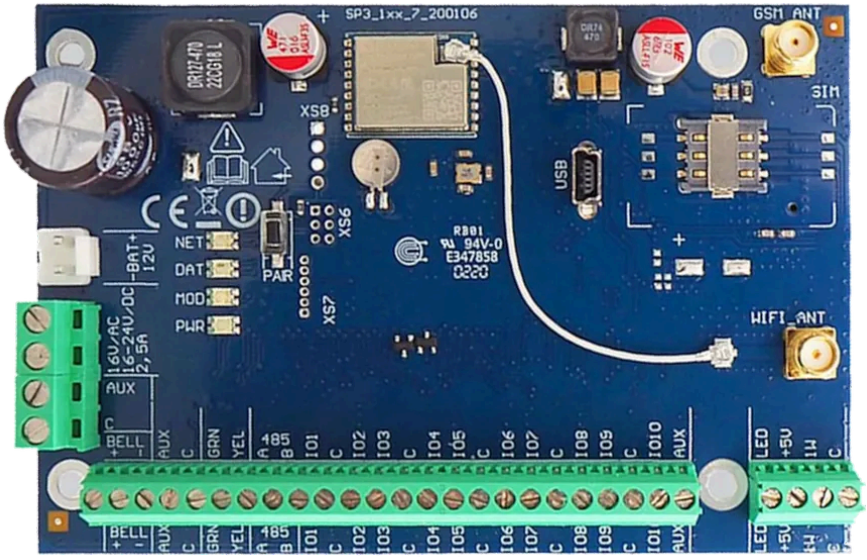
Centrala alarmowa „FLEXi” SP3 – instrukcja instalacji i programowania

Instrukcja instalacji i programowania centrali alarmowej Trikdis „FLEXi” SP3: zasilanie, podłączenie stref i wyjść PGM, manipulatory i ekspandery, programowanie w TrikdisConfig, transmisja do stacji monitorowania, aplikacja Protegus 2.



Wydanie: 2026-11-17
Zawsze aktualna wersja internetowa: https://pl.mobilamb.eu/instrukcja-flexi-sp3

Spis treści

1. Przegląd

1.1 Do czego służy, jak działa
1.2 Wersje i kody typu
1.3 Dane techniczne
1.4 Kompatybilne moduły i manipulatory
1.5 Elementy płytki i jej zaciski
1.6 Sygnalizacja LED
1.7 Wersje firmware

2. Zasilanie i szybkie uruchomienie

2.1 Zasilacz sieciowy
2.2 Akumulator
2.3 Zawartość opakowania, obudowy: K01 i K02
2.4 Kroki uruchomienia w skrócie

3. Instalacja i podłączenie

3.1 Zalecana kolejność instalacji
3.1.1 Montaż płytki w obudowie
3.1.2 Kolejność podłączania urządzeń
3.2 Podłączenie czujek
3.2.1 Schematy podłączeń
3.3 Podłączenie czujek dymu
3.4 Podłączenie sygnalizatora
3.5 Podłączenie manipulatorów i czytników RFID
3.6 Podłączenie czytników kluczy TM17 i CZ-Dallas
3.7 Podłączenie czujników temperatury
3.8 Podłączenie przekaźnika i lampki LED
3.9 Włączenie centrali

4. Podłączenie ekspanderów i modułów radiowych

4.1 Moduł Ethernet E485
4.2 Odbiornik radiowy RF-SH (Crow)
4.3 Odbiornik radiowy RTX3 (Paradox)
4.4 Odbiornik radiowy RF-HW (Honeywell)
4.5 Odbiornik radiowy RF-S8
4.6 Odbiornik radiowy RF-LORA
4.7 Ekspandery LORA
4.8 Ekspandery serii iO
4.9 Nadajnik radiowy T16
4.10 Moduł Sigfox SF485
4.11 Pomiar napięcia stałego

5. Protegus 2 i sterowanie zdalne

5.1 Połączenie z kontem Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Uzbrajanie i rozbrajanie w aplikacji
5.3 Konfiguracja i sterowanie SMS-em
5.4 Sterowanie połączeniem telefonicznym

6. TrikdisConfig – ustawienia szczegółowo

- 6.1 Pasek stanu
- 6.2 System Options
  - 6.2.1 Zakładka System general
  - 6.2.2 Zakładka Partitions
  - 6.2.3 Zakładka Scheduler
  - 6.2.4 Zakładka Holidays
  - 6.2.5 Zakładka System troubles
  - 6.2.6 Zakładka Access
- 6.3 Reporting to CMS
  - 6.3.1 Zakładka Reporting
  - 6.3.2 Zakładka Settings
- 6.4 Users & Reporting
  - 6.4.1 Karty i breloki RFID
  - 6.4.2 Klucze iButton
  - 6.4.3 Zakładka Protegus
  - 6.4.4 Zakładka SMS answer texts
- 6.5 Modules
- 6.6 Wireless sensors
  - 6.6.1 Rejestracja RF-LORA
  - 6.6.2 Zdalne parowanie czujek
  - 6.6.3 Parowanie przyciskiem LEARN
  - 6.6.4 Urządzenia RF-SH i Crow
- 6.7 Zones
- 6.8 PGM
- 6.9 Sensors
- 6.10 System events
- 6.11 Events log
- 6.12 Przywracanie ustawień fabrycznych

7. Zdalne programowanie

8. Sprawdzenie działania systemu

9. Aktualizacja firmware

10. Rozwiązywanie problemów i najczęstsze pytania

11. Gwarancja i zasady bezpieczeństwa

- 11.1 Gwarancja i ograniczenie odpowiedzialności
- 11.2 Zasady bezpieczeństwa

Zobacz też

1. Przegląd

„FLEXi" SP3 to **centrala alarmowa włamania i pożaru** firmy Trikdis z wbudowanym komunikatorem: przez połączenie Wi-Fi i/lub Ethernet oraz modem 2G / 4G (przez sieć komórkową, jeśli włożona jest karta SIM) przesyła każde wywołane zdarzenie bezpośrednio do stacji monitorowania i do aplikacji Protegus 2 (chmura Protegus). Ma dziesięć zacisków IO o wybieranej funkcji (strefa lub wyjście PGM), obsługuje osiem partycji i – zależnie od wersji firmware – można ją rozbudować do 32 lub 64 stref za pomocą manipulatorów, ekspanderów iO i odbiorników bezprzewodowych. Ustawienia wprowadzasz programem TrikdisConfig przez kabel USB lub zdalnie; użytkownik steruje systemem z manipulatora przewodowego lub bezprzewodowego, kluczem iButton, kartą RFID, z aplikacji Protegus 2, a w wersjach z modemem także SMS-em i połączeniem telefonicznym – może też zdalnie przełączać tryb ochrony różnych obszarów (partycji) budynku. Centrala ma certyfikat EN 50131 Grade 3.

1.1 Do czego służy, jak działa

Do czego służy przede wszystkim

- **System alarmowy małych i średnich budynków**, najlepiej uzupełniony o stację monitorowania: przyjmuje zarówno czujki przewodowe, jak i bezprzewodowe, przekazuje zdarzenia stacji monitorowania i użytkownikowi, a oboje mogą nim sterować zdalnie.
- **Wymiana istniejącej centrali alarmowej**: wartości rezystorów końca linii w czujkach można ustawić w centrali tak, jak w wymienianej centrali, dzięki czemu czujek nie trzeba przerabiać pojedynczo.
- **Automatyka** obok ochrony: brama garażowa i furtka, nawadnianie, oświetlenie, ogrzewanie, wentylacja, chłodzenie i wszystko inne, co można włączać i wyłączać – z wyjść PGM, z logiką działania, harmonogramem lub w trybie termostatu.

Jak działa

- **Raportuje do stacji monitorowania** przez wbudowane połączenie Wi-Fi, Ethernet lub sieć komórkową; z modułem dodatkowym także kanałem Ethernet (E485), radiowym VHF/UHF (T16) lub Sigfox (SF485), z wybieranym priorytetem. Zdarzenia może odbierać każda stacja monitorowania, która ma programowy lub sprzętowy odbiornik IP Trikdis albo odbiornik IP obsługujący protokół SIA DC-09. Może wysyłać równolegle do odbiorników dwóch różnych firm ochrony, każdej z odbiornikiem głównym i zapasowym.
- **Powiadamia użytkownika** w aplikacji Protegus 2 komunikatem push i osobnym sygnałem dźwiękowym, a wersje z modemem także SMS-em na maksymalnie 8 numerów telefonu. Połączeniem z nagranym wcześniej komunikatem głosowym (na maksymalnie 8 numerów) potrafi powiadamiać tylko stara wersja SP3_12xx z firmware co najwyżej 1.13. Można ustawić, aby zdarzenie trafiało najpierw do stacji monitorowania, a dopiero potem do użytkownika.
- **Można nią sterować zdalnie**: uzbrajanie, rozbrajanie, tryb dzienny (Stay) i nocny (Sleep), przełączanie urządzeń podłączonych do wyjść PGM i monitorowanie temperatury z aplikacji; w wersjach z modemem także SMS-em i połączeniem telefonicznym.
- **Wejścia i wyjścia**: 10 zacisków IO, każdy może pracować jako wejście (typy NC, NO, EOL, ATZ, z ustawianą wartością rezystorów w obwodach EOL i ATZ) lub jako wyjście typu otwarty kolektor; liczbę wejść można zwiększyć do 64 za pomocą manipulatorów oraz ekspanderów iO, iO-8, iO8-LORA, iO-LORA i iO-WL, a liczbę wyjść tymi samymi ekspanderami do 16; dwa dedykowane wyjścia (BELL dla sygnalizatora, LED dla lampki sygnalizacyjnej); siedem trybów pracy wyjść, a każdemu wyjściu można przypisać logikę działania, wcześniej ustawiony harmonogram lub na przykład tryb termostatu; na

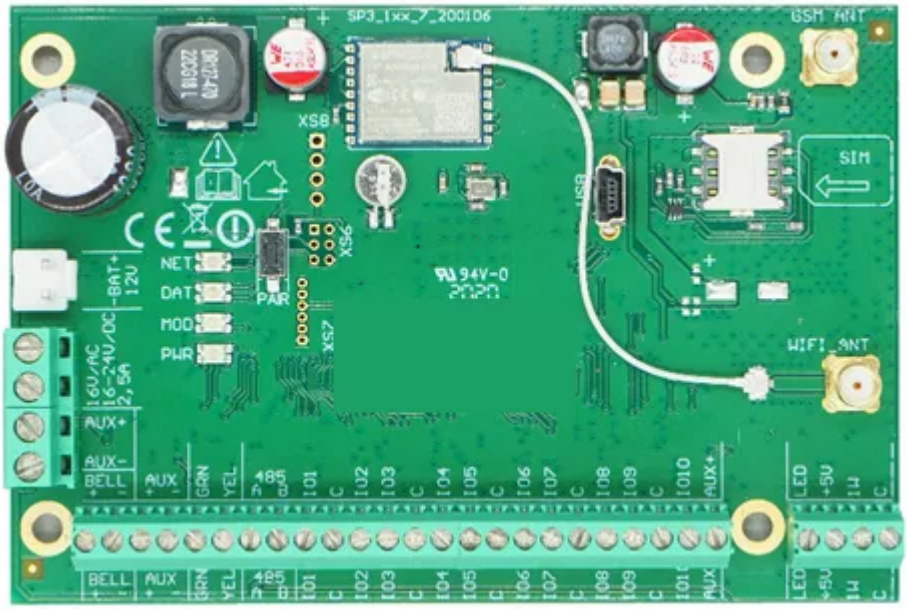
magistrali 1-Wire maksymalnie 8 czujników temperatury, 1 czujnik temperatury i wilgotności albo czytnik iButton; na magistrali manipulatorów GRN / YEL 8 manipulatorów tego samego typu i odbiornik radiowy Paradox RTX3 (4.3); na magistrali RS485 ekspandery iO, odbiorniki radiowe (RF-LORA, RF-SH, RF-S8, RF-HW), moduły E485, T16 i SF485.

- **Obsługa**: 40 kodów użytkowników (1 kod główny i 39 kodów zwykłych, 4- lub 6-cyfrowych), które mogą służyć także jako kody przymusu – kod rozbraja alarm, ale stacja monitorowania otrzymuje osobny sygnał, że rozbrojenie nastąpiło pod przymusem. Manipulatory Trikdis, Paradox i Crow, czytniki iButton CZ-Dallas i TM17 (wycofany), czytniki RFID Wiegand 26/34.
- **Instalacja i konfiguracja**: zestawy w metalowej obudowie z wbudowanym zasilaniem, w kilku rozmiarach, z transformatorem obniżającym lub zasilaczem impulsowym; ustawienia fabryczne w większości małych i średnich obiektów (w siedmiu na dziesięć) można stosować bez zmian; dotychczasową centralę można wymienić bez wymiany rezystorów w czujkach; ustawienia można zapisać do pliku; dwa poziomy dostępu (instalator i administrator); TrikdisConfig zdalnie nie tylko konfiguruje, ale też pokazuje działanie centrali.

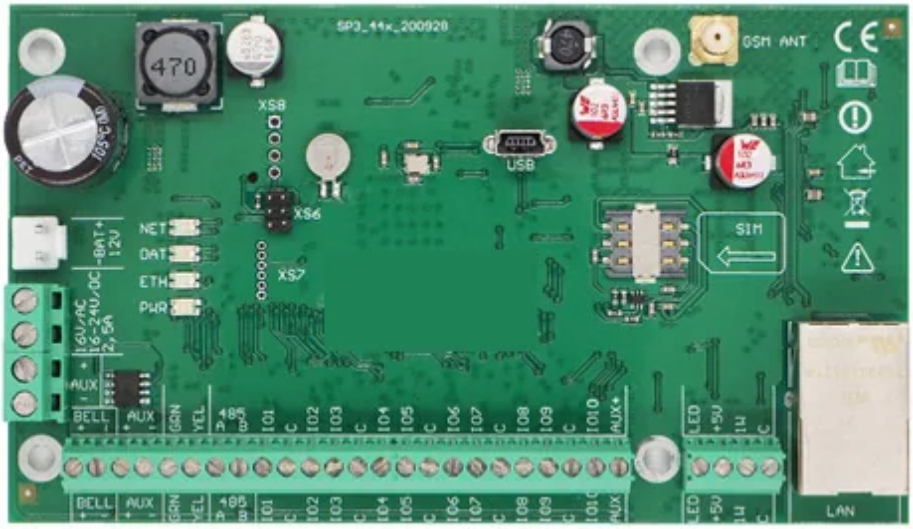
1.2 Wersje i kody typu

Centrala to jedna płytka drukowana, dostępna w sześciu wersjach zależnie od wbudowanych modułów komunikacyjnych. Wersję oznacza pierwsza cyfra (**y**) kodu **SP3_yxxz** w nazwie pliku firmware; to samo widzisz na pasku stanu TrikdisConfig, a podczas aktualizacji można wgrać tylko firmware z tą samą cyfrą (punkt 1.7).

Wersja	Połączenie	Kod (y)	Gniazdo SIM
SP3 WiFi	Wi-Fi	2	–
SP3 Ethernet	sieć przewodowa (Ethernet, RJ45)	3	–
SP3 WiFi + 2G	Wi-Fi + modem 2G (GSM/GPRS)	5	1 × nano-SIM
SP3 WiFi + 4G	Wi-Fi + modem 4G (LTE)	1	1 × nano-SIM
SP3 Ethernet + 4G	Ethernet + modem 4G (LTE)	6	1 × nano-SIM
SP3 Ethernet + 2 SIM 4G	Ethernet + modem 4G (LTE), z dwoma gniazdami SIM	sprawdź na pasku stanu urządzenia	2 × nano-SIM



Rysunek 1. Płytka drukowana „FLEXi" SP3 w wersji WiFi + 2G: złącza SMA anteny Wi-Fi i anteny sieci komórkowej, gniazdo nano-SIM i listwy zaciskowe.



Rysunek 2. „FLEXi" SP3 w wersji Ethernet + 4G: gniazdo Ethernet RJ45 w miejscu złącza anteny Wi-Fi.

Jeden lub dwa kanały komunikacji. Wersje WiFi i Ethernet komunikują się jednym kanałem, wersje z modemem dwoma (dual path): oprócz połączenia przewodowego także przez sieć komórkową.

WiFijeden kanał
Ethernetjeden kanał
WiFi + 2Gdwa kanały · 1 SIM
WiFi + 4Gdwa kanały · 1 SIM
Ethernet + 4Gdwa kanały · 1 SIM
Ethernet + 2 SIM 4Gdwa kanały · 2 SIM

- Przez Wi-Fi i Ethernet dostęp z telefonu jest szybki i nie ma kosztów transmisji danych komórkowych.
- Jeśli przewodowy internet zostanie przerwany albo router wyłączy się podczas zaniku zasilania, centrala z modemem sama przełączy się na sieć komórkową.
- Dzięki dwóm wzajemnie się zabezpieczającym kanałom (dual path) sygnał dotrze do celu, nawet jeśli jedna z dróg zawiedzie.

- Przez szybkie połączenie Wi-Fi, Ethernet i 4G wygodnie przeprowadza się zdalne programowanie i aktualizację firmware.

Modem **2G** w wersjach z modemem pracuje w pasmach 850 / 900 / 1800 / 1900 MHz, a modem **4G (LTE)** w pasmach B1 / B3 / B7 / B8 / B20 / B28 używanych w Europie (EMEA); dla innych regionów (Ameryka Łacińska, Australia, Ameryka Północna) produkowane są także wersje z modemem o innym przydziale pasm (pasma podaje tabela w punkcie 1.3). Wi-Fi 2,4 GHz, 802.11 b/g/n, z szyfrowaniem WPA / WPA2.

1.3 Dane techniczne

Parametr	Wartość
Napięcie zasilania [AC / DC]	16 V AC lub 16–24 V DC, 2,5 A
Pobór prądu	maks. 50 mA w czuwaniu; maks. 200 mA krótkotrwale, podczas wysyłania
Zasilanie rezerwowe [BAT]	akumulator ołowiowy 12 V, 4 Ah lub 7 Ah
Prąd ładowania akumulatora	maks. 500 mA
Zasilanie urządzeń zewnętrznych [AUX]	12 V DC, maks. 1 A
Wyjście sygnalizatora [BELL]	1 A
Wyjście LED [LED]	0,1 A
Wyjście PGM (zacisk IO jako wyjście)	otwarty kolektor, maks. 0,1 A
Moduł Wi-Fi	wbudowany w wersjach Wi-Fi; 2,4 GHz, 802.11 b/g/n, WPA / WPA2 / WPA mieszany
Konfiguracja sieci	DHCP lub ręczna
Karta SIM	w wersjach z modemem 1 (w wersji z 2 SIM 2) nano-SIM
Pasma modemu 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Pasma modemu 4G (LTE) – „FLEXi" SP3_14E / SP3_24E, EMEA i Tajlandia	B1 / B3 / B7 / B8 / B20 / B28
Pasma modemu 4G (LTE) – „FLEXi" SP3_24S, Ameryka Łacińska / Australia / Nowa Zelandia	B1 / B3 / B4 / B5 / B7 / B8 / B28
Pasma modemu 4G (LTE) – „FLEXi" SP3_24A, Ameryka Północna	B2 / B4 / B12
Kierunki wysyłania zdarzeń	odbiorniki główne i zapasowe 2 firm ochrony; chmura Protegus, aplikacja Protegus 2 na iOS / Android; SMS na 8 numerów telefonu; połączenie na 8 numerów telefonu – jeśli użytkownik odbierze, centrala komunikatem głosowym mówi, co się stało (tylko wersja SP3_12xx z firmware co najwyżej 1.13)
Kanały wysyłania zdarzeń	GPRS lub 4G, Wi-Fi, Ethernet (wbudowany lub z modułem E485), SMS; połączenie głosowe na maksymalnie 8 numerów telefonu (tylko wersja SP3_12xx z firmware co najwyżej 1.13); radio VHF/UHF (z komunikatorem T16); Sigfox (z modułem SF485)
Połączenie ze stacją monitorowania	TCP/IP lub UDP/IP albo SMS

Parametr	Wartość
Kodowanie zdarzeń	Contact ID
Szyfrowanie	TRK AES-128, SIA IP AES-128
Zegar wewnętrzny	jest
Bufor komunikatów	60 zdarzeń
Dziennik zdarzeń	maks. 1000 zdarzeń; po zapełnieniu najstarsze jest usuwane
Kody użytkowników	40 (4- lub 6-cyfrowe)
Kod przymusu	jeden z dwóch trybów wprowadzania do wyboru podczas programowania
Zaciski o podwójnej funkcji [IO]	10; funkcja IN lub OUT wybierana podczas programowania. Jako wejście: NC, NO, EOL, EOL_T, 3EOL, ATZ, ATZ_T. Jako wyjście: otwarty kolektor (OC), maks. 100 mA
Partycje	8
Strefy	10 (20 z podwajaniem stref ATZ); z ekspanderami do 64 (punkt 1.7)
Wyjścia PGM	2 (12, jeśli zaciski IO są ustawione jako wyjścia; z ekspanderami 16)
Manipulatory	maks. 8 (typy wymienia punkt 1.4)
Czytniki RFID (Wiegand 26/34)	maks. 2
Długość magistrali 1-Wire [1 WIRE]	maks. 30 m
Czujniki temperatury	Maxim / Dallas DS18S20, DS18B20; seria AM2301
Liczba czujników temperatury na magistrali 1-Wire	8 (Dallas) lub 1 (AM2301)
Klucze elektroniczne (iButton) [1 WIRE]	Maxim / Dallas DS1990A, maks. 40 kluczy
Długość magistrali RS485	maks. 100 m
Urządzenia na magistrali RS485	maks. 8
Warunki pracy	−10 °C … +50 °C, wilgotność względna maks. 80 % przy +20 °C, bez kondensacji
Wymiary płytki	117 × 79 × 25 mm; wersje Ethernet + 4G 137 × 79 × 25 mm
Masa	0,1 kg

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 Kompatybilne moduły i manipulatory

Wyjście AUX centrali daje urządzeniom zewnętrznym maksymalnie 1 A; do doboru akumulatora rezerwowego (punkt 2.1) trzeba zsumować łączny pobór prądu podłączonych modułów. Lista fabryczna:

Moduł	Pobór prądu
Manipulator SK-LED TouchPad (Protegus SK232 LED W)	60–150 mA
Manipulator SK-LCD TouchPad (FLEXi SK232LCD – w sklepie manipulator FLEXi LCD)	25–60 mA
Manipulator SK LCD Button	maks. 70 mA

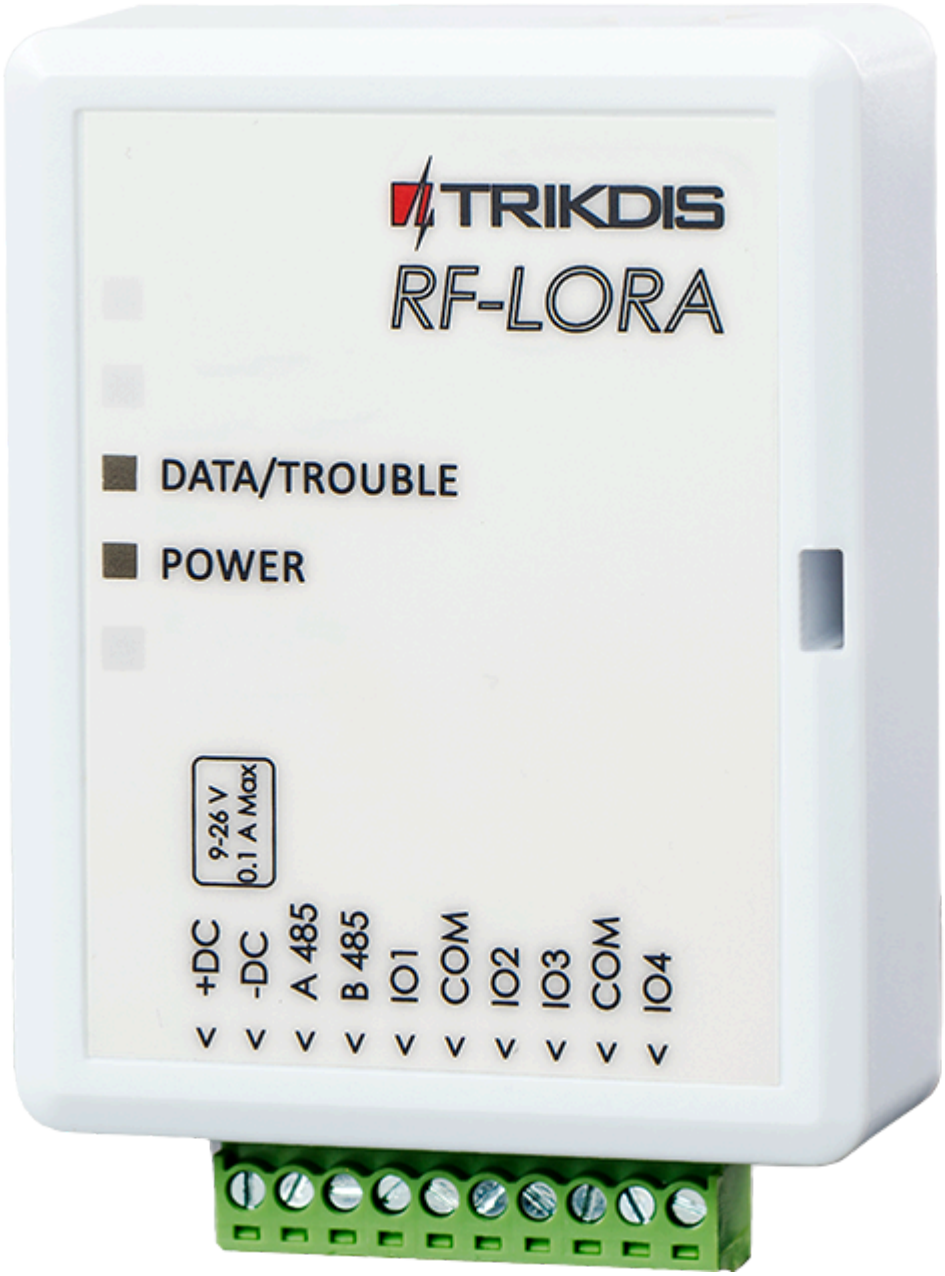
Moduł	Pobór prądu
Manipulator SK LED Button	maks. 70 mA
Manipulator Paradox K636	40–70 mA
Manipulator Paradox K10H(V)	44–72 mA
Manipulator Paradox K32 LED, K32+ LED	49–148 mA
Manipulator Paradox K32LCD+	70–150 mA
Manipulator Paradox K35	30–70 mA
Manipulator Paradox TM50	100–230 mA
Manipulator Paradox TM70	200–330 mA
Manipulator Crow CR16, CR-LCD	40–75 mA
Ekspander iO-8	maks. 20 mA
Ekspander iO	maks. 50 mA
iO-MOD – nadajnik-odbiornik radiowy iO-WL	50–150 mA
Ekspander bezprzewodowy iO-WL	maks. 200 mA
Odbiornik radiowy RF-SH (do czujek Crow)	maks. 100 mA
Nadajnik-odbiornik radiowy Paradox RTX3	maks. 200 mA
Nadajnik-odbiornik radiowy RF-HW (do czujek Honeywell)	maks. 100 mA
Nadajnik-odbiornik radiowy RF-S8 (do czujek S8)	maks. 100 mA
Nadajnik-odbiornik radiowy RF-LORA (do czujek i modułów LORA)	50–150 mA
Ekspander iO-LORA, iO8-LORA	maks. 50 mA
Przycisk napadowy PB-LORA	własna bateria, 3 V CR123A
Moduł przekaźnikowy REL-LORA	maks. 45 mA
Moduł Ethernet E485	50–150 mA
Czytnik iButton TM17	maks. 50 mA
Czytnik iButton CZ-Dallas	maks. 25 mA
Komunikator radiowy VHF / UHF T16	100 mA – 1,2 A
Czytnik RFID (Wiegand 26/34)	maks. 100 mA

Manipulatory. Do magistrali GRN / YEL można podłączyć maksymalnie 8 manipulatorów tego samego typu:

Trikdis PROTEGUS SK232LED, FLEXI LCD, FLEXI LED, SK-LCD Button, SK-LED Button
Paradox K32LCD+, K32+, K32LED, K32+ LED, K35, K10H, K10V, K636, TM50*****, TM70*****
Crow CR16, CR-LCD
A LED-es kezelők csak az első 2 partíció állapotát képesek megjeleníteni, de kezelhetik mind a 8 partíciót.
*Ez a kezelő csak az első 2 partíciót kapcsolhatja ki/be.

Urządzenia bezprzewodowe. Typ odbiornika radiowego zależy od wersji firmware centrali (punkt 1.7): centrala pracuje jednocześnie tylko z jednym rodzajem odbiornika.

Vezeték nélküli érzékelők és eszközök hozzáadása a FLEXi SP3 riasztórendszerhez





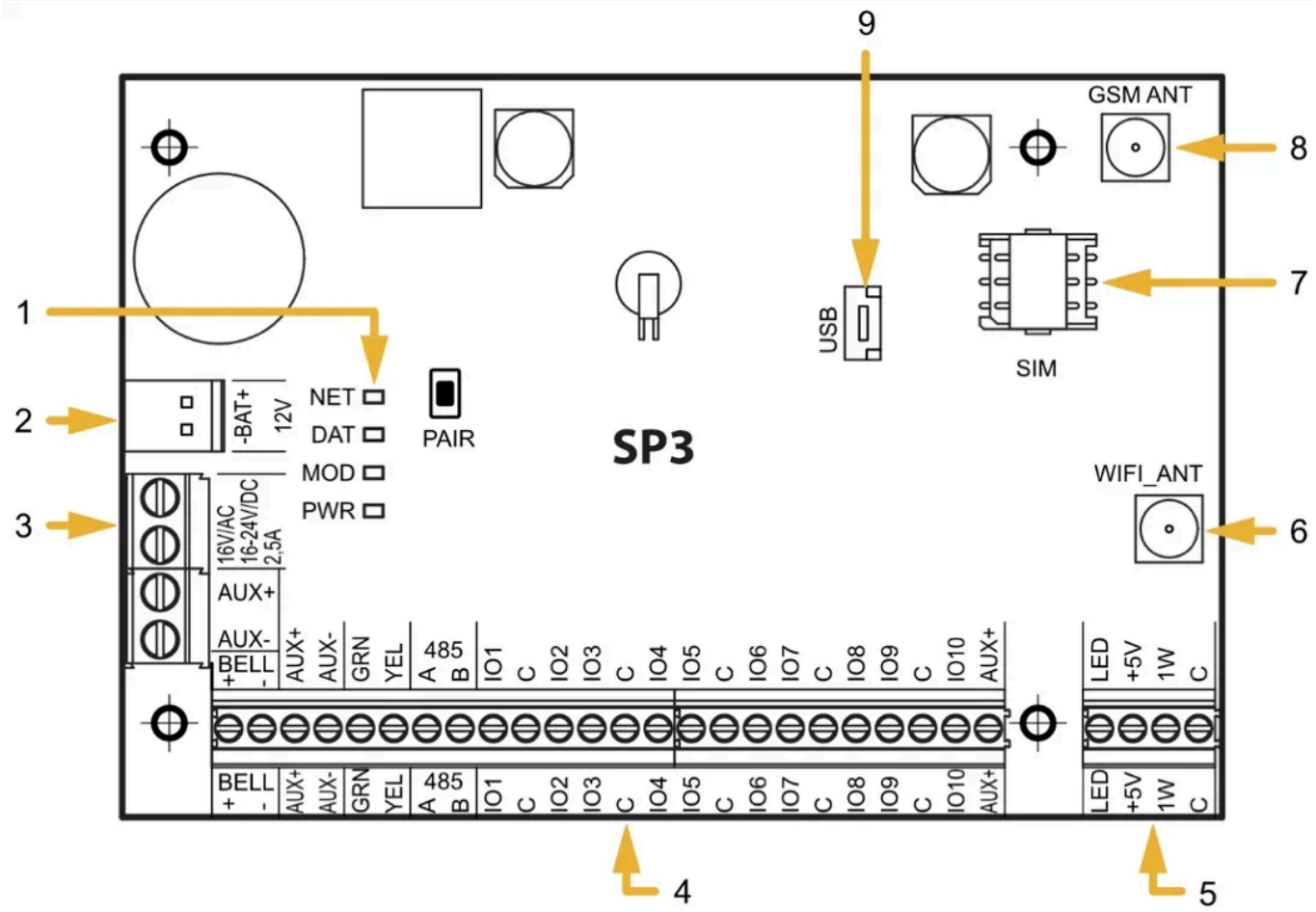
A **TRIKDIS RF-LORA** vagy **Paradox RTX3** vezeték nélküli bővítő modullal a „klasszikus" vezetékes riasztó hibrid vagy teljesen vezeték nélküli módon is működhet. Hasznos, ha nincs lehetőség vezeték kiépítésére és vezeték nélküli érzékelőkre vagy egyéb vezeték nélküli eszközökre van szükség.

A RIKDIS RF-LORA-hoz a Trikdis vezeték nélküli bővítőket, érzékelőket és eszközöket lehet párosítani.

A Paradox RTX3-mal a Paradox vezeték nélküli érzékelőket, eszközöket és billentyűzeteket lehet használni.

1.5 Elementy płytki i jej zaciski

Rysunek pokazuje główne elementy płytki; funkcje zacisków wymienia tabela pod rysunkiem.



Rysunek 3. Płytka drukowana „FLEXi" SP3 (wersja Wi-Fi + komórkowa). W wersji Ethernet w miejscu elementu 6 jest gniazdo Ethernet RJ45.

- 1 Diody LED sygnalizujące połączenie i działanie (punkt 1.6)
- 2 Zaciski zasilania rezerwowego (akumulatora)
- 3 Zaciski zasilania głównego
- 4 Zaciski urządzeń zewnętrznych
- 5 Zaciski magistrali danych 1-WIRE
- 6 Złącze SMA anteny Wi-Fi
- 7 Gniazdo nano-SIM
- 8 Złącze SMA anteny sieci komórkowej
- 9 Gniazdo USB Mini-B do programowania

Zacisk	Funkcja
AC/DC (2 zaciski)	Zasilanie główne: 16 V AC lub biegun dodatni i ujemny 16–24 V DC
BAT+	Biegun dodatni zasilania rezerwowego (akumulator 12 V)
BAT–	Biegun ujemny zasilania rezerwowego
AUX+	+12 V dla urządzeń zewnętrznych (maks. 1 A)
AUX–	Wspólny minus
BELL+	Wyjście sygnalizatora: +12 V dla sygnalizatora
BELL–	Wyjście sygnalizatora: kluczowany biegun ujemny sygnalizatora (maks. 1 A)
GRN	Magistrala manipulatorów (dane)
YEL	Magistrala manipulatorów (dane)
A 485	Przewód A magistrali RS485

Zacisk	Funkcja
B 485	Przewód B magistrali RS485
IO1 – IO9	Wejścia/wyjścia (ustawienie fabryczne: wejście)
IO10	Wejście/wyjście (ustawienie fabryczne: wyjście PGM, reset czujek pożarowych)
C	Wspólny minus
LED	Wyjście PGM (ustawienie fabryczne: sygnalizacja stanu systemu)
+5 V	Zasilanie +5 V dla urządzeń 1-Wire
1 WIRE	Magistrala danych 1-Wire
C	Wspólny minus

Listwy zaciskowe są odłączane, dzięki czemu przewody możesz podłączyć także bez płytki, a płytkę można wyjąć podczas serwisu.

1.6 Sygnalizacja LED

LED	Sygnał	Znaczenie
NET	miga na zielono	karta SIM loguje się do sieci komórkowej
	świeci na zielono	karta SIM zalogowała się do sieci komórkowej
	miga na żółto	siła sygnału sieci komórkowej, 0–5 mignięć; 3 już wystarczają
DAT	nie świeci	brak niewysłanych zdarzeń
	świeci na zielono	trwa wysyłanie komunikatu
	świeci na żółto	niewysłane zdarzenia czekają w buforze
MOD (wersja Wi-Fi)	miga na zielono	łączenie z siecią Wi-Fi
	świeci na zielono	połączono z siecią Wi-Fi
ETH (wersja Ethernet)	miga na zielono	brak kabla LAN lub błąd DHCP
	świeci na zielono	połączono z siecią przewodową
PWR	miga na zielono	brak usterek działania
	1 czerwone mignięcie	brak karty SIM
	2 czerwone mignięcia	błędny kod PIN karty SIM
	3 czerwone mignięcia	nie może połączyć się z siecią komórkową
	4 czerwone mignięcia	nie może połączyć się z odbiornikiem stacji monitorowania na 1. kanale
	5 czerwonych mignięć	nie może połączyć się z odbiornikiem stacji monitorowania na 2. kanale
	6 czerwonych mignięć	zegar wewnętrzny nie jest ustawiony
	7 czerwonych mignięć	niskie napięcie zasilania rezerwowego (akumulatora)
	8 czerwonych mignięć	brak zasilania sieciowego (AC)
	9 czerwonych mignięć	nie może połączyć się z siecią Wi-Fi

Usuwanie usterek omawia rozdział 10.

1.7 Wersje firmware

Nazwa pliku firmware centrali ma postać **SP3_yxxz_NNNN.fw**. **y** to wersja sprzętowa (punkt 1.2) – podczas aktualizacji nie można jej zmienić. **z** określa typ odbiornika bezprzewodowego, a tym samym liczbę obsługiwanych stref; wybierasz go podczas aktualizacji, dopasowując do używanego odbiornika radiowego. **NNNN** to numer wersji firmware; zwykle warto używać najwyższej wersji.

Firmware (z)	Odbiornik bezprzewodowy	Czujki bezprzewodowe	Strefy	Manipulatory	Moduły
SP3_xxx0	RF-SH (wycofany), RF-LORA	Crow	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-SH
SP3_xxx1	Paradox RTX3, RF-LORA	Paradox	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA
SP3_xxx2	RF-HW, RF-LORA	Honeywell (345 MHz, nieużywane w Europie)	64	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-HW
SP3_xxx4	RF-LORA, RF-S8	MAXIMUM (M4), S8 (Heyi)	64	Trikdis (FLEXi), Paradox	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-S8

Firmware **SP3_xxx4** jest potrzebny tylko do czujek bezprzewodowych: z nim działają urządzenia bezprzewodowe MAXIMUM (RF-LORA) i S8 (RF-S8), z 64 strefami. Potrzebna jest co najmniej wersja 1.21, a do urządzeń S8 wersja 1.22. Ekspandery LORA podłączane przez RF-LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) działają ze wszystkimi czterema wersjami. Do ekspandera Paradox RTX3 potrzebny jest **SP3_xxx1**, z 32 strefami. Zawsze wgrywaj najnowszą wersję: w listopadzie 2026 jest to 1.27, z poprawioną komunikacją, w której usunięto wysyłanie zbyt wielu SMS-ów. Kodowanie i zasady wyboru opisuje osobny artykuł: Firmware FLEXi SP3: jak wybrać właściwy?. Kroki aktualizacji – w rozdziale 9.

2. Zasilanie i szybkie uruchomienie

Centralę, a wraz z nią cały system alarmowy, zasila sieciowe źródło zasilania, a rezerwę zapewnia akumulator 12 V. W tym rozdziale znajdziesz zasady zasilania, zestawy fabryczne i krótką kolejność kroków uruchomienia; szczegóły podłączenia są w rozdziałach 3 i 4, a ustawień w rozdziałach 5 i 6.

2.1 Zasilacz sieciowy

Centrala pracuje z napięcia **16 V AC** lub **16–24 V DC**, ze źródła o obciążalności co najmniej **2,5 A**. Przy prądzie przemiennym zasila ją z sieci transformator obniżający klasy II, przy prądzie stałym zasilacz impulsowy 16–24 V (w obudowach K01 i K02 dostępnych u nas Mean Well APV-35-24). Zasilanie główne podłączasz do

dwóch zacisków **AC/DC** płytki; przy prądzie stałym biegun dodatni i ujemny w kolejności oznaczonej przy zaciskach. W obu przypadkach – przy zasilaniu prądem przemiennym i stałym – obowiązkowe jest podłączenie zasilania rezerwowego, akumulatora 12 V, aby zasilanie było ciągłe, bez przerw (punkt 2.2).

Wyłącznik nadprądowy i uziemienie

W obwodzie zasilania trzeba zainstalować dwubiegunowy automatyczny wyłącznik nadprądowy, którego otwarte styki są oddalone o co najmniej 3 mm; wyłącznik powinien znajdować się w miejscu znanym i dostępnym dla specjalisty serwisującego centralę. W przypadku metalowej obudowy uziem obudowę. Obudowa, zasilacz, akumulator i urządzenie programujące muszą spełniać wymagania normy EN 60950.

Obliczanie zapotrzebowania na prąd. Według EN 50131 zasilanie rezerwowe po zaniku zasilania sieciowego musi podtrzymywać pracę systemu przez **12 godzin** (Grade 2) lub **60 godzin** (Grade 3). W tym celu zsumuj prąd centrali w czuwaniu (50 mA) i pobór prądu podłączonych manipulatorów, modułów, czujek i sygnalizatorów – dane urządzeń Trikdis i obsługiwanych urządzeń innych producentów podaje tabela w punkcie 1.4 – i do tego dobierz pojemność akumulatora. Zacisk **AUX+** może dać urządzeniom zewnętrznym łącznie maksymalnie 1 A; jeśli potrzeba więcej, użyj osobnego zasilacza ze wspólnym minusem.

2.2 Akumulator

Zasilanie rezerwowe to **akumulator ołowiowy 12 V, 4 Ah lub 7 Ah** (dla Grade 3 co najmniej 7 Ah), podłączony do zacisków **BAT+ / BAT−** płytki kablem połączeniowym dołączonym do zestawu. Centrala ładuje go prądem maksymalnie 500 mA.

- Jeśli zasilanie sieciowe zaniknie, centrala wysyła zdarzenie **AC Fault** (awaria zasilania sieciowego) i przełącza się na akumulator.
- Przy 11,5 V powstaje zdarzenie **Low Battery** (akumulator się rozładowuje); poniżej 9,5 V centrala **odłącza** akumulator, aby chronić go przed głębokim rozładowaniem.
- Po powrocie zasilania sieciowego wysyła zdarzenie **AC Restore** i zaczyna ładowanie; przy 12,6 V wysyła zdarzenie **Battery Restore** (akumulator w porządku).

Aby spełnić wymaganie klasy II, akumulator musi naładować się w ciągu 72 godzin, a dla klasy III w ciągu 24 godzin – wynika to łącznie z pojemności akumulatora i prądu ładowania 500 mA.

2.3 Zawartość opakowania, obudowy: K01 i K02

Centrala jest dostępna sama (płytka) lub z przygotowaną metalową obudową. W fabrycznym opakowaniu płytki: płytka „FLEXi" SP3, kabel do podłączenia akumulatora, 20 rezystorów 2,2 kΩ i 10 rezystorów 4,7 kΩ, 4 plastikowe dystanse do mocowania, a do wersji z modemem antena ME301M z podstawą magnetyczną i kablem 2,5 m (według fabrycznej listy zawartości 2 szt.). **Kabel USB Mini-B** potrzebny do programowania i akumulator nie wchodzą w skład zestawu.

W wersjach z obudową centrala jest zamontowana w metalowej obudowie z wyłącznikiem sabotażowym, z przygotowanym zasilaniem: zasilacz impulsowy Mean Well APV-35-24, punkt podłączenia sieci 230 V z bezpiecznikiem 3,15 A, wszystko okablowane. Są dwa rozmiary obudowy:

Obudowa	Wymiary	Uwagi
K01 – metalowa obudowa normalnej wielkości	285 × 280 × 80 mm	do wszystkich wersji SP3
K02 – mała metalowa obudowa	200 × 210 × 80 mm	wersja Ethernet + 4G się w niej nie mieści

Metalowe pudełko z normalnym rozmiarem z PSU dla panelu sterowania Flexi SP3

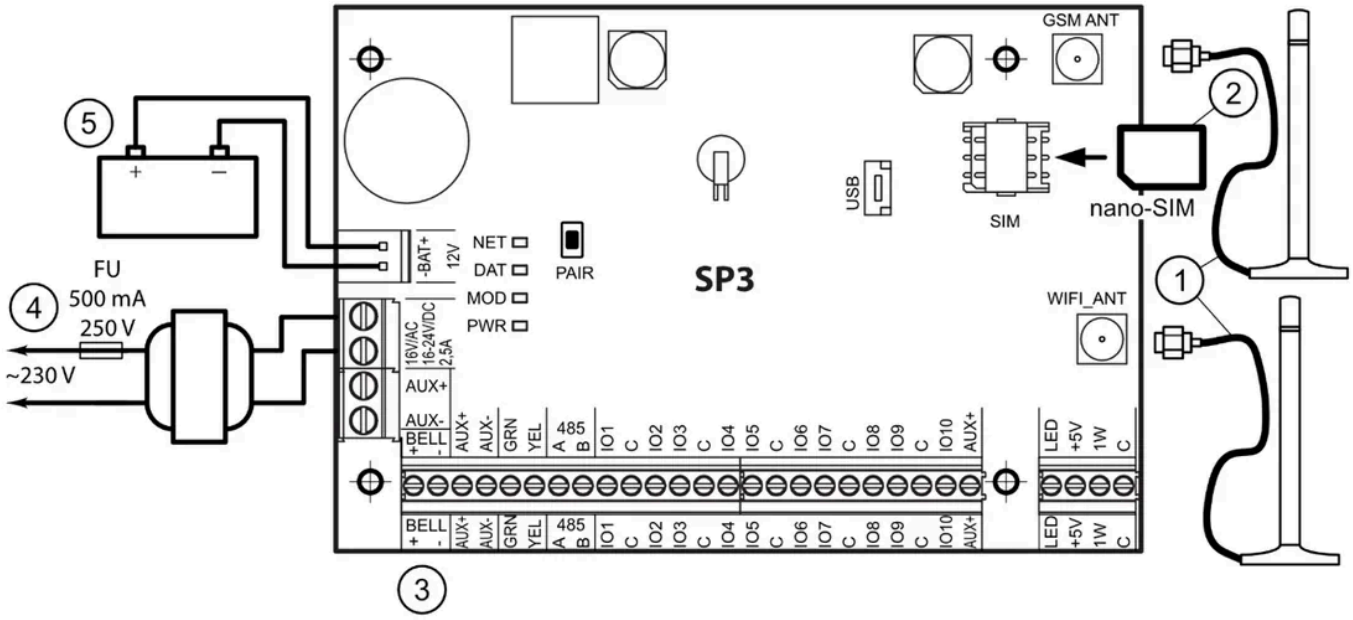
Małe metalowe pudełko z PSU dla panelu sterowania Flexi SP3

W obu obudowach (K01 i K02) jest zasilacz impulsowy Mean Well z listwą zaciskową z bezpiecznikiem 3,15 A; w starszych obudowach K01 był jeszcze transformator 230 V / 16 V, 40 VA. Do zestawów fabrycznych (SP3 KIT, SP3 KITi) oprócz płytki zamontowanej w metalowej obudowie dołączone są 2 anteny ME301M (z kablem 2,5 m), kabel do podłączenia akumulatora, 20 rezystorów 2,2 kΩ i 10 rezystorów 4,7 kΩ oraz czujnik sabotażowy.

2.4 Kroki uruchomienia w skrócie

Czego będziesz potrzebować

Kabel USB Mini-B · płaski śrubokręt do listew zaciskowych · rezystory 2,2 kΩ i 4,7 kΩ z zestawu · akumulator 12 V 7 Ah · do wersji z modemem aktywna karta nano-SIM z usługą transmisji danych (wcześniej wyłącz żądanie PIN w telefonie) · do wersji Wi-Fi nazwa i hasło sieci · program TrikdisConfig na komputerze z Windows.



Rysunek 4. Podłączenie zasilania i kolejność uruchomienia. Zasilanie sieciowe: transformator („Transformer"), ~230 V / 16 V, 40 VA, 50 Hz, z bezpiecznikiem 500 mA / 250 V (FU) w gałęzi 230 V, lub zasilacz prądu stałego 16–24 V, 2,5 A („or DC power supply source 16-24 V, 2,5 A"); zasilanie rezerwowe: akumulator („Battery"), 12 V, 7 Ah.

- 1 Przykręcenie anteny komórkowej i Wi-Fi do złączy antenowych
- 2 Włożenie karty nano-SIM do gniazda SIM
- 3 Podłączenie urządzeń do listew zaciskowych
- 4 Podłączenie zasilania sieciowego do zacisków AC/DC
- 5 Podłączenie akumulatora do zacisków BAT+ / BAT−

1. **Zaplanuj system.** Wyznacz miejsce obudowy, manipulatorów, sygnalizatorów akustycznych i optycznych oraz sterowanych urządzeń; na podstawie chronionego obszaru i właściwości czujek określ liczbę, typ i miejsce czujek.
2. **Zamontuj płytkę w obudowie** za pomocą plastikowych dystansów i uziem metalową obudowę (punkt 3.1).
3. **Przykręć anteny** (komórkową i Wi-Fi) i włóż aktywowaną kartę nano-SIM (wersja z modemem).

4. **Podłącz urządzenia** zgodnie ze schematami podłączeń: czujki otwarcia, czujki ruchu, pożarowe i inne (3.2–3.3), sygnalizator (3.4), manipulatory i czytniki (3.5–3.6), czujnik temperatury (3.7), przekaźniki i lampka sygnalizacyjna (3.8), wyłącznik sabotażowy obudowy; ekspandery i odbiorniki radiowe według rozdziału 4.
5. **Włącz zasilanie sieciowe** na zaciski AC/DC. Po włączeniu centrala rozpoznaje manipulatory, ekspandery i czytniki prawidłowo podłączone do magistrali 1-WIRE i GRN / YEL (punkt 3.9).
6. **Podłącz akumulator** do zacisków BAT+ / BAT−.
7. **Skonfiguruj centralę w TrikdisConfig** przez kabel USB (rozdział 6). Ustawienia fabryczne są dobre dla większości małych i średnich obiektów; co zwykle trzeba przejrzeć: partycje i podstawowe dane systemu (**System Options**, 6.2), typ i zachowanie stref (**Zones**, 6.7), użytkowników, ich kody i numery telefonów (**Users & Reporting**, 6.4), dokładny czas (6.2), dane karty SIM (6.2), odbiorniki stacji monitorowania – fabrycznie wyłączone (**Reporting to CMS**, 6.3) –, chmurę Protegus – fabrycznie włączoną – i powiadomienia SMS (6.4, 6.10), działanie wyjść PGM (6.8). Zalecane ustawienia szczegółowo:
    - **System.** Jeśli chcesz uzbrajać grupy stref oddzielnie, podziel system na partycje i ustaw właściwości partycji (6.2.2). Każdą strefę ustaw zgodnie z właściwościami czujki i zachowaniem alarmowym oczekiwanym dla zdarzenia strefy (6.7); w systemie podzielonym na partycje każdą strefę przypisujesz do wybranej partycji. Do obsługi z manipulatora, kluczem iButton lub z telefonu (SMS-em) trzeba utworzyć użytkowników i nadać im uprawnienia (6.4).
    - **Wysyłanie komunikatów.** Dokładny czas trzeba ustawić po to, aby komunikaty otrzymywały prawidłowy znacznik czasu (6.2.1). Raportowanie zdarzeń jest fabrycznie włączone dla wszystkich zdarzeń: jeśli wystąpi zdarzenie, jego raport trafia do ustawionych odbiorców ustawionymi kanałami; raportowanie poszczególnych zdarzeń możesz wyłączyć w oknie **System events** (6.10). Jeśli centrala wysyła przez sieć komórkową, wprowadź dane karty SIM (6.2.1). Transmisja do stacji monitorowania jest fabrycznie wyłączona (6.3). Chmura Protegus jest fabrycznie włączona, powiadomienia SMS i połączenia fabrycznie wyłączone; ustawienie wysyłania na telefon użytkownika opisuje punkt 6.10.
    - **Sterowanie zdalne.** Połączeniem i SMS-em może sterować systemem ten, czyj numer telefonu jest na liście użytkowników (6.4). Połączeniem można nie tylko uzbroić i rozbroić cały system lub jego część, ale też włączać i wyłączać urządzenia podłączone do wyjść PGM – co trzeba w tym celu ustawić na wyjściu, opisuje punkt 5.4. SMS-em można też zmienić niektóre parametry pracy centrali, uzbroić i rozbroić cały system lub jego część oraz przełączać urządzenia podłączone do wyjść PGM – lista komend jest w punkcie 5.3.
8. **Zmień kody fabryczne** na wartości znane tylko tobie: kod główny w oknie **Users & Reporting**, hasło SMS w polu **SMS Password** grupy **System Options** → **Access**, kody dostępu TrikdisConfig w tej samej grupie **Access**.
9. **Połącz system z aplikacją Protegus 2** (punkt 5.1).
10. **Sprawdź działanie** zgodnie z rozdziałem 8: zdarzenie z manipulatora, dotarcie do stacji monitorowania i do Protegus 2, wyjścia, zdalne uzbrajanie.

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 płytki, kolejność podłączania, a następnie podłączenie czujek, czujek dymu, sygnalizatorów, manipulatorów i czytników, czujników temperatury oraz przekaźników. Znaczenie zacisków podaje tabela w punkcie 1.5; podłączenie ekspanderów i modułów radiowych jest w rozdziale 4. Na rysunkach nazwy zacisków SP3 są po lewej stronie, a podłączanego urządzenia po prawej.

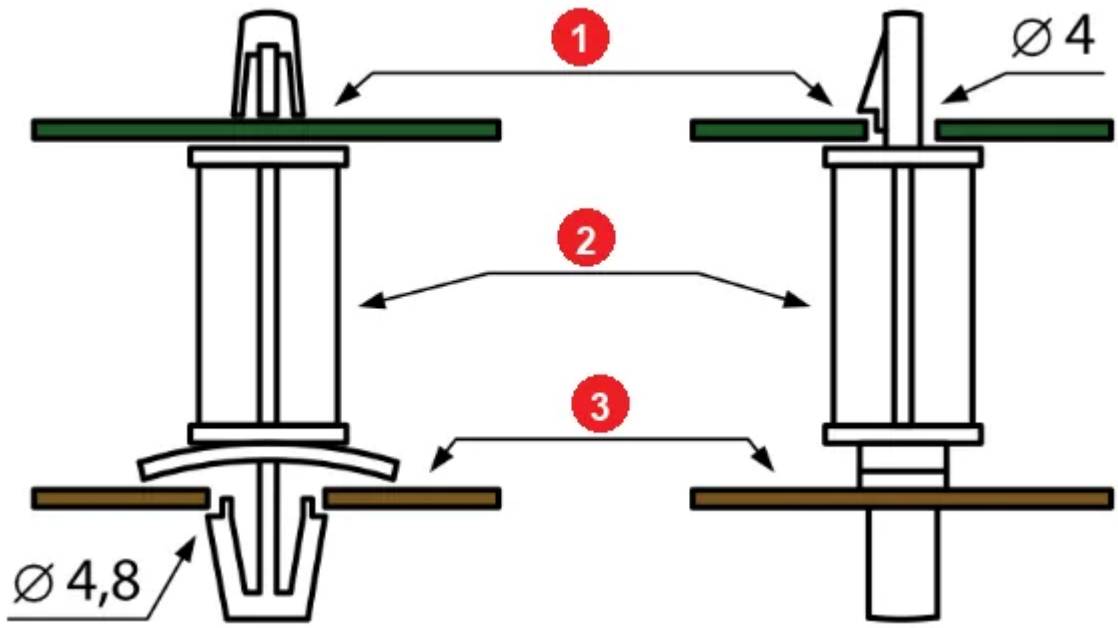
3.1 Zalecana kolejność instalacji

Zaprojektowanie systemu:

- Naszkicuj plan pomieszczeń i zaznacz, gdzie będzie obudowa centrali, manipulator lub manipulatory, sygnalizatory akustyczne i optyczne oraz urządzenia sterowane przez centralę automatycznie lub zdalnie.
- Na podstawie miejsca, potrzeb ochrony i właściwości branych pod uwagę czujek określ liczbę, typ i miejsce czujek.

3.1.1 Montaż płytki w obudowie

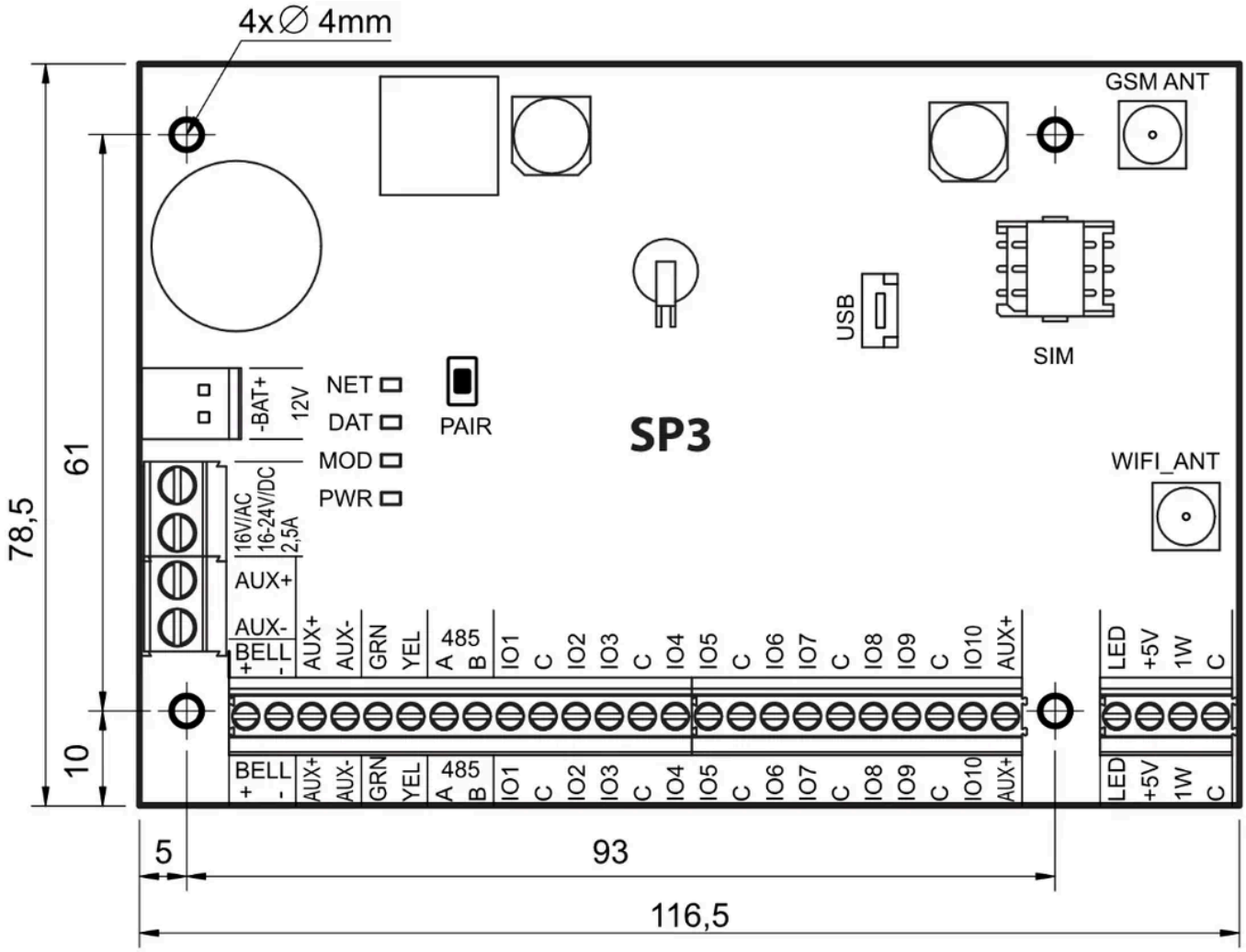
Płytka jest przeznaczona do obudowy, w której jest już transformator obniżający (z bezpiecznikiem 500 mA) i miejsce na akumulator rezerwowy. Płytkę zamocuj w wybranej obudowie z tworzywa lub metalu za pomocą **plastikowych dystansów**; **metalową obudowę trzeba uziemić**. Obudowa musi spełniać wymagania norm EN 60950 i EN 50131.



Rysunek 5. Mocowanie płytki plastikowym dystansem (po lewej widok z przodu – „Front view", po prawej widok z boku – „Side view"). Otwór w płytce Ø4 mm, otwór w obudowie Ø4,8 mm.

- 1 płytka drukowana SP3 („SP3 circuit board")
- 2 dystans („Spacer")
- 3 obudowa („Box housing")

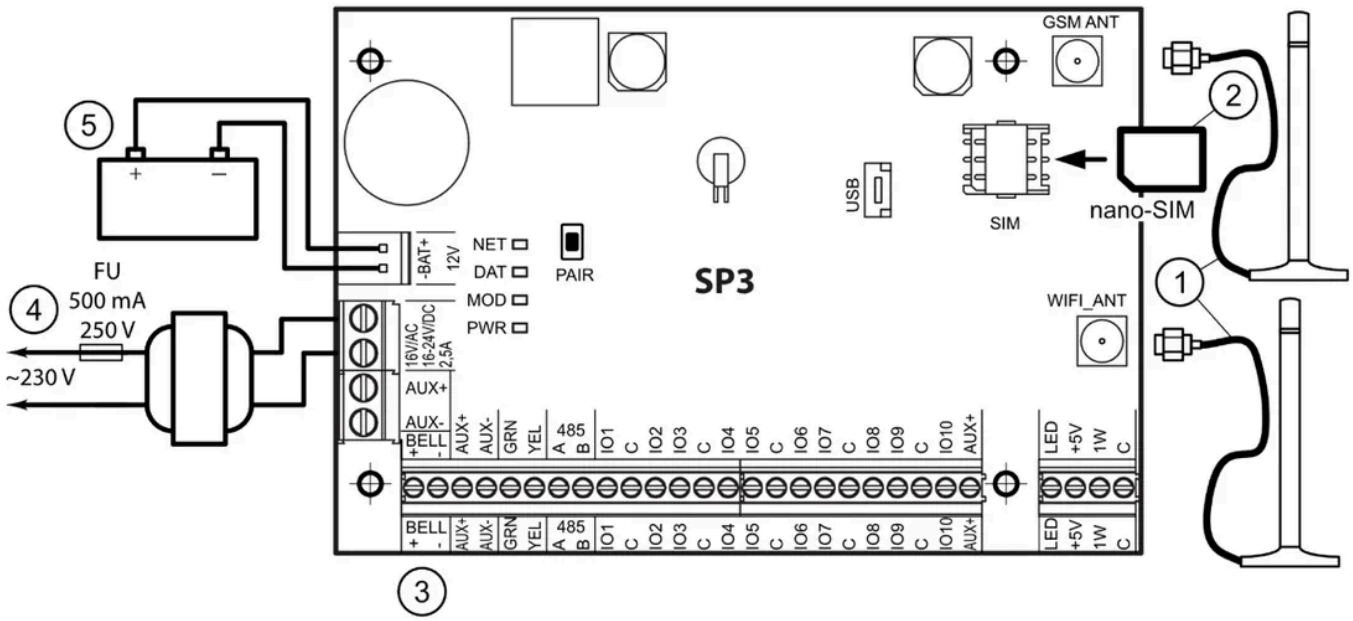
Wymiary płytki to 116,5 × 78,5 mm. Środki czterech otworów mocujących Ø4 mm są oddalone od siebie o 93 mm w poziomie i 61 mm w pionie; lewe otwory są 5 mm od lewej krawędzi, dolne 10 mm od dolnej krawędzi.



Rysunek 6. Wymiary płytki i otworów mocujących w milimetrach.

3.1.2 Kolejność podłączania urządzeń

Urządzenia podłączaj w poniższej kolejności; zasilanie i akumulator zawsze na końcu.



Rysunek 7. Przegląd zasilania i połączeń. Zasilanie sieciowe: transformator ~230 V / 16 V, 40 VA, 50 Hz („Transformer"; po stronie 230 V z bezpiecznikiem 500 mA, 250 V) lub zasilacz napięcia stałego 16–24 V, 2,5 A („or DC power supply source 16-24 V, 2,5 A"); akumulator rezerwowy („Battery"), 12 V, 7 Ah.

- 1 antena GSM i Wi-Fi na złącza antenowe
- 2 karta nano-SIM do gniazda SIM
- 3 urządzenia do zewnętrznej listwy zaciskowej
- 4 zasilanie sieciowe do zacisków AC/DC
- 5 akumulator do zacisków BAT+ / BAT−

1. Przykręć **antenę GSM** i **antenę Wi-Fi** do złączy antenowych (zależnie od wersji jedną lub obie, punkt 1.2).
2. W wersji z modemem włóż do gniazda **aktywowaną kartę nano-SIM**. Żądanie PIN warto wcześniej wyłączyć w telefonie.
3. W wersji z Ethernetem (SP3_3E, SP3_44E) włóż **kabel LAN** do gniazda RJ45.
4. Na podstawie zamieszczonych tu schematów podłączeń, własnych schematów podłączanych urządzeń i projektu podłącz czujki otwarcia drzwi i okien, czujki ruchu, pożarowe i inne, sygnalizatory akustyczne i optyczne, manipulatory i sterowane urządzenia. Do zacisków płytki podłącz też **wyłącznik sabotażowy** otwarcia drzwiczek obudowy i oderwania jej od ściany.
5. Podłącz przewody zasilacza sieciowego do zacisków **AC/DC** płytki i włącz zasilanie. Centrala rozpoznaje manipulatory, ekspandery i moduły pośredniczące prawidłowo podłączone do magistrali 1-WIRE i YEL/GRN.
6. Włóż akumulator do obudowy i podłącz jego końcówki do zacisków **BAT+ / BAT−**.

Akumulator musi naładować się w ciągu 72 godzin, aby system spełniał 2. stopień zabezpieczenia (Grade 2), i w ciągu 24 godzin dla 3. stopnia (Grade 3).

Listwę zaciskową można zdjąć: dzięki temu urządzenie można jednym ruchem odłączyć od zasilania lub zrestartować, łatwiej się nim posługiwać podczas podłączania, a do programowania przez USB można je zanieść do komputera.

Zalecaną kolejność ustawień (partycje, strefy, użytkownicy, czas, transmisja, sterowanie zdalne, zmiana kodów) podsumowuje punkt 2.4, szczegóły rozdział 6.

3.2 Podłączenie czujek

Na płytce **10 zacisków IO** (IO1–IO10) przyjmuje obwody czujek. Fabrycznie IO1–IO9 to wejścia, a IO10 to wyjście PGM (reset czujek pożarowych, zobacz 3.3). Liczbę wejść można zwiększyć ekspanderami (iO, iO-8, iO-WL, RF-SH, iO-LORA, iO8-LORA) maksymalnie do 64. Każdy zacisk można ustawić jako wejście (strefę), a na stronie **Zones** (6.7) można ustawić właściwości strefy: typ obwodu (**NO, NC, EOL, EOL_T, 3EOL, ATZ, ATZ_T**), czułość na krótkotrwałe zdarzenia w obwodzie oraz funkcję strefy (opóźniona, natychmiastowa, natychmiastowa stay, nadążna, nadążna stay, pożarowa, stacyjka (keyswitch), 24-godzinna, cicha, cicha 24-godzinna). Ekspandery iO-8 i iO8-LORA obsługują wszystkie typy obwodów centrali.

Rezystory końca linii. Dla obwodów EOL, EOL_T, 3EOL, ATZ i ATZ_T możesz w TrikdisConfig wybrać jeden z siedmiu zestawów rezystorów (**System Options → System general → EOL Type**, 6.2.1), dlatego przy wymianie starej centrali w czujkach mogą zostać dotychczasowe rezystory. RT to rezystor obwodu sabotażowego, R1 pierwszej, a R2 drugiej czujki (przy 3EOL – obwodu maskowania). Obok zestawu wymienione są centrale alarmowe, których fabryczne wartości rezystorów są z nim zgodne:

Zestaw	RT	R1	R2
1 – domyślny Trikdis: Bosch AMAX, Risco LightSYS Plus, Satel INTEGRA (EOL)	**2,2 kΩ**	**2,2 kΩ**	**4,7 kΩ**
2 – Paradox, Honeywell Galaxy Flex, Hikvision AX Hybrid PRO (3EOL)	1 kΩ	1 kΩ	2,2 kΩ
3 – DSC PowerSeries, Eldes ESIM364	5,6 kΩ	5,6 kΩ	3,3 kΩ
4 – Eldes ESIM364 (tryb 6 stref, z sabotażem)	5,6 kΩ	3,3 kΩ	5,6 kΩ
5	3,3 kΩ	6,8 kΩ	3,3 kΩ
6 – Crow Runner, Texecom Premier Elite, Pyronix Enforcer	2,2 kΩ	4,7 kΩ	8,2 kΩ
7	4,7 kΩ	4,7 kΩ	2,2 kΩ

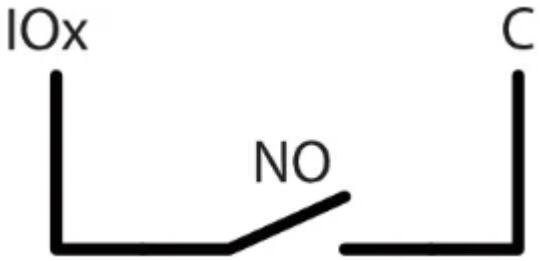
Przy wymienionych markach zgodne są rezystor sabotażowy i rezystor czujki (RT, R1), a przy Satel INTEGRA – podłączenie z jednym rezystorem (EOL). Przy podwajaniu stref (ATZ) i podłączeniu 3EOL zgodny musi być także R2: dotyczy to zestawu 2 dla Paradox i Hikvision AX Hybrid PRO, zestawu 3 dla Eldes ESIM364 i zestawu 6 dla Crow Runner. Tam, gdzie w starej centrali wartość rezystora była ustawiana (na przykład Crow, Risco, Honeywell Galaxy, Pyronix, Texecom), decyduje rezystor w czujkach. Podłączenie Honeywell VISTA (2 kΩ) i dwurezystorowe podłączenie Satel (2EOL, 2 × 1,1 kΩ) nie jest zgodne z żadnym zestawem.

3.2.1 Schematy podłączeń

Na rysunkach **IOx** to wybrany zacisk IO, **C** to wspólny zacisk ujemny; NC to styk normalnie zamknięty, NO normalnie otwarty.

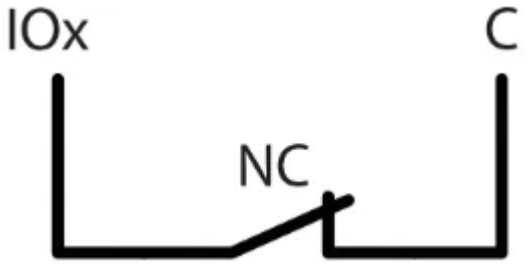
Oznaczenia na rysunkach. R1, R2, RT – rezystor; RT to rezystor obwodu sabotażowego. Czerwone **T** oznacza styk sabotażowy, niebieska liczba – numer czujki; znaczenie każdego oznaczenia podano też pod danym rysunkiem.

NO – normalnie otwarty, bez rezystora końca linii. Czujka po zadziałaniu zamyka obwód między IOx a C.



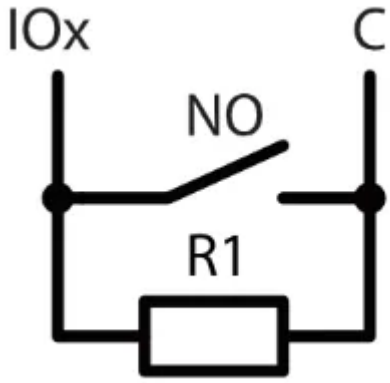
Rysunek 8. Strefa NO: styk normalnie otwarty między zaciskami IOx i C.

NC – normalnie zamknięty, bez rezystora końca linii. Czujka po zadziałaniu przerywa obwód między IOx a C.

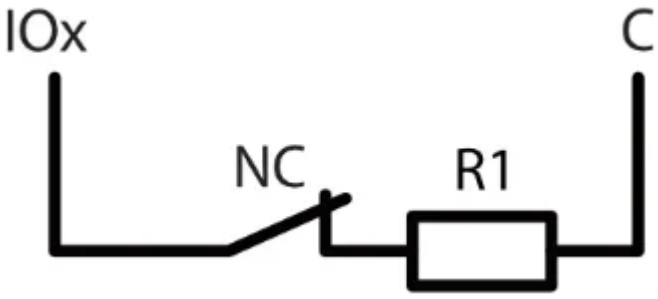


Rysunek 9. Strefa NC: styk normalnie zamknięty między zaciskami IOx i C.

EOL – z rezystorem końca linii. Przy czujce NO rezystor R1 jest równolegle do styku, przy czujce NC szeregowo z nim, między IOx a C; dzięki temu centrala wykrywa także przerwanie i zwarcie przewodu.

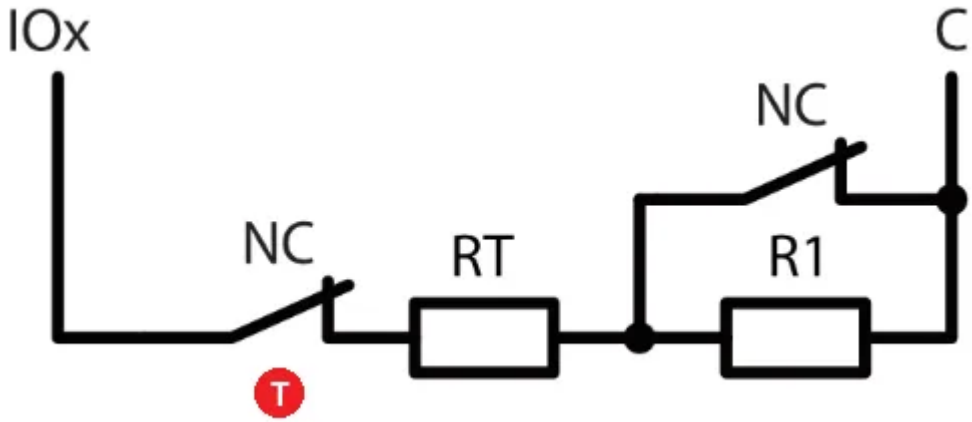


Rysunek 10. Strefa NO z rezystorem końca linii (EOL): R1 równolegle do otwartego styku, między IOx a C.



Rysunek 11. Strefa NC z rezystorem końca linii (EOL): R1 szeregowo z zamkniętym stykiem, między IOx a C.

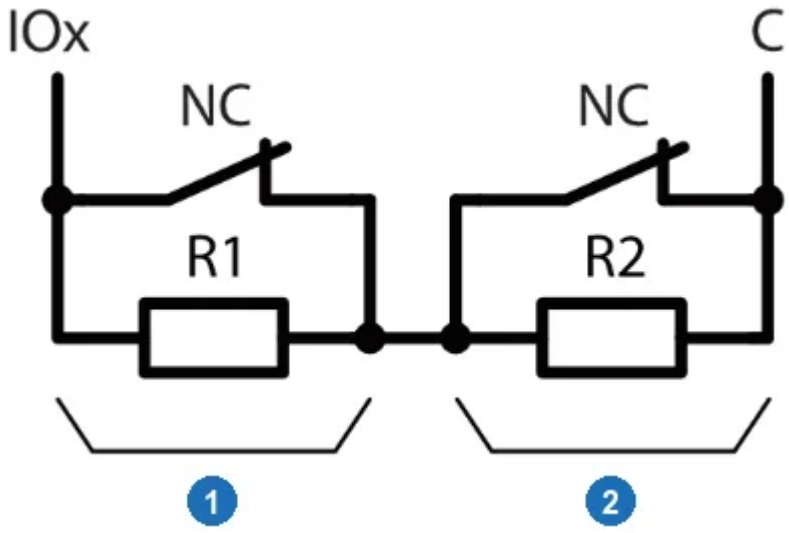
EOL_T – z rezystorem końca linii, z wykrywaniem sabotażu i uszkodzenia przewodu. Od IOx szeregowo styk sabotażowy NC i RT, następnie styk alarmowy NC równolegle z R1 między RT a C.



Rysunek 12. Strefa EOL_T: IOx → styk sabotażowy NC → RT → (styk alarmowy NC równolegle z R1) → C.

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

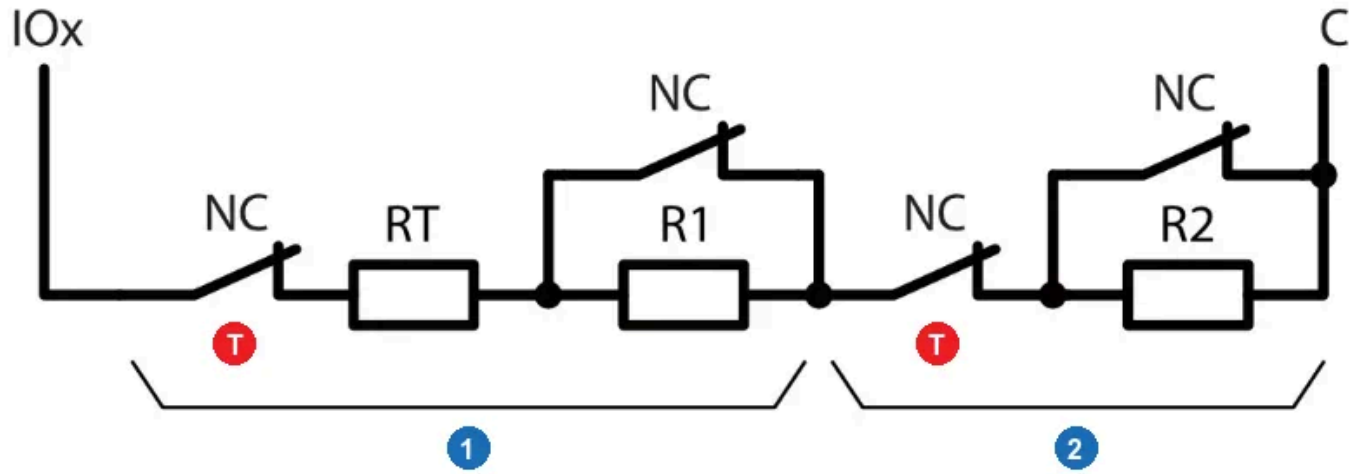
ATZ – podwajanie stref. Dwie czujki na jednym zacisku: między IOx a C szeregowo dwa obwody, w pierwszym styk NC równolegle z R1, w drugim styk NC równolegle z R2. Dzięki temu na 10 zaciskach można obsłużyć 20 stref.



Rysunek 13. Strefa ATZ: styk NC 1. czujki równolegle z R1, szeregowo z nim styk NC 2. czujki równolegle z R2, między IOx a C.

- 1 obwód 1. czujki („Detector terminal 1")
- 2 obwód 2. czujki („Detector terminal 2")

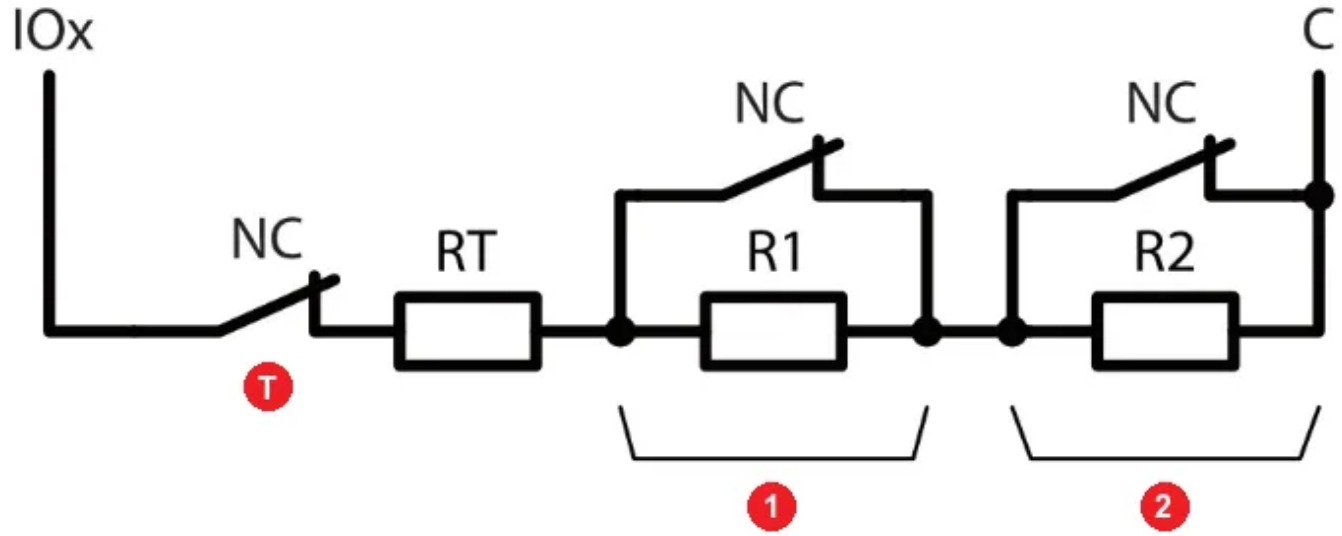
ATZ_T – podwajanie stref z wykrywaniem sabotażu i uszkodzenia przewodu. Jak ATZ, ale w obwodzie obu czujek szeregowo jest też styk sabotażowy NC, w pierwszym obwodzie razem z rezystorem RT.



Rysunek 14. Strefa ATZ_T: 1. czujka – styk sabotażowy NC i RT szeregowo, następnie styk NC równolegle z R1; 2. czujka – styk sabotażowy NC szeregowo, następnie styk NC równolegle z R2; oba obwody szeregowo między IOx a C.

- T styk sabotażowy („Tamper"), sygnalizuje otwarcie obudowy czujki
- 1 obwód 1. czujki („Detector terminal 1")
- 2 obwód 2. czujki („Detector terminal 2")

3EOL – trzy rezystory końca linii: alarm, sabotaż i maskowanie. W obrębie jednej czujki obwód sabotażowy, alarmowy i antymaskingowy (anti-masking) można rozpoznać oddzielnie.

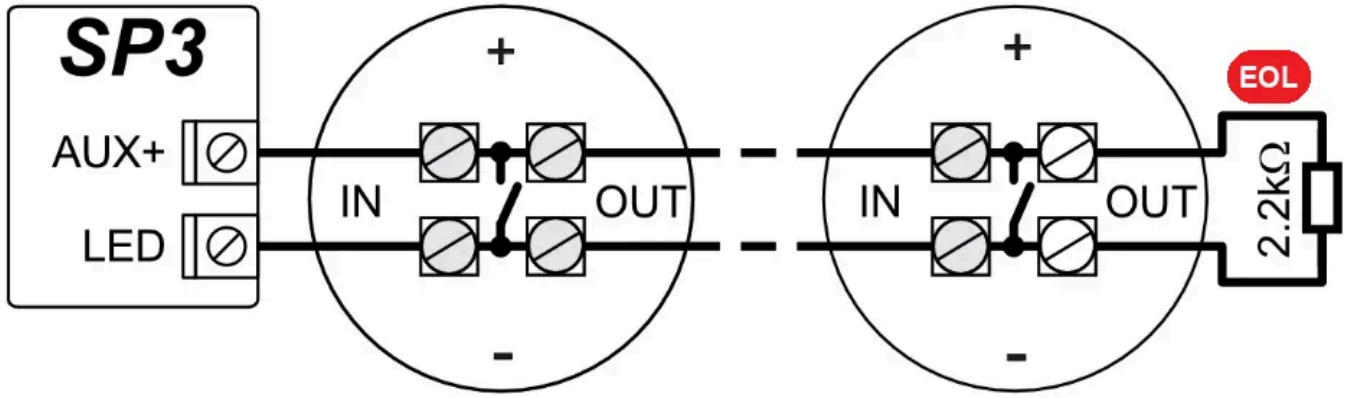


Rysunek 15. Strefa 3EOL: IOx → styk sabotażowy NC i RT szeregowo → obwód alarmowy (styk NC równolegle z R1) → obwód maskowania (styk NC równolegle z R2) → C.

- T styk sabotażowy („Tamper"), sygnalizuje otwarcie obudowy czujki
- 1 obwód alarmowy („Alarm")
- 2 obwód antymaskingowy („Anti-masking"), sygnalizuje zasłonięcie czujki

3.3 Podłączenie czujek dymu

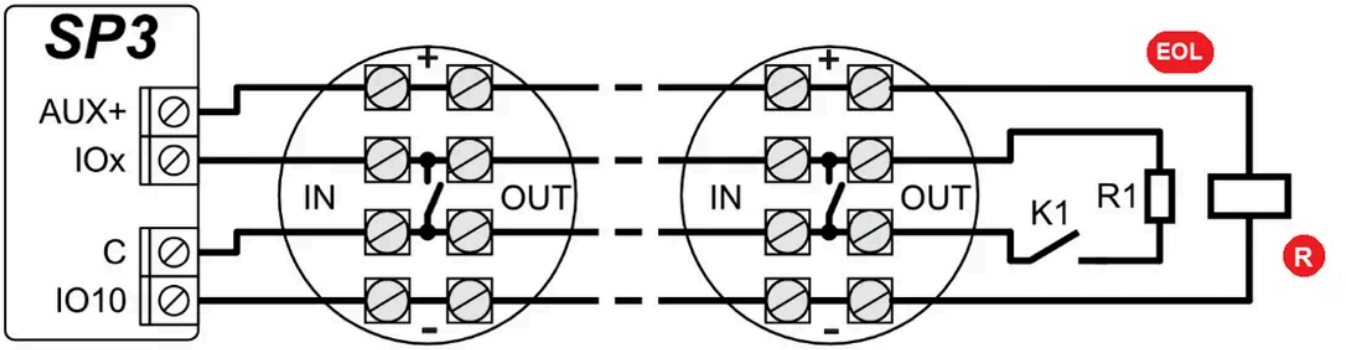
Dwuprzewodowe czujki dymu na wyjściu LED. Jeśli podłączasz czujki pożarowe w ten sposób, na stronie **System Options** zaznacz pole **LED out as 2Wire fire** (6.2).



Rysunek 16. Dwuprzewodowe czujki dymu na wyjściu LED: AUX+ → zacisk + IN pierwszej czujki, LED → − IN; zaciski + OUT i − OUT każdej czujki do tego samego zacisku IN następnej czujki; za ostatnią czujką rezystor końca linii 2,2 kΩ między przewodem + i −.

- EOL rezystor końca linii 2,2 kΩ („End of line resistor")

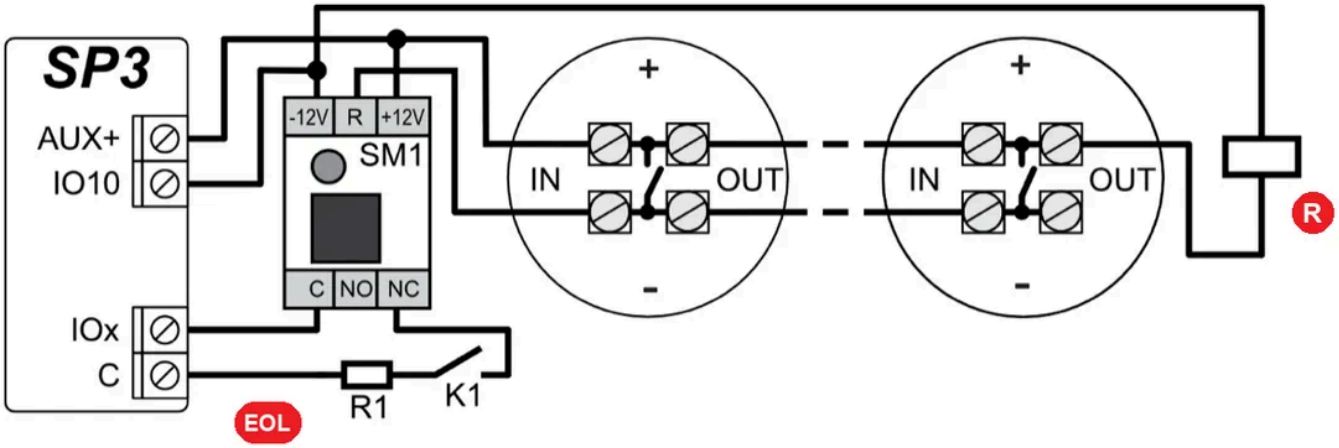
Czteroprzewodowe czujki dymu. Wejściu obwodu czujek dymu (IOx) przypisz funkcję strefy **pożarowa** (6.7). Zasilanie czujek czteroprzewodowych przełącza wyjście PGM IO10, do którego należy funkcja **Fire Sensor Reset** (reset czujek pożarowych) (6.8) – to ustawienie fabryczne IO10. Przekaźnik K1 sygnalizuje przerwanie przewodu i usunięcie czujki.



Rysunek 17. Czteroprzewodowe czujki dymu z przekaźnikiem K1. Od góry do dołu: AUX+ → zacisk + pierwszej czujki, IOx → górny styk, C → dolny styk, IO10 → − IN; cztery zaciski OUT do tego samego zacisku IN następnej czujki; za ostatnią czujką styk K1 i rezystor końca linii R1 szeregowo między przewodem IOx i C; cewka K1 między przewodem AUX+ i IO10.

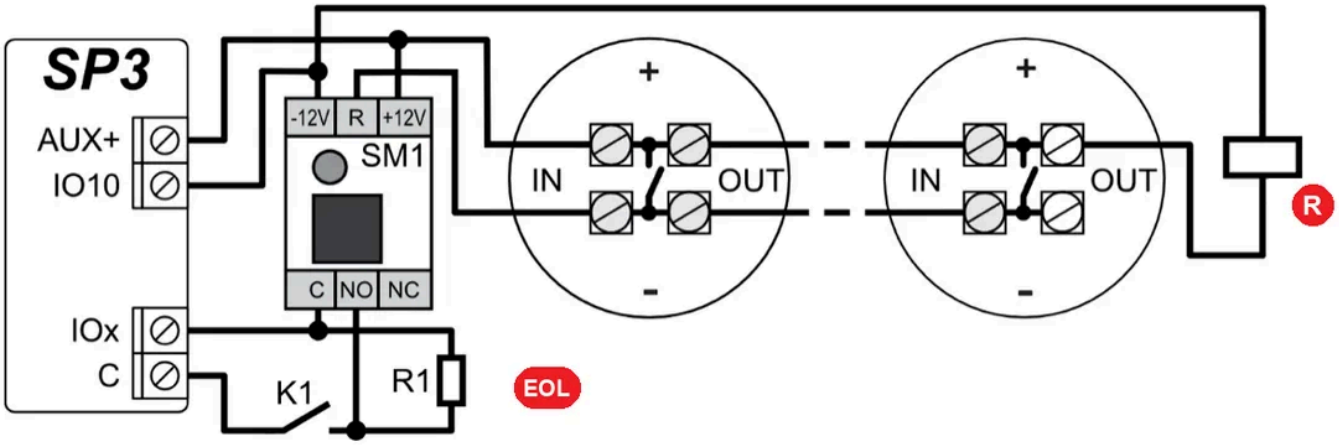
- R przekaźnik **K1** („Relay")
- EOL rezystor końca linii **R1** („End of line resistor")

Dwuprzewodowe czujki dymu z modułem SM1. Z modułem SM1 czujki dwuprzewodowe można podłączyć do jednego wejścia IO; przekaźnik K1 również tutaj sygnalizuje przerwanie przewodu i usunięcie czujki. Obwód nadzoru można wykonać na dwa sposoby:



Rysunek 18. Dwuprzewodowe czujki dymu z modułem SM1: AUX+ → SM1 +12V i + IN pierwszej czujki; IO10 → SM1 −12V i cewka K1; SM1 R → − IN czujki; zaciski IN/OUT czujek połączone łańcuchowo, ostatni + OUT do K1. Obwód nadzoru: IOx → SM1 C; zacisk C SP3 → rezystor końca linii R1 → styk K1 → SM1 NC.

- R przekaźnik **K1** („Relay")
- EOL rezystor końca linii **R1** („End of line resistor")

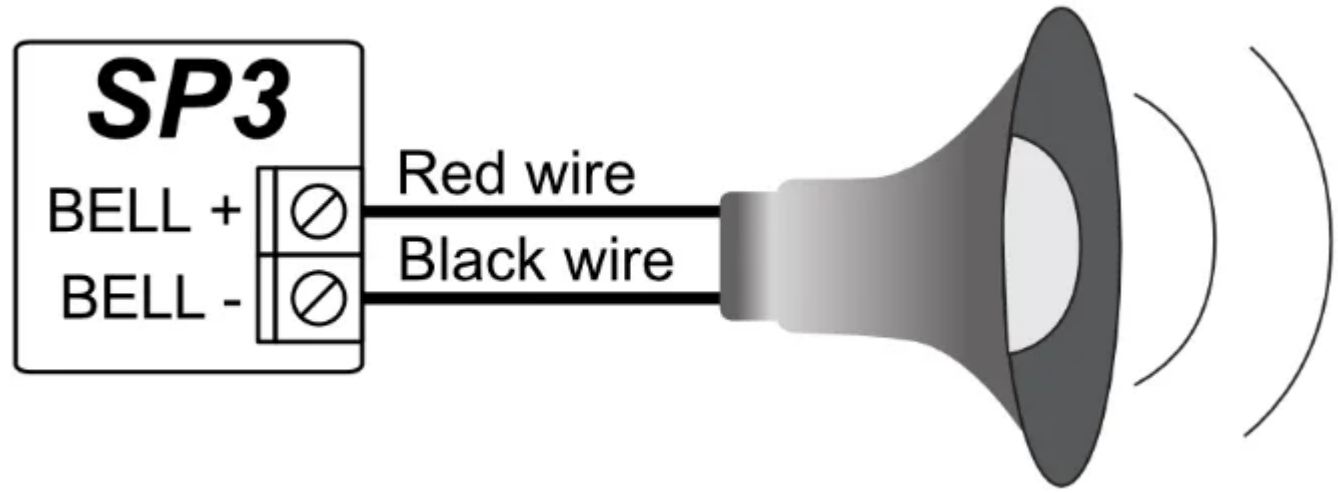


Rysunek 19. To samo z drugim obwodem nadzoru: R1 między zaciskami C i NO modułu SM1; zacisk C SP3 przez styk K1 do zacisku NO modułu SM1.

- R przekaźnik **K1** („Relay")
- EOL rezystor końca linii **R1** („End of line resistor")

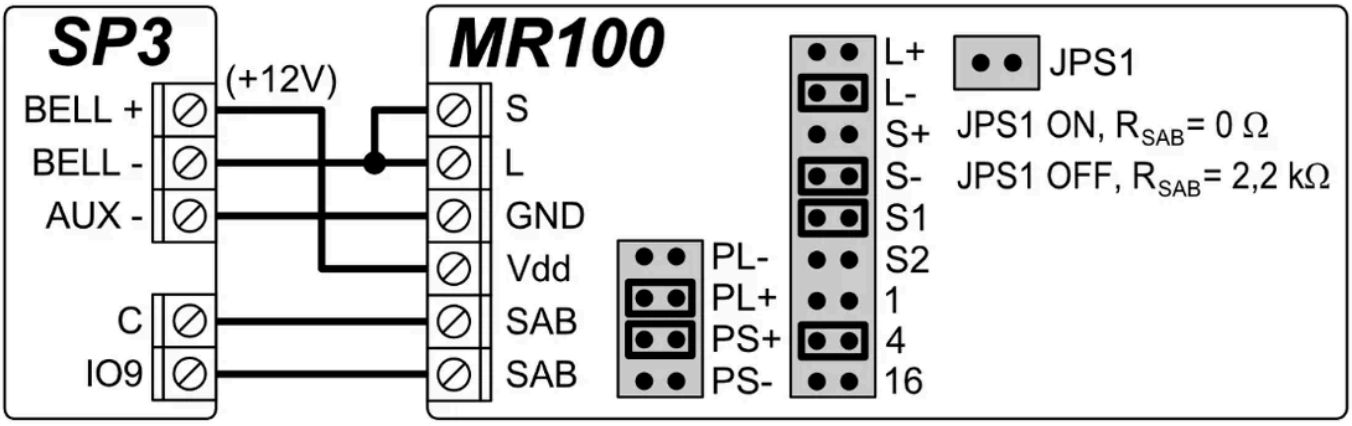
3.4 Podłączenie sygnalizatora

Sygnalizator podłącz do wyjścia **BELL+ / BELL−** (obciążalność wyjścia BELL to 1 A, zobacz dane techniczne w punkcie 1.3).



Rysunek 20. Sygnalizator na wyjściu BELL: BELL+ → przewód czerwony, BELL− → przewód czarny.

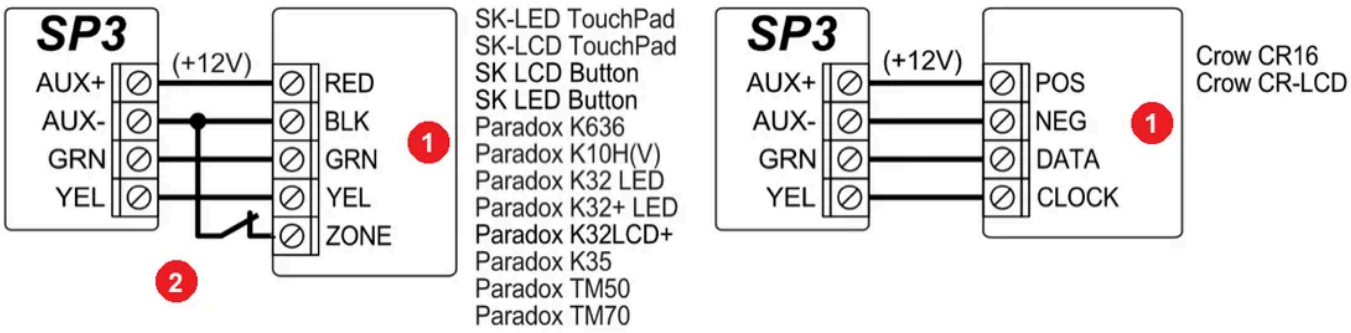
Przy zewnętrznym sygnalizatorze MR100 centrala nadzoruje także obwód sabotażowy (SAB): fabrycznie z rezystorem EOL 2,2 kΩ, na wejściu **IO9**. IO9 jest fabrycznie strefą 24-godzinną, ale można to dowolnie zmienić. Jeśli obwód sabotażowy sygnalizatora monitorujesz w centrali innym trybem EOL, zewrzyj styki JPS1 i włącz w obwód sabotażowy szeregowo rezystor o odpowiedniej wartości.



Rysunek 21. Sygnalizator zewnętrzny MR100 („Outdoor siren"): BELL+ (+12 V) → Vdd, BELL− → S i L, AUX− → GND, C i IO9 → dwa zaciski SAB (sabotaż). Punkty zwarte na rysunku: PL+, PS+, L−, S−, S1 i 4. JPS1 zwarte („ON"): R_SAB = 0 Ω, JPS1 rozwarte („OFF"): R_SAB = 2,2 kΩ.

3.5 Podłączenie manipulatorów i czytników RFID

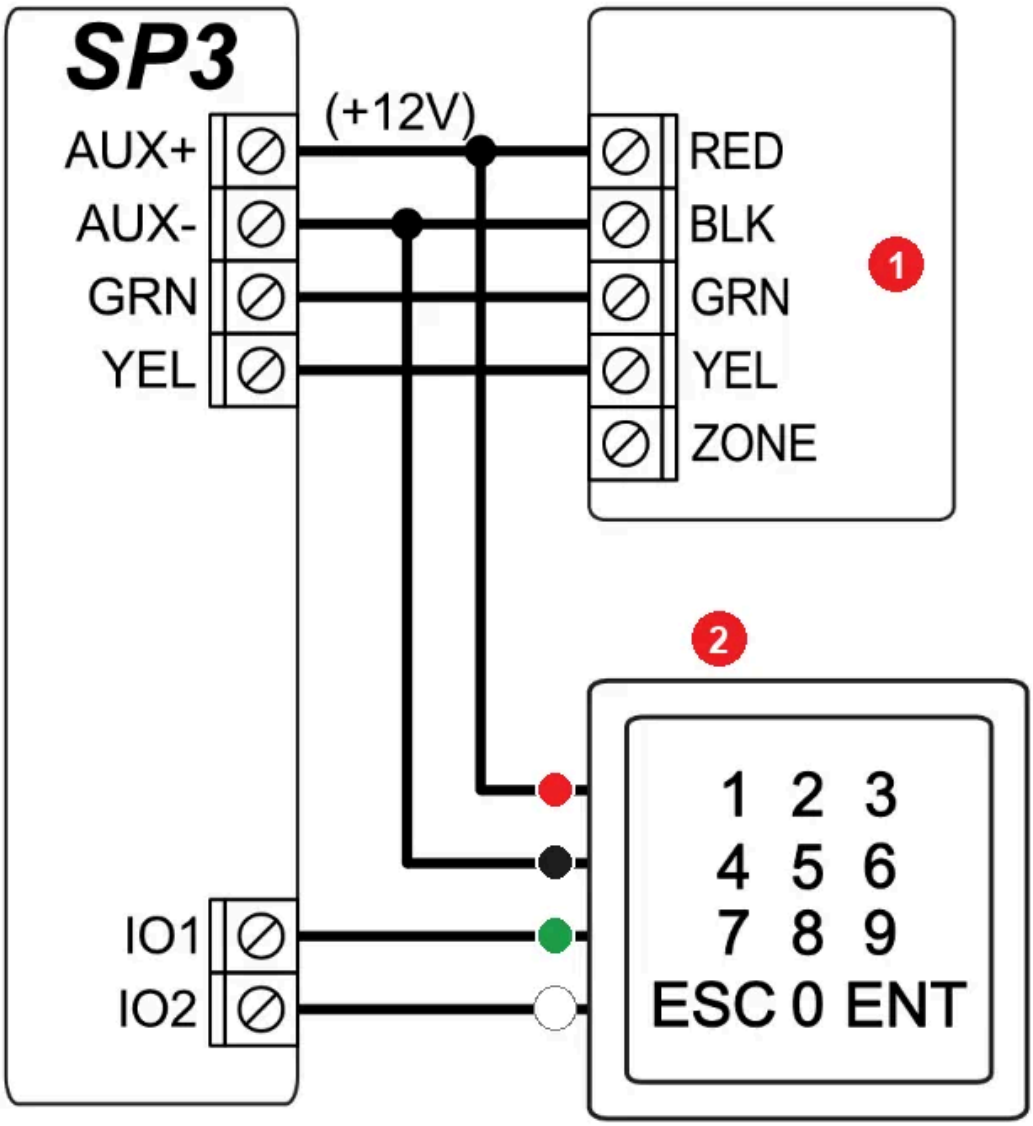
Należą tu manipulatory na magistrali manipulatorów i czytniki RFID z protokołem Wiegand 26/34. Do magistrali manipulatorów (**GRN**, **YEL**) można podłączyć maksymalnie **8 manipulatorów tego samego typu**. Typ manipulatora ustaw na stronie **Modules** (6.5); podłączone urządzenia centrala automatycznie rozpoznaje i przypisuje. Manipulator ma też własne wejście strefowe (ZONE): drugi koniec podłączonej tu czujki idzie do zacisku AUX−. Obsługę systemu z manipulatorów (kody użytkowników, blokowanie stref, iButton i RFID, połączenie, SMS, wyjścia PGM) opisuje osobna instrukcja użytkownika SP3 przygotowana dla manipulatorów Protegus i Paradox.



Rysunek 22. Podłączenie manipulatorów. SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button oraz Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50, TM70: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; zacisk ZONE manipulatora przez styk czujki do zacisku AUX−. Crow CR16 i CR-LCD: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK.

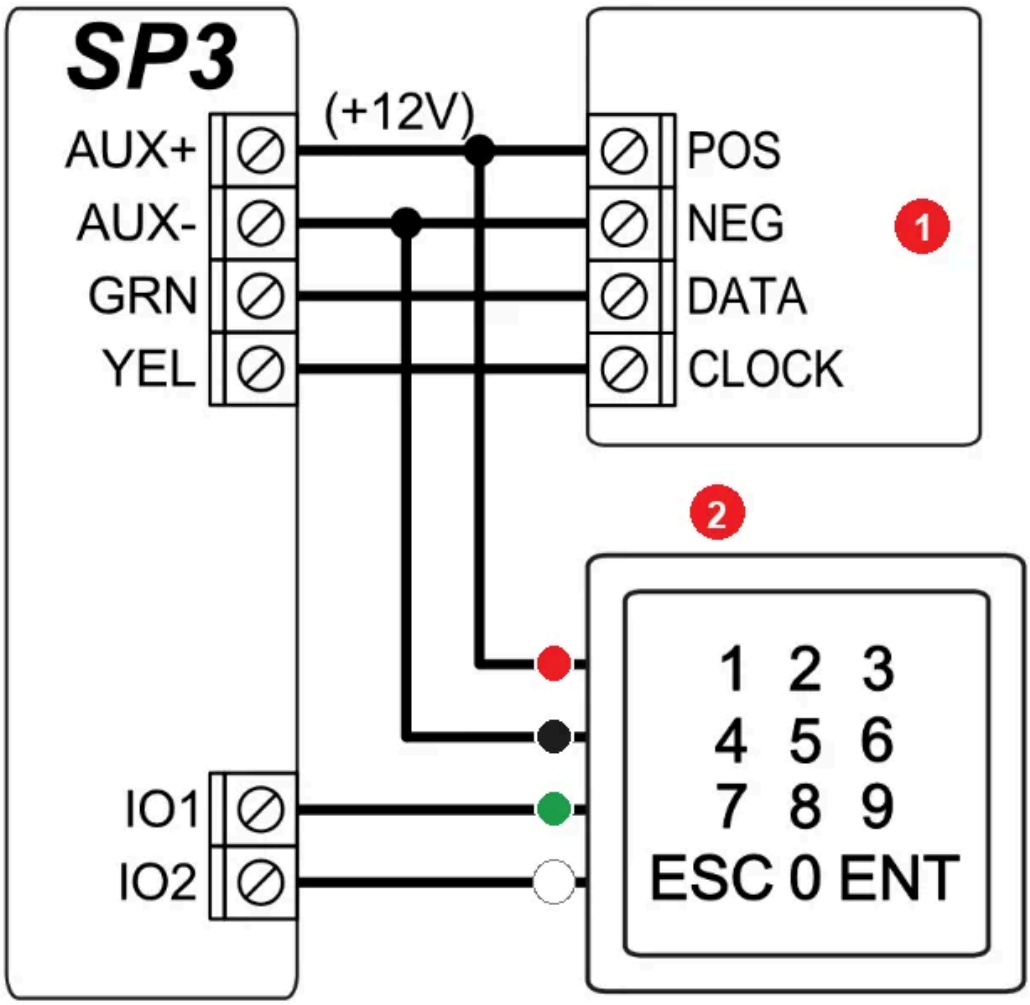
- 1 manipulator („Keypad")
- 2 strefa manipulatora („Keypad zone")

Czytnik RFID (Wiegand 26/34). Do centrali można podłączyć maksymalnie **2 czytniki**. Przewody danych czytnika (D0, D1) podłącza się albo do magistrali manipulatorów (GRN, YEL), albo do zacisków **IO1** i **IO2**, zgodnie z rysunkami. Jeśli są dwa czytniki (strona wejścia i wyjścia), do centrali nie można już podłączyć manipulatora.



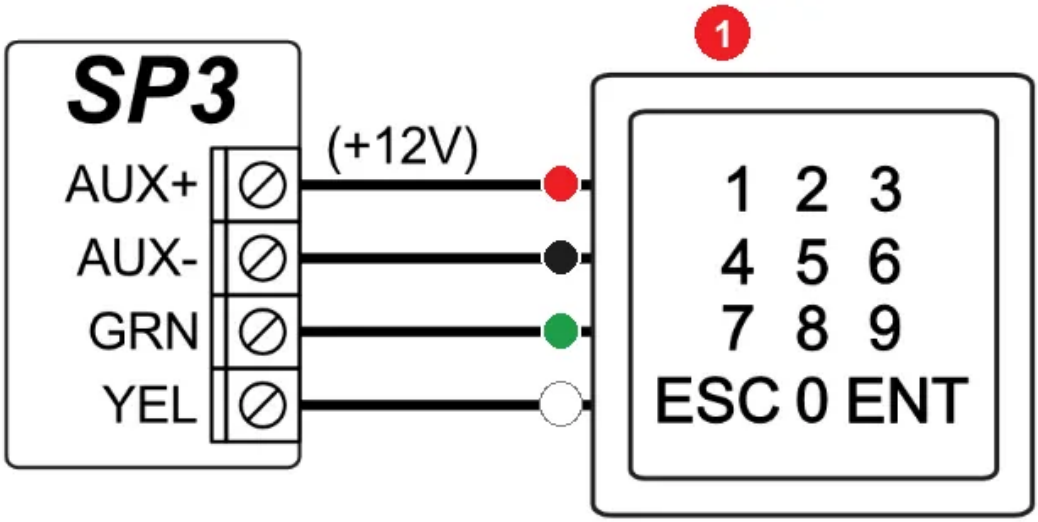
Rysunek 23. Manipulator i czytnik wejściowy razem. Manipulator (SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50 lub TM70) na magistrali zgodnie z poprzednim rysunkiem: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; przewód czerwony czytnika (+U) → AUX+, czarny (GND) → AUX−, zielony (D0) → IO1, biały (D1) → IO2.

- 1 manipulator („Keypad”)
- 2 czytnik wejściowy: czytnik RFID z klawiaturą, Wiegand 26/34 („Entry reader”, „RFID reader with keypad (Wiegand 26/34)”)
- przewód czerwony, +U („R - red wire (+U)”)
- przewód czarny, GND („B - black wire (GND)”)
- przewód zielony, D0 („G - green wire (D0)”)
- przewód biały, D1 („W - white wire (D1)”)



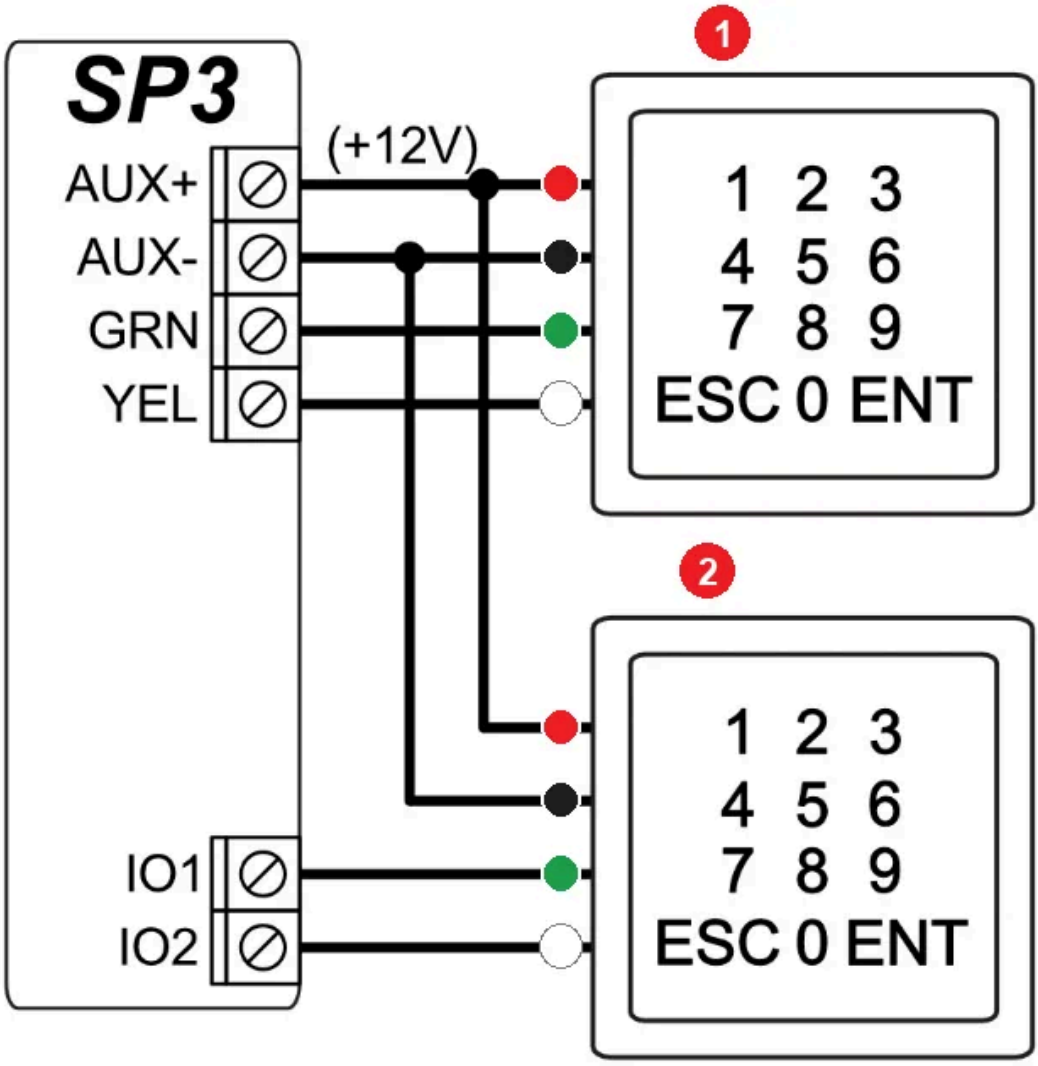
Rysunek 24. Manipulator Crow CR16 lub Crow CR-LCD i czytnik wejściowy razem. Manipulator na magistrali: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK; przewód czerwony czytnika (+U) → AUX+, czarny (GND) → AUX−, zielony (D0) → IO1, biały (D1) → IO2.

- 1 manipulator („Keypad")
- 2 czytnik wejściowy: czytnik RFID z klawiaturą, Wiegand 26/34 („Entry reader", „RFID reader with keypad (Wiegand 26/34)")
- przewód czerwony, +U („R - red wire (+U)")
- przewód czarny, GND („B - black wire (GND)")
- przewód zielony, D0 („G - green wire (D0)")
- przewód biały, D1 („W - white wire (D1)")



Rysunek 25. Jeden czytnik na magistrali manipulatorów, bez manipulatora: przewód czerwony czytnika (+U) → AUX+, czarny (GND) → AUX−, zielony (D0) → GRN, biały (D1) → YEL.

- 1 czytnik wejściowy: czytnik RFID z klawiaturą, Wiegand 26/34 („Entry reader", „RFID reader with keypad (Wiegand 26/34)")
- przewód czerwony, +U („R - red wire (+U)")
- przewód czarny, GND („B - black wire (GND)")
- przewód zielony, D0 („G - green wire (D0)")
- przewód biały, D1 („W - white wire (D1)")



Rysunek 26. Dwa czytniki, oba to czytniki RFID z klawiaturą, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)"). Czytnik wejściowy: przewód czerwony (+U) → AUX+, czarny (GND) → AUX−, zielony (D0) → GRN, biały (D1) → YEL. Czytnik wyjściowy: czerwony (+U) → AUX+, czarny (GND) → AUX−, zielony (D0) → IO1, biały (D1) → IO2.

- 1 czytnik wejściowy („Entry reader")
- 2 czytnik wyjściowy („Exit reader")
- przewód czerwony, +U („R - red wire (+U)")
- przewód czarny, GND („B - black wire (GND)")
- przewód zielony, D0 („G - green wire (D0)")
- przewód biały, D1 („W - white wire (D1)")

3.6 Podłączenie czytników kluczy TM17 i CZ-Dallas

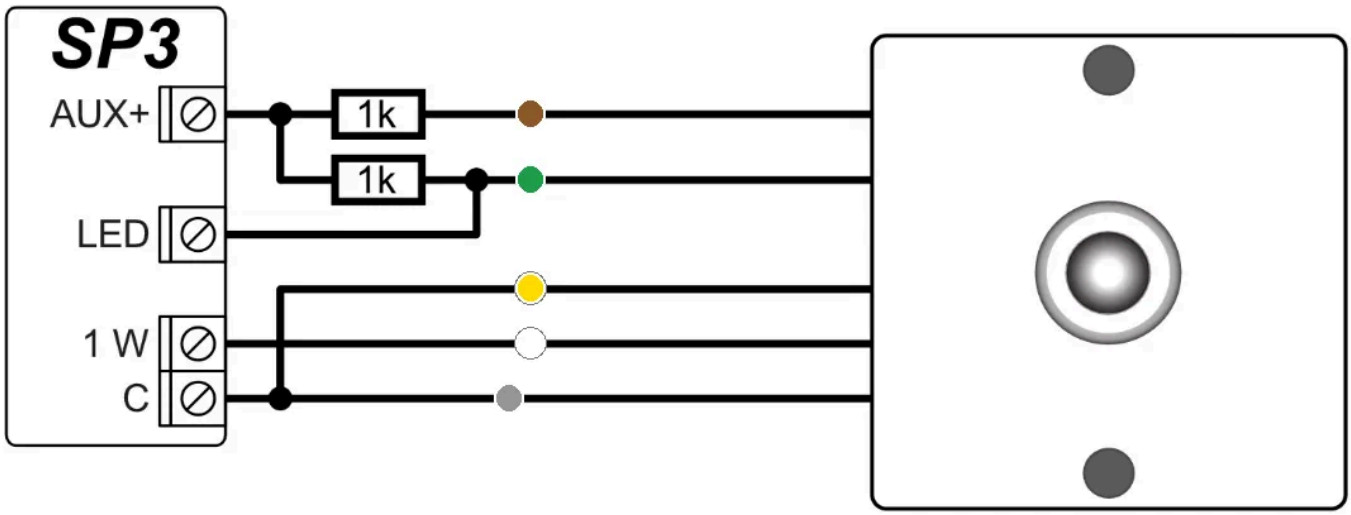
Wycofane akcesorium

Czytnik kluczy iButton **TM17** to wycofane akcesorium, które nie jest już dostępne w sprzedaży. Opis pozostał dla istniejących systemów.

Czytnik kluczy iButton **CZ-Dallas** podłącza się do magistrali **1 WIRE**, przewodem o długości maksymalnie 30 m. Czytnik **TM17** podłącza się do magistrali **RS485**, przewodem o długości maksymalnie 100 m.

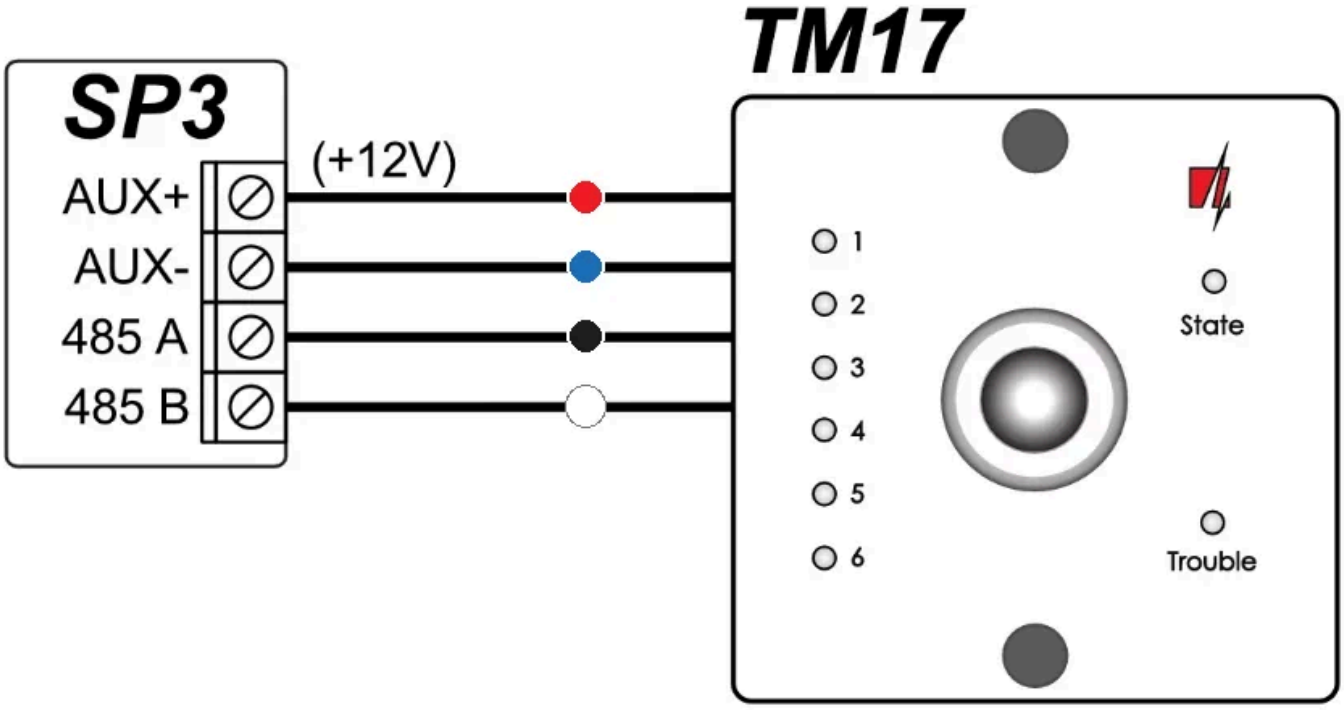
„Maksymalnie 30 m" i „maksymalnie 100 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

Do sygnalizacji świetlnej CZ-Dallas ustaw typ wyjścia **LED** na **System state** (stan systemu) (6.8): przy uzbrojonym systemie pierścień czytnika świeci na czerwono, przy rozbrojonym na żółto.



Rysunek 27. Czytnik CZ-Dallas („CZ-Dallas reader"): AUX+ → każdy osobno przez rezystor 1 kΩ na przewód brązowy (RED LED+) i zielony (GREEN LED+); wyjście LED na przewód zielony, za rezystorem; 1 W → przewód biały; C → przewód żółty (LED−) i szary. Wyjście LED trzeba ustawić na typ **System state** (stan systemu) („The output LED must be set to the »System state« type.") – przy uzbrojonym alarmie światło czytnika iButton jest czerwone („Security alarm system is arm - the iButton reader light is red."), przy rozbrojonym żółte („Security alarm system is disarm - the iButton reader light is yellow.").

- przewód brązowy, RED LED+ („Brown wire", „RED LED+") – światło czerwone
- przewód zielony, GREEN LED+ („Green wire", „GREEN LED+") – światło zielone
- przewód żółty, LED− („Yellow wire", „LED-")
- przewód biały („White wire")
- przewód szary („Gray wire")

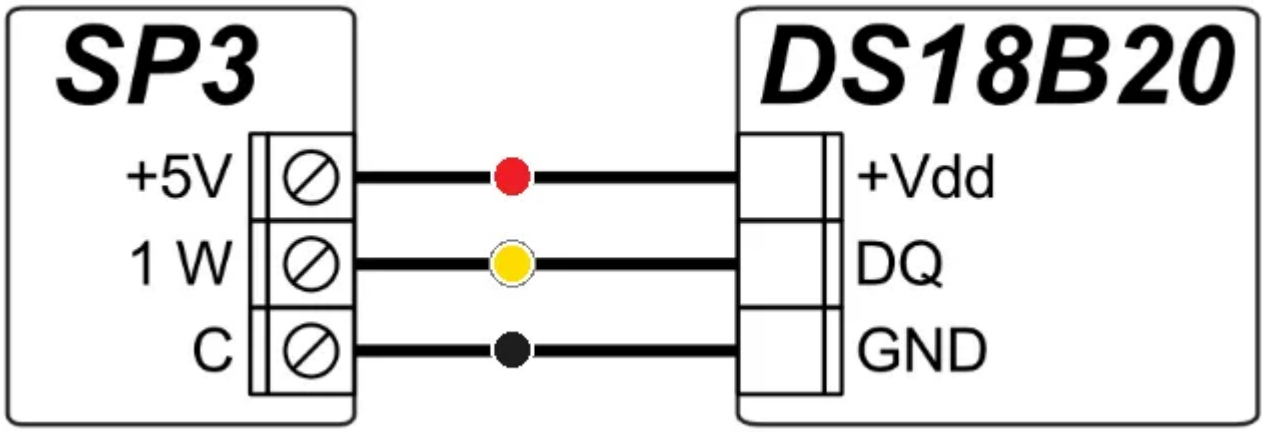


Rysunek 28. Czytnik TM17: AUX+ (+12 V) → przewód czerwony, AUX− → niebieski, 485 A → czarny, 485 B → biały.

- przewód czerwony („Red wire")
- przewód niebieski („Blue wire")
- przewód czarny („Black wire")
- przewód biały („White wire")

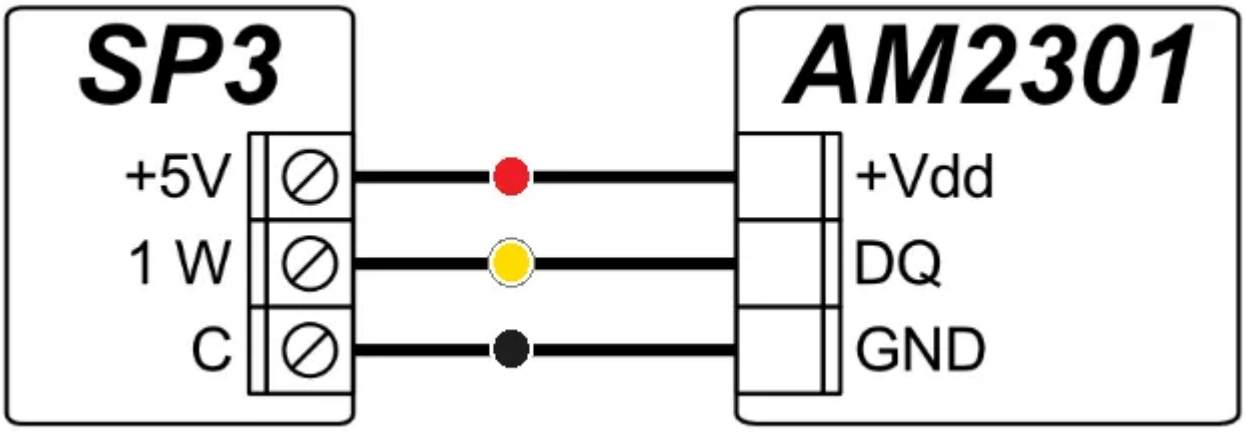
3.7 Podłączenie czujników temperatury

Do magistrali 1 WIRE można podłączyć maksymalnie **8 czujników temperatury Maxim / Dallas DS18S20 lub DS18B20** albo **1 czujnik temperatury i wilgotności AM2301**; centrala automatycznie je rozpoznaje i przypisuje, a wartości są widoczne na stronie **Sensors** (6.9). Przy przewodzie dłuższym niż pół metra użyj kabla ze skrętką (UTP 4×2×0,5 lub STP 4×2×0,5). Zacisk **+5V** płytki zasila urządzenia podłączone do magistrali 1 WIRE: 5 V DC, maks. 0,2 A, z zabezpieczeniem przed przeciążeniem – po przekroczeniu dopuszczalnego prądu wyjście automatycznie się wyłącza.



Rysunek 29. Czujnik temperatury DS18B20 („Temperature sensor"): +5V → +Vdd (czerwony), 1 W → DQ (żółty), C → GND (czarny).

- przewód czerwony („Red wire")
- przewód żółty („Yellow wire")
- przewód czarny („Black wire")

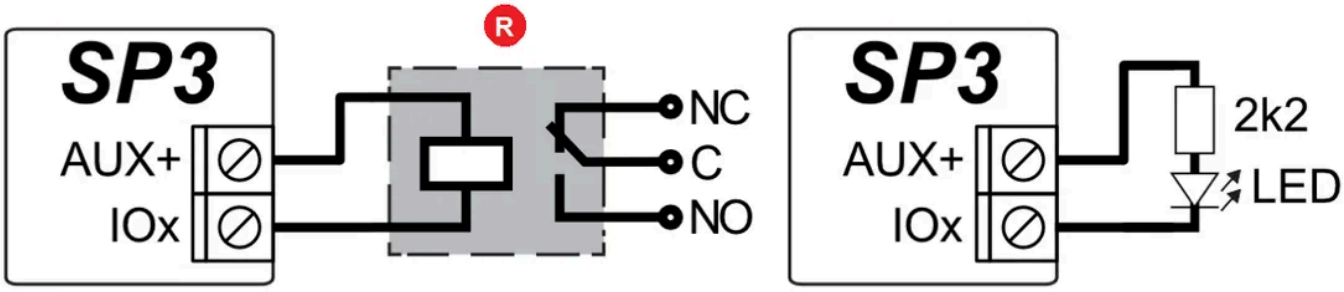


Rysunek 30. Czujnik temperatury i wilgotności AM2301 („Temperature and humidity sensor"): +5V → +Vdd (czerwony), 1 W → DQ (żółty), C → GND (czarny).

- przewód czerwony („Red wire")
- przewód żółty („Yellow wire")
- przewód czarny („Black wire")

3.8 Podłączenie przekaźnika i lampki LED

Stykami przekaźnika można zdalnie przełączać różne urządzenia elektryczne. Wybrany zacisk IO trzeba ustawić jako wyjście (OUT) z funkcją **Remote control** (sterowanie zdalne) (6.8). Wyjście IO jest typu otwarty kolektor, o obciążalności maksymalnie 100 mA, dlatego większy odbiornik zawsze przełączaj przez przekaźnik.



Rysunek 31. Po lewej przekaźnik: cewka między AUX+ a IOx, styki przekaźnika NC, C, NO. Po prawej lampka LED: AUX+ → rezystor 2,2 kΩ → LED → IOx.

- R przekaźnik („Relay")

3.9 Włączenie centrali

Włącz zasilanie sieciowe. Diody LED płytki pokazują (pełna tabela w punkcie 1.6):

- dioda **PWR** miga na zielono – napięcie zasilania jest prawidłowe;
- w wersji z modemem dioda **NET** świeci na zielono i co pewien czas co najmniej trzy razy mignie na żółto – zielony oznacza, że karta SIM połączyła się z siecią komórkową, a liczba żółtych mignięć (0–5) pokazuje siłę sygnału;
- w wersji Wi-Fi dioda **MOD** miga na zielono, dopóki centrala łączy się z siecią Wi-Fi, i świeci stale na zielono, gdy połączenie zostanie nawiązane.

Właściwa siła sygnału komórkowego to **3** (trzy żółte mignięcia diody NET). Jeśli mignięć jest mniej, sygnał sieci komórkowej jest niewystarczający: wybierz inne miejsce dla centrali lub anteny albo użyj czulszej anteny. Jeśli diody pokazują coś innego, przyczynę znajdziesz w tabeli w punkcie 1.6. Jeśli nie świeci żadna dioda centrali,

sprawdź zasilanie i połączenia.

4. Podłączenie ekspanderów i modułów radiowych

Większość ekspanderów i modułów komunikacyjnych podłącza się do magistrali danych **RS485**. Zasilanie modułu zapewniają zaciski **AUX+** (+12 V) i **AUX–**, przewody danych idą do zacisków **485 A** i **485 B**, zawsze A → A, B → B. Do magistrali można podłączyć maksymalnie **8 urządzeń**, a długość przewodu magistrali to maksymalnie **100 m**. Wyjątkiem jest odbiornik Paradox RTX3, który podłącza się do magistrali manipulatorów (GRN, YEL) (4.3). Moduły ustawiasz na stronie **Modules** (6.5), a urządzenia radiowe dodajesz na stronie **Wireless** (6.6).

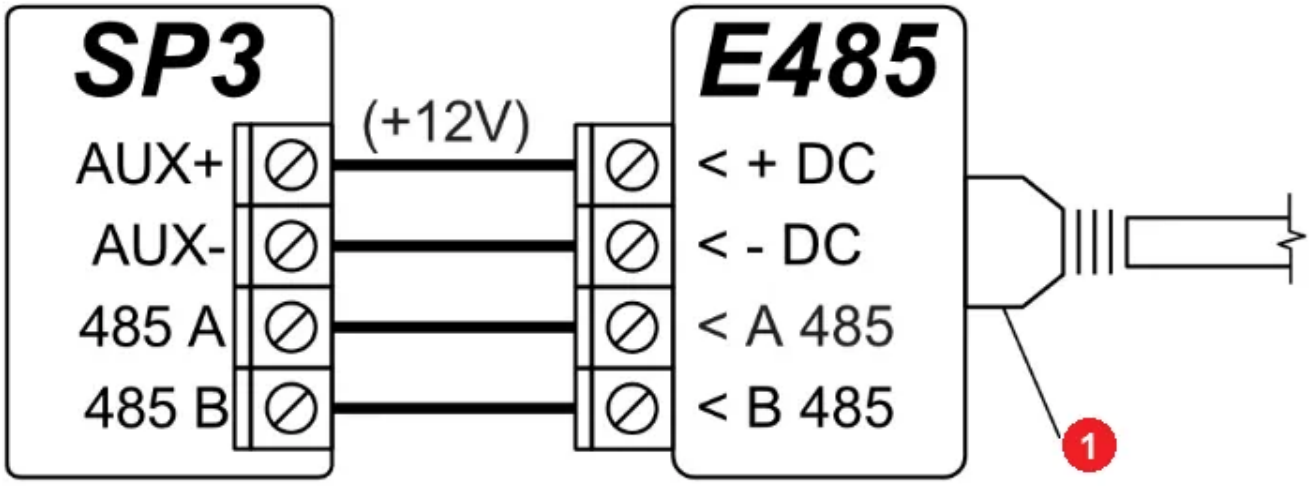
„Maksymalnie 100 m" to teoretyczne maksimum w idealnych warunkach – zobacz uwagę w punkcie 1.3.

Spośród odbiorników radiowych każda wersja firmware obsługuje tylko swój własny; pełna tabela wersji i obsługiwanych modułów jest w punkcie 1.7.

Moduł	System radiowy	Wymagany firmware (1.7)
RF-SH	Crow	SP3_xxx0, wersja 1.01 lub nowsza (SP3_xxx0_0101)
RTX3	Paradox	SP3_xxx1, wersja 1.12 lub nowsza (SP3_xxx1_0112)
RF-HW	Honeywell	SP3_xxx2, wersja 1.14 lub nowsza (SP3_xxx2_0114)
RF-S8	S8	SP3_xxx4, wersja 1.22 lub nowsza (SP3_xxx4_0122)
RF-LORA	urządzenia LoRa „Maximum"	do urządzeń bezprzewodowych MAXIMUM SP3_xxx4, wersja 1.21 lub nowsza (SP3_xxx4_0121); do ekspanderów LORA dowolna wersja
E485, T16, SF485, iO, iO-8, iO-WL, iO-MOD, ekspandery LORA	–	dowolna wersja

4.1 Moduł Ethernet E485

Z modułem E485 centrala wysyła i odbiera raporty zdarzeń i komendy sterujące przez przewodowy internet. Jeśli do centrali podłączony jest E485, raporty do stacji monitorowania i do Protegus 2 idą przez przewodowy internet, a mobilny internet nie jest używany; jeśli połączenie przewodowe zostanie przerwane, centrala przełącza się na mobilny internet, a po przywróceniu połączenia przewodowego automatycznie na nie wraca. Priorytet kanałów (SIM, Wi-Fi, LAN – E485) ustawiasz na stronie **Reporting to CMS** (6.3), a ustawienia E485 na stronie **Modules** (6.5). Z E485 centrala nie potrzebuje karty SIM.



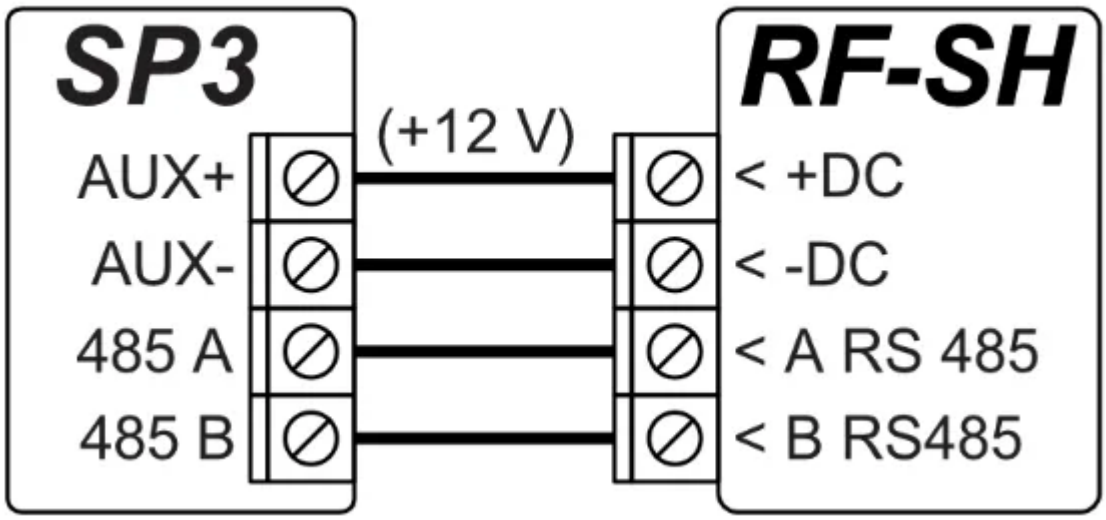
Rysunek 32. Moduł Ethernet E485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; do gniazda RJ45 modułu E485 kabel LAN. Połączenie RS485 („RS485 connection"), maksymalnie 100 m („up to 100 m").

- 1 kabel LAN („LAN cable")

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.

4.2 Odbiornik radiowy RF-SH (Crow)

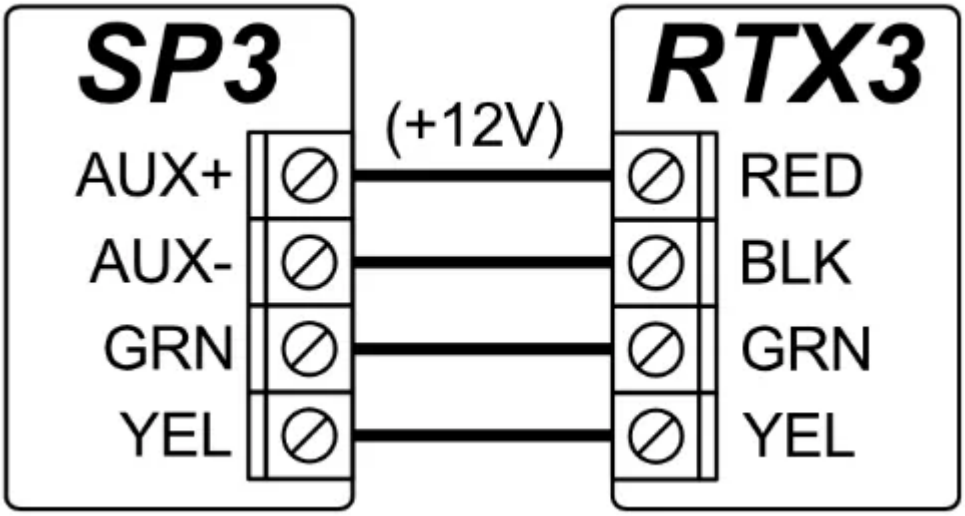
Z odbiornikiem RF-SH centrala obsługuje urządzenia bezprzewodowe Crow: maksymalnie 32 czujki, 16 sygnalizatorów, 42 piloty i 8 manipulatorów radiowych. Wymagany firmware: SP3_xxx0_0101 lub nowszy (1.7).



Rysunek 33. RF-SH: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

4.3 Odbiornik radiowy RTX3 (Paradox)

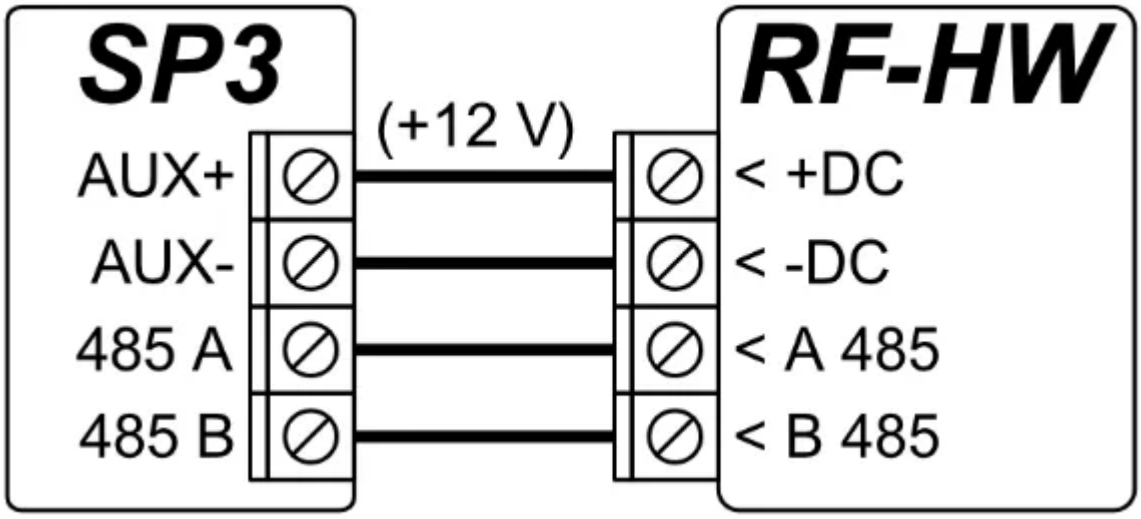
Odbiornik RTX3 podłącza się nie do RS485, lecz do **magistrali manipulatorów**. Z nim centrala obsługuje urządzenia bezprzewodowe Paradox: czujki otwarcia, czujki ruchu, czujkę zbicia szyby G550, czujkę dymu SD360, piloty REM2 i REM25, sygnalizatory SR230 i SR250, manipulator K37, ekspander PGM i stref 2WPGM, wzmacniacz sygnału RPT1. Wymagany firmware: SP3_xxx1_0112 lub nowszy (1.7). O firmware RTX3, jego podłączeniu oraz dodawaniu i usuwaniu urządzeń Paradox mówi osobny artykuł: FLEXi SP3 i bezprzewodowy moduł rozszerzeń Paradox RTX3.



Rysunek 34. RTX3 na magistrali manipulatorów: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL.

4.4 Odbiornik radiowy RF-HW (Honeywell)

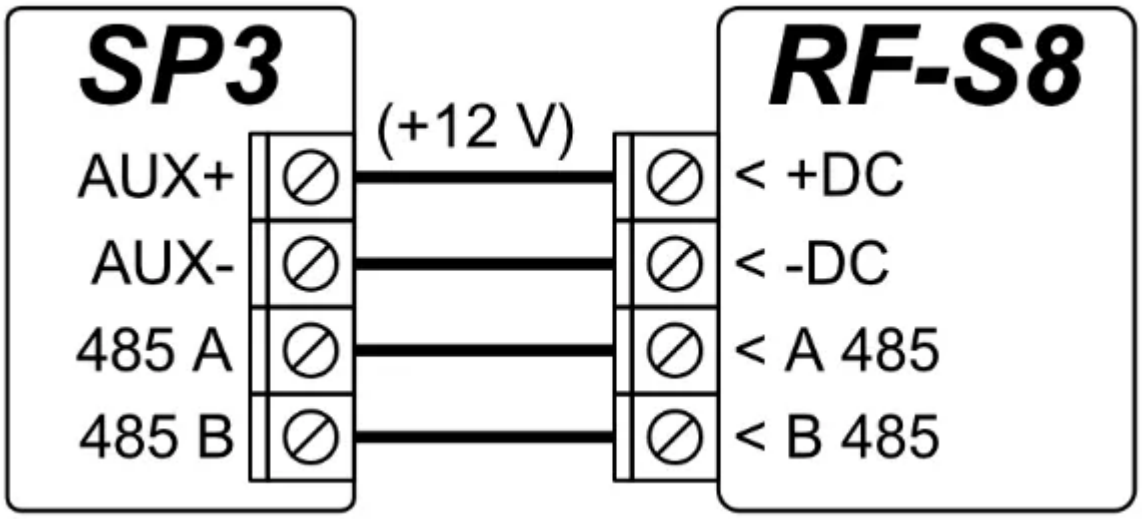
Z odbiornikiem RF-HW centrala obsługuje bezprzewodowe czujki, sygnalizatory, manipulatory i piloty Honeywell. Wymagany firmware: SP3_xxx2_0114 lub nowszy (1.7).



Rysunek 35. RF-HW: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.5 Odbiornik radiowy RF-S8

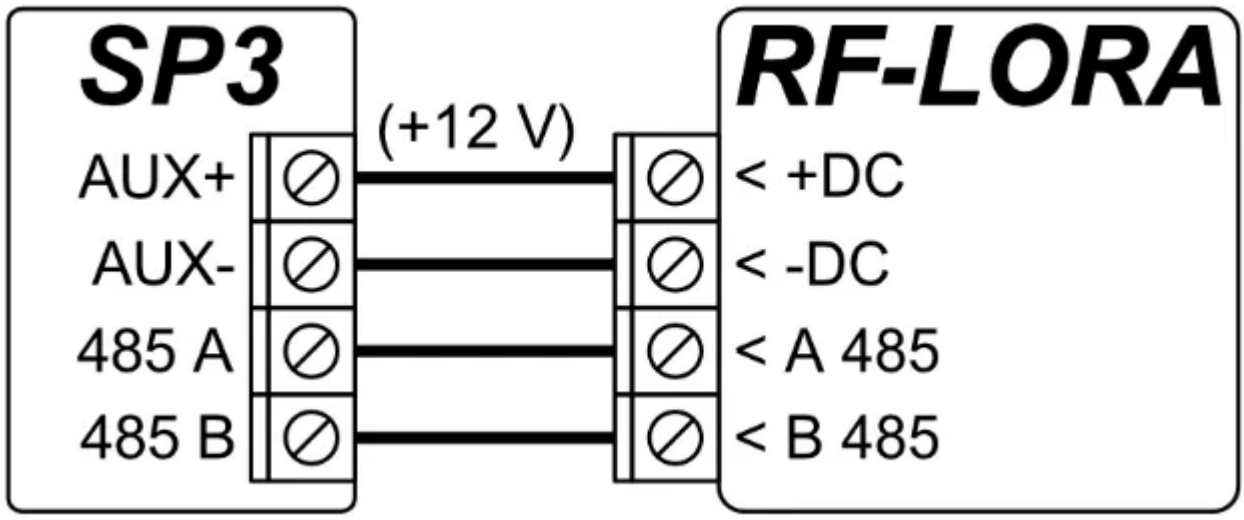
Z odbiornikiem RF-S8 centrala obsługuje bezprzewodowe czujki, sygnalizatory i piloty S8. Wymagany firmware: SP3_xxx4_0122 lub nowszy (1.7). Rejestrację RF-S8, wymianę firmware i parowanie urządzeń S8 opisuje osobna instrukcja: Instrukcja nadajnika-odbiornika RF-S8 i czujek S8.



Rysunek 36. RF-S8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.6 Odbiornik radiowy RF-LORA

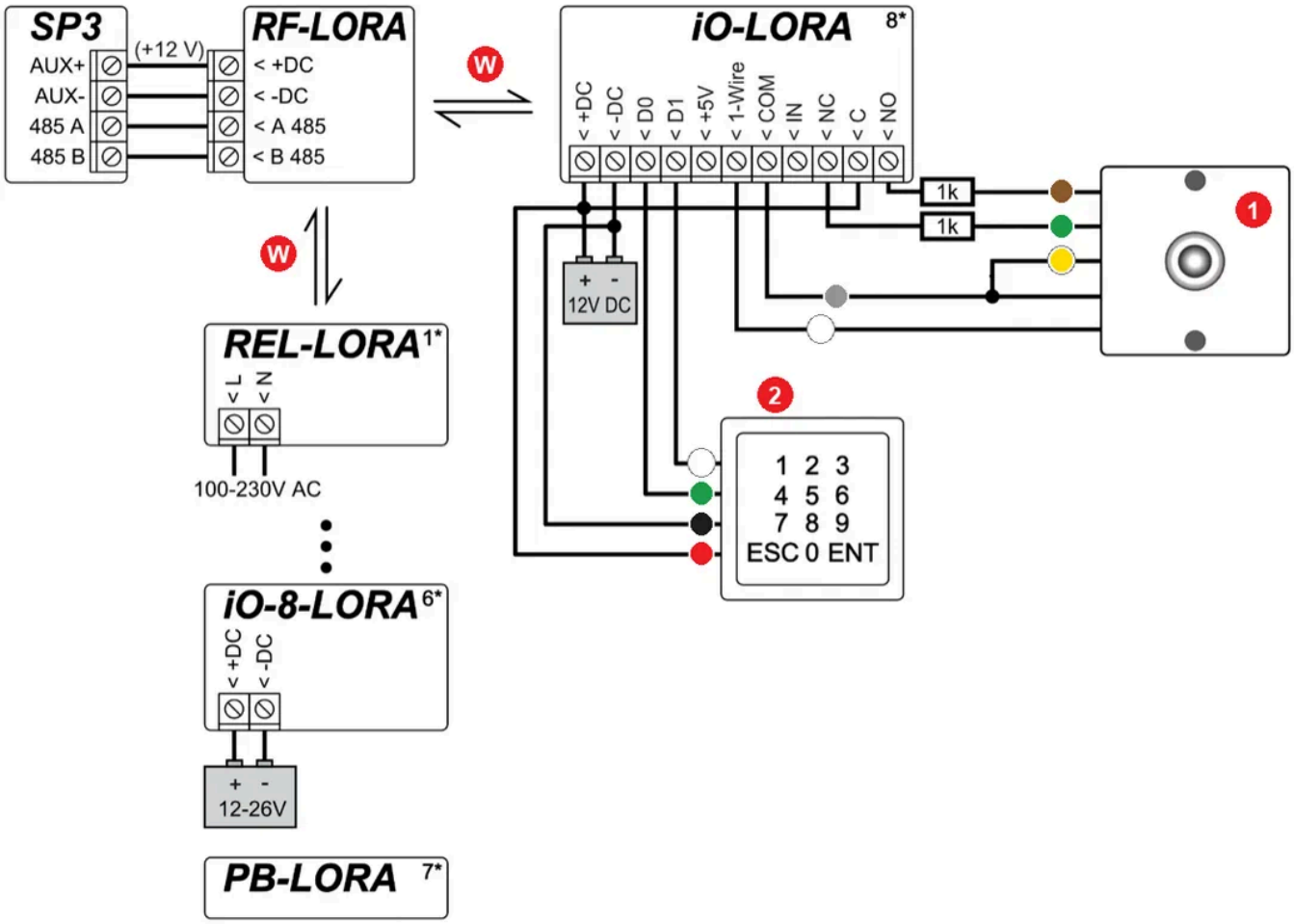
Z odbiornikiem RF-LORA centrala obsługuje radiowe urządzenia LoRa „Maximum": maksymalnie 32 czujki, 16 sygnalizatorów i 32 piloty, a także ekspandery LORA (4.7). Do czujek, sygnalizatorów i pilotów MAXIMUM potrzebny jest firmware SP3_xxx4 w wersji 1.21 lub nowszej; ekspandery LORA działają z dowolną wersją firmware (1.7). Odbiornik ustawia się na stronie **Modules** (6.5), a urządzenia dodaje na stronie **Wireless** (6.6).



Rysunek 37. RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.7 Ekspandery LORA

Ekspandery LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) łączą się z centralą radiowo przez odbiornik RF-LORA, z odległości maksymalnie 5000 m. **iO-LORA**: ekspander wejść i wyjść z możliwością podłączenia czytnika iButton CZ-Dallas, zasilany 12 V DC; podłączony do niego czytnik Wiegand nie działa z SP3. **iO8-LORA**: ekspander z ośmioma wejściami/wyjściami, zasilany 12–26 V, ze wszystkimi typami obwodów centrali (3.2). **PB-LORA**: przycisk napadowy. **REL-LORA**: moduł przekaźnikowy, zasilany 100–230 V AC.



Rysunek 38. Ekspandery LORA przez odbiornik RF-LORA. SP3 → RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; RF-LORA radiowo, z odległości maksymalnie 5000 m, łączy się z jednostkami iO-LORA, iO8-LORA, PB-LORA i REL-LORA. REL-LORA: L, N → 100–230 V AC. iO8-LORA: +DC, −DC → 12–26 V. iO-LORA: +DC, −DC → 12 V DC; przewód czerwony czytnika wejściowego (+U) → +DC, czarny (GND) → −DC, zielony (D0) → D0, biały (D1) → D1; połączenie 1-Wire czytnika CZ-Dallas maksymalnie 30 m („1-Wire connection up to 30 m"): 1-Wire → biały, COM → szary i żółty (LED−), C → +DC, NO → 1 kΩ → brązowy (RED LED+), NC → 1 kΩ → zielony (Green LED+). Wyjście xOUT trzeba ustawić na typ **System State** (stan systemu) („The output xOUT must be set to the »System State« type.") – przy uzbrojonym alarmie światło czytnika iButton jest czerwone („Security alarm is on - the iButton reader light is red."), przy rozbrojonym zielone („The security alarm is off - the iButton reader light is green.").

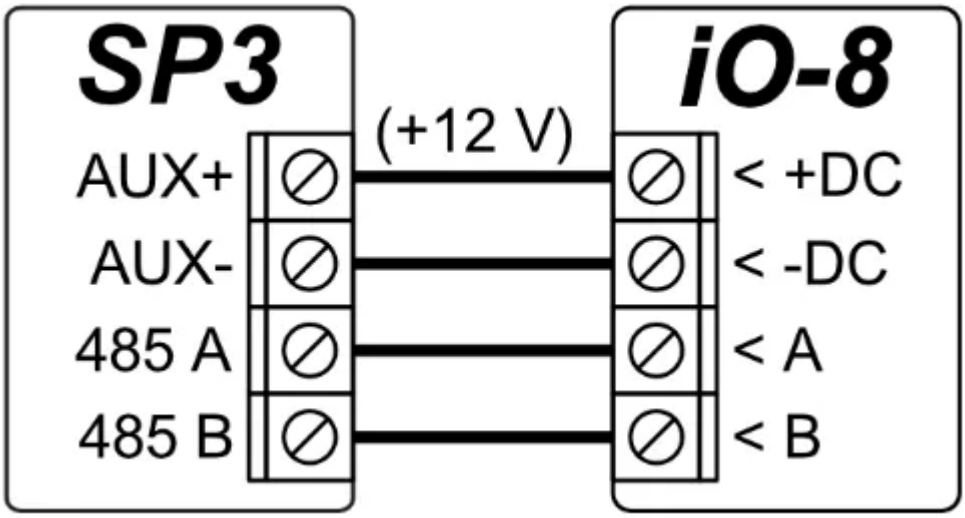
- 1 czytnik iButton CZ-Dallas („CZ-Dallas reader")
- 2 czytnik wejściowy: czytnik RFID z klawiaturą, Wiegand 26/34 („Entry reader", „RFID reader with keypad (Wiegand 26/34)") – z FLEXi SP3 w ten sposób nie działa
- W połączenie bezprzewodowe („Wireless connection"), maksymalnie 5000 m („up to 5000 m")
- przewód brązowy, RED LED+ („Brown wire", „RED LED+") – światło czerwone
- przewód zielony: w czytniku CZ-Dallas Green LED+, światło zielone („Green wire", „Green LED+"); w czytniku wejściowym D0 („G - green wire (D0)")
- przewód żółty, LED− („Yellow wire", „LED-")
- przewód szary („Gray wire")
- przewód biały („White wire"); w czytniku wejściowym D1 („W - white wire (D1)")
- przewód czerwony, +U („R - red wire (+U)")
- przewód czarny, GND („B - black wire (GND)")

Czytnik wejściowy (2) podłączony na rysunku do iO-LORA nie działa z FLEXi SP3. Czytnik RFID podłącz bezpośrednio do centrali (3.5).

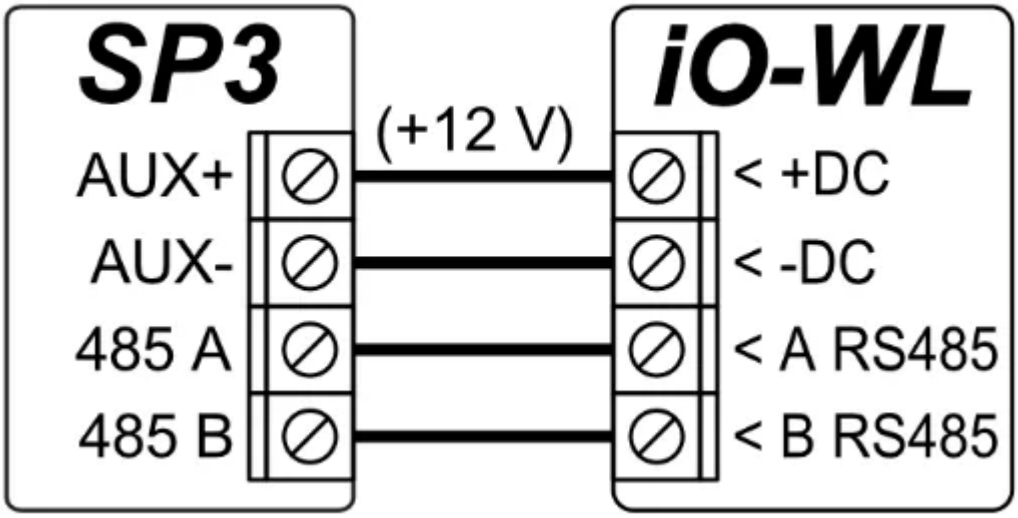
Odległości „do … m” to teoretyczne maksima osiągalne w idealnych warunkach. W praktyce jakość i przebieg kabla, źródła zakłóceń, a przy łączach radiowych także ściany i ukształtowanie terenu dają znacznie mniejszy zasięg. Planuj z zapasem, a przy długich odcinkach sprawdź połączenie podczas uruchomienia.

4.8 Ekspandery serii iO

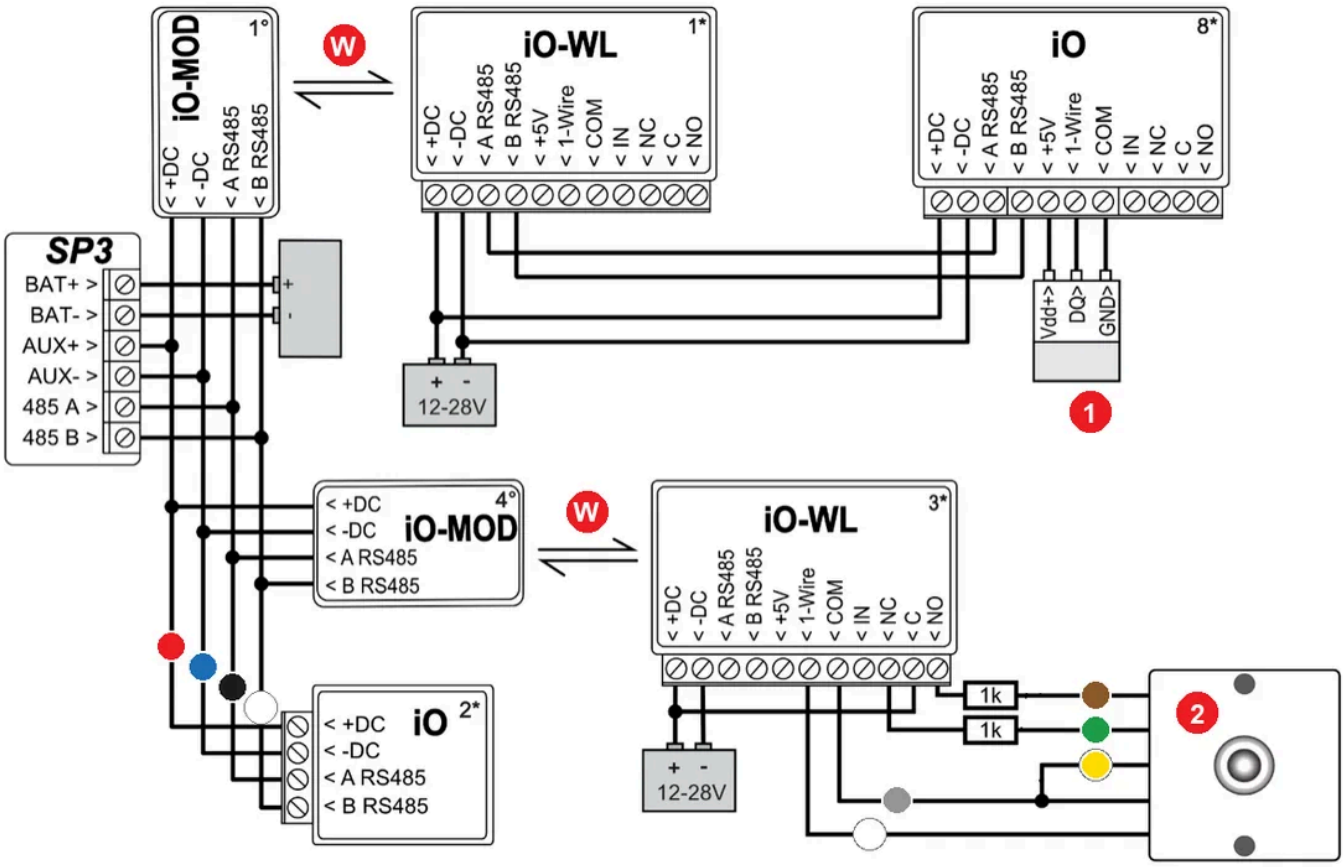
Jeśli centrala potrzebuje więcej wejść (IN) lub wyjść (OUT), podłącz do niej przewodowy lub bezprzewodowy ekspander Trikdis serii iO (iO, iO-8, iO-WL, iO-MOD). **iO**: ekspander wejść/wyjść z podłączeniem 1-Wire. **iO-8**: ekspander z ośmioma wejściami/wyjściami, ze wszystkimi typami obwodów centrali (3.2). **iO-WL**: ekspander bezprzewodowy, który łączy się z centralą przez nadajnik-odbiornik **iO-MOD**, z odległości maksymalnie 300 m; można go też podłączyć przewodowo do magistrali RS485. W systemie może być maksymalnie 8 modułów rozszerzeń i maksymalnie 4 iO-MOD. Ekspandery ustawia się na stronie **Modules** (6.5).



Rysunek 39. iO-8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A, 485 B → B.



Rysunek 40. iO-WL przewodowo: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.



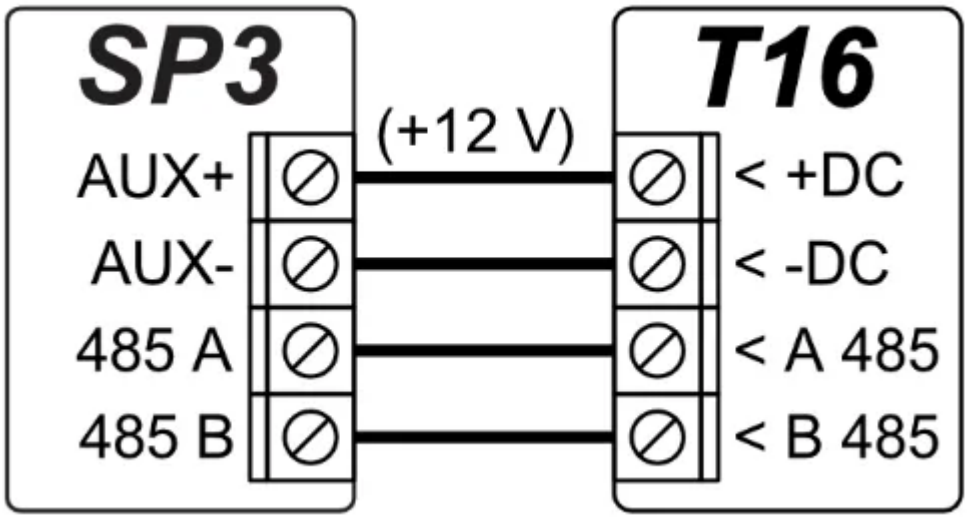
Rysunek 41. Przegląd systemu iO. SP3: BAT+ / BAT− → akumulator 12 V („Battery 12V"); AUX+ (czerwony) i AUX− (niebieski) → +DC i −DC na jednostce iO-MOD i iO; 485 A (czarny) i 485 B (biały) → A RS485 i B RS485. Dwa moduły iO-MOD radiowo, z odległości maksymalnie 300 m, łączą się każdy z jedną jednostką iO-WL. Górne iO-WL i iO pracują ze wspólnego zasilania 12–28 V, między nimi połączenie RS485 („RS485 connection"), maksymalnie 300 m („up to 300 m"); zaciski +5V, 1-Wire i COM modułu iO → Vdd+, DQ i GND czujnika temperatury DS18B20 / DS18S20. Dolne iO-WL (12–28 V) obsługuje czytnik CZ-Dallas, połączenie 1-Wire maksymalnie 30 m („1-Wire connection up to 30 m"): 1-Wire → biały, COM → szary i żółty (LED−), C → +DC, NO → 1 kΩ → brązowy (RED LED+), NC → 1 kΩ → zielony (Green LED+). Wyjście xOUT trzeba ustawić na typ **System State** (stan systemu) („The output xOUT must be set to the »System State« type.") – przy uzbrojonym alarmie światło czytnika iButton jest czerwone („Security alarm is on - the iButton reader light is red."), przy rozbrojonym zielone („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 ° maksymalnie 4 moduły iO-MOD („° up to 4 iO-MOD modules").

- 1 czujnik temperatury, DS18B20 lub DS18S20 („Temperature sensor: DS18B20 or DS18S20")
- 2 czytnik iButton CZ-Dallas („CZ-Dallas reader")
- W połączenie bezprzewodowe („Wireless connection"), maksymalnie 300 m („up to 300 m")
- przewód czerwony („Red wire")
- przewód niebieski („Blue wire")
- przewód czarny („Black wire")
- przewód biały („White wire")
- przewód brązowy, RED LED+ („Brown wire", „RED LED+") – światło czerwone
- przewód zielony, Green LED+ („Green wire", „Green LED+") – światło zielone
- przewód żółty, LED− („Yellow wire", „LED-")
- przewód szary („Gray wire")

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.

4.9 Nadajnik radiowy T16

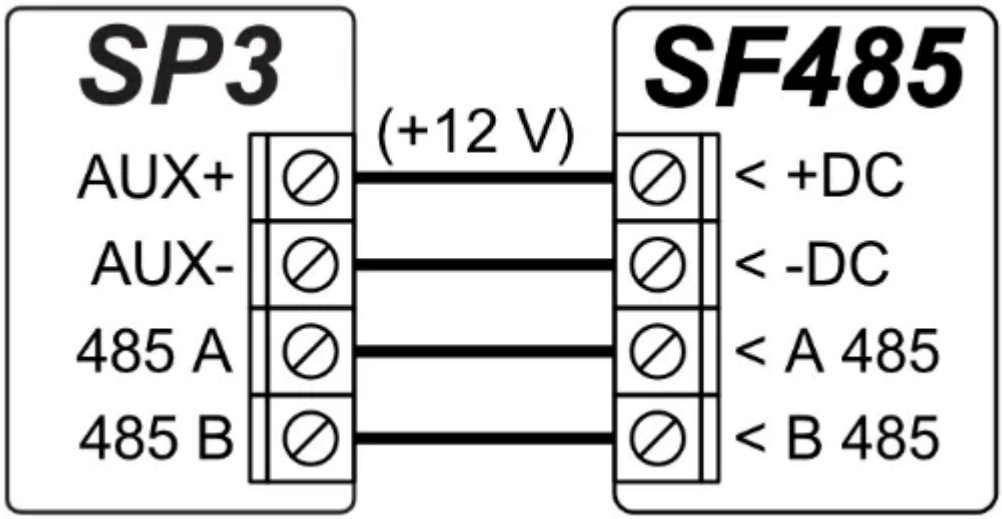
Nadajnik radiowy VHF/UHF T16 przekazuje zdarzenia centrali przez sieć radiową Trikdis do stacji monitorowania: wysyła zarówno własne zdarzenia, jak i otrzymane od centrali, a stacja monitorowania może przekazywać je użytkownikowi.



Rysunek 42. T16: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.10 Moduł Sigfox SF485

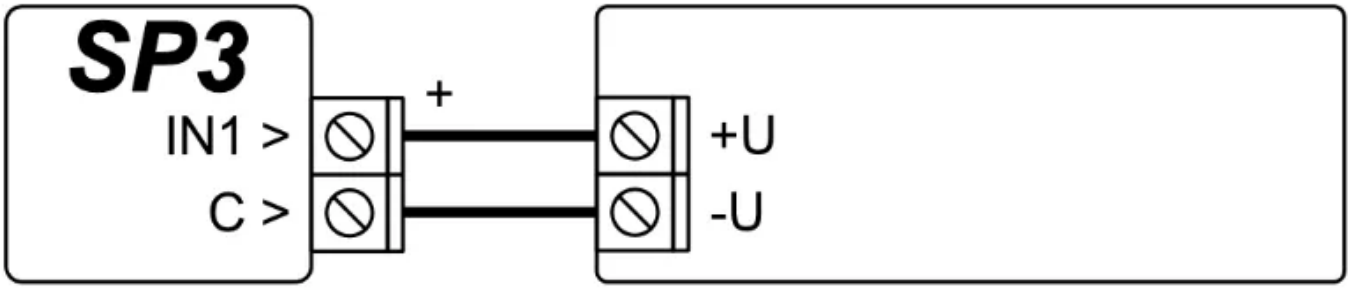
SF485 to kanał zapasowy: jeśli kanał główny zawiedzie, wysyła zdarzenia centrali przez sieć Sigfox do stacji monitorowania lub do aplikacji Protegus 2, w formacie Contact ID.



Rysunek 43. SF485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.11 Pomiar napięcia stałego

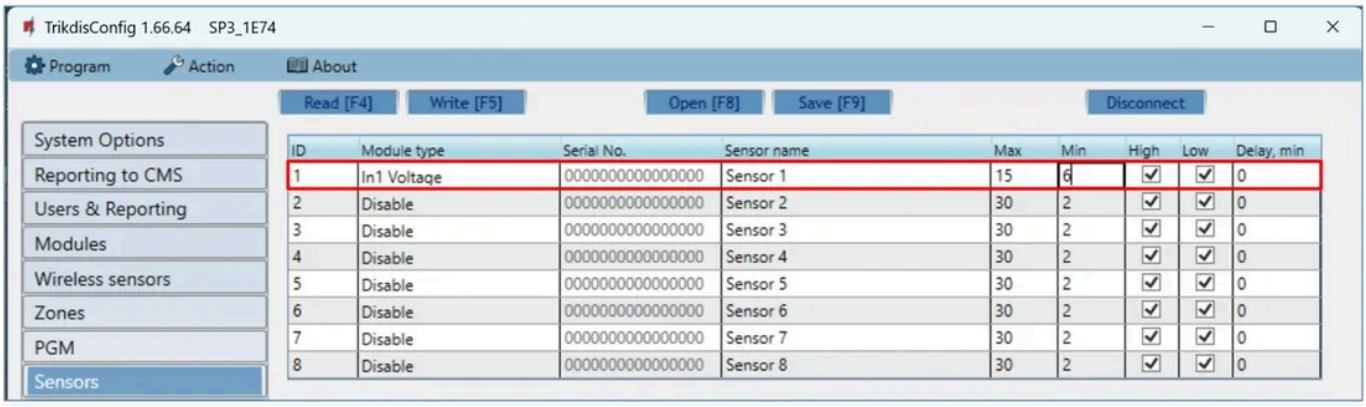
Centrala potrafi mierzyć napięcie stałe 0–30 V; **powyżej 30 V płytka ulegnie uszkodzeniu**. Biegun dodatni mierzonego napięcia podłącza się do zacisku IO1 (na rysunku fabrycznym IN1), a ujemny do zacisku C.



Rysunek 44. Pomiar napięcia: mierzone urządzenie („Equipment whose voltage is measured") +U → IO1 (na rysunku IN1), −U → C.

Podłącz centralę kablem USB do komputera i uruchom TrikdisConfig (rozdział 6); program automatycznie rozpozna podłączoną centralę i otworzy jej okno ustawień. Na stronie **Sensors** dodaj czujnik **In1 Voltage** i wartości graniczne:

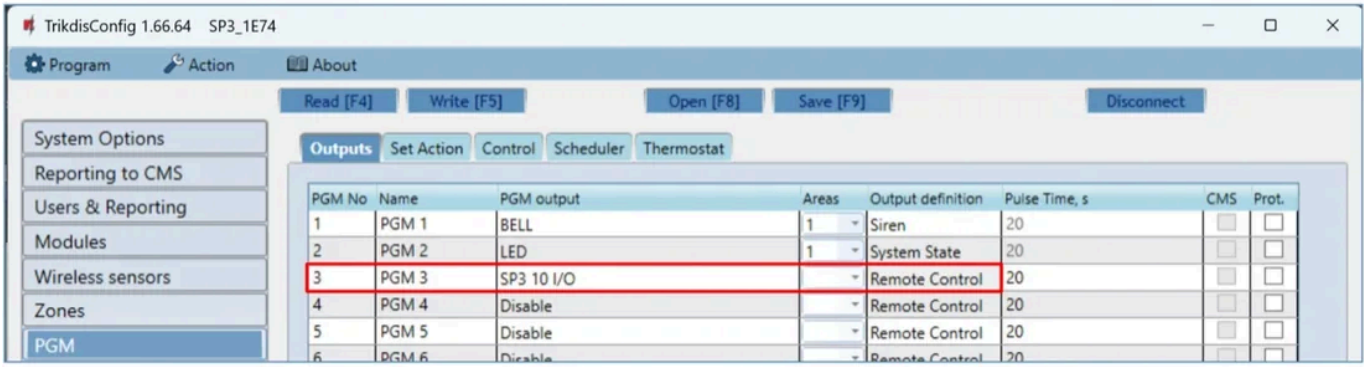
- **Max** – powyżej tego napięcia powstaje zdarzenie, jeśli zaznaczone jest pole **High**;
- **Min** – poniżej tego napięcia powstaje zdarzenie, jeśli zaznaczone jest pole **Low**.



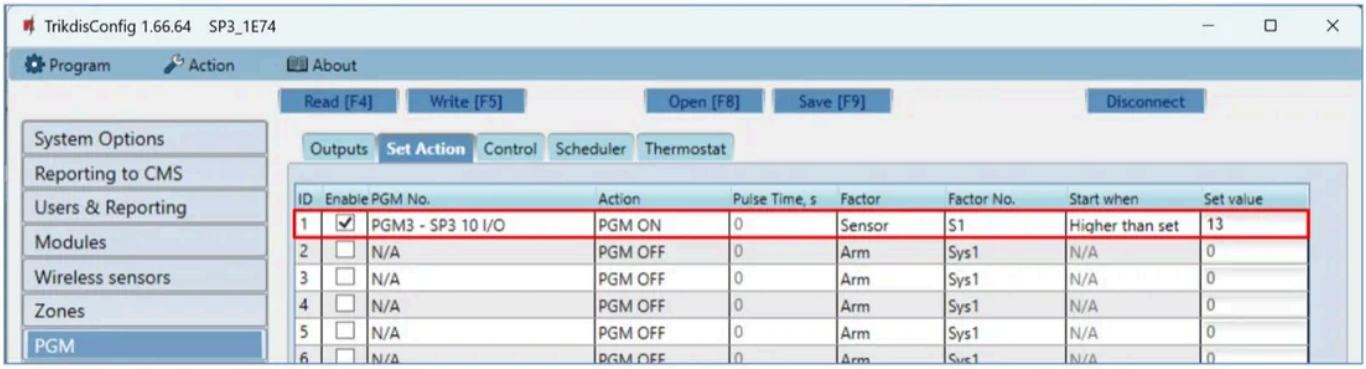
Rysunek 45. Strona Sensors: czujnik In1 Voltage o identyfikatorze 1, Max 15, Min 6, zaznaczone High i Low, Delay 0 minut.

Mierzone napięcie może też sterować wyjściem PGM. Na karcie **Outputs** strony **PGM** ustaw wyjście w trybie **Remote Control**, a następnie na karcie **Set Action** podaj warunek:

- **Enable** – włączenie PGM;
- **PGM No.** – sterowane wyjście PGM;
- **Action** – działanie wyjścia: **PGM OFF** (wyłącza), **PGM ON** (włącza), **Pulse OFF** (na komendę wyłącza na czas impulsu, potem włącza z powrotem), **Pulse ON** (włącza na czas impulsu, potem wyłącza);
- **Pulse time, s** – długość impulsu, 0–9999 s;
- **Factor** – źródło warunku: **Sensor**;
- **Factor No.** – wejście pomiaru napięcia (S1);
- **Start when** – warunek: **Higher than set** (powyżej ustawionej wartości) lub **Lower than set** (poniżej);
- **Set value** – monitorowane napięcie (V).



Rysunek 46. Karta Outputs strony PGM: 3. PGM na 10. zacisku I/O SP3, typ Remote Control, czas impulsu 20 s.



Rysunek 47. Karta Set Action: zaznaczone Enable, PGM No. PGM3, Action PGM ON, Pulse Time 0, Factor Sensor, Factor No. S1, Start when Higher than set, Set value 13 V.

5. Protegus 2 i sterowanie zdalne

„FLEXi" SP3 możesz sterować zdalnie na trzy sposoby: z aplikacji Protegus 2, SMS-em i połączeniem telefonicznym. Aplikacja działa w każdej wersji, która ma dostęp do internetu (WiFi, Ethernet lub sieć komórkowa). Komendy SMS i sterowanie połączeniem są dostępne tylko w wersjach z modemem sieci komórkowej (na przykład SP3_24E, SP3_44E, SP3_12E) i tylko z działającą kartą SIM. W wersji SP3_3E (WiFi + Ethernet) nie ma modemu.

5.1 Połączenie z kontem Protegus 2

W Protegus 2 użytkownik uzbraja i rozbraja system, widzi stan stref i partycji oraz otrzymuje powiadomienia o zdarzeniach. Zanim dodasz centralę do konta, sprawdź:

- **Napięcie zasilania** – dioda **POWER** świeci stale na zielono.
- **Sieć** – dioda **NET** świeci stale na zielono (sieć komórkowa) i/lub dioda **MOD** świeci stale na zielono (moduł WiFi lub Ethernet). Znaczenie diod opisuje punkt 1.6.
- **Karta SIM** – w wersji z modemem karta SIM jest aktywna, a kod PIN został wpisany w TrikdisConfig (**System Options** → **SIM** → **PIN**) albo żądanie PIN zostało wyłączone na karcie.
- **Usługa w chmurze** – na karcie **Users & Reporting** → **Protegus** w TrikdisConfig zaznaczone jest **Enable cloud service** (6.4). Fabryczna wartość **Cloud access code** to 123456; jeśli ją zmienisz, aplikacja przy dodawaniu systemu poprosi o nowy kod.
- **Unikalny identyfikator** – numer **IMEI/Unique ID** centrali znajdziesz na naklejce na opakowaniu i na płytce; widać go też w lewym dolnym rogu TrikdisConfig po odczytaniu centrali.

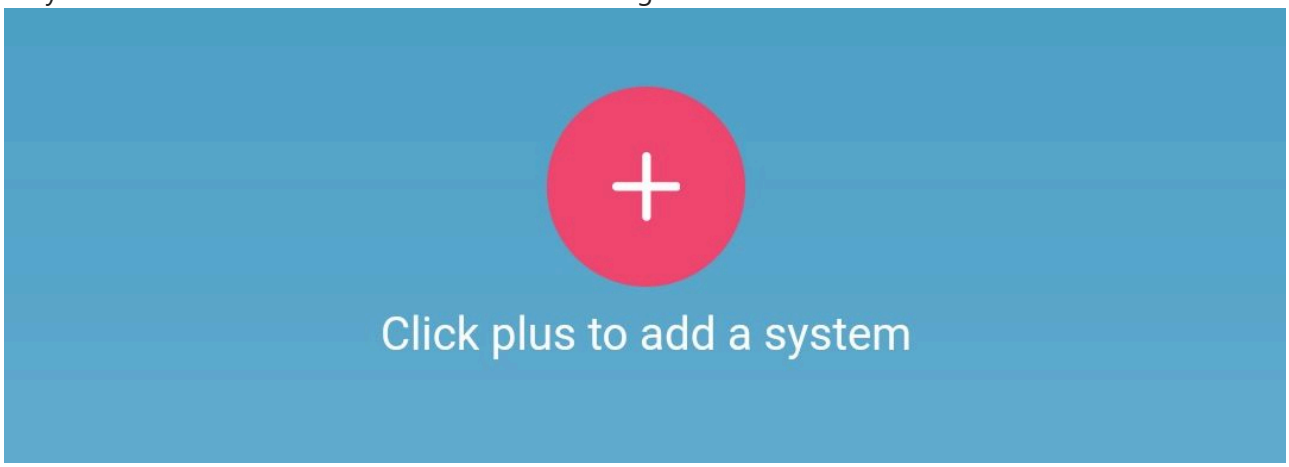
Jeśli nie masz jeszcze konta Protegus, załóż je na stronie www.protegus.app linkiem **Sign up** i aktywuj, klikając link otrzymany w e-mailu; następnie zainstaluj aplikację Protegus 2 na telefonie i zaloguj się swoją nazwą użytkownika i hasłem.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



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

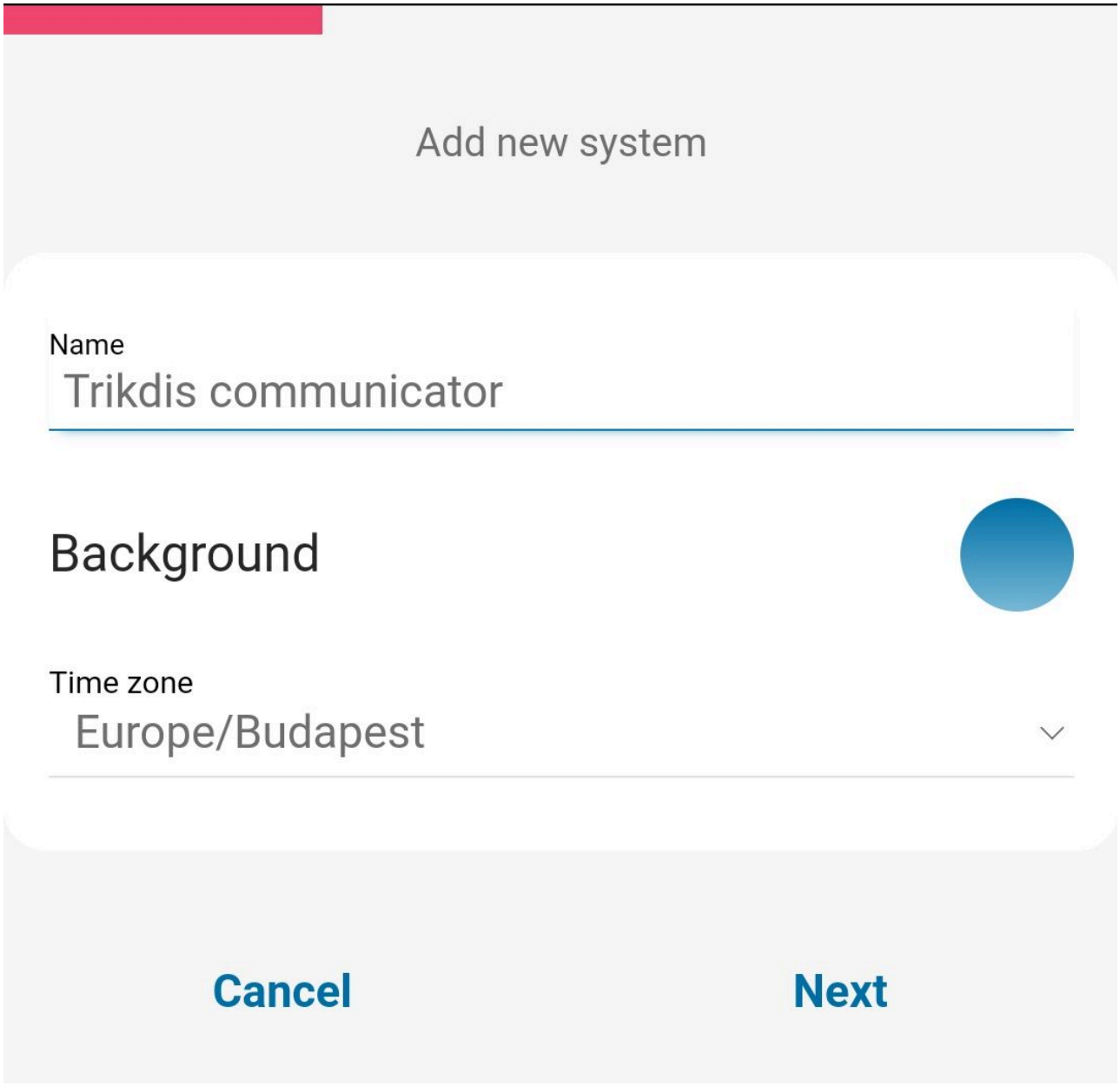


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

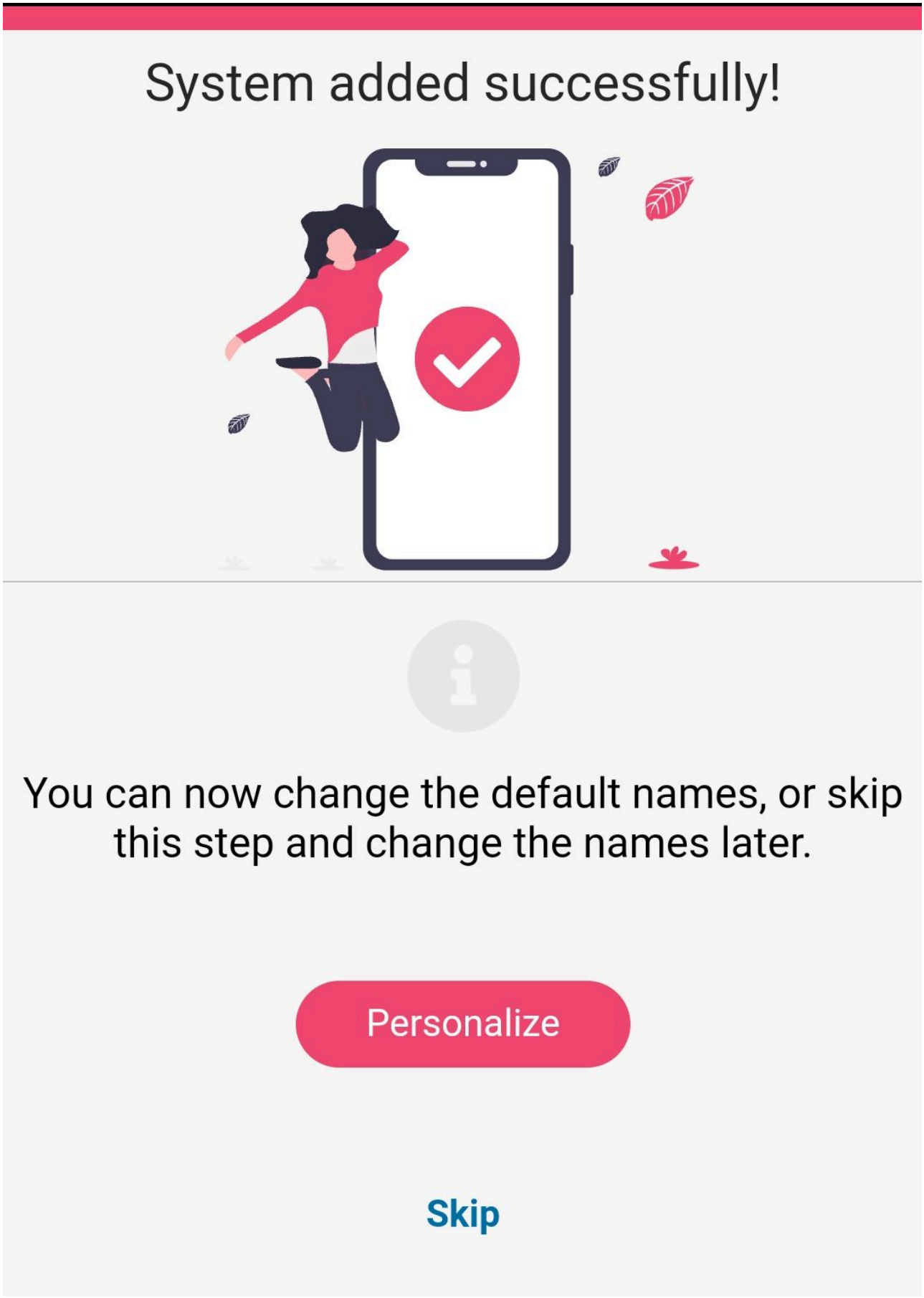
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



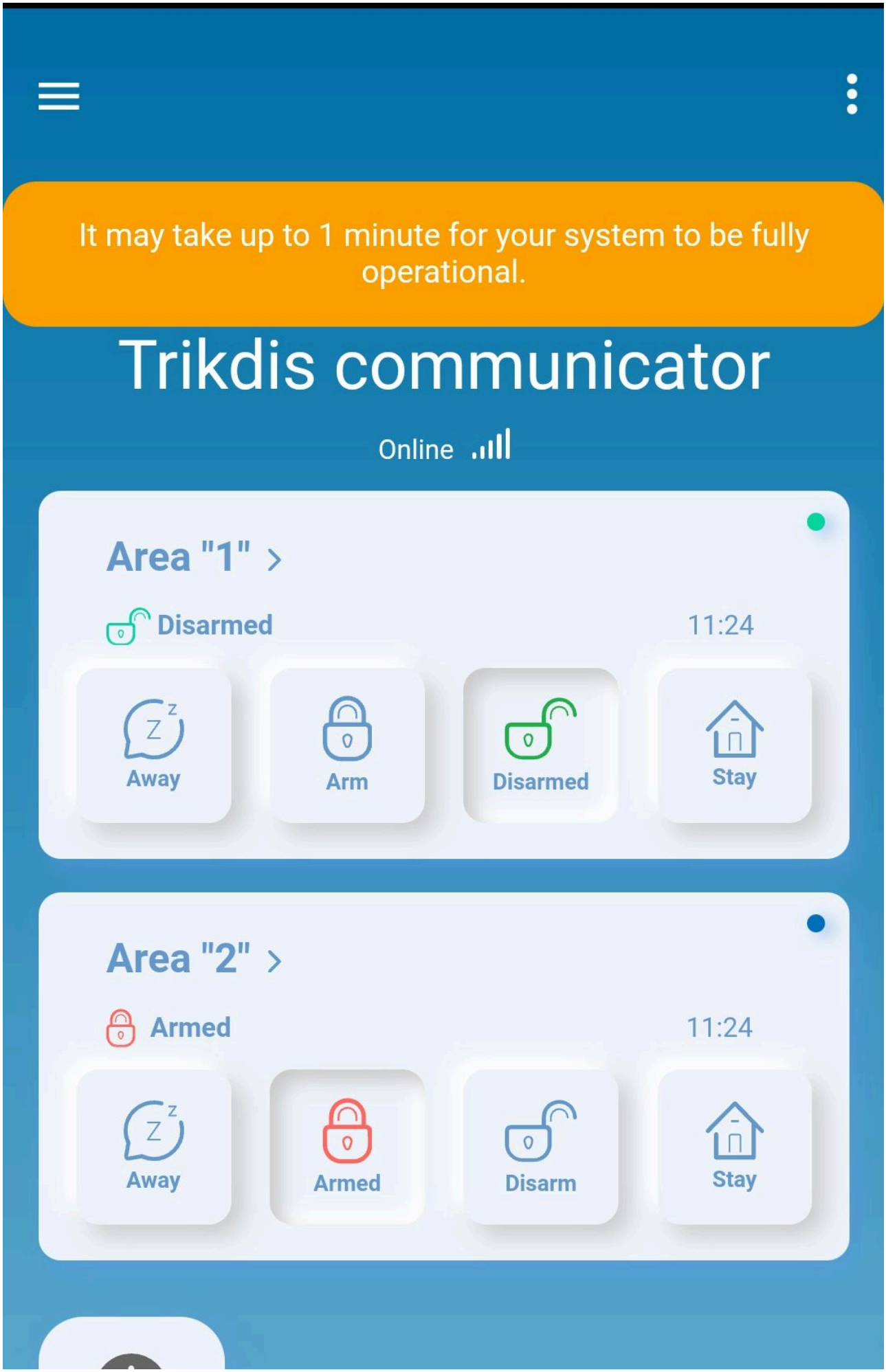
6. Add meg a rendszer nevét és válassz idozónát

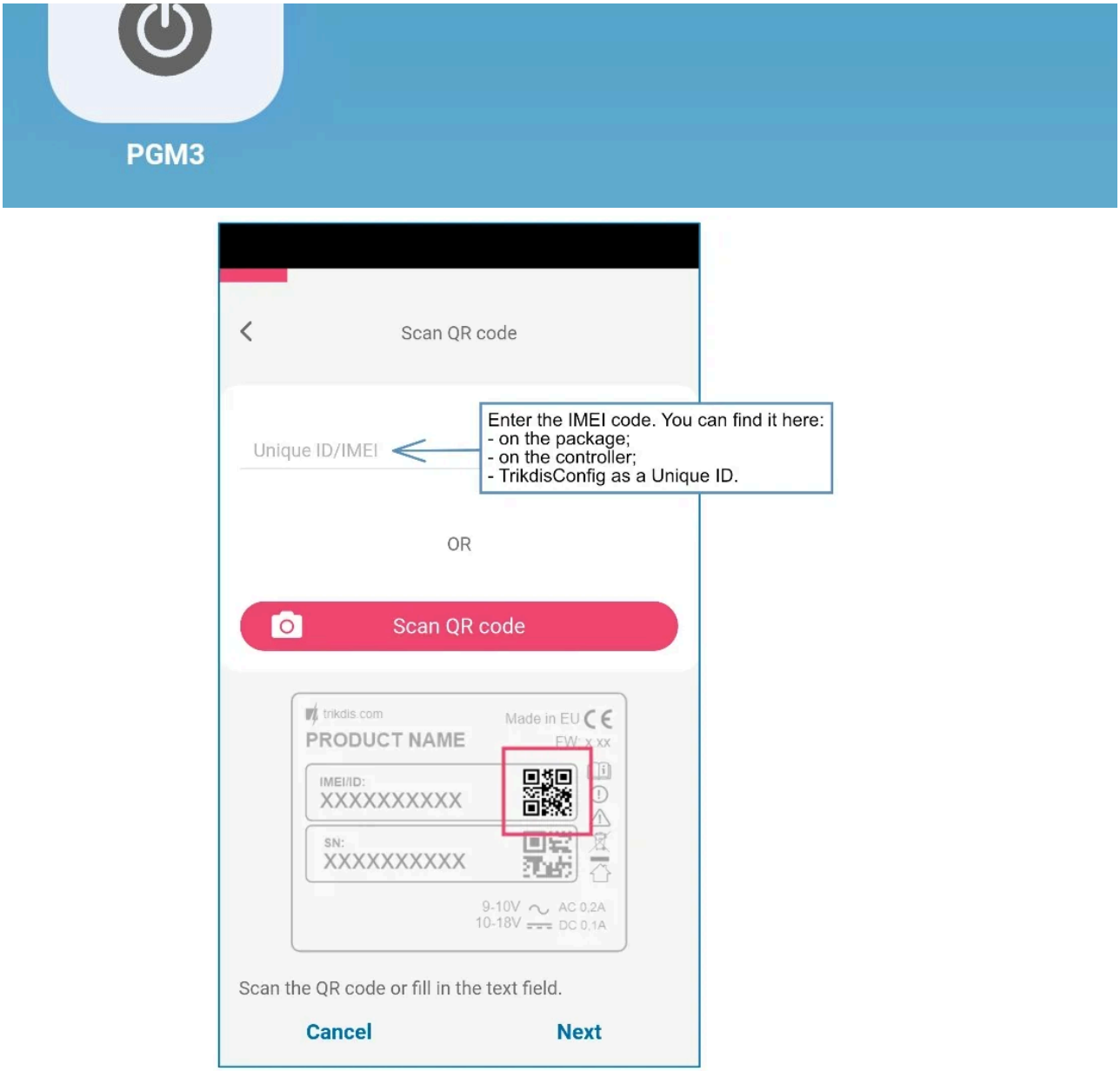


7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.



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


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



Rysunek 48. Dodawanie systemu w Protegus 2: wpisujesz numer **IMEI/Unique ID** albo skanujesz kamerą kod QR z naklejki.

Kolejni użytkownicy

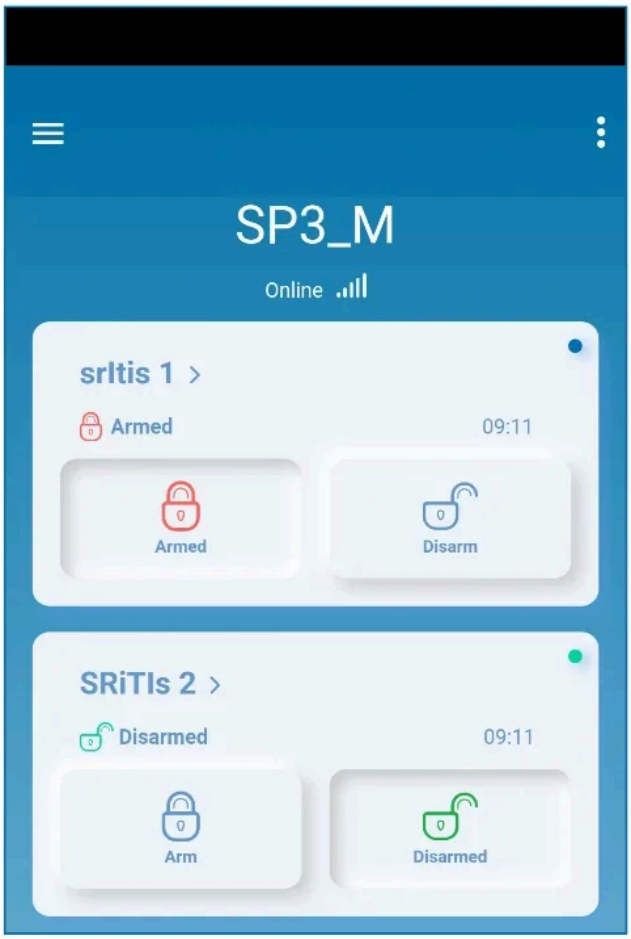
Właściciel może zaprosić kolejnych użytkowników w Protegus 2. Na adresy wpisane w kolumnie **Email** na karcie **Users & Reporting** → **Users** w TrikdisConfig system również wysyła zaproszenie, dzięki czemu użytkownik widzi system ze swojego konta (6.4).

5.2 Uzbrajanie i rozbrajanie w aplikacji

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

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

W SP3 po dotknięciu kłódki musisz wpisać **kod użytkownika** centrali. Jest to kod z kolumny **Code** na karcie **Users & Reporting** → **Users** w TrikdisConfig, a nie hasło konta Protegus 2. Każda partycja jest wyświetlana na osobnej karcie i widzisz tylko te partycje, do których użytkownik ma uprawnienia w kolumnie **Areas**. Oprócz pełnego uzbrojenia z aplikacji uruchamiasz też tryby częściowe: **Stay** (zostajesz w domu, strefy wewnętrzne nie są uzbrajane) i **Sleep** (tryb nocny). W którym trybie strefa czuwa, decyduje pole **Definition** strefy (6.7).



Rysunek 49. Dwie partycje w Protegus 2: 1. uzbrojona (czerwona, zamknięta kłódka), 2. rozbrojona (zielona, otwarta kłódka).

Jeśli aplikacja nie nadąża za centralą

Jeśli po komendach nic się nie dzieje albo aplikacja pokazuje coś zupełnie innego niż rzeczywisty stan centrali, otwórz w Protegus 2 menu **Settings** → **System configuration** i w wierszu **System out of sync?** naciśnij przycisk **Sync**. Aplikacja ponownie odczyta ustawienia centrali.

5.3 Konfiguracja i sterowanie SMS-em

Tylko w wersjach z modemem. SMS wysyłasz na numer karty SIM centrali. Każda wiadomość ma taką samą budowę:

Komenda spacja **Hasło** spacja **Dane**

Hasło to sześciocyfrowe **SMS password** (**System Options** → **Access**, 6.2). Jego wartość fabryczna to **123456**. Ze względów bezpieczeństwa przy uruchomieniu zmień je na hasło znane tylko tobie w TrikdisConfig lub komendą `PSW` – i nie zapomnij go –, a numeru karty SIM centrali nie podawaj niepotrzebnie. Pole danych

zależy od komendy, przy wielu komendach jest puste.

Kto może wysyłać komendy?

Administrator może sterować centralą SMS-em i połączeniem. Jeśli chcesz uprawnić także innego użytkownika, dodaj jego numer telefonu na karcie **Users & Reporting** → **Users** w TrikdisConfig (6.4) lub komendą `SETN`. Centrala wysyła odpowiedzi z tekstami podanymi na karcie **SMS answer texts**.

Polecenie	Dane	Co robi	Przykład
INFO	–	Zapytanie o stan: nazwa obiektu, stan partycji, IMEI, poziom sygnału, wersja firmware, numer seryjny.	`INFO 123456`
RESET	–	Ponowne uruchomienie centrali.	`RESET 123456`
OUTPUTx	ON	Włączenie wyjścia x.	`OUTPUT1 123456 ON`
	OFF	Wyłączenie wyjścia x.	`OUTPUT1 123456 OFF`
	PULSE=ttt	Włączenie wyjścia x na ttt sekund (trzy cyfry).	`OUTPUT1 123456 PULSE=002`
PSW	nowe hasło	Zmiana hasła SMS.	`PSW 123456 654123`
TIME	RRRR/MM/DD,gg:mm:ss	Ustawienie daty i godziny.	`TIME 123456 2026/10/30,10:02:00`
TXTA	nazwa obiektu	Ustawienie nazwy obiektu (pojawia się ona w raportach).	`TXTA 123456 Dom`
RDR	numer telefonu#tekst	Tekst po znaku # centrala przekazuje SMS-em na podany numer. Numer zaczyna się od znaku + i kodu kraju.	`RDR 123456 +48601234567#przekazany tekst`
ASKI	–	Stan wejść (IN) w wiadomości SMS.	`ASKI 123456`
ASKO	–	Stan wyjść (OUT) w wiadomości SMS.	`ASKO 123456`
ASKA	–	Stan partycji w wiadomości SMS.	`ASKA 123456`
ASKT	–	Wartości wszystkich czujników temperatury w wiadomości SMS.	`ASKT 123456`
ARM	SYS:x	Uzbrojenie partycji x (1–8).	`ARM 123456 SYS:1`
DISARM	SYS:x	Rozbrojenie partycji x (1–8).	`DISARM 123456 SYS:1`
STAY	SYS:x	Uzbrojenie partycji x w trybie Stay (1–8).	`STAY 123456 SYS:1`
SLEEP	SYS:x	Uzbrojenie partycji x w trybie Sleep (1–8).	`SLEEP 123456 SYS:1`

Polecenie	Dane	Co robi	Przykład
FRS	–	Reset zasilania czujek pożarowych, jeśli definicja jednego z wyjść to **Fire Sensor Reset**.	`FRS 123456`
SETN	PhoneX=numer#nazwa#e-mail	Dodanie użytkownika w wierszu x z numerem telefonu, nazwą i adresem e-mail; numer telefonu i nazwę oddziela znak #. Numer zaczyna się od znaku + i kodu kraju.	`SETN 123456 PHONE5=+48601234567#JAN#jan@przyklad.pl`
	PhoneX=DEL	Usunięcie numeru telefonu i nazwy z wiersza x.	`SETN 123456 PHONE5=DEL`
UUSD	*kod#	Wysłanie kodu USSD do operatora komórkowego (na przykład sprawdzenie salda). Polecenie występuje w centrali właśnie pod nazwą UUSD.	`UUSD 123456 *245#`
CONNECT	Protegus=ON	Połączenie z chmurą Protegus.	`CONNECT 123456 PROTEGUS=ON`
	Protegus=OFF	Rozłączenie połączenia z Protegus.	`CONNECT 123456 PROTEGUS=OFF`
	Code=123456	Kod dostępu do chmury Protegus (**Cloud access code**).	`CONNECT 123456 CODE=123456`
	IP=adres:port	Adres IP i port głównego kanału do stacji monitorowania.	`CONNECT 123456 IP=0.0.0.0:8000`
	IP=0	Wyłączenie kanału głównego.	`CONNECT 123456 IP=0`
	ENC=123456	Klucz szyfrowania TRK.	`CONNECT 123456 ENC=123456`
	APN=nazwa	Nazwa APN karty SIM.	`CONNECT 123456 APN=INTERNET`
	USER=nazwa	Nazwa użytkownika APN.	`CONNECT 123456 USER=User`
	PSW=hasło	Hasło APN.	`CONNECT 123456 PSW=Password`

Pierwsze sprawdzenie

Komenda `INFO` to najszybszy sposób, by na miejscu sprawdzić, że karta SIM działa, centrala przyjmuje komendy i jaka jest siła sygnału. Odpowiedź przychodzi w ciągu kilku sekund.

5.4 Sterowanie połączeniem telefonicznym

Nie w każdej wersji

Sterowanie połączeniem nie działa w centralach **SP3_xx7x**. Typ **SP3_12xx** z firmware 1.14 lub nowszym nie odtwarza komunikatów głosowych, ale komendy z klawiatury telefonu nadal działają.

Warunki:

1. Numer telefonu dzwoniącego jest na karcie **Users & Reporting** → **Users**, a u użytkownika zaznaczona jest kolumna **PGM** (sterowanie wyjściami z telefonu) albo system jest podzielony na co najmniej jedną partycję, do której użytkownik ma uprawnienia.
2. Pole **Output definition** sterowanego wyjścia ma wartość **Remote control** (6.8). Przy sterowaniu impulsowym wypełnione jest też pole **Pulse time**.

Zadzwoń na numer karty SIM centrali. Centrala odbierze połączenie, a następnie na klawiaturze telefonu wybierz komendę:

Klawisze	Funkcja	Przykład
[1][partycja][#]	Uzbrojenie podanej partycji.	`12#` – uzbrojenie partycji 2
[2][partycja][#]	Rozbrojenie podanej partycji.	`22#` – rozbrojenie partycji 2
[3][wyjście][#][stan]	Sterowanie podanym wyjściem. Stan: 0 – wyłącz, 1 – włącz, 2 – wyłącz na czas impulsu, 3 – włącz na czas impulsu.	`31#1` – włączenie wyjścia 1; `32#3` – włączenie wyjścia 2 na czas impulsu

Tylko w starych centralach SP3_12xx (firmware co najwyżej 1.13), do komunikatów głosowych:

Klawisze	Funkcja	Przykład
[4][#][numer nagrania][#]	Rozpoczęcie nagrywania komunikatu głosowego (1–5).	`4#1#`
[5]	Odsłuchanie przed chwilą nagranego komunikatu.	`5`
[6]	Zapisanie nagrania.	`6`

Nagrywanie komunikatów głosowych

Początek i koniec nagrania sygnalizuje sygnał dźwiękowy. Jeden komunikat trwa maksymalnie 15 sekund. Koniec odsłuchiwania także sygnalizuje sygnał dźwiękowy, a kolejną czynność rozpoczynaj dopiero po nim. Nagrany komunikat centrala odtwarza podczas alarmu użytkownikowi, do którego dzwoni: który komunikat należy do której strefy, określa pole **Sound** strefy (6.7). Połączenie z komunikatem głosowym jest dostępne tylko w wersji SP3_12xx z firmware co najwyżej 1.13.

6. TrikdisConfig – ustawienia szczegółowo

TrikdisConfig to bezpłatny program konfiguracyjny firmy Trikdis działający w systemie Windows. Za jego pomocą odczytujesz i zapisujesz wszystkie ustawienia centrali: lokalnie przez USB lub zdalnie przez chmurę Protegus. Program pobierzesz ze strony trikdis.com (w polu wyszukiwania wpisz: TrikdisConfig).

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

Połączenie przez USB

1. Zainstaluj i uruchom TrikdisConfig.
2. Połącz centralę z komputerem kablem USB Mini-B. Program rozpozna centralę i otworzy okno konfiguracji SP3.
3. Naciśnij przycisk **Read [F4]**. Jeśli program poprosi o kod, wpisz kod administratora lub kod instalatora (6.2.6). Przy fabrycznym kodzie administratora program o nic nie pyta.
4. Ustaw, co trzeba, a następnie naciśnij przycisk **Write [F5]**. Dopiero wtedy ustawienia trafią do centrali.

Tryb programowania

Jeśli podłączysz kabel USB do działającej centrali będącej pod napięciem, centrala przejdzie w tryb programowania i do odłączenia kabla nie realizuje zadań alarmowych. W działającym systemie uprzedź użytkownika, a na koniec odłącz kabel.

Przyciski w górnym wierszu: **Read [F4]** – odczyt z centrali; **Write [F5]** – zapis do centrali; **Open [F8]** – otwarcie ustawień zapisanych wcześniej w pliku; **Save [F9]** – zapis bieżących ustawień do pliku; **Disconnect** – rozłączenie. Okna w menu po lewej stronie: **System Options**, **Reporting to CMS**, **Users & Reporting**, **Modules**, **Wireless sensors**, **Zones**, **PGM**, **Sensors**, **System events**, **Events Log** i **Firmware** (aktualizacja oprogramowania, rozdział 9). W lewym dolnym rogu widać pola wyboru **Remember password** i **Show passwords**, przycisk **Default settings** → **Restore** (6.12) oraz numer **IMEI/Unique ID** centrali.

Zapisz do pliku

Plik zapisany przyciskiem **Save [F9]** to dokumentacja systemu. Po wymianie płyty lub przywróceniu ustawień fabrycznych przyciskiem **Open [F8]**, a potem **Write [F5]** wczytasz całość w kilka minut.

Centralę możesz skonfigurować także zdalnie: na ekranie startowym TrikdisConfig w polu **Remote access** wpisz numer **IMEI/Unique ID** centrali i naciśnij przycisk **Configure** (rysunek w punkcie 6.6.2, cała procedura w rozdziale 7). Warunkiem jest włączona usługa chmurowa (6.4.3) i działające połączenie sieciowe.

6.1 Pasek stanu

Gdy centrala jest podłączona, dolny wiersz programu i pole w lewym dolnym rogu pokazują dane urządzenia.

Pole	Znaczenie
IMEI/Unique ID	Unikalny identyfikator centrali. W wersji z modemem jest to IMEI, w wersji WiFi/Ethernet identyfikator sprzętowy. Wymaga go aplikacja Protegus 2 oraz **Remote access**.
Status	Stan operacji (na przykład „reading done”).
Device	Typ centrali w postaci SP3_xxxx.
SN	Numer seryjny centrali.
BL	Wersja programu rozruchowego (bootloadera).
FW	Wersja oprogramowania (firmware).
HW	Wersja sprzętu.
State	Sposób połączenia: **USB** lub zdalne.

Pole	Znaczenie
Role	Poziom dostępu po wpisaniu kodu: **Administrator** lub **Installer**.



Rysunek 50. Pasek stanu TrikdisConfig. Wartości **IMEI/Unique ID** i **SN** zostały na rysunku ukryte.

Przycisk **Read [F4]** odczytuje i wyświetla ustawienia zapisane w centrali. Dalej omawiamy pola okno po oknie.

6.2 System Options

Składa się z sześciu zakładek: **System general**, **Partitions**, **Scheduler**, **Holidays**, **System troubles** i **Access**.

6.2.1 Zakładka System general

Grupa **General**:

- **Object ID** – identyfikator obiektu, czterocyfrowa liczba szesnastkowa (0–9, A–F). Nadaje go stacja monitorowania (CMS); potrzebny tylko wtedy, gdy centrala raportuje do stacji monitorowania. Nie można użyć FFFE i FFFF.
- **Object name** – nazwa obiektu, maksymalnie 20 liter i cyfr. Pojawia się w raportach SMS.
- **Test period** – jeśli zaznaczysz, centrala wysyła raport testowy w takich odstępach czasu, chyba że zaznaczone jest także **Start test at** i podano godzinę.
- **Start test at** – codzienna godzina raportu testowego.
- **Areas in test SMS** – testowy SMS zawiera także stan podanych partycji.
- **Clear Events after reset** – przy ponownym uruchomieniu niewysłane jeszcze zdarzenia są usuwane z bufora.
- **Text language** – SMS-y używają znaków specyficznych dla wybranego języka.
- **Suspend event reporting when … same events per … s** – wstrzymanie przesyłania zdarzeń, jeśli to samo zdarzenie powtarza się w podanym czasie więcej razy niż podana liczba (na przykład uszkodzona czujka). **Restore event reporting after** – po tylu minutach (0–999) centrala znów raportuje zdarzenie.
- **Call** – przy zdarzeniu centrala dzwoni do użytkownika tyle razy. Jeśli połączenie zostanie odebrane lub odrzucone, nie dzwoni dalej. Jedno połączenie trwa 20 sekund.
- **EOL Type** – wartości rezystorów końca linii podłączonych do stref: RT to rezystor sabotażu, R1 – 1. czujki, R2 – 2. czujki. Podłączenie pokazuje rozdział 3.
- **Communication path test** – co taki czas centrala wysyła do stacji monitorowania wiadomość próbną także kanałami zapasowymi, a następnie wraca na kanał główny.
- **LED out as 2Wire fire** – zaznacz, jeśli do wyjścia LED podłączasz dwuprzewodową czujkę pożarową.

Grupa **SIM**:

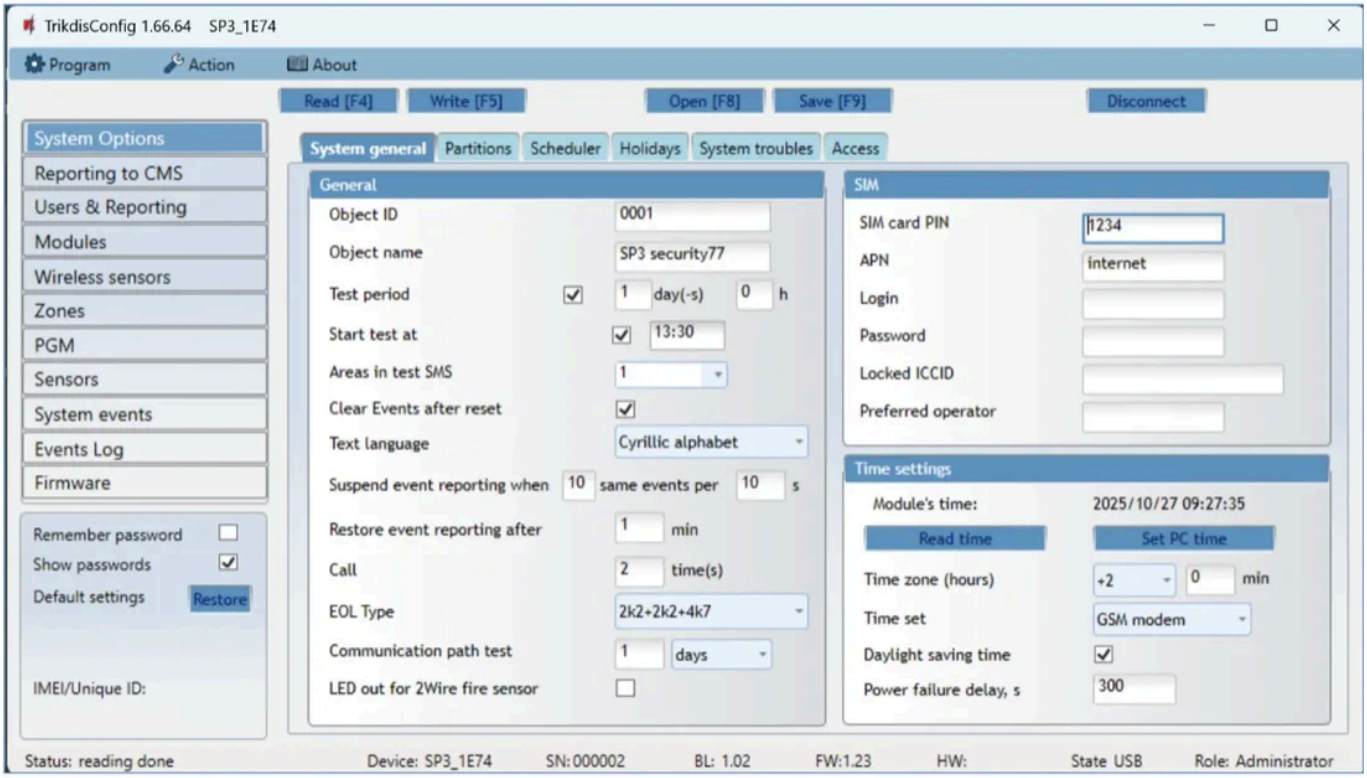
- **PIN** – kod PIN karty SIM. Jeśli karta nie wymaga PIN-u, pozostaw wartość fabryczną.
- **APN** – nazwa punktu dostępu do internetu operatora komórkowego. Obowiązkowa, jeśli centrala raportuje przez internet mobilny do chmury Protegus lub do stacji monitorowania.
- **Login**, **Password** – nazwa użytkownika i hasło APN, tylko jeśli operator ich wymaga.
- **Locked ICCID** – numer ICCID karty SIM. Jeśli go wypełnisz, centrala działa tylko z tą kartą.
- **Preferred operator** – kod operatora (MCC + MNC). Jeśli go wypełnisz, centrala loguje się tylko do sieci tego operatora.

Kody operatorów – przykład: Polska

Plus 26001, T-Mobile 26002, Orange 26003, Play 26006. Kod twojego operatora składa się w ten sam sposób z kodu MCC kraju i kodu MNC operatora. Jeśli pole pozostanie puste, centrala wybiera sieć automatycznie; kod wpisz tylko wtedy, gdy centrala ma pozostać w określonej sieci.

Grupa **Time settings**:

- **Set PC time** – zapisuje do centrali czas komputera. Jeśli w polu **Time synchronization** ustawiono **Disabled**, ten czas pozostaje; jeśli **modem** lub **server**, centrala po włączeniu synchronizuje się z tego źródła.
- **Time zone (Hours)** – strefa czasowa; w Polsce (Europa Środkowa) +1.
- **Time set** – serwer czasu, z którym centrala synchronizuje się po włączeniu.
- **Daylight saving time** – automatyczna zmiana czasu letniego i zimowego.
- **AC failure delay** – zanik zasilania sieciowego centrala zgłasza z takim opóźnieniem; jego powrót także z opóźnieniem.

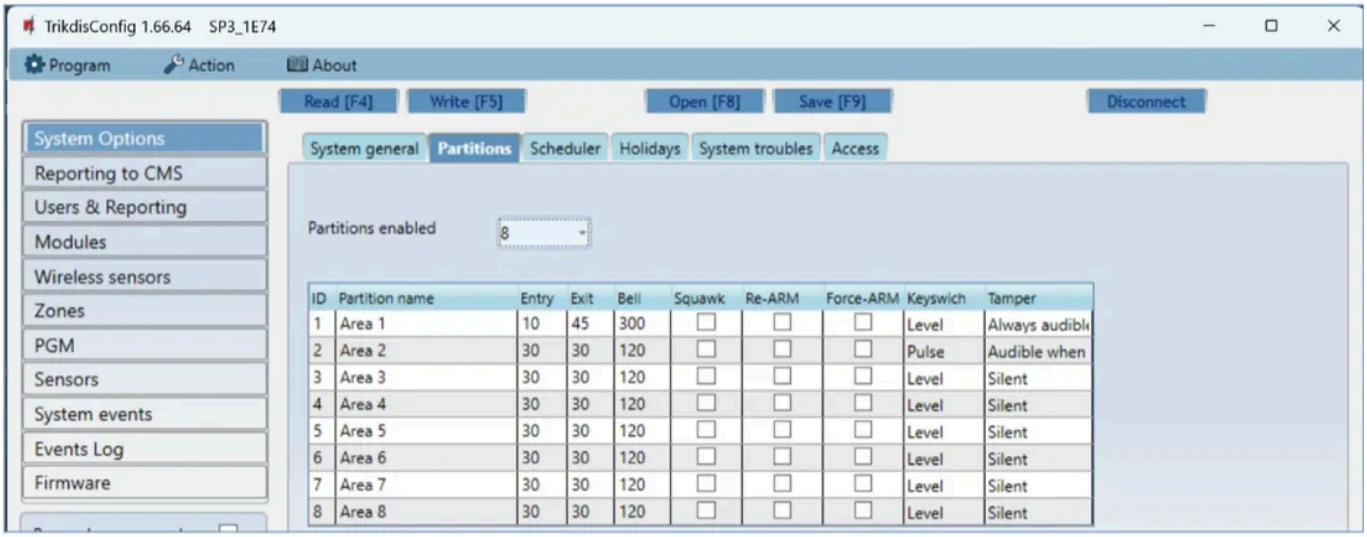


Rysunek 51. System Options → System general: grupy General, SIM i Time settings.

6.2.2 Zakładka Partitions

- **Partitions enabled** – na ile niezależnych części (partycji) dzielisz system.
- **Partition name** – nazwa partycji.
- **Entry** – czas na wejście, 0–999 s. Tyle masz czasu, aby przejść przez strefę Delay do manipulatora i rozbroić system.
- **Exit** – czas na wyjście, 0–999 s. Po uzbrojeniu – licząc od wpisania kodu uzbrajającego na manipulatorze – tyle masz czasu, aby opuścić pomieszczenie przez strefę Delay. Przy uzbrajaniu zdalnym (na przykład z Protegus 2) system uzbraja się natychmiast, bez czasu na wyjście.
- **Bell** – czas działania sygnalizatora przy alarmie, 0–999 s.
- **Squawk** – sygnalizator przy uzbrojeniu piknie raz, przy rozbrojeniu dwa razy.

- **Re-ARM** – automatyczne ponowne uzbrojenie, jeśli system rozbrojono zdalnie, ale w czasie na wejście nikt nie naruszył strefy Delay.
- **Force-ARM** – uzbrojenie wymuszone. System można uzbroić także wtedy, gdy strefy Stay są otwarte, o ile strefa wejściowa jest zamknięta.
- **Keyswitch** – strefa klucza uzbraja i rozbraja impulsem (**Pulse**) lub poziomem (**Level**).
- **Tamper** – obsługa zdarzenia sabotażu, gdy centrala wykryje sabotaż czujki: **Silent** (do odbiorców idzie tylko raport, sygnalizator milczy), **Audible when armed** (raport idzie, sygnalizator włącza się tylko, gdy sabotaż nastąpi w uzbrojonym systemie), **Always Audible** (raport idzie, a sygnalizator włącza się także w rozbrojonym systemie).

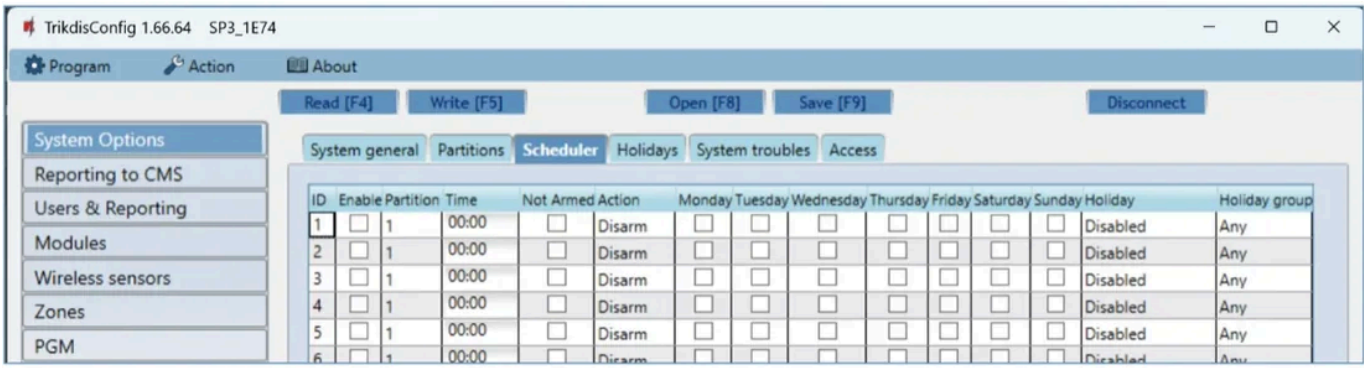


Rysunek 52. System Options → Partitions: czasy na wejście, na wyjście i czas sygnalizatora oraz zachowanie dla każdej partycji.

6.2.3 Zakładka Scheduler

Automatyczne uzbrajanie i rozbrajanie według dni tygodnia, z uwzględnieniem świąt.

- **Enable** – włączenie harmonogramu.
- **Partition** – której partycji dotyczy.
- **Time** – godzina wykonania operacji.
- **Not Armed** – operacja wykona się tylko wtedy, gdy centrala nie jest uzbrojona w trybie pełnym (Away).
- **Action** – tryb do ustawienia: **Disarm**, **Arm**, **Sleep** lub **Stay**.
- **Monday … Sunday** – w które dni obowiązuje.
- **Holiday** – zachowanie w dzień świąteczny: **Disabled** (brak święta), **Ignore on holidays** (w święto się nie wykonuje), **Additional when holidays** (wykonuje się także w święto), **Only holidays** (wykonuje się tylko w święto).
- **Holiday group** – którą grupę świąt (**Any**, 1–4) traktować jako święto. Przy **Any** liczy się każde aktywne święto.



Rysunek 53. System Options → Scheduler: tygodniowy plan uzbrajania i rozbrajania.

6.2.4 Zakładka Holidays

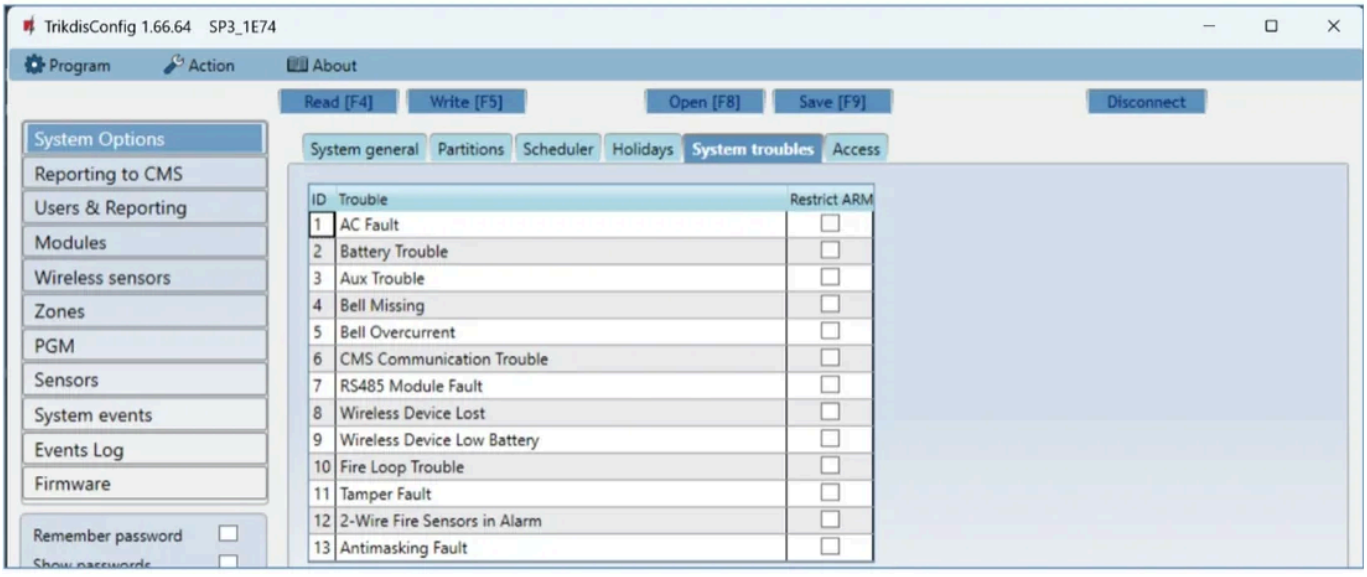
- **Enable** – włączenie święta.
- **Start date**, **Stop date** – pierwszy i ostatni dzień święta. Przy święcie jednodniowym obie daty są takie same.
- **Group 1 … Group 4** – święta układasz w grupy, harmonogram odwołuje się do nich.



Rysunek 54. System Options → Holidays: dni świąteczne w czterech grupach.

6.2.5 Zakładka System troubles

Jeśli zaznaczysz tu usterkę wewnętrzną, systemu nie da się uzbroić, dopóki ta usterka trwa. W ten sposób możesz wymusić, aby na przykład nie uzbrajano systemu z rozładowanym akumulatorem lub bez zasilania sieciowego.



Rysunek 55. System Options → System troubles: które usterki blokują uzbrojenie.

6.2.6 Zakładka Access

Grupa **Access codes**:

- **Administrator Code** – wartość fabryczna 123456. Pełny dostęp do ustawień. Sześć znaków, litery łacińskie i/lub cyfry.
- **SMS password** – wartość fabryczna 123456. Hasło poleceń SMS (5.3), dzięki któremu możesz bezpiecznie sterować systemem SMS-em; ze względów bezpieczeństwa zmień je na sześciocyfrowe hasło znane tylko tobie.
- **Installer Code** – wartość fabryczna 654321. Dostęp instalatora do ustawień; ze względów bezpieczeństwa zmień go na sześciocyfrowy kod znany tylko tobie.

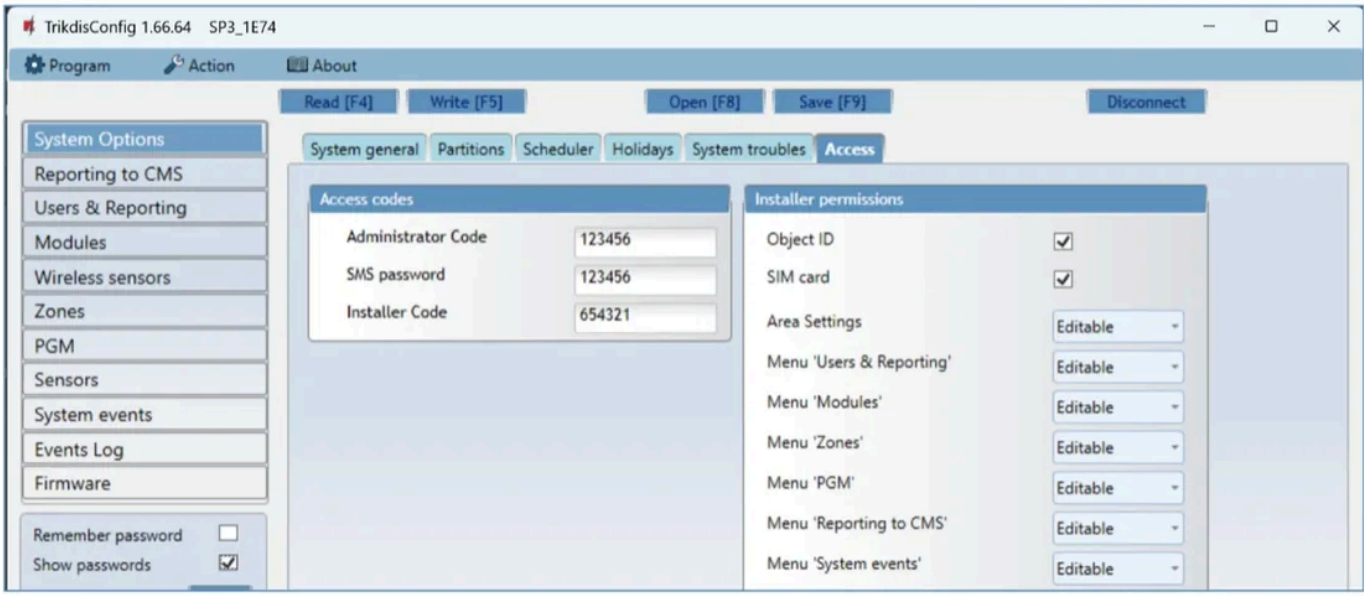
Grupa **Installer permissions** – tu określasz, co może ustawiać osoba logująca się kodem instalatora.

Fabryczny kod administratora

Dopóki kod administratora ma fabryczną wartość 123456, po **Read [F4]** program pokazuje ustawienia bez pytania o kod.

Przed przekazaniem

Przed przekazaniem systemu zmień wszystkie trzy kody. Kod administratora należy do właściciela; kod instalatora i jego uprawnienia właściciel może później zmienić.



Rysunek 56. System Options → Access: trzy kody i uprawnienia instalatora.

6.3 Reporting to CMS

Centrala wysyła zdarzenia do stacji monitorowania (CMS) przez internet mobilny (IP) lub SMS-em. Możesz podać kilka kanałów: kanał główny (**Primary**) i równoległy (**Parallel**) działają jednocześnie, więc zdarzenia mogą otrzymywać dwa odbiorniki; do każdego z nich można przypisać kanał zapasowy (**Backup**), który włącza się, gdy połączenie kanału głównego lub równoległego zostanie przerwane. Połączenie jest szyfrowane i chronione hasłem, do odbioru potrzebny jest odbiornik Trikdis: przez IP programowy odbiornik IPcom, sprzętowy odbiornik RL14 lub RM14; do SMS-ów RL14, RM14 lub GM14. SMS nadaje się na kanał zapasowy, bo działa także bez internetu mobilnego; jako kanał główny nie jest zalecany.

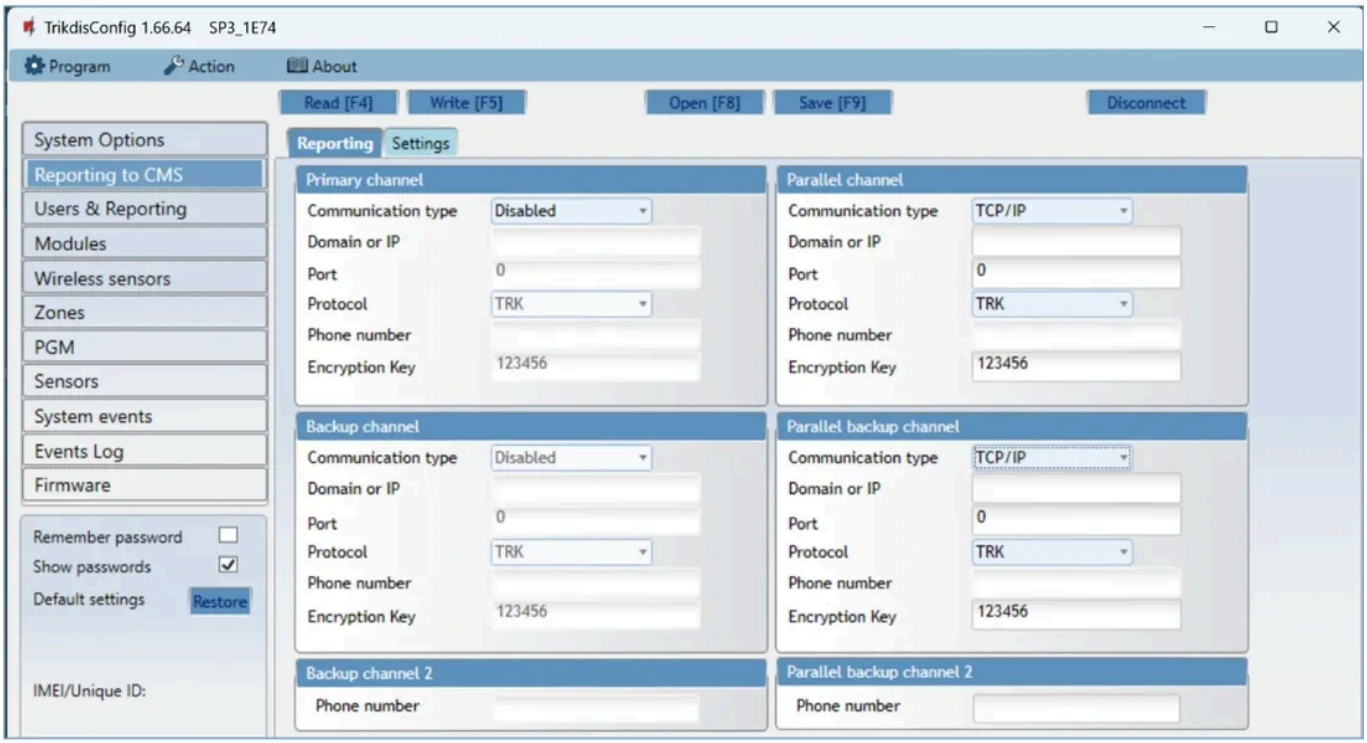
6.3.1 Zakładka Reporting

Grupy **Primary channel**, **Backup channel**, **Parallel channel** i **Parallel backup channel**:

- **Communication type** – protokół używany z odbiornikiem: **TCP/IP**, **UDP/IP**, **SMS** lub **Disabled**.
- **Domain or IP** – nazwa domeny lub adres IP odbiornika.
- **Port** – port odbiornika.
- **Protocol** – **TRK** dla odbiornika Trikdis, **SIA DC-09** dla odbiornika IP przyjmującego format SIA DC-09.
- **Phone number** – tylko przy SMS: numer telefonu odbiornika SMS Trikdis z międzynarodowym kodem kraju (na przykład 48…).
- **Encryption key** – sześciocyfrowy klucz szyfrowania, musi być zgodny z kluczem odbiornika.

Jeśli wypełnisz także kanał równoległy, zdarzenia idą jednocześnie oboma kanałami, więc otrzymują je jednocześnie dwa odbiorniki (na przykład lokalna i centralna stacja monitorowania). Oba kanały nie mogą wskazywać na ten sam odbiornik.

Backup channel 2 i **Parallel backup channel 2** – zapas SMS: w polu **Phone number** wpisujesz numer odbiornika SMS stacji monitorowania (z kodem kraju). Centrala wysyła tutaj, jeśli nie uda się wysłać ani kanałem głównym, ani równoległym, ani zapasowym; jest to szczególnie przydatne, bo działa także wtedy, gdy w sieci operatora komórkowego nie ma połączenia IP. Działa tylko wtedy, gdy pierwszy kanał i jego zapas są kanałami IP. SMS jest wysyłany przy pierwszym włączeniu oraz wtedy, gdy połączenie IP na pierwszym kanale i na jego zapasie zostanie przerwane.



Rysunek 57. Reporting to CMS → Reporting: kanały główne, zapasowe i równoległe.

6.3.2 Zakładka Settings

Grupa **Settings**:

- **Return to primary after** – po tylu minutach centrala próbuje wrócić na kanał główny.
- **IP Ping period** – odstęp sygnałów kontrolnych połączenia IP w sekundach; włącza się go zaznaczeniem.

- **SMS Ping period** – odstęp sygnałów kontrolnych kanału SMS w minutach; włącza się go zaznaczeniem.
- **Backup reporting after** – po tylu nieudanych wysyłkach centrala przełącza się na kanał zapasowy.
- **DNS1**, **DNS2** – adresy serwerów DNS. Przy każdym ustawieniu IP podaj adres DNS obsługiwany przez operatora.
- **Object ID in SIA DC-09**, **SIA DC-09 receiver No.**, **Line No.** – numer obiektu, numer odbiornika i numer linii dla protokołu SIA DC-09.
- **Local time in SIA** – w wiadomościach wysyłanych do stacji monitorowania podawany jest czas własny centrali.

Grupa **Reporting mode** – którą drogą centrala ma się komunikować ze stacją monitorowania i z Protegus 2. Kolejność typów ma znaczenie: jeśli połączenie **Main type** nie powstanie, centrala przełącza się na drogę **Backup type**, a potem **Backup type 2**.

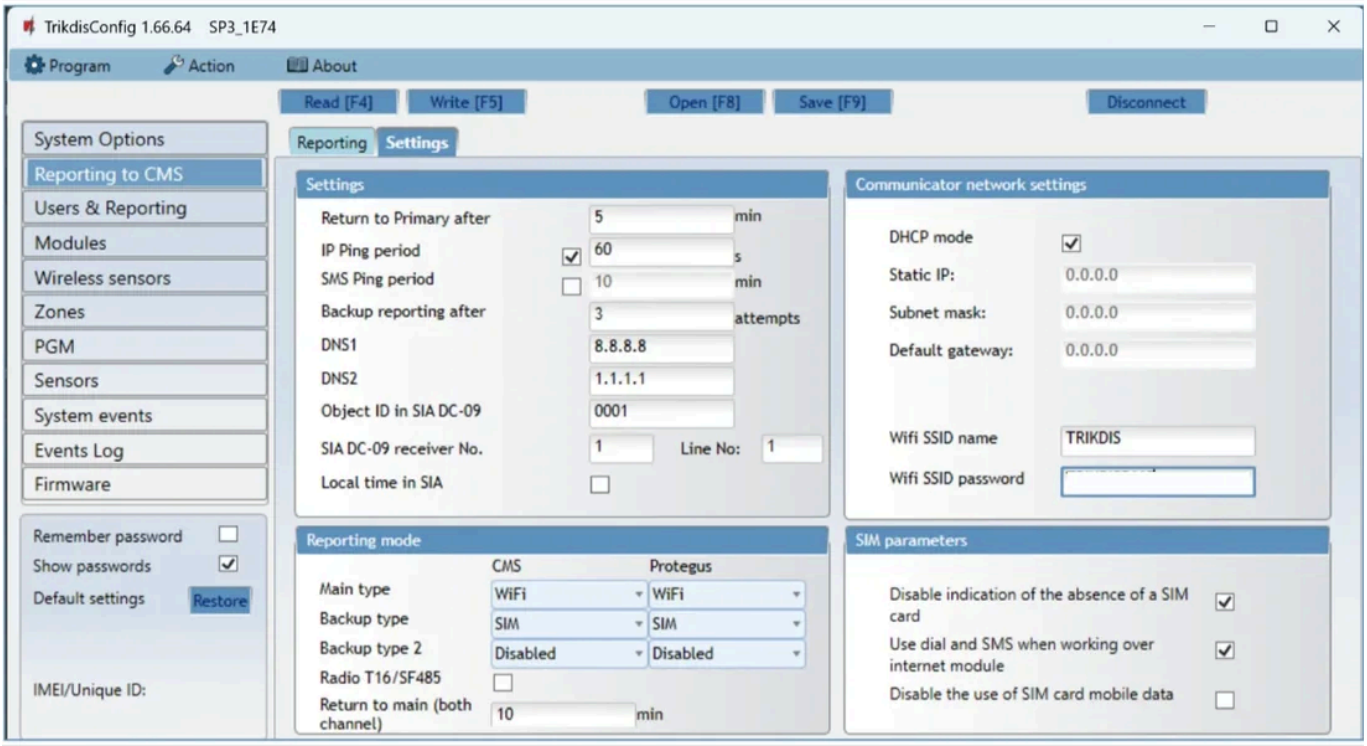
- **Main type**, **Backup type**, **Backup type 2** – **SIM**, **WiFi** lub **LAN(E485)**, osobno w kolumnie CMS i Protegus.
- **Radio T16 (SF485)** – zaznacz, jeśli wysyła także nadajnik radiowy T16. T16 działa jako kanał zapasowy, jeśli używane jest co najmniej jedno z połączeń SIM, WiFi lub LAN; jeśli innego połączenia nie ma, T16 jest kanałem głównym. T16 wysyła raporty tylko do stacji monitorowania.
- **Return to main (both channel)** – po tylu minutach centrala próbuje wrócić na drogę główną, jeśli wysyłała drogą zapasową.

Grupa **Communicator network settings** (wersja WiFi):

- **DHCP mode** – po zaznaczeniu centrala automatycznie otrzymuje adres IP, maskę podsieci i bramę.
- **Static IP**, **Subnet mask**, **Default gateway** – do ustawienia ręcznego.
- **WiFi SSID name**, **WiFi SSID password** – nazwa i hasło sieci WiFi.

Grupa **SIM parameters**:

- **Disable indication of the absence of a SIM card** – centrala nie sygnalizuje braku karty SIM.
- **Use dial and SMS when working over internet module** – po zaznaczeniu połączenia głosowe i SMS działają także wtedy, gdy centrala raportuje przez WiFi lub LAN. Bez zaznaczenia, gdy jest WiFi, centrala nie używa SMS-ów ani połączeń; jeśli bez zaznaczenia nie ma WiFi, centralą nadal można sterować połączeniem i SMS-em, a centrala wysyła SMS-y do użytkownika.
- **Disable the use of SIM card mobile data** – centrala nie używa danych mobilnych karty SIM, wysyła tylko przez WiFi. Jeśli WiFi chwilowo zaniknie, przechowuje zdarzenia i wysyła je później.

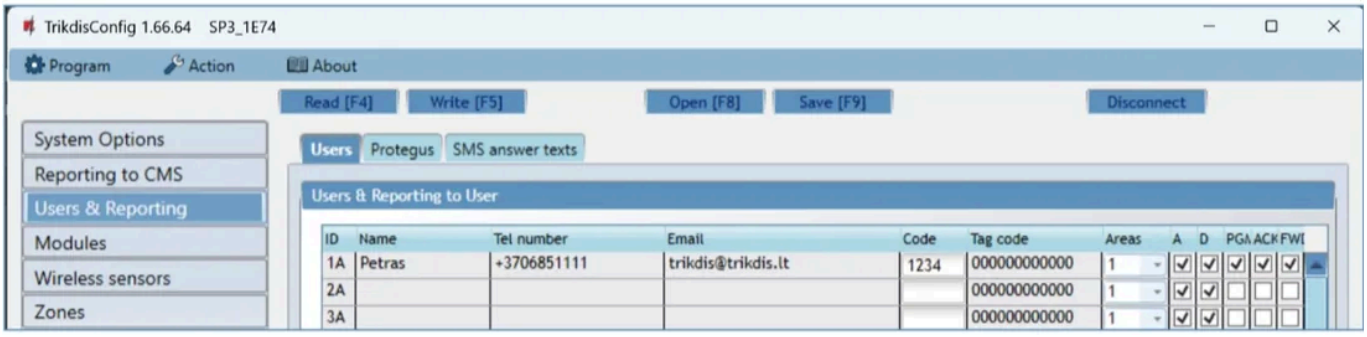


Rysunek 58. Reporting to CMS → Settings: sygnały kontrolne, kolejność połączeń, parametry WiFi i SIM.

6.4 Users & Reporting

W wierszach zakładki **Users** (grupa **Users & Reporting to User**) dodajesz użytkowników:

- **Name** – nazwa użytkownika, pojawia się w SMS-ach o zdarzeniach.
- **Tel number** – numer telefonu z międzynarodowym kodem kraju. Z tego numeru użytkownik może sterować systemem i na niego otrzymuje SMS-y. Pierwsze osiem numerów otrzymuje raporty SMS-em i połączeniem.
- **Email** – adres e-mail; użytkownik otrzymuje zaproszenie do Protegus 2.
- **Code** – kod użytkownika do uzbrajania i rozbrajania.
- **Tag code** – numer identyfikacyjny karty RFID, breloka RFID lub klucza iButton.
- **Areas** – którymi partycjami może sterować.
- **A**, **D** – może uzbrajać lub rozbrajać.
- **PGM** – może przełączać wyjścia połączeniem telefonicznym, sygnałami DTMF (5.4).
- **ACK** – centrala potwierdza SMS-em wykonanie otrzymanych poleceń.
- **FWD** – SMS-y od osób niebędących użytkownikami (informacja o saldzie, reklama) centrala przekazuje temu użytkownikowi.



Rysunek 59. Users & Reporting → Users: użytkownicy, kody, identyfikatory i uprawnienia.

6.4.1 Karty i breloki RFID

Karty i breloka RFID nie uczysz przez przyłożenie do czytnika: numer identyfikacyjny karty wpisujesz ręcznie jako liczbę dziesiętną w polu **Tag code**, a następnie **Write [F5]**. Numer jest wydrukowany na większości kart.



Rysunek 60. Numery wydrukowane na karcie RFID: pierwsza grupa cyfr w ramce to **Tag code**.

Jeden czytnik Wiegand bez manipulatora, do otwierania drzwi

1. Przewody danych czytnika podłączasz do zacisków **GRN** i **YEL** płyty.
2. Na zakładce **Modules** → **Keypads** w grupie **Keypad parameters** ustaw **Keypad type** na **Wiegand reader**, także wtedy, gdy nie ma manipulatora.
3. W oknie **PGM** w polu **Output definition** sterowanego wyjścia ustaw **Remote control**, a **Pulse time, s** na przykład na 5.
4. Na zakładce **PGM** → **Control** w wierszu czytnika zaznacz pole **En**, w polu **PGM** wpisz numer wyjścia, a **PGM mode** ustaw na **Pulse**.

6.4.2 Klucze iButton

Uczenie czytnikiem **TM17**:

1. Jeśli lista **Tag code** jest pusta, pierwszy wprowadzony klucz trafia do pierwszego wiersza listy i staje się kluczem głównym (Master).
2. Aby włączyć tryb uczenia, przytrzymaj klucz główny przy „oku" czytnika co najmniej 10 sekund. W trybie uczenia dioda **State** czytnika TM17 miga na zielono.
3. Przykładaj klucze użytkowników do czytnika po kolei. Trzy sygnały dźwiękowe oznaczają, że klucz został dodany do systemu.
4. Na koniec ponownie przyłóż klucz główny do czytnika; dioda **State** przestaje migać.
5. Aby usunąć wszystkie klucze (razem z kluczem głównym), przytrzymaj klucz główny przy czytniku co najmniej 20 sekund.

Z czytnikiem **CZ-Dallas** tak samo, tylko bez sygnalizacji diodą: klucz główny przez 10 sekund, klucze użytkowników po kolei, na koniec ponownie klucz główny; usuwanie – 20 sekund.

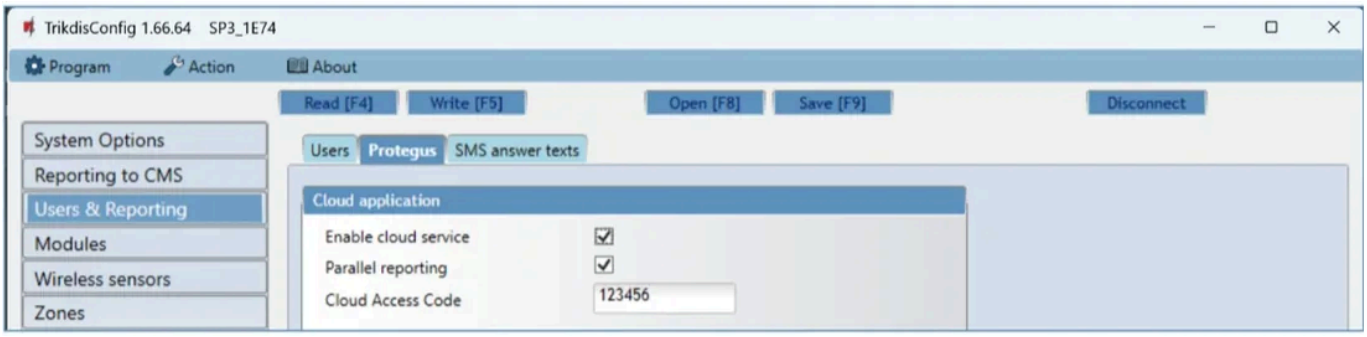
Rola klucza głównego

Klucz główny służy do wprowadzania pozostałych kluczy. Jeśli używasz go także do uzbrajania i rozbrajania, polecenie jest wykonywane z opóźnieniem.

6.4.3 Zakładka Protegus

Grupa **Cloud application**:

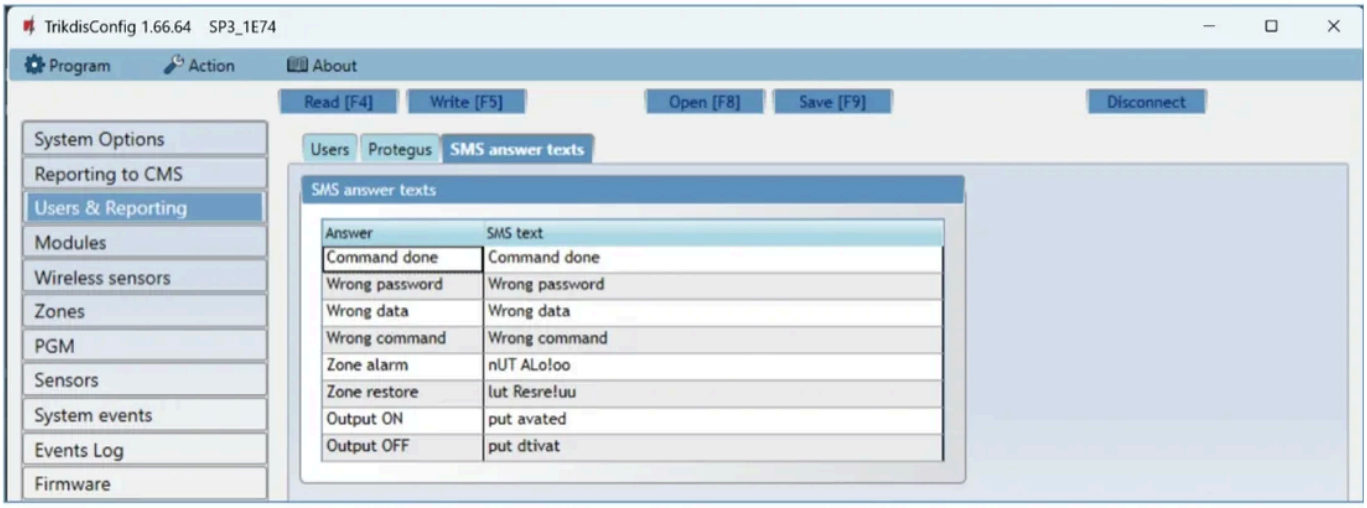
- **Enable cloud service** – włączenie chmury Protegus. Przez nią centrala komunikuje się z Protegus 2 i przez nią można ją zdalnie konfigurować w TrikdisConfig.
- **Parallel reporting** – zdarzenia idą jednocześnie kanałem głównym do stacji monitorowania i do Protegus 2.
- **Cloud access code** – sześciocyfrowy kod połączenia z Protegus 2, wartość fabryczna 123456.



Rysunek 61. Users & Reporting → Protegus: przełącznik usługi chmurowej i kod dostępu.

6.4.4 Zakładka SMS answer texts

Treść odpowiedzi na polecenia SMS możesz zmienić w kolumnie **SMS text**, na przykład na język polski.



Rysunek 62. Users & Reporting → SMS answer texts: treść SMS-ów z odpowiedziami.

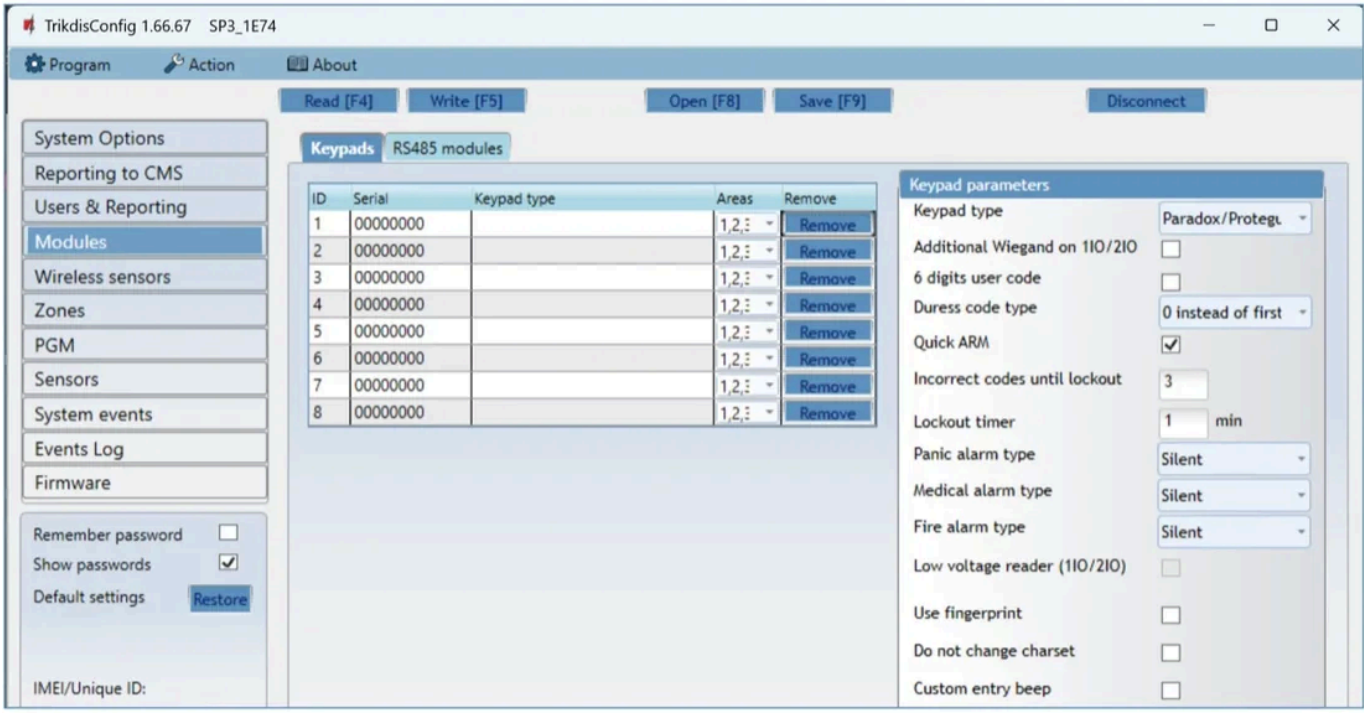
6.5 Modules

Zakładka **Keypads**:

- **Serial** – numer seryjny manipulatora, centrala rozpoznaje go automatycznie. Aby go usunąć, wpisz zera lub naciśnij przycisk **Remove**.
- **Keypad type** – typ manipulatora, rozpoznawany automatycznie.
- **Areas** – którymi partycjami może sterować manipulator (tylko w manipulatorach FLEXi SK LCD, FLEXi SK LED, SK LCD Button i SK LED Button).
- **Remove** – usunięcie manipulatora z listy.

Grupa **Keypad parameters**:

- **Keypad type** – typ manipulatora podłączonego do zacisków **GRN** i **YEL**: **Crow CR16**, **Paradox LED** lub **Wiegand reader**.
- **Additional Wiegand on 1IO/2IO** – zaznacz, jeśli do zacisków **IO1** i **IO2** podłączasz drugi czytnik RFID. Nie można ich wtedy używać jako wejść ani wyjść.
- **6 digits user code** – sześciocyfrowy kod użytkownika na manipulatorze. Do istniejącego kodu czterocyfrowego program dopisuje dwie pierwsze cyfry (z 1234 powstaje 123412); w ten sposób przekształcany jest każdy czterocyfrowy kod użytkownika.
- **Duress code type** – typ kodu przymusu. Pod przymusem uzbrajasz nim lub rozbrajasz system: system wykonuje polecenie i po cichu wysyła alarm do stacji monitorowania.
- **Quick ARM** – przyciski **ARM**, **STAY** i **SLEEP** manipulatora uzbrajają bez kodu.
- **Incorrect codes until lockout** – po tylu błędnych kodach manipulator się blokuje.
- **Lockout timer** – czas blokady w minutach.
- **Panic alarm type**, **Medical alarm type**, **Fire alarm type** – działanie przycisków funkcyjnych manipulatora: napadowego, medycznego i pożarowego po ich naciśnięciu: **Audible** (włącza się sygnalizator, manipulator daje głośny alarm, a raport idzie do Protegus 2 i do stacji monitorowania), **Silent** (do Protegus 2 i do stacji monitorowania idzie tylko raport, centrala wyłącza głośny alarm), **Disabled** (raport nie idzie ani do Protegus 2, ani do stacji monitorowania).
- **Low voltage reader (1IO/2IO)** – jeśli podłączony czytnik RFID nie działa, przełączasz tym protokół między centralą a czytnikiem.
- **Use fingerprint** – dla czytnika linii papilarnych z protokołem Wiegand 26/34.
- **Do not change charset** – na manipulatorze SK-LCD TouchPad kodowanie znaków nazw stref i partycji pozostaje bez zmian.
- **Custom entry beep** – dźwięk czasu na wejście na manipulatorze jest przerywany.

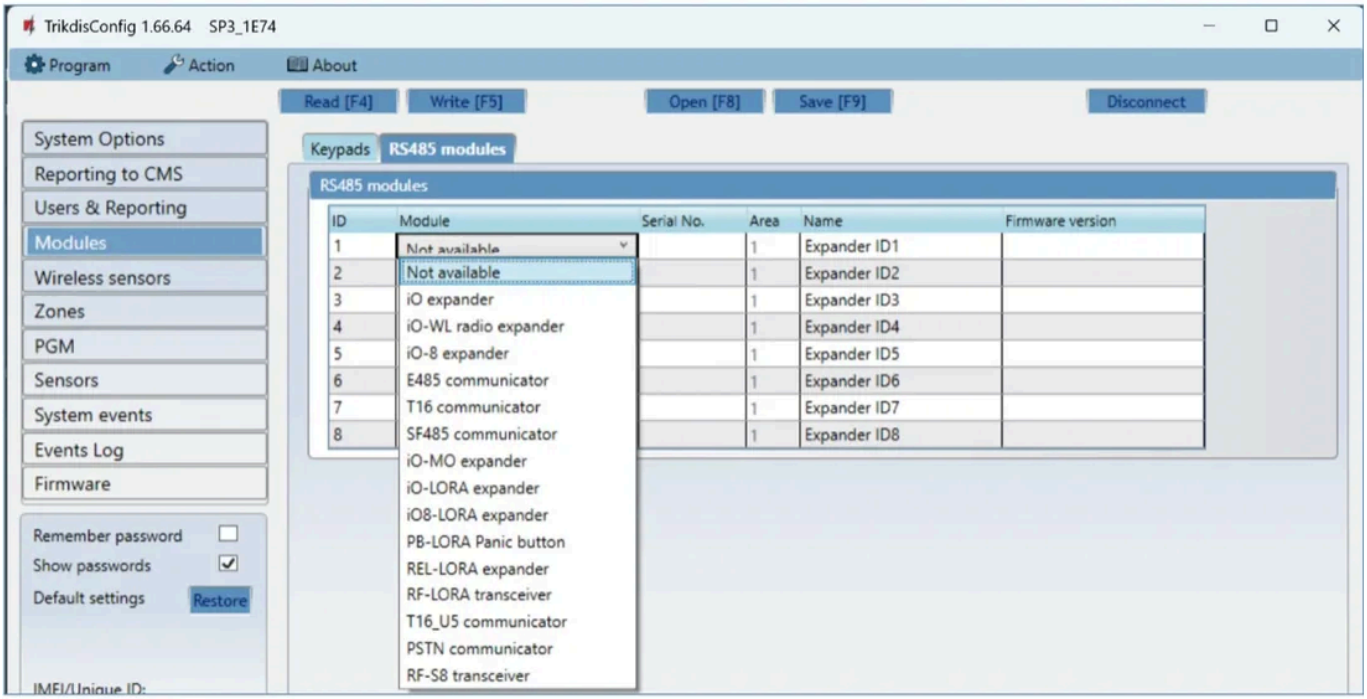


Rysunek 63. Modules → Keypads: rozpoznane manipulatory i parametry manipulatorów.

Zakładka **RS485 modules**:

- **ID** – numer kolejny modułu.
- **Module** – typ ekspandera z listy: iO, iO-WL, TM17, iO-8, RF-SH, E485, T16, SF485, iO-MO, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-LORA, RF-HW, RF-S8.
- **Serial No.** – obowiązkowa, sześciocyfrowa liczba z naklejki na obudowie i opakowaniu modułu.

- **Area** – partycja modułu. TM17 pokazuje stan i strefy tej partycji.
- **Name** – nazwa modułu.
- **Firmware version** – gdy tylko centrala znajdzie moduł, pojawia się tu wersja jego oprogramowania. Jest to znak, że moduł działa.



Rysunek 64. Modules → RS485 modules: lista ekspanderów z listą rozwijaną **Module**.

Zakładka **E485 settings** – ustawienia sieciowe komunikatora LAN E485: **DHCP mode** (adres automatyczny: po zaznaczeniu centrala automatycznie odczytuje ustawienia sieci – maskę podsieci, bramę – i automatycznie otrzymuje adres IP) lub do ustawienia ręcznego **Static IP**, **Subnet mask**, **Default gateway**.



Rysunek 65. Modules → E485 settings: adresacja modułu LAN E485.

6.6 Wireless sensors

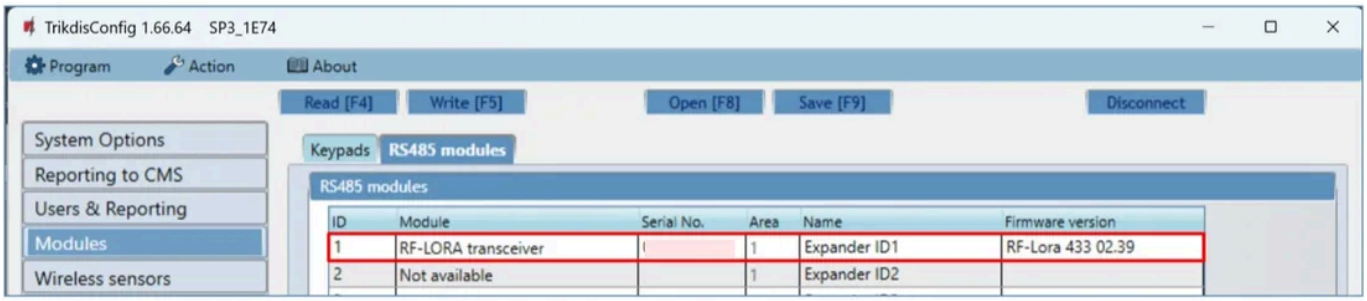
Z modułem RF-LORA centrala „FLEXi" SP3 używa bezprzewodowych czujek, sygnalizatorów i pilotów producenta Maximum. Wymaga to w centrali oprogramowania z kodem odbiornika 4, co najmniej w wersji 1.21 (SP3_xxx4_0121 lub nowszej; 4. cyfra nazwy oprogramowania to typ odbiornika, zob. 1.7). Nadajnik-odbiornik RF-LORA podłączasz do magistrali RS485 centrali (4.6). Najpierw rejestrujesz moduł RF-LORA w centrali (6.6.1), potem uczysz czujki: zdalnie z TrikdisConfig (6.6.2) lub przyciskiem LEARN modułu (6.6.3). Parowanie czujek S8 działających z odbiornikiem RF-S8 opisuje rozdział 4 instrukcji nadajnika-odbiornika RF-S8 i czujek S8.



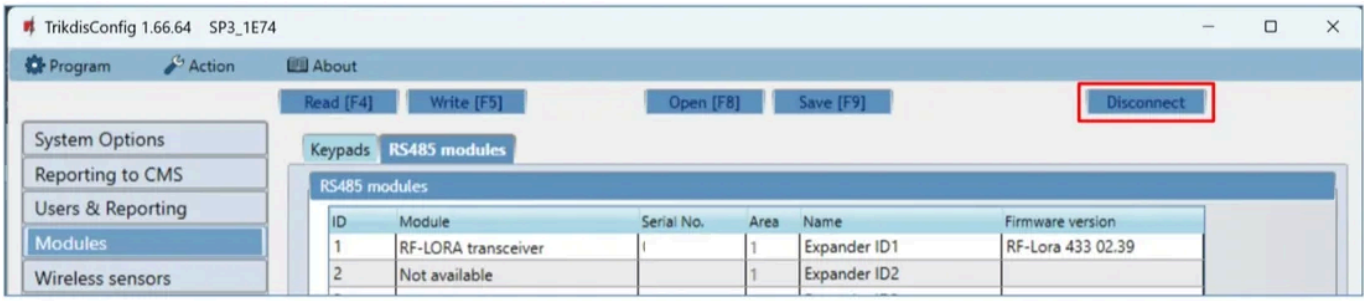
Rysunek 66. Okno **Wireless sensors**: lista wprowadzonych urządzeń, nad nią przyciski **Learn sensors** i **Update**.

6.6.1 Rejestracja RF-LORA

1. Włącz zasilanie centrali i odczekaj 1 minutę.
2. Uruchom TrikdisConfig i podłącz centralę do komputera kablem USB Mini-B.
3. Naciśnij przycisk **Read [F4]** i otwórz zakładkę **Modules** → **RS485 modules**. Jeśli na liście jest **RF-LORA transceiver** z numerem seryjnym i wersją oprogramowania, gotowe – pozostałe kroki pomijasz.
4. Jeśli go nie ma, w pustym wierszu w polu **Module** wybierz pozycję **RF-LORA transceiver**.
5. W polu **Serial No.** wpisz numer seryjny modułu z naklejki na obudowie lub opakowaniu.
6. **Write [F5]**, a następnie odłącz kabel USB.
7. Odczekaj 1 minutę, aż centrala i RF-LORA się połączą.
8. Podłącz ponownie kabel USB i naciśnij przycisk **Read [F4]**. W oknie **Modules** pojawi się wersja oprogramowania RF-LORA: moduł jest zarejestrowany.
9. Odłącz kabel USB, naciśnij przycisk **Disconnect** i odczekaj 1 minutę.



Rysunek 67. Na zakładce **RS485 modules** wiersz zarejestrowanego RF-LORA: typ, **Area**, nazwa i **Firmware version**. Numer seryjny został na rysunku ukryty.

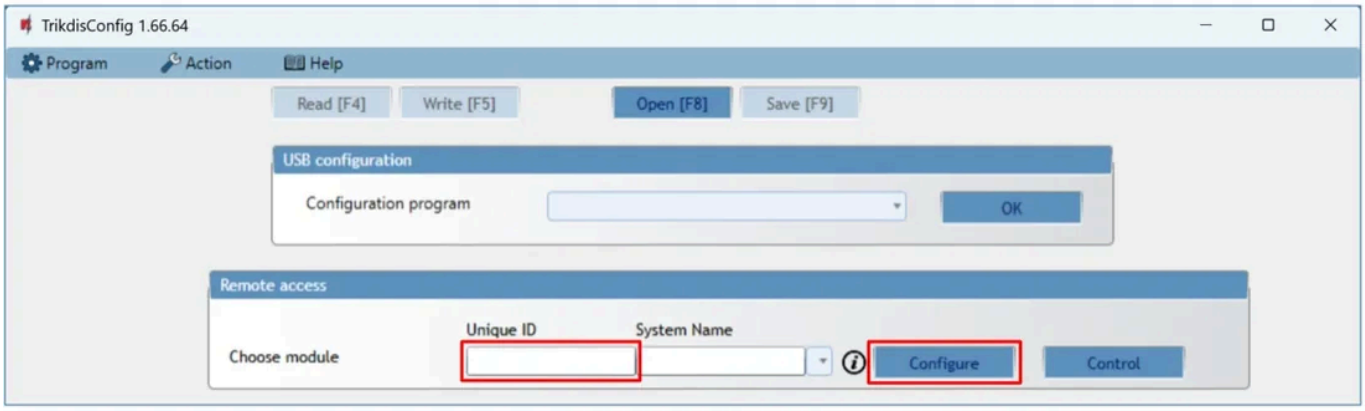


Rysunek 68. Po odczycie pojawia się wersja oprogramowania RF-LORA, następnie **Disconnect**.

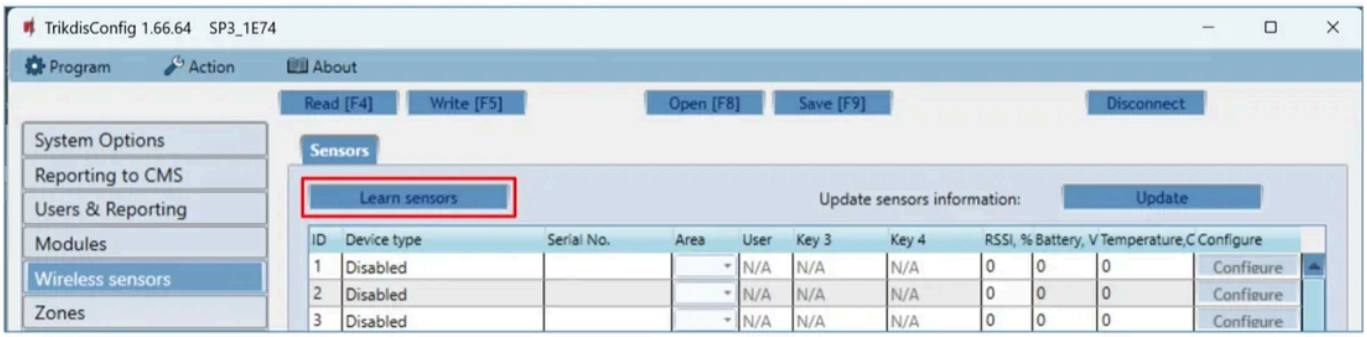
6.6.2 Zdalne parowanie czujek

Warunki zdalnej konfiguracji: aktywowana karta SIM z podanym lub wyłączonym PIN-em i internetem mobilnym (lub połączenie WiFi), włączona usługa chmurowa (6.4.3), zasilanie i połączenie sieciowe (dioda **NET** świeci stale na zielono).

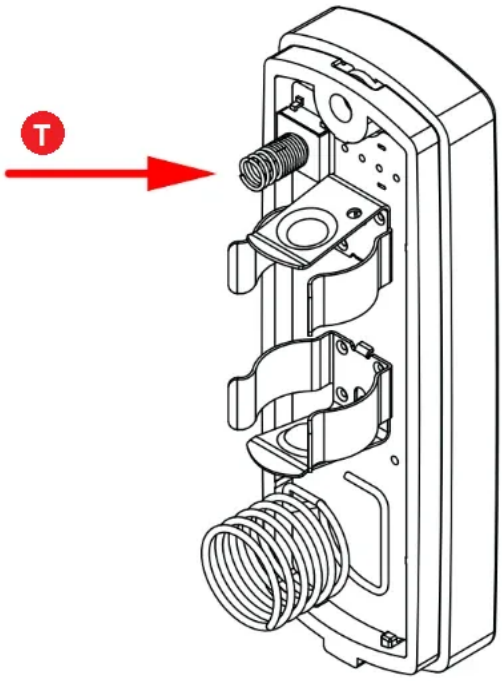
1. Na ekranie startowym TrikdisConfig w polu **Unique ID** grupy **Remote access** wpisz numer **IMEI/Unique ID** centrali (z naklejki na płycie i na opakowaniu) i naciśnij przycisk **Configure**.
2. W otwartym oknie **Read [F4]**; w razie potrzeby wpisz kod administratora lub instalatora.
3. Otwórz okno **Wireless sensors** i naciśnij przycisk **Learn sensors**. RF-LORA przechodzi w tryb uczenia, jego dioda **DATA/TROUBLE** zaczyna migać na zielono-czerwono, a TrikdisConfig otwiera okno uczenia.
4. Włóż baterie do czujek (czujki ruchu, otwarcia, zalania, dymu, sygnalizator). Możesz wprowadzać kilka czujek jednocześnie. RF-LORA powinien być co najmniej 1 m od czujek.
5. Naciśnij przycisk **TAMPER** (sabotaż) czujki. Dioda **DATA/TROUBLE** RF-LORA krótko mignie na zielono (czujka została dodana), a po kilku sekundach znów miga na zielono-czerwono.
6. TrikdisConfig otwiera nowe okno: podaj wartości **Zone number** i **Zone definition** czujki, następnie **Save**. Czujka trafia na listę.
7. Przy następnej czujce znów przycisk **TAMPER** i tak dalej. Na koniec naciśnij przycisk **Stop learning**.
8. Na pytanie odpowiedz **Yes**: czujki zostaną zapisane w centrali (**No**, jeśli chcesz jeszcze coś w nich zmienić). Odczekaj kilka minut, potem **Read [F4]**: w oknie **Wireless sensors** widać wprowadzone czujki, a w kolumnie **Serial No.** ich numery seryjne.
9. W oknie **Zones** sprawdź, czy czujki trafiły do właściwej strefy i partycji. Jeśli pole **Type** strefy ma wartość **EOL_T**, działa także nadzór sabotażu czujki. Po zmianie **Write [F5]**.



Rysunek 69. Grupa **Remote access** na ekranie startowym: **Unique ID**, **System Name**, **Configure**.

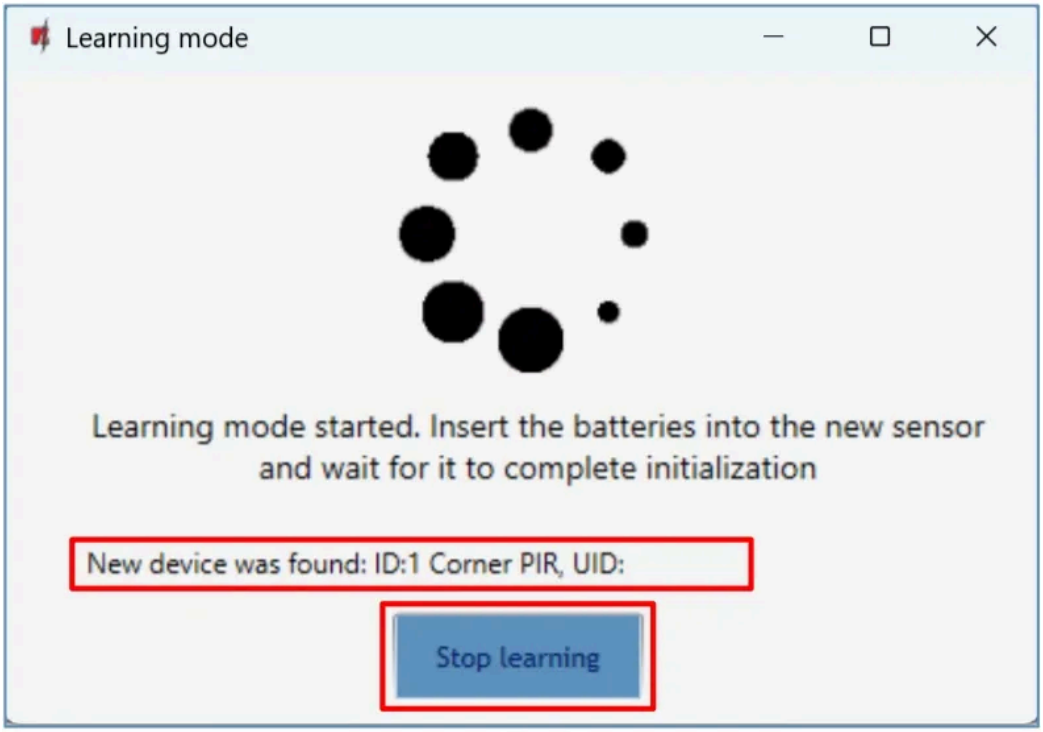


Rysunek 70. Przycisk **Learn sensors** w oknie **Wireless sensors** uruchamia tryb uczenia.

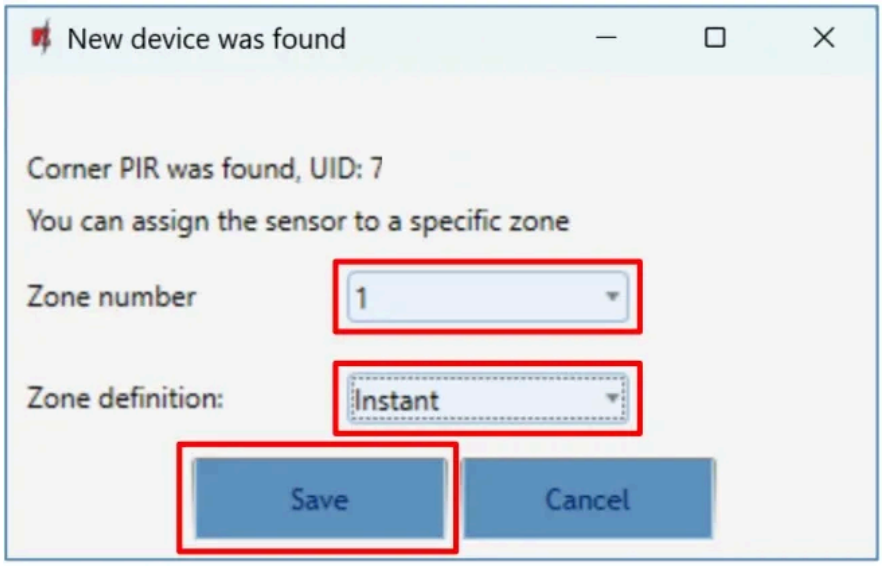


Rysunek 71. Naciśnięcie przycisku **TAMPER** pod tylną pokrywą czujki zgłasza czujkę.

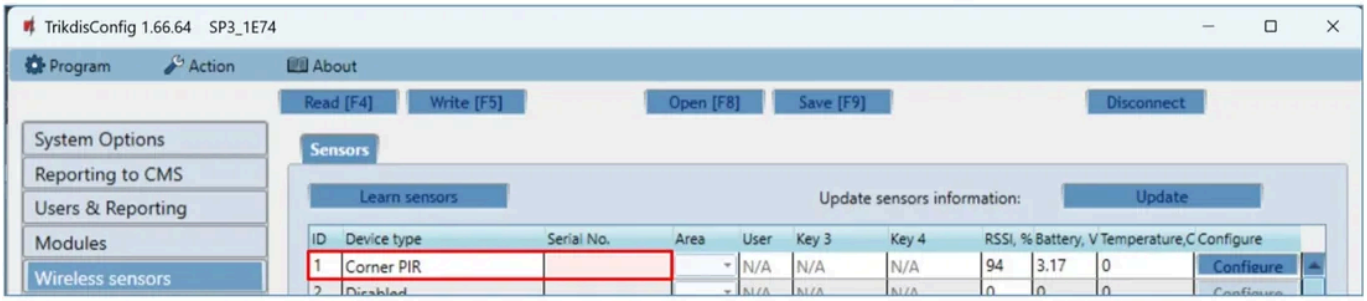
- T przycisk sabotażu („Tamper”)



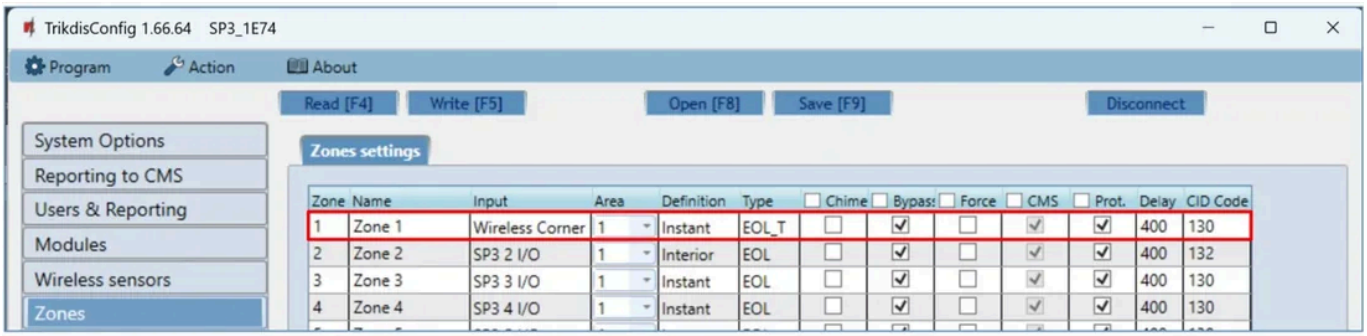
Rysunek 72. Okno uczenia: typ i identyfikator znalezionej czujki, poniżej przycisk **Stop learning**. Identyfikator został na rysunku ukryty.



Rysunek 73. Okno nowego urządzenia: **Zone number**, **Zone definition**, **Save**.



Rysunek 74. Wprowadzona czujka na liście, z siłą sygnału (**RSSI**), napięciem baterii i temperaturą. Numer seryjny został na rysunku ukryty.



Rysunek 75. W oknie **Zones** strefa czujki bezprzewodowej z typem **EOL_T**: nadzorowany jest także sygnał sabotażu.

Usuwanie czujki bezprzewodowej

Połącz się z centralą przez USB lub zdalnie, **Read [F4]**, następnie w kolumnie **Device type** okna **Wireless sensors** przy czujce do usunięcia wybierz pozycję **Disabled** i **Write [F5]**.

6.6.3 Parowanie przyciskiem LEARN

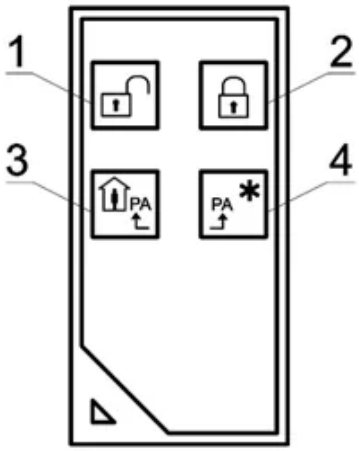
1. RF-LORA musi być zarejestrowany w centrali (6.6.1), a centrala włączona.
2. Zdejmij pokrywę RF-LORA. Naciśnij i przytrzymaj przycisk **LEARN**, aż dioda **DATA/TROUBLE** zacznie migać na zielono-czerwono, a następnie go puść. Miganie oznacza tryb uczenia.
3. Włóż baterie do czujek i naciśnij przycisk **TAMPER** czujki. Krótkie zielone mignięcie diody **DATA/TROUBLE** oznacza sukces, po kilku sekundach znów miga na zielono-czerwono. Przy następnej czujce znów przycisk **TAMPER**.

4. Na koniec naciśnij i przytrzymaj przycisk **LEARN**, aż zielono-czerwone miganie ustanie, a następnie go puść. RF-LORA wyszedł z trybu uczenia.
5. Podłącz centralę przez USB do komputera, uruchom TrikdisConfig, **Read [F4]**. W oknie **Wireless sensors** widać wprowadzone urządzenia z ich siedmiocyfrowymi numerami seryjnymi.
6. W oknie **Zones** sprawdź strefy i partycje, po zmianie **Write [F5]**.

6.6.4 Urządzenia RF-SH i Crow

Starsze systemy z modułem RF-SH używają urządzeń bezprzewodowych serii Crow FW2 i Shepherd (SH). RF-SH nie jest już dostępny; opis pozostał tu w skrócie do serwisowania istniejących systemów, podłączenie modułu pokazuje punkt 4.2.

- **Rejestracja RF-SH** – jak przy RF-LORA (6.6.1): na zakładce **Modules** → **RS485 modules RF-SH**, **Serial No.**, **Write [F5]**, odłącz USB, odczekaj 1 minutę, podłącz USB, **Read [F4]**; pojawienie się wersji oprogramowania oznacza sukces.
- **Czujki FW2** – naciskaj przycisk **LEARN** modułu, aż dioda **LEARN** zacznie migać na zielono. Włóż baterię do czujki i poczekaj, aż jej diody zgasną. Wyjdź przyciskiem **LEARN**, USB, **Read [F4]**: siedmiocyfrowy numer seryjny musi być zgodny z numerem na obudowie. Podaj strefę i partycję, **Write [F5]**. Usuwanie: **Device type** → **Disabled**.
- **Pilot FW2** – przytrzymaj jednocześnie przyciski 3 i 4, aż dioda mignie na żółto, a potem na zielono. Na liście podaj jego partycję i użytkownika; funkcję przycisków 3 i 4 (uzbrojenie, rozbrojenie, cichy lub głośny alarm napadowy) wybierasz w tabeli. Reset pilota: przyciski 2 i 3 jednocześnie, aż zobaczysz zielono-czerwone miganie.
- **Sygnalizator FW2** – włącz zasilanie sygnalizatora; lampa błyskowa przez 30 sekund miga powoli. W tym czasie przytrzymaj przycisk **LEARN** na płytce sygnalizatora, aż lampa zacznie migać szybko, i puść go. Reset: włącz zasilanie, trzymając wciśnięty przycisk **LEARN**, do trzech mignięć.
- **Czujki i manipulator SH** – włóż baterię; świecenie zielonej diody przez 3 sekundy oznacza udane wprowadzenie. Jeśli się nie udało, wyjmij baterię na 10 sekund i spróbuj ponownie.



Rysunek 76. Pilot Crow FW2: do wprowadzenia przytrzymujesz jednocześnie przyciski 3 i 4.

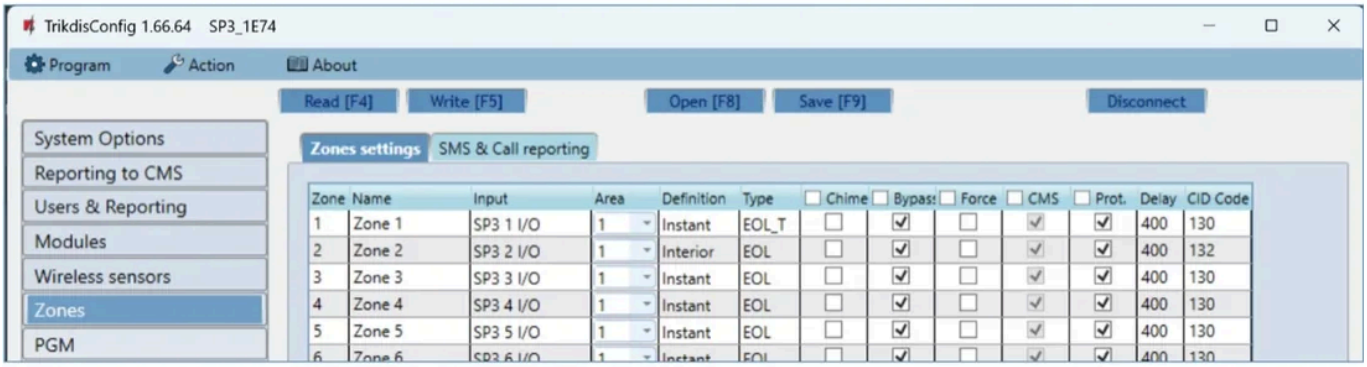
6.7 Zones

Zakładka **Zones settings**:

- **Zone No** – numer kolejny strefy.

- **Name** – nazwa strefy.
- **Input** – które wejście **IN** centrali lub ekspandera należy do strefy.
- **Area** – partycja strefy.
- **Definition** – działanie strefy:
    - **Delay** – strefa opóźniona, dla magnetycznej czujki otwarcia drzwi wejściowych. Dla tego typu strefy możesz ustawić czas na wejście i na wyjście. Po uzbrojeniu, w czasie na wyjście strefę Delay można swobodnie naruszać (można otworzyć drzwi); jeśli po upływie czasu na wyjście jest nadal naruszona, włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy. W uzbrojonym systemie naruszenie strefy Delay uruchamia czas na wejście, w którym trzeba rozbroić system; jeśli nie rozbroisz go do końca czasu na wejście, włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy.
    - **Interior** – strefa nadążna, dla czujki ruchu przy drzwiach wejściowych. W uzbrojonym systemie jej naruszenie włącza wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy. Jeśli w uzbrojonym systemie najpierw zostanie naruszona strefa Delay, strefę Interior można swobodnie naruszać w ustawionym czasie na wejście; jeśli w czasie na wejście nie rozbroisz systemu, włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy.
    - **Interior Stay** – strefa nadążna, dla czujki ruchu przy drzwiach wejściowych; działa tak samo jak Interior: w uzbrojonym systemie jej naruszenie włącza wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy, ale jeśli najpierw została naruszona strefa Delay, w czasie na wejście można ją swobodnie naruszać. W systemie uzbrojonym w trybie STAY strefy Interior Stay nie są chronione (centrala ich nie nadzoruje).
    - **Instant** – strefa natychmiastowa, dla czujek ruchu. Jeśli w uzbrojonym systemie strefa Instant zostanie naruszona, bez czasu na wejście, natychmiast włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy.
    - **Instant Stay** – strefa natychmiastowa, dla czujek ruchu. Jeśli w uzbrojonym systemie strefa Instant Stay zostanie naruszona, natychmiast włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport alarmowy. W systemie uzbrojonym w trybie STAY strefy Instant Stay nie są chronione.
    - **Fire** – dla czujek pożarowych. Jej naruszenie natychmiast uruchamia wyjścia **Siren** i **Flash** i wysyłany jest raport.
    - **Keyswitch** – dla stacyjki (przełącznika z kluczem) lub innego przełącznika: strefa uzbraja i rozbraja. Uzbrojenie następuje po upływie czasu na wyjście.
    - **24_hour** – dla czujek zbicia szyby i czujek sabotażowych. Zawsze nadzorowana, jej naruszenie natychmiast wywołuje alarm: włączają się wyjścia **Siren** i **Flash** i wysyłany jest raport o zdarzeniu.
    - **Silent** – po uzbrojeniu jej naruszenie natychmiast wysyła raport, ale wyjścia **Siren** i **Flash** się nie włączają.
    - **Silent 24h** – dla przycisku napadowego. Niezależnie od stanu systemu natychmiast wysyłany jest raport o zdarzeniu, bez sygnalizatora: wyjścia **Siren** i **Flash** się nie włączają.
- **Type** – typ obwodu podłączonego do wejścia, z listy: **NC** (normalnie zamknięty), **NO** (normalnie otwarty), **EOL** (z rezystorem końca linii), **EOL_T** (z rezystorem końca linii i nadzorem sabotażu), **ATZ** (dwie strefy na jednym wejściu: dwa normalnie zamknięte obwody strefowe z rezystorami końca linii, bez nadzoru sabotażu – dla tego typu wybierz na liście **Input** także drugą strefę ATZ), **ATZ_T** (dwie strefy z nadzorem sabotażu: dwa normalnie zamknięte obwody strefowe z rezystorami końca linii i nadzorem sabotażu – także tu wybierz drugą strefę ATZ na liście **Input**), **3EOL** (z rezystorem końca linii i nadzorem sabotażu, dla czujek ruchu z funkcją przeciw maskowaniu – anti-masking). Wartości rezystorów podajesz w polu **System Options** → **EOL Type** (6.2.1).
- **Chime** – gong: przy otwarciu strefy manipulator piknie.
- **Bypass** – strefę można zablokować (pominąć).

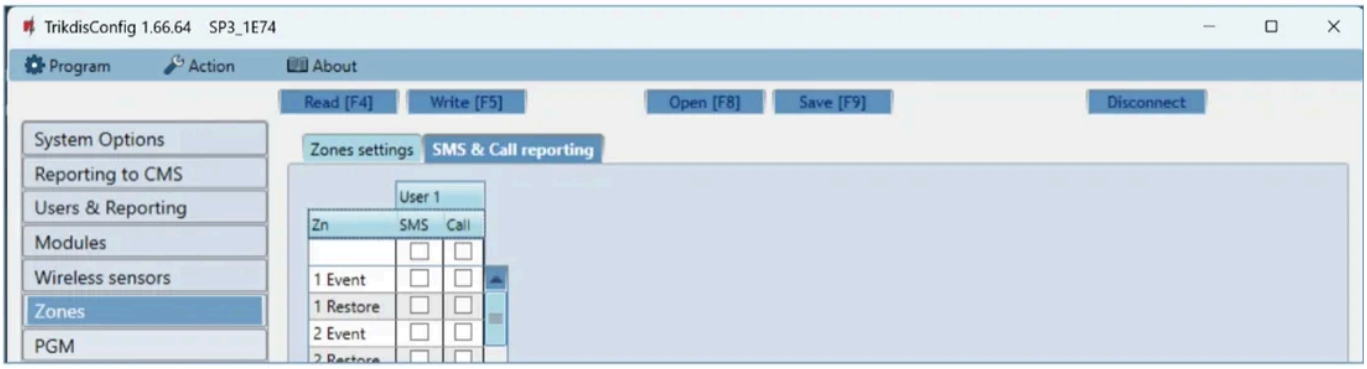
- **Force** – uzbrojenie wymuszone: system można uzbroić także przy otwartej strefie; strefa otwarta w chwili uzbrojenia jest tymczasowo pomijana, po jej zamknięciu (przywróceniu) znów jest nadzorowana, a jej późniejsze naruszenie wywołuje alarm.
- **CMS** – zdarzenia strefy idą do stacji monitorowania.
- **Prot.** – zdarzenia strefy idą do chmury Protegus.
- **Delay** – czas reakcji wejścia w milisekundach.
- **CID code** – kod Contact ID zdarzenia, wypełnia się automatycznie przy wyborze definicji.
- **Sound** – numer komunikatu głosowego, który centrala przy alarmie odtwarza użytkownikowi, do którego dzwoni (tylko SP3_12xx, oprogramowanie najwyżej w wersji 1.13).



Rysunek 77. Zones → Zones settings: definicja, typ obwodu i opcje stref.

Zakładka **SMS & Call reporting** – widoczna tylko wtedy, gdy w oknie **Users & Reporting** jest co najmniej jeden numer telefonu.

- **Zn** – numer strefy i rodzaj zdarzenia: **Event** (alarm) lub **Restore** (przywrócenie).
- **User / SMS and Call** – dla każdego użytkownika zaznaczasz, czy ma otrzymać SMS i/lub połączenie o zdarzeniu strefy.



Rysunek 78. Zones → SMS & Call reporting: kto otrzymuje SMS lub połączenie o zdarzeniach poszczególnych stref.

6.8 PGM

Zakładka **Outputs**:

- **PGM No** – numer kolejny wyjścia PGM.
- **Name** – nazwa wyjścia.
- **PGM output** – które wyjście **OUT** centrali lub ekspandera należy do PGM.
- **Area** – partycja wyjścia.
- **Output definition** – działanie wyjścia:
  - **Siren** – dla sygnalizatora.

- **Remote control** – do przełączania urządzenia zewnętrznego (z aplikacji, SMS-em, połączeniem, czytnikiem).
- **Fire Sensor Reset** – do resetu czujek pożarowych po alarmie.
- **System State** – dla wskaźnika stanu, na przykład dioda LED pokazuje, czy system jest uzbrojony.
- **Flash** – dla lampy błyskowej: po uzbrojeniu sygnał ciągły, przy alarmie impulsowy, po rozbrojeniu zanika.
- **Thermostat** – tryb termostatu. Do centrali musi być podłączona czujka temperatury, utrzymywaną temperaturę podajesz na zakładce **Thermostat**.
- **Buzzer** – powtarza sygnały dźwiękowe manipulatora.

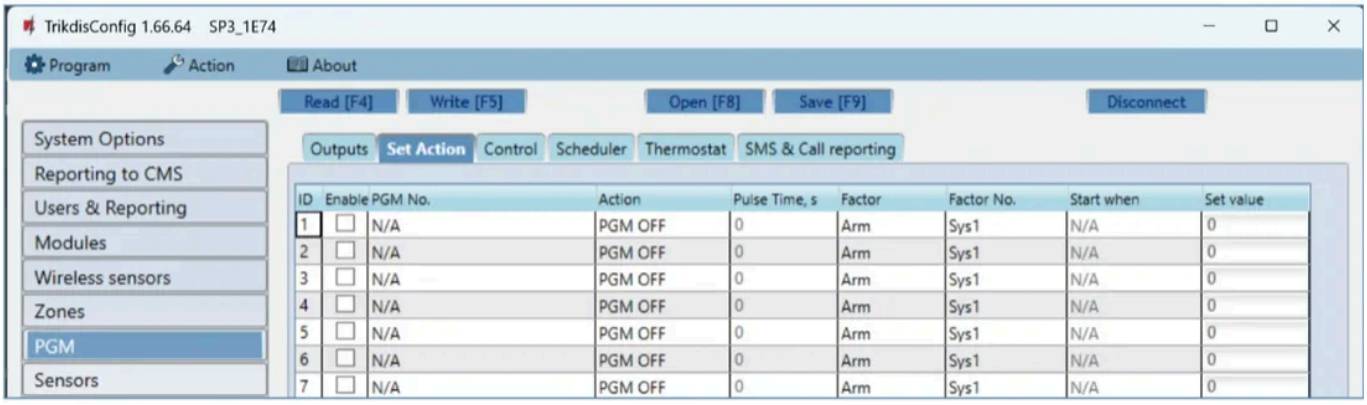
- **Pulse time, s** – czas włączenia przy pracy impulsowej, 0–9999 s.
- **CMS**, **Prot.** – raport o włączeniu i wyłączeniu wyjścia idzie do stacji monitorowania lub do chmury Protegus.



Rysunek 79. PGM → Outputs: definicja wyjść i czas impulsu.

Zakładka **Set Action** – co przełącza wyjście:

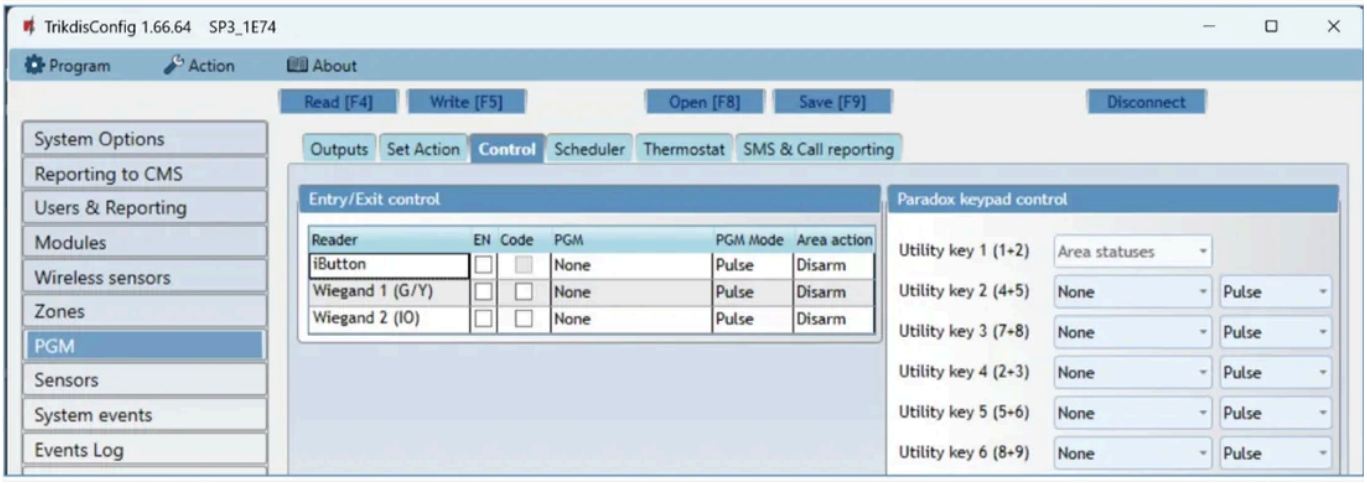
- **ID** – numer wiersza.
- **Enable** – włączenie reguły.
- **PGM No.** – sterowane wyjście, które przełącza zdarzenie opisane w kolumnach **Factor**, **Factor No.**, **Start when** i **Set value**.
- **Action** – **PGM OFF** (wyłącza), **PGM ON** (włącza), **Pulse OFF** (normalnie włączone, wyłączone na czas **Pulse time**), **Pulse ON** (normalnie wyłączone, włączone na czas **Pulse time**).
- **Pulse time, s** – 0–9999 s.
- **Factor**, **Factor No.** – zdarzenie wyzwalające i jego numer: **Zone**, **Sensor**, **Jamming**, **Sensor lost**, **iButton**, **Arm**, **Disarm**, **SMS received**, **Zone(follow)**, **Stay**, **Sleep**, **AC lost**, **Low battery**, **Zone tamper**. Do wyjścia można przypisać także harmonogram – harmonogram pokazuje, kiedy wyjście ma być włączone; na zakładce **Scheduler** można utworzyć najwyżej dziesięć różnych.
- **Start when** – dodatkowy warunek dla zdarzenia wyzwalającego.
- **Set value** – wartość zależna od warunku: treść otrzymanego SMS-a, napięcie lub temperatura. Jeśli centrala rozpozna tę wartość, wykonuje operację wybraną w kolumnie **Action**. Przy SMS-ie słowo kluczowe przełączające wyjście oddzielasz znakami `%` od reszty otrzymanej wiadomości: `%tekst%` – wiadomość zawiera tekst (na przykład `%hoUSe%`: w wiadomości jest „hoUSe", jak w wiadomości `VacationhoUSe25864`); `tekst%` – wiadomość zaczyna się od tekstu (na przykład `hoUSe%`: wiadomość zaczyna się od „hoUSe", jak `hoUSeddss`); `%tekst` – wiadomość kończy się tekstem (na przykład `%hoUSe`: wiadomość kończy się na „hoUSe", jak `1144hoUSe`). Tekst rozróżnia małe i wielkie litery.



Rysunek 80. PGM → Set Action: wyjścia przełączane zdarzeniem, SMS-em lub wartością.

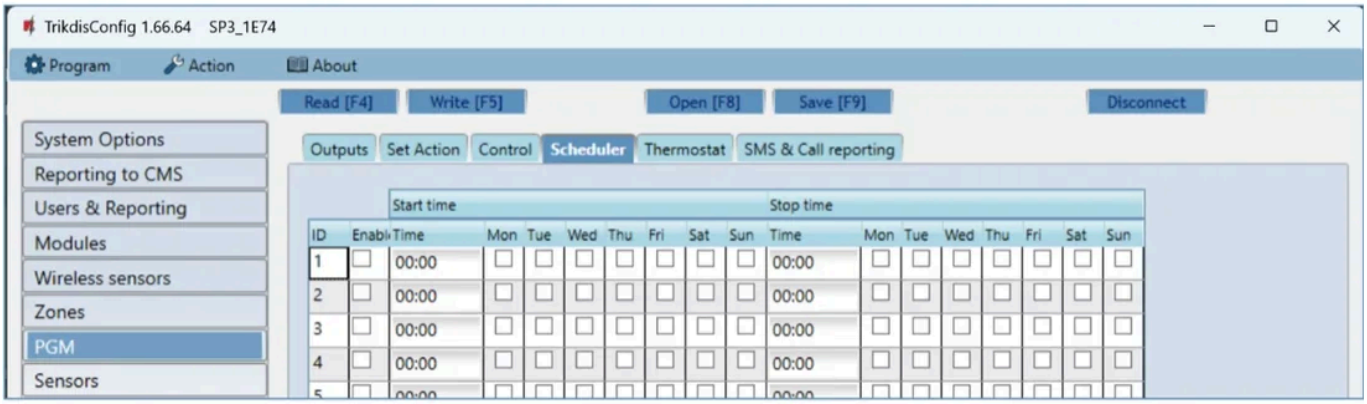
Zakładka **Control**:

- Grupa **Entry/Exit control**: **Reader** – czytniki, które można podłączyć (iButton, Wiegand 1 na zaciskach **G/Y**, Wiegand 2 na zaciskach **IO**); **En** – czytnik może sterować wyjściem; **Code** – operację (przełączenie wyjścia PGM lub sterowanie centralą) można wykonać także kodem użytkownika; **PGM** – sterowane wyjście (musi być w trybie **Remote control**); **PGM mode** – **Pulse** lub **Level**; **Area action** – co ma się stać ze stanem uzbrojenia systemu, gdy do czytnika zostanie przyłożony klucz lub karta.
- Grupa **Paradox keypad control**: **Utility key** – przytrzymanie przycisku pomocniczego manipulatora przez 3 sekundy przełącza wyjście: na czas impulsu (**Pulse**) lub zmienia jego stan (**Level**).



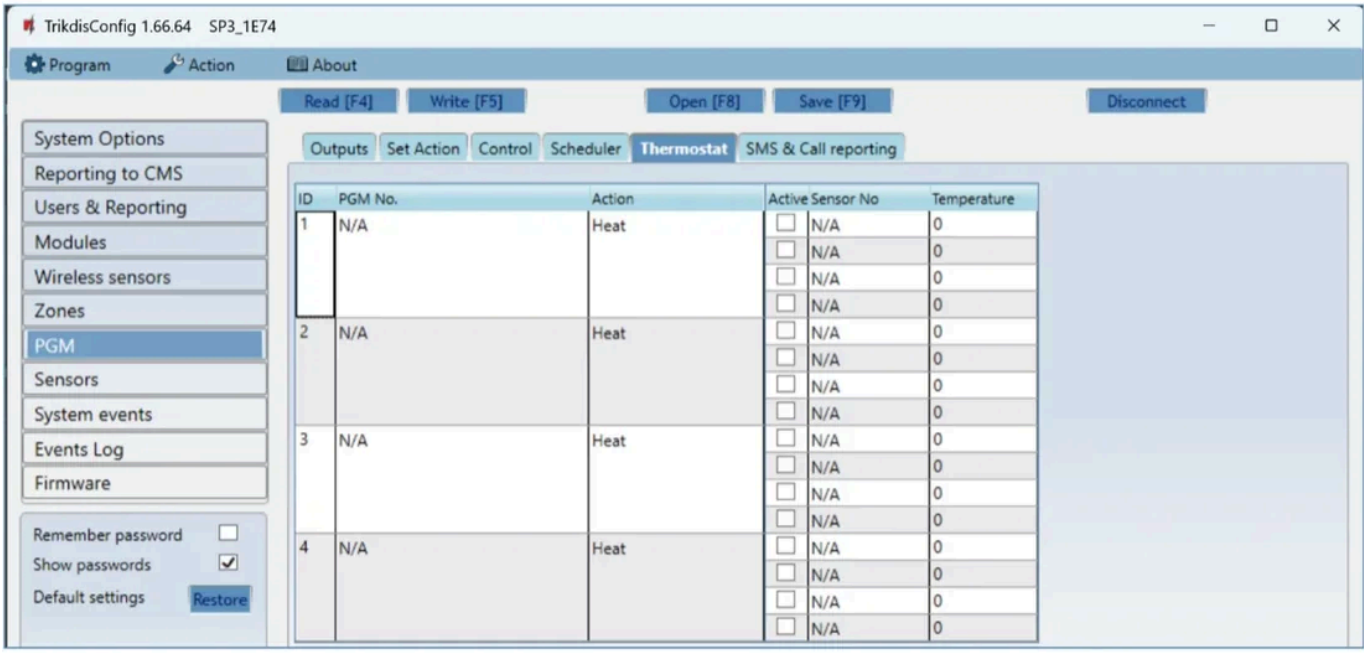
Rysunek 81. PGM → Control: sterowanie wyjściami z czytników i przycisków manipulatora Paradox.

Zakładka **Scheduler** – **ID**, **Enable**, **Start time** (włączenie), **Stop time** (wyłączenie), **Mon – Sun** (dni).



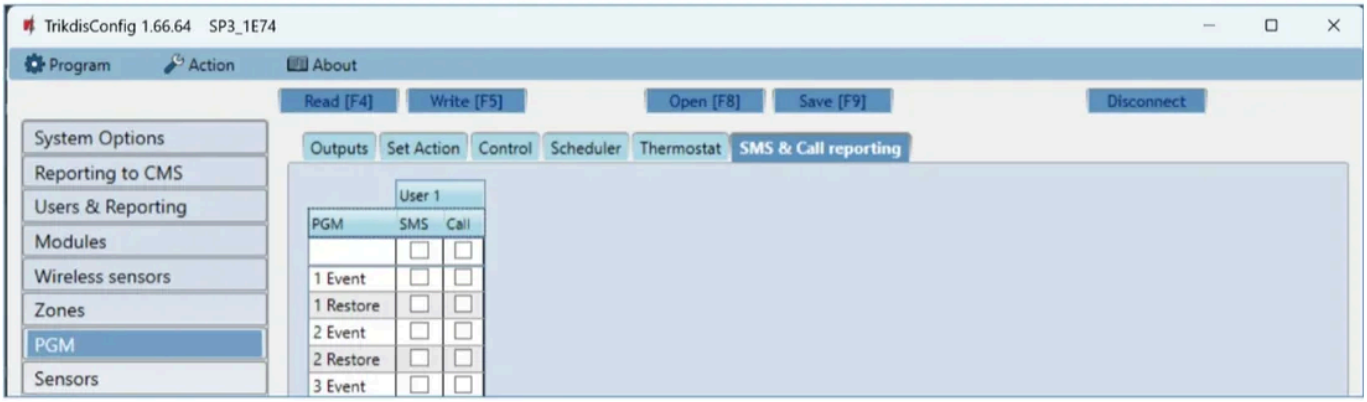
Rysunek 82. PGM → Scheduler: harmonogram wyjść, najwyżej dziesięć harmonogramów.

Zakładka **Thermostat** – **ID**; **PGM No.** (sterowane wyjście); **Action** (grzanie lub chłodzenie); **Active** (termostat działa z wybraną czujką); **Sensor No** (czujka temperatury); **Temperature** (utrzymywana temperatura).



Rysunek 83. PGM → Thermostat: wyjście do regulacji temperatury.

Zakładka **SMS & Call reporting** – widoczna tylko wtedy, gdy jest numer telefonu użytkownika, i można ją ustawić tylko dla pierwszych ośmiu użytkowników. **PGM** – numer wyjścia i rodzaj zdarzenia (**Event** – włączenie, **Restore** – wyłączenie); **User / SMS and Call** – kto otrzymuje SMS i/lub połączenie.

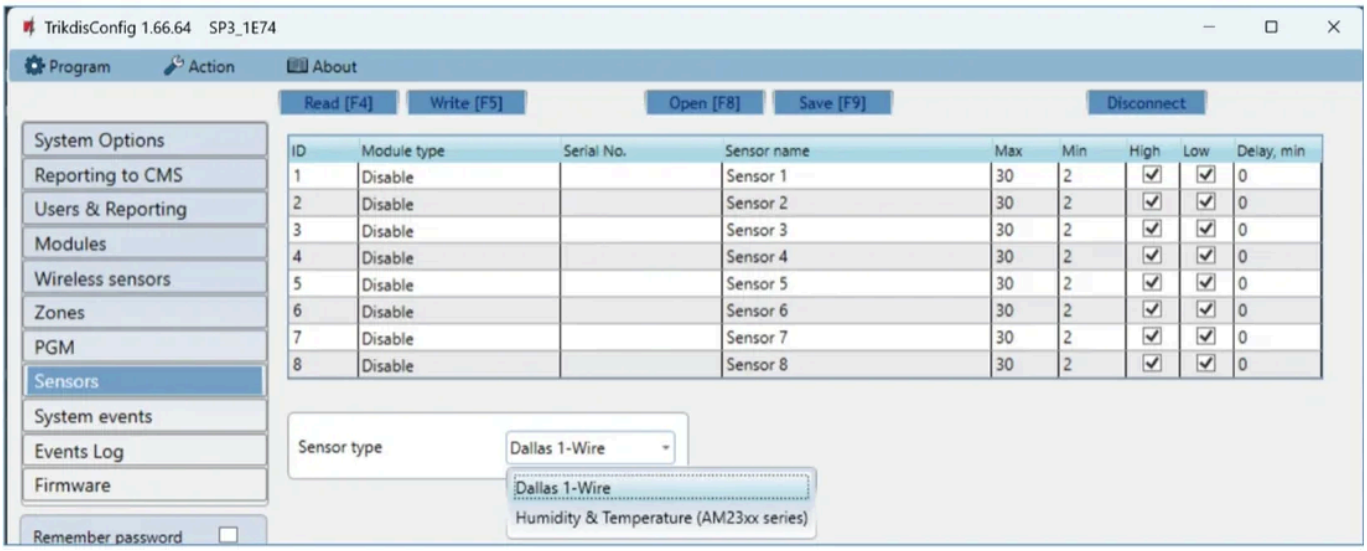


Rysunek 84. PGM → SMS & Call reporting: powiadamianie o przełączeniu wyjść.

6.9 Sensors

- **ID** – numer kolejny czujki temperatury.
- **Module type** – czujka przypisana do identyfikatora.
- **Serial No.** – numer seryjny czujki podłączonej do centrali.
- **Sensor name** – nazwa czujki.
- **Max** – przy temperaturze powyżej tej wartości powstaje zdarzenie, jeśli zaznaczono **High**.
- **Min** – przy temperaturze poniżej tej wartości powstaje zdarzenie, jeśli zaznaczono **Low**.
- **Delay, min** – zdarzenie zostanie wysłane tylko wtedy, gdy przekroczenie wartości granicznej trwa przez tyle minut.

- **Sensor type** – **Dallas 1-Wire**: najwyżej osiem czujek, rozpoznawanych automatycznie; **Humidity & Temperature (AM23xx series)**: jedna czujka wilgotności i temperatury AM2301, którą trzeba wybrać ręcznie w kolumnie **Module type**.

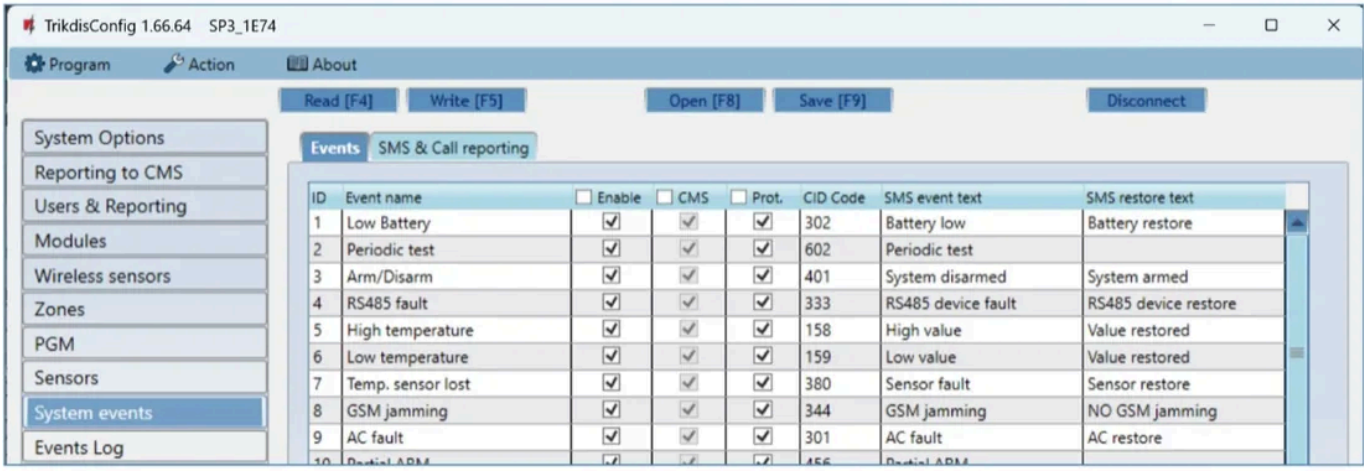


Rysunek 85. Okno **Sensors**: wartości graniczne czujek temperatury. Kolumnę numerów seryjnych pozostawiliśmy na rysunku pustą.

6.10 System events

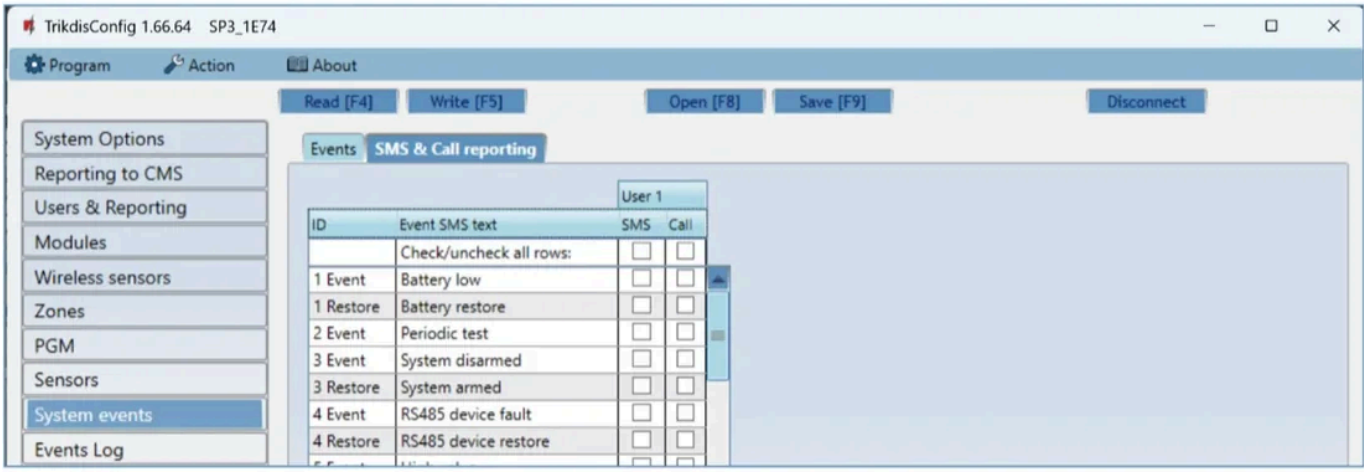
Zakładka **Events**:

- **ID** – numer kolejny zdarzenia.
- **Event name** – nazwa zdarzenia.
- **Enable** – nadzorowanie i raportowanie zdarzenia.
- **CMS**, **Prot.** – raport do stacji monitorowania lub do chmury Protegus.
- **CID Code** – kod Contact ID zdarzenia.
- **SMS event text**, **SMS restore text** – treść SMS-a o zdarzeniu i o przywróceniu.



Rysunek 86. System events → **Events**: kod, kierunek i treść SMS zdarzeń systemowych.

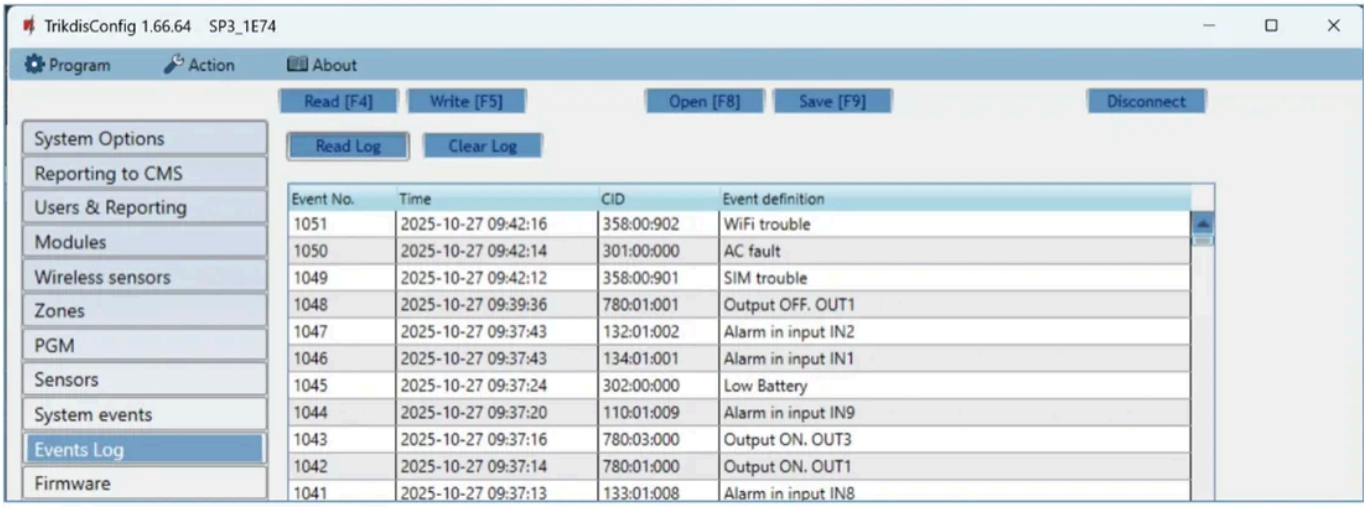
Zakładka **SMS & Call reporting** – widoczna tylko wtedy, gdy jest numer telefonu użytkownika. **ID** – numer i rodzaj zdarzenia (**Event**, **Restore**); **Event SMS text** – treść SMS-a; **User / SMS and Call** – kto otrzymuje SMS i/lub połączenie.



Rysunek 87. System events → SMS & Call reporting: powiadamianie o zdarzeniach systemowych.

6.11 Events log

- **Read Log** – odczyt dziennika zdarzeń z pamięci centrali.
- **Clear Log** – usunięcie dziennika.
- Kolumny tabeli: **Event No.**, **Time**, kod **CID**, **Event definition**. Dziennik pokazuje najwyżej 1000 zdarzeń.



Rysunek 88. Okno **Events log**: ostatnie 1000 zdarzeń centrali.

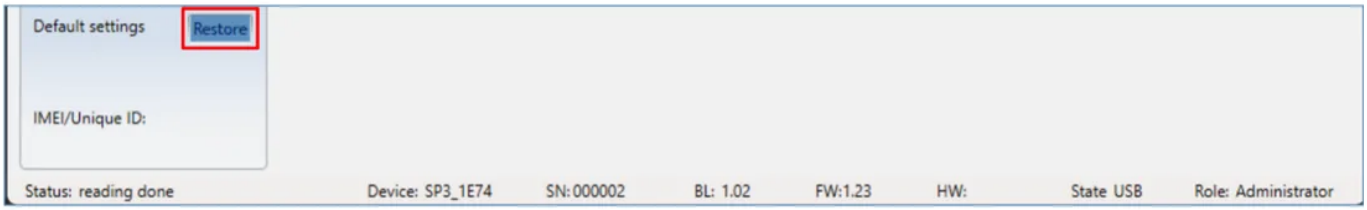
Wyszukiwanie usterek w dzienniku

Przy spornym alarmie najpierw odczytaj dziennik: widać, która strefa, kiedy i z jakim kodem zgłosiła zdarzenie oraz czy raport został wysłany.

6.12 Przywracanie ustawień fabrycznych

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

Kodem instalatora jest to możliwe tylko wtedy, gdy administrator tego nie zablokował na zakładce **System Options → Access** (6.2.6).



Rysunek 89. Przycisk **Restore** w grupie **Default settings** w lewym dolnym rogu przywraca ustawienia fabryczne.

Po przywróceniu

Kody wracają do wartości fabrycznych (6.2.6), PIN karty SIM, APN, dane WiFi, użytkownicy i strefy zostają usunięte. Jeśli wcześniej zapisałeś ustawienia do pliku (**Save [F9]**), możesz je wczytać przyciskami **Open [F8]** i **Write [F5]**.

7. Zdalne programowanie

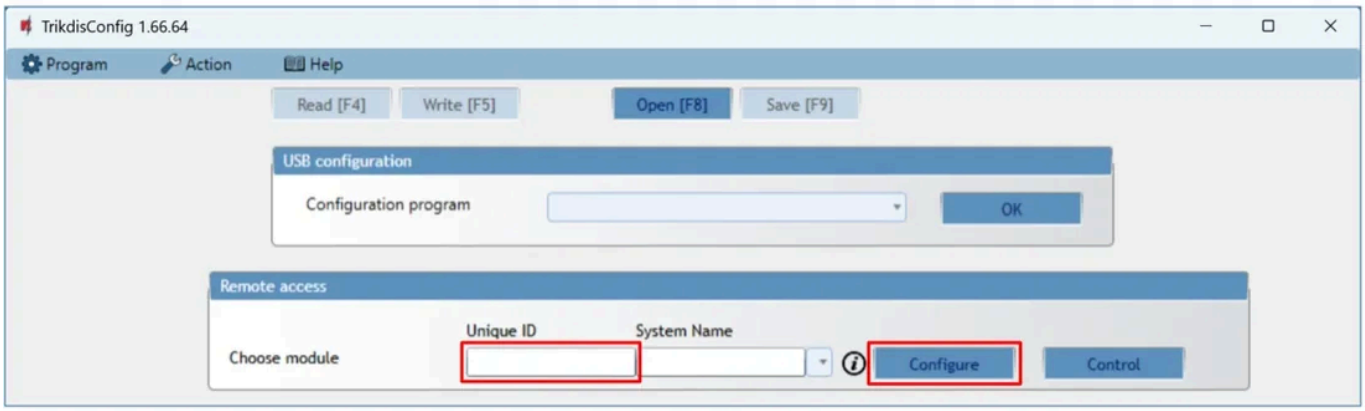
TrikdisConfig łączy się z „FLEXi" SP3 nie tylko przez kabel USB, ale też **zdalnie, przez chmurę Protegus**: możesz zmieniać ustawienia już zamontowanej centrali, odczytywać dziennik zdarzeń, a nawet aktualizować firmware bez wyjazdu na miejsce.

Do zdalnego dostępu potrzebne jest:

1. Centrala musi być włączona i mieć połączenie sieciowe: dioda **PWR** miga na zielono, przy sieci komórkowej dioda **NET** świeci na zielono, przy Wi-Fi dioda **MOD**, a przy Ethernecie dioda **ETH** świeci na zielono (punkt 1.6). W wersji z modemem karta SIM jest aktywna, a żądanie PIN jest wyłączone lub PIN jest wpisany.
2. **Chmura Protegus** musi być włączona – ustaw to w oknie **Users & Reporting** przy pierwszym uruchomieniu przez USB (punkt 6.4).
3. Musisz znać **unikalny identyfikator** centrali (**IMEI / Unique ID** – na etykiecie płytki i obudowy oraz na pasku stanu TrikdisConfig) oraz kod administratora lub instalatora.

Kroki:

1. Uruchom program TrikdisConfig.
2. W części **Remote access** wpisz w polu **Unique ID** unikalny identyfikator centrali.
3. Opcjonalnie nadaj systemowi nazwę w polu **System name** – program ją zapamięta i następnym razem wybierzesz ją z listy rozwijanej.
4. Naciśnij przycisk **Configure**.
5. W otwartym oknie kliknij przycisk **Read [F4]** i podaj kod administratora lub instalatora. Po zaznaczeniu **Remember password** program go zapamięta.
6. Wprowadź zmiany, a następnie przycisk **Write [F5]** wyślij je do centrali.



Rysunek 90. TrikdisConfig – Remote access: pole Unique ID, System name i przycisk Configure.

Zdalne programowanie można uruchomić także z aplikacji Protegus 2 hasłem instalatora; do szczegółowych ustawień potrzebny jest jednak TrikdisConfig. Zdalne połączenie przez sieć komórkową wiąże się z transmisją danych – przy aktualizacji firmware nawet kilku megabajtów.

8. Sprawdzenie działania systemu

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

1. **Sprawdź diody LED.** Dioda **PWR** powinna migać na zielono bez czerwonych mignięć, dioda sieci (**NET**, **MOD** lub **ETH**) świecić na zielono, a dioda **DAT** zgasnąć po wysłaniu zdarzeń (punkt 1.6). Jeśli PWR miga na czerwono, szukaj usterki zgodnie z rozdziałem 10.
2. **Wywołaj zdarzenie.** Uzbrój, a następnie rozbrój system na manipulatorze albo w uzbrojonym systemie naruszysz strefę, aby powstał alarm.
3. **Sprawdź dotarcie zdarzenia.** Zdarzenie powinno pojawić się w oprogramowaniu stacji monitorowania i/lub na liście zdarzeń aplikacji Protegus 2 – z właściwym numerem partycji, strefy i użytkownika. We własnym dzienniku centrali (**Events log**, punkt 6.11) też zobaczysz, czy zdarzenie powstało i czy zostało wysłane.
4. **Strefy po kolei.** Naruszaj po kolei wszystkie strefy (otwarcie, ruch, przycisk testowy czujki dymu, sabotaż) i sprawdź, czy na manipulatorze i w Protegus 2 sygnalizuje właściwa strefa.
5. **Wyjścia.** Przełączaj wyjścia PGM zdalnie z Protegus 2 i sprawdź, czy podłączone urządzenie (sygnalizator, lampka sygnalizacyjna, przekaźnik) rzeczywiście zadziała.
6. **Zdalne uzbrajanie.** Jeśli system jest sterowany także zdalnie, uzbrój i rozbrój go również z aplikacji Protegus 2 i obserwuj, czy stan manipulatora za tym nadąża.
7. **Zanik zasilania.** Odłącz zasilanie sieciowe: centrala powinna dalej pracować z akumulatora, a powinno dotrzeć zdarzenie **AC Fault**, a po ponownym włączeniu **AC Restore** (punkt 2.2).

Fabrycznie centrala nie wysyła do stacji monitorowania (punkt 6.3), natomiast chmura Protegus jest fabrycznie włączona. Jeśli stacja monitorowania nie otrzymuje zdarzeń, najpierw sprawdź ustawienia **Reporting to CMS** oraz 4 lub 5 mignięć diody PWR.

9. Aktualizacja firmware

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

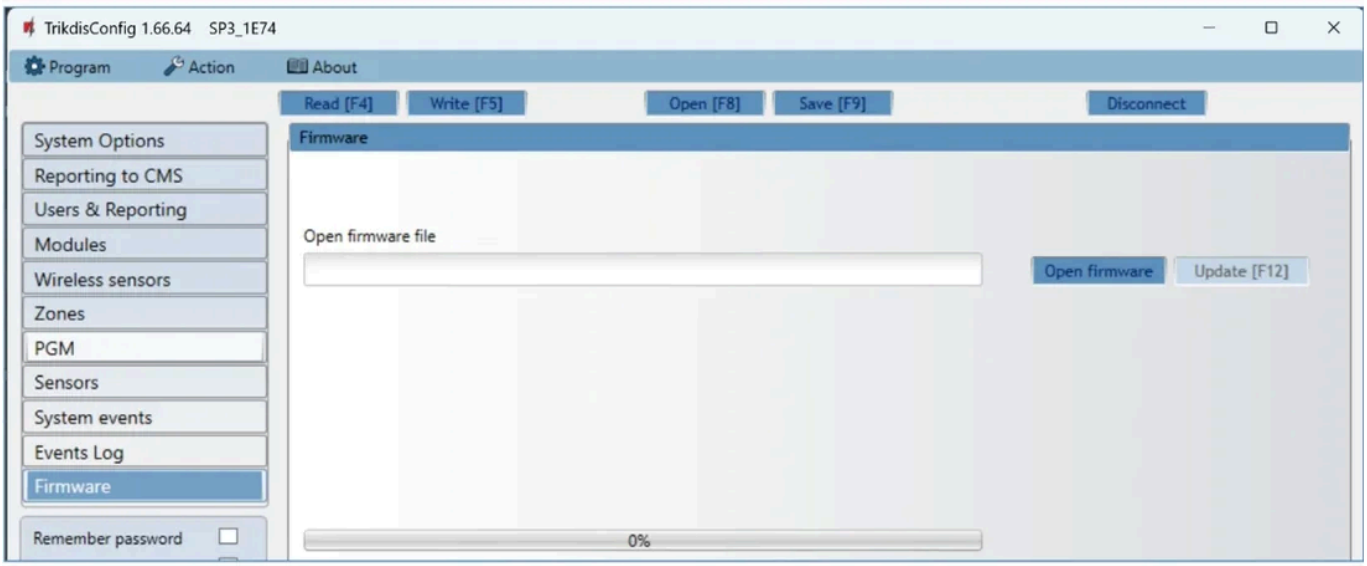
Który plik wybrać?

Nazwa pliku firmware to **SP3_yxxz_NNNN.fw** (punkt 1.7). Cyfra **y** to wersja sprzętowa: wgrać można tylko plik przeznaczony dla wersji danej centrali, przy innej wersji program zgłosi błąd. Cyfra **z** to typ czujek bezprzewodowych – dla czujek MAXIMUM (RF-LORA) i S8 (RF-S8) **4**, dla Paradox RTX3 **1** –, wybierz ją odpowiednio do instalacji; od niej zależy też liczba obsługiwanych stref (32 lub 64). Zasady wyboru opisuje artykuł Firmware FLEXi SP3: jak wybrać właściwy?.

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

Po połączeniu TrikdisConfig automatycznie zaproponuje aktualizację firmware, jeśli jest nowsza wersja; potrzebne jest do tego połączenie z internetem. Program antywirusowy lub zapora sieciowa mogą blokować automatyczne pobieranie firmware; wtedy zezwól TrikdisConfig na dostęp albo pobierz plik ręcznie (po rejestracji ze strony producenta) i otwórz go na stronie Firmware. Na końcu aktualizacji kliknij przycisk **Write [F5]** i dopiero potem odłącz kabel USB.

10. Rozwiązywanie problemów i najczęstsze pytania

Najczęstsze pytania i usterki, wychodząc od diod LED płytki (znaczenie diod w punkcie 1.6). Jeśli odpowiedź odsyła do szczegółowego rozdziału, tam znajdziesz dokładne miejsce ustawienia.

Dioda PWR miga na czerwono – co oznacza liczba mignięć?

Dioda **PWR** przy normalnej pracy miga na zielono. Jeśli jest usterka, miga na czerwono, a liczba mignięć mówi, w czym problem:

Mignięcia	Usterka	Gdzie szukać
1	brak karty SIM	nano-SIM w gnieździe, styk (2.4, 6.2)
2	błędny kod PIN karty SIM	PIN na stronie **System Options** albo wyłącz żądanie PIN w telefonie (6.2)
3	nie może połączyć się z siecią komórkową	antena, siła sygnału (żółte mignięcia diody **NET**: 0–5, 3 już wystarczają), czy karta SIM jest aktywna
4	brak połączenia z odbiornikiem stacji monitorowania na 1. kanale	**Reporting to CMS**: adres, port, TCP/UDP, klucz szyfrowania, identyfikator obiektu (6.3)
5	brak połączenia z odbiornikiem stacji monitorowania na 2. kanale	to samo dla odbiornika zapasowego (6.3)
6	zegar wewnętrzny nie jest ustawiony	ustawienie czasu na stronie **System Options** (6.2)
7	napięcie zasilania rezerwowego jest niewystarczające	akumulator i końcówki, wiek akumulatora, prąd ładowania (2.2)
8	brak zasilania sieciowego (AC)	zasilacz, wyłącznik nadprądowy, zaciski zasilania głównego (2.1)
9	nie może połączyć się z siecią Wi-Fi	nazwa sieci i hasło, sieć 2,4 GHz (zobacz następne pytanie)

Centrala nie znajduje sieci Wi-Fi

1. Moduł Wi-Fi „FLEXi" SP3 łączy się **tylko z siecią 2,4 GHz** (802.11 b/g/n, WPA / WPA2). Sieci 5 GHz nie widzi; jeśli router używa wspólnej nazwy dla obu pasm, pasmo 2,4 GHz musi być włączone.
2. Sprawdź nazwę sieci i hasło na stronie **System Options** (6.2) oraz czy router nie filtruje urządzeń według adresu MAC.
3. Dioda **MOD** miga na zielono podczas łączenia i świeci stale na zielono, gdy połączenie zostanie nawiązane.
4. W metalowej obudowie sygnał Wi-Fi może być słaby: centrala działa niezawodnie z anteną poza obudową, z routerem blisko obudowy lub przy silniejszym sygnale.

Sieć jest, ale do Protegus 2 nie docierają zdarzenia

1. Dioda **DAT** świeci na żółto, jeśli w pamięci jest niewysłany komunikat: wtedy problemem jest połączenie, a nie ustawienia. Sprawdź diodę **NET** / **MOD** i mignięcia PWR.
2. Połączenie z chmurą Protegus jest fabrycznie włączone; jeśli zostało wyłączone, włącz je ponownie polem **Enable cloud service** na karcie **Users & Reporting → Protegus** (6.4.3). Na karcie **Reporting to CMS → Settings** można ustawić tylko, którą drogą (SIM, Wi-Fi, LAN) idzie ruch do Protegus.
3. Na stronie **System events** wysyłanie danego zdarzenia musi być włączone (6.10) – tego, co jest tu wyłączone, centrala nie wysyła żadnym kanałem.
4. Czy urządzenie jest połączone z kontem Protegus 2 (5.1)? Do dodania nowego systemu potrzebny jest unikalny identyfikator urządzenia.

Stacja monitorowania nie otrzymuje zdarzeń

1. Transmisja do stacji monitorowania jest **fabrycznie wyłączona**; trzeba ją włączyć na stronie **Reporting to CMS** i wpisać dane odbiornika (6.3).
2. 4 lub 5 czerwonych mignięć diody PWR oznacza, że na 1. lub 2. kanale nie ma połączenia z odbiornikiem: adres, port, protokół (TCP/UDP), klucz szyfrowania, identyfikator obiektu.
3. Jeśli ustawiona jest zarówno stacja monitorowania, jak i Protegus 2, zdarzenie idzie najpierw do odbiornika, potem do użytkownika – zdarzenie widoczne w Protegus 2 nie oznacza więc, że odbiornik też je otrzymał.

Który firmware wgrać? Co oznaczają cyfry w nazwie pliku?

Nazwa pliku firmware to `SP3_yxxz_NNNN.fw`. **Pierwsza** cyfra (y) to wersja sprzętowa – 1: Wi-Fi + 4G, 2: Wi-Fi, 3: LAN / LAN + Wi-Fi, 5: Wi-Fi + 2G, 6: LAN + 4G –, której przy aktualizacji nie można zmienić; TrikdisConfig zgłosi, jeśli wybierzesz plik nieprzeznaczony dla danego sprzętu. **Ostatnia** cyfra (z) określa typ odbiornika bezprzewodowego, a tym samym liczbę stref: 0 RF-SH (32 strefy), 1 Paradox RTX3 (32), 2 Honeywell (64, nieużywane w Europie), 4 czujki MAXIMUM (RF-LORA) lub S8 (RF-S8) (64; do ekspanderów LORA niepotrzebna). Tę cyfrę można zmieniać: do innego odbiornika potrzebny jest firmware z inną cyfrą z (1.7 i rozdział 9). Czterocyfrowa liczba na końcu to wersja; ogólna zasada: używaj najwyższej.

Ile mogę mieć stref i od czego to zależy?

Płytka ma **10** zacisków IO, każdy może być strefą (wejściem) lub wyjściem PGM. Z podwajaniem stref (ATZ) do jednego zacisku można podłączyć dwie czujki, co daje **20** stref. Manipulatorami, ekspanderami serii iO i LORA oraz odbiornikiem bezprzewodowym liczbę stref można rozszerzyć do **32 lub 64** – do której, decyduje ostatnia cyfra firmware (poprzednie pytanie). Liczba partycji to 8.

Wymieniam starą centralę – czy muszę wymienić rezystory w czujkach?

Nie. W „FLEXi" SP3 wartości rezystorów końca linii można ustawić, dlatego istniejące czujki mogą pozostać z rezystorami używanymi w starej centrali. Typ strefy (NC, NO, EOL, 3EOL, ATZ) i wartości rezystorów ustawiasz na stronie **Zones** (3.2 i 6.7).

Chcę podłączyć do wyjścia większy odbiornik (sygnalizator, zamek, bramę)

Zacisk IO jako wyjście jest typu otwarty kolektor, o obciążalności **maksymalnie 100 mA** – bezpośrednio można do niego podłączyć tylko lampkę sygnalizacyjną lub cewkę małego przekaźnika. Do większego odbiornika użyj przekaźnika zgodnie z punktem 3.8. Wyjście **BELL** ma obciążalność 1 A, a wyjście **AUX** daje urządzeniom zewnętrznym maksymalnie 1 A przy 12 V DC – zsumuj pobór prądu manipulatorów, ekspanderów i czujek z tabeli 1.4 i nie przekraczaj go.

Jakiego manipulatora mogę użyć i ilu?

Centrala obsługuje manipulatory Trikdis FLEXi / SK oraz wymienione manipulatory Paradox i Crow (lista i pobór prądu w punkcie 1.4). Na jednej magistrali **maksymalnie 8 manipulatorów**, i muszą być **tego samego typu**. Manipulatory LED obsługują tylko dwie pierwsze partycje; do większej liczby partycji potrzebny jest manipulator LCD. Manipulator FLEXi LCD przechowuje jednocześnie cztery języki; jeśli nie ma wśród nich polskiego, trzeba zaktualizować firmware manipulatora: https://pl.mobilamb.eu/proces-aktualizacji-oprogramowania-flexi-lcd-keypad .

Chcę użyć odbiornika Paradox RTX3

Do RTX3 ostatnia cyfra firmware musi być **1** (`SP3_xxx1_NNNN.fw`); plik znajdziesz w folderze instalacyjnym TrikdisConfig, w podfolderze `Firmwares\SP3\RTX3`, a przebieg aktualizacji w rozdziale 9. Po wymianie strona **Wireless** pokaże, jeśli RTX3 nie jest jeszcze zarejestrowany. Częstotliwość RTX3 i urządzeń bezprzewodowych musi być taka sama (433 lub 868 MHz) – sprawdź przed zakupem. Szczegóły: https://pl.mobilamb.eu/flexi-sp3-bezprzewodowy-modul-rozszerzen-paradox-rtx3 .

Centrala nie odpowiada na komendy SMS

1. SMS-em i połączeniem telefonicznym można sterować tylko wersjami **z modemem** (2G / 4G); centralą tylko z Wi-Fi lub tylko z Ethernetem nie.
2. Budowa wiadomości i lista komend są w punkcie 5.3; fabryczne hasło SMS to `123456`, które warto od razu zmienić w grupie **System Options** → **Access** (6.2).
3. Połączeniem i SMS-em może sterować tylko użytkownik, którego numer telefonu jest na liście użytkowników na stronie **Users & Reporting** (6.4).

Co koniecznie ustawić przy pierwszym uruchomieniu?

Z ustawieniami fabrycznymi działa większość małych i średnich systemów, ale nie pomijaj tych: zmiana **kodu głównego** oraz kodów dostępu instalatora / administratora (6.2, 6.4), ustawienie **czasu** (6.2), typ stref i rezystory (6.7), użytkownicy i ich numery telefonów (6.4), dane odbiornika stacji monitorowania, jeśli jest (6.3), oraz połączenie systemu z kontem Protegus 2 (5.1). Na końcu wykonaj sprawdzenie z rozdziału 8.

11. Gwarancja i 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.

11.1 Gwarancja i ograniczenie odpowiedzialności

Centrala alarmowa jest objęta gwarancją przez **24 miesiące** od zakupu; w tym czasie producent bezpłatnie naprawia usterki z jego winy. Warunkiem gwarancji jest zainstalowanie centrali przez wykwalifikowaną osobę zgodnie z tą instrukcją i przepisami dotyczącymi urządzeń elektrycznych oraz eksploatacja zgodnie z nimi. Do naprawy centralę należy wysłać w opakowaniu producenta, z opisem objawów usterki; po upływie gwarancji konserwacja i naprawa są odpłatne.

Gwarancja wygasa przedwcześnie, jeśli

- centralę naprawiała lub próbowała naprawiać nieuprawniona osoba;
- była używana niezgodnie z przeznaczeniem;
- była przechowywana lub zainstalowana w nieodpowiednim miejscu (nieodpowiednie warunki klimatyczne, agresywne środowisko chemiczne);
- została uszkodzona mechanicznie lub celowo zniszczona;
- została uszkodzona w wyniku siły wyższej (na przykład uderzenia pioruna).

Producent nie odpowiada za

- nieprawidłowe działanie centrali, jeśli nie została zainstalowana lub nie była używana zgodnie z instrukcją;
- nieprawidłowe działanie centrali, jeśli jego przyczyną jest usterka lub zanik połączenia z siecią komórkową lub internetem albo usterka sieci operatora;
- ograniczenie, zaprzestanie lub przerwy w świadczeniu usług sieci komórkowej lub internetu albo dostaw energii elektrycznej oraz wynikające z tego szkody majątkowe lub niemajątkowe;
- szkody majątkowe lub niemajątkowe poniesione przez kupującego lub użytkownika w wyniku rozboju, włamania, kradzieży, pożaru lub innego zdarzenia szkodowego.

11.2 Zasady bezpieczeństwa

- Przed użyciem centrali przeczytaj tę instrukcję. „FLEXi" SP3 jest urządzeniem elektrycznym: może je instalować i serwisować tylko wykwalifikowana osoba, z przestrzeganiem instrukcji i przepisów dotyczących instalacji urządzeń elektrycznych.
- **Podczas instalacji centrala musi być odłączona od napięcia**; przed każdym podłączaniem i serwisowaniem odłącz zasilanie: od sieci wyłącznikiem nadprądowym, od akumulatora przez zdjęcie końcówek.
- Centralę zamontuj w miejscu niedostępnym dla osób nieuprawnionych, w bezpiecznej odległości od wrażliwych urządzeń elektronicznych. Płytka nie jest odporna na drgania, oddziaływania mechaniczne, wilgoć i agresywne środowisko chemiczne; spełnia wymagania klasy środowiskowej II normy EN 50131.
- Obudowa, transformator, akumulator i urządzenie programujące muszą spełniać wymagania bezpieczeństwa normy EN 60950.
- Centrala pracuje z sieci 230 V, 50 Hz przez transformator obniżający klasy II (16–18 V AC) lub z zasilacza 16–24 V DC; jako zasilanie rezerwowe potrzebny jest akumulator 12 V o pojemności co najmniej 7 Ah. Pobór prądu zależy od podłączonych urządzeń zewnętrznych (punkt 2.1).
- W obwodzie zasilania trzeba zainstalować dwubiegunowy automatyczny wyłącznik nadprądowy, którego otwarte styki są oddalone o co najmniej 3 mm; wyłącznik powinien znajdować się w miejscu znanym i dostępnym dla specjalisty serwisującego centralę.
- Usterki wynikające z nieprawidłowej instalacji lub użytkowania oraz modyfikacje i naprawy niezatwierdzone przez producenta powodują utratę gwarancji.
- Przestrzegaj lokalnych przepisów dotyczących odpadów: uszkodzonego urządzenia, akumulatora i części nie wyrzucaj razem z odpadami komunalnymi.

Zobacz też

- Firmware FLEXi SP3: jak wybrać właściwy? – znaczenie kodu sprzętowego i kodu odbiornika, który firmware do jakiego systemu.
- FLEXi SP3 + bezprzewodowy moduł rozszerzeń Paradox RTX3 – bezprzewodowe czujki Paradox z SP3.
- Nadajnik-odbiornik RF-S8 i czujki S8 – instrukcja instalacji i parowania – urządzenia bezprzewodowe S8 z SP3: podłączenie, firmware, parowanie.
- Elastyczna bezprzewodowa kontrola dostępu z systemem GATOR RF-LoRa – moduły RF-LORA i iO-LORA w systemie.
- Trikdis FLEXi SP3 uzyskał certyfikat GRADE 3 – co oznacza certyfikat.
- Trikdis FLEXi SP3 – prezentacja inteligentnej centrali alarmowej – prezentacja centrali, wymiana starej centrali.
- Proces aktualizacji firmware manipulatora FLEXi LCD – języki manipulatora i jego aktualizacja.

- Manipulator Trikdis FLEXi Keypad SK-LED button – krótka instrukcja użytkownika i manipulator SK-LCD button – krótka instrukcja użytkownika – dla użytkownika.
- Zdalne uzbrajanie stacyjką z aplikacji Protegus 2 – jeśli wyjście PGM SP3 uzbraja inną centralę.
- Dodawanie kamery IP do Protegus 2 – podgląd na żywo na ekranie głównym Protegus 2.
- Dokumentacja w języku angielskim: docs.trikdis.com – Security control panel “FLEXi” SP3.

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

Powiązane produkty

Inteligentny panel alarmowy Trikdis FLEXi SP3 Ethernet

Inteligentny panel alarmowy Trikdis FLEXi SP3 WiFi

Inteligentny panel alarmowy Trikdis FLEXi SP3 WiFi + 4G

Inteligentny panel alarmowy Trikdis FLEXi SP3 WiFi + 2G

Inteligentny panel alarmowy Trikdis FLEXi SP3 Ethernet + 4G

Inteligentny panel alarmowy Trikdis FLEXi SP3 Ethernet + 2 SIM 4G

Metalowe pudełko z normalnym rozmiarem z PSU dla panelu sterowania Flexi SP3

Małe metalowe pudełko z PSU dla panelu sterowania Flexi SP3

Klawiatura Trikdis Flexi LCD

Klawiatura LED Trikdis Flexi

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-flexi-sp3