Komunikator G16 – instrukcja dla instalatora i użytkownika

Instrukcja dla instalatora i użytkownika komunikatora Trikdis G16: podłączenie do magistrali danych lub portu szeregowego centrali alarmowej, programowanie centrali, karta SIM i konfiguracja w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-g16

Spis treści

1. Przegląd

1.1 Do czego służy, jak działa
1.2 Zgodne centrale alarmowe
1.3 Wersje
1.4 Główne cechy
1.5 Elementy komunikatora
1.6 Zaciski
1.7 Sygnalizacja diod
1.8 Dane techniczne

2. Szybkie uruchomienie w 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 antena
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 modułu W485 i E485
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 Dodawanie urządzenia
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Sterowanie bezpośrednie kodem klawiatury
5.3 Uzbrajanie strefą przełącznika kluczowego
5.4 Uzbrajanie i rozbrajanie z aplikacji
5.5 Sterowanie wiadomościami SMS

6. TrikdisConfig – ustawienia szczegółowo

6.1 Pasek stanu
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 SIM card
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Przywracanie ustawień fabrycznych

7. Zdalne programowanie

8. Sprawdzenie działania komunikatora

9. Aktualizacja firmware

10. Rozwiązywanie problemów i najczęstsze pytania

11. Zasady bezpieczeństwa

Zobacz też

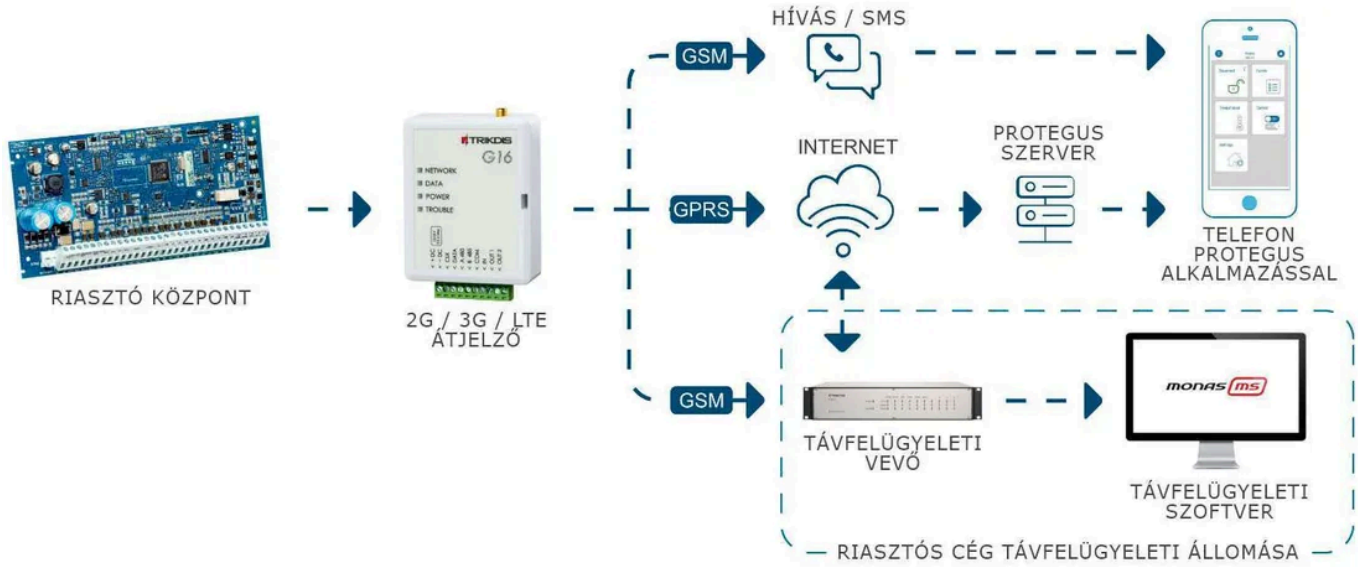
1. Przegląd

G16 to **komunikator komórkowy z bezpośrednim podłączeniem** firmy Trikdis: nie łączy się z wyjściem linii telefonicznej centrali alarmowej, lecz z **magistralą klawiatur lub portem szeregowym** centrali. Zdarzenia odczytuje bezpośrednio z centrali – razem z numerem strefy, partycji i użytkownika – i przesyła je transmisją danych w sieci komórkowej do odbiornika stacji monitorowania oraz do chmury Protegus, do aplikacji użytkownika. Współpracuje z obsługiwanymi centralami DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell i Crow; w typach **sterowanych bezpośrednio** użytkownik uzbraja i rozbraja system z aplikacji Protegus 2 własnym kodem klawiatury, bez osobnej strefy typu przełącznik kluczowy (keyswitch). Aplikacji Protegus 2 można używać ze wszystkimi centralami alarmowymi obsługiwanymi przez G16, niezależnie od producenta. Do central innych marek, które mają tylko wyjście linii telefonicznej, przeznaczony jest komunikator G16T (TIP/RING).

1.1 Do czego służy, jak działa

- **Odczytuje centralę bezpośrednio.** Przez magistralę centrali każde zdarzenie trafia do komunikatora natychmiast, z własną numeracją centrali; nie trzeba ustawiać dialera centrali i nie ma wybierania w formacie Contact ID.
- **Raportuje do stacji monitorowania.** Zdarzenia wysyła przez połączenie IP do programowego lub sprzętowego odbiornika Trikdis (protokół TRK) – współpracują one z dowolnym oprogramowaniem stacji monitorowania – albo do dowolnego odbiornika uniwersalnego (SIA DC-09 2007/2012, SUR-GARD TL150). Odbiornikowi SUR-GARD przekazuje kody Contact ID z centrali przekształcone na kody SIA. Połączenie sprawdza domyślnie co 30 sekund (lub w ustawionym przez ciebie odstępie), a w razie błędu przełącza się na kanał zapasowy.
- **Powiadamia użytkownika.** Aplikacja Protegus 2 pokazuje, co się wydarzyło, w powiadomieniach push – z osobnym dźwiękiem dopasowanym do zdarzenia – i na liście zdarzeń; użytkownik może z aplikacji uzbrajać i rozbrajać system oraz przełączać podłączone urządzenia (oświetlenie, bramę, wentylację, ogrzewanie, nawadnianie itp.). Może być powiadamiany także SMS-em i połączeniem telefonicznym.
- **Działa jednocześnie lub osobno** ze stacją monitorowania i z użytkownikiem: można go używać tylko z Protegus 2 (bez stacji monitorowania), tylko ze stacją monitorowania albo z obiema. Jeśli ustawione są obie, zdarzenie wysyła najpierw do stacji monitorowania, a potem do użytkownika.
- **Rezerwa SMS.** Stację monitorowania powiadamia także SMS-em, jeśli transmisja danych w sieci operatora nie działa; może wysyłać równolegle do dwóch odbiorników, do każdego z osobnym kanałem zapasowym.
- **Ma własne wejścia i wyjścia.** Trzy zaciski I/O o podwójnej funkcji można wykorzystać jako wejście (czujka, sabotaż) lub jako sterowane wyjście (strefa przełącznika kluczowego, przekaźnik); wyjścia możesz przełączać z aplikacji Protegus 2 i poleceniem SMS. Wersja 4G przez magistralę RS485 może z ekspanderem iO-8 uzyskać 8 dodatkowych I/O, a z modułem W485 lub E485 komunikować się także przez WiFi lub przewodowy internet – sieć komórkowa jest wtedy drogą zapasową.

Budowę systemu pokazuje poniższy rysunek: magistrala centrali alarmowej jest podłączona do G16, G16 przez sieć komórkową łączy się z internetem, a stamtąd z odbiornikiem stacji monitorowania i z chmurą Protegus; użytkownik widzi system w aplikacji Protegus 2.



Rysunek 1. Miejsce G16 w systemie: centrala alarmowa → G16 → sieć komórkowa → odbiornik stacji monitorowania i chmura Protegus → aplikacja Protegus 2. Użytkownik może otrzymywać także SMS-y i połączenia (GSM), a odbiornik stacji monitorowania – SMS jako rezerwę.

- 1 Centrala alarmowa (magistrala klawiatur lub port szeregowy)
- 2 Komunikator G16 (2G / 4G)
- 3 Połączenie i SMS do użytkownika
- 4 Transmisja danych komórkowych → internet → chmura Protegus
- 5 Telefon z aplikacją Protegus 2
- 6 Odbiornik stacji monitorowania
- 7 Oprogramowanie stacji monitorowania (stacja monitorowania firmy ochrony)

1.2 Zgodne centrale alarmowe

G16 można podłączyć do poniższych central. W typach **sterowanych bezpośrednio** uzbrajanie i rozbrajanie z aplikacji odbywa się kodem klawiatury; w 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

Lista od czasu do czasu się zmienia; aktualny stan znajdziesz w wyszukiwarce zgodności. Poza nimi G16 można używać także z centralami **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 i MATRIX 816**, **DSC PC5015** oraz **Paradox DIGIPLEX EVO96 i NE96**. Z centralami **DSC PowerSeries NEO** G16 nie działa: do magistrali NEO producent nie dopuszcza urządzeń zewnętrznych, zobacz DSC Power Series NEO i komunikatory Trikdis: zgodność i rozwiązania.

1.3 Wersje

Ta instrukcja została przygotowana dla **wersji sprzętowej 4** G16, ale **można jej używać także dla wersji sprzętowej 3**: podłączenie, konfiguracja i działanie obu wersji są w dużej mierze takie same. Instrukcja dotyczy w równym stopniu wersji z modemem 2G, 3G i 4G. Różnice zestawia poniższa tabela; tam, gdzie tekst podaje dane wersji 4, w wersji 3 weź pod uwagę te z tabeli.

	Sprzęt w wersji 3 (v3)	**Sprzęt w wersji 4 (v4)**
Typy (w TrikdisConfig)	np. G16_3210 (2G); powstały też wersje z modemem 3G i 4G	G16_G410 (2G), G16_54E0 (4G)
Wejścia/wyjścia	1 wejście o wybieranym typie (IN) + 2 wyjścia z otwartym kolektorem (OUT1, OUT2, maks. 0,15 A)	3 zaciski I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3), każdy może być wejściem lub wyjściem z otwartym kolektorem (maks. 0,15 A)
Ustawianie wejść/wyjść	Strona System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	Strona **IN/OUT** (punkt 6.6)
Pobór prądu	100 mA; podczas wysyłania maksymalnie 250 mA	60–100 mA; podczas wysyłania maksymalnie 500 mA
Magistrala RS485 (iO-8, W485, E485)	tylko w wersji 3G i 4G	tylko w wersji 4G (G16_54E0)

Wersja sprzętowa 4 jest produkowana z dwoma modemami:

Typ	Modem	Częstotliwości	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	brak
G16_54E0	4G (LTE)	pasma LTE zależne od regionu	jest

Wersję sprzętu znajdziesz na pasku stanu TrikdisConfig (**HW**) i na etykiecie z tyłu urządzenia. O wprowadzeniu wersji 4 jest osobny artykuł: Nadchodzi wersja sprzętowa v4 komunikatorów GSM G16 i G16T.

1.4 Główne cechy

Połączenie z centralą alarmową

- Maksymalnie 4 przewodami (+DC, −DC, CLK, DATA) podłącza się do magistrali klawiatur 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).
- Każde zdarzenie centrali przekazuje z pełną informacją o zdarzeniu (kod, partycja, strefa lub użytkownik); sygnalizuje przerwanie połączenia (dioda TROUBLE, zdarzenie COMMUNICATION).
- Centrale sterowane bezpośrednio można z aplikacji uzbrajać i rozbrajać kodem klawiatury; Protegus 2 pokazuje także stan stref.

Komunikacja ze stacją monitorowania

- Połączenie IP z odbiornikami Trikdis (odbiornik programowy IPcom, RL14, RM14) i z odbiornikami uniwersalnymi (SIA DC-09, TL150).
- Kanał główny, zapasowy i równoległy; zapasowe powiadomienie SMS do odbiornika SMS Trikdis (RL14, RM14, GM14).
- Szyfrowanie komunikatów AES-128; bufor zdarzeń na 60 komunikatów.

Funkcje dla użytkownika

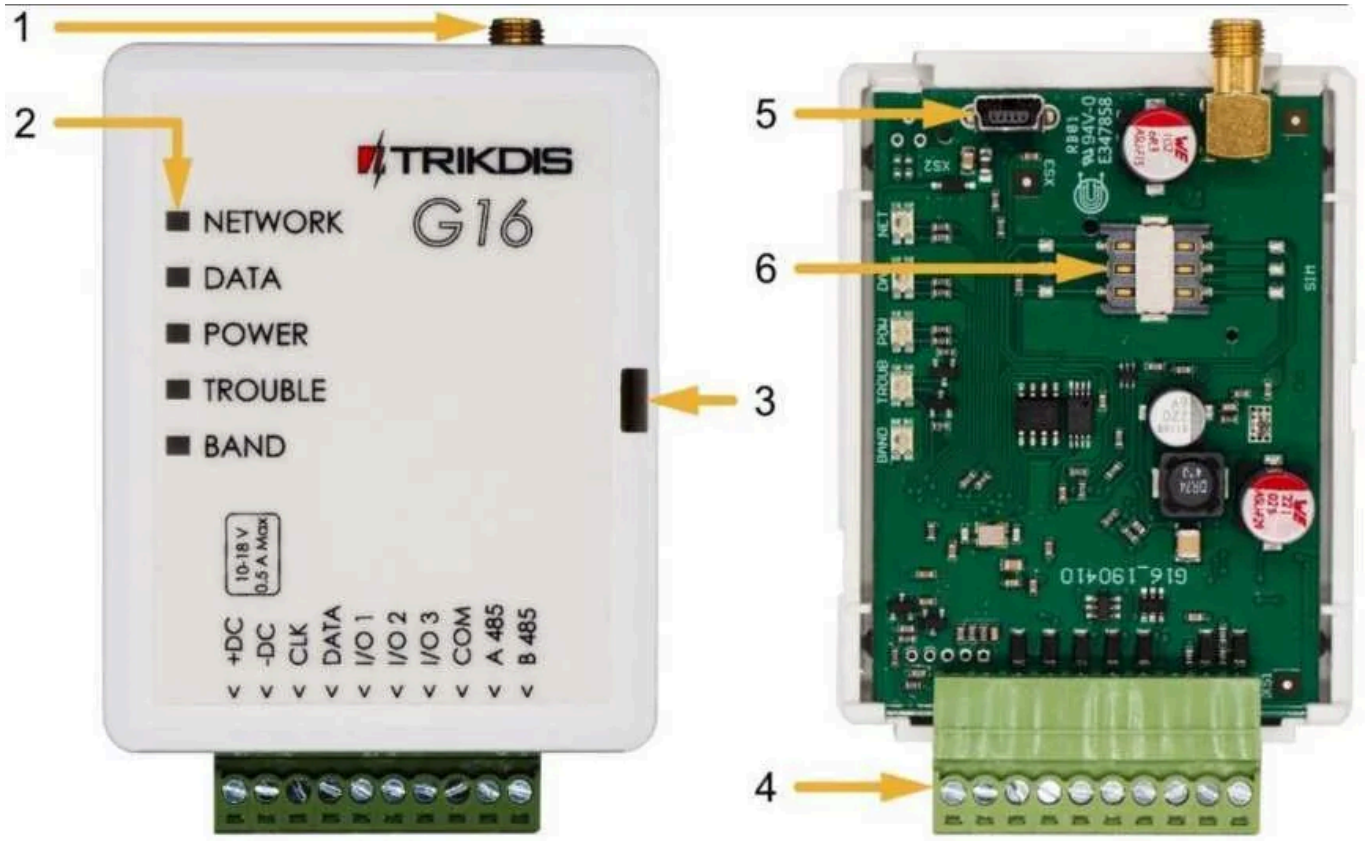
- Aplikacja mobilna i webowa Protegus 2: powiadomienia, lista zdarzeń, uzbrajanie i rozbrajanie, przełączanie wyjść.
- Sterowanie i podstawowa konfiguracja także poleceniami SMS.
- Powiadamianie także SMS-em i połączeniem telefonicznym, na maksymalnie 4 numery telefonów.
- Wielopoziomowe uprawnienia 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.

1.5 Elementy komunikatora

Płytka drukowana G16 znajduje się w białej obudowie z tworzywa; pokrywę przednią można zdjąć, a listwę zaciskową odłączyć. Na poniższym zdjęciu widać wersję 4G; w wersji 2G nie ma diody BAND ani zacisków A 485 / B 485.



Rysunek 2. Elementy G16 (wersja 4G) z przodu i z otwartą obudową.

- 1 Złącze SMA anteny GSM
- 2 Diody sygnalizacyjne (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Otwór ułatwiający zdjęcie pokrywy przedniej
- 4 Odłączana listwa zaciskowa
- 5 Gniazdo USB Mini-B do programowania
- 6 Gniazdo karty Nano-SIM

Listwę zaciskową można zdjąć: dzięki temu urządzenie można jednym ruchem odłączyć od zasilania lub zrestartować, łatwiej się nią posługiwać przy podłączaniu, a do programowania przez USB urządzenie można zanieść do komputera.

1.6 Zaciski

Zacisk	Funkcja
+DC	Zasilanie, +10–18 V DC
−DC	Zasilanie, minus
CLK	Linia zegara / linia szeregowa magistrali centrali
DATA	Linia danych magistrali centrali
I/O 1	1. wyjście/wejście (ustawienie fabryczne: nieużywane)
I/O 2	2. wyjście/wejście (ustawienie fabryczne: wejście, NO)
I/O 3	3. wyjście/wejście (ustawienie fabryczne: wyjście)
COM	Wspólny punkt (minus) wejść i wyjść
A 485	Przewód A magistrali RS485 (tylko wersja 4G)
B 485	Przewód B magistrali RS485 (tylko wersja 4G)

Opis listwy zaciskowej jest także na pokrywie przedniej, dlatego przy podłączaniu nie trzeba zdejmować pokrywy. To, do którego zacisku centrali idą CLK i DATA, zależy od producenta – schematy podłączeń zawiera punkt 3.3.

1.7 Sygnalizacja diod

Diody na pokrywie przedniej to najważniejsze narzędzia przy uruchamianiu i szukaniu usterek. Odczytuj je razem: POWER pokazuje zasilanie, NETWORK sieć, TROUBLE usterkę, a BAND (tylko 4G) typ sieci.

NETWORK – połączenie z siecią

Sygnalizacja	Znaczenie
nie świeci	Brak połączenia z siecią komórkową
miga na żółto	Trwa łączenie z siecią komórkową
świeci na zielono	Połączony z siecią komórkową
świeci na zielono, miga na żółto	Połączony; liczba żółtych mignięć to **poziom sygnału**: w 2G dobry sygnał to 5 mignięć, w 4G 3 mignięcia

DATA – transmisja danych

Sygnalizacja	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

Sygnalizacja	Znaczenie
nie świeci	Brak zasilania lub zasilanie jest odłączone
świeci na zielono	Włączony, napięcie zasilania jest prawidłowe
świeci na żółto	Nieprawidłowe napięcie zasilania (maksymalnie 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

Sygnalizacja	Znaczenie
nie świeci	Brak usterki
1 czerwone mignięcie	Brak karty SIM
2 czerwone mignięcia	Błąd PIN karty SIM (zły kod PIN)
3 czerwone mignięcia	Błąd programowania (brak APN)
4 czerwone mignięcia	Nie może zalogować się do sieci komórkowej (błąd rejestracji)
5 czerwonych mignięć	Nie może połączyć się z siecią transmisji danych (GPRS/UMTS/LTE)
6 czerwonych mignięć	Brak połączenia z odbiornikiem stacji monitorowania i/lub z serwerem Protegus (przyczyną może być też awaria połączenia internetowego)
7 czerwonych mignięć	Przerwane połączenie z centralą alarmową (połączenie magistralą lub szeregowe)
miga na czerwono (podczas programowania)	Błąd pamięci
świeci na czerwono (podczas programowania)	Uszkodzony firmware

BAND – typ sieci (tylko wersja 4G)

Zielone mignięcia	Sieć
1	brak
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.8 Dane techniczne

Parametr	Wartość
Połączenie z centralą alarmową	magistrala klawiatur lub port szeregowy, zależnie od typu centrali (maksymalnie 4 przewody: +DC, −DC, CLK, DATA; na magistrali Caddx i Pyronix CLK nie jest używany)
Wejścia/wyjścia	3 I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3): jako wejście NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (rezystor końcowy 2,2 kΩ); jako wyjście z otwartym kolektorem (OC), maks. 0,15 A / 30 V DC
Rozbudowa	Przez magistralę RS485 (tylko wersja 4G): ekspander iO-8 (+8 I/O) i inne ekspandery serii iO; moduł WiFi W485, moduł Ethernet E485
Modem 2G	850 / 900 / 1800 / 1900 MHz
Modem 4G	pasma LTE zależne od regionu
Napięcie zasilania	10–18 V DC
Pobór prądu	60–100 mA nominalnie; maksymalnie 500 mA podczas wysyłania
Protokoły transmisji	TRK, DC-09_2007, DC-09_2012, TL150
Bufor zdarzeń	60 komunikatów

Parametr	Wartość
Szyfrowanie	AES-128
Programowanie	TrikdisConfig (Windows) kablem USB Mini-B lub zdalnie; polecenia SMS
Warunki pracy	−10 … +50 °C, maks. 80 % wilgotności względnej (przy +20 °C)
Wymiary	92 × 65 × 26 mm
Masa	80 g

2. Szybkie uruchomienie w TrikdisConfig

Wszystkie ustawienia G16 wykonuje się programem **TrikdisConfig** działającym w systemie Windows – kablem USB lub zdalnie. W tym rozdziale opisujemy najkrótszą drogę: urządzenie konfigurujesz na biurku przed podłączeniem, a na 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 kabel do magistrali centrali – do portu szeregowego Paradox kabel **CRP2** lub **CRP2B**, do portu szeregowego Texecom kabel **CRP4** · płaski śrubokręt 2,5 mm · antena komórkowa o odpowiednim zysku (w miejscu o słabym zasięgu antena o większym zysku) · aktywna karta nano-SIM z usługą transmisji danych (żądanie PIN można wyłączyć) · instrukcja instalatora centrali alarmowej. Potrzebne akcesoria trzeba zamówić osobno u dystrybutora.

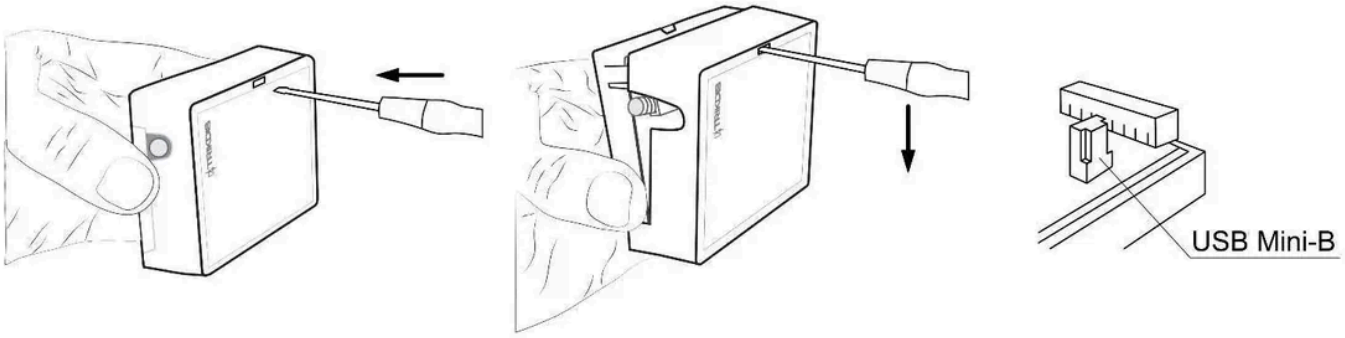
1. Pobierz i zainstaluj program TrikdisConfig. Na stronie producenta (www.trikdis.com) wpisz w pole wyszukiwania: „TrikdisConfig”.

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

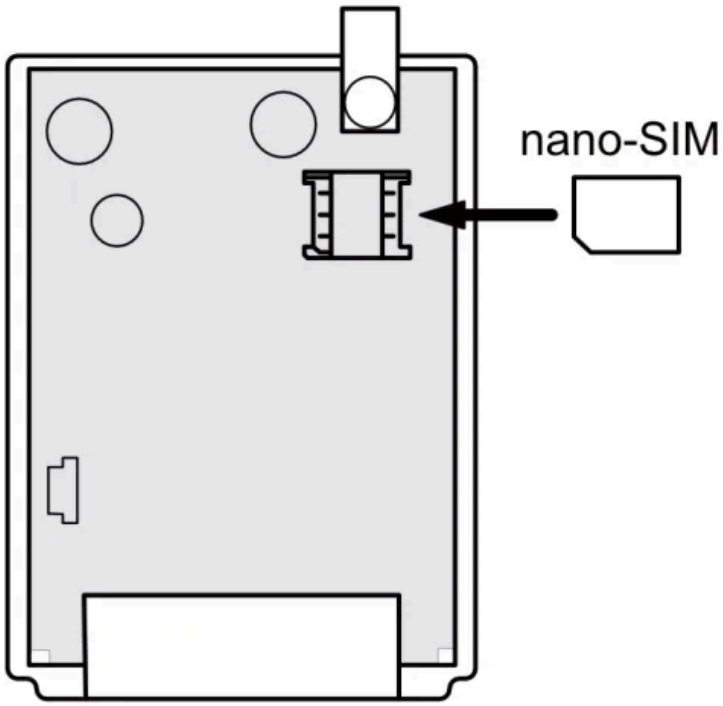
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Otwórz pokrywę przednią G16. Włóż płaski śrubokręt do otworu na górnej krawędzi pokrywy i, podważając w dół, delikatnie odepnij pokrywę przednią. Poniższy rysunek pokazuje otwieranie i położenie gniazda USB.



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

3. Włóż kartę nano-SIM do gniazda w kierunku pokazanym na rysunku. Karta musi być aktywna, mieć usługę transmisji danych, a jeśli to możliwe, wyłącz na niej żądanie PIN w telefonie (wtedy nie trzeba wpisywać PIN-u do urządzenia).



Rysunek 4. Położenie karty nano-SIM na płytce drukowanej.

4. Połącz G16 z komputerem kablem USB Mini-B. USB daje wystarczające zasilanie do programowania, osobny zasilacz nie jest potrzebny.

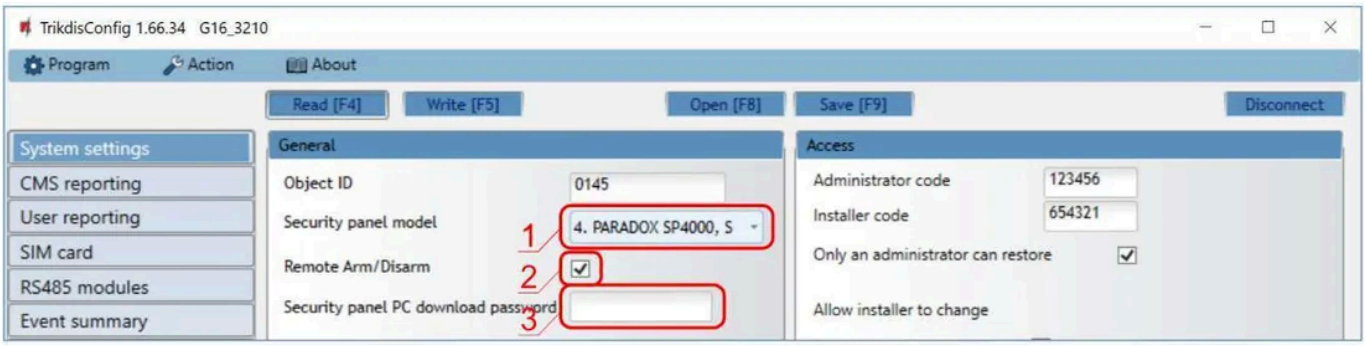
Ostrzeżenie

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

5. 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** podaj, do jakiej centrali trafi komunikator.



Rysunek 5. 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 klawiatury. Pojawia się tylko w typach sterowanych bezpośrednio; w pozostałych centralach uzbrajanie rozwiązuje się strefą przełącznika kluczowego (punkt 3.4) – wtedy zostaw puste.
- 3 **Security panel PC download password** – w 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 potrzebne jest także ustawienie w samej 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

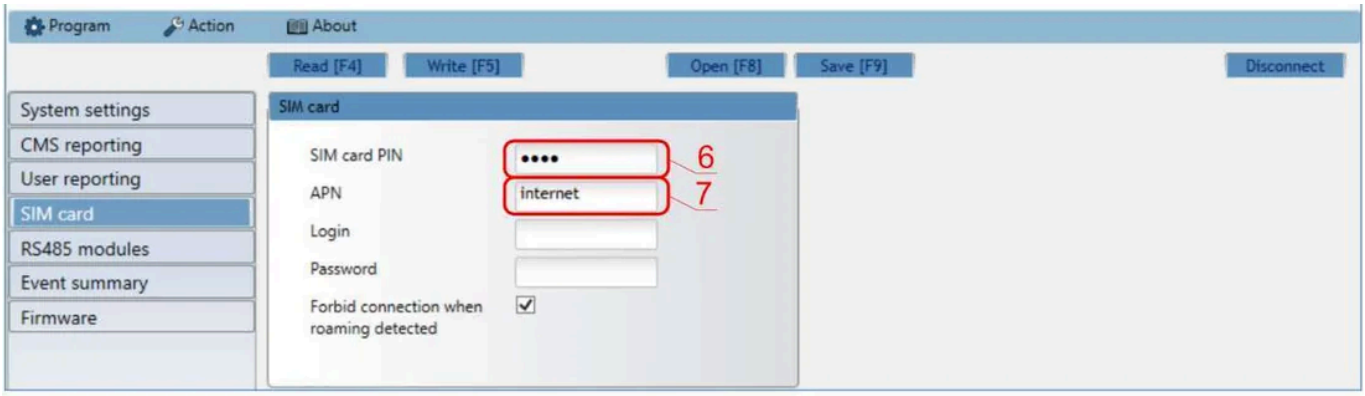
Jeśli użytkownik ma widzieć system i sterować nim z aplikacji Protegus 2, na stronie **User reporting**, w zakładce **PROTEGUS Cloud** ustaw następujące pozycje.



Rysunek 6. 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.**

Następnie na stronie **SIM card** podaj dane karty.



Rysunek 7. TrikdisConfig – strona SIM card.

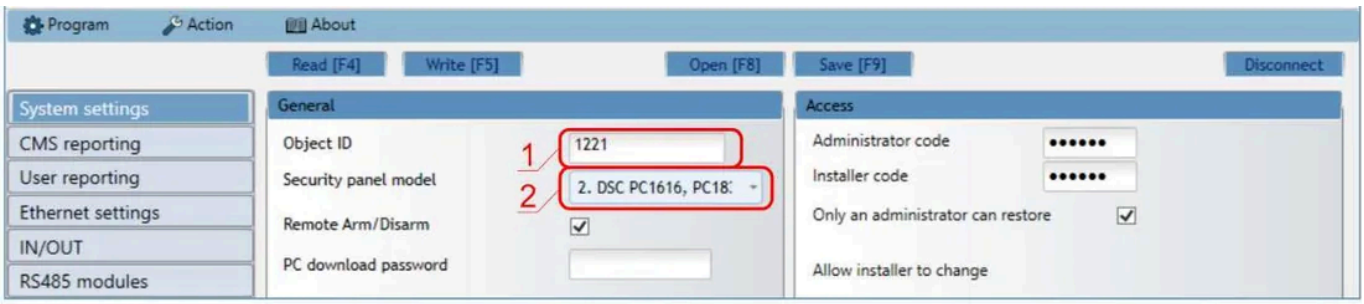
- 6 **SIM card PIN** – kod PIN karty (jeśli żądanie PIN jest wyłączone, może zostać wartość fabryczna).
- 7 **APN** – punkt dostępu do transmisji danych operatora (zobacz niżej).

APN (Access Point Name) to punkt dostępu do transmisji danych operatora komórkowego; bez niego urządzenie nie połączy się z internetem. Dokładną wartość otrzymasz od operatora karty SIM i znajdziesz ją także na stronie operatora; APN „internet" jest ogólny i działa w sieciach wielu operatorów. Znane APN-y europejskich operatorów prowadzimy w osobnym artykule: Ustawienie APN – lista europejskich operatorów komórkowych.

Do karty danych IoT / M2M (komunikacja między maszynami) operator zwykle podaje **inny APN niż do kart dla klientów indywidualnych** – z APN-em dla klientów indywidualnych urządzenie się nie połączy. Tę wartość także znajdziesz w artykule o APN albo poproś o nią operatora; jeśli operator podaje również nazwę użytkownika i hasło, wpisz także je.

2.4 Połączenie ze stacją monitorowania

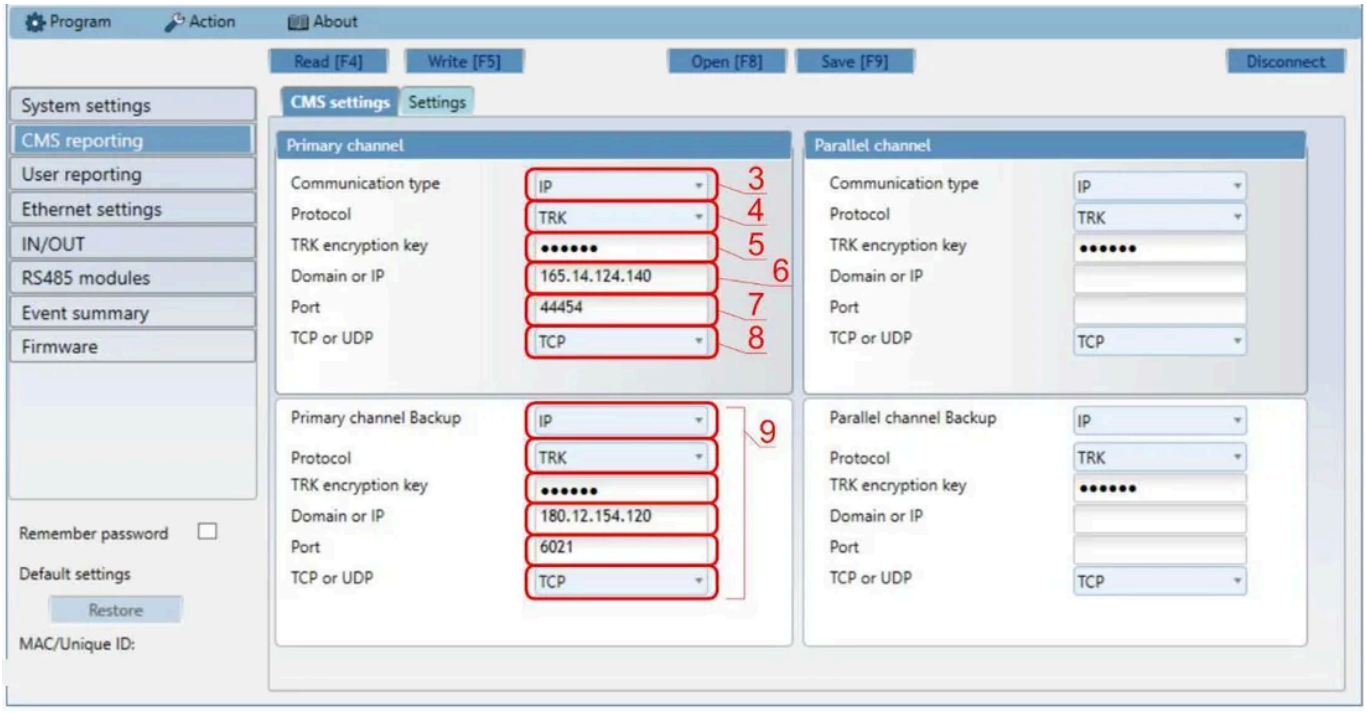
Jeśli urządzenie raportuje także do odbiornika stacji monitorowania, na stronie **System settings** podaj również identyfikator obiektu.



Rysunek 8. TrikdisConfig – strona System settings, grupa General.

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

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

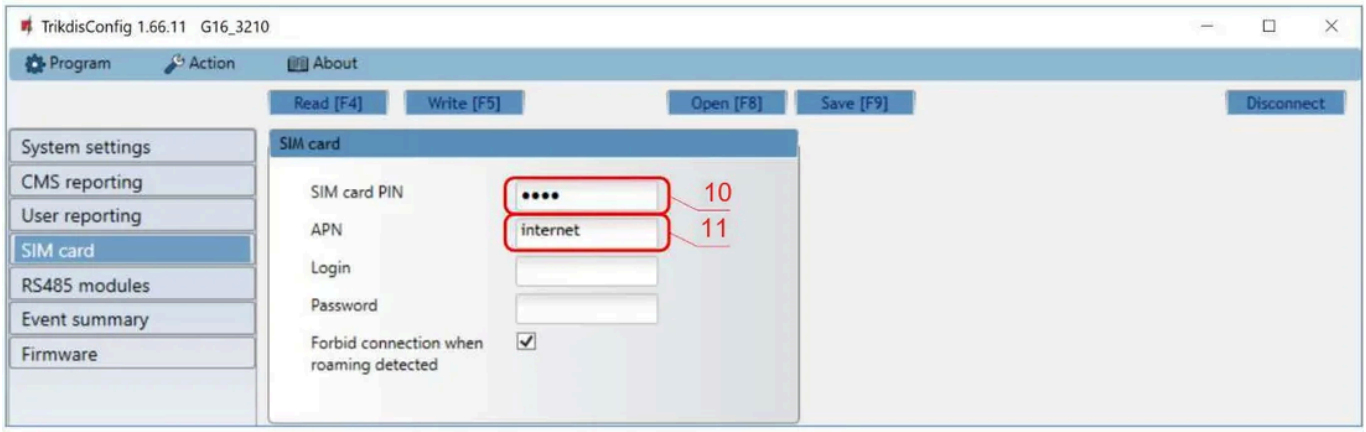


Rysunek 9. TrikdisConfig – CMS reporting, zakładka CMS settings.

- 3 **Communication type** – wybierz połączenie **IP** (SMS nie jest zalecany jako kanał główny).
- 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; dopasowany do ustawień odbiornika.
- 9 **Primary channel Backup** – kanał zapasowy na wypadek awarii kanału głównego; wypełnij go tak samo, zalecane jest jego podanie.

Zalecane jest także ustawienie **Parallel channel** (kanału równoległego) i należącego do niego kanału zapasowego, jeśli zdarzenia muszą otrzymywać dwa odbiorniki; w polu **Backup SMS reporting number** – to także jest zalecane – możesz wpisać numer telefonu odbiornika SMS Trikdis: urządzenie zaraz po pierwszym uruchomieniu wyśle na niego SMS, a później raportuje SMS-em wtedy, gdy nie działa żaden kanał IP.

Na koniec na stronie **SIM card** podaj dane karty, jeśli nie zrobiłeś tego jeszcze w punkcie 2.3.



Rysunek 10. TrikdisConfig – strona SIM card.

- 10 **SIM card PIN** – kod PIN karty.
- 11 **APN** – punkt dostępu operatora (zobacz punkt 2.3).

Raportowanie SMS-em do stacji monitorowania działa tylko z odbiornikiem Trikdis (odbiornik IP/SMS RL14, odbiornik wielokanałowy RM14 lub odbiornik SMS GM14); wtedy potrzebny jest tylko klucz szyfrowania i numer telefonu. Przy protokole **DC-09** w zakładce **Settings** podaj także numer obiektu, linii i odbiornika DC-09.

Po zakończeniu ustawień naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB. Urządzenie jest wtedy gotowe do podłączenia.

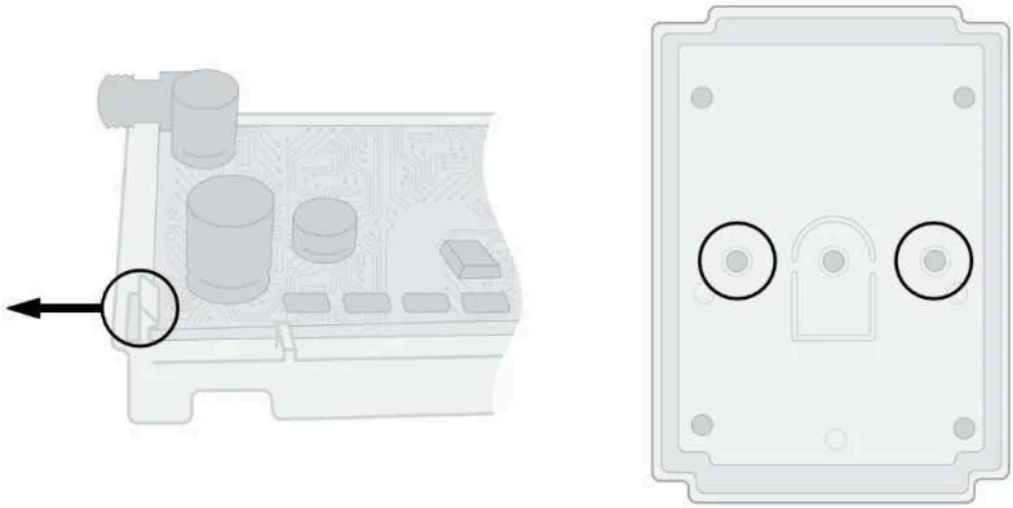
3. Instalacja i podłączenie

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 pokrywę przednią (zobacz punkt 2.1) i odłącz listwę zaciskową.
2. Włóż kartę nano-SIM, jeśli nie zrobiłeś tego przy uruchamianiu.
3. Wyjmij płytkę drukowaną z tylnej części obudowy: otwórz zatrzask w rogu (zobacz rysunek).
4. Przykręć tylną część obudowy wkrętami w wybranym miejscu.
5. Włóż płytkę drukowaną z powrotem do tylnej części obudowy i podłącz z powrotem listwę zaciskową.
6. Przykręć antenę GSM.
7. Załóż z powrotem pokrywę przednią.



Rysunek 11. Wyjmowanie płytki drukowanej: otwarcie zatrzasku w rogu (po lewej) i otwory montażowe tylnej części obudowy (po prawej, zakreślone).

Karta SIM musi być aktywna, a do pracy przez IP musi działać na niej transmisja danych. Jeśli nie chcesz, aby TrikdisConfig prosił o kod PIN, wyłącz żądanie PIN na karcie w telefonie.

3.2 Umiejscowienie i antena

- Komunikator umieść w **suchym miejscu wewnątrz budynku**, najlepiej w pobliżu obudowy centrali alarmowej, aby przewód magistrali był krótki.
- **W metalowej obudowie** sygnał komórkowy jest silnie tłumiony. Jeśli komunikator trafi do metalowej obudowy centrali, wyprowadź antenę na zewnątrz obudowy lub użyj anteny z dłuższym kablem.

- Przed ostatecznym zamocowaniem **sprawdź poziom sygnału**: liczba żółtych mignięć diody NETWORK powinna wynosić w 2G co najmniej 5, a w 4G co najmniej 3 (zobacz punkt 1.7). Jeśli jest mniejsza, poszukaj lepszego miejsca albo zmień antenę na czulszą, którą można umieścić dalej.
- Antenę i komunikator trzymaj z dala od transformatora centrali i przewodów sieci elektrycznej.



A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna használata.

3.3 Podłączenie do centrali alarmowej

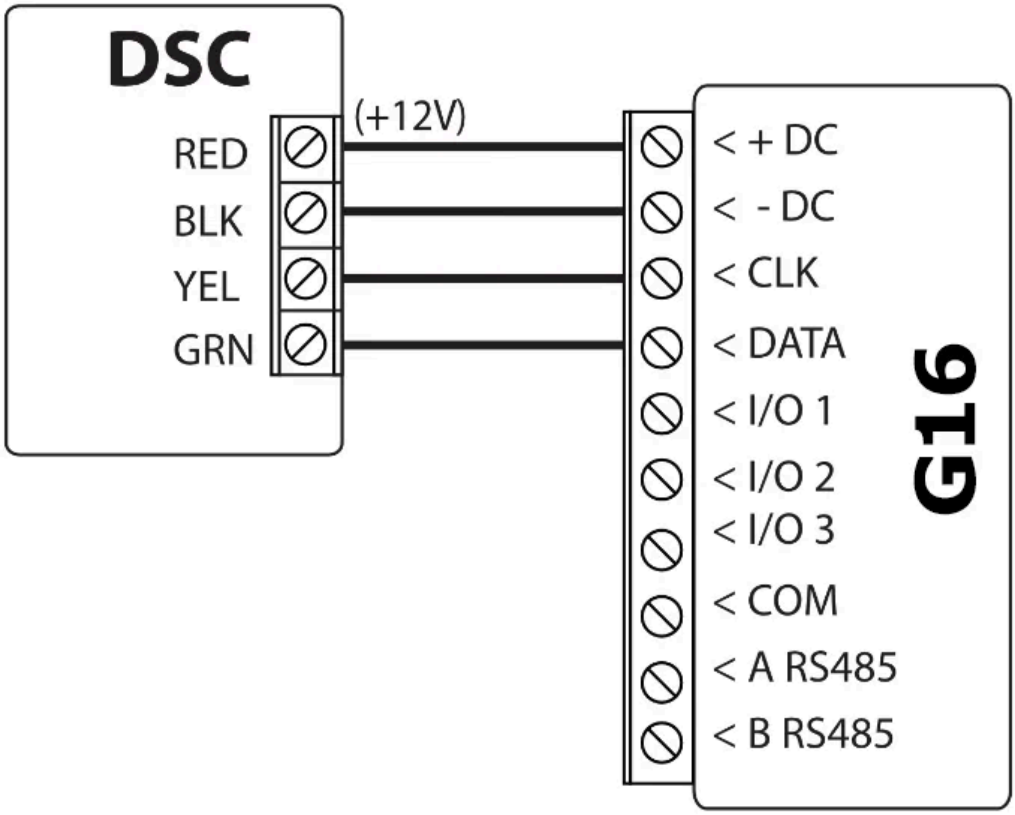
G16 łączy się z centralą **maksymalnie czterema przewodami** (na magistrali Caddx i Pyronix CLK nie jest używany): na zaciski **+DC** i **−DC** trafia zasilanie pomocnicze 12 V (AUX) centrali, a na zaciski **CLK** i **DATA** dwa przewody danych magistrali klawiatur lub portu szeregowego centrali. To, 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 można podłączyć do listwy zaciskowej G16.

G16 podczas wysyłania może pobierać nawet 500 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** programu TrikdisConfig trzeba wybrać typ podłączonej centrali (punkt 2.2); u niektórych producentów potrzebne jest także ustawienie w centrali (rozdział 4).

3.3.1 DSC PowerSeries

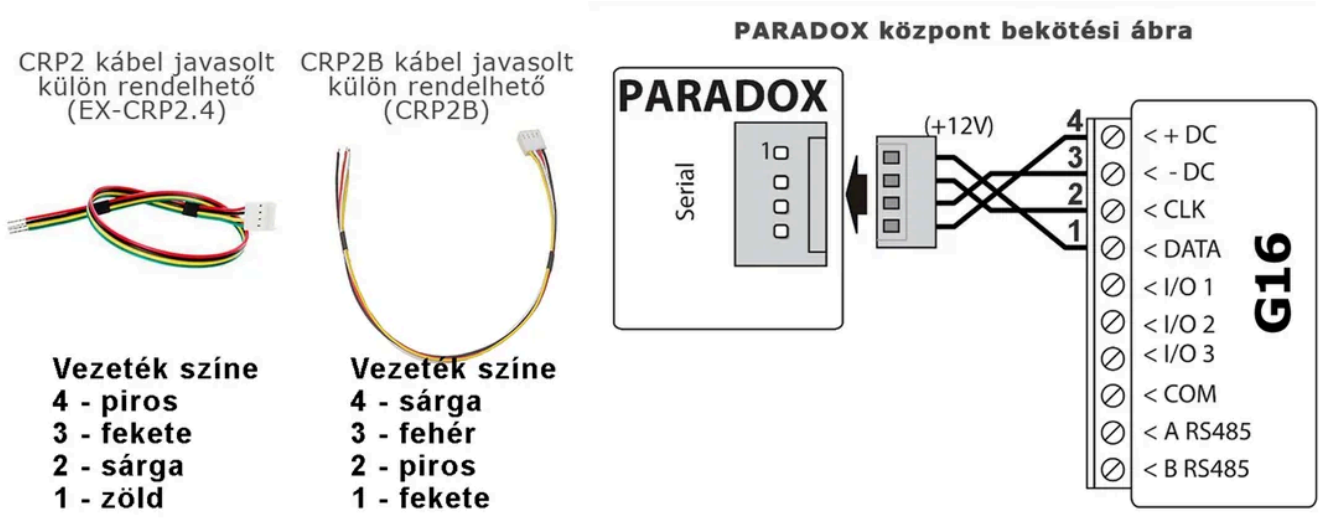
Cztery zaciski Keybus: **RED** → +DC, **BLK** → −DC, **YEL** → CLK, **GRN** → DATA.



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

3.3.2 Paradox

Do **portu szeregowego** (SERIAL) central Paradox komunikator podłącza się fabrycznym kablem **CRP2** lub **CRP2B**; koniec kabla od strony centrali pasuje do złącza szeregowego, a drugi koniec podłączasz do listwy zaciskowej G16. 4 piny złącza: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Kolory żył obu kabli się różnią – rysunek pokazuje przyporządkowanie kolorów dla obu kabli. Oznaczenia złącza szeregowego Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

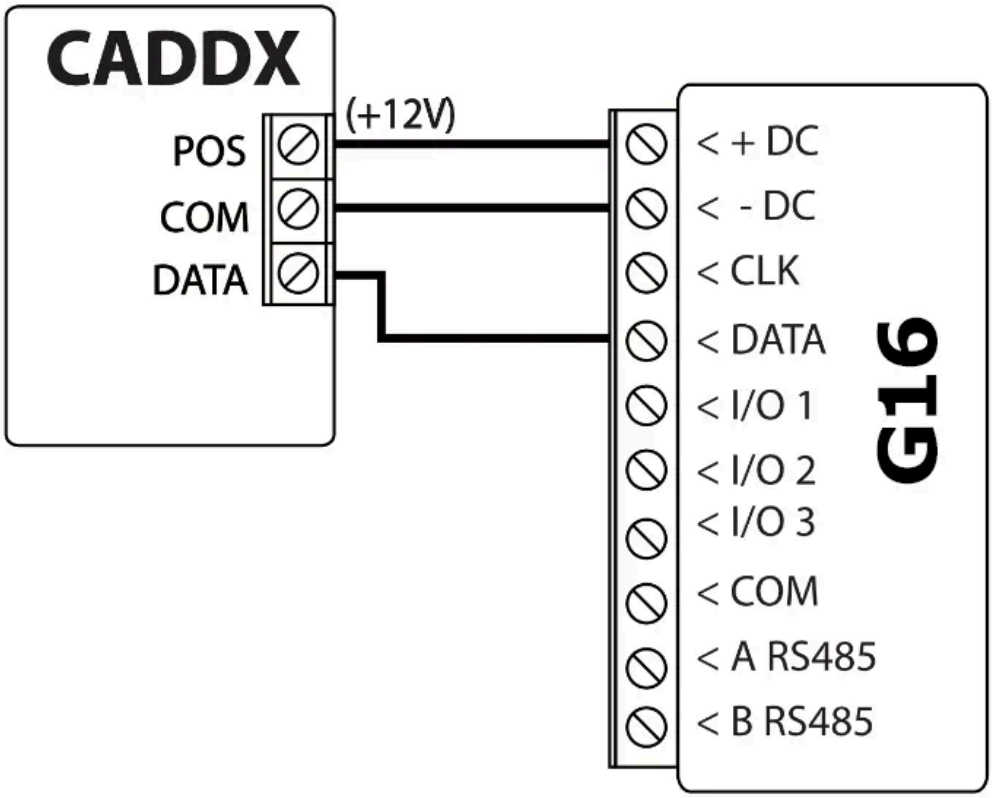


Rysunek 13. Podłączenie do portu szeregowego centrali Paradox kablem CRP2 (EX-CRP2.4) lub CRP2B. CRP2: 4 czerwony → +DC, 3 czarny → −DC, 2 żółty → CLK, 1 zielony → DATA. CRP2B: 4 żółty → +DC, 3 biały → −DC, 2 czerwony → CLK, 1 czarny → DATA.

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

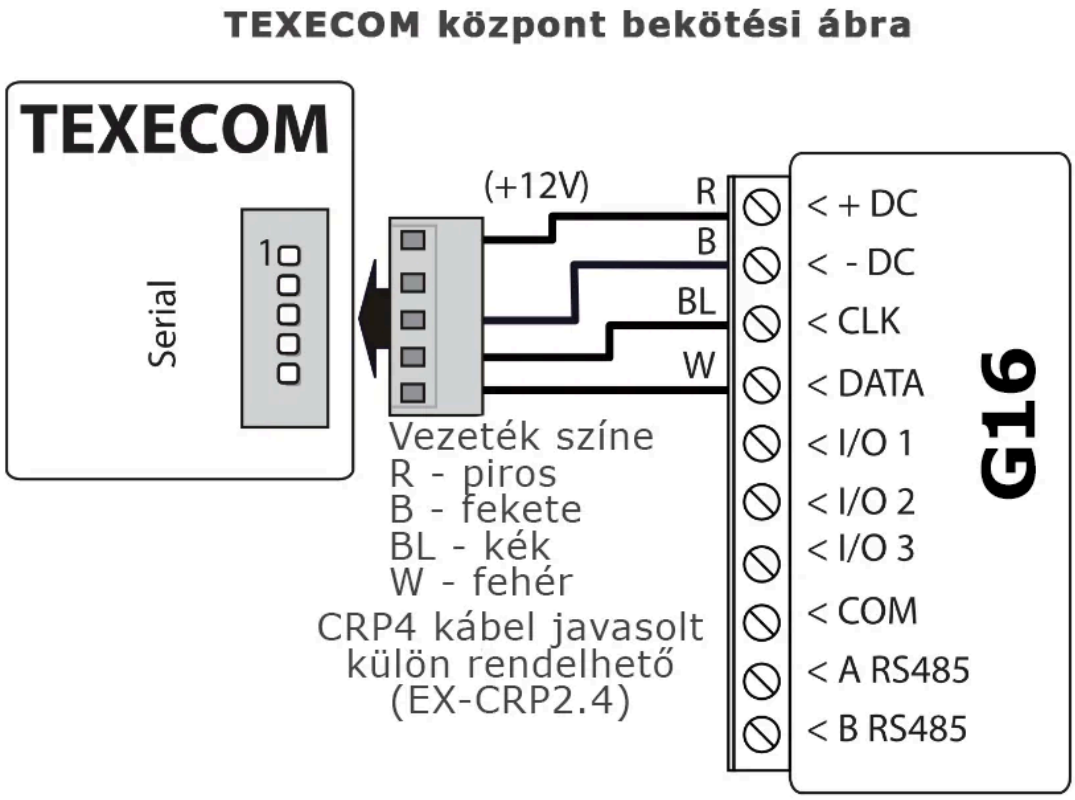
Trzy zaciski magistrali klawiatur: **POS** → +DC, **COM** → −DC, **DATA** → DATA. Zacisk **CLK** nie jest używany.



Rysunek 14. Podłączenie do magistrali klawiatur centrali Caddx NetworX („Keypad bus"): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK pozostaje wolny.

3.3.4 Texecom Premier / Premier Elite

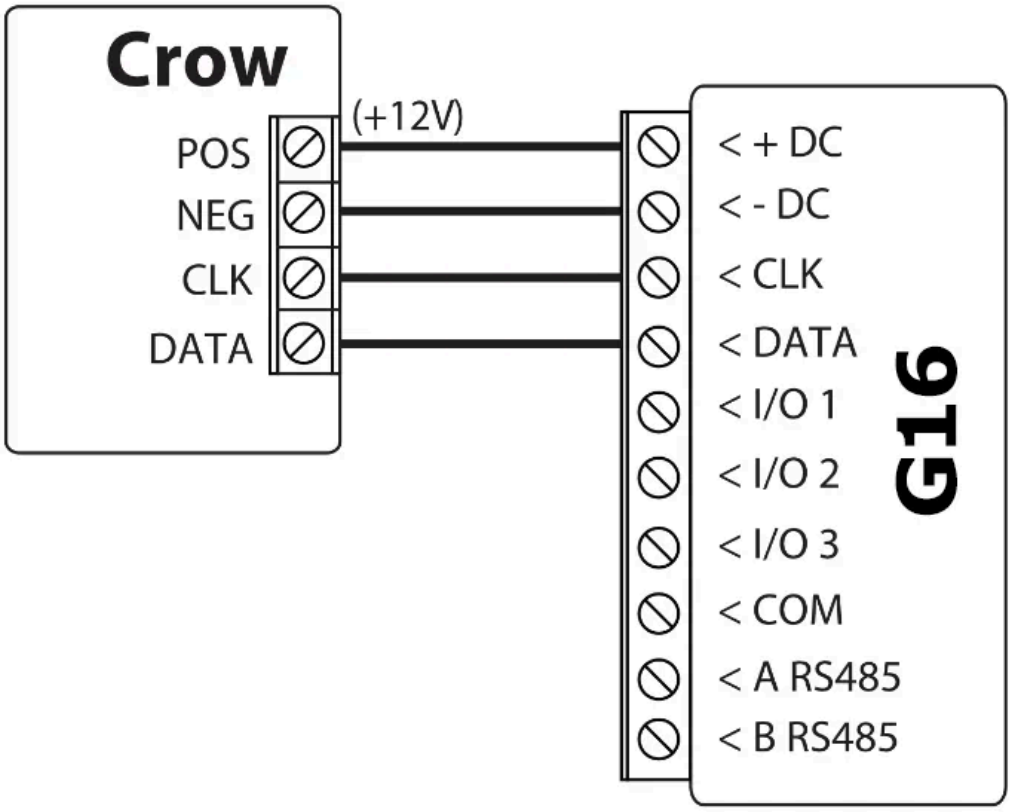
Do portu szeregowego centrali komunikator podłącza się fabrycznym kablem **CRP4**: **czerwony (R)** → +DC, **czarny (B)** → −DC, **niebieski (BL)** → CLK, **biały (W)** → DATA.



Rysunek 15. Podłączenie do portu szeregowego centrali Texecom kablem CRP4: czerwony → +DC, czarny → −DC, niebieski → CLK, biały → DATA.

3.3.5 Crow Runner

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



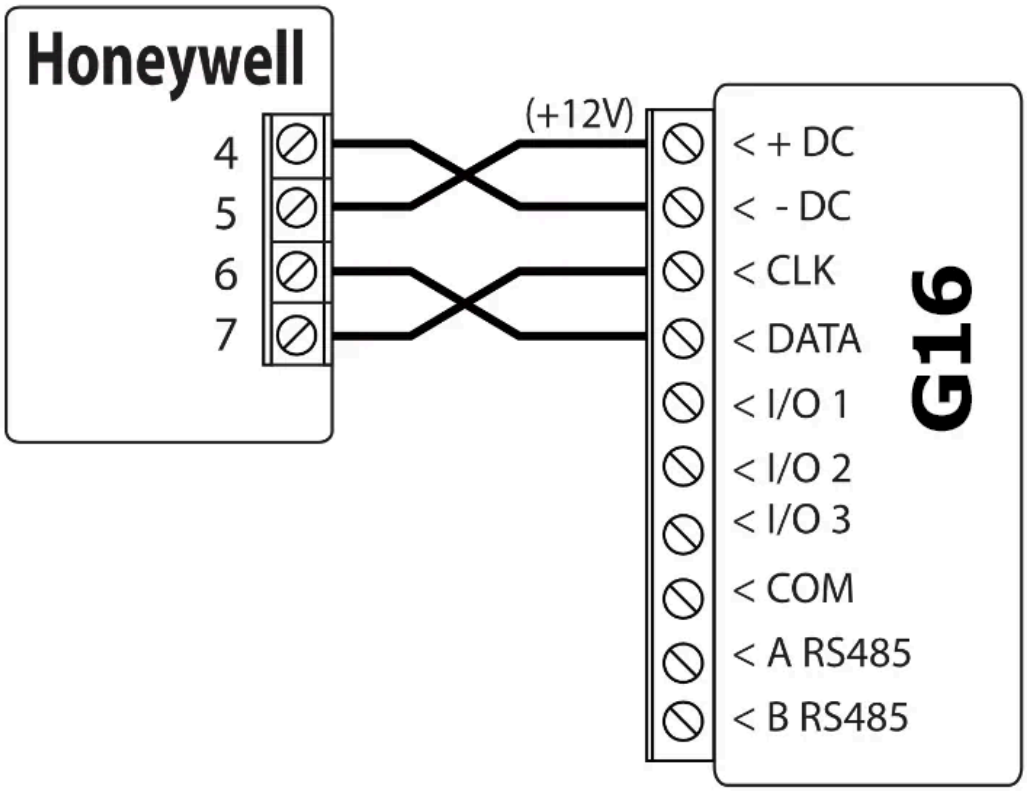
Rysunek 16. Podłączenie do magistrali klawiatur central Crow Runner 4/8 i Runner 8/16 („Keypad bus"): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Magistrala klawiatur 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

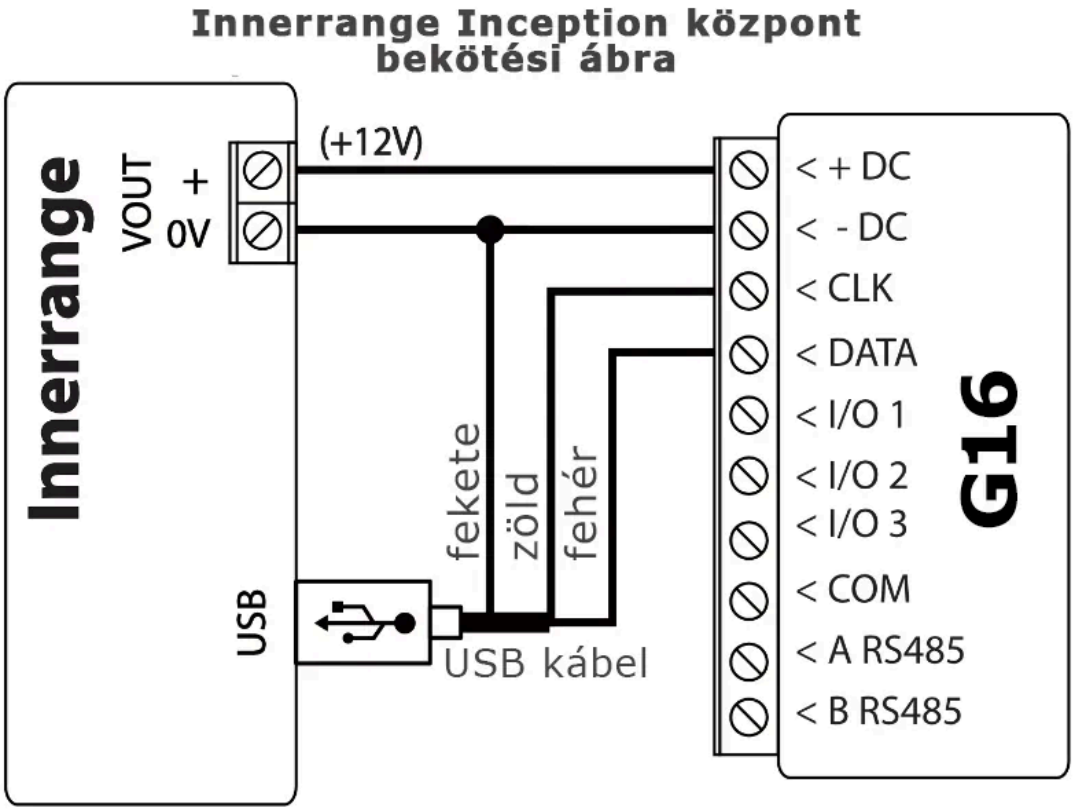
Numerowane zaciski magistrali klawiatur central Vista-15, Vista-20 i Vista-48: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (wyjście danych, żółty) → CLK, **6** (wejście danych, zielony) → DATA.



Rysunek 17. Podłączenie do magistrali klawiatur central Honeywell Vista-20 / Vista-48 („Keypad bus"): 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception i Integriti

Komunikator otrzymuje zasilanie z zacisków zasilania centrali **Inception** (**VOUT +** → +DC, **0V** → −DC), a połączenie danych realizuje 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).

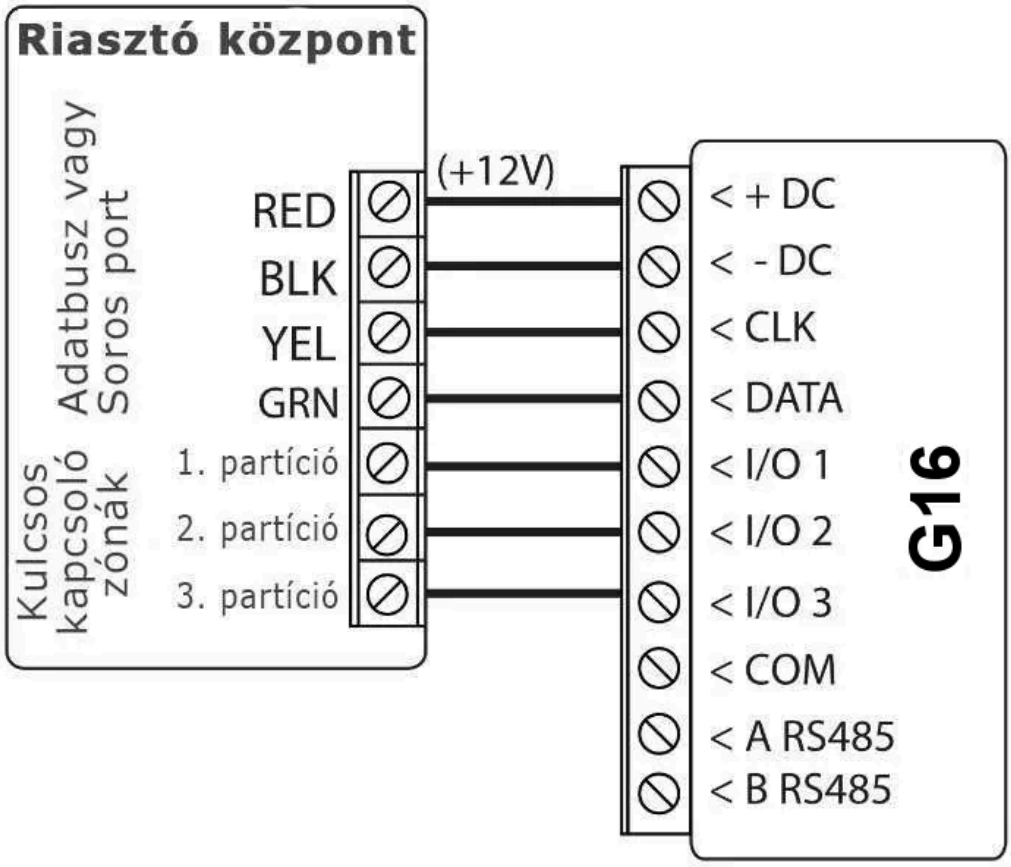


Rysunek 18. Podłączenie do centrali InnerRange Inception: zasilanie z zacisków VOUT + i 0V, dane z portu USB kablem 993030USB (czarny → 0V, zielony → CLK, biały → DATA).

Do portu 0 (Port 0) centrali **Integriti** można się podłączyć kablem INTG-996795: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Podłączenie strefy przełącznika kluczowego

Jeśli centrala nie należy do typów sterowanych bezpośrednio 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 go do strefy przełącznika kluczowego centrali. Wyjście po aktywacji zwiera strefę do COM (minusa); rezystor końcowy strefy podłącz zgodnie z typem strefy centrali. Ponieważ G16 ma trzy zaciski I/O, można obsługiwać nawet trzy partycje osobnymi wyjściami.



Rysunek 19. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego: komunikator odczytuje zdarzenia z magistrali centrali, a wyjścia I/O 1–3 przełączają strefę przełącznika kluczowego 1.–3. partycji centrali.

- Na stronie **System settings** programu TrikdisConfig pole **Remote Arm/Disarm** musi pozostać **puste** – obu rozwiązań nie można używać jednocześnie.
- Strefa przełącznika kluczowego może być impulsowa lub dwustanowa; w aplikacji Protegus 2 trzeba ustawić ten sam tryb (punkt 5.3).
- W **wersji sprzętowej 3** dwa wyjścia (OUT1, OUT2) mogą obsługiwać dwie partycje; pole **System settings** → **Output OUT1 & OUT2 mode** musi być w położeniu **Remote control** (fabrycznie).

O szczegółach i pułapkach uzbrajania przełącznikiem kluczowym jest osobny artykuł: Zdalne uzbrajanie przełącznikiem kluczowym z aplikacji Protegus 2.

3.5 Podłączenie wejść

Zaciski I/O komunikatora jako wejścia mogą też odbierać sygnały z dodatkowych czujników (np. styku sabotażowego, przycisku napadowego, termostatu), niezależnie od centrali alarmowej. Wejście podłącza się między wybrany zacisk I/O a zacisk COM.

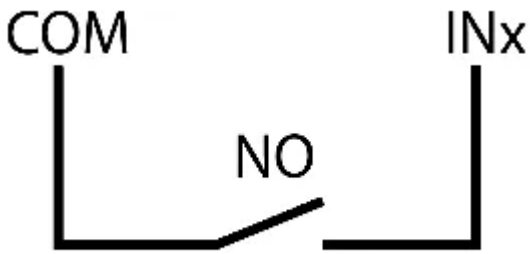
Wejścia obsługują następujące typy obwodów: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Rezystor końca linii ma wartość **2,2 kΩ**. Przy pojedynczej parametryzacji (EOL) zarówno zwarcie, jak i przerwa są traktowane jako alarm; podwójna parametryzacja (DEOL) z dwoma rezystorami rozróżnia 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	–

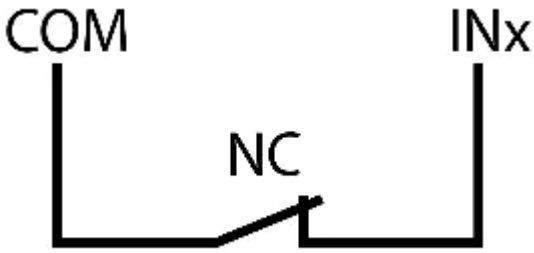
Typ	Stan spoczynkowy	Alarm	Sabotaż
NO	otwarty	zamknięty	–
NC/EOL	2,2 kΩ	przerwa lub zwarcie	–
NO/EOL	2,2 kΩ	zwarcie lub przerwa	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	przerwa lub zwarcie
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	przerwa lub zwarcie

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**.

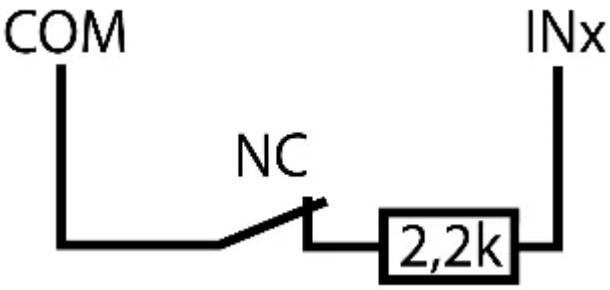
Podłączenie obwodów wejściowych: typy NO, NC, NC/EOL, NO/EOL, NO/DEOL i NC/DEOL z rezystorem końcowym 2,2 kΩ; w typach DEOL podłączony jest także obwód sabotażowy.



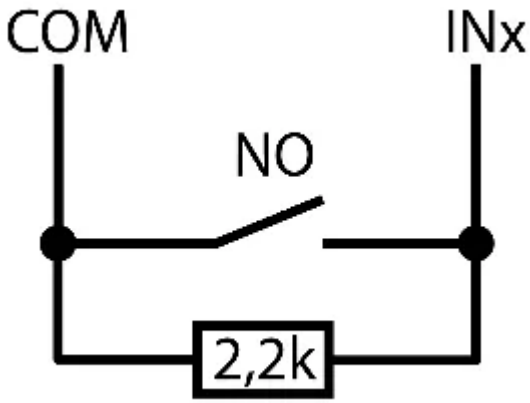
Rysunek 20. NO – obwód normalnie otwarty: zamknięty – alarm, otwarty – stan spoczynkowy.



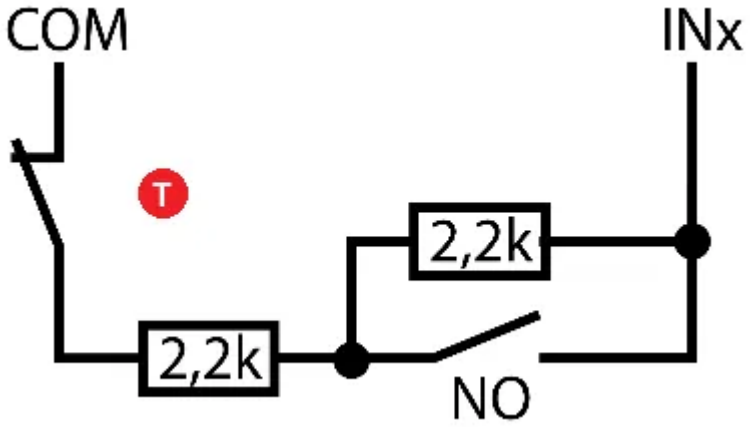
Rysunek 21. NC – obwód normalnie zamknięty: otwarty – alarm, zamknięty – stan spoczynkowy.



Rysunek 22. NC/EOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.

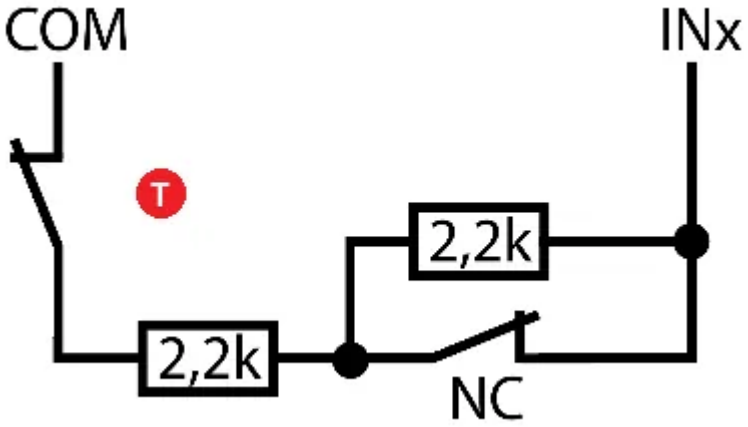


Rysunek 23. NO/EOL – obwód normalnie otwarty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynkowy.



Rysunek 24. 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



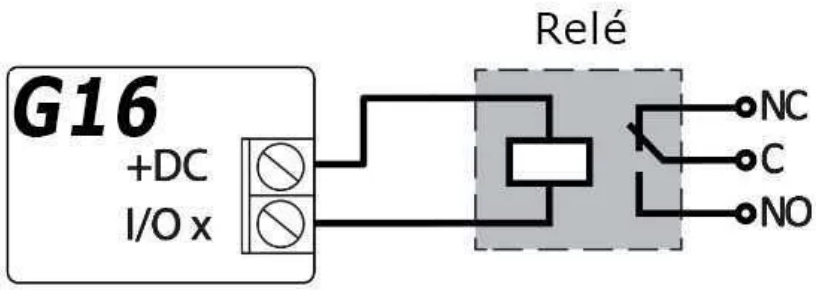
Rysunek 25. NC/DEOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – stan spoczynkowy, 3,3–5,5 kΩ – alarm.

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

W **wersji sprzętowej 3** jest jedno wejście (IN); jego typ ustawiasz w polu **System settings → Input IN type**.

3.6 Podłączenie wyjścia z przekaźnikiem

Zaciski I/O jako wyjścia są wyjściami z otwartym kolektorem (OC): w stanie aktywnym zwierają podłączone obciążenie do minusa, prądem maksymalnie 0,15 A, do 30 V DC. Większy odbiornik lub urządzenie zasilane napięciem sieciowym przełączaj **przez przekaźnik**: jeden koniec cewki przekaźnika trafia na +DC, a drugi na zacisk I/O. Stykami przekaźnika można włączać i wyłączać różne urządzenia elektryczne. W tym celu zacisk I/O trzeba ustawić na stronie **IN/OUT** programu TrikdisConfig jako wyjście (**OUT**) (punkt 6.6).

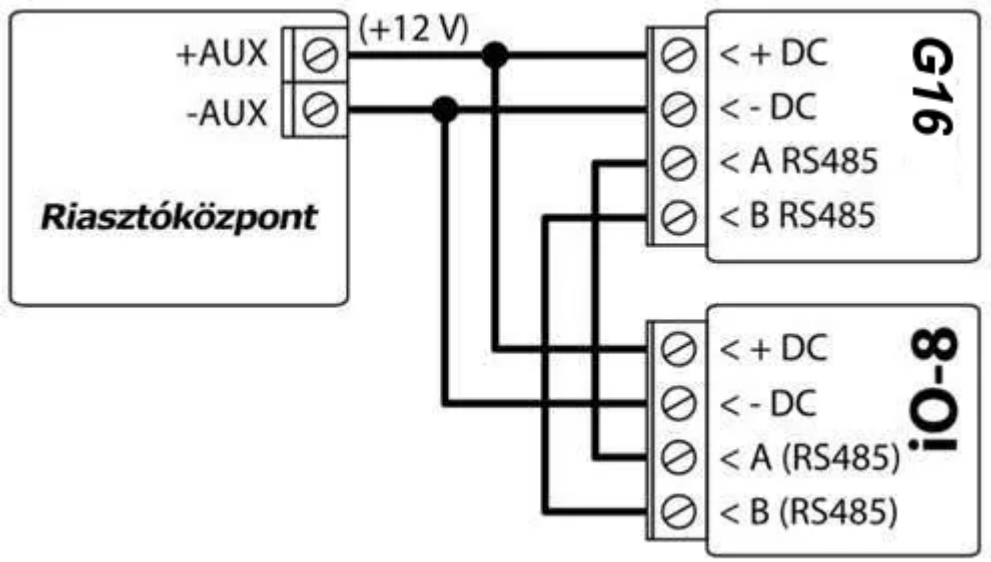


Rysunek 26. Podłączenie przekaźnika do wyjścia komunikatora: cewka trafia między zacisk +DC a zacisk I/O x, a styki (NC, C, NO) przełączają odbiornik.

Wyjścia możesz przełączać z aplikacji Protegus 2 lub poleceniem SMS (rozdział 5).

3.7 Podłączenie ekspandera iO-8

Jeśli potrzeba więcej wejść lub wyjść, do magistrali RS485 **wersji 4G** można podłączyć maksymalnie cztery ekspandery **iO-8**; każdy daje 8 dodatkowych I/O o podwójnej funkcji. Zaciski A 485 i B 485 połącz z zaciskami A i B modułu, a zasilanie modułu weź z wyjścia AUX 12 V centrali. Sposób podłączenia opisuje także własna instrukcja iO-8. Moduł trzeba dodać na stronie **RS485 modules** programu TrikdisConfig (punkt 6.7); zdarzenia wejść trafiają do stacji monitorowania i do Protegus 2, a wyjścia można przełączać z aplikacji.



Rysunek 27. Podłączenie ekspandera iO-8 do magistrali RS485 G16 (A 485 → A, B 485 → B); zasilanie obu urządzeń z wyjścia AUX centrali alarmowej (+12 V).

G16 z modemem 2G (G16_G410) nie ma magistrali RS485, dlatego nie można do niego podłączyć modułu iO-8, W485 ani E485.

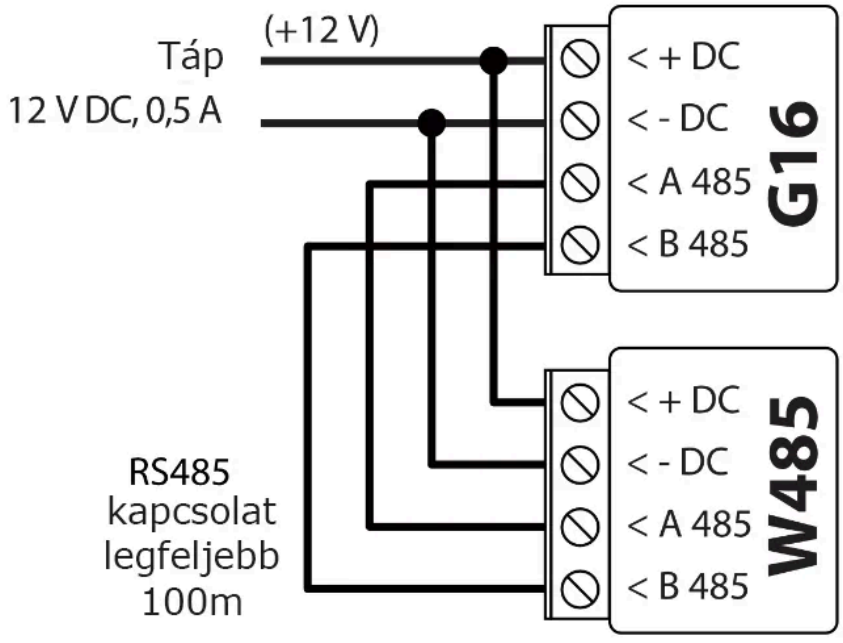
3.8 Podłączenie modułu W485 i E485

Rozszerzenie Ethernet lub Wi-Fi – W485 i E485. Komunikator można uzupełnić modułem Wi-Fi W485 lub modułem Ethernet E485: zdarzenia trafiają do stacji monitorowania i do aplikacji Protegus 2 przez przewodowy internet lub przez Wi-Fi.

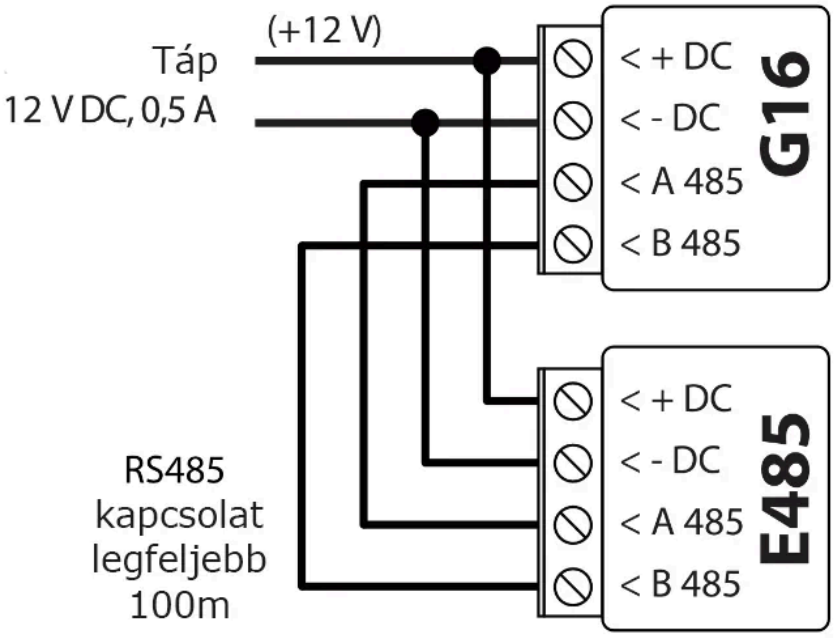
- **Podłączenie:** przez magistralę RS485, ze wspólnego zasilania z komunikatorem (wejście zasilania modułu 9–28 V DC); osobny zasilacz nie jest potrzebny.
- **Internet jest kanałem głównym:** dopóki działa, wszystko idzie przez niego. Jeśli połączenie zostanie przerwane, komunikator sam przełącza się na sieć komórkową, a gdy tylko internet wróci, wraca na IP.
- **Nie tylko transmisja zdarzeń:** przez ten kanał działa także aplikacja Protegus 2 (powiadomienia, zdalne sterowanie).
- **E485** – przewodowy Ethernet (RJ45). **W485** – Wi-Fi 2,4 GHz (WPA / WPA2), tam, gdzie nie poprowadzono kabla UTP.
- W razie potrzeby można go używać także bez karty SIM. Konfiguracja: programem TrikdisConfig, przez USB.

Moduł Ethernet Trikdis E485 (RS485) | **Trikdis W485 Moduł WiFi (RS485)**

Dopóki działa połączenie WiFi lub Ethernet, G16 komunikuje się przez nie i nie używa transmisji danych komórkowych; gdy połączenie zostanie przerwane, przełącza się na transmisję danych komórkowych, a po przywróceniu połączenia wraca do modułu. Do działania modułu **w G16 musi być karta SIM**.



Rysunek 28. Podłączenie modułu WiFi W485 do G16 przez magistralę RS485. Oba urządzenia pracują ze wspólnego zasilania 12 V DC (co najmniej 0,5 A) (wejście zasilania modułu 9–28 V DC); kabel RS485 może mieć maksymalnie 100 m długości.



Rysunek 29. Podłączenie modułu Ethernet E485 do G16 przez magistralę RS485. Oba urządzenia pracują ze wspólnego zasilania 12 V DC (co najmniej 0,5 A) (wejście zasilania modułu 9–28 V DC); kabel RS485 może mieć maksymalnie 100 m długości.

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.

Ustawienia sieciowe modułów wykonujesz na stronie **RS485 modules** programu TrikdisConfig (punkt 6.7).

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 pokrywie przedniej powinieneś zobaczyć:

- **POWER** świeci na zielono – zasilanie jest prawidłowe;
- **NETWORK** świeci na zielono i miga na żółto – połączony z siecią; liczba mignięć to poziom sygnału (dobry to 5 w 2G, 3 w 4G);
- **TROUBLE** nie świeci.

Jeśli dioda NETWORK daje mniej żółtych mignięć, poziom sygnału nie jest wystarczający: poszukaj innego miejsca dla komunikatora lub użyj czulszej anteny (punkt 3.2). Każda inna sygnalizacja diod oznacza jakąś usterkę – zidentyfikuj ją według tabel z punktu 1.7. Jeśli TROUBLE miga, liczba mignięć wskazuje przyczynę (punkt 1.7). **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 G16 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** programu TrikdisConfig opcję **Remote Arm/Disarm**, a w centralach Paradox i Texecom podaj także hasło PC lub UDL centrali w polu **Security panel PC download password** (punkty 2.2 i 6.2).

Jeśli centralą sterujesz nie bezpośrednio, lecz przez strefę przełącznika kluczowego (punkt 3.4), pole **Remote Arm/Disarm** musi pozostać 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

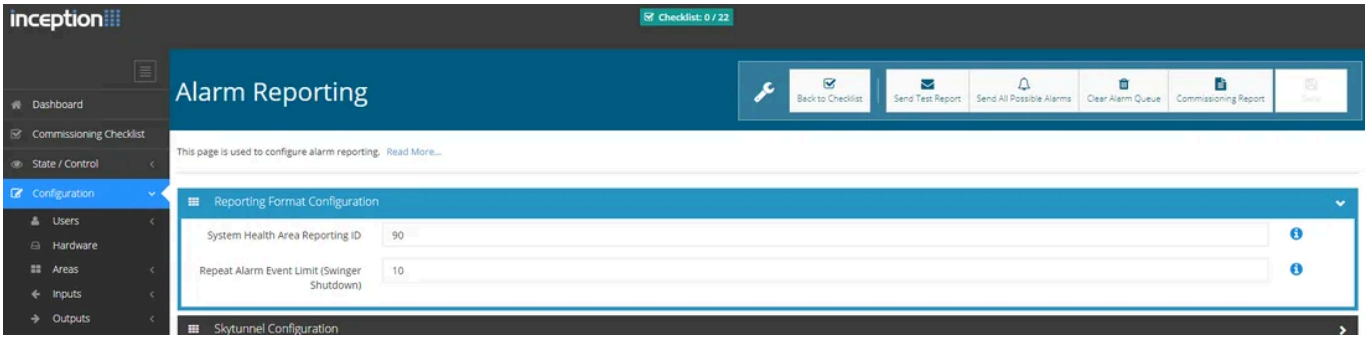
Firmware centrali **InnerRange Inception** musi mieć wersję co najmniej **2.3.0.3507-r0**, a centrala potrzebuje połączenia z internetem. Ustawienia wprowadzasz w interfejsie WWW centrali:

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 30. Interfejs webowy Inception – Configuration → General → Alarm Reporting.



Rysunek 31. 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 przełączać wyjścia komunikatora. W G16 uzbrajanie może odbywać się na dwa sposoby: w centralach **sterowanych bezpośrednio** użytkownik używa własnego **kodu klawiatury**, a w centralach podłączonych przez strefę przełącznika kluczowego – **wyjścia** komunikatora.

5.1 Dodawanie urządzenia

Przed dodaniem urządzenia sprawdź:

1. Karta SIM jest aktywna i działa na niej transmisja danych; jej kod PIN jest wpisany do urządzenia albo żądanie PIN jest wyłączone.
2. Na stronie **User reporting** → **PROTEGUS Cloud** programu 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, a dioda **NETWORK** świeci na zielono i miga na żółto.

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

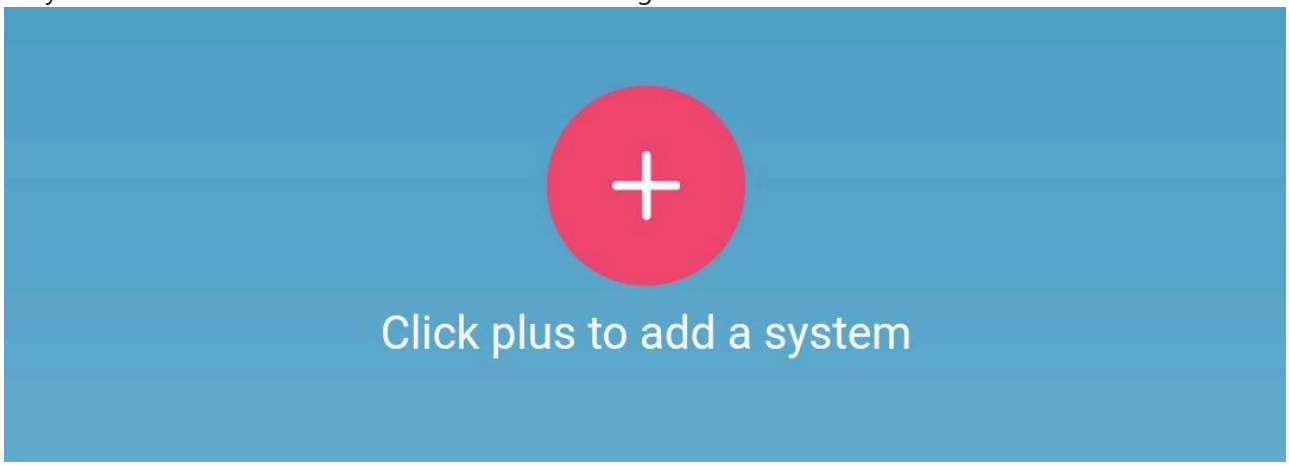
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

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

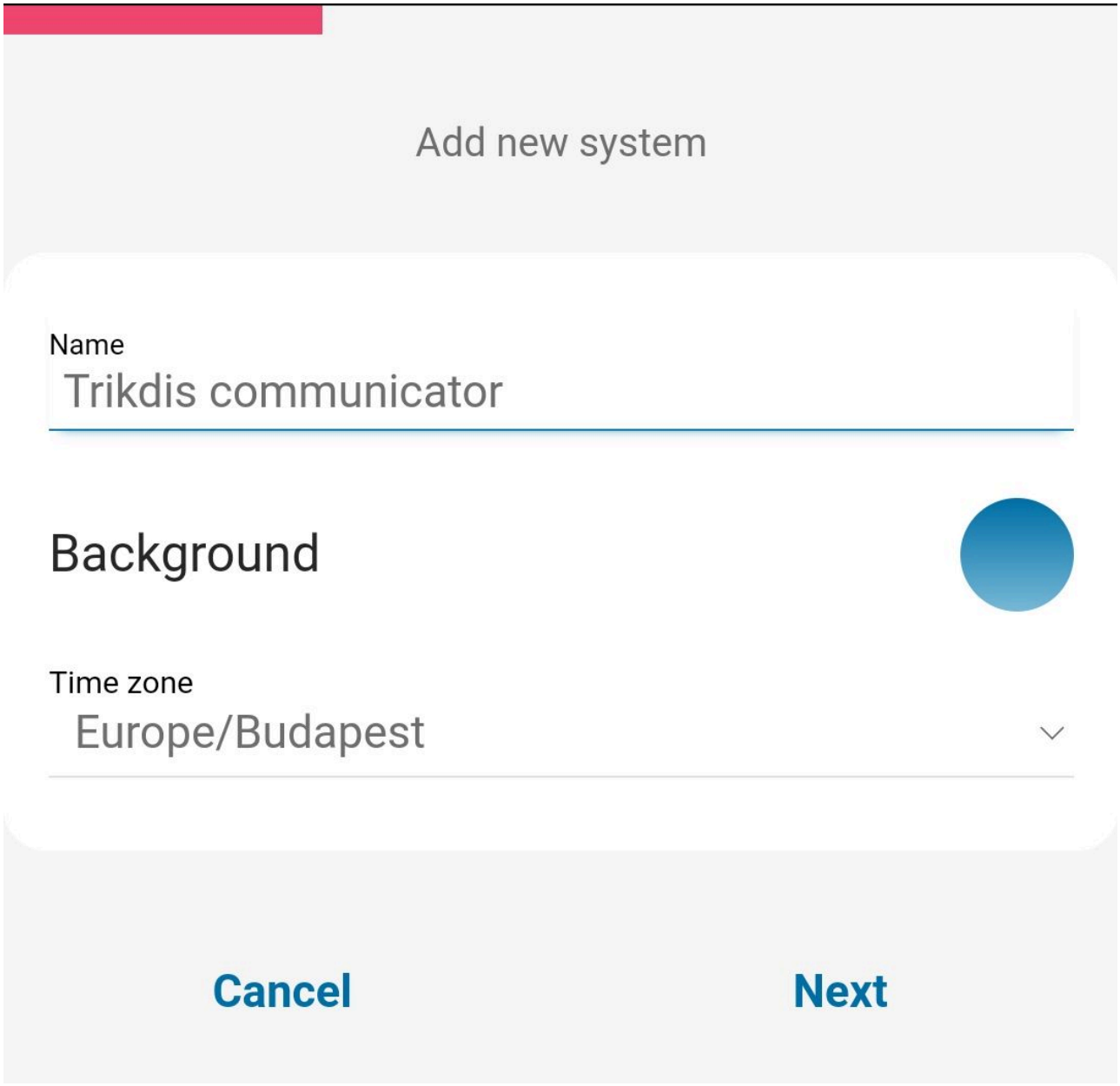


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán

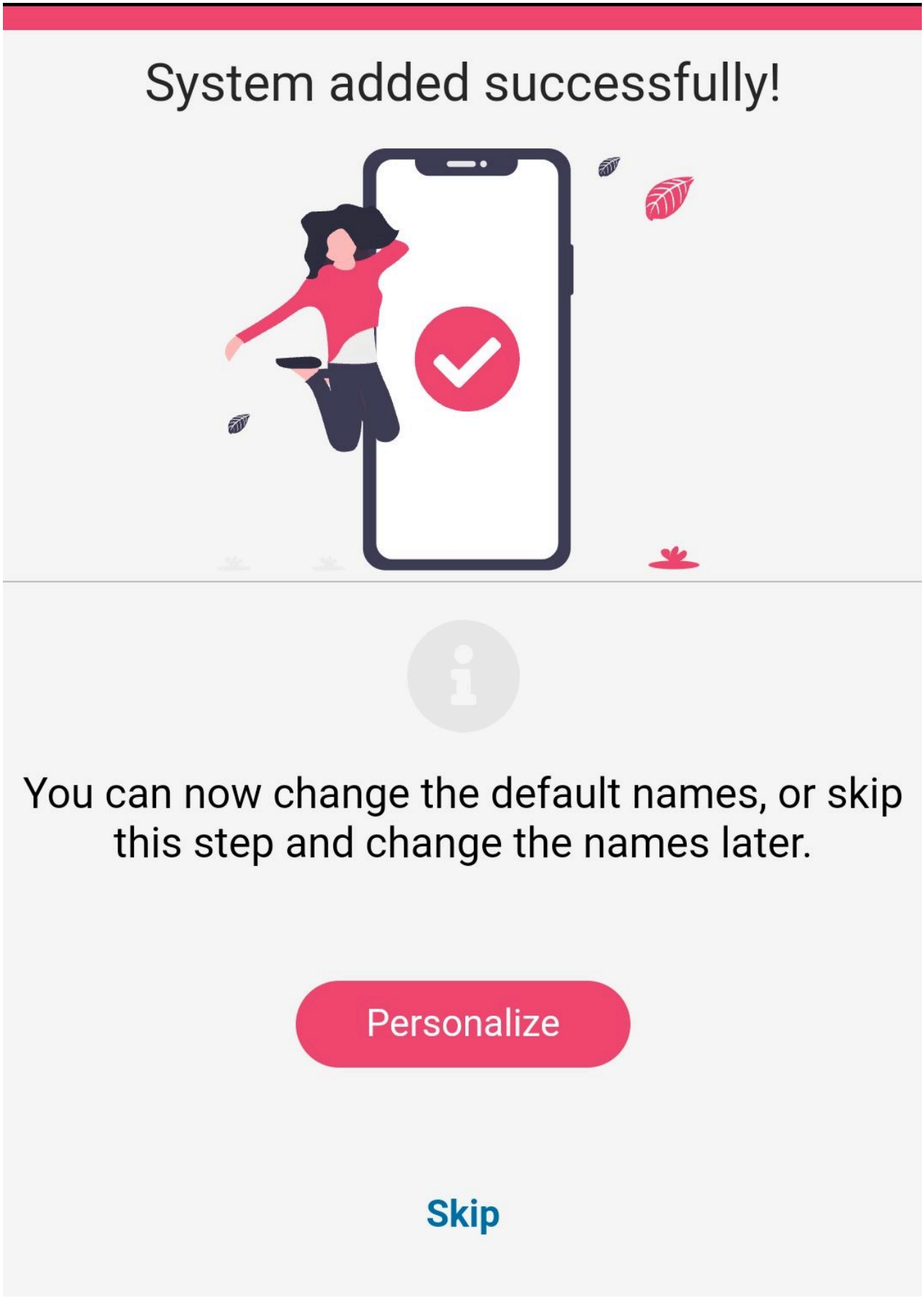
- Az eszköz papírdobozán
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



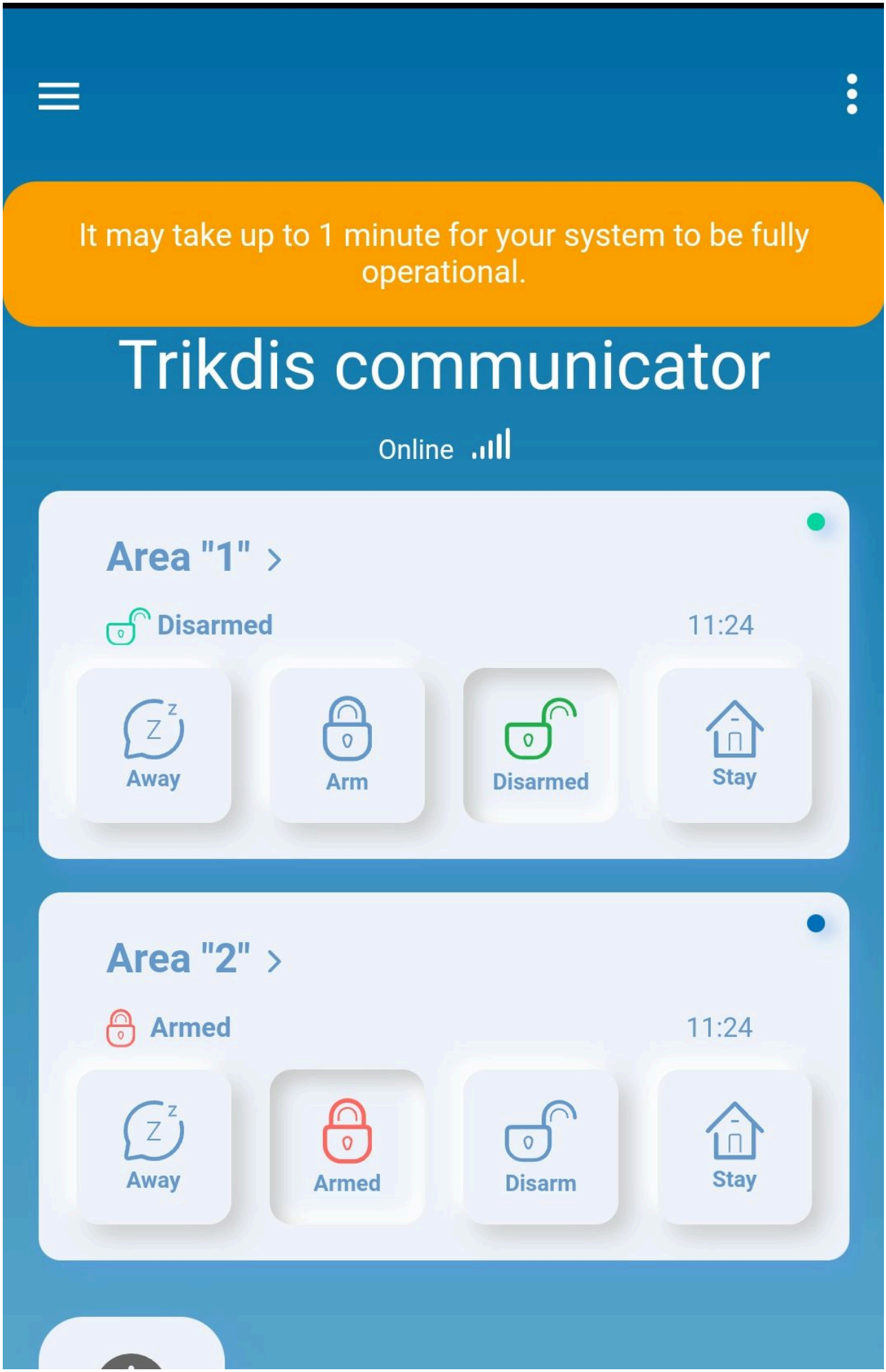
6. Add meg a rendszer nevét és válassz idozónát



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



Unikalny identyfikator urządzenia (**IMEI**) można odczytać na pudełku i z tyłu urządzenia, pokazuje go także pasek stanu TrikdisConfig.

5.2 Sterowanie bezpośrednie kodem klawiatury

Jeśli centrala należy do typów sterowanych bezpośrednio (punkt 1.2), a na stronie **System settings** programu 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 klawiatury centrali** – ten sam, którego używa na klawiaturze. Osobne wyjście ani 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 już do odczytu zdarzeń) – zobacz rozdział 4.
- Kod klawiatury sprawdza centrala, a w dzienniku zdarzeń centrali zapisywany jest użytkownik, a 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 także stan stref i możliwe jest blokowanie stref – szczegóły w artykule o sterowaniu bezpośrednim DSC.

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

5.3 Uzbrajanie strefą przełącznika kluczowego

Jeśli centrali 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 klawiatury centrali; przy uzbrajaniu przełącznikiem kluczowym – jeśli jest włączone – o hasło Protegus 2.

5.5 Sterowanie wiadomościami SMS

Komunikatorem można też sterować i programować go za pomocą wiadomości SMS. Budowa wiadomości:

`HASŁO spacja POLECENIE spacja DANE` – na przykład `123456 OUTPUT1 ON`

Z hasłem **administratora** można używać wszystkich poleceń, z hasłem **instalatora** poleceń INFO, RESET i OUTPUTx. `x` to numer wyjścia: zacisk I/O ustawiony jako wyjście (1, 2 lub 3), który chcesz przełączyć.

Polecenie	Dane	Co robi	Przykład
`INFO`	–	Pobiera informacje o urządzeniu: typ, IMEI, numer seryjny, wersja firmware	`123456 INFO`
`RESET`	–	Uruchamia urządzenie ponownie	`123456 RESET`
`OUTPUTx`	`ON`	Włącza wyjście x	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Wyłącza wyjście x	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Podaje impuls na wyjściu x; `tttt` = długość impulsu w sekundach, czterema cyframi	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Włącza lub wyłącza połączenie z Protegus	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adres:port`	Adres IP i port kanału głównego	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=klucz`	Klucz szyfrowania TRK	`123456 CONNECT ENC=123456`

Polecenie	Dane	Co robi	Przykład
`CONNECT`	`APN=nazwa`	APN karty SIM	`123456 CONNECT APN=internet`
`CONNECT`	`USER=nazwa`	Nazwa użytkownika APN (jeśli operator jej wymaga)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=hasło`	Hasło APN (jeśli operator go wymaga)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Wybór typu centrali alarmowej według numeru pozycji na liście **Security panel model** w TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=hhhh` / `DIR=OFF`	4-cyfrowe hasło sterowania bezpośredniego (hasło PC lub UDL centrali); `DIR=OFF` je wyłącza	`123456 CONNECT DIR=1122`

Możesz ograniczyć, z jakich numerów telefonów urządzenie przyjmuje polecenia: TrikdisConfig → strona **User reporting** → **Control by SMS**. Jeśli nie podano żadnego numeru, urządzenie wykona polecenie z poprawnym hasłem przysłane z dowolnego numeru.

6. TrikdisConfig – ustawienia szczegółowo

Po lewej stronie okna TrikdisConfig widać listę stron (System settings, CMS reporting, User reporting, SIM card, 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 G16 strona po stronie.

6.1 Pasek stanu

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

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

Po wprowadzeniu ustawień zapisujesz je w urządzeniu przyciskiem **Write [F5]**; przyciskami **Open [F8]** i **Save [F9]** możesz zapisać cały zestaw ustawień do pliku i wczytać go do innego urządzenia. **Save [F9]** zapisuje ustawienia do pliku konfiguracyjnego, a **Open [F8]** otwiera zapisany plik; zapisane ustawienia możesz później

wczytać także do innych urządzeń, dzięki czemu szybko skonfigurujesz wiele urządzeń z identycznymi ustawieniami.

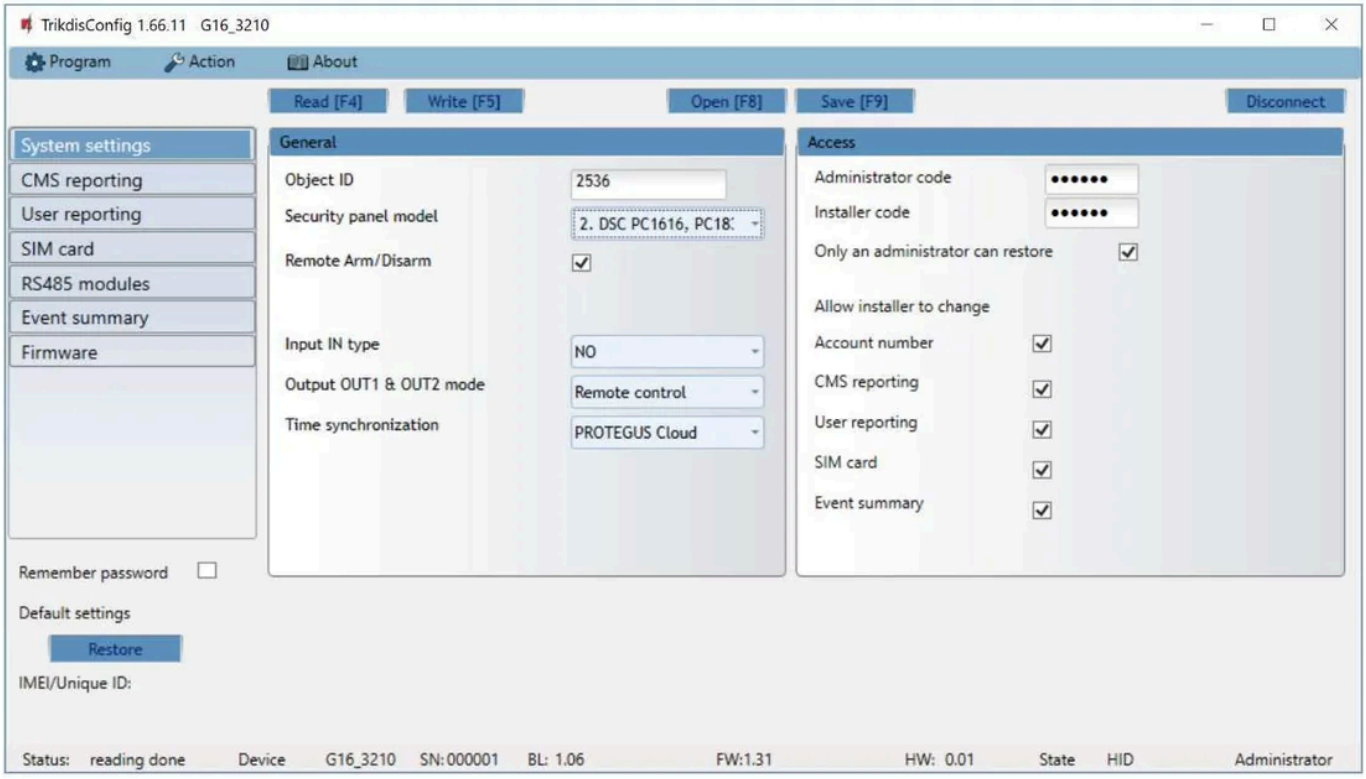
W polu **Device** dla G16 musi być oznaczenie typu G16 (na przykład G16_G410 lub G16_54E0). Po odczycie program pokazuje ustawienia zapisane w G16; ustaw je zgodnie z poniższymi opisami stron.



Rysunek 32. Pasek stanu TrikdisConfig z odczytanym G16: identyfikator, stan, typ, numer seryjny, wersje, sposób połączenia i poziom dostępu.

6.2 System settings

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



Rysunek 33. TrikdisConfig – strona System settings: grupy General i Access (na zdjęciu wersja sprzętowa 3, G16_3210; w wersji 4 nie ma pól Input IN type i Output OUT1 & OUT2 mode, zostały przeniesione na stronę IN/OUT).

- **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe, 0–9, A–F). Obowiązkowy, jeśli urządzenie raportuje także do stacji monitorowania; nie można użyć `FFFE` ani `FFFF`.
- **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 z Protegus 2 swoim kodem klawiatury. Pojawia się tylko w typach central sterowanych bezpośrednio; w centrali potrzebne jest do tego ustawienie zależne od producenta (rozdział 4). Przy uzbrajaniu strefą przełącznika kluczowego zostaw puste.
- **Security panel PC download password** – do sterowania bezpośredniego 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 set** – źródło zegara urządzenia (domyślnie **Cloud application**, chmura Protegus).

- W **wersji sprzętowej 3** znajdują się tu jeszcze pola **Input IN type** (typ wejścia: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) i **Output OUT1 & OUT2 mode** (tryb dwóch wyjść; do uzbrajania przełącznikiem kluczowym **Remote control**).

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

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

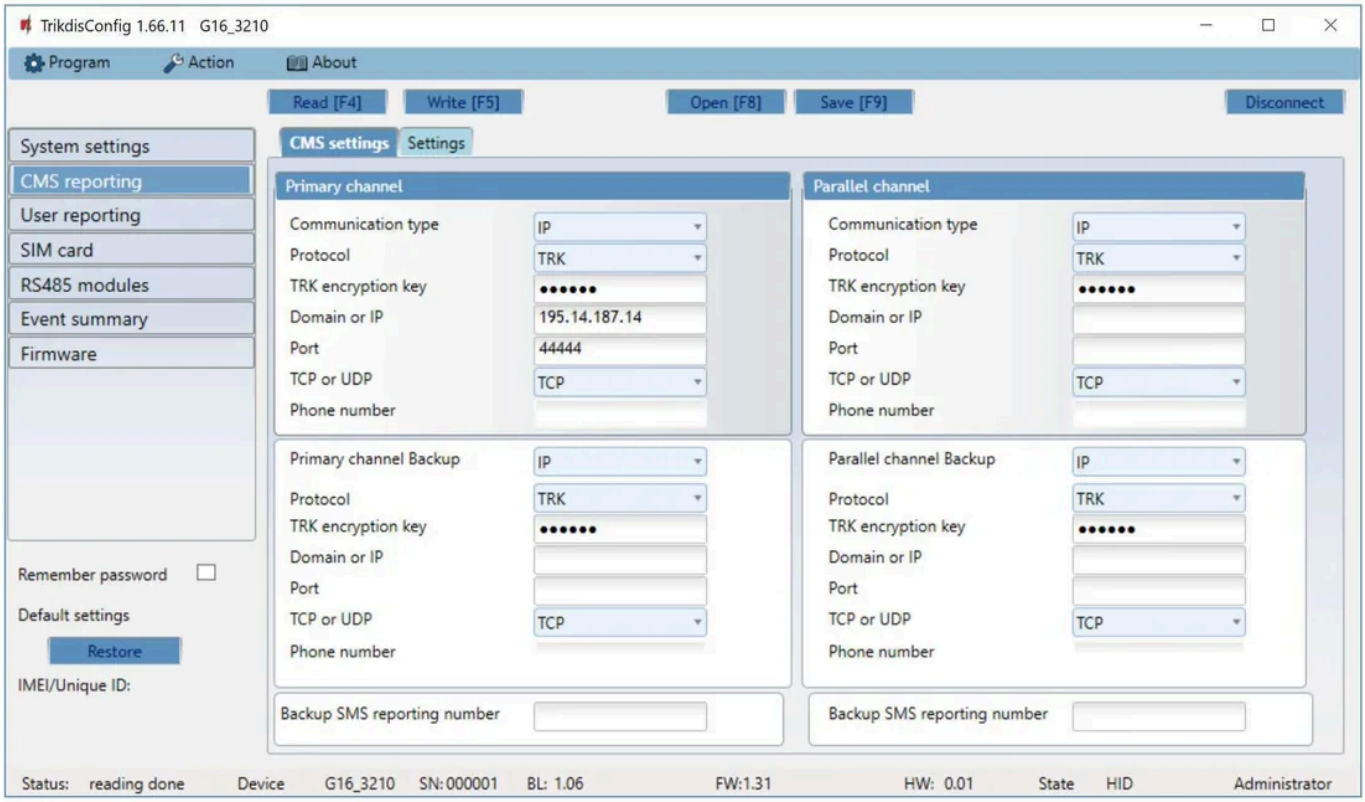
- **Administrator code** – dostęp do wszystkich ustawień (hasło fabryczne: `123456`; hasło ma 6 znaków: cyfry lub litery łacińskie).
- **Installer code** – dostęp, który można ograniczyć (hasło fabryczne: `654321`).
- **Only an administrator can restore** – po zaznaczeniu przywrócenie ustawień fabrycznych 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 transmisją danych komórkowych (IP) lub SMS-em. Zdarzenia mogą iść kilkoma kanałami: kanał **główny** i **równoległy** działają jednocześnie (do dwóch odbiorników naraz), a do każdego z nich należy kanał **zapasowy**, który wchodzi do działania, gdy dany kanał zostanie przerwany. Komunikacja jest szyfrowana i chroniona hasłem; do odbioru potrzebny jest odbiornik Trikdis (odbiornik programowy IPcom, RL14, RM14) albo odbiornik uniwersalny obsługujący protokół DC-09 / TL150. Odbiorniki Trikdis przekazują zdarzenia do oprogramowania stacji monitorowania: przez połączenie IP odbiornik programowy **IPcom** (Windows / Linux), odbiornik IP/SMS **RL14** lub odbiornik wielokanałowy **RM14**; do odbioru SMS odbiornik RL14, RM14 lub odbiornik SMS **GM14**.



Rysunek 34. TrikdisConfig – CMS reporting, zakładka CMS settings: kanał główny, zapasowy i równoległy.

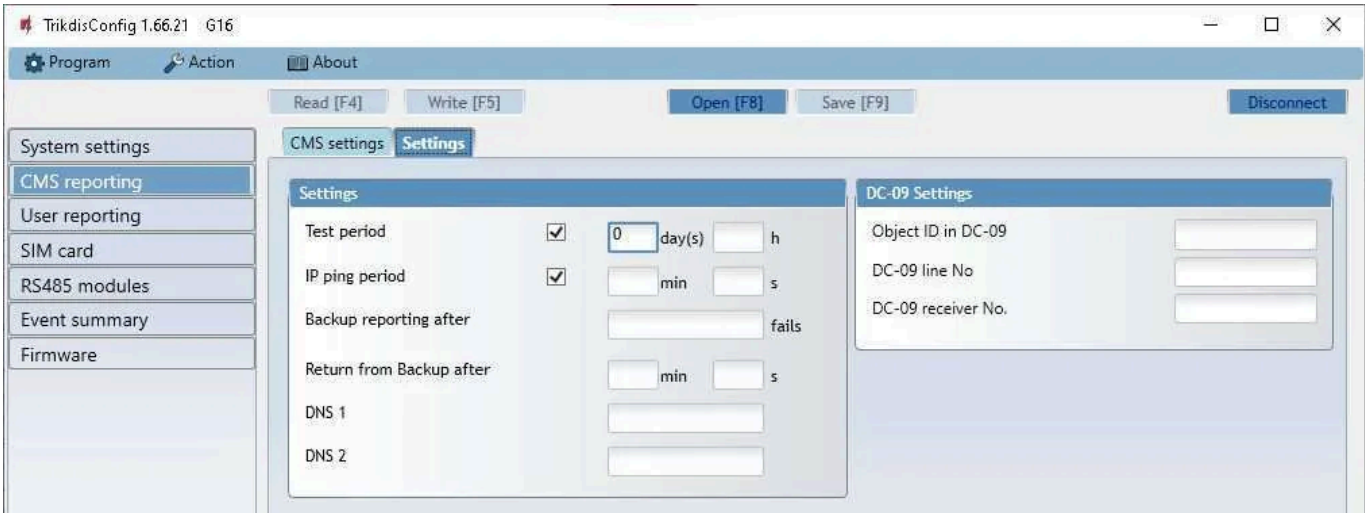
Primary channel – kanał główny

- **Communication type** – IP lub SMS. SMS dobrze nadaje się na rezerwę – działa także bez transmisji danych komórkowych – ale nie jest zalecany jako kanał główny.
- **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.
- **Phone number** – tylko przy komunikacji SMS: numer telefonu odbiornika SMS Trikdis z kodem kraju (np. `CCxxxxxxxxx`, gdzie CC to kod kraju).

Primary channel Backup – kanał zapasowy. Przejmuje komunikację, jeśli kanał główny nie działa; jego ustawienia są takie same jak powyżej.

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

Backup SMS reporting number – zapasowy numer SMS. Wchodzi do działania, jeśli wysyłanie nie powiedzie się ani kanałem głównym, ani równoległym, ani zapasowym; jest przydatny, bo działa także bez połączenia IP. Jest aktywny tylko wtedy, gdy kanał główny i zapasowy są w trybie IP. Urządzenie wysyła SMS do odbiornika SMS stacji monitorowania po pierwszym uruchomieniu, a także wtedy, gdy połączenie TCP/IP lub UDP/IP zostanie przerwane zarówno w kanale głównym, jak i w jego kanale zapasowym. W pole wpisz numer telefonu odbiornika SMS Trikdis stacji monitorowania z kodem kraju (np. `CCxxxxxxxxx`).



Rysunek 35. TrikdisConfig – CMS reporting, zakładka Settings: raport testowy, PING, czasy kanału zapasowego, DNS i dane DC-09.

W 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**.

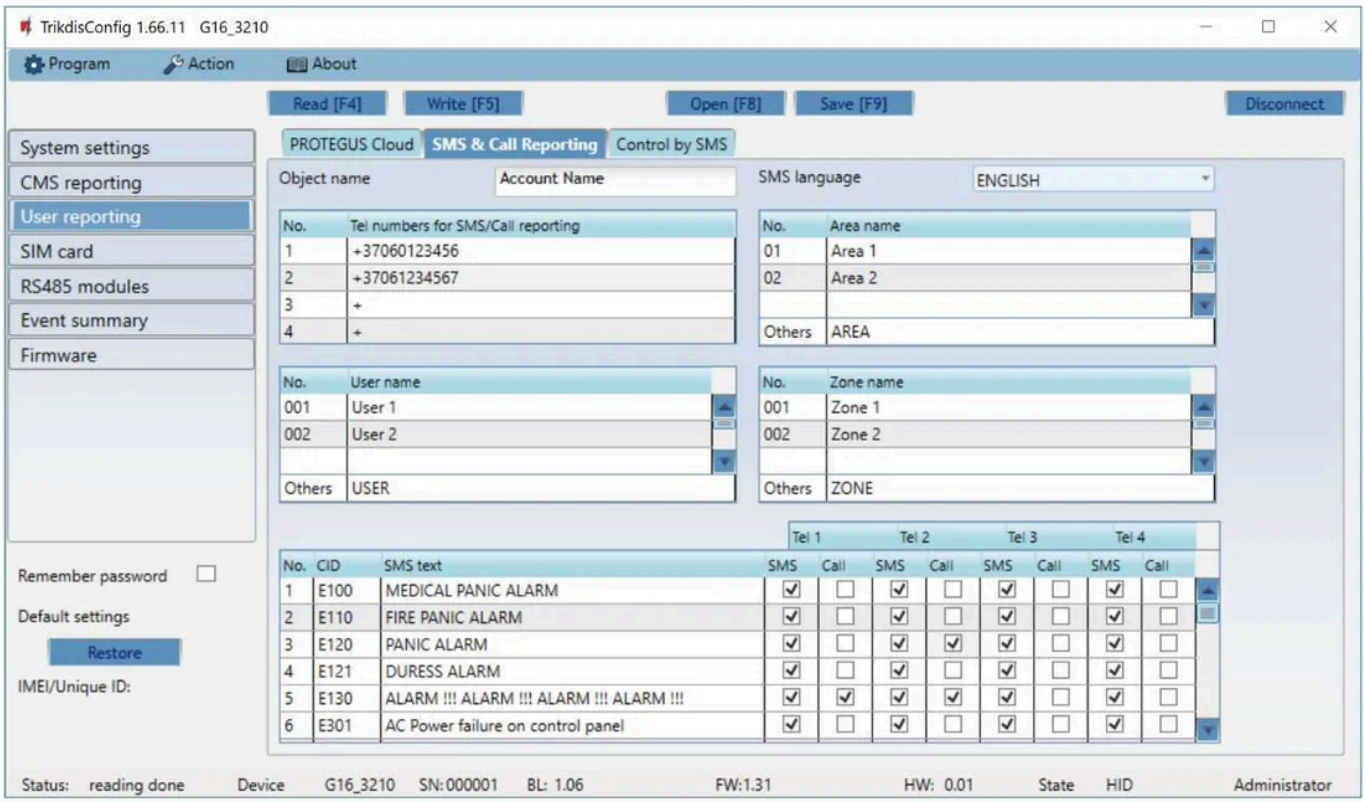
DC-09 Settings (po prawej stronie karty) – wypełniasz tylko wtedy, gdy na którymś kanale wysyłasz protokołem DC-09_2007 lub DC-09_2012; grupa pojawia się, gdy w polu **Protocol** któregoś kanału wybrano DC-09_2007 lub DC-09_2012:

- **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.

Na dole zakładki: **DNS 1, DNS 2** – serwery nazw; są potrzebne, jeśli odbiornik podałeś nazwą domeny, a nie adresem IP. Domyślnie jest to publiczny DNS Google. Grupa **DC-09 settings** jest widoczna tylko wtedy, gdy w którymś kanale ustawiony jest protokół DC-09.

6.4 User reporting

W zakładce **PROTEGUS Cloud** włączasz usługę Protegus. Dzięki usłudze Protegus użytkownik może zdalnie monitorować komunikator i system oraz nimi sterować; więcej informacji: www.protegus.app.

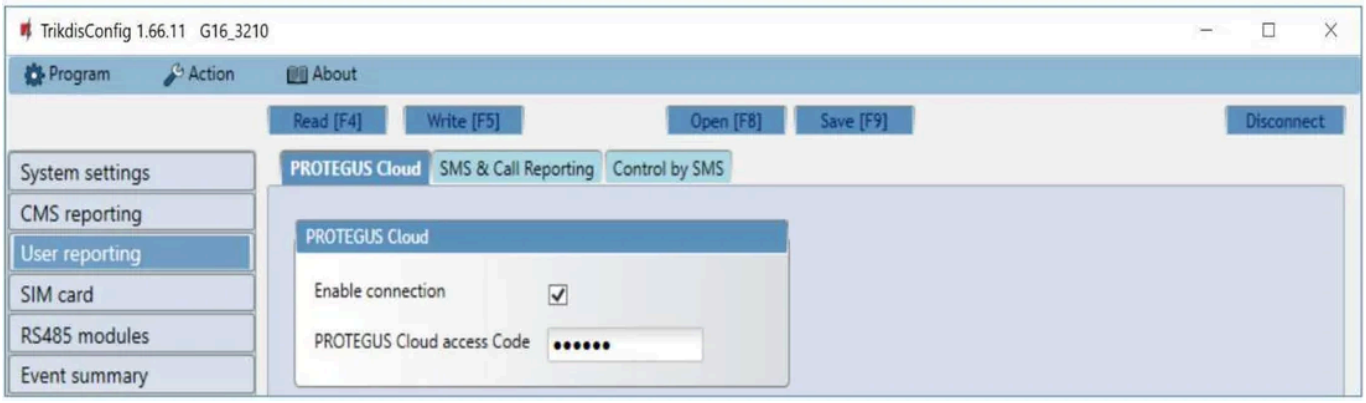


Rysunek 36. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

- **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.

W zakładce **SMS & Call Reporting** użytkownik może otrzymywać powiadomienia o zdarzeniach także SMS-em lub połączeniem telefonicznym.

W razie alarmu urządzenie najpierw wysyła SMS na wszystkie wpisane numery telefonów, a następnie dzwoni do nich po kolei od Tel 1 do Tel 4. Każdy numer jest wybierany raz i dzwoni przez 20 sekund; połączenie uznaje się za udane, jeśli numer dzwoni (wystarczy też odebranie lub odrzucenie). Modem wykonuje połączenie przez 2G lub VoLTE. Tam, gdzie operator wyłączył 2G i nie zatwierdził modemu dla VoLTE, SMS dociera, ale telefon nie dzwoni. To nie jest błąd konfiguracji. W takim miejscu korzystaj z SMS i aplikacji Protegus 2.



Rysunek 37. TrikdisConfig – User reporting, zakładka SMS & Call Reporting.

- **Object name** – nazwa systemu; pojawia się w każdym SMS-ie.
- **SMS language** – język SMS-ów (dla znaków diakrytycznych danego języka).

- **Tel numbers for SMS/Call reporting** – maksymalnie 4 numery telefonów z kodem kraju (`+CC…`, `00CC…` lub `CC…`, gdzie CC to kod kraju).
- **Area name, User name, Zone name** – nazwy partycji, użytkowników i stref; urządzenie używa ich w treści SMS-ów. W odpowiedniej tabeli wpisz numer partycji, użytkownika lub strefy, a obok jego nazwę. Przy centrali odczytywanej z magistrali przychodzą własne numery stref i użytkowników centrali – do nich podaj nazwy.
- **CID event table** – dla każdego zdarzenia można ustawić, który numer otrzyma SMS lub połączenie; można też zmienić treść komunikatu i kod Contact ID oraz dodać nowe zdarzenie.

W zakładce **Control by SMS** ustawiasz odbieranie poleceń SMS (polecenia opisuje punkt 5.5).

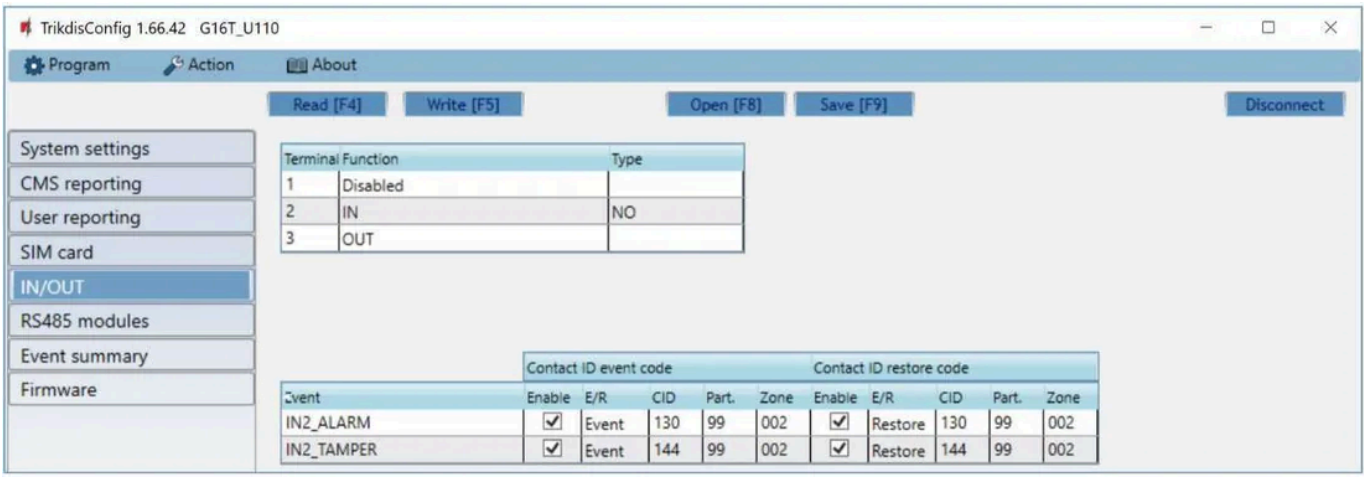


Rysunek 38. TrikdisConfig – User reporting, zakładka Control by SMS.

- **Reply text** – treść czterech odpowiedzi na polecenie SMS: polecenie wykonane (Command done), złe hasło (Wrong password), złe polecenie (Wrong command), złe dane (Wrong data).
- **Tel numbers for control by SMS** – maksymalnie 4 numery; urządzenie przyjmuje polecenia tylko z tych numerów. Jeśli pole jest puste, przyjmuje polecenie z poprawnym hasłem z dowolnego numeru; bezpieczeństwo zapewnia wtedy to, że w poleceniu obowiązkowe jest hasło administratora lub instalatora.

6.5 SIM card

Bez danych karty SIM urządzenie nie połączy się z siecią transmisji danych.



Rysunek 39. TrikdisConfig – strona SIM card.

- **SIM card PIN** – kod PIN karty. Żądanie PIN możesz wyłączyć, jeśli włożysz kartę do telefonu komórkowego i tam je zablokujesz. Jeśli żądanie PIN jest wyłączone, może zostać wartość fabryczna pola.

- **APN** – punkt dostępu operatora (Access Point Name); bez niego komunikator nie połączy się z internetem. Znajdziesz go także na stronie operatora; APN „internet" jest ogólny i działa w sieciach wielu operatorów. Znane APN-y operatorów wymienia artykuł o APN (do karty IoT / M2M operator podaje osobny APN, zobacz punkt 2.3).
- **Login, Password** – nazwa użytkownika i hasło APN, jeśli operator ich wymaga.
- **Forbid connection when roaming detected** – przydatne w pobliżu granicy państwa: nie pozwala, aby urządzenie połączyło się z siecią sąsiedniego kraju.

Przed użyciem upewnij się, że karta SIM jest aktywna i ma włączoną usługę transmisji danych do komunikacji IP.

6.6 IN/OUT

Tutaj określasz rolę trzech zacisków I/O komunikatora o podwójnej funkcji: **Disabled** (nieużywany), **IN** (wejście) lub **OUT** (wyjście). Dla wejścia trzeba też podać typ (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Ustawienie fabryczne: I/O 1 nieużywany, I/O 2 wejście (NO), I/O 3 wyjście.



Rysunek 40. TrikdisConfig – strona IN/OUT: funkcja zacisków I/O i zdarzenia wejść.

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

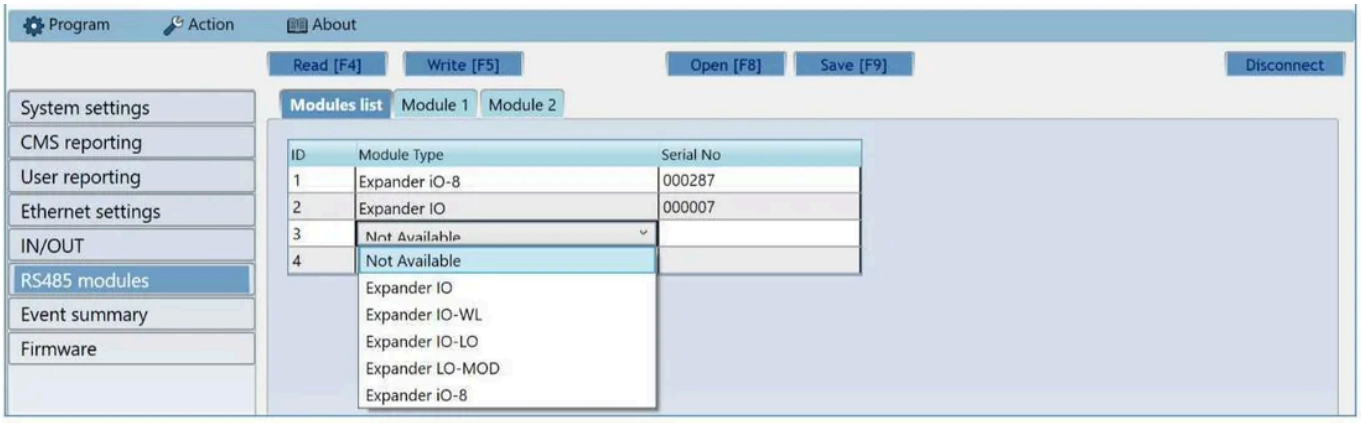
- **Enable** – włącza wysyłanie komunikatu.
- **E/R** – typ zdarzenia: Event (alarm) lub Restore (powrót do normy).
- **CID** – kod Contact ID.
- **Part.** – numer partycji w komunikacie.
- **Zone** – numer strefy w komunikacie.

W **wersji sprzętowej 3** nie ma strony IN/OUT: typ jedynego wejścia ustawiasz w polu **System settings** → **Input IN type**, tryb dwóch wyjść w polu **Output OUT1 & OUT2 mode**, a zdarzenia wejścia (IN_ALARM, IN_TAMPER) na stronie **Event summary**.

6.7 RS485 modules

Ekspandery iO-8 i moduły W485 / E485 podłączone do magistrali RS485 trzeba dodać w zakładce **Modules list**.

W G16 z modemem 2G (G16_G410) tej strony nie można używać: wersja 2G nie ma magistrali RS485.

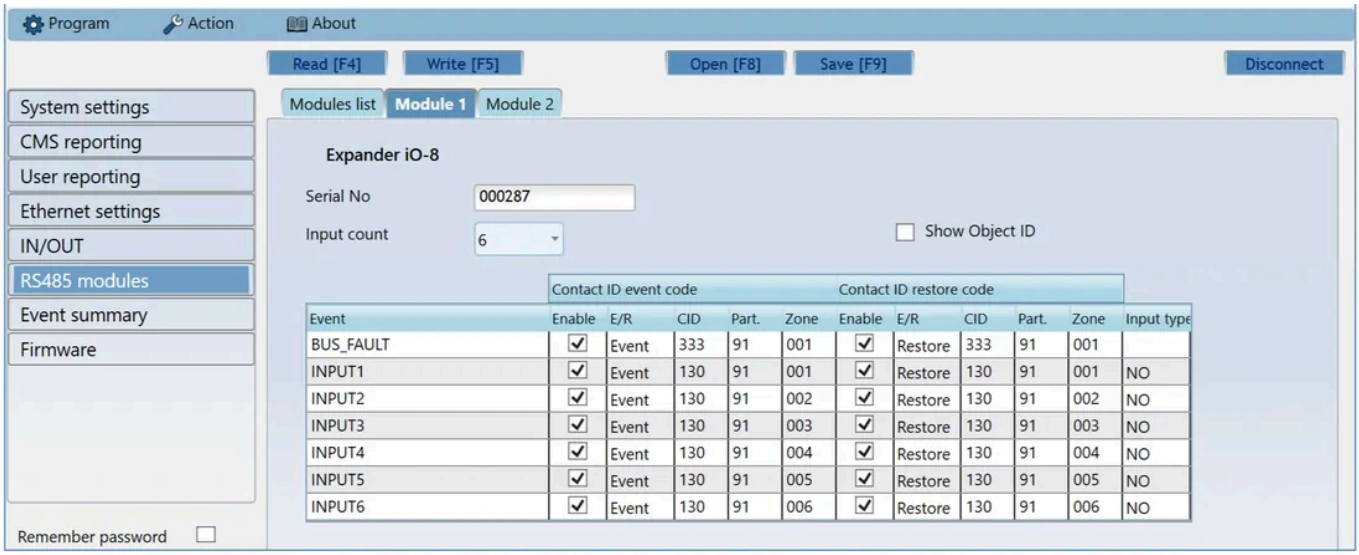


Rysunek 41. TrikdisConfig – RS485 modules, zakładka Modules list: typ modułu (Expander iO-8, W17u/W485, E485) i numer seryjny.

- **Module Type** – typ podłączonego modułu z listy (Expander iO-8, W17u/W485, E485).
- **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 maksymalnie 4 moduły.



Rysunek 42. TrikdisConfig – RS485 modules, zakładka modułu iO-8.

- **Input Count** – ile zacisków ma być wejściami; pozostałe będą wyjściami. Typ wejścia (**Input type**: NO lub NC) można podać w tabeli. Rolę wyjść (uzbrajanie / rozbrajanie strefą przełącznika kluczowego lub przełączanie urządzenia) ustawiasz w aplikacji Protegus 2.
- W tabeli możesz przypisać kod Contact ID do usterki magistrali (**BUS_FAULT**, Contact ID 333) oraz do zdarzeń naruszenia i powrotu do normy wejść (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Po naruszeniu wejścia komunikator wysyła zdarzenie z ustawionym kodem do odbiornika stacji monitorowania, do aplikacji Protegus 2 i SMS-em na numer telefonu użytkownika. Domyślnie 1. moduł raportuje z partycją 91, a 4. moduł z partycją 94. Po zaznaczeniu **Show Object ID** można dla wejść podać także identyfikator obiektu inny niż komunikatora.
- Jeśli użytkownik ma otrzymywać SMS lub połączenie także z wejść ekspandera, dodaj kod Contact ID przypisany do wejścia także do tabeli zdarzeń zakładki **SMS & Call Reporting**.

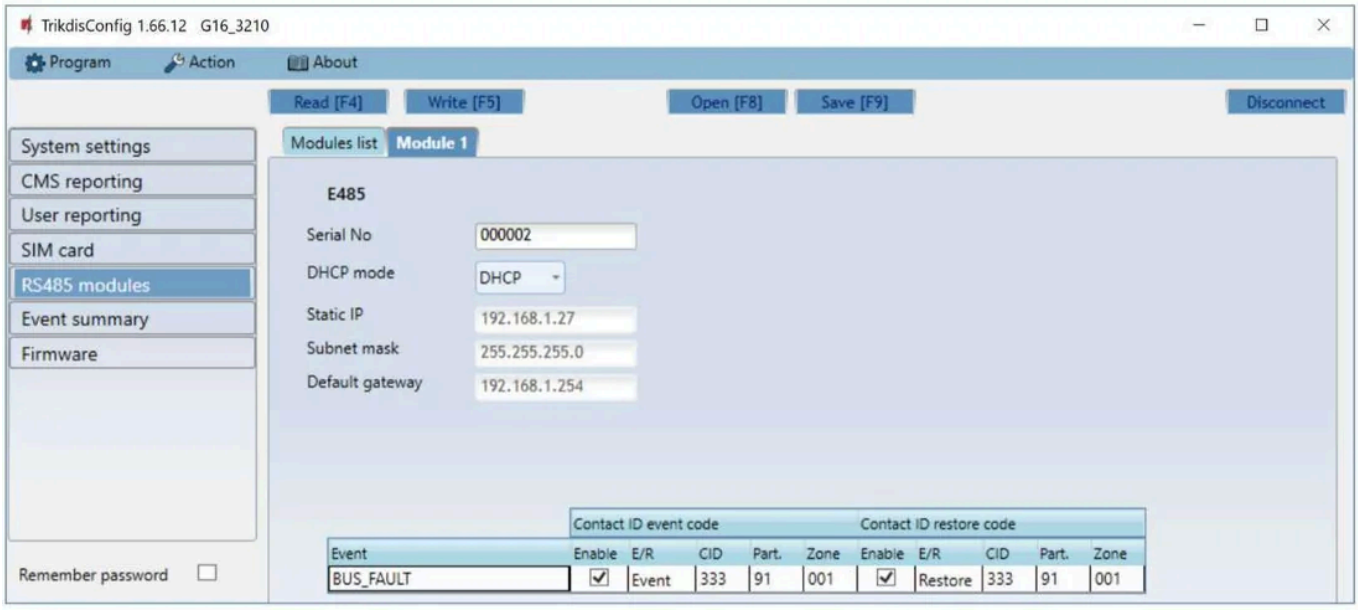
Moduł WiFi W485 (na liście W17u/W485) – dane sieci WiFi i ustawienia sieciowe.



Rysunek 43. TrikdisConfig – RS485 modules, zakładka modułu W485.

- **DHCP mode** – automatyczne (DHCP) lub ręczne (Static) ustawienia sieciowe.
- **Static IP**, **Subnet mask**, **Default gateway** – przy ustawieniu ręcznym.
- **Wifi SSID name**, **Wifi SSID password** – nazwa i hasło sieci WiFi.
- W tabeli możesz przypisać kod Contact ID do usterek magistrali RS485 (przerwanie i przywrócenie połączenia między modułem a G16); zdarzenie otrzymuje zarówno stacja monitorowania, jak i Protegus 2.

Moduł Ethernet E485 – te same ustawienia sieciowe bez WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); w tabeli także tutaj możesz przypisać kod Contact ID do usterki magistrali RS485 (przerwanie i przywrócenie połączenia między E485 a G16), który otrzymuje zarówno stacja monitorowania, jak i Protegus 2.



Rysunek 44. TrikdisConfig – RS485 modules, zakładka modułu E485.

Do działania W485 i E485 musi być ustawione połączenie G16 ze stacją monitorowania i/lub z Protegus (punkty 2.3 i 2.4), a w G16 musi być karta SIM. Dopóki działa połączenie przewodowe lub WiFi, komunikator komunikuje się przez nie i nie używa transmisji danych komórkowych.

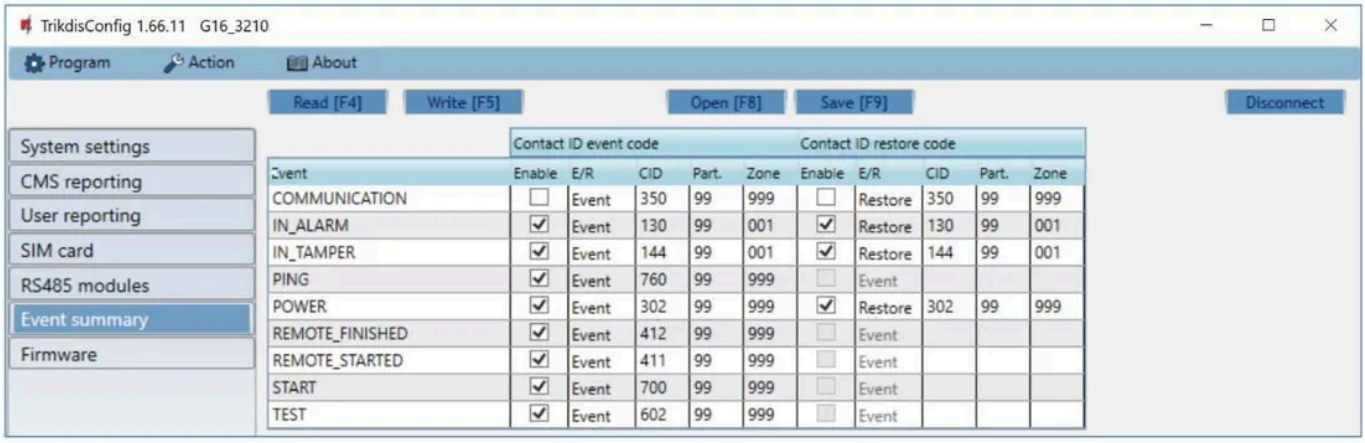
6.8 Event summary

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

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

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

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



Rysunek 45. TrikdisConfig – strona Event summary: wewnętrzne komunikaty urządzenia (na zdjęciu wersja sprzętowa 3, w której zdarzenia IN_ALARM i IN_TAMPER wejścia oraz PING również są tutaj; w wersji 4 zdarzenia wejść są na stronie IN/OUT).

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.

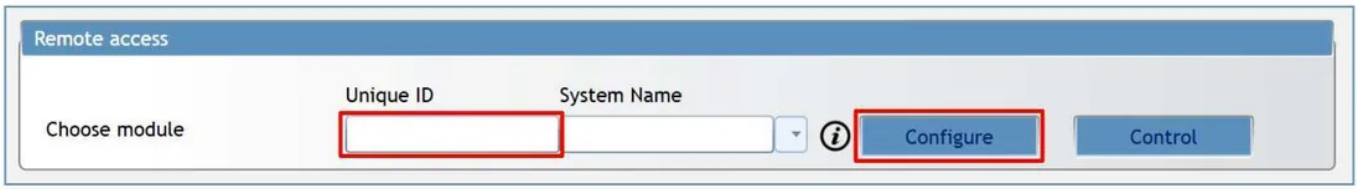
Do zdalnego dostępu potrzebne jest:

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 46. TrikdisConfig – Remote access: identyfikator urządzenia, 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 także, czy komunikator rzeczywiście odczytuje dane z centrali: uzbrój i rozbrój centralę z klawiatury 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 także próbne uzbrojenie z aplikacji, kodem klawiatury użytkownika.

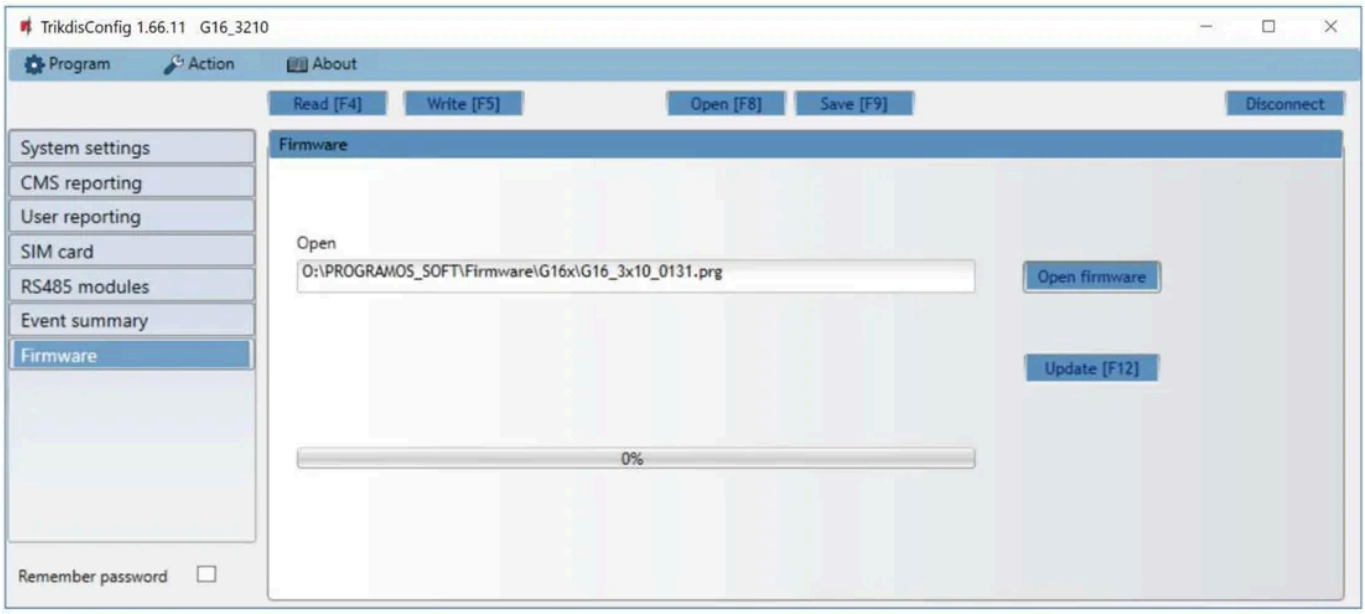
9. Aktualizacja firmware

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

Do aktualizacji potrzebne jest połączenie z internetem. Program antywirusowy, zapora sieciowa lub restrykcyjne ustawienia sieci mogą zablokować automatyczne pobieranie firmware; wtedy zmień ustawienia programu antywirusowego (zezwól TrikdisConfig na dostęp do internetu) albo pobierz plik ręcznie i otwórz go na stronie Firmware.

10. Rozwiązywanie problemów i najczęstsze pytania

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. Zobacz mignięcia diody **TROUBLE**: 1 = brak SIM, 2 = zły PIN, 3 = brak APN, 4 = nie może połączyć się z siecią komórkową, 5 = nie może połączyć się z siecią transmisji danych.
2. Sprawdź, czy karta SIM jest aktywna, ma usługę transmisji danych i dobrze siedzi w gnieździe.
3. Jeśli żądanie PIN jest włączone na karcie, podaj PIN na stronie **SIM card** albo wyłącz żądanie PIN w telefonie.
4. Sprawdź antenę: jest przykręcona, nie jest w metalowej obudowie, poziom sygnału jest odpowiedni (punkty 1.7 i 3.2).

Jest sieć, 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 i port odbiornika, ustawienie TCP/UDP oraz klucz szyfrowania (**CMS reporting**).
2. Jeśli odbiornik jest podany nazwą domeny, sprawdź ustawienie DNS (**CMS reporting** → **Settings**).
3. Sprawdź, czy pakiet danych karty SIM nie blokuje potrzebnego portu (niektóre karty M2M dopuszczają tylko określone adresy).

Dioda TROUBLE miga siedem razy – komunikator nie widzi centrali

1. Sprawdź podłączenie według rysunku z punktu 3.3: najczęstszym błędem są zamienione przewody **CLK** i **DATA** albo linia danych podłączona do złego zacisku centrali.
2. W polu **System settings** → **Security panel model** programu TrikdisConfig musi być wybrany dokładny typ podłączonej centrali.
3. W centralach Texecom, Caddx, Honeywell i InnerRange potrzebne jest także ustawienie w centrali (rozdział 4) – bez niego centrala nie wysyła 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** G16 nie działa (do magistrali NEO nie można podłączyć urządzeń zewnętrznych) – tu potrzebny jest komunikator na linię telefoniczną.

Zdarzenia przychodzą, ale nie mogę uzbroić systemu z aplikacji

Przy sterowaniu bezpośrednim:

1. Na stronie **System settings** musi być zaznaczone **Remote Arm/Disarm**.
2. W centralach Paradox i Texecom **Security panel PC download password** musi być takie samo jak hasło 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).

Ze strefą przełącznika kluczowego:

1. **Remote Arm/Disarm** musi być puste, a zacisk I/O na stronie **IN/OUT** musi być 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. Wpisz IMEI dokładnie, z pudełka lub z tyłu urządzenia.
4. Usługa transmisji danych karty SIM i APN muszą być w porządku (dioda NETWORK świeci na zielono, a dioda DATA gaśnie po zdarzeniu).

Nie mogę zalogować 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 utrzymuje 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.

Dlaczego nie widzę strony RS485 modules albo dlaczego iO-8 nie działa?

G16 z modemem 2G (G16_G410) nie ma magistrali RS485; iO-8, W485 i E485 można podłączyć tylko do wersji 4G (G16_54E0). Do modułu W485 i E485 w G16 musi być także karta SIM.

Mam urządzenie 2G – jak długo będzie działać?

Wyłączanie sieci 2G postępuje u każdego operatora w innym tempie; do długotrwałej pracy zalecamy wersję 4G, którą można też rozbudować przez magistralę RS485.

Ile danych zużywa urządzenie?

Komunikaty zdarzeń i PING-i są bardzo małe; transfer zależy głównie od okresu PING i częstotliwości raportów testowych. W przeciętnym systemie domowym miesięczny transfer zwykle nie przekracza 10 MB. Dokładna wartość zależy od ustawień i jednostki rozliczeniowej operatora, dlatego przy karcie z limitem danych warto sprawdzić transfer w pierwszym miesiącu.

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 zabezpieczających może wykonywać tylko wykwalifikowany instalator.
- Przed instalacją uważnie przeczytaj instrukcję; nieprzestrzeganie zaleceń może prowadzić do nieprawidłowego działania lub uszkodzenia.
- Przed podłączeniem, przy każdym podłączaniu elektrycznym i przed serwisem odłącz urządzenie od zasilania.
- Usterki wynikające z nieprawidłowej instalacji lub użytkowania oraz modyfikacje i naprawy niedopuszczone przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów o odpadach: uszkodzonego urządzenia i jego części nie wyrzucaj do odpadów komunalnych.

Zobacz też

- Wyszukiwarka zgodności – który komunikator pasuje do której centrali alarmowej.
- G16 – sterowanie bezpośrednie centralami alarmowymi DSC PowerSeries – uzbrajanie kodem klawiatury, stany stref, blokowanie stref.
- DSC Power Series NEO i komunikatory Trikdis: zgodność i rozwiązania – dlaczego G16 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.
- Nadchodzi wersja sprzętowa v4 komunikatorów GSM G16 i G16T – co się zmieniło w porównaniu z wersją 3.
- Ustawienie APN – lista europejskich operatorów komórkowych – APN karty SIM według operatora.
- Dokumentacja w języku angielskim: docs.trikdis.com – instrukcje w serwisie docs.trikdis.com są w języku angielskim.

Powiązane produkty

Trikdis G16 4G GSM inteligentny moduł komunikacyjny

Trikdis G16 2G GSM inteligentny moduł komunikacyjny

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-g16