Komunikator GT i GT+ – instrukcja dla instalatora i użytkownika

Instrukcja dla instalatora i użytkownika komunikatorów Trikdis GT i GT+: podłączenie do magistrali danych, portu szeregowego lub wyjścia linii telefonicznej centrali alarmowej, programowanie centrali, konfiguracja w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2.



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

Spis treści

1. Przegląd

- 1.1 Do czego służy, jak działa
- 1.2 Wersje: GT i GT+
- 1.3 Zgodne centrale alarmowe
- 1.4 Elementy komunikatora
- 1.5 Zaciski
- 1.6 Sygnalizacja diod
- 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 DSC – magistrala danych (Keybus)
  - 3.3.2 DSC – Keybus i TIP/RING (tylko GT+)
  - 3.3.3 Paradox – port szeregowy
  - 3.3.4 Paradox SP/MG – Keybus i TIP/RING
  - 3.3.5 UTC Interlogix (Caddx) – magistrala danych
  - 3.3.6 Texecom – port szeregowy
  - 3.3.7 InnerRange Inception
  - 3.3.8 InnerRange Integriti
  - 3.3.9 Honeywell Vista – magistrala danych
  - 3.3.10 Dowolna centrala – TIP/RING
- 3.4 Podłączenie strefy przełącznika kluczowego
- 3.5 Podłączenie wejść
- 3.6 Podłączenie wyjścia z przekaźnikiem
- 3.7 Podłączenie ekspandera iO-8
- 3.8 Włączenie i pierwsze sprawdzenie
- A TRIKDIS átjelző elindítása

4. Programowanie centrali alarmowej

- 4.1 Podłączenie do magistrali danych lub portu szeregowego
  - 4.1.1 DSC
  - 4.1.2 Paradox
  - 4.1.3 Texecom
  - 4.1.4 UTC Interlogix (Caddx)
  - 4.1.5 InnerRange
  - 4.1.6 Honeywell Ademco Vista
- 4.2 Podłączenie do linii telefonicznej (TIP/RING)
  - 4.2.1 Programowanie dialera Honeywell Vista
  - 4.2.2 Dialer UTC Interlogix (Caddx) NX

5. Zdalne sterowanie aplikacją Protegus 2

- 5.1 Dodawanie urządzenia

A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Uzbrajanie i rozbrajanie wyjściem
5.3 Uzbrajanie i rozbrajanie z aplikacji
5.4 Sterowanie wiadomościami SMS

6. TrikdisConfig – ustawienia szczegółowo

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

7. Zdalne programowanie

8. Sprawdzenie działania komunikatora

9. Aktualizacja firmware

10. Rozwiązywanie problemów i najczęstsze pytania

11. Zasady bezpieczeństwa

Zobacz też

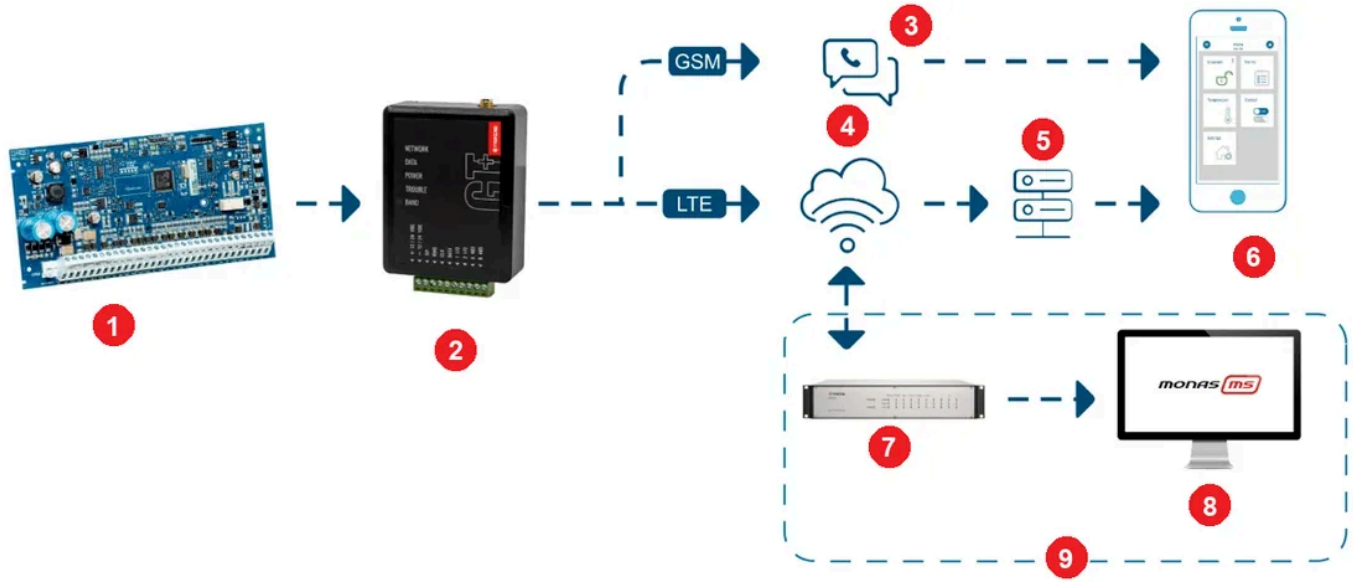
1. Przegląd

GT i GT+ to **komunikatory 4G sieci komórkowej** firmy Trikdis, które przekazują zdarzenia centrali alarmowej do stacji monitorowania i do aplikacji Protegus 2. Z centralą można je połączyć na dwa sposoby: **bezpośrednio**, do magistrali danych lub portu szeregowego centrali (w centralach DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange i Honeywell), albo do **komunikatora linii telefonicznej dowolnej centrali** (TIP/RING), który wysyła zdarzenia w formacie Contact ID, tonami DTMF. Komunikator przekazuje stacji monitorowania pełną informację o zdarzeniu (kod, partycja, strefa lub użytkownik). Aplikacją Protegus 2 użytkownik zdalnie steruje systemem i otrzymuje powiadomienia o zdarzeniach; aplikacja działa ze wszystkimi centralami obsługiwanymi przez komunikator, niezależnie od producenta centrali. Raportowania do stacji monitorowania i Protegus 2 można używać jednocześnie. Ta instrukcja została przygotowana dla komunikatorów 4G GT i GT+; różnice między obiema wersjami zestawia punkt 1.2.

1.1 Do czego służy, jak działa

- **Raportuje do stacji monitorowania.** Zdarzenia wysyła przez połączenie IP do programowego lub sprzętowego odbiornika Trikdis (protokół TRK8) – współpracują one z dowolnym oprogramowaniem stacji monitorowania – do odbiornika SIA DC-09 albo do odbiornika SUR-GARD (TL150). Odbiornikowi SUR-GARD przekazuje kody Contact ID otrzymane z centrali przekształcone na kody SIA; tabela konwersji znajduje się w załączniku angielskiej dokumentacji (docs.trikdis.com). Połączenie z odbiornikiem sprawdza co 30 sekund (lub w ustawionym odstępie) komunikatem PING; jeśli kanał główny zostanie przerwany, przełącza się na kanał zapasowy. Z kanałem równoległym zdarzenia trafiają jednocześnie do dwóch odbiorników. Jeśli włączona jest także usługa Protegus, zdarzenie najpierw otrzymuje stacja monitorowania, a dopiero potem aplikacje użytkowników.
- **Powiadamia użytkownika.** Aplikacja Protegus 2 sygnalizuje zdarzenia powiadomieniem push z osobnym dźwiękiem; użytkownik może z aplikacji uzbrajać i rozbrajać system oraz przełączać podłączone urządzenia (oświetlenie, bramę, wentylację, ogrzewanie, nawadnianie itp.). W aplikacji uprawnienia administratora, instalatora i użytkownika są różne. Oprócz Protegus 2 powiadomienia można otrzymywać także SMS-em i połączeniem telefonicznym.
- **Steruje centralą bezpośrednio.** Po podłączeniu do magistrali danych lub portu szeregowego komunikator widzi także stany partycji i stref centrali, a użytkownik uzbraja i rozbraja system z Protegus 2 własnym kodem klawiatury – nie jest do tego potrzebna strefa przełącznika kluczowego. GT+ można podłączyć do central DSC jednocześnie do magistrali danych (Keybus) i do zacisków TIP/RING: magistrala służy do sterowania i odczytu stanów, a zdarzenia są wysyłane z własnymi kodami Contact ID centrali (punkt 3.3.2).
- **Ma własne wejścia i wyjścia.** Dwa zaciski I/O o podwójnej funkcji można wykorzystać jako wejście (IN) lub jako sterowane wyjście (OUT). Wyjścia można przełączać z aplikacji Protegus 2 i poleceniem SMS. Ekspanderami iO-8 podłączonymi do magistrali RS485 można dodać kolejne wejścia i wyjścia.
- **Konfiguracja.** Ustawienia można zapisać do pliku i wpisać do innych komunikatorów. Są dwa poziomy dostępu: administratora stacji monitorowania i instalatora. Komunikator można konfigurować także zdalnie, a jego firmware można aktualizować zdalnie.

Budowę systemu pokazuje poniższy rysunek: centrala alarmowa jest podłączona do komunikatora, komunikator przez sieć komórkową (LTE) łączy się z internetem, a stamtąd z odbiornikiem stacji monitorowania (i jego oprogramowaniem) oraz z serwerem Protegus; użytkownik widzi system w aplikacji Protegus 2, a przez sieć komórkową może otrzymywać także SMS-y i połączenia.



Rysunek 1. Miejsce komunikatora w systemie: centrala alarmowa → GT / GT+ → sieć komórkowa → internet → odbiornik stacji monitorowania i serwer Protegus → aplikacja Protegus 2; SMS-y i połączenia bezpośrednio przez sieć komórkową.

- 1 centrala alarmowa („Alarm panel")
- 2 komunikator LTE GT / GT+ („LTE communicator")
- 3 połączenie i SMS („Call/SMS")
- 4 internet („Internet")
- 5 serwer Protegus („Protegus server")
- 6 telefon z aplikacją Protegus („Phone with Protegus software")
- 7 odbiornik stacji monitorowania („Receiver")
- 8 oprogramowanie stacji monitorowania („Monitoring software")
- 9 stacja monitorowania firmy ochrony („Monitoring station in security company") – w przerywanej ramce

1.2 Wersje: GT i GT+

GT i GT+ to to samo urządzenie w dwóch wersjach: ich podłączenie, konfiguracja i działanie są niemal takie same, dlatego opisujemy je w jednej instrukcji. Różnice zestawia poniższa tabela; tam, gdzie tekst podaje dane GT+, w GT weź pod uwagę te z tabeli.

	GT	**GT+**
Napięcie zasilania	10–18 V DC	10–32 V DC
Oznaczenie zacisków zasilania	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Podłączenie centrali DSC	tylko do magistrali danych (Keybus)	do magistrali danych albo do magistrali danych i zacisków TIP/RING razem – wtedy zdarzenia są wysyłane z własnymi kodami Contact ID centrali (np. pożar: E110), a nie jako alarm ogólny (E130)
Ustawienie podłączenia do linii telefonicznej (TIP/RING) w TrikdisConfig (**Panel settings → Communication protocol**)	**2. Dual tone**	**2. AUTO** (na liście można wybrać także **3. MANUAL**)
Sprawdzenie w DSC z podłączeniem magistrala + TIP/RING (rozdział 8)	–	alarm strefy pożarowej ma przyjść jako E110

	GT	GT+
Wszystko inne: wejścia/wyjścia, magistrala RS485, modem, diody, wymiary, protokoły, Protegus 2, polecenia SMS	takie same	takie same

Obie wersje są produkowane z trzema rodzajami modemu; na rynek europejski (w tym polski) przeznaczona jest wersja europejska (EU). Typ modemu i wersję sprzętową znajdziesz na pasku stanu TrikdisConfig (**Device**, **HW**) i na etykiecie urządzenia.

Modem	Sieć i pasma częstotliwości
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (Ameryka Łacińska)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Zgodne centrale alarmowe

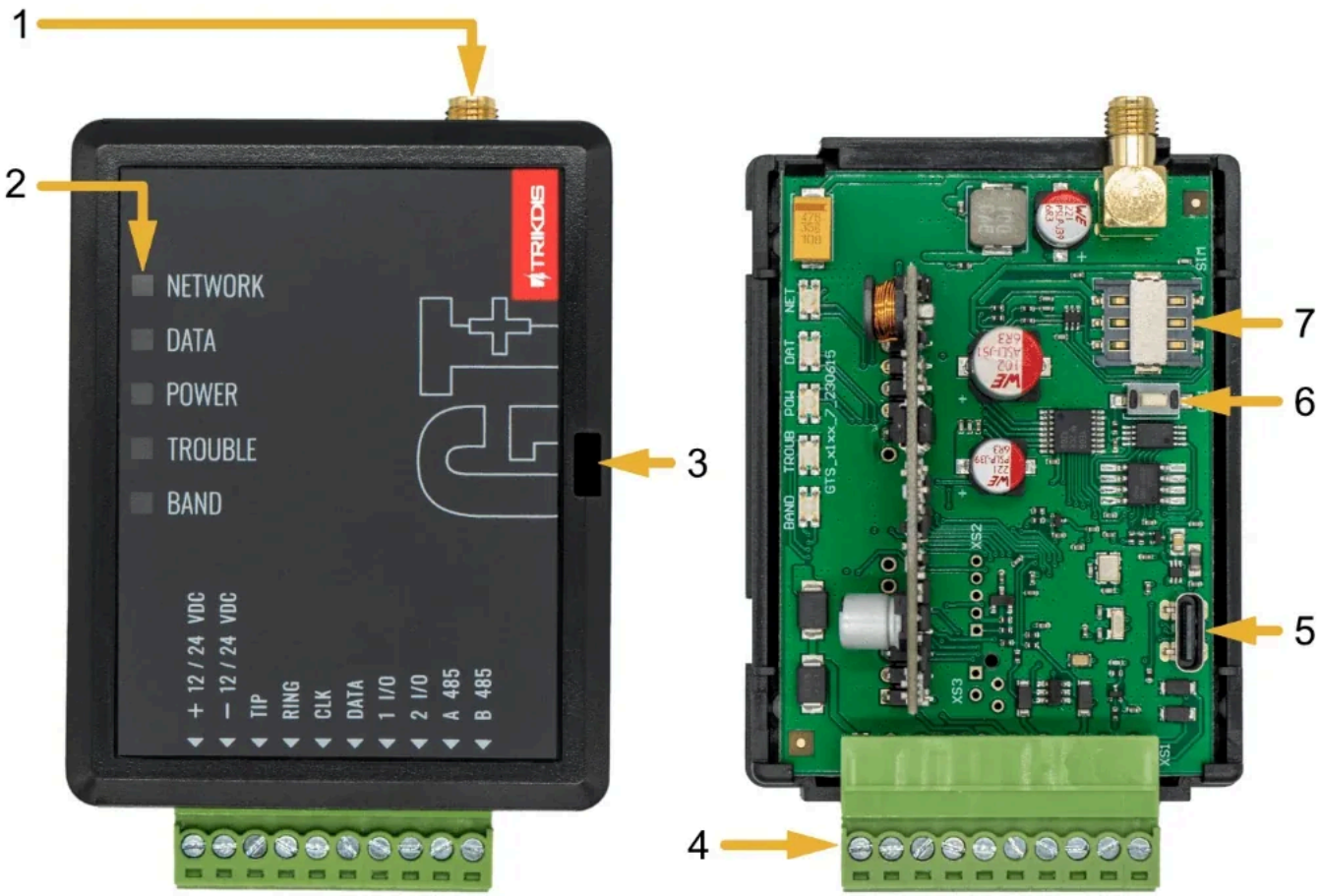
Poniższe centrale można podłączyć do komunikatora bezpośrednio, przez magistralę danych lub port szeregowy. Kolumna „sterowanie bezpośrednie" pokazuje, czy użytkownik może z Protegus 2 uzbrajać i rozbrajać system własnym kodem klawiatury bez dodatkowego podłączenia; tam, gdzie nie jest to możliwe, komunikator odczytuje zdarzenia z magistrali, a do sterowania potrzebna jest strefa przełącznika kluczowego (punkt 3.4).

Producent	Typ	Podłączenie	Sterowanie bezpośrednie
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	magistrala danych (Keybus); GT+: także Keybus + TIP/RING	tak
DSC	PC5020	magistrala danych (Keybus)	nie
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	port szeregowy (kabel EX-CRP2.4) albo Keybus + TIP/RING	tak
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	port szeregowy (kabel EX-CRP2.4) albo Keybus + TIP/RING	tak
Paradox	Digiplex EVO192, EVOHD, EVOHD+	port szeregowy (kabel EX-CRP2.4)	tak
Paradox	Digiplex EVO48	port szeregowy (kabel EX-CRP2.4)	nie
Paradox	Spectra 1727, 1728, 1738; Esprit E55	port szeregowy (kabel EX-CRP2.4)	nie
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	magistrala danych	tak
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	port szeregowy (kabel EX-CRP4)	tak
InnerRange	Inception, Integriti	port szeregowy (kablem producenta)	nie
Honeywell	Ademco Vista-15, Vista-20, Vista-48	magistrala danych	tak

- Firmware central **Paradox** sterowanych bezpośrednio musi mieć wersję co najmniej **V.4**. W nowszych centralach Paradox (SP+, MG+, EVOHD+) port szeregowy może być fabrycznie zablokowany; o odblokowaniu mówi punkt 4.1.2. Centrale Spectra SP / SP+ i Magellan MG / MG+ można zamiast portu szeregowego podłączyć także do magistrali danych (Keybus) i zacisków TIP/RING razem – nie jest do tego potrzebne płatne odblokowanie (punkt 3.3.4).
- Centrale **wszystkich innych producentów** łączy się przez ich komunikator linii telefonicznej (TIP/RING), jeśli wysyła on zdarzenia w formacie Contact ID z wybieraniem DTMF; wtedy do sterowania potrzebna jest strefa przełącznika kluczowego.
- Który komunikator Trikdis i jakie podłączenie pasuje do twojej centrali, sprawdzisz w wyszukiwarce zgodności.

1.4 Elementy komunikatora

Płytka drukowana komunikatora znajduje się w czarnej obudowie z tworzywa; pokrywę przednią można odpiąć, a listwę zaciskową zdjąć. Na poniższym rysunku widać GT+; GT wygląda tak samo, tylko napis na obudowie to GT, a zaciski zasilania są oznaczone +12 VDC / −12 VDC.



Rysunek 2. Elementy komunikatora z przodu (po lewej) i z otwartą obudową (po prawej).

- 1 Złącze SMA anteny komórkowej
- 2 Diody sygnalizacyjne (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Otwór ułatwiający odpięcie pokrywy przedniej
- 4 Odłączana listwa zaciskowa do podłączeń zewnętrznych
- 5 Gniazdo USB-C do programowania
- 6 Przycisk RESET
- 7 Gniazdo karty nano-SIM

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

1.5 Zaciski

Zacisk (GT)	Zacisk (GT+)	Funkcja
+12 VDC	**+12 / 24 VDC**	Zasilanie, biegun dodatni: +10–18 V DC (GT), +10–32 V DC (GT+)
−12 VDC	**−12 / 24 VDC**	Zasilanie, 0 V
TIP	**TIP**	Zacisk TIP komunikatora linii telefonicznej centrali alarmowej
RING	**RING**	Zacisk RING komunikatora linii telefonicznej centrali alarmowej
CLK	**CLK**	Magistrala szeregowa lub magistrala danych (zegar) do bezpośredniego podłączenia centrali
DATA	**DATA**	Magistrala szeregowa lub magistrala danych (dane) do bezpośredniego podłączenia centrali
1 I/O	**1 I/O**	1. wejście/wyjście (ustawienie fabryczne: wejście, NO)
2 I/O	**2 I/O**	2. wejście/wyjście (ustawienie fabryczne: wejście, NO)
A 485	**A 485**	Przewód A magistrali RS485
B 485	**B 485**	Przewód B magistrali RS485

Na schematach podłączeń zaciski zasilania są jednolicie oznaczone **+DC** i **−DC** (w GT to zacisk +12 VDC / −12 VDC, w GT+ zacisk +12 / 24 VDC / −12 / 24 VDC), a zaciski RS485 – **A RS485** / **B RS485** (na urządzeniu A 485 / B 485). Opis listwy zaciskowej znajduje się także na pokrywie przedniej.

1.6 Sygnalizacja diod

Diody na pokrywie przedniej to najważniejsze narzędzie przy uruchamianiu i szukaniu usterek. Odczytuj je razem: POWER pokazuje zasilanie, NETWORK sieć, TROUBLE usterkę, a BAND 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, miga na żółto	Połączony z siecią komórkową; liczba żółtych mignięć to **poziom sygnału**: w 4G odpowiedni sygnał to 3 mignięcia

DATA – transmisja danych

Sygnalizacja	Znaczenie
nie świeci	Brak zdarzeń oczekujących na wysłanie
świeci na zielono	W pamięci są zdarzenia oczekujące na wysłanie

Sygnalizacja	Znaczenie
miga na zielono	Transmisja danych między komunikatorem a komputerem (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 odpowiednie
świeci na żółto	Nieodpowiednie napięcie zasilania (najwyżej 11,5 V)
świeci na zielono, miga na żółto	Gotowy do programowania (podczas programowania)
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 zarejestrować się w sieci komórkowej (błąd rejestracji)
5 czerwonych mignięć	Nie może zarejestrować się w sieci transmisji danych (GPRS/UMTS)
6 czerwonych mignięć	Brak połączenia z odbiornikiem stacji monitorowania
7 czerwonych mignięć	Przerwane połączenie z centralą alarmową
8 czerwonych mignięć	Ustawiony ICCID nie zgadza się z ICCID karty SIM (punkt 6.6)
miga na czerwono (podczas programowania)	Błąd pamięci
świeci na czerwono (podczas programowania)	Uszkodzony firmware

BAND – typ sieci

Zielone mignięcia	Sieć
1	brak
2	GSM

Zielone mignięcia	Sieć
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	magistrala szeregowa, magistrala danych (Keybus) lub linia telefoniczna (TIP/RING, Contact ID, DTMF)
Wejścia/wyjścia	2 zaciski I/O o podwójnej funkcji: 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. Rozszerzalne ekspanderami iO-8
Modem	EG915U-EU (Europa), EG915U-LA (Ameryka Łacińska) lub BG95-M5 (LTE Cat M1) – pasma częstotliwości wymienia tabela w punkcie 1.2
Napięcie zasilania	GT: 10–18 V DC; GT+: 10–32 V DC
Pobór prądu	maksymalnie 100 mA w czuwaniu; maksymalnie 200 mA podczas wysyłania danych
Protokoły transmisji	TRK8, DC-09_2007, DC-09_2012, TL150
Szyfrowanie	AES-128
Programowanie	TrikdisConfig (Windows) kablem USB-C lub zdalnie
Warunki pracy	−10 … +50 °C, maks. 80 % wilgotności względnej (przy +20 °C)
Wymiary	92 × 62 × 26 mm
Masa	80 g

2. Szybkie uruchomienie w TrikdisConfig

Wszystkie ustawienia komunikatora wykonuje się programem **TrikdisConfig** działającym w systemie Windows – kablem USB-C lub zdalnie. W tym rozdziale opisujemy najkrótszą drogę: urządzenie konfigurujesz na biurku przed podłączeniem, a na obiekcie trzeba je już tylko podłączyć. Opisujemy, które ustawienia są potrzebne, aby komunikator wysyłał zdarzenia do stacji monitorowania i aby systemem można było sterować z aplikacji Protegus 2; szczegółowe objaśnienie ustawień zawiera rozdział 6.

2.1 Przygotowanie

Czego będziesz potrzebować

Kabel USB-C do programowania · co najmniej 4-żyłowy kabel między komunikatorem a centralą · do portu szeregowego Paradox kabel CRP2.4 · płaski śrubokręt 2,5 mm · antena komórkowa o odpowiednim zysku, jeśli na obiekcie zasięg jest słaby · aktywna karta SIM (żądanie PIN można wyłączyć) · instrukcja instalatora centrali alarmowej.

Potrzebne akcesoria zamów osobno u dystrybutora.

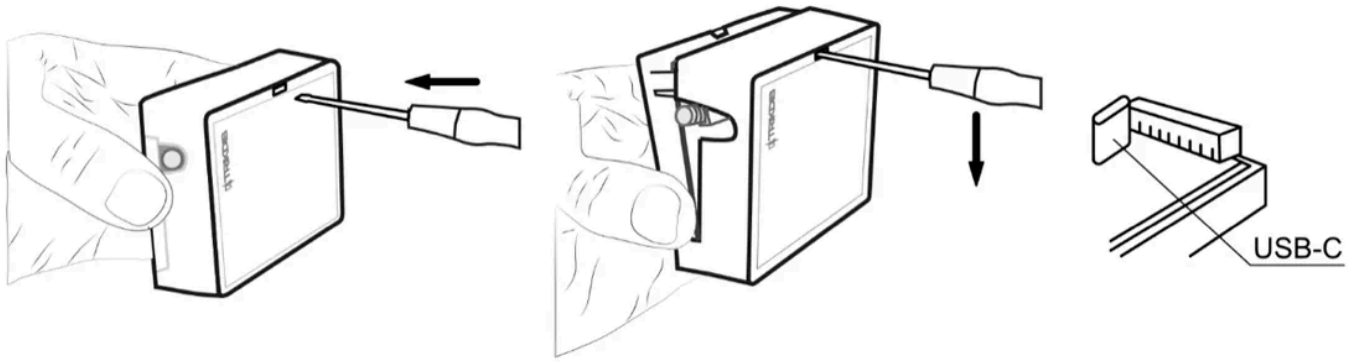
1. Pobierz i zainstaluj program TrikdisConfig. Na stronie producenta (www.trikdis.com) wpisz w pole wyszukiwania: „TrikdisConfig”.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

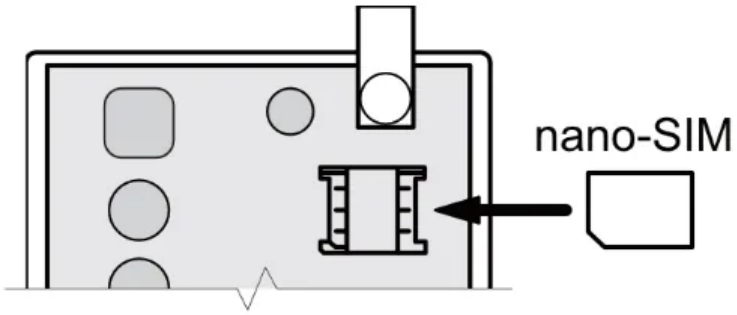
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Otwórz obudowę komunikatora płaskim śrubokrętem: włóż śrubokręt u góry, w szczelinę obok anteny, i podważ na zewnątrz, a następnie na dole, przy otworze, w dół. Rysunek pokazuje także położenie gniazda USB-C na krawędzi płytki drukowanej.



Rysunek 3. Odpinanie pokrywy przedniej płaskim śrubokrętem; powiększony fragment pokazuje położenie gniazda USB-C.

3. Włóż kartę nano-SIM do gniazda w kierunku pokazanym na rysunku. Karta musi być aktywna, mieć usługę mobilnej 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 komunikator z komputerem kablem USB-C.

Ostrzeżenie

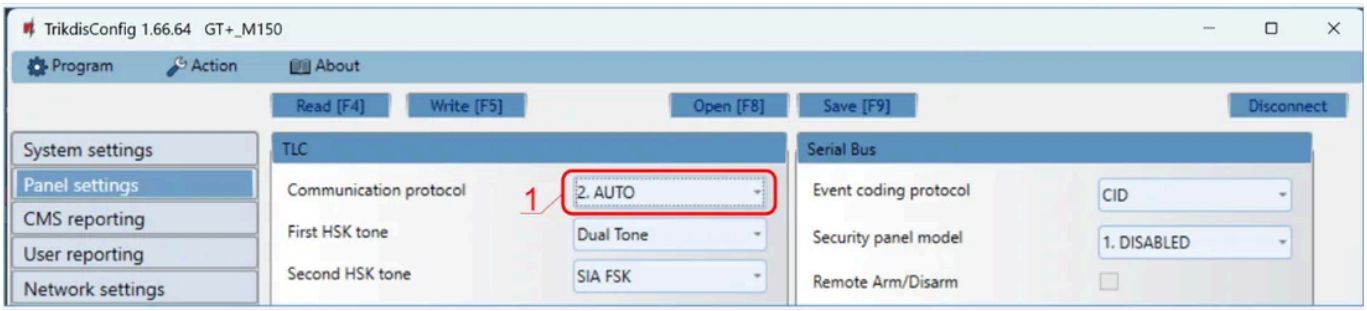
Dopóki urządzenie jest podłączone kablem USB do komputera, pracuje w trybie programowania: przestaje normalnie działać, nie dozoruje, nie wysyła zdarzeń, nie da się nim sterować, jest zasilane z USB, a po odłączeniu kabla uruchamia się ponownie. Dlatego urządzenie nie może być swobodnie dostępne: musi 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 Połączenie z aplikacją Protegus 2

Najpierw na stronie **Panel settings** podaj, jak komunikator jest połączony z centralą.

Jeśli podłączasz go do wyjścia linii telefonicznej centrali (TIP/RING): w polu **Communication protocol** wybierz wartość **AUTO** (w GT drugim elementem listy jest **Dual tone** – tam wybierz ją).



Rysunek 5. TrikdisConfig – Panel settings, grupa TLC (na rysunku ustawienie GT+).

- 1 **Communication protocol** – przy podłączeniu TIP/RING **2. AUTO** (GT: **2. Dual tone**).

Jeśli podłączasz go do magistrali danych lub portu szeregowego centrali: ustaw centralę w grupie **Serial bus**.



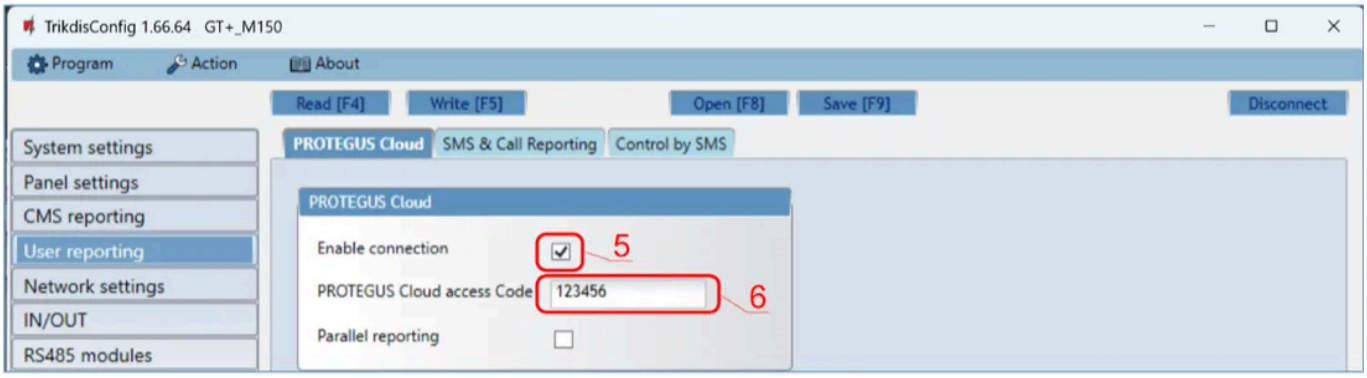
Rysunek 6. TrikdisConfig – Panel settings, grupa Serial bus.

- 2 **Security panel model** – typ podłączonej centrali.
- 3 **Remote Arm/Disarm** – zaznacz, jeśli użytkownicy chcą sterować centralą z Protegus 2 własnym kodem klawiatury. Pojawia się tylko przy centralach, którymi można sterować bezpośrednio.
- 4 **Security panel PC download password** – do bezpośredniego sterowania centralą Paradox i Texecom hasło PC lub UDL ustawione w centrali; oba muszą być takie same.

GT+, centrala DSC na magistrali danych i zaciskach TIP/RING razem: Communication protocol ustaw na **AUTO**, **Security panel model** na typ DSC i zaznacz opcję **Remote Arm/Disarm**, jeśli centralą będzie się sterować z Protegus 2 (punkt 3.3.2).

Do sterowania bezpośredniego trzeba ustawić także centralę alarmową – opisuje to rozdział 4, gdzie znajdziesz też sposób podania hasła PC lub UDL.

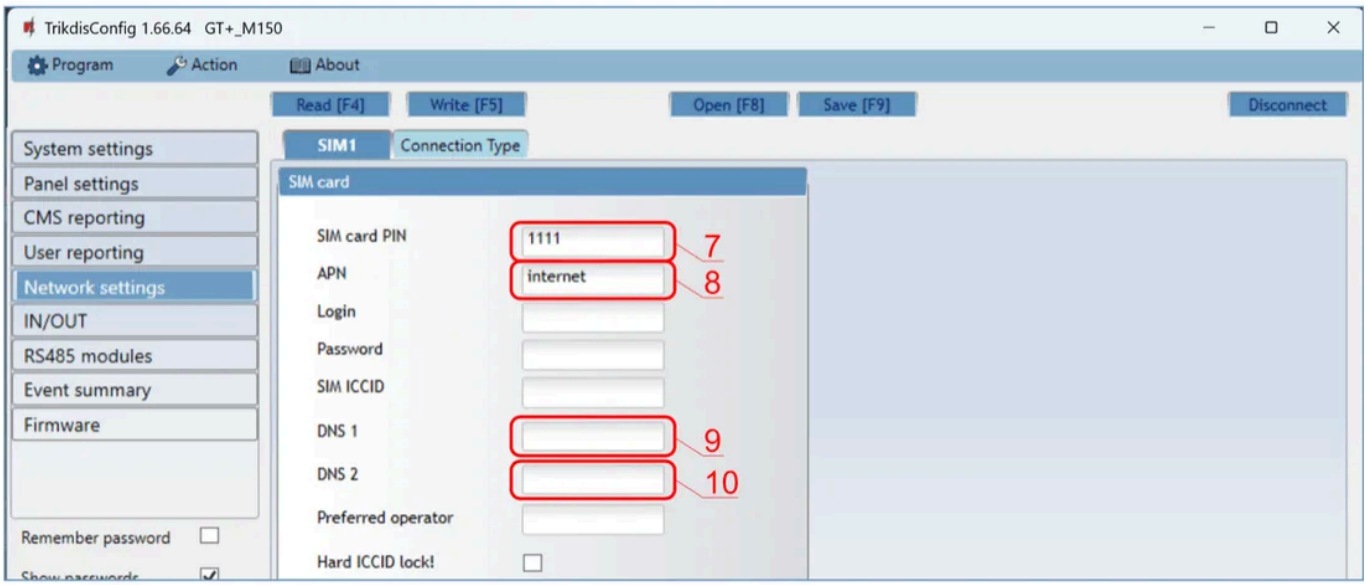
Następnie na stronie **User reporting**, na karcie **PROTEGUS Cloud**, włącz połączenie z chmurą.



Rysunek 7. TrikdisConfig – User reporting, karta PROTEGUS Cloud.

- 5 **Enable connection** – zaznacz: włącza połączenie z chmurą Protegus.
- 6 **PROTEGUS Cloud access Code** – kod dostępu do Protegus 2 (fabrycznie `123456`). Zmień go, jeśli chcesz, aby użytkownik musiał go podać przy dodawaniu systemu do aplikacji. Ważne: jeśli później zmienisz kod w TrikdisConfig, trzeba go zmienić także w aplikacji Protegus 2.

Na koniec na stronie **Network settings**, na karcie **SIM1**, podaj dane karty.



Rysunek 8. TrikdisConfig – Network settings, karta SIM1.

- 7 **SIM card PIN** – kod PIN karty (jeśli żądanie PIN jest wyłączone, może zostać wartość fabryczna).
- 8 **APN** – punkt dostępu do transmisji danych operatora (zobacz niżej).
- 9 **DNS 1** – podstawowy serwer nazw; fabrycznie DNS Google. Niezależnie od ustawień IP sprawdź, czy adresy DNS działają u twojego operatora.
- 10 **DNS 2** – zapasowy serwer nazw (fabrycznie także Google).

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

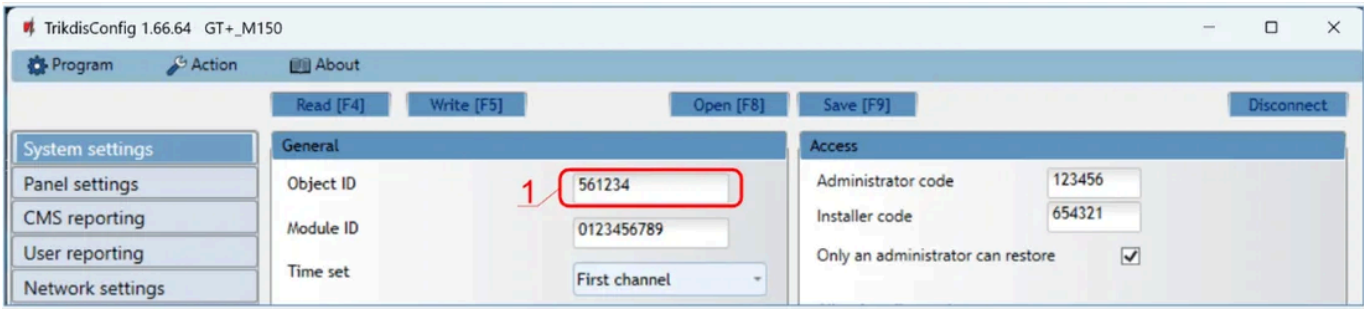
Do karty danych IoT / M2M (komunikacja między maszynami) operator zwykle podaje **inny APN niż do kart dla klientów indywidualnych** – z APN-em dla klientów indywidualnych urządzenie się nie połączy. Tę wartość także znajdziesz w artykule o APN albo poproś o nią operatora; jeśli operator podaje również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

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

Przy podłączeniu do linii telefonicznej (TIP/RING) nie zapomnij włączyć i ustawić dialera centrali alarmowej, w przeciwnym razie centrala nie wyśle żadnego zdarzenia; do sterowania bezpośredniego trzeba ustawić także centrale Paradox, Texecom, Caddx, InnerRange i Honeywell. Ustawienie centrali opisuje rozdział 4.

2.3 Połączenie ze stacją monitorowania

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

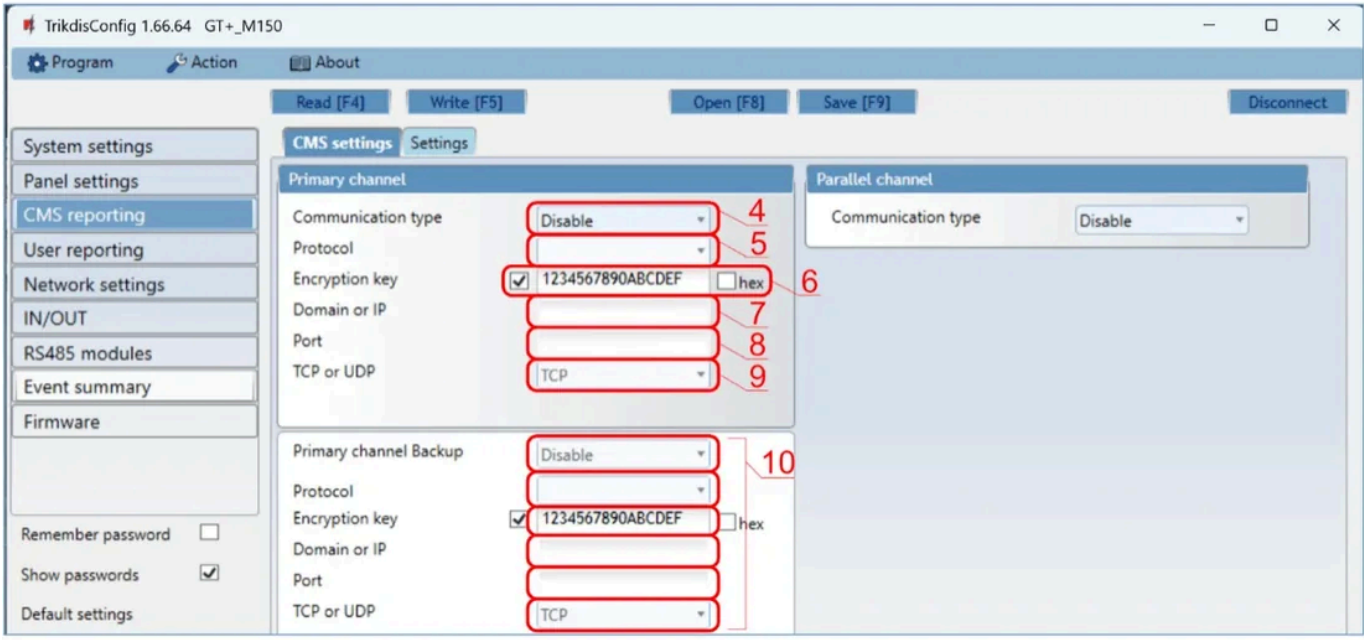


Rysunek 9. TrikdisConfig – strona System settings, grupa General.

- 1 **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (6 znaków szesnastkowych, 0–9, A–F). Nie można używać `FFFE` i `FFFF`.

Na stronie **Panel settings** podaj sposób podłączenia centrali, jeśli nie zrobiłeś tego w punkcie 2.2: przy podłączeniu TIP/RING **Communication protocol** ustaw na **AUTO** (GT: **Dual tone**); przy podłączeniu do magistrali danych lub portu szeregowego wybierz w polu **Security panel model** typ podłączonej centrali (rysunki w punkcie 2.2).

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



Rysunek 10. TrikdisConfig – CMS reporting, karta CMS settings.

- 4 **Communication type** – wybierz połączenie **IP**.
- 5 **Protocol** – **TRK8** dla odbiornika Trikdis, **DC-09_2007** lub **DC-09_2012** dla odbiornika uniwersalnego, **TL150** dla odbiornika SUR-GARD.
- 6 **Encryption key** – klucz szyfrowania ustawiony w odbiorniku.
- 7 **Domain or IP** – nazwa domeny lub adres IP odbiornika.
- 8 **Port** – numer portu odbiornika.
- 9 **TCP or UDP** – protokół transmisji; dopasuj go do ustawienia odbiornika.
- 10 **Primary channel Backup** – kanał zapasowy na wypadek awarii kanału głównego; wypełnij go tak samo, zalecamy go podać.

Na koniec na stronie **Network settings**, na karcie **SIM1**, podaj dane karty (**SIM card PIN**, **APN**, **DNS 1, DNS 2**), jeśli nie zrobiłeś tego w punkcie 2.2.

Przy protokole **DC-09** na karcie **Settings** podaj także numer linii i odbiornika (**Line No.**, **Receiver No.**, punkt 6.4). GT i GT+ raportują do stacji monitorowania tylko przez połączenie IP, nie mają zapasowego kanału SMS.

Na koniec konfiguracji naciśnij przycisk **Write [F5]** (zapis), poczekaj na potwierdzenie i odłącz kabel USB. Urządzenie jest gotowe do podłączenia. Przy podłączeniu do linii telefonicznej także tutaj trzeba włączyć i ustawić dialer centrali alarmowej, w przeciwnym razie centrala nie wyśle żadnego zdarzenia (rozdział 4).

3. Instalacja i podłączenie

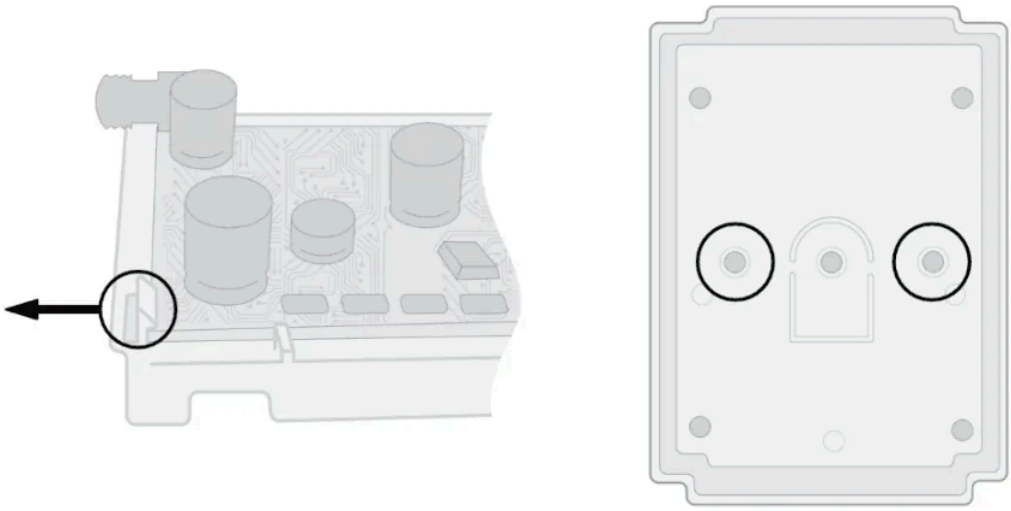
Figyelem!

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 pokrywę przednią (zobacz punkt 2.1) i zdejmij listwę zaciskową.
2. Włóż kartę nano-SIM do gniazda, jeśli nie zrobiłeś tego przy uruchamianiu.
3. Wyjmij płytkę drukowaną z podstawy obudowy: otwórz zatrzask obok złącza antenowego i wyjmij płytkę (zobacz rysunek).

4. Przykręć podstawę obudowy śrubami w wybranym miejscu (na rysunku otwory na śruby zaznaczone kółkiem).
5. Włóż płytkę drukowaną z powrotem do podstawy obudowy i ponownie podłącz listwę zaciskową.
6. Przykręć antenę komórkową.
7. Załóż pokrywę przednią.



Rysunek 11. Wyjmowanie płytki drukowanej z podstawy obudowy (po lewej: zatrzask i kierunek wyjmowania) oraz otwory na śruby w podstawie obudowy (po prawej).

Karta SIM musi być aktywna, a do pracy przez IP musi działać na niej mobilna transmisja danych. Jeśli nie chcesz, aby TrikdisConfig prosił o kod PIN, włóż kartę do telefonu komórkowego i tam wyłącz żądanie PIN.

3.2 Umiejscowienie i antena

- Komunikator umieść w **suchym miejscu wewnątrz budynku**, najlepiej w pobliżu obudowy centrali alarmowej, aby okablowanie było krótkie.
- W **metalowej obudowie** sygnał komórkowy jest mocno tłumiony. Jeśli komunikator trafi 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 w 4G musi wynosić co najmniej 3 (punkt 1.6). Jeśli jest mniejsza, poszukaj lepszego miejsca albo przejdź na czulszą antenę, którą można umieścić dalej.
- Antenę i komunikator trzymaj z dala od transformatora centrali i przewodów sieci elektrycznej.



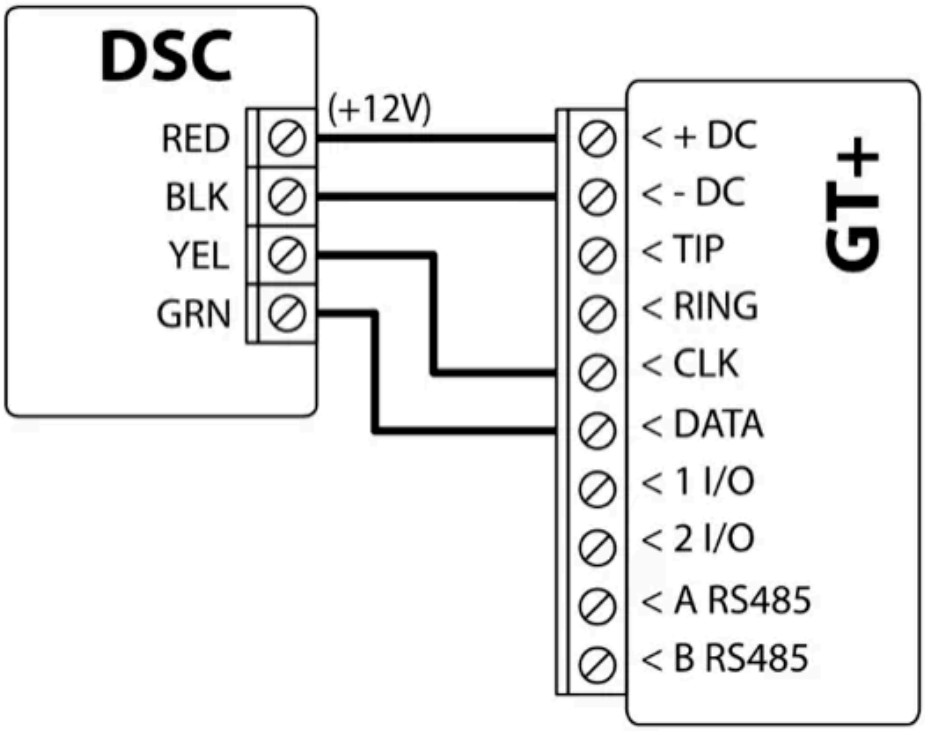
A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna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

3.3 Podłączenie do centrali alarmowej

Postępuj według tego z poniższych schematów, który pasuje do twojej centrali. Na schematach **+DC** i **–DC** to zaciski zasilania komunikatora (GT: +12 VDC / −12 VDC, GT+: +12 / 24 VDC / −12 / 24 VDC), a **A RS485** / **B RS485** to zaciski A 485 / B 485. Komunikator otrzymuje zasilanie z wyjścia zasilania pomocniczego (AUX) centrali, dzięki czemu przy zaniku zasilania akumulator centrali zasila także komunikator. Na schematach jest GT+; podłączenie GT jest takie samo.

3.3.1 DSC – magistrala danych (Keybus)

Magistralę Keybus centrali DSC podłącz do komunikatora czterema przewodami: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

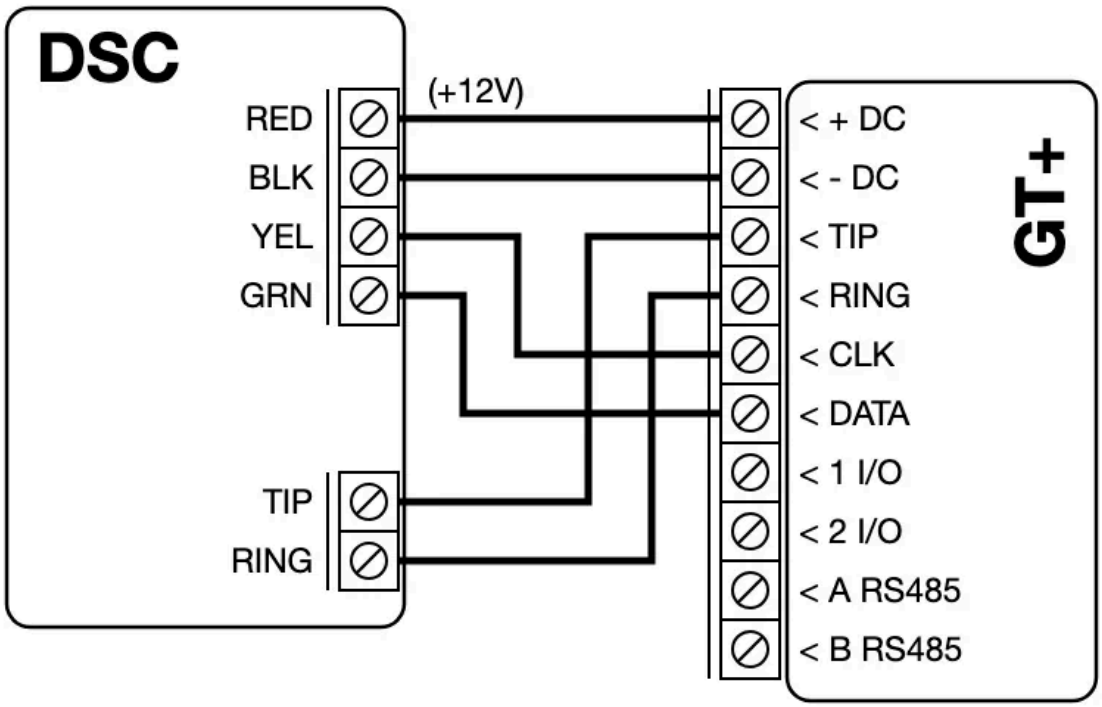


Rysunek 12. Podłączenie centrali DSC do magistrali danych (Keybus, „Keypad bus"): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Podłączony tylko do magistrali Keybus komunikator otrzymuje od centrali ogólny stan stref, ale nie zna typu strefy (pożarowa, włamaniowa, zalania itp.). Dlatego każdy alarm raportuje **jako alarm ogólny, kodem Contact ID E130**, a niektóre stacje monitorowania obsługują go inaczej niż faktycznie naruszony typ strefy. Jeśli chcesz wysyłać zdarzenia z własnymi kodami Contact ID centrali (na przykład alarm pożarowy: E110), w GT+ podłącz także zaciski TIP/RING (punkt 3.3.2).

3.3.2 DSC – Keybus i TIP/RING (tylko GT+)

GT+ można podłączyć do centrali DSC jednocześnie do magistrali danych i do wyjścia linii telefonicznej: oprócz przewodów Keybus połącz także zaciski centrali **TIP** → **TIP** i **RING** → **RING** z zaciskami komunikatora.



Rysunek 13. Podłączenie centrali DSC do magistrali danych („Keypad bus") i do zacisków TIP/RING razem (GT+): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA oraz TIP → TIP, RING → RING.

W takim przypadku Keybus służy do sterowania i odczytu stanów (zdalne uzbrajanie i rozbrajanie, stany partycji i stref), a zdarzenia wysyła dialer linii telefonicznej centrali przez zaciski TIP/RING, czyli trafiają one z własnymi kodami Contact ID centrali. Dopóki podłączenie TIP/RING działa, komunikator nie wysyła po raz drugi zdarzeń przychodzących z Keybus.

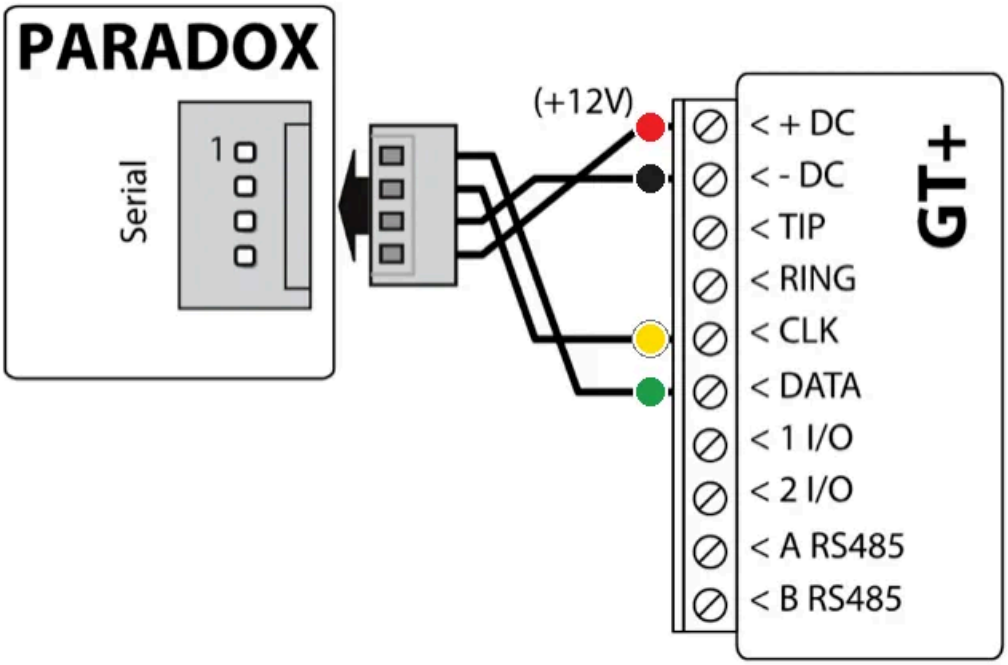
Do tego podłączenia na stronie **Panel settings** programu TrikdisConfig ustaw:

1. **Communication protocol**: **AUTO**.
2. **Security panel model**: typ centrali DSC.
3. **Remote Arm/Disarm**: zaznacz, jeśli użytkownicy chcą sterować centralą z aplikacji Protegus 2.

Trzeba też zaprogramować dialer linii telefonicznej centrali DSC, aby wysyłał zdarzenia – opisuje to punkt 4.1.1.

3.3.3 Paradox – port szeregowy

Do portu szeregowego centrali Paradox komunikator podłącza się zamawianym osobno kablem **EX-CRP2.4**: **czerwony → +DC**, **czarny → −DC**, **żółty → CLK**, **zielony → DATA**.



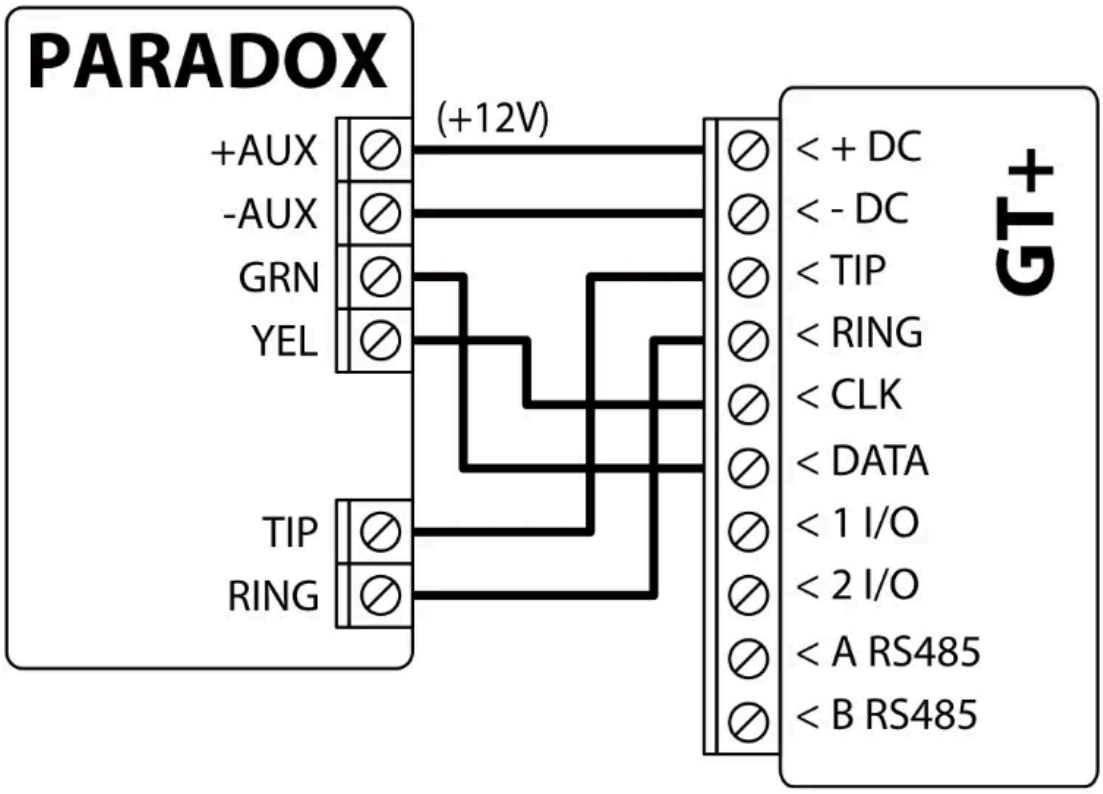
Rysunek 14. Podłączenie centrali Paradox do portu szeregowego kablem EX-CRP2.4 (do zamówienia osobno; „Use the EX-CRP2.4 cable (ordered separately)"): czerwony → +DC, czarny → −DC, żółty → CLK, zielony → DATA.

- przewód czerwony („R - red")
- przewód czarny („B - black")
- przewód żółty („Y - yellow")
- przewód zielony („G - green")

W nowszych centralach Paradox (SP+, MG+, EVOHD+) port szeregowy może być fabrycznie zablokowany; o odblokowaniu mówi punkt 4.1.2. W centralach Spectra SP / SP+ i Magellan MG / MG+ zamiast portu szeregowego można użyć także podłączenia z następnego punktu.

3.3.4 Paradox SP/MG – Keybus i TIP/RING

Centralę Paradox Spectra SP, SP+ oraz Magellan MG, MG+ można zamiast portu szeregowego podłączyć do jej magistrali danych (Keybus) i zacisków TIP/RING razem: **+AUX → +DC**, **−AUX → −DC**, **GRN → DATA**, **YEL → CLK** oraz **TIP → TIP**, **RING → RING**. To podłączenie korzysta z magistrali Keybus centrali zamiast portu szeregowego, dlatego nie jest do niego potrzebne płatne odblokowanie portu szeregowego Paradox.



Rysunek 15. Podłączenie centrali Paradox SP / SP+ / MG / MG+ do magistrali Keybus (magistrala danych, „Keypad bus") i do zacisków TIP/RING razem: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Do tego podłączenia firmware komunikatora musi mieć wersję co najmniej **1.21** (aktualizację opisuje rozdział 9).

Do tego podłączenia na stronie **Panel settings** programu TrikdisConfig ustaw:

1. **Communication protocol**: **AUTO** (GT: **Dual tone**).
2. **Security panel model**: **7. Paradox SP+/MG+ series KeyBus**.
3. **Remote Arm/Disarm**: zaznacz, jeśli użytkownicy chcą sterować centralą z aplikacji Protegus 2 własnym kodem klawiatury.
4. **Security panel PC download password**: do sterowania bezpośredniego podaj hasło PC ustawione w centrali; oba muszą być takie same.

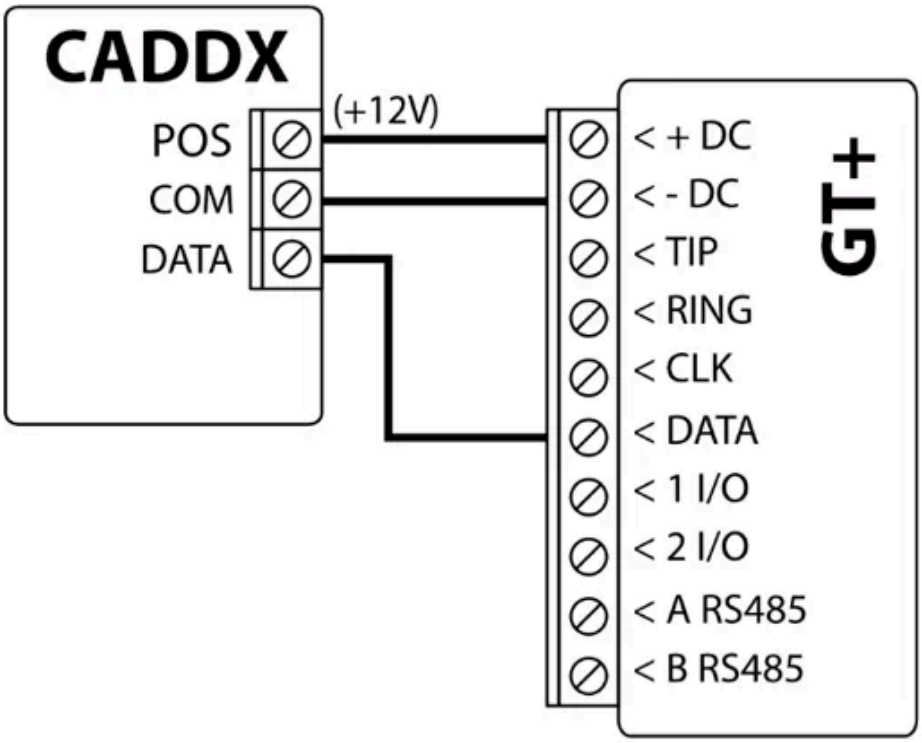


Rysunek 16. TrikdisConfig – Panel settings dla podłączenia Keybus + TIP/RING: Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm zaznaczone, PC download password podane.

Centralę Paradox też trzeba zaprogramować, aby wysyłała zdarzenia do stacji monitorowania i aby można nią było sterować z Protegus 2 – opisuje to punkt 4.1.2.

3.3.5 UTC Interlogix (Caddx) – magistrala danych

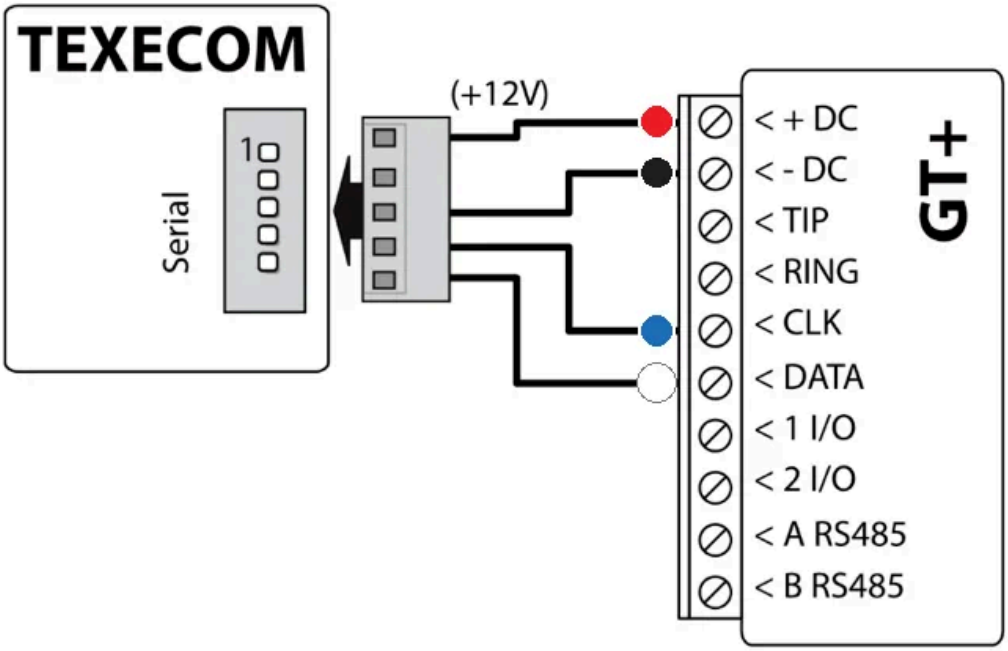
Magistralę danych centrali Caddx NetworX podłącz do komunikatora trzema przewodami: **POS** → **+DC**, **COM** → **–DC**, **DATA** → **DATA**. Zaciski TIP, RING i CLK nie są potrzebne.



Rysunek 17. Podłączenie centrali UTC Interlogix (Caddx) NetworX do magistrali danych („Keypad bus"): POS → +DC, COM → −DC, DATA → DATA.

3.3.6 Texecom – port szeregowy

Do portu szeregowego centrali Texecom Premier / Premier Elite komunikator podłącza się zamawianym osobno kablem **EX-CRP4**: **czerwony** → **+DC**, **czarny** → **–DC**, **niebieski** → **CLK**, **biały** → **DATA**.

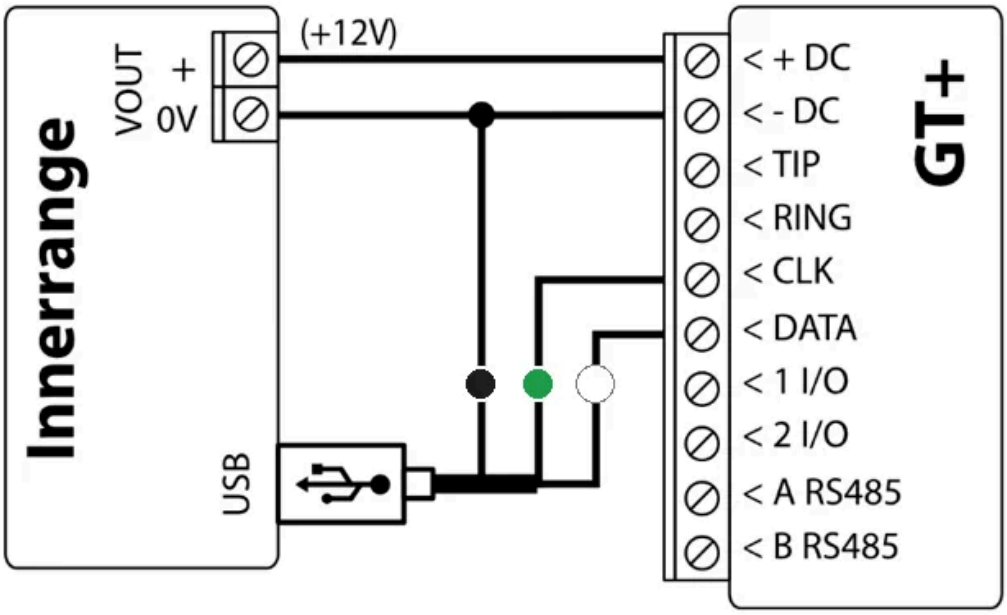


Rysunek 18. Podłączenie centrali Texecom do portu szeregowego kablem EX-CRP4 (do zamówienia osobno; „Use the EX-CRP4 cable (ordered separately)"): czerwony → +DC, czarny → −DC, niebieski → CLK, biały → DATA.

- przewód czerwony („R - red")
- przewód czarny („B - black")
- przewód niebieski („BL - blue")
- przewód biały („W - white")

3.3.7 InnerRange Inception

Komunikator otrzymuje zasilanie z wyjścia zasilania centrali Inception (**VOUT +** → **+DC**, **VOUT 0V** → **−DC**), a połączenie danych idzie z portu USB centrali, kablem Inner Range **993030USB**: **czarny** → **0V / −DC**, **zielony** → **CLK**, **biały** → **DATA**.

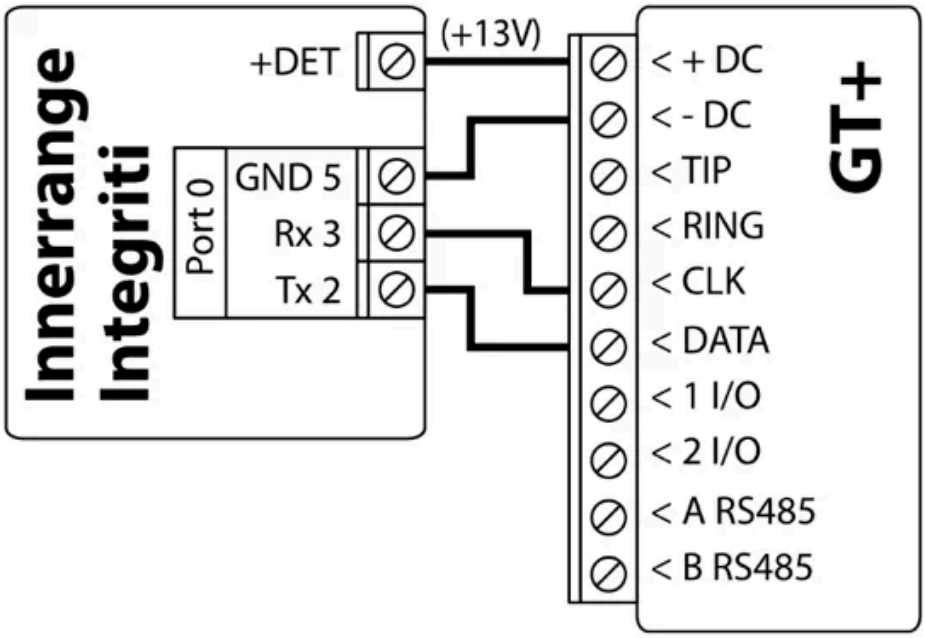


Rysunek 19. Podłączenie InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; z portu USB kablem 993030USB („Cable, Inner Range part number 993030USB") czarny → −DC, zielony → CLK, biały → DATA.

- przewód czarny („Black wire")
- przewód zielony („Green wire")
- przewód biały („White wire")

3.3.8 InnerRange Integriti

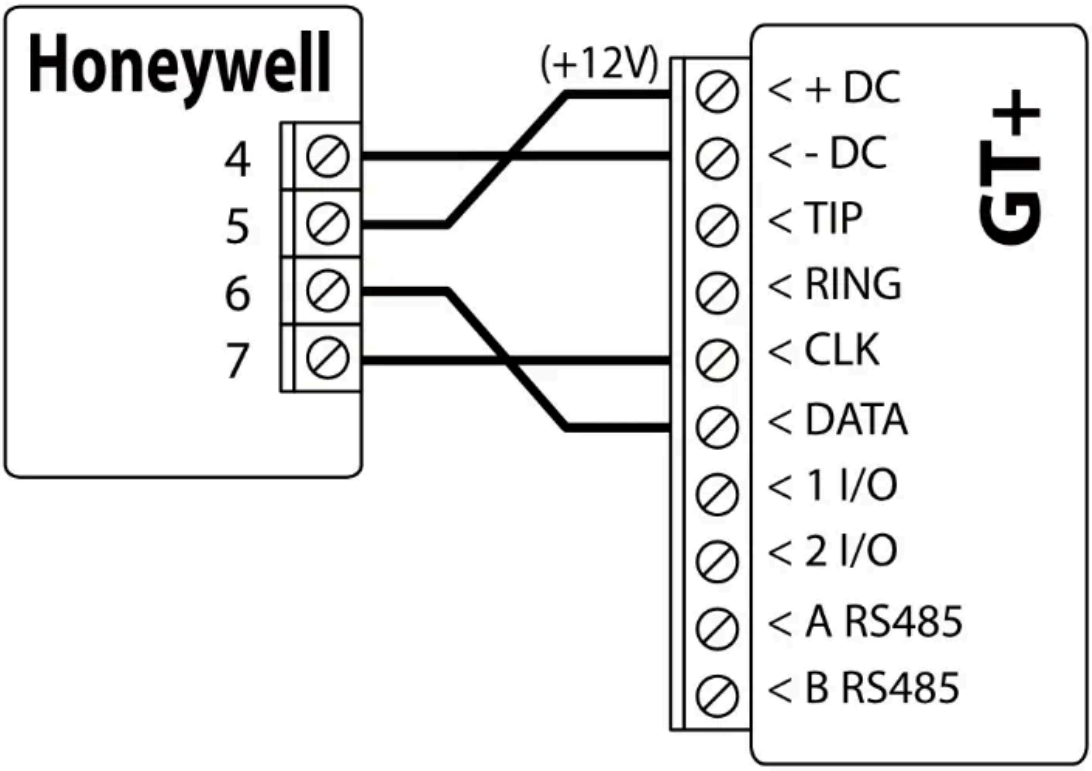
Do portu szeregowego **Port 0** centrali Integriti komunikator podłącza się kablem Inner Range **INTG-996795**: **+DET (+13 V) → +DC**, **GND (5) → −DC**, **Rx (3) → CLK**, **Tx (2) → DATA**.



Rysunek 20. Podłączenie InnerRange Integriti do Port 0 kablem INTG-996795 („Cable, Inner Range part number INTG-996795"): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – magistrala danych

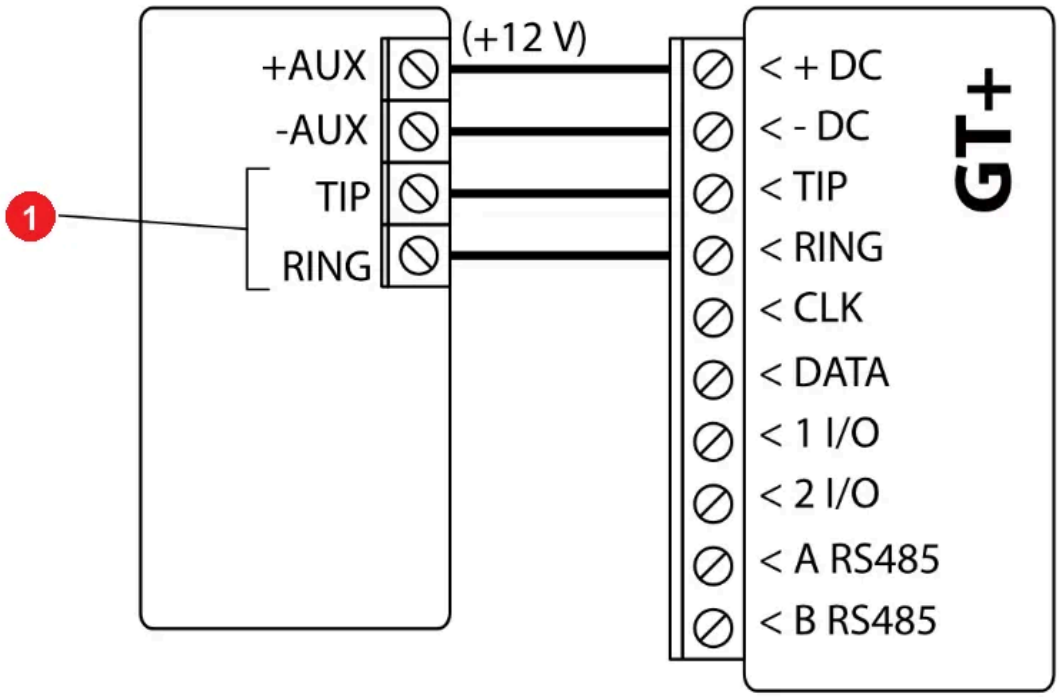
Magistralę klawiatur centrali Honeywell Ademco Vista-15, Vista-20 i Vista-48 podłącz do komunikatora z zacisków centrali: **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.



Rysunek 21. Podłączenie centrali Honeywell Vista-15 / -20 / -48 do magistrali danych („Keypad bus"): zacisk 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.10 Dowolna centrala – TIP/RING

Każdą inną centralę można podłączyć przez jej komunikator linii telefonicznej: zasilanie z wyjścia zasilania pomocniczego centrali (**+AUX** → **+DC**, **−AUX** → **−DC**), wyjście linii telefonicznej do zacisków **TIP** i **RING** komunikatora (**TIP** → **TIP**, **RING** → **RING**). Trzeba ustawić dialer centrali (punkt 4.2).



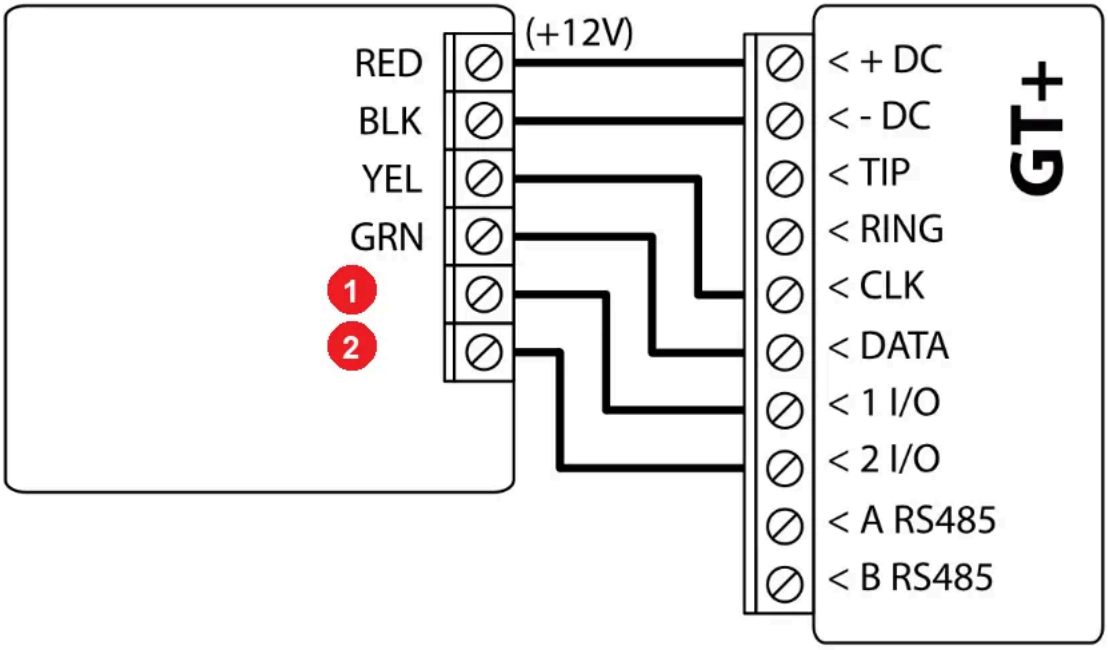
Rysunek 22. Podłączenie do komunikatora linii telefonicznej centrali („Control panel"): +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

- 1 zaciski komunikatora linii telefonicznej centrali („Telephone line communicator terminals")

3.4 Podłączenie strefy przełącznika kluczowego

Jeśli chcesz uzbrajać i rozbrajać centralę z aplikacji Protegus 2 w taki sposób, że wyjście komunikatora (PGM) przełącza **strefę przełącznika kluczowego** centrali, postępuj według tego podłączenia. Dwa zaciski I/O o podwójnej funkcji komunikatora można ustawić jako wyjścia (OUT, PGM), dzięki czemu dwa wyjścia mogą sterować dwiema partycjami systemu: strefę przełącznika kluczowego 1. partycji podłącz do zacisku **1 I/O**, a 2. partycji do zacisku **2 I/O**. Przy takim podłączeniu na stronie **Panel settings** programu TrikdisConfig odznacz **Remote Arm/Disarm**, zaciski na stronie **IN/OUT** ustaw na funkcję **OUT** (punkt 6.7), a w aplikacji Protegus 2 przypisz wyjścia do partycji według punktu 5.2.

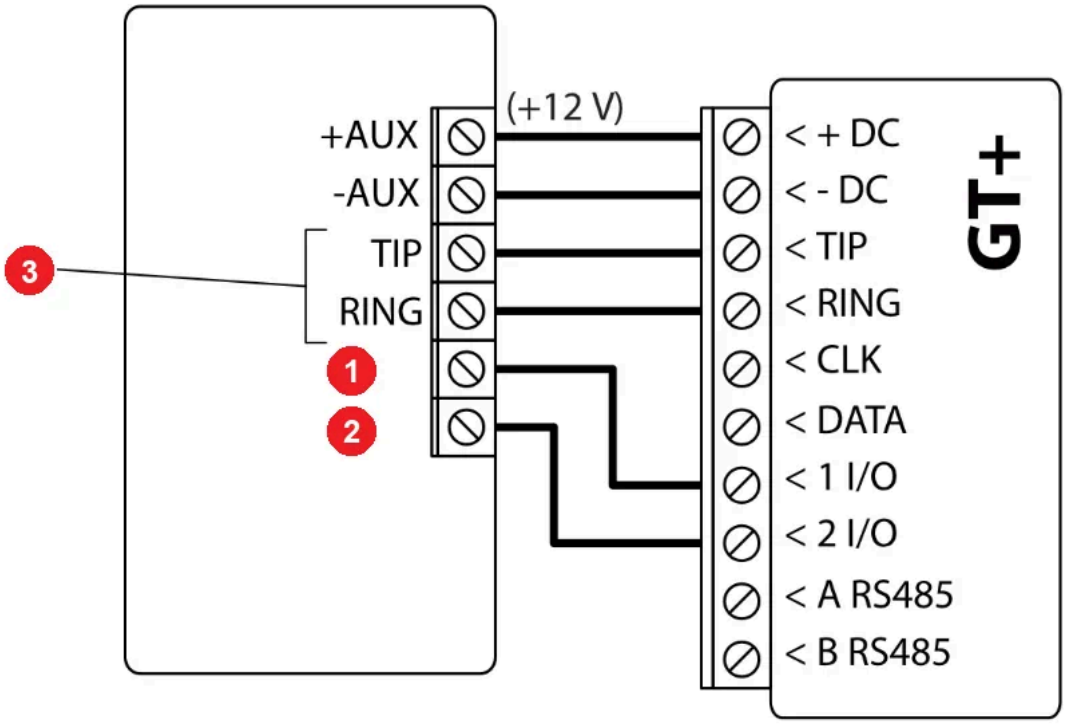
Przy podłączeniu do magistrali danych lub portu szeregowego połączenie danych między centralą a komunikatorem pozostaje (komunikator odczytuje zdarzenia z magistrali), a uzbrajanie i rozbrajanie odbywa się przez strefę przełącznika kluczowego:



Rysunek 23. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego („Zones (keyswitch)") przy podłączeniu do magistrali danych lub portu szeregowego („Keypad bus or serial"): zacisk RED centrali alarmowej („Control panel terminals") → +DC, BLK → −DC, YEL → CLK, GRN → DATA; strefa 1. partycji → 1 I/O, strefa 2. partycji → 2 I/O.

- 1 strefa przełącznika kluczowego 1. partycji („1-st Area")
- 2 strefa przełącznika kluczowego 2. partycji („2-nd Area")

Przy podłączeniu do linii telefonicznej (TIP/RING) centrala wysyła zdarzenia swoim dialerem, a uzbrajanie i rozbrajanie odbywa się tak samo przez strefę przełącznika kluczowego:



Rysunek 24. Uzbrajanie i rozbrajanie strefą przełącznika kluczowego („Zone (keyswitch)") przy podłączeniu do linii telefonicznej: zacisk +AUX centrali alarmowej („Control panel") → +DC, −AUX → −DC, TIP → TIP, RING → RING; strefa 1. partycji → 1 I/O, strefa 2. partycji → 2 I/O.

- 1 strefa przełącznika kluczowego 1. partycji („1-st Area")
- 2 strefa przełącznika kluczowego 2. partycji („2-nd Area")
- 3 zaciski komunikatora linii telefonicznej centrali („Telephone line communicator terminals")

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

3.5 Podłączenie wejść

Dwa zaciski I/O o podwójnej funkcji komunikatora jako wejścia (IN) można wykorzystać także do podłączenia dodatkowych czujników (np. styku sabotażowego, przycisku napadowego), niezależnie od centrali alarmowej. Do wejścia można podłączyć obwód NO, NC, NO/EOL, NC/EOL, NO/DEOL lub NC/DEOL; ustawienie fabryczne obu zacisków to wejście, NO. Typ wejścia ustawiasz na stronie **IN/OUT** programu TrikdisConfig, w polu **Type**. Wejście trzeba podłączyć między wybrany zacisk I/O a zacisk **−DC** (COM), zgodnie z wybranym typem.

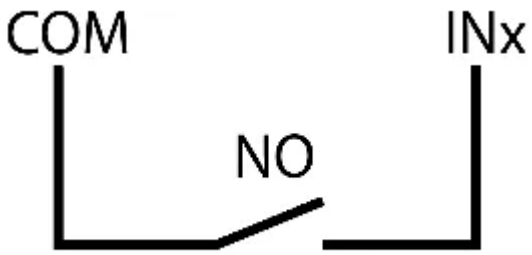
Wejścia obsługują następujące typy obwodów: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Rezystor końca linii ma wartość **2,2 kΩ**. Przy pojedynczej parametryzacji (EOL) zarówno zwarcie, jak i przerwa są traktowane jako alarm; podwójna parametryzacja (DEOL) z dwoma rezystorami rozróżnia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

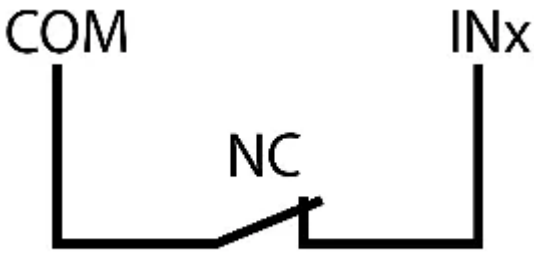
Typ	Stan spoczynkowy	Alarm	Sabotaż
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	przerwa lub zwarcie
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	przerwa lub zwarcie

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**.

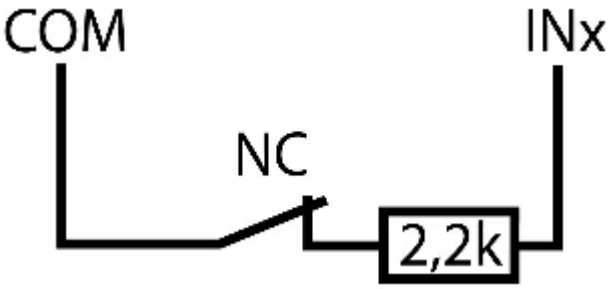
Podłączenie obwodów wejściowych między punkt COM a INx: NO, NC, NC/EOL, NO/EOL oraz z wykrywaniem sabotażu NO/DEOL i NC/DEOL, z rezystorami końcowymi 2,2 kΩ; poszczególne stany (zwarcie, przerwa, 2,2 kΩ, 3,3–5,5 kΩ) objaśnia tabela w punkcie 3.5.



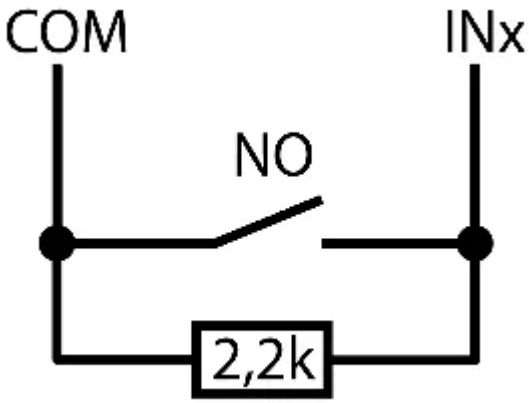
Rysunek 25. NO – obwód normalnie otwarty: zamknięty – alarm, otwarty – stan spoczynku.



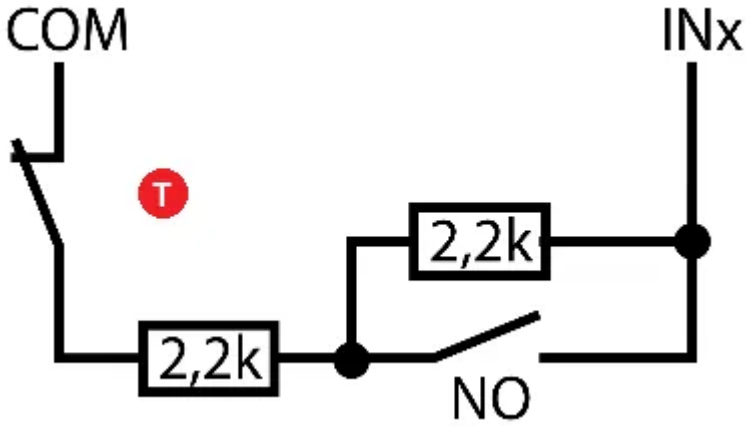
Rysunek 26. NC – obwód normalnie zamknięty: otwarty – alarm, zamknięty – stan spoczynku.



Rysunek 27. NC/EOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynku.

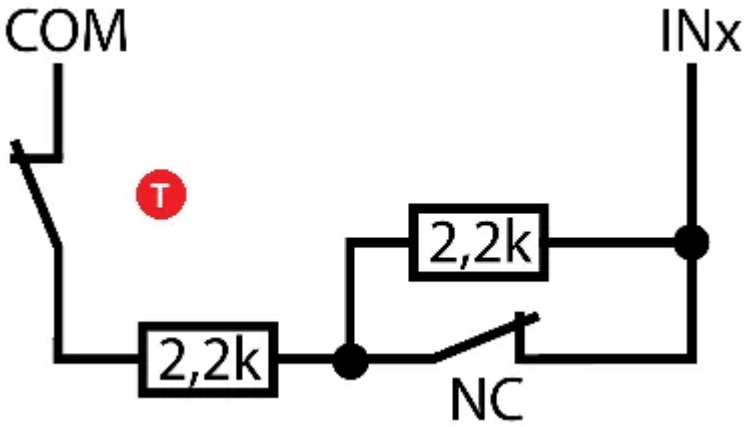


Rysunek 28. NO/EOL – obwód normalnie otwarty z rezystorem końcowym 2,2 kΩ: zwarcie lub przerwa – alarm, 2,2 kΩ – stan spoczynku.



Rysunek 29. 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 spoczynku.

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



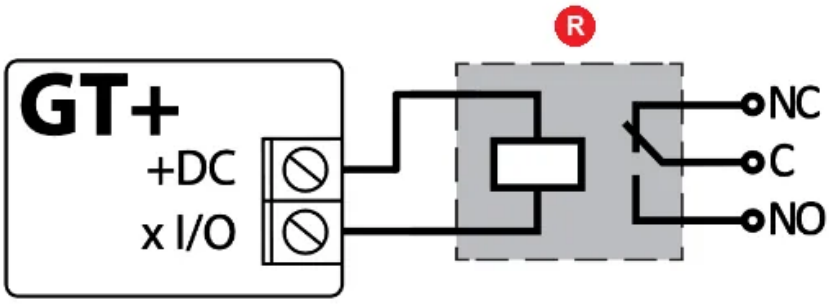
Rysunek 30. NC/DEOL – obwód normalnie zamknięty z rezystorem końcowym 2,2 kΩ i wykrywaniem sabotażu: zwarcie lub przerwa – sabotaż, 2,2 kΩ – stan spoczynku, 3,3–5,5 kΩ – alarm.

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

Jeśli potrzeba więcej wejść lub wyjść, podłącz do komunikatora ekspander Trikdis **iO-8** (punkt 3.7); jego podłączenie opisuje także instrukcja iO-8.

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 najwyżej 0,15 A, do 30 V DC. Stykami przekaźnika możesz włączać i wyłączać różne urządzenia elektryczne: jeden koniec cewki przekaźnika trafia na **+DC**, drugi na zacisk **x I/O**, a odbiornik przełączają styki przekaźnika (NC, C, NO). Używany zacisk I/O trzeba na stronie **IN/OUT** programu TrikdisConfig ustawić jako wyjście (**OUT**).



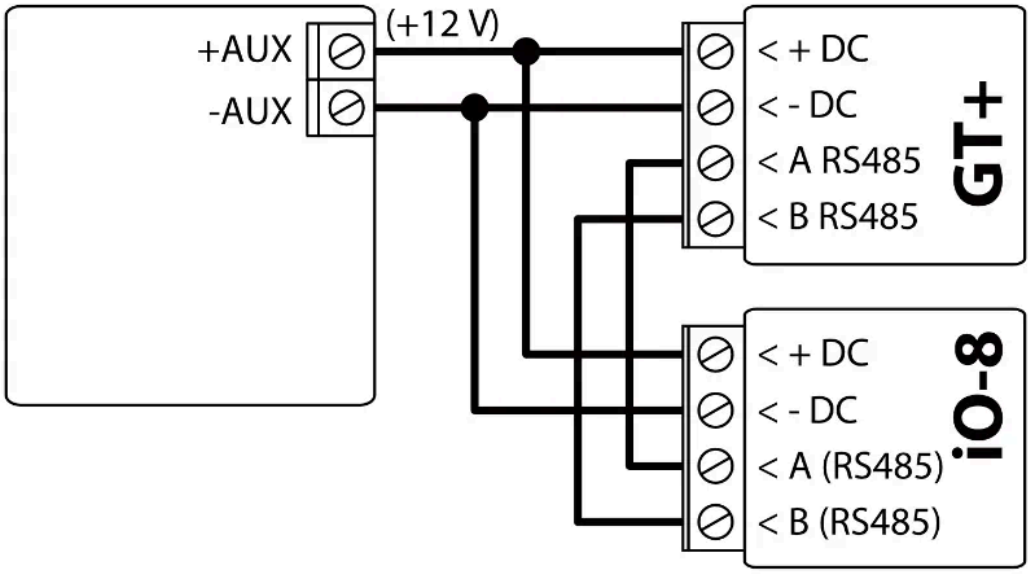
Rysunek 31. Podłączenie przekaźnika do wyjścia komunikatora: cewka trafia między +DC a zacisk x I/O, styki (NC, C, NO) przełączają odbiornik.

- R przekaźnik („Relay")

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 komunikatora 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 (RS485)** i **B (RS485)** modułu; zasilanie zarówno komunikator, jak i ekspander otrzymują z wyjścia zasilania pomocniczego centrali (**+AUX** → **+DC**, **−AUX** → **−DC** w obu urządzeniach). Ekspander trzeba dodać i ustawić na stronie **RS485 modules** programu TrikdisConfig (punkt 6.8).



Rysunek 32. Podłączenie ekspandera iO-8 do magistrali RS485 komunikatora; zasilanie z wyjścia AUX centrali alarmowej („Control panel"), dla obu urządzeń.

3.8 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 zasilania centrali alarmowej. Na pokrywie przedniej powinieneś zobaczyć:

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

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

4. Programowanie centrali alarmowej

Ustawienie centrali zależy od tego, jak ją podłączyłeś: do magistrali danych lub portu szeregowego (punkt 4.1) albo przez jej komunikator linii telefonicznej, do zacisków TIP/RING (punkt 4.2). W GT+ przy podłączeniu DSC Keybus + TIP/RING potrzebne są oba: ustawienia podłączenia do Keybus i zaprogramowanie dialera centrali (punkt 4.1.1).

4.1 Podłączenie do magistrali danych lub portu szeregowego

Tu opisujemy, jak ustawić centralę, aby komunikator odczytywał jej zdarzenia i mógł nią zdalnie sterować. Do zdalnego sterowania na stronie **Panel settings** programu TrikdisConfig opcja **Remote Arm/Disarm** musi być zaznaczona (punkt 2.2).

4.1.1 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.

GT+, podłączenie Keybus i TIP/RING (punkt 3.3.2): dialer linii telefonicznej centrali trzeba zaprogramować, aby wysyłał zdarzenia. Poniższa tabela dotyczy centrali DSC PowerSeries PC1616 (PC1832, PC1864). Na klawiaturze podłączonej do centrali wejdź w programowanie: **[*][8][kod instalatora]**, a następnie podaj numer sekcji.

Sekcja	Wartość
[301] Pierwszy numer telefonu	Dowolny numer dłuższy niż cztery cyfry, na początku **bez D** (na przykład `5555555`). D oznacza czekanie na sygnał zgłoszenia; bez niego centrala wybiera szybciej. Komunikator odbiera każde połączenie
[310] Identyfikator obiektu systemu	4-cyfrowy identyfikator obiektu, po nim `FF` (na przykład `1234FF`). Zamiast cyfry 0 użyj HEX `A`
[311] Identyfikator obiektu 1. partycji	4-cyfrowy identyfikator obiektu; zamiast 0 HEX `A`
[350] Format komunikatora	`03` (Contact ID) dla 1. numeru telefonu
[351]–[376] Kierunki wywołań	Włącz dla 1. numeru telefonu potrzebne grupy zdarzeń: Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Grupę Opening/Closing sprawdź osobno: w niektórych centralach DSC jest fabrycznie wyłączona
[380] 1. opcja komunikatora	Opcja 1 **WŁ.** (komunikator włączony); opcja 3 **WYŁ.** (wybieranie DTMF)
[381] 2. opcja komunikatora	Opcja 7 **WYŁ.** (kody raportowania Contact ID centrala tworzy automatycznie)
[320]–[349] Kody raportowania	Dla raportowanych zdarzeń dowolna wartość, byle nie `00`
[015] 3. opcja systemowa	Opcja 7 **WYŁ.** (nadzór linii telefonicznej, TLM, wyłączony)

Wyłącz nadzór linii telefonicznej (TLM): jeśli pozostanie włączony, centrala może zgłaszać usterkę linii telefonicznej. Opóźnienie usterki TLM ustawiasz w sekcji **[377]**.

Powyższe numery sekcji dotyczą central PC1616, PC1832 i PC1864 (instrukcja instalacji v4.x). W innych typach DSC numery sekcji mogą się różnić – sprawdź instrukcję programowania centrali.

4.1.2 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.

W komunikatorach GT i GT+ pole **Security panel PC download password** znajduje się na stronie **Panel settings** programu TrikdisConfig, w grupie **Serial bus** (punkty 2.2 i 6.3).

Podłączenie Keybus i TIP/RING (SP / SP+ / MG / MG+, punkt 3.3.4): centralę trzeba ponadto zaprogramować tak, aby wysyłała zdarzenia do stacji monitorowania i aby można nią było sterować z Protegus 2:

Sekcja	Wartość	Sekcja	Wartość
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

4.1.3 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]**.

W komunikatorach GT i GT+ pole **Security panel PC download password** znajduje się na stronie **Panel settings** programu TrikdisConfig, w grupie **Serial bus**; UDL passcode musi być z nim zgodny.

4.1.4 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.

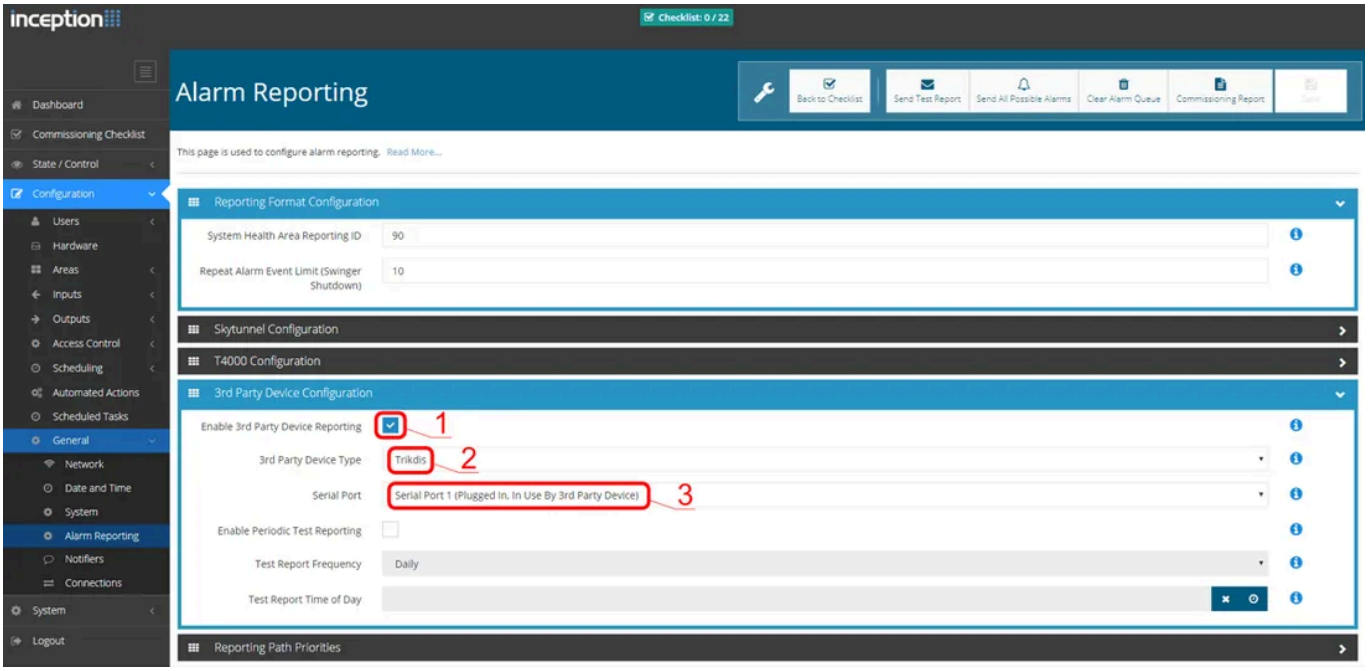
4.1.5 InnerRange

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.



Rysunek 33. InnerRange Inception – Configuration → General → Alarm Reporting, grupa 3rd Party Device Configuration: Enable 3rd Party Device Reporting zaznaczone, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 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]**.

4.2 Podłączenie do linii telefonicznej (TIP/RING)

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.

Centrale DSC, Paradox, Caddx, Texecom, InnerRange i Honeywell można podłączyć do komunikatora także przez ich wyjście linii telefonicznej (punkt 3.3.10) – wtedy także w nich trzeba ustawić dialer, a sterowanie bezpośrednie nie jest dostępne.

4.2.1 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`.

4.2.2 Dialer UTC Interlogix (Caddx) NX

Programowanie centrali Interlogix NX-4V2 (NX-6V2, NX-8V2), jeśli komunikator jest podłączony do zacisków TIP/RING centrali. Na klawiaturze wpisz kolejno:

Lokalizacja (location)	Klawisze	Uwagi
	`*89713`	Wejście w programowanie (`9713` to fabryczny kod instalatora)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Świecą wszystkie diody stref (1. segment)
Location 4	`12345678*`	Świecą wszystkie diody stref (2. segment)
Location 4	`12345678*#`	
Location 23	`23#`	Świecą wszystkie diody stref (3. segment)
Location 23	`**`	Świecą wszystkie diody stref (3. segment)
Location 23	`12345678*#`	Świecą wszystkie diody stref (3. segment)
Location 37	`37#`	Świecą wszystkie diody stref (3. segment)
Location 37	`**`	Świecą wszystkie diody stref (4. segment)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT EXIT`	Wyjście z programowania

5. Zdalne sterowanie aplikacją Protegus 2

Aplikacją mobilną i webową Protegus 2 użytkownik zdalnie widzi stan systemu, otrzymuje powiadomienia o zdarzeniach, może uzbrajać i rozbrajać system oraz przełączać wyjścia komunikatora. Aplikację można pobrać na Androida i iOS (Google Play, App Store) albo używać jej w przeglądarce: web.protegus.app. Zaloguj się swoją nazwą użytkownika i hasłem albo zarejestruj nowe konto.

5.1 Dodawanie urządzenia

Przed dodaniem urządzenia sprawdź:

1. Karta SIM jest aktywna i działa na niej mobilna transmisja danych; jej kod PIN jest podany w urządzeniu albo żądanie PIN jest wyłączone.
2. Na karcie **User reporting** → **PROTEGUS Cloud** programu TrikdisConfig zaznaczone jest **Enable connection** (punkt 6.5).

3. Dioda **POWER** świeci na zielono.
4. Dioda **NETWORK** świeci na zielono i miga na żółto (urządzenie jest w sieci).

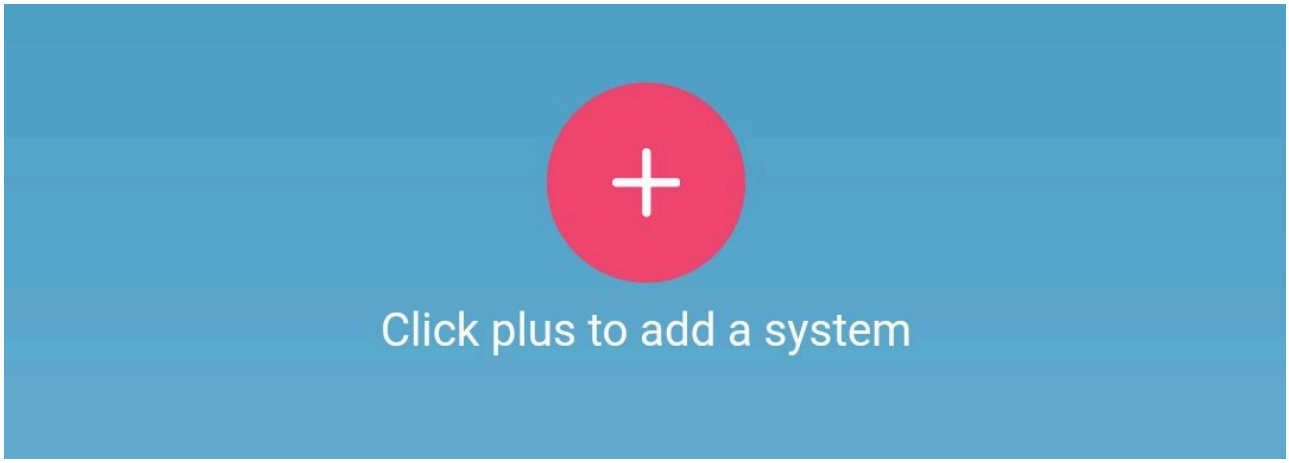
Dioda DATA to najprostszy test internetu. Dioda DATA świeci, gdy w pamięci urządzenia jest komunikat oczekujący na wysłanie. Zielona dioda NETWORK mówi tylko tyle, że połączenie sieciowe zostało nawiązane – urządzenie z siecią komórkową zalogowało się do sieci operatora, a w urządzeniu z Ethernetem połączenie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



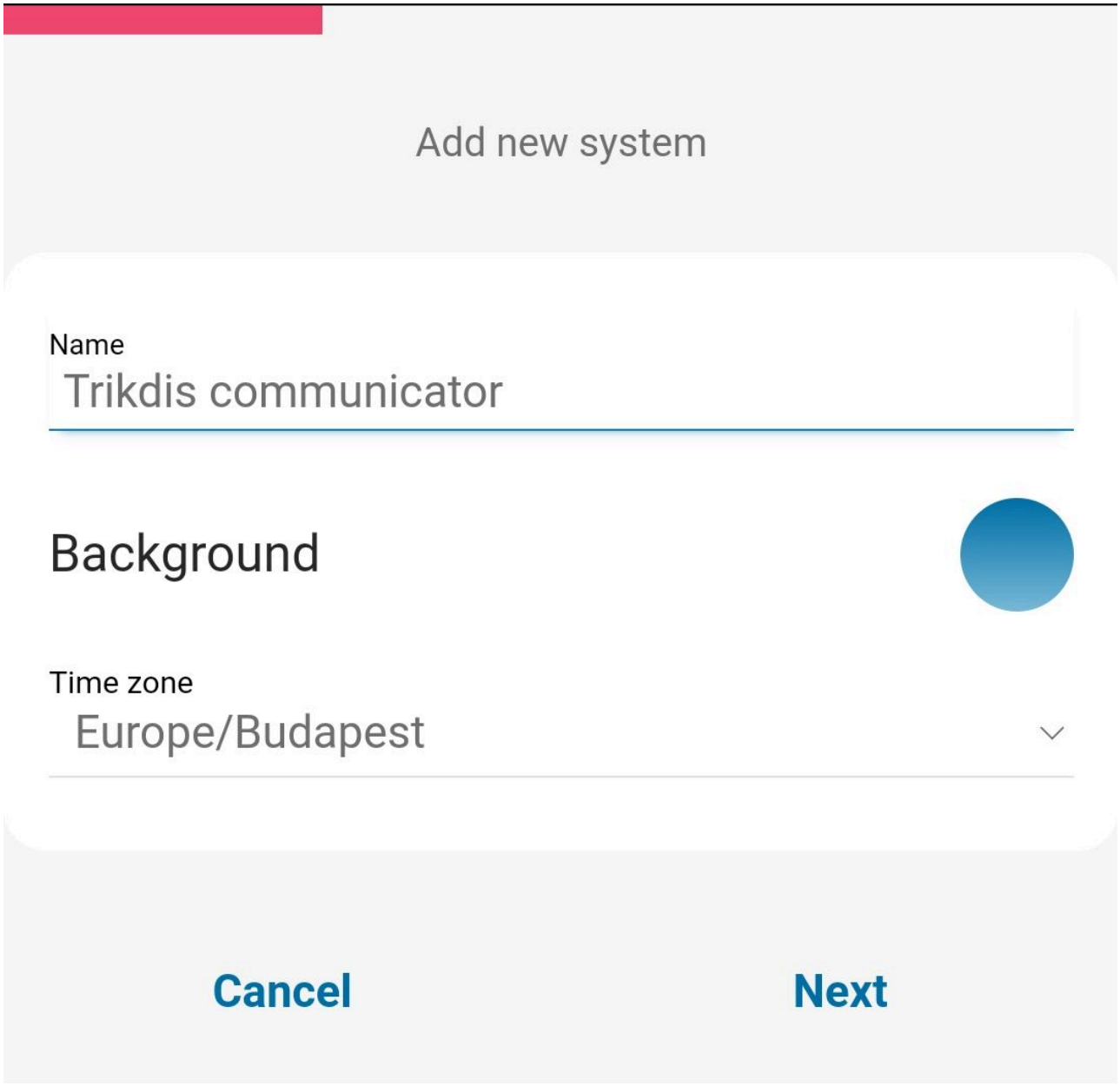
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



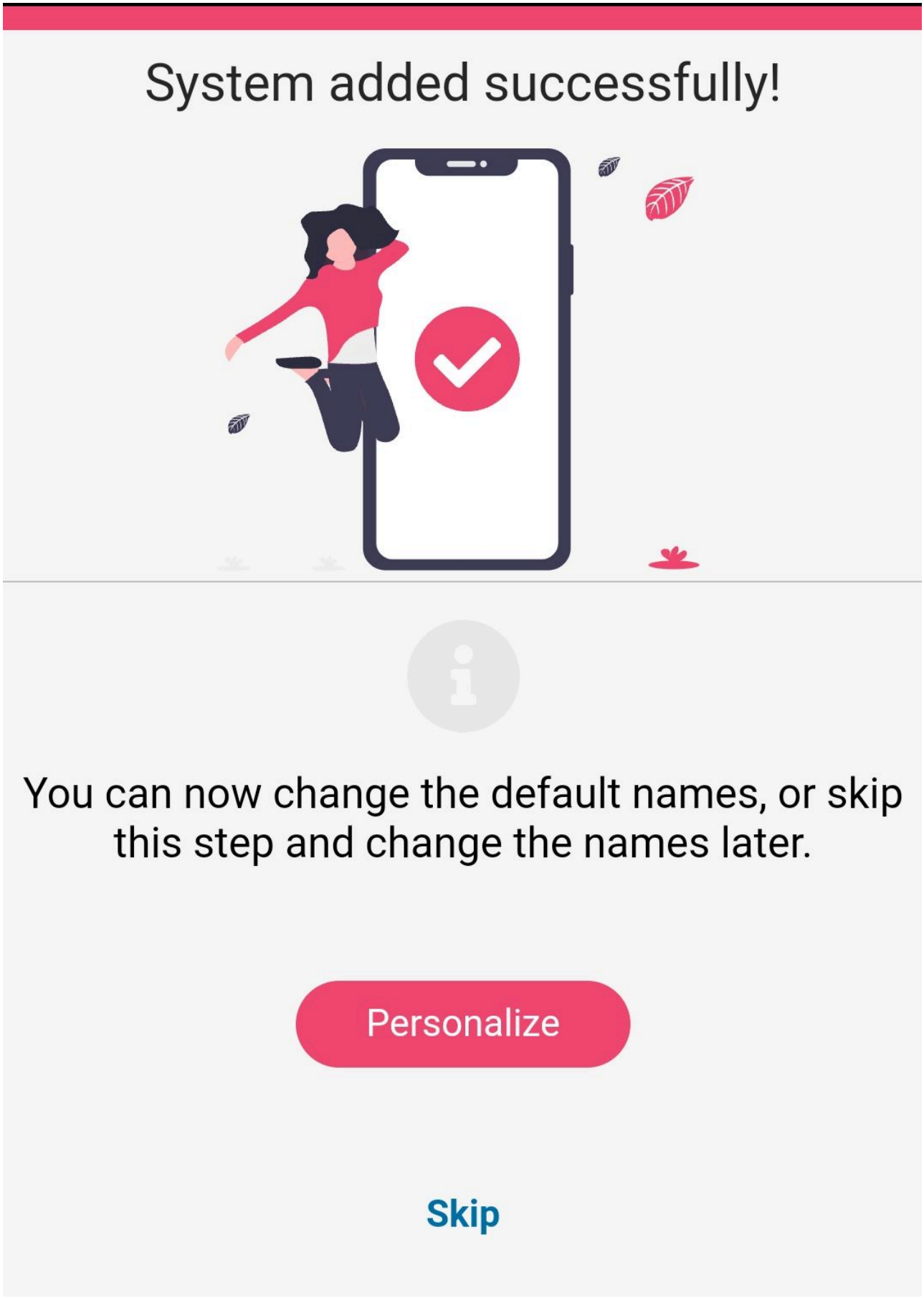
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matrican
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



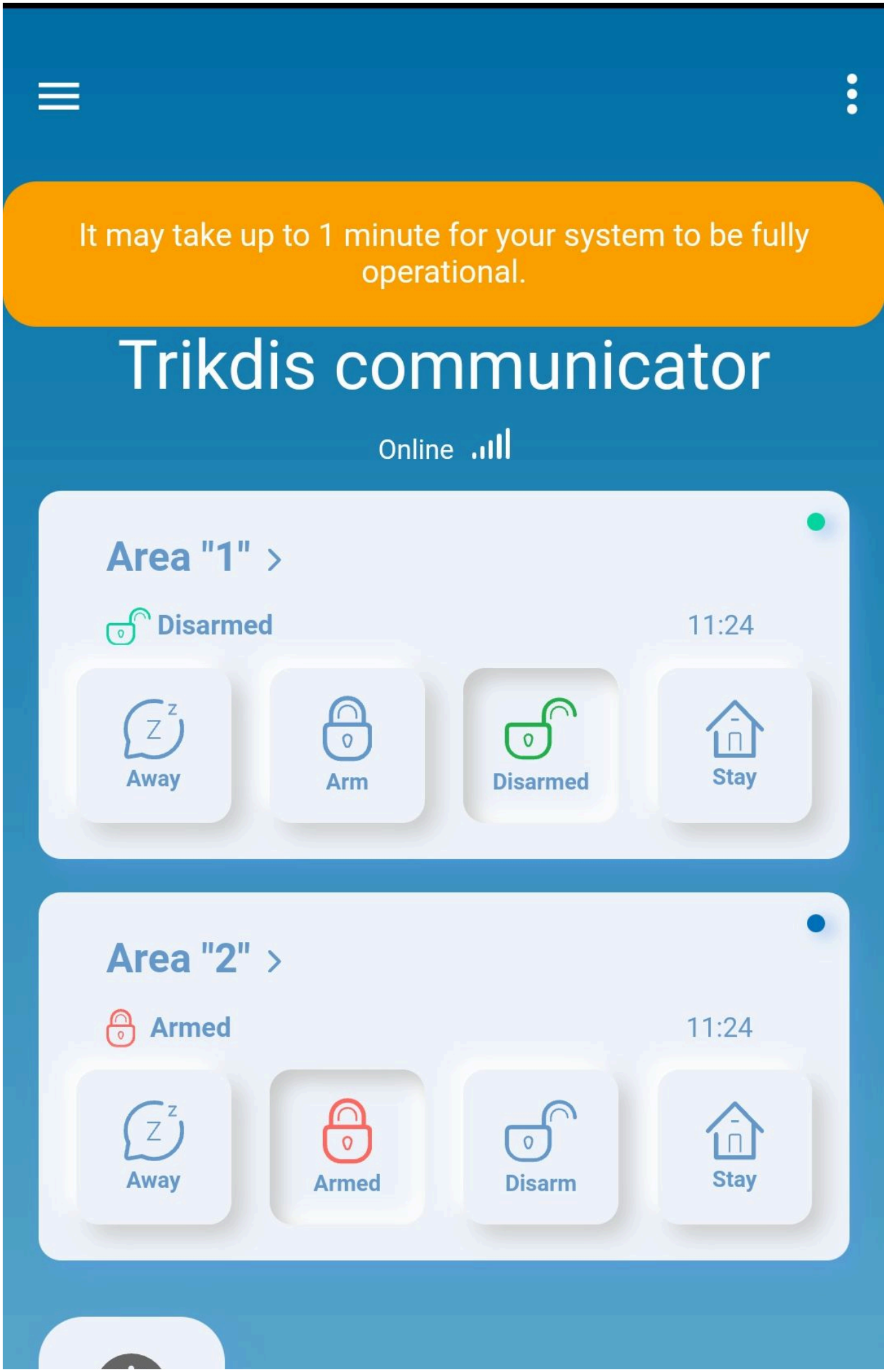
6. Add meg a rendszer nevét és válassz idozónát

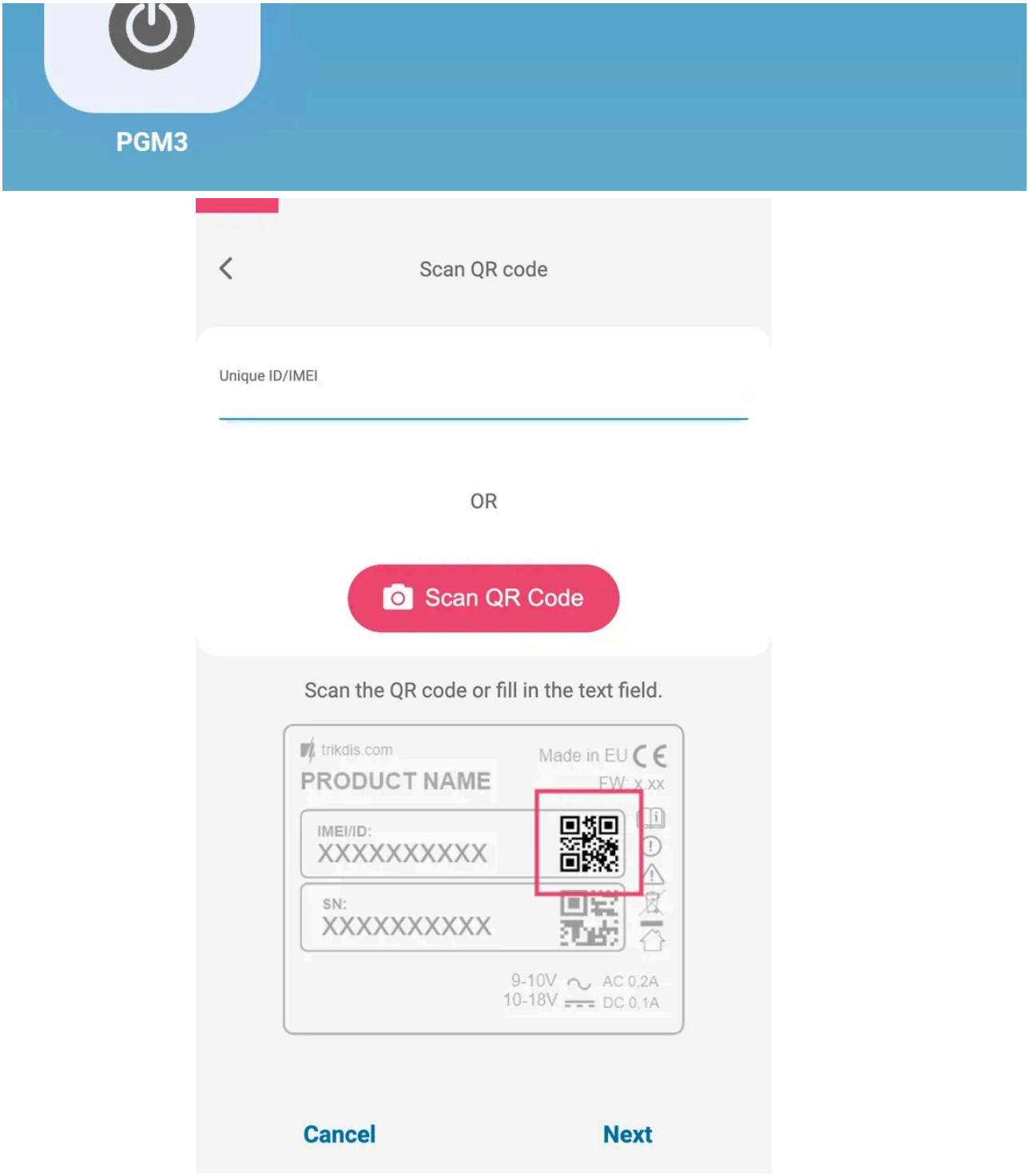


7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.

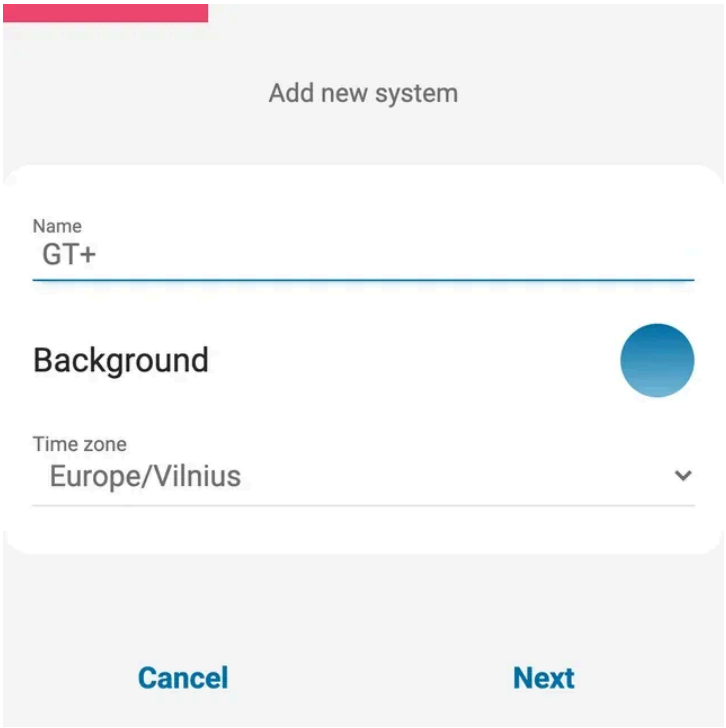


8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


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



Rysunek 34. Protegus 2 – dodawanie nowego systemu: wpisanie IMEI / Unique ID lub zeskanowanie kodu QR z etykiety, a następnie Next.



Rysunek 35. Protegus 2 – podanie nazwy systemu (Name), a następnie Next.

Unikalny identyfikator urządzenia (**IMEI / Unique ID**) jest podany na etykiecie urządzenia i na naklejce pudełka, pokazuje go też pasek stanu TrikdisConfig. Jeśli **PROTEGUS Cloud access Code** w urządzeniu nie jest fabryczny, aplikacja poprosi o niego przy dodawaniu.

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.

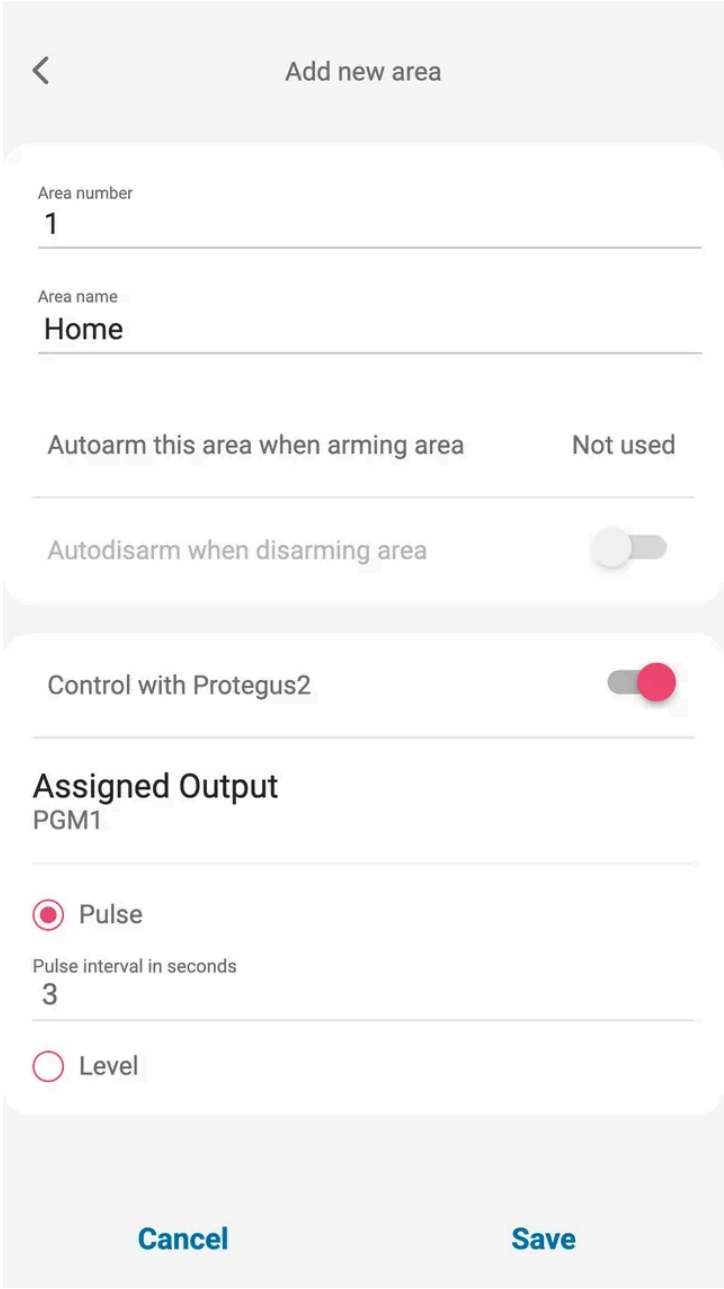
Ustawienie możesz wprowadzić podczas tworzenia systemu, przy dodawaniu partycji, albo później w ustawieniach systemu, przy edycji partycji. Podczas tworzenia systemu prowadzi cię kreator Protegus 2: kliknij przycisk **Continue** (Dalej), podaj nazwę partycji (**Area name**) i włącz sterowanie wyjściem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

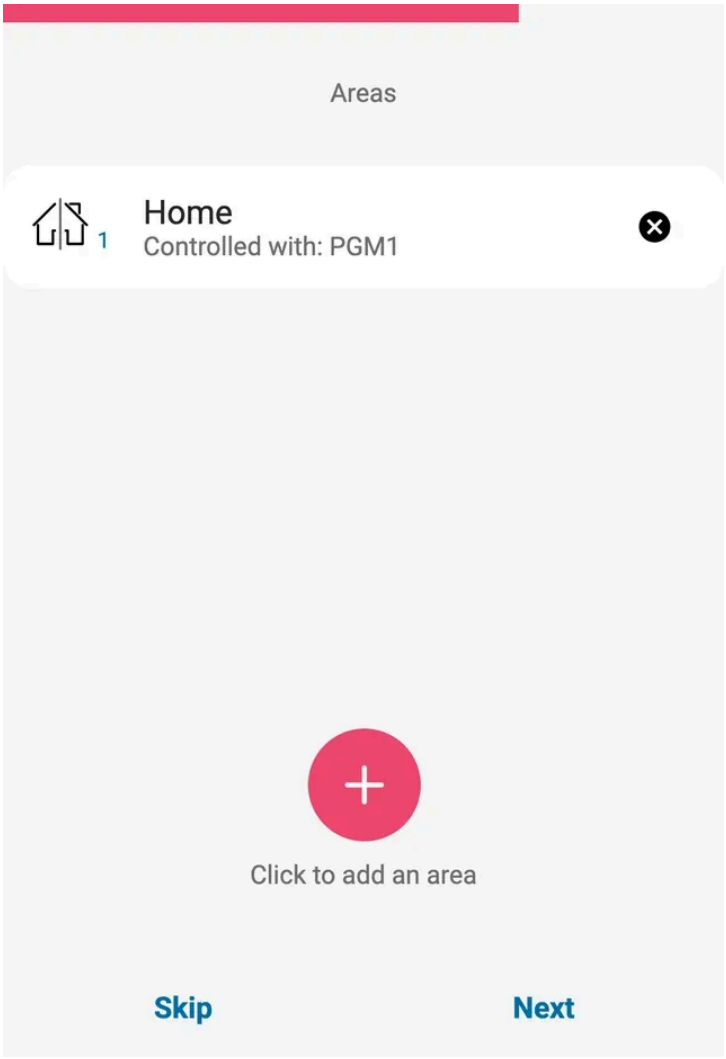
Protegus 2 może poprawnie pokazywać stan partycji tylko wtedy, gdy centrala wysyła zdarzenia uzbrojenia i rozbrojenia z właściwym numerem partycji. Szczegółom i pułapkom uzbrajania przez strefę typu klucz poświęcony jest osobny artykuł: Zdalne uzbrajanie przez strefę typu klucz z aplikacji Protegus 2.



Rysunek 36. Protegus 2 – ekran „Systemem nie sterujemy zdalnie" przy tworzeniu systemu: przyciskiem Continue przechodzisz do ustawienia partycji i wyjścia PGM.



Rysunek 37. Protegus 2 – dodawanie partycji (Add new area): Area number, Area name, Control with Protegus2 włączone, Assigned Output PGM1, Pulse (3 s) lub Level, a następnie Save.

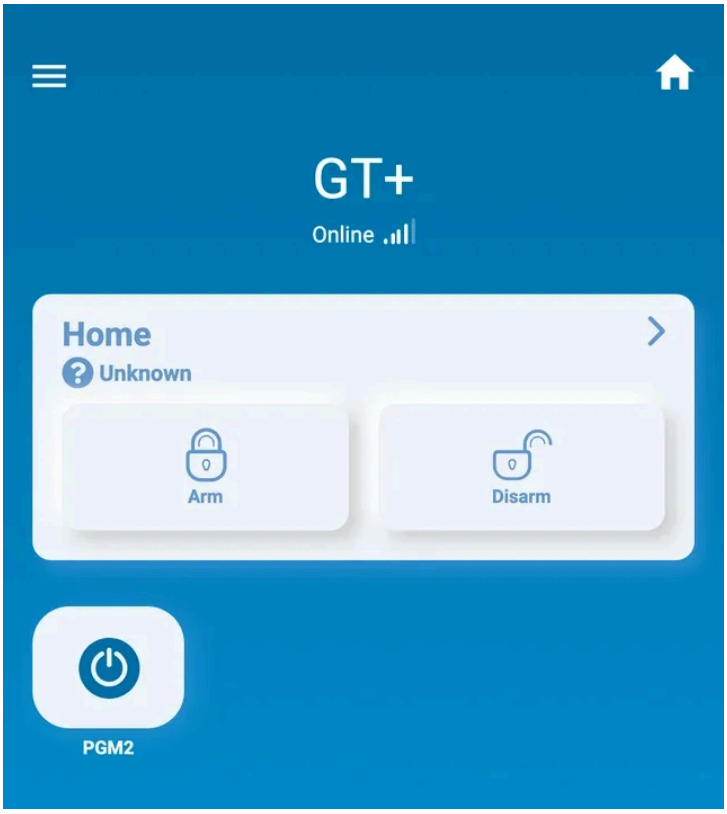


Rysunek 38. Protegus 2 – lista partycji (Areas): partycją Home steruje PGM1; kolejną partycję dodasz przyciskiem Click to add an area, kreator zamkniesz przyciskiem Skip.

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.



Rysunek 39. Protegus 2 – ekran główny systemu: stan partycji, przyciski Arm i Disarm, pod nimi przełączane wyjście PGM.

5.4 Sterowanie wiadomościami SMS

Komunikatorem można sterować także poleceniami SMS. Budowa wiadomości: `Hasło Polecenie Dane` (oddzielone spacją). Jako hasła możesz używać kodu **administratora** (fabrycznie `123456`) do poleceń `INFO`, `RESET` i `OUTPUTx`, a kodu **instalatora** (fabrycznie `654321`) do poleceń `INFO` i `OUTPUTx`.

Polecenie	Dane	Co robi	Przykład
`INFO`	–	Prosi o informacje o urządzeniu. Odpowiedź: typ urządzenia, numer IMEI, numer seryjny i wersja firmware.	`123456 INFO`
`RESET`	–	Uruchamia urządzenie ponownie (tylko kodem administratora).	`123456 RESET`
`OUTPUTx`	`ON`	Włącza wyjście x (x = 1 lub 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Wyłącza wyjście x.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Włącza wyjście w trybie impulsowym na podany czas; `tttt` to długość impulsu w sekundach, czterema cyframi.	`123456 OUTPUT2 PULSE=0002`

Wyjście można przełączać tylko wtedy, gdy na stronie **IN/OUT** programu TrikdisConfig dany zacisk I/O jest ustawiony jako wyjście (**OUT**). Z jakich numerów telefonów urządzenie ma przyjmować polecenia, możesz ograniczyć na karcie **User reporting** → **Control by SMS** (punkt 6.5).

6. TrikdisConfig – ustawienia szczegółowo

Po lewej stronie okna TrikdisConfig widać listę stron (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, RS485 modules, Event summary, Firmware), u góry pasek przycisków (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), a na dole pasek stanu. Ten rozdział omawia po kolei, strona po stronie, ustawienia GT i GT+; tam, gdzie obie wersje się różnią, zaznaczamy to osobno.

6.1 Pasek stanu

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

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

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

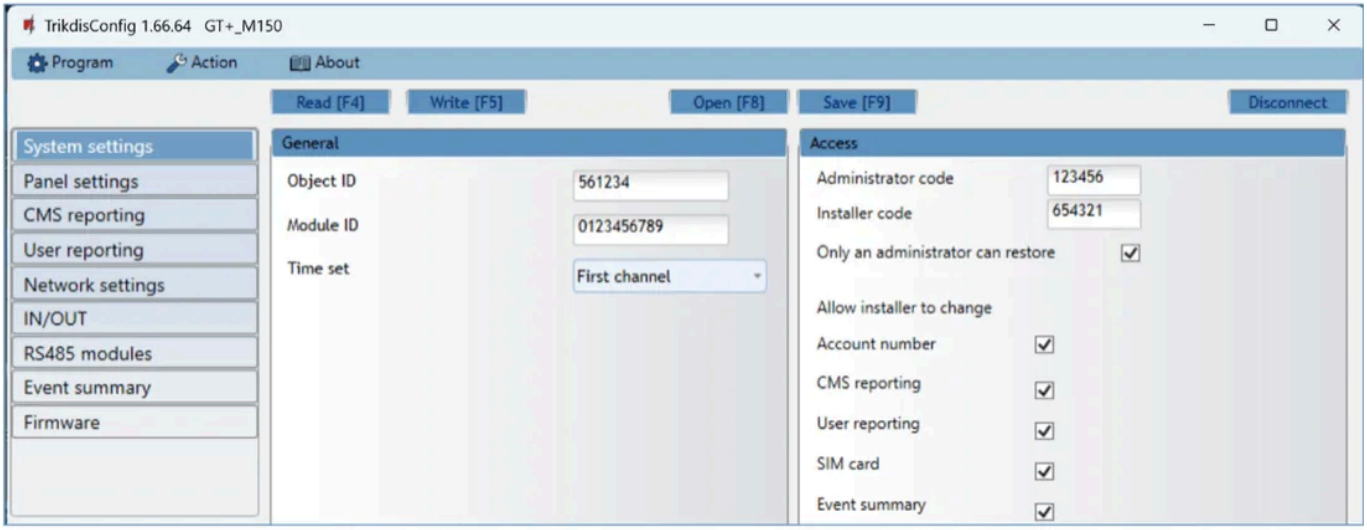


Rysunek 40. Pasek stanu TrikdisConfig po odczycie GT+: identyfikator, stan, typ (Device: GT+_M150), numer seryjny, wersje, sposób połączenia i poziom dostępu.

W polu **Device** w GT musi być oznaczenie typu GT, a w GT+ – GT+ (na rysunku GT+_M150; przyrostek literowo-cyfrowy oznacza wersję sprzętową). Po **Read [F4]** program odczyta i pokaże wartości ustawione w urządzeniu; potrzebne ustawienia wykonaj według poniższych opisów stron.

6.2 System settings

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



Rysunek 41. TrikdisConfig – strona System settings: grupy General i Access.

- **Object ID** – identyfikator obiektu otrzymany od stacji monitorowania (6 znaków szesnastkowych: 0–9, A–F; nie można używać `FFFE` i `FFFF`). Obowiązkowy, jeśli urządzenie raportuje także do stacji monitorowania.
- **Module ID** – numer identyfikacyjny modułu.
- **Time set** – z którego serwera urządzenie synchronizuje zegar.

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

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

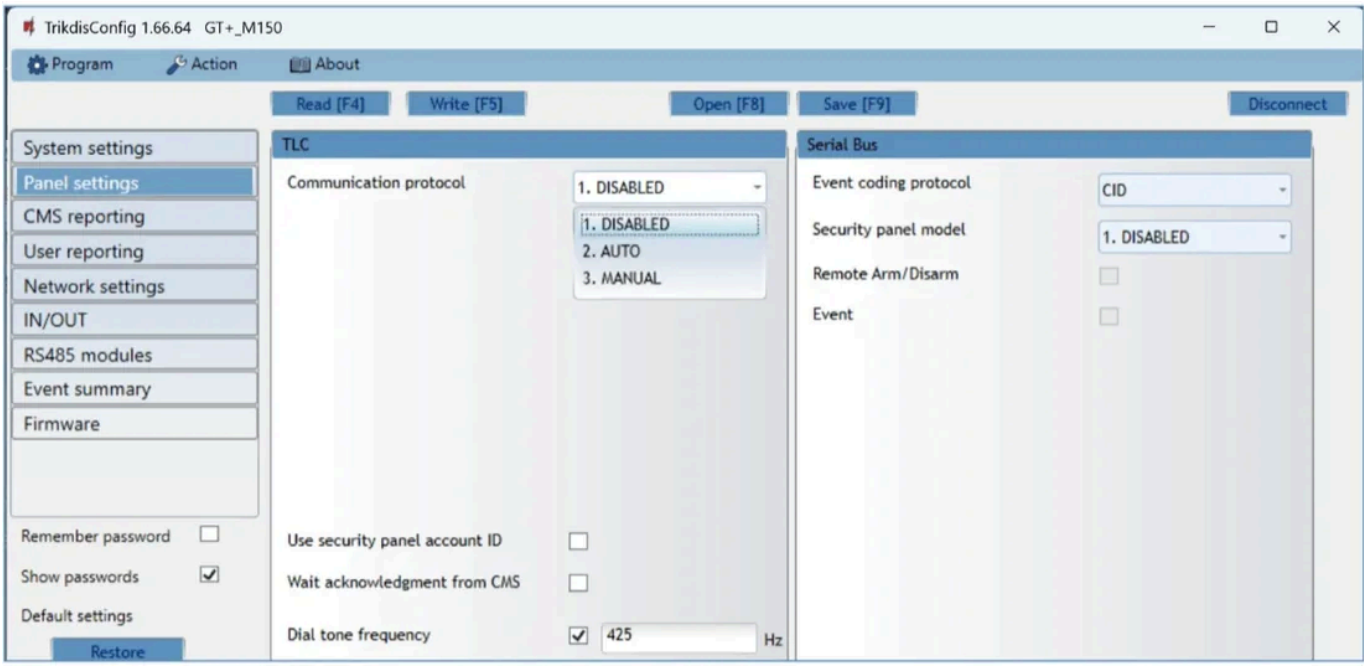
- **Administrator code** – dostęp do wszystkich ustawień (hasło fabryczne: `123456`; hasło ma 6 znaków: cyfry lub litery łacińskie).
- **Installer code** – dostęp, który można ograniczyć (hasło fabryczne: `654321`).
- **Only an administrator can restore** – po zaznaczeniu przywrócenie ustawień fabrycznych 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!

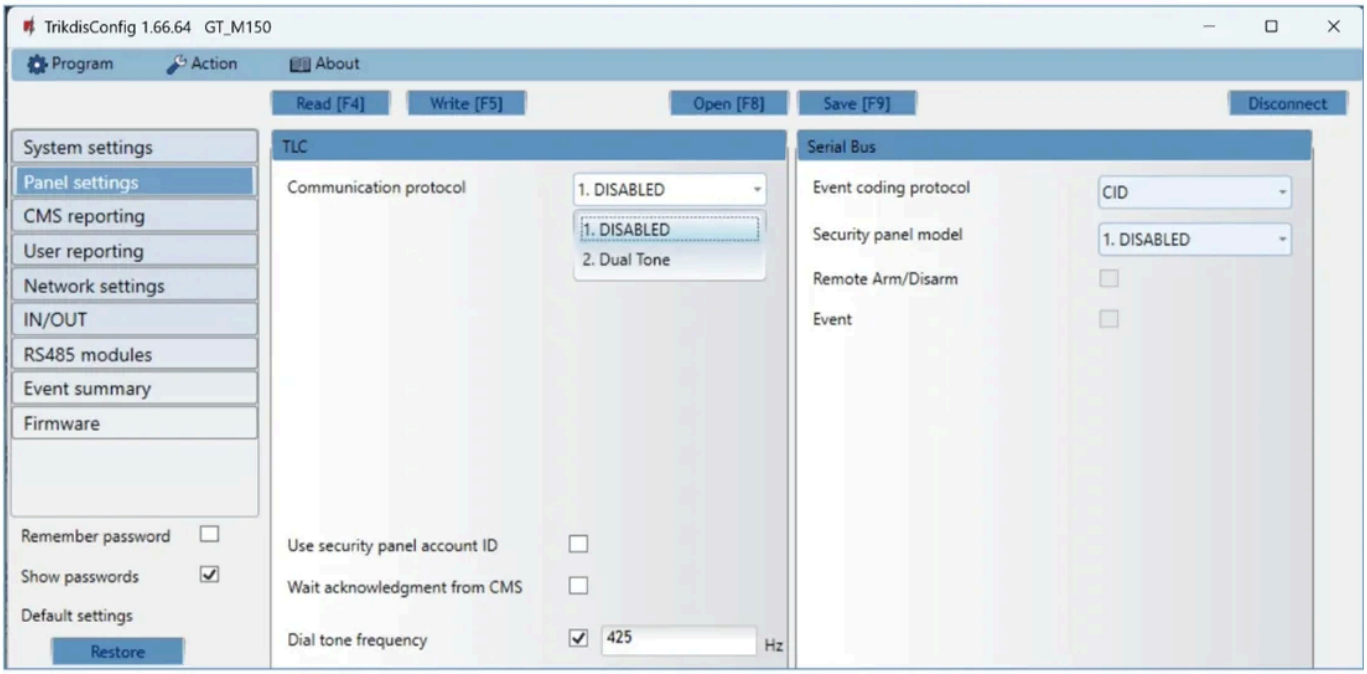
Przy uruchomieniu zmień co najmniej hasło administratora i zapisz je w bezpiecznym miejscu. Zapomnianego hasła nie da się usunąć nawet przywróceniem ustawień fabrycznych, bo do tego także potrzebne jest hasło: wtedy zresetować je może tylko producent lub dystrybutor, po dostarczeniu mu urządzenia. Wyjątkiem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

6.3 Panel settings

Na tej stronie podajesz, jak komunikator jest połączony z centralą alarmową: grupa **TLC** zawiera ustawienia podłączenia do linii telefonicznej (TIP/RING), a grupa **Serial bus** ustawienia podłączenia do magistrali danych lub portu szeregowego. Tu są też wspólne ustawienia dotyczące obsługi zdarzeń centrali.



Rysunek 42. TrikdisConfig – Panel settings w GT+: lista Communication protocol grupy TLC (1. DISABLED, 2. AUTO, 3. MANUAL), pod nią grupa Serial bus i ustawienia wspólne.



Rysunek 43. TrikdisConfig – Panel settings w GT: lista Communication protocol zawiera tu 1. DISABLED i 2. Dual tone.

Grupa TLC – jeśli komunikator jest podłączony do zacisków TIP/RING centrali:

- **Communication protocol** – włączenie lub wyłączenie interfejsu linii telefonicznej DTMF komunikatora. GT+: **1. DISABLED** (wyłączony), **2. AUTO**, **3. MANUAL**; GT: **1. DISABLED**, **2. Dual tone**. Przy podłączeniu TIP/RING wybierz wartość AUTO (GT: Dual tone).

Ustawienia pod grupą, obowiązujące przy obu sposobach podłączenia:

- **Use security panel account ID** – po zaznaczeniu komunikator nie używa własnego Object ID, lecz identyfikatora obiektu ustawionego w centrali i wysyłanego przez centralę.

- **Wait acknowledgment from CMS** – po zaznaczeniu komunikator po każdym zdarzeniu czeka na potwierdzenie odbiornika (kiss-off) i dopiero potem potwierdza zdarzenie centrali; jeśli potwierdzenie nie przyjdzie na czas, wysyła komunikat ponownie. Jeśli urządzenie nie raportuje do stacji monitorowania, pozostaw tę opcję wyłączoną.
- **Dial tone frequency** – częstotliwość sygnału zgłoszenia, którym komunikator komunikuje się z dialerem centrali (domyślnie 425 Hz; to standardowy sygnał zgłoszenia w większości krajów Europy, także w Polsce).



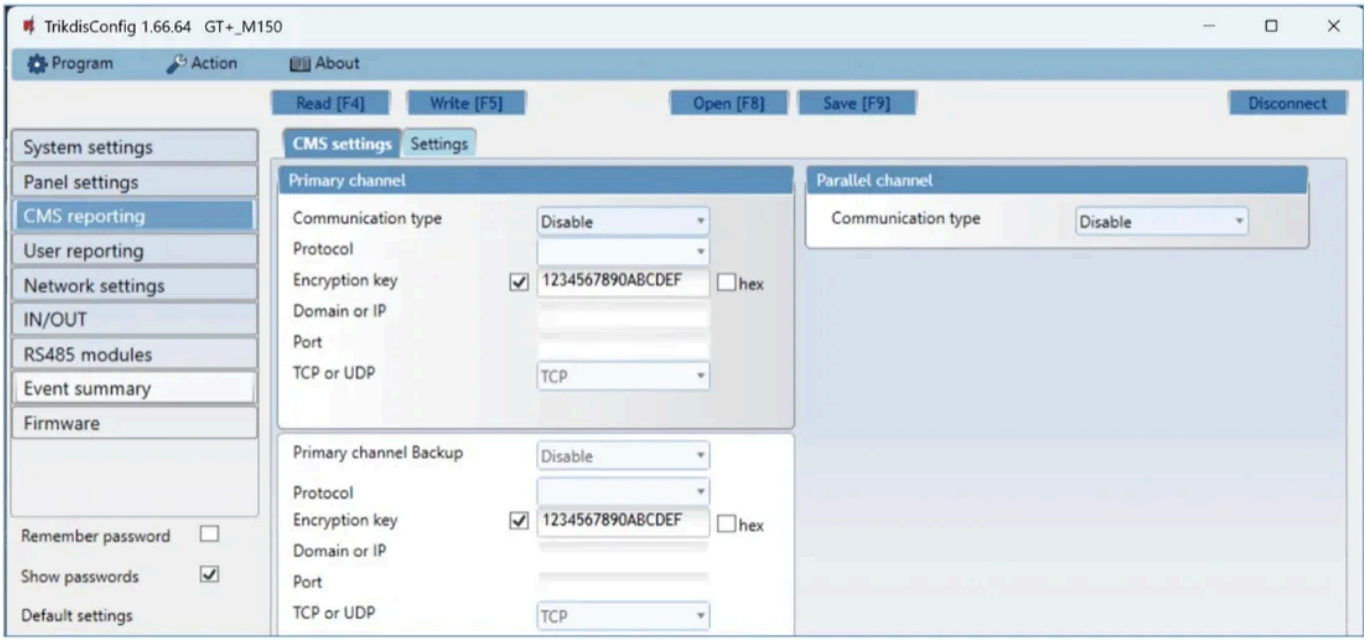
Rysunek 44. TrikdisConfig – Panel settings, grupa Serial bus: Event coding protocol CID, Security panel model (na rysunku Paradox SP/MG), Remote Arm/Disarm i Event zaznaczone, Security panel PC download password podane.

Grupa Serial bus – jeśli komunikator jest podłączony do magistrali danych lub portu szeregowego centrali:

- **Event coding protocol** – protokół kodowania zdarzeń (CID).
- **Security panel model** – typ podłączonej centrali alarmowej z listy (do podłączenia Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING wybierz element **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – po zaznaczeniu komunikator steruje centralą bezpośrednio (uzbrajanie i rozbrajanie z Protegus 2). Widoczne tylko przy centralach, którymi można sterować bezpośrednio. Do sterowania bezpośredniego trzeba ustawić także centralę według rozdziału 4.
- **Security panel PC download password** – do bezpośredniego sterowania centralą Paradox i Texecom hasło PC lub UDL; musi być zgodne z hasłem ustawionym w centrali, którego podanie opisuje rozdział 4.

6.4 CMS reporting

Komunikator wysyła zdarzenia do stacji monitorowania przez mobilną transmisję danych (IP). Zdarzenia mogą iść kilkoma kanałami: kanał **główny** i **równoległy** działają jednocześnie (do dwóch odbiorników naraz), a do każdego z nich należy kanał **zapasowy**, który zaczyna działać, gdy dany kanał zostanie przerwany. Komunikacja jest szyfrowana i chroniona hasłem; do odbioru i przekazywania zdarzeń do oprogramowania stacji monitorowania potrzebny jest odbiornik Trikdis (odbiornik programowy IPcom – Windows lub Linux –, odbiornik IP/SMS RL14 lub odbiornik wielokanałowy RM14) albo odbiornik uniwersalny obsługujący protokół DC-09 / TL150. GT i GT+ raportują do stacji monitorowania tylko kanałem IP, nie mają kanału SMS.



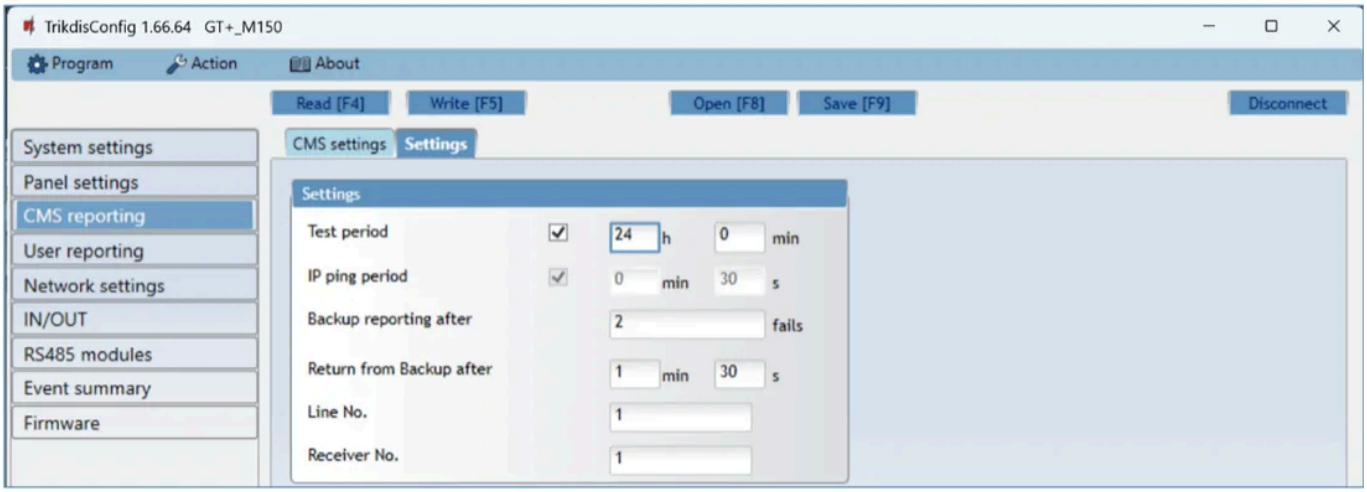
Rysunek 45. TrikdisConfig – CMS reporting, karta CMS settings: kanał główny, zapasowy i równoległy.

Primary channel – kanał główny

- **Communication type** – sposób połączenia z odbiornikiem: **IP**.
- **Protocol** – **TRK8** (odbiorniki Trikdis), **DC-09_2007** lub **DC-09_2012** (odbiorniki uniwersalne), **TL150** (odbiorniki SUR-GARD).
- **Encryption key** – klucz szyfrowania komunikatów; w komunikatorze i w odbiorniku musi być taki sam.
- **Domain or IP**, **Port** – nazwa domeny lub adres IP odbiornika i jego port.
- **TCP or UDP** – protokół transmisji.

Parallel channel – kanał równoległy. Oprócz kanału głównego wysyła jednocześnie do drugiego odbiornika (na przykład do lokalnej i centralnej stacji monitorowania). Jego ustawienia są takie same jak kanału głównego.

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



Rysunek 46. TrikdisConfig – CMS reporting, karta Settings: raport testowy, PING, czasy kanału zapasowego i dane DC-09.

Na karcie **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**.

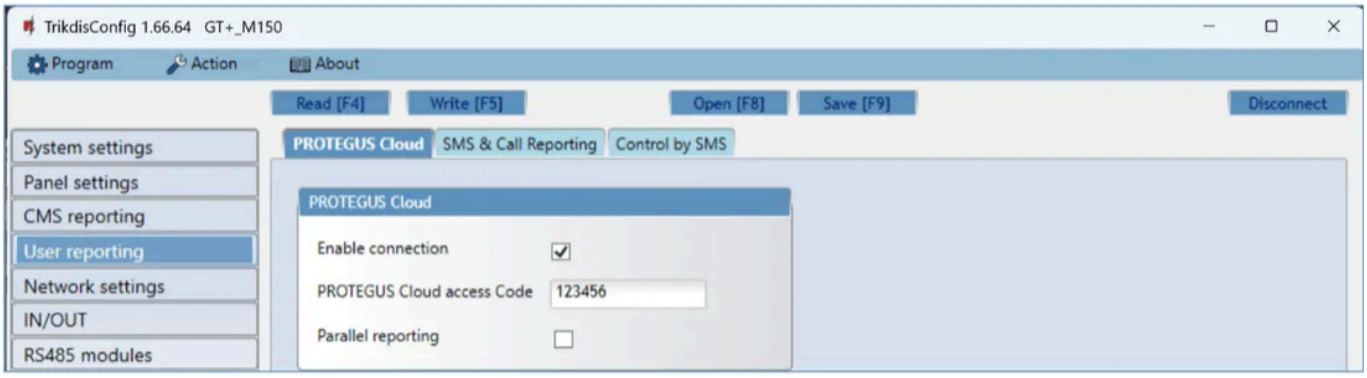
DC-09 Settings (po prawej stronie karty) – wypełniasz tylko wtedy, gdy na którymś kanale wysyłasz protokołem DC-09_2007 lub DC-09_2012; grupa pojawia się, gdy w polu **Protocol** któregoś kanału wybrano DC-09_2007 lub DC-09_2012:

- **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 karcie Settings GT i GT+ w grupie DC-09 są pola **Line No.** (numer linii) i **Receiver No.** (numer odbiornika); grupa pojawia się, jeśli w polu **Protocol** któregoś kanału wybrano DC-09_2007 lub DC-09_2012.

6.5 User reporting

Na karcie **PROTEGUS Cloud** włączasz usługę Protegus, dzięki której użytkownik zdalnie nadzoruje komunikator i podłączony do niego system oraz nimi steruje; szczegóły: www.protegus.app.

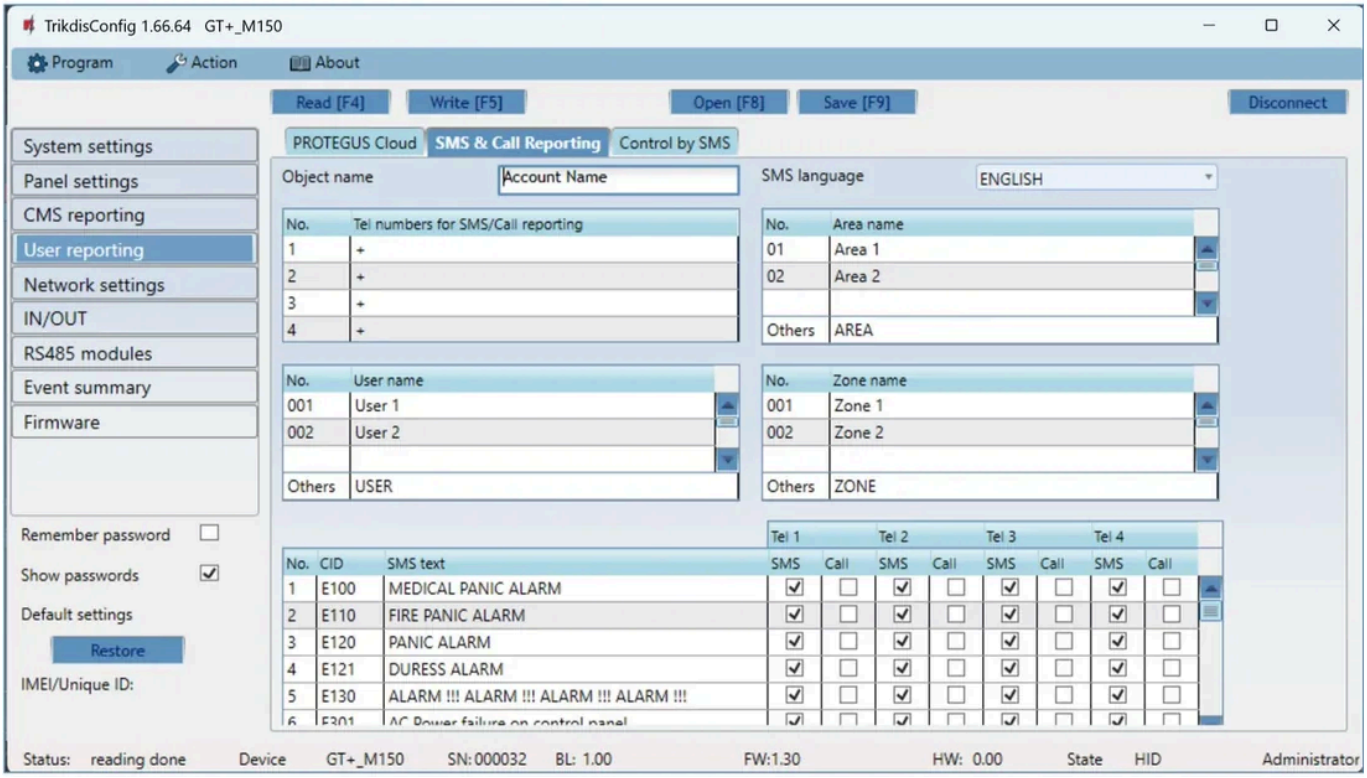


Rysunek 47. TrikdisConfig – User reporting, karta PROTEGUS Cloud.

- **Enable connection** – włącza usługę Protegus: urządzenie wymienia dane z aplikacją Protegus 2, a TrikdisConfig może się z nim łączyć zdalnie.
- **PROTEGUS Cloud access Code** – 6-cyfrowy kod do połączenia z Protegus 2 (fabrycznie `123456`). Jeśli zmienisz go w TrikdisConfig, trzeba go zmienić także w aplikacji Protegus 2.
- **Parallel reporting** – po zaznaczeniu komunikaty idą jednocześnie kanałem głównym (do stacji monitorowania) i do Protegus 2.

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

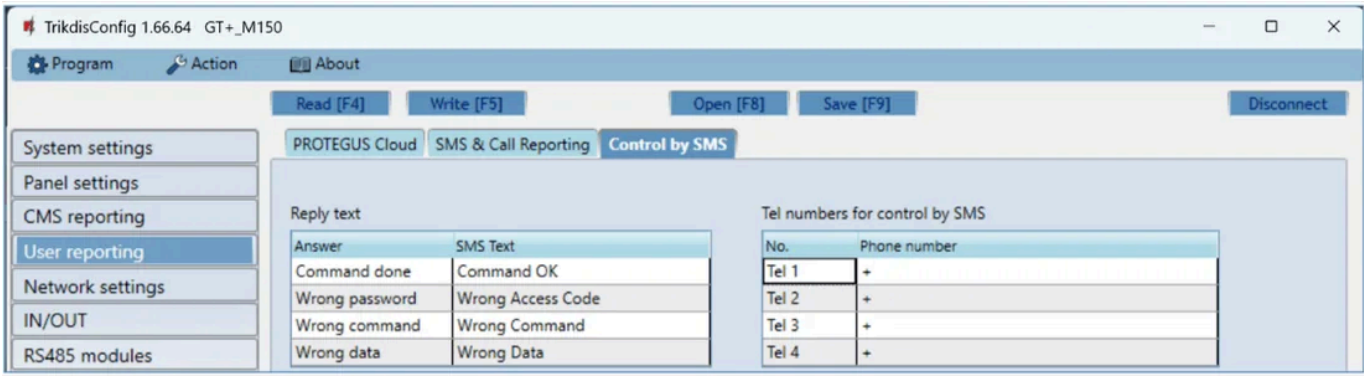
W razie alarmu urządzenie najpierw wysyła SMS na wszystkie wpisane numery telefonów, a następnie dzwoni do nich po kolei od Tel 1 do Tel 4. Każdy numer jest wybierany raz i dzwoni przez 20 sekund; połączenie uznaje się za udane, jeśli numer dzwoni (wystarczy też odebranie lub odrzucenie). Modem wykonuje 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 48. TrikdisConfig – User reporting, karta SMS & Call Reporting.

- **Object name** – nazwa systemu; występuje w każdym SMS-ie.
- **SMS language** – język SMS-ów (komunikaty można wysyłać także z własnymi znakami danego języka).
- **Tel numbers for SMS/Call reporting** – maksymalnie 4 numery telefonów, które otrzymują SMS lub połączenie o zdarzeniach; podaj je z kodem kraju (`+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 jego nazwę.
- **CID event table** – dla każdego zdarzenia można ustawić, który numer otrzymuje SMS lub połączenie. Treść SMS-a i kod Contact ID zdarzeń domyślnych można zmienić, a także dodać nowe zdarzenie z opisem.

Na karcie **Control by SMS** ustawiasz przyjmowanie poleceń SMS: poleceniami można przełączać wyjścia i prosić o informacje o urządzeniu (polecenia opisuje punkt 5.4).



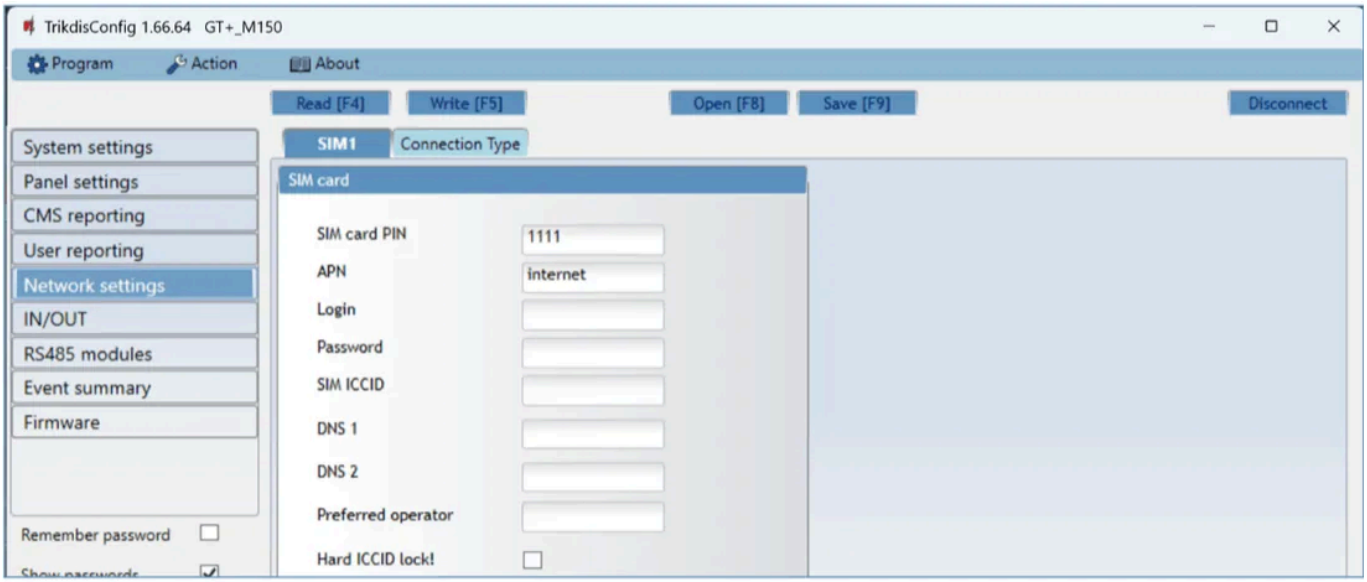
Rysunek 49. TrikdisConfig – User reporting, karta Control by SMS.

- **Reply text** – treść odpowiedzi na polecenie SMS: polecenie wykonane (Command done), złe hasło (Wrong password), złe polecenie (Wrong command), złe dane (Wrong data). Treści można edytować.
- **Tel numbers for control by SMS** – numery telefonów, z których urządzenie przyjmuje polecenia.

Jeśli nie podano tu żadnego numeru telefonu, urządzenie przyjmuje polecenia z dowolnego numeru. Bezpieczeństwo zapewnia wtedy to, że w poleceniu obowiązkowe jest hasło administratora lub instalatora.

6.6 Network settings

Przed użyciem upewnij się, że karta SIM jest aktywna i działa. Jeśli wysyłasz zdarzenia kanałem IP lub do Protegus 2 przez mobilny internet, na karcie musi być włączona także usługa mobilnej transmisji danych.

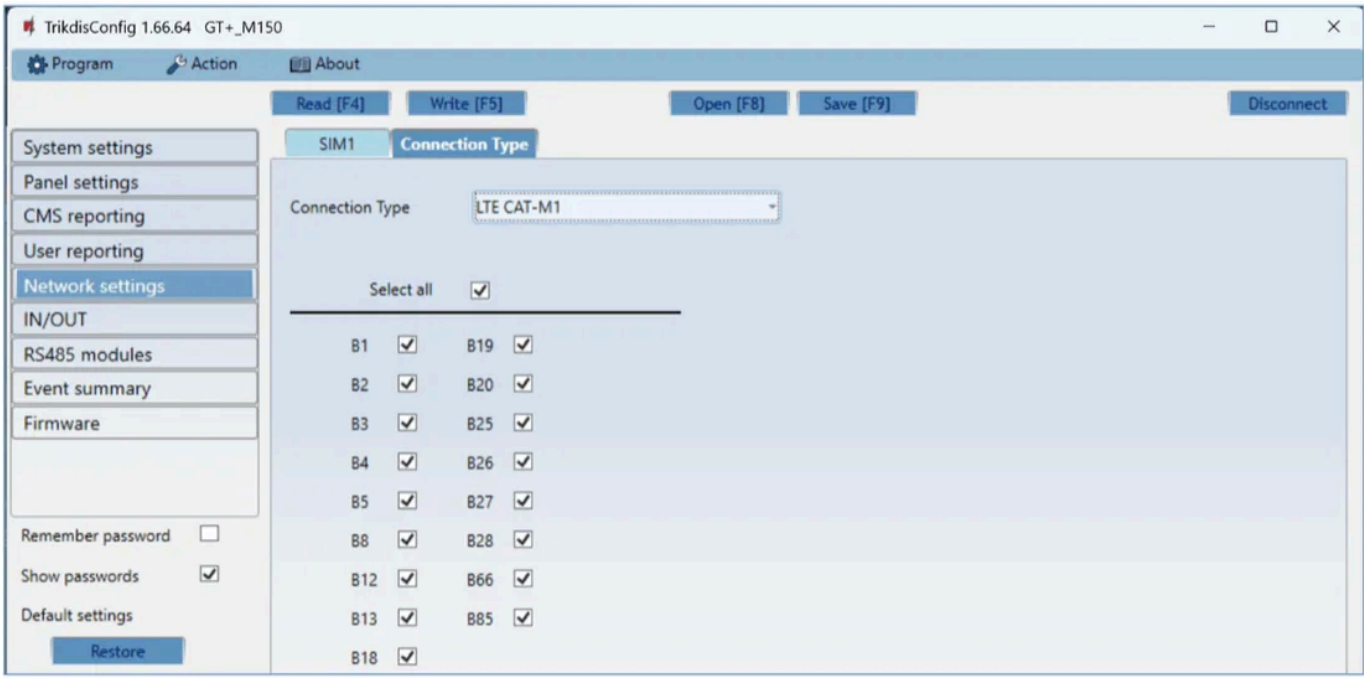


Rysunek 50. TrikdisConfig – Network settings, karta SIM1: dane karty SIM.

Karta SIM1, grupa SIM card

- **SIM card PIN** – kod PIN karty. Żądanie PIN możesz wyłączyć, wkładając kartę do telefonu komórkowego i wyłączając je tam; wtedy może zostać wartość fabryczna pola.
- **APN** – punkt dostępu operatora (Access Point Name); bez niego urządzenie nie połączy się z internetem. Wartość znajdziesz na stronie operatora karty SIM; `internet` jest ogólny i działa w sieciach wielu operatorów. Znane APN-y operatorów wymienia artykuł o APN (przy karcie IoT / M2M operator podaje osobny APN, zobacz punkt 2.2).
- **Login, Password** – nazwa użytkownika i hasło do połączenia z internetem, jeśli operator ich wymaga.
- **SIM ICCID** – numer ICCID karty SIM, jeśli chcesz, aby urządzenie działało tylko z tą kartą. Jeśli ICCID włożonej karty się nie zgadza, dioda TROUBLE miga 8 razy (punkt 1.6).

- **DNS 1, DNS 2** – serwery nazw (DNS, Domain Name System: podaje adres IP przypisany do nazwy domeny); są potrzebne, jeśli odbiornik podałeś w polu **Domain or IP** nazwą domeny, a nie adresem IP. Domyślnie publiczny DNS Google. Niezależnie od ustawień IP sprawdź, czy adresy DNS działają u twojego operatora.
- **Preferred operator** – kod operatora komórkowego (MCC + MNC); jeśli go podasz, urządzenie łączy się tylko z siecią wybranego operatora.
- **Hard ICCID lock** – po zaznaczeniu i ponownym uruchomieniu urządzenia komunikator jest ściśle powiązany z kartą SIM o podanym numerze ICCID.

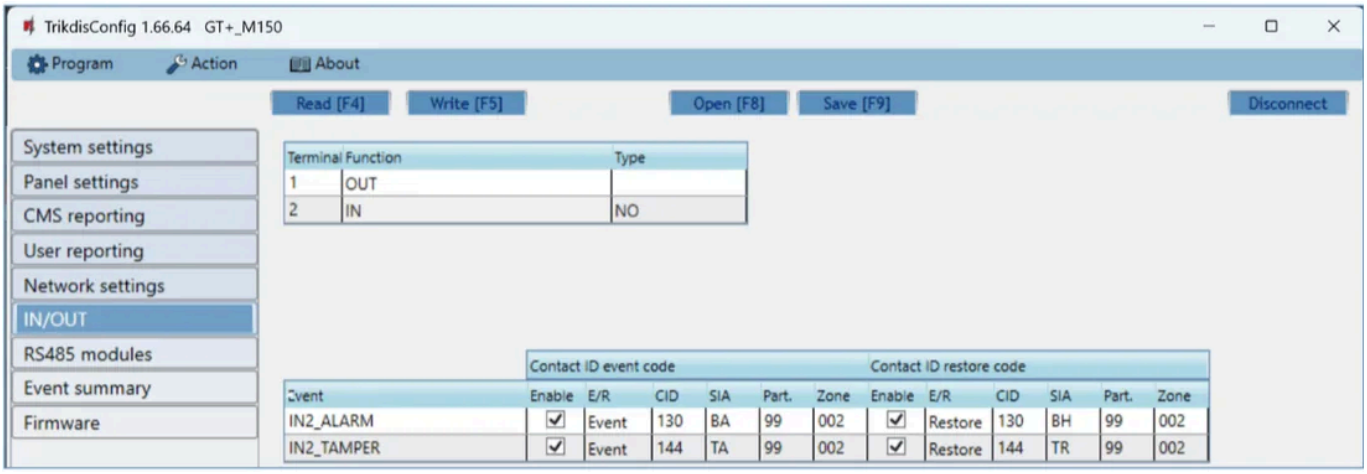


Rysunek 51. TrikdisConfig – Network settings, karta Connection Type: wybór pasm LTE wersji z modemem CAT-M1.

Karta Connection Type – obowiązuje tylko w wersji z modemem CAT-M1 (BG95-M5): tu możesz podać, w których pasmach częstotliwości LTE ma działać modem urządzenia (**Select all** = wszystkie).

6.7 IN/OUT

Tu podajesz rolę dwóch zacisków I/O o podwójnej funkcji komunikatora: **Off** (nieużywany), **IN** (wejście) lub **OUT** (wyjście). Przy wejściu w polu **Type** trzeba podać także typ podłączonego obwodu (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).



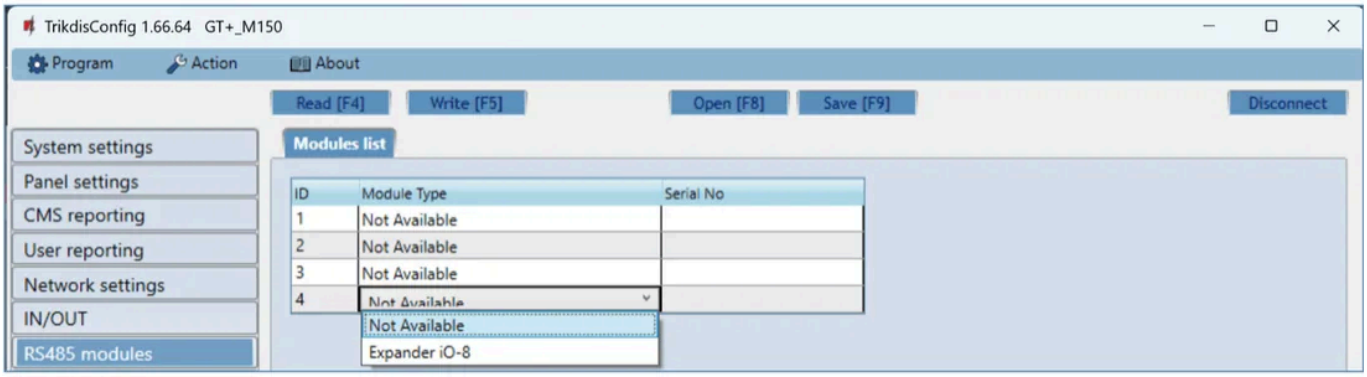
Rysunek 52. TrikdisConfig – strona IN/OUT: zacisk 1 jako wyjście (OUT), zacisk 2 jako wejście (IN, NO); pod spodem zdarzenia alarmu i sabotażu wejścia 2 z kodem CID i SIA.

Przy naruszeniu czujnika podłączonego do wejścia komunikator wysyła własne zdarzenie (**INx_ALARM**, Contact ID 130, SIA BA; przywrócenie BH), a przy naruszeniu obwodu sabotażowego – zdarzenie sabotażu (**INx_TAMPER**, 144, SIA TA; przywrócenie TR) do stacji monitorowania i do Protegus 2; w tabeli pojawiają się zdarzenia każdego zacisku ustawionego jako wejście. Kolumny tabeli:

- **Enable** – włącza wysyłanie komunikatu do stacji monitorowania i do Protegus 2.
- **E/R** – typ komunikatu: Event (zdarzenie) lub Restore (przywrócenie).
- **CID** – kod Contact ID (można go zmienić albo zostawić fabryczny).
- **SIA** – kod SIA (można go zmienić albo zostawić fabryczny).
- **Part.** – numer partycji w komunikacie.
- **Zone** – numer strefy w komunikacie.

6.8 RS485 modules

Ekspanderami **iO-8** podłączonymi do magistrali RS485 można dodać do komunikatora kolejne wejścia i wyjścia. Podłączone ekspandery trzeba dodać na karcie **Modules list**.

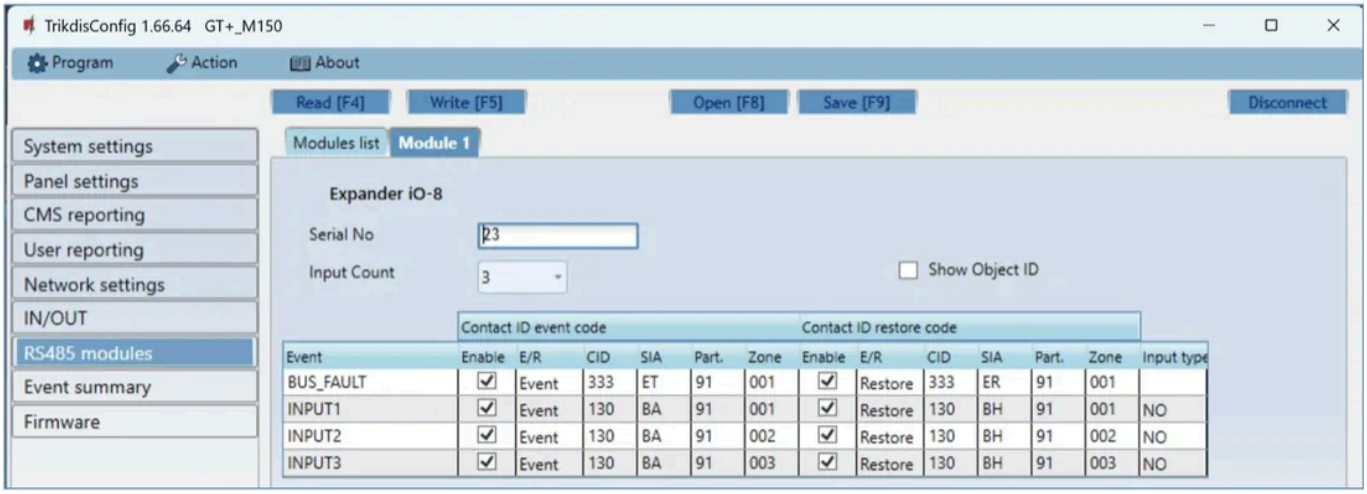


Rysunek 53. TrikdisConfig – RS485 modules, karta Modules list: na 4. pozycji lista Module type (Not Available, Expander iO-8).

- **Module type** – typ modułu podłączonego do magistrali z listy (**Expander iO-8**).
- **Serial No** – 6-cyfrowy numer seryjny modułu (na obudowie modułu i na naklejce opakowania).

Po wybraniu modułu i podaniu numeru seryjnego przejdź na kartę **RS485 modules** → **Module**: dodany moduł ma własną, numerowaną kartę (Module 1 …) ze swoimi ustawieniami.

Ekspander iO-8 – 8 zacisków I/O o podwójnej funkcji; do komunikatora można podłączyć maksymalnie cztery iO-8.



Rysunek 54. TrikdisConfig – RS485 modules, karta Module 1 (iO-8): Input Count, Show Object ID oraz zdarzenia BUS_FAULT, INPUT1–INPUT3 z kodem CID i SIA, z partycją 91.

- **Input Count** – ile zacisków ma być wejściami (IN); pozostałe będą wyjściami (OUT). Rolę wyjść (uzbrajanie / rozbrajanie lub przełączanie urządzenia) ustawiasz bezpośrednio w aplikacji Protegus 2.
- W tabeli do usterki magistrali (**BUS_FAULT**, Contact ID 333) i do wejść (**INPUTx**, 130) możesz przypisać kod zdarzenia i przywrócenia; przy naruszeniu wejścia komunikator wysyła zdarzenie z ustawionym kodem do odbiornika stacji monitorowania i do Protegus 2. Kolumny wiersza zdarzenia (Contact ID event code) i przywrócenia (Contact ID restore code): **Enable** (włączenie), **E/R** (Event lub Restore), **CID** (kod Contact ID), **SIA** (kod SIA), **Part.** (partycja – automatycznie zależy od numeru porządkowego modułu: dla 1. modułu 91, dla 4. modułu 94), **Zone** (numer strefy).
- **Object ID** – dla wejścia można podać także identyfikator obiektu inny niż komunikatora (kolumna pojawia się po zaznaczeniu **Show Object ID**).
- **Input type** – typ wejścia: NO, NC lub EOL.

6.9 Event summary

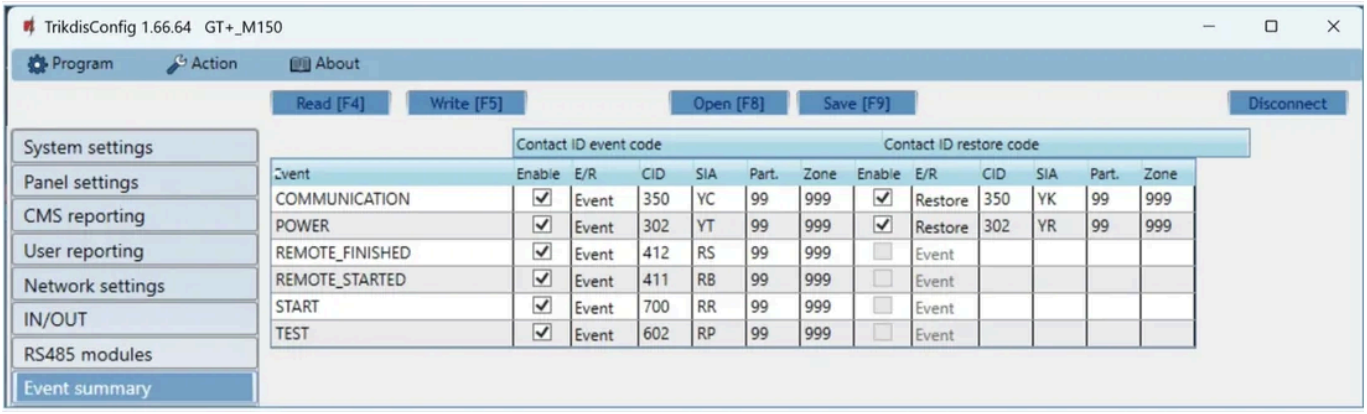
Na tej stronie włączasz lub wyłączasz **własne, wewnętrzne komunikaty** urządzenia oraz zmieniasz ich kod Contact ID, numer partycji i strefy. Komunikatu wyłączonego tutaj urządzenie nie wysyła żadnym kanałem. Fabrycznie komunikaty są wysyłane z partycją 99 i strefą 999.

Komunikat	Contact ID	Kiedy powstaje
COMMUNICATION	350	Przerwana komunikacja między komunikatorem a centralą alarmową (fabrycznie wyłączony). Komunikator podłączony do magistrali lub portu szeregowego wykrywa ją bezpośrednio; komunikator podłączony do linii telefonicznej – tylko przy włączonym **Line supervision**.
POWER	302	Nieprawidłowe (niskie) napięcie zasilania; jego powrót to osobny komunikat.
REMOTE_STARTED	411	Rozpoczęło się zdalne programowanie za pomocą TrikdisConfig.
REMOTE_FINISHED	412	Zdalne programowanie zostało zakończone.
START	700	Urządzenie połączyło się z siecią (uruchomienie).
TEST	602	Okresowy raport testowy.

Komunikat	Contact ID	Kiedy powstaje
PING	760	Komunikat życia PING. Nie występuje na liście każdego urządzenia: na ekranie wcześniejszej wersji sprzętowej tak, na stronie Event summary nowszych wersji nie ma takiego wiersza. Jego odstęp ustawiasz w polu **CMS reporting** → **Settings** → **IP ping period**.

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

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



Rysunek 55. TrikdisConfig – strona Event summary: wewnętrzne komunikaty urządzenia z kodem CID i SIA (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

Na liście GT i GT+ są komunikaty **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** i **TEST**, każdy także z kodem SIA. Komunikat COMMUNICATION oznacza usterkę połączenia między centralą a komunikatorem: przy podłączeniu do magistrali danych lub portu szeregowego komunikator wykrywa ją bezpośrednio (dioda TROUBLE miga 7 razy).

6.10 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**.



Rysunek 56. TrikdisConfig – przycisk Restore w grupie Default settings.

Ustawienia fabryczne można przywrócić także na urządzeniu, bez komputera: przy włączonym zasilaniu naciśnij i przytrzymaj przycisk **RESET** na płytce drukowanej (punkt 1.4) przez **10 sekund**, aż zgasną diody NETWORK, POWER i TROUBLE, a następnie zaświeci się dioda POWER. Wtedy puść przycisk: ustawienia fabryczne zostały przywrócone.

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.

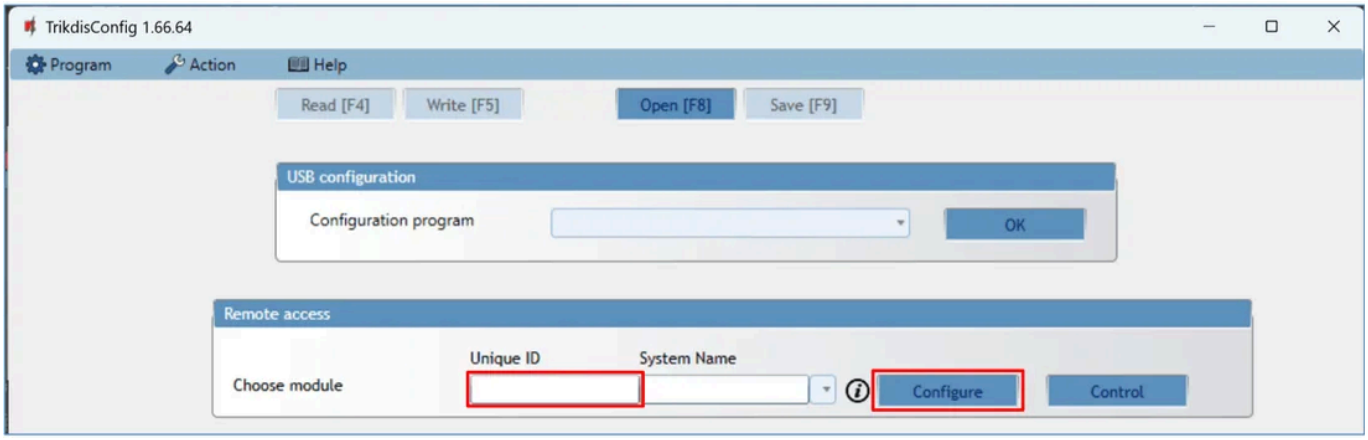
Do zdalnego dostępu potrzebne jest:

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 57. TrikdisConfig – grupa Remote access: pole Unique ID, lista System name i przycisk Configure.

Unikalnym identyfikatorem GT i GT+ jest **IMEI**; jest podany na etykiecie urządzenia i na naklejce pudełka. Do zdalnego dostępu karta SIM musi być aktywna, jej kod PIN podany albo żądanie PIN wyłączone; na karcie **User reporting** → **PROTEGUS Cloud** musi być zaznaczone **Enable connection** (punkt 6.5); dioda **POWER** musi świecić na zielono, a dioda **NETWORK** świecić na zielono i migać na żółto.

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.

6. **Centrala DSC z podłączeniem Keybus + TIP/RING (GT+).** Uzbrój system i wywołaj alarm strefy pożarowej. Stacja monitorowania musi otrzymać zdarzenie z kodem Contact ID odpowiadającym typowi strefy (na przykład E110 – alarm pożarowy), a nie jako alarm ogólny (E130).

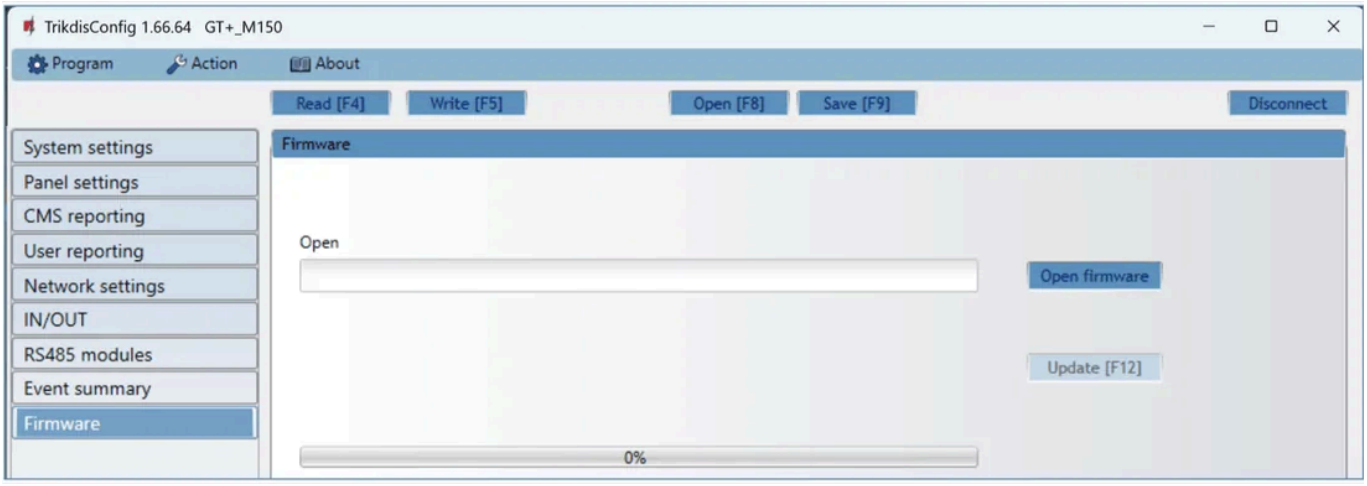
9. Aktualizacja firmware

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 58. TrikdisConfig – strona Firmware: przycisk Open firmware, przycisk Update [F12] i wskaźnik postępu.

Do aktualizacji potrzebne jest połączenie z internetem. Program antywirusowy, zapora sieciowa lub restrykcyjne ustawienia dostępu do internetu mogą uniemożliwić automatyczną aktualizację firmware; wtedy trzeba zmienić ustawienia programu antywirusowego. Do podłączenia Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING (punkt 3.3.4) potrzebny jest firmware w wersji co najmniej 1.21.

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 zarejestrować się w sieci komórkowej, 5 = nie może zarejestrować się w sieci transmisji danych (punkt 1.6).
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 karcie **Network settings** → **SIM1** albo wyłącz żądanie PIN w telefonie.
4. Sprawdź APN (punkt 2.2): przy karcie IoT / M2M operator podaje osobny APN.
5. Sprawdź antenę: jest przykręcona, nie jest w metalowej obudowie, poziom sygnału jest odpowiedni (dioda NETWORK miga na żółto co najmniej 3 razy; punkty 1.6 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, protokół i klucz szyfrowania (**CMS reporting**).
2. Jeśli odbiornik jest podany nazwą domeny, sprawdź ustawienie DNS (**Network settings** → **SIM1** → **DNS 1, DNS 2**).
3. Sprawdź, czy pakiet danych karty SIM nie blokuje potrzebnego portu (niektóre karty M2M dopuszczają tylko określone adresy).

Dioda TROUBLE miga 7 razy – brak połączenia z centralą

1. Przy podłączeniu do magistrali danych lub portu szeregowego sprawdź przewody CLK i DATA oraz to, czy w polu **Panel settings** → **Security panel model** wybrany jest typ podłączonej centrali (punkt 6.3).
2. W centrali Paradox sprawdź, czy port szeregowy nie jest zablokowany (punkt 4.1.2); w centralach Texecom i Paradox **Security panel PC download password** musi być zgodne z ustawionym w centrali.
3. Przy podłączeniu do linii telefonicznej dialer centrali musi być włączony, w trybie DTMF, z formatem Contact ID i podanym numerem telefonu (punkt 4.2), a **Communication protocol** musi być ustawiony na AUTO (GT: Dual tone).

Dioda TROUBLE miga 8 razy – niezgodność ICCID

Numer podany w polu **Network settings** → **SIM1** → **SIM ICCID** nie zgadza się z ICCID włożonej karty SIM: urządzenie działa tylko z podaną kartą. Włóż z powrotem oryginalną kartę albo zmień (usuń) ICCID; przy **Hard ICCID lock** po zmianie uruchom urządzenie ponownie (punkt 6.6).

DSC: każdy alarm przychodzi jako alarm ogólny E130

Podłączony tylko do magistrali Keybus komunikator otrzymuje od centrali stan stref, ale nie typ strefy, dlatego każdy alarm raportuje kodem E130 (punkt 3.3.1). Jeśli stacja monitorowania oczekuje kodu odpowiadającego typowi strefy (na przykład pożar: E110): podłącz **GT+** oprócz Keybus także do zacisków TIP/RING i zaprogramuj dialer centrali (punkty 3.3.2 i 4.1.1). W GT tego podwójnego podłączenia nie ma; tam własne kody centrali idą przez dialer centrali tylko przy podłączeniu TIP/RING, ale wtedy nie ma sterowania bezpośredniego, a do uzbrajania potrzebna jest strefa przełącznika kluczowego (punkt 3.4).

Paradox: port szeregowy jest zablokowany albo brak połączenia

W nowszych centralach Paradox (SP+, MG+, EVOHD+) port szeregowy może być fabrycznie zablokowany; o odblokowaniu mówi punkt 4.1.2 i artykuł Odblokowanie zablokowanego portu szeregowego w centralach alarmowych Paradox. W centralach Spectra SP / SP+ i Magellan MG / MG+ zamiast portu szeregowego można użyć także podłączenia Keybus + TIP/RING (punkt 3.3.4), do którego nie jest potrzebne odblokowanie, ale firmware komunikatora musi mieć wersję co najmniej 1.21 (rozdział 9).

Nie mogę uzbroić systemu z Protegus 2

1. Przy sterowaniu bezpośrednim **Panel settings** → **Remote Arm/Disarm** musi być zaznaczone, a centrala ustawiona według punktu 4.1 (Paradox: hasło PC, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: opisane ustawienia). W tabeli w punkcie 1.3 sprawdź, czy centralą w ogóle można sterować bezpośrednio.
2. Przy uzbrajaniu przełącznikiem kluczowym (punkt 3.4) zacisk na stronie **IN/OUT** musi być ustawiony na **OUT**, strefa centrali musi być strefą przełącznika kluczowego, a w Protegus 2 wyjście musi być przypisane do partycji, w tym samym trybie co w centrali (impulsowym lub dwustanowym; punkt 5.2).
3. Protegus 2 pokazuje stan partycji na podstawie zdarzeń uzbrojenia i rozbrojenia centrali: centrala musi je raportować (Opening/Closing).

Protegus 2 nie widzi urządzenia

1. Na karcie **User reporting** → **PROTEGUS Cloud** musi być zaznaczone **Enable connection**.
2. Przy dodawaniu trzeba podać **PROTEGUS Cloud access Code** ustawiony w urządzeniu; jeśli zmieniłeś kod w TrikdisConfig, zmień go także w aplikacji.
3. IMEI wpisz dokładnie, z etykiety urządzenia lub z naklejki pudełka (albo zeskanuj kod QR).
4. Usługa transmisji danych karty SIM i APN muszą być w porządku (dioda NETWORK świeci na zielono, a dioda DATA po zdarzeniu gaśnie).

Nie mogę połączyć się zdalnie przez TrikdisConfig

1. Urządzenie musi być online (dioda NETWORK świeci na zielono, miga na żółto), a połączenie Protegus musi być włączone (**Enable connection**).
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

W TrikdisConfig nie da się tego zrobić, bo przywrócenie także wymaga hasła. Można to jednak zrobić przyciskiem **RESET** urządzenia (punkt 6.10): przy włączonym zasilaniu przytrzymaj go przez 10 sekund. Wszystkie ustawienia zostaną usunięte.

GT czy GT+ – który jest potrzebny?

Podłączenie, konfiguracja i działanie obu wersji są takie same; różnice zestawia tabela w punkcie 1.2. GT+ działa także z zasilaniem 10–32 V DC (również w systemach 24 V) i w centralach DSC obsługuje podłączenie Keybus + TIP/RING, dzięki czemu zdarzenia idą z własnymi kodami Contact ID centrali. Jeśli te funkcje nie są potrzebne, GT potrafi to samo.

Ile danych zużywa urządzenie?

Komunikaty zdarzeń i PING-i są bardzo małe; ruch zależy głównie od okresu PING i częstotliwości raportów testowych. W przeciętnym systemie domowym miesięczny ruch zwykle nie przekracza 10 MB. Dokładna wartość zależy od ustawień i jednostki rozliczeniowej operatora, dlatego przy karcie z limitem danych warto sprawdzić ruch 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 przeczytaj instrukcję; nieprzestrzeganie zaleceń może prowadzić do nieprawidłowego działania lub uszkodzenia urządzenia.
- Przed podłączeniem, przy każdym podłączaniu elektrycznym i przed serwisem odłącz urządzenie od zasilania.
- Modyfikacje, przeróbki i naprawy niedopuszczone przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów o odpadach: niezdatnego do użytku urządzenia i jego części nie wyrzucaj do odpadów komunalnych. Symbol przekreślonego kosza na kółkach (WEEE) na urządzeniu oznacza, że trzeba je oddać osobno, jako zużyty sprzęt elektroniczny.

Zobacz też

- Wyszukiwarka zgodności – który komunikator Trikdis i jakie podłączenie pasuje do twojej centrali alarmowej.
- Komunikator Trikdis + centrala alarmowa DSC: krótka instrukcja dla instalatora – kroki podłączenia DSC w skrócie.
- Komunikator Trikdis + centrala alarmowa Paradox: krótka instrukcja dla instalatora – kroki podłączenia Paradox w skrócie.
- DSC Power Series NEO i komunikatory Trikdis: zgodność i rozwiązania – dlaczego NEO nie można podłączyć do magistrali danych i jakie jest rozwiązanie.
- Odblokowanie zablokowanego portu szeregowego w centralach alarmowych Paradox – odblokowanie portu szeregowego central SP+, MG+ i EVOHD+.
- Zdalne uzbrajanie przełącznikiem kluczowym z aplikacji Protegus 2 – szczegóły i pułapki uzbrajania przełącznikiem kluczowym.
- Ustawienie APN – lista europejskich operatorów komórkowych – APN-y operatorów, także dla kart IoT / M2M.
- Dokumentacja w języku angielskim: docs.trikdis.com – na stronie GT i GT+ znajduje się także tabela konwersji kodów Contact ID → SIA (załącznik). Instrukcje w serwisie docs.trikdis.com są w języku angielskim.

Powiązane produkty

Trikdis GT 4G inteligentny moduł komunikacyjny

Trikdis GT+ 4G inteligentny moduł komunikacyjny **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-gt