Centrala alarmowa CG17 – instrukcja instalacji i programowania

Instrukcja instalacji i programowania komórkowej centrali alarmowej Trikdis CG17: podłączenie i karta SIM, czujki, wyjścia, ekspandery, konfiguracja w TrikdisConfig, raportowanie do stacji monitorowania, Protegus 2, polecenia SMS i sterowanie połączeniem.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-cg17

Spis treści

1. Przegląd

1.1 Do czego służy, jak działa
1.2 Wersje
1.3 Dane techniczne
1.4 Części centrali
1.5 Zaciski
1.6 Sygnalizacja diod LED
1.7 Narzędzia potrzebne do instalacji

2. Szybka konfiguracja

2.1 Konfiguracja dla aplikacji Protegus 2
2.2 Konfiguracja dla stacji monitorowania

3. Instalacja i podłączenie

3.1 Montaż i włożenie karty SIM
3.2 Podłączenie wejść
3.3 Podłączenie czujek dymu
3.4 Podłączenie czujnika temperatury
3.5 Podłączenie przekaźnika i diody LED
3.6 Podłączenie czytników kluczy iButton
3.7 Podłączenie ekspanderów serii iO
3.8 Podłączenie sygnalizatora
3.9 System ekspanderów iO (iO, iO-WL, iO-MOD)
3.10 Podłączenie czujnika poziomu paliwa Strela
Konfiguracja i przygotowanie czujnika
3.11 Podłączenie akumulatora
3.12 Podłączenie do centrali alarmowej
3.13 Pomiar napięcia stałego
3.14 Moduł Wi-Fi W485
3.15 Moduł Ethernet E485
3.16 RF-LORA i ekspandery LORA

4. Sterowanie

4.1 Sterowanie z aplikacji Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.1.1 Uzbrajanie i rozbrajanie
4.1.2 Dodawanie kolejnych użytkowników
4.2 Sterowanie poleceniami SMS
4.3 Sterowanie połączeniem telefonicznym

5. Konfiguracja programem TrikdisConfig

5.1 Pasek stanu
5.2 Strona „System Options”
5.2.1 Karta System general
5.2.2 Karta Access – kody dostępu
5.3 Strona „Reporting to CMS”
5.4 Strona „Users & Reporting”
5.4.1 Rejestracja kluczy dotykowych (iButton)

5.4.2 Rejestracja kart RFID
5.4.3 Karta SMS answer texts – SMS-y z odpowiedzią
5.5 Strona „Modules”
5.5.1 Karta W485 settings – moduł Wi-Fi
5.5.2 Karta E485 settings – moduł Ethernet
5.5.3 Czujnik poziomu paliwa Strela RS485
5.5.4 Karta Internal modules – moduł GPS
5.6 Strona „Zones”
5.6.1 Karta Zones settings – strefy
5.6.2 Karta SMS & Call reporting
5.7 Strona „PGM”
5.7.1 Karta Outputs – wyjścia
5.7.2 Karta Set Action – sterowanie zdarzeniem
5.7.3 Karta Scheduler – harmonogram
5.7.4 Karta Thermostat – termostat
5.7.5 Karta SMS & Call reporting
5.8 Strona „Sensors”
5.9 Strona „System events”
5.9.1 Karta Events – zdarzenia systemowe
5.9.2 Karta SMS & Call reporting
5.10 Strona „Events Log”
5.11 Przywracanie ustawień fabrycznych
6. Programowanie zdalne
6.1 Zdalna konfiguracja parametrów
6.2 Zdalne sterowanie z TrikdisConfig
7. Sprawdzenie instalacji
8. Aktualizacja oprogramowania układowego
9. Zasady bezpieczeństwa
Zobacz też

1. Przegląd

CG17 to centrala alarmowa z wbudowanym komunikatorem komórkowym, którą można używać także samodzielnie. Działa jako pełnowartościowa centrala alarmowa, a dodatkowo pozwala zdalnie sterować urządzeniami w domu i wokół niego: bramą garażową, furtką, ogrzewaniem, chłodzeniem, systemem nawadniania, oświetleniem, wentylacją. Zdarzenia wysyła zarówno do stacji monitorowania, jak i do właściciela; właściciel otrzymuje je w aplikacji mobilnej i internetowej **Protegus 2**.

Centrala obsługuje 12 stref przewodowych i bezprzewodowych, które możesz pogrupować w 8 partycji. Za pomocą CG17:

- zainstalujesz prosty system alarmowy, który można zdalnie nadzorować i którym można zdalnie sterować;
- zdalnie sterujesz różnymi urządzeniami (np. ogrzewaniem, wentylacją, bramą automatyczną);
- monitorujesz temperaturę, poziom paliwa i napięcie stałe;
- powiadamiasz użytkowników o zdarzeniach;
- wysyłasz komunikaty o zdarzeniach do odbiornika firmy ochroniarskiej (stacji monitorowania).



Rysunek 1. Centrala alarmowa CG17: z przodu diody NETWORK, DATA, POWER i TROUBLE, u góry złącze anteny, u dołu listwy zaciskowe.

1.1 Do czego służy, jak działa

Komunikaty do stacji monitorowania

- Zdarzenia wysyła do programowych i sprzętowych odbiorników Trikdis, które współpracują z dowolnym oprogramowaniem stacji monitorowania.
- Komunikaty o zdarzeniach może wysyłać także do odbiorników SIA DC-09.
- Połączenie z odbiornikiem IP nadzoruje sygnałami kontrolnymi (polling) wysyłanymi co 30 sekund (lub w ustawionym odstępie czasu).
- Ma kanał zapasowy: używa go, gdy połączenie w kanale głównym zostanie przerwane.
- Zdarzenia może zgłaszać stacji monitorowania także SMS-em. SMS zostanie wysłany nawet wtedy, gdy w sieci operatora komórkowego nie działa transmisja danych.
- Jeśli usługa Protegus jest włączona, zdarzenie trafia najpierw do stacji monitorowania, a dopiero potem do użytkowników aplikacji.

Współpraca z aplikacją Protegus 2

- Powiadomienia push i powiadomienia ze specjalnym dźwiękiem o zdarzeniach.
- Zdalne uzbrajanie i rozbrajanie systemu.
- Zdalne sterowanie podłączonymi urządzeniami (oświetleniem, bramą, wentylacją, ogrzewaniem, nawadnianiem itp.).
- Zdalne monitorowanie temperatury (z ekspanderem iO, iO-WL lub iO-LORA).
- Osobne uprawnienia dla administratora, instalatora i użytkownika.
- Użytkownicy mogą dowiadywać się o zdarzeniach także SMS-em i połączeniem telefonicznym.

Powiadamianie użytkowników

- Dzwoni na podane numery telefonów (maksymalnie 8 użytkowników).
- Wysyła SMS-y o zdarzeniach.
- Wysyła do aplikacji Protegus 2 powiadomienia push i powiadomienia ze specjalnym dźwiękiem o zdarzeniach.

Zdalne sterowanie systemem i wyjściami

- z aplikacji Protegus 2;
- kluczem iButton (dotykowym) przez czytnik kluczy;
- czytnikiem RFID z klawiaturą (Wiegand 26/34);
- połączeniem na numer telefonu urządzenia;
- wiadomością SMS;
- automatyczną regułą „jeśli… to”: np. gdy aktywuje się wejście lub temperatura przekroczy wartość progową, włącza się wyjście.

Możliwości rozbudowy

- Przewodowe lub bezprzewodowe ekspandery serii iO i LORA, którymi można zwiększyć liczbę wejść (IN) i wyjść (OUT).
- Odbiornik GPS (przydatny do ochrony bankomatów i automatów sprzedających).
- Czujnik poziomu paliwa – do ochrony zbiorników paliwa lub monitorowania poziomu.
- Zasilanie zapasowe i ładowanie akumulatora 12 V.

Wejścia i wyjścia

- 1 wejście, 2 wyjścia i 3 zaciski I/O, które można ustawić jako wejście (IN) lub sterowane wyjście (OUT).
- Jednoprzewodowa magistrala danych (1-Wire) do czujników temperatury (maksymalnie 8) i czytnika kluczy iButton.

- Liczbę wejść (IN) lub wyjść (OUT) można zwiększyć do 12 przewodowymi lub bezprzewodowymi ekspanderami serii iO.

Instalacja i konfiguracja

- Fabryczne ustawienia domyślne do pracy jako centrala alarmowa lub komunikator.
- Ustawienia można zapisać do pliku i szybko wgrać do innych urządzeń.
- Konfiguracja kablem USB lub zdalnie, programem TrikdisConfig.
- Dwa poziomy dostępu (typy kont): instalator i administrator.

1.2 Wersje

Ta instrukcja dotyczy CG17 z modemem 4G; jego kody typu to: **CG17_14**, **CG17_1E** i **CG17_1S**. Dokładny kod typu widzisz w polu **Device** na pasku stanu TrikdisConfig (punkt 5.1).

Trikdis CG17 4G GSM Compact Security Panel

Wersja z modemem 2G (**CG17_12**) została wycofana, dlatego instrukcja podaje tylko dane wersji 4G.

1.3 Dane techniczne

Parametr	Wartość
Pasma modemu 4G (LTE)	Europa: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28, GSM B2 / B3 / B5 / B8; Ameryka Łacińska: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66, GSM B2 / B3 / B5 / B8
Napięcie zasilania [AC / DC]	16–24 V DC lub 16–18 V AC
Pobór prądu	w stanie czuwania maksymalnie 50 mA, podczas nadawania krótkotrwale maksymalnie 200 mA
Zasilanie zapasowe [BAT]	akumulator ołowiowy 12 V
Prąd ładowania akumulatora	maksymalnie 500 mA
Zasilanie urządzeń zewnętrznych [+12V]	12 V DC, maksymalnie 1 A
Zaciski dwufunkcyjne [IN/OUT]	3; jako wejście typu NC, NO, EOL = 10 kΩ lub EOL_T, jako wyjście typu otwarty kolektor (OC), maksymalnie 100 mA
Liczba partycji	8
Liczba stref	4 (z ekspanderami do 12)
Liczba wyjść PGM	2 (5, jeśli zaciski I/O ustawisz jako wyjścia; z ekspanderami do 12)
Długość magistrali 1-Wire [1 WIRE]	maksymalnie 30 m
Kompatybilne czujniki temperatury	Maxim® / Dallas® DS18S20, DS18B20
Liczba czujników temperatury na magistrali 1-Wire	maksymalnie 8

Parametr	Wartość
Kompatybilne klucze iButton [1 WIRE]	Maxim® / Dallas® DS1990A
Liczba kluczy iButton	maksymalnie 12
Długość magistrali RS485	maksymalnie 100 m
Liczba urządzeń podłączanych do magistrali RS485	maksymalnie 8
Obsługiwane moduły	ekspander **iO8**; ekspander **iO**; **iO-MOD** – nadajnik-odbiornik radiowy iO-WL; ekspander bezprzewodowy **iO-WL**; moduł Ethernet **E485**; moduł Wi-Fi **W485**; czytnik kluczy iButton **TM17**; czytnik kluczy iButton **CZ-Dallas**; **FLS** – czujnik poziomu paliwa Strela RS485; ekspander **iO-LORA**; ekspander **iO8-LORA**; przycisk napadowy **PB-LORA**; ekspander **REL-LORA**
Bufor niewysłanych zdarzeń	60 zdarzeń
Liczba kanałów komunikacji	2 (kanał 1: główny i zapasowy; kanał 2: Protegus)
Zegar wewnętrzny	jest
Wysyłanie zdarzeń	GPRS lub 4G, SMS
Połączenie ze stacją monitorowania	TCP/IP lub UDP/IP, a także SMS
Protokoły transmisji	TRK, szyfrowany SIA DC-09_2007, SIA DC-09_2012, SIA DC-09_IPcom
Warunki pracy	–10 … +50 °C; wilgotność względna maksymalnie 70 % w zakresie 0 … +40 °C (bez kondensacji)
Wymiary	113 × 70 × 25 mm
Masa	100 g

Wycofane akcesorium

Spośród modułów z tabeli **iO**, **iO-WL**, **iO-MOD**, **TM17**, **CZ-Dallas** i **Strela RS485 (FLS)** to wycofane akcesoria, które nie są już dostępne w sprzedaży; ich opis pozostał dla istniejących systemów.

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

1.4 Części centrali

Liczby na rysunku oznaczają części centrali: po lewej zamknięta obudowa, po prawej płytka drukowana ze zdjętą pokrywą.



Rysunek 2. Części CG17.

- 1 złącze SMA anteny komórkowej
- 2 diody sygnalizacyjne LED
- 3 otwór do zdejmowania górnej pokrywy
- 4 listwy zaciskowe do podłączeń zewnętrznych
- 5 złącze USB Mini-B do programowania CG17
- 6 gniazdo karty nano-SIM

1.5 Zaciski

Nazwy zacisków są podane na pokrywie, nad listwami zaciskowymi (od lewej do prawej).

Zacisk	Przeznaczenie
AC/+DC	napięcie zasilania: biegun dodatni 16–18 V AC lub 16–24 V DC
AC/−DC	napięcie zasilania: biegun ujemny 16–18 V AC lub 16–24 V DC
BAT+	biegun dodatni zapasowego akumulatora 12 V
BAT−	biegun ujemny zapasowego akumulatora 12 V
+5V	dodatni zacisk zasilania 5 V dla urządzeń 1-Wire
1 WIRE	zacisk magistrali danych 1-Wire
A RS485	zacisk A magistrali RS485
B RS485	zacisk B magistrali RS485
1 IN	wejście 1 (fabrycznie: **Delay** – strefa opóźniona, typ EOL)
2 I/O	wejście lub wyjście: wejście 2 albo wyjście typu otwarty kolektor (OC) (fabrycznie: **Interior** – strefa wewnętrzna, typ EOL)

Zacisk	Przeznaczenie
COM	wspólny zacisk ujemny
3 I/O	wejście lub wyjście: wejście 3 albo wyjście typu otwarty kolektor (OC) (fabrycznie: **Instant** – strefa natychmiastowa, typ EOL)
4 I/O	wejście lub wyjście: wejście 4 albo wyjście typu otwarty kolektor (OC) (fabrycznie: **Fire** – strefa pożarowa, typ EOL)
+12V	dodatni zacisk zasilania 12 V dla urządzeń zewnętrznych
5 OUT	wyjście typu otwarty kolektor (OC) (fabrycznie: **Fire sensor reset** – reset czujek pożarowych)
6 OUT	wyjście typu otwarty kolektor (OC) (fabrycznie: **Siren** – sygnalizator)

1.6 Sygnalizacja diod LED

Dioda	Świecenie	Znaczenie
NETWORK	zielona, ciągła	połączony z siecią komórkową
	miganie na żółto	poziom sygnału sieci komórkowej, 0–5 mignięć; 3 już wystarczą
DATA	zielona, ciągła	trwa wysyłanie wiadomości
	żółta, ciągła	w buforze są niewysłane zdarzenia
POWER	miganie na zielono	napięcie zasilania prawidłowe
	miganie na żółto	napięcie zasilania nieprawidłowe
	miganie na zielono i żółto	tryb konfiguracji
TROUBLE	nie świeci	brak usterki
	1 mignięcie	brak karty SIM
	2 mignięcia	błędny kod PIN karty SIM
	3 mignięcia	nie może połączyć się z siecią komórkową
	4 mignięcia	nie może połączyć się z odbiornikiem IP w kanale głównym
	5 mignięć	nie może połączyć się z odbiornikiem IP w kanale zapasowym
	6 mignięć	zegar wewnętrzny CG17 nie jest ustawiony
	7 mignięć	napięcie zasilania zapasowego (akumulatora) jest niewystarczające
	8 mignięć	brak zasilania AC
	9 mignięć	błąd połączenia z modułem RS485

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.

1.7 Narzędzia potrzebne do instalacji

Przed rozpoczęciem instalacji sprawdź, czy masz pod ręką wszystko, co potrzebne; akcesoria możesz zamówić u swojego sprzedawcy:

1. kabel USB Mini-B do konfiguracji (rozdział 2);
2. płaski śrubokręt do otwarcia obudowy (rozdział 2);
3. wkręty do zamocowania obudowy (punkt 3.1);
4. aktywną kartę nano-SIM, z której można dzwonić, wysyłać i odbierać SMS-y oraz korzystać z mobilnego internetu (punkt 3.1);
5. zasilacz: 16–24 V DC lub 16–18 V AC;
6. akumulator ołowiowy 12 V, jeśli używasz także zasilania zapasowego.

W zestawie z CG17 jest antena komórkowa ANT01S. Jeśli w miejscu instalacji sygnał jest słaby albo urządzenie jest ekranowane metalową skrzynką lub grubą ścianą, użyj anteny zewnętrznej z przewodem 2,5 m:

Antena magnetyczna Trikdis ME301M z drutem 2,5 m

Trikdis Ant04 GSM Stick-on Antena z drutem 2,5 m

2. Szybka konfiguracja

Ten rozdział opisuje ustawienia, dzięki którym CG17 wysyła zdarzenia do stacji monitorowania (punkt 2.2), a systemem można sterować z aplikacji Protegus 2 (punkt 2.1).

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!

1. Płaskim śrubokrętem otwórz obudowę CG17 tak, jak pokazuje rysunek.



Rysunek 3. Zdejmowanie pokrywy: włóż śrubokręt do otworu z boku obudowy i podważając w dół, odepnij pokrywę. Pod nią, na płytce drukowanej, jest złącze USB Mini-B.

2. Połącz CG17 z komputerem kablem **USB Mini-B**.
3. Uruchom TrikdisConfig. Program automatycznie rozpozna podłączoną centralę CG17 i otworzy jej okno konfiguracji.

4. Kliknij przycisk **Read [F4]**: program odczyta ustawienia CG17. Jeśli program o to poprosi, w wyskakującym oknie podaj 6-cyfrowy kod administratora lub instalatora.

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

2.1 Konfiguracja dla aplikacji Protegus 2

Na stronie **System Options**, w grupie **SIM**:

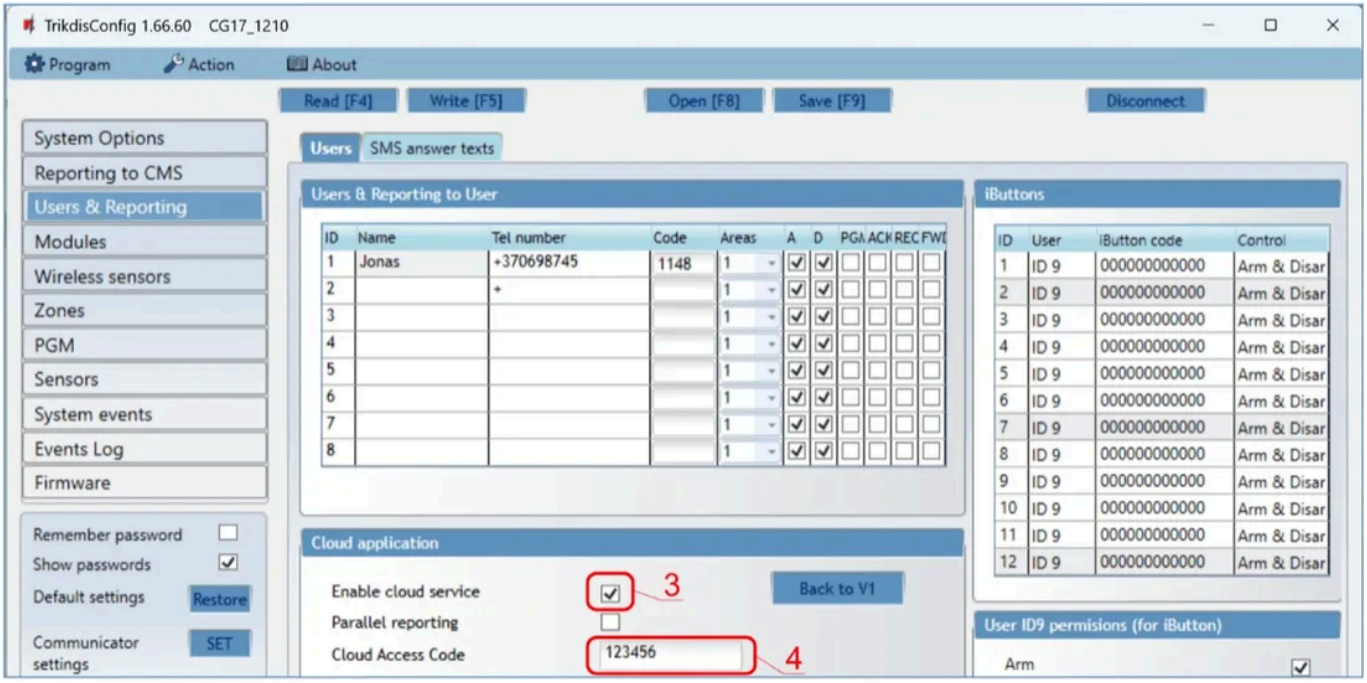


Rysunek 4. TrikdisConfig – **System Options**, karta **System general**, grupa **SIM**.

- 1 **SIM card PIN** – kod PIN karty SIM
- 2 **APN** – punkt dostępu mobilnego internetu

1. Podaj kod PIN karty SIM (**SIM card PIN**).
2. W polu **APN** wpisz APN swojego operatora komórkowego. Znajdziesz go na stronie operatora; „internet" jest uniwersalny i działa w sieciach wielu operatorów. Dane operatorów europejskich: Ustawienie APN – lista europejskich operatorów komórkowych.

Na stronie **Users & Reporting**, w grupie **Cloud application**:



Rysunek 5. TrikdisConfig – **Users & Reporting**, grupa **Cloud application**.

- 3 **Enable cloud service** – włączenie chmury Protegus
- 4 **Cloud Access Code** – kod dostępu do chmury (fabrycznie `123456`)

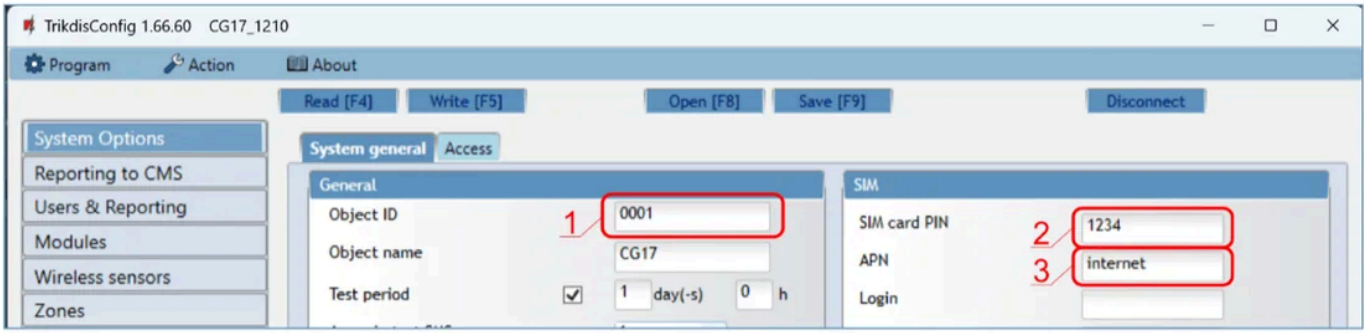
3. Zaznacz pole **Enable cloud service**: w ten sposób włączysz połączenie z chmurą Protegus.
4. Jeśli chcesz, aby użytkownicy przy dodawaniu systemu do Protegus 2 musieli podać kod, zmień wartość **Cloud Access Code** (fabrycznie `123456`).

Po zakończeniu ustawień kliknij przycisk **Write [F5]** i odłącz kabel USB. Dodawanie systemu do aplikacji Protegus 2: punkt 4.1.

Pozostałe ustawienia CG17 w TrikdisConfig opisuje rozdział 5.

2.2 Konfiguracja dla stacji monitorowania

Ustawienia połączenia ze stacją monitorowania są na stronie **System Options**:



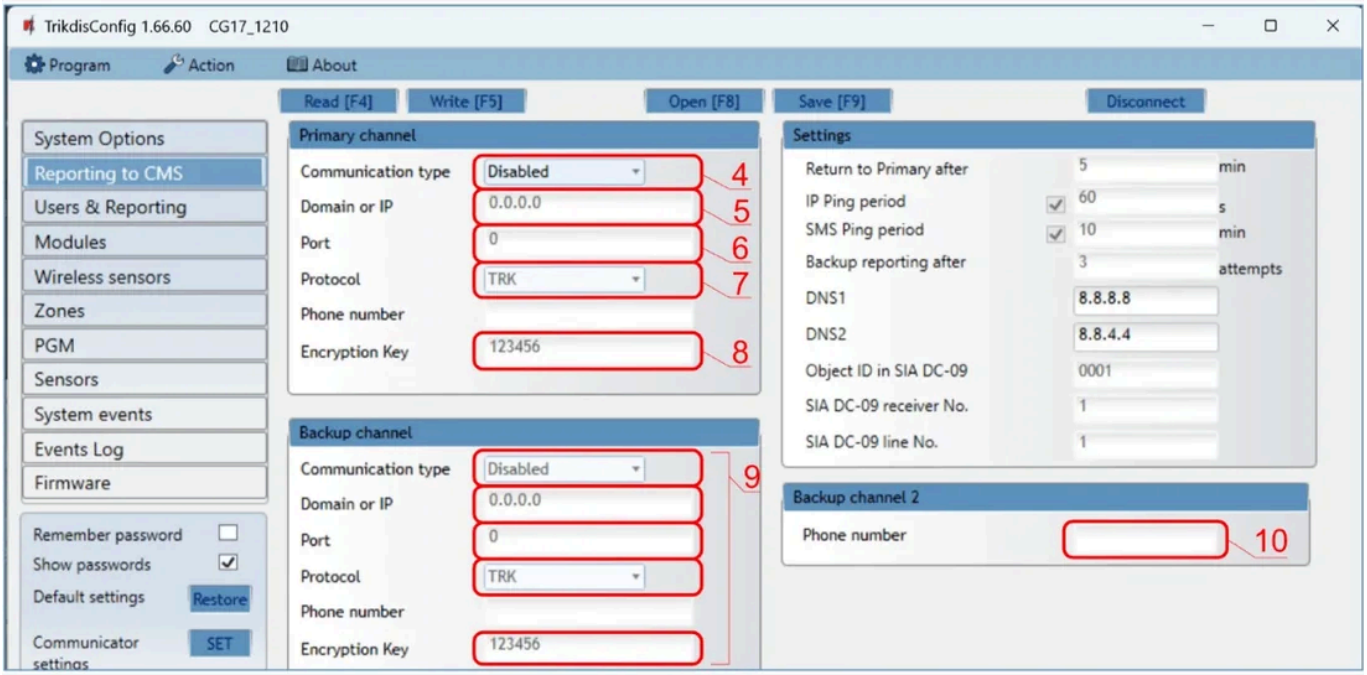
Rysunek 6. TrikdisConfig – **System Options**, karta **System general**.

- 1 **Object ID** – identyfikator obiektu
- 2 **SIM card PIN** – kod PIN karty SIM
- 3 **APN** – punkt dostępu mobilnego internetu

1. Podaj identyfikator obiektu otrzymany od stacji monitorowania (**Object ID**): 4 znaki, 0–9 i A–F. **Nie używaj identyfikatorów FFFE i FFFF.**
2. Podaj kod PIN karty SIM (**SIM card PIN**).

3. W polu **APN** wpisz APN swojego operatora komórkowego. Znajdziesz go na stronie operatora; „internet" jest uniwersalny i działa w sieciach wielu operatorów.

Na stronie **Reporting to CMS** są ustawienia kanału głównego (**Primary channel**):



Rysunek 7. TrikdisConfig – **Reporting to CMS**.

- 4 **Communication type** – typ połączenia
- 5 **Domain or IP** – adres odbiornika
- 6 **Port** – port odbiornika
- 7 **Protocol** – protokół transmisji
- 8 **Encryption Key** – klucz szyfrowania
- 9 **Backup channel** – kanał zapasowy
- 10 **Backup channel 2** – numer telefonu rezerwy SMS

4. **Communication type** – wybierz sposób połączenia IP (**TCP/IP** lub **UDP/IP**). Nie zalecamy SMS-a jako kanału głównego.
5. **Domain or IP** – wpisz nazwę domeny lub adres IP odbiornika.
6. **Port** – wpisz port sieciowy odbiornika.
7. **Protocol** – wybierz protokół komunikatów o zdarzeniach: **TRK** (do odbiorników Trikdis), **DC-09_2007**, **DC-09_2012** lub **DC-09_IPcom** (do odbiorników uniwersalnych).
8. **Encryption Key** – wpisz klucz szyfrowania ustawiony w odbiorniku.

Jeśli raportujesz do stacji monitorowania SMS-em, wystarczy wypełnić pola **Encryption Key** i **Phone number**. Wiadomości SMS odbierają tylko odbiorniki Trikdis: odbiornik IP/SMS **RL14**, odbiornik wielokanałowy **RM14** i odbiornik SMS **GM14**. Jeśli wybrałeś protokół **DC-09**, w grupie **Settings** strony **Reporting to CMS** podaj także numer obiektu, linii i odbiornika (punkt 5.3).

9. (Zalecane) Ustaw kanał zapasowy (**Backup channel**).
10. (Zalecane) Podaj numer telefonu używany do raportowania SMS-em w **Backup channel 2**.

Po zakończeniu ustawień kliknij przycisk **Write [F5]** i odłącz kabel USB.

Pozostałe ustawienia CG17 w TrikdisConfig opisuje rozdział 5.

3. Instalacja i podłączenie

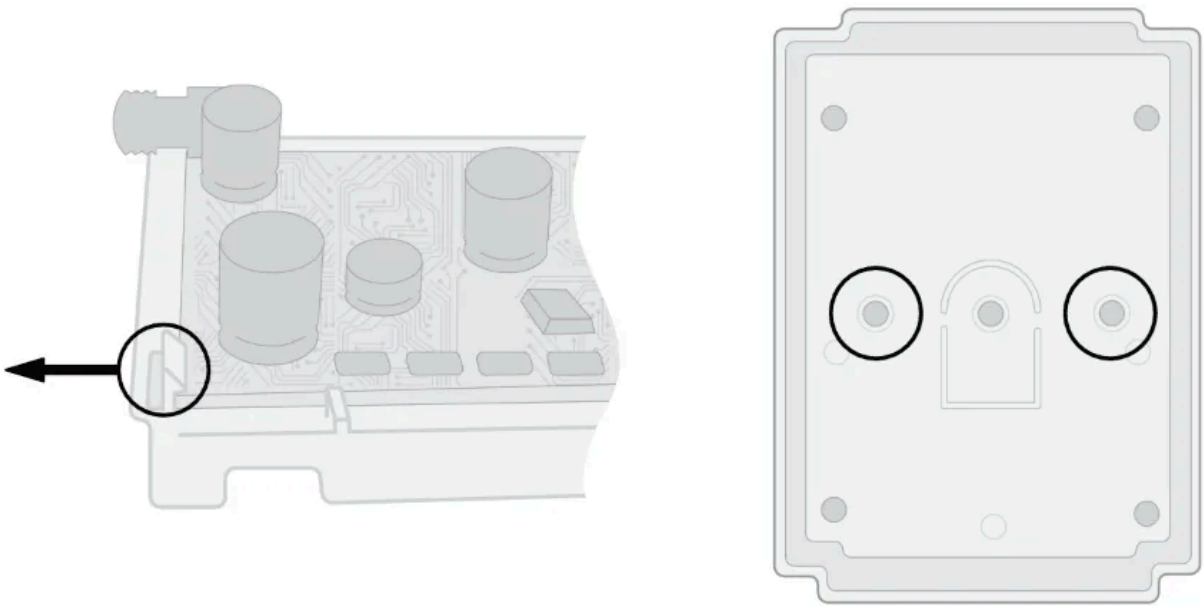
Figyelem!

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

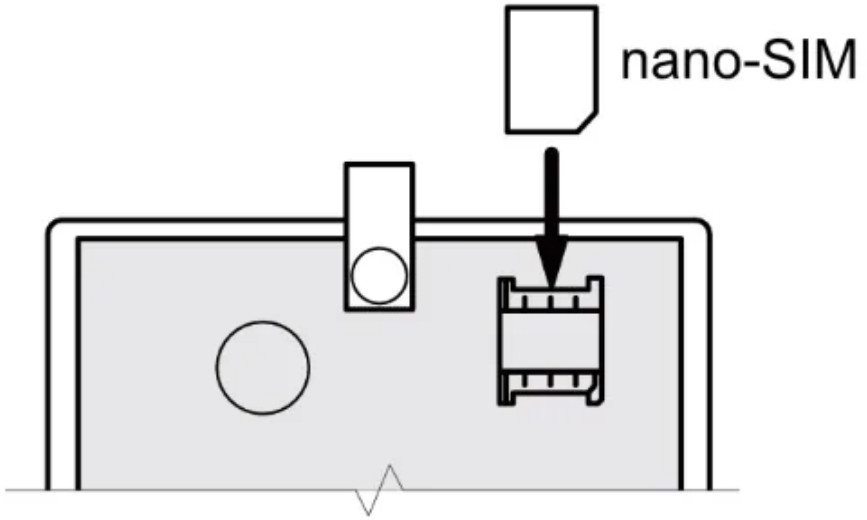
Ten rozdział opisuje montaż CG17 i włożenie karty SIM, podłączenie czujek, wyjść, sygnalizatora i akumulatora, a następnie podłączenie czytników kluczy, ekspanderów i modułów komunikacyjnych (iO8, W485, E485, RF-LORA i iO-LORA). Przeznaczenie zacisków podaje punkt 1.5. Na rysunkach „x IN" lub „INx" oznacza wybrane wejście, a „x OUT" lub „xOUT" – wybrane wyjście.

3.1 Montaż i włożenie karty SIM

1. Zanim zaczniesz, sprawdź, czy w planowanym miejscu montażu CG17 sygnał sieci komórkowej jest wystarczający.
2. Zdejmij górną pokrywę (odepnij ją płaskim śrubokrętem, jak na rysunku na początku rozdziału 2), a następnie zdejmij listwy zaciskowe.
3. Wyjmij płytkę drukowaną z obudowy: wciśnij zatrzask i wyciągnij płytkę.
4. Przykręć tylną część obudowy wkrętami w wybranym miejscu.
5. Włóż z powrotem płytkę drukowaną i listwy zaciskowe.
6. Przykręć antenę komórkową do złącza SMA (punkt 1.4).
7. Włóż kartę nano-SIM do gniazda. Karta SIM musi być aktywowana w sieci komórkowej i mieć włączone wszystkie potrzebne usługi: musi umożliwiać dzwonienie, wysyłanie i odbieranie SMS-ów oraz korzystanie z mobilnego internetu. O włączenie usług zapytaj operatora komórkowego karty SIM.



Rysunek 8. Po lewej zatrzask płytki drukowanej (wciśnięty w kierunku strzałki zwalnia płytkę), po prawej dwa otwory na wkręty w tylnej części obudowy.



Rysunek 9. Wkładanie karty nano-SIM („nano-SIM") w kierunku strzałki do gniazda na płytce drukowanej.

Sprawdź, czy karta SIM jest aktywowana. Jeśli łączysz się także kanałem IP (przez mobilny internet), usługa mobilnego internetu musi być włączona. Jeśli nie chcesz podawać kodu PIN w TrikdisConfig, włóż kartę SIM do telefonu komórkowego i wyłącz w nim żądanie kodu PIN.

8. Jeśli chcesz konfigurować CG17 także zdalnie, włóż do niego kartę SIM z wyłączonym żądaniem kodu PIN, a następnie wyślij na numer telefonu CG17 taki SMS: `CONNECT 123456 PROTEGUS=ON,APN=INTERNET`. 123456 to fabryczne hasło SMS administratora (**SMS password**, punkt 5.2), `PROTEGUS=ON` włącza usługę chmury Protegus, a `APN=INTERNET` to punkt dostępu mobilnego internetu (jeśli twój operator ma inny, wpisz jego APN). Opis poleceń SMS jest w punkcie 4.2.
9. Konfigurację zdalną opisuje punkt 6.1.
10. Załóż z powrotem górną pokrywę.

Listwy zaciskowe są wyjmowane: wyjmując listwę z zaciskami zasilania (**AC/+DC**, **AC/−DC**, **BAT+**, **BAT−**), jednym ruchem odłączysz zasilanie urządzenia lub je zrestartujesz; przy podłączaniu listwy łatwiej się obsługuje, a do programowania przez USB urządzenie można zanieść do komputera.

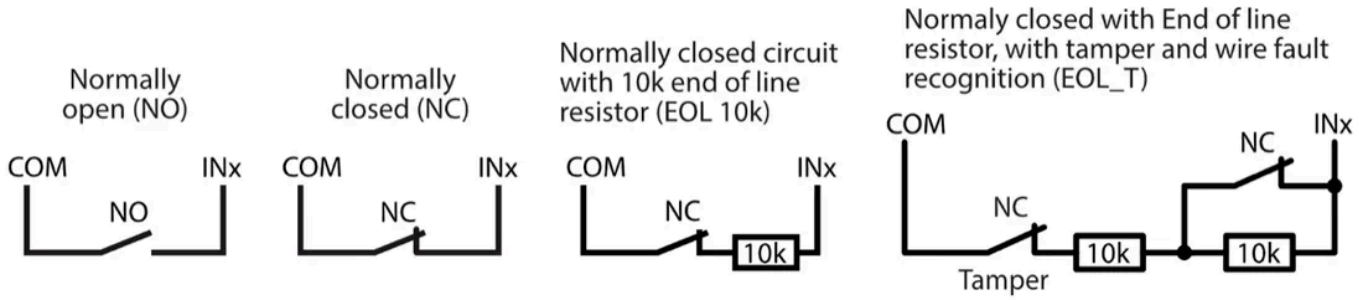
3.2 Podłączenie wejść

CG17 ma cztery wejścia (IN) do podłączenia czujek systemu alarmowego. Sposoby podłączenia czujki: **NO** – styk normalnie otwarty; **NC** – styk normalnie zamknięty; **EOL** – obwód normalnie zamknięty z rezystorem końca linii 10 kΩ; **EOL_T** – obwód normalnie zamknięty z rezystorem końca linii 10 kΩ, z rozpoznawaniem sabotażu i uszkodzenia przewodu.

Fabryczne ustawienia stref (wejść):

Strefa	Ustawienie fabryczne
1 IN	**Delay** – strefa opóźniona, typ EOL, partycja 1
2 I/O	**Interior** – strefa wewnętrzna, typ EOL, partycja 1
3 I/O	**Instant** – strefa natychmiastowa, typ EOL, partycja 1
4 I/O	**Fire** – strefa pożarowa, typ EOL, partycja 1

Zmianę ustawień stref i ich przypisanie do partycji opisuje punkt 5.6 (okno **Zones**). Możliwe sposoby podłączenia:

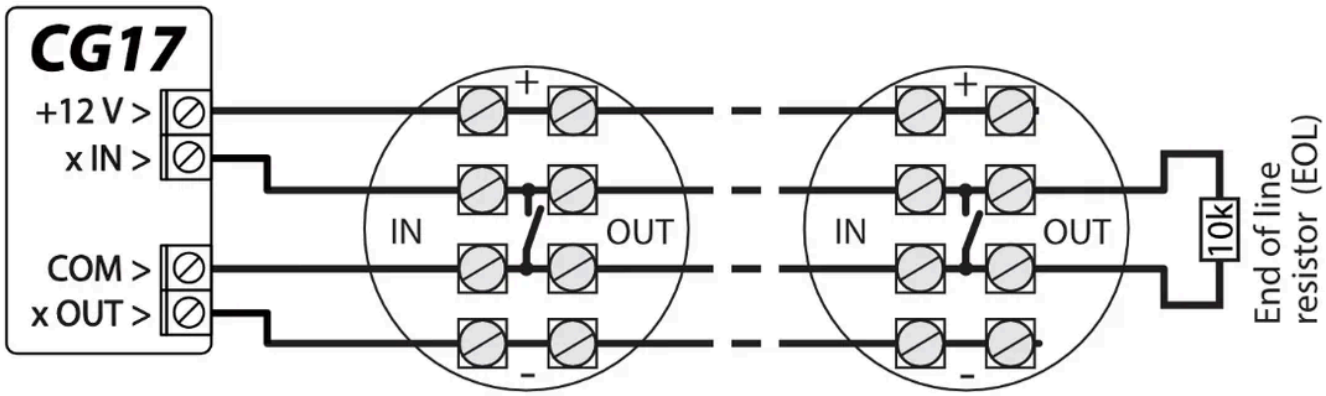


Rysunek 10. Sposoby podłączenia wejść między zaciskami COM i INx (wybrane wejście). Od lewej do prawej: styk normalnie otwarty („Normally open (NO)"); styk normalnie zamknięty („Normally closed (NC)"); obwód normalnie zamknięty z szeregowo podłączonym rezystorem końca linii 10 kΩ („Normally closed circuit with 10k end of line resistor (EOL 10k)"); obwód normalnie zamknięty z rezystorem końca linii, z rozpoznawaniem sabotażu i uszkodzenia przewodu („Normaly closed with End of line resistor, with tamper and wire fault recognition (EOL_T)"): COM → styk sabotażowy NC („Tamper") → 10 kΩ → styk alarmowy NC, równolegle do niego 10 kΩ → INx.

3.3 Podłączenie czujek dymu

Aby czujkę dymu można było zresetować po alarmie, nadaj jednemu wyjściu PGM funkcję **Fire Sensor Reset** (reset czujek pożarowych): TrikdisConfig, okno **PGM**, karta **Outputs** (punkt 5.7). Fabrycznie tę funkcję ma wyjście **5 OUT**, a **4 I/O** jest strefą pożarową (**Fire**). Na rysunkach x OUT to to wyjście, a x IN – strefa czujek dymu.

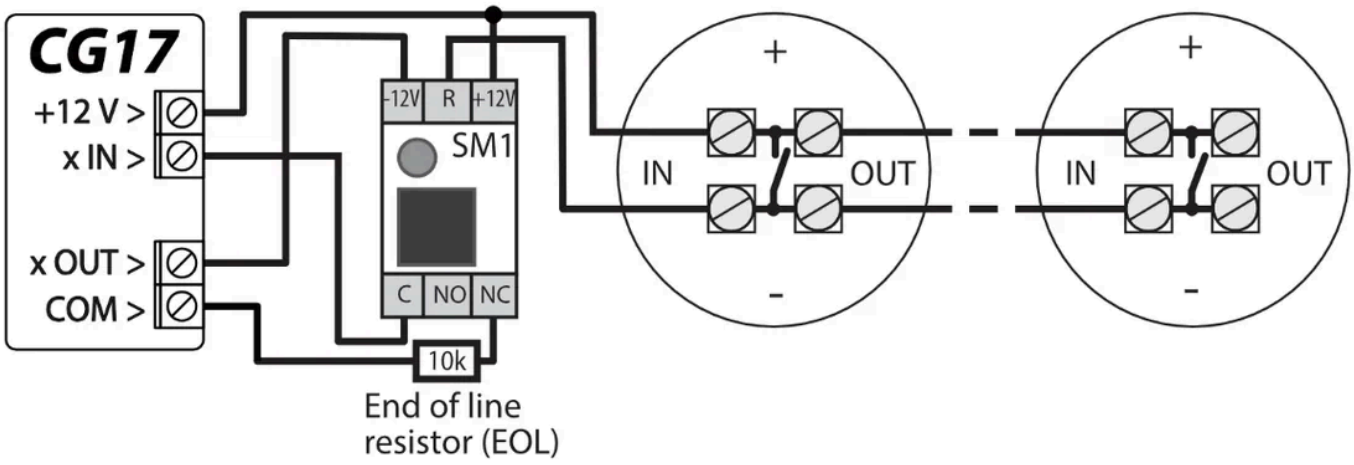
- **Podłączenie czteroprzewodowej czujki dymu**



Rysunek 11. Czteroprzewodowe czujki dymu w łańcuchu: zacisk +12 V CG17 → zacisk + czujek, x OUT → zacisk − (zasilanie czujek); x IN i COM → dwa zaciski sygnałowe, między nimi styk alarmowy czujki. Przewody biegną od zacisków wejściowych („IN") czujki przez zaciski wyjściowe („OUT") do następnej czujki; między dwa zaciski sygnałowe ostatniej czujki włącza się rezystor końca linii („End of line resistor (EOL)") 10 kΩ („10k").

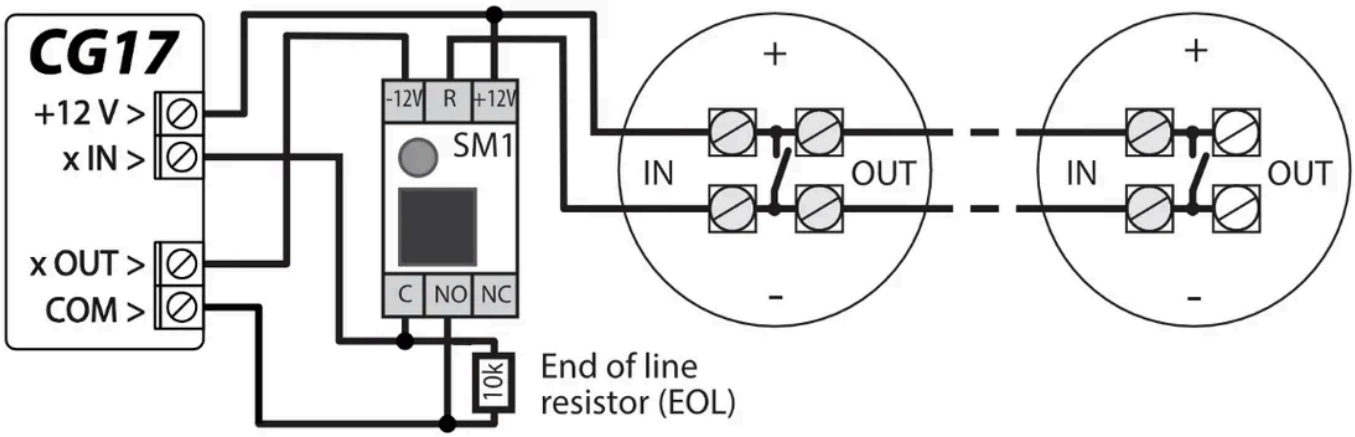
- **Podłączenie dwuprzewodowej czujki dymu** z modułem SM1*:

1. Ze strefą typu EOL (lub strefą typu NC, bez rezystora końca linii):



Rysunek 12. Dwuprzewodowe czujki dymu ze stykiem NC modułu SM1: zacisk +12 V CG17 → zacisk +12V SM1 i zacisk + pierwszej czujki; x OUT → zacisk -12V SM1; zacisk R SM1 → zacisk − czujki; zaciski wejściowe („IN") i wyjściowe („OUT") czujek w łańcuchu. Obwód strefy: x IN → zacisk C SM1; COM → rezystor końca linii („End of line resistor (EOL)") 10 kΩ („10k") → zacisk NC SM1.

2. Ze strefą typu EOL (lub strefą typu NO, bez rezystora końca linii):



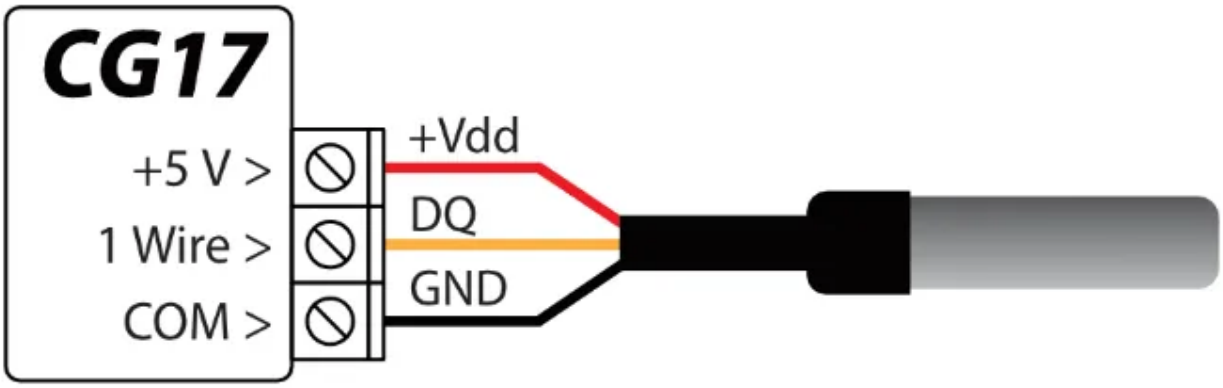
Rysunek 13. To samo ze stykiem NO modułu SM1: podłączenie zasilania i czujek jest takie samo; x IN → zacisk C SM1, zacisk NO SM1 → COM; rezystor końca linii („End of line resistor (EOL)") 10 kΩ („10k") między przewodem x IN i COM, równolegle do styku NO.

*SM1 to moduł pośredniczący Trikdis, dzięki któremu dwuprzewodową czujkę dymu można po alarmie zresetować zdalnie.

3.4 Podłączenie czujnika temperatury

- Czujniki temperatury podłącz według poniższego rysunku. Do CG17 można podłączyć maksymalnie 8 czujników temperatury Maxim® / Dallas® DS18S20 lub DS18B20.
- Jeśli przewód czujnika jest dłuższy niż 0,5 m, użyj kabla typu skrętka (UTP 4×2×0,5 lub STP 4×2×0,5).

DS18B20 Czujnik temperatury z drutem 1m

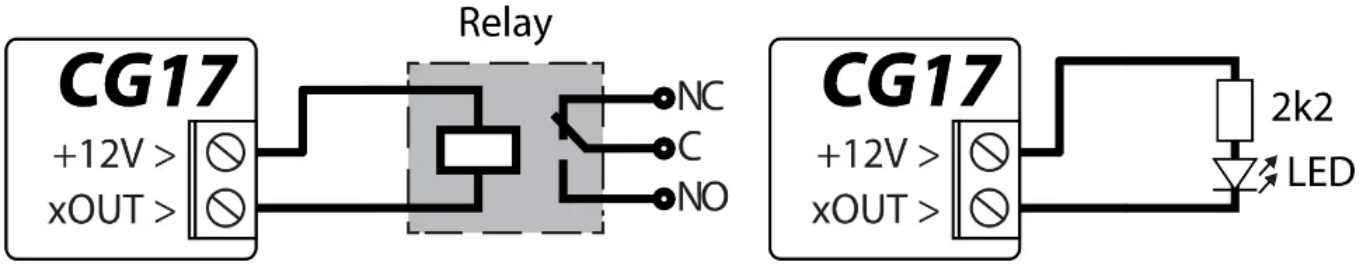


Rysunek 14. Podłączenie czujnika temperatury: zacisk +5 V CG17 → +Vdd (przewód czerwony), 1 Wire → DQ (przewód żółty), COM → GND (przewód czarny).

Kolory przewodów: Vdd – przewód czerwony, podłącz go do zacisku **+5V**; DQ – przewód żółty, do zacisku **1 WIRE**; GND – przewód czarny, do zacisku **COM**. Czujniki konfiguruje się w oknie **Sensors** (punkt 5.8).

3.5 Podłączenie przekaźnika i diody LED

Wyjścia (**5 OUT**, **6 OUT** oraz ustawione jako wyjścia **2 I/O**, **3 I/O** i **4 I/O**) są typu otwarty kolektor (punkt 1.5): cewkę przekaźnika lub diodę LED podłącz między zacisk **+12V** a wyjście. Stykami przekaźnika możesz przełączać urządzenie zewnętrzne (funkcja **Remote Control**), a dioda LED może sygnalizować stan systemu (funkcja **System state**); funkcje wyjść opisuje punkt 5.7.



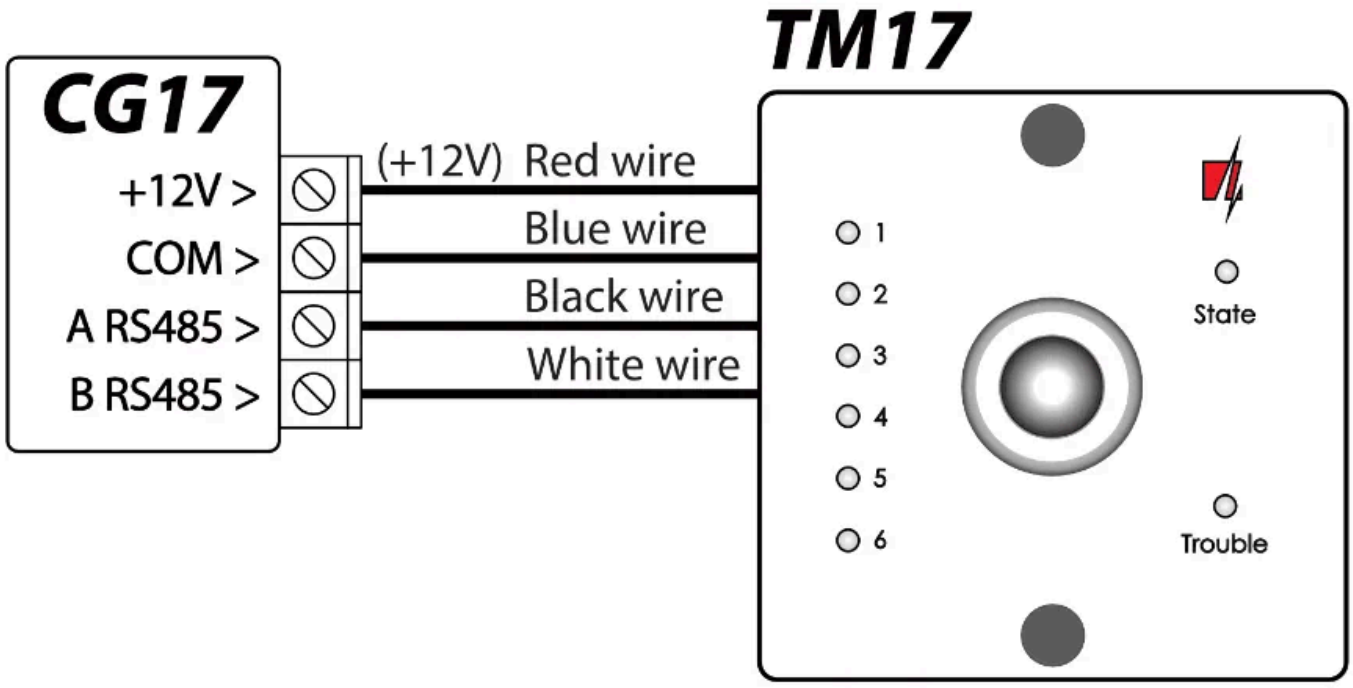
Rysunek 15. Po lewej przekaźnik („Relay"): cewka między zaciskami +12V i xOUT, styki przekaźnika NC, C i NO. Po prawej dioda LED („LED"): +12V → rezystor 2,2 kΩ („2k2") → LED → xOUT.

3.6 Podłączenie czytników kluczy iButton

Wycofane akcesorium

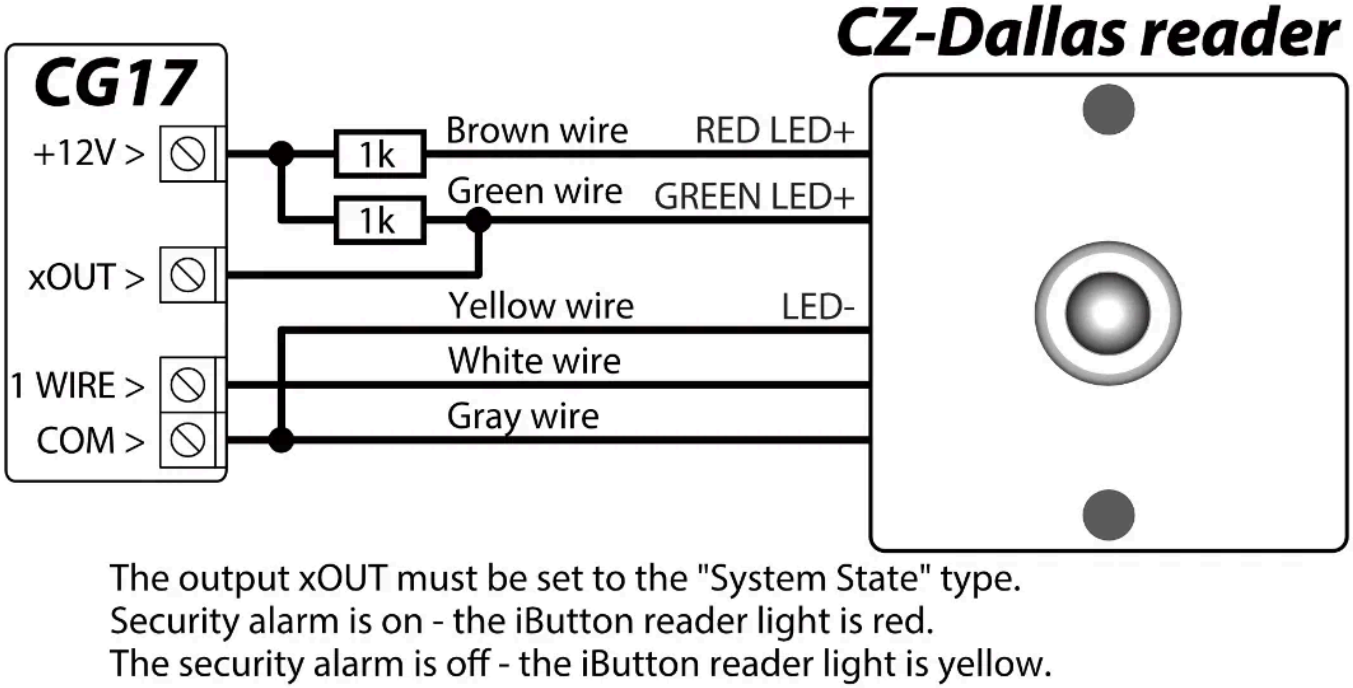
Czytniki kluczy iButton **TM17** i **CZ-Dallas** to wycofane akcesoria, które nie są już dostępne w sprzedaży. Opis pozostał dla istniejących systemów.

Czytnik **TM17** podłącz do magistrali danych **RS485**; przewód magistrali może mieć maksymalnie 100 m. Do CG17 można podłączyć maksymalnie osiem czytników TM17.



Rysunek 16. Czytnik TM17: zacisk +12V CG17 → przewód czerwony („(+12V) Red wire"), COM → niebieski („Blue wire"), A RS485 → czarny („Black wire"), B RS485 → przewód biały („White wire"). Na panelu przednim czytnika diody 1–6, dioda stanu („State") i dioda usterki („Trouble"), pośrodku powierzchnia dotykowa klucza iButton.

Czytnik kluczy iButton (CZ-Dallas) podłącz do zacisku **1 WIRE**; przewód może mieć maksymalnie 30 m.



The output xOUT must be set to the "System State" type.
Security alarm is on - the iButton reader light is red.
The security alarm is off - the iButton reader light is yellow.

Rysunek 17. Czytnik CZ-Dallas („CZ-Dallas reader"): zacisk +12V CG17 → każdy przez osobny rezystor 1 kΩ („1k") na przewód brązowy („Brown wire", dioda czerwona: „RED LED+") i na przewód zielony („Green wire", dioda zielona: „GREEN LED+"); xOUT na przewód zielony, za rezystorem; 1 WIRE → przewód biały („White wire"); COM → przewód żółty („Yellow wire", „LED-") i szary („Gray wire"). Wyjście xOUT musi być ustawione na typ **System State** (stan systemu) („The output xOUT must be set to the »System State« type.") – przy uzbrojonym alarmie dioda czytnika iButton świeci na czerwono („Security alarm is on - the iButton reader light is red."), przy rozbrojonym na żółto („The security alarm is off - the iButton reader light is yellow.").

„Maksymalnie 100 m" i „maksymalnie 30 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

Przypisanie (rejestrację) kluczy do CG17 opisuje punkt 5.4.1.

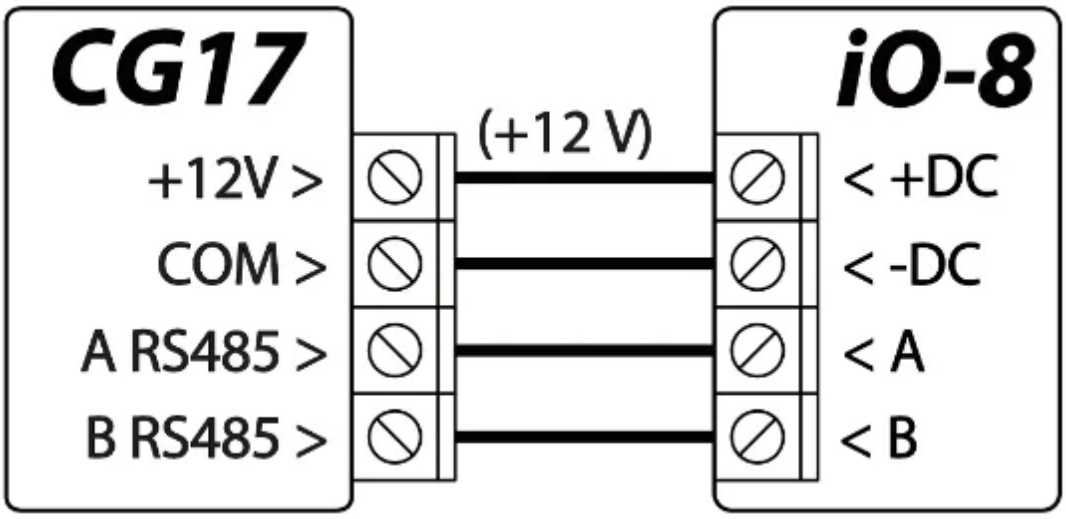
3.7 Podłączenie ekspanderów serii iO

Wycofane akcesorium

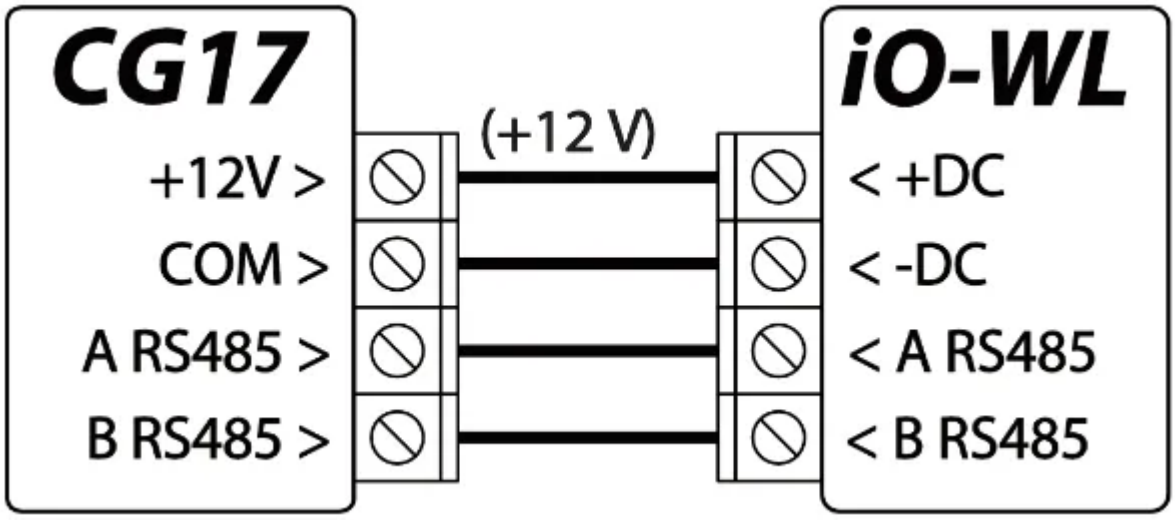
iO-WL to wycofane akcesorium, które nie jest już dostępne w sprzedaży; ekspander **iO8** jest nadal dostępny.

Jeśli CG17 potrzebuje więcej wejść (IN) lub wyjść (OUT), podłącz do niego przewodowy lub bezprzewodowy ekspander wejść i wyjść serii iO firmy Trikdis. Konfigurację ekspanderów w CG17 opisuje punkt 5.5 (okno **Modules**). Do CG17 można podłączyć maksymalnie osiem ekspanderów **iO8**; możesz używać wszystkich stref iO8 albo tylko niektórych. Łączna liczba stref CG17 razem z ekspanderami wynosi 12.

Trikdis IO8 PRZEWIDY MODUŁ EXPADER



Rysunek 18. Podłączenie ekspandera iO8 („iO-8"): zacisk +12V CG17 („(+12 V)") → +DC, COM → −DC, A RS485 → A, B RS485 → B.

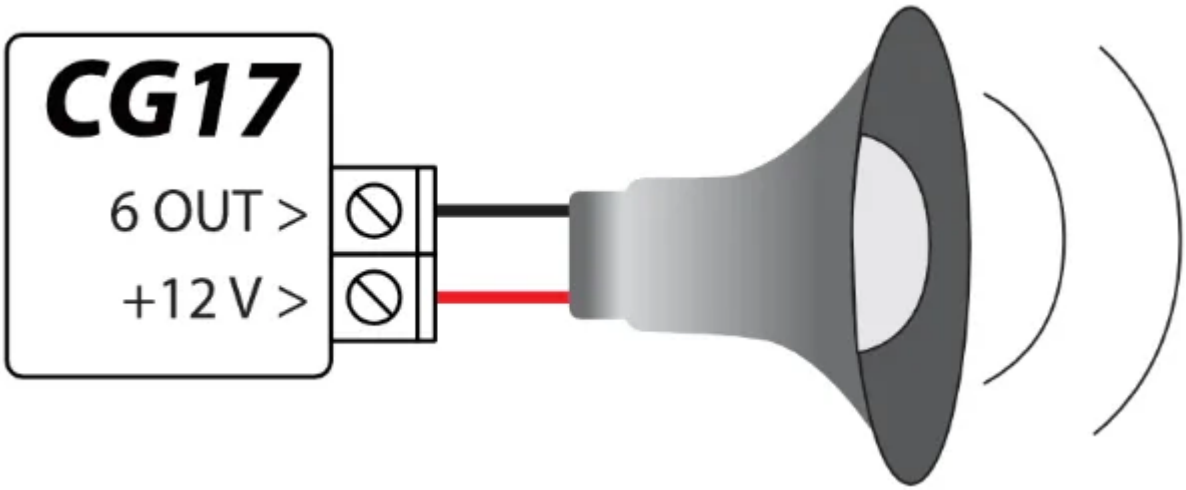


Rysunek 19. Przewodowe podłączenie ekspandera iO-WL („iO-WL"): zacisk +12V CG17 („(+12 V)") → +DC, COM → −DC, A RS485 → A RS485, B RS485 → B RS485.

3.8 Podłączenie sygnalizatora

- Sygnalizator o poborze prądu maksymalnie 1 A można podłączyć do wyjścia **5 OUT** lub **6 OUT**.

- Sygnalizator o poborze prądu maksymalnie 100 mA można podłączyć do dowolnego wyjścia OUT.
- Wyjście musi otrzymać funkcję **Siren** (sygnalizator) i trzeba przypisać do niego partycję systemu alarmowego (okno **PGM**, **Output definition** i **Areas**, punkt 5.7). Fabrycznie wyjściem sygnalizatora jest **6 OUT**.



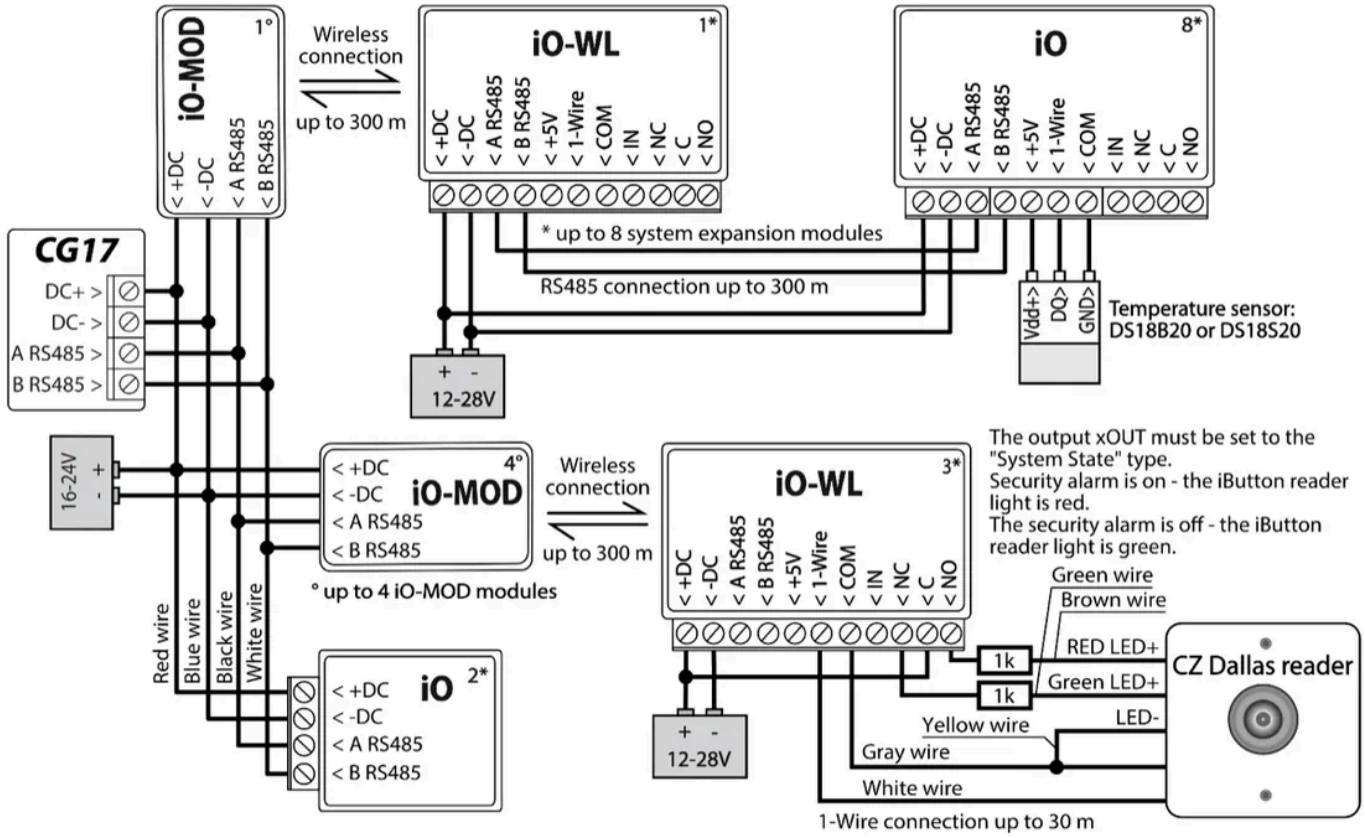
Rysunek 20. Sygnalizator na wyjściu 6 OUT: 6 OUT → przewód czarny, +12 V → przewód czerwony.

3.9 System ekspanderów iO (iO, iO-WL, iO-MOD)

Wycofane akcesorium

iO, **iO-WL** i **iO-MOD** to wycofane akcesoria, które nie są już dostępne w sprzedaży. Opis pozostał dla istniejących systemów; do nowego systemu nadają się ekspandery iO8 lub LORA (punkt 3.16).

Rysunek pokazuje kompletny system iO: na magistrali RS485 przewodowe moduły iO i iO-MOD, ekspandery iO-WL połączone drogą radiową z nadajnikami-odbiornikami iO-MOD, a na nich czujnik temperatury i czytnik iButton.



Rysunek 21. Przegląd systemu iO. Zaciski zasilania CG17 („DC+", „DC-"; na CG17 AC/+DC i AC/−DC) są połączone z zasilaczem 16–24 V („16-24V") oraz z przewodem czerwonym („Red wire") i niebieskim („Blue wire") magistrali, zaciski A RS485 i B RS485 z przewodem czarnym („Black wire") i białym („White wire"); na magistrali zaciski +DC, −DC, A RS485 i B RS485 modułów iO-MOD (1°), iO-MOD (4°) i iO (2*). Połączenie bezprzewodowe („Wireless connection"), maksymalnie 300 m („up to 300 m"): między iO-MOD (1°) a iO-WL (1*)* oraz między iO-MOD (4°) a iO-WL (3*). iO-WL (1*)* i iO (8*) pracują ze wspólnego zasilania 12–28 V („12-28V"), między nimi połączenie RS485 („RS485 connection"), maksymalnie 300 m („up to 300 m"); zaciski +5V, 1-Wire i COM modułu iO (8*)* → zaciski Vdd+, DQ i GND czujnika temperatury („Temperature sensor: DS18B20 or DS18S20"). iO-WL (3*) pracuje z własnego zasilania 12–28 V i obsługuje czytnik CZ-Dallas („CZ Dallas reader") połączeniem 1-Wire o długości maksymalnie 30 m („1-Wire connection up to 30 m"): zacisk C przekaźnika podłączony do +DC, NO → 1 kΩ („1k") → przewód brązowy („Brown wire", dioda czerwona: „RED LED+"), NC → 1 kΩ → przewód zielony („Green wire", dioda zielona: „Green LED+"), COM → przewód szary („Gray wire") i żółty („Yellow wire", „LED-"), 1-Wire → przewód biały („White wire"). Wyjście musi być ustawione na typ ***System State*** *(stan systemu) („The output xOUT must be set to the »System State« type.") – przy uzbrojonym alarmie dioda czytnika iButton świeci na czerwono („Security alarm is on - the iButton reader light is red."), przy rozbrojonym na zielono („The security alarm is off - the iButton reader light is green."). Jednostek oznaczonych gwiazdką może być maksymalnie 8 modułów rozszerzeń systemu („* up to 8 system expansion modules"), a oznaczonych symbolem ° – maksymalnie 4 moduły iO-MOD („° up to 4 iO-MOD modules").

„Maksymalnie 300 m" i „maksymalnie 30 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

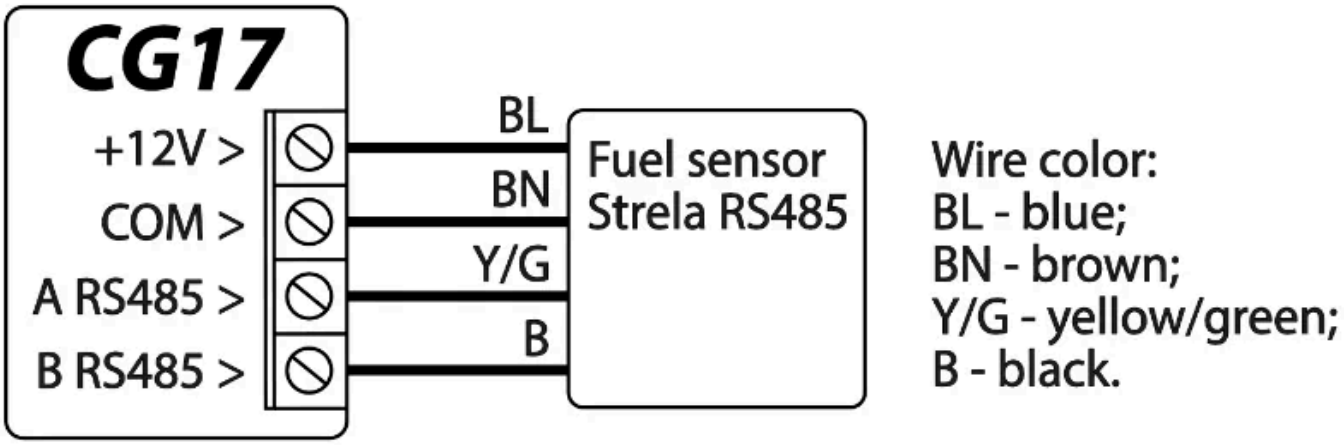
- Jeśli przewód czujnika temperatury jest dłuższy niż 0,5 m, użyj kabla typu skrętka (UTP 4×2×0,5 lub STP 4×2×0,5).
- Do jednej centrali CG17 można podłączyć:
  - maksymalnie cztery moduły iO-MOD;
  - maksymalnie osiem modułów iO i/lub iO-WL.
- Czytniki kluczy iButton i czujniki temperatury podłącz do zacisku „1-Wire".

3.10 Podłączenie czujnika poziomu paliwa Strela

Wycofane akcesorium

Czujnik poziomu paliwa **Strela RS485** to wycofane akcesorium, u nas niedostępne w sprzedaży. Opis pozostał dla istniejących systemów.

Do CG17 można podłączyć jeden czujnik poziomu paliwa **Strela RS485**. Jeśli czujnik poziomu paliwa jest podłączony, do CG17 nie można podłączyć żadnego innego modułu (iO8, iO, iO-WL, TM17, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA). Czujnik trzeba dodać w CG17 w oknie **Modules** (punkt 5.5.3).

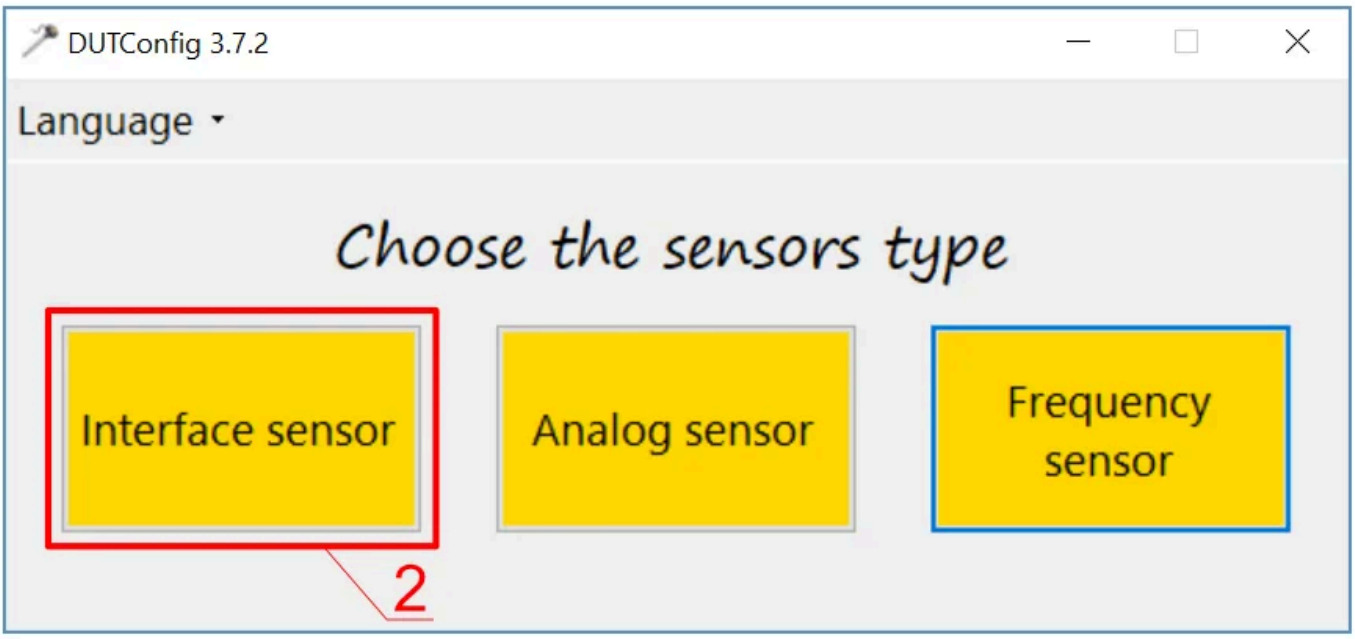


Rysunek 22. Czujnik poziomu paliwa Strela RS485 („Fuel sensor Strela RS485"): zacisk +12V CG17 → przewód BL, COM → BN, A RS485 → Y/G, B RS485 → B. Kolory przewodów („Wire color"): BL – niebieski („blue"), BN – brązowy („brown"), Y/G – żółto-zielony („yellow/green"), B – czarny („black").

Konfiguracja i przygotowanie czujnika

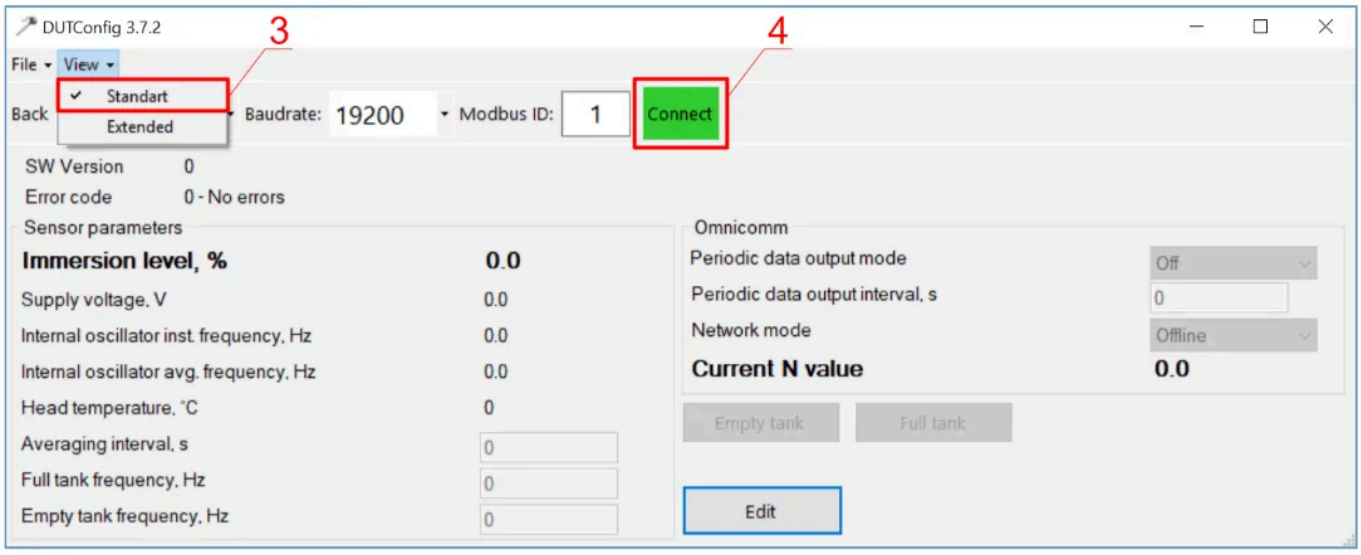
Czujnik poziomu paliwa (Strela RS485) trzeba obowiązkowo skalibrować programem kalibracyjnym Strela **DUTConfig** (pobierz) i podać w nim pojemność zbiornika paliwa – w przeciwnym razie pomiar czujnika może być niedokładny.

1. Podłącz czujnik poziomu paliwa do komputera przez adapter programujący. Naciśnij „brązowy" przycisk adaptera, aby w części RS-485 UART zaświeciła się zielona dioda.
2. Uruchom program **DUTConfig** i wybierz typ **Interface sensor** (czujnik z interfejsem).



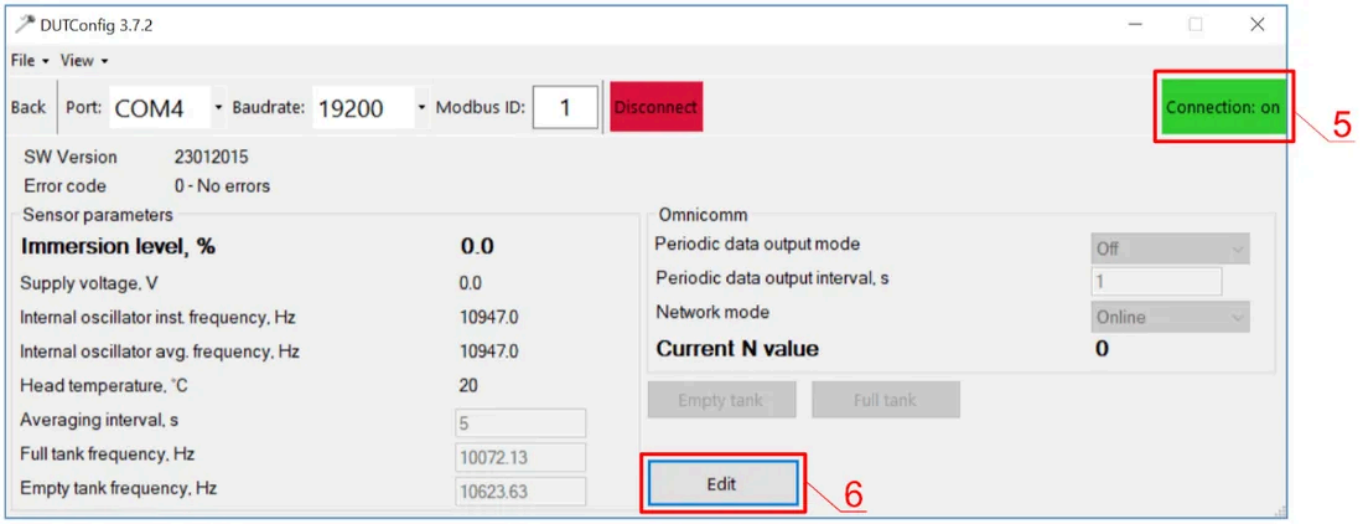
Rysunek 23. DUTConfig – wybór typu czujnika („Choose the sensors type"): **Interface sensor** – czujnik z interfejsem (2); pozostałe możliwości to czujnik analogowy („Analog sensor") i czujnik z wyjściem częstotliwościowym („Frequency sensor"); w menu **Language** można wybrać język programu.

3. W menu **View** (widok) wybierz widok **Standart** (standardowy).
4. Kliknij przycisk **Connect** (połącz) i poczekaj.



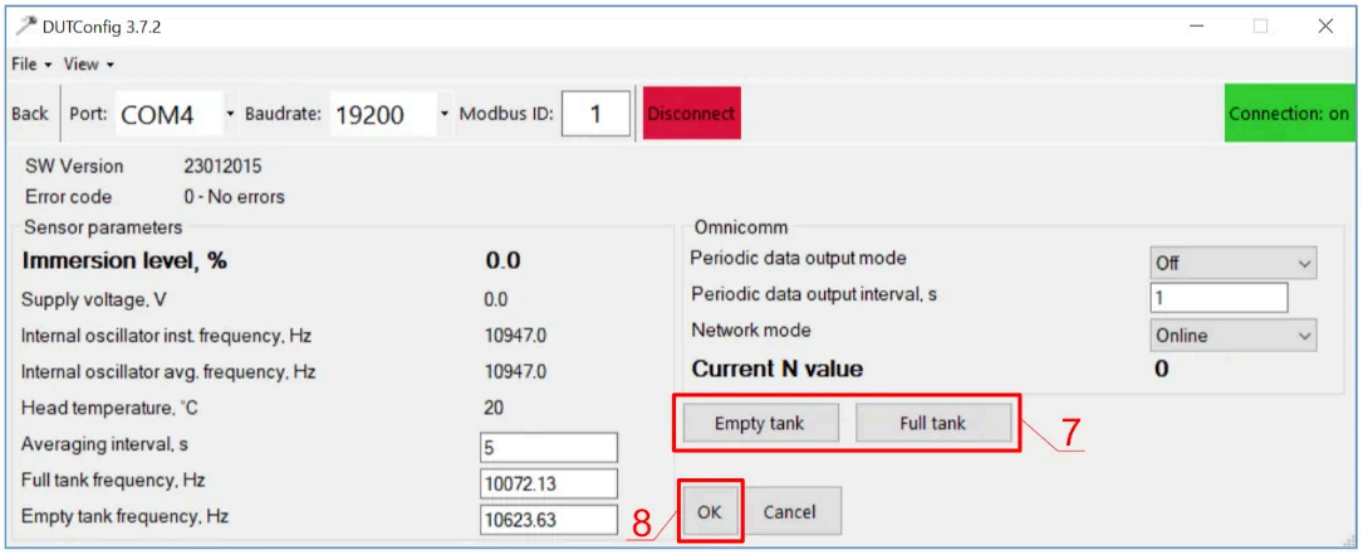
Rysunek 24. Okno ustawień czujnika w DUTConfig: w menu **View** widok **Standart** (3) i zielony przycisk **Connect** (4); obok prędkość transmisji (**Baudrate**, 19200) i identyfikator Modbus (**Modbus ID**, 1), poniżej parametry czujnika (**Sensor parameters**), ustawienia Omnicomm oraz przyciski **Empty tank**, **Full tank** i **Edit**.

5. Gdy czujnik połączy się z DUTConfig, pojawi się napis **Connection: on** (połączenie: włączone).



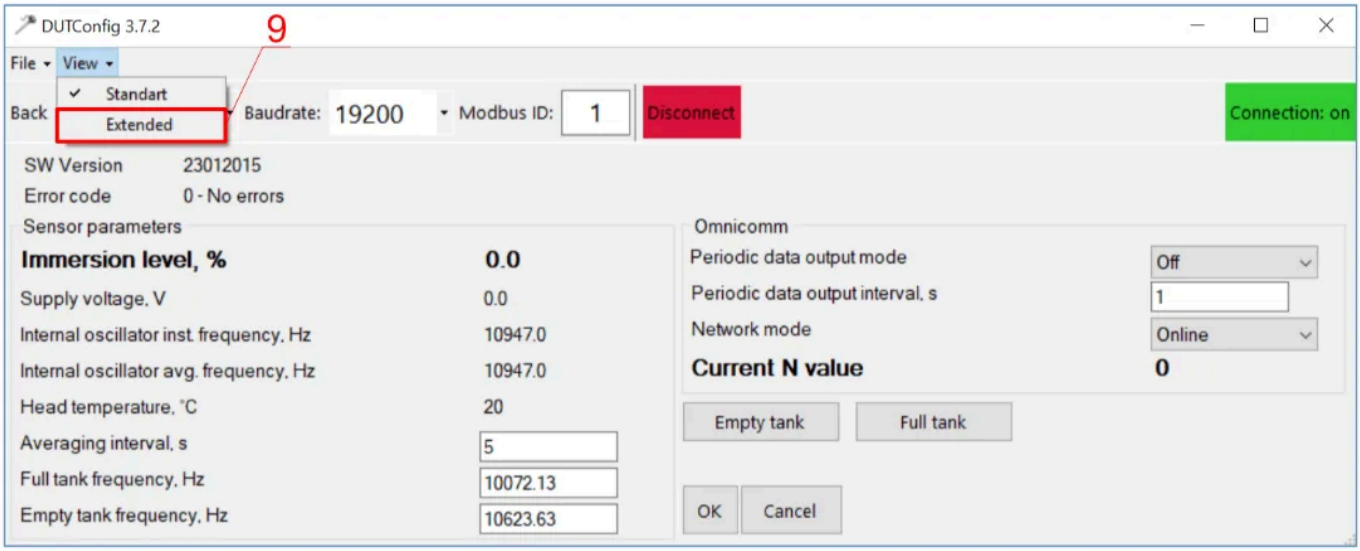
Rysunek 25. Połączony czujnik: port (**Port**, w przykładzie COM4), przycisk **Disconnect**, napis **Connection: on** (5) i przycisk **Edit** (6).

6. Kliknij przycisk **Edit** (edycja) i skalibruj czujnik przy pełnym i pustym zbiorniku.
7. Kalibracja w rzeczywistych warunkach: a) przy pełnym zbiorniku, z czujnikiem w zbiorniku, kliknij przycisk **Full tank** (pełny zbiornik); b) przy pustym zbiorniku, z czujnikiem wyjętym ze zbiornika, kliknij przycisk **Empty tank** (pusty zbiornik).
8. Aby zapisać wartości, kliknij przycisk **OK**.



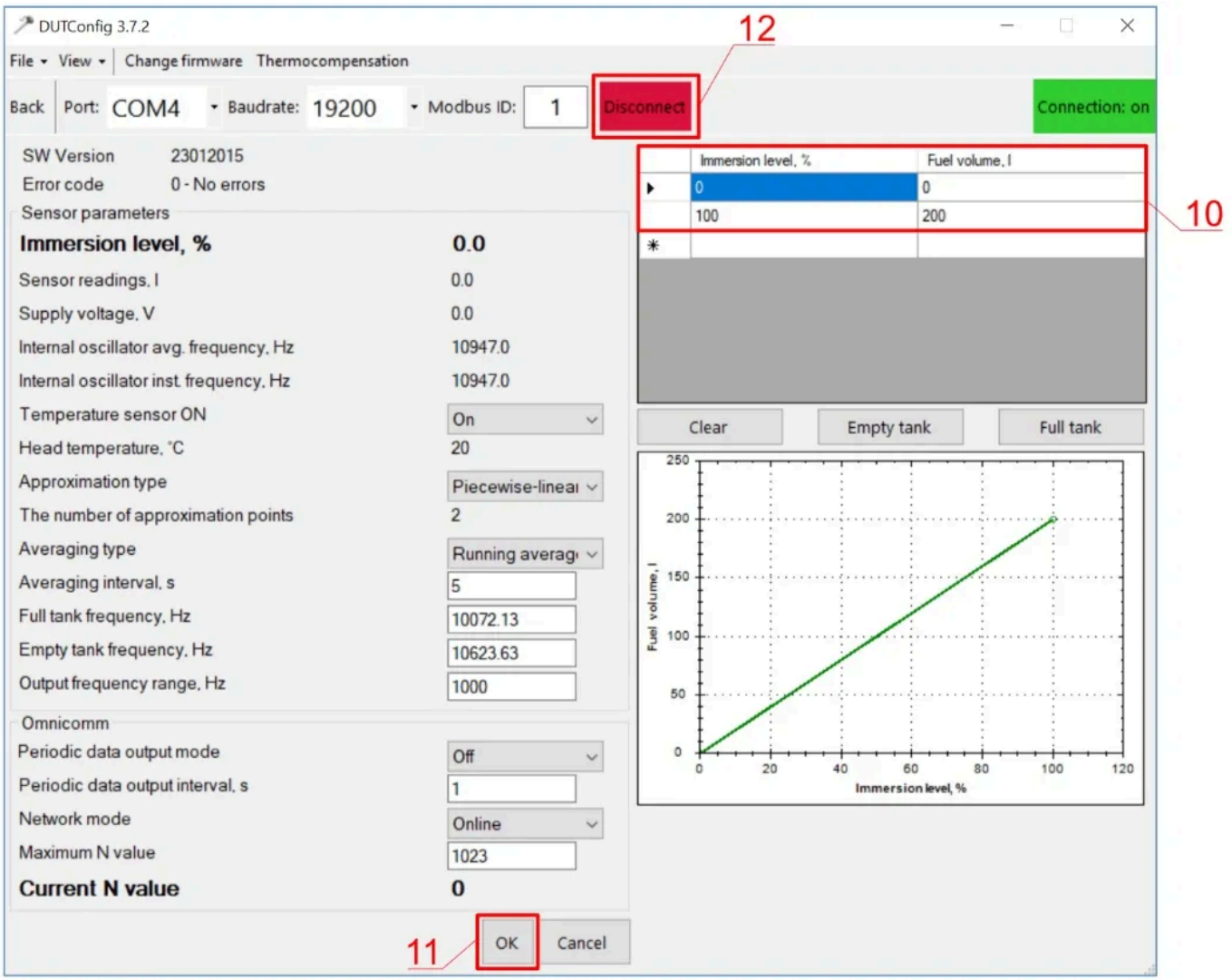
Rysunek 26. Kalibracja: przyciski **Empty tank** (pusty zbiornik) i **Full tank** (pełny zbiornik) (7), zapis przyciskiem **OK** (8); przycisk **Cancel** odrzuca zmianę.

9. Przełącz menu **View** na widok **Extended** (rozszerzony).



Rysunek 27. Menu **View**: widok **Standart** (standardowy) i **Extended** (rozszerzony) – wybrany **Extended** (9).

10. Wypełnij tabelę zgodnie z kształtem zbiornika. Prosty sposób: zanurzenie 0 % ustaw na 0 litrów, a 100 % na pojemność twojego zbiornika (w przykładzie zbiornik ma 200 litrów).
11. Po wypełnieniu tabeli kliknij przycisk **OK**.



Rysunek 28. Tabela widoku rozszerzonego (10): poziom zanurzenia („Immersion level, %") i ilość paliwa („Fuel volume, l") – w przykładzie 0 % = 0 l, 100 % = 200 l – obok ich wykres; przycisk **OK** (11) i przycisk **Disconnect** (12). W menu dostępna jest też wymiana oprogramowania układowego („Change firmware") i kompensacja temperaturowa („Thermocompensation").

12. Kliknij przycisk **Disconnect** (rozłącz).
13. Odłącz czujnik od komputera i podłącz go do CG17.

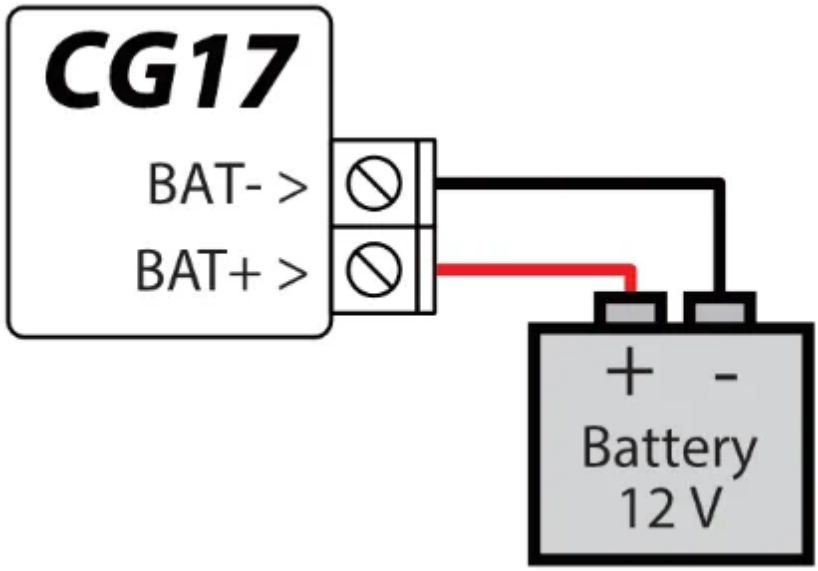
3.11 Podłączenie akumulatora

Do CG17 można podłączyć akumulator 12 V. Gdy zaniknie zasilanie sieciowe (AC), CG17 wysyła komunikat o zdarzeniu **AC fault** (awaria zasilania sieciowego) i automatycznie przełącza się na akumulator 12 V.

- Gdy napięcie akumulatora spadnie do 11,5 V, CG17 wysyła komunikat o zdarzeniu **Battery low** (niski poziom akumulatora).
- Gdy napięcie akumulatora spadnie poniżej 9,5 V i nie ma zasilania sieciowego, CG17 się wyłącza.
- Gdy zasilanie sieciowe powróci, CG17 wysyła komunikat o zdarzeniu **AC restore** (przywrócenie zasilania sieciowego) i automatycznie rozpoczyna się ładowanie akumulatora.
- Gdy napięcie akumulatora wzrośnie do 12,6 V, CG17 wysyła komunikat o zdarzeniu **Battery restore** (akumulator w porządku).

Podłączenie akumulatora:

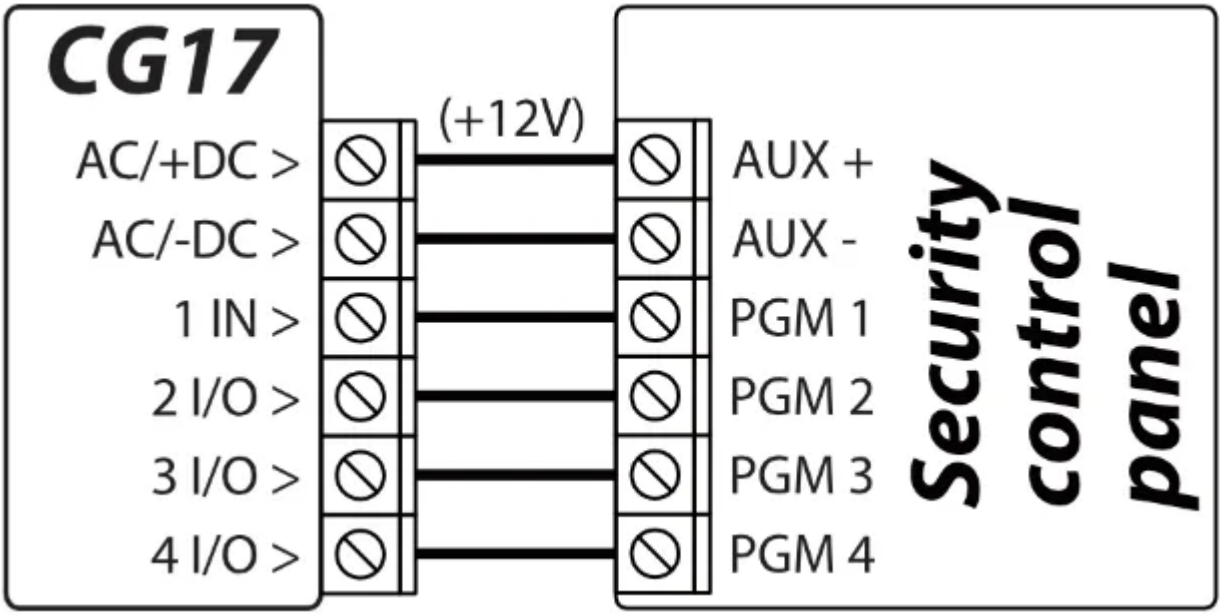
- Umieść akumulator zapasowy w obudowie montażowej.
- Podłącz przewody akumulatora do zacisków zasilania zapasowego CG17: **BAT+** i **BAT−**.
- Sprawdź, czy prąd ładowania CG17 (maksymalnie 500 mA, punkt 1.3) wystarczy do ładowania akumulatora.



Rysunek 29. Podłączenie akumulatora: BAT− → przewód czarny → biegun − akumulatora, BAT+ → przewód czerwony → biegun +; akumulator 12 V („Battery 12 V").

3.12 Podłączenie do centrali alarmowej

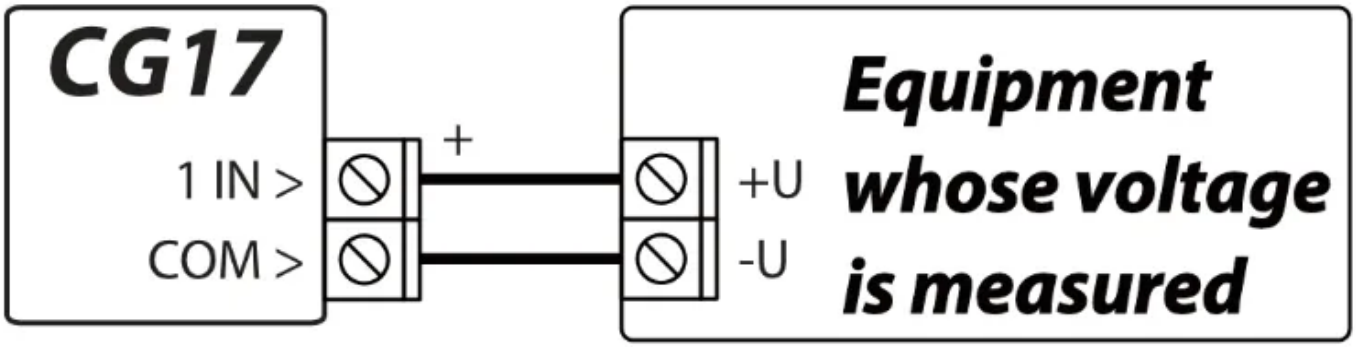
W tym podłączeniu CG17 pracuje jako komunikator: wyjścia PGM centrali alarmowej sterują wejściami CG17. Typ (**Type**) wejść CG17 musi być **NO** lub **NC**, a definicja (**Definition**) **24 hours** (strefa 24-godzinna) – okno **Zones**, punkt 5.6. Do wejść możesz też podać tekst SMS (okno **Zones**, karta **SMS & Call reporting**, **SMS text**): ten tekst otrzyma użytkownik, gdy wejście zgłosi naruszenie lub powróci do normy. Wyjścia PGM centrali alarmowej trzeba w ustawieniach centrali przypisać do wybranych zdarzeń.



Rysunek 30. Podłączenie CG17 do centrali alarmowej („Security control panel"): przewód zasilania +12 V („(+12V)") między zaciskiem AC/+DC CG17 a zaciskiem AUX+ centrali, AC/−DC → AUX−; zacisk 1 IN CG17 → wyjście PGM 1 centrali, 2 I/O → PGM 2, 3 I/O → PGM 3, 4 I/O → PGM 4.

3.13 Pomiar napięcia stałego

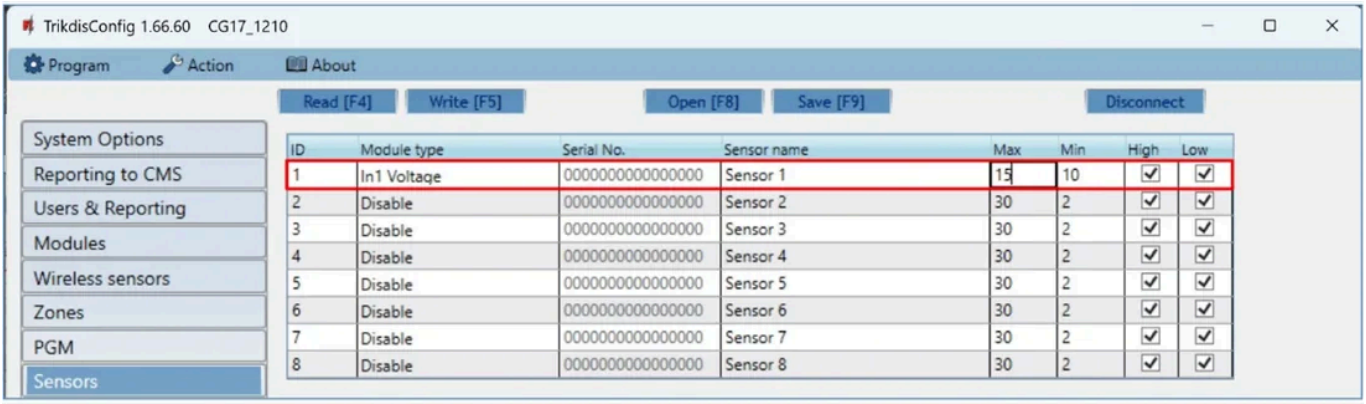
CG17 można używać także do pomiaru napięcia stałego. Do pomiaru można wybrać dowolne z czterech wejść (**1 IN**, **2 I/O**, **3 I/O**, **4 I/O**); w TrikdisConfig odpowiadają im typy czujnika **In1 Voltage** … **In4 Voltage**. Zakres pomiaru wynosi 0–30 V; **powyżej 30 V CG17 ulegnie uszkodzeniu**. Mierzone napięcie podłącz do zacisków **1 IN** i **COM**: 1 IN to zacisk dodatni, a COM ujemny (dalszy opis także dotyczy wejścia 1 IN).



Rysunek 31. Pomiar napięcia: zacisk +U mierzonego urządzenia („Equipment whose voltage is measured") → 1 IN, zacisk −U → COM.

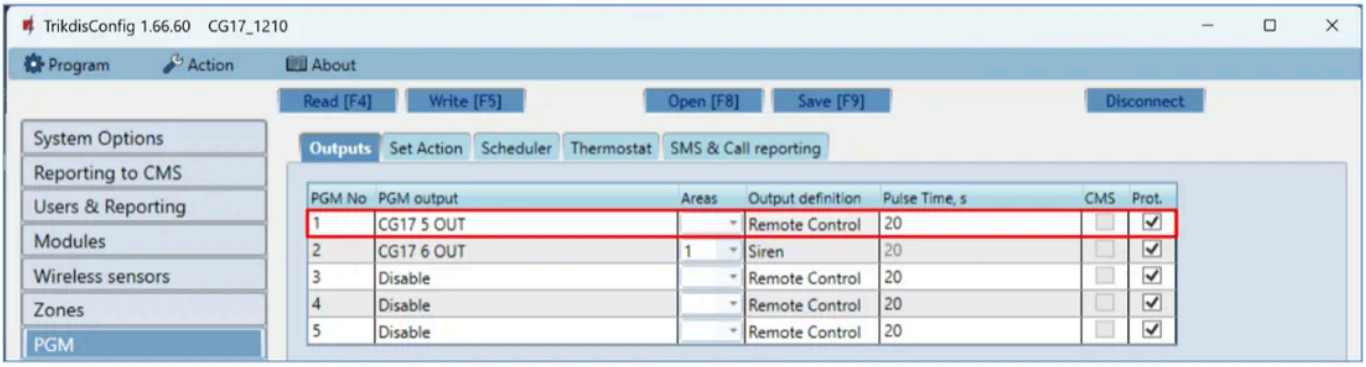
Podłącz CG17 do komputera kablem USB Mini-B i uruchom TrikdisConfig: program automatycznie rozpozna podłączoną centralę CG17 i otworzy jej okno konfiguracji. W oknie **Sensors** (punkt 5.8) wybierz typ **In1 Voltage** i podaj granice napięcia, po przekroczeniu których powstaje komunikat o zdarzeniu:

- **Max** – jeśli napięcie jest wyższe, powstaje komunikat o zdarzeniu; w tym celu trzeba zaznaczyć pole **High**.
- **Min** – jeśli napięcie jest niższe, powstaje komunikat o zdarzeniu; w tym celu trzeba zaznaczyć pole **Low**.



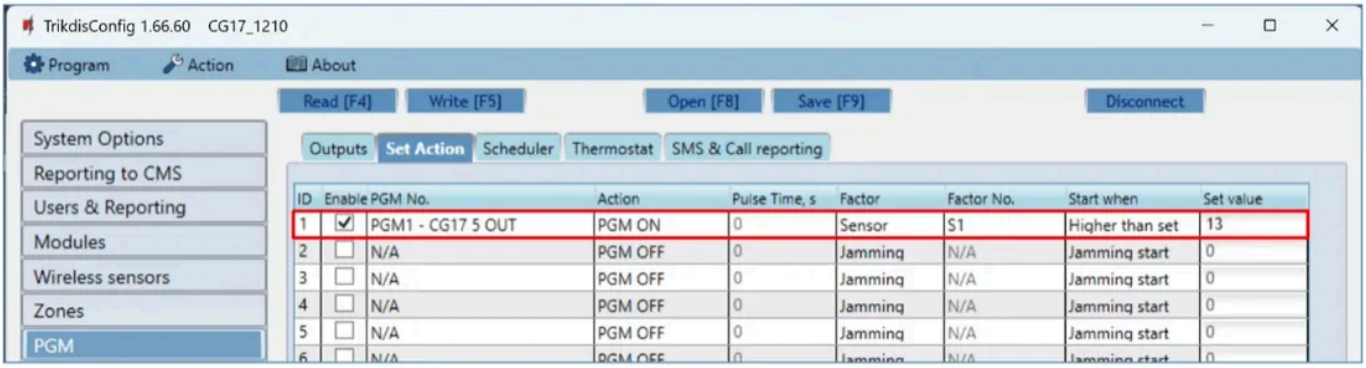
Rysunek 32. TrikdisConfig – **Sensors**: w wierszu 1 **Module type In1 Voltage**, **Max** 15, **Min** 10 V, pola **High** i **Low** zaznaczone; pozostałe wiersze wyłączone (**Disable**).

Zmierzone napięcie może też sterować wyjściem PGM: wyjście przełącza się powyżej lub poniżej ustawionej wartości. W tym celu w TrikdisConfig wybierz wyjście PGM i ustaw je na działanie **Remote Control** (sterowanie zdalne) (okno **PGM**, karta **Outputs**, punkt 5.7).



Rysunek 33. TrikdisConfig – **PGM**, karta **Outputs**: PGM 1 to wyjście **CG17 5 OUT**, jego typ (**Output definition**) to **Remote Control**, czas impulsu (**Pulse Time**) 20 s.

Przejdź na kartę **Set Action** (ustawienie akcji).



Rysunek 34. TrikdisConfig – **PGM**, karta **Set Action**: w wierszu 1 **Enable** zaznaczone, **PGM No.** PGM1 – CG17 5 OUT, **Action** PGM ON, **Pulse Time** 0, **Factor** Sensor, **Factor No.** S1, **Start when** Higher than set, **Set value** 13 – wyjście włącza się powyżej 13 V.

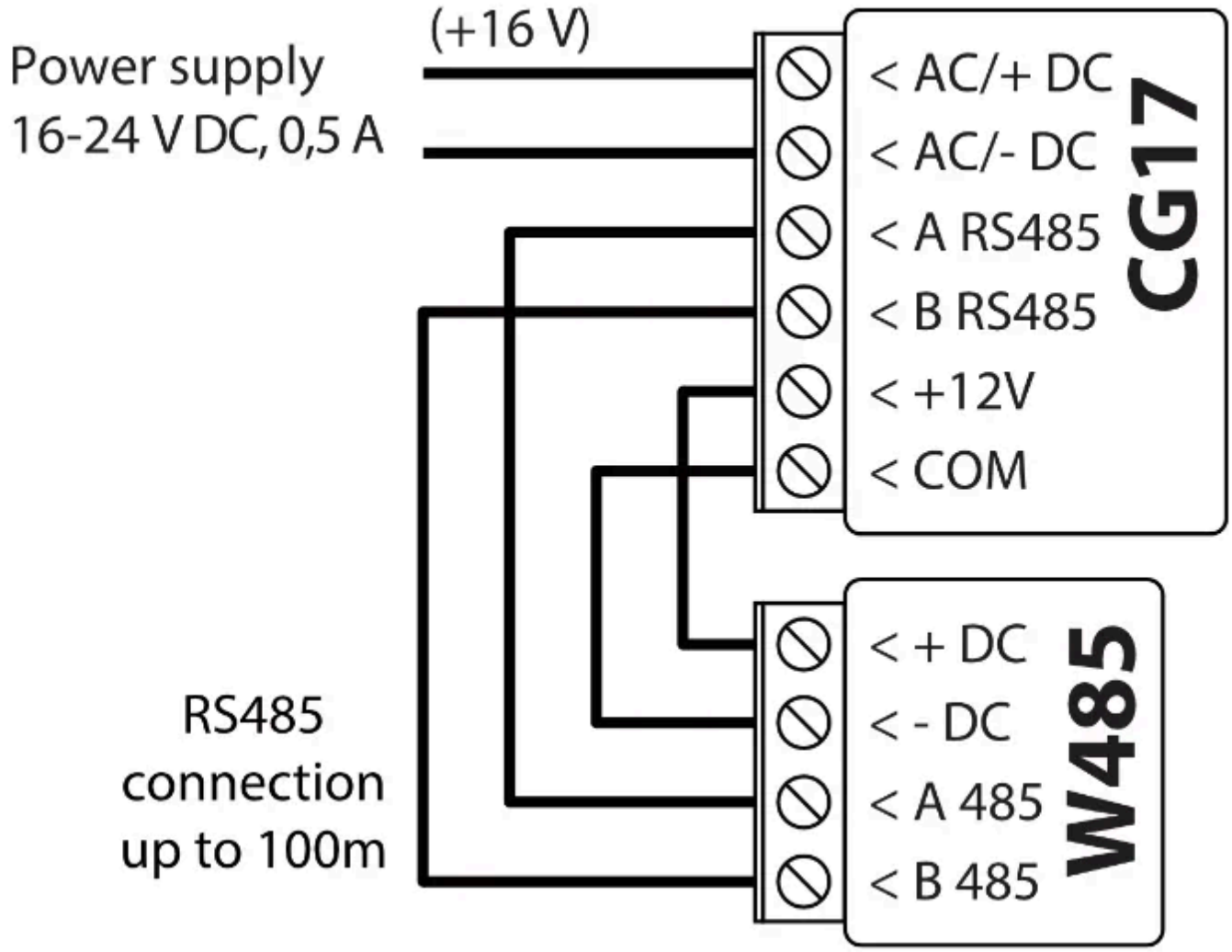
- **Enable** – włączenie PGM.
- **PGM No.** – wyjście PGM, którym steruje wejście 1 IN.
- **Action** – tryb działania wyjścia PGM:
  - **PGM OFF** – wyłączenie wyjścia PGM.
  - **PGM ON** – włączenie wyjścia PGM.

    - **Pulse OFF** – wyłączenie wyjścia PGM na czas impulsu (po poleceniu wyjście wyłącza się na czas impulsu, a potem włącza).
    - **Pulse ON** – włączenie wyjścia PGM na czas impulsu (po poleceniu wyjście włącza się na czas impulsu, a potem wyłącza).
- **Pulse time, s** – długość impulsu, 0–9999 s.
- **Factor** – źródło warunku: czujnik (**Sensor**).
- **Factor No.** – wejście mierzące napięcie, tu 1 IN (na obrazku **S1**).
- **Start when** – dodatkowy warunek włączenia wyjścia PGM (na obrazku **Higher than set** – powyżej ustawionej wartości).
- **Set value** – napięcie (V), które CG17 monitoruje i według którego steruje wyjściem PGM.

3.14 Moduł Wi-Fi W485

Moduł **W485** wysyła komunikaty CG17 przez lokalną sieć Wi-Fi, przez router internetowy, do stacji monitorowania i do aplikacji Protegus 2. Dopóki jest połączenie Wi-Fi, CG17 (od oprogramowania układowego **1.13**) wysyła komunikaty o zdarzeniach przez moduł W485. Gdy Wi-Fi zostanie przerwane, CG17 wysyła komunikaty przez mobilny internet, a po powrocie Wi-Fi wraca do W485. Konfigurację modułu w CG17 opisuje punkt 5.5 (okno **Modules**). **Z W485 CG17 może pracować także bez karty SIM** – bez karty SIM nie działa jednak rezerwa przez sieć komórkową ani SMS, ani połączenia. Do CG17 można podłączyć jeden moduł W485. Moduł podłącza się do magistrali **RS485** (A–A, B–B), w odległości maksymalnie 100 m.

Trikdis W485 Moduł WiFi (RS485)



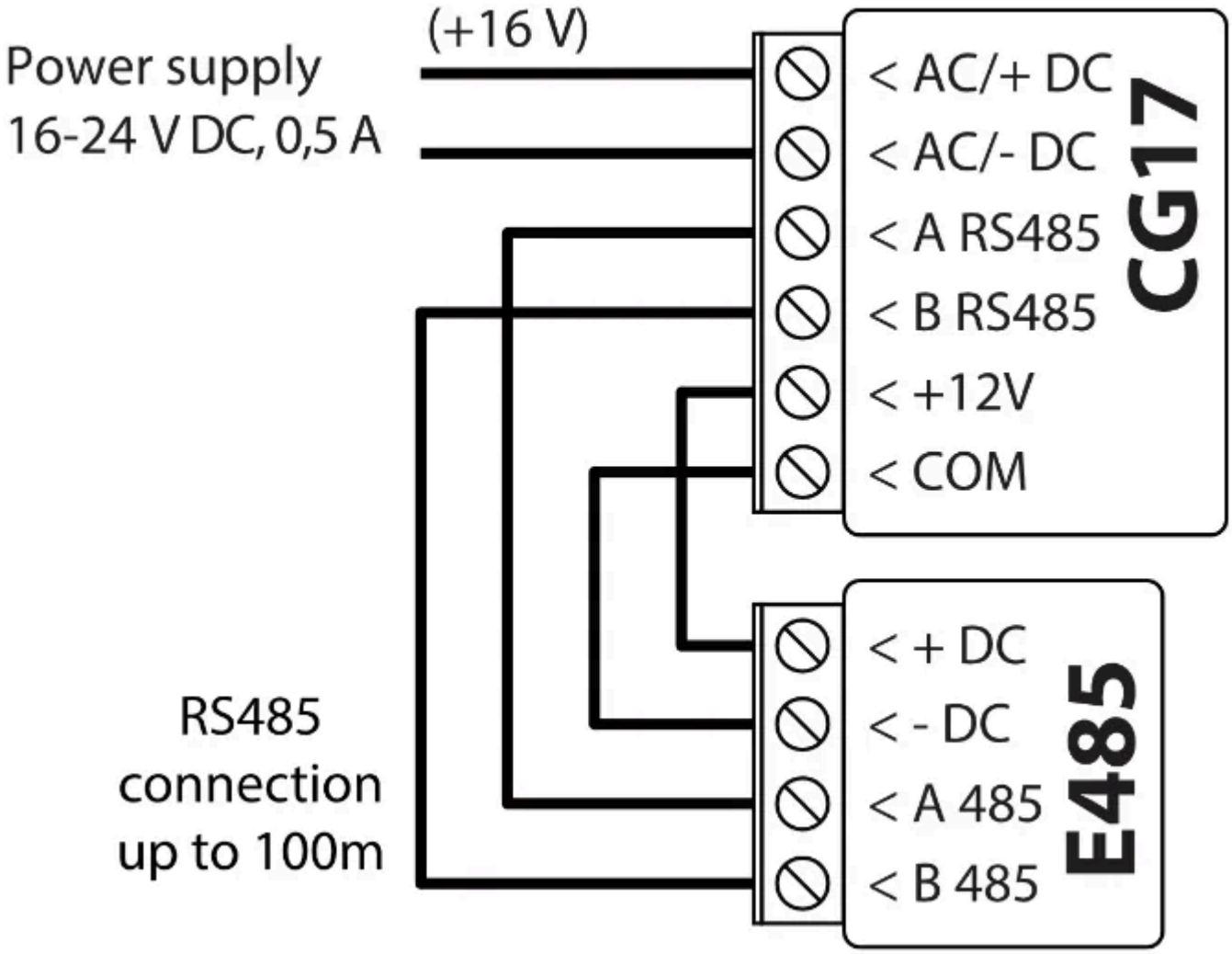
Rysunek 35. Podłączenie modułu W485: biegun dodatni („(+16 V)") zasilacza 16–24 V DC, 0,5 A („Power supply 16-24 V DC, 0,5 A") do zacisku AC/+DC CG17, ujemny do AC/−DC; zacisk +12V CG17 → +DC modułu W485, COM → −DC; połączenie RS485 („RS485 connection"), maksymalnie 100 m („up to 100m"): A RS485 – A 485, B RS485 – B 485.

„Maksymalnie 100 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

3.15 Moduł Ethernet E485

Moduł **E485** wysyła komunikaty CG17 przez przewodowy internet do stacji monitorowania i do aplikacji Protegus 2. Z E485 (od oprogramowania układowego CG17 w wersji **1.13**) komunikaty do stacji monitorowania i do Protegus idą przez przewodowy internet, a CG17 nie korzysta z mobilnego internetu. Gdy przewodowe połączenie internetowe zostanie przerwane, CG17 wysyła komunikaty przez mobilny internet, a po powrocie połączenia przewodowego ponownie przez E485. Konfigurację modułu w CG17 opisuje punkt 5.5 (okno **Modules**). **Z E485 CG17 może pracować także bez karty SIM** – bez karty SIM nie działa jednak rezerwa przez sieć komórkową ani SMS, ani połączenia. Do CG17 można podłączyć jeden moduł E485. Moduł podłącza się do magistrali **RS485** (A–A, B–B), w odległości maksymalnie 100 m.

Moduł Ethernet Trikdis E485 (RS485)



Rysunek 36. Podłączenie modułu E485: biegun dodatni („(+16 V)") zasilacza 16–24 V DC, 0,5 A („Power supply 16-24 V DC, 0,5 A") do zacisku AC/+DC CG17, ujemny do AC/−DC; zacisk +12V CG17 → +DC modułu E485, COM → −DC; połączenie RS485 („RS485 connection"), maksymalnie 100 m („up to 100m"): A RS485 – A 485, B RS485 – B 485.

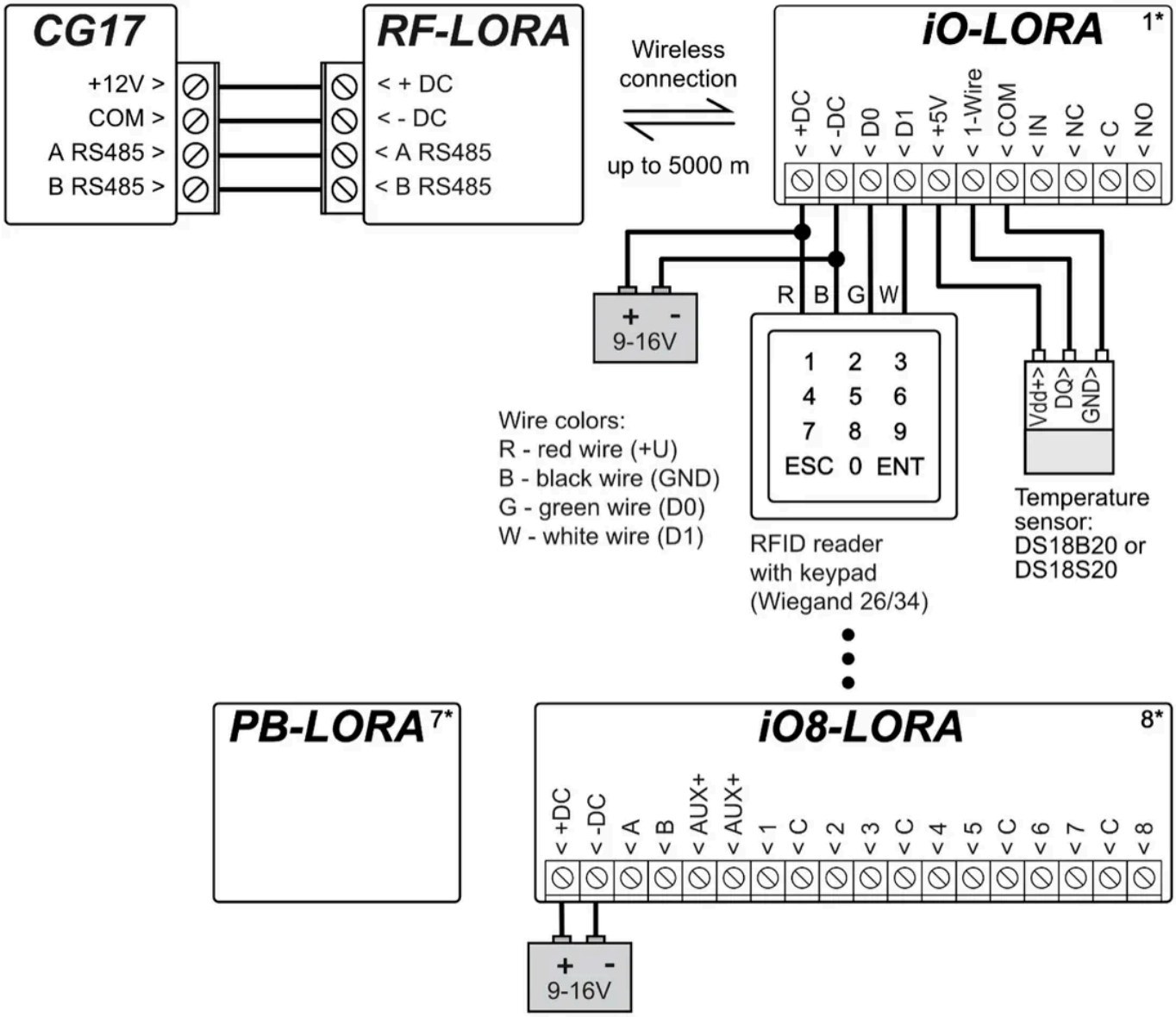
„Maksymalnie 100 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

3.16 RF-LORA i ekspandery LORA

Funkcja działa z oprogramowaniem układowym CG17 w wersji **1.18** lub nowszej. Podłącz do CG17 nadajnik-odbiornik **RF-LORA**: potem można używać modułów **iO-LORA**, **iO8-LORA**, **PB-LORA** i **REL-LORA**. Do CG17 można podłączyć jeden nadajnik-odbiornik RF-LORA.

Moduł Expander Trikdis RF-LORA **Moduł Expander Trikdis Io-Lora**

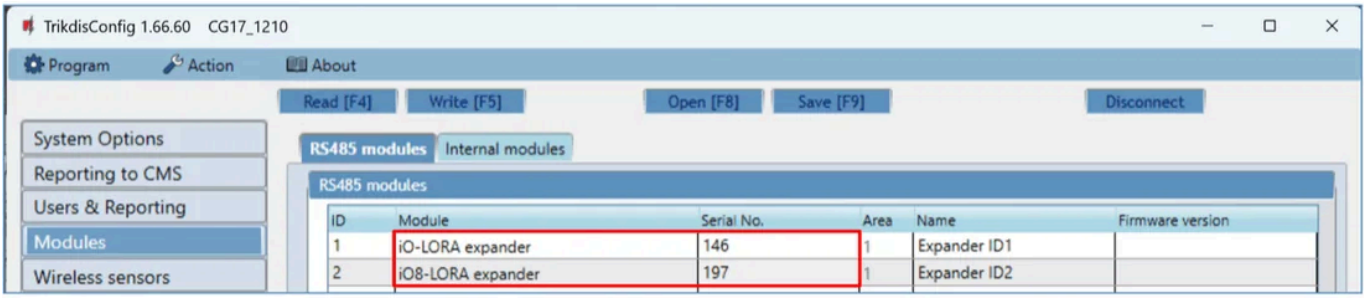
Moduł Expander Trikdis IO8-LORA



Rysunek 37. Ekspandery LORA przez nadajnik-odbiornik RF-LORA: zaciski +12V, COM, A RS485 i B RS485 CG17 → zaciski +DC, −DC, A RS485 i B RS485 RF-LORA; połączenie bezprzewodowe („Wireless connection"), maksymalnie 5000 m („up to 5000 m") między RF-LORA a modułami LORA. iO-LORA (1*) pracuje z własnego zasilania 9–16 V („9-16V"); podłączony do niego czytnik RFID z klawiaturą, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)"), kolory przewodów („Wire colors"): czerwony, +U („R - red wire (+U)") → +DC; czarny, GND („B - black wire (GND)") → −DC; zielony, D0 („G - green wire (D0)") → D0; biały, D1 („W - white wire (D1)") → D1; a także czujnik temperatury („Temperature sensor: DS18B20 or DS18S20"): Vdd+ → +5V, DQ → 1-Wire, GND → COM. Kropki oznaczają kolejne moduły: na rysunku widać jeszcze przycisk napadowy PB-LORA (7*) i ekspander iO8-LORA (8*) pracujący z własnego zasilania 9–16 V.

„Maksymalnie 5000 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

Konfiguracja w TrikdisConfig: uruchom TrikdisConfig i podłącz CG17 do komputera kablem USB Mini-B albo połącz się z nim zdalnie (punkt 6.1). Kliknij przycisk **Read [F4]**: program pokaże aktualne ustawienia CG17. Jeśli program o to poprosi, podaj w wyskakującym oknie kod administratora lub instalatora. W oknie **Modules**, z listy w kolumnie **Module**, wybierz używany moduł LORA, a w polu **Serial No.** wpisz numer seryjny modułu (punkt 5.5).



Rysunek 38. TrikdisConfig – **Modules**, karta **RS485 modules**: w kolumnie **Module** wybrane moduły LORA (**iO-LORA expander**, **iO8-LORA expander**), w kolumnie **Serial No.** ich numery seryjne; **Area** – partycja, **Name** – nazwa modułu.

Po zmianach kliknij przycisk **Write [F5]** i poczekaj na zakończenie aktualizacji. Na koniec kliknij przycisk **Disconnect** i odłącz kabel USB Mini-B.

4. Sterowanie

CG17 możesz sterować zdalnie na trzy sposoby: z aplikacji **Protegus 2** (punkt 4.1), **poleceniem SMS** (punkt 4.2) i **połączeniem telefonicznym** (punkt 4.3). Zdalną zmianę ustawień i zdalne sterowanie z TrikdisConfig opisuje rozdział 6.

4.1 Sterowanie z aplikacji Protegus 2

Dzięki Protegus 2 użytkownicy zdalnie sterują systemem alarmowym, widzą stan systemu i otrzymują powiadomienia o zdarzeniach systemu.

Zanim dodasz system

CG17 możesz dodać do Protegus 2, jeśli:

1. usługa chmury Protegus jest włączona: w oknie **Users & Reporting** TrikdisConfig, w grupie ustawień **Cloud application**, zaznaczone jest pole **Enable cloud service** (punkt 5.4; SMS-em: `CONNECT 123456 PROTEGUS=ON`, punkt 4.2);
2. w urządzeniu jest aktywowana karta SIM, a jej kod PIN jest podany (okno **System Options**, grupa **SIM**, punkt 5.2) lub żądanie PIN jest wyłączone;
3. jest zasilanie: dioda **POWER** świeci na zielono;
4. urządzenie jest połączone z siecią: dioda **NETWORK** świeci na zielono i miga na żółto.

Jeśli dioda **NETWORK** lub **DATA** świeci ciągle na żółto, urządzenie nie może połączyć się z siecią komórkową i/lub z Protegus 2. Sygnalizację diod LED opisuje punkt 1.6.

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

A rendszer létrehozása a Protegus 2 alkalmazásban

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

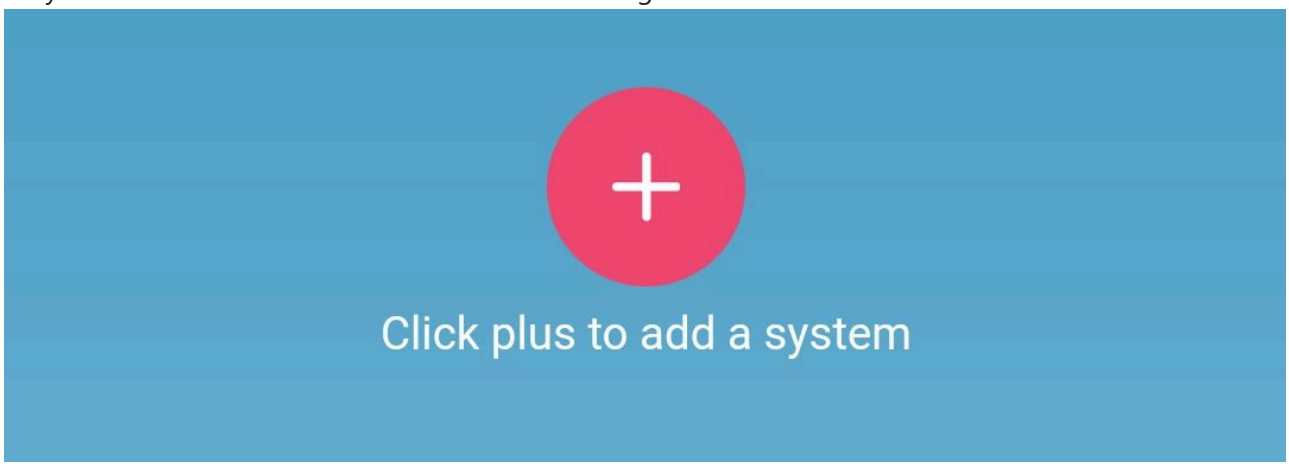
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

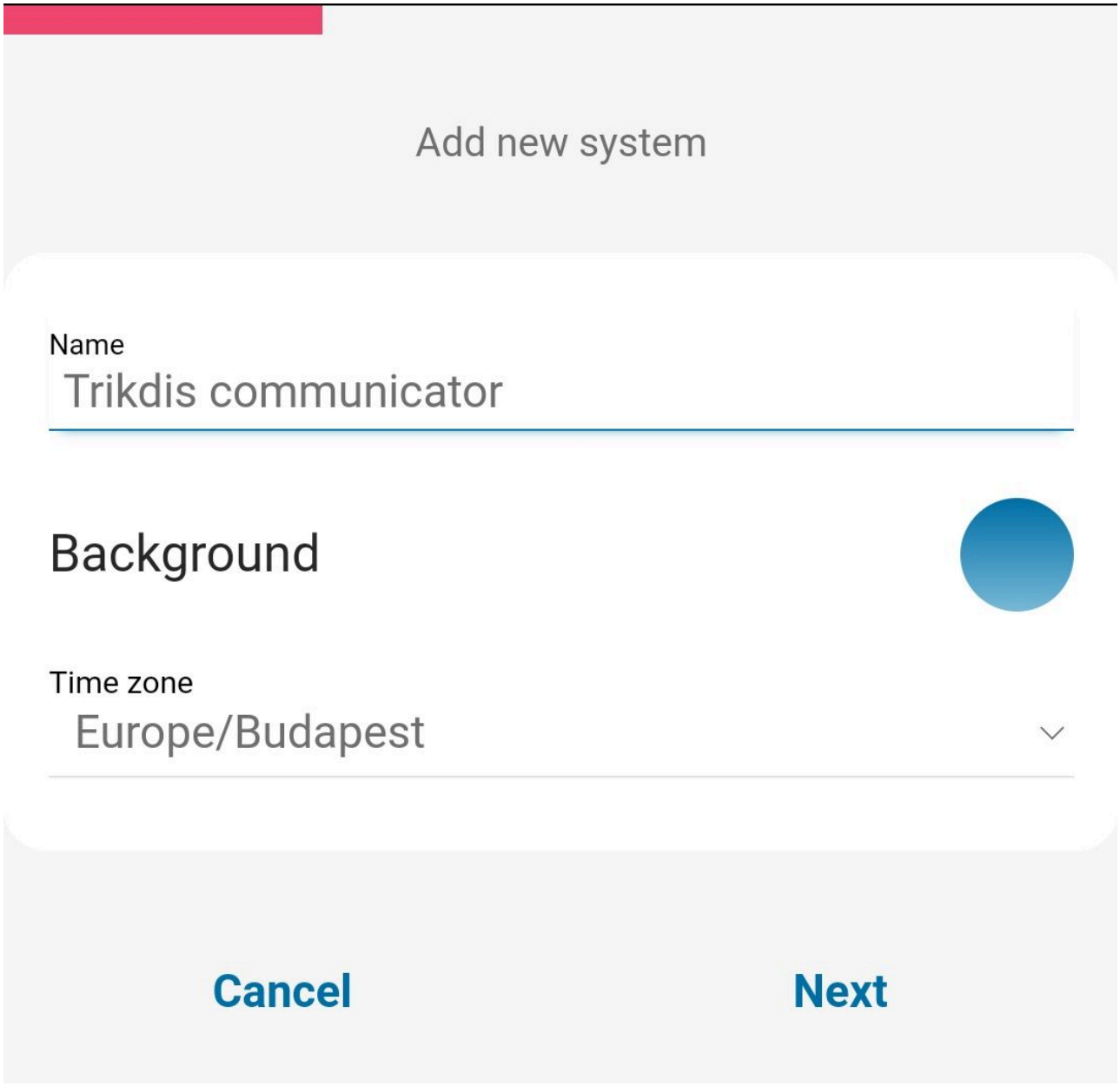
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



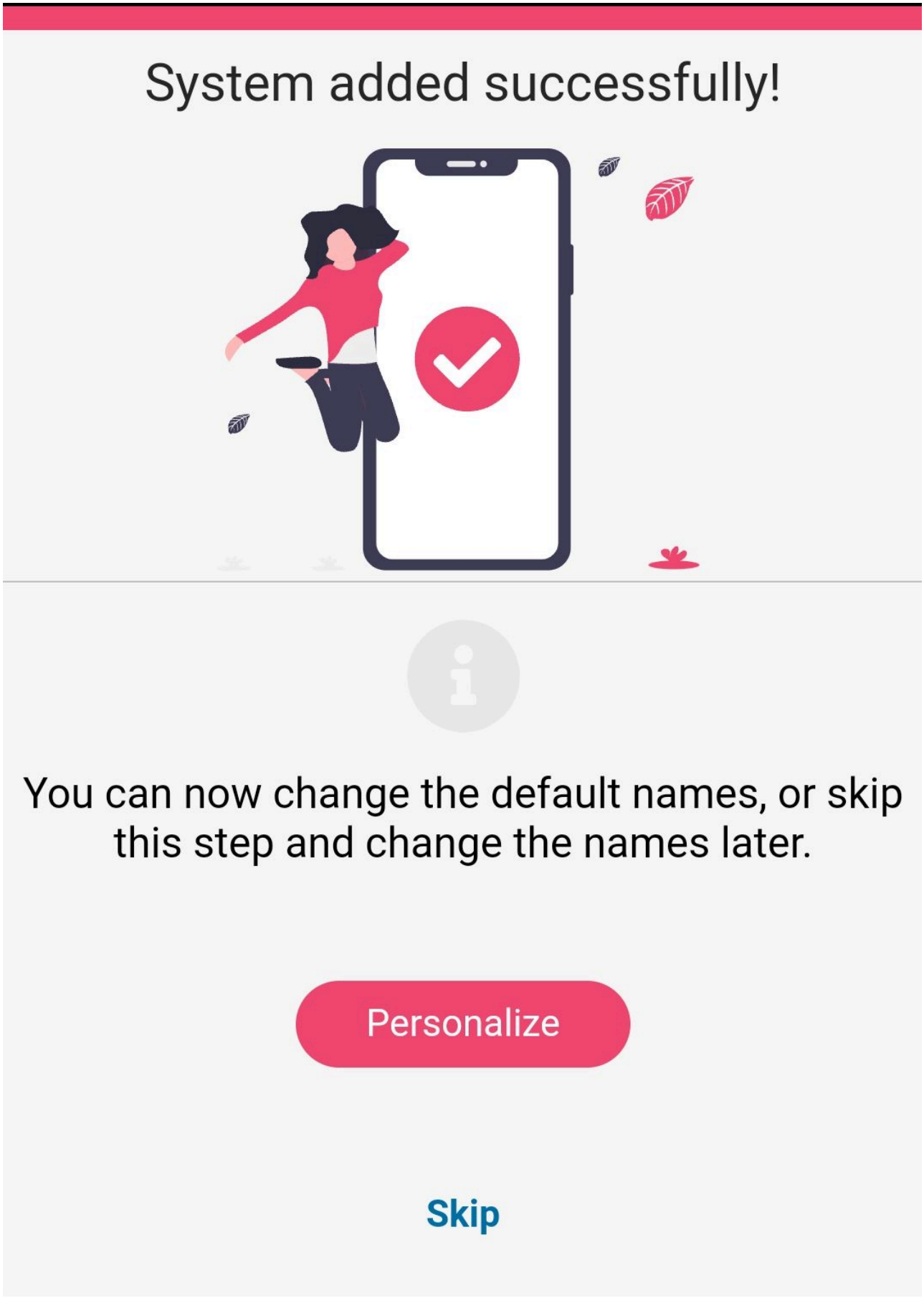
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



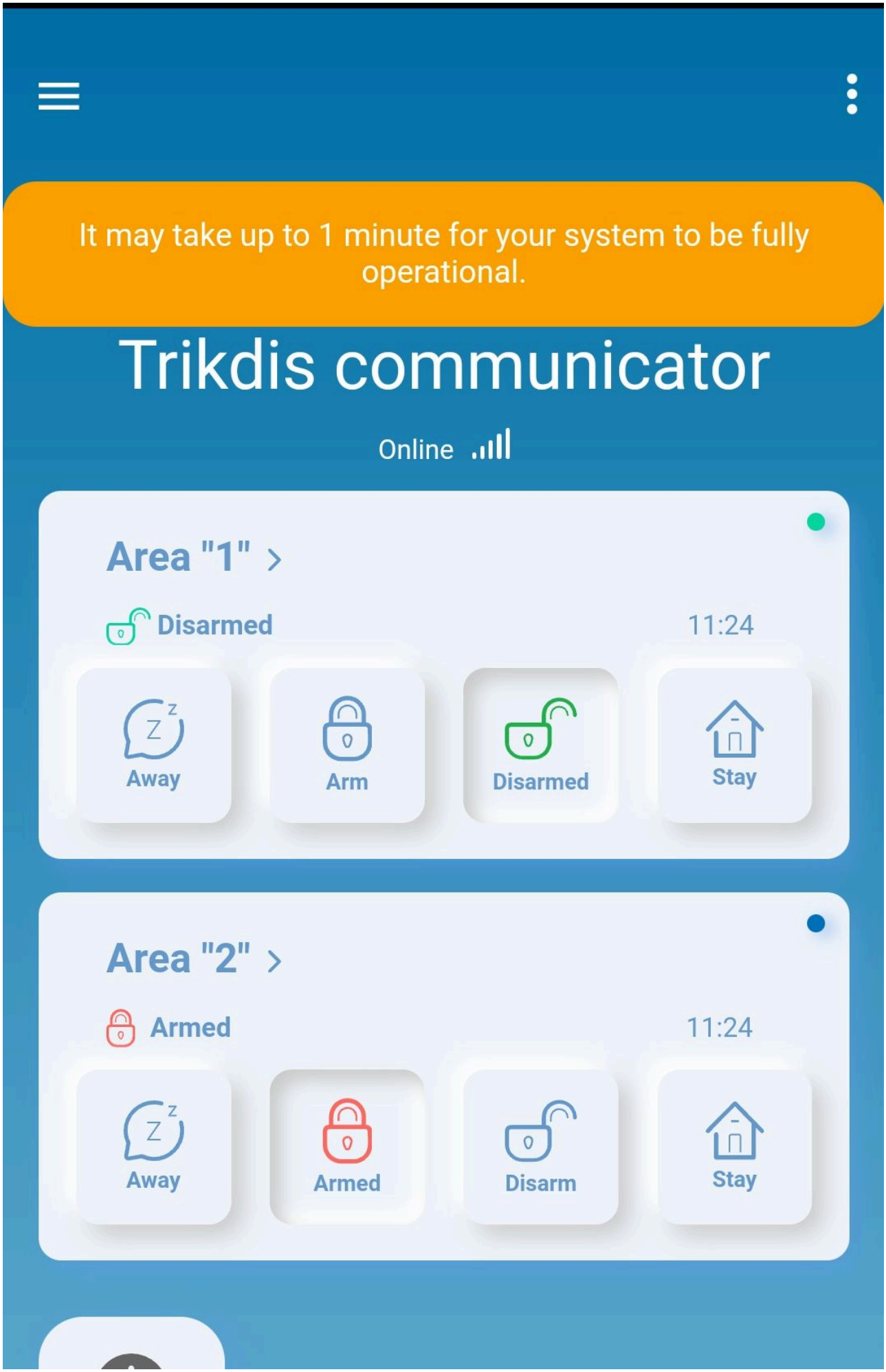
6. Add meg a rendszer nevét és válassz idozónát



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



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


It may take up to 1 minute for your system to be fully operational.
Trikdis communicator
Online
Area "1" >
Disarmed
11:24
Away
Arm
Disarmed
Stay
Area "2" >
Armed
11:24
Away
Armed
Disarm
Stay



Przy dodawaniu CG17 zwróć uwagę na następujące rzeczy:

1. Unikalnym identyfikatorem (**Unique ID**) jest numer **IMEI** CG17: znajdziesz go na naklejce na urządzeniu i na pudełku, widzisz go też na pasku stanu TrikdisConfig (punkt 5.1).
2. Jeśli instalator zmienił fabryczną wartość `123456` pola **Cloud Access Code** (punkt 5.4), aplikacja przy dodawaniu poprosi także o ten kod.

Zobacz też

Protegus – aplikacja na Androida / iPhone'a i aplikacja internetowa · Powiadomienia push w przeglądarce w aplikacji Protegus 2

4.1.1 Uzbrajanie i rozbrajanie

1. Otwórz aplikację Protegus 2 i w oknie systemu naciśnij przycisk **Arm** (uzbrojenie).
2. W menu wybierz tryb do włączenia i podaj kod użytkownika (kod podany w kolumnie **Code** okna **Users & Reporting** TrikdisConfig, punkt 5.4).
3. Gdy system zmieni tryb, zmieni się także ikona **Arm**.



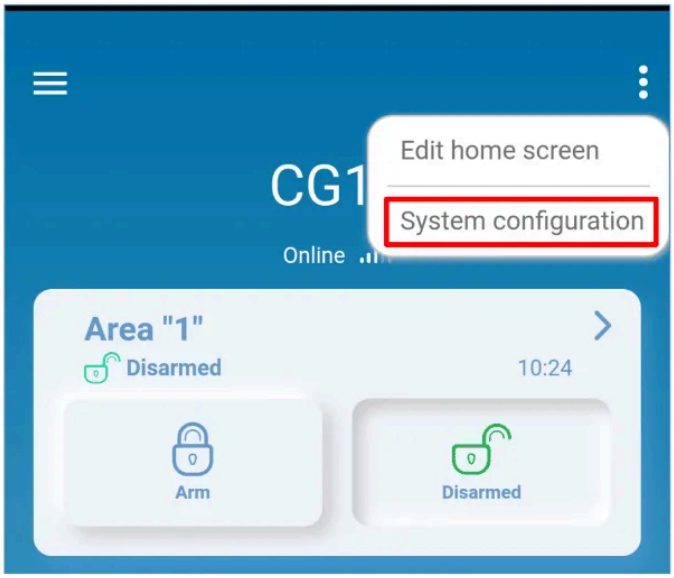
Rysunek 39. CG17 w Protegus 2: **Area "1"** (partycja 1) jest rozbrojona (**Disarmed**), uzbrajasz ją zaznaczonym w ramce przyciskiem **Arm**. U góry nazwa systemu i stan **Online** (dostępny) z poziomem sygnału.

Jeśli uzbrajasz system z Protegus 2 lub połączeniem telefonicznym, centrala nie odlicza czasu na wyjście (**Exit time**, punkt 5.2).

4.1.2 Dodawanie kolejnych użytkowników

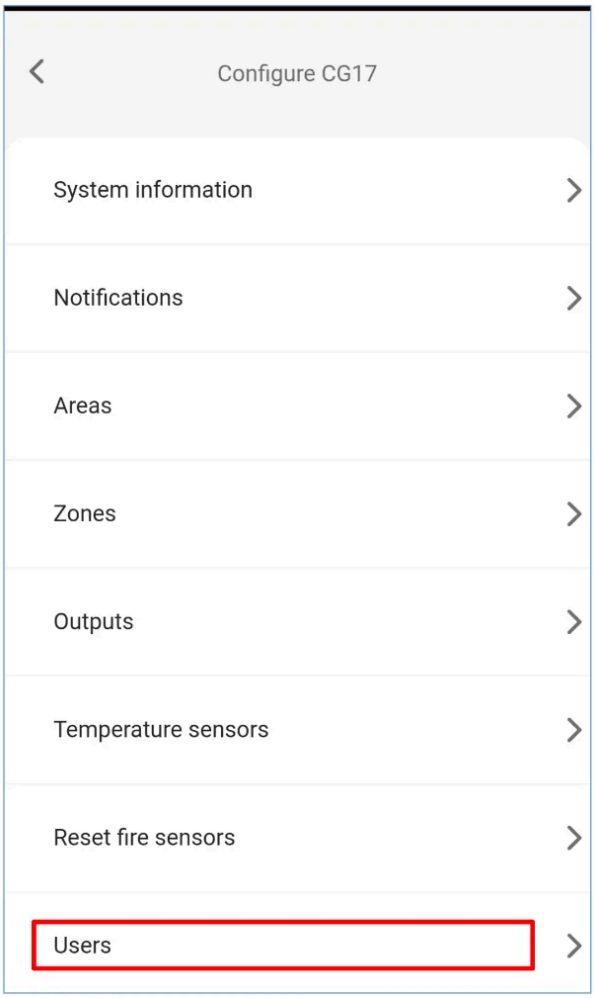
Uruchom aplikację Protegus 2 na telefonie i zaloguj się swoją nazwą użytkownika i hasłem.

1. Otwórz menu **Settings** (ustawienia): dotknij ikony trzech kropek w prawym górnym rogu okna systemu.
2. Wybierz pozycję **System configuration** (konfiguracja systemu).



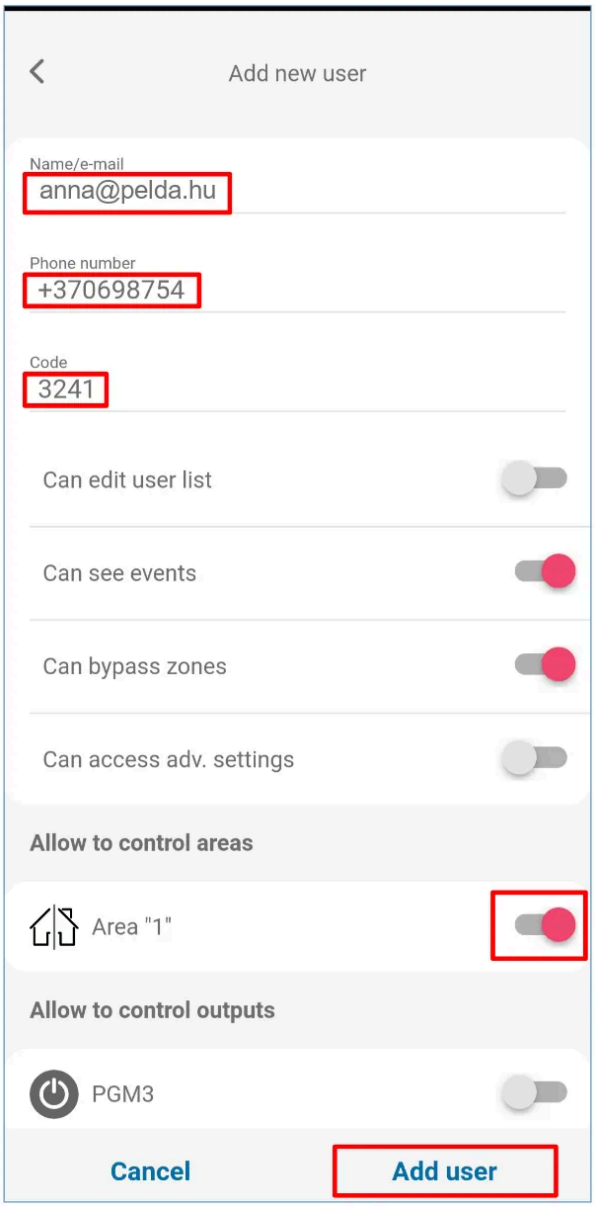
Rysunek 40. Menu trzech kropek w prawym górnym rogu: **Edit home screen** (edycja ekranu głównego) i zaznaczona w ramce pozycja **System configuration** (konfiguracja systemu).

3. Wybierz pozycję **Users** (użytkownicy).



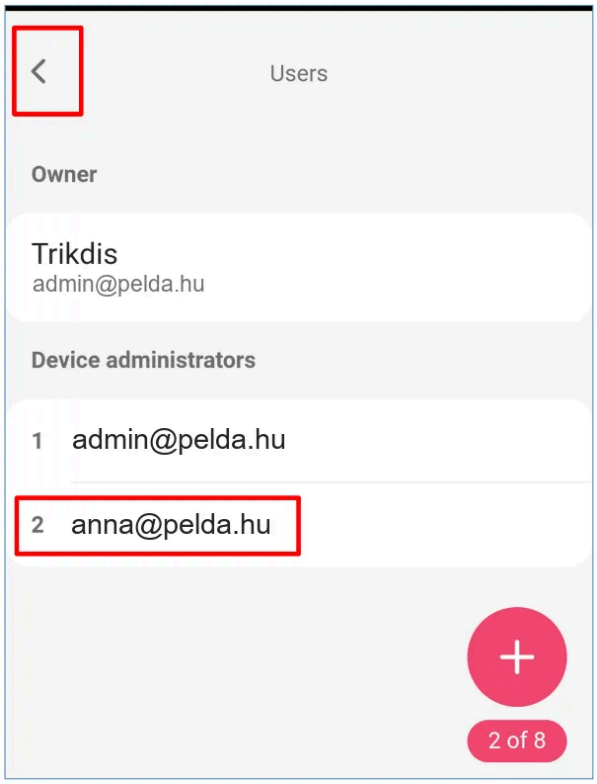
Rysunek 41. Menu **Configure CG17** (konfiguracja CG17): **System information** (informacje o systemie), **Notifications** (powiadomienia), **Areas** (partycje), **Zones** (strefy), **Outputs** (wyjścia), **Temperature sensors** (czujniki temperatury), **Reset fire sensors** (reset czujek pożarowych) i zaznaczona w ramce pozycja **Users** (użytkownicy).

4. Naciśnij przycisk **+** (**Add new user** – nowy użytkownik).
5. Podaj adres e-mail lub nazwę użytkownika.
6. Podaj numer telefonu użytkownika.
7. Podaj kod użytkownika.
8. Zaznacz, którą partycją użytkownik może sterować.
9. Zaznacz, którym wyjściem PGM użytkownik może sterować.
10. Naciśnij przycisk **Add user** (dodaj użytkownika).



Rysunek 42. Formularz **Add new user** (nowy użytkownik): **Name/e-mail** (nazwa lub adres e-mail), **Phone number** (numer telefonu), **Code** (kod); uprawnienia: **Can edit user list** (może edytować listę użytkowników), **Can see events** (widzi zdarzenia), **Can bypass zones** (może blokować strefy), **Can access adv. settings** (ma dostęp do ustawień zaawansowanych); poniżej przełączniki **Allow to control areas** (partycje, którymi może sterować) i **Allow to control outputs** (wyjścia, którymi może sterować), na dole przycisk **Add user**.

11. Nowy użytkownik pojawi się na liście użytkowników.
12. Przyciskiem **Back** (wstecz) wróć do okna głównego.



Rysunek 43. Lista **Users** (użytkownicy): **Owner** (właściciel systemu) i **Device administrators** (administratorzy urządzenia), w wierszu 2 nowy użytkownik; w lewym górnym rogu zaznaczona w ramce strzałka powrotu (**Back**). Oznaczenie **2 of 8**: z 8 możliwych użytkowników dodano 2.

4.2 Sterowanie poleceniami SMS

Polecenie SMS wyślij na numer telefonu karty SIM włożonej do CG17. W poleceniach `xxxxxx` to 6-znakowe hasło SMS administratora (fabrycznie `123456`; w TrikdisConfig: **System Options** → **Access** → **SMS password**, punkt 5.2). Jeśli na liście użytkowników przy danym użytkowniku zaznaczone jest pole **ACK** (punkt 5.4), CG17 po każdym poleceniu SMS wysyła mu SMS z odpowiedzią; treść odpowiedzi możesz zmienić na karcie **SMS answer texts** okna **Users & Reporting**.

Uzbrajanie i rozbrajanie SMS-em – tymi SMS-ami uzbrajasz lub rozbrajasz system alarmowy:

```
ARM xxxxxx SYS:x
```

```
DISARM xxxxxx SYS:x
```

Znak	Znaczenie
`xxxxxx`	6-znakowe hasło administratora (fabrycznie `123456`)
`x`	numer partycji systemu alarmowego (1–8)

Zmiana hasła administratora – ze względów bezpieczeństwa zmień fabryczne hasło SMS administratora. Wyślij SMS w takiej postaci:

```
PSW 123456 xxxxxx
```

Znak	Znaczenie
`123456`	fabryczne hasło administratora
`xxxxxx`	nowe, 6-znakowe hasło administratora

Nadawanie uprawnień innym użytkownikom – SMS-em i połączeniem telefonicznym systemem można sterować tylko z numerów telefonów znajdujących się na liście użytkowników. Z telefonu administratora wyślij SMS-em numer telefonu i imię pozostałych osób, aby one także mogły sterować systemem:

`SETN xxxxxx PHONEx=+PHONENR#NAME`

Znak	Znaczenie
`xxxxxx`	6-znakowe hasło administratora
`x`	numer porządkowy użytkownika na liście (jeśli wpiszesz **1**, przekażesz swoje uprawnienia administratora innemu użytkownikowi)
`PHONENR`	numer telefonu użytkownika
`NAME`	imię użytkownika

Reset czujek dymu – czujki dymu możesz zresetować (reset) także zdalnie, SMS-em:

`FRS xxxxxx`

`xxxxxx` – 6-cyfrowe hasło administratora.

Wyjście OUT, do którego są podłączone czujki pożarowe, musi mieć typ resetu czujek pożarowych (w oknie **PGM** TrikdisConfig: **Output definition** → **Fire Sensor Reset**, punkt 5.7). Wyjście **5 OUT** ma ten typ fabrycznie.

Lista poleceń SMS (w każdym z nich hasło stoi po słowie polecenia, w przykładach fabryczne `123456`):

Polecenie	Dane	Opis
`INFO`	–	dane centrali: odpowiedź zawiera typ centrali, numer IMEI, numer seryjny i wersję oprogramowania układowego. Przykład: `INFO 123456`
`RESET`	–	ponowne uruchomienie urządzenia. Przykład: `RESET 123456`
`OUTPUTx`	`ON`	włączenie wyjścia; **x** to numer wyjścia. Przykład: `OUTPUT1 123456 ON`
`OUTPUTx`	`OFF`	wyłączenie wyjścia; **x** to numer wyjścia. Przykład: `OUTPUT1 123456 OFF`
`OUTPUTx`	`PULSE=ttt`	włączenie wyjścia na określony czas: **x** to numer wyjścia OUT, **ttt** to czas impulsu w sekundach, liczbą trzycyfrową. Przykład: `OUTPUT1 123456 PULSE=002`
`PSW`	nowe hasło	zmiana hasła. Przykład: `PSW 123456 654123`
`TIME`	`RRRR/MM/DD,GG:MM:SS`	ustawienie daty i godziny. Przykład: `TIME 123456 2026/10/30,12:23:00`
`TXTA`	nazwa obiektu	zapisanie nazwy obiektu. Przykład: `TXTA 123456 Dom`
`TXTE`	`Z1=` … `Z12=`	treść SMS-a wysyłanego przy alarmie strefy; Z1…Z12 – numer wejścia (strefy). Przykład: `TXTE 123456 Z1=ALARM Strefa1`
`TXTR`	`Z1=` … `Z12=`	treść SMS-a wysyłanego przy przywróceniu strefy; Z1…Z12 – numer wejścia (strefy). Przykład: `TXTR 123456 Z1=Strefa1 przywrocona`

Polecenie	Dane	Opis
`RDR`	`numer telefonu#treść SMS`	przekazanie SMS-a na podany numer telefonu; numer musi zaczynać się od znaku + i międzynarodowego numeru kierunkowego kraju. Przykład: `RDR 123456 +48601234567#przekazany tekst`
`ASKI`	–	SMS o stanie wejść (IN). Przykład: `ASKI 123456`
`ASKO`	–	SMS o stanie wyjść (OUT). Przykład: `ASKO 123456`
`ASKT`	–	SMS z wartościami wszystkich czujników temperatury. Przykład: `ASKT 123456`
`DISARM`	`SYS:x`	rozbrojenie alarmu; **x** to numer partycji (1–8). Przykład: `DISARM 123456 SYS:1`
`ARM`	`SYS:x`	uzbrojenie alarmu; **x** to numer partycji (1–8). Przykład: `ARM 123456 SYS:1`
`FRS`	–	reset wyjścia czujek pożarowych, jeśli do wyjścia OUT przypisana jest funkcja resetu czujek pożarowych (**Fire Sensor Reset**, punkt 5.7). Przykład: `FRS 123456`
`SETN`	`PHONEx=numer telefonu#imię`	dodanie numeru telefonu i nazwy użytkownika do użytkownika x; **x** to wiersz numeru telefonu na liście. Numer musi zaczynać się od znaku + i międzynarodowego numeru kierunkowego kraju, numer i imię oddziela `#`. Przykład: `SETN 123456 PHONE5=+48601234567#JAN`
`SETN`	`PHONEx=DEL`	usunięcie numeru telefonu i imienia użytkownika. Przykład: `SETN 123456 PHONE5=DEL`
`UUSD`	`*kod USSD#`	wysłanie kodu USSD do operatora komórkowego. Przykład: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON`	połączenie z usługą chmury Protegus. Przykład: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`Protegus=OFF`	odłączenie od usługi chmury Protegus. Przykład: `CONNECT 123456 PROTEGUS=OFF`
`CONNECT`	`Code=123456`	kod usługi chmury Protegus (**Cloud Access Code**, punkt 5.4). Przykład: `CONNECT 123456 CODE=123456`
`CONNECT`	`IP=0.0.0.0:8000`	adres IP TCP i port serwera kanału głównego. Przykład: `CONNECT 123456 IP=0.0.0.0:8000`
`CONNECT`	`IP=0`	wyłączenie kanału głównego. Przykład: `CONNECT 123456 IP=0`
`CONNECT`	`ENC=123456`	klucz szyfrowania TRK. Przykład: `CONNECT 123456 ENC=123456`
`CONNECT`	`APN=Internet`	nazwa APN. Przykład: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`USER=user`	nazwa użytkownika APN. Przykład: `CONNECT 123456 USER=User`
`CONNECT`	`PSW=password`	hasło APN. Przykład: `CONNECT 123456 PSW=Password`
`SETHx`	–	ustawienia termostatu: **x** to numer termostatu (1, 2, 3 lub 4); parametry opisują kolejne wiersze.
`SETHx`	`Ty=45`	temperatura trybu **y** (można ustawić 4 tryby). Przykład – tryb 2 termostatu 1 na +45 °C: `SETH1 123456 T2=45`
`SETHx`	`Sy=2`	numer czujnika temperatury, który mierzy w trybie **y** (można ustawić 4 tryby). Przykład – w trybie 1 termostatu 2 mierzy czujnik temperatury 2: `SETH2 123456 S1=2`

Polecenie	Dane	Opis
`SETHx`	`O=1`	wyjście OUT przypisane do termostatu (typ wyjścia musi być **Remote Control** lub **Thermostat**, punkt 5.7). Przykład – wyjście 1 do termostatu 1: `SETH1 123456 O=1`
`SETHx`	`A=2`	czujnik temperatury decydujący o pracy termostatu: który z czujników podanych dla czterech trybów ma być aktywny. Przykład – w termostacie 1 aktywny jest czujnik trybu 3: `SETH1 123456 A=3`
`SETHx`	`M=C`	tryb pracy termostatu: **C** – chłodzenie, **H** – ogrzewanie. Przykład – termostat 1 w trybie chłodzenia: `SETH1 123456 M=C`
`SETHx`	kilka ustawień, po przecinku	jednym SMS-em można zmienić jedno lub kilka ustawień, poszczególne ustawienia oddziela przecinek. Przykład: `SETH2 123456 T2=55,S3=5,A=3,O=1,M=H` – temperatura trybu 2 termostatu 2 wynosi +55 °C; tryb 3 działa według czujnika temperatury 5; aktywny jest czujnik trybu 3; termostat przełącza wyjście OUT 1; tryb pracy to ogrzewanie.
`ASKH`	–	SMS o ustawieniach wszystkich termostatów: czy termostat jest włączony, czy chłodzi, czy grzeje, numer aktywnego trybu i wszystkie ustawione temperatury. Przykład: `ASKH 123456`

W miejsce numeru telefonu i imienia z przykładów wpisz własne dane. Lista APN-ów: Ustawienie APN – lista europejskich operatorów komórkowych.

4.3 Sterowanie połączeniem telefonicznym

Jeśli do systemu nie dodano jeszcze żadnego użytkownika, administratorem systemu zostaje ten, kto pierwszy zadzwoni do CG17: potem tylko on może sterować CG17 połączeniem telefonicznym i poleceniem SMS. Dlatego pierwsze połączenie wykonaj z telefonu właściciela lub instalatora. Jeśli chcesz pozwolić na sterowanie połączeniem także innym użytkownikom, dodaj ich w TrikdisConfig (punkt 5.4) lub poleceniem SMS (`SETN`, punkt 4.2).

Polecenia CG17 wydawane połączeniem – sterowanie wyjściami OUT połączeniem telefonicznym:

1. Jeśli system alarmowy składa się z jednej partycji albo użytkownik nie ma uprawnień do sterowania wyjściami (kolumna **PGM** listy użytkowników, punkt 5.4): zadzwoń do CG17. Centrala odrzuci połączenie, a tryb ochrony systemu alarmowego zmieni się na przeciwny: uzbrojony system się rozbroi, a rozbrojony uzbroi.
2. Jeśli użytkownik ma uprawnienia do sterowania wyjściami OUT, a typ wyjścia OUT w TrikdisConfig to **Remote Control** (punkt 5.7), albo system alarmowy CG17 składa się z dwóch lub więcej partycji: zadzwoń do CG17. CG17 odbierze połączenie i polecenia możesz wpisywać na klawiaturze telefonu (zobacz tabelę).

Polecenia z klawiatury telefonu

Klawisze	Funkcja	Opis
`[1]`	zmiana trybu ochrony	zmienia tryb ochrony na przeciwny do bieżącego. Przykład: `1`

Klawisze	Funkcja	Opis
`[2][numer wyjścia][#][stan][*]`	sterowanie wybranym wyjściem OUT	przełącza podane wyjście OUT. Stan: `0` – wyłączenie; `1` – włączenie; `2` – wyłączenie na czas impulsu; `3` – włączenie na czas impulsu (czas impulsu podajesz w tabeli **PGM** TrikdisConfig, punkt 5.7); `*` – koniec polecenia. Przykład – włączenie wyjścia 5 OUT: `21#1*`; włączenie wyjścia 6 OUT na czas impulsu (**Pulse time**) podany w tabeli **PGM**: `22#3*`
`[6][numer partycji][#]`	uzbrojenie podanej partycji systemu alarmowego	Przykład – uzbrojenie partycji 2: `62#`
`[7][numer partycji][#]`	rozbrojenie podanej partycji systemu alarmowego	Przykład – rozbrojenie partycji 1: `71#`

5. Konfiguracja programem TrikdisConfig

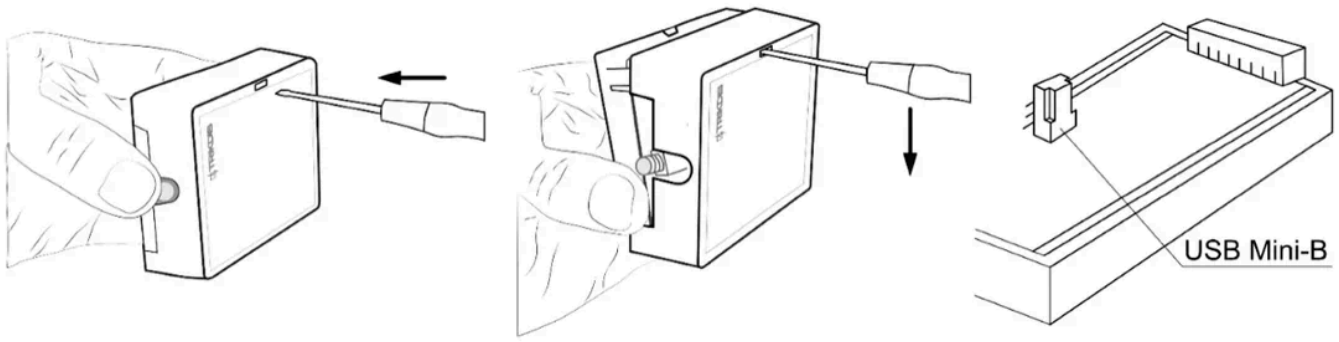
Parametry CG17 ustawiasz programem **TrikdisConfig** – przez kabel USB lub zdalnie (rozdział 6). Podstawowe ustawienia potrzebne dla aplikacji Protegus 2 i stacji monitorowania opisuje rozdział 2; ten rozdział przedstawia po kolei strony programu.

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!

1. Płaskim śrubokrętem zdejmij pokrywę CG17 tak, jak pokazuje rysunek.
2. Połącz CG17 z komputerem kablem **USB Mini-B**.
3. Uruchom TrikdisConfig. Program automatycznie rozpozna podłączoną centralę CG17 i otworzy jej okno programowania.
4. Kliknij przycisk **Read [F4]**: program odczyta bieżące ustawienia CG17. Jeśli program o to poprosi, w wyskakującym oknie podaj kod **administratora** lub **instalatora** (kody fabryczne: punkt 5.2.2).



Rysunek 44. Zdejmowanie pokrywy: włóż płaski śrubokręt do otworu z boku obudowy i podważając w dół, odepnij pokrywę. Pod nią, na płytce drukowanej, jest złącze **USB Mini-B**.

Ostrzeżenie

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

5.1 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 45. Pasek stanu CG17: w lewym polu **IMEI/Unique ID**, obok **Status: reading done**, **Device: CG17_1210** (kod typu), **SN** (numer seryjny), wersja **BL**, **FW** i **HW**, **State: USB** (sposób połączenia) i **Role: Administrator** (poziom dostępu). W polu **Device** musi stać oznaczenie typu **CG17**.

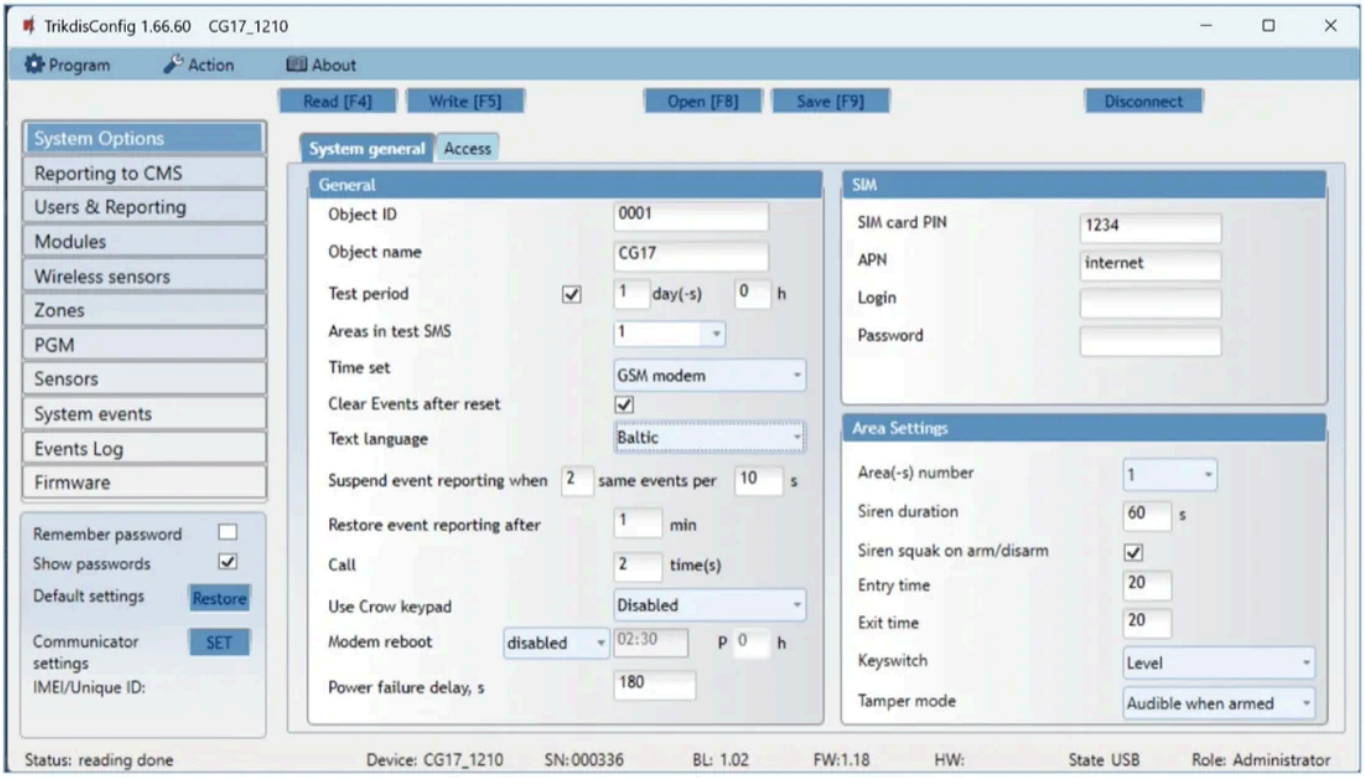
Po kliknięciu przycisku **Read [F4]** program odczytuje i wyświetla ustawienia zapisane w CG17; potrzebne parametry ustawiasz na stronach opisanych w kolejnych punktach. Jeśli chcesz wrócić do ustawień fabrycznych, kliknij przycisk **Restore** w lewej dolnej części ekranu (punkt 5.11).

5.2 Strona „System Options"

Strona ma dwie karty: na karcie **System general** podajesz ustawienia ogólne, ustawienia karty SIM i partycji, a na karcie **Access** – kody dostępu.

5.2.1 Karta System general

Tu podajesz identyfikator obiektu, ustawienia komunikatów testowych, synchronizacji czasu i wysyłania zdarzeń, dane karty SIM oraz czasy partycji.



Rysunek 46. TrikdisConfig – **System Options**, karta **System general**: grupy **General**, **SIM** i **Area Settings**.

Grupa General

- **Object ID** – jeśli wysyłasz zdarzenia do stacji monitorowania, wpisz identyfikator obiektu otrzymany od stacji monitorowania (4-cyfrowa liczba szesnastkowa, 0–9, A–F). Nie używaj identyfikatorów FFFE i FFFF.
- **Object name** – nazwa urządzenia, która pojawia się w SMS-ach o zdarzeniach (maksymalnie 20 znaków, litery i cyfry).
- **Test period** – po zaznaczeniu CG17 wysyła w ustawionych odstępach czasu okresowy komunikat testowy (**Test**).
- **Areas in test SMS** – komunikat testowy zawiera także stan wybranych partycji.
- **Time set** – źródło synchronizacji czasu. Po wybraniu **IP server** CG17 dostosowuje się do czasu odbiornika IP, a po wybraniu **Cellular modem** (na obrazku **GSM modem**) – do czasu serwera operatora komórkowego.
- **Clear Events after reset** – po ponownym uruchomieniu (reset) urządzenie usuwa wszystkie niewysłane komunikaty o zdarzeniach.
- **Text language** – język SMS-ów: CG17 używa w SMS-ach znaków specjalnych tego języka.
- **Suspend event reporting when … same events per … s** – wstrzymuje wysyłanie zdarzeń, jeśli podana liczba jednakowych zdarzeń wystąpi w podanej liczbie sekund.
- **Restore event reporting after** – po tym czasie kończy się wstrzymanie wysyłania zdarzeń (0–999 minut).
- **Call** – po zdarzeniu CG17 dzwoni do użytkownika (użytkowników) podaną liczbę razy. Jeśli połączenie zostanie odrzucone lub odebrane, CG17 przestaje dzwonić. Jedno połączenie trwa 20 sekund.
- **Modem reboot** – ponowne uruchomienie modemu o podanej godzinie.

- **AC failure delay** (na obrazku **Power failure delay, s**) – jeśli zaniknie zasilanie główne, CG17 wysyła powiadomienie o awarii zasilania po podanym opóźnieniu. Gdy napięcie zasilania powróci, powiadomienie o przywróceniu także wysyła po podanym opóźnieniu.

Grupa SIM

- **SIM card PIN** – kod PIN karty SIM.
- **APN** – nazwa internetowego punktu dostępu operatora komórkowego. Trzeba ją podać, jeśli komunikaty o zdarzeniach idą mobilną transmisją danych (GPRS) do chmury Protegus lub do stacji monitorowania. APN-y operatorów: Ustawienie APN – lista europejskich operatorów komórkowych.
- **Login**, **Password** – jeśli operator karty SIM tego wymaga, podaj tu nazwę użytkownika i hasło APN.

Grupa Area Settings

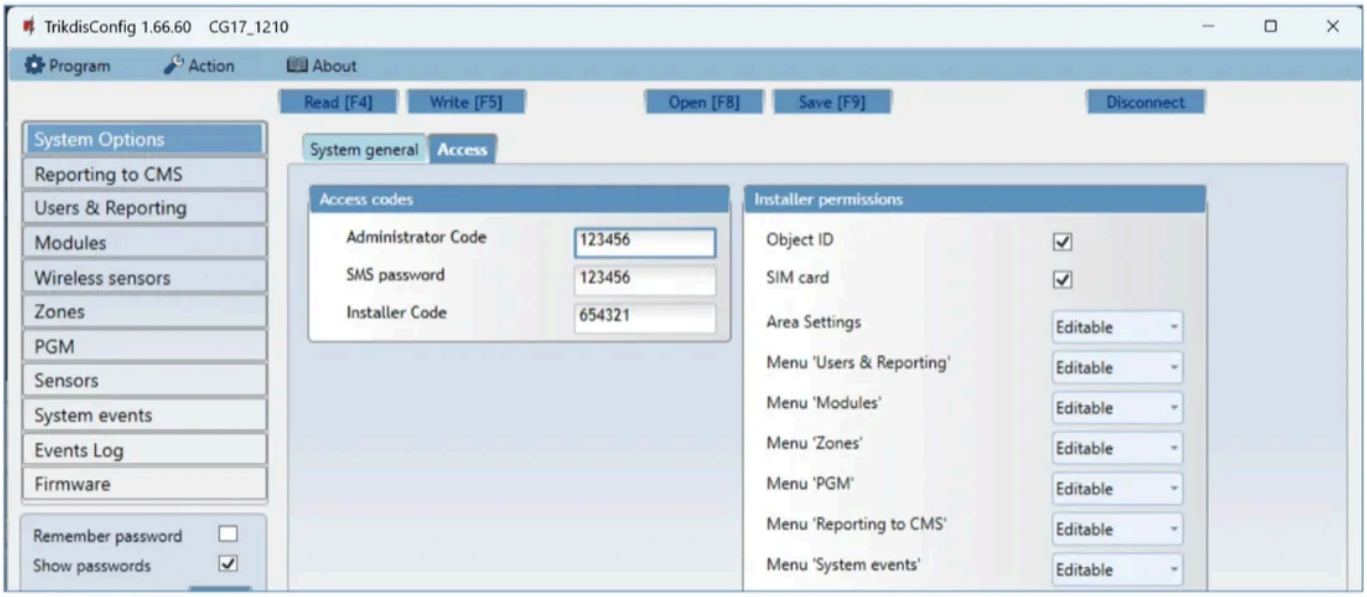
- **Area(-s) number** – liczba niezależnych od siebie części (partycji) systemu alarmowego.

Jeśli podłączony jest sygnalizator, a jedno wyjście OUT (przypisane do partycji) ma typ **Siren** (punkt 5.7.1):

- **Siren duration** – przy alarmie sygnalizator działa przez ten czas (0–999 s).
- **Siren squak on arm/disarm** – przy uzbrojeniu sygnalizator odzywa się krótko raz, przy rozbrojeniu dwa razy.
- **Entry time** – czas na wejście przez strefę opóźnioną (**Delay**) (0–999 s).
- **Exit time** – czas na wyjście przez strefę opóźnioną (**Delay**) (0–999 s). Jeśli uzbrajasz system z aplikacji Protegus 2 lub połączeniem telefonicznym, system nie odlicza czasu na wyjście.
- **Keyswitch** – sposób uzbrajania i rozbrajania strefą przełącznika kluczykowego (**Keyswitch**): **Pulse** (impuls) lub **Level** (poziom).
- **Tamper mode** – reakcja systemu, gdy czujka zgłosi sabotaż:
- **Silent** – odbiorcy otrzymują komunikat o zdarzeniu, ale sygnalizator się nie włącza;
- **Audible when armed** – odbiorcy otrzymują komunikat o zdarzeniu, a sygnalizator włącza się tylko wtedy, gdy sabotaż nastąpi w stanie uzbrojenia;
- **Always Audible** – odbiorcy otrzymują komunikat o zdarzeniu, a sygnalizator włącza się także przy rozbrojonym systemie.

5.2.2 Karta Access – kody dostępu

Tu podajesz kody dostępu i uprawnienia instalatora.



Rysunek 47. TrikdisConfig – **System Options**, karta **Access**: w grupie **Access codes Administrator Code**, **SMS password** i **Installer Code**; w grupie **Installer permissions** to, które ustawienia (np. **Object ID**, **SIM card**, **Area Settings**) i które strony (**Users & Reporting**, **Modules**, **Zones**, **PGM**, **Reporting to CMS**, **System events**) instalator może zmieniać (**Editable**).

Grupa Access codes

- **Administrator Code** – kod administratora (fabrycznie `123456`): daje pełny dostęp do ustawień. Dokładnie 6 znaków, litery łacińskie i/lub cyfry.
- **SMS password** – hasło sterowania SMS-em (fabrycznie `123456`). Dla większego bezpieczeństwa zmień je na 6-znakowy kod znany tylko tobie.
- **Installer Code** – kod instalatora (fabrycznie `654321`): za jego pomocą instalator uzyskuje dostęp do ustawień. Ze względów bezpieczeństwa zmień go na 6-znakowy kod znany tylko tobie.

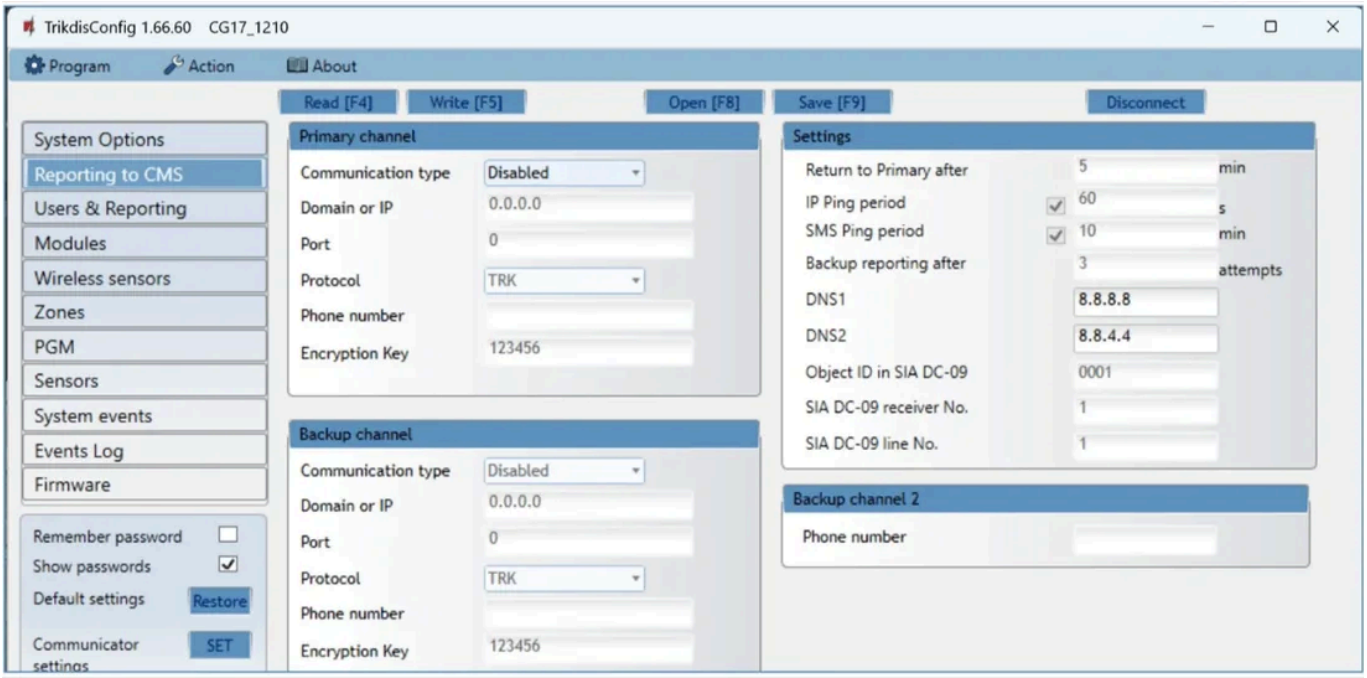
Dopóki ustawiony jest fabryczny kod administratora (`123456`), program nie pyta o kod: po kliknięciu przycisku **Read [F4]** od razu pojawiają się ustawienia zapisane w urządzeniu.

Grupa Installer permissions

- Tu ustawiasz uprawnienia instalatora.

5.3 Strona „Reporting to CMS”

CG17 może wysyłać komunikaty o zdarzeniach do odbiornika stacji monitorowania (CMS) firmy ochroniarskiej. Tu podajesz dane dostępu do odbiornika i sposób działania kanałów.



Rysunek 48. TrikdisConfig – **Reporting to CMS**: ustawienia **Primary channel** (kanał główny) i **Backup channel** (kanał zapasowy), pod nimi grupa **Settings** (odstępy ping, serwery DNS, identyfikatory SIA DC-09) i **Backup channel 2** (zapasowy kanał SMS).

Grupa Primary channel i Backup channel

- **Communication type** – sposób połączenia z odbiornikiem: **TCP/IP**, **UDP/IP** lub **SMS**.
- **Domain or IP** – nazwa domeny lub adres IP odbiornika.
- **Port** – port sieciowy odbiornika.
- **Protocol** – **TRK** do odbiorników Trikdis, **SIA DC-09** do odbiorników uniwersalnych.
- **Phone number** – numer telefonu odbiornika stacji monitorowania, który potrafi odbierać SMS-y.
- **Encryption Key** – 6-cyfrowy klucz szyfrowania; musi być zgodny z kluczem ustawionym w odbiorniku stacji monitorowania.

Grupa Settings

- **Return to primary after** – po tylu minutach CG17 próbuje wrócić do kanału głównego (**Primary channel**).
- **IP Ping period** – odstęp wysyłania sygnałów kontrolnych PING przez mobilną transmisję danych (GPRS), w sekundach. Aby sygnały były wysyłane, zaznacz pole.
- **SMS PING period** – odstęp wysyłania sygnałów kontrolnych PING kanałem SMS, w minutach. Aby sygnały były wysyłane, zaznacz pole.
- **Backup reporting after** – po tylu nieudanych próbach wysłania CG17 przełącza się z kanału głównego na kanał zapasowy (**Backup channel**).
- **DNS1**, **DNS2** – adresy serwerów DNS.
- **Object ID in SIA DC-09** – numer obiektu przy protokole SIA DC-09.
- **SIA DC-09 receiver No.** – numer odbiornika.
- **SIA DC-09 line No.** – numer linii.

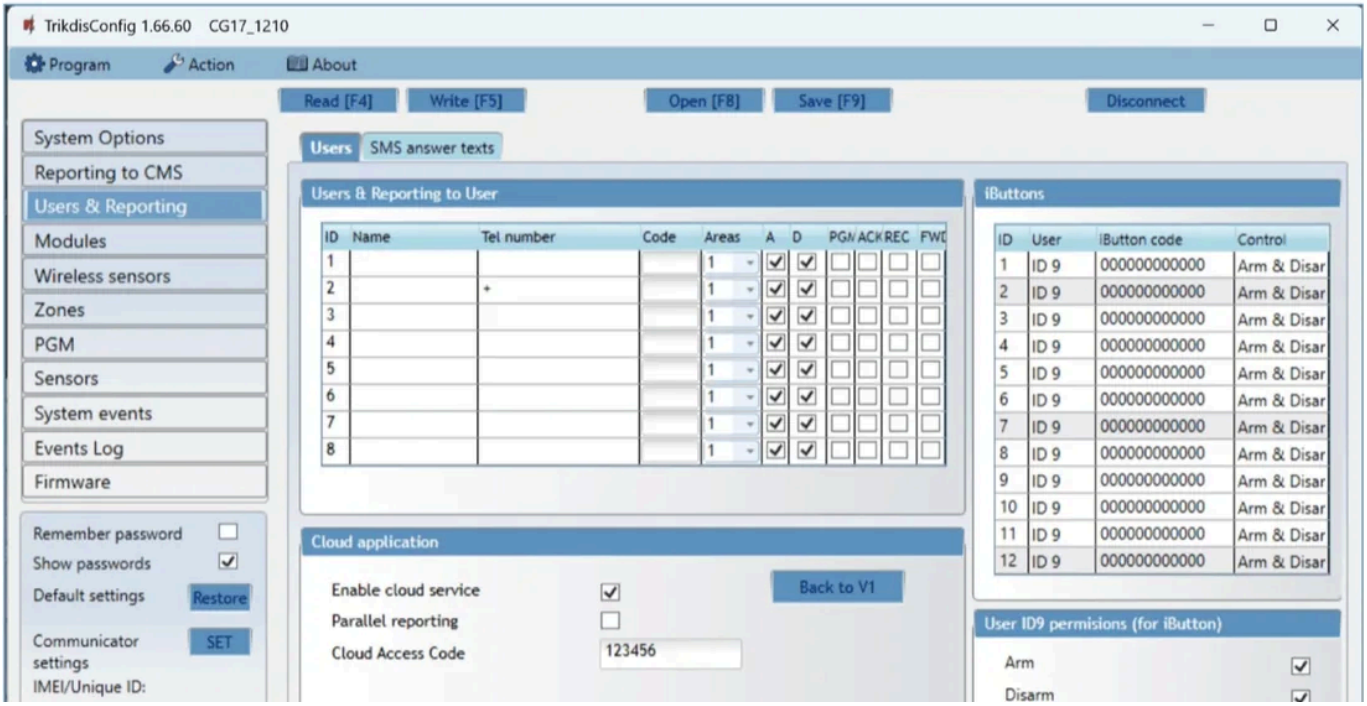
Grupa Backup channel 2

- **Phone number** – numer telefonu odbiornika stacji monitorowania, który potrafi odbierać SMS-y, z numerem kierunkowym kraju (np. 48xxxxxxxxx). Ten zapasowy kanał SMS (**Backup SMS**) CG17 wykorzystuje, gdy nie może wysłać wiadomości ani kanałem głównym (**Primary**), ani zapasowym

(**Backup**). Działa także wtedy, gdy w sieci operatora komórkowego zostanie przerwane połączenie IP. Działa tylko wtedy, gdy w kanale głównym i zapasowym ustawiony jest tryb GPRS (mobilna transmisja danych). CG17 wysyła SMS do stacji odbiorczej: 1) gdy włączysz ją po raz pierwszy; 2) gdy w kanale głównym i zapasowym zostanie przerwane połączenie TCP/IP lub UDP/IP.

5.4 Strona „Users & Reporting"

Na karcie **Users** ustawiasz użytkowników, połączenie z chmurą Protegus i klucze dotykowe (iButton); na karcie **SMS answer texts** – treść SMS-ów z odpowiedzią (punkt 5.4.3).



Rysunek 49. TrikdisConfig – **Users & Reporting**, karta **Users**: lista użytkowników (kolumny **Name**, **Tel number**, **Code**, **Areas**, **A**, **D**, **PGM**, **ACK**, **REC**, **FWD**), pod nią lista **iButtons**, obok grupa **Cloud application** i uprawnienia **User ID9** (**Arm**, **Disarm**).

Grupa Users & Reporting to User

- **ID** – numer porządkowy użytkownika na liście.
- **Name** – imię lub adres e-mail użytkownika; ta nazwa pojawia się w SMS-ach o zdarzeniach. Administrator może podać użytkownikowi także adres e-mail: dzięki temu użytkownik może logować się do aplikacji Protegus 2.
- **Tel number** – numer telefonu użytkownika z międzynarodowym numerem kierunkowym (np. +48…). Z tego numeru można zdalnie sterować systemem alarmowym i na ten numer przychodzą SMS-y.
- **Code** – własny kod użytkownika do uzbrajania i rozbrajania.
- **Areas** – partycje, którymi użytkownik może sterować. **User ID9** może sterować tylko partycją 1; nie można tego zmienić.
- **A** – zaznacz, jeśli użytkownik może uzbrajać (ARM) system.
- **D** – zaznacz, jeśli użytkownik może rozbrajać (DISARM) system.
- Jeśli **PGM** i **REC** nie są zaznaczone, ale **A** i **D** tak: gdy użytkownik zadzwoni do CG17, centrala odrzuci połączenie, a stan systemu alarmowego zmieni się na przeciwny (uzbroi się lub rozbroi).
- Jeśli zaznaczone jest tylko **PGM**: użytkownik może zadzwonić do CG17 i poleceniami tonowymi DTMF (klawiaturą telefonu) włączyć lub wyłączyć wybrane wyjście (punkt 4.3).
- **REC** – zarezerwowane dla przyszłej funkcji.

- **ACK** – po zaznaczeniu CG17 po każdym poleceniu otrzymanym SMS-em wysyła użytkownikowi wiadomość z odpowiedzią (**SMS answer text**) (punkt 5.4.3).
- **FWD** – po zaznaczeniu CG17 przekazuje użytkownikowi SMS-y otrzymane od nadawców spoza systemu (np. powiadomienie o saldzie karty SIM, wiadomości reklamowe).

Grupa Cloud application

- **Enable cloud service** – włącza usługę Protegus (**Protegus service**): CG17 może wymieniać dane z aplikacją Protegus 2 i można go konfigurować zdalnie programem TrikdisConfig (rozdział 6).
- **Parallel reporting** – wiadomości wysyła równolegle kanałem głównym i do Protegus 2.
- **Cloud Access Code** – 6-cyfrowy kod do połączenia z Protegus 2 (fabrycznie `123456`, punkt 2.1).

Grupa iButtons

Do jednego użytkownika można przypisać kilka kluczy. Każdy nowo zarejestrowany klucz trafia do użytkownika **User ID9** (No name – bez nazwy). Nazwę można nadać tylko ośmiu użytkownikom. Uprawnienia **User ID9** ustawiasz w grupie **User ID9 permissions**.

- **ID** – numer porządkowy klucza na liście.
- **User** – użytkownik, do którego należy klucz. Jeśli chcesz przypisać klucz do użytkownika, w miejsce **ID9** wpisz numer porządkowy użytkownika z tabeli **Users & Reporting to User** (np. dla użytkownika 3: **ID3** zamiast **ID9**).
- **iButton code** – numer identyfikacyjny klucza dotykowego iButton lub karty RFID.
- **Control** – co ma zrobić system, gdy czytnik (np. TM17) odczyta klucz: **None** (nic), **Arm** (uzbraja), **Disarm** (rozbraja) lub **Arm & Disarm** (uzbraja i rozbraja).

5.4.1 Rejestracja kluczy dotykowych (iButton)

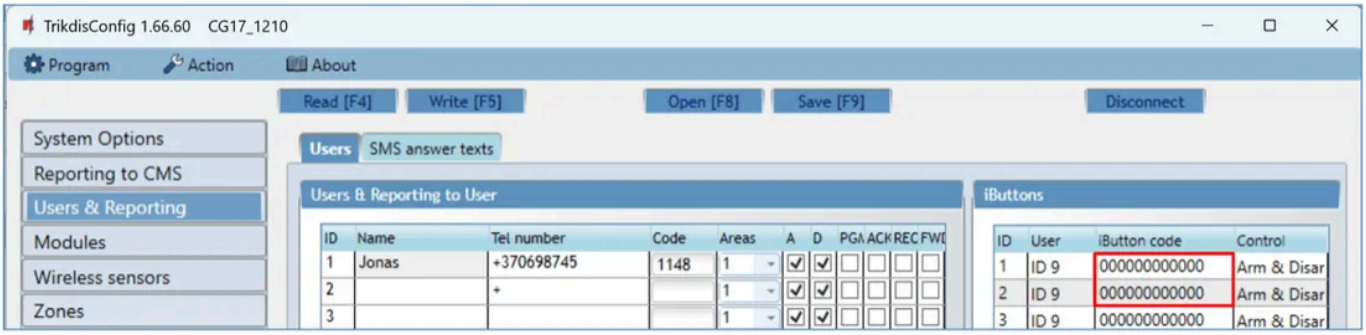
Podłączenie czytnika kluczy opisuje punkt 3.6. Klucze dotykowe rejestrujesz tak:

1. Jeśli lista **iButtons** jest pusta, pierwszy zarejestrowany klucz trafia do pierwszego wiersza listy i staje się kluczem głównym (**Master key**).
2. Aby włączyć tryb rejestracji, przyłóż klucz główny do czytnika na co najmniej 10 sekund. W trybie rejestracji dioda **State** czytnika TM17 miga na zielono.
3. Przykładaj klucze użytkowników do czytnika pojedynczo. Czytnik sygnalizuje zarejestrowanie klucza 3 sygnałami dźwiękowymi.
4. Gdy skończysz z kluczami użytkowników, aby wyłączyć tryb rejestracji, przyłóż ponownie klucz główny do czytnika. Wtedy dioda **State** TM17 przestaje migać.
5. Aby usunąć wszystkie klucze (łącznie z kluczem głównym), przyłóż klucz główny do czytnika na co najmniej 20 sekund.

Klucza głównego używaj tylko do rejestrowania pozostałych kluczy dotykowych.

5.4.2 Rejestracja kart RFID

Do tego potrzebny jest moduł iO-LORA podłączony do CG17, do którego podłączony jest czytnik RFID z klawiaturą (punkt 3.16). Numer identyfikacyjny karty RFID wpisz w pole **iButton code** listy **iButtons**.

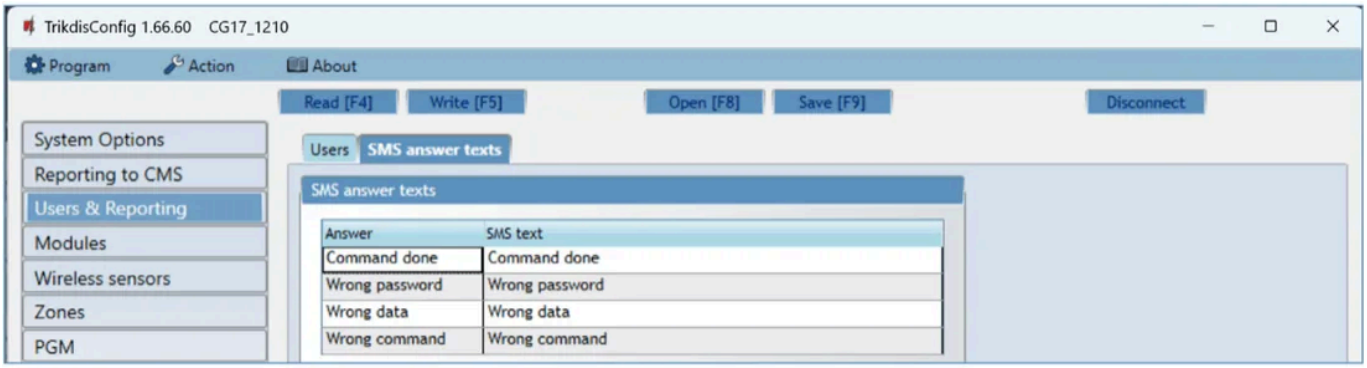


Rysunek 50. TrikdisConfig – karta **Users**: na liście użytkowników przykładowy użytkownik (**Jonas**) z numerem telefonu; na liście **iButtons** zaznaczone na czerwono pole **iButton code**, tu wpisuje się numer identyfikacyjny karty RFID.

Po zmianach kliknij przycisk **Write [F5]** i poczekaj, aż aktualizacja się zakończy.

5.4.3 Karta SMS answer texts – SMS-y z odpowiedzią

Tu możesz zmienić treść wiadomości z odpowiedzią, które CG17 wysyła na polecenia SMS (punkt 4.2).



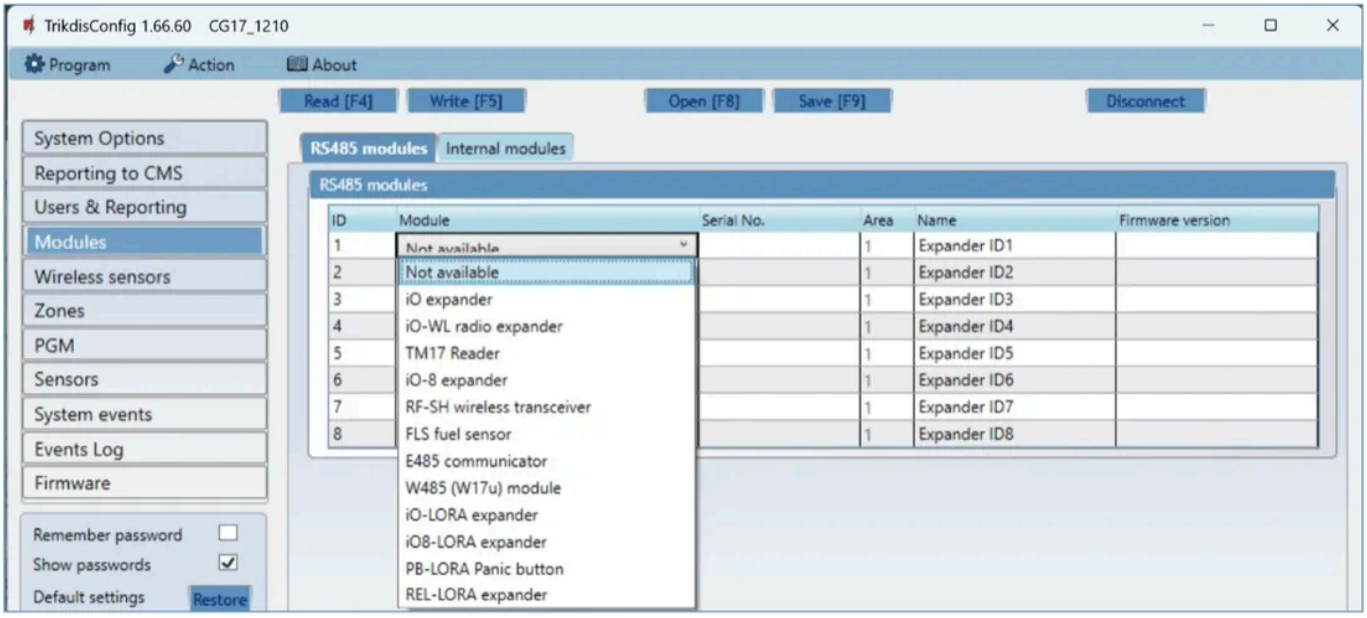
Rysunek 51. TrikdisConfig – **Users & Reporting**, karta **SMS answer texts**: treść odpowiedzi **Command done** (polecenie wykonane), **Wrong password** (błędne hasło), **Wrong data** (błędne dane) i **Wrong command** (błędne polecenie).

Grupa SMS answer texts

- Treść odpowiedzi na polecenia sterujące wysłane SMS-em możesz edytować w polu **SMS text**.

5.5 Strona „Modules”

Tu dodajesz do CG17 moduły podłączone do magistrali RS485. Po wybraniu **W485** lub **E485** pojawia się karta ustawień modułu (**W485 settings**, **E485 settings**); ustawienia modułu GPS są na karcie **Internal modules** (punkt 5.5.4).



Rysunek 52. TrikdisConfig – **Modules**, karta **RS485 modules**: na rozwijanej liście **Module** moduły do wyboru, np. **iO expander**, **iO-WL radio expander**, **TM17 Reader**, **iO-8 expander**, **FLS fuel sensor**, **E485 communicator**, **W485 (W17u) module**, **iO-LORA expander**, **iO8-LORA expander**, **PB-LORA Panic button**, **REL-LORA expander**.

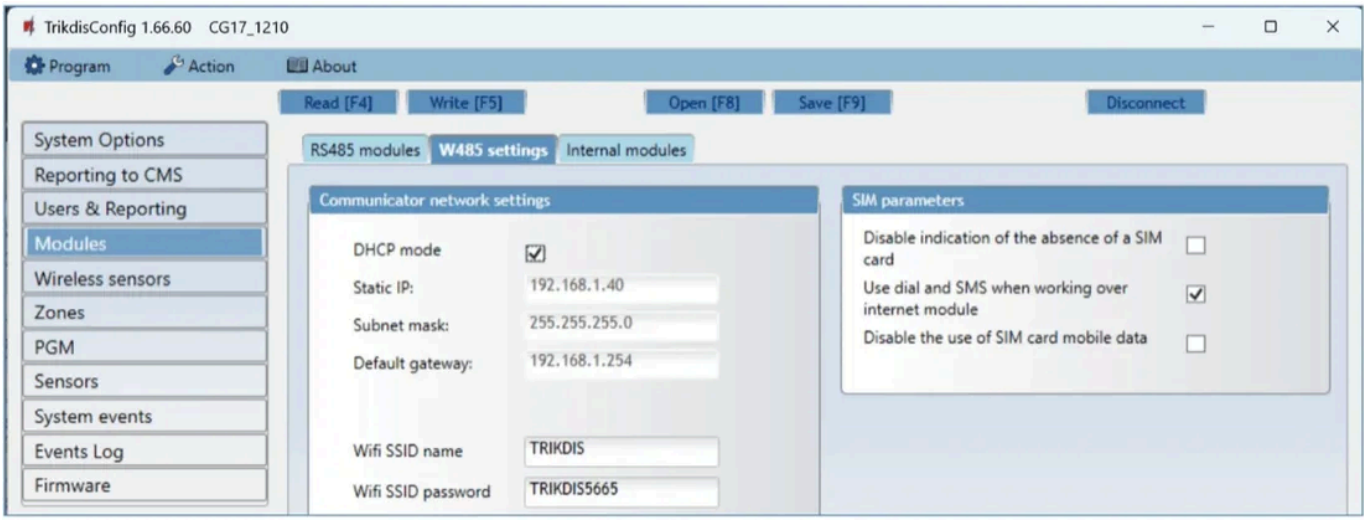
Grupa RS485 modules

- **ID** – numer porządkowy modułu na liście.
- **Module** – wybierz z listy używany moduł: **iO**, **iO-WL**, **TM17**, **iO8**, **FLS**, **E485**, **W485**, **iO-LORA**, **iO8-LORA**, **PB-LORA**, **REL-LORA**.
- **Serial No.** – 6-cyfrowy numer seryjny modułu, trzeba go obowiązkowo podać; znajdziesz go na naklejce na obudowie i opakowaniu modułu.
- **Area** – partycja, do której przypisujesz moduł. TM17 pokazuje stan tej partycji, do której jest przypisany, i stref przypisanych do tej partycji.
- **Name** – możesz nadać modułowi nazwę.
- **Firmware version** – wersja oprogramowania układowego modułu; pojawia się, gdy CG17 wykryje podłączony moduł.

Podłączenie modułów: TM17 – punkt 3.6; iO8 i iO-WL – punkt 3.7; iO – punkt 3.9; Strela RS485 (FLS) – punkt 3.10; W485 – punkt 3.14; E485 – punkt 3.15; iO-LORA, iO8-LORA, PB-LORA i REL-LORA (przez nadajnik-odbiornik RF-LORA) – punkt 3.16.

5.5.1 Karta W485 settings – moduł Wi-Fi

Po wybraniu modułu Wi-Fi **W485** na tej karcie podajesz dane sieci Wi-Fi i sposób korzystania z karty SIM.



Rysunek 53. TrikdisConfig – **Modules**, karta **W485 settings**: grupa **Communicator network settings** (DHCP, adres IP, maska podsieci, brama, nazwa i hasło sieci Wi-Fi) i grupa **SIM parameters**.

Grupa Communicator network settings

- **DHCP mode** – sposób rejestracji modułu Wi-Fi w sieci: automatyczny lub ręczny.
- **Static IP** – stały adres IP w trybie ręcznym.
- **Subnet mask** – maska podsieci w trybie ręcznym.
- **Default gateway** – adres bramy w trybie ręcznym.
- **Wifi SSID name** – nazwa sieci Wi-Fi, z którą łączy się W485.
- **Wifi SSID password** – hasło sieci Wi-Fi.

Grupa SIM parameters

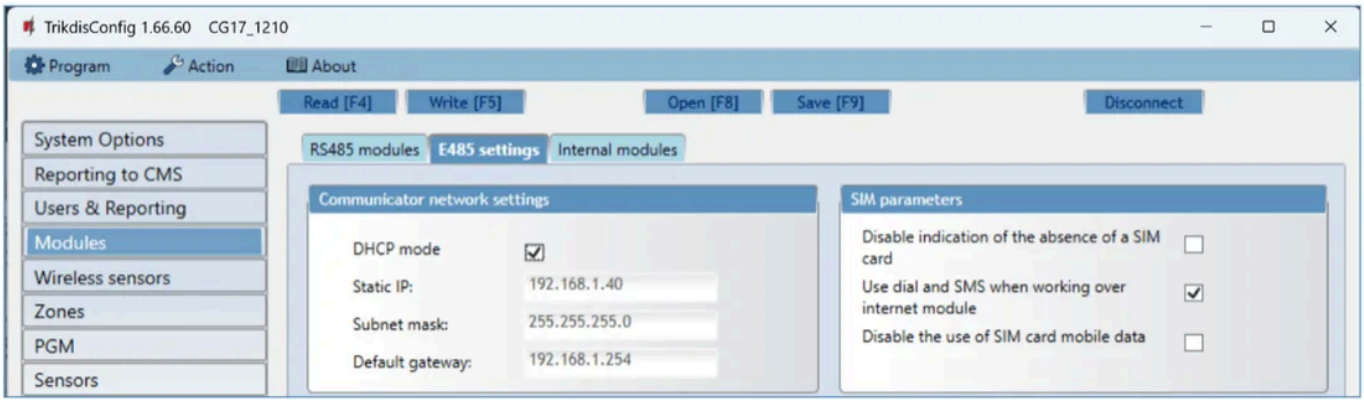
- **Disable indication of the absence of a SIM card** – po zaznaczeniu CG17 nie sygnalizuje braku karty SIM, jeśli pracuje bez niej.
- **Use dial and SMS when working over internet module** – po zaznaczeniu CG17 wysyła powiadomienie jednocześnie połączeniem, SMS-em i przez podłączony moduł Wi-Fi W485. Jeśli pole zostawisz puste i sieć Wi-Fi jest dostępna, CG17 nie używa SMS-ów ani połączeń. Jeśli pole zostawisz puste i sieci Wi-Fi nie ma, CG17 obsługuje połączenia i wiadomości SMS oraz wysyła SMS do użytkownika.
- **Disable the use of SIM card mobile data** – po zaznaczeniu CG17 nie korzysta z mobilnej transmisji danych karty SIM: dane idą tylko przez moduł W485. Jeśli sieć Wi-Fi zniknie, CG17 przechowuje dane w pamięci i po powrocie sieci wysyła je przez W485.

Do zdarzenia błędu magistrali danych RS485 możesz przypisać kod zdarzenia i przywrócenia Contact ID. Gdy połączenie między W485 a CG17 zostanie przerwane lub przywrócone, CG17 wysyła wiadomość z przypisanym kodem CID do stacji monitorowania i do aplikacji Protegus 2. Na stronie **System events** zdarzenie występuje pod nazwą **RS485 fault** (punkt 5.9.1).

- Ustaw CG17 tak, aby wysyłał wiadomości do stacji monitorowania i do Protegus 2: zobacz punkt 2.2 (połączenie ze stacją monitorowania) i punkt 2.1 (połączenie z aplikacją Protegus 2).
- Jeśli CG17 (od wersji oprogramowania układowego 1.13) pracuje z modułem W485, nie potrzebuje karty SIM.

5.5.2 Karta E485 settings – moduł Ethernet

Po wybraniu modułu Ethernet **E485** na tej karcie podajesz dane sieci przewodowej i sposób korzystania z karty SIM.



Rysunek 54. TrikdisConfig – **Modules**, karta **E485 settings**: grupa **Communicator network settings** (DHCP, adres IP, maska podsieci, brama) i grupa **SIM parameters**.

Grupa Communicator network settings

- **DHCP mode** – sposób rejestracji modułu Ethernet w sieci: automatyczny lub ręczny.
- **Static IP** – stały adres IP w trybie ręcznym.
- **Subnet mask** – maska podsieci w trybie ręcznym.
- **Default gateway** – adres bramy w trybie ręcznym.

Grupa SIM parameters

- **Disable indication of the absence of a SIM card** – po zaznaczeniu CG17 nie sygnalizuje braku karty SIM, jeśli pracuje bez niej.
- **Use dial and SMS when working over internet module** – po zaznaczeniu CG17 wysyła powiadomienie jednocześnie połączeniem, SMS-em i przez podłączony moduł Ethernet E485. Jeśli pole zostawisz puste i połączenie internetowe jest dostępne, CG17 nie używa SMS-ów ani połączeń. Jeśli pole zostawisz puste i połączenia internetowego nie ma, CG17 obsługuje połączenia i wiadomości SMS oraz wysyła SMS do użytkownika.
- **Disable the use of SIM card mobile data** – po zaznaczeniu CG17 nie korzysta z mobilnej transmisji danych karty SIM: dane idą tylko przez moduł E485. Jeśli połączenie internetowe zniknie, CG17 przechowuje dane w pamięci i po powrocie połączenia wysyła je przez E485.

Do zdarzenia błędu magistrali danych RS485 możesz przypisać kod zdarzenia i przywrócenia Contact ID. Gdy połączenie między E485 a CG17 zostanie przerwane lub przywrócone, CG17 wysyła wiadomość z przypisanym kodem CID do stacji monitorowania i do aplikacji Protegus 2. Na stronie **System events** zdarzenie występuje pod nazwą **RS485 fault** (punkt 5.9.1).

- Ustaw CG17 tak, aby wysyłał wiadomości do stacji monitorowania i do Protegus 2: zobacz punkt 2.2 (połączenie ze stacją monitorowania) i punkt 2.1 (połączenie z aplikacją Protegus 2).
- Jeśli CG17 (od wersji oprogramowania układowego 1.13) pracuje z modułem E485, nie potrzebuje karty SIM.

5.5.3 Czujnik poziomu paliwa Strela RS485

Wycofane akcesorium

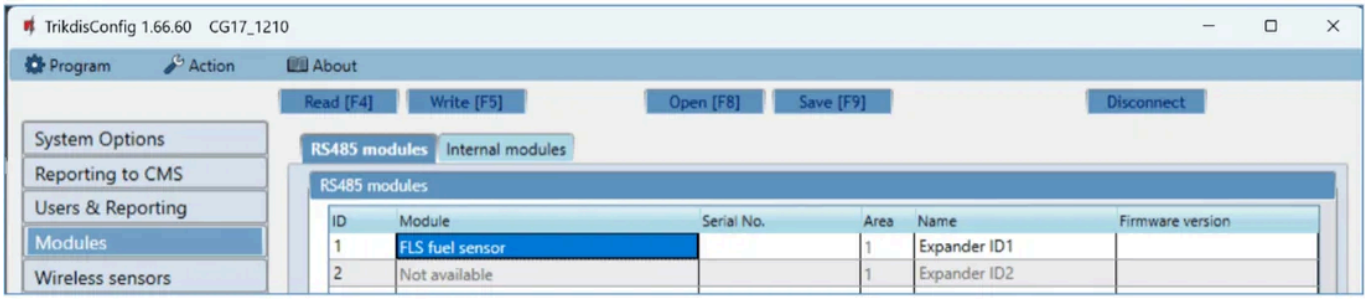
Czujnik poziomu paliwa **Strela RS485** to wycofane akcesorium, u nas niedostępne w sprzedaży. Opis konfiguracji pozostał dla istniejących systemów.

Czujnik poziomu paliwa **Strela RS485** (podłączenie: punkt 3.10) konfigurujesz na stronach **Modules** i **Sensors**.

Czujnik Strela RS485 przed użyciem trzeba skalibrować programem **DUTconfig** producenta czujnika: podłącz czujnik do komputera przez adapter i skalibruj go. Jeśli Strela RS485 jest podłączony do CG17, pozostałe moduły RS485 (iO, iO-WL, TM17, iO8, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA) nie działają.

Grupa RS485 modules

- **Module** – wybierz moduł **FLS fuel sensor**.



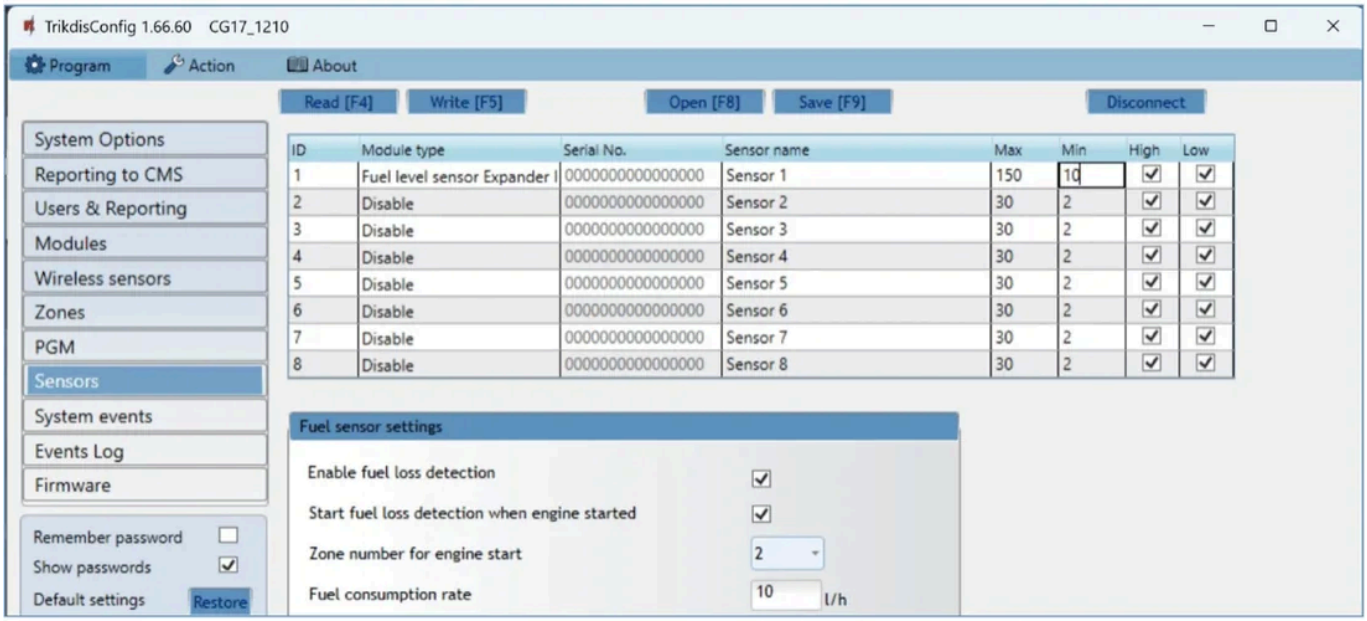
Rysunek 55. TrikdisConfig – **Modules**, karta **RS485 modules**: w wierszu 1 wybrany **FLS fuel sensor** (czujnik poziomu paliwa).

1. Kliknij przycisk **Write [F5]** i poczekaj, aż zapisywanie danych się zakończy.
2. Odłącz kabel USB od CG17 i poczekaj około 1 minuty.
3. Podłącz z powrotem kabel USB do CG17 i kliknij przycisk **Read [F4]**. Program odczyta i wyświetli ustawienia zapisane w CG17.
4. Na stronie **Modules** pojawią się numer seryjny (**Serial No.**) i wersja oprogramowania układowego (**Firmware version**) czujnika Strela RS485.



Rysunek 56. Po odczycie w wierszu **FLS fuel sensor** pojawiają się numer seryjny (**Serial No.**) i wersja oprogramowania układowego (**Firmware version**) czujnika.

Następnie otwórz stronę **Sensors** (punkt 5.8).



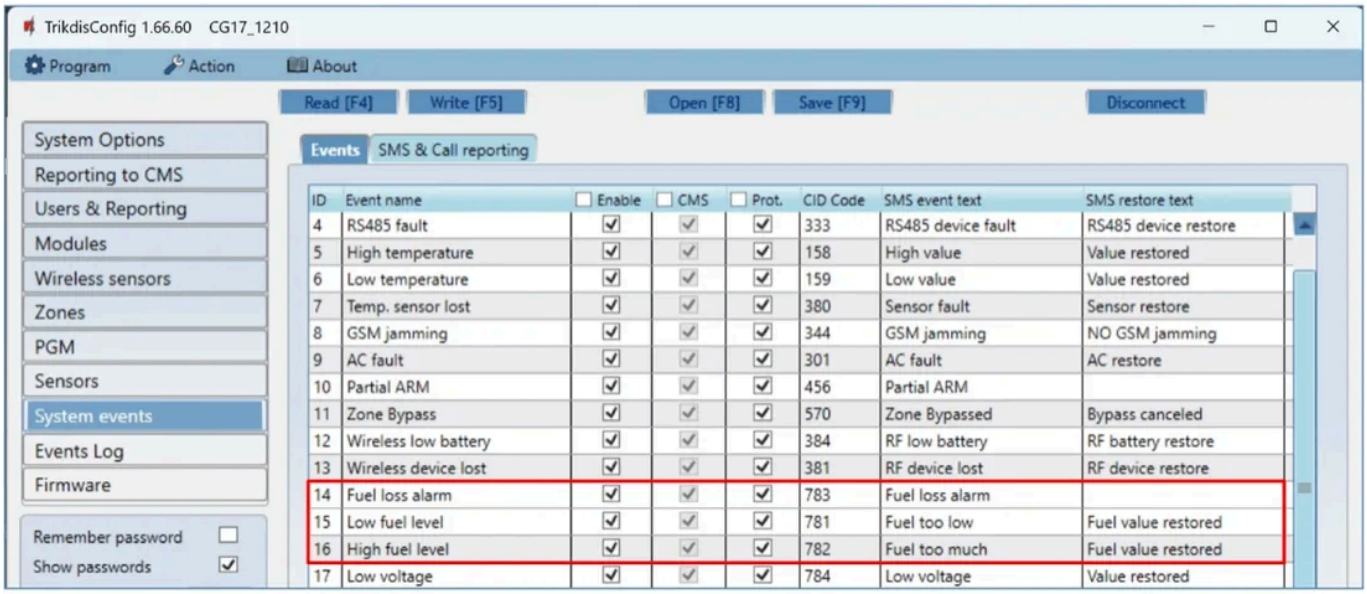
Rysunek 57. TrikdisConfig – **Sensors**: w wierszu 1 **Fuel level sensor** (czujnik poziomu paliwa) z wartościami **Max** i **Min**, poniżej grupa **Fuel sensor settings**.

- **Module type** – wybierz typ **Fuel level sensor**.
- **Sensor name** – nadaj czujnikowi nazwę.
- **Max** – największa ilość paliwa w litrach. Jeśli rzeczywista ilość jest większa, CG17 tworzy komunikat o zdarzeniu; aby komunikat został wysłany, zaznacz pole **High**.
- **Min** – najmniejsza ilość paliwa w litrach. Jeśli rzeczywista ilość jest mniejsza, CG17 tworzy komunikat o zdarzeniu; aby komunikat został wysłany, zaznacz pole **Low**.

Grupa Fuel sensor settings

- **Enable fuel loss detection** – po zaznaczeniu CG17 monitoruje poziom paliwa.
- **Start fuel loss detection when engine started** – po zaznaczeniu monitorowanie zaczyna się przy uruchomieniu silnika. Sygnał uruchomienia silnika trzeba doprowadzić do tego wejścia (strefy) CG17, które podajesz w następnym polu.
- **Zone number for engine start** – numer wejścia (IN) CG17, które aktywuje uruchomienie silnika.
- **Fuel consumption rate** – wielkość zużycia paliwa (l/h).

O nagłej zmianie poziomu paliwa użytkownik otrzymuje SMS; treść SMS-a możesz edytować na stronie **System events** (punkt 5.9.1).



Rysunek 58. TrikdisConfig – **System events**: zaznaczone na czerwono zdarzenia paliwa – **Fuel loss alarm** (utrata paliwa), **Low fuel level** (niski poziom), **High fuel level** (wysoki poziom) – z kodem Contact ID i treścią SMS.

Działanie czujnika poziomu paliwa

Czujnik Strela RS485 podłącz do CG17 według punktu 3.10 i ustaw w CG17 parametry pomiaru. Czujnik mierzy w następujących przypadkach:

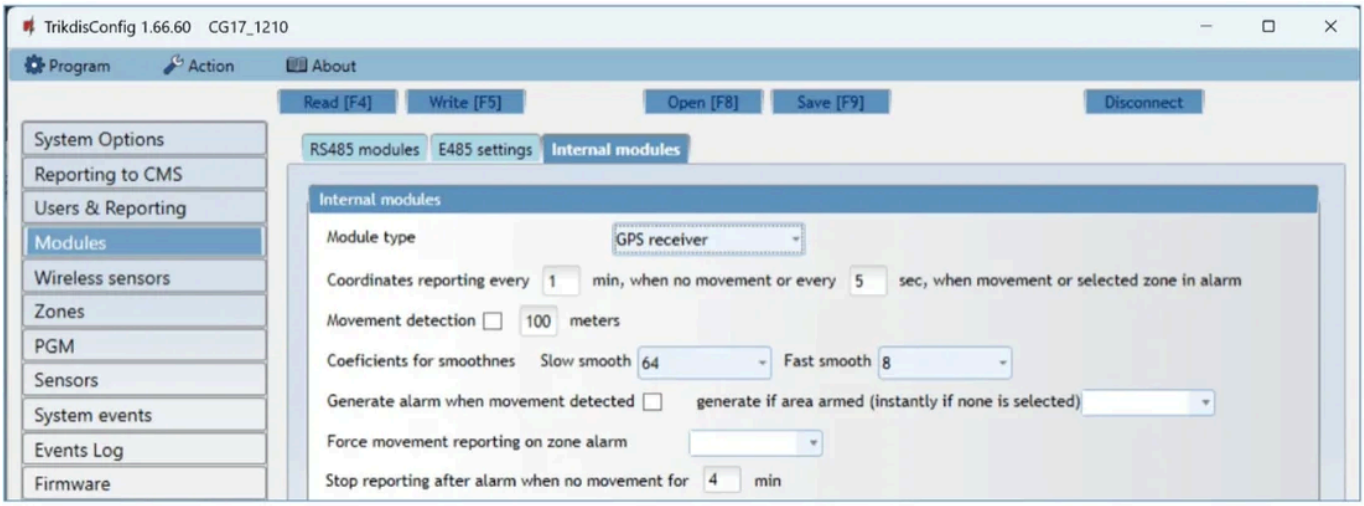
1. Jeśli zaznaczone jest **Enable fuel loss detection**: po włączeniu CG17 czujnik zaczyna monitorować zużycie paliwa, a po wyłączeniu CG17 pomiar się zatrzymuje.
2. Jeśli zaznaczone są zarówno **Enable fuel loss detection**, jak i **Start fuel loss detection when engine started**, i podałeś numer wejścia (IN), które przy uruchomieniu silnika włącza monitorowanie: monitorowanie zaczyna się przy uruchomieniu silnika i zatrzymuje się, gdy wejście powróci do normy (silnik się zatrzyma).

Przy każdym włączeniu czujnik mierzy aktualny poziom paliwa i porównuje go z poziomem zapisanym przed wyłączeniem. Jeśli aktualny poziom jest niższy, CG17 wysyła wiadomość o utracie paliwa do firmy ochroniarskiej i/lub do użytkowników.

Podczas pracy czujnik w określonych odstępach czasu mierzy poziom paliwa i porównuje go z wielkością zużycia. Jeśli w danym odstępie zużycie jest większe od podanej wielkości (**Fuel consumption rate**), CG17 wysyła wiadomość do firmy ochroniarskiej i/lub do użytkowników.

5.5.4 Karta Internal modules – moduł GPS

Na tej karcie podajesz ustawienia modułu GPS: odstęp wysyłania współrzędnych, wykrywanie ruchu i alarm.



Rysunek 59. TrikdisConfig – **Modules**, karta **Internal modules**: odbiornik GPS (**GPS receiver**) z odstępami wysyłania współrzędnych, odległością wykrywania ruchu (w metrach), współczynnikami wygładzania i ustawieniami alarmu.

Grupa Internal modules

- **Module type** – wybierz używany moduł GPS.
- **Coordinates reporting every __ min, when no movement or every __ sec, when movement or selected zone in alarm** – odstęp wysyłania współrzędnych: w minutach w normalnej pracy (brak ruchu), w sekundach, gdy CG17 wykrywa ruch lub wybrana strefa jest w alarmie.
- **Movement detection** – po zaznaczeniu CG17 wszczyna alarm, jeśli odchylenie współrzędnych jest większe od podanego; wtedy wysyła współrzędne częściej.
- **Coefficients for smoothness, Slow smooth** – bez ruchu CG17 wysyła uśrednione współrzędne: średnią z podanej liczby współrzędnych (256 lub innej podanej liczby).
- **Coefficients for smoothness, Fast smooth** – przy ruchu lub alarmie strefy CG17 wysyła uśrednione współrzędne: średnią z podanej liczby współrzędnych (8 lub innej podanej liczby).
- **Generate alarm when movement detected** – po zaznaczeniu przy wykryciu ruchu CG17 wysyła kod zdarzenia Contact ID do stacji monitorowania i powiadamia użytkownika w Protegus 2.
- **Force movement reporting on zone alarm** – podaj strefę systemu alarmowego, do której podłączona jest czujka. Jeśli czujka zgłosi naruszenie (alarm strefy), CG17 wysyła współrzędne częściej.
- **Stop reporting after alarm when no movement for __ min** – czas w minutach: jeśli w tym czasie współrzędne się nie zmienią i nie ma alarmu strefy, wysyłanie współrzędnych wraca do trybu normalnego.

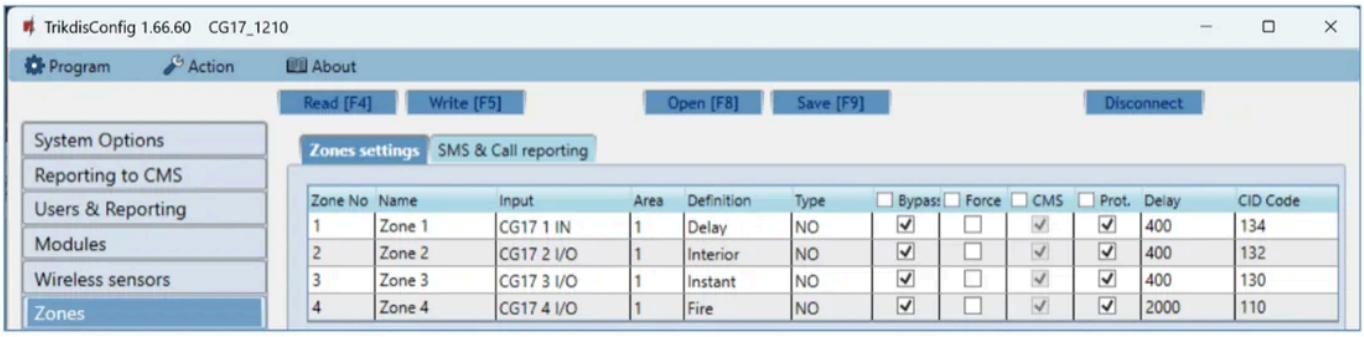
Wiadomości ze współrzędnymi trafiają do programu nadzorczego **Monas MS**.

5.6 Strona „Zones”

Na stronie **Zones** ustawiasz strefy (karta **Zones settings**) oraz to, którzy użytkownicy mają otrzymywać SMS lub połączenie o zdarzeniach stref (karta **SMS & Call reporting**).

5.6.1 Karta Zones settings – strefy

Tu do każdej strefy przypisujesz wejście, partycję, typ strefy i kod Contact ID.



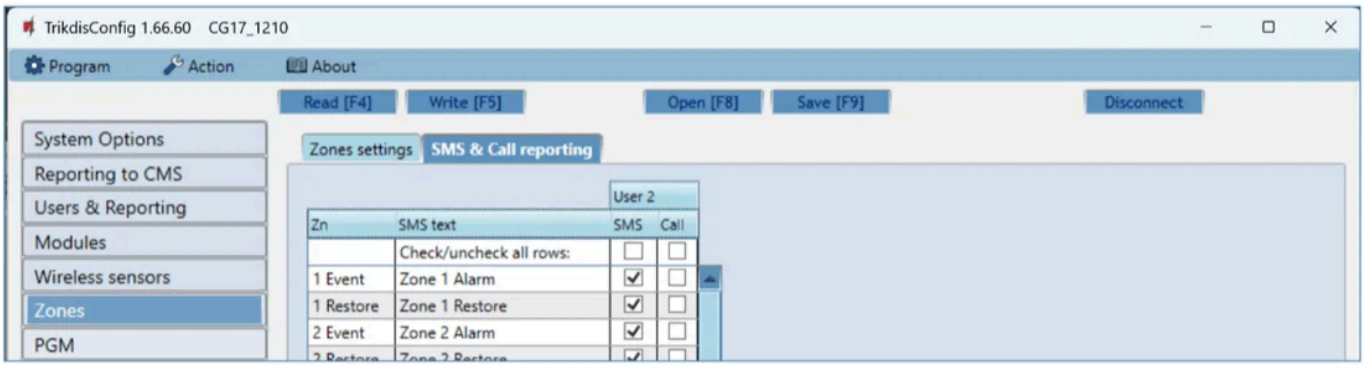
Rysunek 60. TrikdisConfig – **Zones**, karta **Zones settings**: cztery strefy z nazwą, wejściem (**Input**), partycją (**Area**), typem strefy (**Definition**: Delay, Interior, Instant, Fire), typem obwodu (**Type**), polami **Bypass**, **Force**, **CMS** i **Prot.**, czasem reakcji (**Delay**) i kodem Contact ID (**CID Code**).

- **Zone No** – numer porządkowy strefy na liście.
- **Name** – nazwa strefy.
- **Input** – wejście (IN) przypisane do strefy: wejście CG17 lub modułu rozszerzeń.
- **Area** – partycja, do której należy strefa.
- **Definition** – typ strefy. Dla każdej strefy możesz wybrać jeden:
- **Delay** – strefa opóźniona, do czujnika otwarcia drzwi wejściowych. Dla tego typu strefy można ustawić czas na wejście i wyjście. Po uzbrojeniu naruszenie strefy w czasie na wyjście jest dozwolone; jeśli po upływie tego czasu strefa nadal jest naruszona, włączają się wyjścia OUT typu **Siren** i **Flash**, a CG17 wysyła wiadomość o alarmie. Przy uzbrojonym systemie naruszenie strefy uruchamia odliczanie czasu na wejście, w którym system trzeba rozbroić; jeśli po upływie tego czasu system nadal nie jest rozbrojony, włączają się wyjścia **Siren** i **Flash**, a CG17 wysyła wiadomość o alarmie.
- **Interior** – strefa wewnętrzna (warunkowo opóźniona), do czujki ruchu przy drzwiach wejściowych. Przy uzbrojonym systemie naruszenie strefy włącza wyjścia **Siren** i **Flash**, a CG17 wysyła wiadomość o alarmie. Jeśli przy uzbrojonym systemie jako pierwsza zostanie naruszona strefa **Delay**, w ustawionym czasie na wejście można naruszyć także strefę **Interior**; jeśli nie rozbroisz systemu przed upływem czasu na wejście, włączają się wyjścia **Siren** i **Flash**, a CG17 wysyła wiadomość o alarmie.
- **Instant** – strefa natychmiastowa, do czujek ruchu. Jeśli zostanie naruszona przy uzbrojonym systemie, włączają się wyjścia **Siren** i **Flash**, a CG17 wysyła wiadomość o alarmie.
- **Fire** – strefa pożarowa, do czujek pożarowych. Po jej naruszeniu wyjścia **Siren** i **Flash** włączają się natychmiast, a CG17 wysyła wiadomość o zdarzeniu.
- **Keyswitch** – strefa przełącznika kluczykowego, do manipulatora lub innego przełącznika. Gdy przełącznik naruszy strefę, system się uzbraja lub rozbraja. Przy uzbrajaniu system uzbraja się po upływie ustawionego czasu na wyjście (**Exit time**).
- **24 hours** – strefa 24-godzinna, do czujek zbicia szyby i sabotażu. Po jej naruszeniu wyjścia **Siren** i **Flash** włączają się natychmiast, a CG17 wysyła wiadomość o zdarzeniu.
- **Silent** – strefa cicha: jeśli zostanie naruszona przy uzbrojonym systemie, CG17 natychmiast wysyła komunikat o zdarzeniu, ale wyjścia **Siren** i **Flash** się nie włączają.
- **Silent 24h** – cicha strefa 24-godzinna, do przycisków napadowych: po jej naruszeniu CG17 niezależnie od stanu systemu natychmiast wysyła komunikat o zdarzeniu, ale wyjścia **Siren** i **Flash** się nie włączają.
- **Type** – typ obwodu podłączonego do wejścia (IN) (punkt 3.2): **NC** – normalnie zamknięty; **NO** – normalnie otwarty; **EOL** – z rezystorem końca linii 10 kΩ; **EOL_T** – z rezystorem końca linii i nadzorem sabotażu.
- **Bypass** – po zaznaczeniu strefa jest zablokowana: CG17 ignoruje jej sygnały.
- **Force** – po zaznaczeniu system można uzbroić także przy otwartej strefie. Przy uzbrojonym systemie naruszenie strefy w trybie **Force** wywołuje alarm.
- **CMS** – po zaznaczeniu zdarzenia strefy trafiają do stacji monitorowania (CMS).
- **Prot.** – po zaznaczeniu zdarzenia strefy trafiają do chmury Protegus.

- **Delay** – czas reakcji wejścia (IN) w milisekundach (ms).
- **CID code** – kod Contact ID zdarzeń. Program ustawia go automatycznie przy wyborze typu strefy (**Definition**).

5.6.2 Karta SMS & Call reporting

Ta karta jest widoczna tylko wtedy, gdy na stronie **Users & Reporting** podałeś numer telefonu co najmniej jednego użytkownika (punkt 5.4).



Rysunek 61. TrikdisConfig – **Zones**, karta **SMS & Call reporting**: treść SMS-a dla zdarzeń stref (**Event**) i przywróceń (**Restore**), dla każdego użytkownika (**User 2**) z polami **SMS** i **Call**.

- **Zn** – numer strefy ze słowem identyfikującym zdarzenie: **Event** (zdarzenie) lub **Restore** (przywrócenie).
- **SMS text** – opis zdarzenia strefy w SMS-ach wysyłanych do użytkowników.
- **SMS/Call** – zaznacz, w jaki sposób użytkownicy mają być powiadamiani o zdarzeniach: SMS-em i/lub połączeniem.

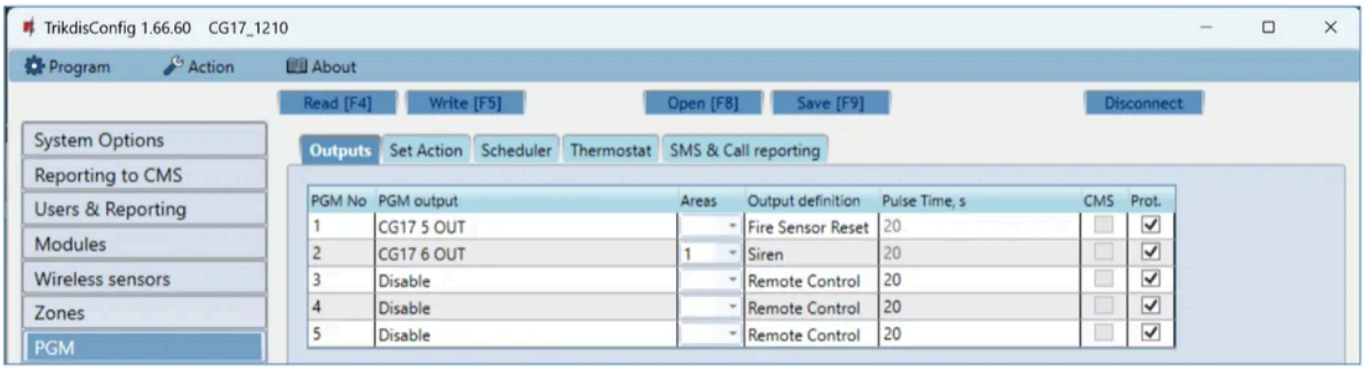
Modem wykonuje połączenie przez 2G lub VoLTE. Tam, gdzie operator wyłączył 2G i nie zatwierdził modemu dla VoLTE, SMS dociera, ale telefon nie dzwoni. To nie jest błąd konfiguracji. W takim miejscu korzystaj z SMS i aplikacji Protegus 2.

5.7 Strona „PGM”

Na stronie **PGM** ustawiasz działanie wyjść OUT, ich sterowanie powiązane ze zdarzeniami, harmonogram, termostaty oraz powiadamianie SMS-em i połączeniem o wyjściach.

5.7.1 Karta Outputs – wyjścia

Tu przypisujesz wyjścia OUT CG17 lub urządzeń zewnętrznych do PGM i ustawiasz ich działanie.



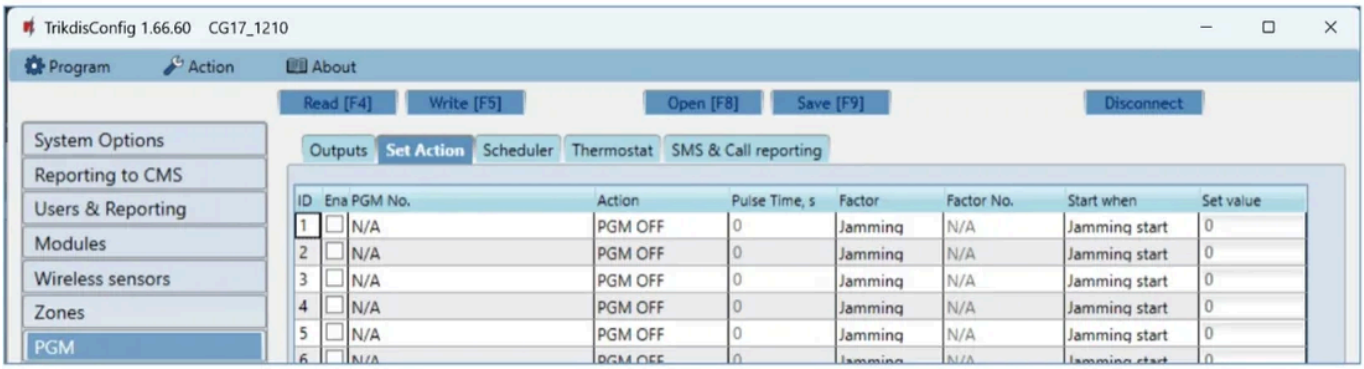
Rysunek 62. TrikdisConfig – **PGM**, karta **Outputs**: PGM z przypisanym wyjściem, partycją (**Areas**), działaniem (**Output definition**, np. **Fire Sensor Reset**, **Siren**, **Remote Control**), czasem impulsu (**Pulse Time**) i polami **CMS**, **Prot.**.

- **PGM No** – numer porządkowy PGM na liście.

- **PGM output** – wyjście OUT przypisane do PGM: wyjście CG17 lub urządzenia zewnętrznego.
- **Areas** – partycja, do której przypisujesz wyjście.
- **Output definition** – tryb działania wyjścia OUT:
- **Siren** – do podłączenia sygnalizatora (punkt 3.8);
- **Remote Control** – do sterowania urządzeniami zewnętrznymi;
- **Fire Sensor Reset** – do resetu czujki pożarowej po alarmie (punkt 3.3);
- **System state** – do wskaźnika stanu systemu alarmowego; np. dioda LED może pokazywać, czy system jest uzbrojony, czy rozbrojony (punkt 3.5);
- **Flash** – przy uzbrojonym systemie daje sygnał ciągły, przy alarmie sygnał impulsowy; po rozbrojeniu systemu sygnał znika;
- **Thermostat** – CG17 steruje wyjściem OUT według temperatury ustawionego czujnika temperatury (punkt 5.7.4).
- **Pulse time, s** – czas włączenia wyjścia OUT, 0–9999 s.
- **CMS** – po zaznaczeniu wiadomości o włączeniu i wyłączeniu wyjścia PGM trafiają do stacji monitorowania (CMS).
- **Prot.** – po zaznaczeniu wiadomości o włączeniu i wyłączeniu wyjścia PGM trafiają do chmury Protegus.

5.7.2 Karta Set Action – sterowanie zdarzeniem

Tu podajesz, jakie zdarzenie automatycznie przełącza wyjścia OUT.



Rysunek 63. TrikdisConfig – **PGM**, karta **Set Action**: wiersze reguł z polem włączenia, sterowanym PGM (**PGM No.**), akcją (**Action**, np. **PGM OFF**), czasem impulsu, zdarzeniem wyzwalającym (**Factor**, np. **Jamming** – zagłuszanie sygnału komórkowego) oraz kolumnami **Factor No.**, **Start when** (np. **Jamming start**) i **Set value**.

- **ID** – numer porządkowy wyjścia na liście.
- **Enable** – włącza PGM.
- **PGM No.** – sterowane wyjście OUT: to wyjście CG17 przełącza, gdy wystąpi zdarzenie podane w kolumnach **Factor**, **Factor No.**, **Start when** i **Set value**.
- **Action** – akcja:
- **PGM OFF** – wyjście OUT przechodzi w stan wyłączony („Off”);
- **PGM ON** – wyjście OUT przechodzi w stan włączony („On”);
- **Pulse OFF** – stanem podstawowym wyjścia jest włączenie („On”); na polecenie wyłącza się („Off”) na czas impulsu (**Pulse time**), a potem automatycznie wraca do włączonego stanu podstawowego;
- **Pulse ON** – stanem podstawowym wyjścia jest wyłączenie („Off”); na polecenie włącza się („On”) na czas impulsu (**Pulse time**), a potem automatycznie wraca do wyłączonego stanu podstawowego.
- **Pulse time, s** – czas impulsu, 0–9999 s.
- **Factor**/**Factor No.** – zdarzenie, które przełącza wyjście OUT: **Zone** (strefa), **Sensor** (czujnik), **Schedule** (harmonogram), **Jamming** (zagłuszanie sygnału komórkowego), **Sensor lost** (utrata czujnika), **iButton** (klucz dotykowy), **Arm** (uzbrojenie), **Disarm** (rozbrojenie), **SMS received** (odebrany SMS).

- Do wyjścia możesz przypisać także harmonogram, aby przełączało się o podanych godzinach. Na karcie **Scheduler** możesz przygotować 10 harmonogramów (punkt 5.7.3).
- **Start when** – dodatkowy warunek zależny od zdarzenia **Factor**: kiedy wyjście OUT ma się włączyć.
- **Set value** – zależnie od warunku wybranego w kolumnie **Factor** (**SMS received**, **Sensor**) podajesz tu wartość, którą można sterować wyjściem PGM: treść odebranego SMS-a albo wartość napięcia lub temperatury (pomiar napięcia: punkt 3.13; czujnik temperatury: punkt 3.4).

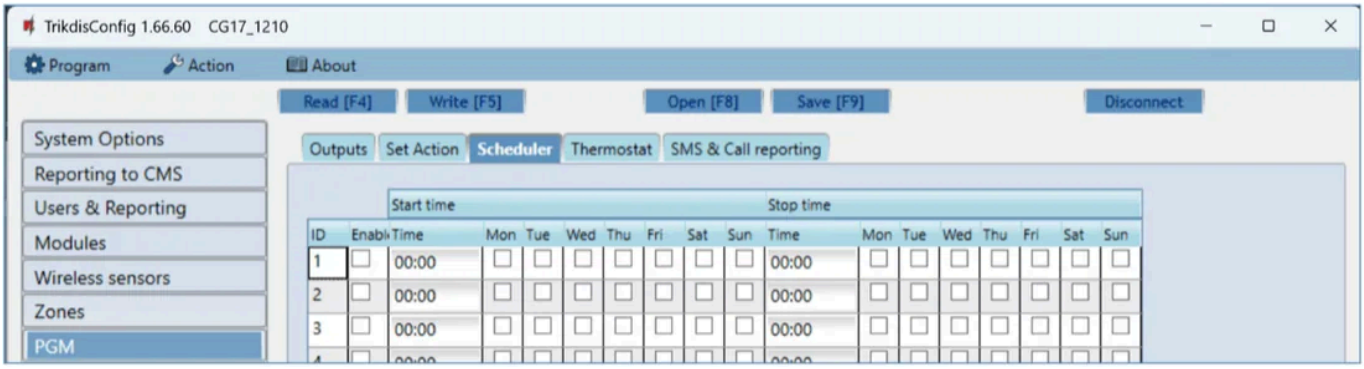
W treści SMS-a sterujące słowo kluczowe jest oddzielone od reszty SMS-a znakami `%`:

- `%.....%` – część treści odebranego SMS-a musi być zgodna z tekstem wpisanym między znakami `%`. Przykład: `%sMS%` – SMS musi zawierać tekst „sMS"; taki SMS: `1155sMS332`.
- `.....%` – początek treści odebranego SMS-a musi być zgodny z tekstem wpisanym przed znakiem `%`. Przykład: `sMS%` – SMS musi zaczynać się od „sMS"; taki SMS: `sMS332`.
- `%.....` – koniec treści odebranego SMS-a musi być zgodny z tekstem wpisanym po znaku `%`. Przykład: `%sMS` – SMS musi kończyć się na „sMS"; taki SMS: `1155sMS`.

W treści SMS-a małe i wielkie litery są rozróżniane.

5.7.3 Karta Scheduler – harmonogram

Tu przygotowujesz harmonogramy (maksymalnie 10), które na karcie **Set Action** możesz przypisać do wyjść.

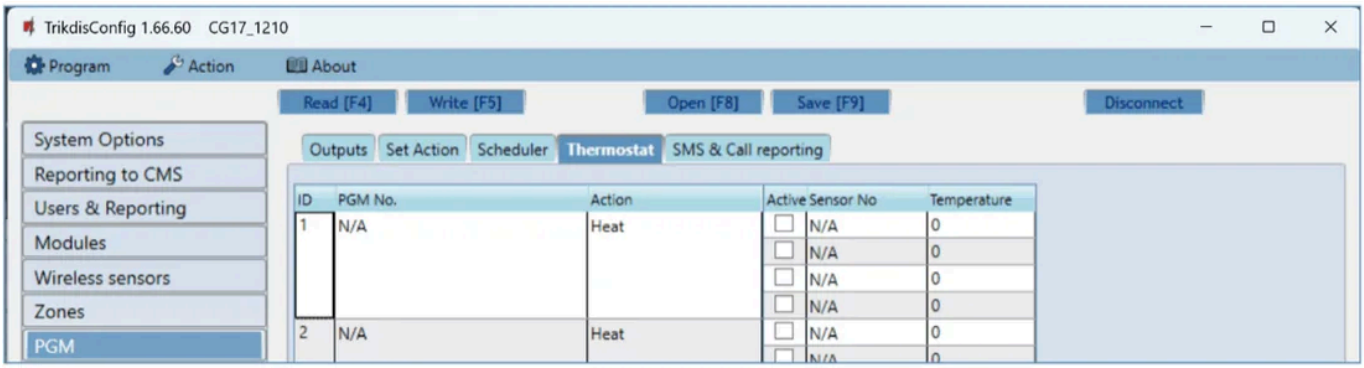


Rysunek 64. TrikdisConfig – **PGM**, karta **Scheduler**: wiersze harmonogramów z polem **Enable**, godziną rozpoczęcia (**Start time**) i zakończenia (**Stop time**) oraz dniami tygodnia (**Mon**–**Sun**).

- **ID** – numer porządkowy harmonogramu na liście.
- **Enable** – włącza harmonogram.
- **Start time** – godzina, o której wyjście OUT się włącza (początek harmonogramu).
- **Stop time** – godzina, o której wyjście OUT się wyłącza (koniec harmonogramu).
- **Mon**–**Sun** – zaznacz dni tygodnia, w które wyjście OUT ma się włączać i wyłączać.

5.7.4 Karta Thermostat – termostat

Tu przypisujesz do wyjść OUT termostaty działające na podstawie czujników temperatury (punkt 3.4).

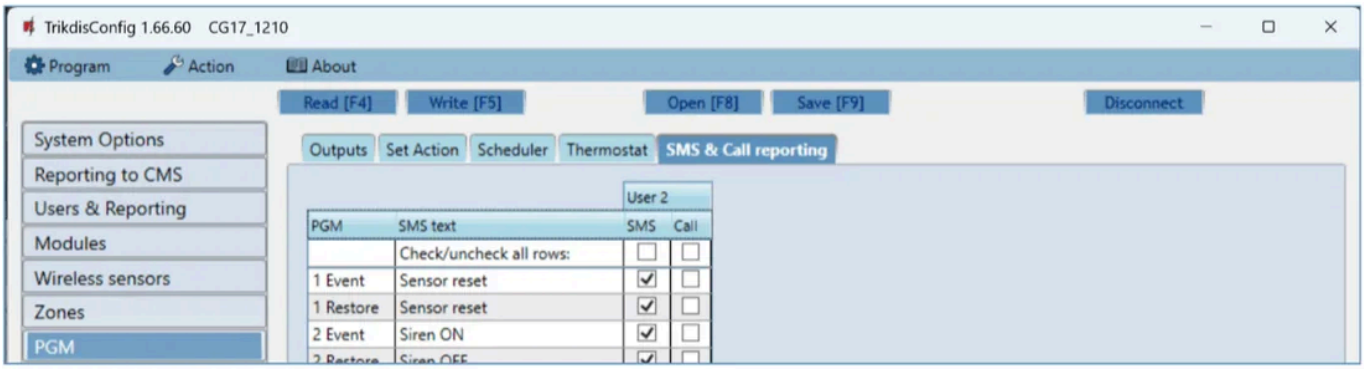


Rysunek 65. TrikdisConfig – **PGM**, karta **Thermostat**: wiersze termostatów ze sterowanym PGM (**PGM No.**), trybem działania (**Action**, np. **Heat**), polem **Active**, numerem czujnika (**Sensor No**) i temperaturą (**Temperature**).

- **ID** – numer porządkowy termostatu na liście.
- **PGM No.** – numer wyjścia PGM, którym steruje termostat.
- **Action** – tryb działania termostatu: ogrzewanie (**heat**) lub chłodzenie (**cool**).
- **Active** – po zaznaczeniu termostat działa z wybranym czujnikiem temperatury, według ustawionej temperatury.
- **Sensor No** – czujnik temperatury przypisany do termostatu.
- **Temperature** – temperatura, którą utrzymuje termostat.

5.7.5 Karta SMS & Call reporting

Ta karta jest widoczna tylko wtedy, gdy na stronie **Users & Reporting** podałeś numer telefonu co najmniej jednego użytkownika (punkt 5.4).

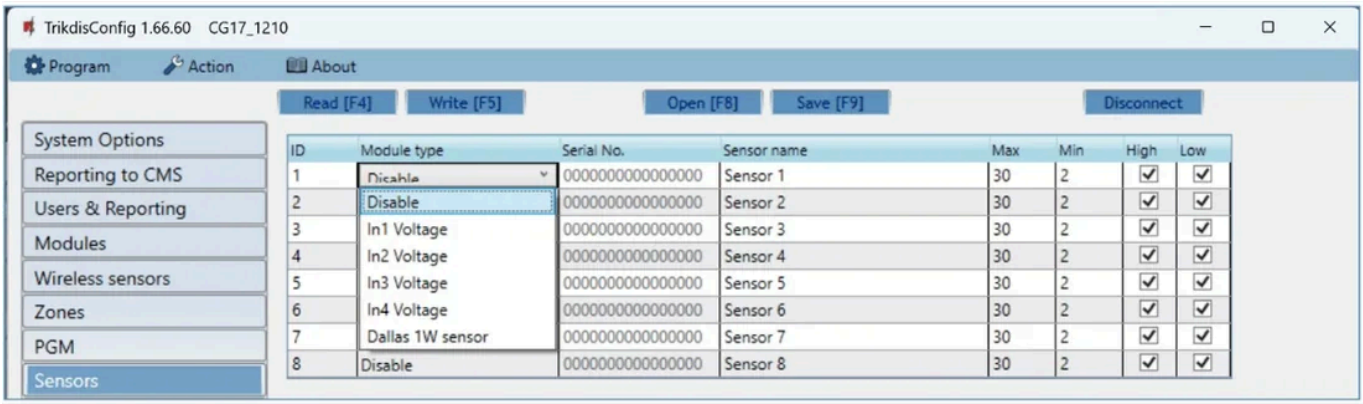


Rysunek 66. TrikdisConfig – **PGM**, karta **SMS & Call reporting**: treść SMS-a dla zdarzeń włączenia (**Event**) i wyłączenia (**Restore**) wyjść, dla każdego użytkownika (**User 2**) z polami **SMS** i **Call**.

- **PGM** – numer wyjścia OUT i typ zdarzenia: **Event** – włączenie wyjścia OUT, **Restore** – wyłączenie wyjścia OUT.
- **SMS text** – nazwa zdarzenia włączenia lub wyłączenia wyjścia OUT w SMS-ach o zdarzeniach.
- **User / SMS and Call** – wybierz, którzy użytkownicy mają otrzymywać SMS i/lub połączenie przy włączeniu lub wyłączeniu wyjścia OUT.

5.8 Strona „Sensors”

Tu dodajesz czujniki temperatury (podłączenie: punkt 3.4). Na liście **Module type** można wybrać także pomiar napięcia wejść (**In1 Voltage**–**In4 Voltage**, punkt 3.13); konfiguracja czujnika poziomu paliwa Strela RS485 jest w punkcie 5.5.3.



Rysunek 67. TrikdisConfig – **Sensors**: osiem miejsc na czujniki; na otwartej liście **Module type Disable** (brak), **In1 Voltage**–**In4 Voltage** (napięcie wejścia) i **Dallas 1W sensor** (czujnik temperatury 1-Wire); obok kolumny **Serial No.**, **Sensor name**, **Max**, **Min**, **High** i **Low**.

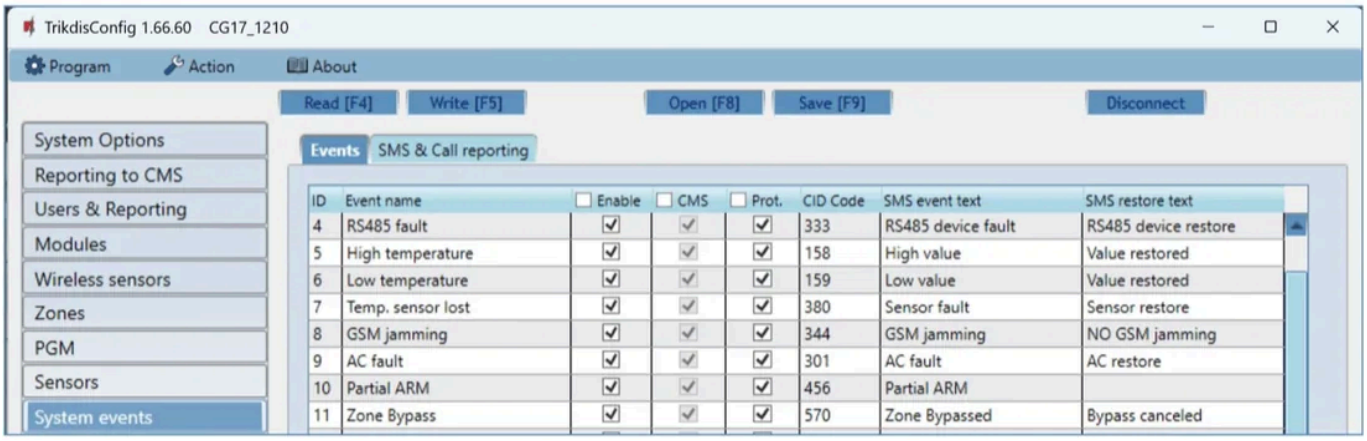
- **ID** – numer porządkowy czujnika na liście.
- **Module type** – wybrany czujnik temperatury trafia do tego numeru porządkowego (**ID**).
- **Serial No.** – numer seryjny czujnika temperatury; odczytuje go centrala.
- **Sensor name** – nadaj czujnikowi temperatury nazwę.
- **Max** – jeśli temperatura jest wyższa, CG17 tworzy komunikat o zdarzeniu. W tym celu zaznacz pole **High**.
- **Min** – jeśli temperatura jest niższa, CG17 tworzy komunikat o zdarzeniu. W tym celu zaznacz pole **Low**.

5.9 Strona „System events”

Na stronie **System events** ustawiasz własne zdarzenia systemowe CG17 (np. błąd RS485, wysoka i niska temperatura, zagłuszanie sygnału komórkowego, awaria zasilania) i powiadomienia o nich.

5.9.1 Karta Events – zdarzenia systemowe

Tu podajesz, które zdarzenia systemowe mają trafiać do stacji monitorowania i do chmury Protegus, z jakim kodem Contact ID i jaką treścią SMS.



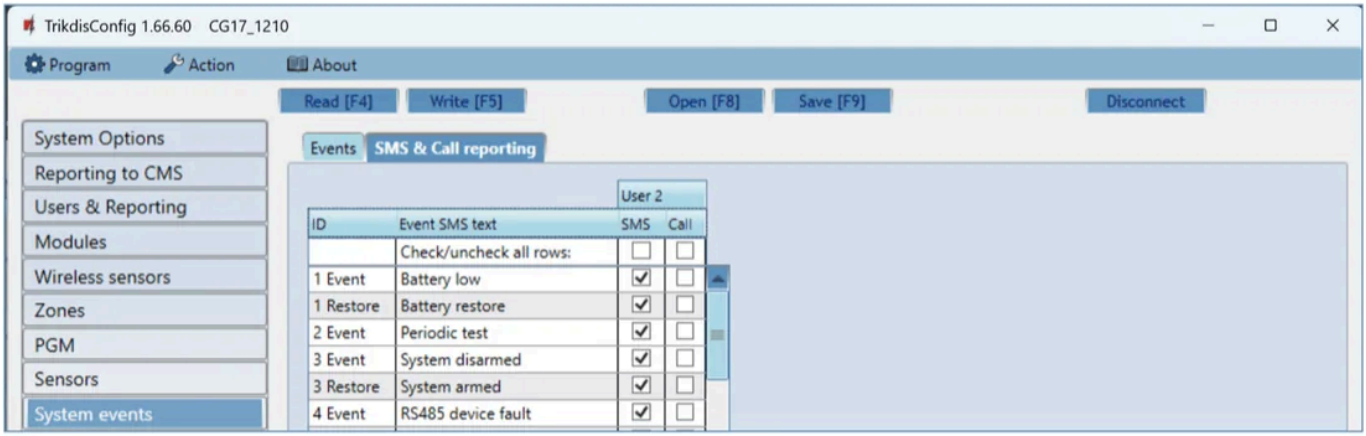
Rysunek 68. TrikdisConfig – **System events**, karta **Events**: zdarzenia systemowe (np. **RS485 fault**, wysoka i niska temperatura, zagłuszanie sygnału komórkowego, awaria zasilania) z polami **Enable**, **CMS** i **Prot.**, kodem Contact ID i treściami SMS.

- **ID** – numer porządkowy zdarzenia na liście.
- **Event name** – nazwa zdarzenia.
- **Enable** – włącza monitorowanie zdarzenia.
- **CMS/Prot.** – wiadomości o wybranym zdarzeniu trafiają do stacji monitorowania i/lub do chmury Protegus.

- **CID code** – kod Contact ID zdarzenia.
- **SMS event text** – treść SMS-a o zdarzeniu.
- **SMS restore text** – treść SMS-a o przywróceniu.

5.9.2 Karta SMS & Call reporting

Ta karta jest widoczna tylko wtedy, gdy na stronie **Users & Reporting** podałeś numer telefonu co najmniej jednego użytkownika (punkt 5.4).

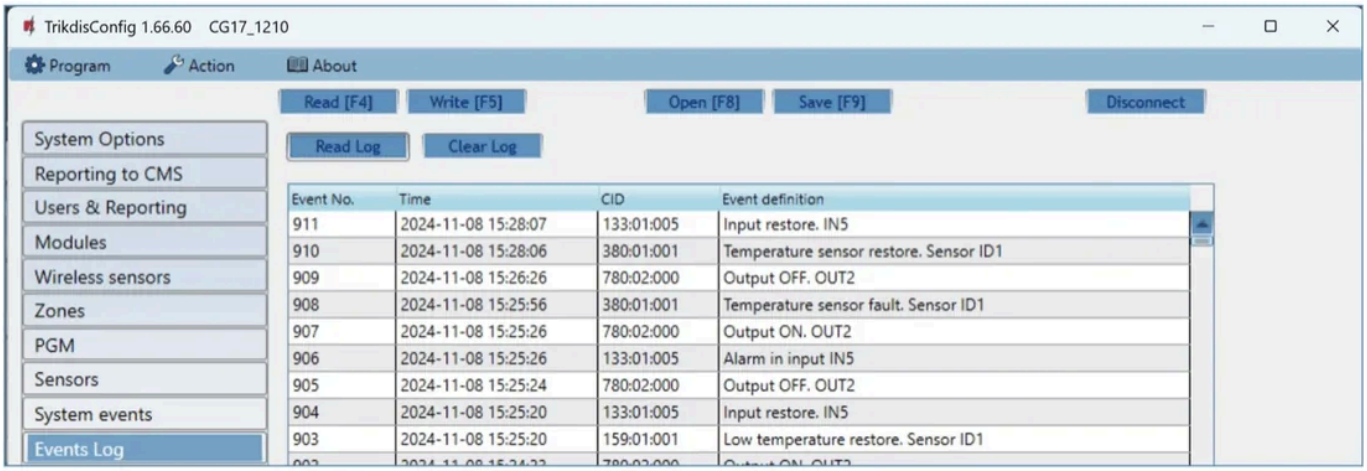


Rysunek 69. TrikdisConfig – **System events**, karta **SMS & Call reporting**: treść SMS-a zdarzeń systemowych (np. **Battery low**, **Periodic test**, **System disarmed**, **System armed**, **RS485 device fault**), dla każdego użytkownika (**User 2**) z polami **SMS** i **Call**.

- **ID** – numer zdarzenia i słowo identyfikujące: **Event** (zdarzenie) lub **Restore** (przywrócenie).
- **Event SMS text** – treść SMS-ów o zdarzeniach.
- **User / SMS and Call** – podaj, w jaki sposób użytkownicy mają być powiadamiani o poszczególnych zdarzeniach: SMS-em i/lub połączeniem.

5.10 Strona „Events Log"

Własny dziennik zdarzeń CG17: tu możesz odczytać i usunąć zdarzenia zapisane w jego pamięci.



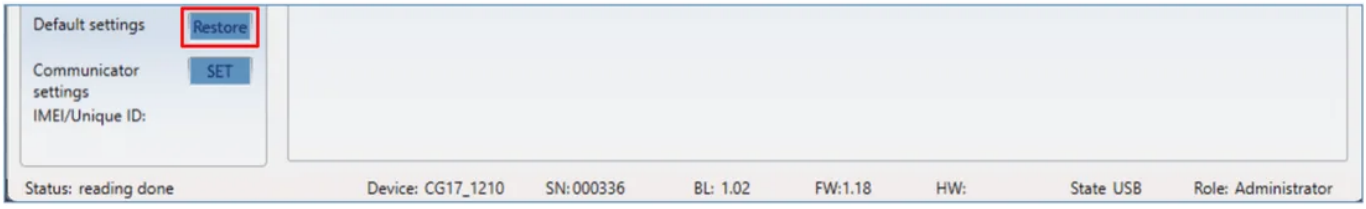
Rysunek 70. TrikdisConfig – **Events Log**: przyciski **Read Log** i **Clear Log**, pod nimi zdarzenia z numerem porządkowym (**Event No.**), czasem (**Time**), kodem Contact ID (**CID**) i opisem (**Event definition**).

- Przycisk **Read Log** – odczytuje wpisy dziennika zdarzeń z pamięci urządzenia.
- Przycisk **Clear Log** – usuwa wpisy dziennika zdarzeń z pamięci urządzenia.

- W tabeli widać numer porządkowy zdarzenia (**Event No.**), jego czas (**Time**), kod Contact ID (**CID**) i opis (**Event definition**). Na stronie **Events Log** można wyświetlić maksymalnie 1000 zdarzeń zapisanych w pamięci CG17.

5.11 Przywracanie ustawień fabrycznych

Aby przywrócić ustawienia fabryczne centrali, kliknij przycisk **Restore** w grupie **Default settings**, w lewej dolnej części okna programowania TrikdisConfig. Wcześniej warto zapisać bieżące ustawienia do pliku (**Save [F9]**, punkt 5.1).



Rysunek 71. TrikdisConfig – przycisk **Restore** grupy **Default settings** (zaznaczony na czerwono) w lewej dolnej części okna programowania, nad paskiem stanu.

6. Programowanie zdalne

Ustawienia CG17 możesz odczytywać i zmieniać zdalnie przez chmurę Protegus (punkt 6.1), a z TrikdisConfig możesz też zdalnie sterować centralą (punkt 6.2) – w żadnym z tych przypadków nie musisz jechać na miejsce instalacji.

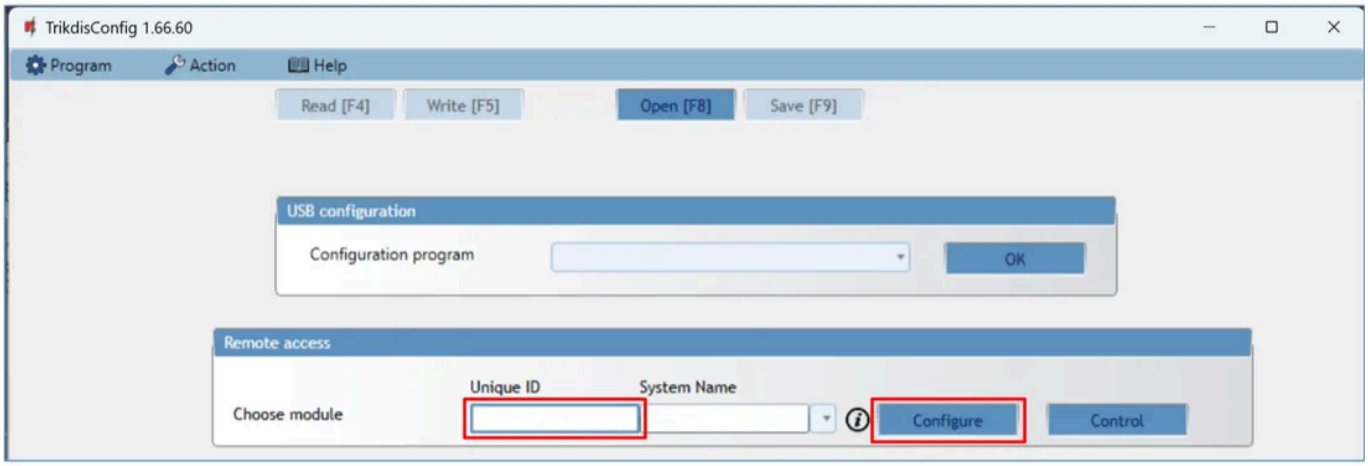
6.1 Zdalna konfiguracja parametrów

Warunki programowania zdalnego

Programowanie zdalne działa tylko wtedy, gdy:

1. usługa chmury Protegus (**Protegus cloud**) jest włączona: w oknie **Users & Reporting** TrikdisConfig, w grupie ustawień **Cloud application**, zaznaczone jest pole **Enable cloud service** (punkt 5.4; SMS-em: `CONNECT 123456 PROTEGUS=ON`, punkt 4.2);
2. w urządzeniu jest aktywowana karta SIM, a jej kod PIN jest podany lub żądanie PIN jest wyłączone;
3. jest zasilanie: dioda **POWER** świeci na zielono;
4. urządzenie jest połączone z siecią: dioda **NETWORK** świeci na zielono i miga na żółto.

1. Pobierz program TrikdisConfig ze strony www.trikdis.com.
2. Upewnij się, że centrala jest połączona z internetem, a połączenie z Protegus jest włączone.
3. Uruchom TrikdisConfig i w polu **Unique ID** grupy **Remote access** (dostęp zdalny) wpisz numer **IMEI** CG17 (znajdziesz go na naklejce z tyłu urządzenia i na pudełku).
4. W polu **System Name** (nazwa systemu) nadaj nazwę centrali CG17 identyfikowanej tym numerem IMEI i kliknij przycisk **Configure**.

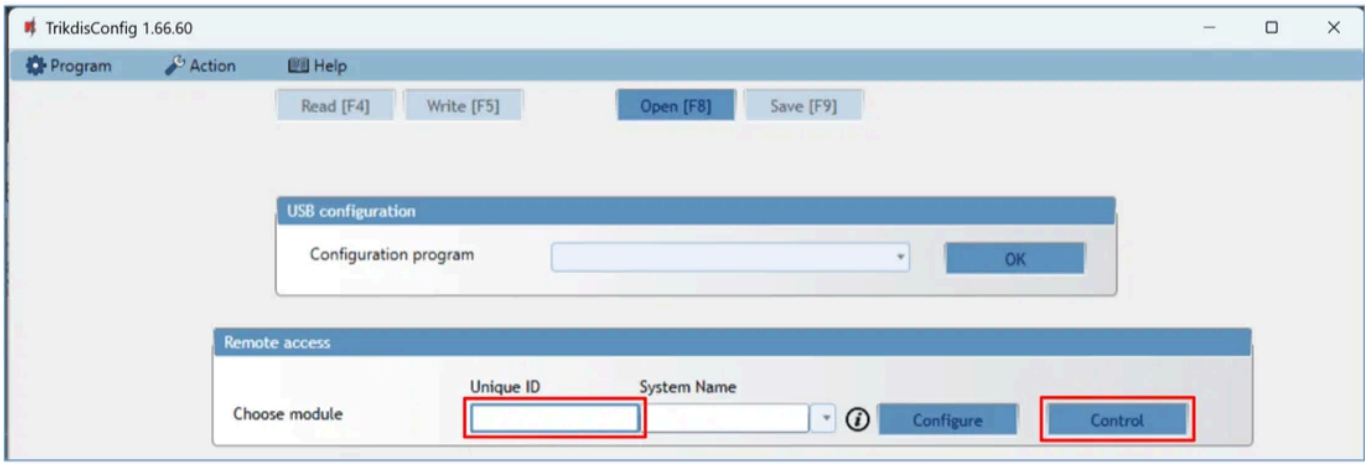


Rysunek 72. TrikdisConfig – grupa **Remote access** (dostęp zdalny) okna startowego: w zaznaczone w ramce pole **Unique ID** wpisuje się numer IMEI, obok pole **System Name** (nazwa systemu); zaznaczony w ramce przycisk **Configure** otwiera programowanie zdalne.

5. Kliknij przycisk **Read [F4]**: program odczyta aktualne ustawienia CG17. Jeśli pojawi się okno z prośbą o **Administrator code** (kod administratora), podaj 6-znakowy kod administratora. Jeśli chcesz, aby program zapamiętał kod, zaznacz pole **Remember password** i kliknij przycisk **Write [F5]**.
6. Wprowadź potrzebne zmiany w ustawieniach CG17 i kliknij przycisk **Write [F5]**. Jeśli chcesz zakończyć połączenie z CG17, kliknij przycisk **Disconnect** i zamknij TrikdisConfig.

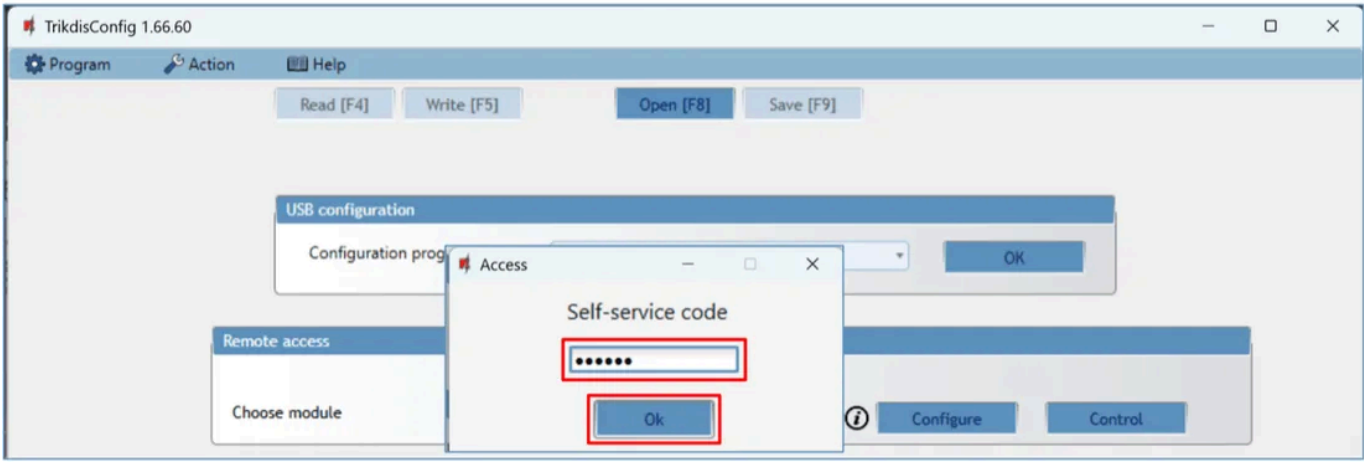
6.2 Zdalne sterowanie z TrikdisConfig

1. Pobierz program TrikdisConfig ze strony www.trikdis.com (w polu wyszukiwania wpisz: „TrikdisConfig") i zainstaluj go.
2. Upewnij się, że centrala alarmowa jest połączona z internetem. Usługa chmury Protegus (**Protegus cloud**) musi być włączona (punkt 6.1).
3. Uruchom TrikdisConfig i w polu **Unique ID** grupy **Remote access** wpisz numer **IMEI** CG17 (znajdziesz go na naklejce z tyłu urządzenia i na pudełku).



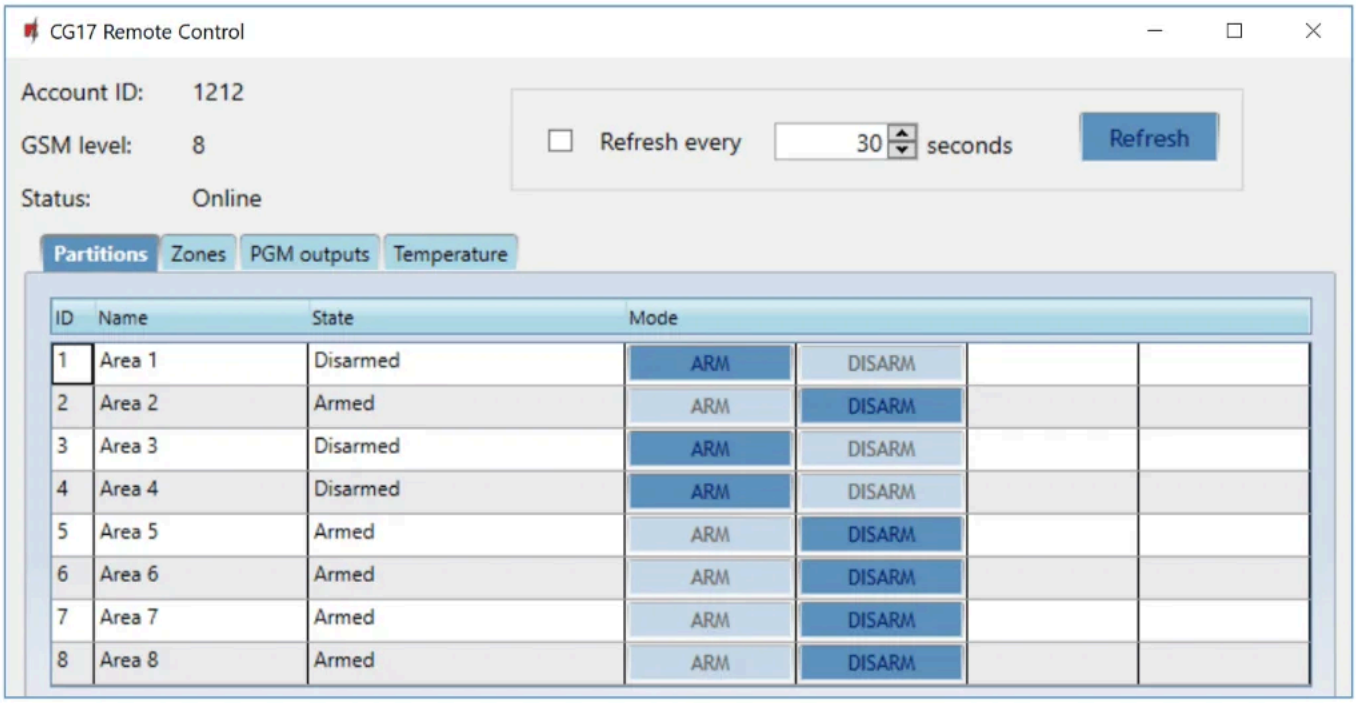
Rysunek 73. TrikdisConfig – grupa **Remote access**: zaznaczone w ramce pole **Unique ID** i zaznaczony w ramce przycisk **Control** (sterowanie).

4. Kliknij przycisk **Control**.
5. Podaj kod **Self-service code** (fabrycznie `123456`) i naciśnij przycisk **OK**.



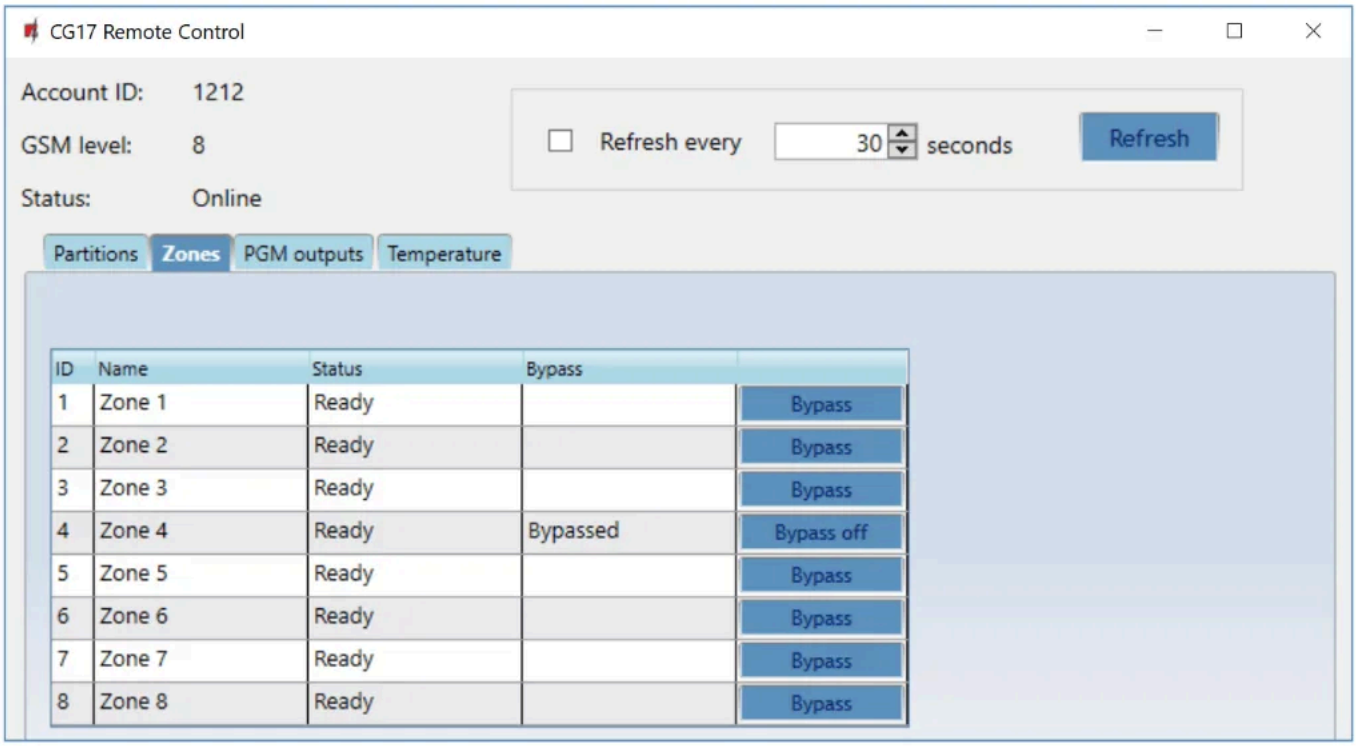
Rysunek 74. Okno **Access** (dostęp): w pole **Self-service code** wpisz kod, a następnie naciśnij przycisk **Ok**.

6. Otworzy się okno **Remote control** (sterowanie zdalne): tu możesz sterować partycjami centrali alarmowej, obserwować stan stref, przełączać wyjścia PGM i monitorować temperaturę.
7. Karta **Partitions** (partycje): naciśnij przycisk **DISARM** (lub **ARM**) i podaj kod użytkownika – partycja centrali alarmowej zostanie rozbrojona (lub uzbrojona).



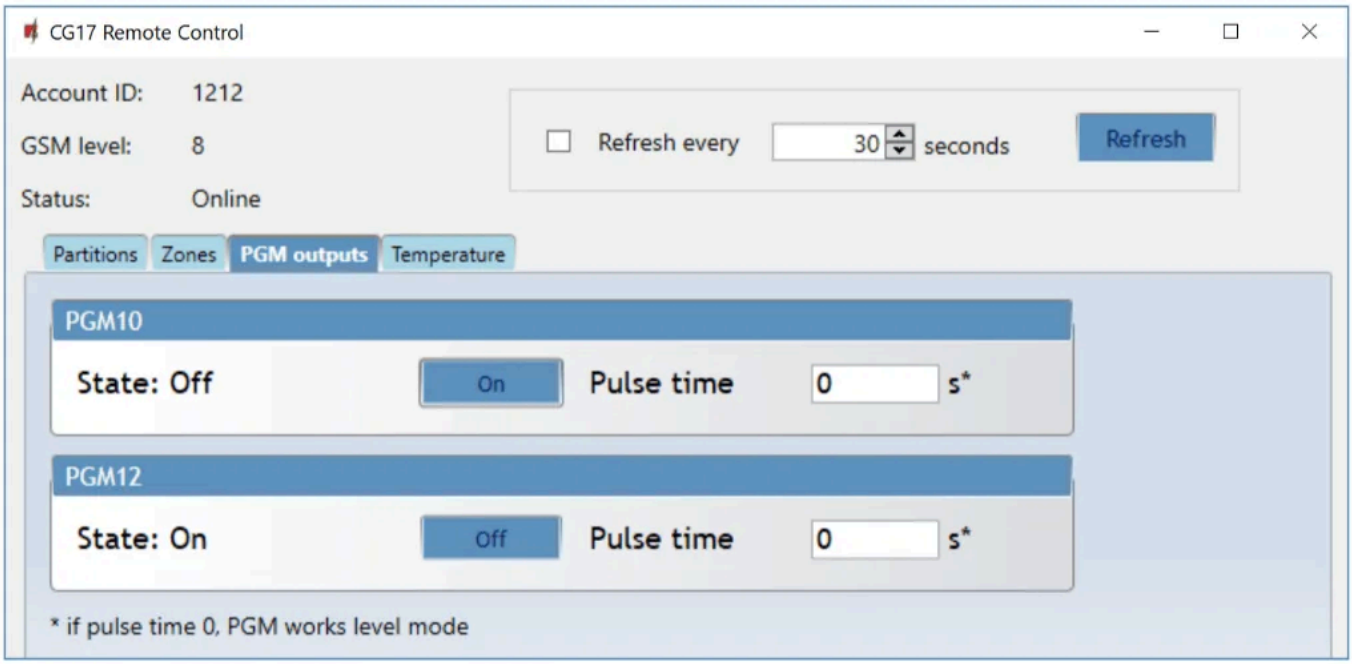
Rysunek 75. Karta **Partitions** (partycje) okna **CG17 Remote Control**: dla każdej partycji nazwa (**Name**), stan (**State**: **Armed** – uzbrojona, **Disarmed** – rozbrojona) i przycisk **ARM** / **DISARM**. U góry **Account ID** (numer obiektu), **GSM level** (poziom sygnału) i **Status** (stan); przyciskiem **Refresh** odświeżasz dane, a polem **Refresh every ... seconds** – automatycznie, w podanych odstępach czasu.

8. Karta **Zones** (strefy): to okno pokazuje stan stref; strefy możesz też blokować (**Bypass**).



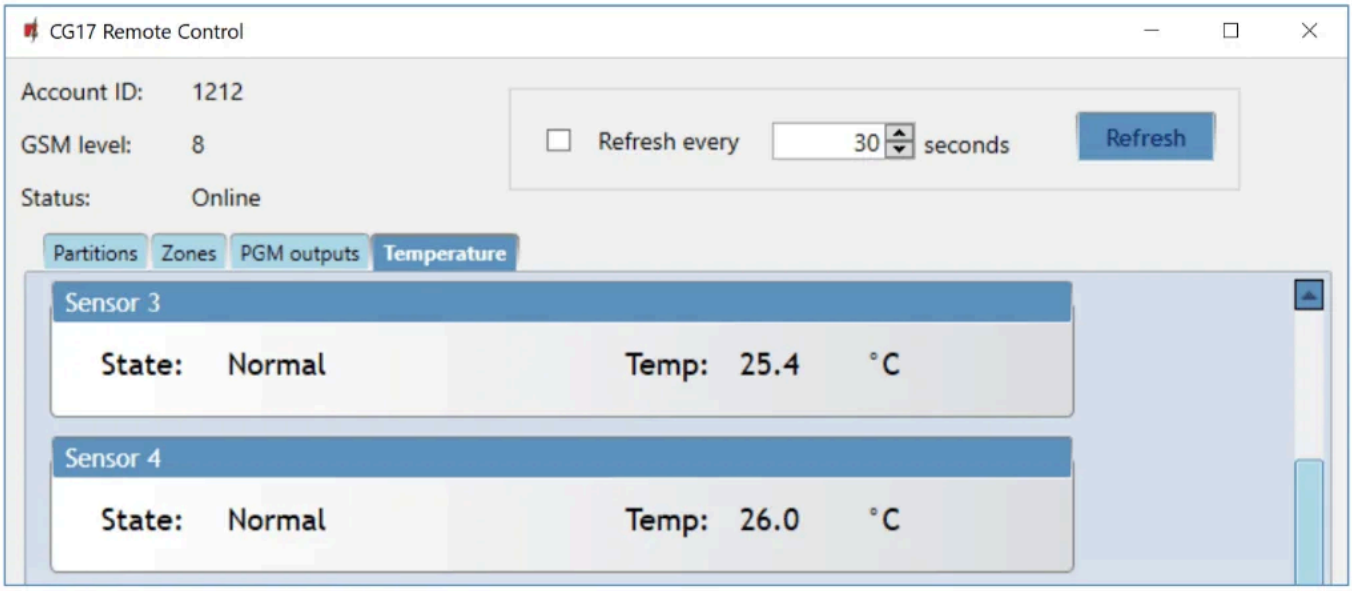
Rysunek 76. Karta **Zones** (strefy): dla każdej strefy stan (**Status**, **Ready** – gotowa) i przycisk **Bypass** (blokowanie); przy zablokowanej strefie (**Bypassed**) przycisk **Bypass off** usuwa blokadę.

9. Karta **PGM outputs** (wyjścia PGM): tu możesz przełączać wyjścia PGM typu **Remote Control**.



Rysunek 77. Karta **PGM outputs** (wyjścia PGM): dla każdego wyjścia stan (**State: Off** – wyłączone, **State: On** – włączone), przycisk przełączania **On** / **Off** i pole **Pulse time** (czas impulsu, s). Na dole okna: jeśli czas impulsu wynosi 0, PGM pracuje w trybie sterowania poziomem (level).

10. Karta **Temperature** (temperatura): tu możesz obserwować zmierzone wartości czujników temperatury.



Rysunek 78. Karta **Temperature** (temperatura): dla każdego czujnika (**Sensor**) stan (**State: Normal** – w porządku) i zmierzona temperatura (**Temp**, °C).

7. Sprawdzenie instalacji

Po zakończeniu konfiguracji i instalacji przetestuj cały system:

1. Sprawdź, czy jest napięcie zasilania (dioda **POWER** miga na zielono).
2. Sprawdź połączenie z siecią komórkową po diodzie **NETWORK**. Poziom sygnału 5 jest wystarczający (przez 4 sekundy ciągłe zielone światło, a potem pięć żółtych mignięć), w sieci 3G także poziom 3 (przez 4 sekundy ciągłe zielone światło, a potem trzy żółte mignięcia). Jeśli czerwona dioda **TROUBLE** mignie 5 razy, poszukaj dla CG17 innego miejsca.
3. Aby sprawdzić wejścia, aktywuj je i zobacz, czy odbiorcy otrzymują prawidłowe wiadomości.
4. Aby sprawdzić wyjścia, włącz je zdalnie i zobacz, czy odbiorcy otrzymują prawidłowe wiadomości i czy wyjścia przełączają się prawidłowo.
5. Wypróbuj alarm: sprawdź, czy stacja monitorowania prawidłowo odbiera zdarzenia.

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.

Dane centrali (typ, numer IMEI, numer seryjny, wersję oprogramowania układowego), stan wejść i wyjść oraz wartości czujników temperatury możesz sprawdzić także SMS-em: `INFO 123456`, `ASKI 123456`, `ASKO 123456`, `ASKT 123456`. Polecenie wyślij z telefonu znajdującego się na liście użytkowników, a w miejsce fabrycznego hasła `123456` wpisz swoje hasło administratora (punkt 4.2).

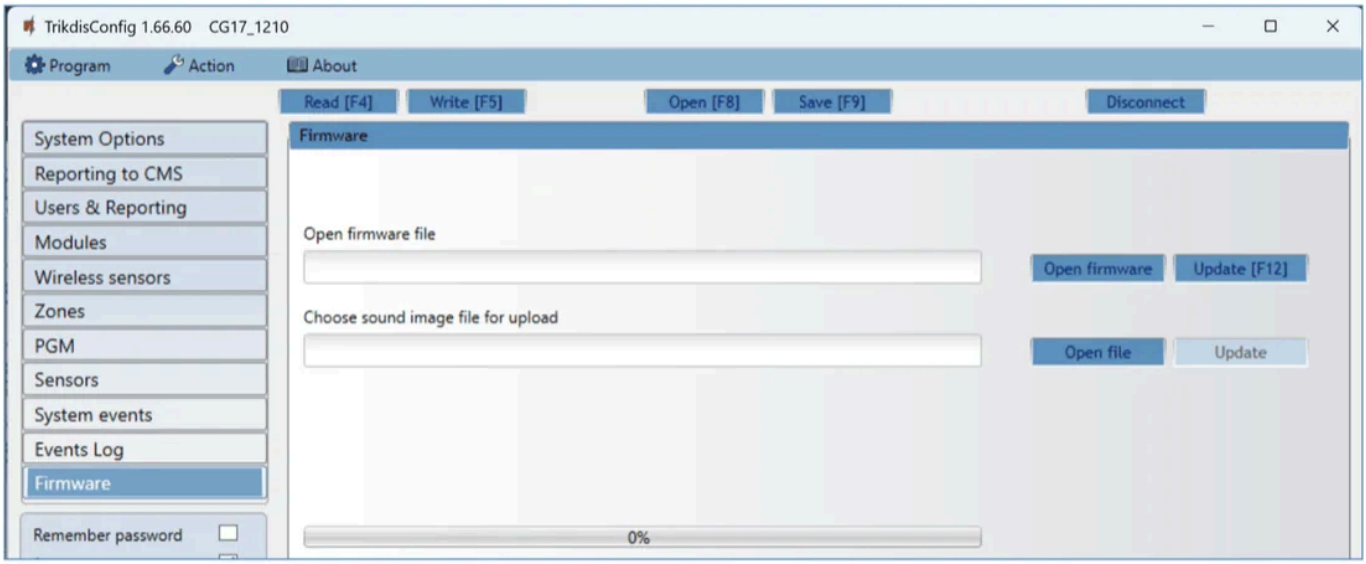
8. Aktualizacja oprogramowania układowego

Jeśli CG17 jest połączony z TrikdisConfig i dostępne jest nowsze oprogramowanie układowe, program sam zaproponuje aktualizację – komputer musi mieć wtedy dostęp do internetu. Jeśli na komputerze działa program antywirusowy, może on blokować automatyczną aktualizację; wtedy trzeba zmienić ustawienia programu antywirusowego.

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 79. TrikdisConfig – CG17, strona **Firmware**: pole **Open firmware file**, przyciski **Open firmware** i **Update [F12]**, na dole wskaźnik postępu. Środkowy wiersz **Choose sound image file for upload** (wgrywanie pliku dźwiękowego, przyciski **Open file** i **Update**) nie jest potrzebny do aktualizacji oprogramowania układowego.

CG17 podłącz kablem **USB Mini-B** (złącze jest pod pokrywą, rozdział 2); połączenie zdalne opisuje punkt 6.1.

9. 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.

- Elektroniczny system sygnalizacji włamania (system alarmowy) może instalować i serwisować tylko wykwalifikowana osoba.
- Przed instalacją uważnie przeczytaj tę instrukcję, aby uniknąć błędów prowadzących do nieprawidłowego działania, a nawet uszkodzenia urządzenia.
- **Przed każdym podłączeniem elektrycznym odłącz napięcie zasilania** – także akumulator zapasowy.
- Zmiany, modyfikacje lub naprawy nieautoryzowane przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów dotyczących odpadów: nie wyrzucaj urządzenia ani jego części razem z odpadami domowymi – wycofane z użytku urządzenie oddaj jako odpad elektroniczny.

Zobacz też

- Ekspander wejść i wyjść iO8 – instrukcja instalacji – ekspander iO8 do CG17.
- Moduł Wi-Fi W485 i moduł Ethernet E485 – instrukcja instalacji i konfiguracji – połączenie Wi-Fi i Ethernet do CG17.
- Ustawienie APN – lista europejskich operatorów komórkowych – jeśli mobilne połączenie danych się nie zestawia.
- Protegus – aplikacja na Androida / iPhone'a i aplikacja internetowa – o aplikacji.
- Dokumentacja w języku angielskim: docs.trikdis.com – Cellular security control panel CG17.

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

Powiązane produkty

Trikdis CG17 4G GSM Compact Security Panel **Trikdis IO8 PRZEWIDY MODUŁ EXPADER**
Moduł Expander Trikdis IO8-LORA **Moduł Expander Trikdis RF-LORA**
Moduł Expander Trikdis Io-Lora **Trikdis W485 Moduł WiFi (RS485)**
Moduł Ethernet Trikdis E485 (RS485) **DS18B20 Czujnik temperatury z drutem 1m**
Akumulator żelowy 12 V 7 Ah do centrali alarmowej
Trikdis Ant04 GSM Stick-on Antena z drutem 2,5 m
Antena magnetyczna Trikdis ME301M z drutem 2,5 m

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-cg17