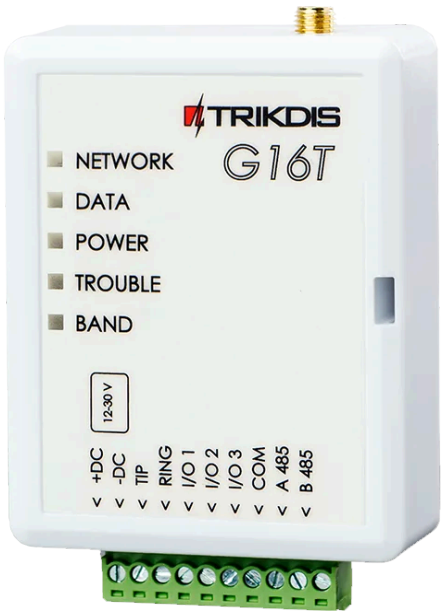
Komunikator G16T – instrukcja dla instalatora i użytkownika

Instrukcja dla instalatora i użytkownika komunikatora Trikdis G16T: podłączenie do centrali alarmowej, karta SIM i konfiguracja w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2, sprawdzenie działania i rozwiązywanie problemów.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-g16t

Spis treści

1. Przegląd

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

2. Szybkie uruchomienie w TrikdisConfig

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

3. Instalacja i podłączenie

- 3.1 Kroki instalacji
- 3.2 Umiejscowienie i antena
- 3.3 Podłączenie do centrali alarmowej
  - 3.3.1 W uzasadnionych przypadkach: nadzór linii
- 3.4 Podłączenie strefy typu klucz
- 3.5 Podłączenie wejść
- 3.6 Podłączenie wyjścia z przekaźnikiem
- 3.7 Podłączenie ekspandera iO-8
- 3.8 Podłączenie modułów W485 i E485
- 3.9 Włączenie i pierwsze sprawdzenie
- A TRIKDIS átjelző elindítása

4. Programowanie centrali alarmowej

- 4.1 Programowanie dialera Honeywell Vista
- 4.2 Centrale innych producentów

5. Zdalne sterowanie aplikacją Protegus 2

- 5.1 Dodanie urządzenia
- A rendszer létrehozása a Protegus 2 alkalmazásban
- 5.2 Uzbrajanie i rozbrajanie wyjściem
- 5.3 Uzbrajanie i rozbrajanie z aplikacji
- 5.4 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

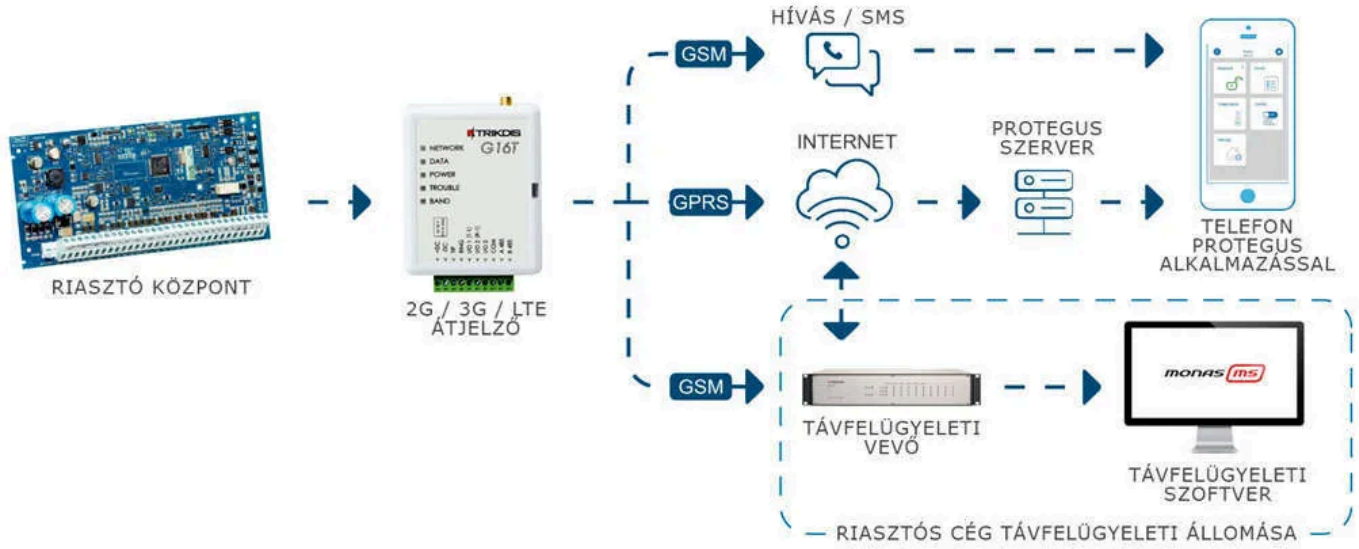
1. Przegląd

G16T to **uniwersalny komunikator komórkowy** firmy Trikdis: podłącza się do wyjścia linii telefonicznej centrali alarmowej (TIP/RING) i zachowuje się jak centrala telefoniczna. Centrala alarmowa „wybiera numer" i wysyła komunikat Contact ID tonami DTMF, a G16T odbiera połączenie, dekoduje komunikat i przesyła go przez komórkową transmisję danych do odbiornika stacji monitorowania oraz do chmury Protegus, do aplikacji użytkownika. Dzięki temu można z nim używać **centrali dowolnego producenta**, która ma dialer Contact ID – centrali nie trzeba wymieniać, wystarczy skonfigurować jej dialer. Komunikatory G16T mają certyfikat najwyższego stopnia zabezpieczenia **EN 50131 Grade 4**.

1.1 Do czego służy i jak działa

- **Transmisja 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). W kierunku odbiornika SUR-GARD zamienia kody Contact ID otrzymane z centrali na kody SIA; tabela konwersji znajduje się w załączniku do angielskiej dokumentacji Trikdis. Połączenie sprawdza domyślnie co 30 sekund (lub w ustawionym odstępie), a w razie błędu przełącza się na kanał zapasowy.
- **Powiadamianie użytkownika.** Aplikacja Protegus 2 pokazuje zdarzenia w powiadomieniach push z osobnym dźwiękiem i na liście zdarzeń; użytkownik może w aplikacji uzbrajać i rozbrajać system oraz sterować podłączonymi urządzeniami (oświetlenie, brama, wentylacja, ogrzewanie, nawadnianie itp.). Aplikacja działa z każdą centralą alarmową, do której podłączony jest komunikator, niezależnie od producenta centrali.
- **Jednocześnie lub osobno** obsługuje stację monitorowania i użytkownika: można go używać tylko z Protegus 2 (bez stacji monitorowania), tylko ze stacją monitorowania albo z oboma. Jeśli skonfigurowane są oba, zdarzenie najpierw trafia do stacji monitorowania, a potem do użytkownika.
- **Zapasowy kanał SMS.** Powiadamia stację monitorowania także SMS-em, jeśli transmisja danych w sieci operatora nie działa; potrafi wysyłać równolegle do dwóch odbiorników, każdy z osobnym kanałem zapasowym.
- **Własne wejścia i wyjścia.** Trzy zaciski I/O o podwójnej funkcji mogą pracować jako wejścia (czujka, sabotaż) lub jako sterowane wyjścia (strefa typu klucz, przekaźnik). Na magistrali RS485 wersji 4G ekspander iO-8 dodaje kolejne 8 I/O (inne przewodowe lub bezprzewodowe ekspandery serii iO dodają kolejne wejścia i wyjścia, a ekspander iO lub iO-WL umożliwia zdalny pomiar temperatury), a z modułem W485 lub E485 komunikator może łączyć się także przez WiFi lub internet przewodowy – wtedy sieć komórkowa jest drogą zapasową.

Budowę systemu pokazuje poniższa ilustracja: wyjście linii telefonicznej centrali alarmowej jest podłączone do G16T, G16T łączy się z internetem przez sieć komórkową, stamtąd z odbiornikiem stacji monitorowania i z chmurą Protegus, a użytkownik widzi system w aplikacji Protegus 2.



Rysunek 1. Miejsce G16T w systemie: centrala alarmowa → G16T → sieć komórkowa → odbiornik stacji monitorowania i chmura Protegus → aplikacja Protegus 2.

1.2 Wersje

Ta instrukcja dotyczy **wersji sprzętowej 4** komunikatora G16T, ale **można jej używać także dla wersji sprzętowej 3**: podłączenie, konfiguracja i działanie obu wersji są w dużej mierze takie same. Różnice zebrano w poniższej tabeli; tam, gdzie tekst podaje dane wersji 4, przy wersji 3 uwzględnij tę tabelę.

	Sprzęt w wersji 3 (v3)	**Sprzęt w wersji 4 (v4)**
Typy	G16T_321x (2G), G16T_331x (3G), G16T_341x (4G), G16T_3M10 (LTE Cat-M1 + 2G) – wszystkie na 1 kartę SIM	G16T_G410 (2G), G16T_E120 (4G, z rezerwą 2G)
Wejścia/wyjścia	2 wejścia o wybieranym typie (T-1/IN1, R-1/IN2 – mogą służyć także do nadzoru linii telefonicznej) + 1 wyjście typu otwarty kolektor (OUT, maks. 0,15 A)	3 zaciski I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3), każdy może pracować jako wejście lub jako wyjście typu otwarty kolektor (maks. 0,15 A)
Pobór prądu	60–100 mA; podczas wysyłania do 250 mA	60–100 mA; podczas wysyłania do 500 mA
Częstotliwości modemu	2G: 850 / 900 / 1800 / 1900 MHz; 3G: 800 / 850 / 900 / 1900 / 2100 MHz; 4G: zależne od regionu	2G: 850 / 900 / 1800 / 1900 MHz; 4G: zależne od regionu
Wymiary	92 × 62 × 26 mm	92 × 65 × 26 mm
Magistrala RS485 (iO-8, W485, E485)	jest	tylko w wersji 4G (G16T_E120)

Wersja sprzętowa 4 jest produkowana z dwoma modemami:

Typ	**Modem**	**Częstotliwości**	**RS485 (iO-8, W485, E485)**
G16T_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	brak
G16T_E120	4G (LTE), z rezerwą 2G	zależne od regionu	jest

Wersję sprzętową znajdziesz na pasku stanu TrikdisConfig (**HW**) i na naklejce na tylnej części obudowy urządzenia.

1.3 Główne cechy

Połączenie z centralą alarmową

- Standardowe podłączenie do wyjścia linii telefonicznej centrali: DC+, DC−, TIP i RING. W uzasadnionych przypadkach można go podłączyć także z nadzorem linii (przewodami T-1 i R-1): wtedy połączenie między centralą a komunikatorem jest **nadzorowane**, przerwanie przewodu komunikator sygnalizuje.
- Centrala wysyła zdarzenia w formacie Contact ID, wybieraniem DTMF; G16T przekazuje pełną informację o zdarzeniu (kod, partycja, strefa lub użytkownik).

Komunikacja ze stacją monitorowania

- Połączenie IP z odbiornikami Trikdis (programowy odbiornik 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

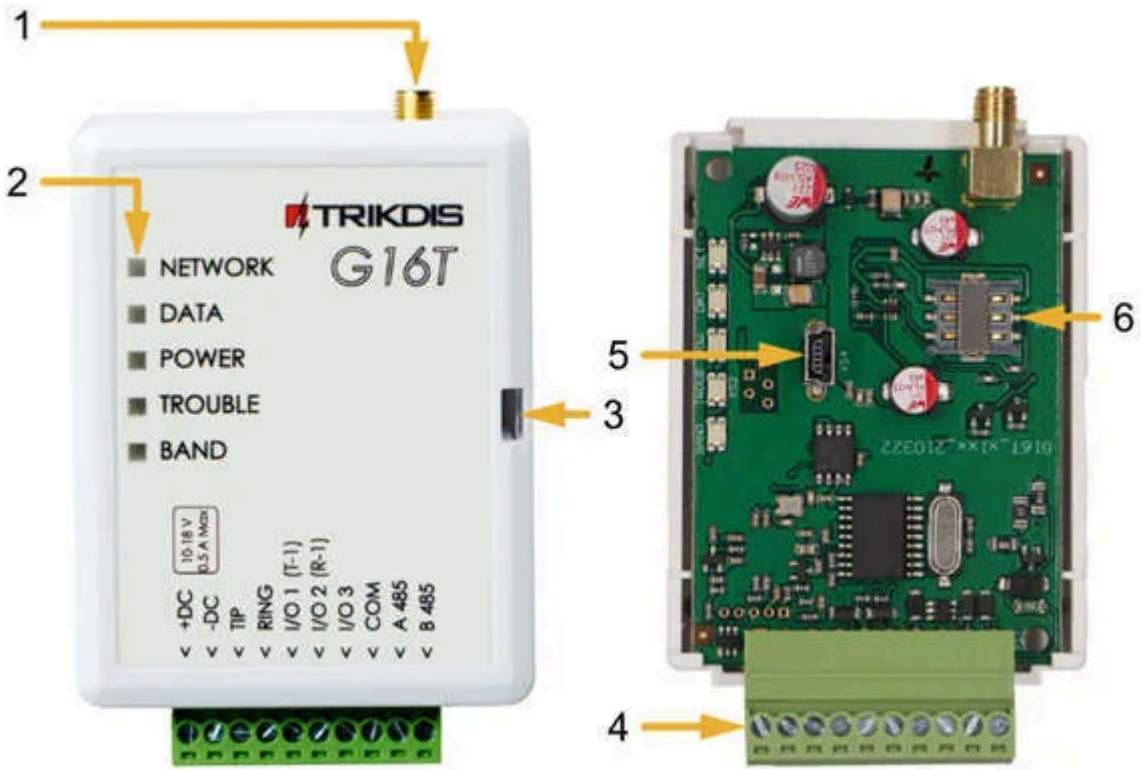
- Aplikacja mobilna i webowa Protegus 2: powiadomienia push z osobnym dźwiękiem, lista zdarzeń, uzbrajanie i rozbrajanie, sterowanie wyjściami.
- Zdalny pomiar temperatury (z ekspanderem iO lub iO-WL).
- Sterowanie i podstawowa konfiguracja także poleceniami SMS.
- Powiadomienia także SMS-em i połączeniem telefonicznym, na maksymalnie 4 numery telefonu.
- 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 (stacja monitorowania) i instalator.
- Zdalna konfiguracja i aktualizacja w programie TrikdisConfig.

1.4 Elementy komunikatora

Płytka drukowana G16T znajduje się w białej obudowie z tworzywa; przednią pokrywę można zdjąć, a listwę zaciskową odłączyć. Na ilustracji poniżej widać wersję 4G; wersja 2G nie ma diody BAND ani zacisków A 485 / B 485.



Rysunek 2. Elementy G16T (wersja 4G) z przodu i przy otwartej obudowie.

- 1 Złącze SMA anteny GSM
- 2 Diody LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Otwór ułatwiający zdjęcie przedniej pokrywy
- 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, przy podłączaniu łatwiej ją obsłużyć, a do programowania przez USB urządzenie można zanieść do komputera.

1.5 Zaciski

Zacisk	Funkcja
+DC	Zasilanie, +10–18 V DC
–DC	Zasilanie, minus
TIP	Zacisk TIP centrali alarmowej
RING	Zacisk RING centrali alarmowej
I/O 1 (T-1)	1. wejście/wyjście lub punkt T-1 nadzoru linii telefonicznej
I/O 2 (R-1)	2. wejście/wyjście lub punkt R-1 nadzoru linii telefonicznej
I/O 3	3. wejście/wyjście
COM	Wspólny (ujemny) punkt dla wejść i wyjść
A 485	Przewód A magistrali RS485 (tylko wersja 4G)
B 485	Przewód B magistrali RS485 (tylko wersja 4G)

Opis zacisków jest także na przedniej pokrywie, więc przy podłączaniu nie trzeba jej zdejmować.

1.6 Sygnalizacja LED

Diody LED na przedniej pokrywie to najważniejsze narzędzie przy uruchamianiu i diagnozowaniu. 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 3G/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 odłączone
świeci na zielono	Włączony, napięcie zasilania prawidłowe
świeci na żółto	Nieprawidłowe napięcie zasilania (maks. 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

Sygnalizacja	Znaczenie
2 czerwone mignięcia	Błąd PIN karty SIM (błędny 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
7 czerwonych mignięć	Przerwane połączenie z centralą alarmową
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)

1.7 Dane techniczne

Parametr	Wartość
Połączenie z centralą alarmową	przewodowa linia telefoniczna (TIP/RING), Contact ID, DTMF
Wejścia/wyjścia	3 I/O o podwójnej funkcji (I/O 1, I/O 2, I/O 3): jako wejście NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (rezystor parametryczny 2,2 kΩ); jako wyjście typu otwarty kolektor (OC), maks. 0,15 A / 30 V DC
Rozbudowa	na magistrali 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; do 500 mA podczas wysyłania
Protokoły transmisji	TRK, DC-09_2007, DC-09_2012, TL150
Bufor zdarzeń	60 komunikatów
Szyfrowanie	AES-128
Programowanie	TrikdisConfig (Windows) przez kabel USB Mini-B lub zdalnie; polecenia SMS
Warunki pracy	−10 … +50 °C, maks. 80 % wilgotności względnej (przy +20 °C)
Wymiary	92 × 65 × 26 mm

Parametr	Wartość
Masa	80 g

2. Szybkie uruchomienie w TrikdisConfig

Wszystkie ustawienia G16T wprowadza się w programie **TrikdisConfig** działającym w systemie Windows – przez kabel USB lub zdalnie. W tym rozdziale opisujemy najkrótszą drogę: urządzenie konfigurujesz na biurku, przed podłączeniem, a na miejscu instalacji wystarczy je już tylko podłączyć. Szczegółowe objaśnienie ustawień zawiera rozdział 6.

2.1 Przygotowanie

Czego będziesz potrzebować

Kabel USB Mini-B · kabel co najmniej 4-żyłowy do centrali · płaski śrubokręt 2,5 mm · antena komórkowa o odpowiednim zysku (jeśli na miejscu zasięg jest słaby) · aktywna karta nano-SIM z usługą transmisji danych · instrukcja instalatora centrali alarmowej.

Potrzebne akcesoria zamów osobno u dystrybutora.

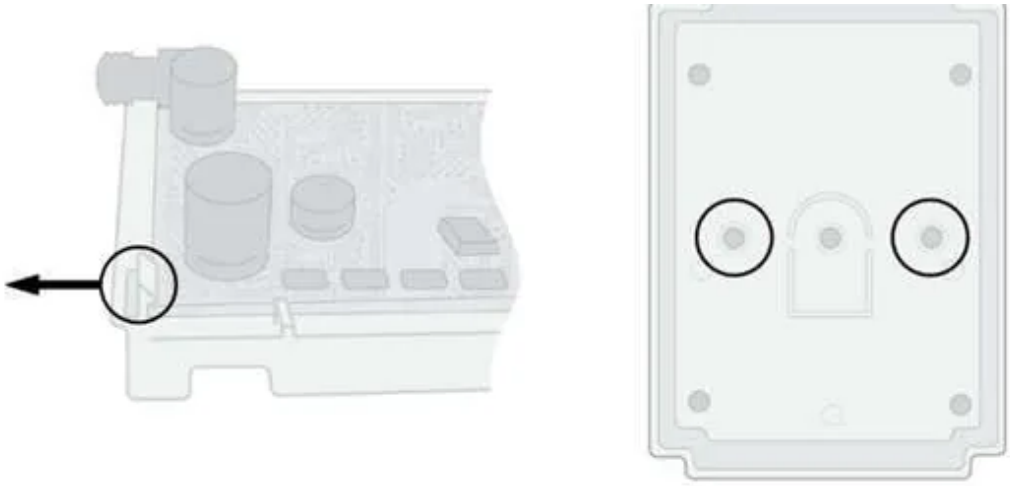
1. Pobierz i zainstaluj program TrikdisConfig. Na stronie www.trikdis.com wpisz w polu wyszukiwania: „TrikdisConfig".

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

TrikdisConfig Letöltés a trikdis.com oldalról.

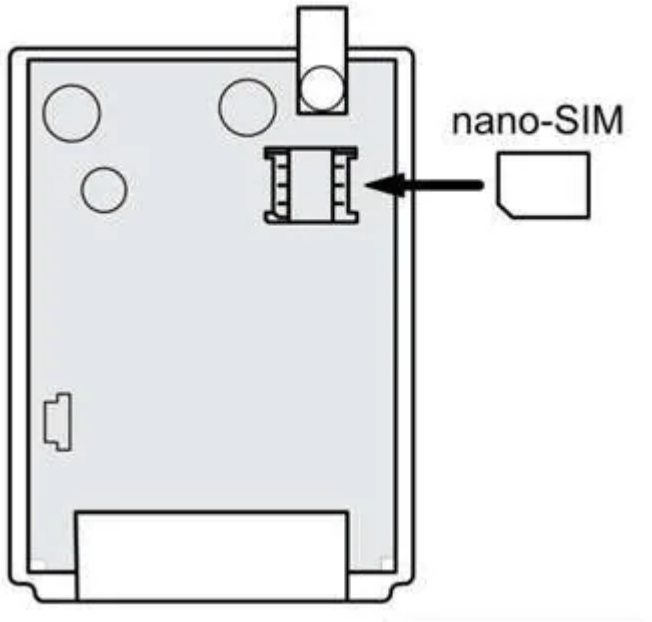
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Otwórz przednią pokrywę G16T. Włóż płaski śrubokręt w boczny otwór i delikatnie podważ pokrywę. Ilustracja poniżej pokazuje miejsce zatrzasku i otwory montażowe w tylnej części obudowy.



Rysunek 3. Zdejmowanie przedniej pokrywy (po lewej) i otwory montażowe tylnej części obudowy (po prawej).

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



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

4. Połącz G16T z komputerem kablem USB Mini-B. USB daje wystarczające zasilanie do programowania, osobny zasilacz nie jest potrzebny.



Rysunek 5. Połączenie z komputerem kablem USB Mini-B.

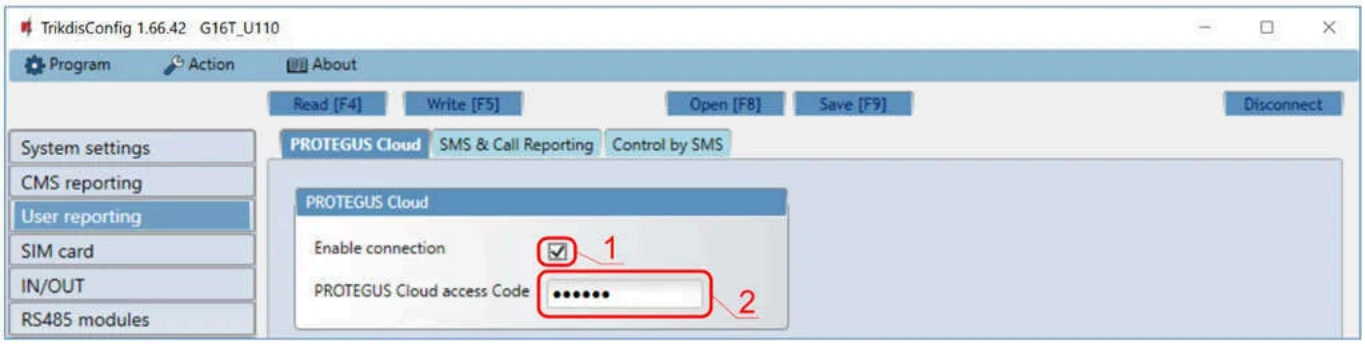
Ostrzeżenie

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

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

2.2 Połączenie z aplikacją Protegus 2

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



Rysunek 6. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

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

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



Rysunek 7. TrikdisConfig – strona SIM card.

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

APN (Access Point Name) to punkt dostępu operatora komórkowego do transmisji danych; bez niego urządzenie nie połączy się z internetem. Dokładną wartość otrzymasz od operatora karty SIM. Znane APN-y operatorów węgierskich i innych europejskich prowadzimy w osobnym artykule: Ustawienia APN – lista europejskich operatorów komórkowych. Jeśli nie masz od operatora innych danych, wypróbuj APN `internet`: jest ogólny i działa w sieciach wielu operatorów.

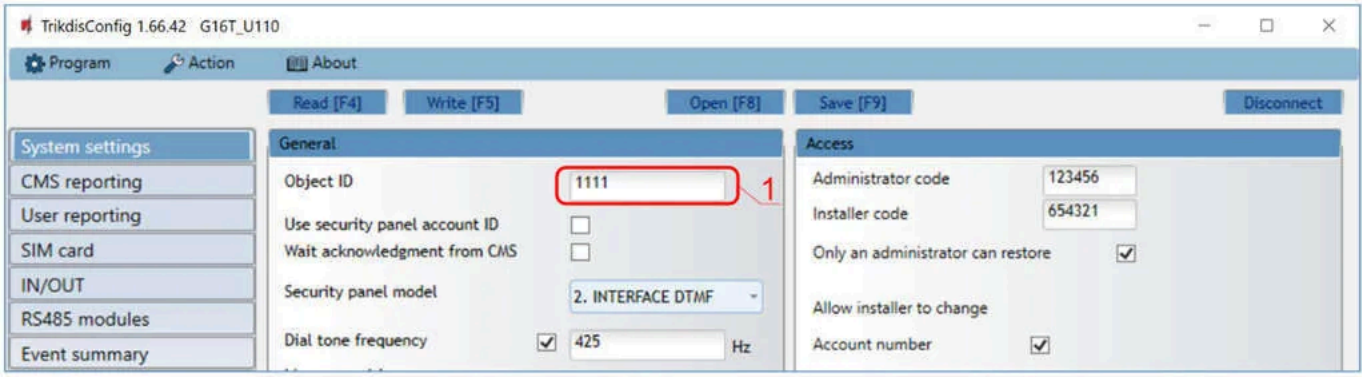
Do karty danych IoT / M2M (komunikacja między maszynami) operator zwykle podaje **inny APN niż do kart dla klientów indywidualnych** – z APN-em dla klientów indywidualnych urządzenie się nie połączy. Tę wartość także znajdziesz w artykule o APN albo poproś o nią operatora; jeśli operator podaje również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

Jeśli urządzenie nie wysyła zdarzeń do stacji monitorowania, konfiguracja jest na tym zakończona: naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB.

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

2.3 Połączenie ze stacją monitorowania

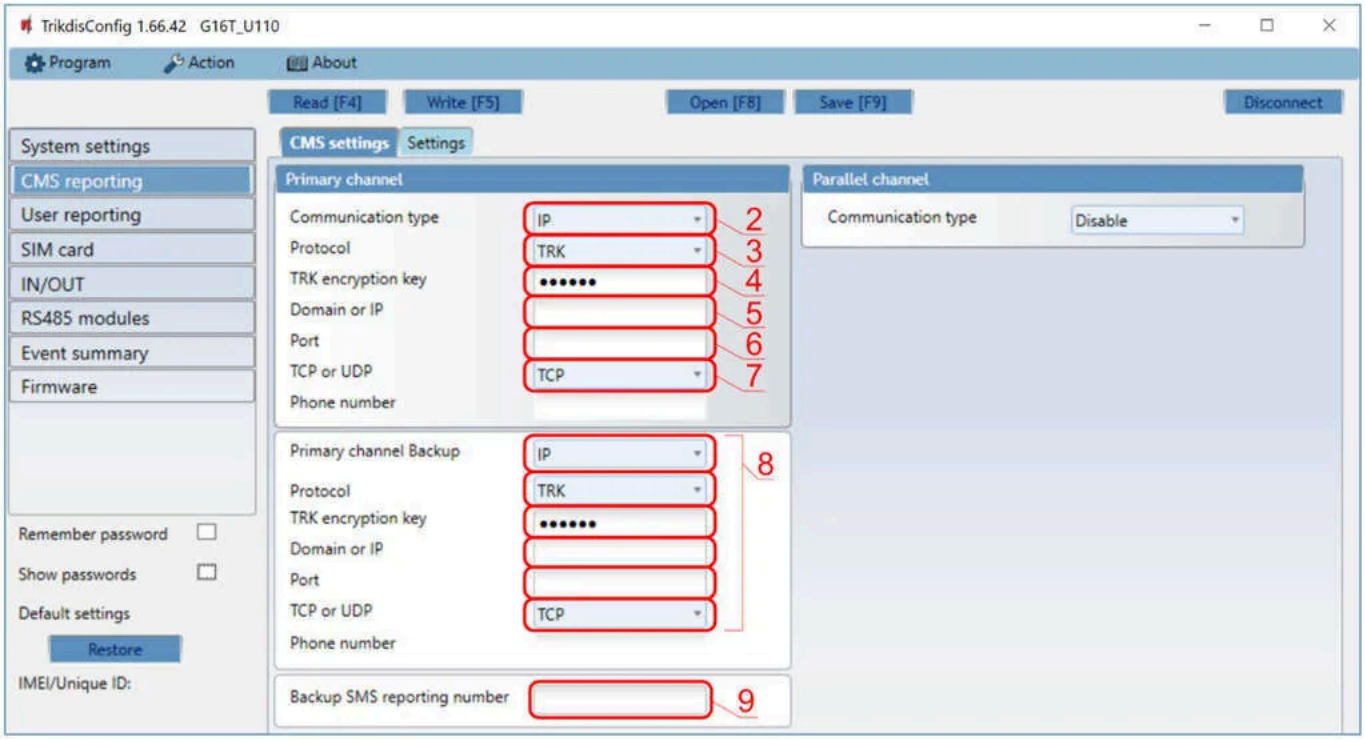
Jeśli urządzenie wysyła zdarzenia także do odbiornika stacji monitorowania, najpierw na stronie **System settings** wpisz identyfikator obiektu.



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`.

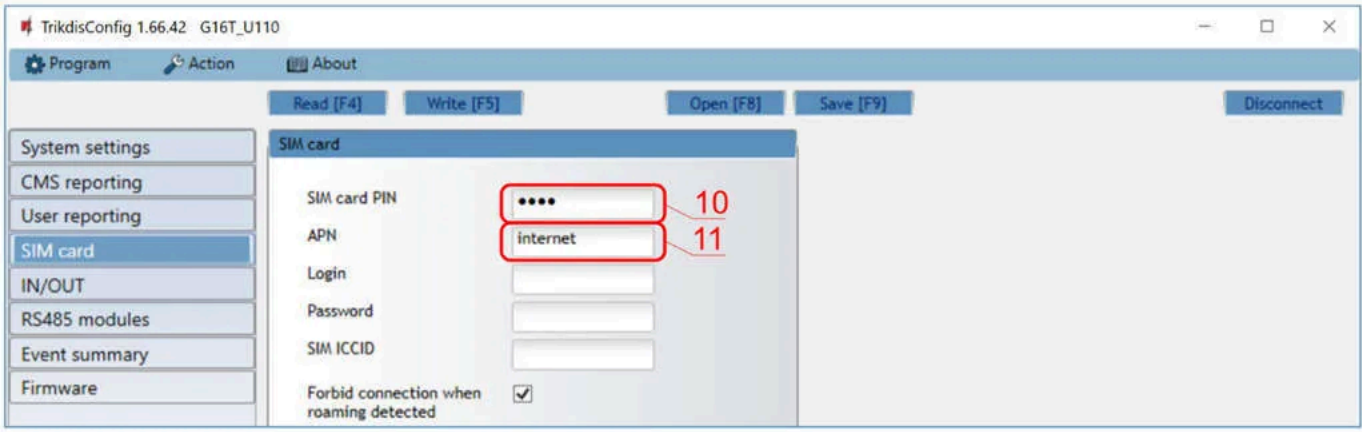
Następnie na stronie **CMS reporting**, w części **Primary channel** (kanał główny), ustaw dane odbiornika.



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

- 2 **Communication type** – wybierz połączenie **IP** (SMS nie jest zalecany jako kanał główny).
- 3 **Protocol** – **TRK** dla odbiornika Trikdis, **DC-09_2007** lub **DC-09_2012** dla odbiornika uniwersalnego, **TL150** dla odbiornika SUR-GARD.
- 4 **TRK encryption key** – 6-cyfrowy klucz szyfrowania ustawiony w odbiorniku.
- 5 **Domain or IP** – nazwa domeny lub adres IP odbiornika.
- 6 **Port** – numer portu odbiornika.
- 7 **TCP or UDP** – protokół transmisji; zgodny z ustawieniem odbiornika.
- 8 **Primary channel Backup** – kanał zapasowy na wypadek awarii kanału głównego; wypełnij go tak samo, zalecamy go ustawić.
- 9 **Backup SMS reporting number** – jeśli jest odbiornik SMS Trikdis, wpisz tu jego numer telefonu: urządzenie od razu po pierwszym uruchomieniu wyśle na niego SMS, a potem raportuje SMS-em wtedy, gdy nie działa żaden kanał IP.

Na koniec na stronie **SIM card** wpisz dane karty, jeśli nie zrobiłeś tego jeszcze w punkcie 2.2.



Rysunek 10. TrikdisConfig – strona SIM card.

- 10 **SIM card PIN** – kod PIN karty.
- 11 **APN** – punkt dostępu operatora (patrz punkt 2.2).

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

Po zakończeniu konfiguracji naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB. Urządzenie jest gotowe do podłączenia. Także w tym przypadku trzeba włączyć i skonfigurować dialer linii telefonicznej centrali alarmowej, w przeciwnym razie centrala nie wyśle zdarzeń (rozdział 4).

3. Instalacja i podłączenie

Figyelem!

Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

3.1 Kroki instalacji

1. Zdejmij przednią pokrywę (patrz punkt 2.1) i odłącz listwę zaciskową.
2. Włóż kartę nano-SIM, jeśli nie zrobiłeś tego podczas uruchamiania.
3. Wyjmij płytkę drukowaną z tylnej części obudowy: otwórz zatrzask w rogu (patrz ilustracja w punkcie 2.1).
4. Przykręć tylną część obudowy 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 przednią pokrywę.

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

3.2 Umiejscowienie i antena

- Komunikator umieść w **suchym miejscu wewnątrz budynku**, najlepiej blisko obudowy centrali alarmowej, aby okablowanie było krótkie.
- **W metalowej obudowie** sygnał komórkowy jest silnie tłumiony. Jeśli komunikator trafia do metalowej obudowy centrali, wyprowadź antenę na zewnątrz obudowy albo użyj anteny z dłuższym kablem.
- Przed ostatecznym zamocowaniem **sprawdź poziom sygnału**: liczba żółtych mignięć diody NETWORK powinna wynosić w 2G co najmniej 5, w 4G co najmniej 3 (patrz punkt 1.6). 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 od przewodów sieci elektrycznej.

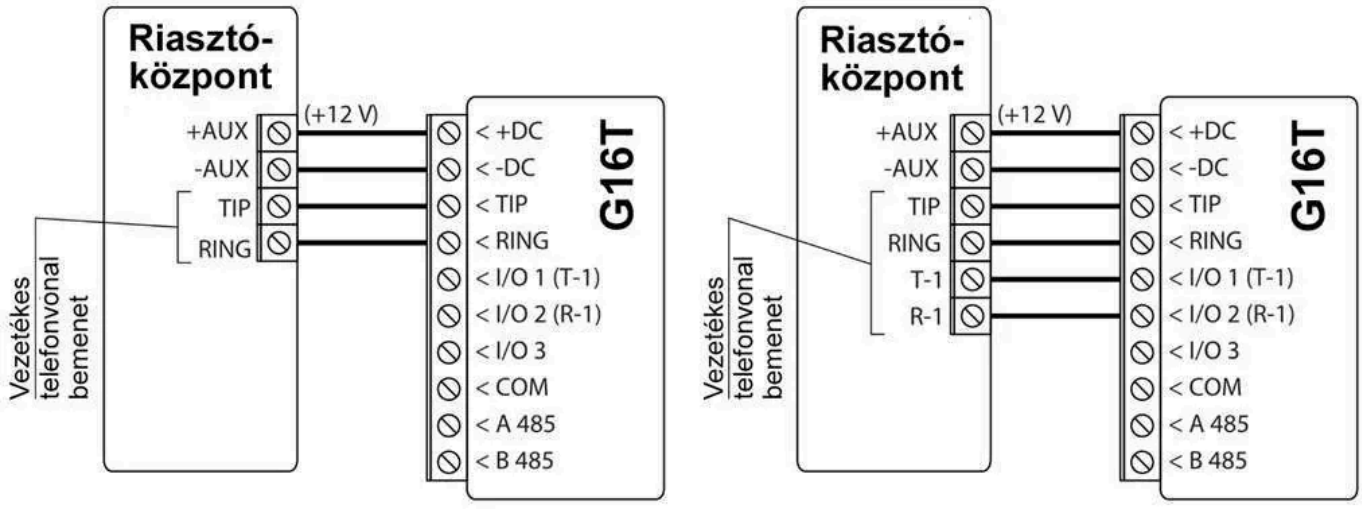


A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna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

3.3 Podłączenie do centrali alarmowej

G16T podłącza się do wyjścia linii telefonicznej centrali (TIP/RING), a zasilanie dostaje z 12-woltowego wyjścia zasilania pomocniczego centrali (AUX).

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



Rysunek 11. Podłączenie do wyjścia linii telefonicznej centrali: po lewej podłączenie standardowe, po prawej podłączenie z nadzorem linii.

G16T podczas wysyłania może pobierać do 500 mA. Sprawdź, czy wyjście AUX centrali to wytrzyma razem z innymi podłączonymi urządzeniami. Ponieważ zasilanie daje centrala, przy zaniku zasilania sieciowego akumulator centrali zasila także komunikator.

3.3.1 W uzasadnionych przypadkach: nadzór linii

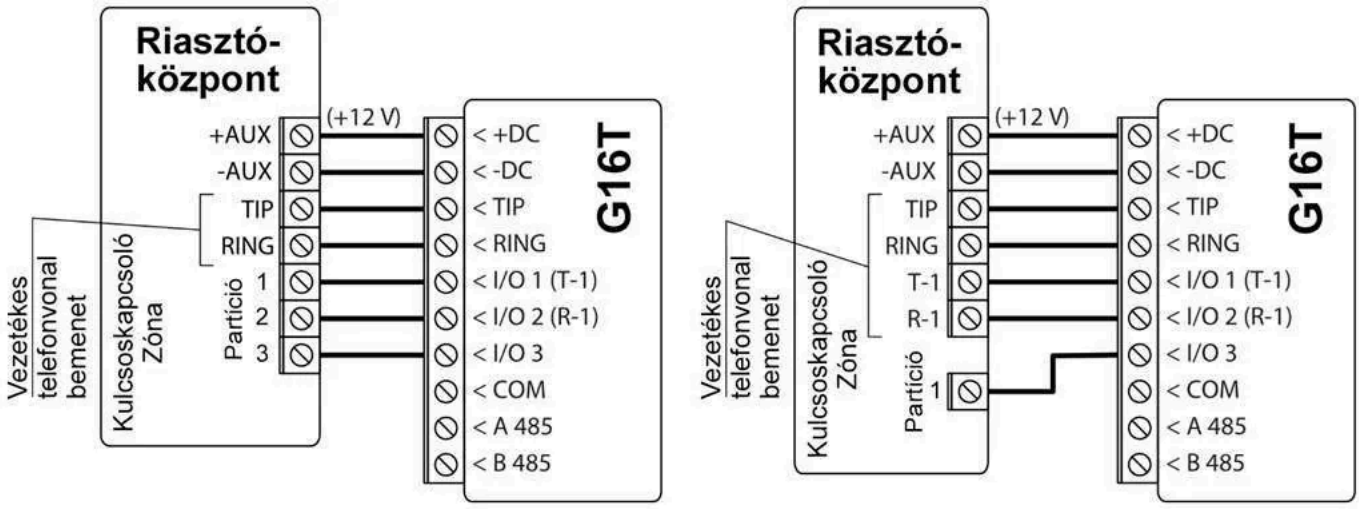
Potrzebny tylko wtedy, gdy wymagany jest nadzór linii: komunikator sygnalizuje wtedy przerwanie połączenia między nim a centralą alarmową.

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

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

3.4 Podłączenie strefy typu klucz

Jeśli chcesz uzbrajać i rozbrajać centralę zdalnie, z aplikacji Protegus 2, ustaw jeden z zacisków I/O komunikatora jako **wyjście** i podłącz go do **strefy typu klucz** centrali. Po aktywacji wyjście zwiera strefę do COM (minusa); rezystor parametryczny strefy podłącz zgodnie z typem strefy w centrali. Ponieważ G16T ma trzy zaciski I/O, można obsługiwać nawet trzy partycje, każdą osobnym wyjściem. Zacisk użyty do strefy typu klucz ustaw na stronie **IN/OUT** w TrikdisConfig na funkcję **OUT** (punkt 6.6). Sprzęt w wersji 3 ma jedno programowalne wyjście (OUT), które może sterować jedną partycją; tam pole **Output OUT1 mode** na stronie **System settings** musi mieć wartość **Remote control** (to ustawienie fabryczne).



Rysunek 12. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego: po lewej podłączenie standardowe, po prawej podłączenie z nadzorem linii (wtedy do przełącznika kluczowego pozostaje I/O 3).

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

3.5 Podłączenie wejść

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

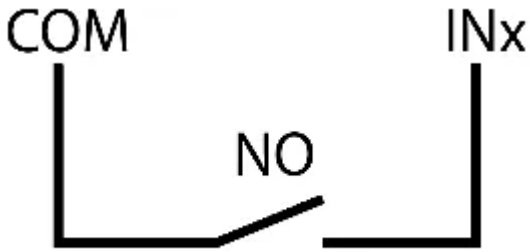
Wejścia obsługują następujące typy obwodów: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Rezystor końca linii ma wartość **2,2 kΩ**. Przy pojedynczej parametryzacji (EOL) zarówno zwarcie, jak i przerwa są traktowane jako alarm; podwójna parametryzacja (DEOL) z dwoma rezystorami rozróżnia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

(zwarcie lub przerwa). Ustawienie fabryczne to NO (normalnie otwarte); typ wejścia ustawiasz na stronie **IN/OUT** programu TrikdisConfig, zgodnie z podłączeniem.

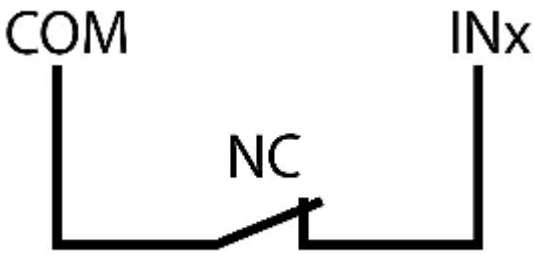
Typ	Stan spoczynkowy	Alarm	Sabotaż
NC	zamknięty	otwarty	–
NO	otwarty	zamknięty	–
NC/EOL	2,2 kΩ	przerwa lub zwarcie	–
NO/EOL	2,2 kΩ	zwarcie lub przerwa	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	przerwa lub zwarcie
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	przerwa lub zwarcie

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

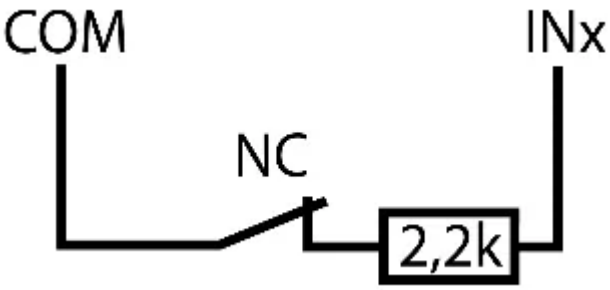
Podłączenie obwodów wejściowych: typy NC, NO, EOL i DEOL z rezystorem parametrycznym 2,2 kΩ, a przy typach DEOL z obwodem sabotażowym.



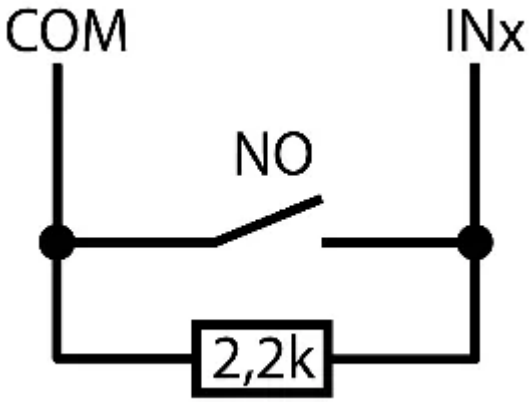
Rysunek 13. NO – obwód normalnie otwarty: zamknięty – alarm, otwarty – stan spoczynku.



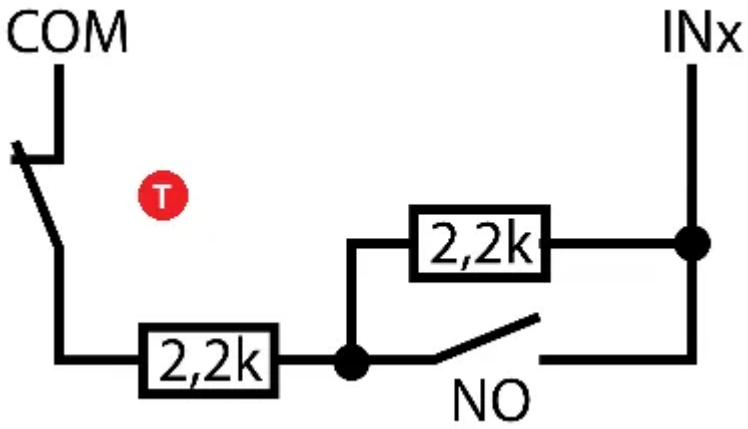
Rysunek 14. NC – obwód normalnie zamknięty: otwarty – alarm, zamknięty – stan spoczynku.



Rysunek 15. NC/EOL – obwód normalnie zamknięty z rezystorem parametrycznym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynku.

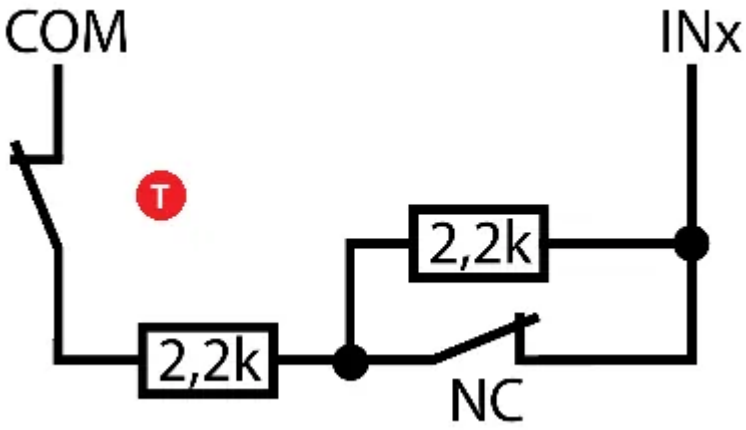


Rysunek 16. NO/EOL – obwód normalnie otwarty z rezystorem parametrycznym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynku.



Rysunek 17. NO/DEOL – obwód normalnie otwarty z rezystorem parametrycznym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – alarm, 3,3–5,5 kΩ – stan spoczynku.

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

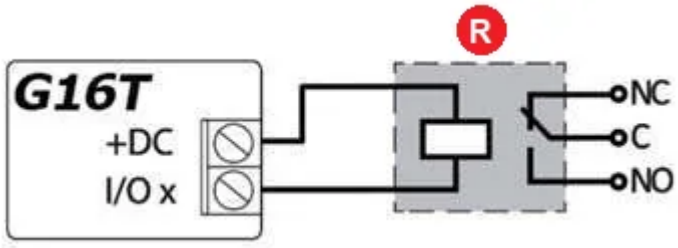


Rysunek 18. NC/DEOL – obwód normalnie zamknięty z rezystorem parametrycznym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – stan spoczynku, 3,3–5,5 kΩ – alarm.

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

3.6 Podłączenie wyjścia z przekaźnikiem

Zaciski I/O jako wyjścia są wyjściami typu otwarty kolektor (OC): w stanie aktywnym zwierają podłączone obciążenie do minusa, maksymalnie 0,15 A, do 30 V DC. Większy odbiornik lub urządzenie zasilane napięciem sieciowym przełączaj **przez przekaźnik**: jeden koniec cewki przekaźnika podłącz do +DC, a drugi do zacisku I/O.



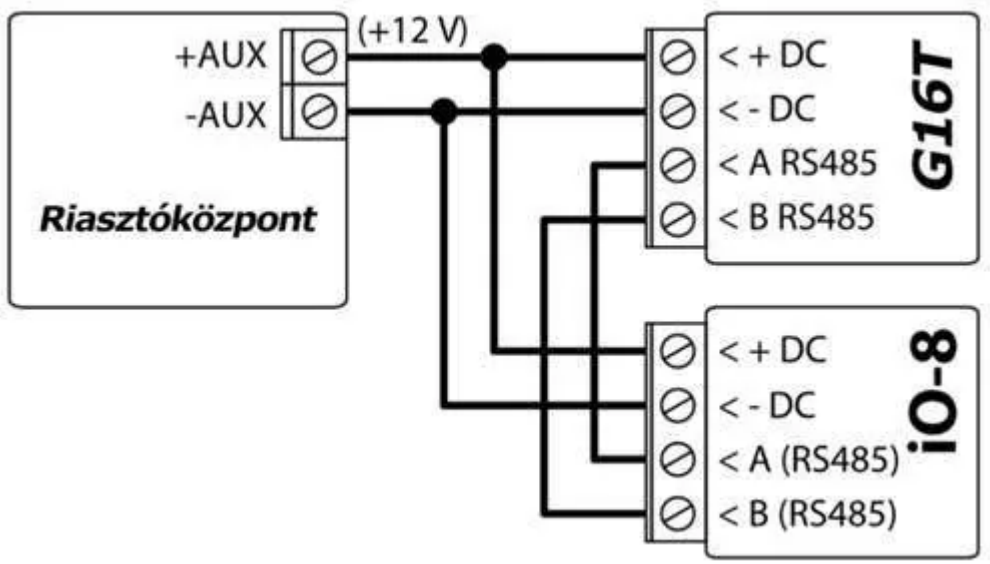
Rysunek 19. Podłączenie przekaźnika do wyjścia komunikatora: cewka między zaciskiem +DC a zaciskiem I/O x, styki (NC, C, NO) przełączają odbiornik.

- R przekaźnik („Relay")

Wyjściami sterujesz 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. Do tej samej magistrali można podłączyć także pozostałe przewodowe lub bezprzewodowe ekspandery serii iO firmy Trikdis, na przykład gdy chcesz podłączyć czujnik temperatury: ekspander **iO** ma 1 wejście, 1 wyjście przekaźnikowe i magistralę 1-Wire do czujników temperatury (konfiguracja w punkcie 6.7). Zaciski A 485 i B 485 połącz z zaciskami A i B modułu, a zasilanie modułu weź z 12 V centrali. Moduł trzeba dodać na stronie **RS485 modules** w TrikdisConfig (punkt 6.7).



Rysunek 20. Podłączenie ekspandera iO-8 do magistrali RS485 komunikatora G16T; zasilanie z wyjścia AUX centrali alarmowej.

G16T z modemem 2G (G16T_G410) nie ma magistrali RS485, dlatego nie można do niego podłączyć ekspandera iO-8 ani modułów W485 i E485.

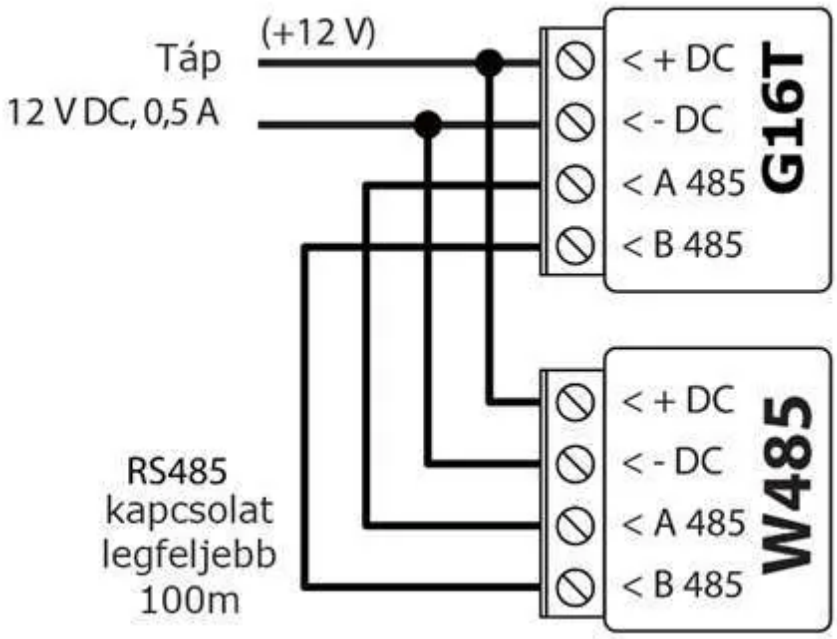
3.8 Podłączenie modułów W485 i E485

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.

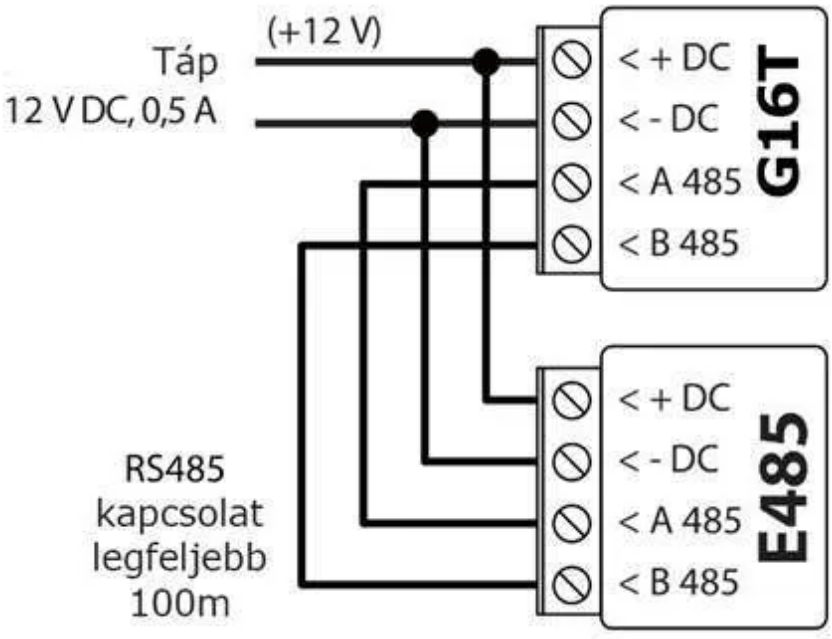
- **Podłączenie:** przez magistralę RS485, ze wspólnego zasilania z komunikatorem (wejście zasilania modułu 9–28 V DC); osobny zasilacz nie jest potrzebny.
- **Internet jest kanałem głównym:** dopóki działa, wszystko idzie przez niego. Jeśli połączenie zostanie przerwane, komunikator sam przełącza się 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 połączenie WiFi lub Ethernet działa, G16T komunikuje się przez nie (komunikaty do stacji monitorowania i do Protegus idą przez router WiFi lub przez internet przewodowy, komórkowa transmisja danych nie jest wtedy używana); jeśli połączenie zostanie przerwane, przełącza się na komórkową transmisję danych, a po przywróceniu połączenia wraca na moduł. Do działania modułu **w G16T musi być karta SIM**.



Rysunek 21. Podłączenie modułu WiFi W485 do G16T przez magistralę RS485. Oba urządzenia pracują ze wspólnego zasilacza 12 V DC (co najmniej 0,5 A) (wejście zasilania modułu 9–28 V DC); kabel RS485 może mieć długość do 100 m.



Rysunek 22. Podłączenie modułu Ethernet E485 do G16T przez magistralę RS485. Oba urządzenia pracują ze wspólnego zasilacza 12 V DC (co najmniej 0,5 A) (wejście zasilania modułu 9–28 V DC); kabel RS485 może mieć długość do 100 m.

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 wprowadzasz na stronie **RS485 modules** w 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 przedniej pokrywie powinieneś zobaczyć:

- **POWER** świeci na zielono – zasilanie prawidłowe;
- **NETWORK** świeci na zielono i miga na żółto – połączony z siecią; liczba mignięć to poziom sygnału (dobry w 2G: 5, w 4G: 3); jeśli naliczysz mniej, sygnał jest słaby: poszukaj innego miejsca dla komunikatora albo użyj czulszej anteny (punkt 3.2);
- **TROUBLE** nie świeci.

Jeśli TROUBLE miga, liczba mignięć wskazuje przyczynę (punkt 1.6); każda inna odbiegająca sygnalizacja LED także oznacza jakąś usterkę – jej przyczynę znajdziesz w tabelach punktu 1.6. Jeśli nie świeci żadna dioda, sprawdź zasilanie i okablowanie.

4. Programowanie centrali alarmowej

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

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

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

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

4.1 Programowanie dialera Honeywell Vista

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

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

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

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

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

4.2 Centrale innych producentów

W instrukcji instalatora każdej centrali szukaj tych samych czterech ustawień: włączenie komunikatora linii telefonicznej, numer telefonu odbiornika, tryb wybierania (DTMF) i format komunikacji (Contact ID). Jeśli centrala przed wybieraniem numeru czeka na sygnał zgłoszenia (dial tone), daje go G16T; jeśli połączenie mimo to się nie rozpoczyna, wyłącz w centrali wykrywanie sygnału zgłoszenia (opcja „wybieranie bez sygnału zgłoszenia" lub podobna).

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

5. Zdalne sterowanie aplikacją Protegus 2

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

5.1 Dodanie urządzenia

Przed dodaniem urządzenia sprawdź:

1. Karta SIM jest aktywna i działa na niej komórkowa transmisja danych; jej kod PIN jest wpisany w urządzeniu albo żądanie PIN-u jest wyłączone.
2. Na zakładce **User reporting** → **PROTEGUS Cloud** w TrikdisConfig zaznaczone jest **Enable connection**, a **Protegus Cloud access code** jest ustawiony (po utworzeniu systemu nie można go już zmienić).
3. Dioda **POWER** świeci na zielono, dioda **NETWORK** świeci na zielono i miga na żółto.

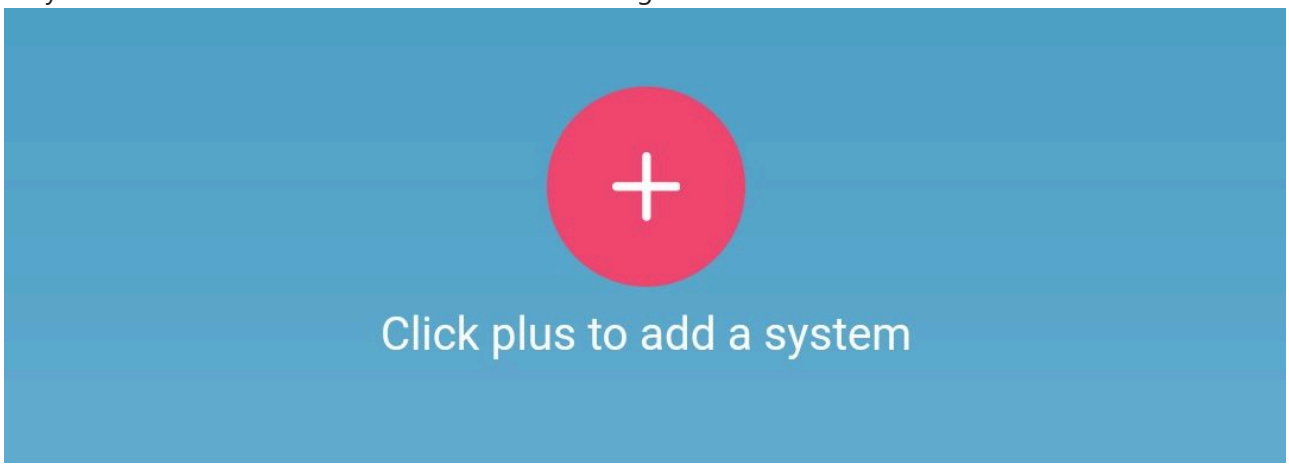
Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie 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



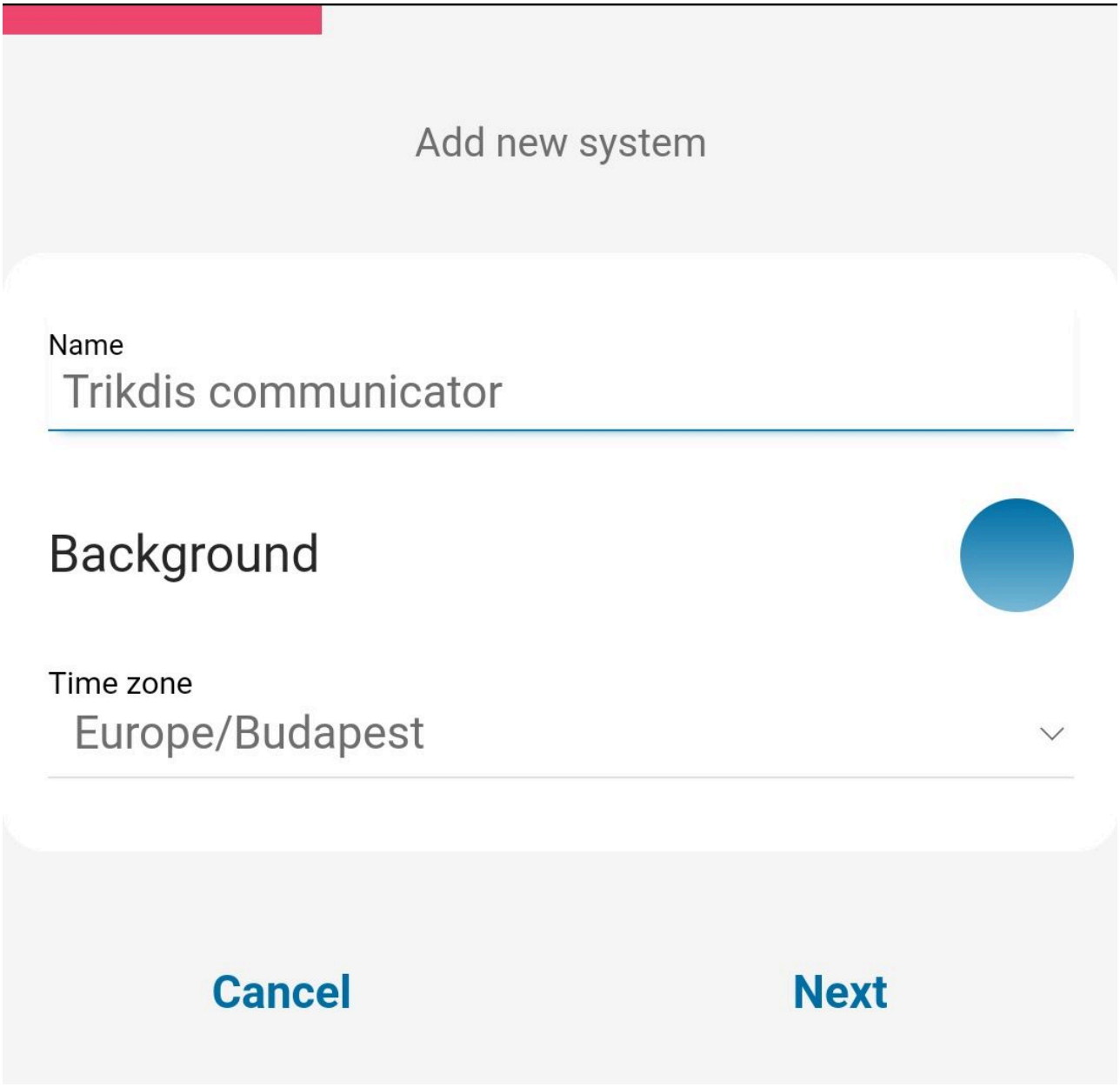
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



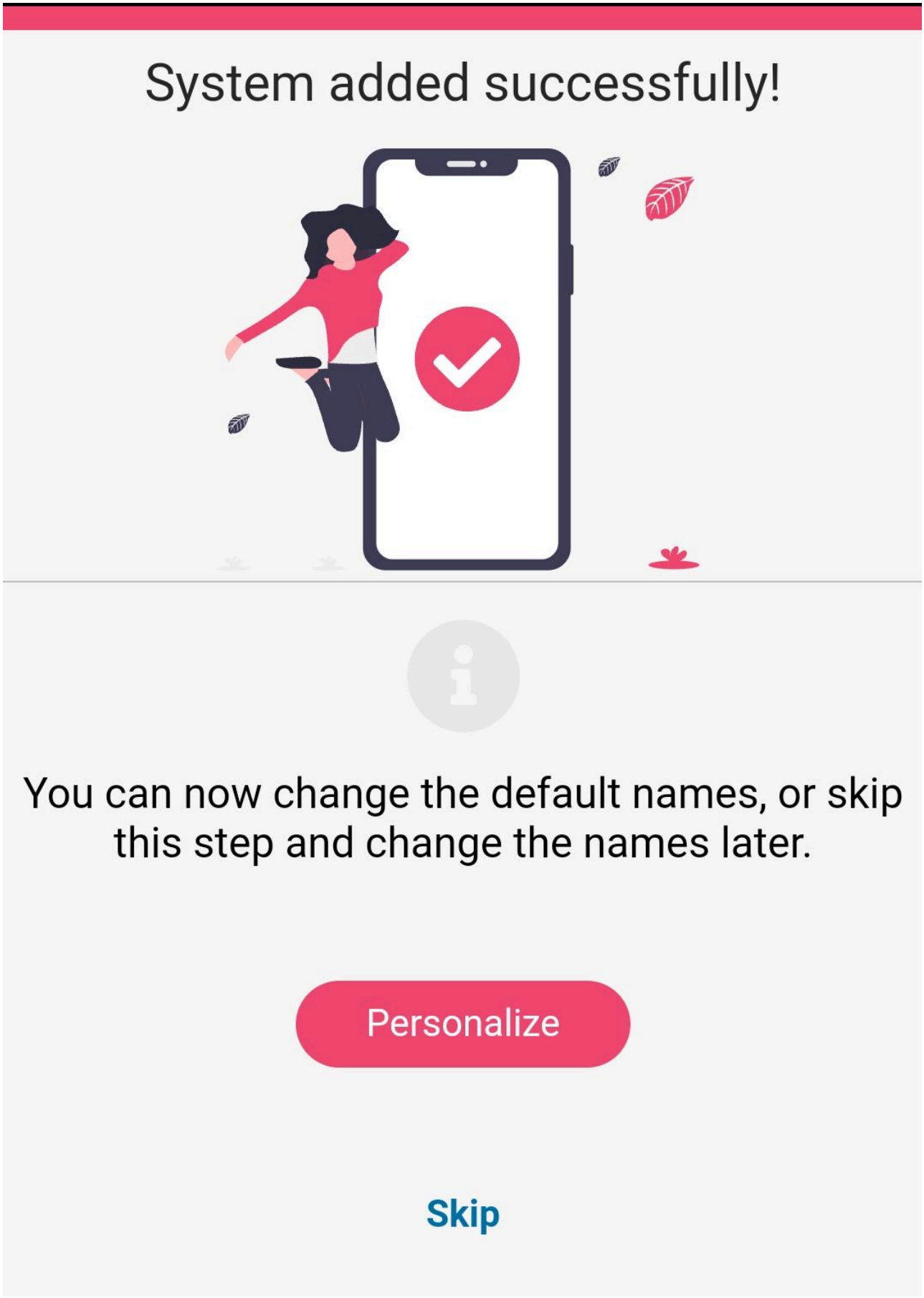
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



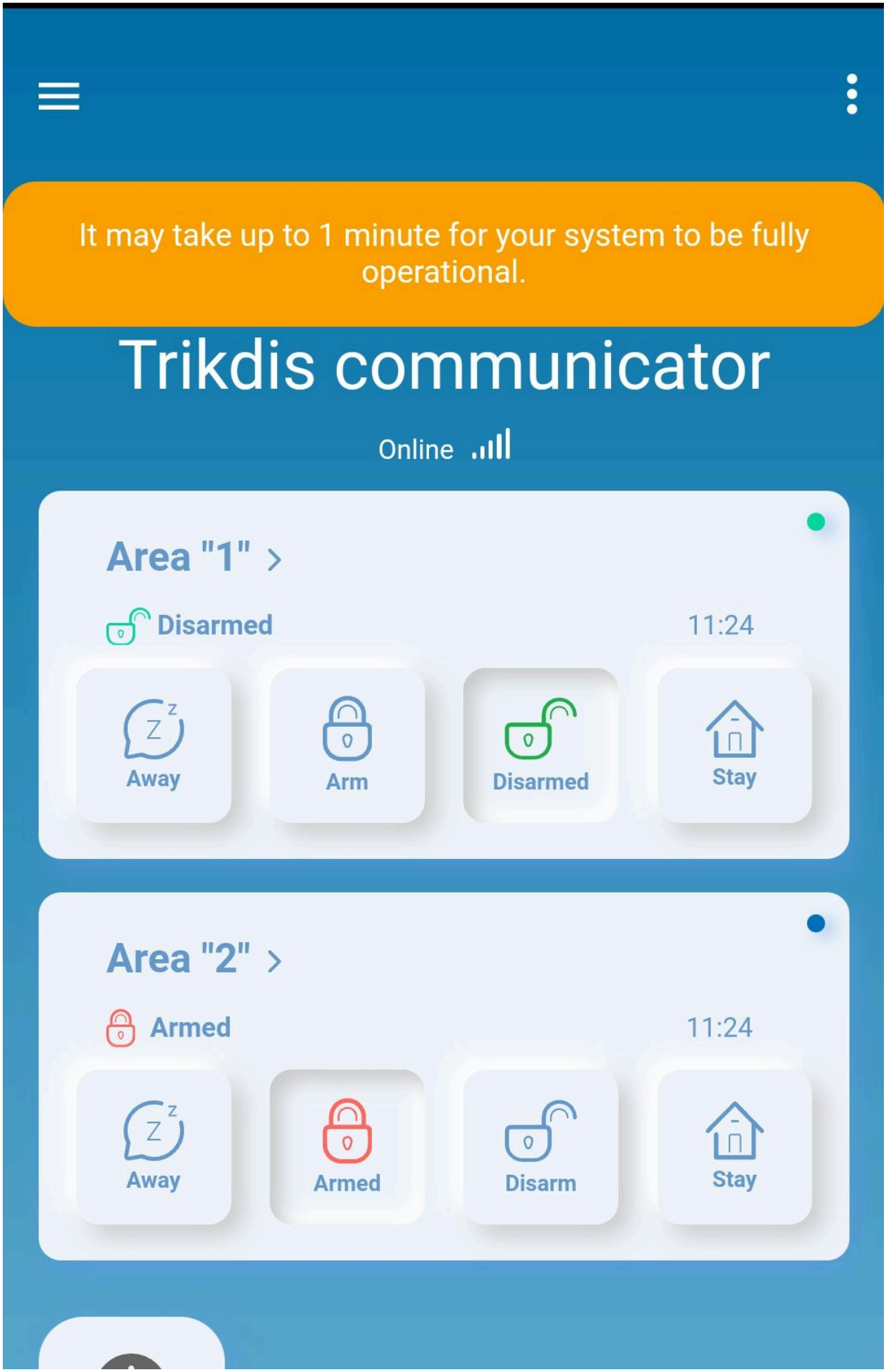
6. Add meg a rendszer nevét és válassz idozónát



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**) jest podany na pudełku i na tylnej części obudowy urządzenia, pokazuje go też pasek stanu TrikdisConfig.

5.2 Uzbrajanie i rozbrajanie wyjściem

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

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

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

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

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

5.3 Uzbrajanie i rozbrajanie z aplikacji

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

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

5.4 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.

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`
`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`

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.

W G16T polecenie `CONNECT` ma jeszcze jeden parametr: `CP=1` wyłącza, a `CP=2` włącza interfejs linii telefonicznej komunikatora. Przykład: `123456 CONNECT CP=2`.

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 po kolei, strona po stronie, ustawienia G16T.

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.

Etykieta	Znaczenie
Device	Typ urządzenia (oznaczenie modelu). Sprawdź, czy widnieje tu typ twojego urządzenia.
SN	Numer seryjny.
BL	Wersja bootloadera.
FW	Wersja firmware.
HW	Wersja sprzętu.
State	Sposób połączenia: USB lub zdalne (remote).
Administrator / Installer	Poziom dostępu osoby programującej (po wprowadzeniu hasła).

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

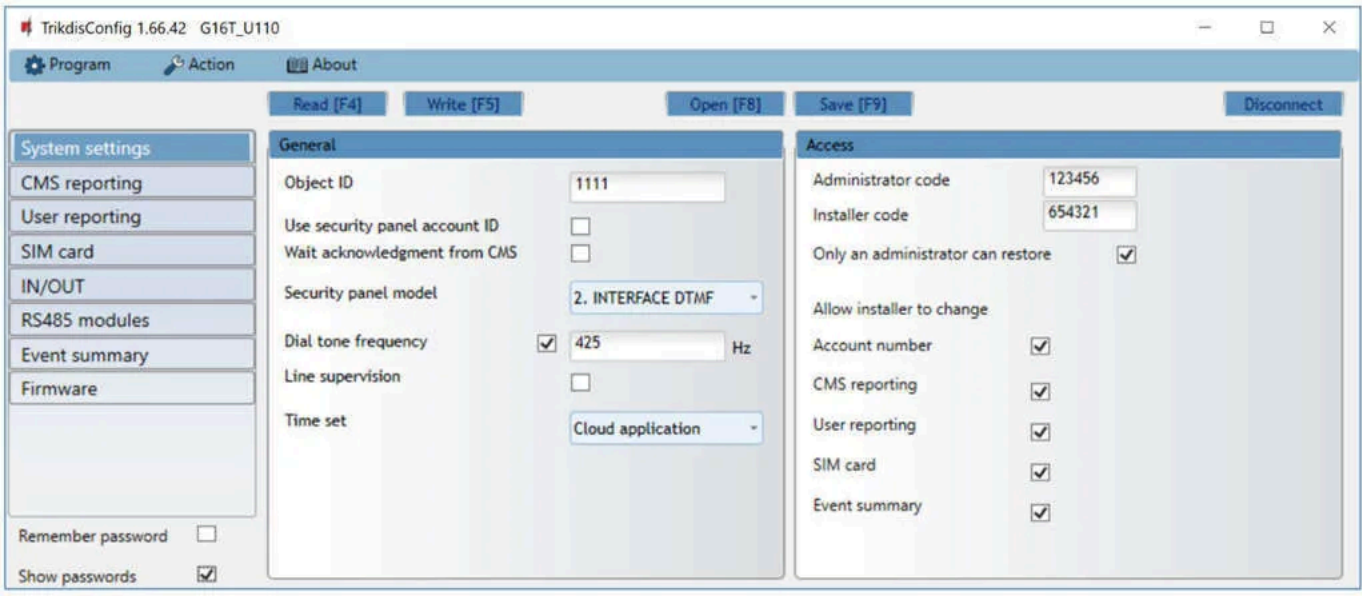


Rysunek 23. Pasek stanu TrikdisConfig z odczytanym G16T: identyfikator, stan, typ, numer seryjny, wersje, sposób połączenia i poziom dostępu.

Po **Read [F4]** program odczytuje i pokazuje wartości ustawione w urządzeniu; potrzebne ustawienia wprowadź zgodnie z poniższymi opisami stron.

6.2 System settings

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



Rysunek 24. TrikdisConfig – strona System settings: grupy General i Access.

- **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (4 znaki szesnastkowe: 0–9, A–F; nie można użyć `FFFE` ani `FFFF`). Obowiązkowy, jeśli urządzenie wysyła zdarzenia także do stacji monitorowania.
- **Use security panel account ID** – po zaznaczeniu komunikator używa nie własnego Object ID, lecz identyfikatora wysłanego przez centralę w komunikacie Contact ID. Przydatne, gdy kilka partycji raportuje z osobnymi identyfikatorami.
- **Wait acknowledgment from CMS** – po zaznaczeniu komunikator po każdym zdarzeniu czeka na potwierdzenie z odbiornika i dopiero potem wysyła do centrali sygnał zakończenia (kiss-off). Jeśli potwierdzenia nie ma, centrala wysyła zdarzenie ponownie. W systemie bez stacji monitorowania, tylko z Protegus 2, pozostaw tę opcję wyłączoną (stan fabryczny).
- **Security panel model** – typ interfejsu linii telefonicznej (tym ustawieniem włączasz lub wyłączasz interfejs DTMF linii telefonicznej komunikatora); domyślnie **2. INTERFACE DTMF**.
- **Dial tone frequency** – częstotliwość sygnału zgłoszenia, który G16T podaje do centrali (domyślnie 425 Hz – taki sygnał zgłoszenia stosuje się w Polsce i w większości krajów europejskich).
- **Line supervision** – nadzór przewodów między centralą a komunikatorem; wymaga także podłączenia przewodów T-1 i R-1 (punkt 3.3.1).
- Typ wejść i rolę wyjść w sprzęcie w wersji 4 ustawiasz na stronie **IN/OUT** (punkt 6.6). W sprzęcie w wersji 3 te dwa pola są tutaj: **Input IN1-IN2 type** – typ wejścia z listy (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL); **Output OUT1 mode** – tryb pracy wyjścia z listy.
- **Time set** – źródło czasu zegara urządzenia (domyślnie **Cloud application**, chmura Protegus).

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

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

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

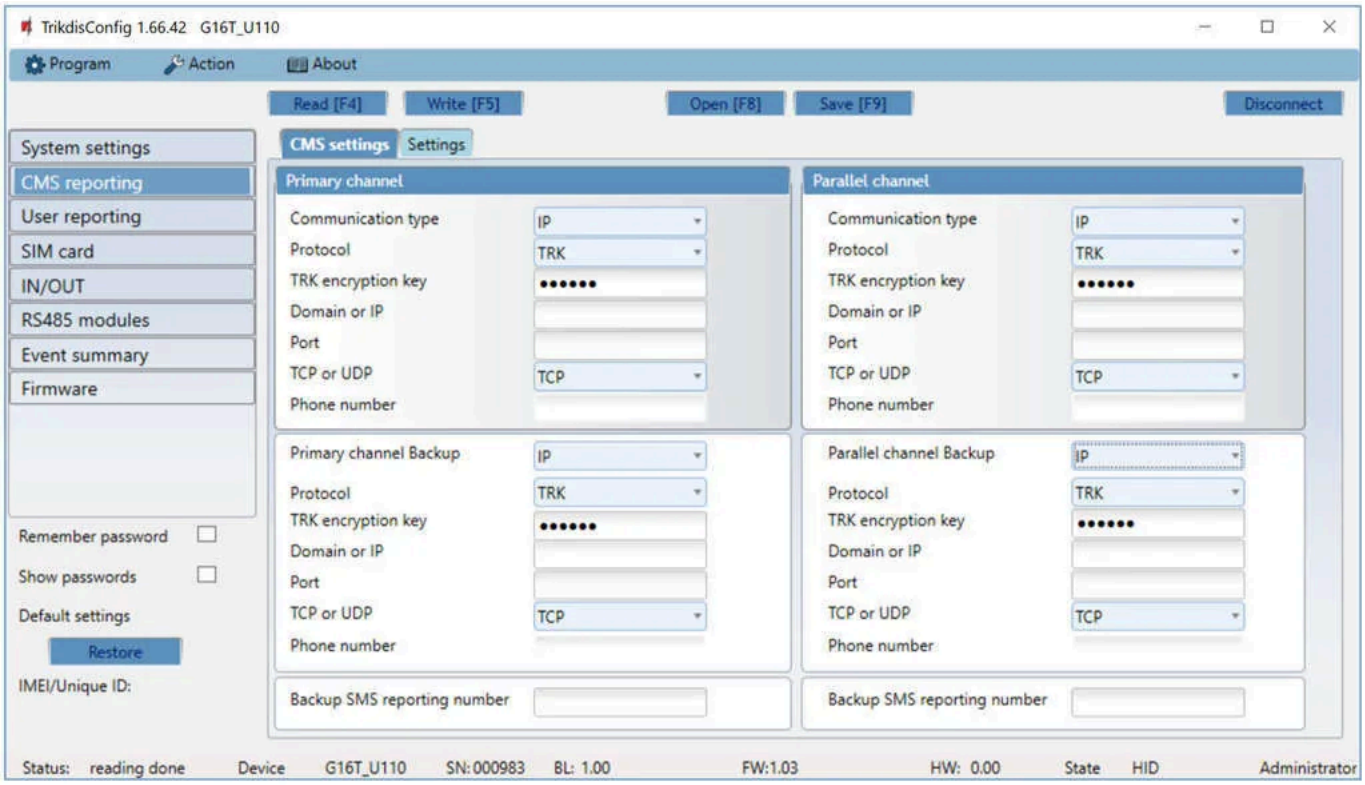
Nie zostawiaj w urządzeniu haseł fabrycznych!

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

6.3 CMS reporting

Komunikator wysyła zdarzenia do stacji monitorowania przez komórkową transmisję danych (IP) lub SMS-em. Zdarzenia mogą iść kilkoma kanałami: kanał **główny** i **równoległy** działają jednocześnie (do dwóch odbiorników naraz), a każdy z nich ma kanał **zapasowy**, który wchodzi do działania, gdy dany kanał zostanie przerwany. Komunikacja jest szyfrowana i chroniona hasłem; do odbioru i przekazywania zdarzeń do oprogramowania stacji monitorowania potrzebny jest odbiornik Trikdis (programowy odbiornik IPcom – Windows lub Linux –, RL14, RM14; do odbioru SMS odbiornik IP/SMS RL14, odbiornik wielokanałowy RM14

lub odbiornik SMS GM14) albo odbiornik uniwersalny obsługujący protokół DC-09 / TL150. SMS jest szczególnie przydatny jako kanał zapasowy, bo działa bez internetu mobilnego; jako kanału głównego go nie zalecamy.



Rysunek 25. TrikdisConfig – CMS reporting, zakładka CMS settings: kanał główny, zapasowy i równoległy.

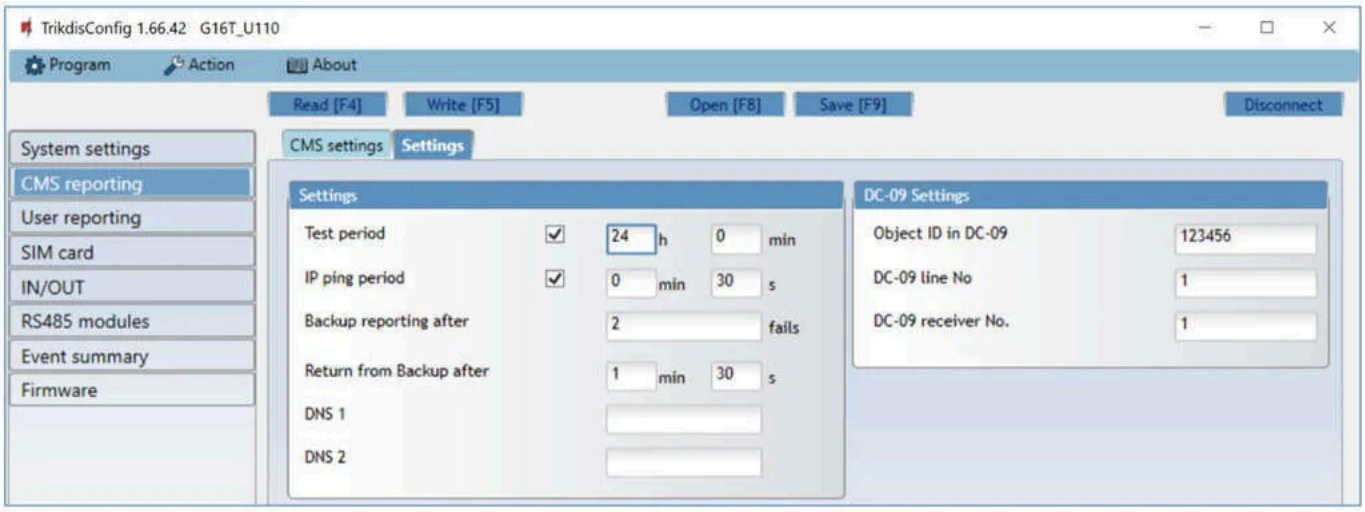
Primary channel – kanał główny

- **Communication type** – IP lub SMS.
- **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. `48xxxxxxxxx` dla polskiego numeru).

Primary channel Backup – kanał zapasowy. Przejmuje komunikację, gdy 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 do centralnej stacji monitorowania). Ma własny kanał zapasowy.

Backup SMS reporting number – zapasowy numer SMS. Wchodzi do działania, gdy wysłanie nie powiedzie się ani kanałem głównym, ani równoległym, ani zapasowym; jest przydatny, bo działa bez połączenia IP. Jest aktywny tylko wtedy, gdy kanał główny i zapasowy pracują w trybie IP. Urządzenie wysyła SMS do odbiornika SMS stacji monitorowania po pierwszym uruchomieniu oraz wtedy, gdy połączenie TCP/IP lub UDP/IP zostanie przerwane zarówno w kanale głównym, jak i w jego kanale zapasowym. Numer telefonu odbiornika SMS Trikdis wpisz z kodem kraju (np. `48xxxxxxxxx` dla polskiego numeru).



Rysunek 26. TrikdisConfig – CMS reporting, zakładka Settings: raport testowy, PING, czasy kanału zapasowego, DNS i dane DC-09.

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

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

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

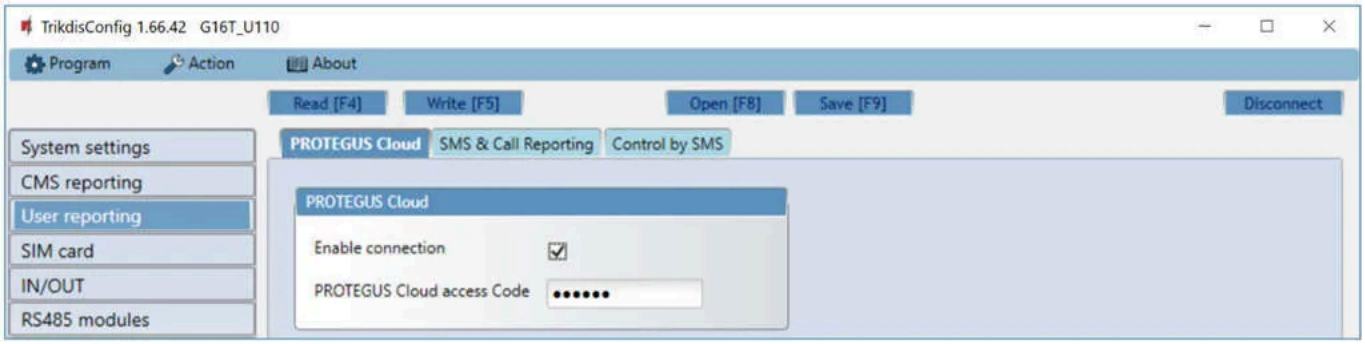
DC-09 Settings (po prawej stronie karty) – wypełniasz tylko wtedy, gdy na którymś kanale wysyłasz protokołem DC-09_2007 lub DC-09_2012; grupa pojawia się, gdy w polu **Protocol** któregoś kanału wybrano DC-09_2007 lub DC-09_2012:

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

Na dole zakładki: **DNS 1, DNS 2** – serwery nazw (DNS, Domain Name System: podaje adres IP odpowiadający nazwie domeny); są potrzebne, jeśli odbiornik podałeś nazwą domeny, a nie adresem IP. Domyślnie publiczny DNS Google.

6.4 User reporting

Na zakładce **PROTEGUS Cloud** włączasz usługę Protegus. Dzięki usłudze Protegus użytkownik może zdalnie monitorować komunikator i podłączony do niego system oraz nimi sterować; szczegóły: www.protegus.app.

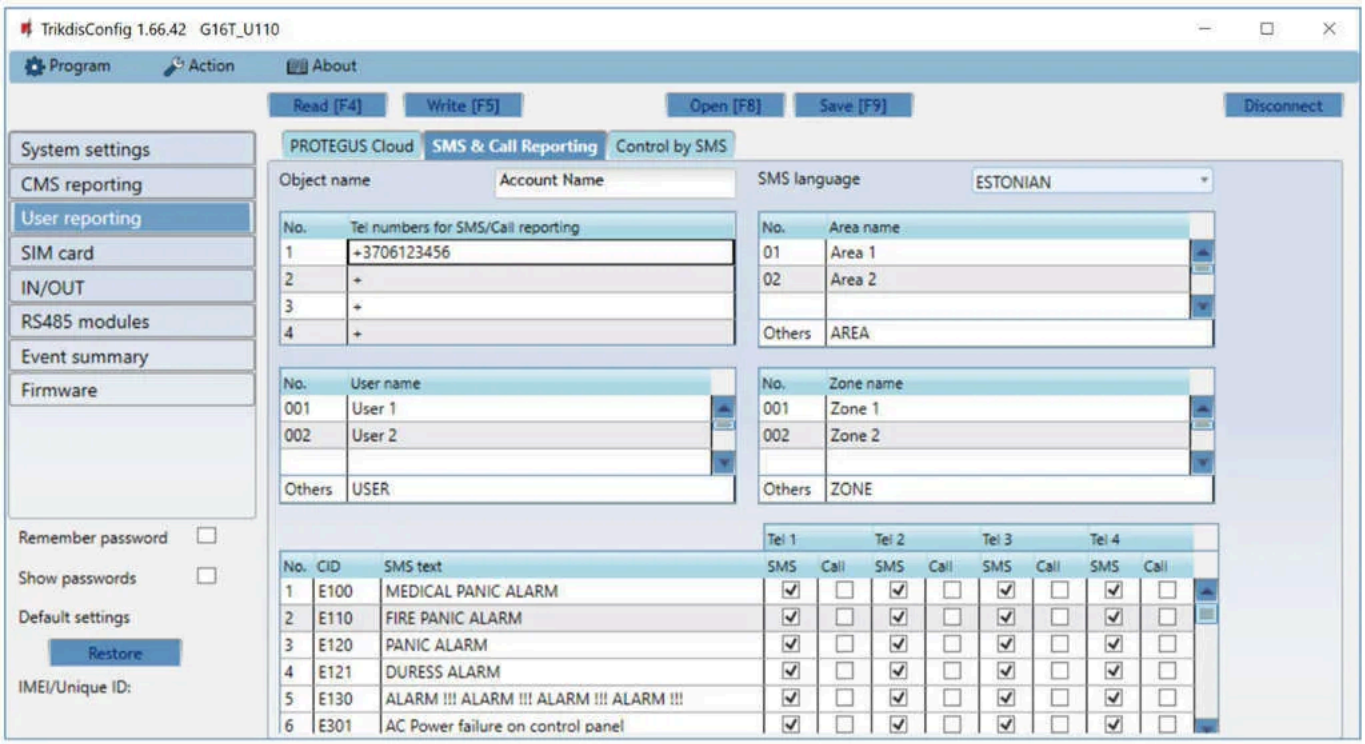


Rysunek 27. TrikdisConfig – User reporting, zakładka PROTEGUS Cloud.

- **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.

Na 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.

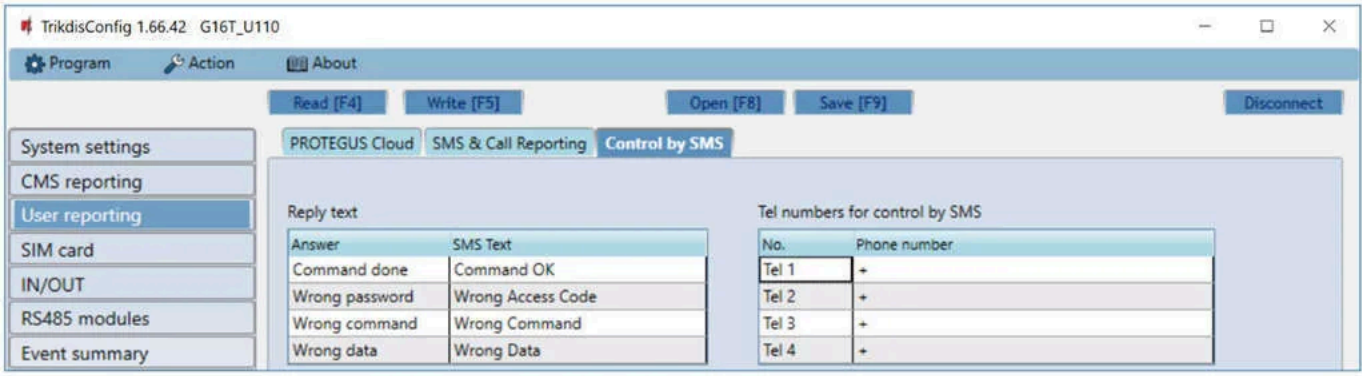


Rysunek 28. TrikdisConfig – User reporting, zakładka SMS & Call Reporting.

- **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 telefonu z kodem kraju (np. dla polskiego numeru `+48...`, `0048...` lub `48...`).
- **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 jej nazwę.

- **CID event table** – dla każdego zdarzenia można ustawić, który numer otrzyma SMS lub połączenie; treść komunikatu i kod Contact ID też można zmienić, można też dodać nowe zdarzenie.

Na zakładce **Control by SMS** ustawiasz odbiór poleceń SMS (polecenia opisuje punkt 5.4).

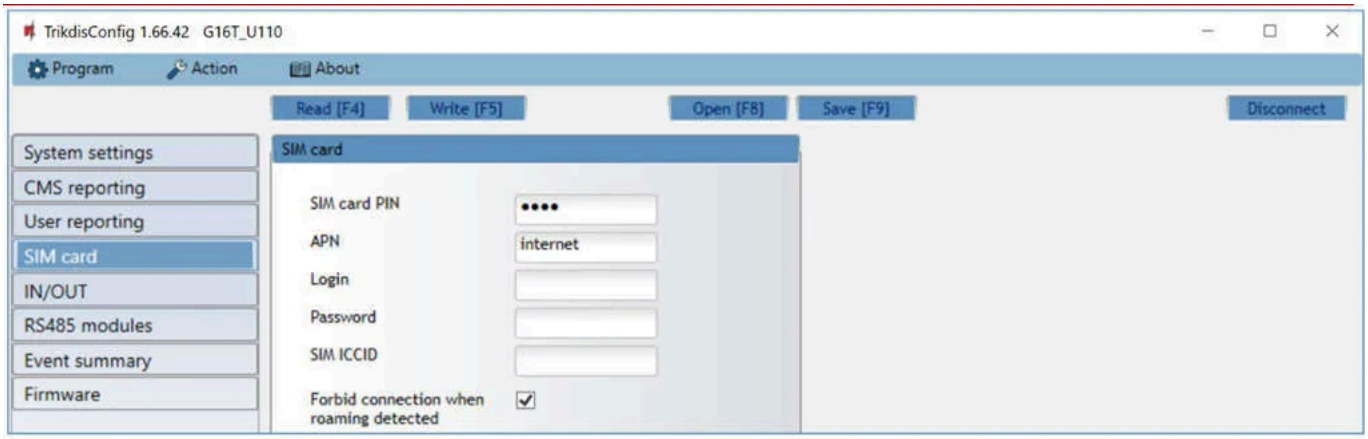


Rysunek 29. TrikdisConfig – User reporting, zakładka Control by SMS.

- **Reply text** – treść czterech odpowiedzi na polecenie SMS: polecenie wykonane (Command done), błędne hasło (Wrong password), błędne polecenie (Wrong command), błędne dane (Wrong data). Treść odpowiedzi można edytować.
- **Tel numbers for control by SMS** – maksymalnie 4 numery; urządzenie przyjmuje polecenia tylko z tych numerów. Jeśli lista jest pusta, 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.



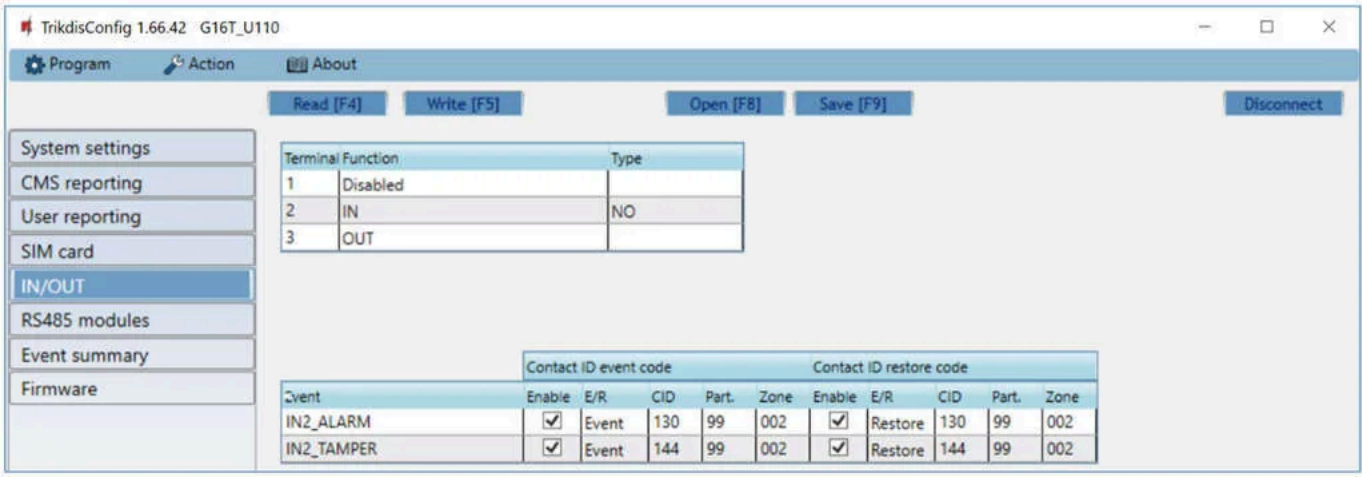
Rysunek 30. TrikdisConfig – strona SIM card.

- **SIM card PIN** – kod PIN karty. Żądanie PIN-u wyłączysz, wkładając kartę do telefonu komórkowego i wyłączając je tam. Jeśli żądanie PIN-u jest wyłączone, w polu może zostać wartość fabryczna.
- **APN** – punkt dostępu operatora; znane APN-y operatorów wymienia artykuł o APN (dla karty IoT / M2M operator podaje osobny APN, patrz punkt 2.2). APN jest potrzebny do połączenia urządzenia z internetem; jeśli nie masz innych danych, wypróbuj APN `internet`, który jest ogólny i działa w sieciach wielu operatorów.
- **Login, Password** – nazwa użytkownika i hasło APN, jeśli operator ich wymaga.
- **Forbid connection when roaming detected** – przydatne w pobliżu granicy państwa: zapobiega połączeniu urządzenia 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 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). W sprzęcie w wersji 3 te ustawienia są na stronie **System settings** (punkt 6.2).



Rysunek 31. TrikdisConfig – strona IN/OUT: funkcja zacisków I/O i zdarzenia wejść.

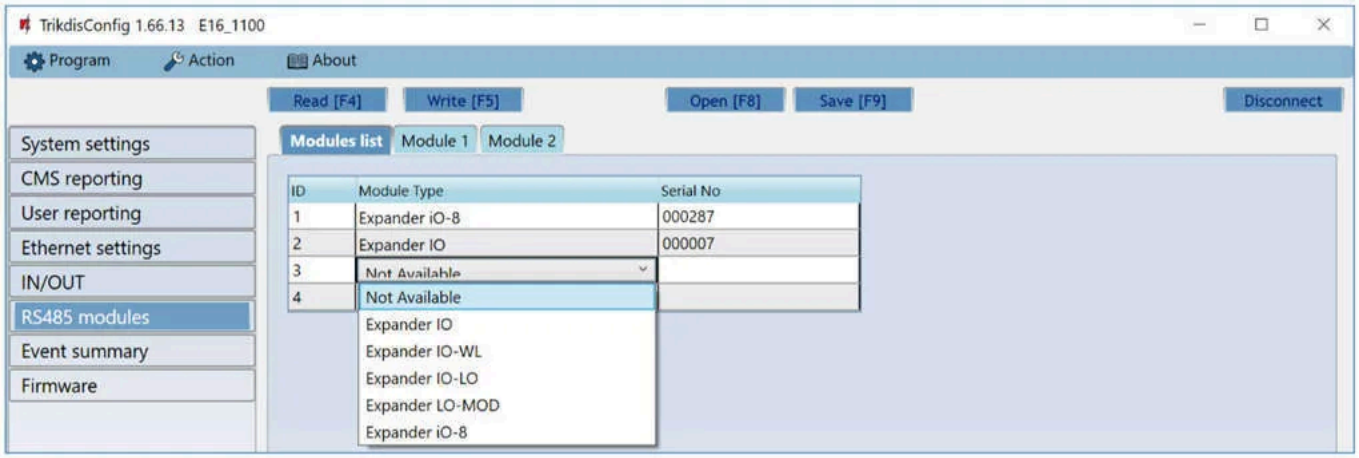
Po naruszeniu czujki podłączonej do wejścia komunikator wysyła własne zdarzenie (**INx_ALARM**, Contact ID 130), a po naruszeniu obwodu sabotażowego zdarzenie sabotażu (**INx_TAMPER**, 144) do stacji monitorowania i do Protegus 2; w tabeli pojawiają się zdarzenia każdego zacisku ustawionego jako wejście.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

6.7 RS485 modules

Ekspandery serii iO dodają do komunikatora kolejne wejścia, wyjścia i magistralę szeregową do czujników temperatury. Ekspandery iO-8 (i pozostałe ekspandery serii iO) oraz moduły W485 / E485 podłączone do magistrali RS485 trzeba dodać na zakładce **Modules list**.

W G16T z modemem 2G (G16T_G410) z tej strony nie można korzystać: wersja 2G nie ma magistrali RS485.

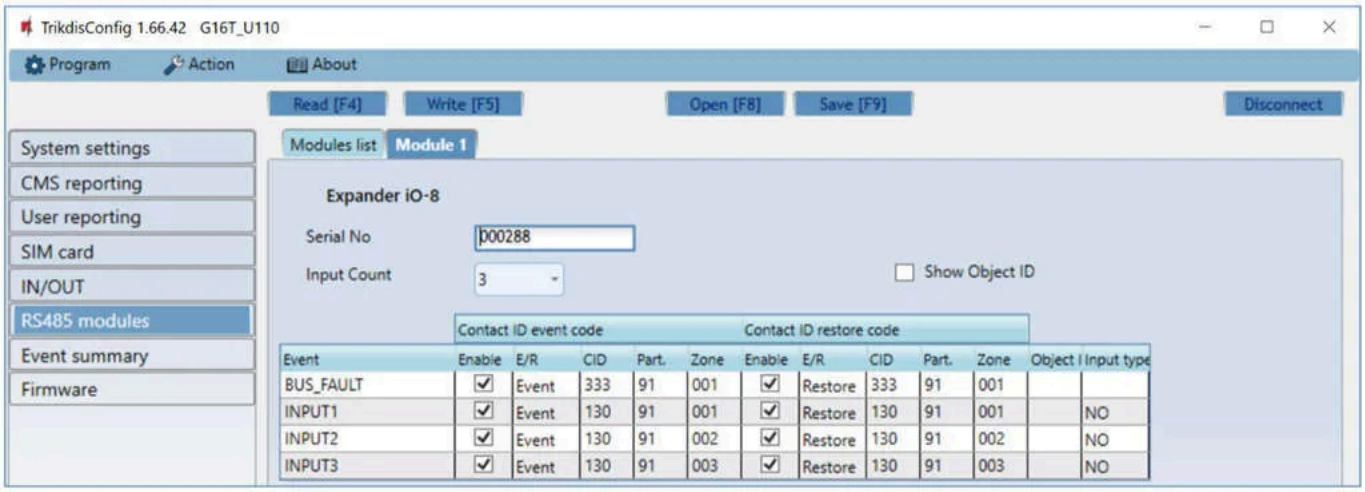


Rysunek 32. TrikdisConfig – RS485 modules, zakładka Modules list.

- **Module Type** – typ podłączonego modułu z listy (iO-8 i inne ekspandery serii iO, W485, E485).
- **Serial No** – 6-cyfrowy numer seryjny modułu (na module i na jego pudełku, SN).

Po wybraniu modułu i wpisaniu numeru seryjnego naciśnij przycisk **Write [F5]**, odłącz kabel USB i odczekaj minutę, aż komunikator zarejestruje moduł. Następnie podłącz kabel ponownie, 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.



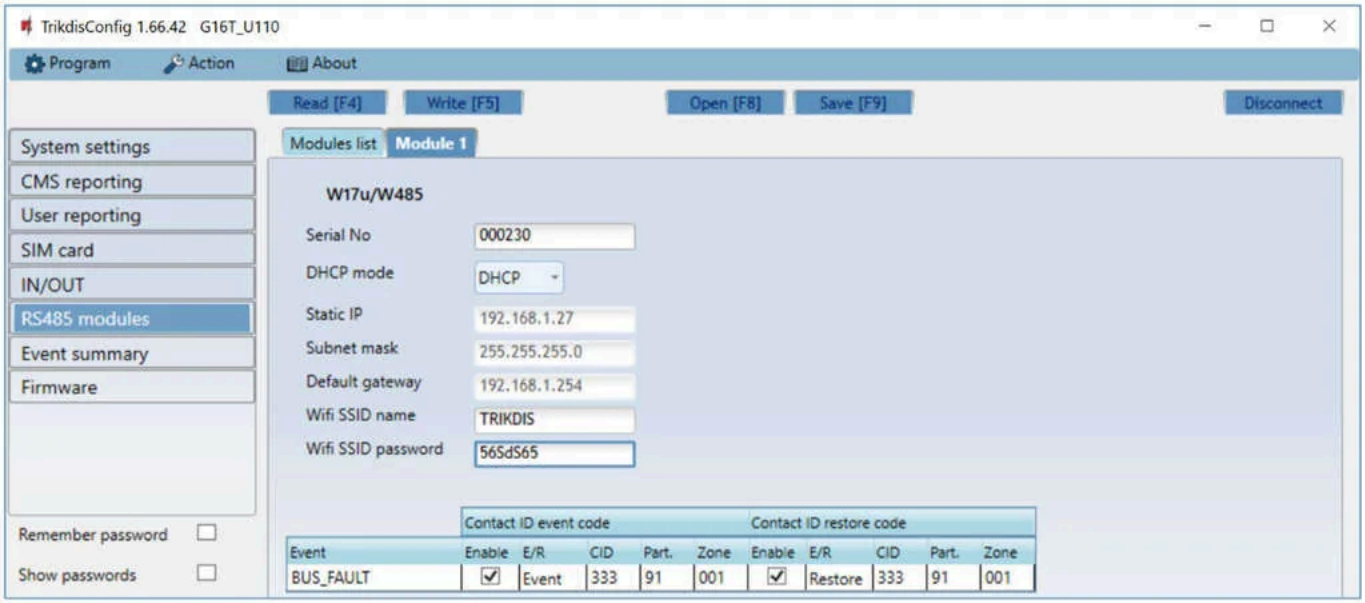
Rysunek 33. TrikdisConfig – RS485 modules, zakładka modułu iO-8.

- **Input Count** – ile zacisków ma być wejściami; pozostałe będą wyjściami. Typ wejścia (**Input type**: NO lub NC) podaje się w tabeli. Rolę wyjść (uzbrajanie / rozbrajanie lub sterowanie urządzeniem) ustawiasz w aplikacji Protegus 2.
- W tabeli możesz przypisać kod Contact ID usterce magistrali (**BUS_FAULT**, Contact ID 333) oraz zdarzeniom 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 i do Protegus 2. Domyślnie 1. moduł raportuje z partycją 91, a 4. moduł z partycją 94. Po zaznaczeniu **Show Object ID** można dla wejść podać identyfikator obiektu inny niż identyfikator komunikatora.
- Jeśli użytkownik ma otrzymywać SMS lub połączenie także o naruszeniu wejść ekspandera, kod zdarzenia Contact ID przypisany do wejścia dodaj także do tabeli na zakładce **User reporting** → **SMS & Call Reporting**.

Ekspander iO – 1 wejście, 1 wyjście przekaźnikowe (styki przekaźnika) i magistrala szeregowa 1-Wire do czujników temperatury. Wyjściem przekaźnikowym można sterować także według warunków logicznych (JEŚLI … TO).

- **Input IN1 type** – typ wejścia (NO lub NC).
- **Max °C (T1)** – jeśli temperatura jest wyższa, urządzenie wysyła zdarzenie; w tym celu zdarzenie trzeba włączyć w tabeli.
- **Min °C (T2)** – jeśli temperatura jest niższa, urządzenie wysyła zdarzenie; w tym celu zdarzenie trzeba włączyć w tabeli.
- W tabeli możesz przypisać do wejścia kod Contact ID zdarzenia i powrotu do normy tak samo jak przy ekspanderze iO-8; po naruszeniu wejścia komunikator wysyła zdarzenie z ustawionym kodem do odbiornika stacji monitorowania i do Protegus 2.

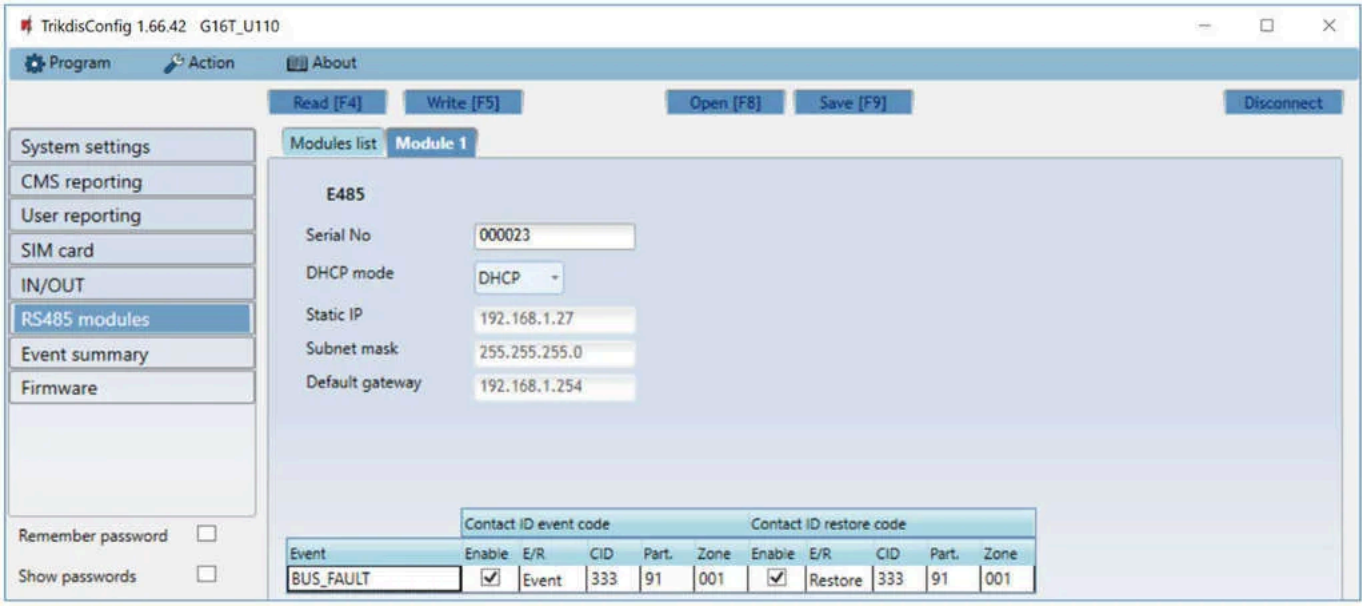
Moduł WiFi W485 (na liście W17u/W485) – dane sieci WiFi i ustawienia sieciowe.



Rysunek 34. TrikdisConfig – RS485 modules, zakładka modułu W485.

- **DHCP mode** – automatyczna lub ręczna konfiguracja sieci.
- **Static IP**, **Subnet mask**, **Default gateway** – przy konfiguracji ręcznej.
- **Wifi SSID name**, **Wifi SSID password** – nazwa i hasło sieci WiFi.
- W tabeli możesz przypisać kod Contact ID usterkom magistrali RS485 (przerwanie i przywrócenie połączenia między modułem a G16T); 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**); tak samo możesz przypisać kod Contact ID usterkom magistrali RS485 (przerwanie i przywrócenie połączenia między modułem a G16T); zdarzenie otrzymuje zarówno stacja monitorowania, jak i Protegus 2.



Rysunek 35. TrikdisConfig – RS485 modules, zakładka modułu E485.

Do działania W485 i E485 w G16T musi być skonfigurowane połączenie ze stacją monitorowania i/lub z Protegus (punkty 2.2 i 2.3), a w podstawowym przypadku w G16T musi być także karta SIM (w razie potrzeby może działać także bez karty SIM: tę funkcję Trikdis dodał później, na prośbę klientów).

6.8 Event summary

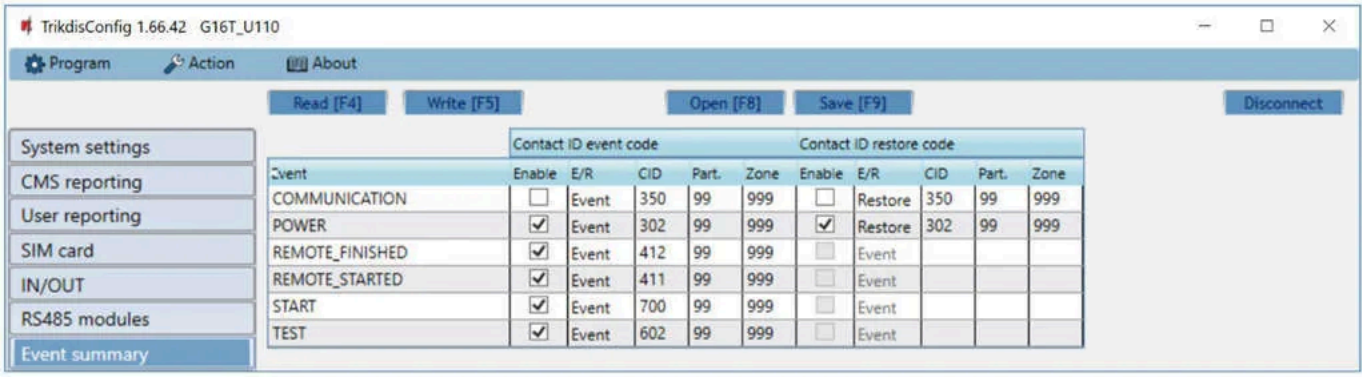
Na tej stronie włączasz lub wyłączasz **własne, wewnętrzne komunikaty** urządzenia oraz zmieniasz ich kod Contact ID, numer partycji i strefy. Komunikatu wyłączonego tutaj urządzenie nie wysyła żadnym kanałem. Fabrycznie komunikaty są wysyłane z partycją 99 i strefą 999.

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 36. TrikdisConfig – strona Event summary: wewnętrzne komunikaty urządzenia.

6.9 Przywracanie ustawień fabrycznych

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

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

7. Zdalne programowanie

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

Do zdalnego dostępu potrzebne jest:

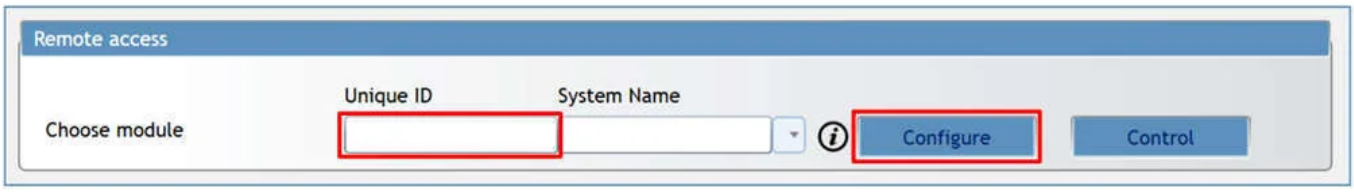
1. Urządzenie musi być włączone i mieć połączenie z siecią (diody **POWER** i **NETWORK** świecą na zielono; w urządzeniu z siecią komórkową dioda NETWORK miga też na żółto). W urządzeniu z siecią komórkową włożona karta SIM musi być aktywna, a jej kod PIN musi być wpisany w urządzeniu albo żądanie kodu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

Kroki:

1. Uruchom program TrikdisConfig.
2. W części **Remote access**, w polu **Unique ID** wpisz unikalny identyfikator urządzenia (IMEI lub MAC).

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

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



Rysunek 37. TrikdisConfig – Remote access: identyfikator urządzenia, nazwa systemu i przycisk Configure.

Włączenie chmury Protegus opisuje punkt 6.4.

8. Sprawdzenie działania komunikatora

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

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

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

9. Aktualizacja firmware

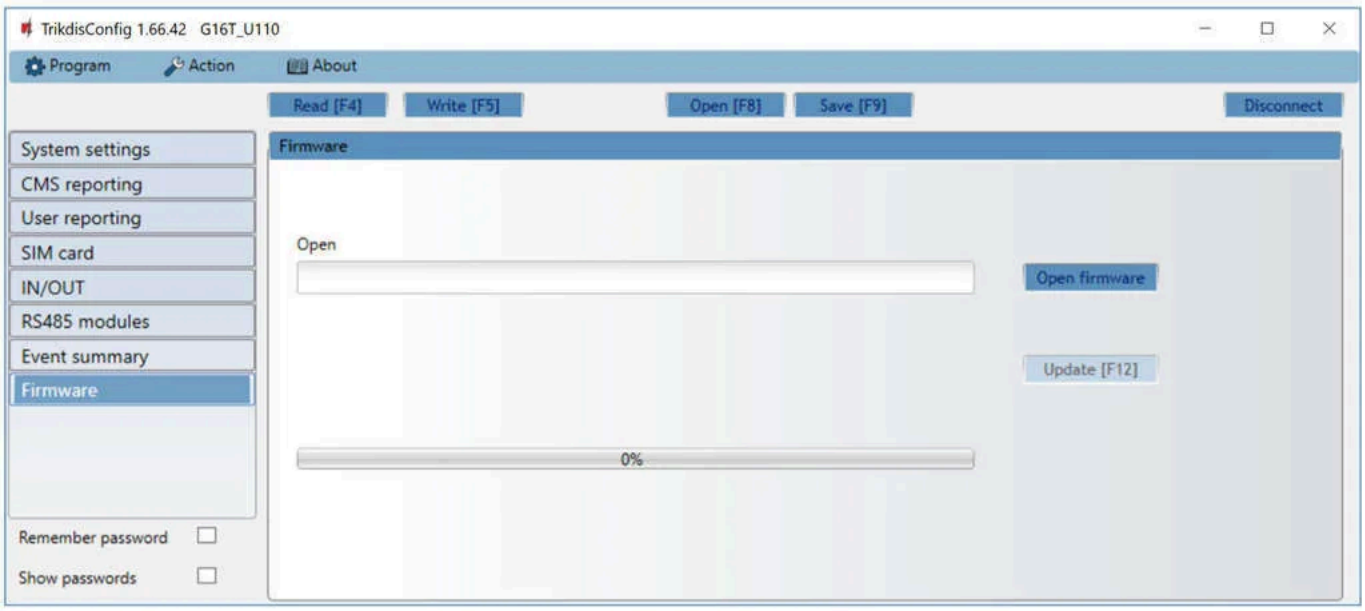
Ha bármikor az USB bedugásakor a program azt jelzi, hogy új firmware verzió jelent meg a Trikdis eszközhöz, fogadd el a frissítést és telepítsd!

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

1. Uruchom program TrikdisConfig i podłącz urządzenie kablem USB albo połącz się z nim zdalnie w trybie programowania.
2. Jeśli jest dostępny nowszy firmware, program zaproponuje jego pobranie – zaakceptuj.

3. Wybierz stronę **Firmware** i kliknij przycisk **Open firmware**. Wybierz plik firmware.
4. Naciśnij przycisk **Update [F12]**, poczekaj na zakończenie aktualizacji, a następnie w wyskakującym oknie kliknij **OK**. W tym czasie nie odłączaj kabla i nie przerywaj połączenia.

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



Rysunek 38. TrikdisConfig – strona Firmware: Open firmware i Update [F12].

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

10. Rozwiązywanie problemów i najczęstsze pytania

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

Dioda NETWORK nie świeci – brak sieci

1. Sprawdź mignięcia diody **TROUBLE**: 1 = brak karty SIM, 2 = błędny PIN, 3 = brak APN, 4 = nie może połączyć się z siecią GSM, 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 na karcie włączone jest żądanie PIN-u, wpisz PIN na stronie **SIM card** albo wyłącz żądanie PIN-u w telefonie.
4. Sprawdź antenę: jest przykręcona, nie znajduje się w metalowej obudowie, poziom sygnału jest odpowiedni (punkty 1.6 i 3.2).

Sieć jest, ale stacja monitorowania nie otrzymuje zdarzeń

Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie

działa do routera – ale nie to, że urządzenie ma też dostęp do internetu. Jeśli dioda NETWORK jest zielona, a dioda DATA świeci ciągle także po zdarzeniu lub raporcie testowym, połączenie z internetem nie działa: komunikat nie może zostać wysłany. W sieci komórkowej najczęściej winny jest APN albo usługa transmisji danych karty SIM, przy Ethernecie router, zapora sieciowa (firewall) lub DNS. Jeśli dioda DATA zgaśnie, komunikat został wysłany, a połączenie danych działa prawidłowo.

1. 6 mignięć diody **TROUBLE** oznacza brak połączenia z odbiornikiem: sprawdź adres i port odbiornika, ustawienie TCP/UDP i klucz szyfrowania (**CMS reporting**).
2. Jeśli odbiornik jest podany nazwą domeny, sprawdź ustawienia DNS (**CMS reporting → Settings**).
3. Sprawdź, czy pakiet danych karty SIM nie blokuje potrzebnego portu (niektóre karty M2M dopuszczają tylko określone adresy).

Centrala nie wysyła zdarzeń do komunikatora

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

Protegus 2 nie widzi urządzenia

1. Na zakładce **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. IMEI wpisz dokładnie, z pudełka lub z tylnej części obudowy.
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 połączyć się zdalnie przez TrikdisConfig

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

Zapomniałem hasła

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

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

G16T z modemem 2G (G16T_G410) nie ma magistrali RS485; iO-8, W485 i E485 można podłączyć tylko do wersji 4G (G16T_E120). Do modułu W485 i E485 w podstawowym przypadku w G16T musi być także karta SIM; w razie potrzeby może działać także bez karty SIM (funkcja dodana przez Trikdis później, na prośbę klientów).

Mam urządzenie 2G – jak długo będzie działać?

Wyłączanie sieci 2G postępuje u każdego operatora w innym tempie; do długotrwałej pracy zalecamy wersję 4G, która ma także rezerwę 2G. Wersję 4G można ponadto rozbudować przez magistralę RS485.

Ile danych zużywa urządzenie?

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

- Instalację i konserwację urządzeń zabezpieczających może wykonywać tylko wykwalifikowany instalator.
- Przed instalacją przeczytaj instrukcję; nieprzestrzeganie zaleceń może prowadzić do nieprawidłowego działania lub uszkodzenia.
- Przed podłączaniem, przed każdym połączeniem elektrycznym i przed serwisowaniem odłącz urządzenie od zasilania.
- Usterki wynikające z nieprawidłowej instalacji lub użytkowania, a także modyfikacje i naprawy niezatwierdzone przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów dotyczących odpadów: nie wyrzucaj uszkodzonego urządzenia ani jego części razem z odpadami komunalnymi.

Zobacz też

- Zdalne uzbrajanie strefą typu klucz z aplikacji Protegus 2 – szczegóły i pułapki uzbrajania strefą typu klucz.
- Nadchodzi wersja sprzętowa 4 komunikatorów GSM G16 i G16T – co zmieniło się w porównaniu z poprzednią wersją.
- Nowości w komunikatorze G16T v3 – zapowiedź produktu.
- Dokumentacja w języku angielskim: docs.trikdis.com.

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

Powiązane produkty

Trikdis G16T 4G GSM inteligentny moduł komunikacyjny (TIP-RING)

Trikdis G16T 2G GSM inteligentny moduł komunikacyjny (TIP-RING)

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-g16t