Komunikátor G16 – návod pre inštalátora a používateľa

Návod pre inštalátora a používateľa komunikátora Trikdis G16: pripojenie na dátovú zbernicu alebo sériový port zabezpečovacej ústredne, programovanie ústredne, SIM a nastavenie v TrikdisConfig, hlásenie na PCO, aplikácia Protegus 2.



Vydanie: 2026-11-17
Vždy aktuálna webová verzia: https://trikdis.sk/g16-navod

Obsah

1. Prehľad

1.1 Na čo slúži a ako funguje
1.2 Kompatibilné zabezpečovacie ústredne
1.3 Verzie
1.4 Hlavné vlastnosti
1.5 Časti komunikátora
1.6 Svorky
1.7 Signalizácia LED
1.8 Technické údaje

2. Rýchle spustenie s TrikdisConfig

2.1 Príprava
2.2 Typ ústredne a priame ovládanie
2.3 Spojenie s aplikáciou Protegus 2
2.4 Spojenie s PCO

3. Inštalácia a zapojenie

3.1 Postup inštalácie
3.2 Umiestnenie a anténa
3.3 Pripojenie k zabezpečovacej ústredni
3.3.1 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception a Integriti
3.4 Zapojenie zóny kľúčového spínača
3.5 Zapojenie vstupov
3.6 Zapojenie výstupu s relé
3.7 Pripojenie rozširujúceho modulu iO-8
3.8 Pripojenie modulu W485 a E485
3.9 Zapnutie a prvá kontrola
A TRIKDIS átjelző elindítása

4. Programovanie zabezpečovacej ústredne

4.1 DSC
4.2 Paradox
4.3 Texecom
4.4 UTC Interlogix (Caddx)
4.5 Crow a Pyronix
4.6 Honeywell Ademco Vista
4.7 InnerRange Inception a Integriti

5. Ovládanie na diaľku aplikáciou Protegus 2

5.1 Pridanie zariadenia
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Priame ovládanie kódom klávesnice
5.3 Stráženie zónou kľúčového spínača
5.4 Zapínanie a vypínanie z aplikácie
5.5 Ovládanie správami SMS

6. TrikdisConfig – nastavenia podrobne

6.1 Stavový riadok
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 SIM card
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 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

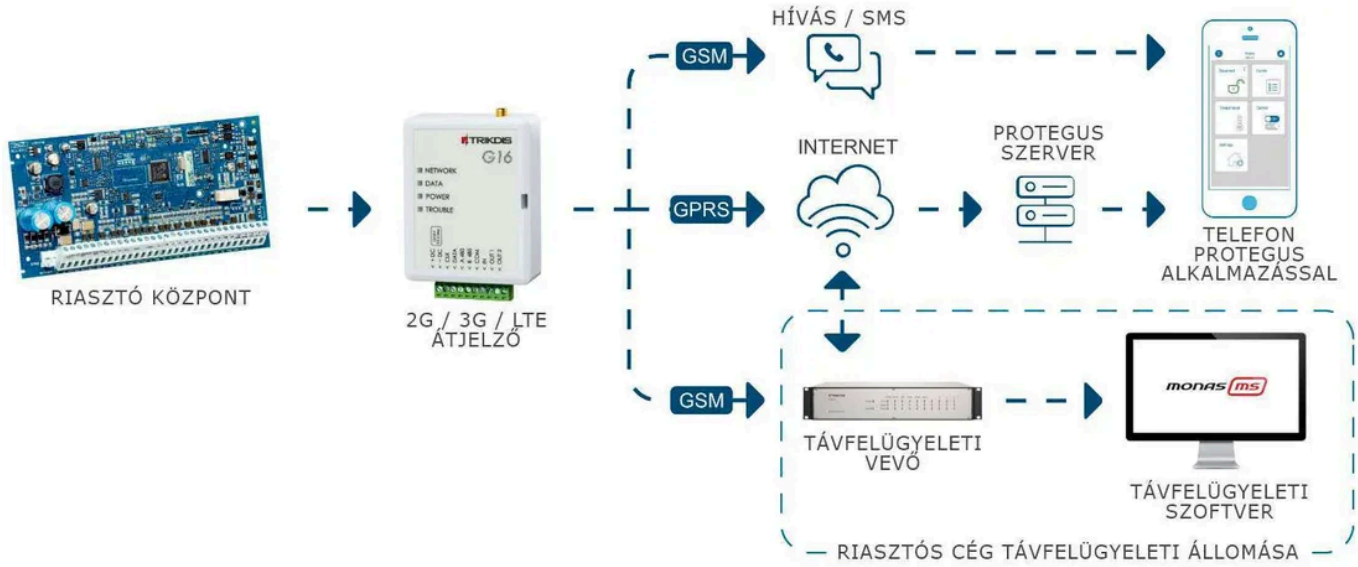
1. Prehľad

G16 je **komunikátor pre mobilnú sieť s priamym pripojením** od Trikdis: nepripája sa na telefónny výstup zabezpečovacej ústredne, ale na **zbernicu klávesnice alebo sériový port** ústredne. Udalosti číta priamo z ústredne – spolu s číslom zóny, partície a používateľa – a cez mobilné dátové spojenie ich posiela prijímaču PCO a do cloudu Protegus, do aplikácie používateľa. Pracuje s podporovanými ústredňami DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell a Crow; pri **priamo ovládateľných** typoch používateľ zapína a vypína stráženie z aplikácie Protegus 2 vlastným kódom klávesnice, bez samostatnej zóny kľúčového spínača. Aplikáciu Protegus 2 môžeš používať so všetkými zabezpečovacími ústredňami, ktoré G16 podporuje, bez ohľadu na výrobcu. K ústredniam iných značiek, ktoré majú len telefónny výstup, je určený komunikátor G16T (TIP/RING).

1.1 Na čo slúži a ako funguje

- **Číta ústredňu priamo.** Na zbernici ústredne sa každá udalosť dostane do komunikátora okamžite, s vlastným číslovaním ústredne; telefónny vytáčač ústredne netreba nastavovať a nie je ani vytáčanie Contact ID.
- **Hlási na PCO.** Udalosti posiela cez IP spojenie softvérovému alebo hardvérovému prijímaču Trikdis (protokol TRK) – tie spolupracujú s ľubovoľným softvérom PCO –, prípadne ľubovoľnému univerzálnemu prijímaču (SIA DC-09 2007/2012, SUR-GARD TL150). Prijímaču SUR-GARD odovzdáva kódy Contact ID z ústredne prevedené na kódy SIA. Spojenie predvolene kontroluje každých 30 sekúnd (alebo v intervale, ktorý nastavíš), a pri chybe prepne na záložný kanál.
- **Upozorňuje používateľa.** Aplikácia Protegus 2 ukazuje, čo sa stalo, v push správe – so samostatným zvukovým signálom podľa udalosti – a v zozname udalostí; používateľ môže z aplikácie zapínať a vypínať stráženie a ovládať pripojené zariadenia (osvetlenie, bránu, vetranie, kúrenie, zavlažovanie atď.). Upozornenie môže dostať aj cez SMS a telefonickým hovorom.
- **Súčasne alebo samostatne** pracuje s PCO a s používateľom: môžeš ho používať len s Protegus 2 (bez PCO), len s PCO, alebo s oboma. Ak sú nastavené obe, udalosť pošle najprv na PCO, potom používateľovi.
- **Záloha cez SMS.** PCO upozorní aj cez SMS, ak dátové spojenie v sieti operátora nefunguje; vie posielať aj dvom prijímačom paralelne, každému s vlastným záložným kanálom.
- **Má vlastné vstupy a výstupy.** Tri svorky I/O s dvojitou funkciou môžeš použiť ako vstupy (detektor, sabotáž) alebo ako ovládateľné výstupy (zóna kľúčového spínača, relé); výstupy môžeš ovládať z aplikácie Protegus 2 aj príkazom SMS. Na zbernici RS485 verzie 4G pridá rozširujúci modul iO-8 ďalších 8 I/O a s modulom W485 alebo E485 vie komunikovať aj cez WiFi, resp. káblové internetové pripojenie – vtedy je mobilná sieť záložnou cestou.

Štruktúru systému ukazuje obrázok nižšie: zbernica zabezpečovacej ústredne sa pripája na G16, G16 sa cez mobilnú sieť dostane na internet, odtiaľ na prijímač PCO a do cloudu Protegus, a používateľ vidí systém v aplikácii Protegus 2.



Obrázok 1. Miesto G16 v systéme: zabezpečovacia ústredňa → G16 → mobilná sieť → prijímač PCO a cloud Protegus → aplikácia Protegus 2. Používateľ môže dostať aj SMS a hovor (GSM), prijímač PCO ako zálohu SMS.

- 1 Zabezpečovacia ústredňa (zbernica klávesnice alebo sériový port)
- 2 Komunikátor G16 (2G / 4G)
- 3 Hovor a SMS pre používateľa
- 4 Mobilné dátové spojenie → internet → cloud Protegus
- 5 Telefón s aplikáciou Protegus 2
- 6 Prijímač PCO
- 7 Softvér PCO (pult centralizovanej ochrany bezpečnostnej firmy)

1.2 Kompatibilné zabezpečovacie ústredne

G16 môžeš pripojiť k ústredniam nižšie. Pri **priamo ovládateľných** typoch sa stráženie zapína a vypína z aplikácie kódom klávesnice; pri ostatných zónou kľúčového spínača (bod 3.4). Na priame ovládanie ústrední Paradox musí mať ústredňa firmvér aspoň **V.4**; na novších typoch Paradox (SP+, MG5050+, EVOHD+) je sériový port z výroby zablokovaný, pred použitím ho treba odblokovať.

Priamo ovládateľné ústredne – udalosti dostáva komunikátor cez dátovú zbernicu alebo sériový port a zakódovanie / odkódovanie funguje bez ďalšej kabeláže:

Výrobca	Pripojenie	Typy
Paradox	sériový port	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* nad firmvérom 7.50)
DSC	dátová zbernica	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	dátová zbernica	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	sériový port	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	dátová zbernica	Ademco Vista-15, Vista-20, Vista-48

Na novších ústredniach Paradox označených * je sériový port z výroby zamknutý; externé zariadenie s ním komunikuje až po odomknutí.

Soros port feloldás útmutató

Ústredne ovládateľné kľúčovým spínačom – udalosti dostáva komunikátor cez dátovú zbernicu alebo sériový port, na ovládanie je potrebné zapojenie a naprogramovanie kľúčového spínača (bod 3.4):

Výrobca	Pripojenie	Typy
Paradox	sériový port	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	dátová zbernica	PC1404, PC5020
Texecom	sériový port	Premier 412, 816, 832, 832+
Inner Range	dátová zbernica	Inception, Integriti
Crow	dátová zbernica	Runner 4/8, 8/16

Zoznam sa občas mení; aktuálny stav nájdeš vo Vyhľadávači kompatibility. Okrem nich ho môžeš použiť aj s ústredňami **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 a MATRIX 816**, **DSC PC5015** a **Paradox DIGIPLEX EVO96 a NE96**. S ústredňami **DSC PowerSeries NEO** G16 nefunguje: na zbernicu NEO výrobca nepovoľuje externé zariadenie, pozri DSC Power Series NEO a komunikátory Trikdis: kompatibilita a riešenia.

1.3 Verzie

Tento návod je pripravený pre **hardvérovú verziu 4** komunikátora G16, ale **môžeš ho použiť aj pre hardvérovú verziu 3**: zapojenie, nastavenie a fungovanie oboch verzií je z väčšej časti rovnaké. Návod platí rovnako pre verziu s modemom 2G, 3G aj 4G. Rozdiely zhŕňa tabuľka nižšie; kde text uvádza údaj verzie 4, pri verzii 3 ber do úvahy tento.

	Hardvér 3 (v3)	Hardvér 4 (v4)
Typy (v TrikdisConfig)	napr. G16_3210 (2G); vyrábala sa aj verzia s modemom 3G a 4G	G16_G410 (2G), G16_54E0 (4G)
Vstupy/výstupy	1 vstup voliteľného typu (IN) + 2 výstupy s otvoreným kolektorom (OUT1, OUT2, max. 0,15 A)	3 svorky I/O s dvojitou funkciou (I/O 1, I/O 2, I/O 3), každú môžeš použiť ako vstup alebo ako výstup s otvoreným kolektorom (max. 0,15 A)
Nastavenie vstupov/výstupov	stránka System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	stránka **IN/OUT** (bod 6.6)
Odber prúdu	100 mA; pri odosielaní najviac 250 mA	60–100 mA; pri odosielaní najviac 500 mA
Zbernica RS485 (iO-8, W485, E485)	len na verzii 3G a 4G	len na verzii 4G (G16_54E0)

Hardvérová verzia 4 sa vyrába s dvoma modemami:

Typ	Modem	Frekvencie	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	nie
G16_54E0	4G (LTE)	pásma LTE podľa regiónu	áno

Hardvérovú verziu nájdeš v stavovom riadku TrikdisConfig (**HW**) a na štítku na zadnej strane zariadenia. O uvedení verzie 4 je samostatný článok: Prichádza hardvérová verzia v4 komunikátorov G16 a G16T.

1.4 Hlavné vlastnosti

Spojenie so zabezpečovacou ústredňou

- Najviac 4 vodičmi (+DC, −DC, CLK, DATA) sa pripája na zbernicu klávesnice ústredne (DSC, Caddx, Crow, Pyronix, Honeywell) alebo na jej sériový port (Paradox, Texecom, InnerRange); k sériovému portu je k dispozícii originálny kábel (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Každú udalosť ústredne odovzdá s úplnou informáciou o udalosti (kód, partícia, zóna alebo používateľ); prerušenie spojenia hlási (LED TROUBLE, udalosť COMMUNICATION).
- Priamo ovládateľné ústredne môžeš z aplikácie zapínať a vypínať kódom klávesnice; Protegus 2 ukazuje aj stav zón.

Komunikácia s PCO

- IP spojenie s prijímačmi Trikdis (softvérový prijímač IPcom, RL14, RM14) a s univerzálnymi prijímačmi (SIA DC-09, TL150).
- Hlavný, záložný a paralelný kanál; záložné upozornenie cez SMS na prijímač SMS Trikdis (RL14, RM14, GM14).
- Šifrovanie správ AES-128; pamäť udalostí 60 správ.

Funkcie pre používateľa

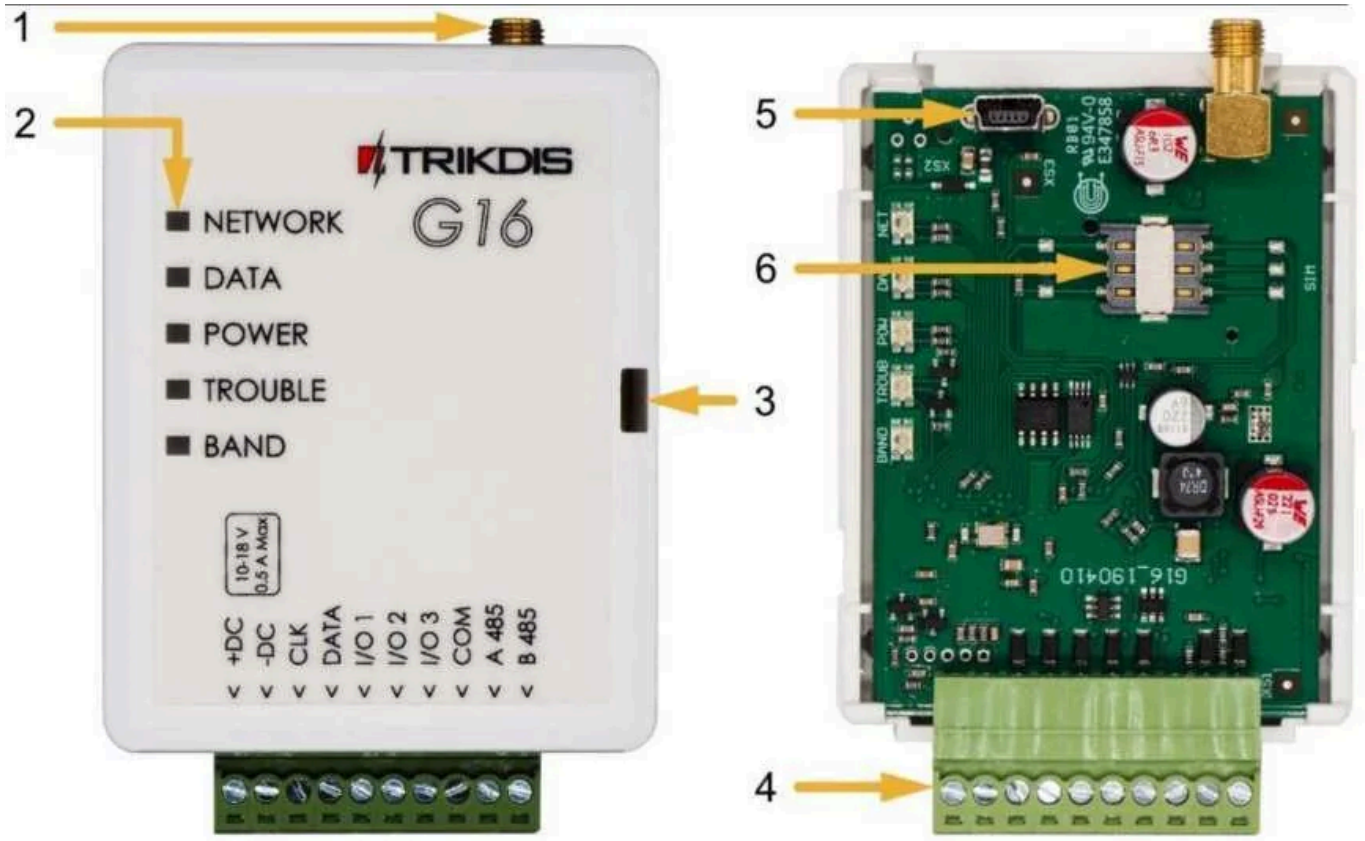
- Mobilná a webová aplikácia Protegus 2: upozornenia, zoznam udalostí, zapínanie a vypínanie stráženia, ovládanie výstupov.
- Ovládanie a základné nastavenie aj príkazmi SMS.
- Upozornenie aj cez SMS a telefonickým hovorom, najviac na 4 telefónne čísla.
- Viacúrovňové používateľské práva v aplikácii (administrátor, inštalátor, používateľ).

Inštalácia a nastavenie

- Nastavenia môžeš uložiť do súboru a nahrať do iného komunikátora.
- Dve úrovne prístupu: administrátor a inštalátor.
- Na diaľku ho môžeš nastaviť a aktualizovať softvérom TrikdisConfig.

1.5 Časti komunikátora

G16 má plošný spoj v bielej plastovej krabičke; predný kryt je odnímateľný, svorkovnica sa dá vytiahnuť. Na obrázku nižšie je verzia 4G; verzia 2G nemá LED BAND ani svorky A 485 / B 485.



Obrázok 2. Časti G16 (verzia 4G) spredu a s otvorenou krabičkou.

- 1 Konektor SMA pre anténu GSM
- 2 Indikačné LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Otvor na uľahčenie zloženia predného krytu
- 4 Odnímateľná svorkovnica
- 5 Zásuvka USB Mini-B na programovanie
- 6 Držiak karty nano-SIM

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.

1.6 Svorky

Svorka	Funkcia
+DC	Napájanie, +10–18 V DC
–DC	Napájanie, záporný pól
CLK	Hodinová / sériová linka zbernice ústredne
DATA	Dátová linka zbernice ústredne
I/O 1	1. výstup/vstup (výrobné nastavenie: nepoužitý)
I/O 2	2. výstup/vstup (výrobné nastavenie: vstup, NO)
I/O 3	3. výstup/vstup (výrobné nastavenie: výstup)
COM	Spoločný (záporný) bod pre vstupy a výstupy
A 485	Vodič A zbernice RS485 (len verzia 4G)
B 485	Vodič B zbernice RS485 (len verzia 4G)

Popis svorkovnice je aj na prednom kryte, preto pri zapájaní nemusíš kryt skladať. Na ktorú svorku ústredne ide CLK a DATA, sa u jednotlivých výrobcov líši – schémy zapojenia sú v bode 3.3.

1.7 Signalizácia LED

LED na prednom kryte sú najdôležitejšou pomôckou pri uvádzaní do prevádzky a hľadaní chýb. Čítaj ich spolu: POWER ukazuje napájanie, NETWORK sieť, TROUBLE chybu a BAND (len 4G) typ siete.

NETWORK – sieťové spojenie

Signál	Význam
nesvieti	Nie je spojenie s mobilnou sieťou
bliká na žlto	Prebieha pripájanie k mobilnej sieti
svieti na zeleno	Pripojený k mobilnej sieti
svieti na zeleno, bliká na žlto	Pripojený; počet žltých bliknutí je **úroveň signálu**: na 2G je dobrý signál 5 bliknutí, na 4G 3 bliknutia

DATA – dátová prevádzka

Signál	Význam
nesvieti	Žiadna správa nečaká na odoslanie
svieti na zeleno	V pamäti sú správy čakajúce na odoslanie
bliká na zeleno	Prebieha odosielanie alebo príjem dát (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

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

TROUBLE – chyba

Signál	Význam
nesvieti	Žiadna chyba
1 červené bliknutie	Chýba SIM karta
2 červené bliknutia	Chyba PIN SIM (nesprávny kód PIN)
3 červené bliknutia	Chyba programovania (chýba APN)
4 červené bliknutia	Nevie sa prihlásiť do mobilnej siete (chyba registrácie)
5 červených bliknutí	Nevie sa pripojiť k dátovej sieti (GPRS/UMTS/LTE)
6 červených bliknutí	Nie je spojenie s prijímačom PCO a/alebo so serverom Protegus (príčinou môže byť aj chyba internetového pripojenia)
7 červených bliknutí	Prerušilo sa spojenie so zabezpečovacou ústredňou (zbernica alebo sériové spojenie)
bliká na červeno (počas programovania)	Chyba pamäte
svieti na červeno (počas programovania)	Poškodený firmvér

BAND – typ siete (len verzia 4G)

Zelené bliknutia	Sieť
1	žiadna
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.8 Technické údaje

Parameter	Hodnota
Spojenie so zabezpečovacou ústredňou	zbernica klávesnice alebo sériový port, podľa typu ústredne (najviac 4 vodiče: +DC, −DC, CLK, DATA; na zbernici Caddx a Pyronix sa CLK nepoužíva)
Vstupy/výstupy	3 I/O s dvojitou funkciou (I/O 1, I/O 2, I/O 3): 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
Rozšírenie	na zbernici RS485 (len verzia 4G): rozširujúci modul iO-8 (+8 I/O) a ďalšie rozširujúce moduly série iO; modul W485 WiFi, E485 Ethernet
Modem 2G	850 / 900 / 1800 / 1900 MHz
Modem 4G	pásma LTE podľa regiónu
Napájacie napätie	10–18 V DC
Odber prúdu	60–100 mA menovitý; najviac 500 mA pri odosielaní
Prenosové protokoly	TRK, DC-09_2007, DC-09_2012, TL150

Parameter	Hodnota
Pamäť udalostí	60 správ
Šifrovanie	AES-128
Programovanie	TrikdisConfig (Windows) káblom USB Mini-B alebo na diaľku; príkazy SMS
Prevádzkové prostredie	−10 … +50 °C, max. 80 % relatívnej vlhkosti (pri +20 °C)
Rozmery	92 × 65 × 26 mm
Hmotnosť	80 g

2. Rýchle spustenie s TrikdisConfig

Všetky nastavenia G16 sa robia programom **TrikdisConfig**, ktorý beží vo Windows – cez kábel USB alebo na diaľku. V tejto kapitole opisujeme najkratšiu cestu: zariadenie nastavíš na stole ešte pred zapojením, potom ho na mieste už len zapojíš. Podrobné vysvetlenie nastavení obsahuje kapitola 6.

2.1 Príprava

Čo budeš potrebovať

Kábel USB Mini-B · aspoň 4-žilový kábel k zbernici ústredne – k sériovému portu Paradox kábel **CRP2** alebo **CRP2B**, k sériovému portu Texecom kábel **CRP4** · plochý skrutkovač 2,5 mm · mobilná anténa s vhodným ziskom (na mieste so slabým pokrytím anténa s väčším ziskom) · aktívna karta nano-SIM s mobilnými dátami (požiadavku na PIN môžeš vypnúť) · inštalačný návod zabezpečovacej ústredne. Potrebné príslušenstvo treba objednať samostatne u predajcu.

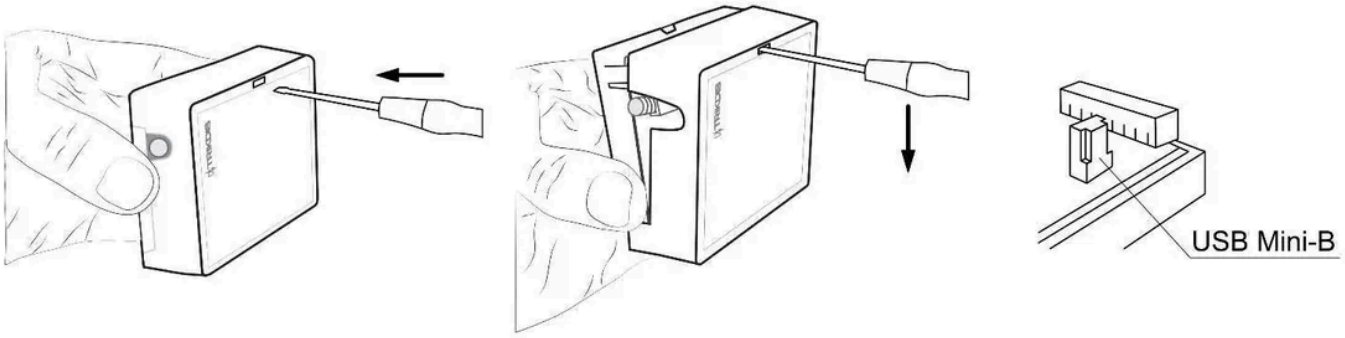
1. Stiahni a nainštaluj softvér TrikdisConfig. Na webe výrobcu (www.trikdis.com) zadaj do vyhľadávacieho poľa: „TrikdisConfig".

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

TrikdisConfig Letöltés a trikdis.com oldalról.

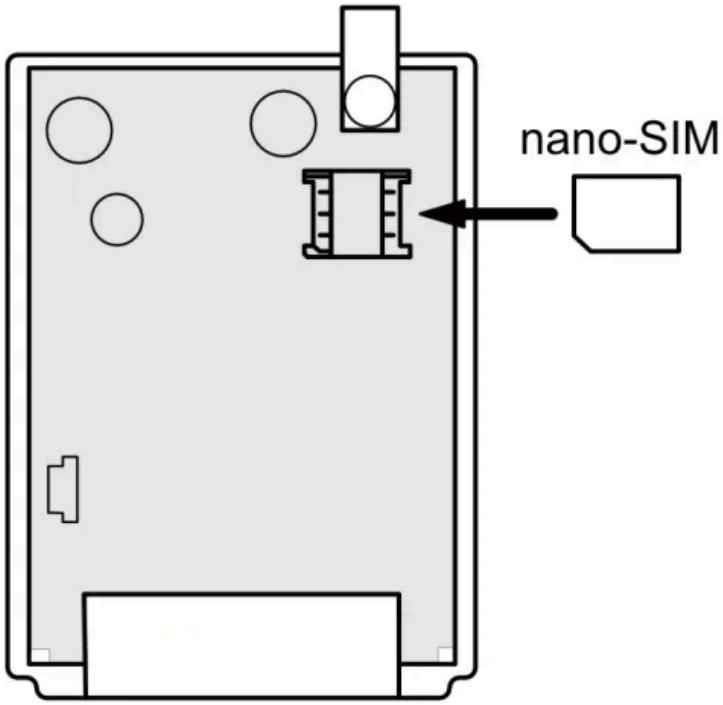
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Otvor predný kryt G16. Plochý skrutkovač zasuň do otvoru na hornej hrane krytu a páčením smerom nadol jemne odpoj predný kryt. Obrázok nižšie ukazuje otváranie a miesto zásuvky USB.



Obrázok 3. Odpojenie predného krytu plochým skrutkovačom (vľavo, v strede) a miesto zásuvky USB Mini-B na plošnom spoji (vpravo).

3. Vlož kartu nano-SIM do držiaka v smere, ktorý ukazuje obrázok. 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).



Obrázok 4. Miesto karty nano-SIM na plošnom spoji.

4. Prepoj G16 s počítačom káblom USB Mini-B. USB dáva na programovanie dostatočné napájanie, samostatný zdroj netreba.

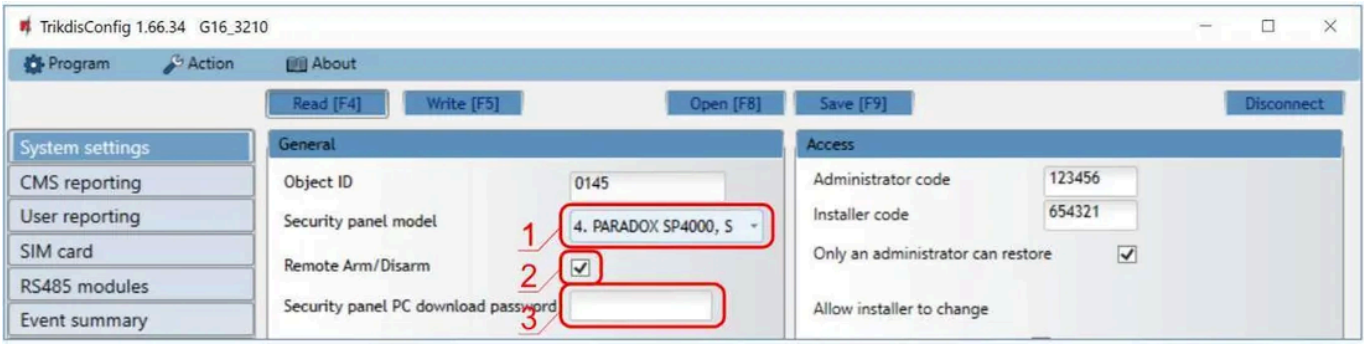
Upozornenie

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`).

2.2 Typ ústredne a priame ovládanie

Nech používaš ktorýkoľvek režim, najprv na stránke **System settings** zadaj, na akú ústredňu sa komunikátor pripojí.



Obrázok 5. TrikdisConfig – stránka System settings, skupina General.

- 1 **Security panel model** – typ pripojenej zabezpečovacej ústredne zo zoznamu; od neho závisí, ako komunikátor číta zbernicu.
- 2 **Remote Arm/Disarm** – zaškrtni, ak chce používateľ zapínať a vypínať stráženie ústredne z aplikácie Protegus 2 vlastným kódom klávesnice. Zobrazí sa len pri priamo ovládateľných typoch; pri ostatných ústredniach sa stráženie rieši zónou kľúčového spínača (bod 3.4) – vtedy ho nechaj prázdne.
- 3 **Security panel PC download password** – pri ústredni Paradox a Texecom heslo PC, resp. UDL ústredne (4 znaky); musí sa zhodovať s heslom nastaveným v ústredni. Pole sa zobrazí po zaškrtnutí Remote Arm/Disarm.

Pri viacerých ústredniach treba nastavenie aj v ústredni: pri ústredni Caddx, Honeywell a InnerRange už na čítanie udalostí (povolenie zbernice, resp. sériového portu), pri ústredni Paradox a Texecom na priame ovládanie (heslo PC, resp. UDL) – kapitola 4 to opisuje pre každého výrobcu, aj so zmenou hesla.

2.3 Spojenie s aplikáciou Protegus 2

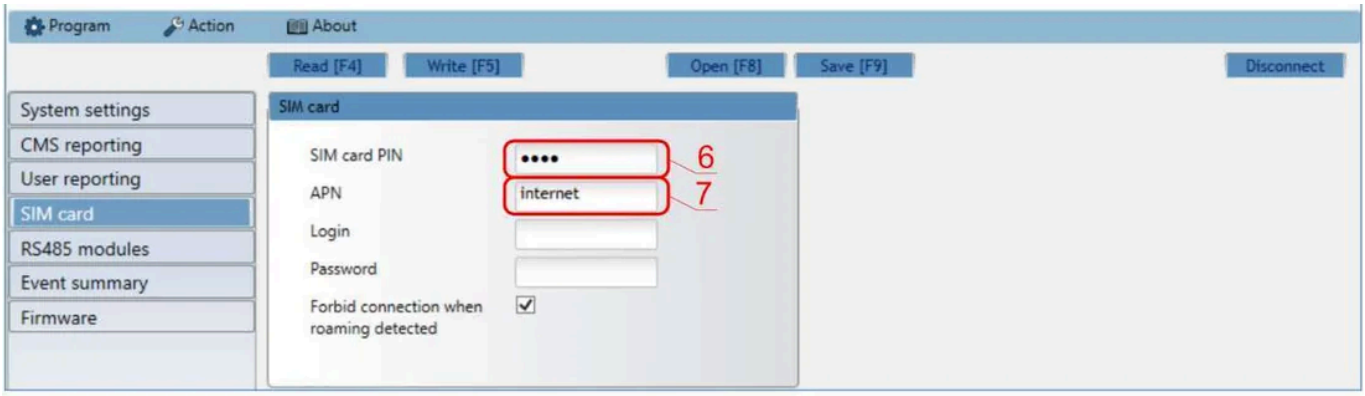
Ak chce používateľ vidieť a ovládať systém z aplikácie Protegus 2, na stránke **User reporting**, na záložke **PROTEGUS Cloud** nastav nasledujúce.



Obrázok 6. TrikdisConfig – User reporting, záložka PROTEGUS Cloud.

- 4 **Enable connection** – zaškrtni: povolí spojenie s cloudom Protegus.
- 5 **Protegus Cloud access code** – zmeň výrobné heslo `123456`. Toto heslo bude treba zadať v aplikácii pri vytváraní systému; **po vytvorení systému ho už nemožno zmeniť.**

Potom na stránke **SIM card** zadaj údaje karty.



Obrázok 7. TrikdisConfig – stránka SIM card.

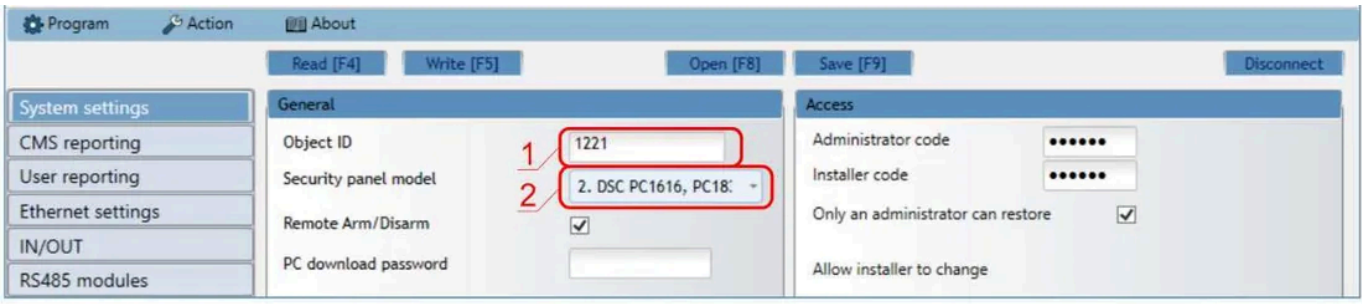
- 6 **SIM card PIN** – kód PIN karty (ak je požiadavka na PIN vypnutá, môže zostať výrobná hodnota).
- 7 **APN** – prístupový bod dátového spojenia operátora (pozri nižšie).

APN (Access Point Name) je prístupový bod dátového spojenia mobilného operátora; bez neho sa zariadenie nevie pripojiť na internet. Presnú hodnotu dostaneš od operátora SIM karty a nájdeš ju aj na jeho webe; APN „internet" je všeobecný, funguje v sieti mnohých operátorov. Známe APN európskych operátorov vedieme v samostatnom článku: Nastavenie APN – zoznam európskych mobilných 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.

2.4 Spojenie s PCO

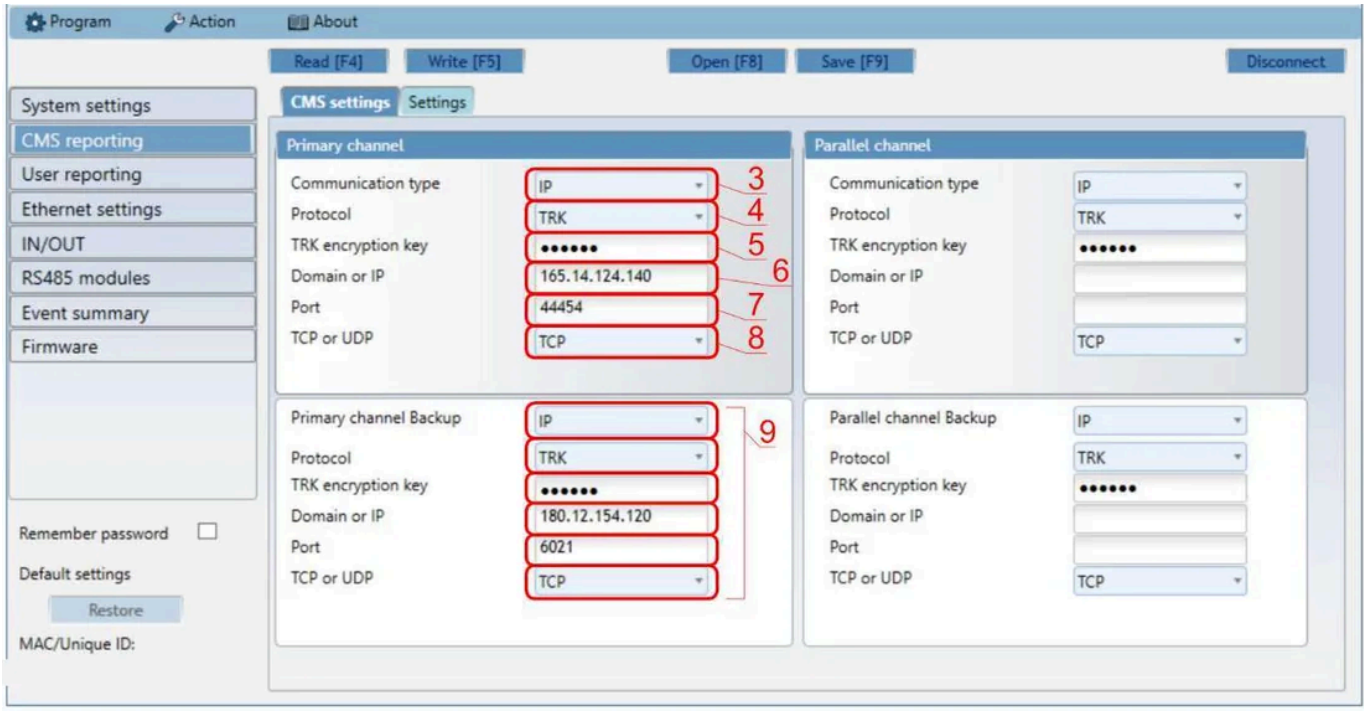
Ak zariadenie hlási aj na prijímač PCO, na stránke **System settings** zadaj aj identifikátor objektu.



Obrázok 8. TrikdisConfig – stránka System settings, skupina General.

- 1 **Object ID** – identifikátor objektu, ktorý dostaneš od PCO (4 hexadecimálne znaky, 0–9, A–F). `FFFE` a `FFFF` nemožno použiť.
- 2 **Security panel model** – typ pripojenej zabezpečovacej ústredne (ak si ho ešte nenastavil v bode 2.2).

Potom na stránke **CMS reporting**, v časti **Primary channel** (hlavný kanál) nastav údaje prijímača.

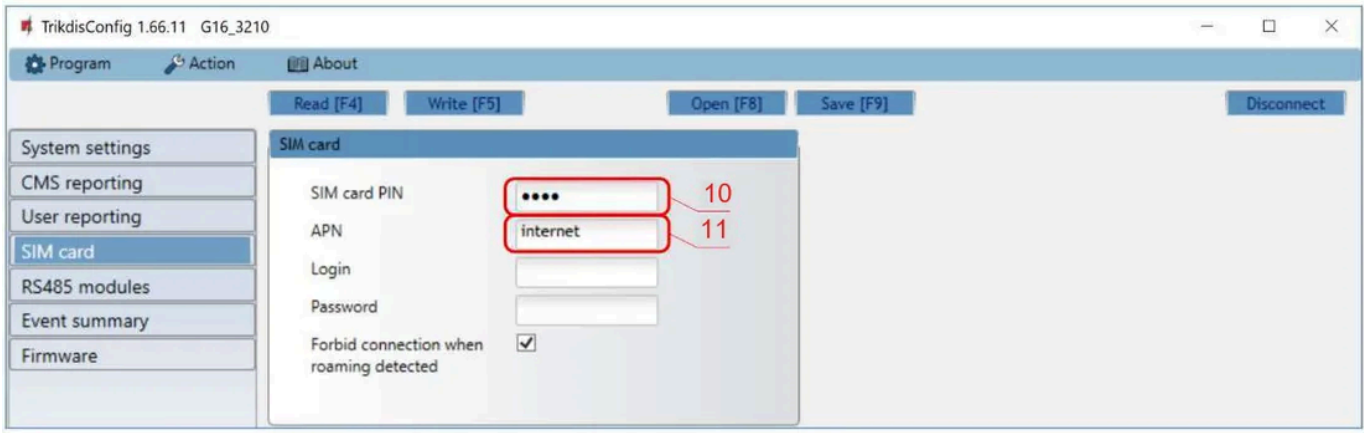


Obrázok 9. TrikdisConfig – CMS reporting, záložka CMS settings.

- 3 **Communication type** – zvoľ spojenie **IP** (SMS sa ako hlavný kanál neodporúča).
- 4 **Protocol** – **TRK** pre prijímač Trikdis, **DC-09_2007** alebo **DC-09_2012** pre univerzálny prijímač, **TL150** pre prijímač SUR-GARD.
- 5 **TRK encryption key** – 6-miestny šifrovací kľúč nastavený v prijímači.
- 6 **Domain or IP** – doménové meno alebo IP adresa prijímača.
- 7 **Port** – číslo portu prijímača.
- 8 **TCP or UDP** – protokol prenosu; prispôsob ho nastaveniu prijímača.
- 9 **Primary channel Backup** – záložný kanál pre prípad chyby hlavného; vyplň ho rovnako, odporúča sa ho zadať.

Odporúča sa nastaviť aj **Parallel channel** (paralelný kanál) a jeho záložný kanál, ak majú udalosti dostať dva prijímače; do poľa **Backup SMS reporting number** – aj to sa odporúča – môžeš zadať telefónne číslo prijímača SMS Trikdis: zariadenie sem po prvom spustení hneď pošle SMS a potom hlási cez SMS vtedy, keď nefunguje ani jeden kanál IP.

Nakoniec na stránke **SIM card** zadaj údaje karty, ak si to ešte neurobil v bode 2.3.



Obrázok 10. TrikdisConfig – stránka SIM card.

- 10 **SIM card PIN** – kód PIN karty.
- 11 **APN** – prístupový bod operátora (pozri bod 2.3).

Hlásenie cez SMS na PCO funguje len s prijímačom Trikdis (prijímač IP/SMS RL14, viackanálový prijímač RM14 alebo prijímač SMS GM14); vtedy treba len šifrovací kľúč a telefónne číslo. Pri protokole **DC-09** zadaj na záložke **Settings** aj číslo objektu, linky a prijímača DC-09.

Na konci nastavení stlač tlačidlo **Write [F5]** (zápis), počkaj na potvrdenie a vytiahni kábel USB. Zariadenie je tým pripravené na zapojenie.

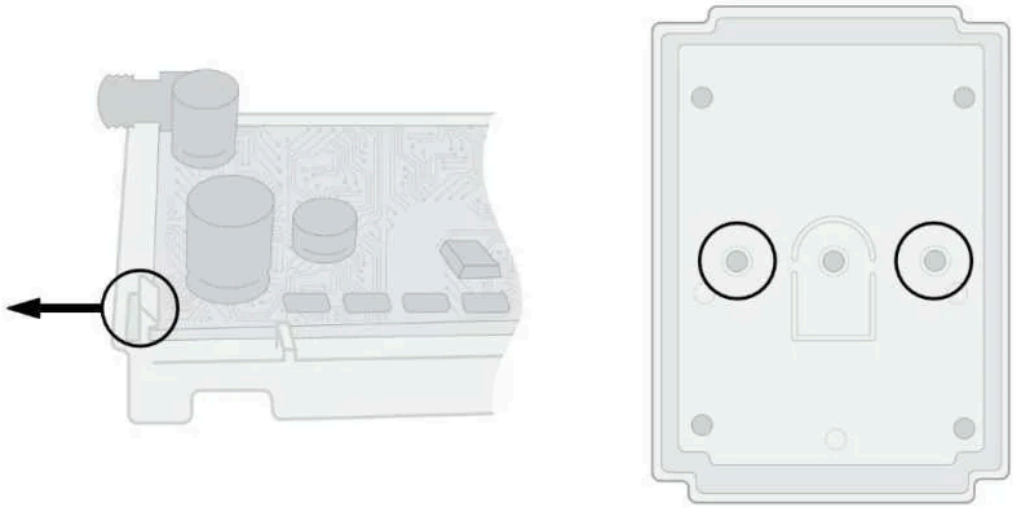
3. Inštalácia a zapojenie

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, ak si to ešte neurobil pri uvádzaní do prevádzky.
3. Vyber plošný spoj zo zadného dielu: otvor západku v rohu (pozri obrázok).
4. Zadný diel pripevni skrutkami na zvolené miesto.
5. Vlož plošný spoj späť do zadného dielu a zasuň späť svorkovnicu.
6. Naskrutkuj anténu GSM.
7. Nasaď späť predný kryt.



Obrázok 11. Vybratie plošného spoja: otvorenie západky v rohu (vľavo) a upevňovacie otvory zadného dielu (vpravo, zakrúžkované).

SIM karta má byť aktívna a na použitie cez IP na nej musí fungovať mobilné dátové spojenie. Ak nechceš, aby TrikdisConfig pýtal kód PIN, vypni požiadavku na PIN na karte v telefóne.

3.2 Umiestnenie a anténa

- Komunikátor umiestni na **suché miesto vo vnútri**, podľa možnosti blízko krabice zabezpečovacej ústredne, aby bol vodič zbernice krátky.
- **V kovovej krabici** sa mobilný signál výrazne oslabí. Ak komunikátor ide do kovového krytu ústredne, anténu vyveď mimo krabice alebo použi anténu s dlhším káblom.

- Pred definitívnym upevnením **skontroluj úroveň signálu**: počet žltých bliknutí LED NETWORK má byť na 2G aspoň 5, na 4G aspoň 3 (pozri bod 1.7). Ak je ich menej, hľadaj lepšie miesto alebo prejdi na citlivejšiu anténu, ktorú môžeš umiestniť ďalej.
- Anténu a komunikátor drž ďalej od transformátora ústredne a od sieťových vodičov.



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

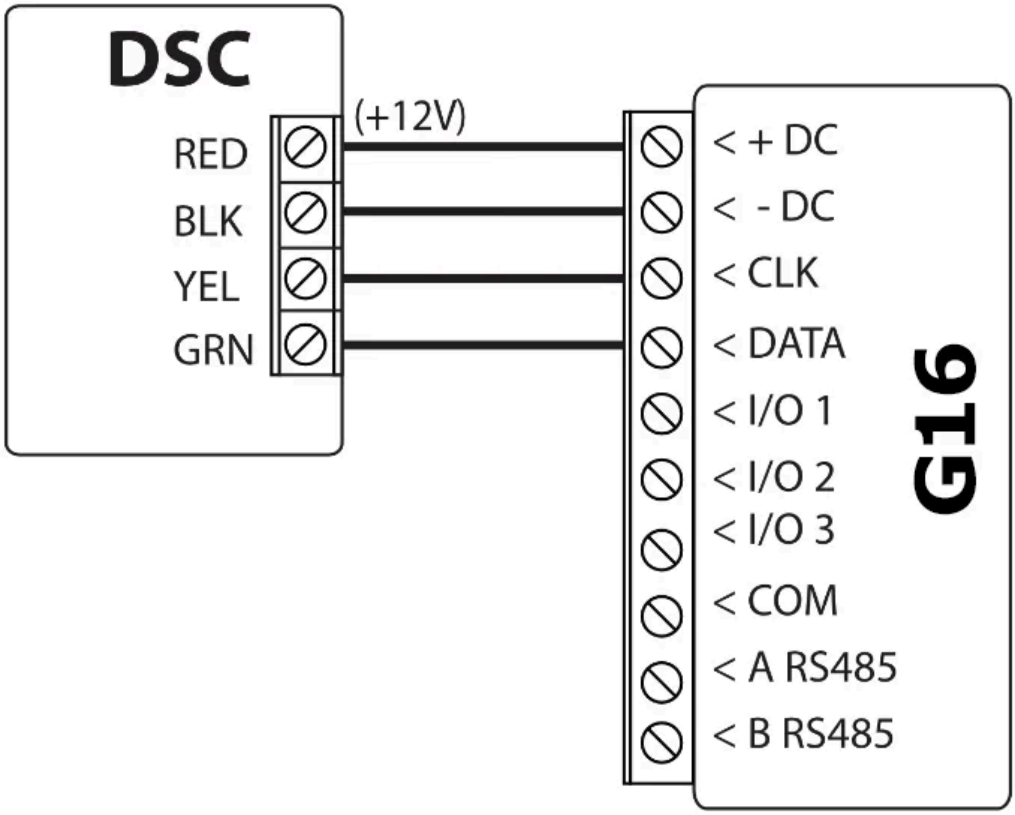
G16 sa k ústredni pripája **najviac štyrmi vodičmi** (na zbernici Caddx a Pyronix sa CLK nepoužíva): na svorky **+DC** a **−DC** ide 12 V pomocné napájanie ústredne (AUX), na svorky **CLK** a **DATA** dva dátové vodiče zbernice klávesnice alebo sériového portu ústredne. Ktorá svorka ústredne je ktorá, sa u jednotlivých výrobcov líši – zapájaj podľa schém nižšie. K ústredniam so sériovým portom (Paradox, Texecom) je k dispozícii originálny kábel, ktorého jeden koniec pasuje do konektora ústredne a druhý koniec sa zapája do svorkovnice G16.

G16 môže pri odosielaní odoberať až 500 mA. Over, či to výstup AUX ústredne zvládne spolu s ostatnými pripojenými zariadeniami. Keďže napájanie dáva ústredňa, pri výpadku prúdu napája akumulátor ústredne aj komunikátor. Väčšina ústrední zariadeniu na zbernici pri prehodených vodičoch neublíži, ale prehodenie **+DC a −DC** môže komunikátor zničiť – pred zapojením skontroluj polaritu.

Po zapojení treba v TrikdisConfig v poli **System settings → Security panel model** zvoliť typ zapojenej ústredne (bod 2.2); pri niektorých výrobcoch treba nastavenie aj v ústredni (kapitola 4).

3.3.1 DSC PowerSeries

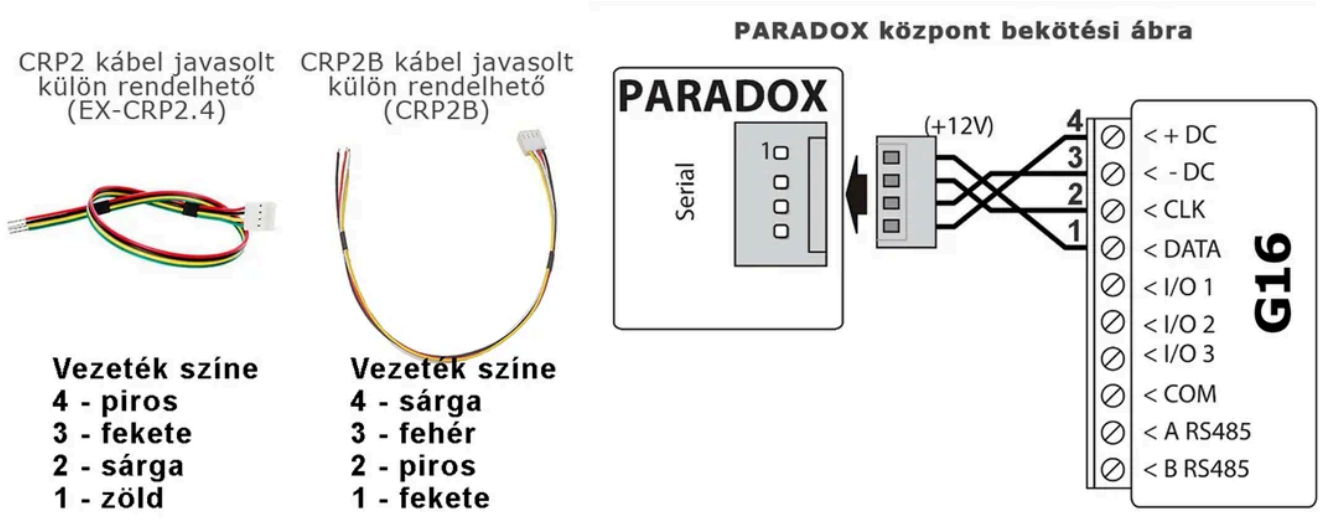
Štyri svorky Keybusu: **RED** → +DC, **BLK** → −DC, **YEL** → CLK, **GRN** → DATA.



Obrázok 12. Pripojenie na Keybus ústredne DSC PowerSeries (zbernica klávesnice, „Keypad bus"): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Na **sériový port** (SERIAL) ústrední Paradox sa komunikátor pripája originálnym káblom **CRP2** alebo **CRP2B**; koniec kábla na strane ústredne pasuje do sériového konektora, druhý koniec zapojíš do svorkovnice G16. 4 kolíky konektora: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Farby žíl oboch káblov sa líšia – schéma ukazuje farebné priradenie oboch káblov. Označenie sériového konektora Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

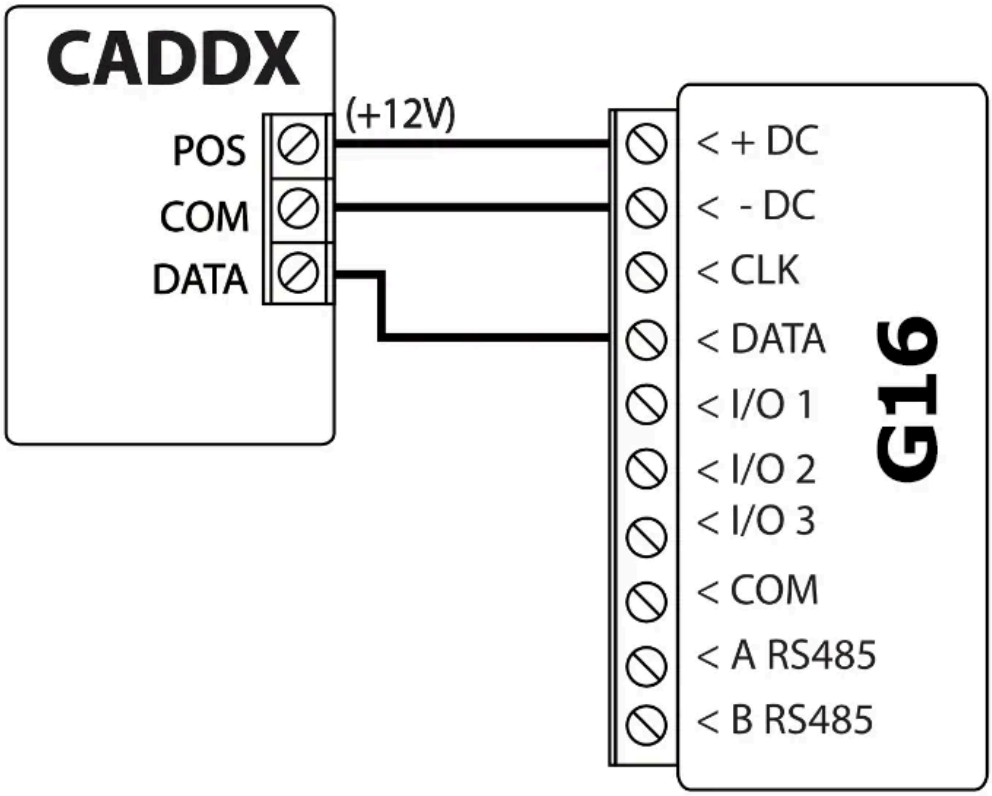


Obrázok 13. Pripojenie na sériový port ústredne Paradox káblom CRP2 (EX-CRP2.4), resp. CRP2B. CRP2: 4 červená → +DC, 3 čierna → −DC, 2 žltá → CLK, 1 zelená → DATA. CRP2B: 4 žltá → +DC, 3 biela → −DC, 2 červená → CLK, 1 čierna → DATA.

Na novších ústredniach Paradox môže byť sériový port z výroby zablokovaný – postup odblokovania je v bode 4.2 a v článku Odblokovanie zablokovaného sériového portu na ústredniach Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

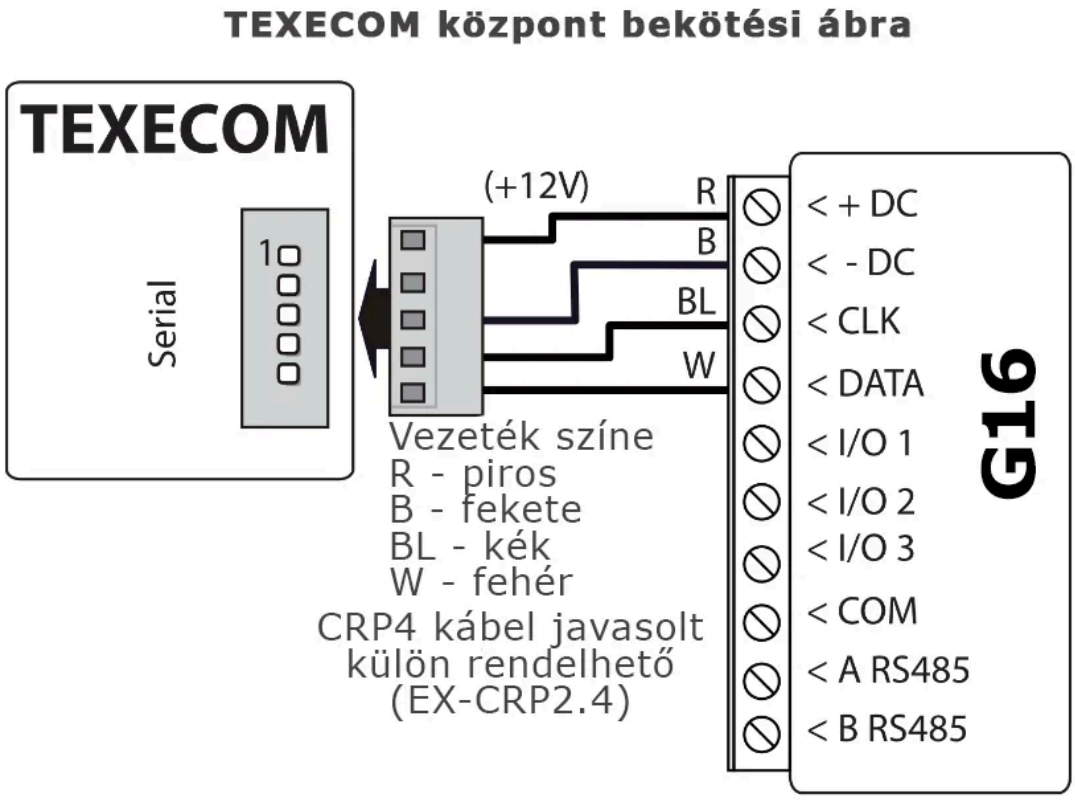
Tri svorky zbernice klávesnice: **POS** → +DC, **COM** → −DC, **DATA** → DATA. Svorka **CLK** sa nepoužíva.



Obrázok 14. Pripojenie na zbernicu klávesnice ústredne Caddx NetworX („Keypad bus"): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK zostáva voľná.

3.3.4 Texecom Premier / Premier Elite

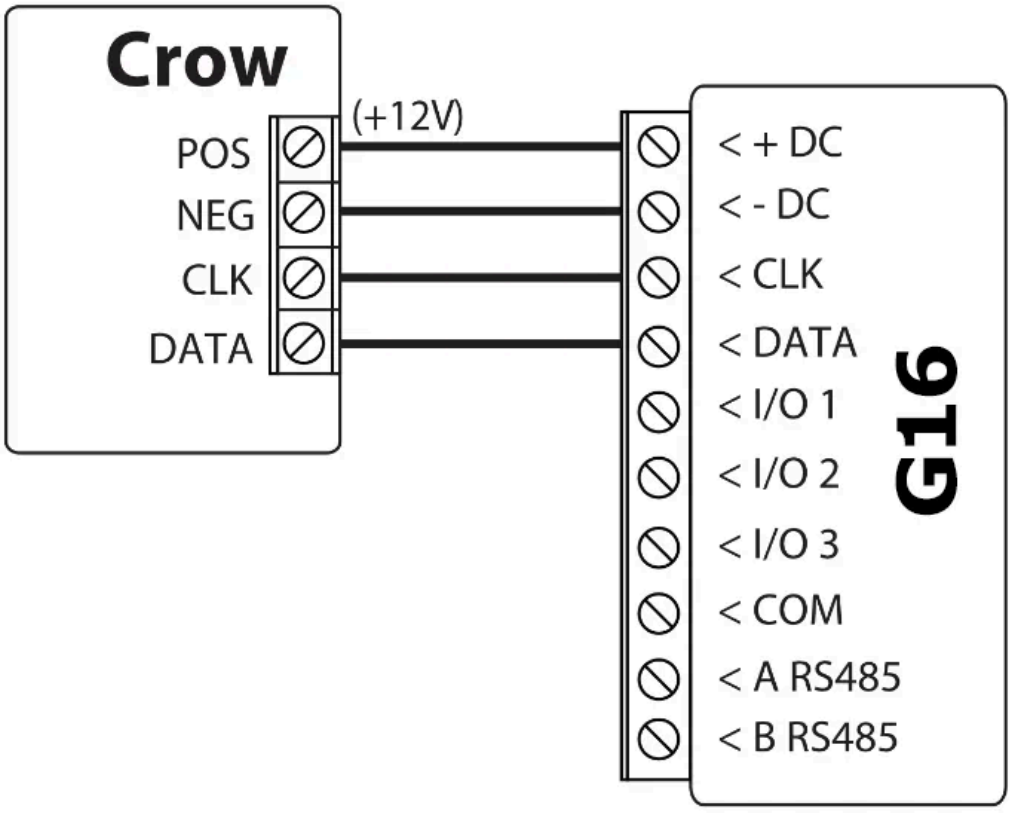
Na sériový port ústredne sa komunikátor pripája originálnym káblom **CRP4**: **červená (R)** → +DC, **čierna (B)** → −DC, **modrá (BL)** → CLK, **biela (W)** → DATA.



Obrázok 15. Pripojenie na sériový port ústredne Texecom káblom CRP4: červená → +DC, čierna → −DC, modrá → CLK, biela → DATA.

3.3.5 Crow Runner

Zbernica klávesnice Crow Runner 4/8 a Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.



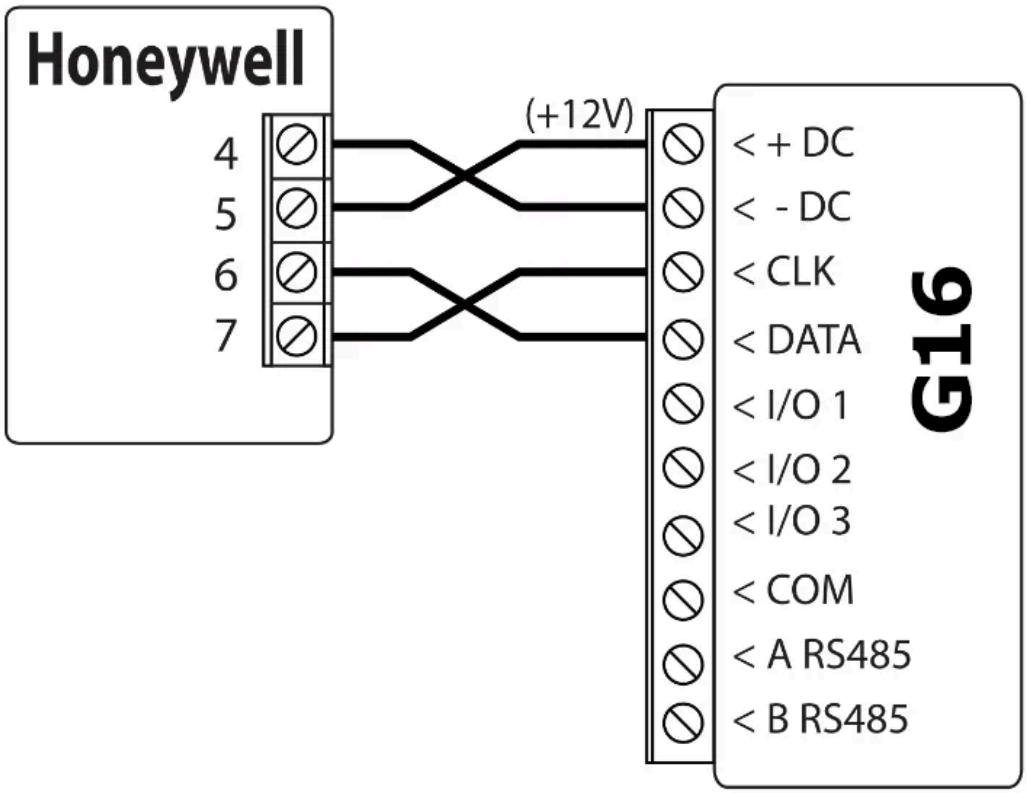
Obrázok 16. Pripojenie na zbernicu klávesnice ústredne Crow Runner 4/8 a Runner 8/16 („Keypad bus"): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Zbernica klávesnice ústrední Pyronix: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. Svorka **CLK** sa nepoužíva. Po zapojení a nastavení komunikátora ústredňu odpoj od napájania a znova spusti, aby komunikátor prijala (bod 4.5).

3.3.7 Honeywell Ademco Vista

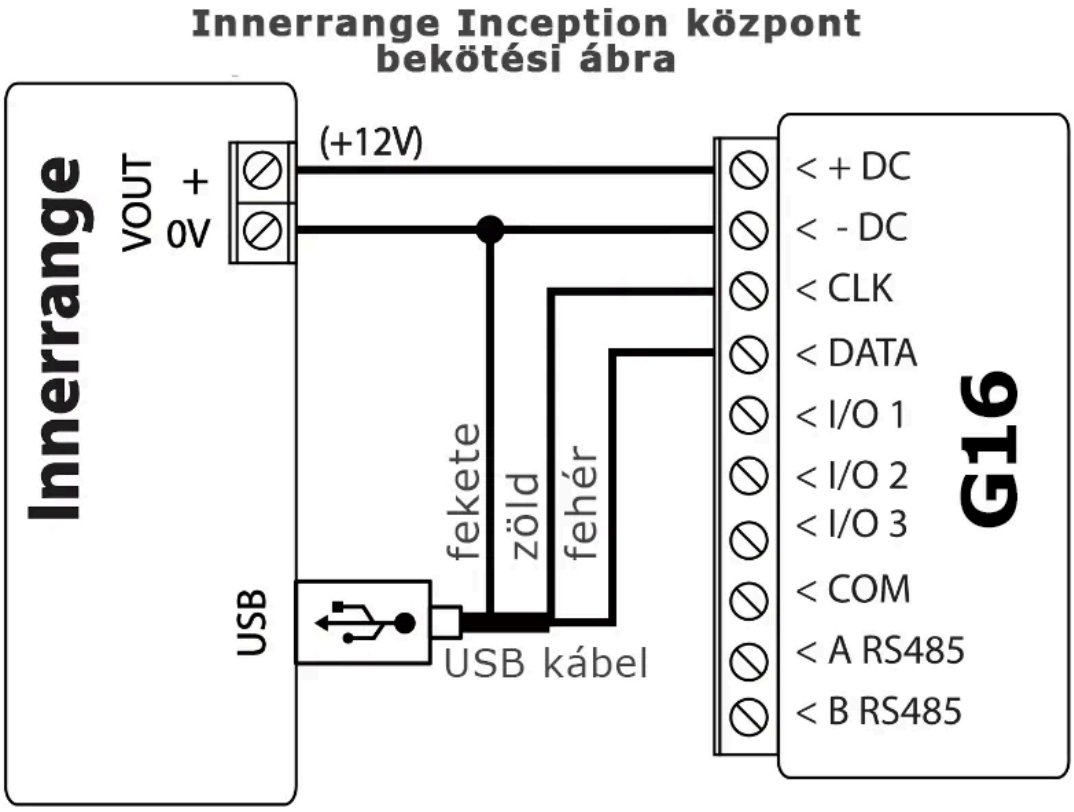
Číslované svorky zbernice klávesnice ústredne Vista-15, Vista-20 a Vista-48: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (dátový výstup, žltý) → CLK, **6** (dátový vstup, zelený) → DATA.



Obrázok 17. Pripojenie na zbernicu klávesnice ústredne Honeywell Vista-20 / Vista-48 („Keypad bus"): 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception a Integriti

Komunikátor dostáva napájanie z napájacích svoriek ústredne **Inception** (**VOUT +** → +DC, **0V** → −DC) a dátové spojenie sa robí z portu USB ústredne káblom InnerRange 993030USB: **čierna** → 0V (−DC), **zelená** → CLK, **biela** → DATA. V ústredni treba povoliť použitie sériového portu (bod 4.7).

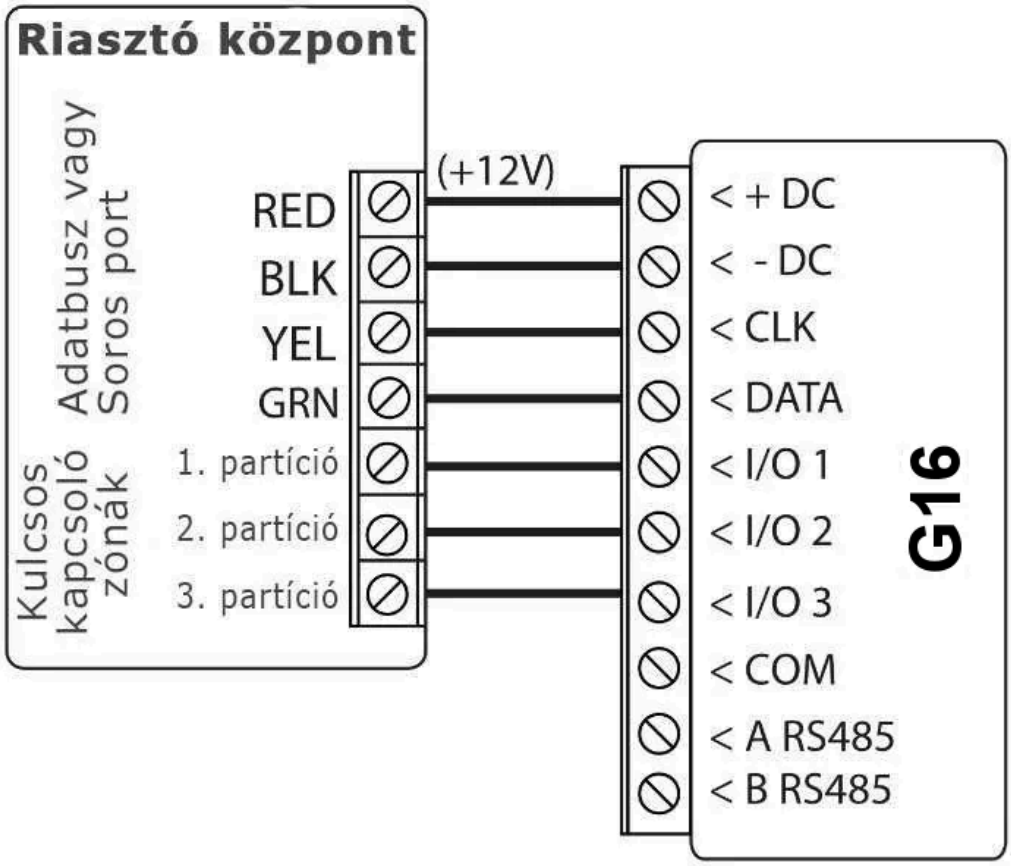


Obrázok 18. Pripojenie k ústredni InnerRange Inception: napájanie zo svoriek VOUT + a 0V, dáta z portu USB káblom 993030USB (čierna → 0V, zelená → CLK, biela → DATA).

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

3.4 Zapojenie zóny kľúčového spínača

Ak ústredňa nepatrí medzi priamo ovládateľné typy alebo priame ovládanie nechceš používať, zapínanie a vypínanie stráženia na diaľku vyriešiš **zónou kľúčového spínača**: jednu svorku I/O komunikátora nastavíš ako **výstup** (stránka IN/OUT, bod 6.6) a pripojíš ju na zónu kľúčového spínača ústredne. Výstup pri aktivácii stiahne zónu na COM (záporný pól); zakončovací odpor zóny zapoj podľa typu zóny ústredne. Keďže G16 má tri svorky I/O, môžeš samostatným výstupom ovládať až tri partície.



Obrázok 19. Zapínanie a vypínanie stráženia zónou kľúčového spínača: komunikátor číta udalosti zo zbernice ústredne a výstupy I/O 1–3 spínajú zónu kľúčového spínača 1.–3. partície ústredne.

- Na stránke **System settings** v TrikdisConfig nechaj **Remote Arm/Disarm prázdne** – obe naraz použiť nemožno.
- Zóna kľúčového spínača môže byť impulzná alebo dvojpolohová; v aplikácii Protegus 2 treba nastaviť ten istý režim (bod 5.3).
- Na **hardvérovej verzii 3** môžu dva výstupy (OUT1, OUT2) ovládať dve partície; pole **System settings → Output OUT1 & OUT2 mode** má byť v polohe **Remote control** (výrobné nastavenie).

O podrobnostiach a úskaliach zapínania stráženia kľúčovým spínačom je samostatný článok: Zapínanie stráženia na diaľku kľúčovým spínačom z aplikácie Protegus 2.

3.5 Zapojenie vstupov

Svorky I/O komunikátora môžeš ako vstupy použiť aj na pripojenie ďalších detektorov (napr. sabotážny spínač, panické tlačidlo, teplotný spínač), nezávisle od zabezpečovacej ústredne. Vstup treba zapojiť medzi zvolenú svorku I/O a svorku COM.

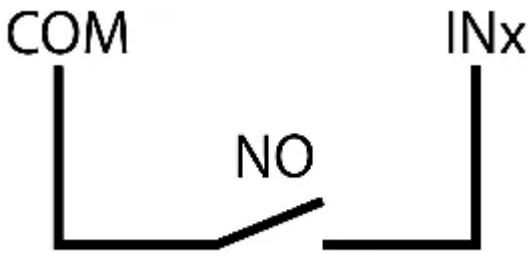
Vstupy prijímajú tieto typy obvodov: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. Zakončovací odpor je **2,2 kΩ**. Pri jednoduchom zakončení (EOL) sa skrat aj prerušenie považujú za poplach; dvojité zakončenie (DEOL) s dvoma odpormi rozlišuje poplach a sabotáž (skrat alebo prerušenie) 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	–

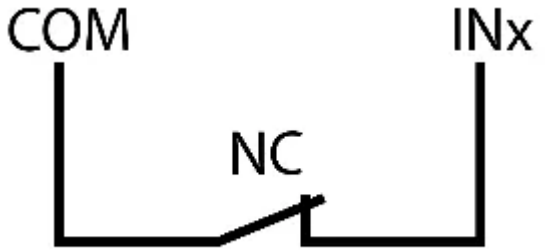
Typ	Kľudový stav	Poplach	Sabotáž
NC/EOL	2,2 kΩ	prerušenie alebo skrat	–
NO/EOL	2,2 kΩ	skrat alebo prerušenie	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	prerušenie alebo skrat
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	prerušenie alebo skrat

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**.

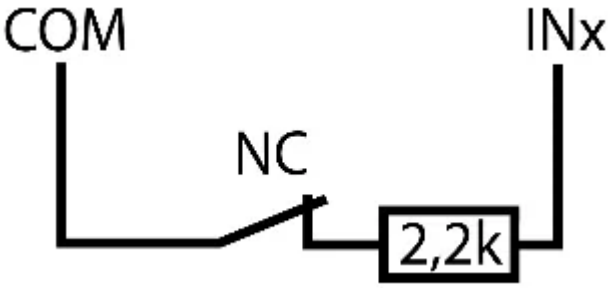
Zapojenie vstupných obvodov: typ NO, NC, NC/EOL, NO/EOL, NO/DEOL a NC/DEOL so zakončovacím odporom 2,2 kΩ; pri typoch DEOL je zapojený aj sabotážny obvod.



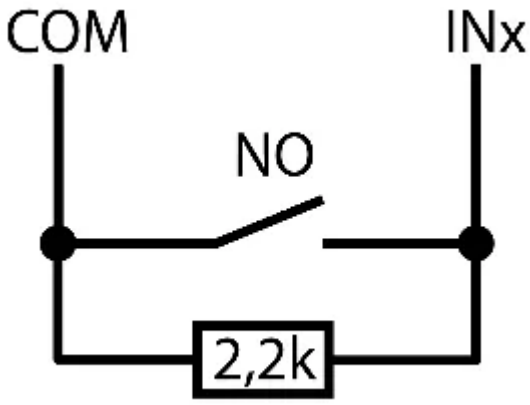
Obrázok 20. NO – v pokoji rozpojený obvod: zopnutý – poplach, rozpojený – pokojový stav.



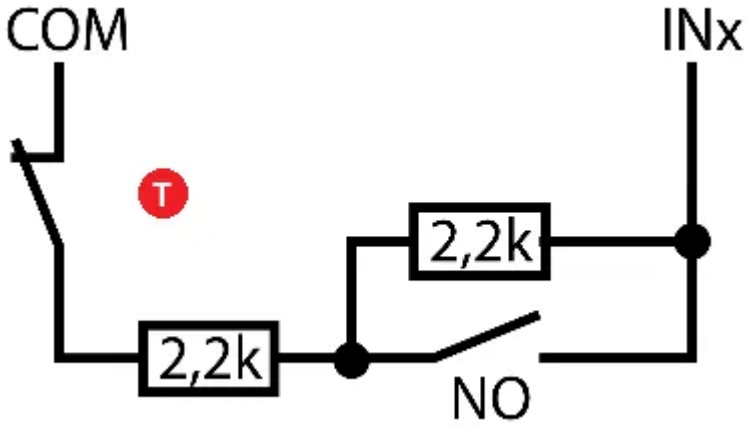
Obrázok 21. NC – v pokoji zopnutý obvod: rozpojený – poplach, zopnutý – pokojový stav.



Obrázok 22. NC/EOL – v pokoji zopnutý obvod so zakončovacím odporom 2,2 kΩ: skrat alebo prerušenie – poplach, 2,2 kΩ – pokojový stav.

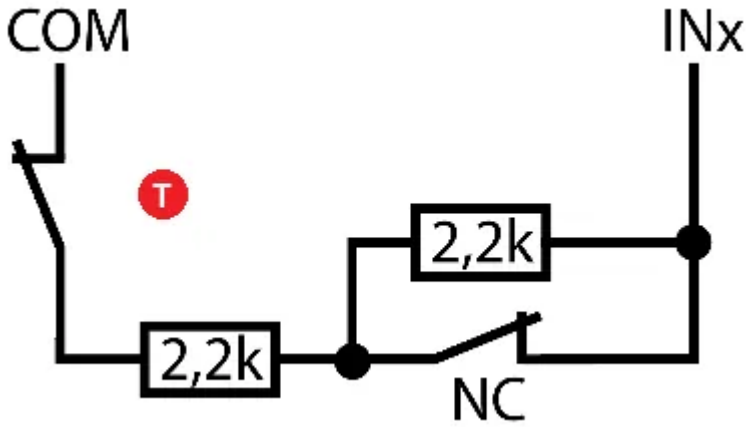


Obrázok 23. NO/EOL – v pokoji rozpojený obvod so zakončovacím odporom 2,2 kΩ: skrat alebo prerušenie – poplach, 2,2 kΩ – pokojový stav.



Obrázok 24. 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 detektora



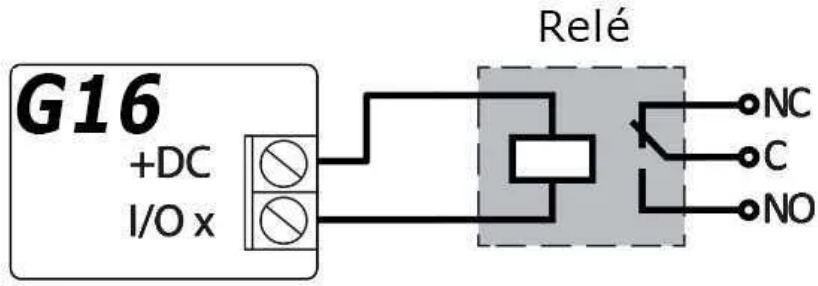
Obrázok 25. NC/DEOL – v pokoji zopnutý obvod so zakončovacím odporom 2,2 kΩ a rozpoznaním sabotáže: skrat alebo prerušenie – sabotáž, 2,2 kΩ – pokojový stav, 3,3–5,5 kΩ – poplach.

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

Hardvérová verzia 3 má jeden vstup (IN); jeho typ nastavíš v poli **System settings → Input IN type**.

3.6 Zapojenie výstupu s relé

Svorky I/O sú ako výstupy výstupy s otvoreným kolektorom (OC): v aktívnom stave stiahnu pripojenú záťaž na záporný pól, najviac 0,15 A, do 30 V DC. Väčší spotrebič alebo zariadenie na sieťové napätie spínaj **cez relé**: jeden koniec cievky relé ide na +DC, druhý na svorku I/O. Kontaktmi relé môžeš zapínať a vypínať rôzne elektrické zariadenia. Svorku I/O treba na to na stránke **IN/OUT** v TrikdisConfig nastaviť ako výstup (**OUT**) (bod 6.6).

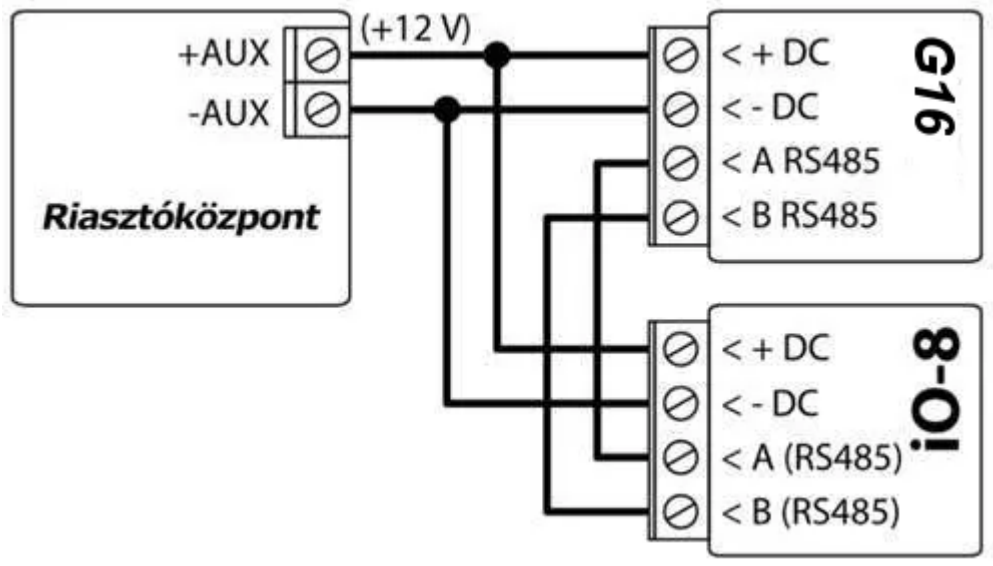


Obrázok 26. Pripojenie relé na výstup komunikátora: cievka ide medzi svorku +DC a I/O x, kontakty (NC, C, NO) spínajú spotrebič.

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

3.7 Pripojenie rozširujúceho modulu iO-8

Ak treba viac vstupov alebo výstupov, na zbernicu RS485 **verzie 4G** môžeš pripojiť najviac štyri rozširujúce moduly **iO-8**; každý pridá 8 ďalších I/O s dvojitou funkciou. Svorky A 485 a B 485 prepoj so svorkami A a B modulu, napájanie modulu ber z 12 V výstupu AUX ústredne. Spôsob pripojenia opisuje aj vlastný návod iO-8. Modul treba pridať na stránke **RS485 modules** v TrikdisConfig (bod 6.7); udalosti vstupov idú na PCO a do Protegus 2, výstupy môžeš ovládať z aplikácie.



Obrázok 27. Pripojenie rozširujúceho modulu iO-8 na zbernicu RS485 komunikátora G16 (A 485 → A, B 485 → B); obe zariadenia sú napájané z výstupu AUX zabezpečovacej ústredne (+12 V).

G16 s modemom 2G (G16_G410) nemá zbernicu RS485, preto k nemu nemožno pripojiť modul iO-8, W485 ani E485.

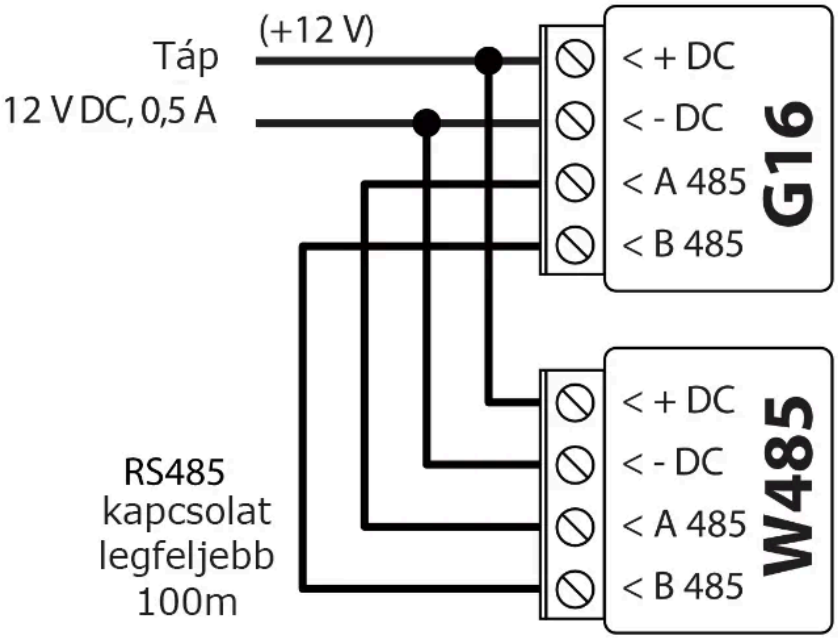
3.8 Pripojenie modulu W485 a E485

Rozšírenie o Ethernet alebo Wi-Fi – W485 a E485. Komunikátor môžeš doplniť modulom Wi-Fi W485 alebo ethernetovým modulom E485: udalosti idú na PCO a do aplikácie Protegus 2 cez káblový internet alebo Wi-Fi.

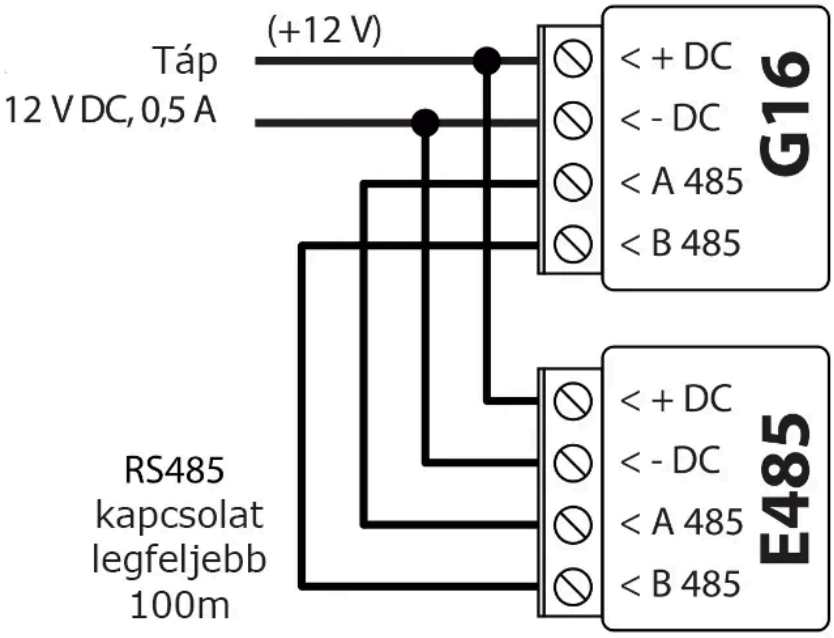
- **Pripojenie:** cez zbernicu RS485, zo spoločného napájania s komunikátorom (napájací vstup modulu 9–28 V DC); samostatný zdroj netreba.
- **Internet je primárny kanál:** kým funguje, ide cez neho všetko. Ak sa preruší, komunikátor sa sám prepne na mobilnú sieť a hneď ako sa internet vráti, prepne sa späť na IP.
- **Nielen prenos na PCO:** cez tento kanál funguje aj aplikácia Protegus 2 (upozornenia, vzdialené ovládanie).
- **E485** – káblový Ethernet (RJ45). **W485** – Wi-Fi 2,4 GHz (WPA / WPA2), tam, kde nie je natiahnutý UTP kábel.
- V prípade potreby sa dá používať aj bez SIM karty. Nastavenie: softvérom TrikdisConfig, cez USB.

Trikdis E485 Ethernet Modul (RS485) | **Trikdis W485 WiFi Modul (RS485)**

Kým spojenie WiFi, resp. Ethernet funguje, G16 komunikuje cez neho a mobilné dátové spojenie nepoužíva; ak sa spojenie preruší, prepne na mobilné dáta a po obnovení spojenia sa vráti na modul. Na fungovanie modulu **musí byť v G16 SIM karta**.



Obrázok 28. Pripojenie modulu W485 WiFi ku G16 cez zbernicu RS485. Obe zariadenia sú napájané zo spoločného zdroja 12 V DC (aspoň 0,5 A) (napájací vstup modulu 9–28 V DC); kábel RS485 môže byť dlhý najviac 100 m.



Obrázok 29. Pripojenie modulu E485 Ethernet ku G16 cez zbernicu RS485. Obe zariadenia sú napájané zo spoločného zdroja 12 V DC (aspoň 0,5 A) (napájací vstup modulu 9–28 V DC); kábel RS485 môže byť dlhý najviac 100 m.

Vzdialenosti „najviac … m“ sú teoretické maximá dosiahnuteľné za ideálnych podmienok. V praxi dajú kvalita a trasa kábla, zdroje rušenia a pri rádiovom spojení steny a terén podstatne kratší dosah. Plánuj s rezervou a pri dlhom úseku skontroluj spojenie pri uvedení do prevádzky.

Sieťové nastavenia modulov urobíš na stránke **RS485 modules** v TrikdisConfig (bod 6.7).

3.9 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 zabezpečovacej ústredne spustí aj komunikátor. Na prednom kryte máš vidieť:

- **POWER** svieti na zeleno – napájanie je v poriadku;
- **NETWORK** svieti na zeleno a bliká na žlto – pripojil sa k sieti; počet bliknutí je úroveň signálu (na 2G je dobrých 5, na 4G 3);
- **TROUBLE** nesvieti.

Ak LED NETWORK dáva menej žltých bliknutí, úroveň signálu nestačí: nájdi komunikátoru iné miesto alebo použi citlivejšiu anténu (bod 3.2). Každá iná signalizácia LED znamená nejakú chybu – identifikuj ju podľa tabuliek v bode 1.7. Ak TROUBLE bliká, počet bliknutí určuje príčinu (bod 1.7). **7 bliknutí** znamená chýbajúce spojenie s ústredňou: skontroluj vodiče CLK a DATA, zvolený typ ústredne a – kde treba – programovanie ústredne (kapitola 4). Ak nesvieti ani jedna LED, skontroluj napájanie a zapojenie.

4. Programovanie zabezpečovacej ústredne

Táto kapitola pre každého výrobcu opisuje, čo treba nastaviť v zabezpečovacej ústredni, aby G16 čítal udalosti a – kde sa dá – ovládal ústredňu na diaľku. Pri väčšine ústrední netreba na čítanie udalostí nič programovať; na **priame ovládanie** zaškrtni na stránke **System settings** v TrikdisConfig možnosť **Remote Arm/Disarm** a pri ústredni Paradox, resp. Texecom zadaj aj heslo PC, resp. UDL ústredne v poli **Security panel PC download password** (body 2.2 a 6.2).

Ak ústredňu neovládaš priamo, ale cez zónu kľúčového spínača (bod 3.4), **Remote Arm/Disarm** nechaj prázdne a táto kapitola sa týka len nastavení potrebných na čítanie udalostí.

4.1 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.

4.2 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.

4.3 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]**.

4.4 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
108	3	12345678

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

4.5 Crow a Pyronix

Ústredne **Crow Runner 4/8** a **Runner 8/16** nevyžadujú žiadne osobitné nastavenie.

Ani ústredne **Pyronix** nevyžadujú programovanie, ale po nastavení a zapojení komunikátora **odpoj ústredňu od napájania** (sieť aj akumulátor) a znova ju spusti: ústredňa prijme komunikátor pripojený na jej zbernicu pri štarte.

4.6 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]**.

4.7 InnerRange Inception a Integriti

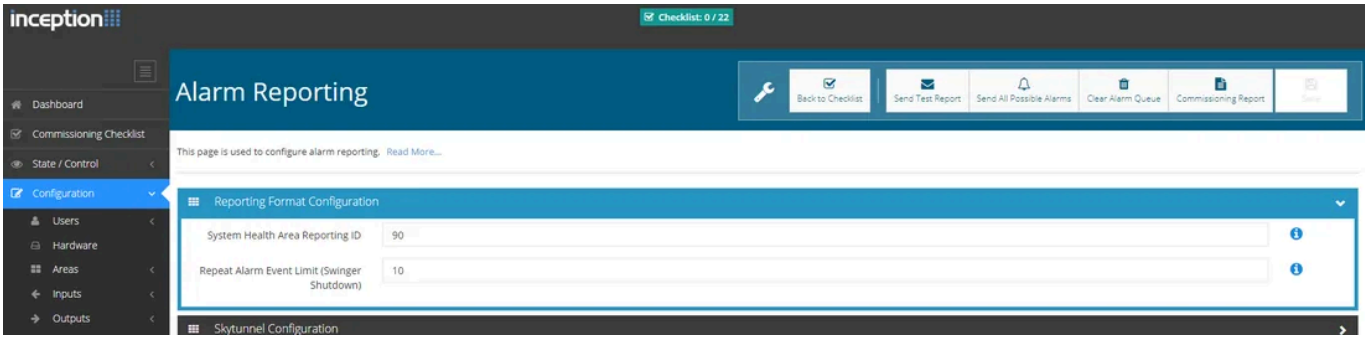
Firmvér ústredne **InnerRange Inception** musí byť minimálne **2.3.0.3507-r0** a ústredňa potrebuje internetové pripojenie. Nastavenie vykonáš vo webovom rozhraní ústredne:

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.

Inception a Integriti odovzdávajú komunikátoru udalosti; na zapínanie a vypínanie stráženia treba zónu kľúčového spínača (body 1.2 a 3.4).



Obrázok 30. Webové rozhranie Inception – Configuration → General → Alarm Reporting.



Obrázok 31. Inception – 3rd Party Device Configuration.

- 1 **Enable 3rd Party Device Reporting** – zaškrtnuté.
- 2 **3rd Party Device Type** – Trikdis.
- 3 **Serial Port** – Serial Port 1 (Plugged In, In Use By 3rd Party Device).

5. Ovládanie na diaľku aplikáciou Protegus 2

S mobilnou a webovou aplikáciou Protegus 2 používateľ na diaľku vidí stav systému, dostáva upozornenia na udalosti, môže zapínať a vypínať stráženie a ovládať výstupy komunikátora. Pri G16 sa stráženie môže zapínať dvoma spôsobmi: pri **priamo ovládateľných** ústredniach vlastným **kódom klávesnice** používateľa, pri ústredniach zapojených cez zónu kľúčového spínača **výstupom** komunikátora.

5.1 Pridanie zariadenia

Pred pridaním zariadenia skontroluj:

1. SIM karta je aktívna a funguje na nej mobilné dátové spojenie; jej kód PIN je zadaný v zariadení alebo je požiadavka na PIN vypnutá.
2. Na stránke **User reporting** → **PROTEGUS Cloud** v TrikdisConfig je zaškrtnuté **Enable connection** a je nastavený **Protegus Cloud access code** (po vytvorení systému ho už nemožno zmeniť).
3. LED **POWER** svieti na zeleno, LED **NETWORK** svieti na zeleno a bliká na žlto.

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

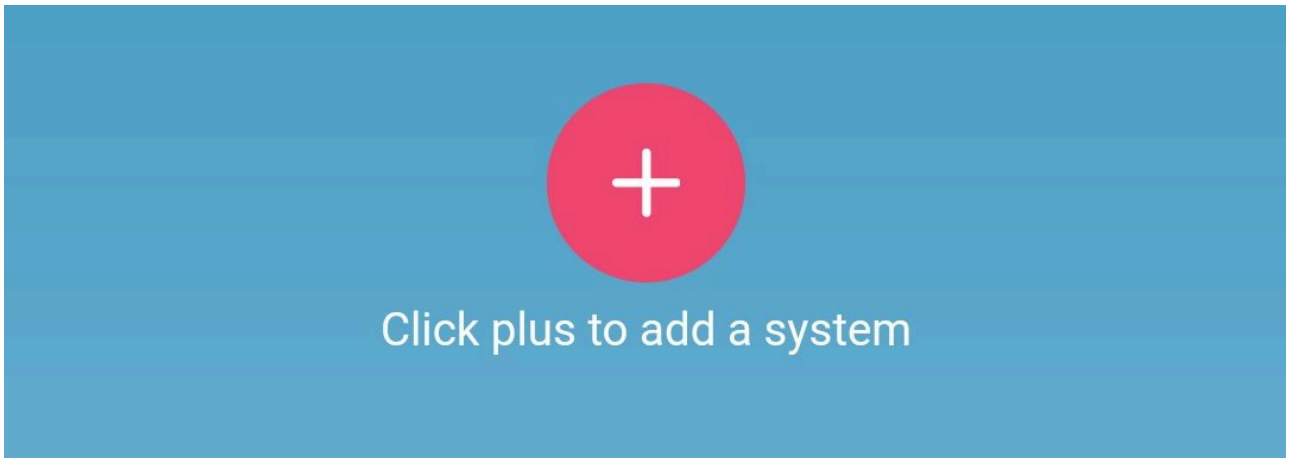
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

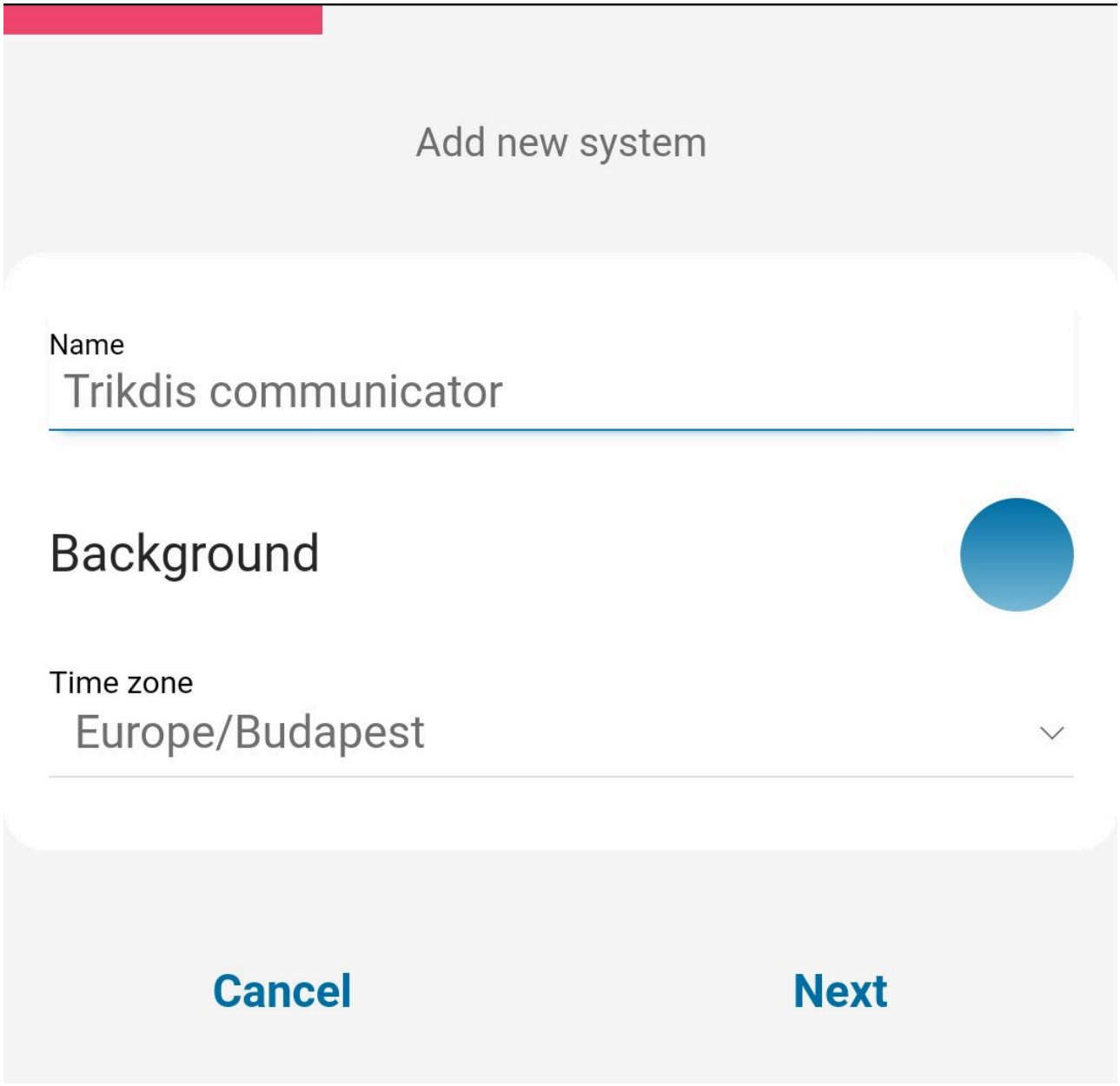
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



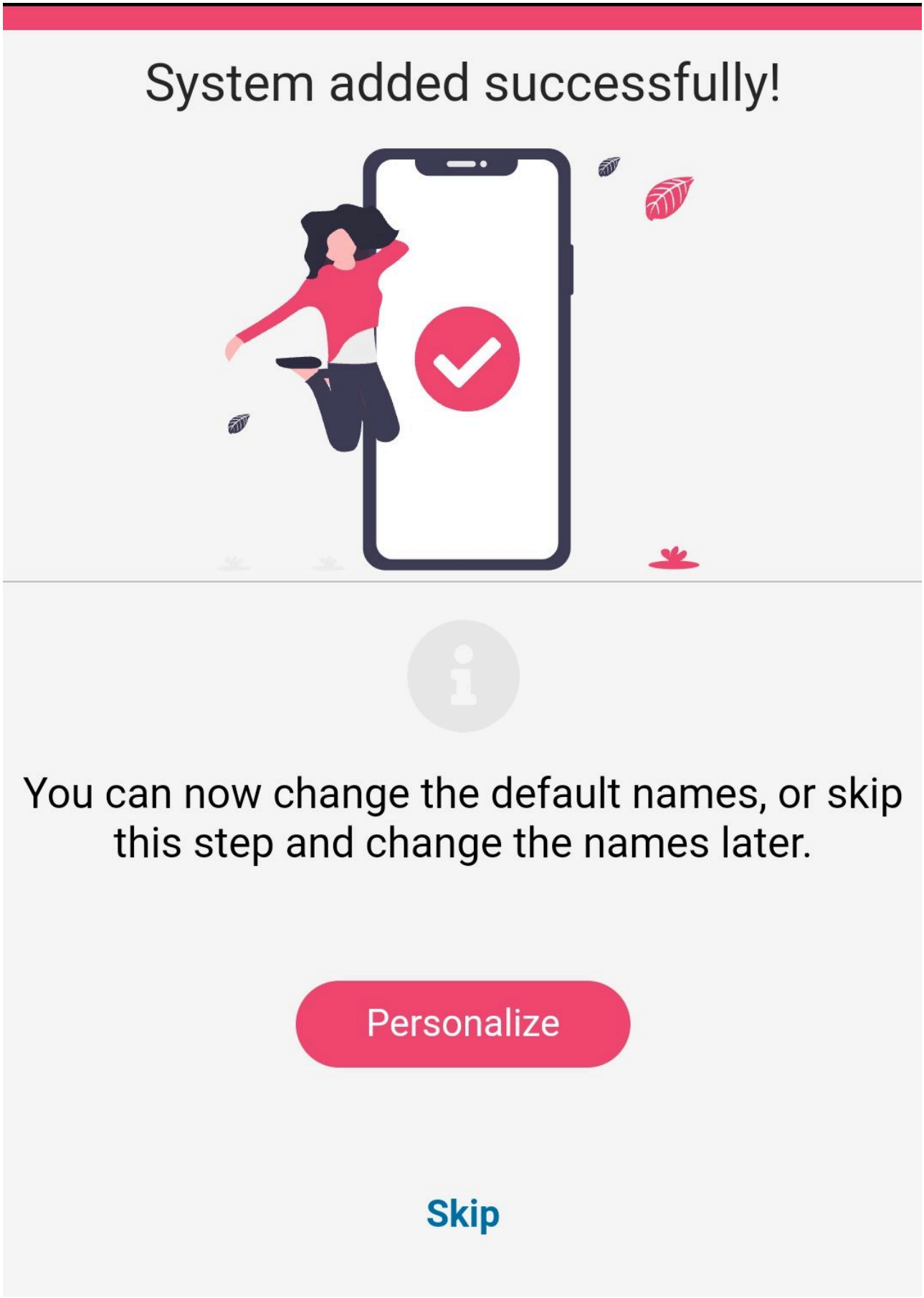
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



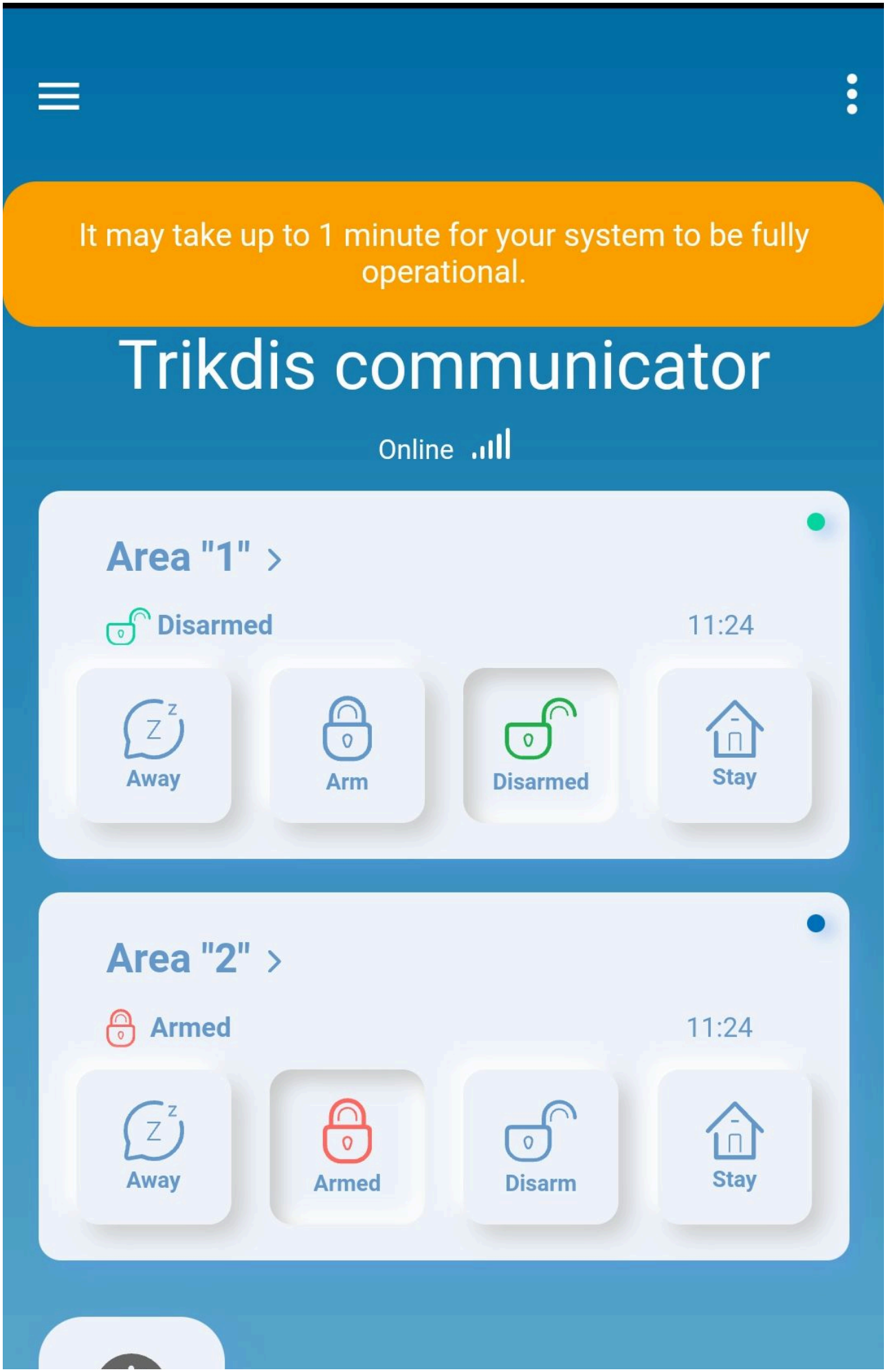
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Jedinečný identifikátor zariadenia (**IMEI**) je uvedený na krabici a na zadnej strane zariadenia a ukazuje ho aj stavový riadok TrikdisConfig.

5.2 Priame ovládanie kódom klávesnice

Ak ústredňa patrí medzi priamo ovládateľné typy (bod 1.2) a na stránke **System settings** v TrikdisConfig je zaškrtnuté **Remote Arm/Disarm**, Protegus 2 ukazuje partície ústredne so stavom načítaným zo zbernice a na zapnutie / vypnutie stráženia zadá používateľ v aplikácii **kód klávesnice ústredne** – ten istý, ktorý používa na klávesnici. Samostatný výstup ani zóna kľúčového spínača netreba.

- V ústredni na to treba podľa výrobcu nastavenie (Paradox: heslo PC, Texecom: heslo UDL; pri ústredni Caddx, Honeywell a InnerRange povolenie zbernice, resp. sériového portu už aj na čítanie udalostí) – pozri kapitolu 4.
- Kód klávesnice overuje ústredňa a aj denník udalostí ústredne zaznamená používateľa, nie komunikátor.
- Pri ústredni Paradox **nesmie byť** kód používateľa **hlavný kód**; po zmene kódu reštartuj komunikátor (bod 4.2).
- Pri ústredni DSC PowerSeries ukazuje aplikácia aj stav zón a dá sa aj premosťovať zóny – podrobnosti v článku o priamom ovládaní DSC.

Pri vytváraní systému sa Protegus 2 opýta, či stráženie ovláda výstup komunikátora. Pri priamom ovládaní k partícii **nepriraďuj** výstup (**Control with Protegus2** vypnuté): partíciu riadi ústredňa, stav prichádza zo zbernice.

5.3 Stráženie zónou kľúčového spínača

Ak ústredňu nemožno ovládať priamo alebo ju tak nechceš používať, jeden výstup komunikátora pripojíš na zónu kľúčového spínača ústredne (bod 3.4), v TrikdisConfig zostane **Remote Arm/Disarm** prázdne a v Protegus 2 priradíš k partícii výstup.

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.

5.4 Zapínanie a vypínanie 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.

Pri priamom ovládaní aplikácia pýta kód klávesnice ústredne; pri zapínaní stráženia kľúčovým spínačom – ak je zapnuté – heslo Protegus 2.

5.5 Ovládanie správami SMS

Komunikátor sa dá ovládať a programovať aj SMS správami. Štruktúra správy:

`HESLO medzera PRÍKAZ medzera DÁTA` – napríklad `123456 OUTPUT1 ON`

S heslom **administrátora** sa dajú použiť všetky príkazy, s heslom **inštalátora** príkazy INFO, RESET a OUTPUTx. `x` je číslo výstupu: svorka I/O nastavená ako výstup (1, 2 alebo 3), ktorú chceš zopnúť.

Príkaz	Dáta	Čo robí	Príklad
`INFO`	–	Vyžiada si informácie o zariadení: typ, IMEI, sériové číslo, verzia firmvéru	`123456 INFO`
`RESET`	–	Reštartuje zariadenie	`123456 RESET`
`OUTPUTx`	`ON`	Zapne x. výstup	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Vypne x. výstup	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Dá impulz na x. výstupe; `tttt` = dĺžka impulzu v sekundách, štyrmi číslicami	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Povolí, resp. zakáže spojenie s Protegus	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adresa:port`	IP adresa a port primárneho kanála	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=kľúč`	Šifrovací kľúč TRK	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=názov`	APN SIM karty	`123456 CONNECT APN=internet`

Príkaz	Dáta	Čo robí	Príklad
`CONNECT`	`USER=meno`	Používateľské meno APN (ak ho operátor vyžaduje)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=heslo`	Heslo APN (ak ho operátor vyžaduje)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Výber typu zabezpečovacej ústredne poradovým číslom zo zoznamu **Security panel model** v TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=hhhh` / `DIR=OFF`	4-miestne heslo priameho ovládania (PC heslo, resp. UDL heslo ústredne); `DIR=OFF` ho vypne	`123456 CONNECT DIR=1122`

Môžeš obmedziť, z ktorých telefónnych čísel zariadenie prijme príkaz: TrikdisConfig → stránka **User reporting** → **Control by SMS**. Ak nie je zadané ani jedno číslo, vykoná príkaz so správnym heslom z akéhokoľvek čísla.

6. TrikdisConfig – nastavenia podrobne

V ľavej časti okna TrikdisConfig je zoznam stránok (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), hore rad tlačidiel (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), dole stavový riadok. Táto kapitola prechádza nastavenia G16 stránku po stránke.

6.1 Stavový riadok

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.
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.

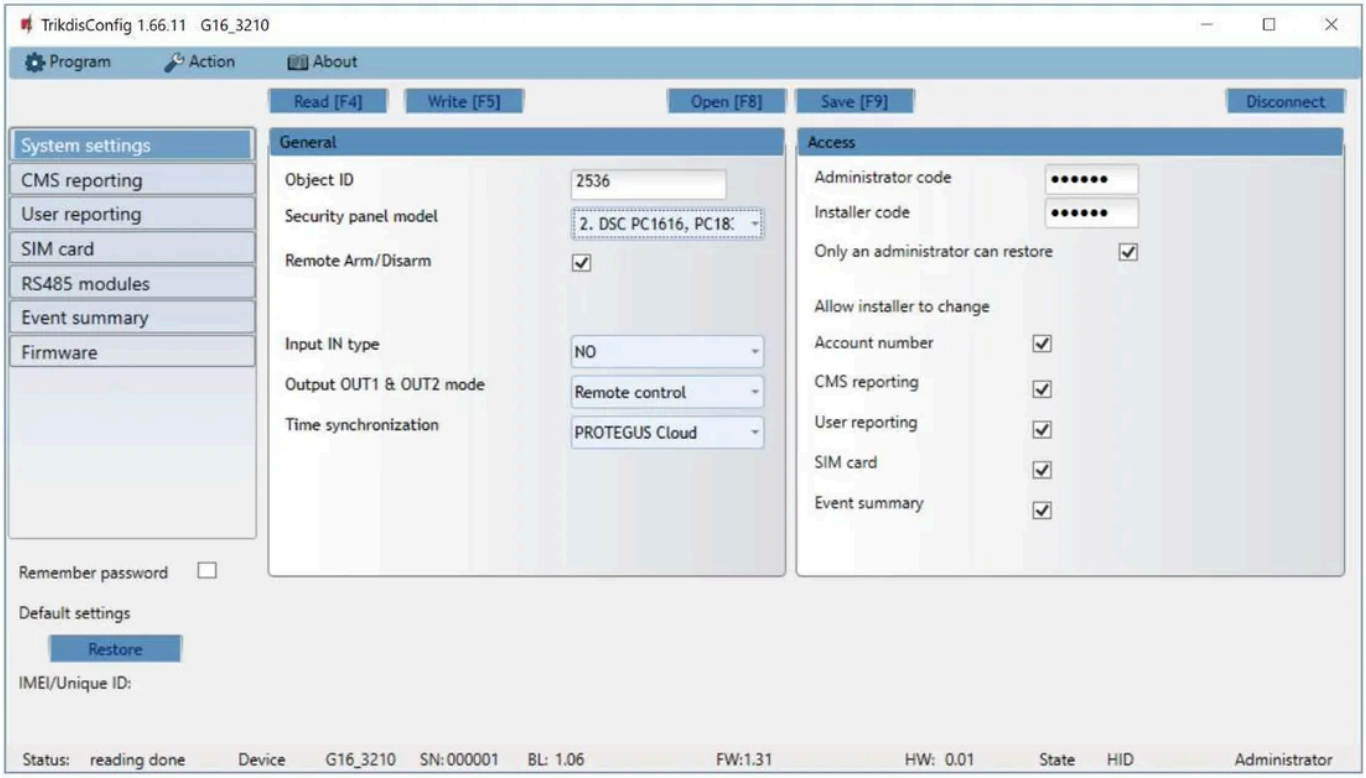
V poli **Device** má pri G16 byť typové označenie G16 (napríklad G16_G410 alebo G16_54E0). Po načítaní program ukazuje nastavenia uložené v G16; nastav ich podľa opisov stránok nižšie.



Obrázok 32. Stavový riadok TrikdisConfig s načítaným G16: identifikátor, stav, typ, sériové číslo, verzie, spôsob pripojenia a úroveň prístupu.

6.2 System settings

Stránka má dve skupiny: v skupine **General** nastavuješ základné fungovanie zariadenia a jeho spojenie so zabezpečovacou ústredňou, v skupine **Access** úrovne prístupu.



Obrázok 33. TrikdisConfig – stránka System settings: skupina General a Access (na obrázku hardvérová verzia 3, G16_3210; verzia 4 nemá polia Input IN type a Output OUT1 & OUT2 mode, tie sa presunuli na stránku IN/OUT).

- **Object ID** – identifikátor objektu, ktorý dostaneš od PCO (4 hexadecimálne znaky, 0–9, A–F). Povinný, ak zariadenie hlási aj na PCO; `FFFE` a `FFFF` nemožno použiť.
- **Security panel model** – typ pripojenej zabezpečovacej ústredne zo zoznamu. Od neho závisí, ako komunikátor číta zbernicu, preto zvoľ presný typ zapojenej ústredne.
- **Remote Arm/Disarm** – po zaškrtnutí komunikátor ovláda ústredňu priamo: používateľ zapína a vypína stráženie z Protegus 2 svojím kódom klávesnice. Zobrazí sa len pri priamo ovládateľných typoch ústrední; v ústredni na to treba podľa výrobcu nastavenie (kapitola 4). Pri zapínaní stráženia zónou kľúčového spínača ho nechaj prázdne.
- **Security panel PC download password** – na priame ovládanie ústredne Paradox a Texecom heslo PC, resp. UDL ústredne (4 znaky); musí sa zhodovať s heslom nastaveným v ústredni (body 4.2 a 4.3).
- **Time set** – zdroj hodín zariadenia (predvolene **Cloud application**, cloud Protegus).
- Na **hardvérovej verzii 3** je tu ešte pole **Input IN type** (typ vstupu: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) a pole **Output OUT1 & OUT2 mode** (režim dvoch výstupov; na zapínanie stráženia kľúčovým spínačom **Remote control**).

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

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

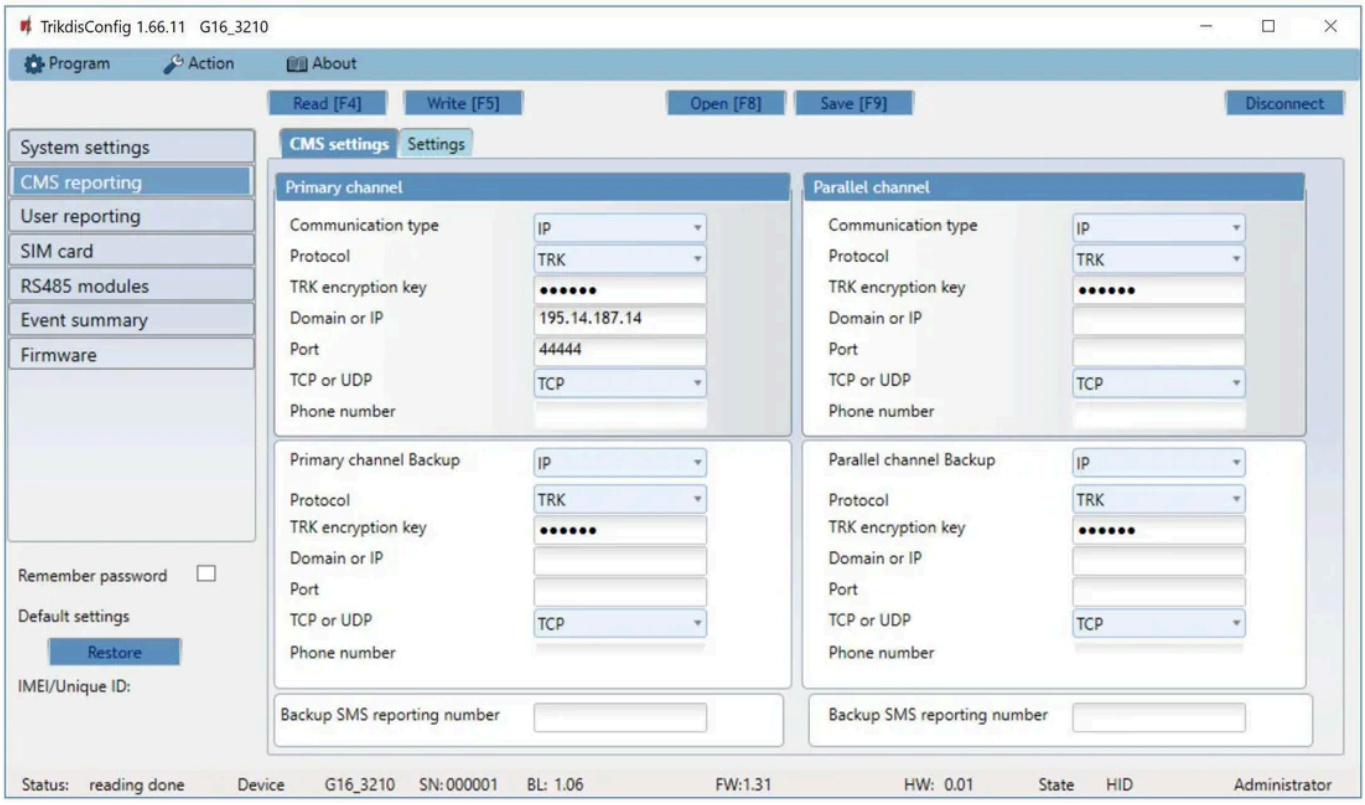
- **Administrator code** – prístup ku všetkým nastaveniam (výrobné heslo: `123456`; heslo má 6 znakov: číslice alebo latinské písmená).
- **Installer code** – prístup, ktorý sa dá obmedziť (výrobné heslo: `654321`).
- **Only an administrator can restore** – ak je zaškrtnuté, obnovenie výrobných nastavení 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.

6.3 CMS reporting

Komunikátor posiela udalosti na PCO cez mobilné dátové spojenie (IP) alebo cez SMS. Udalosti môžu ísť viacerými kanálmi: **hlavný** a **paralelný** kanál fungujú súčasne (dvom prijímačom naraz) a ku každému patrí **záložný** kanál, ktorý sa uplatní, ak sa daný kanál preruší. Komunikácia je šifrovaná a chránená heslom; na príjem treba prijímač Trikdis (softvérový prijímač IPcom, RL14, RM14) alebo univerzálny prijímač podporujúci protokol DC-09 / TL150. Prijímače Trikdis odovzdávajú udalosti softvéru PCO: cez IP spojenie softvérový prijímač **IPcom** (Windows / Linux), prijímač IP/SMS **RL14** alebo viackanálový prijímač **RM14**; na príjem SMS RL14, RM14 alebo prijímač SMS **GM14**.



Obrázok 34. TrikdisConfig – CMS reporting, záložka CMS settings: hlavný, záložný a paralelný kanál.

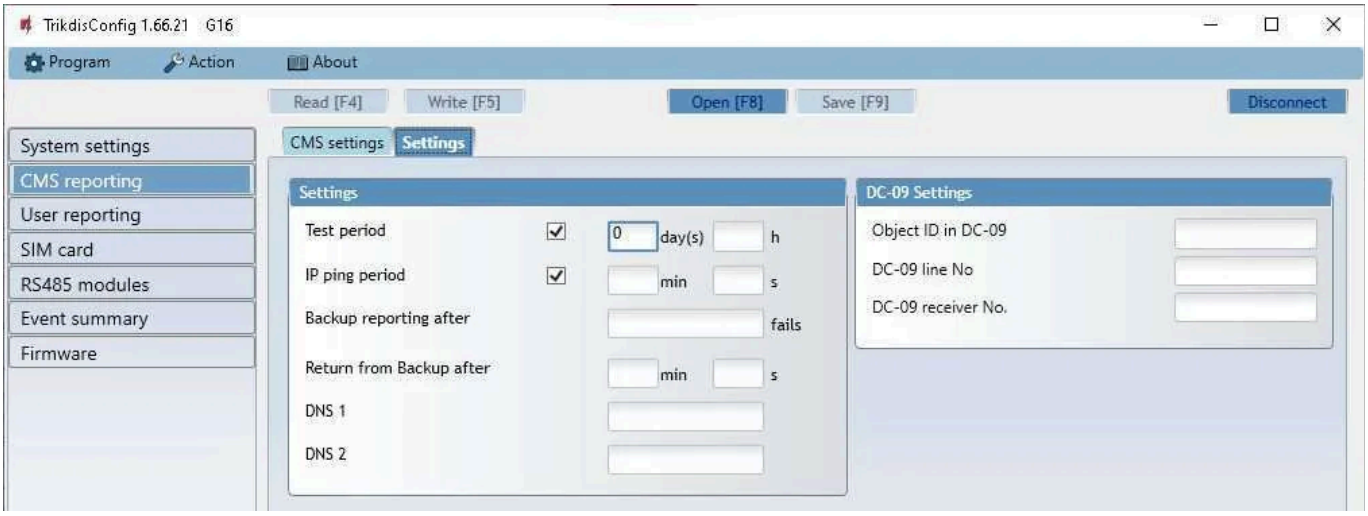
Primary channel – hlavný kanál

- **Communication type** – IP alebo SMS. SMS je dobrá ako záloha – funguje, aj keď nie je mobilné dátové spojenie –, ako hlavný kanál sa neodporúča.
- **Protocol** – TRK (prijímače Trikdis), DC-09_2007 alebo DC-09_2012 (univerzálne prijímače), TL150 (SUR-GARD).
- **TRK encryption key** – 6-miestny šifrovací kľúč; v komunikátore a v prijímači musí byť rovnaký.
- **Domain or IP**, **Port** – adresa a port prijímača.
- **TCP or UDP** – protokol prenosu.
- **Phone number** – len pri komunikácii cez SMS: telefónne číslo prijímača SMS Trikdis s predvoľbou krajiny (napr. `CCxxxxxxxxx`, kde CC je predvoľba krajiny).

Primary channel Backup – záložný kanál. Preberie komunikáciu, ak hlavný kanál nefunguje; jeho nastavenia sú rovnaké ako vyššie.

Parallel channel – paralelný kanál. Popri hlavnom posiela súčasne druhému prijímaču (napríklad miestnemu a centrálnemu PCO). Má vlastný záložný kanál.

Backup SMS reporting number – záložné číslo SMS. Uplatní sa, ak sa nepodarí odoslať ani hlavným, ani paralelným, ani záložným kanálom; je užitočné, lebo funguje aj bez IP spojenia. Je aktívne, len ak sú hlavný aj záložný kanál v režime IP. Zariadenie pošle SMS prijímaču SMS na PCO po prvom spustení a tiež vtedy, keď sa spojenie TCP/IP alebo UDP/IP preruší na hlavnom kanáli aj na jeho zálohe. Do poľa zadaj telefónne číslo prijímača SMS Trikdis na PCO, s predvoľbou krajiny (napr. `CCxxxxxxxxx`).



Obrázok 35. TrikdisConfig – CMS reporting, záložka Settings: testovacie hlásenie, PING, časovanie záložného kanála, DNS a údaje DC-09.

Na záložke **Settings** nastavuješ časovania a údaje DC-09.

- **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**.

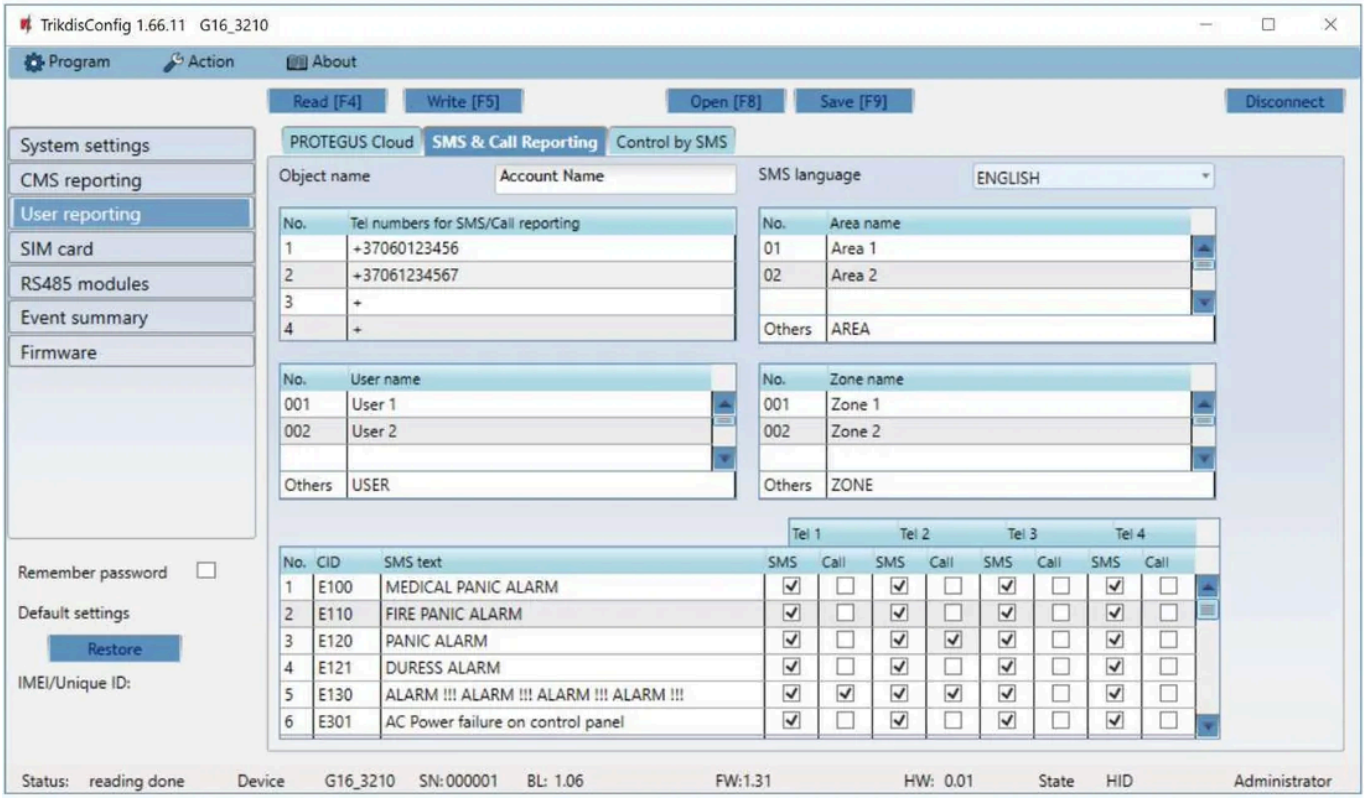
DC-09 Settings (na pravej strane karty) – vyplniť ich treba iba vtedy, ak na niektorom kanáli posielaš protokolom DC-09_2007 alebo DC-09_2012; skupina sa zobrazí, keď je v poli **Protocol** niektorého kanála vybraný DC-09_2007 alebo DC-09_2012:

- **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.

V dolnej časti záložky: **DNS 1, DNS 2** – menné servery; potrebné, ak si prijímač zadal doménovým menom, a nie IP adresou. Predvolený je verejný DNS Google. Skupina **DC-09 settings** je viditeľná, len ak je na niektorom kanáli nastavený protokol DC-09.

6.4 User reporting

Na záložke **PROTEGUS Cloud** povolíš službu Protegus. So službou Protegus môže používateľ na diaľku sledovať a ovládať komunikátor aj systém; viac informácií: www.protegus.app.

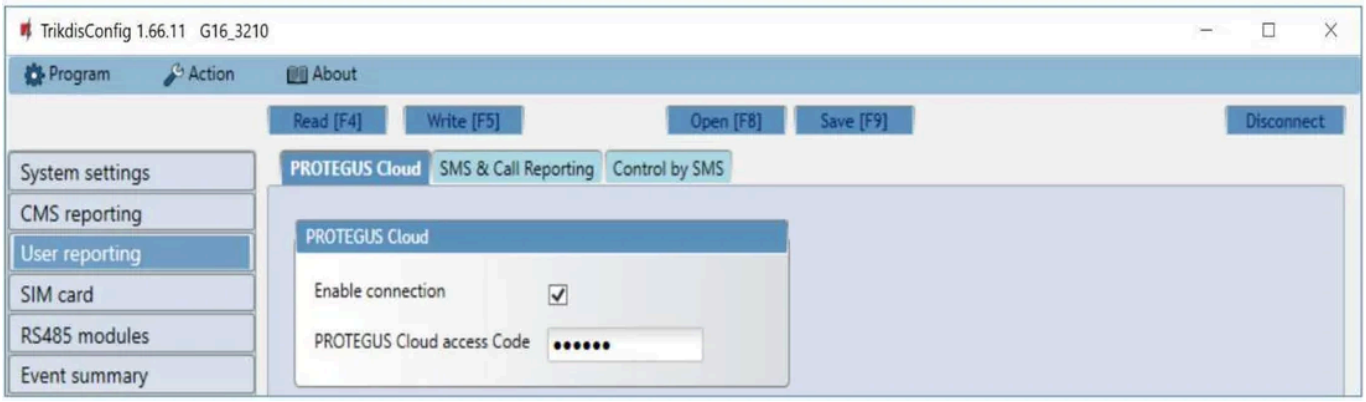


Obrázok 36. TrikdisConfig – User reporting, záložka PROTEGUS Cloud.

- **Enable connection** – povolí spojenie s cloudom Protegus a vzdialený prístup TrikdisConfig.
- **Protegus Cloud access code** – 6-miestny kód pre spojenie Protegus (z výroby `123456`). Nastaviť ho možno len pred vytvorením systému v Protegus 2, dodatočne ho zmeniť nemožno.

Na záložke **SMS & Call Reporting** môže používateľ dostávať upozornenia na udalosti aj cez SMS alebo telefonickým hovorom.

Pri poplachu zariadenie najprv odošle SMS na všetky zadané telefónne čísla a potom ich jedno po druhom volá od Tel 1 po Tel 4. Každé číslo volá raz a zvoní 20 sekúnd; hovor sa považuje za úspešný, ak číslo zvoní (stačí aj prijatie alebo odmietnutie). Modem uskutoční hovor cez 2G alebo VoLTE. Tam, kde operátor vypol 2G a modem nepovolil pre VoLTE, SMS príde, ale telefón nezazvoní. Nejde o chybu nastavenia. Na takom mieste používajte SMS a aplikáciu Protegus 2.



Obrázok 37. TrikdisConfig – User reporting, záložka SMS & Call Reporting.

- **Object name** – názov systému; je v každej SMS.
- **SMS language** – jazyk SMS (kvôli diakritickým znakom jazyka).
- **Tel numbers for SMS/Call reporting** – najviac 4 telefónne čísla s predvoľbou krajiny (`+CC…`, `00CC…` alebo `CC…`, kde CC je predvoľba krajiny).
- **Area name, User name, Zone name** – názvy partícií, používateľov a zón; zariadenie ich používa v texte SMS. Do príslušnej tabuľky zadaj číslo partície, používateľa alebo zóny a vedľa neho názov. Pri ústredni čítanej zo zbernice prichádzajú vlastné čísla zón a používateľov ústredne, k nim zadaj názvy.
- **CID event table** – pre každú udalosť môžeš nastaviť, ktoré číslo dostane SMS alebo hovor; text správy aj kód Contact ID môžeš zmeniť, môžeš pridať aj novú udalosť.

Na záložke **Control by SMS** nastavuješ príjem príkazov SMS (príkazy opisuje bod 5.5).

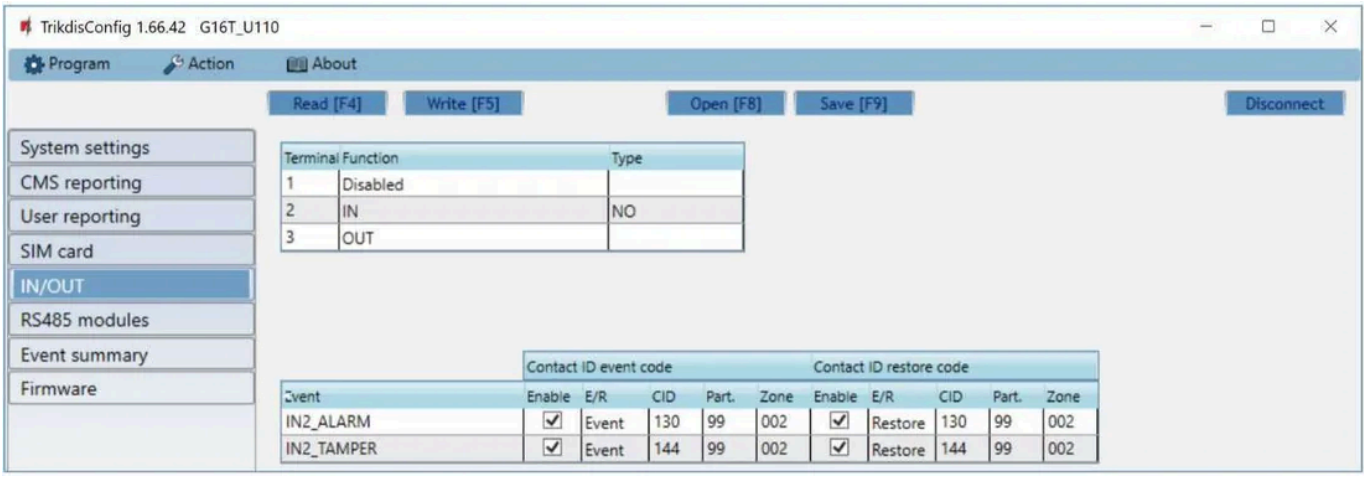


Obrázok 38. TrikdisConfig – User reporting, záložka Control by SMS.

- **Reply text** – text štyroch odpovedí na príkaz SMS: úspešný príkaz (Command done), nesprávne heslo (Wrong password), nesprávny príkaz (Wrong command), nesprávne údaje (Wrong data).
- **Tel numbers for control by SMS** – najviac 4 čísla; zariadenie prijme príkaz len z týchto čísel. Ak je pole prázdne, prijme príkaz so správnym heslom z ľubovoľného čísla; bezpečnosť aj vtedy zaručuje to, že v príkaze je povinné heslo administrátora alebo inštalátora.

6.5 SIM card

Bez údajov SIM karty sa zariadenie nepripojí na dátovú sieť.



Obrázok 39. TrikdisConfig – stránka SIM card.

- **SIM card PIN** – kód PIN karty. Požiadavku na PIN môžeš vypnúť, ak kartu vložíš do mobilného telefónu a tam ju zakážeš. Ak je požiadavka na PIN vypnutá, môže v poli zostať výrobná hodnota.
- **APN** – prístupový bod operátora (Access Point Name); bez neho sa komunikátor nevie pripojiť na internet. Nájdeš ho aj na webe operátora; APN „internet" je všeobecný, 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 APN, ak ich operátor vyžaduje.
- **Forbid connection when roaming detected** – užitočné blízko štátnej hranice: zabráni, aby sa zariadenie pripojilo do siete susednej krajiny.

Pred použitím sa uisti, že SIM karta je aktívna a na komunikáciu cez IP sú na nej povolené mobilné dáta.

6.6 IN/OUT

Tu zadáš úlohu troch svoriek I/O komunikátora s dvojitou funkciou: **Disabled** (nepoužitá), **IN** (vstup) alebo **OUT** (výstup). Pri vstupe treba zadať aj typ (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Výrobné nastavenie: I/O 1 nepoužitý, I/O 2 vstup (NO), I/O 3 výstup.



Obrázok 40. TrikdisConfig – stránka IN/OUT: funkcia svoriek I/O a udalosti vstupov.

Pri narušení detektora pripojeného na vstup pošle komunikátor vlastnú udalosť (**INx_ALARM**, Contact ID 130) a pri narušení sabotážneho obvodu udalosť sabotáže (**INx_TAMPER**, 144) na PCO a do Protegus 2; v tabuľke sa zobrazia udalosti každej svorky nastavenej ako vstup. Stĺpce tabuľky:

- **Enable** – povolí odosielanie správy.
- **E/R** – typ udalosti: Event (poplach) alebo Restore (obnovenie).

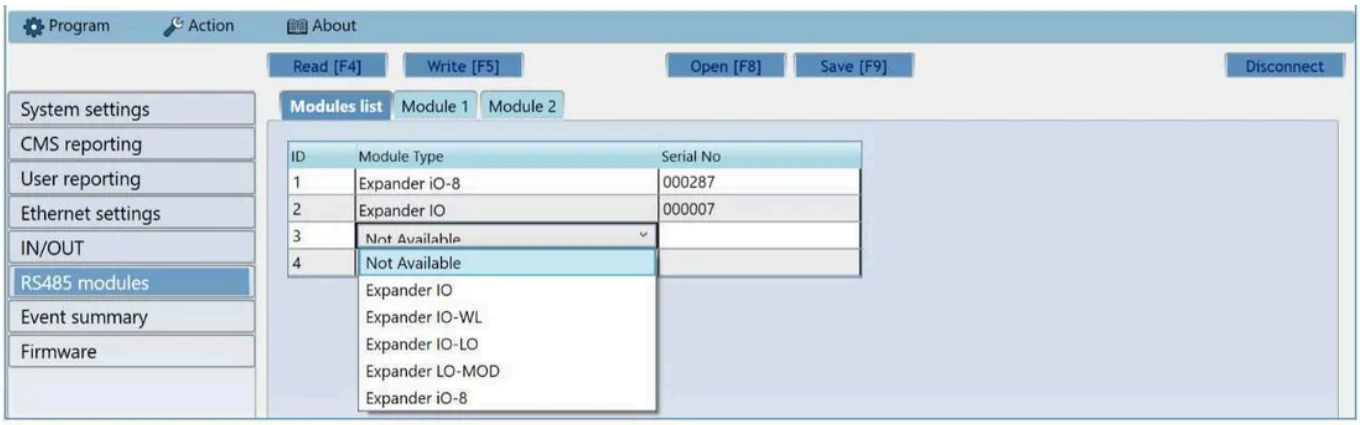
- **CID** – kód Contact ID.
- **Part.** – číslo partície v správe.
- **Zone** – číslo zóny v správe.

Hardvérová verzia 3 nemá stránku IN/OUT: typ jediného vstupu nastavíš v poli **System settings → Input IN type**, režim dvoch výstupov v poli **Output OUT1 & OUT2 mode** a udalosti vstupu (IN_ALARM, IN_TAMPER) na stránke **Event summary**.

6.7 RS485 modules

Rozširujúce moduly iO-8 a moduly W485 / E485 pripojené na zbernicu RS485 treba pridať na záložke **Modules list**.

Na G16 s modemom 2G (G16_G410) túto stránku nemožno použiť: verzia 2G nemá zbernicu RS485.

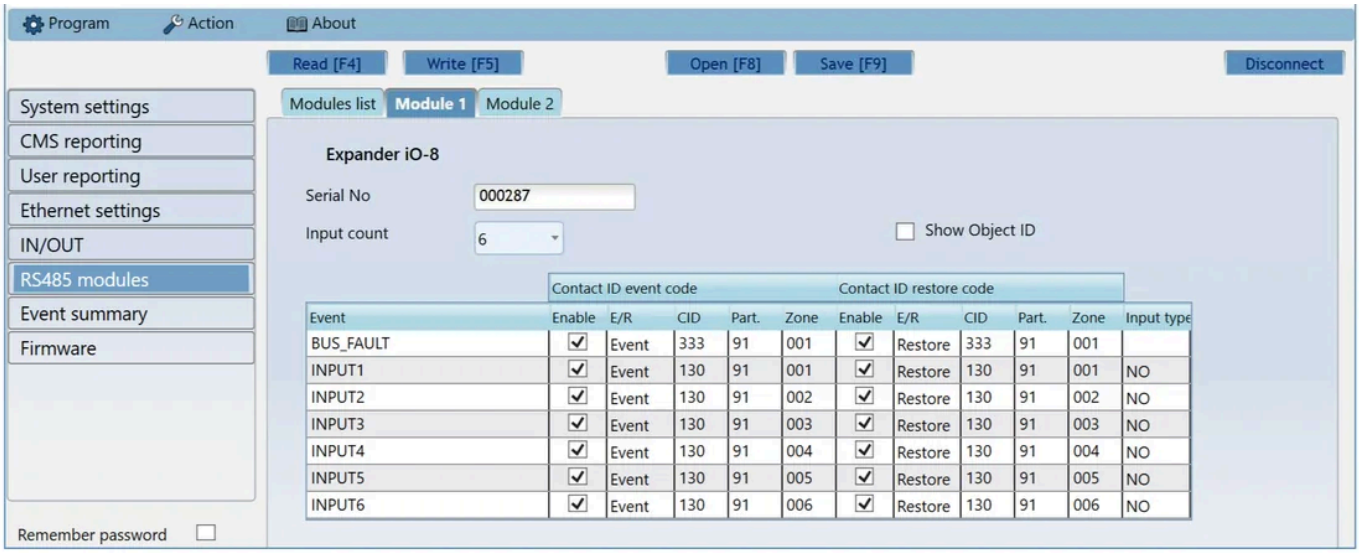


Obrázok 41. TrikdisConfig – RS485 modules, záložka Modules list: typ modulu (Expander iO-8, W17u/W485, E485) a jeho sériové číslo.

- **Module Type** – typ pripojeného modulu zo zoznamu (Expander iO-8, W17u/W485, E485).
- **Serial No** – 6-miestne sériové číslo modulu (na module a na jeho krabici, SN).

Po výbere modulu a zadaní sériového čísla stlač tlačidlo **Write [F5]**, vytiahni kábel USB a počkaj minútu, kým komunikátor modul zaregistruje. Potom kábel znova zapoj, načítaj zariadenie (**Read [F4]**) a na stránke RS485 modules sa zobrazí vlastná očíslovaná záložka modulu.

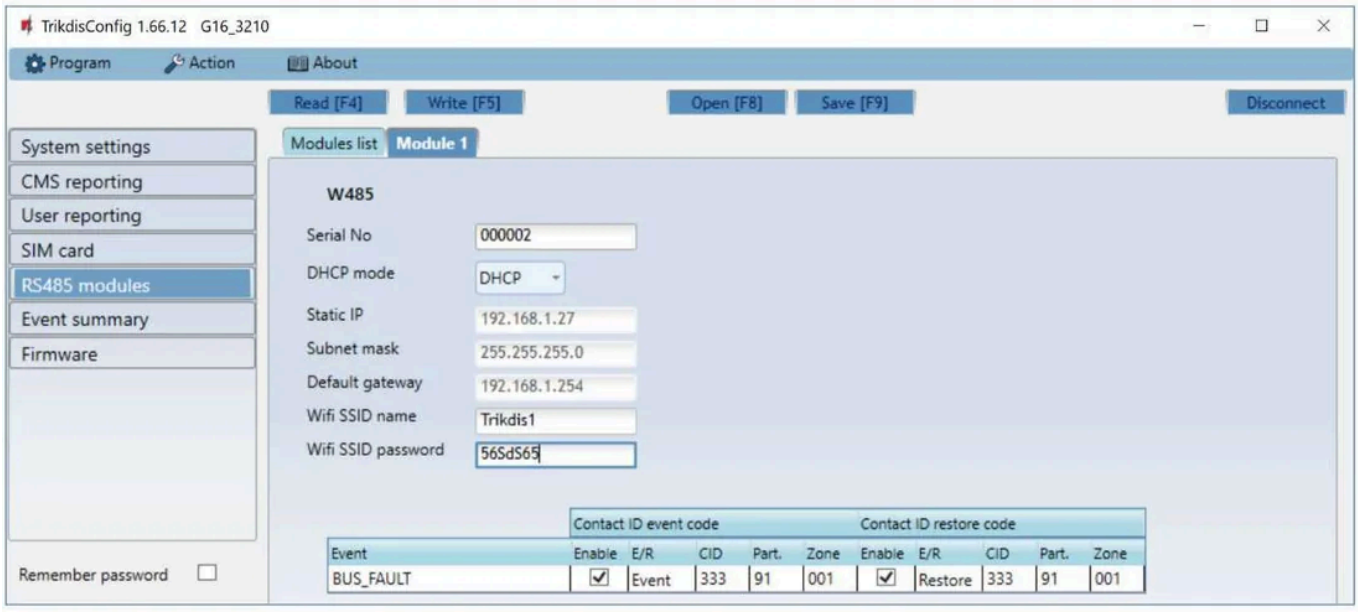
Rozširujúci modul iO-8 – 8 I/O s dvojitou funkciou; ku komunikátoru môžeš pripojiť najviac 4 moduly.



Obrázok 42. TrikdisConfig – RS485 modules, záložka modulu iO-8.

- **Input Count** – koľko svoriek má byť vstupmi; ostatné budú výstupy. Typ vstupu (**Input type**: NO alebo NC) môžeš zadať v tabuľke. Úlohu výstupov (zapínanie / vypínanie stráženia zónou kľúčového spínača alebo ovládanie zariadenia) nastavíš v aplikácii Protegus 2.
- V tabuľke môžeš chybe zbernice (**BUS_FAULT**, Contact ID 333) a udalostiam narušenia a obnovenia vstupov (**INPUTx**, 130) priradiť kód Contact ID (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Pri narušení vstupu pošle komunikátor udalosť s nastaveným kódom prijímaču PCO, aplikácii Protegus 2 a cez SMS na telefónne číslo používateľa. Predvolene hlási 1. modul s partíciou 91, 4. modul s partíciou 94. Zaškrtnutím **Show Object ID** môžeš vstupom zadať aj identifikátor objektu odlišný od identifikátora komunikátora.
- Ak má používateľ dostávať o vstupoch rozširujúceho modulu aj SMS alebo hovor, pridaj kód Contact ID priradený vstupu aj do tabuľky udalostí na záložke **SMS & Call Reporting**.

Modul W485 WiFi (v zozname W17u/W485) – údaje siete WiFi a sieťové nastavenia.

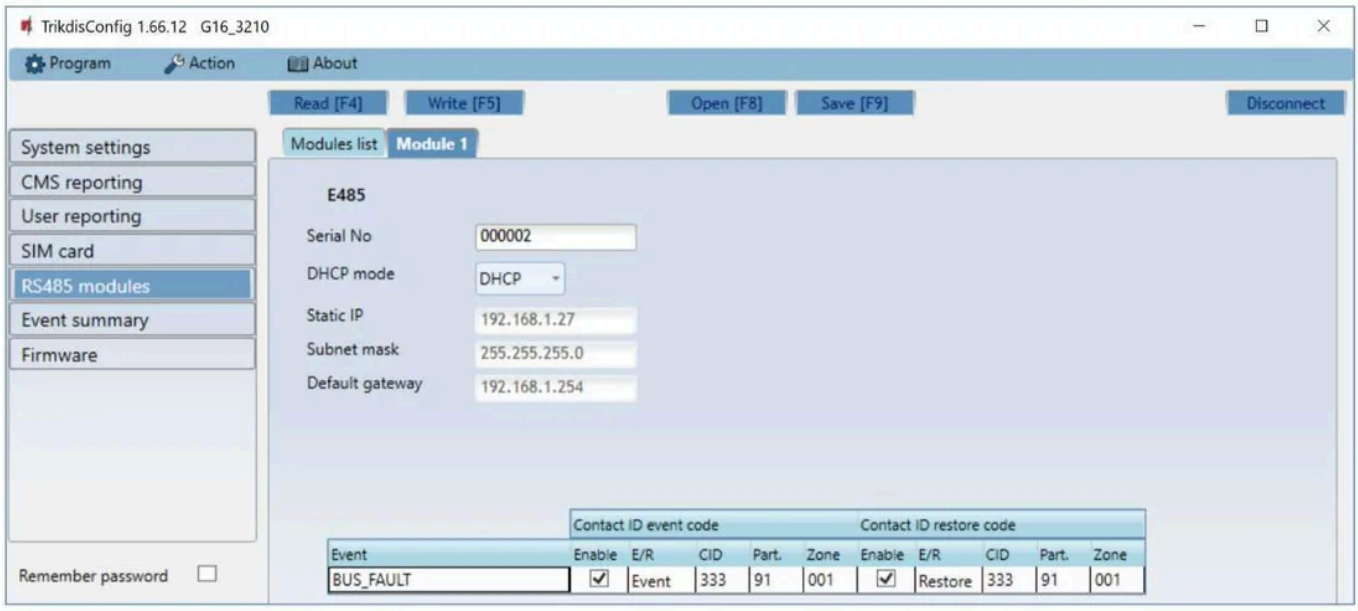


Obrázok 43. TrikdisConfig – RS485 modules, záložka modulu W485.

- **DHCP mode** – automatické (DHCP) alebo ručné (Static) sieťové nastavenie.
- **Static IP**, **Subnet mask**, **Default gateway** – pri ručnom nastavení.
- **Wifi SSID name**, **Wifi SSID password** – názov a heslo siete WiFi.

- V tabuľke môžeš chybám zbernice RS485 (prerušenie a obnovenie spojenia medzi modulom a G16) priradiť kód Contact ID; udalosť dostane PCO aj Protegus 2.

Modul E485 Ethernet – rovnaké sieťové nastavenia bez WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); aj tu môžeš v tabuľke chybe zbernice RS485 (prerušenie a obnovenie spojenia medzi E485 a G16) priradiť kód Contact ID, ktorý dostane PCO aj Protegus 2.



Obrázok 44. TrikdisConfig – RS485 modules, záložka modulu E485.

Na fungovanie W485 a E485 musí byť v G16 nastavené spojenie s PCO a/alebo s Protegus (body 2.3 a 2.4) a v G16 musí byť SIM karta. Kým funguje káblové alebo WiFi spojenie, komunikátor komunikuje cez neho a mobilné dátové spojenie nepoužíva.

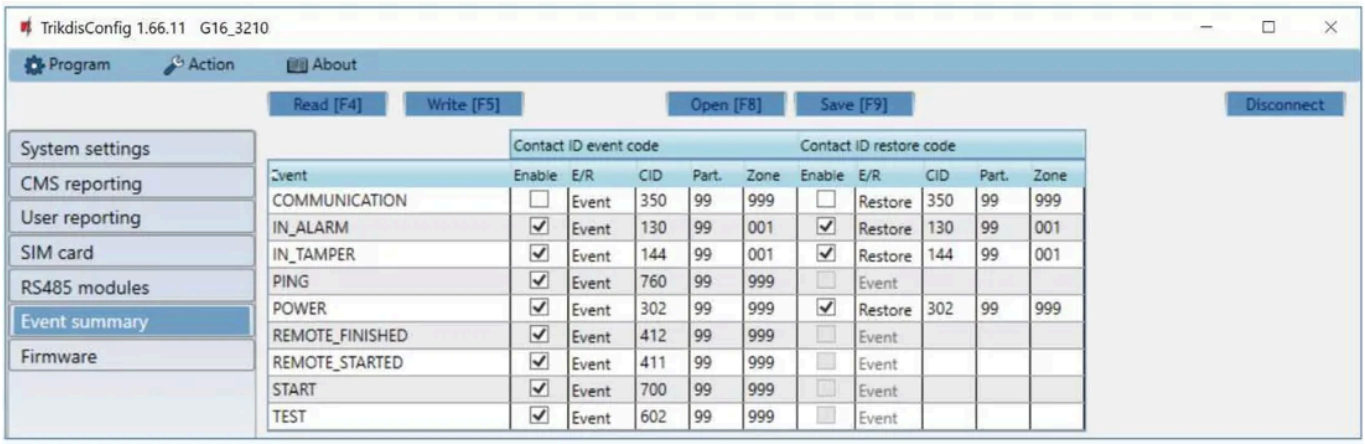
6.8 Event summary

Na tejto stránke môžeš zapnúť alebo vypnúť **vlastné, interné správy** zariadenia a zmeniť ich kód Contact ID, číslo partície a zóny. Správu, ktorú tu zakážeš, zariadenie neodošle žiadnym kanálom. Z výroby sa správy posielajú s partíciou 99 a zónou 999.

Správa	Contact ID	Kedy vzniká
COMMUNICATION	350	Prerušila sa komunikácia medzi komunikátorom a zabezpečovacou ústredňou (z výroby zakázané). Komunikátor pripojený na zbernicu alebo sériový port to zistí priamo; komunikátor na telefónnej linke iba so zapnutým **Line supervision**.
POWER	302	Nevyhovujúce (nízke) napájacie napätie; jeho obnovenie je samostatná správa.
REMOTE_STARTED	411	Začalo sa vzdialené programovanie cez TrikdisConfig.
REMOTE_FINISHED	412	Vzdialené programovanie sa skončilo.
START	700	Zariadenie sa pripojilo k sieti (spustenie).
TEST	602	Periodická testovacia správa.
PING	760	Správa signálu života PING. Nie je v zozname každého zariadenia: na obrazovke staršej hardvérovej verzie áno, na stránke Event summary novších verzií takýto riadok nie je. Jej interval nastavíš v poli **CMS reporting → Settings → IP ping period**.

- **Enable** – povolí odosielanie správy na PCO a do Protegus 2.
- **E/R** – typ správy: Event (udalosť) alebo Restore (obnovenie) – daný riadok znamená vznik udalosti alebo jej obnovenie.
- **Part.** – číslo partície (oblasti), ktoré zariadenie posiela pri internej udalosti a pri obnovení.
- **Zone** – číslo zóny, ktoré zariadenie posiela pri internej udalosti a pri obnovení.
- Kód **CID**, **partíciu** a **zónu** môžeš prepísať pri ktorejkoľvek udalosti; kde je obnovenie (Restore), jeho kód sa dá zadať samostatne.

Udalosti vlastných vstupov (**INx_ALARM**, **INx_TAMPER**) sa nastavujú na stránke **IN/OUT**, udalosti rozširujúcich modulov (**BUS_FAULT**, **INPUTx**) na stránke **RS485 modules**, na karte modulu. Povolenie a interval testovacej správy sa nastavujú v poli **CMS reporting → Settings → Test period**.



Obrázok 45. TrikdisConfig – stránka Event summary: interné správy zariadenia (na obrázku hardvérová verzia 3, pri ktorej sú tu aj udalosti vstupu IN_ALARM a IN_TAMPER a PING; na verzii 4 sú udalosti vstupov na stránke IN/OUT).

6.9 Obnovenie výrobných nastavení

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**.

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.

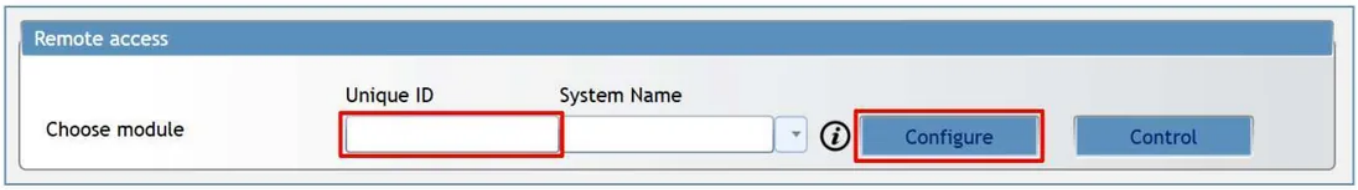
Na vzdialený prístup je potrebné:

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 46. TrikdisConfig – Remote access: identifikátor zariadenia, názov systému a tlačidlo Configure.

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.

Pri ústredni pripojenej na zbernicu skontroluj aj to, či komunikátor naozaj číta z ústredne: zapni a vypni stráženie ústredne na klávesnici a pozri, či sa udalosť v zozname udalostí Protegus 2 (a na PCO) zobrazí so správnym číslom partície a používateľa. Pri priamom ovládaní urob aj skúšobné zapnutie stráženia z aplikácie, kódom klávesnice používateľa.

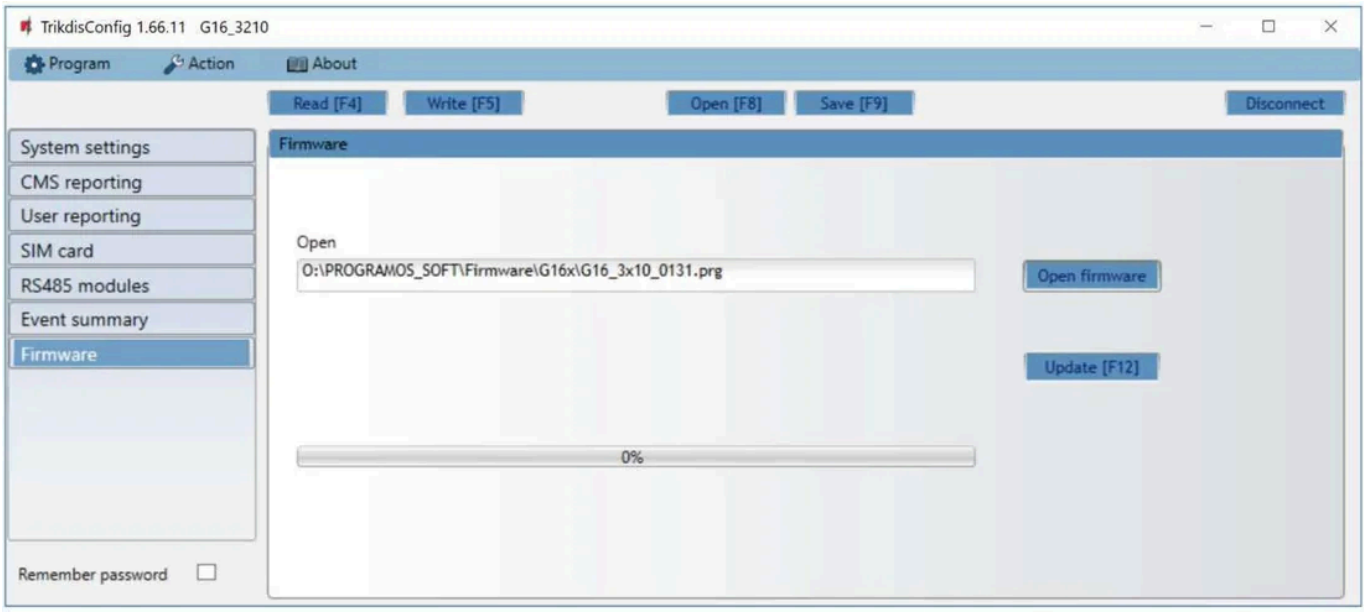
9. Aktualizácia firmvéru

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 47. TrikdisConfig – stránka Firmware: Open firmware a Update [F12].

Na aktualizáciu treba internetové pripojenie. Antivírus, firewall alebo prísne sieťové nastavenie môže zabrániť automatickému stiahnutiu firmvéru; vtedy uprav antivírus (povoľ TrikdisConfig prístup na internet) alebo stiahni súbor ručne a otvor ho na stránke Firmware.

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 nesvieti – nie je sieť

1. Pozri bliknutia LED **TROUBLE**: 1 = chýba SIM, 2 = nesprávny PIN, 3 = chýba APN, 4 = nevie sa pripojiť k mobilnej sieti, 5 = nevie sa pripojiť k dátovej sieti.
2. Skontroluj, či je SIM karta aktívna, má dátovú službu a dobre sedí v držiaku.
3. Ak je na karte zapnutá požiadavka na PIN, zadaj PIN na stránke **SIM card** alebo požiadavku na PIN vypni v telefóne.

4. Skontroluj anténu: je naskrutkovaná, nie je v kovovej krabici, úroveň signálu je vyhovujúca (body 1.7 a 3.2).

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. 6 bliknutí LED **TROUBLE** znamená, že nie je spojenie s prijímačom: skontroluj adresu prijímača, port, nastavenie TCP/UDP a šifrovací kľúč (**CMS reporting**).
2. Ak je prijímač zadaný doménovým menom, skontroluj nastavenie DNS (**CMS reporting** → **Settings**).
3. Pozri, či dátový balík SIM karty neblokuje potrebný port (niektoré karty M2M povoľujú len určené adresy).

LED TROUBLE blikne sedemkrát – komunikátor nevidí ústredňu

1. Skontroluj zapojenie podľa schémy v bode 3.3: najčastejšou chybou sú prehodené vodiče **CLK** a **DATA** alebo dátová linka zapojená na nesprávnu svorku ústredne.
2. V poli **System settings** → **Security panel model** v TrikdisConfig má byť zvolený presný typ zapojenej ústredne.
3. Pri ústredni Texecom, Caddx, Honeywell a InnerRange treba nastavenie aj v ústredni (kapitola 4) – bez neho ústredňa na zbernici nedáva dáta.
4. Pri ústredni Paradox môže byť sériový port z výroby zablokovaný – takto ho odblokuješ.
5. Ústredňu Pyronix po zapojení odpoj od napájania a znova spusti, aby komunikátor prijala.
6. S ústredňou DSC PowerSeries **NEO** G16 nefunguje (na zbernicu NEO nepovoľuje externé zariadenie) – sem treba komunikátor pre telefónnu linku.

Udalosti prichádzajú, ale z aplikácie neviem zapnúť stráženie

Pri priamom ovládaní:

1. Na stránke **System settings** má byť zaškrtnuté **Remote Arm/Disarm**.
2. Pri ústredni Paradox a Texecom sa má **Security panel PC download password** zhodovať s heslom PC, resp. UDL ústredne (body 4.2 a 4.3).
3. Pri ústredni Paradox má mať ústredňa firmvér aspoň **V.4**; kód používateľa nemá byť hlavný kód; po zmene kódu reštartuj komunikátor.
4. Pri ústredni Honeywell Vista má byť povolená 2. adresa AUI (bod 4.6).
5. V Protegus 2 **nemá** byť k partícii priradený výstup (Control with Protegus2 vypnuté).

So zónou kľúčového spínača:

1. **Remote Arm/Disarm** má byť prázdne, svorka I/O má byť na stránke **IN/OUT** nastavená na **OUT**.
2. Zóna ústredne má byť typu kľúčový spínač a v Protegus 2 má byť k partícii priradený správny výstup, v impulznom alebo dvojpolohovom režime podľa zóny (bod 5.3).

Protegus 2 nevidí zariadenie

1. Na stránke **User reporting → PROTEGUS Cloud** má byť zaškrtnuté **Enable connection**.
2. Pri vytváraní systému treba zadať **Protegus Cloud access code** nastavený v zariadení; po vytvorení systému ho v zariadení už nemožno zmeniť.
3. IMEI zadaj presne, z krabice alebo zo zadnej strany zariadenia.
4. Dátová služba SIM karty a APN majú byť v poriadku (LED NETWORK je zelená a LED DATA po udalosti zhasne).

Neviem sa na diaľku prihlásiť cez TrikdisConfig

1. Zariadenie má byť online (LED NETWORK zelená) a má byť povolené spojenie Protegus.
2. **CMS reporting → Settings → IP ping period** nemá byť dlhší ako 5 minút: PING udržiava spojenie potrebné na vzdialený prístup.
3. Skontroluj heslo administrátora alebo inštalátora.

Zabudol som heslo

Zabudnuté heslo sa nedá zistiť a nedá sa vymazať ani obnovením výrobných nastavení, pretože aj na obnovenie je potrebné heslo. Vtedy ho vie obnoviť iba výrobca alebo distribútor: zariadenie mu treba doručiť. Nastavené heslá si preto zapíš na bezpečné miesto.

Prečo nevidím stránku RS485 modules alebo prečo nefunguje iO-8?

G16 s modemom 2G (G16_G410) nemá zbernicu RS485; iO-8, W485 a E485 môžeš pripojiť len k verzii 4G (G16_54E0). Pre modul W485 a E485 musí byť v G16 aj SIM karta.

Mám zariadenie 2G – dokedy bude fungovať?

Vypínanie sietí 2G postupuje u jednotlivých operátorov rôznym tempom; na dlhodobé fungovanie odporúčame verziu 4G, ktorú môžeš rozšíriť aj cez zbernicu RS485.

Koľko dát zariadenie spotrebuje?

Správy o udalostiach a PING sú veľmi malé; prevádzka závisí hlavne od periódy PING a frekvencie testovacích hlásení. Pri bežnom domácom systéme zostáva mesačná prevádzka zvyčajne pod 10 MB. Presná hodnota závisí od nastavení a od jednotky účtovania operátora, preto sa pri karte s dátovým limitom oplatí skontrolovať prevádzku za prvý mesiac.

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 pozorne prečítaj návod; nedodržanie pokynov môže viesť k nesprávnemu fungovaniu alebo poruche.
- Pred zapojením, pri každom elektrickom pripájaní a pred servisom odpoj zariadenie od napájania.
- Chyby spôsobené nesprávnou inštaláciou alebo používaním, ako aj úpravy a opravy, ktoré výrobca nepovolil, rušia záruku.
- Dodržiavaj miestne predpisy o nakladaní s odpadom: chybné zariadenie ani jeho súčasti nevyhadzuj do komunálneho odpadu.

Pozri aj

- Vyhľadávač kompatibility – ktorý komunikátor sa hodí ku ktorej zabezpečovacej ústredni.
- G16 – priame ovládanie zabezpečovacích ústrední DSC PowerSeries – zapínanie stráženia kódom klávesnice, stavy zón, premosťovanie zón.
- DSC Power Series NEO a komunikátory Trikdis: kompatibilita a riešenia – prečo G16 nemožno pripojiť na NEO a aké je riešenie.
- Odblokovanie zablokovaného sériového portu na ústredniach Paradox – odblokovanie sériového portu novších ústrední Paradox.
- Zapínanie stráženia na diaľku kľúčovým spínačom z aplikácie Protegus 2 – podrobnosti a úskalia zapínania stráženia kľúčovým spínačom.
- Prichádza hardvérová verzia v4 komunikátorov G16 a G16T – čo sa zmenilo oproti verzii 3.
- Nastavenie APN – zoznam európskych mobilných operátorov – APN SIM karty podľa operátora.
- Dokumentácia v angličtine: docs.trikdis.com – návody na docs.trikdis.com sú v angličtine.

Súvisiace produkty

Trikdis G16 4G GSM inteligentný komunikátor

Trikdis G16 2G GSM inteligentný komunikačný modul

Prepojovací kábel Trikdis CRP2 sériového portu pre zabezpečovacie panely Paradox

Prepojovací kábel CRP2B sériového portu pre zabezpečovacie panely Paradox

Sériový kábel Trikdis CRP4 pre riadiace panely Texecom

Trikdis io8 káblový expanderový modul

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/g16-navod