Komunikátor GET – návod pre inštalatéra a používateľa

Návod pre inštalatéra a používateľa ku komunikátoru Trikdis GET Ethernet + 4G: pripojenie k zabezpečovacej ústredni, nastavenie LAN a SIM v TrikdisConfig, hlásenie na PCO, aplikácia Protegus 2.



Vydanie: 2026-11-17
Vždy aktuálna webová verzia: https://trikdis.sk/get-navod

Obsah

1. Prehľad

1.1 Na čo slúži a ako funguje
1.2 Verzie: GET, GT a GT+
1.3 Kompatibilné zabezpečovacie ústredne
1.4 Časti komunikátora
1.5 Svorky
1.6 Signalizácia LED
1.7 Technické údaje

2. Rýchle spustenie

2.1 Príprava
2.2 Spojenie s aplikáciou Protegus 2
2.3 Spojenie s PCO

3. Inštalácia a zapojenie

3.1 Postup inštalácie
3.2 Umiestnenie v skrinke ústredne, anténa
3.3 Pripojenie k zabezpečovacej ústredni
3.3.1 DSC – dátová zbernica (Keybus)
3.3.2 Paradox – sériový port
3.3.3 Paradox SP/MG – Keybus a TIP/RING
3.3.4 UTC Interlogix (Caddx) – dátová zbernica
3.3.5 Texecom – sériový port
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – dátová zbernica
3.3.9 Ľubovoľná ústredňa – TIP/RING
3.4 Zapojenie zóny kľúčového spínača
3.5 Zapojenie vstupov
3.6 Zapojenie výstupu s relé
3.7 Zapnutie a prvá kontrola
A TRIKDIS átjelző elindítása

4. Programovanie zabezpečovacej ústredne

4.1 Pripojenie na dátovú zbernicu alebo sériový port
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Pripojenie na telefónnu linku (TIP/RING)
4.2.1 Programovanie vytáčača Honeywell Vista
4.2.2 Vytáčač UTC Interlogix (Caddx) NX

5. Diaľkové ovládanie aplikáciou Protegus 2

5.1 Pridanie zariadenia
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Zapínanie a vypínanie stráženia výstupom

5.3 Zapínanie a vypínanie stráženia z aplikácie

6. Nastavenia podrobne

6.1 Pripojenie ku komunikátoru
6.2 System settings (System options)
6.3 Panel settings
6.4 CMS reporting (Reporting to CMS)
6.4.1 Kanály prijímača (CMS settings)
6.4.2 Test, PING a poradie spojení
6.5 User reporting (Protegus Cloud)
6.6 Network settings
6.6.1 LAN (Ethernet)
6.6.2 SIM1 a SIM2
6.7 IN/OUT
6.8 Event summary (System events)
6.9 Obnovenie výrobných nastavení

7. Programovanie na diaľku

8. Kontrola fungovania komunikátora

9. Aktualizácia firmvéru

10. Hľadanie chýb a časté otázky

11. Bezpečnostné pokyny

Pozri aj

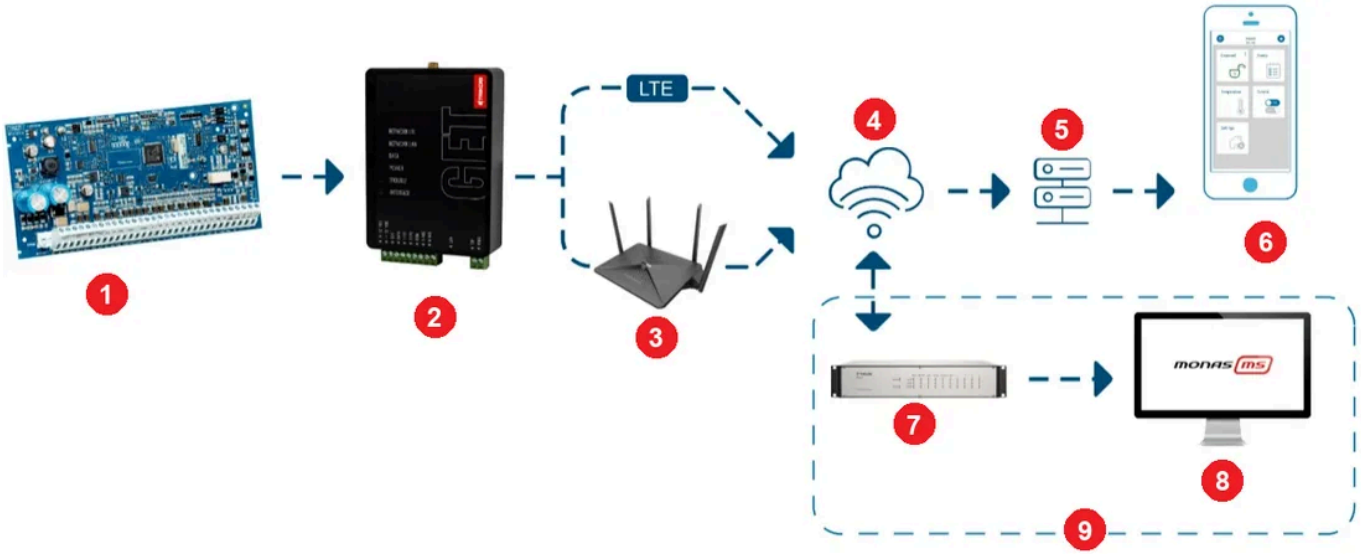
1. Prehľad

GET je **komunikátor Ethernet + 4G** od Trikdis, ktorý udalosti zabezpečovacej ústredne posiela cez káblovú lokálnu sieť (LAN) alebo cez mobilnú sieť na PCO a do aplikácie Protegus 2. K ústredni ho môžeš pripojiť dvoma spôsobmi: **priamo**, na dátovú zbernicu alebo sériový port ústredne (pri ústredniach DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange a Honeywell), alebo **na telefónny komunikátor ľubovoľnej ústredne** (TIP/RING), ktorý udalosti posiela vo formáte Contact ID tónmi DTMF. Komunikátor odovzdá PCO úplnú informáciu o udalosti (kód, partícia, zóna alebo používateľ). Aplikáciou Protegus 2 používateľ ovláda systém na diaľku a dostáva upozornenia na udalosti; aplikácia funguje so všetkými ústredňami, ktoré komunikátor podporuje, bez ohľadu na výrobcu ústredne. Hlásenie na PCO a Protegus 2 môžeš používať aj súčasne. Tento návod je určený pre komunikátor GET s modemom LTE (4G); rozdiely medzi GET, GT a GT+ zhŕňa bod 1.2.

1.1 Na čo slúži a ako funguje

- **Hlási na PCO.** Udalosti posiela cez IP spojenie – po káblovej sieti alebo po mobilnej sieti – softvérovému alebo hardvérovému prijímaču Trikdis (protokol TRK8) – tie spolupracujú s ľubovoľným softvérom PCO –, prijímaču SIA DC-09 alebo prijímaču SUR-GARD (TL150). Prijímaču SUR-GARD odovzdáva kódy Contact ID z ústredne prevedené na kódy SIA; prevodná tabuľka je v prílohe anglickej dokumentácie na docs.trikdis.com. Spojenie s prijímačom kontroluje každých 30 sekúnd (alebo v nastavenom intervale) správou PING; ak sa hlavný kanál preruší, prepne na záložný kanál. S paralelným kanálom idú udalosti súčasne aj na dva prijímače. Cesty spojenia – LAN, SIM1, SIM2 – môžeš zoradiť: ak hlavná cesta nefunguje, komunikátor prepne na záložnú cestu (bod 6.4.2). Ak je zapnutá aj služba Protegus, udalosť dostane najprv PCO a až potom aplikácia používateľov.
- **Upozorňuje používateľa.** Aplikácia Protegus 2 hlási udalosti push správou a samostatným zvukovým signálom; používateľ môže z aplikácie zapínať a vypínať stráženie a ovládať pripojené zariadenia (osvetlenie, bránu, vetranie, kúrenie, zavlažovanie atď.). V aplikácii má administrátor, inštalátor a používateľ rozdielne práva. GET neposiela upozornenia cez SMS ani hovorom: upozornenie prichádza cez aplikáciu Protegus 2.
- **Ovláda ústredňu priamo.** Ak je pripojený na dátovú zbernicu alebo sériový port, komunikátor vidí aj stavy partícií a zón ústredne a používateľ zapína a vypína stráženie z Protegus 2 vlastným kódom klávesnice – na to netreba zónu kľúčového spínača.
- **Má vlastné vstupy a výstupy.** Dve svorky I/O s dvojitou funkciou môžeš použiť ako vstup (IN) alebo ako ovládateľný výstup (OUT); z výroby sú obe výstupy. Výstupy môžeš ovládať z aplikácie Protegus 2. Svorky **A 485** a **B 485** sa na GET nepoužívajú; rozširujúci modul RS485 sa ku GET pripojiť nedá.
- **Nastavíš ho dvoma nástrojmi.** Nastavenia môžeš urobiť programom TrikdisConfig, ktorý beží vo Windows (cez kábel USB-C alebo na diaľku), a – s firmvérom 1.08 alebo novším – aj z aplikácie Protegus 2 (Settings → Advanced settings). Nastavenia môžeš uložiť do súboru a zapísať do iných komunikátorov. Prístupové úrovne sú dve: administrátor PCO a inštalátor. Komunikátor môžeš nastaviť aj na diaľku a na diaľku sa dá aktualizovať aj jeho firmvér.

Štruktúru systému ukazuje obrázok nižšie: zabezpečovacia ústredňa sa pripája na komunikátor, komunikátor sa na internet dostane dvoma spôsobmi – cez mobilnú sieť (LTE) alebo cez router (LAN) –, odtiaľ na prijímač PCO (a jeho softvér) a na server Protegus; používateľ vidí systém v aplikácii Protegus 2.



Obrázok 1. Miesto komunikátora v systéme: zabezpečovacia ústredňa → GET → mobilná sieť (LTE) alebo router (LAN) → internet → prijímač PCO a server Protegus → aplikácia Protegus 2.

- 1 zabezpečovacia ústredňa („Alarm panel“)
- 2 komunikátor GET LTE („LTE communicator“)
- 3 router („Router“)
- 4 internet („Internet“)
- 5 server Protegus („Protegus server“)
- 6 telefón s aplikáciou Protegus („Phone with Protegus software“)
- 7 prijímač PCO („Receiver“)
- 8 softvér PCO („Monitoring software“)
- 9 pult centralizovanej ochrany bezpečnostnej firmy („Monitoring station in security company“) – v prerušovanom rámčeku

1.2 Verzie: GET, GT a GT+

GET je súrodenec komunikátorov GT a GT+ s ethernetovým portom: pripojenie a programovanie zabezpečovacej ústredne, okruh kompatibilných ústrední, modem, prenosové protokoly a používanie Protegus 2 sú rovnaké, preto majú návody všetkých troch komunikátorov aj rovnaké poradie kapitol. Rozdiely zhŕňa tabuľka nižšie.

	GET	**GT**	**GT+**
Sieťové pripojenie	**LTE (4G) a Ethernet (LAN, RJ45)**; poradie ciest spojenia sa dá nastaviť (Main / Backup / Backup 2: LAN, SIM1, SIM2; bod 6.4.2)	LTE (4G)	LTE (4G)
Karta SIM	**2 držiaky nano-SIM** (SIM1, SIM2); môžeš vložiť jednu alebo dve karty	1 nano-SIM	1 nano-SIM
Napájacie napätie	10–18 V DC	10–18 V DC	10–32 V DC
Odber prúdu	najviac 100 mA v pokoji, 300 mA pri posielaní dát	najviac 100 / 200 mA	najviac 100 / 200 mA
Rozmery, hmotnosť	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g

	GET	GT	GT+
Svorky	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; samostatná zásuvka **LAN** (RJ45) a TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Výrobné nastavenie svoriek I/O	výstup (OUT)	vstup (IN, NO)	vstup (IN, NO)
Zbernica RS485, rozširujúci modul iO-8	svorky A 485 / B 485 sa **nepoužívajú**; rozširujúci modul sa pripojiť nedá	najviac 4 iO-8	najviac 4 iO-8
LED	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (nepoužíva sa)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Bliknutia LED TROUBLE	1 = fyzické spojenie LAN (kábel), 2 = chyba SIM1, 3 = chyba SIM2, 7 = ústredňa	1–8 (SIM, PIN, APN, sieť, prijímač, ústredňa, ICCID)	1–8
SMS a hovor	nie sú upozornenia SMS, príkazy SMS ani hovor: upozornenie a ovládanie idú cez Protegus 2	upozornenie SMS a hovorom, príkazy SMS	upozornenie SMS a hovorom, príkazy SMS
Ústredňa DSC súčasne na dátovej zbernici a na svorkách TIP/RING	nie	nie	áno
Nastavenie pripojenia TIP/RING (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (môžeš zvoliť aj **3. MANUAL**)
Nastavenie z aplikácie Protegus 2	áno (Advanced settings, od firmvéru 1.08)	TrikdisConfig	TrikdisConfig
Pamäť udalostí	60 udalostí	bez údaja	bez údaja
Interné správy (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	ako GT
Modem, prenosové protokoly (TRK8, DC-09, TL150), šifrovanie, kompatibilné ústredne, schémy zapojenia, Protegus 2	rovnaké	rovnaké	rovnaké

Všetky tri komunikátory sa vyrábajú s rovnakými tromi typmi modemu; na európsky trh (aj na Slovensko) je určená európska (EU) verzia. Typ modemu a hardvérovú verziu nájdeš v stavovom riadku TrikdisConfig (**Device**, **HW**) a na štítku zariadenia.

Modem	Sieť a frekvenčné pásma
EG915U-EU (Európa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8

Modem	Sieť a frekvenčné pásma
EG915U-LA (Latinská Amerika)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Kompatibilné zabezpečovacie ústredne

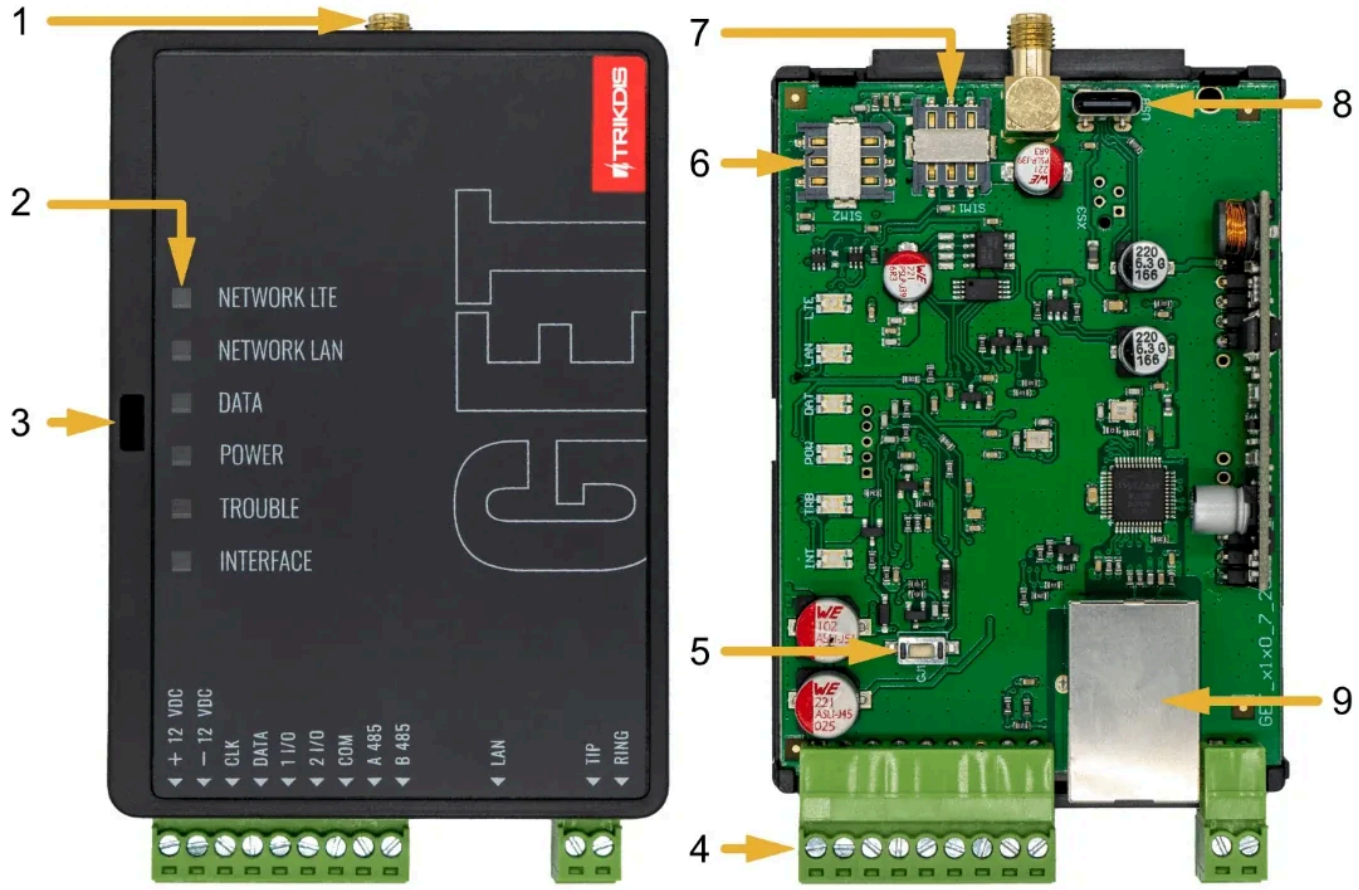
Ústredne nižšie môžeš ku komunikátoru pripojiť priamo, cez dátovú zbernicu alebo sériový port. Stĺpec „Priame ovládanie" ukazuje, či používateľ môže z Protegus 2 vlastným kódom klávesnice zapínať a vypínať stráženie bez ďalšieho zapojenia; kde to nie je možné, komunikátor číta udalosti zo zbernice a na ovládanie treba zónu kľúčového spínača (bod 3.4).

Výrobca	Typ	Pripojenie	Priame ovládanie
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	dátová zbernica (Keybus)	áno
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	sériový port (kábel EX-CRP2.4) alebo Keybus + TIP/RING	áno
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	sériový port (kábel EX-CRP2.4) alebo Keybus + TIP/RING	áno
Paradox	Digiplex EVO192, EVOHD, EVOHD+	sériový port (kábel EX-CRP2.4)	áno
Paradox	Digiplex EVO48	sériový port (kábel EX-CRP2.4)	nie
Paradox	Spectra 1727, 1728, 1738; Esprit E55	sériový port (kábel EX-CRP2.4)	nie
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	dátová zbernica	áno
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	sériový port (kábel EX-CRP4)	áno
InnerRange	Inception, Integriti	sériový port (kábel výrobcu ústredne)	nie
Honeywell	Ademco Vista-15, Vista-20, Vista-48	dátová zbernica	áno

- Priamo ovládané ústredne **Paradox** musia mať firmvér aspoň **V.4**. Na novších ústredniach Paradox (SP+, MG+, EVOHD+) môže byť sériový port z výroby zablokovaný; o odblokovaní hovorí bod 4.1.2. Ústredne Spectra SP / SP+ a Magellan MG / MG+ môžeš namiesto sériového portu pripojiť aj na dátovú zbernicu (Keybus) a svorky TIP/RING spolu – na to netreba platené odblokovanie, ale komunikátor musí mať firmvér aspoň 1.21 (bod 3.3.3).
- Ústredňa **ľubovoľného iného výrobcu** sa pripája cez svoj telefónny komunikátor (TIP/RING), ak posiela udalosti vo formáte Contact ID s vytáčaním DTMF; vtedy treba na ovládanie zónu kľúčového spínača.
- Ktorý komunikátor Trikdis a aké zapojenie sa hodí k tvojej ústredni, nájdeš vo vyhľadávači kompatibility.

1.4 Časti komunikátora

Plošný spoj komunikátora je v čiernej plastovej krabičke; predný kryt sa dá odpojiť, svorkovnica sa dá vytiahnuť. Zásuvka LAN a svorka TIP/RING sú prístupné na boku krabičky, v samostatnom otvore.



Obrázok 2. Časti komunikátora spredu (vľavo) a s otvorenou krabičkou (vpravo).

- 1 Konektor SMA mobilnej antény
- 2 Indikačné LED (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Otvor na odpojenie predného krytu
- 4 Odpojiteľná svorkovnica na vonkajšie zapojenie
- 5 Tlačidlo RESET
- 6 Držiak karty SIM2
- 7 Držiak karty SIM1
- 8 Zásuvka USB-C na programovanie
- 9 Zásuvka Ethernet (LAN) RJ45

Svorkovnica sa dá vytiahnuť: zariadenie tak jedným pohybom odpojíš od napájania alebo reštartuješ, pri zapájaní sa s ňou ľahšie pracuje a na programovanie cez USB môžeš zariadenie preniesť k počítaču.

1.5 Svorky

Svorka	Funkcia
+12 VDC	Napájanie, kladný pól: +10–18 V DC
–12 VDC	Napájanie, 0 V
CLK	Sériová zbernica alebo dátová zbernica (hodinový signál) na priame pripojenie ústredne
DATA	Sériová zbernica alebo dátová zbernica (dáta) na priame pripojenie ústredne
1 I/O	1. vstup/výstup (výrobné nastavenie: výstup, OUT)
2 I/O	2. vstup/výstup (výrobné nastavenie: výstup, OUT)
COM	Spoločný (záporný) bod pre vstupy a výstupy
A 485	Nepoužíva sa

Svorka	Funkcia
B 485	Nepoužíva sa (pár k A 485)
LAN	Zásuvka Ethernet (lokálna sieť) RJ45
TIP	Svorka TIP telefónneho komunikátora zabezpečovacej ústredne
RING	Svorka RING telefónneho komunikátora zabezpečovacej ústredne

Na schémach zapojenia sú napájacie svorky označené **+DC** a **–DC** (na zariadení +12 VDC / −12 VDC) a svorky RS485 **A RS485** / **B RS485** (na zariadení A 485 / B 485). Popis svorkovnice je aj na prednom kryte.

1.6 Signalizácia LED

LED na prednom kryte sú najdôležitejším nástrojom pri uvádzaní do prevádzky a pri hľadaní chýb. Čítaj ich spolu: POWER ukazuje napájanie, NETWORK LTE mobilnú sieť, NETWORK LAN káblovú sieť, TROUBLE chybu; LED INTERFACE nemá na GET žiadnu funkciu.

NETWORK LTE – spojenie s mobilnou sieťou

Signalizácia	Význam
nesvieti	Nie je spojenie s mobilnou sieťou
bliká na žlto	Prebieha pripájanie k mobilnej sieti
svieti na zeleno, bliká na žlto	Pripojený k mobilnej sieti; počet žltých bliknutí je **úroveň signálu**: na 4G sú 3 bliknutia vyhovujúci signál

NETWORK LAN – spojenie s káblovou sieťou

Signalizácia	Význam
nesvieti	Nie je spojenie s počítačovou sieťou
svieti na zeleno	Pripojený k počítačovej sieti

DATA – dátová prevádzka

Signalizácia	Význam
nesvieti	Žiadna udalosť nečaká na odoslanie
svieti na zeleno	V pamäti sú udalosti čakajúce na odoslanie
bliká na zeleno	Prenos dát medzi komunikátorom a počítačom (počas programovania)

Rýchla kontrola

LED DATA je najjednoduchšia kontrola internetu. LED DATA svieti, keď je v pamäti zariadenia správa čakajúca na odoslanie. Zelená LED NETWORK hovorí iba to, že sieťové spojenie je nadviazané – pri zariadení s mobilnou sieťou sa prihlásilo do siete operátora, pri ethernetovom zariadení funguje spojenie po router –, nie však to, že sa zariadenie dostane aj na internet. Ak LED NETWORK svieti nazeleno, ale LED DATA svieti nepretržite aj po udalosti alebo testovacej správe, internetové spojenie nefunguje: správa sa nedá odoslať. V mobilnej sieti je najčastejšie chybné APN alebo dátová služba SIM karty, pri Ethernete router, firewall alebo DNS. Keď LED DATA zhasne, správa odišla a dátové spojenie je v poriadku.

POWER – napájacie napätie

Signalizácia	Význam
nesvieti	Nie je napájanie alebo je napájanie odpojené
svieti na zeleno	Zapnuté, napájacie napätie je v poriadku
svieti na žlto	Nevyhovujúce napájacie napätie (najviac 11,5 V)
svieti na zeleno, bliká na žlto	Pripravený na programovanie (počas programovania)
svieti na žlto (počas programovania)	Nie je spojenie s počítačom

TROUBLE – chyba

Signalizácia	Význam
nesvieti	Žiadna chyba
1 červené bliknutie	Chyba fyzického spojenia káblovej siete (PHY Link) – skontroluj kábel LAN
2 červené bliknutia	Chyba karty SIM1
3 červené bliknutia	Chyba karty SIM2
7 červených bliknutí	Prerušilo sa spojenie so zabezpečovacou ústredňou (sériová zbernica)

INTERFACE – na GET sa nepoužíva.

1.7 Technické údaje

Parameter	Hodnota
Sieťové pripojenie	LTE (4G) a Ethernet (LAN)
Spojenie so zabezpečovacou ústredňou	sériová zbernica, dátová zbernica (Keybus) alebo telefónna linka (TIP/RING, Contact ID, DTMF)
Vstupy/výstupy	2 I/O s dvojitou funkciou: ako vstup NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (zakončovací odpor 2,2 kΩ); ako výstup s otvoreným kolektorom (OC), max. 0,15 A / 30 V DC
Modem	EG915U-EU (Európa), EG915U-LA (Latinská Amerika) alebo BG95-M5 (LTE Cat M1) – frekvenčné pásma uvádza tabuľka v bode 1.2
Karta SIM	2 držiaky nano-SIM (SIM1, SIM2)
Napájacie napätie	10–18 V DC
Odber prúdu	najviac 100 mA v pokoji; najviac 300 mA pri posielaní dát
Prenosové protokoly	TRK8, DC-09_2007, DC-09_2012, TL150
Šifrovanie	AES-128
Pamäť udalostí	60 udalostí
Programovanie	TrikdisConfig (Windows) cez kábel USB-C alebo na diaľku; aplikácia Protegus 2 (od firmvéru 1.08)
Prevádzkové prostredie	−10 … +50 °C, max. 80 % relatívna vlhkosť (pri +20 °C)
Rozmery	113 × 70 × 25 mm
Hmotnosť	110 g

2. Rýchle spustenie

Nastavenia komunikátora môžeš urobiť dvoma nástrojmi: programom **TrikdisConfig**, ktorý beží vo Windows – cez kábel USB-C alebo na diaľku –, a **z aplikácie Protegus 2** (Settings → Advanced settings). V tejto kapitole opisujeme najkratšiu cestu: ktoré nastavenia treba, aby komunikátor posielal udalosti na PCO a aby sa systém dal ovládať z aplikácie Protegus 2. Pri každom kroku uvádzame cestu v aplikácii aj v TrikdisConfig; podrobné vysvetlenie nastavení obsahuje kapitola 6.

2.1 Príprava

Čo budeš potrebovať

Kábel USB-C na programovanie · aspoň 4-žilový kábel medzi komunikátor a ústredňu · k sériovému portu Paradox kábel CRP2.4 · plochý skrutkovač 2,5 mm · mobilná anténa s vhodným ziskom, ak je na mieste slabé pokrytie · aktívna karta SIM (jedna alebo dve; požiadavku na PIN môžeš vypnúť), ak používaš mobilnú sieť · ethernetový kábel k routeru alebo switchu, ak používaš káblovú sieť · inštalačný návod zabezpečovacej ústredne.

Potrebné príslušenstvo objednaj samostatne u predajcu.

Nastavenie cez TrikdisConfig. Zariadenie nastavíš na stole, pred zapojením, potom ho na mieste už len zapojíš.

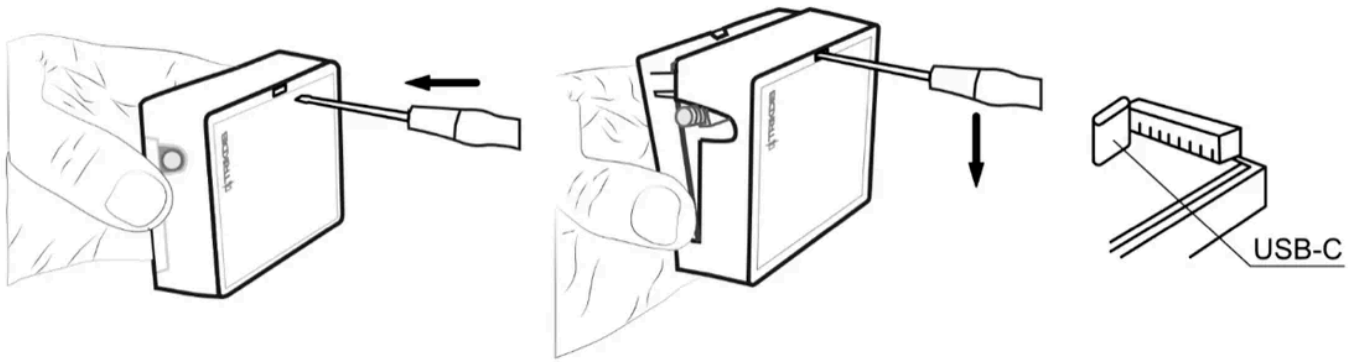
1. Stiahni a nainštaluj softvér TrikdisConfig. Na webe www.trikdis.com zadaj do vyhľadávacieho poľa: „TrikdisConfig“.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

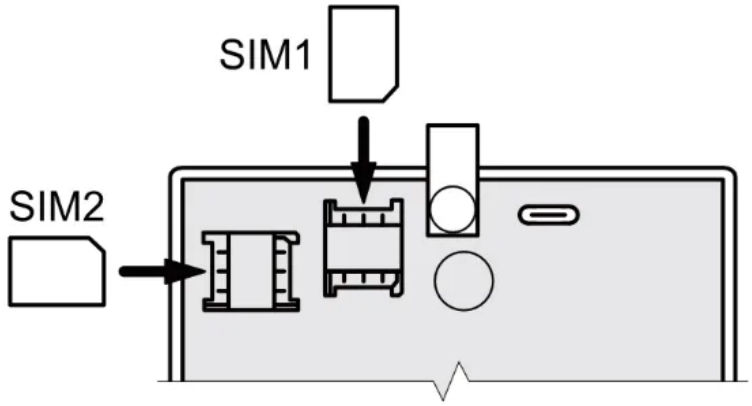
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Otvor krabičku komunikátora plochým skrutkovačom: skrutkovač zasuň hore do štrbiny vedľa antény a páč smerom von, potom dole pri otvore smerom nadol. Obrázok ukazuje aj miesto zásuvky USB-C na okraji plošného spoja.



Obrázok 3. Odpojenie predného krytu plochým skrutkovačom; zväčšený detail ukazuje miesto zásuvky USB-C.

3. Vlož kartu nano-SIM (alebo karty) do držiaka v smere, ktorý ukazuje obrázok: držiak SIM1 je v strede plošného spoja, SIM2 na jeho okraji. Karta má byť aktívna, má mať mobilné dáta a ak sa dá, vypni na nej v telefóne požiadavku na PIN (tak nemusíš PIN zadávať do zariadenia). Ak komunikátor používaš len na káblovej sieti, karta SIM nie je potrebná.



Obrázok 4. Miesto držiakov SIM1 a SIM2 na plošnom spoji, šípky ukazujú smer vloženia karty.

4. Prepoj komunikátor s počítačom káblom USB-C.

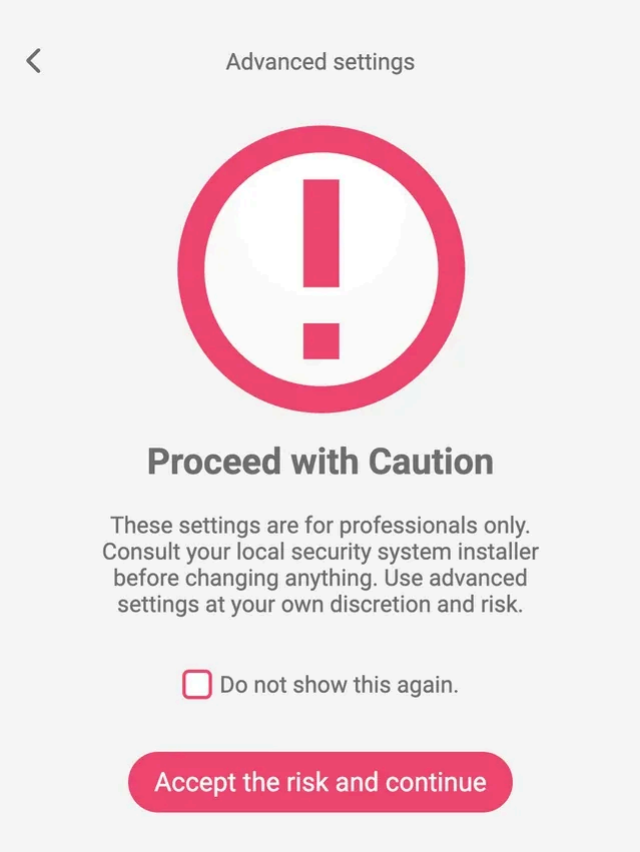
Upozornenie

Kým je zariadenie pripojené USB káblom k počítaču, je v programovacom režime: zastaví sa jeho bežná činnosť, nestráži, nehlási, nedá sa ovládať, napája sa z USB a po odpojení kábla sa reštartuje. Preto zariadenie nesmie byť voľne prístupné: musí byť v uzavretej kovovej skrinke so sabotážnou ochranou (tamper) alebo s pohybovým detektorom, ktorý skrinku stráži. Podrobnosti v FAQ

5. Spusti TrikdisConfig. Program zariadenie rozpozná a otvorí programovacie okno. Klikni na tlačidlo **Read [F4]** (čítanie): program načíta aktuálne nastavenia zariadenia. Ak pýta heslo, zadaj 6-miestny kód administrátora (z výroby `123456`) alebo inštalátora (z výroby `654321`).

Nastavenie z aplikácie Protegus 2. Z aplikácie môžeš nastavovať, ak je komunikátor už online a pridal si ho do svojho účtu Protegus (bod 5.1). Ak sa komunikátor ešte nevie pripojiť – napríklad preto, že karta SIM pýta kód PIN, alebo operátor vyžaduje iný APN –, prvé nastavenie urob cez TrikdisConfig.

1. V aplikácii otvor systém a prejdi do ponuky **Settings** → **Advanced settings**.
2. Pri prvom otvorení ťa aplikácia upozorní (**Proceed with Caution**): tieto nastavenia sú určené pre odborníka. Ťukni na tlačidlo **Accept the risk and continue**; ak zaškrtneš **Do not show this again**, upozornenie sa nabudúce nezobrazí.
3. Aplikácia načíta nastavenia komunikátora. Ak pýta **Service Access code**, zadaj prístupový kód Protegus Cloud komunikátora (z výroby `123456`).
4. Urob nastavenia opísané nižšie a potom ťukni na tlačidlo **Write**: aplikácia ich zapíše do komunikátora.



Obrázok 5. Protegus 2 – upozornenie (Proceed with Caution), ktoré sa zobrazí pri prvom otvorení Advanced settings, a tlačidlo Accept the risk and continue.

Z aplikácie Protegus 2 sa GET dá nastaviť s **firmvérom 1.08 alebo novším** (aktualizáciu opisuje kapitola 9).

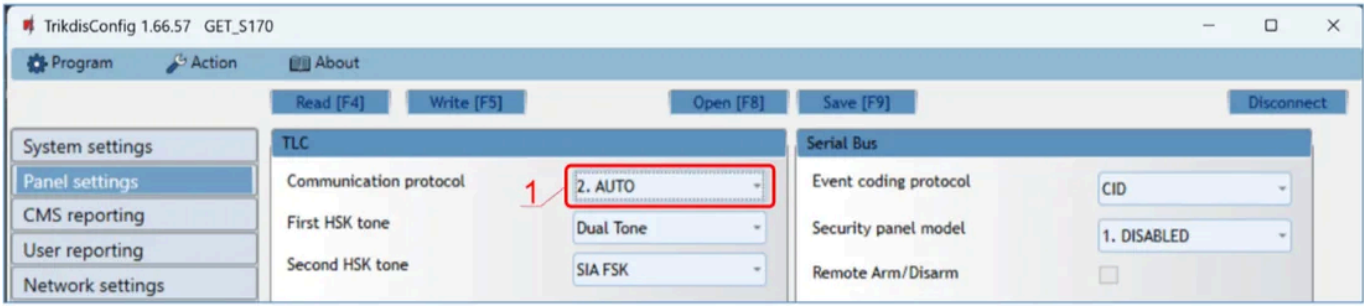
2.2 Spojenie s aplikáciou Protegus 2

V aplikácii (Settings → Advanced settings):

1. **Panel settings** → **TLF** – ak je komunikátor pripojený na svorky TIP/RING ústredne: **Security panel model** nastav na **AUTO**.
2. **Panel settings** → **Serial Bus** – ak je komunikátor pripojený na dátovú zbernicu alebo sériový port ústredne: v poli **Security panel model** vyber typ pripojenej ústredne.
3. Na tom istom mieste zapni voľbu **Remote Arm/Disarm**, ak chcú používatelia ovládať ústredňu z Protegus 2 vlastným kódom klávesnice. Zobrazí sa len pri priamo ovládateľných ústredniach.
4. Na priame ovládanie ústredne Paradox zadaj **PC download password**, pri ústredni Texecom **UDL passcode**; musí sa zhodovať s heslom nastaveným v ústredni.
5. **User reporting** → **Cloud**: zapni voľbu **Enabled** a zmeň **Cloud access code**, ak chceš, aby ho používateľ musel zadať pri pridávaní systému do aplikácie (z výroby `123456`).
6. **Network settings** → **LAN** – ak je komunikátor pripojený na káblovú sieť: zapni voľbu **Use DHCP**.
7. **Network settings** → **SIM** a **SIM2** – pre každú vloženú kartu SIM: zadaj **SIM card PIN** a **APN** a skontroluj, či **DNS1** a **DNS2** fungujú u tvojho operátora.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: v poliach **Main type**, **Backup type** a **Backup type 2** nastav, v akom poradí komunikátor používa spojenie **LAN**, **SIM** (SIM1) a **SIM2**.
9. Ťukni na tlačidlo **Write**.

V TrikdisConfig. Najprv na stránke **Panel settings** zadaj, ako je komunikátor pripojený k ústredni.

Ak ho pripájaš na telefónny výstup ústredne (TIP/RING): v poli **Communication protocol** vyber hodnotu **AUTO**.



Obrázok 6. TrikdisConfig – Panel settings, skupina TLC.

- 1 **Communication protocol** – pri pripojení TIP/RING **2. AUTO**.

Ak ho pripájaš na dátovú zbernicu alebo sériový port ústredne: ústredňu nastav v skupine **Serial bus**.

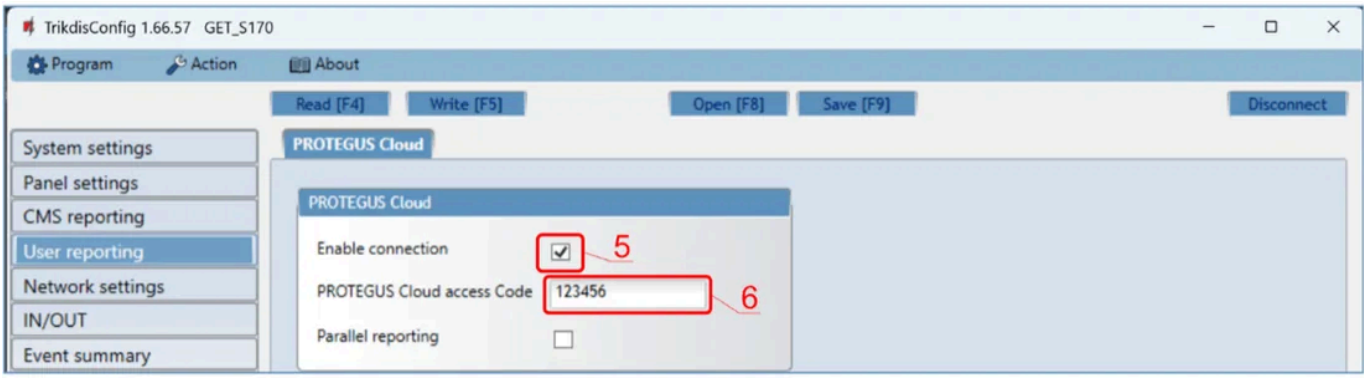


Obrázok 7. TrikdisConfig – Panel settings, skupina Serial bus.

- 2 **Security panel model** – typ pripojenej ústredne.
- 3 **Remote Arm/Disarm** – zaškrtni, ak chcú používatelia ovládať ústredňu z Protegus 2 vlastným kódom klávesnice. Zobrazí sa len pri priamo ovládateľných ústredniach.
- 4 **Security panel PC download password** – na priame ovládanie ústredne Paradox a Texecom heslo PC, resp. UDL nastavené v ústredni; obe sa musia zhodovať.

Na priame ovládanie treba nastaviť aj zabezpečovaciu ústredňu – to opisuje kapitola 4, kde nájdeš aj postup zadania hesla PC, resp. UDL.

Potom na stránke **User reporting**, na karte **PROTEGUS Cloud**, povoľ spojenie s cloudom.



Obrázok 8. TrikdisConfig – User reporting, karta PROTEGUS Cloud.

- 5 **Enable connection** – zaškrtni: povolí spojenie s cloudom Protegus.
- 6 **PROTEGUS Cloud access Code** – prístupový kód do Protegus 2 (z výroby `123456`). Zmeň ho, ak chceš, aby ho používateľ musel zadať pri pridávaní systému do aplikácie. Ak kód neskôr zmeníš, musíš ho prepísať aj v aplikácii Protegus 2.

Ak je komunikátor pripojený na káblovú sieť, na stránke **Network settings**, na karte **LAN** zaškrtni voľbu **Use DHCP**: komunikátor automaticky dostane nastavenia siete (masku podsiete, bránu) a IP adresu.



Obrázok 9. TrikdisConfig – Network settings, karta LAN (Ethernet settings).

- 7 **Use DHCP** – keď je zaškrtnuté, komunikátor dostane IP adresu a sieťové nastavenia automaticky od routera.

Ak je v komunikátore karta SIM (jedna alebo dve karty), na karte **SIM1** (a **SIM2**) zadaj údaje karty.



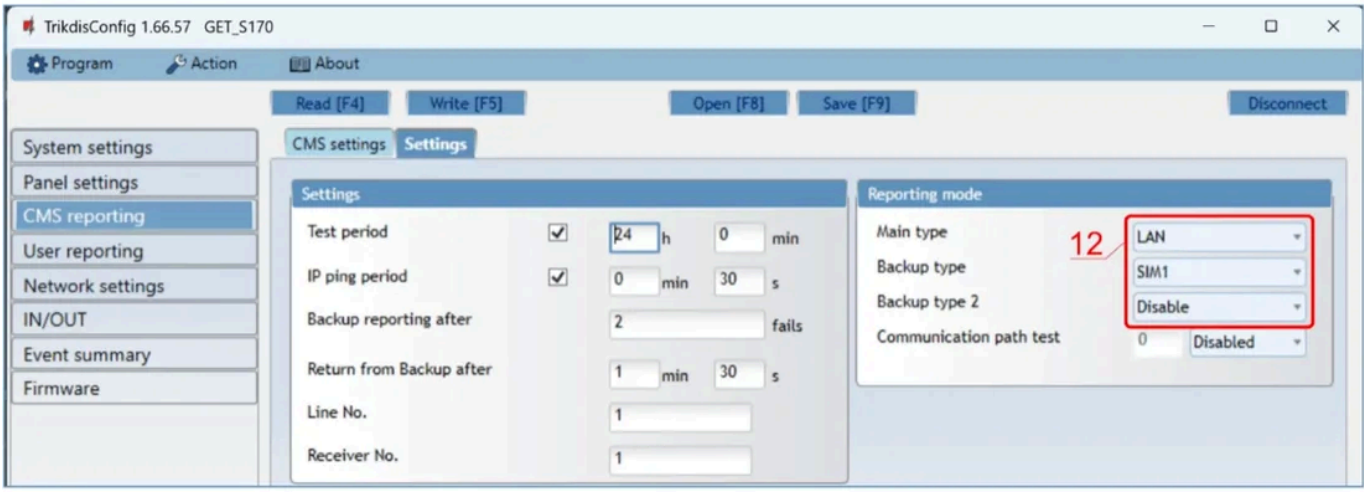
Obrázok 10. TrikdisConfig – Network settings, karta SIM1.

- 8 **SIM card PIN** – kód PIN karty (ak je požiadavka na PIN vypnutá, môže zostať výrobná hodnota).
- 9 **APN** – prístupový bod dátového spojenia operátora (pozri nižšie).
- 10 **DNS 1** – primárny menný server; z výroby DNS Google. Nezávisle od nastavení IP skontroluj, či adresy DNS fungujú u tvojho operátora.
- 11 **DNS 2** – sekundárny menný server (z výroby tiež Google).

APN (Access Point Name) je prístupový bod dátového spojenia mobilného operátora; bez neho sa zariadenie nevie cez mobilnú sieť pripojiť na internet. Presnú hodnotu nájdeš na webe operátora karty SIM. Známe APN slovenských a ďalších európskych operátorov vedieme v samostatnom článku: Nastavenie APN – zoznam európskych mobilných operátorov. Ak od operátora nemáš iný údaj, vyskúšaj APN `internet`: je všeobecný a funguje v sieti mnohých operátorov.

K dátovej karte IoT / M2M (komunikácia medzi strojmi) dáva operátor zvyčajne **iný APN ako ku kartám pre domácnosti** – s APN pre domácnosti sa zariadenie nepripojí. Aj túto hodnotu nájdeš v článku o APN, alebo si ju vyžiadaj od operátora; ak operátor uvedie aj používateľské meno a heslo, zadaj aj tie.

Nakoniec na stránke **CMS reporting**, na karte **Settings**, v skupine **Reporting mode** zadaj poradie spojení: touto cestou posiela komunikátor správy na PCO a do Protegus 2.



Obrázok 11. TrikdisConfig – CMS reporting, karta Settings, skupina Reporting mode (z výroby Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type**: hlavné spojenie (LAN, SIM1 alebo SIM2); **Backup type**: záložné; **Backup type 2**: druhé záložné.

Typy spojenia zadávaš v poradí. Ak sa komunikátor nevie pripojiť spojením **Main type**, prepne na **Backup type** a tak ďalej. Ak záložné spojenie úspešne odovzdalo správu na PCO, komunikátor sa po uplynutí nastaveného času pokúsi vrátiť na hlavné spojenie (bod 6.4.2).

Ak zariadenie na PCO nehlási, nastavenie je hotové: stlač tlačidlo **Write [F5]** (zápis), počkaj na potvrdenie a odpoj kábel USB.

Pri pripojení na telefónnu linku (TIP/RING) nezabudni zapnúť a nastaviť vytáčač zabezpečovacej ústredne, inak ústredňa nepošle žiadnu udalosť; na priame ovládanie treba nastaviť aj ústredne Paradox, Texecom, Caddx, InnerRange a Honeywell. Nastavenie ústredne opisuje kapitola 4.

2.3 Spojenie s PCO

V aplikácii (Settings → Advanced settings):

1. **System options** → **System general**: zadaj identifikátor objektu, ktorý si dostal od PCO (**Account No.**; 0–9, A–F; `FFFE` a `FFFF` sa nedajú použiť). Na hardvérovej verzii **x1x1** s firmvérom **1.31** alebo novším zadávaš identifikátor objektu pre každý kanál zvlášť: **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** Spoznáš to z obrazovky: ak System general ukazuje len pole **Time set**, použi nastavenie kanála.
2. **Panel settings** → **TLF** (pripojenie TIP/RING): **Security panel model** nastav na **AUTO**; alebo **Panel settings** → **Serial Bus** (pripojenie na dátovú zbernicu alebo sériový port): vyber **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel**: zapni voľbu **Enabled** a potom zadaj: **Communication type**: **IP**; adresu prijímača **Domain or IP** a jeho **Port**; **TCP or UDP**; **Protocol**: **TRK8** pre prijímač Trikdis, **DC-09_2007** alebo **DC-09_2012** pre univerzálny prijímač, **TL150** pre prijímač SUR-GARD; a šifrovací kľúč nastavený v prijímači: pri protokole TRK v poli **TRK encryption key**, pri DC-09 zapni voľbu **Enable encryption key** a zadaj **DC-09 encryption key**.
4. (Odporúčané) Rovnako nastav aj **Backup channel** (záložný kanál).
5. **Reporting to CMS** → **CMS settings** → **Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.
6. **Network settings** → **LAN** (káblová sieť): zapni voľbu **Use DHCP**. **Network settings** → **SIM** a **SIM2** (pre každú kartu SIM): **SIM card PIN**, **APN** a skontroluj polia **DNS1**, **DNS2**.
7. Ťukni na tlačidlo **Write**.

V TrikdisConfig. Najprv na stránke **System settings** zadaj identifikátor objektu.

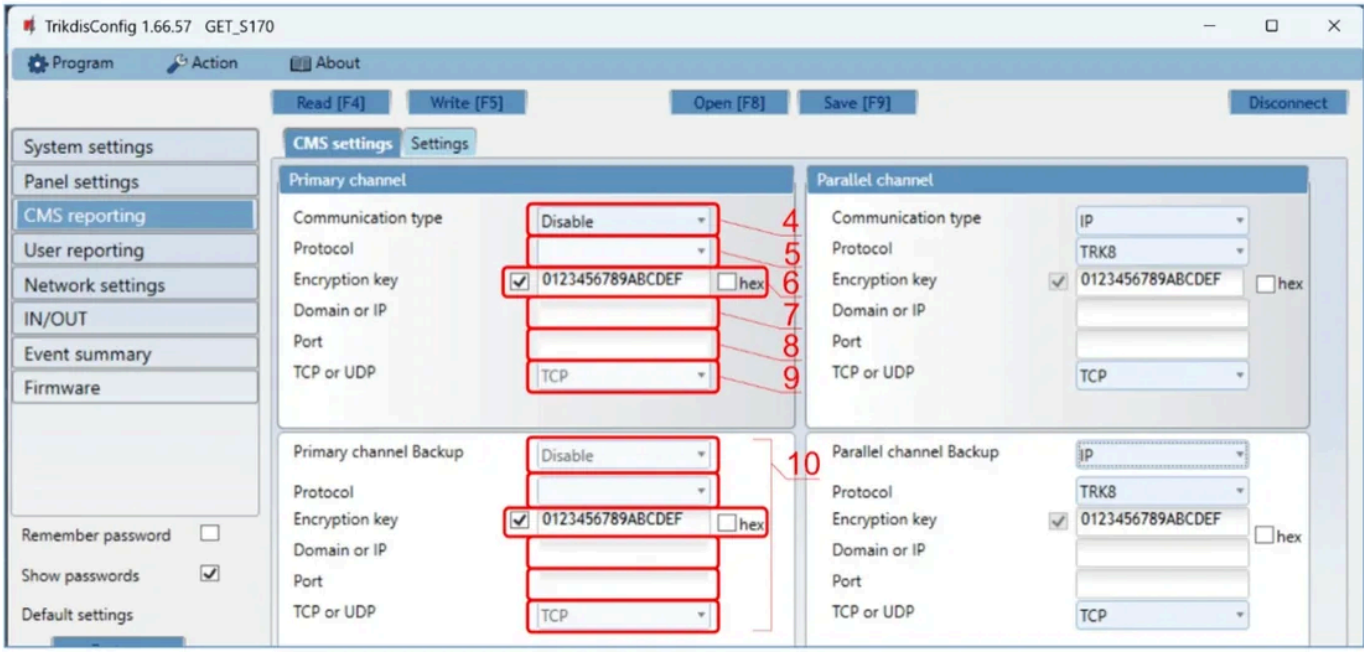


Obrázok 12. TrikdisConfig – stránka System settings, skupina General.

- 1 **Object ID** – identifikátor objektu, ktorý si dostal od PCO (6 hexadecimálnych znakov, 0–9, A–F). `FFFE` a `FFFF` sa nedajú použiť.

Na stránke **Panel settings** zadaj pripojenie ústredne, ak si to ešte neurobil v bode 2.2: pri pripojení TIP/RING nastav **Communication protocol** na **AUTO**; pri pripojení na dátovú zbernicu alebo sériový port vyber v poli **Security panel model** typ pripojenej ústredne (obrázky v bode 2.2).

Potom na stránke **CMS reporting**, na karte **CMS settings**, v časti **Primary channel** (hlavný kanál) nastav údaje prijímača. Na obrázku je okno pred nastavením: pole **Communication type** hlavného kanála je ešte **Disable**.



Obrázok 13. TrikdisConfig – CMS reporting, karta CMS settings.

- 4 **Communication type** – vyber spojenie **IP**.
- 5 **Protocol** – **TRK8** pre prijímač Trikdis, **DC-09_2007** alebo **DC-09_2012** pre univerzálny prijímač, **TL150** pre prijímač SUR-GARD.
- 6 **Encryption key** – šifrovací kľúč nastavený v prijímači.
- 7 **Domain or IP** – doménové meno alebo IP adresa prijímača.
- 8 **Port** – číslo portu prijímača.
- 9 **TCP or UDP** – prenosový protokol; riadi sa nastavením prijímača.
- 10 **Primary channel Backup** – záložný kanál pre prípad chyby hlavného; vyplň ho rovnako, odporúčame ho zadať.

Na karte **Settings**, v skupine **Reporting mode** zadaj poradie spojení (**Main type**, **Backup type**, **Backup type 2**), ak si to ešte neurobil v bode 2.2 – tam nájdeš aj obrázok a opis fungovania.

Nakoniec na stránke **Network settings** zadaj údaje siete, ak si to ešte neurobil v bode 2.2: na karte **LAN** zaškrtnutie **Use DHCP**, na karte **SIM1** (a **SIM2**) údaje karty (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Pri protokole **DC-09** zadaj na karte **Settings** aj číslo linky a prijímača (**Line No.**, **Receiver No.**, bod 6.4.2). GET hlási na PCO len cez IP spojenie – po káblovej sieti alebo mobilnom internete –, záložný kanál SMS nemá.

Na konci nastavenia stlač tlačidlo **Write [F5]** (zápis), počkaj na potvrdenie a odpoj kábel USB. Zariadenie je tým pripravené na zapojenie. Pri pripojení na telefónnu linku treba aj tu zapnúť a nastaviť vytáčač zabezpečovacej ústredne, inak ústredňa nepošle žiadnu udalosť (kapitola 4).

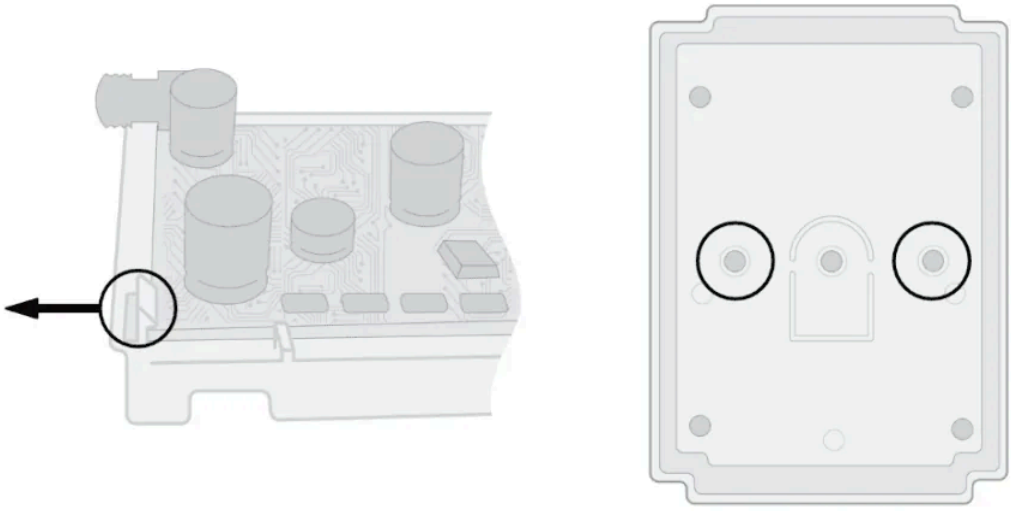
3. Inštalácia a zapojenie

Figyelem!

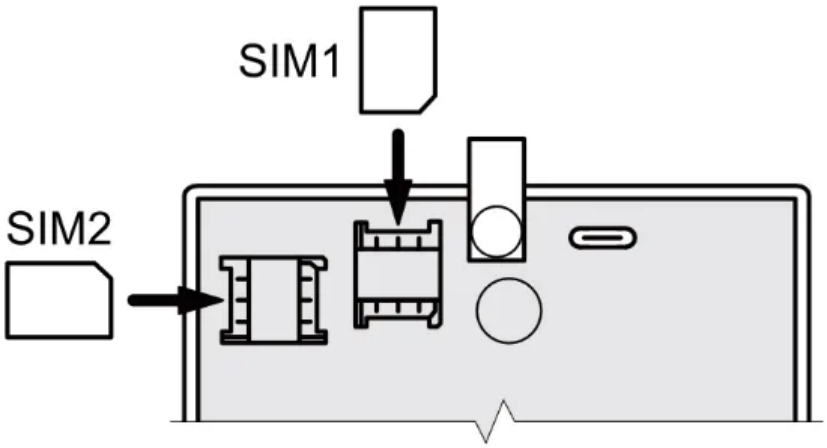
Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

3.1 Postup inštalácie

1. Zlož predný kryt (pozri bod 2.1) a vytiahni svorkovnicu.
2. Vlož kartu nano-SIM – alebo obe – do držiaka, ak si to neurobil už pri uvádzaní do prevádzky.
3. Vyber plošný spoj zo zadného dielu: otvor západku vedľa konektora antény a plošný spoj vyber (pozri obrázok).
4. Zadný diel pripevni skrutkami na zvolené miesto (na obrázku sú otvory na skrutky zakrúžkované), alebo podľa bodu 3.2 priloženou obojstrannou lepiacou páskou.
5. Vlož plošný spoj späť do zadného dielu a zasuň späť svorkovnicu.
6. Naskrutkuj mobilnú anténu.
7. Nasaď späť predný kryt.
8. Ak posielaš udalosti na PCO aj cez káblovú sieť (LAN), zasuň sieťový kábel do zásuvky LAN komunikátora.



Obrázok 14. Vybratie plošného spoja zo zadného dielu (vľavo: západka a smer vyberania) a otvory na skrutky v zadnom diele (vpravo).



Obrázok 15. Miesto dvoch držiakov SIM na plošnom spoji: SIM1 v strede dosky, SIM2 na jej ľavom okraji; šípky ukazujú smer vloženia karty.

Do komunikátora môžeš vložiť jednu alebo dve karty SIM. Karta má byť aktívna a na používanie cez IP na nej musia fungovať mobilné dáta. Ak nechceš, aby TrikdisConfig pýtal kód PIN, vlož kartu do mobilného telefónu a vypni na nej požiadavku na PIN.

3.2 Umiestnenie v skrinke ústredne, anténa

Komunikátor treba umiestniť do **skrinky zabezpečovacej ústredne chránenej sabotážnym kontaktom krytu**. Na vnútornú zadnú stenu skrinky ho pripevni priloženou obojstrannou akrylovou penovou páskou priemyselnej kvality: pásku nalep na čistý, suchý povrch so silným pritlačením, aby spoľahlivo držala. Ak skrinka ústredne takéto bezpečné pripevnenie neumožňuje, komunikátor môžeš namontovať aj do samostatnej skrinky chránenej proti sabotáži.

- **V kovovej skrinke** sa mobilný signál silno zoslabí. Ak komunikátor ide do kovovej skrinky ústredne, anténu vyveď mimo skrinky alebo použi anténu s dlhším káblom.
- Pred konečným pripevnením **skontroluj úroveň signálu**: počet žltých bliknutí LED NETWORK LTE má byť na 4G aspoň 3 (bod 1.6). Ak je menší, nájdi pre anténu lepšie miesto, alebo použi citlivejšiu anténu, ktorú môžeš umiestniť ďalej.
- Anténu a komunikátor drž ďalej od transformátora ústredne a od sieťových vodičov.
- Kábel LAN veď cez káblovú priechodku skrinky do zásuvky RJ45 na boku komunikátora; kábel nesmie ťahať za svorky.



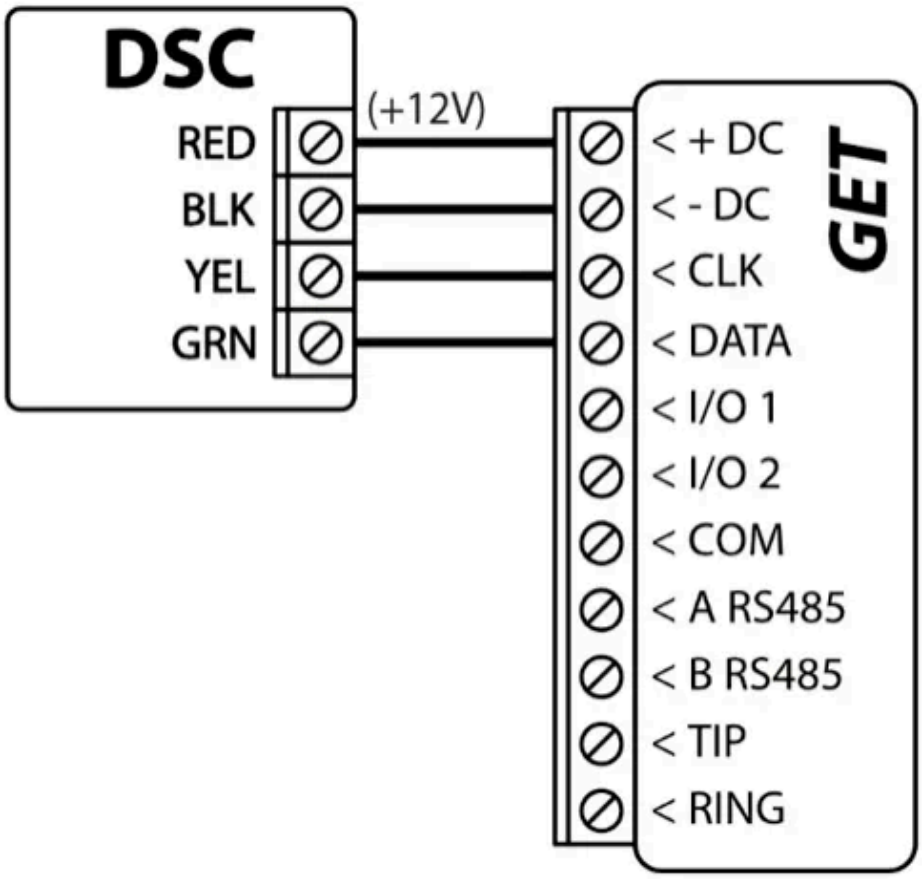
A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna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

3.3 Pripojenie k zabezpečovacej ústredni

Z nasledujúcich schém postupuj podľa tej, ktorá zodpovedá tvojej ústredni. Na schémach sú **+DC** a **–DC** napájacie svorky komunikátora **+12 VDC** / **–12 VDC** a **A RS485** / **B RS485** svorky **A 485** / **B 485** (tie sa na GET nezapájajú). Komunikátor dostáva napájanie z pomocného napájacieho výstupu (AUX) ústredne, takže pri výpadku prúdu napája komunikátor aj akumulátor ústredne.

3.3.1 DSC – dátová zbernica (Keybus)

Zbernicu Keybus ústredne DSC pripoj ku komunikátoru štyrmi vodičmi: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

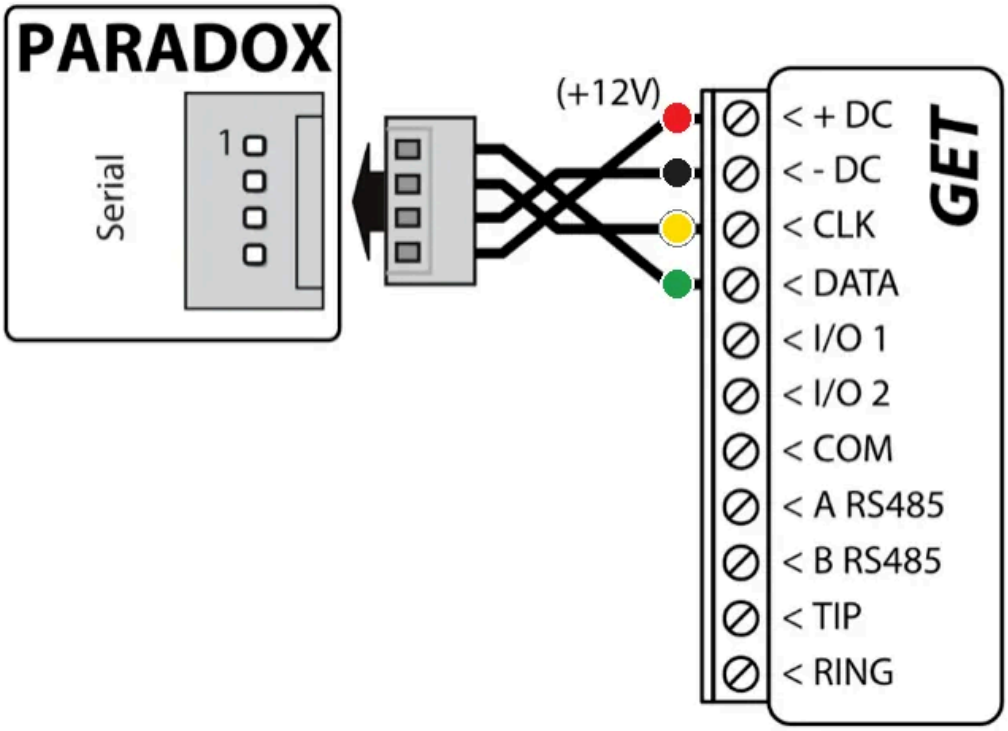


Obrázok 16. Pripojenie ústredne DSC na dátovú zbernicu (Keybus, „Keypad bus"): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

GET obsluhuje ústredňu DSC len na dátovej zbernici; súčasné zapojenie zbernice Keybus a svoriek TIP/RING je len na komunikátore GT+. Keď je pripojený len na Keybus, komunikátor dostáva od ústredne všeobecný stav zón, ale nie typ zóny (požiar, vlámanie, únik vody atď.), preto hlási každý poplach ako **všeobecný poplach s kódom Contact ID E130**. Ak PCO potrebuje vlastné kódy ústredne (napríklad požiarny poplach: E110), udalosti môžeš posielať telefónnym vytáčačom ústredne, zapojením TIP/RING (body 3.3.9 a 4.2); vtedy nie je priame ovládanie.

3.3.2 Paradox – sériový port

Na sériový port ústredne Paradox sa komunikátor pripája samostatne objednávaným káblom **EX-CRP2.4**: **červený → +DC**, **čierny → −DC**, **žltý → CLK**, **zelený → DATA**.



Obrázok 17. Pripojenie ústredne Paradox na sériový port káblom EX-CRP2.4 (objednáva sa samostatne; „Use the EX-CRP2.4 cable (ordered separately)“): červený → +DC, čierny → −DC, žltý → CLK, zelený → DATA.

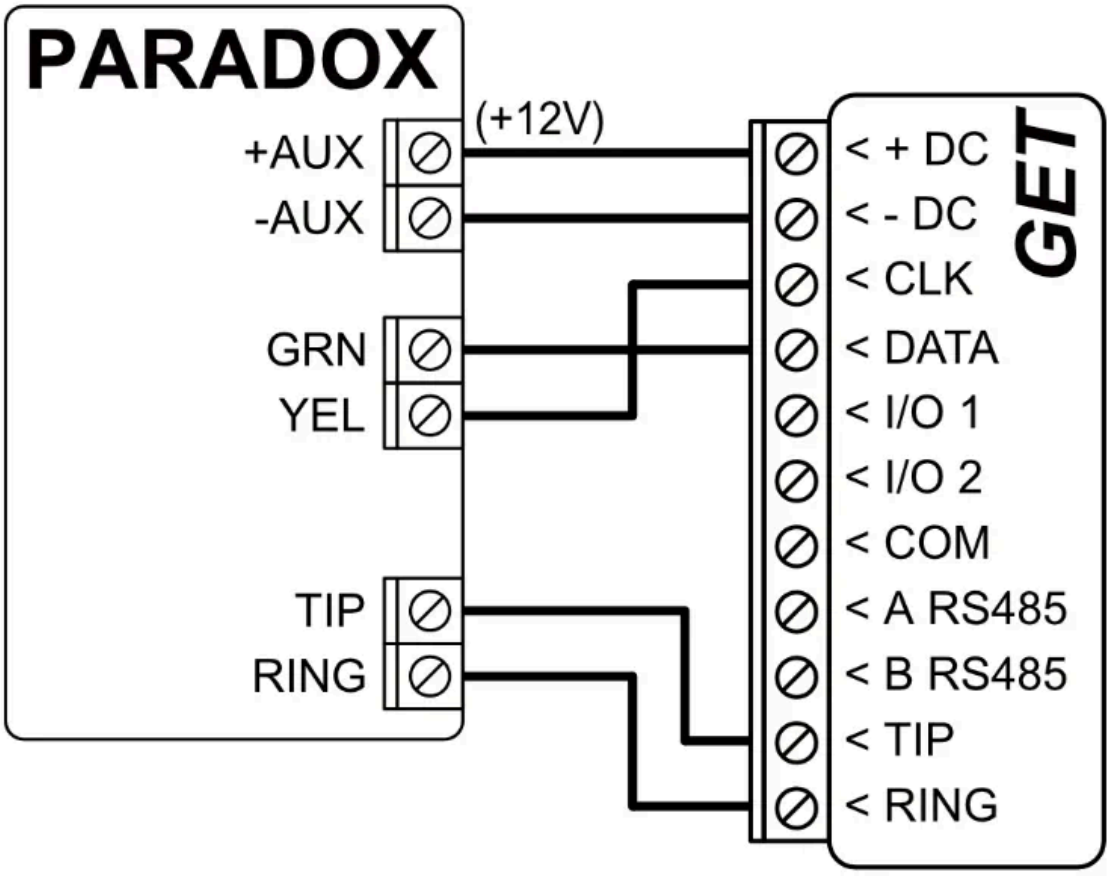
- červený vodič („R - red“)
- čierny vodič („B - black“)
- žltý vodič („Y - yellow“)
- zelený vodič („G - green“)

Na novších ústredniach Paradox (SP+, MG+, EVOHD+) môže byť sériový port z výroby zablokovaný; o odblokovaní hovorí bod 4.1.2. Pri ústredniach Spectra SP / SP+ a Magellan MG / MG+ môžeš namiesto sériového portu použiť aj zapojenie podľa nasledujúceho bodu.

3.3.3 Paradox SP/MG – Keybus a TIP/RING

Ústredňu Paradox Spectra SP, SP+ a Magellan MG, MG+ môžeš namiesto sériového portu pripojiť aj na jej dátovú zbernicu (Keybus) a svorky TIP/RING spolu: **+AUX → +DC**, **−AUX → −DC**, **GRN → DATA**, **YEL → CLK**, ďalej **TIP → TIP**, **RING → RING**. Toto zapojenie používa namiesto sériového portu zbernicu Keybus ústredne, preto naň netreba platené odblokovanie sériového portu Paradox.

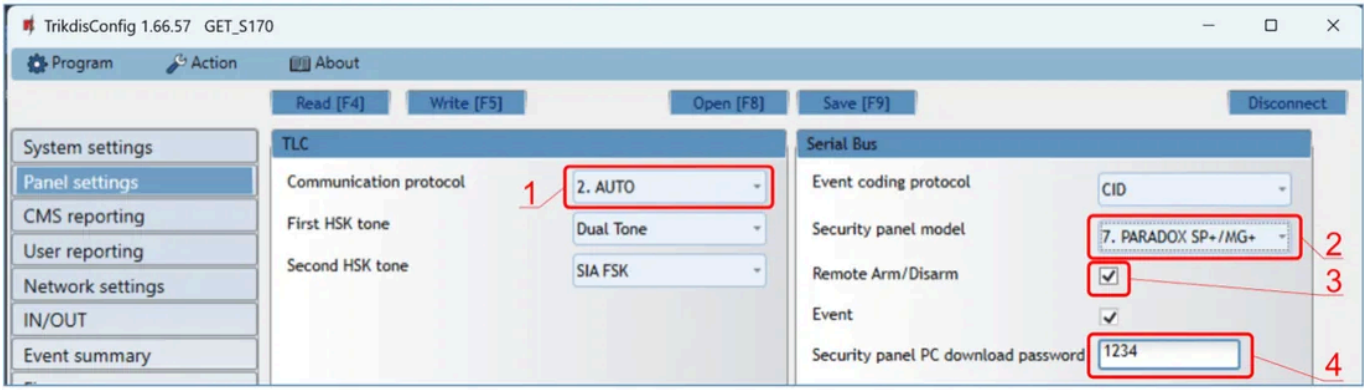
Na toto zapojenie musí mať komunikátor firmvér aspoň **1.21** (aktualizáciu opisuje kapitola 9).



Obrázok 18. Pripojenie ústredne Paradox SP / SP+ / MG / MG+ na Keybus (dátová zbernica, „Keypad bus“) a svorky TIP/RING spolu: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Na toto zapojenie nastav na stránke **Panel settings** v TrikdisConfig:

1. **Communication protocol**: **2. AUTO**.
2. **Security panel model**: zo zoznamu vyber položku **Paradox SP+/MG+ series KeyBus** (na obrázku 7. PARADOX SP+/MG+).
3. **Remote Arm/Disarm**: zaškrtni, ak chcú používatelia ovládať ústredňu z aplikácie Protegus 2 vlastným kódom klávesnice.
4. **Security panel PC download password**: na priame ovládanie zadaj heslo PC nastavené v ústredni; obe sa musia zhodovať.



Obrázok 19. TrikdisConfig – Panel settings pre zapojenie Keybus + TIP/RING: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm zaškrtnuté (3), zadané Security panel PC download password (4).

V aplikácii Protegus 2 sú tie isté nastavenia na kartách **Panel settings** → **TLF** (Security panel model = Communication protocol) a **Panel settings** → **Serial Bus** (bod 6.3).

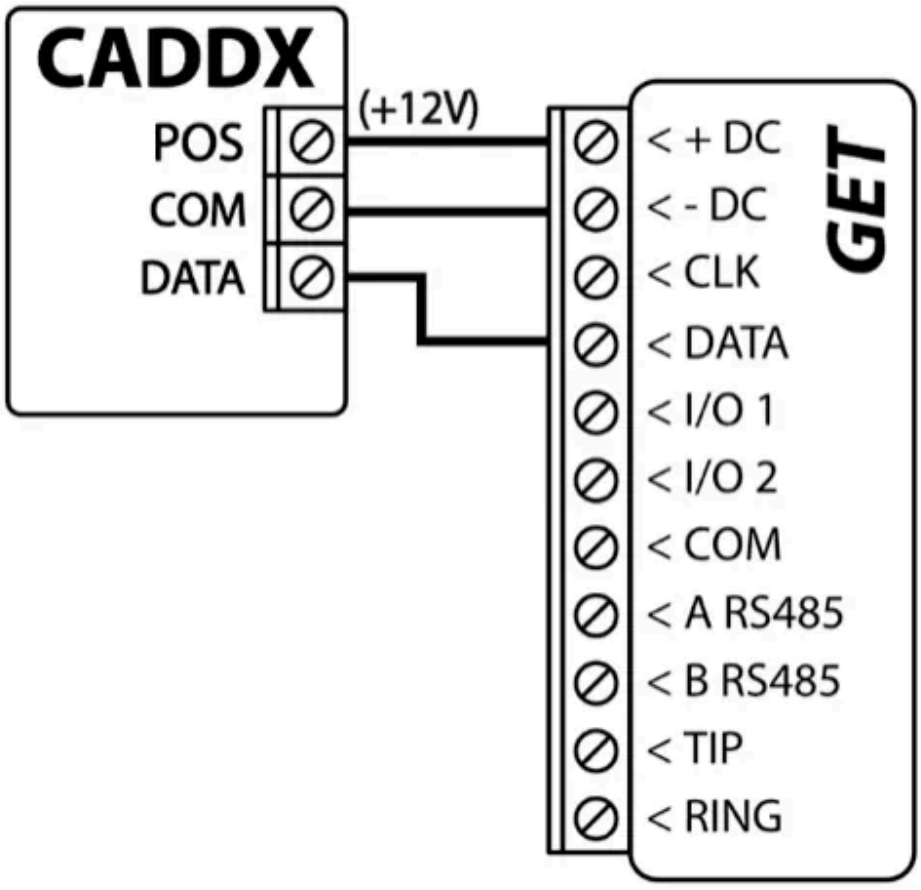
Aj ústredňu Paradox treba naprogramovať, aby posielala udalosti na PCO a dala sa ovládať z Protegus 2 – na klávesnici pripojenej k ústredni nastav tieto bunky:

Bunka	Hodnota	Bunka	Hodnota
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

Heslo PC zapísané do bunky **911** sa musí zhodovať s poľom **Security panel PC download password** komunikátora (bod 4.1.2).

3.3.4 UTC Interlogix (Caddx) – dátová zbernica

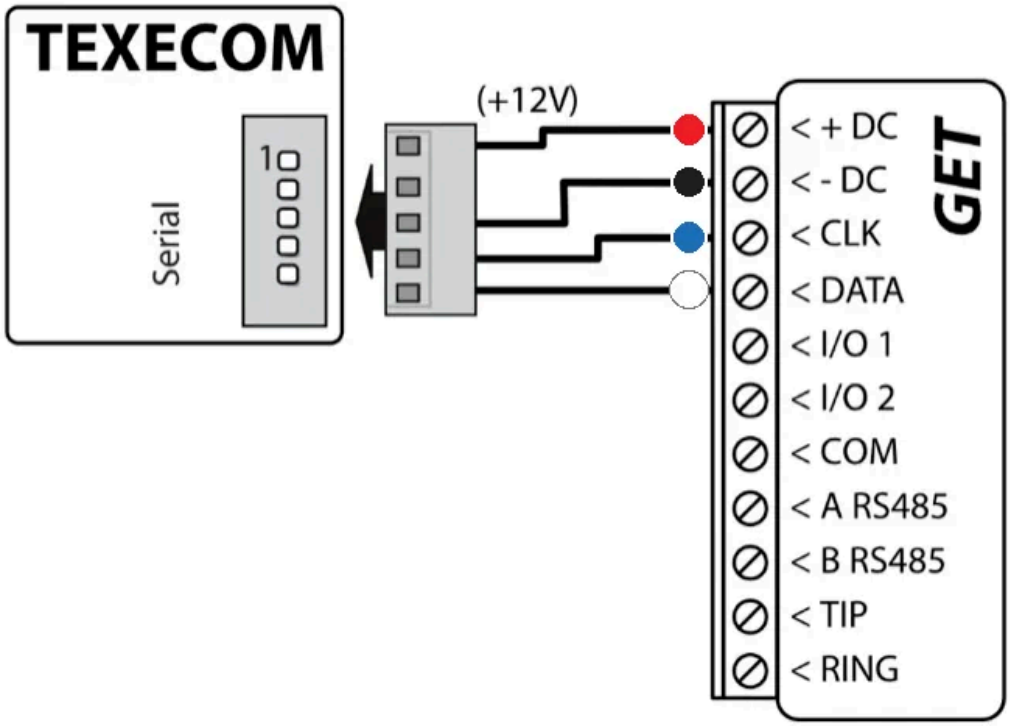
Dátovú zbernicu ústredne Caddx NetworX pripoj ku komunikátoru tromi vodičmi: **POS** → **+DC**, **COM** → **−DC**, **DATA** → **DATA**. Svorky CLK, TIP a RING netreba.



Obrázok 20. Pripojenie ústredne UTC Interlogix (Caddx) NetworX na dátovú zbernicu („Keypad bus"): POS → +DC, COM → −DC, DATA → DATA.

3.3.5 Texecom – sériový port

Na sériový port ústredne Texecom Premier / Premier Elite sa komunikátor pripája samostatne objednávaným káblom **EX-CRP4**: **červený** → **+DC**, **čierny** → **−DC**, **modrý** → **CLK**, **biely** → **DATA**.

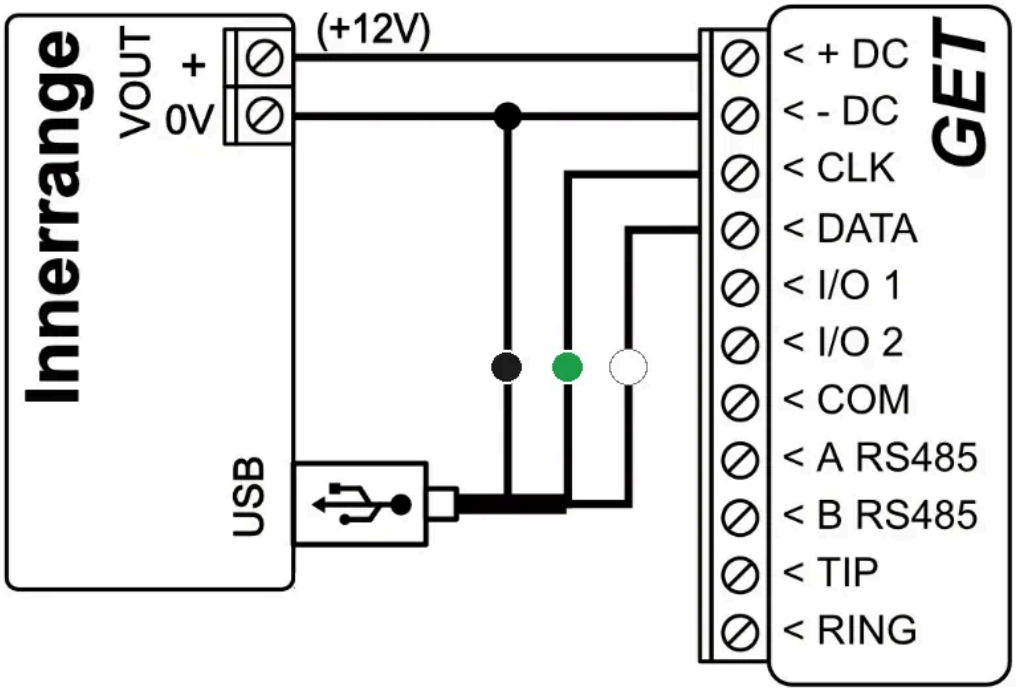


Obrázok 21. Pripojenie ústredne Texecom na sériový port káblom EX-CRP4 (objednáva sa samostatne; „Use the EX-CRP4 cable (ordered separately)"): červený → +DC, čierny → −DC, modrý → CLK, biely → DATA.

- červený vodič („R - red")
- čierny vodič („B - black")
- modrý vodič („BL - blue")
- biely vodič („W - white")

3.3.6 InnerRange Inception

Komunikátor dostáva napájanie z napájacieho výstupu ústredne Inception (**VOUT +** → **+DC**, **VOUT 0V** → **−DC**), dátové spojenie ide z portu USB ústredne káblom Inner Range **993030USB**: **čierny** → **0V / −DC**, **zelený** → **CLK**, **biely** → **DATA**.

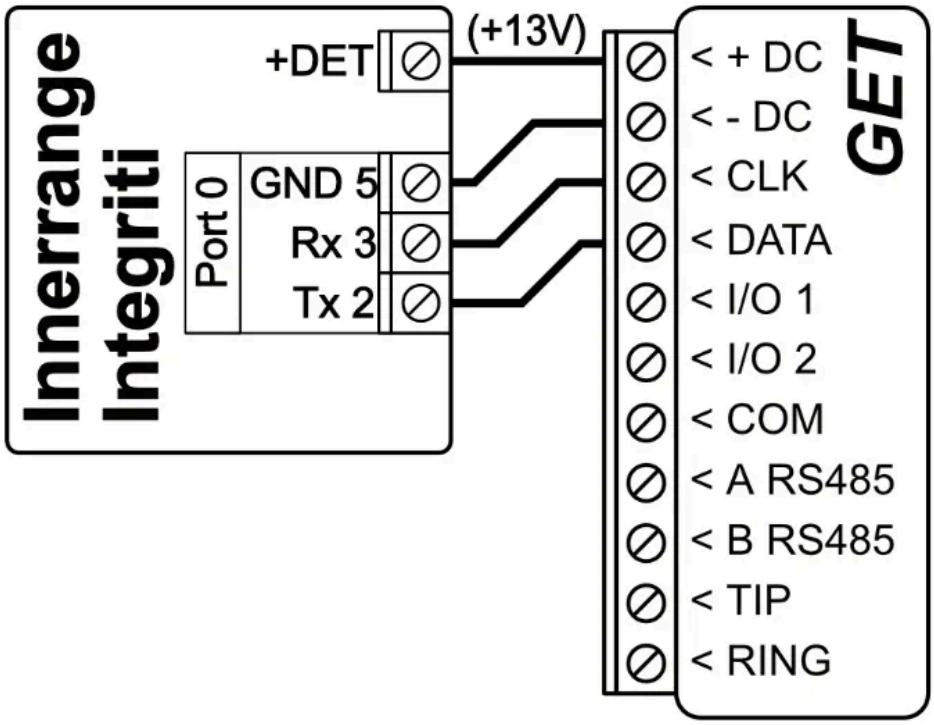


Obrázok 22. Pripojenie InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; z portu USB káblom 993030USB („Cable, Inner Range part number 993030USB“) čierny → −DC, zelený → CLK, biely → DATA.

- čierny vodič („Black wire“)
- zelený vodič („Green wire“)
- biely vodič („White wire“)

3.3.7 InnerRange Integriti

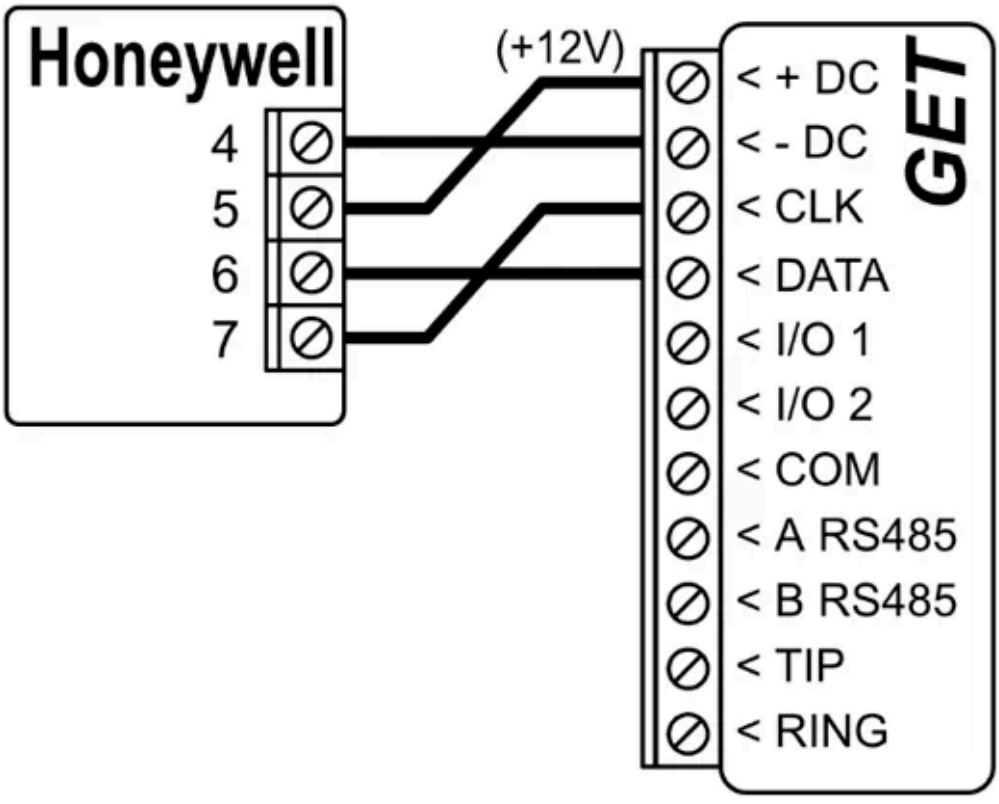
Na sériový port **Port 0** ústredne Integriti sa komunikátor pripája káblom Inner Range **INTG-996795**: **+DET (+13 V) → +DC**, **GND (5) → −DC**, **Rx (3) → CLK**, **Tx (2) → DATA**.



Obrázok 23. Pripojenie InnerRange Integriti na Port 0 káblom INTG-996795 („Cable, Inner Range part number INTG-996795"): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – dátová zbernica

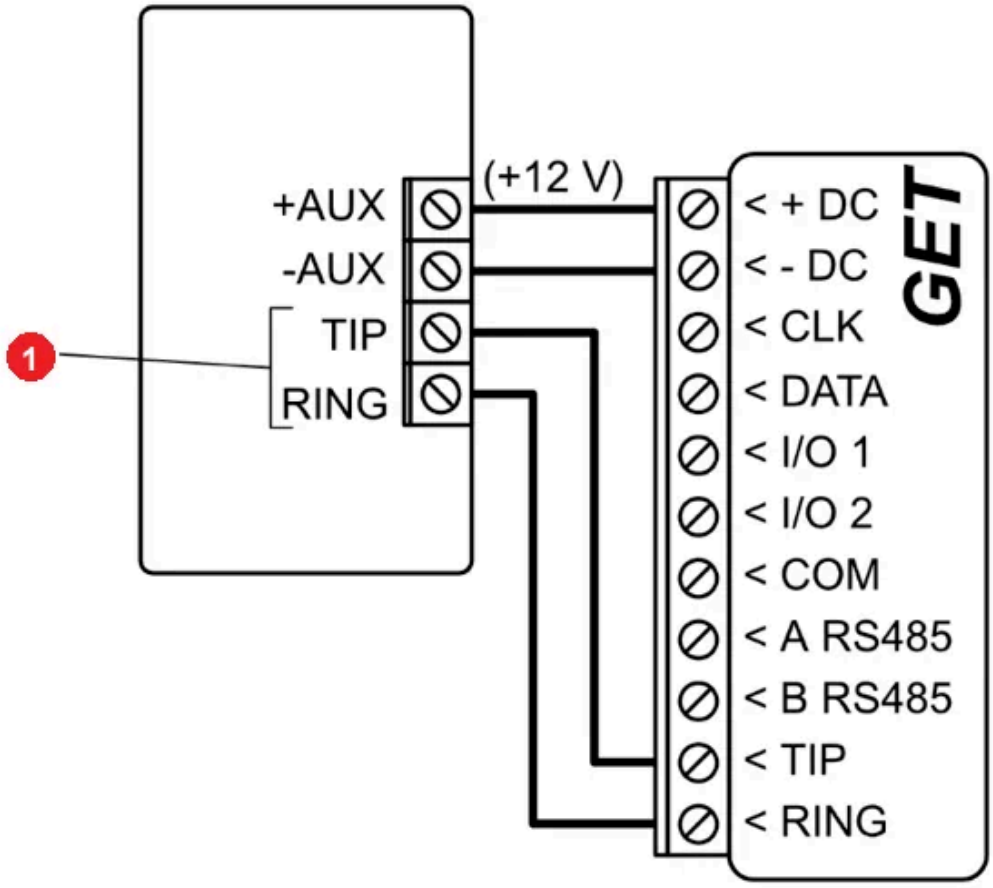
Zbernicu klávesníc ústredne Honeywell Ademco Vista-15, Vista-20 a Vista-48 pripoj zo svoriek ústredne ku komunikátoru: **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.



Obrázok 24. Pripojenie ústredne Honeywell Vista-15 / -20 / -48 na dátovú zbernicu („Keypad bus"): svorka 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Ľubovoľná ústredňa – TIP/RING

Ľubovoľnú inú ústredňu môžeš pripojiť cez jej telefónny komunikátor: napájanie z pomocného napájacieho výstupu ústredne (**+AUX** → **+DC**, **–AUX** → **–DC**), telefónny výstup na svorky **TIP** a **RING** komunikátora (**TIP** → **TIP**, **RING** → **RING**). Vytáčač ústredne treba nastaviť (bod 4.2).



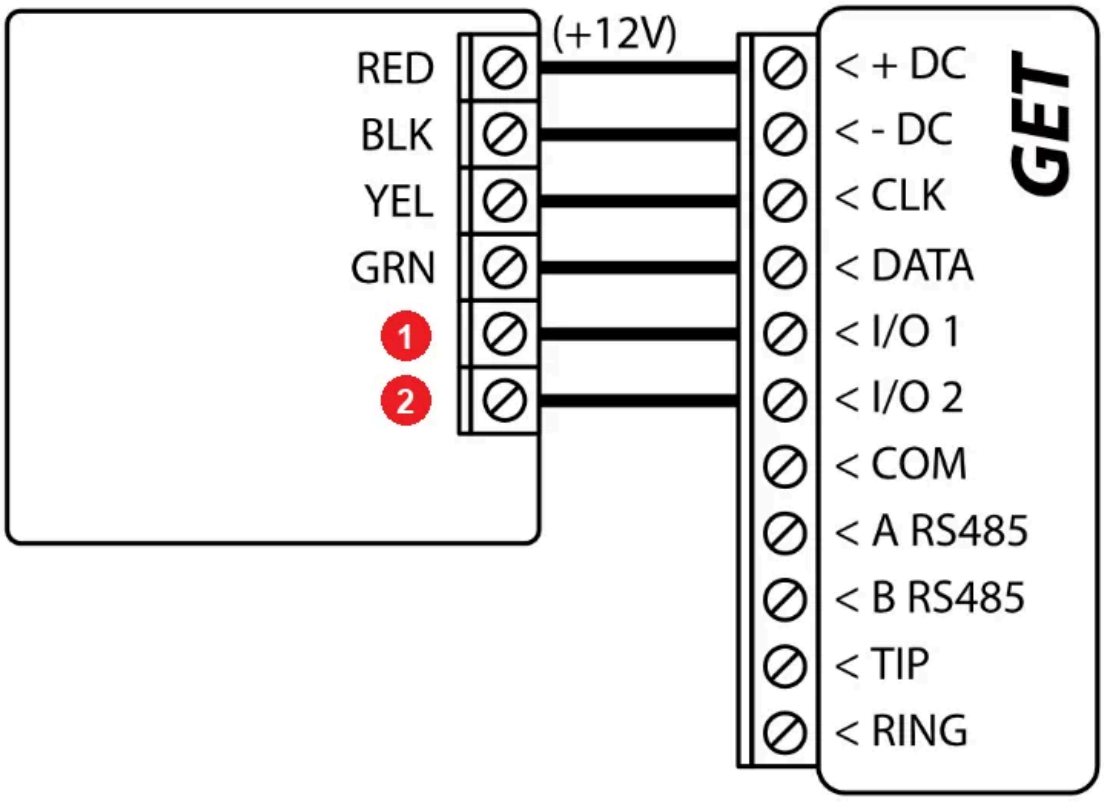
Obrázok 25. Pripojenie na telefónny komunikátor ústredne („Control panel"): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 svorky telefónneho komunikátora ústredne („Telephone line communicator terminals")

3.4 Zapojenie zóny kľúčového spínača

Ak chceš ústredňu zapínať a vypínať z aplikácie Protegus 2 tak, že výstup komunikátora (PGM) spína **zónu kľúčového spínača** ústredne, postupuj podľa tohto zapojenia. Dve svorky I/O komunikátora s dvojitou funkciou pracujú ako výstupy (OUT, PGM) – na GET sú z výroby obe výstupy –, takže dva výstupy môžu ovládať dve partície systému: zónu kľúčového spínača 1. partície pripoj na svorku **1 I/O**, 2. partície na svorku **2 I/O**. Pri takomto zapojení zruš na stránke **Panel settings** v TrikdisConfig zaškrtnutie **Remote Arm/Disarm**, svorky majú byť na stránke **IN/OUT** vo funkcii **OUT** (bod 6.7) a v aplikácii Protegus 2 priraď výstupy k partíciám podľa bodu 5.2.

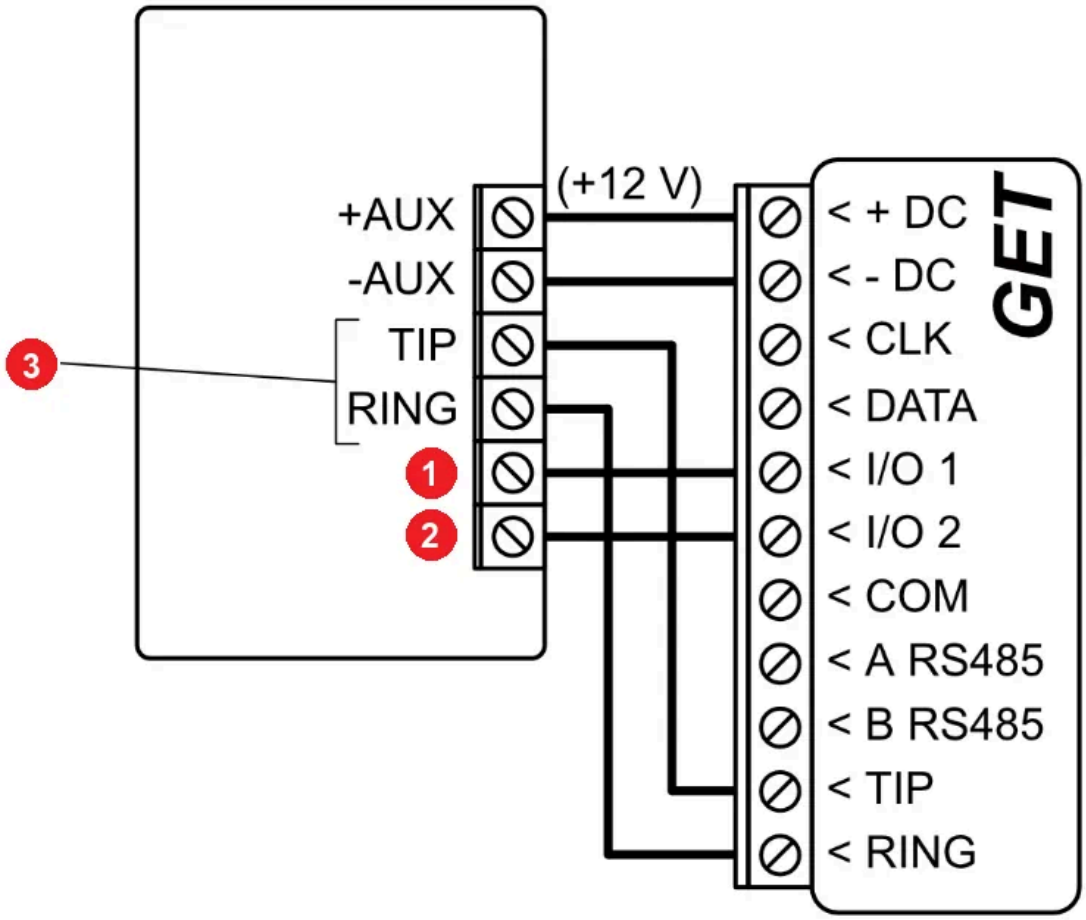
Pri pripojení na dátovú zbernicu alebo sériový port zostáva dátové spojenie medzi ústredňou a komunikátorom (komunikátor číta udalosti zo zbernice), zapínanie a vypínanie stráženia ide cez zónu kľúčového spínača:



Obrázok 26. Zapínanie a vypínanie stráženia zónou kľúčového spínača („Zone (keyswitch)“), pri pripojení na dátovú zbernicu alebo sériový port („Keypad bus or Serial port“): svorka RED zabezpečovacej ústredne („Control panel“) → +DC, BLK → −DC, YEL → CLK, GRN → DATA; zóna 1. partície → 1 I/O, zóna 2. partície → 2 I/O.

- 1 zóna kľúčového spínača 1. partície („1-st Area“)
- 2 zóna kľúčového spínača 2. partície („2-nd Area“)

Pri pripojení na telefónnu linku (TIP/RING) posiela ústredňa udalosti svojím vytáčačom, zapínanie a vypínanie stráženia ide rovnako cez zónu kľúčového spínača:



Obrázok 27. Zapínanie a vypínanie stráženia zónou kľúčového spínača („Zone (keyswitch)“), pri pripojení na telefónnu linku: svorka +AUX zabezpečovacej ústredne („Control panel“) → +DC, −AUX → −DC, TIP → TIP, RING → RING; zóna 1. partície → 1 I/O, zóna 2. partície → 2 I/O.

- 1 zóna kľúčového spínača 1. partície („1-st Area“)
- 2 zóna kľúčového spínača 2. partície („2-nd Area“)
- 3 svorky telefónneho komunikátora ústredne („Telephone line communicator terminals“)

Zóna kľúčového spínača môže byť impulzná alebo dvojpolohová – v aplikácii Protegus 2 treba nastaviť ten istý režim (bod 5.2). O podrobnostiach a úskaliach zapínania stráženia kľúčovým spínačom hovorí samostatný článok: Diaľkové zapínanie stráženia kľúčovým spínačom z aplikácie Protegus 2.

3.5 Zapojenie vstupov

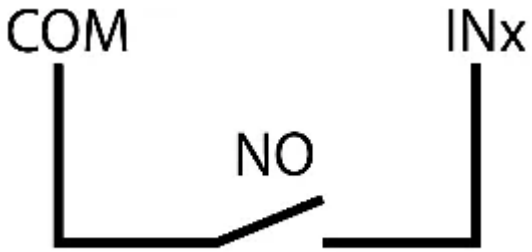
Dve svorky I/O komunikátora s dvojitou funkciou môžeš ako vstupy (IN) použiť aj na pripojenie ďalších snímačov (napr. sabotážneho kontaktu, panikového tlačidla), nezávisle od zabezpečovacej ústredne. Na vstup môžeš pripojiť obvod NO, NC, NO/EOL, NC/EOL, NO/DEOL alebo NC/DEOL. Na GET sú svorky z výroby výstupy: použitú svorku nastav na stránke **IN/OUT** v TrikdisConfig na funkciu **IN** a v poli **Type** zadaj typ pripojeného obvodu; v aplikácii Protegus 2 je to isté na karte **Advanced settings** → **IN/OUT**, v poli **Type** 1. alebo 2. svorky (bod 6.7). Vstup treba zapojiť medzi zvolenú svorku I/O a svorku **COM**, podľa zvoleného typu.

Vstupy prijímajú tieto typy obvodov: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Zakončovací odpor je **2,2 kΩ**. Pri jednoduchom zakončení (EOL) sa skrat aj prerušenie považujú za poplach; dvojité zakončenie (DEOL) s dvoma odpormi rozlišuje poplach a sabotáž (skrat alebo prerušenie) zvlášť. Výrobné nastavenie je NO (v kľudovom stave rozopnutý); typ vstupu nastavíš na stránke **IN/OUT** v TrikdisConfig podľa zapojenia.

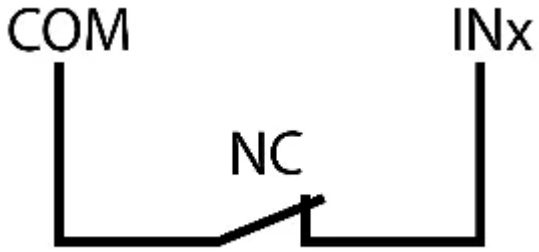
Typ	Kľudový stav	Poplach	Sabotáž
NC	zopnutý	rozopnutý	–
NO	rozopnutý	zopnutý	–
NC/EOL	2,2 kΩ	prerušenie alebo skrat	–
NO/EOL	2,2 kΩ	skrat alebo prerušenie	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	prerušenie alebo skrat
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	prerušenie alebo skrat

Pri narušení vstupu pošle komunikátor vlastnú udalosť na PCO a do Protegus 2; kód Contact ID, číslo partície a zóny tejto udalosti môžeš zadať na stránke **IN/OUT**.

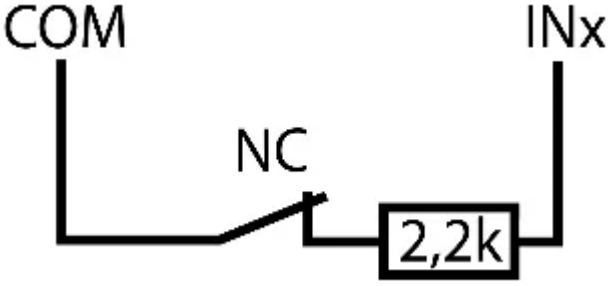
Zapojenie vstupných obvodov medzi bod COM a INx: NO, NC, NC/EOL, NO/EOL, a s rozpoznaním sabotáže NO/DEOL a NC/DEOL, so zakončovacími odpormi 2,2 kΩ; jednotlivé stavy (skrat, prerušenie, 2,2 kΩ, 3,3–5,5 kΩ) vysvetľuje tabuľka v bode 3.5.



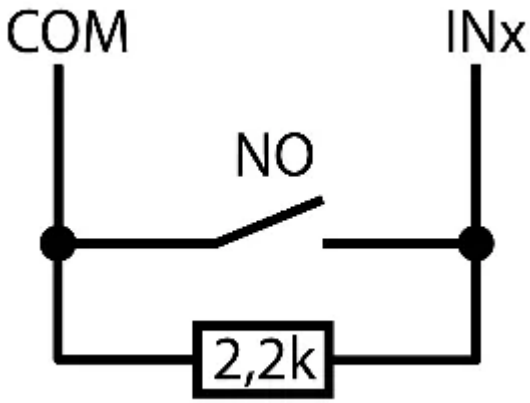
Obrázok 28. NO – v pokoji rozpojený obvod: zopnutý – poplach, rozpojený – pokojový stav.



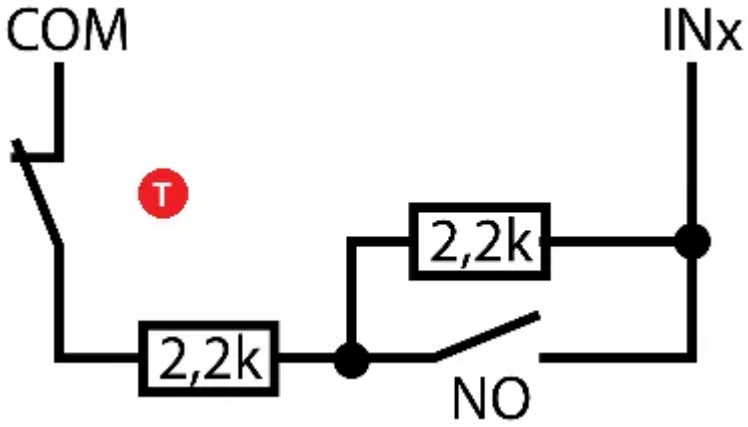
Obrázok 29. NC – v pokoji zopnutý obvod: rozpojený – poplach, zopnutý – pokojový stav.



Obrázok 30. NC/EOL – v pokoji zopnutý obvod so zakončovacím odporom 2,2 kΩ: skrat alebo prerušenie – poplach, 2,2 kΩ – pokojový stav.

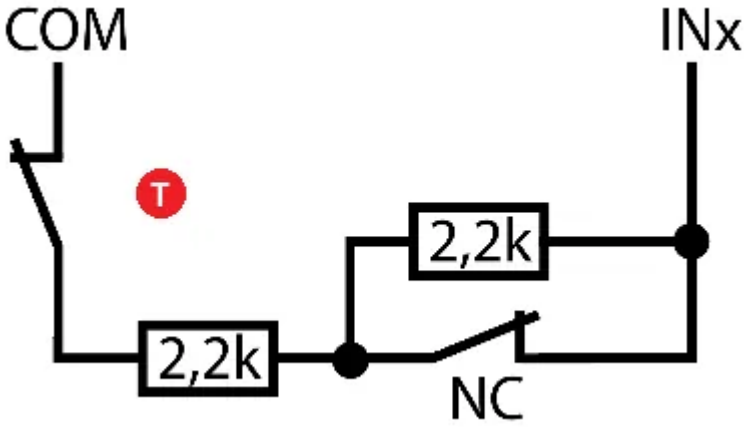


Obrázok 31. NO/EOL – v pokoji rozpojený obvod so zakončovacím odporom 2,2 kΩ: skrat alebo prerušenie – poplach, 2,2 kΩ – pokojový stav.



Obrázok 32. NO/DEOL – v pokoji rozpojený obvod so zakončovacím odporom 2,2 kΩ a rozpoznaním sabotáže: skrat alebo prerušenie – sabotáž, 2,2 kΩ – poplach, 3,3–5,5 kΩ – pokojový stav.

- T sabotážny kontakt („Tamper“), signalizuje otvorenie krytu snímača

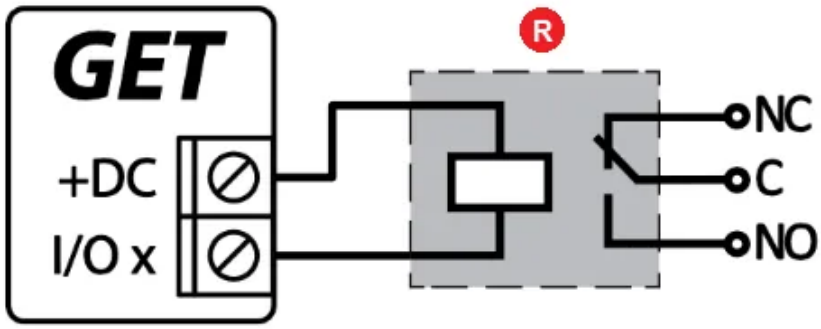


Obrázok 33. NC/DEOL – v pokoji zopnutý obvod so zakončovacím odporom 2,2 kΩ a rozpoznaním sabotáže: skrat alebo prerušenie – sabotáž, 2,2 kΩ – pokojový stav, 3,3–5,5 kΩ – poplach.

- T sabotážny kontakt („Tamper“), signalizuje otvorenie krytu snímača

3.6 Zapojenie výstupu s relé

Svorky I/O sú ako výstupy výstupy s otvoreným kolektorom (OC): v aktívnom stave pripájajú pripojenú záťaž na zápornú svorku, najviac 0,15 A, do 30 V DC. Kontaktmi relé môžeš zapínať a vypínať rôzne elektrické spotrebiče: jeden koniec cievky relé ide na **+DC**, druhý na svorku **x I/O**, spotrebič spínajú kontakty relé (NC, C, NO). Použitá svorka I/O má byť na stránke **IN/OUT** v TrikdisConfig (alebo na karte IN/OUT v aplikácii) výstup (**OUT**) – na GET je to výrobné nastavenie.



Obrázok 34. Pripojenie relé na výstup komunikátora: cievka ide medzi svorku +DC a x I/O, kontakty (NC, C, NO) spínajú spotrebič.

- R relé („Relay“)

Výstupy môžeš ovládať z aplikácie Protegus 2 (kapitola 5).

3.7 Zapnutie a prvá kontrola

A TRIKDIS átjelző elindítása

1. SIM kártyás átjelző esetén a SIM kártyát az elindítás előtt helyezd be a készülékbe.
2. Ethernetes eszköz esetén az Ethernet kábelt elindítás előtt vagy utána is csatlakoztathatod
3. Az indításhoz húzd ki az USB kábelt és csatlakoztasd a lehúzott sorkapcsot

Akkor léphetsz tovább a következő fejezetre, ha az eszköz megfelelően elindul és nem jelez hibát.

- A Power LED zölden világít
- A Trouble LED nem villog pirosan
- A Network LED zölden világít (ha közben sárgán villog az rendben van)
- Ha Data LED nem alszik ki, az azt jelenti, hogy az eszköz nem tud elküldeni valamilyen eseményt. Ez internet / adat kapcsolat hibára utal.

Po zapojení sa zapnutím napájania zabezpečovacej ústredne spustí aj komunikátor. Na prednom kryte máš vidieť:

- **POWER** svieti na zeleno – napájanie je v poriadku;
- **NETWORK LTE** svieti na zeleno a bliká na žlto – pripojil sa k mobilnej sieti; počet žltých bliknutí je úroveň signálu: na 4G sú 3 bliknutia vyhovujúce; ak napočítaš menej, signál je slabý: nájdi pre komunikátor alebo anténu iné miesto, alebo použi citlivejšiu anténu (bod 3.2);
- **NETWORK LAN** svieti na zeleno, ak si zasunul aj sieťový kábel – pripojil sa ku káblovej sieti;
- **TROUBLE** nesvieti.

Ak TROUBLE bliká, počet bliknutí udáva príčinu (bod 1.6); aj každá iná odlišná signalizácia LED znamená nejakú chybu, jej príčinu hľadaj podľa tabuliek v bode 1.6. Ak nesvieti žiadna LED, skontroluj napájanie a zapojenie.

4. Programovanie zabezpečovacej ústredne

Nastavenie ústredne závisí od toho, ako si ju pripojil: cez dátovú zbernicu alebo sériový port (bod 4.1), alebo cez jej telefónny komunikátor, na svorky TIP/RING (bod 4.2). Pri zapojení Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING uvádza nastavenie buniek ústredne tabuľka v bode 3.3.3.

4.1 Pripojenie na dátovú zbernicu alebo sériový port

Tu opisujeme, ako treba nastaviť ústredňu, aby komunikátor čítal jej udalosti a mohol ju ovládať na diaľku. Na diaľkové ovládanie má byť na stránke **Panel settings** v TrikdisConfig (v aplikácii: **Panel settings** → **Serial Bus**) zaškrtnutá voľba **Remote Arm/Disarm** (body 2.2 a 6.3).

4.1.1 DSC

Ústredne **DSC PowerSeries** (zoznam podporovaných typov je v bode 1.2) nevyžadujú žiadne osobitné nastavenie: komunikátor pripojený na Keybus číta udalosti okamžite a po zaškrtnutí **Remote Arm/Disarm** používateľ zakóduje a odkóduje systém z aplikácie svojím vlastným kódom klávesnice. O podrobnostiach priameho ovládania – stavy zón, premostenie zón, automatické rozpoznanie partícií – je samostatný článok: Priame ovládanie zabezpečovacích ústrední DSC PowerSeries.

S ústredňami **DSC PowerSeries NEO** komunikátor nefunguje: k zbernici NEO výrobca nepovoľuje externé zariadenie. Pre NEO je vhodný komunikátor na telefónnu linku (TIP/RING) – pozri DSC Power Series NEO a komunikátory Trikdis: kompatibilita a riešenia.

4.1.2 Paradox

Ústredne **Paradox** treba programovať iba na priame ovládanie; na čítanie udalostí netreba nič nastavovať. Firmvér ústredne musí byť minimálne **V.4**.

Na novších ústredniach Paradox (napríklad série SP+, MG+ a EVOHD+) môže byť sériový port **z výroby zamknutý**: komunikátor nedostáva dáta, kým port neodomkneš. Postup odomknutia: Odomknutie zamknutého sériového portu na zabezpečovacích ústredniach Paradox.

Na ovládanie treba nastaviť **PC heslo** ústredne (PC password) a to isté treba zadať aj do poľa **System settings** → **Security panel PC download password** v TrikdisConfig – obe sa musia zhodovať.

1. Na klávesnici vstúp do inštalátorského programovania ústredne.
2. Otvor sekciu PC hesla: pri sériách **MAGELLAN a SPECTRA** sekciu **911**, pri sérii **DIGIPLEX EVO** sekciu **3012**.
3. Zadaj **4-znakové** heslo. Heslo nemôže byť 0000 a **nesmie začínať nulou**.
4. Ukonči programovanie a **reštartuj ústredňu** – zmena PC hesla začne platiť po reštarte. Potom zadaj to isté heslo do TrikdisConfig.

Typické chyby a ich riešenie

- **Kód klávesnice priradený partícii nemôže byť master kód**: daj používateľovi iný kód a s ním bude zakódovanie / odkódovanie z Protegus 2 fungovať.
- **Po akejkoľvek zmene kódu klávesnice reštartuj komunikátor** (odpojením napájania alebo SMS príkazom `RESET`): kódy načíta pri štarte, neskoršiu zmenu nevidí.

Na komunikátore GET je pole **Security panel PC download password** na stránke **Panel settings** v TrikdisConfig, v skupine **Serial bus**; v aplikácii Protegus 2 **Panel settings → Serial Bus → PC download password** (body 2.2 a 6.3).

Zapojenie Keybus a TIP/RING (SP / SP+ / MG / MG+, bod 3.3.3): ústredňu treba okrem toho naprogramovať tak, aby posielala udalosti na PCO a dala sa ovládať z Protegus 2 – hodnoty buniek (801, 811, 812, 815, 911) uvádza tabuľka v bode 3.3.3.

4.1.3 Texecom

Ústredne **Texecom Premier / Premier Elite** treba naprogramovať na čítanie udalostí aj na ovládanie: treba nastaviť 4-znakové heslo ústredne s názvom **UDL passcode** a to isté zadať do poľa **System settings → Security panel PC download password** v TrikdisConfig – obe sa musia zhodovať.

Softvérom Texecom Wintex: UDL passcode nájdeš na karte **Options** okna **Communication Options**.

Z klávesnice:

1. Zadaj 4-miestny kód inštalátora a stlač tlačidlo **[Menu]** na vstup do programovacieho menu.
2. Hneď potom stlač tlačidlo **[9]**.
3. Stlač **[7][6]**, potom tlačidlo **[2]** a zadaj 4-miestny UDL passcode.
4. Stlač tlačidlo **[Yes]** a potom ukonči programovanie tlačidlom **[Menu]**.

Na komunikátore GET je pole **Security panel PC download password** na stránke **Panel settings** v TrikdisConfig, v skupine **Serial bus** (v aplikácii **Panel settings → Serial Bus → PC download password**); UDL passcode sa s ním musí zhodovať.

4.1.4 UTC Interlogix (Caddx)

Firmvér ústredne **UTC Interlogix (Caddx) NetworX** musí byť minimálne **V2**. Na klávesnici ústredne treba nastaviť:

1. Stlač tlačidlá **[*][8]** a zadaj kód inštalátora (z výroby **9713**).
2. Zadaj **číslo zariadenia** priradené komunikátoru (device address; z výroby **0**).
3. Riadky nasledujúcej tabuľky naprogramuj postupne: zadaj miesto (location), číslo segmentu a potom nastavenie. Tlačidlom **[*]** sa vrátiš do predchádzajúceho poľa. `12345678` znamená, že všetkých osem prepínačov segmentu je zapnutých (na displeji sú viditeľné všetky číslice).

Miesto (location)	Segment	Nastavenie
23	3	12345678
37 (nie je nevyhnutné)	3	12345678
37 (nie je nevyhnutné)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678

Miesto (location)	Segment	Nastavenie
108	3	12345678

4. Keď máš naprogramované všetky riadky, stlač dvakrát tlačidlo **[Exit]** na ukončenie programovania.

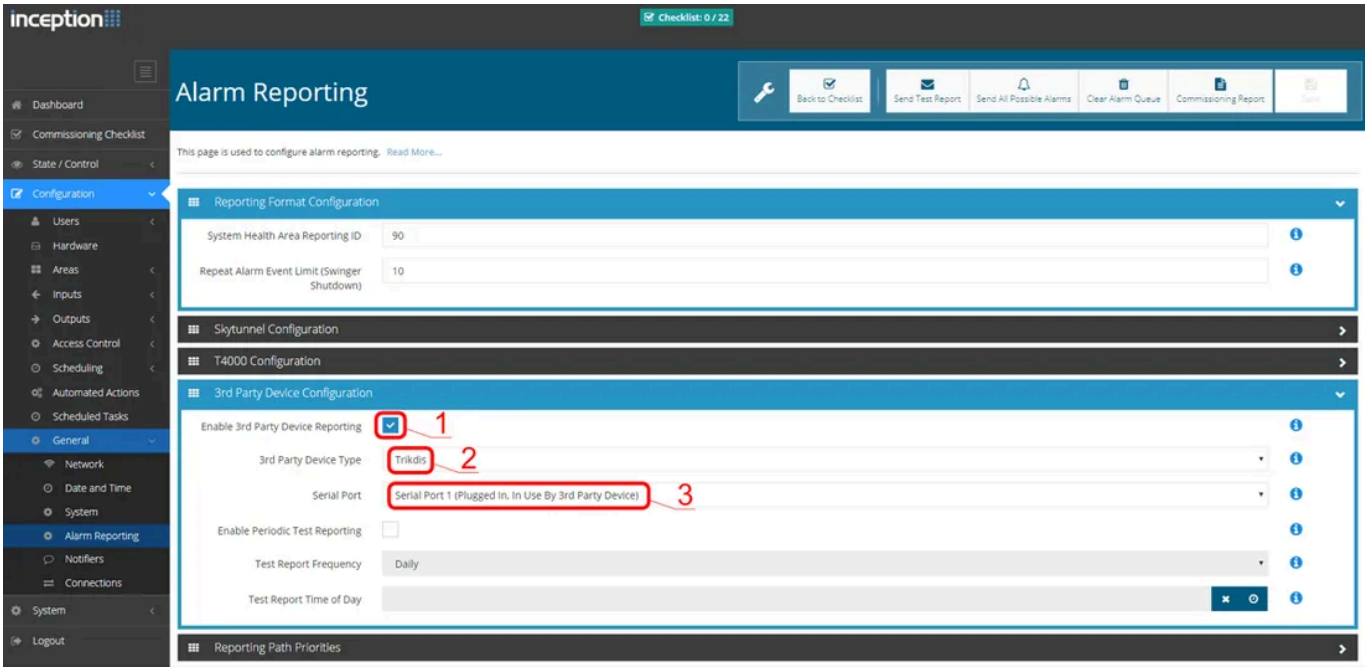
4.1.5 InnerRange

Firmvér ústredne **InnerRange Inception** musí byť minimálne **2.3.0.3507-r0** a ústredňa potrebuje internetové pripojenie. Nastavenie vykonáš vo webovom rozhraní ústredne:

1. Otvor v prehliadači adresu `https://skytunnel.com.au/inception/SERIOVE_CISLO`, kde SERIOVE_CISLO je sériové číslo na krabici ústredne. Prihlás sa účtom inštalátora.
2. Otvor stránku **Configuration → General → Alarm Reporting**.
3. V skupine **3rd Party Device Configuration**: - zaškrtni možnosť **Enable 3rd Party Device Reporting**; - v poli **3rd Party Device Type** vyber hodnotu **Trikdis**; - v poli **Serial Port** vyber hodnotu **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Ulož nastavenia a odhlás sa z rozhrania.

Firmvér ústredne **InnerRange Integriti** musí byť minimálne **19.1.0.36608** a jej programovací softvér (Integriti Professional) minimálne **19.1.0.15396**. Nastavenie vykonáš v programovacom softvéri ústredne:

1. Pri sériovom porte (**TTL Port-0**), ku ktorému je pripojený komunikátor, vyber komunikačný protokol **Trikdis**.
2. Formát dát musí byť **Contact ID**.
3. Nastavenie portu: **19200, 8, N, 1**.
4. Ulož nastavenia a ukonči program.



Obrázok 35. InnerRange Inception – Configuration → General → Alarm Reporting, skupina 3rd Party Device Configuration: Enable 3rd Party Device Reporting zaškrtnuté, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

Firmvér ústredne **Honeywell Ademco Vista-20** a **Vista-48** musí byť minimálne **V5.3**. Nastavenie vykonáš na klávesnici ústredne.

Vstup do programovania – dvoma spôsobmi:

- zadaj kód inštalátora (z výroby **4112**) a potom tlačidlá **[8][0][0]**; alebo
- pripoj ústredňu k napájaniu a **do 50 sekúnd** stlač naraz tlačidlá **[*]** a **[#]** (funguje to iba vtedy, ak sa z programovania predtým vystúpilo tlačidlami [*][9][8]).

Nastavenia:

1. Zapni odosielanie udalostí Contact ID na výstupe rádia s veľkým dosahom (LRR): stlač tlačidlá **[*][2][9][1][#]**.
2. Na vzdialené ovládanie povoľ používanie **2. adresy AUI** (2nd AUI address): stlač tlačidlá **[*][1][8][9][1][1][#]**.

Ukončenie programovania: stlač tlačidlá **[*][9][9]**.

4.2 Pripojenie na telefónnu linku (TIP/RING)

Aby zabezpečovacia ústredňa odosielala udalosti na svojom výstupe telefónnej linky, treba v ústredni zapnúť a nastaviť jej telefónny komunikátor (dialer). Presné programové adresy nájdeš v inštalačnom návode ústredne; podstata nastavenia je u všetkých výrobcov rovnaká:

1. **Zapni komunikátor telefónnej linky (PSTN)** v ústredni.
2. **Ako telefónne číslo zadaj** `1234` pri prijímači PCO – či už je komunikátor pripojený na svorky RING/TIP ústredne, alebo na telefónnu linku. S iným číslom sa môže stať, že ústredňa vytáča, ale komunikátor udalosti nedostane: aj pri jednej ústredni DSC PowerSeries NEO sa prenos spustil až po prepísaní čísla na `1234`.
3. **Režim vytáčania:** DTMF (tónový), nie pulzný.
4. **Protokol:** Contact ID.

Ak chceš ústredňu zakódovať a odkódovať na diaľku výstupom komunikátora, zónu pripojenú na výstup treba v ústredni nastaviť ako **zónu kľúčového spínača**.

Zóna kľúčového spínača môže byť pulzná alebo dvojpolohová. Výstup komunikátora dáva predvolene 3-sekundový impulz; dĺžku impulzu alebo dvojpolohový režim môžeš zmeniť v nastaveniach aplikácie Protegus 2.

Ústredne DSC, Paradox, Caddx, Texecom, InnerRange a Honeywell môžeš ku komunikátoru pripojiť aj cez ich telefónny výstup (bod 3.3.9) – vtedy treba aj pri nich nastaviť vytáčač a priame ovládanie nie je dostupné.

4.2.1 Programovanie vytáčača Honeywell Vista

Na klávesnici vstúp do programovacieho režimu a nastav tieto programové adresy:

Programová adresa	Nastavenie
`*41`	telefónne číslo prijímača PCO: `1234`
`*43`	identifikačné číslo objektu ústredne
`*47`	Tone dial = `1` a počet pokusov o vytáčanie
`*48`	`7` (predvolené)
`*49`	`5` (správa Split/Dual)

Programová adresa	Nastavenie
`*50`	oneskorenie odoslania poplachu narušenia – predvolene `2,0` (30 s); na okamžité odoslanie `0,0`

Pri ústredni **Honeywell Vista 48** nastav okrem toho tieto programové adresy:

Programová adresa	Hodnota	Programová adresa	Hodnota	Programová adresa	Hodnota
`*41`	1234 (telefónne číslo prijímača)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (identifikačné číslo objektu)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

Na konci programovania ukonči programovací režim príkazom `*99`.

4.2.2 Vytáčač UTC Interlogix (Caddx) NX

Programovanie ústredne Interlogix NX-4V2 (NX-6V2, NX-8V2), ak je komunikátor pripojený na svorky TIP/RING ústredne. Na klávesnici zadaj postupne:

Miesto (location)	Klávesy	Poznámka
	`*89713`	Vstup do programovania (`9713` je výrobný kód inštalátora)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Svietia všetky LED zón (1. segment)
Location 4	`12345678*`	Svietia všetky LED zón (2. segment)
Location 4	`12345678*#`	
Location 23	`23#`	Svietia všetky LED zón (3. segment)

Miesto (location)	Klávesy	Poznámka
Location 23	`**`	Svietia všetky LED zón (3. segment)
Location 23	`12345678*#`	Svietia všetky LED zón (3. segment)
Location 37	`37#`	Svietia všetky LED zón (3. segment)
Location 37	`**`	Svietia všetky LED zón (4. segment)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT EXIT`	Výstup z programovania

5. Diaľkové ovládanie aplikáciou Protegus 2

Mobilnou a webovou aplikáciou Protegus 2 používateľ na diaľku vidí stav systému, dostáva upozornenia na udalosti, zapína a vypína stráženie a ovláda výstupy komunikátora. Aplikáciu si stiahneš pre Android a iOS (Google Play, App Store), alebo ju môžeš používať v prehliadači: web.protegus.app. Prihlás sa svojím používateľským menom a heslom, alebo si zaregistruj nový účet. GET neupozorňuje cez SMS ani telefonickým hovorom a neprijíma ani príkazy SMS: diaľkové ovládanie a upozornenia idú cez aplikáciu; aj nastavenia komunikátora sú dostupné z aplikácie (**Settings** → **Advanced settings**, kapitola 6).

5.1 Pridanie zariadenia

Pred pridaním zariadenia skontroluj:

1. Karta SIM je aktívna a jej kód PIN je zadaný v zariadení, alebo je požiadavka na PIN vypnutá – **alebo** je komunikátor pripojený sieťovým káblom (LAN) do lokálnej siete.
2. Na karte **User reporting** → **PROTEGUS Cloud** v TrikdisConfig je zaškrtnuté **Enable connection** (bod 6.5).
3. LED **POWER** svieti na zeleno.
4. LED **NETWORK LTE** svieti na zeleno a bliká na žlto (zariadenie je v mobilnej sieti); pri len káblovom spojení svieti na zeleno LED **NETWORK LAN**.

LED DATA je najjednoduchšia kontrola internetu. LED DATA svieti, keď je v pamäti zariadenia správa čakajúca na odoslanie. Zelená LED NETWORK hovorí iba to, že sieťové spojenie je nadviazané – pri zariadení s mobilnou sieťou sa prihlásilo do siete operátora, pri ethernetovom zariadení funguje spojenie po router –, nie však to, že sa zariadenie dostane aj na internet. Ak LED NETWORK svieti nazeleno, ale LED DATA svieti nepretržite aj po udalosti alebo testovacej správe, internetové spojenie nefunguje: správa sa nedá odoslať. V mobilnej sieti je najčastejšie chybné APN alebo dátová služba SIM karty, pri Ethernete router, firewall alebo DNS. Keď LED DATA zhasne, správa odišla a dátové spojenie je v poriadku.

A rendszer létrehozása a Protegus 2 alkalmazásban

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

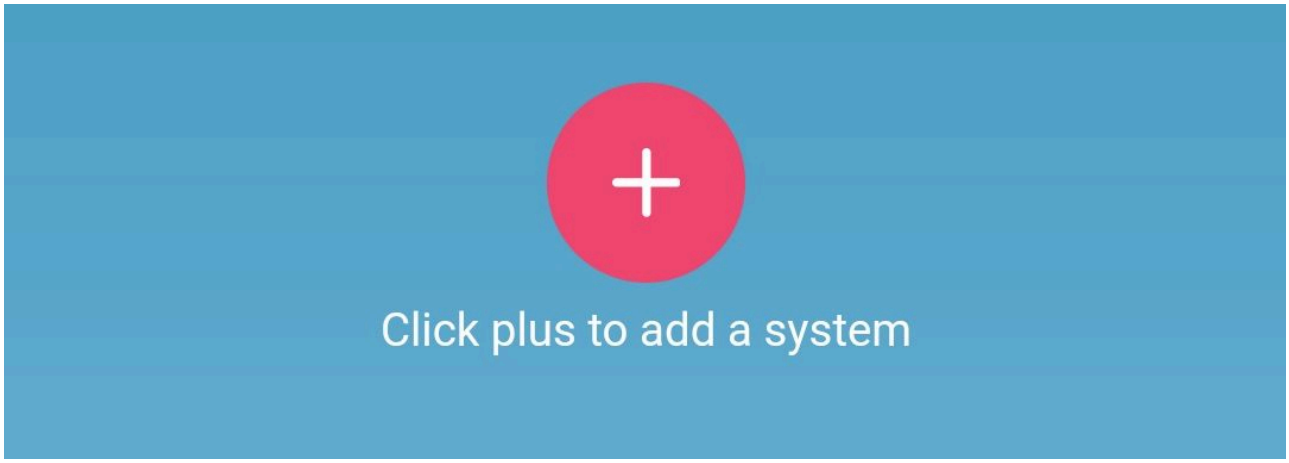








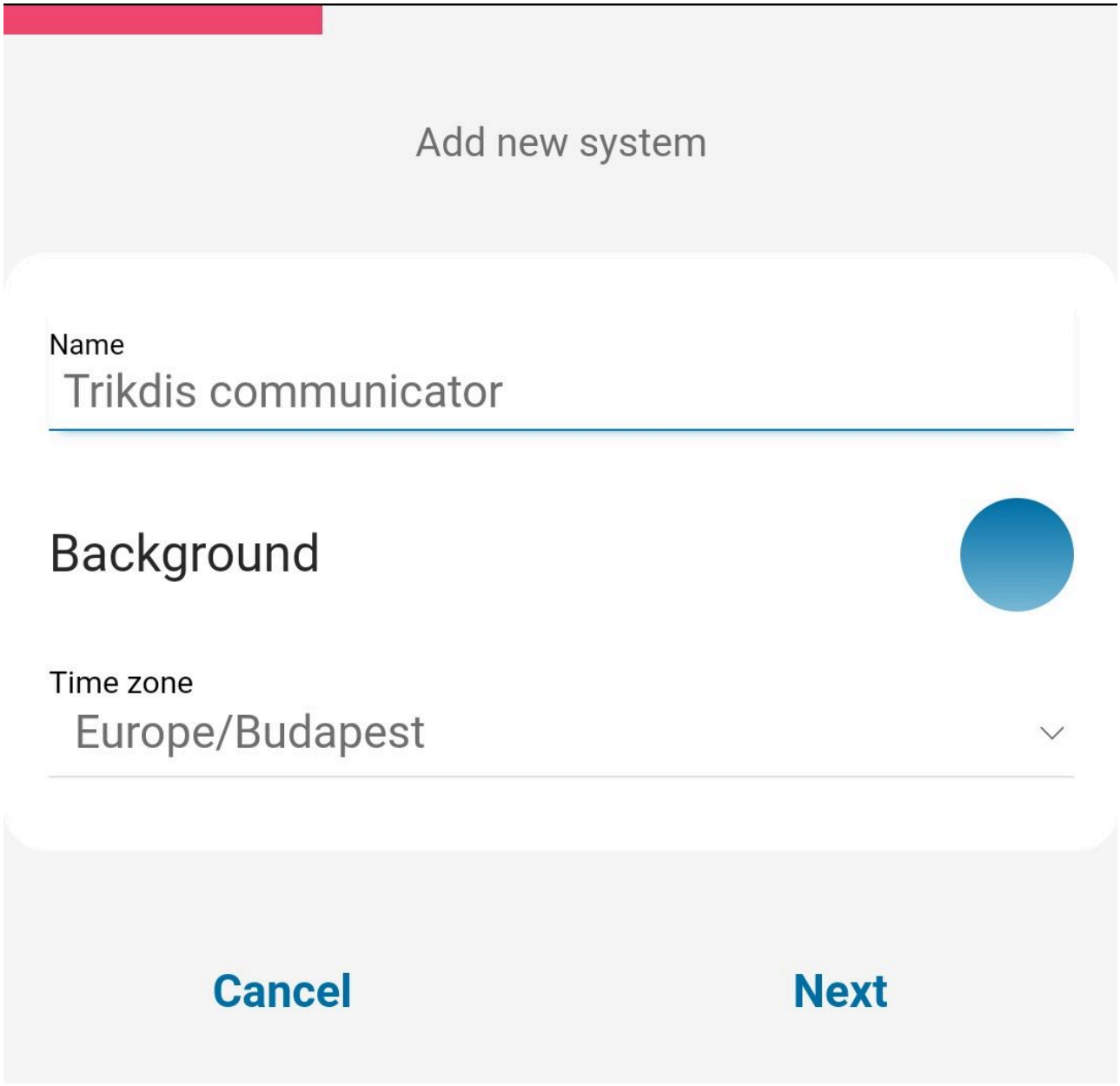
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



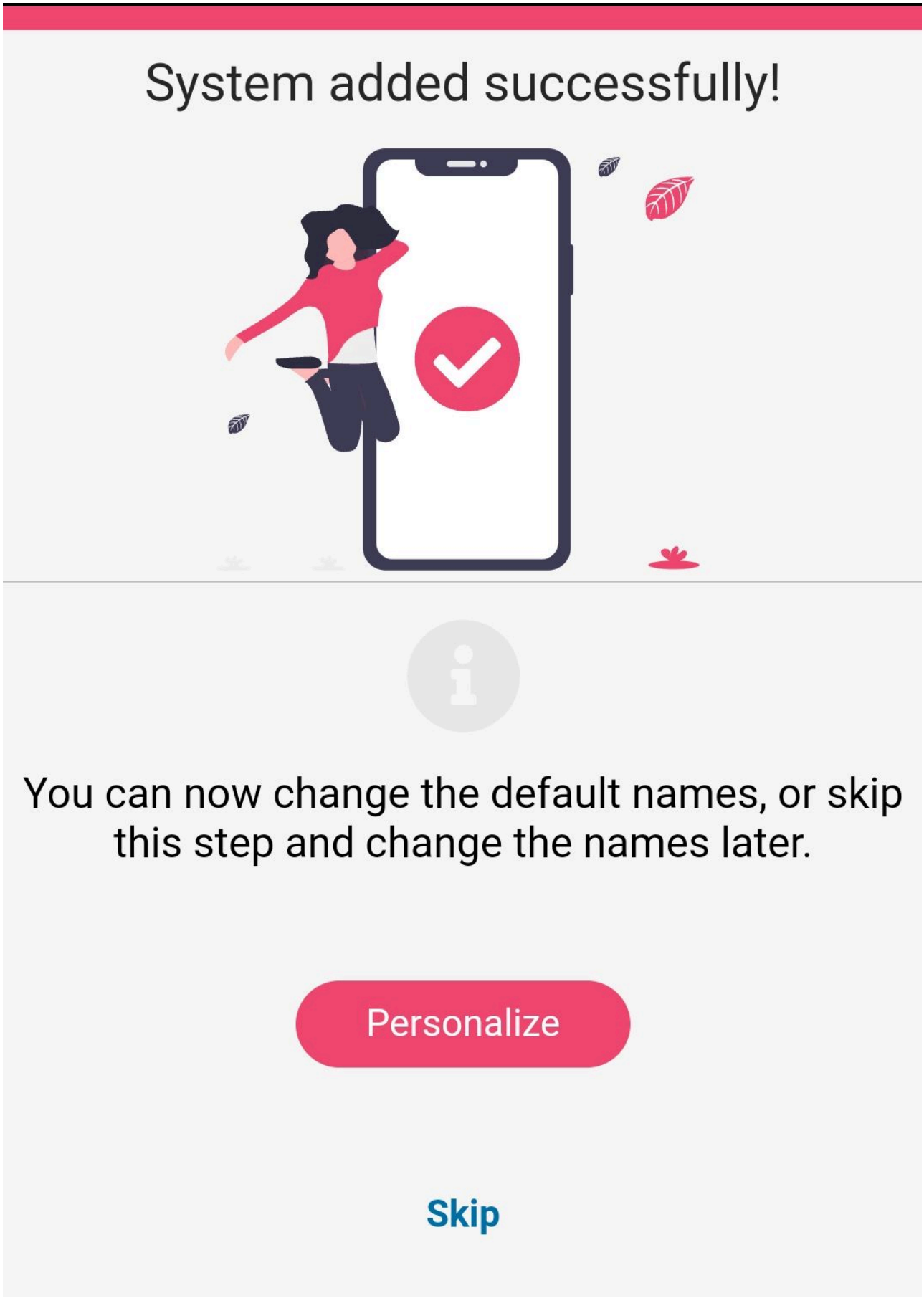
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



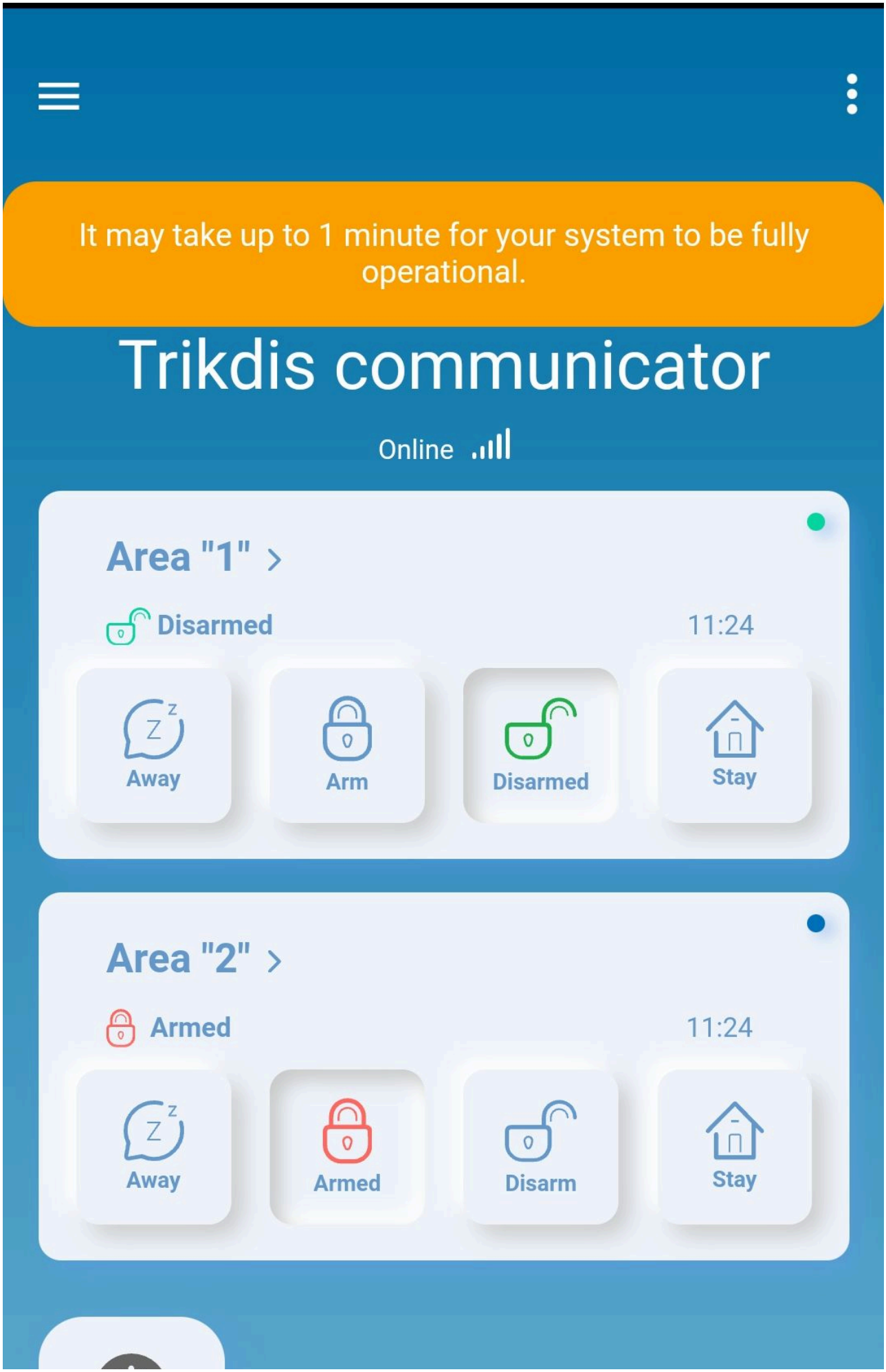
6. Add meg a rendszer nevét és válassz idozónát

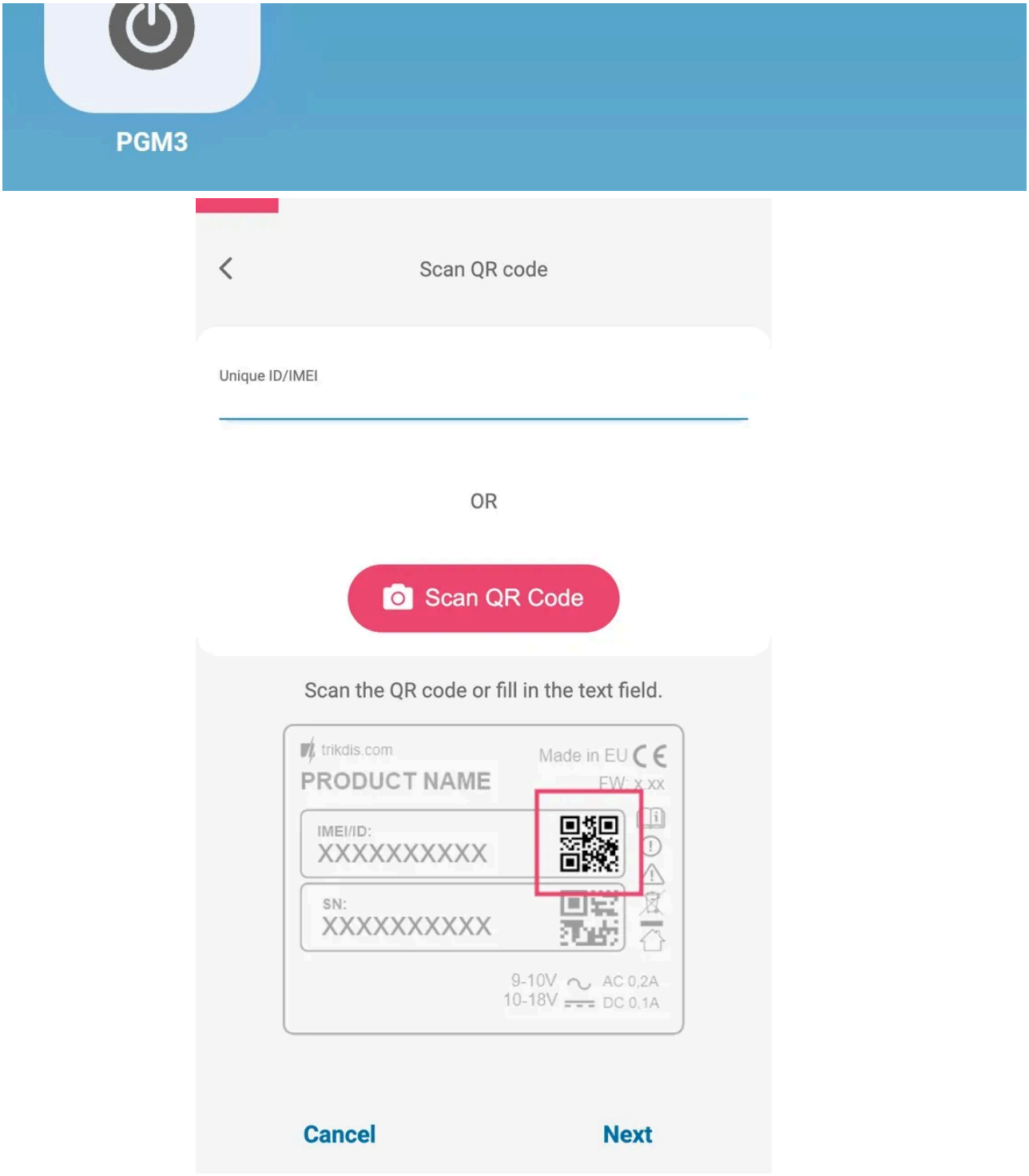


7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.

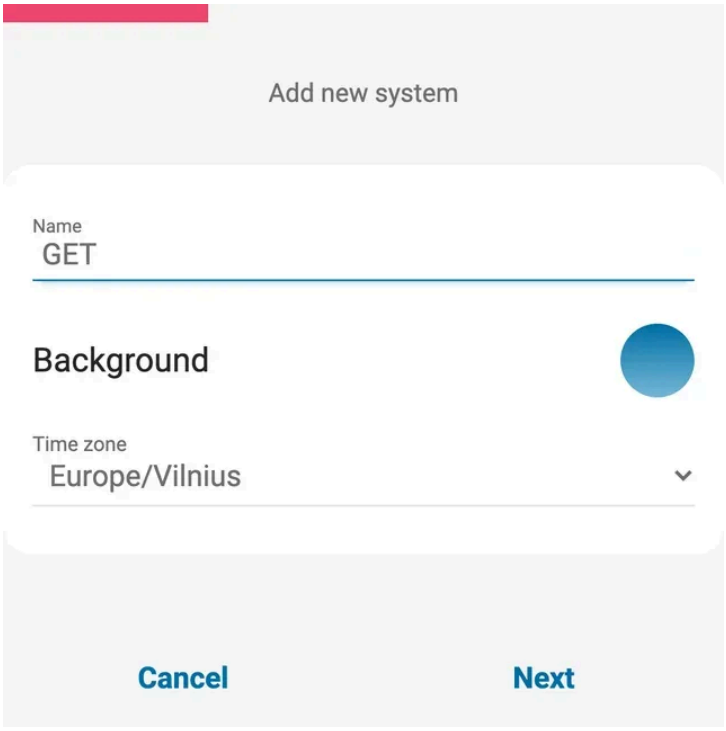


8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


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



Obrázok 36. Protegus 2 – pridanie nového systému: zadanie IMEI / Unique ID alebo načítanie kódu QR zo štítku, potom Next.



Obrázok 37. Protegus 2 – zadanie názvu systému (Name), potom Next.

Jedinečný identifikátor zariadenia (**IMEI / Unique ID**) je na štítku zariadenia a na nálepke krabice a ukazuje ho aj stavový riadok TrikdisConfig. Ak v zariadení **PROTEGUS Cloud access Code** nie je výrobný, aplikácia si ho pri pridávaní vypýta.

5.2 Zapínanie a vypínanie stráženia výstupom

Ak chceš zabezpečovaciu ústredňu zakódovať a odkódovať výstupom komunikátora cez zónu kľúčového spínača ústredne, v aplikácii Protegus 2 pri partícii zadaj, ktorý výstup ju ovláda.

Zóna ústredne, na ktorú je pripojený výstup komunikátora, musí byť v ústredni naprogramovaná ako **zóna kľúčového spínača** a ústredňa musí hlásiť udalosti zakódovania a odkódovania – z nich Protegus 2 zobrazuje stav partície.

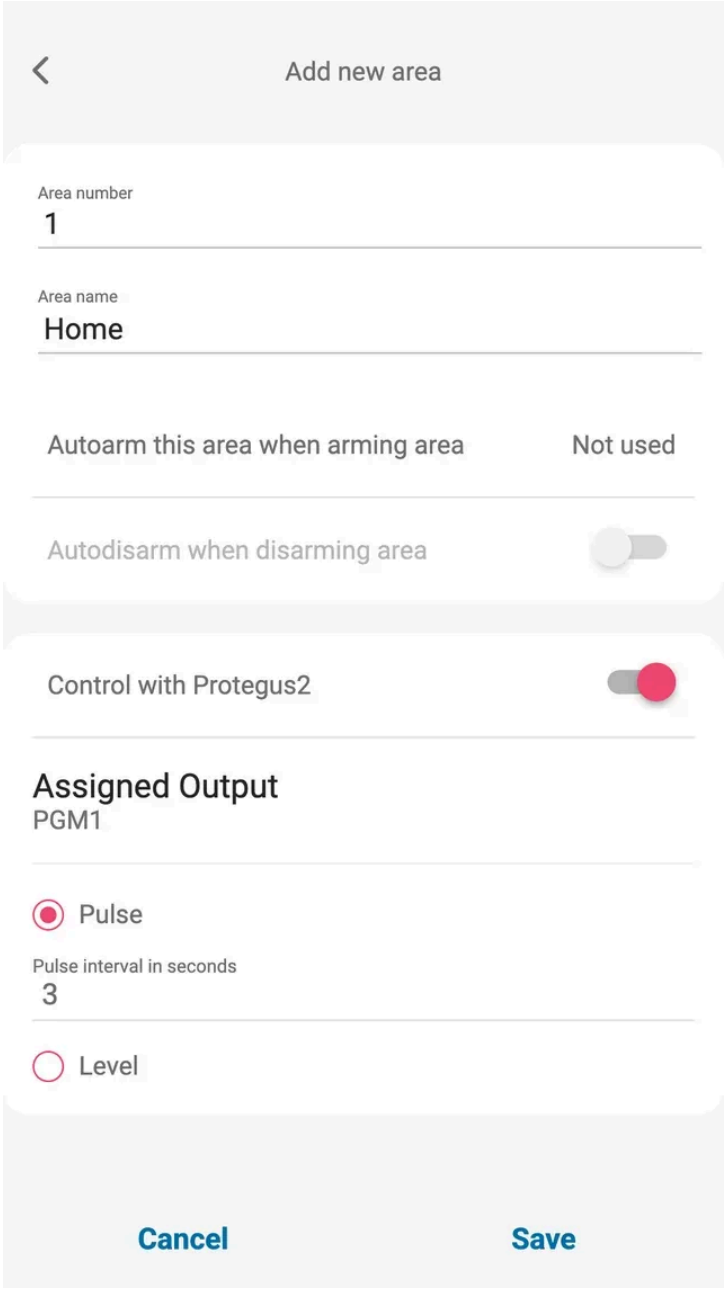
Nastavenie môžeš urobiť pri vytváraní systému, pri pridávaní partícií, alebo neskôr v nastaveniach systému pri úprave partície. Pri vytváraní systému ťa prevedie sprievodca Protegus 2: klikni na tlačidlo **Continue** (Pokračovať), zadaj názov partície (**Area name**) a povoľ ovládanie výstupu PGM z aplikácie Protegus 2 – robí sa to týmito krokmi:

1. Vyber (alebo pridaj) partíciu, ktorú chceš ovládať. Číslo partície sa musí zhodovať s tým, ktoré ústredňa posiela v udalostiach (partícia 1 je 1, partícia 2 je 2).
2. Zapni možnosť **ovládania cez PGM** (Control with Protegus2) a v poli **výstup** (Assigned Output) vyber výstup komunikátora (PGM1, PGM2 …). Jeden výstup môže ovládať iba jednu partíciu.
3. Vyber režim činnosti: **pulzný** (Pulse) alebo **dvojpolohový** (Level) – rovnaký, aký si v ústredni nastavil pri zóne kľúčového spínača. Zvyčajne používame pulzný; zadať sa dá aj dĺžka impulzu (predvolene 3 s).
4. Ulož nastavenie (**Save**). Pri viacerých partíciách to zopakuj pri každej, s jej vlastným výstupom: v sprievodcovi pridáš ďalšiu partíciu tlačidlom **Click to add an area** a jej výstup PGM nastavíš rovnako. Keď máš nastavené všetky partície, pokračuj v sprievodcovi tlačidlom **Skip**.

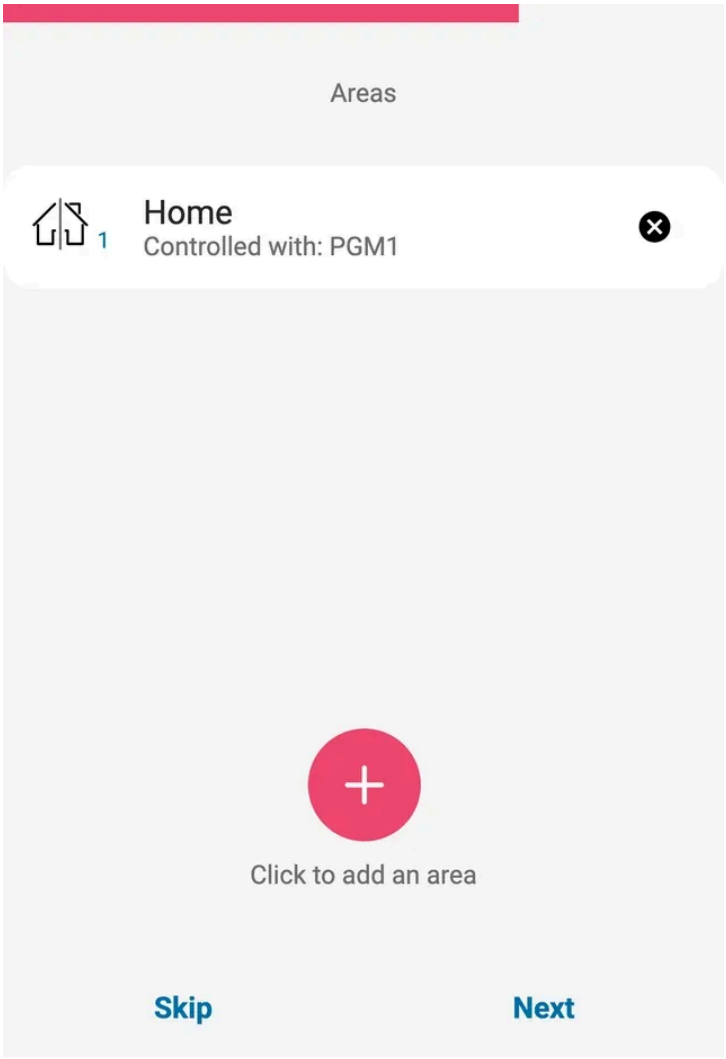
Protegus 2 dokáže správne zobraziť stav partícií iba vtedy, ak ústredňa posiela udalosti zakódovania a odkódovania so správnym číslom partície. O podrobnostiach a úskaliach zakódovania kľúčovým spínačom je samostatný článok: Vzdialené zakódovanie kľúčovým spínačom z aplikácie Protegus 2.



Obrázok 38. Protegus 2 – stránka „Systém neovládame na diaľku“ pri vytváraní systému: tlačidlom Continue prejdeš na nastavenie partície a výstupu PGM.



Obrázok 39. Protegus 2 – pridanie partície (Add new area): Area number, Area name, zapnuté Control with Protegus2, Assigned Output PGM1, Pulse (3 s) alebo Level, potom Save.

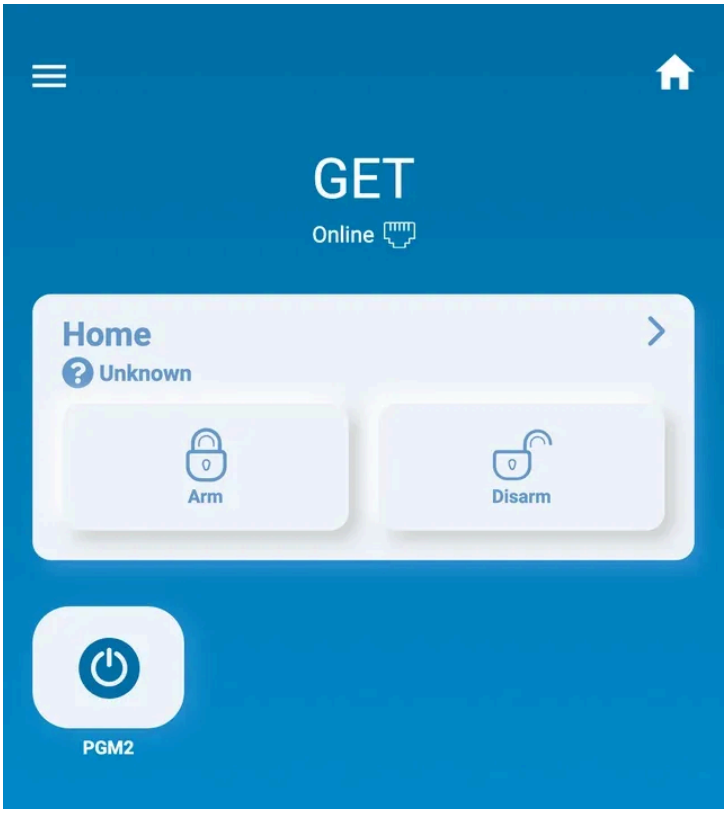


Obrázok 40. Protegus 2 – zoznam partícií (Areas): partíciu Home ovláda PGM1; ďalšiu partíciu pridáš tlačidlom Click to add an area, sprievodcu ukončíš tlačidlom Skip.

5.3 Zapínanie a vypínanie stráženia z aplikácie

1. Otvor systém v aplikácii Protegus 2. Na úvodnej obrazovke má každá partícia vlastnú kartu a zámok: **zatvorený červený zámok** znamená zakódovanú, **otvorený zelený zámok** odkódovanú partíciu.
2. Ťukni na zámok partície a vyber požadovanú akciu: zakódovanie alebo odkódovanie.
3. Ak to aplikácia vyžaduje, zadaj PIN kód.

Zámok prevezme skutočný stav na základe udalosti, ktorá príde zo zabezpečovacej ústredne; aplikácia v zozname udalostí aj v upozornení spätne ohlási, či ústredňa akciu vykonala.



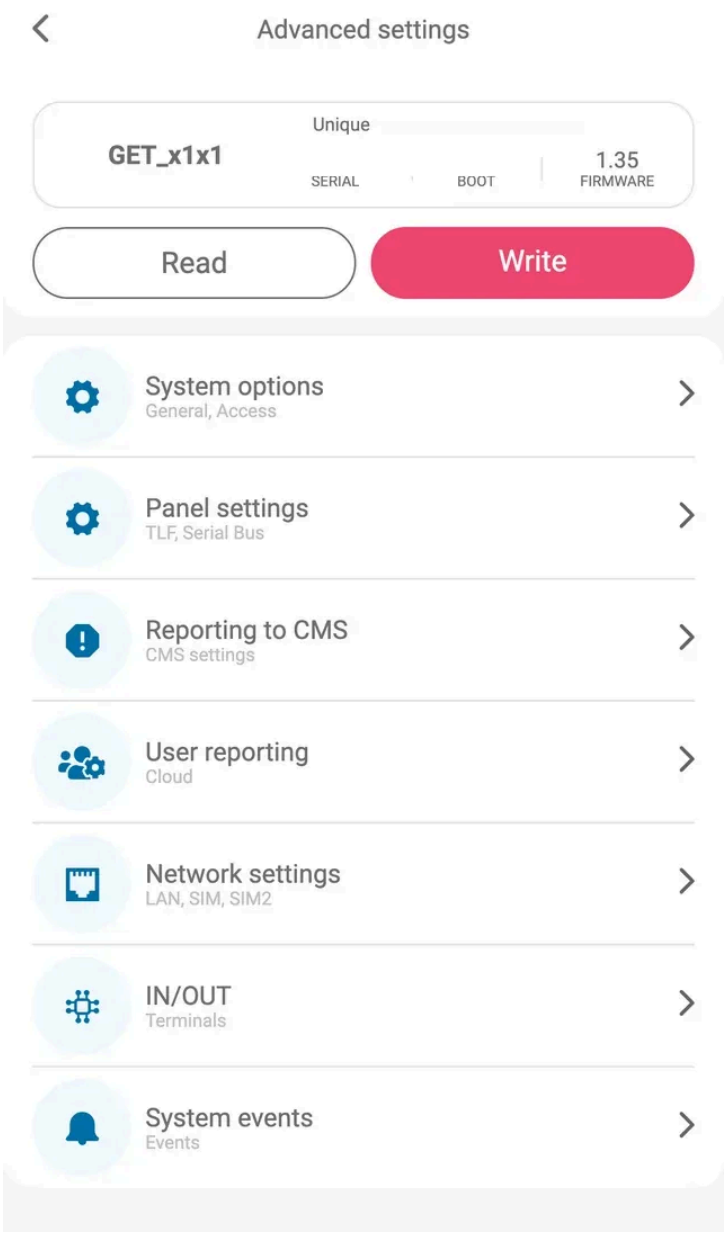
Obrázok 41. Protegus 2 – úvodná obrazovka systému: stav partície, tlačidlá Arm a Disarm, pod nimi ovládateľný výstup PGM.

6. Nastavenia podrobne

Väčšina nastavení GET je dostupná aj v programe **TrikdisConfig**, ktorý beží vo Windows, aj v aplikácii **Protegus 2** (**Settings → Advanced settings**, bod 2.2); kde je niečo len v jednom z nich, upozorníme na to. Každé nastavenie opisujeme raz a v každom bode uvádzame, kde ho nájdeš v oboch nástrojoch; v zátvorke je popis v aplikácii, ak sa líši od TrikdisConfig. V okne TrikdisConfig je vľavo zoznam stránok (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), hore rad tlačidiel (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), dole stavový riadok.

6.1 Pripojenie ku komunikátoru

Aplikácia Protegus 2. Otvor systém a prejdi do ponuky **Settings → Advanced settings**. Hore na každej obrazovke sú údaje pripojeného zariadenia: **Unique ID** (IMEI), **Serial** (výrobné číslo), verzia **Firmware** a **Boot**. Skupiny nastavení v ponuke: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** a **System events**. Po zmene zapíšeš nastavenia do zariadenia tlačidlom **Write**; **Read** znova načíta aktuálne hodnoty zo zariadenia.



Obrázok 42. Protegus 2 – ponuka Advanced settings: hore údaje zariadenia (typ, Unique ID, výrobné číslo, verzia bootu a firmvéru), tlačidlá Read a Write, pod nimi skupiny nastavení.

TrikdisConfig. Po pripojení komunikátora a stlačení **Read [F4]** program ukazuje údaje zariadenia v stavovom riadku.

Po pripojení a načítaní zariadenia (**Read [F4]**) sa v dolnej časti okna zobrazia najdôležitejšie údaje zariadenia:

Nápis	Význam
IMEI / Unique ID, pri ethernetovom zariadení **MAC / Unique ID**	Jedinečný identifikátor zariadenia: pri zariadení so SIM kartou IMEI, pri ethernetovom zariadení MAC adresa. To isté je uvedené na krabici a na zadnej strane zariadenia.
Status	Aktuálny prevádzkový stav.
Device	Typ zariadenia (typové označenie). Skontroluj, či je tu uvedený typ tvojho zariadenia.
SN	Sériové číslo.

Nápis	Význam
BL	Verzia bootloadera.
FW	Verzia firmvéru.
HW	Verzia hardvéru.
State	Spôsob pripojenia: USB alebo na diaľku (remote).
Administrator / Installer	Úroveň prístupu toho, kto programuje (po zadaní hesla).

Po vykonaní nastavení ich tlačidlom **Write [F5]** zapíšeš do zariadenia; tlačidlami **Open [F8]** a **Save [F9]** môžeš celú sadu nastavení uložiť do súboru a nahrať do iného zariadenia. **Save [F9]** uloží nastavenia do konfiguračného súboru, **Open [F8]** otvorí uložený súbor; uložené nastavenia môžeš neskôr nahrať aj do iných zariadení, takže viac zariadení nastavíš rýchlo s rovnakými nastaveniami.



Obrázok 43. Stavový riadok TrikdisConfig s načítaným GET: identifikátor, stav, typ (Device: GET_S170), výrobné číslo, verzia BL (bootloader), FW a HW, spôsob pripojenia a prístupová úroveň.

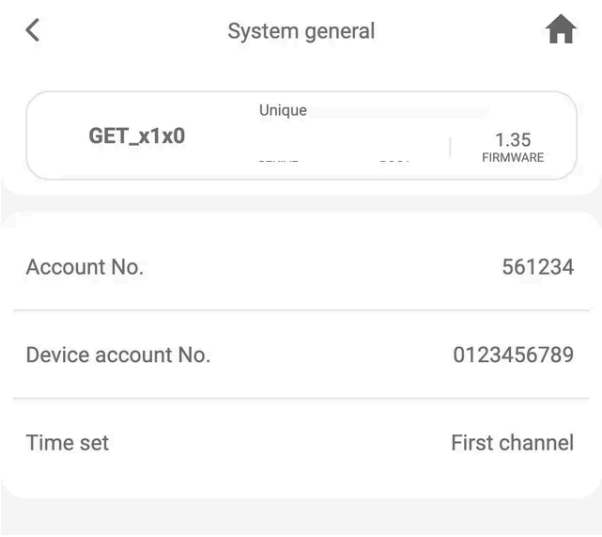
V poli **Device** má byť typové označenie GET (na obrázku GET_S170; prípona z písmena a čísla označuje hardvérovú verziu), **BL** je verzia bootloadera. Po **Read [F4]** program načíta a ukáže hodnoty nastavené v zariadení; potrebné nastavenia urob podľa opisov stránok nižšie.

6.2 System settings (System options)

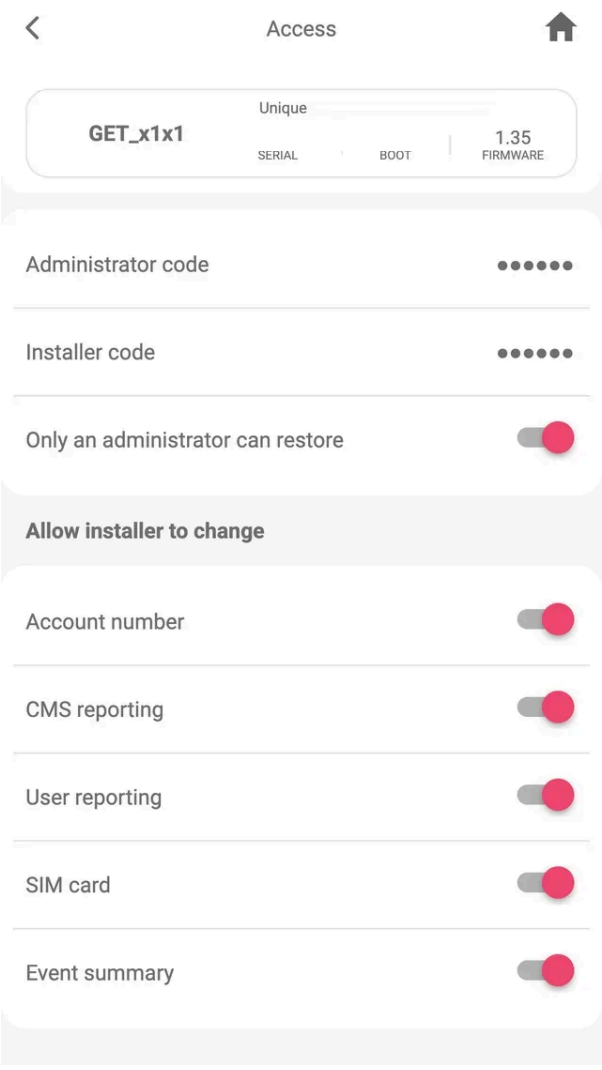
V aplikácii: Advanced settings → System options → System general (identifikátory, synchronizácia času) a **System options → Access** (kódy a práva inštalátora). Kde sú **Account No.** a **Device account No.**, závisí od hardvérovej verzie a firmvéru: na hardvéri **x1x1** s firmvérom **1.31** alebo novším ich nájdeš na karte **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.**; na paralelnom kanáli **Parallel Account no.**) a na karte **Reporting to CMS → Settings** (**Device account No.**), na karte System general zostane len **Time set**; inak sú obe na karte System general.



Obrázok 44. Protegus 2 – System options → System general na hardvéri x1x1 (firmvér 1.35): viditeľné je len Time set, identifikátory sú medzi nastaveniami CMS.

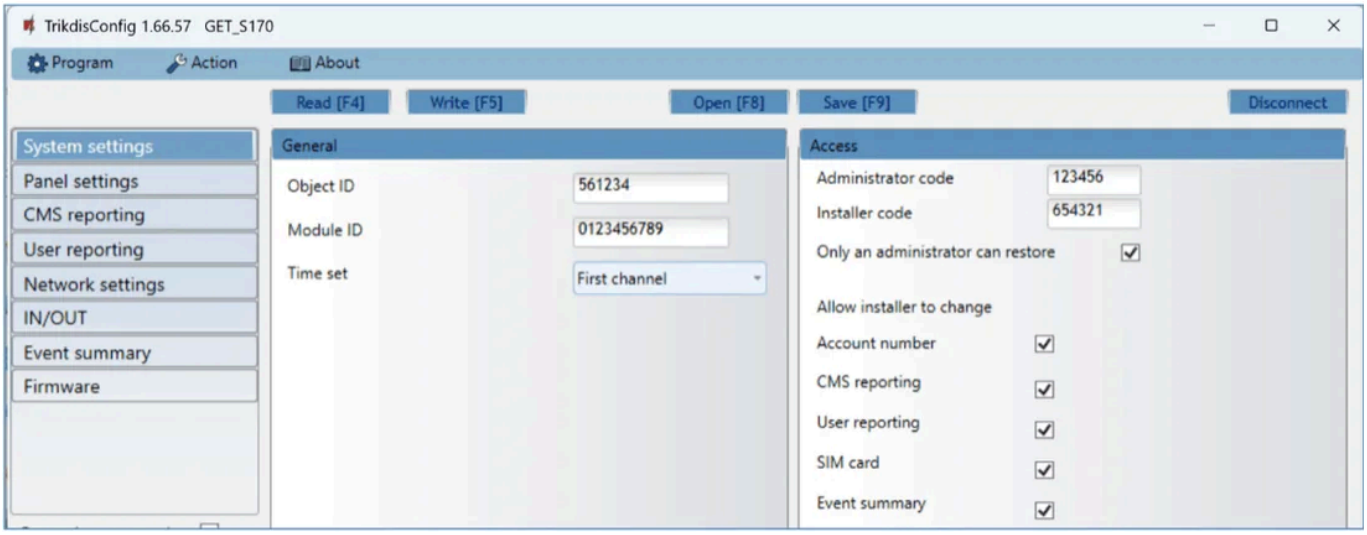


Obrázok 45. Protegus 2 – System options → System general na hardvéri x1x0: Account No., Device account No. a Time set.



Obrázok 46. Protegus 2 – System options → Access: Administrator code, Installer code, Only an administrator can restore a zoznam Allow installer to change (Account number, CMS reporting, User reporting, SIM card, Event summary).

V TrikdisConfig: stránka **System settings** má dve skupiny: v skupine **General** nastavuješ identifikátory zariadenia, v skupine **Access** prístupové úrovne.



Obrázok 47. TrikdisConfig – stránka System settings: skupina General (Object ID, Module ID, Time set) a skupina Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – identifikátor objektu, ktorý si dostal od PCO (6 hexadecimálnych znakov: 0–9, A–F; `FFFE` a `FFFF` sa nedajú použiť). Povinný, ak zariadenie hlási aj na PCO.
- **Module ID** (Device account No.) – identifikačné číslo modulu.
- **Time set** – z ktorého servera zariadenie synchronizuje svoje hodiny.

V skupine **Access** spravuješ prístupové úrovne a heslá.

K nastaveniam zariadenia sú dve úrovne prístupu: **administrátor** a **inštalátor**.

- **Administrator code** – prístup ku všetkým nastaveniam (výrobné heslo: `123456`; heslo má 6 znakov: číslice alebo latinské písmená).
- **Installer code** – prístup, ktorý sa dá obmedziť (výrobné heslo: `654321`).
- **Only an administrator can restore** – ak je zaškrtnuté, obnovenie výrobných nastavení môže spustiť iba administrátor.
- **Allow installer to change** – tu označíš, ktoré skupiny nastavení môže inštalátor meniť: **Account number** (identifikačné číslo objektu), **CMS reporting**, **User reporting**, **SIM card** (pri zariadení s mobilnou sieťou) alebo **Ethernet settings** (pri ethernetovom zariadení), **Event summary**.

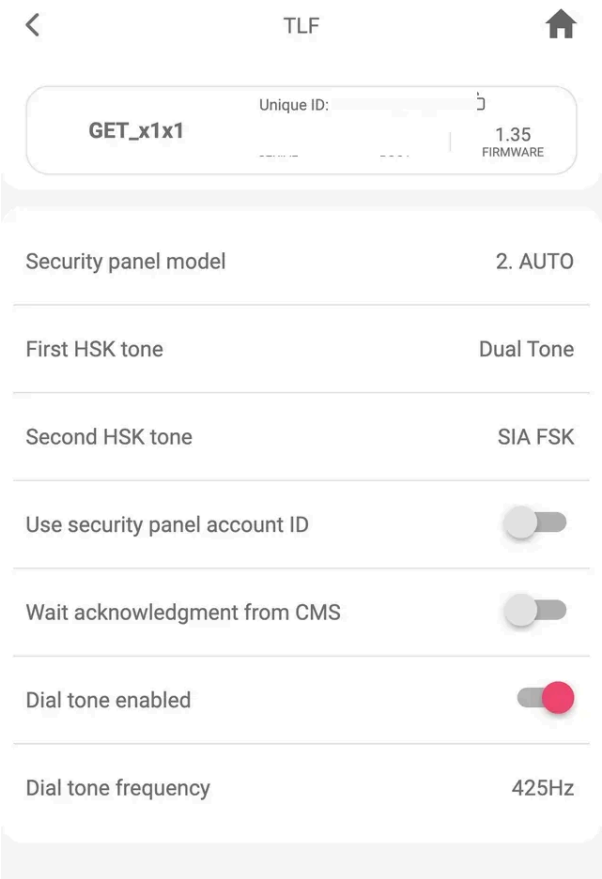
Nenechávaj v zariadení výrobné heslá!

Pri uvedení do prevádzky zmeň aspoň heslo administrátora a zapíš si ho na bezpečné miesto. Zabudnuté heslo sa nedá vymazať ani obnovením výrobných nastavení, pretože aj na to je potrebné heslo: vtedy ho vie obnoviť iba výrobca alebo distribútor, ak mu zariadenie doručíš. Výnimkou je zariadenie s hardvérovým tlačidlom RESET: podržanie tlačidla 10 sekúnd obnoví výrobné nastavenia bez hesla.

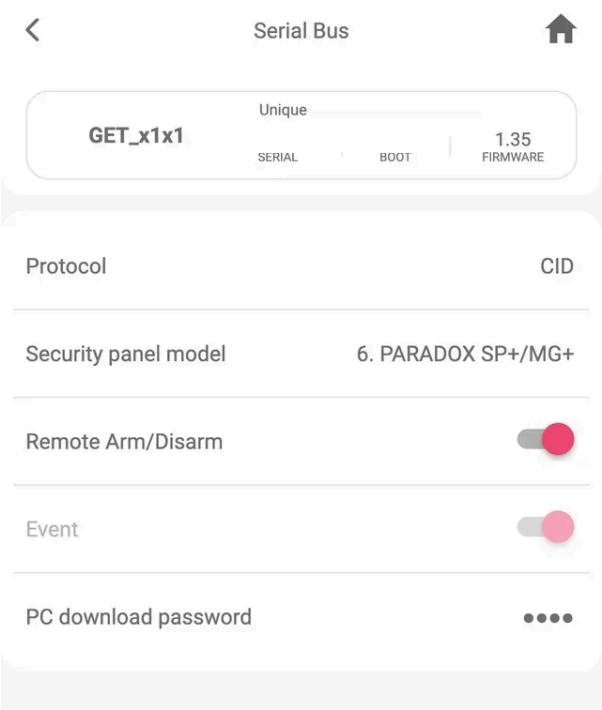
Prihlásenie inštalátora v aplikácii. Ak komunikátor otvoríš kódom inštalátora, Protegus 2 skryje polia **Administrator code** a **Only an administrator can restore** a nastavenia, ktoré administrátor nepovolil, ukazuje len na čítanie. V aplikácii sa právo **SIM card** vzťahuje aj na nastavenia LAN; kde sú identifikátory medzi nastaveniami CMS (pozri vyššie), platí pre ne právo **CMS reporting**.

6.3 Panel settings

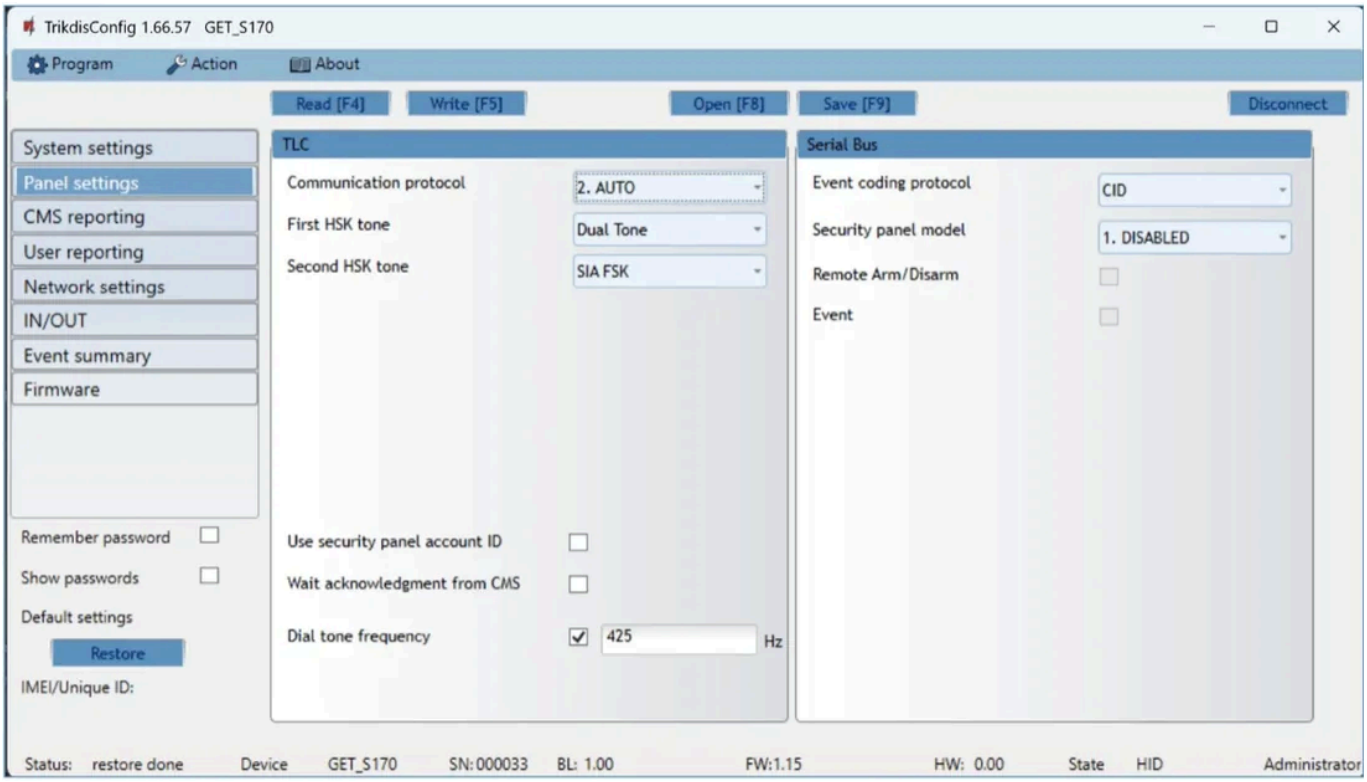
Na tejto stránke zadávaš, ako je komunikátor pripojený k zabezpečovacej ústredni: skupina **TLC** (v aplikácii **TLF**) obsahuje nastavenia pripojenia na telefónnu linku (TIP/RING), skupina **Serial bus** (**Serial Bus**) nastavenia pripojenia na dátovú zbernicu alebo sériový port. V aplikácii: **Advanced settings → Panel settings → TLF**, resp. **Panel settings → Serial Bus**.



Obrázok 48. Protegus 2 – Panel settings → TLF: Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.



Obrázok 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, zapnuté Remote Arm/Disarm, Event (len na čítanie), PC download password.

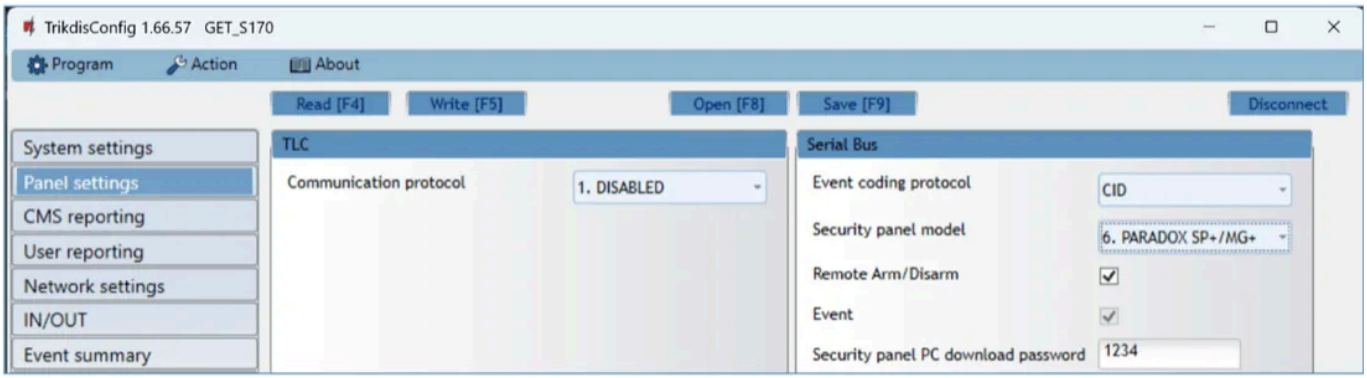


Obrázok 50. TrikdisConfig – Panel settings pri pripojení TIP/RING: v skupine TLC Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; skupina Serial bus je vtedy sivá.

Skupina TLC – ak je komunikátor pripojený na svorky TIP/RING telefónneho komunikátora ústredne:

- **Communication protocol** (Security panel model) – zapnutie (**2. AUTO**), resp. vypnutie (**1. DISABLED**) telefónneho rozhrania DTMF komunikátora. Pri pripojení TIP/RING vyber hodnotu AUTO.

- **First HSK tone**, **Second HSK tone** – tón potvrdenia spojenia (handshake) ústredne, ktorým komunikátor prijíma vytáčač ústredne (na obrázku Dual Tone a SIA FSK).
- **Use security panel account ID** – keď je zaškrtnuté, komunikátor neposiela hodnotu svojho poľa **Object ID**, ale identifikátor objektu nastavený v ústredni a poslaný ústredňou.
- **Wait acknowledgment from CMS** – keď je zaškrtnuté, komunikátor po odoslaní každej udalosti čaká na potvrdenie prijímača IP, že správa prišla; ak potvrdenie nepríde, nedá ústredni signál „kiss-off" a telefónny komunikátor ústredne správu zopakuje.
- **Dial tone frequency** – frekvencia oznamovacieho tónu, ktorým komunikátor komunikuje s vytáčačom ústredne (predvolene 425 Hz, to je aj oznamovací tón na Slovensku a vo väčšine Európy). Na karte TLF v aplikácii je navyše prepínač **Dial tone enabled**: oznamovací tón zapína alebo vypína; frekvenciu môžeš zmeniť len pri zapnutom oznamovacom tóne.



Obrázok 51. TrikdisConfig – Panel settings pri pripojení na dátovú zbernicu alebo sériový port: Communication protocol 1. DISABLED; v skupine Serial bus Event coding protocol CID, Security panel model PARADOX SP+/MG+, zaškrtnuté Remote Arm/Disarm a Event, zadané Security panel PC download password.

Skupina Serial bus – ak je komunikátor pripojený na dátovú zbernicu alebo sériový port ústredne:

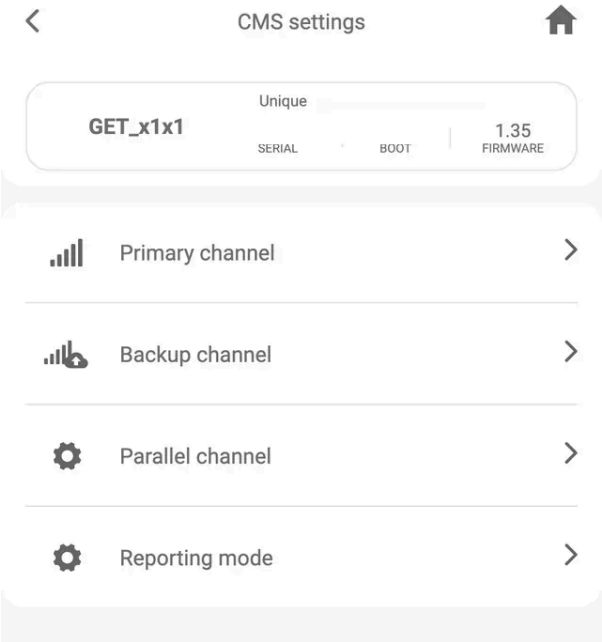
- **Event coding protocol** (Protocol) – protokol hlásenia udalostí: **CID** alebo **SIA**.
- **Security panel model** – typ pripojenej zabezpečovacej ústredne zo zoznamu (pre zapojenie Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING vyber položku **Paradox SP+/MG+ series KeyBus**, bod 3.3.3).
- **Remote Arm/Disarm** – keď je zaškrtnuté, komunikátor ovláda ústredňu priamo (zapínanie a vypínanie stráženia z Protegus 2). Viditeľné len pri priamo ovládateľných ústredniach. Na priame ovládanie treba nastaviť aj ústredňu podľa bodu 4.1.
- **Event** – keď je zaškrtnuté, komunikátor posiela udalosti ústredne na PCO a do Protegus 2. Aplikácia tento prepínač ukazuje, ale nedá sa v nej zmeniť.
- **Security panel PC download password** (PC download password; pri Texecome UDL passcode) – na priame ovládanie ústredne Paradox a Texecom heslo PC, resp. UDL; musí sa zhodovať s heslom nastaveným v ústredni, ktorého zadanie opisuje bod 4.1.

6.4 CMS reporting (Reporting to CMS)

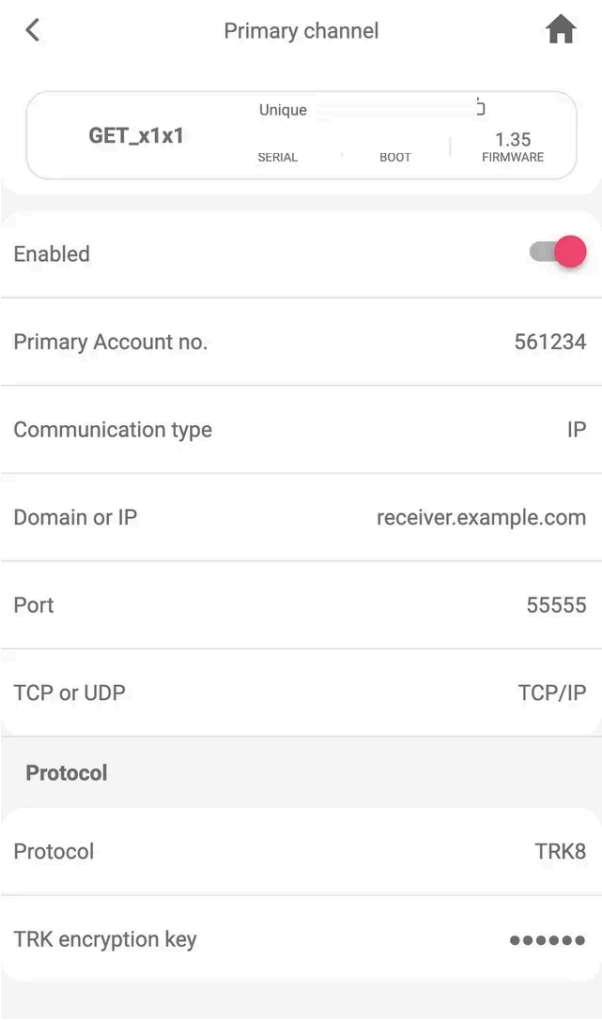
Komunikátor posiela udalosti na PCO cez IP spojenie – po káblovej sieti (LAN) alebo po mobilnej sieti (SIM1, SIM2), v poradí nastavenom v bode 6.4.2. Udalosti môžu ísť aj viacerými kanálmi: **hlavný** a **paralelný** kanál pracujú súčasne (na dva prijímače naraz) a ku každému patrí **záložný** kanál, ktorý nastúpi, ak sa daný kanál preruší. Komunikácia je šifrovaná a chránená heslom. Na protokoly TRK treba prijímač Trikdis, ktorý udalosti prijme a odovzdá softvéru PCO: na spojenie IP softvérový prijímač IPcom (Windows alebo Linux), prijímač IP/SMS RL14 alebo viackanálový prijímač RM14; protokoly DC-09 a TL150 sú určené pre univerzálne, resp. prijímače SUR-GARD (pozri nižšie, **Protocol**).

6.4.1 Kanály prijímača (CMS settings)

V aplikácii: Advanced settings → Reporting to CMS → CMS settings, potom **Primary channel**, **Backup channel** alebo **Parallel channel** (v ňom **Parallel primary channel** a **Parallel backup channel**). Nastavenia kanála sa zobrazia po zapnutí prepínača **Enabled**.

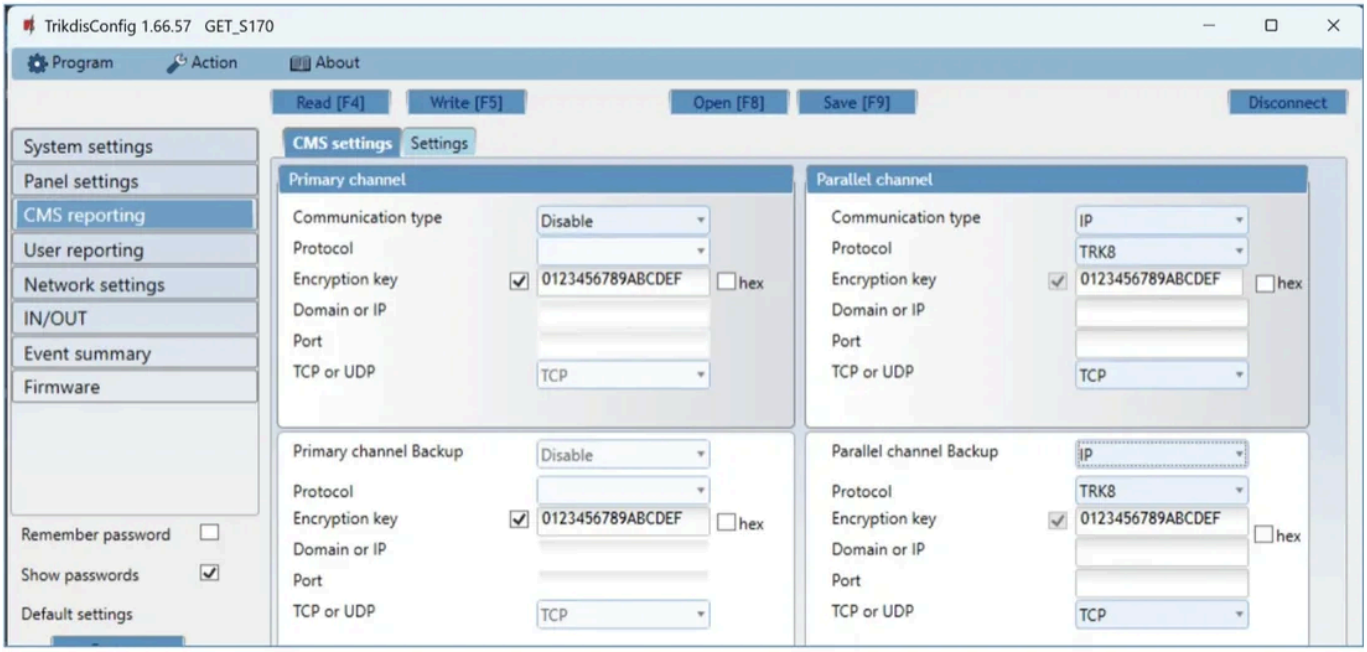


Obrázok 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel a Reporting mode.



Obrázok 53. Protegus 2 – Primary channel na hardvéri x1x1: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 a TRK encryption key.

V TrikdisConfig: karta **CMS settings** na stránke **CMS reporting**.



Obrázok 54. TrikdisConfig – CMS reporting, karta CMS settings: hlavný kanál a jeho záloha, paralelný kanál a jeho záloha (na obrázku paralelný kanál s nastavením IP / TRK8 / TCP).

Primary channel – hlavný kanál

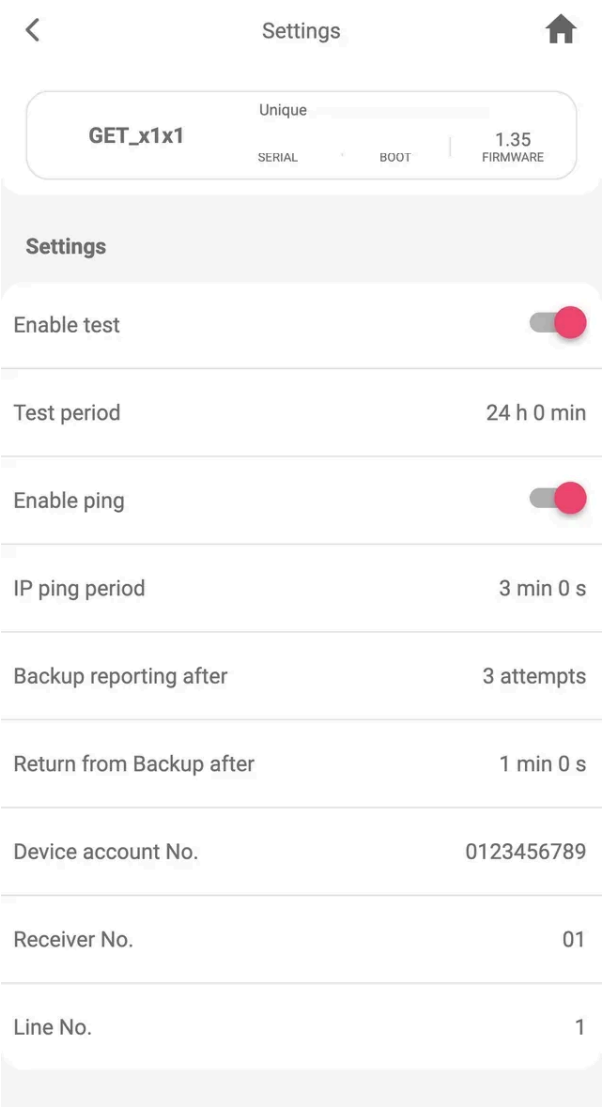
- **Communication type** – spôsob spojenia s prijímačom: **IP**.
- **Protocol** – **TRK8** (prijímače Trikdis), **DC-09_2007** alebo **DC-09_2012** (univerzálne prijímače), **TL150** (prijímače SUR-GARD).
- **Encryption key** (TRK encryption key; pri protokoloch DC-09 **Enable encryption key** a **DC-09 encryption key**, s prepínačom **HEX** pre hexadecimálny kľúč) – šifrovací kľúč správ; v komunikátore a v prijímači musí byť rovnaký. V aplikácii má TRK encryption key najviac 6, DC-09 encryption key najviac 16 znakov (v HEX 32).
- **Domain or IP**, **Port** – doménové meno alebo IP adresa prijímača a jeho sieťový port.
- **TCP or UDP** – prenosový protokol.

Primary channel Backup – záložný kanál. Keď je zapnutý, prevezme komunikáciu, ak hlavný kanál nefunguje; jeho nastavenia sú rovnaké ako vyššie.

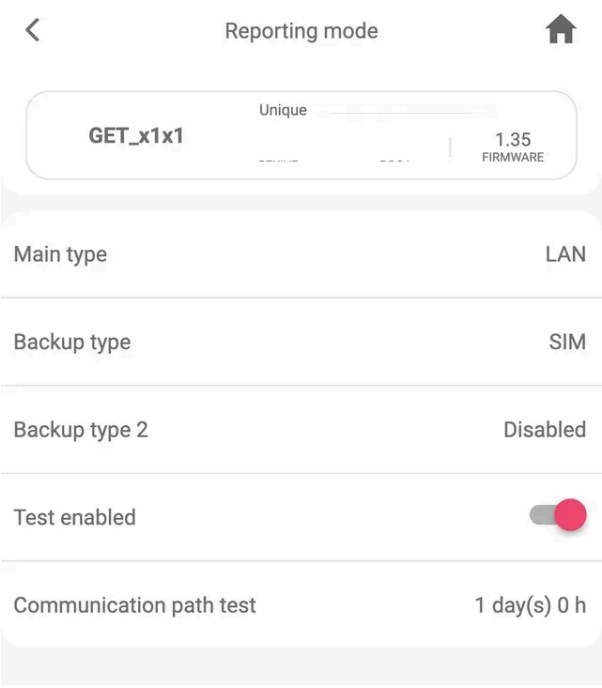
Parallel channel – paralelný kanál. Popri hlavnom kanáli posiela súčasne na druhý prijímač (napríklad na miestne a na centrálne PCO). Jeho nastavenia sú rovnaké ako pri hlavnom kanáli.

6.4.2 Test, PING a poradie spojení

V aplikácii: Advanced settings → Reporting to CMS → Settings (test, PING, časovanie záložného kanála, číslo prijímača a linky) a **Reporting to CMS → CMS settings → Reporting mode** (poradie ciest spojenia). V aplikácii je pri každom intervale prepínač: **Enable test** pre Test period, **Enable ping** pre IP ping period a **Test enabled** pre Communication path test; na karte Reporting mode sú typy spojenia uvedené ako **LAN**, **SIM** (SIM1) a **SIM2**.

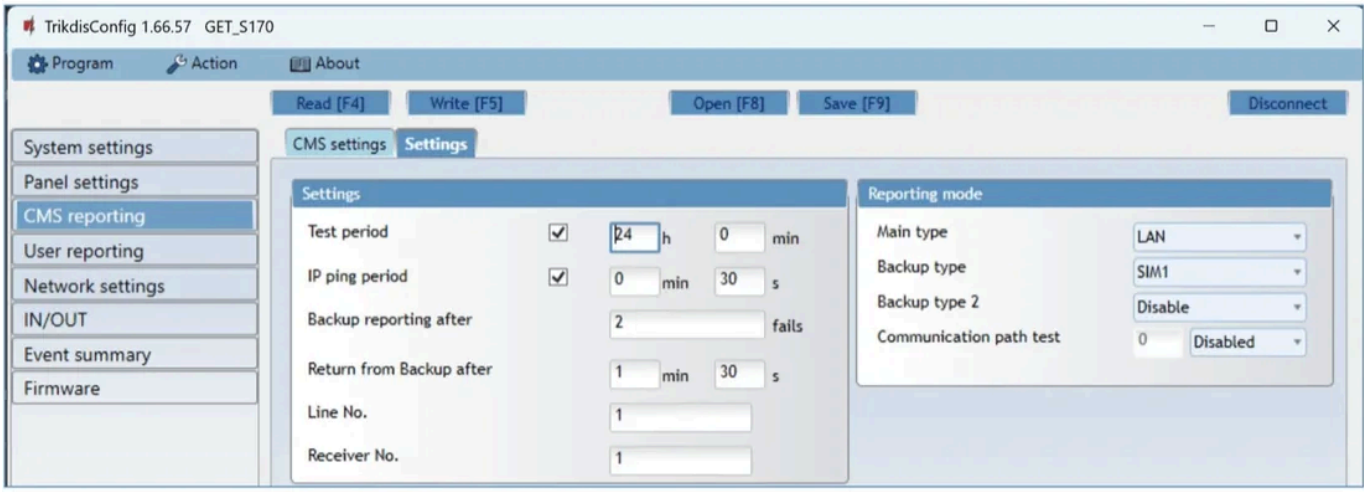


Obrázok 55. Protegus 2 – Reporting to CMS → Settings na hardvéri x1x1: Enable test a Test period, Enable ping a IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.



Obrázok 56. Protegus 2 – CMS settings → Reporting mode: Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled a Communication path test.

V TrikdisConfig: karta **Settings** na stránke **CMS reporting**.



Obrázok 57. TrikdisConfig – CMS reporting, karta Settings: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; v skupine Reporting mode Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **Test period** – interval periodickej testovacej správy (predvolene 24 hodín). Testovacia správa ide ako správa Contact ID na PCO a do Protegus 2.
- **IP ping period** – interval signálu života (PING) na kanáli IP (predvolene 30 s). Zapneš ho zaškrtnutím, čas zadáš v políčkach minút (**min**) a sekúnd (**s**); je potrebný na dohľad nad spojením. Prijímač PING-y neposiela ďalej do softvéru PCO, aby ho nepreťažoval; softvér dostane správu iba vtedy, ak prijímač nedostane PING počas trojnásobku nastaveného času. Ak je napríklad perióda PING 3 minúty, stratu spojenia ohlási po 9. minúte.
- **Backup reporting after** – po tomto počte neúspešných pokusov o odoslanie sa zariadenie prepne na záložný kanál (predvolene 2).
- **Return from Backup after** – po tomto čase sa vráti na primárny kanál (predvolene 1 minúta 30 s).

PING udržiava živé spojenie medzi zariadením a prijímačom a závisí od neho aj vzdialený prístup, ovládanie a programovanie. Preto **neodporúčame periódu PING dlhšiu ako 5 minút**.

DC-09 Settings (na pravej strane karty) – vyplniť ich treba iba vtedy, ak na niektorom kanáli posielaš protokolom DC-09_2007 alebo DC-09_2012; skupina sa zobrazí, keď je v poli **Protocol** niektorého kanála vybraný DC-09_2007 alebo DC-09_2012:

- **Object ID in DC-09** – hexadecimálny identifikátor s dĺžkou 3–16 znakov, pridelí ho PCO.
- **DC-09 line No** – číslo linky.
- **DC-09 receiver No.** – číslo prijímača.

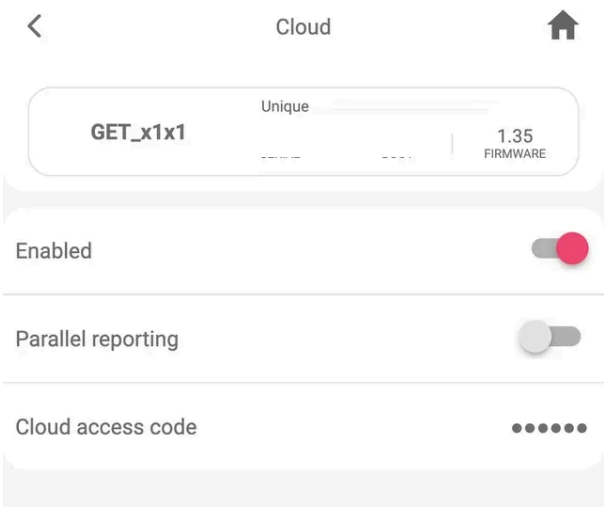
Na karte Settings komunikátora GET sú aj polia **Line No.** (číslo linky prijímača) a **Receiver No.** (číslo prijímača); samostatné pole „Object ID in DC-09" GET nemá.

Skupina Reporting mode – tu zadávaš, akou cestou má komunikátor komunikovať s kanálmi PCO a s Protegus 2. Typy spojenia zadávaš v poradí: ak sa spojenie podľa **Main type** nevytvorí, komunikátor prepne na spojenie podľa **Backup type** a tak ďalej; ak sa správu podarilo poslať záložnou cestou, po uplynutí nastaveného času (Return from backup after) znova skúsi hlavnú cestu.

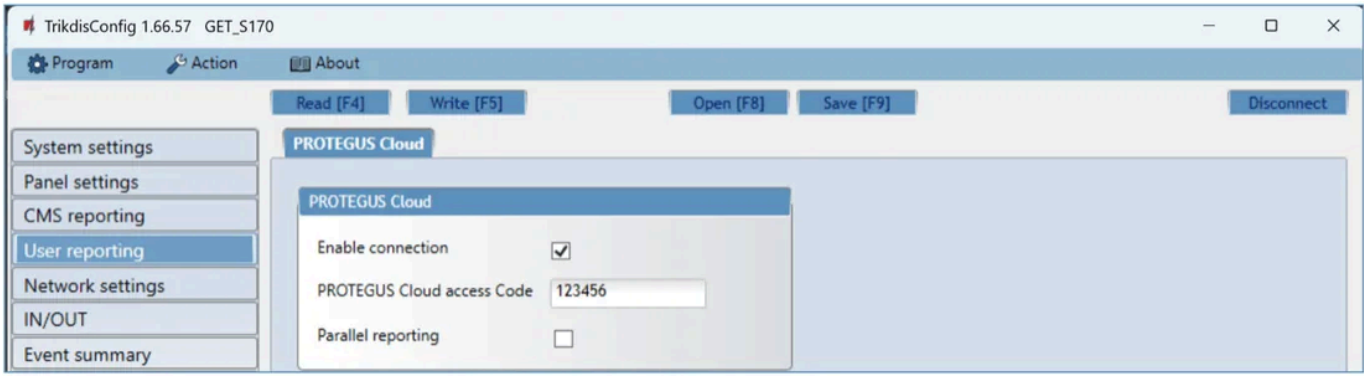
- **Main type** – typ hlavného spojenia s prijímačom a s Protegus 2: **LAN**, **SIM1** alebo **SIM2**.
- **Backup type** – typ záložného spojenia (LAN, SIM1, SIM2).
- **Backup type 2** – typ druhého záložného spojenia (LAN, SIM1, SIM2).
- **Communication path test** – v akom intervale komunikátor vyskúša zvolené typy spojenia (LAN, SIM1, SIM2).

6.5 User reporting (Protegus Cloud)

Službou Protegus 2 používateľ na diaľku sleduje a ovláda komunikátor a systém, ktorý je k nemu pripojený; podrobnosti: web.protegus.app. V aplikácii: **Advanced settings → User reporting → Cloud**; v TrikdisConfig karta **PROTEGUS Cloud** na stránke **User reporting**.



Obrázok 58. Protegus 2 – User reporting → Cloud: Enabled, Parallel reporting, Cloud access code.



Obrázok 59. TrikdisConfig – User reporting, karta PROTEGUS Cloud: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – povolí službu Protegus 2: zariadenie si vymieňa dáta s aplikáciou Protegus 2 a TrikdisConfig sa k nemu dostane aj na diaľku.
- **PROTEGUS Cloud access Code** (Cloud access code) – 6-miestny kód na pripojenie k Protegus 2 (z výroby `123456`). Ak ho zmeníš v TrikdisConfig, musíš ho prepísať aj v aplikácii Protegus 2.
- **Parallel reporting** (v aplikácii viditeľné len vtedy, ak to firmvér podporuje) – keď je zaškrtnuté, správy idú súčasne hlavným kanálom (na PCO) aj do Protegus 2; Protegus 2 a používatelia dostanú správu až potom, ako odišla na PCO.

6.6 Network settings

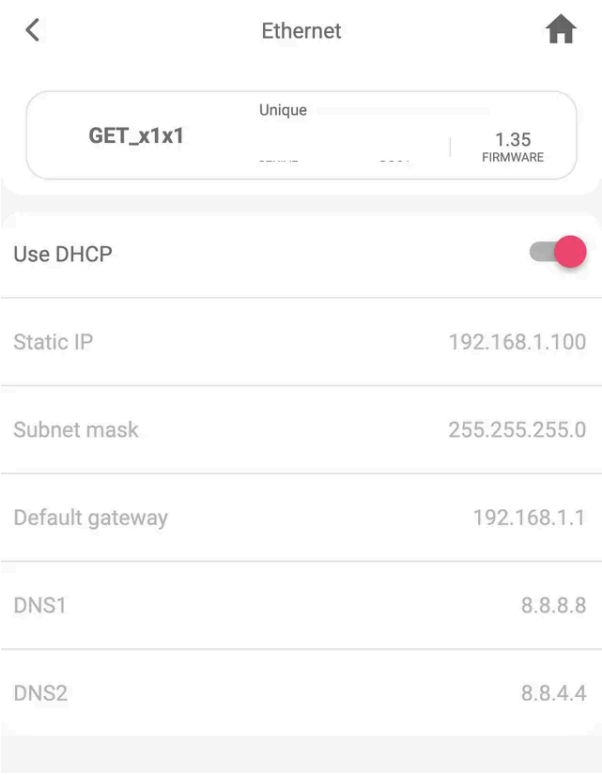
6.6.1 LAN (Ethernet)

Tieto nastavenia treba zadať, ak je komunikátor pripojený na káblovú lokálnu sieť (LAN). V aplikácii: **Advanced settings** → **Network settings** → **LAN**; polia **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** a **DNS2** môžeš meniť len pri vypnutom **Use DHCP**. V TrikdisConfig karta **LAN** na stránke **Network settings**, skupina **Ethernet settings**.

Čo musí sieť zvládnuť? Komunikátor sám nadväzuje odchádzajúce spojenie smerom k prijímaču PCO a do cloudu Protegus, preto na routeri **netreba otvárať ani presmerovať porty** a netreba ani verejnú pevnú IP adresu či dynamické DNS. Čo treba:

- voľný ethernetový port na routeri alebo switchi;
- DHCP (výrobné nastavenie) alebo pevnú IP adresu, masku podsiete, bránu a DNS od správcu siete;
- povolenú odchádzajúcu komunikáciu na adresu a port prijímača (TCP alebo UDP, podľa nastavenia prijímača), ako aj smerom do cloudu Protegus.

Vo filtrovanej – firemnej, inštitucionálnej – sieti to vopred dohodni so správcom siete: na domácich routeroch je štandardne povolené každé odchádzajúce spojenie, v sieti chránenej firewallom však môže byť potrebné samostatné pravidlo.



Obrázok 60. Protegus 2 – Network settings → LAN: zapnuté Use DHCP; polia Static IP, Subnet mask, Default gateway, DNS1 a DNS2 sú vtedy sivé.



Obrázok 61. TrikdisConfig – Network settings, karta LAN, skupina Ethernet settings: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

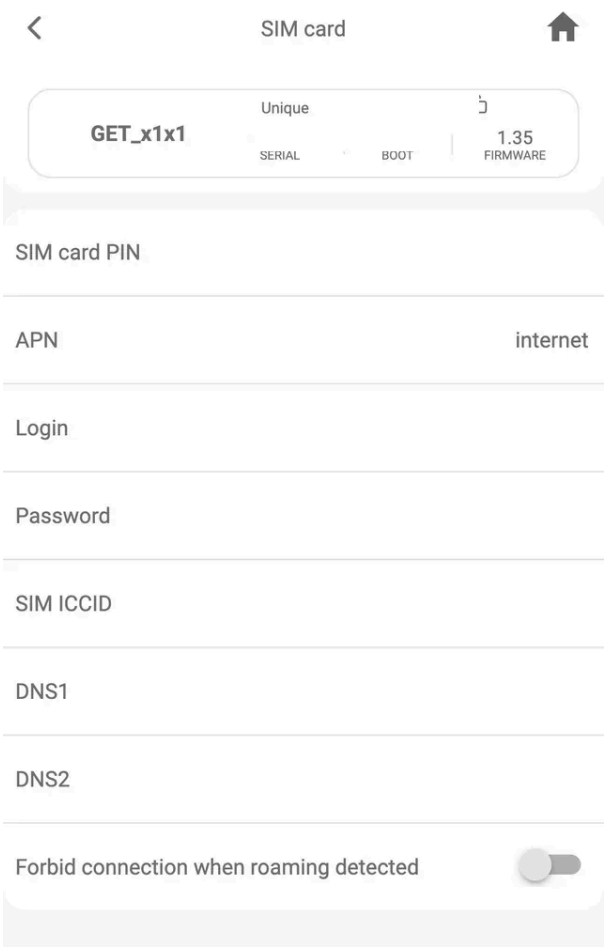
- **Use DHCP** – keď je zaškrtnuté, komunikátor sa do siete prihlási automaticky (adresu dostane od servera DHCP routera). Ak automatické prihlásenie neuspeje, adresy treba zadať ručne:
- **Static IP** – pevná IP adresa komunikátora pri ručnom nastavení.
- **Subnet mask** – maska podsiete pri ručnom nastavení.
- **Default gateway** – adresa brány (routera) pri ručnom nastavení.
- **DNS1, DNS2** – menné servery (DNS, Domain Name System: k doménovému menu priradí IP adresu); treba ich, ak si prijímač zadal v poli **Domain or IP** kanála doménovým menom, a nie IP adresou. Predvolený je verejný DNS Google. Nezávisle od nastavení IP skontroluj, či adresy DNS fungujú u tvojho poskytovateľa internetu.

6.6.2 SIM1 a SIM2

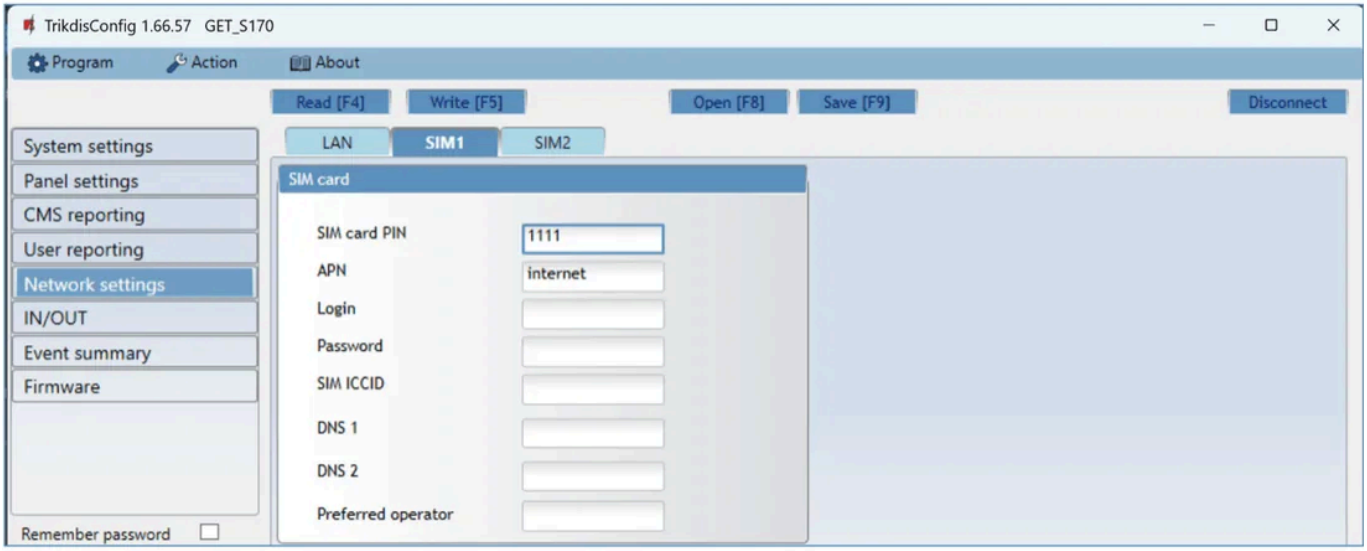
Tieto nastavenia treba zadať pre každú vloženú kartu SIM zvlášť; nastavenia držiakov SIM1 a SIM2 sú rovnaké.

Pred použitím sa uisti, že karta SIM je aktívna a funguje a že sú na nej povolené aj mobilné dáta.

V aplikácii: **Advanced settings** → **Network settings** → **SIM** (SIM1) alebo **SIM2**. V TrikdisConfig karta **SIM1**, resp. **SIM2** na stránke **Network settings**, skupina **SIM card**.



Obrázok 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 a prepínač Forbid connection when roaming detected.



Obrázok 63. TrikdisConfig – Network settings, karta SIM1, skupina SIM card: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (karta SIM2 je rovnaká).

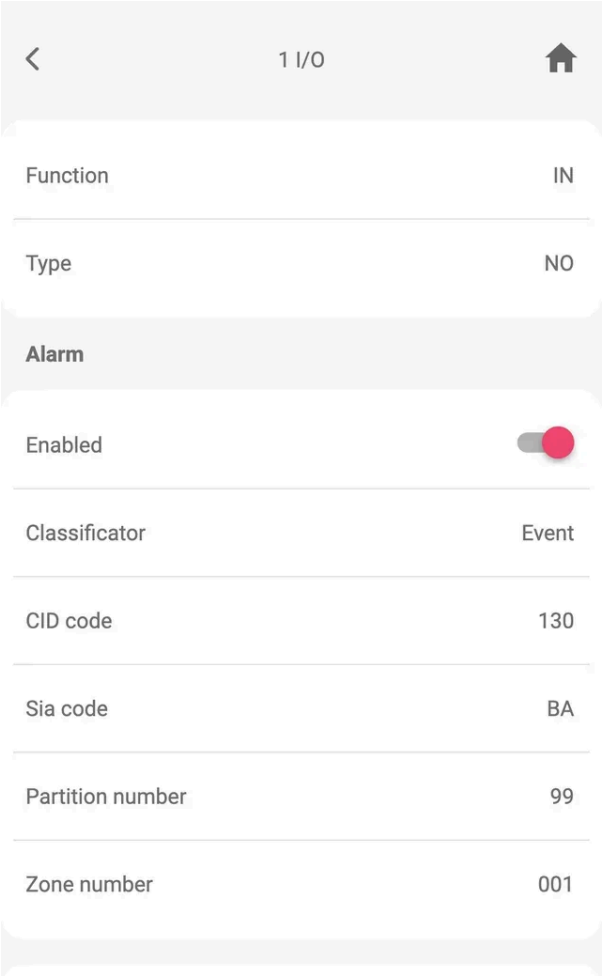
- **SIM card PIN** – kód PIN karty. Požiadavku na PIN vypneš tak, že kartu vložíš do mobilného telefónu a tam ju zakážeš; vtedy môže v poli zostať výrobná hodnota.
- **APN** – prístupový bod operátora (Access Point Name); bez neho sa zariadenie nepripojí na internet. Hodnotu nájdeš na webe operátora karty SIM; `internet` je všeobecný a funguje v sieti mnohých operátorov. Známe APN operátorov uvádza článok o APN (pri karte IoT / M2M dáva operátor samostatný APN, pozri bod 2.3).
- **Login, Password** – používateľské meno a heslo pre internetové pripojenie, ak ich operátor vyžaduje.
- **SIM ICCID** – číslo ICCID karty SIM, ak chceš, aby zariadenie fungovalo len s touto kartou.
- **DNS1, DNS2** – menné servery; treba ich, ak si prijímač zadal v poli **Domain or IP** kanála doménovým menom. Predvolený je verejný DNS Google; skontroluj, či adresy DNS fungujú u tvojho operátora.
- **Preferred operator** – kód mobilného operátora (MCC + MNC); ak ho zadáš, zariadenie sa pripojí len do siete zvoleného operátora. Je **len v TrikdisConfig**.

Na karte SIM v aplikácii je namiesto Preferred operator prepínač **Forbid connection when roaming detected**: keď je zapnutý, komunikátor sa nepripojí, ak zistí roaming. Na hardvérovej verzii **M15** s firmvérom **1.17** alebo novším sa na karte SIM zobrazia aj nastavenia **Generation** a **Bands**: nimi môžeš obmedziť, akú technológiu mobilnej siete a aké frekvenčné pásma komunikátor používa.

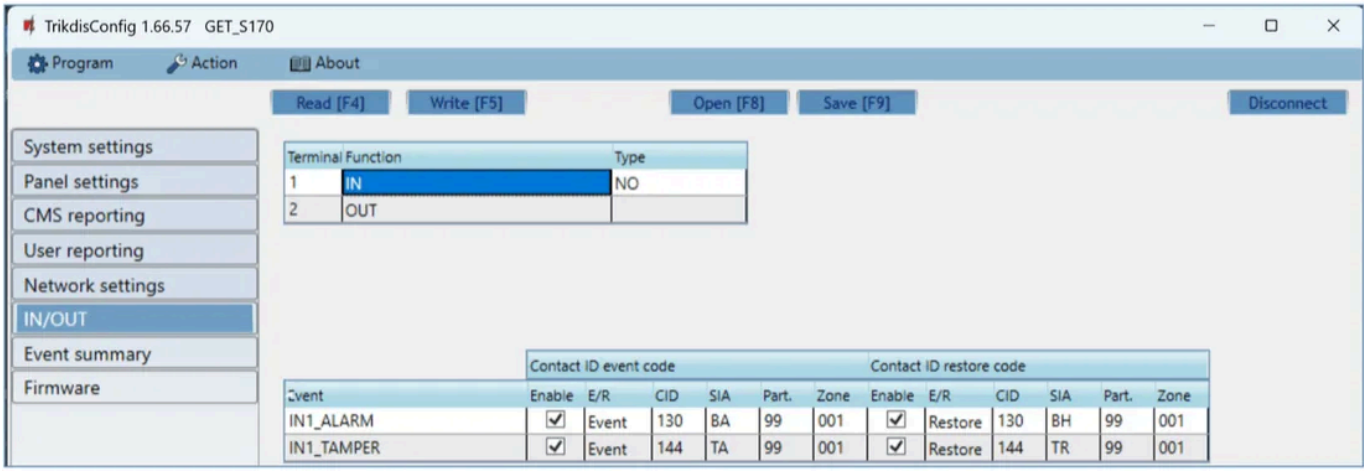
6.7 IN/OUT

Tu zadávaš úlohu dvoch svoriek I/O komunikátora s dvojitou funkciou: **Disabled** (nepoužíva sa), **IN** (vstup) alebo **OUT** (výstup; na GET je to výrobné nastavenie). Pri vstupe treba v poli **Type** zadať aj typ pripojeného obvodu (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Na vstupy môžeš pripojiť ďalšie snímače: pri narušení snímača pošle komunikátor vlastnú udalosť s kódom Contact ID (SIA) priradeným k vstupu na PCO a do Protegus 2.

V aplikácii: **Advanced settings** → **IN/OUT**, potom svorka **1.** alebo **2.**: **Function** (Disabled, IN, OUT) a pri vstupe **Type**; v častiach **Alarm** a **Tamper** sú správy o udalosti a obnovení posielané pri narušení vstupu. V TrikdisConfig stránka **IN/OUT**.



Obrázok 64. Protegus 2 – IN/OUT, 1. svorka: Function IN, Type NO; udalosť Alarm Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.



Obrázok 65. TrikdisConfig – stránka IN/OUT: 1. svorka je vstup (IN, NO), 2. výstup (OUT); pod tým udalosti poplachu a sabotáže 1. vstupu s kódom CID a SIA.

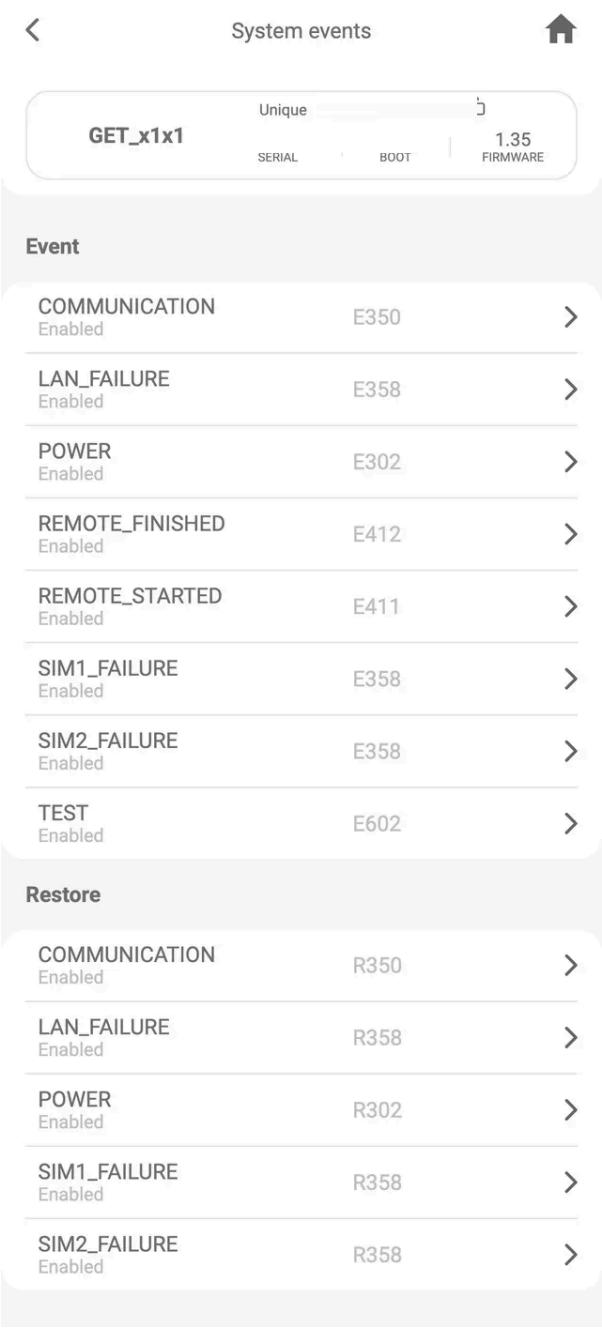
Pri narušení snímača pripojeného na vstup pošle komunikátor poplach (**INx_ALARM**, Contact ID 130, SIA BA; obnovenie BH), pri narušení sabotážneho obvodu udalosť sabotáže (**INx_TAMPER**, 144, SIA TA; obnovenie TR); v tabuľke sa zobrazia udalosti každej svorky nastavenej ako vstup. Stĺpce tabuľky:

- **Enable** (Enabled) – povolí posielanie správy na PCO a do Protegus 2.
- **E/R** (Classificator) – typ správy: Event (udalosť) alebo Restore (obnovenie).

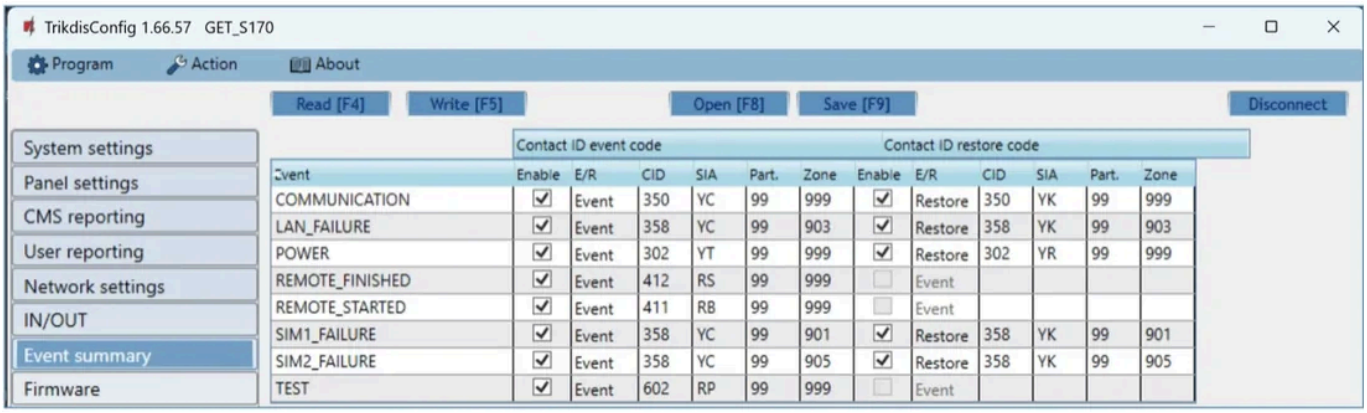
- **CID** (CID code) – kód Contact ID (môžeš ho prepísať alebo nechať výrobný); pri narušení vstupu ide správa s týmto kódom do Protegus 2 a na PCO.
- **SIA** (Sia code) – kód SIA (môžeš ho prepísať alebo nechať výrobný).
- **Part.** (Partition number) – číslo partície v správe (pri udalosti aj pri obnovení).
- **Zone** (Zone number) – číslo zóny v správe.

6.8 Event summary (System events)

Tu môžeš povoliť, zakázať a upraviť vlastné interné správy zariadenia. Správa, ktorú tu zakážeš, neodíde bez ohľadu na akékoľvek iné nastavenie. V aplikácii: **Advanced settings** → **System events**, správy sú v zoznamoch **Event** a **Restore**; na úpravu správu vyber. V TrikdisConfig stránka **Event summary**.



Obrázok 66. Protegus 2 – System events: zoznam Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) a zoznam Restore.



Obrázok 67. TrikdisConfig – stránka Event summary: interné správy zariadenia s kódom CID a SIA, s partíciou 99.

Interné správy GET (v zátvorke výrobný kód Contact ID a zóna):

- **COMMUNICATION** (350, zóna 999) – chyba spojenia medzi ústredňou a komunikátorom; jej obnovenie je samostatná správa.
- **LAN_FAILURE** (358, zóna 903) – chyba spojenia káblovej siete (LAN); jej obnovenie je samostatná správa.
- **POWER** (302, zóna 999) – nízke napájacie napätie; jeho obnovenie je samostatná správa.
- **REMOTE_FINISHED** (412) – koniec diaľkového programovania z TrikdisConfig (odpojenie).
- **REMOTE_STARTED** (411) – diaľkové pripojenie na programovanie GET z TrikdisConfig.
- **SIM1_FAILURE** (358, zóna 901) – chyba spojenia s mobilnou sieťou na SIM1; jej obnovenie je samostatná správa.
- **SIM2_FAILURE** (358, zóna 905) – chyba spojenia s mobilnou sieťou na SIM2; jej obnovenie je samostatná správa.
- **TEST** (602) – periodická testovacia správa.

Zapnutie a interval periodickej správy TEST nastavuješ v poli **Test period** (bod 6.4.2).

- **Enable** (Enabled) – keď je zaškrtnuté, posielanie správy je povolené.
- Pri každej správe môžeš zmeniť kód Contact ID (SIA), ako aj číslo zóny a partície.

6.9 Obnovenie výrobných nastavení

Z aplikácie Protegus 2 sa výrobné nastavenia obnoviť **nedajú**: treba na to tlačidlo **Restore** v TrikdisConfig alebo tlačidlo **RESET** na zariadení.

Na obnovenie výrobných nastavení klikni v ľavej dolnej časti okna TrikdisConfig, v skupine **Default settings**, na tlačidlo **Restore**. Obnovenie vymaže všetky nastavenia – aj heslá –, preto je dobré predtým uložiť nastavenia do súboru (**Save [F9]**).

S heslom inštalátora je to možné iba vtedy, ak to administrátor nezakázal na stránke **System settings** → **Access**.



Obrázok 68. TrikdisConfig – tlačidlo Restore v skupine Default settings.

Výrobné nastavenia môžeš obnoviť aj na zariadení, bez počítača: pri zapnutom napájaní stlač a drž tlačidlo **RESET** na plošnom spoji (bod 1.4) **10 sekúnd**, kým LED NETWORK, POWER a TROUBLE zhasnú a potom sa rozsvieti LED POWER. Vtedy tlačidlo uvoľni: výrobné nastavenia sú obnovené.

7. Programovanie na diaľku

TrikdisConfig sa k zariadeniam Trikdis dostane nielen cez USB kábel, ale aj **na diaľku, cez cloud Protegus**. Nastavenia už namontovaného zariadenia tak môžeš zmeniť bez toho, aby si išiel na miesto.

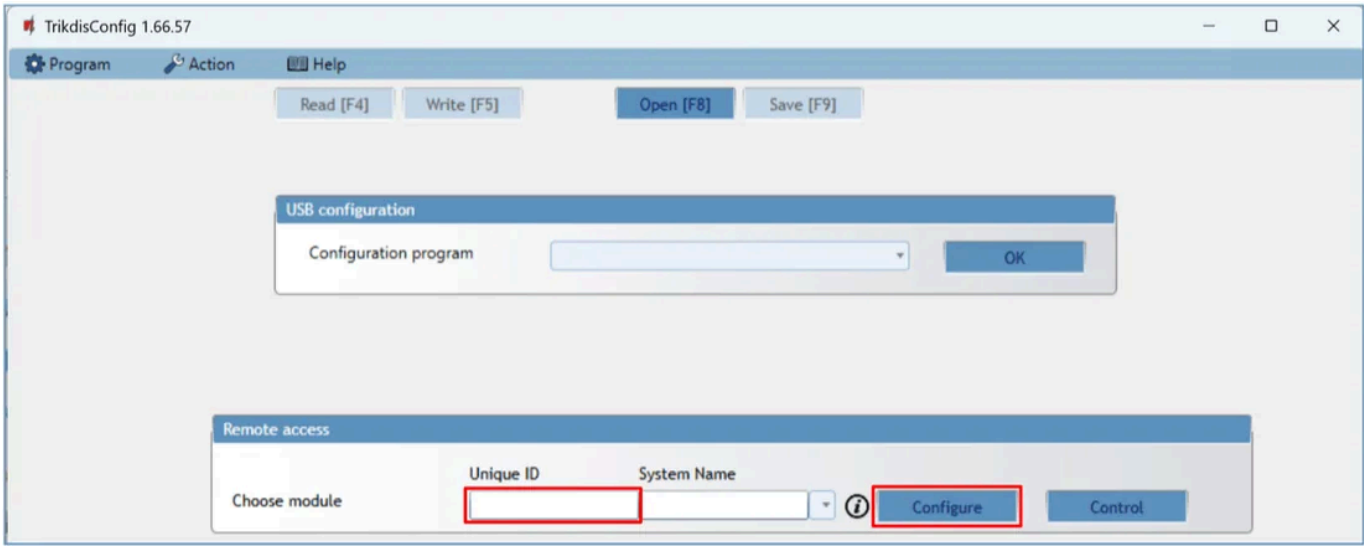
Na vzdialený prístup je potrebné:

1. Zariadenie musí byť zapnuté a mať sieťové spojenie (LED **POWER** a **NETWORK** svietia nazeleno; pri zariadení s mobilnou sieťou NETWORK bliká aj nažlto). Pri zariadení s mobilnou sieťou musí byť vložená SIM karta aktívna a jej PIN kód zadaný v zariadení, alebo musí byť požiadavka na PIN vypnutá; pri ethernetovom zariadení musí byť zapojený sieťový (LAN) kábel a zariadenie sa musí dostať na internet.
2. Na stránke **User reporting** → **PROTEGUS Cloud** v TrikdisConfig musí byť zaškrtnuté **Enable connection** (nastav to cez USB pri prvom uvedení do prevádzky).
3. Musíš poznať **jedinečný identifikátor** zariadenia (IMEI alebo MAC – je na krabici a na zadnej strane zariadenia) a heslo administrátora alebo inštalátora.

Kroky:

1. Spusti softvér TrikdisConfig.
2. V časti **Remote access** zadaj do poľa **Unique ID** jedinečný identifikátor zariadenia (IMEI alebo MAC).
3. Podľa potreby pomenuj systém v poli **System name** – program si ho zapamätá a nabudúce ho môžeš vybrať z rozbaľovacieho zoznamu.
4. Stlač tlačidlo **Configure**.
5. V okne, ktoré sa otvorí, klikni na tlačidlo **Read [F4]** (čítanie) a zadaj heslo. Zaškrtnutím **Remember password** si ho program zapamätá na túto reláciu.
6. Urob zmeny a potom ich tlačidlom **Write [F5]** (zápis) pošli do zariadenia.

Systémy, ktoré si predtým programoval na diaľku a pomenoval, program uloží; zobrazíš ich šípkou vedľa poľa **System name**. Na vymazanie označ v zozname identifikátor, stlač kláves **Delete** a potvrď.



Obrázok 69. TrikdisConfig – skupina Remote access: pole Unique ID, zoznam System name a tlačidlo Configure.

Jedinečný identifikátor GET je **IMEI / Unique ID**; nájdeš ho na štítku zariadenia a na nálepke krabice. Diaľkový prístup funguje len vtedy, ak je karta SIM aktívna a jej kód PIN je zadaný alebo je požiadavka na PIN vypnutá – **alebo** je komunikátor pripojený sieťovým káblom (LAN) –; na karte **User reporting** → **PROTEGUS Cloud** je zaškrtnuté **Enable connection** (bod 6.5); LED **POWER** svieti na zeleno; LED **NETWORK LTE** svieti na zeleno a bliká na žlto (pri len káblovom spojení svieti na zeleno LED **NETWORK LAN**). Začiatok a koniec programovania na diaľku hlási komunikátor správou REMOTE_STARTED a REMOTE_FINISHED (bod 6.8).

8. Kontrola fungovania komunikátora

Po naprogramovaní a zapojení vždy over celý reťazec: zabezpečovacia ústredňa → komunikátor → PCO a/alebo Protegus 2.

Predtým skontroluj, či je napájanie (LED **POWER** svieti nazeleno) a či je sieťové spojenie (LED **NETWORK** svieti nazeleno).

1. **Vyvolaj udalosť.** Zakóduj a potom odkóduj systém na klávesnici, alebo na zakódovanom systéme naruš zónu, aby vznikol poplach.
2. **Over doručenie.** Pozri sa, či sa udalosť objavila v softvéri PCO a/alebo v zozname udalostí aplikácie Protegus 2 – so správnym číslom partície a zóny.
3. **Vstupy.** Naruš detektor pripojený na vlastný vstup komunikátora a over príslušnú udalosť.
4. **Výstupy.** Zopni výstup z aplikácie Protegus 2 a over, že pripojené zariadenie (relé, zóna kľúčového spínača) sa naozaj aktivuje.
5. **Vzdialené zakódovanie.** Ak sa ústredňa dá ovládať na diaľku, zakóduj a odkóduj ju aj z aplikácie Protegus 2.

Ak komunikátor hlási po káblovej aj po mobilnej sieti (bod 6.4.2, Reporting mode), skúšku sa oplatí urobiť oboma cestami: vytiahni kábel LAN, vyvolaj udalosť a pozri, či príde na PCO aj cez kartu SIM; potom kábel zasuň späť.

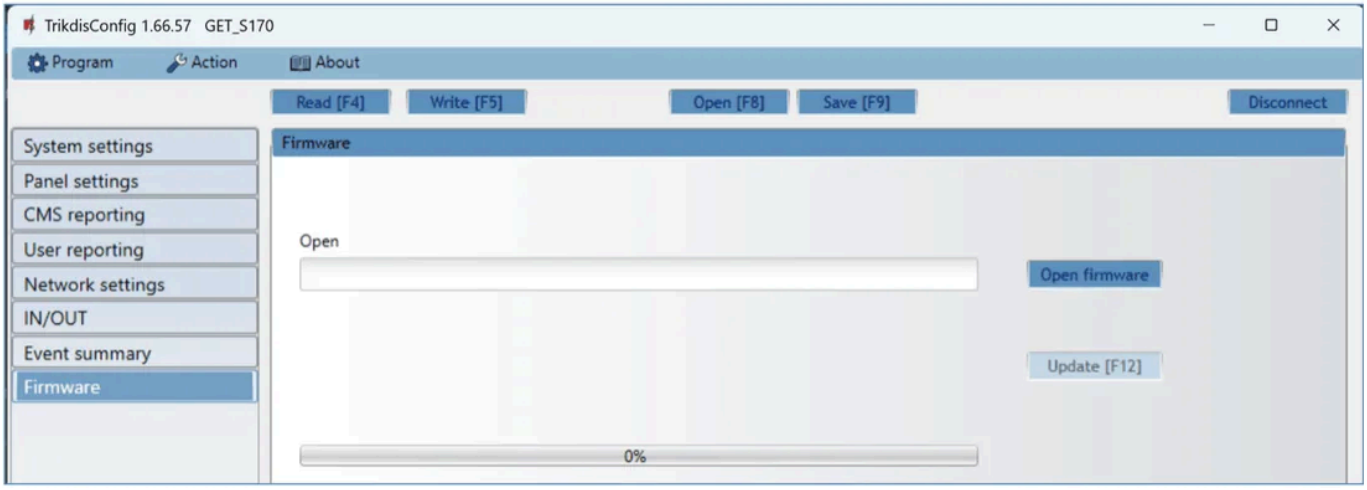
9. Aktualizácia firmvéru

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

Firmvér môžeš aktualizovať aj sám – na novší a v prípade potreby aj na starší. Po aktualizácii zostanú všetky nastavenia zariadenia nezmenené.

1. Spusti softvér TrikdisConfig a pripoj zariadenie USB káblom, alebo sa prihlás do jeho programovania na diaľku.
2. Ak je k dispozícii novší firmvér, program ponúkne jeho stiahnutie – prijmi ho.
3. Vyber stránku **Firmware** a klikni na tlačidlo **Open firmware**. Vyber súbor firmvéru.
4. Stlač tlačidlo **Update [F12]**, počkaj na koniec aktualizácie a potom v kontextovom okne klikni na **OK**. Medzitým nevyťahuj kábel a neprerušuj spojenie.

Súbory firmvéru sú v inštalačnom priečinku TrikdisConfig, v podpriečinku **Firmwares**, v priečinku označenom názvom zariadenia. Ak taký priečinok nie je, buď pre zariadenie nie je aktualizácia, alebo treba aktualizovať samotný softvér TrikdisConfig. Najnovšie súbory si ako registrovaný používateľ môžeš stiahnuť aj z webu výrobcu, zo stránky zariadenia.



Obrázok 70. TrikdisConfig – stránka Firmware: tlačidlo Open firmware, tlačidlo Update [F12] a indikátor priebehu.

Na aktualizáciu treba internetové pripojenie. Antivírus, firewall alebo prísne nastavenie prístupu na internet môže zabrániť automatickej aktualizácii firmvéru; vtedy treba upraviť nastavenia antivírusu.

Niektoré funkcie GET vyžadujú určitú verziu firmvéru:

- **1.08** alebo novší: nastavenie z aplikácie Protegus 2 (Advanced settings, bod 2.2 a kapitola 6);
- **1.17** alebo novší, na hardvérovej verzii **M15**: nastavenia **Generation** a **Bands** na karte SIM v aplikácii (bod 6.6.2);
- **1.21** alebo novší: zapojenie Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING (bod 3.3.3);
- **1.31** alebo novší, na hardvérovej verzii **x1x1**: identifikátory (Account No., Device account No.) sú v aplikácii medzi nastaveniami CMS (bod 6.2).

10. Hľadanie chýb a časté otázky

Najčastejšie otázky a chyby, vychádzajúc zo signalizácie LED. Ak odpoveď odkazuje na podrobnú kapitolu, nájdeš tam presné miesto nastavenia.

LED NETWORK LTE nesvieti – nie je mobilná sieť

1. Pozri bliknutia LED **TROUBLE**: 2 = chyba karty SIM1, 3 = chyba karty SIM2 (bod 1.6).
2. Skontroluj, či je karta SIM aktívna, má mobilné dáta a dobre sedí v držiaku (SIM1 v strede dosky, SIM2 na jej ľavom okraji; bod 3.1).
3. Ak je na karte zapnutá požiadavka na PIN, zadaj PIN na karte **Network settings** → **SIM1** (alebo **SIM2**), alebo požiadavku na PIN vypni v telefóne.
4. Skontroluj APN (bod 2.3): pri karte IoT / M2M dáva operátor samostatný APN.
5. Skontroluj anténu: je naskrutkovaná, nie je v kovovej skrinke, úroveň signálu je vyhovujúca (LED NETWORK LTE blikne na žlto aspoň trikrát; body 1.6 a 3.2).
6. Ak komunikátor hlási po káblovej sieti, chýbajúca mobilná sieť ho sama osebe nezastaví: podľa poradia v **Reporting mode** (bod 6.4.2) pošle udalosť ďalšou dostupnou cestou – ale tak chýba záložná cesta, oplatí sa to dať do poriadku.

LED NETWORK LAN nesvieti – nie je káblová sieť

1. 1 bliknutie LED **TROUBLE** znamená chybu fyzického spojenia káblovej siete: skontroluj kábel LAN na oboch koncoch a to, či port routera alebo switchu funguje (bod 1.6).

2. Ak je kábel v poriadku, pozri kartu **Network settings** → **LAN**: pri DHCP musí adresu prideliť router; pri pevnej adrese musia Static IP, Subnet mask a Default gateway zodpovedať lokálnej sieti (bod 6.6.1).
3. Ak si prijímač zadal doménovým menom, musia v sieti fungovať aj adresy DNS (DNS1, DNS2).

Sieť je, ale PCO nedostáva udalosti

LED DATA je najjednoduchšia kontrola internetu. LED DATA svieti, keď je v pamäti zariadenia správa čakajúca na odoslanie. Zelená LED NETWORK hovorí iba to, že sieťové spojenie je nadviazané – pri zariadení s mobilnou sieťou sa prihlásilo do siete operátora, pri ethernetovom zariadení funguje spojenie po router –, nie však to, že sa zariadenie dostane aj na internet. Ak LED NETWORK svieti nazeleno, ale LED DATA svieti nepretržite aj po udalosti alebo testovacej správe, internetové spojenie nefunguje: správa sa nedá odoslať. V mobilnej sieti je najčastejšie chybné APN alebo dátová služba SIM karty, pri Ethernete router, firewall alebo DNS. Keď LED DATA zhasne, správa odišla a dátové spojenie je v poriadku.

1. Skontroluj adresu prijímača, port, nastavenie TCP/UDP, protokol a šifrovací kľúč (**CMS reporting** → **CMS settings**, bod 6.4.1); kľúč musí byť v komunikátore a v prijímači rovnaký.
2. Pozri nastavenie **Reporting mode** (bod 6.4.2): **Main type** má byť cesta, ktorá je na mieste naozaj dostupná (je zapojený kábel LAN, resp. je karta SIM v zadanom držiaku), a má byť nastavená aj záložná cesta.
3. Ak je prijímač zadaný doménovým menom, skontroluj nastavenie DNS na ceste, ktorou komunikátor hlási (**Network settings** → **LAN**, resp. **SIM1 / SIM2** → **DNS1, DNS2**).
4. Na mobilnej sieti pozri, či dátový balík karty SIM neblokuje potrebný port (niektoré karty M2M povoľujú len určité adresy); na káblovej sieti musí miestny firewall povoliť odchádzajúce spojenie na port prijímača.
5. Ak ústredňa nepošle udalosť (LED DATA sa nerozsvieti), príčina je na strane ústredne: pozri nasledujúci bod.

LED TROUBLE blikne sedemkrát – nie je spojenie s ústredňou

1. Pri pripojení na dátovú zbernicu alebo sériový port skontroluj vodiče CLK a DATA a to, či je v poli **Panel settings** → **Security panel model** vybraný typ pripojenej ústredne (bod 6.3).
2. Pri ústredni Paradox pozri, či nie je sériový port zablokovaný (bod 4.1.2); pri ústredni Texecom a Paradox sa musí **Security panel PC download password** zhodovať s heslom nastaveným v ústredni.
3. Pri pripojení na telefónnu linku má byť vytáčač ústredne zapnutý, v režime DTMF, vo formáte Contact ID, so zadaným telefónnym číslom (bod 4.2), a **Communication protocol** má byť **2. AUTO** (bod 6.3).

Ktorou cestou ide udalosť: cez LAN alebo cez SIM?

Tou, ktorú určuje poradie v **Reporting mode** (bod 6.4.2): cestou podľa **Main type**; ak nefunguje, cestou podľa **Backup type**, potom **Backup type 2**. Ak správa odišla záložnou cestou, komunikátor po uplynutí času **Return from backup after** znova skúsi hlavnú cestu a **Communication path test** v nastavenom intervale vyskúša každú cestu. Spojenie s Protegus 2 používa tú istú cestu. Na káblovej sieti sa mobilné dáta nespotrebúvajú.

Na čo sú dva držiaky SIM?

S kartami dvoch rôznych operátorov bude aj mobilná sieť dvojcestná: v Reporting mode sú SIM1 a SIM2 samostatné typy spojenia, ktorýkoľvek môže byť hlavnou alebo záložnou cestou (bod 6.4.2). Obe karty treba nastaviť samostatne (**Network settings** → **SIM1**, **SIM2**: PIN, APN; bod 6.6.2); chybu SIM2 signalizujú 3 bliknutia LED TROUBLE a správa SIM2_FAILURE (body 1.6 a 6.8). Komunikátor funguje aj s jednou kartou.

DSC: každý poplach prichádza ako všeobecný poplach E130

Keď je pripojený len na Keybus, komunikátor dostáva od ústredne stav zón, ale nie typ zóny, preto hlási každý poplach kódom E130 (bod 3.3.1). Súčasné zapojenie Keybus a TIP/RING GET nemá (to je funkcia GT+). Ak PCO očakáva kód podľa typu zóny (napríklad požiar: E110), pripoj GET len na svorky TIP/RING ústredne a naprogramuj vytáčač (body 3.3.9 a 4.2): tak idú vlastné kódy Contact ID ústredne, ale nie je priame ovládanie – na zapínanie stráženia treba zónu kľúčového spínača (bod 3.4).

Paradox: sériový port je zablokovaný alebo nie je spojenie

Na novších ústredniach Paradox (SP+, MG+, EVOHD+) môže byť sériový port z výroby zablokovaný; o odblokovaní hovorí bod 4.1.2 a článok Odblokovanie zablokovaného sériového portu na ústredniach Paradox. Pri ústredniach Spectra SP / SP+ a Magellan MG / MG+ môžeš namiesto sériového portu použiť aj zapojenie Keybus + TIP/RING (bod 3.3.3), na ktoré netreba odblokovanie, ale komunikátor musí mať firmvér aspoň 1.21 (kapitola 9).

Neviem zapnúť stráženie z Protegus 2

1. Pri priamom ovládaní má byť zaškrtnuté **Panel settings** → **Remote Arm/Disarm** a ústredňa má byť nastavená podľa bodu 4.1 (Paradox: heslo PC, firmvér V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: opísané nastavenia). V tabuľke v bode 1.3 pozri, či sa ústredňa vôbec dá priamo ovládať.
2. Pri zapínaní stráženia kľúčovým spínačom (bod 3.4) má byť svorka na stránke **IN/OUT** nastavená na **OUT** (výrobné nastavenie GET), zóna ústredne má byť zóna kľúčového spínača a v Protegus 2 má byť výstup priradený k partícii, v rovnakom režime ako v ústredni (impulzný alebo dvojpolohový; bod 5.2).
3. Protegus 2 ukazuje stav partície podľa udalostí zapnutia a vypnutia stráženia z ústredne: ústredňa ich musí hlásiť (Opening/Closing).

Protegus 2 nevidí zariadenie

1. Na karte **User reporting** → **PROTEGUS Cloud** má byť zaškrtnuté **Enable connection** (bod 6.5).
2. Pri pridávaní treba zadať **PROTEGUS Cloud access Code** nastavený v zariadení; ak si kód zmenil v TrikdisConfig, prepíš ho aj v aplikácii.
3. IMEI zadaj presne, zo štítku zariadenia alebo z nálepky krabice (alebo načítaj kód QR).
4. Aspoň na jednej ceste musí fungovať internet: LED NETWORK LTE svieti na zeleno a bliká na žlto (karta SIM s mobilnými dátami a správnym APN), alebo LED NETWORK LAN svieti na zeleno (kábel LAN). LED DATA má po udalosti zhasnúť.

Neviem sa na diaľku prihlásiť cez TrikdisConfig

1. Zariadenie má byť online (NETWORK LTE svieti na zeleno a bliká na žlto, alebo NETWORK LAN svieti na zeleno) a spojenie s Protegus má byť povolené (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** nemá byť dlhší ako 5 minút: PING udržiava spojenie potrebné na diaľkový prístup.
3. Skontroluj heslo administrátora alebo inštalátora.

Môžem komunikátor nastaviť z aplikácie?

Áno: s firmvérom 1.08 alebo novším je väčšina nastavení dostupná v ponuke **Settings** → **Advanced settings** v Protegus 2 (bod 2.2 a kapitola 6). Len v TrikdisConfig je: obnovenie výrobných nastavení (bod 6.9), **Preferred operator** (bod 6.6.2) a ručná aktualizácia firmvéru (kapitola 9); prepínač **Event** skupiny Serial bus

aplikácia ukazuje, ale nemení. Po prihlásení kódom inštalátora môžeš meniť len skupiny, ktoré administrátor povolil (bod 6.2).

Zabudol som heslo

V TrikdisConfig sa to nedá, pretože aj obnovenie vyžaduje heslo. Tlačidlom **RESET** na zariadení však áno (bod 6.9): pri zapnutom napájaní ho podrž 10 sekúnd. Všetky nastavenia sa vymažú. Z aplikácie sa obnovenie spustiť nedá.

Koľko dát zariadenie spotrebuje?

Správy o udalostiach a PINGy sú veľmi malé; prevádzka závisí hlavne od periódy PING a od častosti testovacích správ. Pri bežnom systéme v domácnosti zostáva mesačná prevádzka zvyčajne pod 10 MB. Presná hodnota závisí od nastavení a od účtovacej jednotky operátora, preto sa pri karte s dátovým limitom oplatí skontrolovať prevádzku za prvý mesiac. Kým komunikátor hlási po káblovej sieti, dáta karty SIM sa nespotrebúvajú.

11. Bezpečnostné pokyny

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.

- Montáž a údržbu bezpečnostného zariadenia smie robiť len kvalifikovaný technik.
- Pred inštaláciou si prečítaj návod; nedodržanie pokynov môže viesť k nesprávnemu fungovaniu alebo poruche zariadenia.
- Pred zapojením, pri každom elektrickom pripájaní a pred servisom odpoj zariadenie od napájania.
- Úpravy, zmeny a opravy, ktoré výrobca nepovolil, rušia záruku.
- Dodržiavaj miestne predpisy o nakladaní s odpadom: nepoužiteľné zariadenie ani jeho súčasti nevyhadzuj do komunálneho odpadu. Symbol prečiarknutej smetnej nádoby na kolieskach (WEEE) na zariadení znamená, že ho treba odovzdať samostatne ako elektronický odpad.

Pozri aj

- Vyhľadávač kompatibility – ktorý komunikátor Trikdis a aké zapojenie sa hodí k tvojej zabezpečovacej ústredni.
- Komunikátor Trikdis + zabezpečovacia ústredňa DSC: krátky návod pre inštalatéra – kroky zapojenia DSC v skratke.
- Komunikátor Trikdis + zabezpečovacia ústredňa Paradox: krátky návod pre inštalatéra – kroky zapojenia Paradox v skratke.
- DSC Power Series NEO a komunikátory Trikdis: kompatibilita a riešenia – prečo sa NEO nedá pripojiť na dátovú zbernicu a aké je riešenie.

- Odblokovanie zablokovaného sériového portu na ústredniach Paradox – odblokovanie sériového portu ústrední SP+, MG+ a EVOHD+.
- Diaľkové zapínanie stráženia kľúčovým spínačom z aplikácie Protegus 2 – podrobnosti a úskalia zapínania stráženia kľúčovým spínačom.
- Nastavenie APN – zoznam európskych mobilných operátorov – APN operátorov, aj pre karty IoT / M2M.
- Dokumentácia v angličtine: docs.trikdis.com – GET – tu je aj prevodná tabuľka kódov Contact ID → SIA (príloha).

Návody na docs.trikdis.com sú v angličtine.

Súvisiace produkty

Trikdis GET Ethernet + 4G inteligentný komunikátor

Prepojovací kábel Trikdis CRP2 sériového portu pre zabezpečovacie panely Paradox

Trikdis Ant04 GSM Stick anténa s 2,5 m drôtom

Trikdis ME301M Magnetická anténa s 2,5 m drôtom

Autorské práva

Tento návod pripravili trikdis.hu a mobilamb.eu. Jeho text, štruktúra, vlastné obrázky a doplnenia sú naším duševným vlastníctvom a sú chránené autorským právom. Bez nášho súhlasu ho nemožno kopírovať, šíriť ani zverejniť na inej webovej stránke, a to ani celý, ani jeho časti. Na inštaláciu a používanie produktu si ho môžeš voľne stiahnuť a vytlačiť.

Názvy a logá Trikdis a Protegus sú ochranné známky spoločnosti UAB Trikdis.

Vždy aktuálna verzia návodu: https://trikdis.sk/get-navod