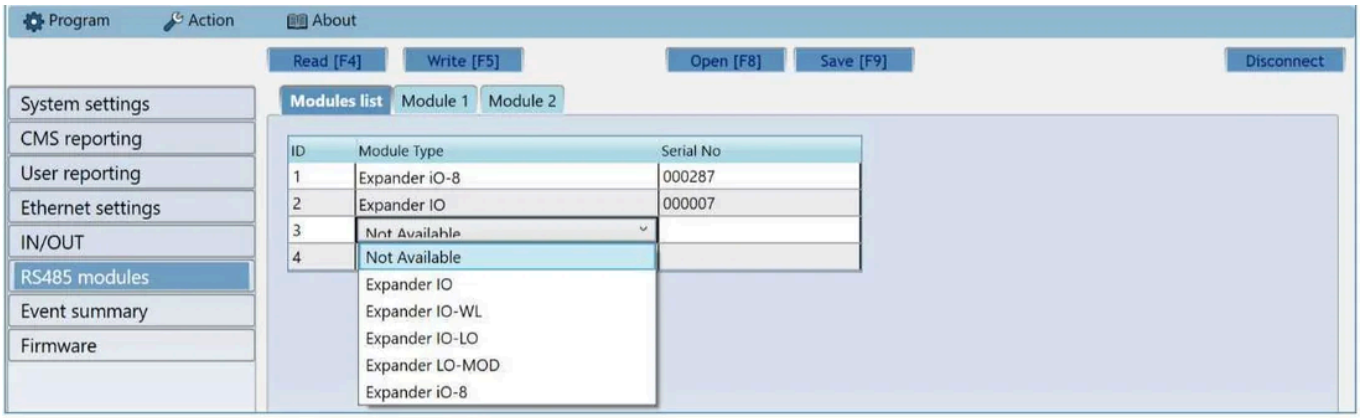
Rysunek 33. TrikdisConfig – strona IN/OUT: funkcja zacisków I/O i zdarzenia wejść.

Przy naruszeniu czujki podłączonej do wejścia komunikator wysyła własne zdarzenie (**INx_ALARM**, Contact ID 130), a przy 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 (przywrócenie).
- **CID** – kod Contact ID; możesz go podać albo pozostawić wartość domyślną. Zdarzenie trafia z tym kodem do Protegus 2 i do stacji monitorowania.
- **Part.** – numer partycji w komunikacie.
- **Zone** – numer strefy w komunikacie.

6.7 RS485 modules

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

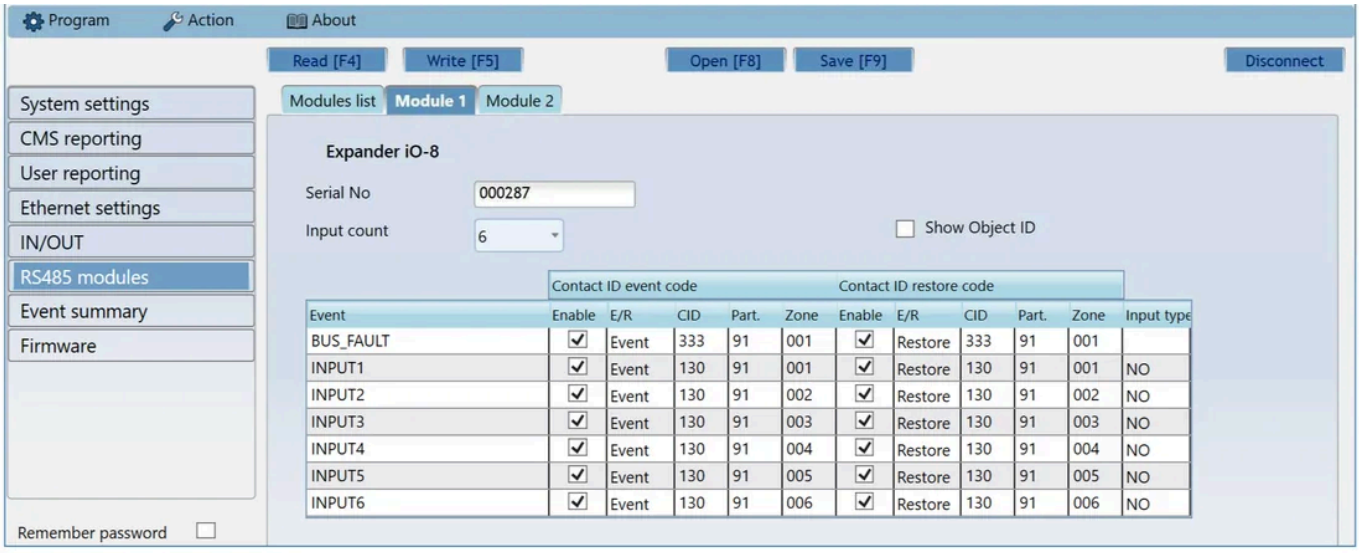


Rysunek 34. TrikdisConfig – RS485 modules, zakładka Modules list: typ modułu (Expander iO-8) i numer seryjny.

- **Module Type** – typ podłączonego modułu z listy (**Expander iO-8**).
- **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 35. TrikdisConfig – RS485 modules, zakładka modułu iO-8 (u góry) i tabela zdarzeń ekspandera (na dole).

- **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 strefą przełącznika kluczowego albo sterowanie urządzeniem) 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 przywrócenia 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** dla wejść można podać identyfikator obiektu inny niż komunikatora.

6.8 Event summary

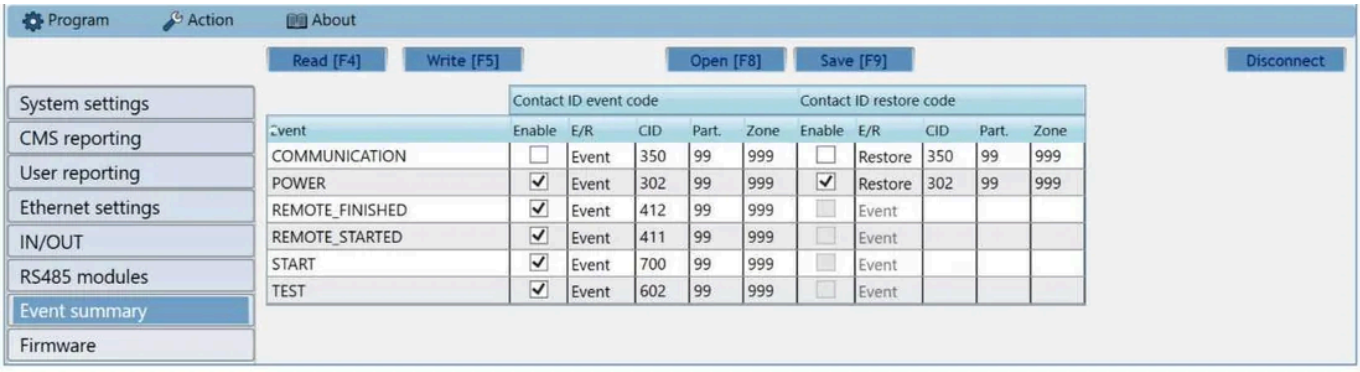
Na tej stronie włączasz lub wyłączasz **własne, wewnętrzne komunikaty** urządzenia oraz zmieniasz ich kod Contact ID, numer partycji i strefy. Komunikatu wyłączonego tutaj urządzenie nie wysyła żadnym kanałem. Fabrycznie komunikaty są wysyłane z partycją 99 i strefą 999.

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.

Komunikat	Contact ID	Kiedy powstaje
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 36. TrikdisConfig – strona Event summary: wewnętrzne komunikaty urządzenia (COMMUNICATION, POWER, REMOTE_FINISHED, REMOTE_STARTED, START, TEST) i należące do nich kody Contact ID.

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.

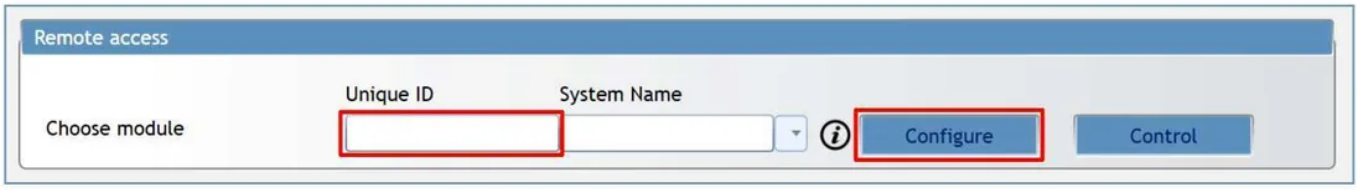
Do zdalnego dostępu potrzebne jest:

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 37. TrikdisConfig – Remote access: identyfikator urządzenia (Unique ID – w E16 adres MAC), nazwa systemu i przycisk Configure.

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.

Przy centrali podłączonej do magistrali sprawdź też, czy komunikator rzeczywiście odczytuje dane z centrali: uzbrój i rozbrój centralę z manipulatora i zobacz, czy na liście zdarzeń Protegus 2 (i w stacji monitorowania) zdarzenie pojawia się z prawidłowym numerem partycji i użytkownika. Przy sterowaniu bezpośrednim wykonaj też próbne uzbrojenie z aplikacji, kodem manipulatora użytkownika.

Sprawdź też zachowanie przy utracie sieci: odłącz kabel Ethernet i zobacz, czy dioda TROUBLE sygnalizuje brak 1 mignięciem, a po ponownym podłączeniu – czy dioda NETWORK znów świeci na zielono i czy zapisane zdarzenia docierają do stacji monitorowania i do aplikacji.

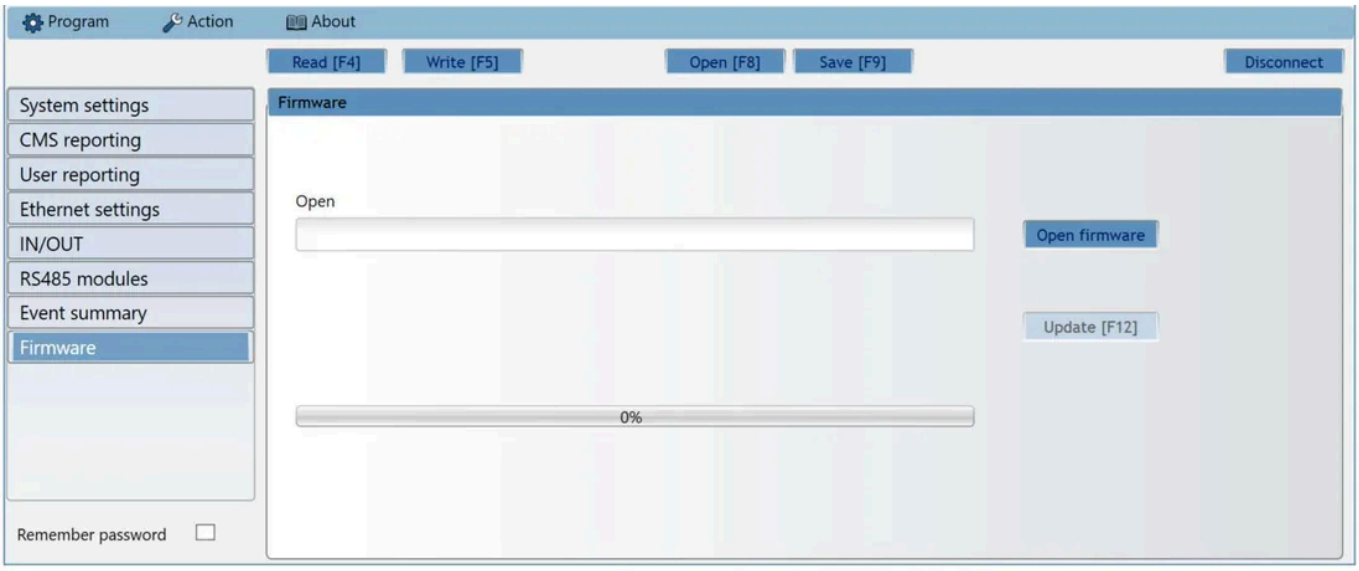
9. Aktualizacja firmware

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 38. TrikdisConfig – strona Firmware: Open firmware i Update [F12] (u góry), wskaźnik postępu aktualizacji (na dole).

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

10. Rozwiązywanie problemów i FAQ

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

Dioda NETWORK nie świeci – brak sieci

1. Sprawdź mignięcia diody **TROUBLE**: 1 = brak fizycznego połączenia (kabel, port), 2 = nie otrzymano adresu IP (DHCP), 3 = nie można rozwiązać nazwy odbiornika lub chmury Protegus (DNS).
2. **1 mignięcie:** sprawdź kabel Ethernet na obu końcach oraz czy port routera lub switcha działa (świeci dioda portu); spróbuj innego portu lub kabla.
3. **2 mignięcia:** na routerze musi być włączony DHCP albo nadaj urządzeniu stały adres IP na stronie **Ethernet settings** (punkt 6.5). W sieci firmowej administrator może dopuścić urządzenie na podstawie adresu MAC.
4. **3 mignięcia:** serwer nazw jest niedostępny. Fabrycznie ustawiony jest publiczny DNS Google; jeśli sieć blokuje zewnętrzne DNS, podaj lokalny serwer nazw na stronie **Ethernet settings**.

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. W sieci filtrowanej zaporą trzeba zezwolić na wychodzący ruch TCP/UDP do portu odbiornika; otwierać portu (przychodzącego) na routerze nie trzeba.

Dioda TROUBLE miga siedem razy – komunikator nie widzi centrali

1. Sprawdź podłączenie według schematu w punkcie 3.3: najczęstszy błąd to zamienione przewody **CLK** i **DATA** albo linia danych podłączona do niewłaściwego zacisku centrali.
2. W polu **System settings** → **Security panel model** w TrikdisConfig musi być wybrany dokładny typ podłączonej centrali.
3. W centralach Texecom, Caddx, Honeywell i InnerRange potrzebne jest też ustawienie w centrali (rozdział 4) – bez niego centrala nie podaje danych na magistralę.
4. W centrali Paradox port szeregowy może być fabrycznie zablokowany – tak go odblokujesz.
5. Centralę Pyronix po podłączeniu odłącz od zasilania i uruchom ponownie, aby zaakceptowała komunikator.
6. Z centralą DSC PowerSeries **NEO** E16 nie działa (do magistrali NEO nie można podłączać urządzeń zewnętrznych) – tu potrzebny jest komunikator na linię telefoniczną (E16T).

Zdarzenia docierają, ale nie mogę uzbroić systemu z aplikacji

Przy sterowaniu bezpośrednim:

1. Na stronie **System settings** musi być zaznaczone **Remote Arm/Disarm**.
2. Przy centralach Paradox i Texecom **Security panel PC download password** musi być zgodne z hasłem PC lub UDL centrali (punkty 4.2 i 4.3).
3. W centrali Paradox firmware centrali musi mieć wersję co najmniej **V.4**; kod użytkownika nie może być kodem głównym (master); po zmianie kodu uruchom ponownie komunikator.
4. W centrali Honeywell Vista musi być włączony 2. adres AUI (punkt 4.6).
5. W Protegus 2 do partycji **nie** może być przypisane wyjście (Control with Protegus2 wyłączone).

Przy strefie przełącznika kluczowego:

1. **Remote Arm/Disarm** musi być puste, a zacisk I/O na stronie **IN/OUT** ustawiony jako **OUT**.
2. Strefa centrali musi być typu przełącznik kluczowy, a w Protegus 2 do partycji musi być przypisane właściwe wyjście, w trybie impulsowym lub dwustanowym odpowiednim dla strefy (punkt 5.3).

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 (Unique ID)** wpisz dokładnie, z pudełka lub z tylnej części urządzenia.
4. Urządzenie musi być online: dioda NETWORK świeci na zielono, TROUBLE nie miga, a dioda DATA gaśnie po zdarzeniu. W sieci z zaporą trzeba zezwolić na połączenie wychodzące do chmury Protegus.

Nie mogę połączyć się zdalnie przez TrikdisConfig

1. Urządzenie musi być online (dioda NETWORK zielona), 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 trzeba otwierać lub przekierowywać porty na routerze?

Nie. E16 nawiązuje tylko **wychodzące** połączenia do odbiornika i chmury Protegus, dlatego nie jest potrzebne ani przekierowanie portów, ani publiczny adres IP; zdalne programowanie również odbywa się przez to połączenie wychodzące. Zwróć tylko uwagę, aby zapora nie blokowała ruchu wychodzącego do portu odbiornika i do chmury Protegus.

Czy działa przez WiFi lub sieć komórkową?

Nie: E16 ma tylko przewodowe złącze Ethernet. Jeśli router nie ma niezawodnego zasilania, zasilaj urządzenia sieciowe z zasilacza awaryjnego (UPS).

Co się dzieje przy zaniku zasilania?

E16 jest zasilany z centrali alarmowej, więc działa dalej z akumulatora centrali, ale router i modem zwykle się wyłączają, a wraz z nimi znika internet. Dopóki nie ma połączenia, dioda TROUBLE sygnalizuje to 1 lub 6 mignięciami, urządzenie zapisuje zdarzenia (najwyżej 60 komunikatów) i po powrocie internetu wysyła je po

kolei. Jeśli utrata internetu jest w danym systemie niedopuszczalna, zasilaj także urządzenia sieciowe z zasilacza awaryjnego (UPS).

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 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

- Wyszukiwarka zgodności – który komunikator pasuje do której centrali alarmowej.
- G16 – sterowanie bezpośrednie centralami alarmowymi DSC PowerSeries – uzbrajanie kodem manipulatora, stan stref, blokowanie stref; tak samo dotyczy E16.
- DSC Power Series NEO i komunikatory Trikdis: zgodność i rozwiązania – dlaczego E16 nie można podłączyć do NEO i jakie jest rozwiązanie.
- Odblokowanie zablokowanego portu szeregowego w centralach alarmowych Paradox – odblokowanie portu szeregowego nowszych central Paradox.
- 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 E16 Ethernet Communicator - Moduł IP

Kabel łączący port szeregowy Trikdis CRP2 do paneli alarmowych Paradox

Kabel łączący port szeregowy CRP2B do paneli alarmowych Paradox

Trikdis CRP4 Kabel szeregowy dla paneli sterowania Texecom

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-e16