GET-communicatiemodule – installatie- en gebruikershandleiding

Installatie- en gebruikershandleiding voor de Trikdis GET Ethernet + 4G-communicatiemodule: aansluiting op de alarmcentrale, LAN- en simkaartinstelling in TrikdisConfig, doormelding naar de meldkamer, de Protegus 2-app.



Uitgave: 2026-11-17
Altijd actuele webversie: https://nl.mobilamb.eu/get-handleiding

Inhoud

1. Overzicht

1.1 Waarvoor dient hij, hoe werkt hij
1.2 Versies: GET, GT en GT+
1.3 Compatibele alarmcentrales
1.4 Onderdelen van de communicatiemodule
1.5 Klemmen
1.6 Ledsignalen
1.7 Technische gegevens

2. Snelle inbedrijfstelling

2.1 Voorbereiding
2.2 Verbinding met de Protegus 2-app
2.3 Verbinding met de meldkamer

3. Installatie en aansluiting

3.1 Stappen van de installatie
3.2 Plaatsing in de behuizing van de centrale, antenne
3.3 Aansluiting op de alarmcentrale
3.3.1 DSC – databus (Keybus)
3.3.2 Paradox – seriële poort
3.3.3 Paradox SP/MG – Keybus en TIP/RING
3.3.4 UTC Interlogix (Caddx) – databus
3.3.5 Texecom – seriële poort
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – databus
3.3.9 Elke centrale – TIP/RING
3.4 Een sleutelschakelaarzone aansluiten
3.5 Ingangen aansluiten
3.6 Een uitgang aansluiten met een relais
3.7 Inschakelen en eerste controle
A TRIKDIS átjelző elindítása

4. De alarmcentrale programmeren

4.1 Aansluiting op databus of seriële poort
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Aansluiting op de telefoonlijn (TIP/RING)
4.2.1 De kiezer van de Honeywell Vista programmeren
4.2.2 De kiezer van de UTC Interlogix (Caddx) NX

5. Besturing op afstand met de Protegus 2-app

5.1 Het apparaat toevoegen
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 In- en uitschakelen met een uitgang

5.3 In- en uitschakelen vanuit de app

6. De instellingen in detail

6.1 Verbinding maken met de communicatiemodule

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Ontvangerkanalen (CMS settings)

6.4.2 Test, PING en de volgorde van de verbindingen

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 en SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Fabrieksinstellingen herstellen

7. Programmeren op afstand

8. De werking van de communicatiemodule controleren

9. Firmware bijwerken

10. Storingen zoeken en veelgestelde vragen

11. Veiligheidsvoorschriften

Zie ook

1. Overzicht

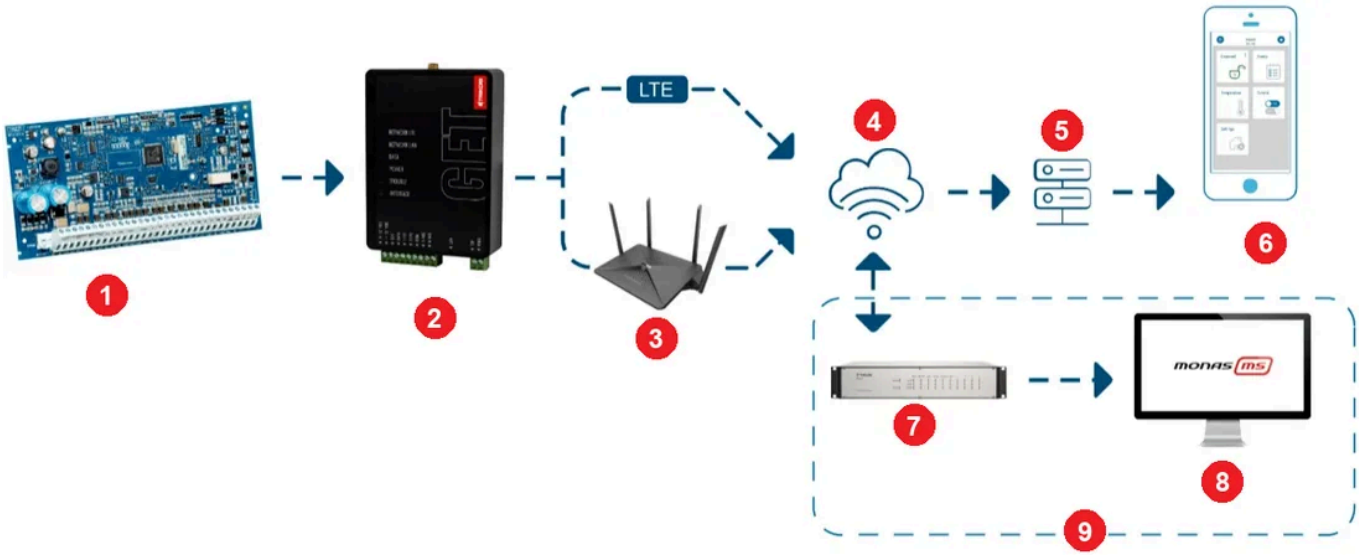
De GET is de **Ethernet + 4G-communicatiemodule** van Trikdis: hij stuurt de gebeurtenissen van de alarmcentrale via het bekabelde lokale netwerk (LAN) of via het mobiele netwerk door naar de meldkamer en naar de Protegus 2-app. Hij kan op twee manieren op de centrale worden aangesloten: **rechtstreeks**, op de databus of seriële poort van de centrale (bij centrales van DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange en Honeywell), of op de **telefoonkiezer van elke centrale** (TIP/RING) die de gebeurtenissen in Contact ID-formaat met DTMF-tonen verstuurt. De communicatiemodule geeft de volledige gebeurtenisinformatie (code, partitie, zone of gebruiker) door aan de meldkamer. Met de Protegus 2-app bestuurt de gebruiker het systeem op afstand en krijgt hij meldingen over de gebeurtenissen; de app werkt met elke centrale die de communicatiemodule ondersteunt, ongeacht het merk van de centrale. Doormelding naar de meldkamer en Protegus 2 kunnen tegelijk worden gebruikt. Deze handleiding is geschreven voor de GET-communicatiemodule met LTE (4G)-modem; de verschillen tussen de GET, de GT en de GT+ staan samengevat in paragraaf 1.2.

1.1 Waarvoor dient hij, hoe werkt hij

- **Hij meldt door naar de meldkamer.** Hij stuurt de gebeurtenissen via een IP-verbinding, over het bekabelde netwerk of het mobiele netwerk, naar een software- of hardwareontvanger van Trikdis (TRK8-protocol) – die werken samen met elke meldkamersoftware –, naar een SIA DC-09-ontvanger of naar een SUR-GARD-ontvanger (TL150). Aan een SUR-GARD-ontvanger geeft hij de Contact ID-codes van de centrale omgezet in SIA-codes door; de omzettingstabel staat in de bijlage van de Engelstalige documentatie op docs.trikdis.com. De verbinding met de ontvanger controleert hij elke 30 seconden (of met het interval dat u instelt) met een PING-bericht; als het primaire kanaal uitvalt, schakelt hij over naar het reservekanaal. Met een parallel kanaal gaan de gebeurtenissen tegelijk naar twee ontvangers. De verbindingsroutes – LAN, SIM1, SIM2 – kunt u in een volgorde zetten: als de hoofdroute niet werkt, schakelt de communicatiemodule over naar de reserveroute (paragraaf 6.4.2). Als ook de Protegus-dienst is ingeschakeld, ontvangt eerst de meldkamer de gebeurtenis, en pas daarna de app van de gebruikers.
- **Hij waarschuwt de gebruiker.** De Protegus 2-app meldt de gebeurtenissen met een pushbericht en een apart geluidssignaal; vanuit de app kan de gebruiker in- en uitschakelen en de aangesloten apparaten schakelen (verlichting, poort, ventilatie, verwarming, beregening enz.). In de app hebben de beheerder, de installateur en de gebruiker verschillende rechten. De GET stuurt geen meldingen per sms of oproep: de meldingen komen via de Protegus 2-app.
- **Hij bestuurt de centrale rechtstreeks.** Bij aansluiting op de databus of de seriële poort ziet de communicatiemodule ook de partitie- en zonestatussen van de centrale, en schakelt de gebruiker vanuit Protegus 2 in en uit met zijn eigen bediendeelcode – daarvoor is geen sleutelschakelaarzone nodig.
- **Hij heeft eigen in- en uitgangen.** Twee I/O-klemmen met dubbele functie kunnen worden gebruikt als ingang (IN) of als bestuurbare uitgang (OUT); af fabriek zijn ze allebei uitgang. De uitgangen kunt u schakelen vanuit de Protegus 2-app. De klemmen **A 485** en **B 485** worden op de GET niet gebruikt; op de GET kan geen RS485-uitbreidingsmodule worden aangesloten.
- **Hij kan met twee hulpmiddelen worden ingesteld.** De instellingen kunnen worden gemaakt met het Windows-programma TrikdisConfig (via een USB-C-kabel of op afstand) en – met firmware 1.08 of nieuwer – ook vanuit de Protegus 2-app (Settings → Advanced settings). De instellingen kunnen in een bestand worden opgeslagen en naar andere communicatiemodules worden geschreven. Er zijn twee

toegangsniveaus: dat van de beheerder van de meldkamer en dat van de installateur. De communicatiemodule kan ook op afstand worden ingesteld, en ook de firmware kan op afstand worden bijgewerkt.

De opbouw van het systeem ziet u in de onderstaande afbeelding: de alarmcentrale is aangesloten op de communicatiemodule, de communicatiemodule bereikt het internet op twee manieren – via het mobiele netwerk (LTE) of via de router (LAN) –, en daarlangs de ontvanger van de meldkamer (met de bijbehorende software) en de Protegus-server; de gebruiker ziet het systeem in de Protegus 2-app.



Afbeelding 1. De plaats van de communicatiemodule in het systeem: alarmcentrale → GET → mobiel netwerk (LTE) of router (LAN) → internet → ontvanger van de meldkamer en Protegus-server → Protegus 2-app.

- 1 alarmcentrale („Alarm panel")
- 2 GET LTE-communicatiemodule („LTE communicator")
- 3 router („Router")
- 4 internet („Internet")
- 5 Protegus-server („Protegus server")
- 6 telefoon met de Protegus-app („Phone with Protegus software")
- 7 ontvanger van de meldkamer („Receiver")
- 8 meldkamersoftware („Monitoring software")
- 9 de meldkamer van het beveiligingsbedrijf („Monitoring station in security company") – in het gestippelde kader

1.2 Versies: GET, GT en GT+

De GET is de broer met Ethernetpoort van de GT- en de GT+-communicatiemodule: de aansluiting en het programmeren van de alarmcentrale, de reeks compatibele centrales, de modem, de transmissieprotocollen en het gebruik van Protegus 2 zijn gelijk, en daarom hebben de handleidingen van de drie communicatiemodules ook dezelfde hoofdstukindeling. De verschillen staan samengevat in de onderstaande tabel.

	GET	GT	GT+
Netwerkverbinding	**LTE (4G) en Ethernet (LAN, RJ45)**; de volgorde van de verbindingsroutes is instelbaar (Main / Backup / Backup 2: LAN, SIM1, SIM2; paragraaf 6.4.2)	LTE (4G)	LTE (4G)

	GET	GT	GT+
Simkaart	**2 nano-simhouders** (SIM1, SIM2); er kunnen één of twee kaarten in	1 nano-sim	1 nano-sim
Voedingsspanning	10–18 V DC	10–18 V DC	10–32 V DC
Stroomverbruik	maximaal 100 mA in rust, 300 mA tijdens het verzenden van gegevens	maximaal 100 / 200 mA	maximaal 100 / 200 mA
Afmetingen, gewicht	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g
Klemmen	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; aparte **LAN**-aansluiting (RJ45) en TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Fabrieksinstelling van de I/O-klemmen	uitgang (OUT)	ingang (IN, NO)	ingang (IN, NO)
RS485-bus, iO-8-uitbreiding	de klemmen A 485 / B 485 worden **niet gebruikt**; er kan geen uitbreiding worden aangesloten	maximaal 4 iO-8	maximaal 4 iO-8
Leds	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (niet gebruikt)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Knipperingen van de TROUBLE-led	1 = fysieke LAN-verbinding (kabel), 2 = SIM1-fout, 3 = SIM2-fout, 7 = centrale	1–8 (sim, pincode, APN, netwerk, ontvanger, centrale, ICCID)	1–8
Sms en oproep	geen sms-melding, geen sms-commando's en geen oproep: melding en besturing gaan via Protegus 2	melding per sms en oproep, sms-commando's	melding per sms en oproep, sms-commando's
DSC-centrale tegelijk op de databus en op de TIP/RING-klemmen	nee	nee	ja
Instelling voor aansluiting op TIP/RING (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (ook **3. MANUAL** kan worden gekozen)
Instellen vanuit de Protegus 2-app	ja (Advanced settings, vanaf firmware 1.08)	TrikdisConfig	TrikdisConfig
Gebeurtenisgeheugen	60 gebeurtenissen	geen gegevens	geen gegevens
Interne berichten (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	als de GT

	GET	GT	GT+
Modem, transmissieprotocollen (TRK8, DC-09, TL150), versleuteling, compatibele centrales, aansluitschema's, Protegus 2	gelijk	gelijk	gelijk

Alle drie de communicatiemodules worden met dezelfde drie soorten modem gemaakt; voor de Europese markt is de Europese (EU-)versie de juiste. Het modemtype en de hardwareversie vindt u in de statusbalk van TrikdisConfig (**Device**, **HW**) en op het label van het apparaat.

Modem	Netwerk en frequentiebanden
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (Latijns-Amerika)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Compatibele alarmcentrales

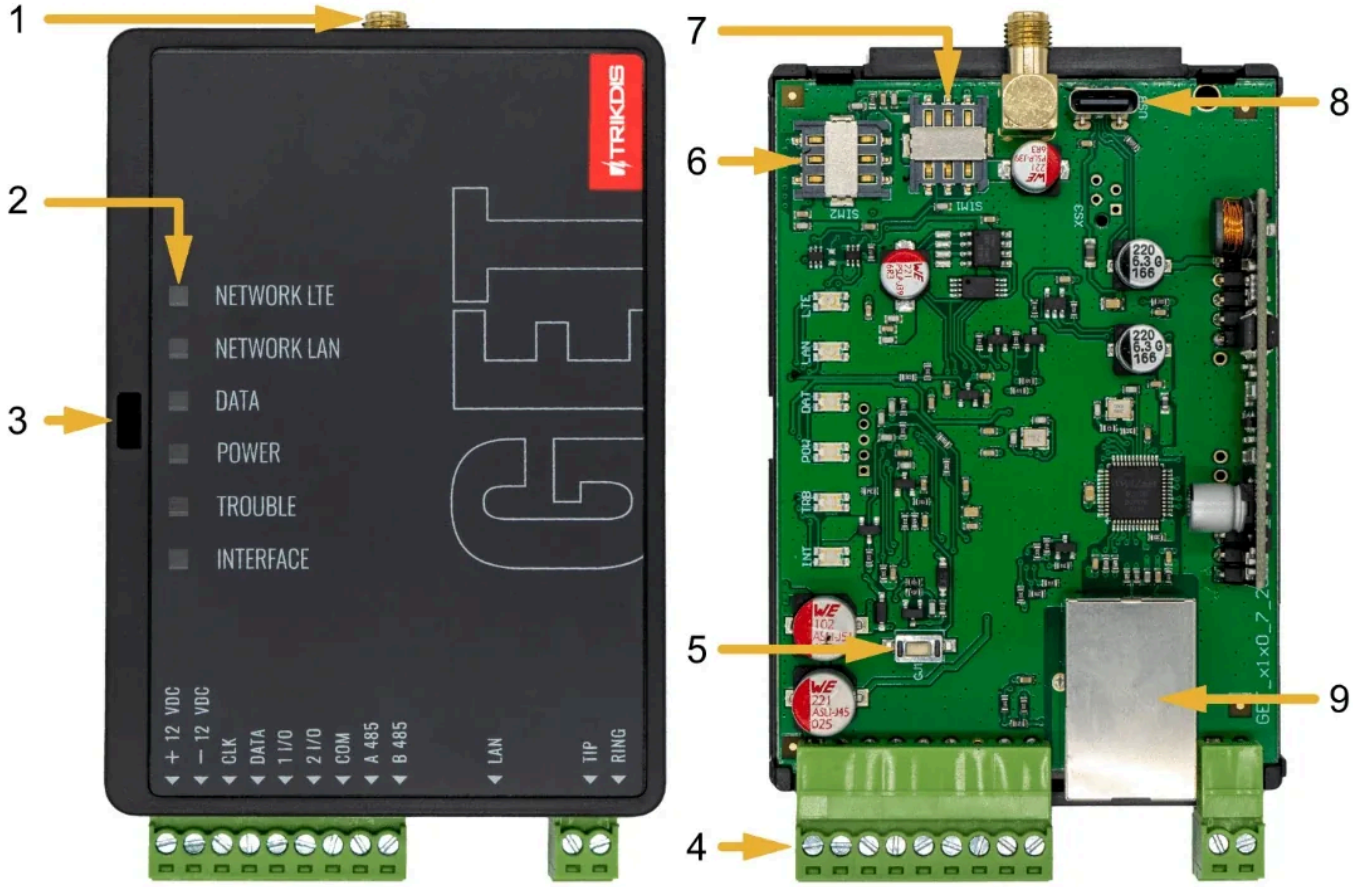
De onderstaande centrales kunnen rechtstreeks, via de databus of de seriële poort, op de communicatiemodule worden aangesloten. De kolom „Directe besturing" geeft aan of de gebruiker vanuit Protegus 2 met zijn eigen bediendeelcode kan in- en uitschakelen zonder extra bedrading; waar dat niet mogelijk is, leest de communicatiemodule de gebeurtenissen van de bus, en voor de besturing is een sleutelschakelaarzone nodig (paragraaf 3.4).

Merk	Type	Aansluiting	Directe besturing
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	databus (Keybus)	ja
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	seriële poort (EX-CRP2.4-kabel), of Keybus + TIP/RING	ja
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	seriële poort (EX-CRP2.4-kabel), of Keybus + TIP/RING	ja
Paradox	Digiplex EVO192, EVOHD, EVOHD+	seriële poort (EX-CRP2.4-kabel)	ja
Paradox	Digiplex EVO48	seriële poort (EX-CRP2.4-kabel)	nee
Paradox	Spectra 1727, 1728, 1738; Esprit E55	seriële poort (EX-CRP2.4-kabel)	nee
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	databus	ja
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	seriële poort (EX-CRP4-kabel)	ja
InnerRange	Inception, Integriti	seriële poort (met de kabel van de fabrikant van de centrale)	nee
Honeywell	Ademco Vista-15, Vista-20, Vista-48	databus	ja

- De firmware van direct bestuurde **Paradox**-centrales moet minimaal **V.4** zijn. Op de nieuwere Paradox-centrales (SP+, MG+, EVOHD+) kan de seriële poort af fabriek vergrendeld zijn; over het ontgrendelen gaat paragraaf 4.1.2. De centrales Spectra SP / SP+ en Magellan MG / MG+ kunnen in plaats van via de seriële poort ook tegelijk op de databus (Keybus) en op de TIP/RING-klemmen worden aangesloten – daarvoor is de betaalde ontgrendeling niet nodig, maar de firmware van de communicatiemodule moet minimaal 1.21 zijn (paragraaf 3.3.3).
- De centrales van **alle andere merken** worden aangesloten via hun telefoonkiezer (TIP/RING), als die de gebeurtenissen in Contact ID-formaat met DTMF-kiezen verstuurt; in dat geval is voor de besturing een sleutelschakelaarzone nodig.
- Welke Trikdis-communicatiemodule en welke aansluiting bij uw centrale past, ziet u in de Compatibiliteitszoeker.

1.4 Onderdelen van de communicatiemodule

De printplaat van de communicatiemodule zit in een zwarte kunststof behuizing; het frontdeksel kan worden losgeklikt, de klemmenstrook kan worden uitgetrokken. De LAN-aansluiting en de TIP/RING-klem zijn aan de zijkant van de behuizing bereikbaar, via een aparte opening.



Afbeelding 2. De onderdelen van de communicatiemodule van voren (links) en met geopende behuizing (rechts).

- 1 SMA-connector voor de mobiele antenne
- 2 Leds (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Opening om het frontdeksel los te klikken
- 4 Afneembare klemmenstrook voor de externe aansluitingen
- 5 RESET-knop
- 6 Houder voor de SIM2-kaart
- 7 Houder voor de SIM1-kaart
- 8 USB-C-aansluiting voor het programmeren
- 9 Ethernet (LAN) RJ45-aansluiting

De klemmenstrook kan worden uitgetrokken: zo kan het apparaat met één beweging spanningsloos worden gemaakt of opnieuw worden opgestart, is het bij het aansluiten makkelijker te hanteren, en kan het voor programmeren via USB naar de computer worden meegenomen.

1.5 Klemmen

Klem	Functie
+12 VDC	Voeding, positief: +10–18 V DC
–12 VDC	Voeding, 0 V
CLK	Seriële bus of databus (klok) voor de rechtstreekse aansluiting van de centrale
DATA	Seriële bus of databus (data) voor de rechtstreekse aansluiting van de centrale
1 I/O	1e in-/uitgang (fabrieksinstelling: uitgang, OUT)
2 I/O	2e in-/uitgang (fabrieksinstelling: uitgang, OUT)
COM	Gemeenschappelijk (negatief) punt voor de ingangen en uitgangen
A 485	Niet gebruikt
B 485	Niet gebruikt (het paar van A 485)
LAN	Ethernet (lokaal netwerk) RJ45-aansluiting
TIP	TIP-klem van de telefoonkiezer van de alarmcentrale
RING	RING-klem van de telefoonkiezer van de alarmcentrale

Op de aansluitschema's zijn de voedingsklemmen aangeduid met **+DC** en **–DC** (op het apparaat +12 VDC / –12 VDC), en de RS485-klemmen met **A RS485** / **B RS485** (op het apparaat A 485 / B 485). Het opschrift van de klemmenstrook staat ook op het frontdeksel.

1.6 Ledsignalen

De leds op het frontdeksel zijn het belangrijkste hulpmiddel bij de inbedrijfstelling en bij het zoeken naar storingen. Lees ze samen: POWER toont de voeding, NETWORK LTE het mobiele netwerk, NETWORK LAN het bekabelde netwerk, TROUBLE de storing; de INTERFACE-led heeft op de GET geen functie.

NETWORK LTE – verbinding met het mobiele netwerk

Signaal	Betekenis
uit	Geen verbinding met het mobiele netwerk
knippert geel	Bezig met verbinden met het mobiele netwerk
brandt groen, knippert geel	Verbonden met het mobiele netwerk; het aantal gele knipperingen is de **signaalsterkte**: op 4G zijn 3 knipperingen een goed signaal

NETWORK LAN – verbinding met het bekabelde netwerk

Signaal	Betekenis
uit	Geen verbinding met het computernetwerk
brandt groen	Verbonden met het computernetwerk

DATA – dataverkeer

Signaal	Betekenis
uit	Geen gebeurtenissen die wachten op verzending
brandt groen	Er staan gebeurtenissen in het geheugen die wachten op verzending
knippert groen	Gegevensoverdracht tussen de communicatiemodule en de computer (tijdens het programmeren)

Snelle controle

De DATA-led is de eenvoudigste internetcontrole. De DATA-led brandt wanneer er in het geheugen van het apparaat een bericht klaarstaat om te worden verzonden. Het groene licht van de NETWORK-led zegt alleen dat de netwerkverbinding tot stand is gekomen – bij een apparaat met mobiel netwerk heeft het zich aangemeld op het netwerk van de provider, bij een Ethernet-apparaat werkt de verbinding tot aan de router –, maar niet dat het apparaat ook het internet bereikt. Als de NETWORK-led groen is, maar de DATA-led ook na een gebeurtenis of testrapport continu blijft branden, werkt de internetverbinding niet: het bericht kan niet worden verzonden. Op een mobiel netwerk ligt de fout meestal bij de APN of de datadienst van de simkaart, bij Ethernet bij de router, de firewall of de DNS. Als de DATA-led uitgaat, is het bericht verzonden en is de dataverbinding in orde.

POWER – voedingsspanning

Signaal	Betekenis
uit	Geen voeding, of de voeding is losgekoppeld
brandt groen	Ingeschakeld, de voedingsspanning is in orde
brandt geel	Onvoldoende voedingsspanning (maximaal 11,5 V)
brandt groen, knippert geel	Klaar voor programmeren (tijdens het programmeren)
brandt geel (tijdens het programmeren)	Geen verbinding met de computer

TROUBLE – storing

Signaal	Betekenis
uit	Geen storing
1 rode knippering	Storing in de fysieke verbinding van het bekabelde netwerk (PHY Link) – controleer de LAN-kabel
2 rode knipperingen	Storing van de SIM1-kaart
3 rode knipperingen	Storing van de SIM2-kaart
7 rode knipperingen	De verbinding met de alarmcentrale is verbroken (seriële bus)

INTERFACE – wordt op de GET niet gebruikt.

1.7 Technische gegevens

Parameter	Waarde
Netwerkverbinding	LTE (4G) en Ethernet (LAN)
Verbinding met de alarmcentrale	seriële bus, databus (Keybus) of telefoonlijn (TIP/RING, Contact ID, DTMF)
In-/uitgangen	2 I/O's met dubbele functie: als ingang NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (eindweerstand 2,2 kΩ); als uitgang open collector (OC), max. 0,15 A / 30 V DC

Parameter	Waarde
Modem	EG915U-EU (Europa), EG915U-LA (Latijns-Amerika) of BG95-M5 (LTE Cat M1) – de frequentiebanden staan in de tabel van paragraaf 1.2
Simkaart	2 nano-simhouders (SIM1, SIM2)
Voedingsspanning	10–18 V DC
Stroomverbruik	maximaal 100 mA in rust; maximaal 300 mA tijdens het verzenden van gegevens
Transmissieprotocollen	TRK8, DC-09_2007, DC-09_2012, TL150
Versleuteling	AES-128
Gebeurtenisgeheugen	60 gebeurtenissen
Programmeren	TrikdisConfig (Windows) via een USB-C-kabel of op afstand; Protegus 2-app (vanaf firmware 1.08)
Gebruiksomgeving	−10 … +50 °C, max. 80 % relatieve luchtvochtigheid (bij +20 °C)
Afmetingen	113 × 70 × 25 mm
Gewicht	110 g

2. Snelle inbedrijfstelling

De instellingen van de communicatiemodule kunnen met twee hulpmiddelen worden gemaakt: met het Windows-programma **TrikdisConfig** – via een USB-C-kabel of op afstand – en vanuit de **Protegus 2-app** (Settings → Advanced settings). In dit hoofdstuk beschrijven we de kortste weg: welke instellingen nodig zijn om de communicatiemodule gebeurtenissen naar de meldkamer te laten sturen, en om het systeem vanuit de Protegus 2-app bestuurbaar te maken. Bij elke stap geven we zowel het pad in de app als in TrikdisConfig; de uitgebreide uitleg van de instellingen staat in hoofdstuk 6.

2.1 Voorbereiding

Wat u nodig hebt

USB-C-kabel voor het programmeren · kabel met minimaal 4 aders tussen de communicatiemodule en de centrale · voor de seriële poort van Paradox een CRP2.4-kabel · platte schroevendraaier van 2,5 mm · een mobiele antenne met voldoende versterking als de dekking ter plaatse zwak is · een actieve simkaart (één of twee; de pincodevraag kan worden uitgeschakeld) als u het mobiele netwerk gebruikt · een Ethernetkabel tot aan de router of switch als u het bekabelde netwerk gebruikt · de installatiehandleiding van de alarmcentrale.

Bestel de benodigde accessoires apart bij de distributeur.

Instellen met TrikdisConfig. U stelt het apparaat op de werktafel in, vóór het aansluiten; daarna hoeft het ter plaatse alleen nog te worden aangesloten.

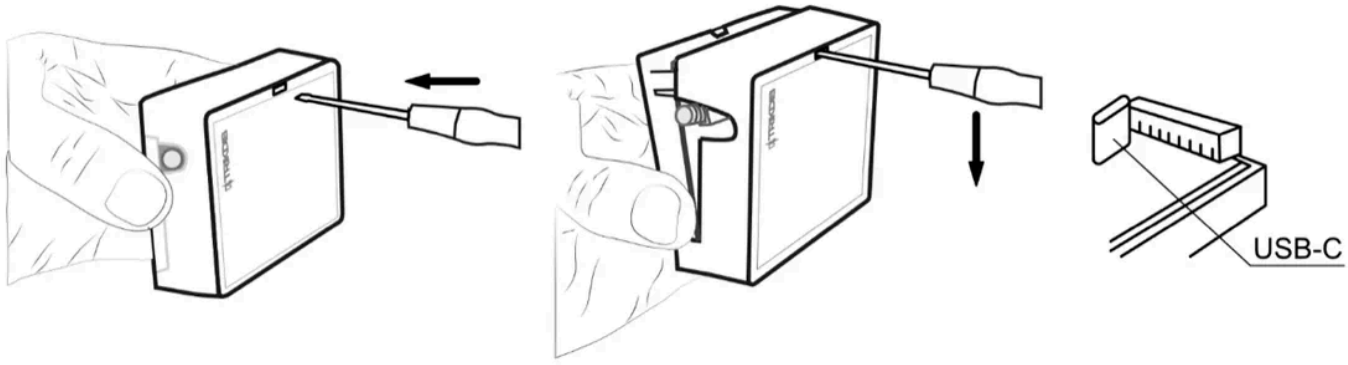
1. Download en installeer de TrikdisConfig-software. Typ op de website van Trikdis (www.trikdis.com) in het zoekveld: „TrikdisConfig”.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

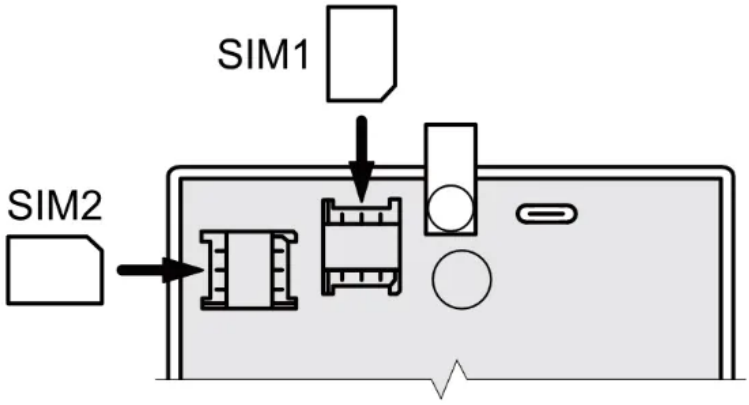
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Open de behuizing van de communicatiemodule met een platte schroevendraaier: steek de schroevendraaier bovenaan in de spleet naast de antenne en wrik naar buiten, daarna onderaan, bij de opening, naar beneden. De afbeelding toont ook de plaats van de USB-C-aansluiting aan de rand van de printplaat.



Afbeelding 3. Het frontdeksel losklikken met een platte schroevendraaier; het vergrote detail is de plaats van de USB-C-aansluiting.

3. Plaats de nano-simkaart (of kaarten) in de houder, in de richting die op de afbeelding te zien is: de SIM1-houder zit in het midden van de printplaat, de SIM2-houder aan de rand. De kaart moet actief zijn, er moet een mobiele datadienst op zitten, en schakel de pincodevraag zo mogelijk uit in een telefoon (dan hoeft u in het apparaat geen pincode in te voeren). Als u de communicatiemodule alleen op het bekabelde netwerk gebruikt, is geen simkaart nodig.



Afbeelding 4. De plaats van de SIM1- en de SIM2-houder op de printplaat; de pijlen tonen de richting waarin de kaart wordt geplaatst.

4. Verbind de communicatiemodule met de computer via een USB-C-kabel.

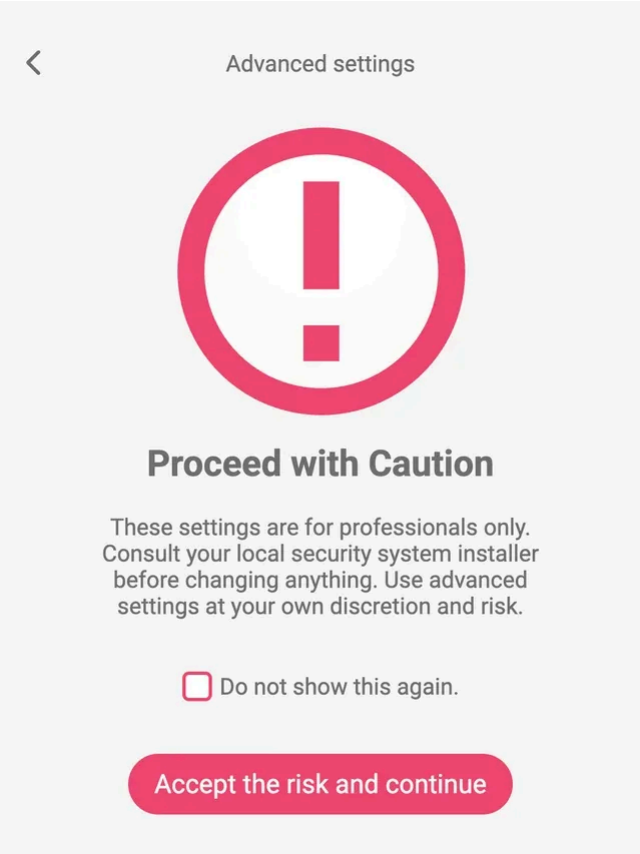
Waarschuwing

Zolang het apparaat via een USB-kabel met de computer is verbonden, staat het in de programmeermodus: de normale werking stopt, het bewaakt niet, meldt niet, is niet te bedienen, wordt via USB gevoed en start opnieuw op nadat de kabel is losgekoppeld. Het apparaat mag daarom niet vrij toegankelijk zijn: plaats het in een afgesloten metalen behuizing met sabotagebeveiliging (tamper) of met een bewegingsmelder die de behuizing bewaakt. Meer details in de FAQ

5. Start TrikdisConfig. Het programma herkent het apparaat en opent het programmeervenster. Klik op de knop **Read [F4]** (lezen): het programma leest de huidige instellingen van het apparaat uit. Als het om een wachtwoord vraagt, voer dan de 6-cijferige code van de beheerder (af fabriek `123456`) of van de installateur (af fabriek `654321`) in.

Instellen vanuit de Protegus 2-app. Vanuit de app kunt u instellen als de communicatiemodule al online is en u hem aan uw Protegus-account hebt toegevoegd (paragraaf 5.1). Als de communicatiemodule nog geen verbinding kan maken – bijvoorbeeld omdat de simkaart om een pincode vraagt, of omdat de provider een andere APN nodig heeft –, voer de eerste instelling dan uit met TrikdisConfig.

1. Open het systeem in de app en ga naar het menu **Settings** → **Advanced settings**.
2. De eerste keer geeft de app een waarschuwing (**Proceed with Caution**): deze instellingen zijn bedoeld voor vakmensen. Tik op de knop **Accept the risk and continue**; met het vinkje **Do not show this again** verschijnt de waarschuwing de volgende keer niet meer.
3. De app leest de instellingen van de communicatiemodule uit. Als hij om een **Service Access code** vraagt, voer dan de Protegus Cloud-toegangscode van de communicatiemodule in (af fabriek `123456`).
4. Maak de hieronder beschreven instellingen en tik daarna op de knop **Write**: de app schrijft ze naar de communicatiemodule.



Afbeelding 5. Protegus 2 – de waarschuwing (Proceed with Caution) die verschijnt wanneer Advanced settings voor het eerst wordt geopend, en de knop Accept the risk and continue.

Vanuit de Protegus 2-app kan de GET worden ingesteld met **firmware 1.08 of nieuwer** (het bijwerken staat beschreven in hoofdstuk 9).

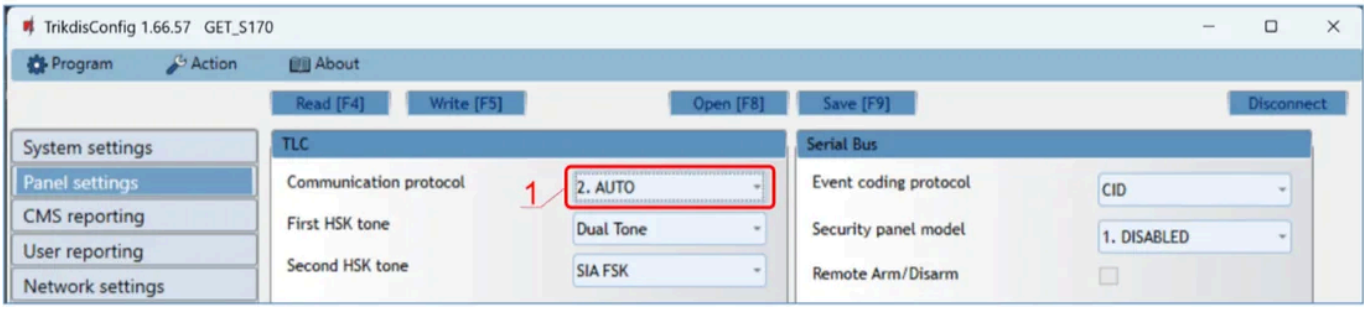
2.2 Verbinding met de Protegus 2-app

In de app (Settings → Advanced settings):

1. **Panel settings** → **TLF** – als de communicatiemodule op de TIP/RING-klemmen van de centrale is aangesloten: zet **Security panel model** op **AUTO**.
2. **Panel settings** → **Serial Bus** – als de communicatiemodule op de databus of seriële poort van de centrale is aangesloten: kies in het veld **Security panel model** het type van de aangesloten centrale.
3. Schakel op dezelfde plaats de optie **Remote Arm/Disarm** in als de gebruikers de centrale vanuit Protegus 2 met hun eigen bediendeelcode willen besturen. Verschijnt alleen bij de direct bestuurbare centrales.
4. Voor directe besturing van een Paradox-centrale voert u het **PC download password** in, bij een Texecom-centrale de **UDL passcode**; die moet overeenkomen met het wachtwoord dat in de centrale is ingesteld.
5. **User reporting** → **Cloud**: schakel de optie **Enabled** in, en wijzig de **Cloud access code** als u wilt dat de gebruiker die moet invoeren wanneer hij het systeem in gebruik neemt (af fabriek `123456`).
6. **Network settings** → **LAN** – als de communicatiemodule op het bekabelde netwerk is aangesloten: schakel de optie **Use DHCP** in.
7. **Network settings** → **SIM** en **SIM2** – voor elke geplaatste simkaart: voer de **SIM card PIN** en de **APN** in, en controleer of **DNS1** en **DNS2** bij uw provider werken.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: stel in de velden **Main type**, **Backup type** en **Backup type 2** in in welke volgorde de communicatiemodule de verbindingen **LAN**, **SIM** (SIM1) en **SIM2** gebruikt.
9. Tik op de knop **Write**.

In TrikdisConfig. Geef eerst op de pagina **Panel settings** aan hoe de communicatiemodule op de centrale is aangesloten.

Als u hem op de telefoonlijnuitgang (TIP/RING) van de centrale aansluit: kies in het veld **Communication protocol** de waarde **AUTO**.



Afbeelding 6. TrikdisConfig – Panel settings, groep TLC.

- 1 **Communication protocol** – bij aansluiting op TIP/RING **2. AUTO**.

Als u hem op de databus of seriële poort van de centrale aansluit: stel de centrale in de groep **Serial bus** in.

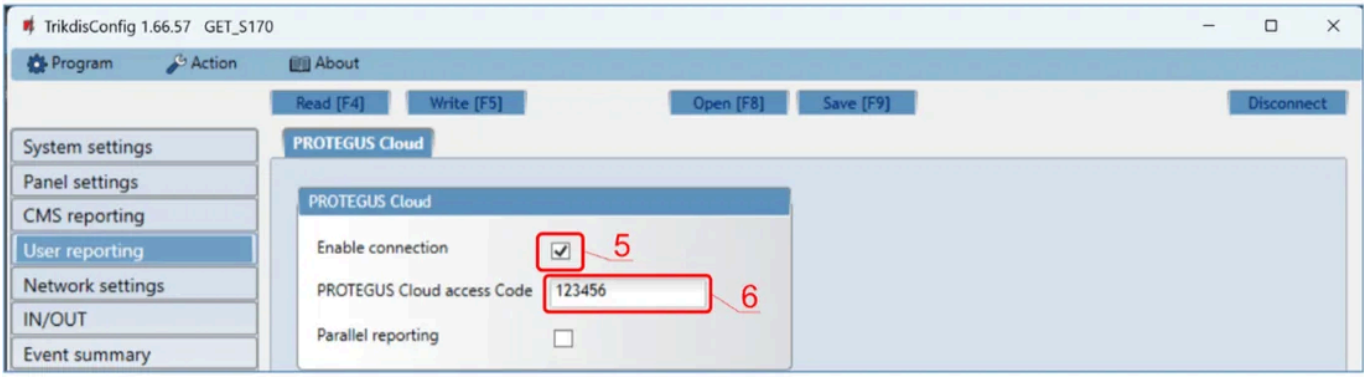


Afbeelding 7. TrikdisConfig – Panel settings, groep Serial bus.

- 2 **Security panel model** – het type van de aangesloten centrale.
- 3 **Remote Arm/Disarm** – vink dit aan als de gebruikers de centrale vanuit Protegus 2 met hun eigen bediendeelcode willen besturen. Verschijnt alleen bij de direct bestuurbare centrales.
- 4 **Security panel PC download password** – voor directe besturing van een Paradox- of Texecom-centrale het PC- resp. UDL-wachtwoord dat in de centrale is ingesteld; de twee moeten overeenkomen.

Voor directe besturing moet ook de alarmcentrale worden ingesteld – dat staat beschreven in hoofdstuk 4, waar u ook vindt hoe u het PC- resp. UDL-wachtwoord invoert.

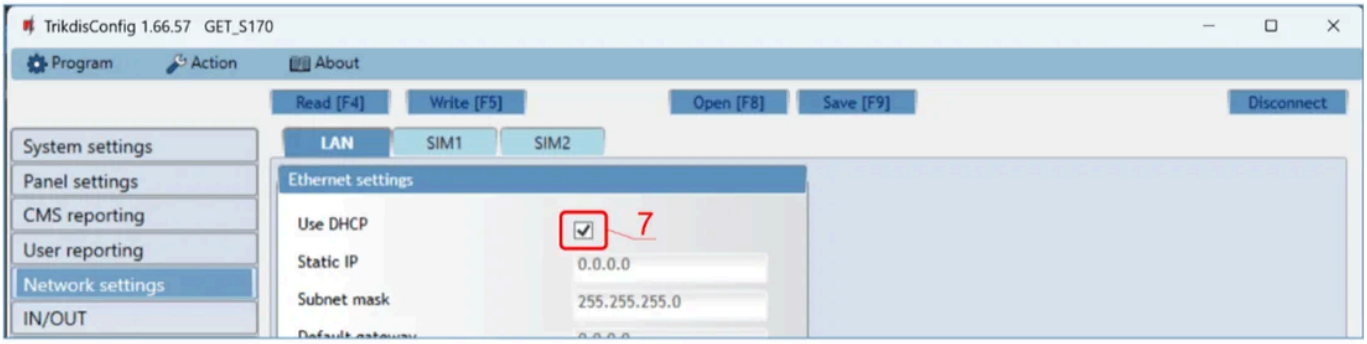
Schakel daarna op de pagina **User reporting**, op het tabblad **PROTEGUS Cloud**, de cloudverbinding in.



Afbeelding 8. TrikdisConfig – User reporting, tabblad PROTEGUS Cloud.

- 5 **Enable connection** – vink dit aan: dit schakelt de verbinding met de Protegus-cloud in.
- 6 **PROTEGUS Cloud access Code** – de toegangscode voor Protegus 2 (af fabriek `123456`). Wijzig deze als u wilt dat de gebruiker die moet invoeren wanneer hij het systeem in gebruik neemt. Als u de code later wijzigt, moet die ook in de Protegus 2-app worden aangepast.

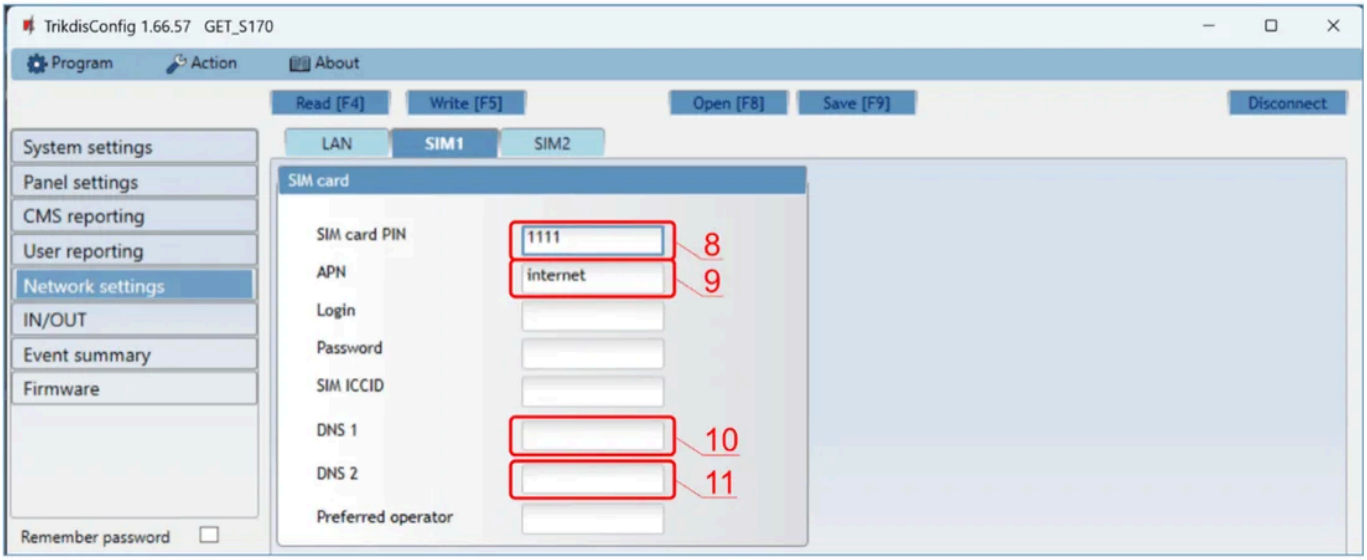
Als de communicatiemodule op het bekabelde netwerk is aangesloten, vinkt u op de pagina **Network settings**, op het tabblad **LAN**, de optie **Use DHCP** aan: de communicatiemodule krijgt de netwerkinstellingen (subnetmasker, gateway) automatisch, en krijgt een IP-adres.



Afbeelding 9. TrikdisConfig – Network settings, tabblad LAN (Ethernet settings).

- 7 **Use DHCP** – aangevinkt krijgt de communicatiemodule automatisch een IP-adres en netwerkinstellingen van de router.

Als er een simkaart (één of twee kaarten) in de communicatiemodule zit, voert u op het tabblad **SIM1** (en **SIM2**) de gegevens van de kaart in.



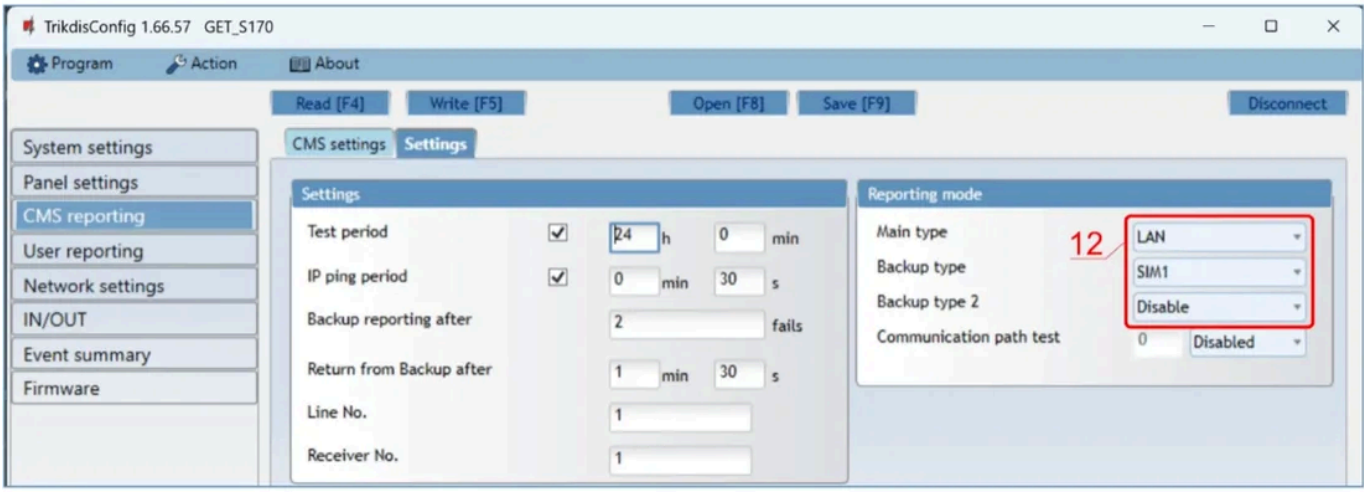
Afbeelding 10. TrikdisConfig – Network settings, tabblad SIM1.

- 8 **SIM card PIN** – de pincode van de kaart (als de pincodevraag is uitgeschakeld, kan de fabriekswaarde blijven staan).
- 9 **APN** – het toegangspunt voor de dataverbinding van de provider (zie hieronder).
- 10 **DNS 1** – primaire naamserver; af fabriek die van Google. Controleer, ongeacht de IP-instellingen, of de DNS-adressen bij uw provider werken.
- 11 **DNS 2** – secundaire naamserver (af fabriek ook die van Google).

De APN (Access Point Name) is het toegangspunt voor de dataverbinding van de mobiele provider; zonder APN kan het apparaat via het mobiele netwerk geen verbinding met het internet maken. De precieze waarde vindt u op de website van de provider van de simkaart. De bekende APN's van Europese providers houden we bij in een apart artikel: APN-instelling – lijst van Europese mobiele providers. Als u van de provider geen andere gegevens hebt, probeer dan de APN `internet`: die is algemeen geldig en werkt in het netwerk van veel providers.

Voor een IoT- / M2M-datakaart (communicatie tussen machines) geeft de provider meestal **een andere APN dan voor consumentenkaarten** – met de consumenten-APN maakt het apparaat geen verbinding. Ook deze waarde vindt u in het APN-artikel, of vraag die aan de provider; als de provider ook een gebruikersnaam en wachtwoord opgeeft, voer die dan ook in.

Geef ten slotte op de pagina **CMS reporting**, op het tabblad **Settings**, in de groep **Reporting mode** de volgorde van de verbindingen op: via deze route stuurt de communicatiemodule de berichten naar de meldkamer en naar Protegus 2.



Afbeelding 11. TrikdisConfig – CMS reporting, tabblad Settings, groep Reporting mode (af fabriek Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type**: de hoofdverbinding (LAN, SIM1 of SIM2); **Backup type**: de reserve; **Backup type 2**: de tweede reserve.

U geeft de verbindingstypes op in volgorde. Als de communicatiemodule met de verbinding **Main type** geen verbinding kan maken, schakelt hij over naar **Backup type**, enzovoort. Als de reserveverbinding het bericht met succes naar de meldkamer heeft doorgestuurd, probeert de communicatiemodule na de ingestelde tijd terug te keren naar de hoofdverbinding (paragraaf 6.4.2).

Als het apparaat niet naar een meldkamer meldt, is de instelling hiermee klaar: druk op de knop **Write [F5]** (schrijven), wacht op de bevestiging en trek de USB-kabel los.

Vergeet bij aansluiting op de telefoonlijn (TIP/RING) niet de kiezer van de alarmcentrale in te schakelen en in te stellen, anders stuurt de centrale geen gebeurtenissen; voor directe besturing moeten ook de centrales van Paradox, Texecom, Caddx, InnerRange en Honeywell worden ingesteld. Het instellen van de centrale staat beschreven in hoofdstuk 4.

2.3 Verbinding met de meldkamer

In de app (Settings → Advanced settings):

1. **System options** → **System general**: voer het objectnummer in dat u van de meldkamer hebt gekregen (**Account No.**; 0–9, A–F; `FFFE` en `FFFF` kunnen niet worden gebruikt). Op hardwareversie **x1x1**, met firmware **1.31** of nieuwer, voert u het objectnummer per kanaal in: **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** U herkent het aan het scherm: als System general alleen het veld **Time set** toont, gebruik dan de instelling van het kanaal.
2. **Panel settings** → **TLF** (aansluiting op TIP/RING): zet **Security panel model** op **AUTO**; of **Panel settings** → **Serial Bus** (aansluiting op databus of seriële poort): kies het **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel**: schakel de optie **Enabled** in en voer daarna in: **Communication type**: **IP**; het adres **Domain or IP** en de **Port** van de ontvanger; **TCP or UDP**; **Protocol**: **TRK8** voor een Trikdis-ontvanger, **DC-09_2007** of **DC-09_2012** voor een universele

ontvanger, **TL150** voor een SUR-GARD-ontvanger; en de versleutelingssleutel die in de ontvanger is ingesteld: bij het TRK-protocol in het veld **TRK encryption key**, bij DC-09 schakelt u de optie **Enable encryption key** in en voert u de **DC-09 encryption key** in.

4. (Aanbevolen) Stel op dezelfde manier het **Backup channel** (reservekanaal) in.
5. **Reporting to CMS** → **CMS settings** → **Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.
6. **Network settings** → **LAN** (bekabeld netwerk): schakel de optie **Use DHCP** in. **Network settings** → **SIM** en **SIM2** (voor elke simkaart): **SIM card PIN**, **APN**, en controleer de velden **DNS1**, **DNS2**.
7. Tik op de knop **Write**.

In TrikdisConfig. Voer eerst op de pagina **System settings** het objectnummer in.

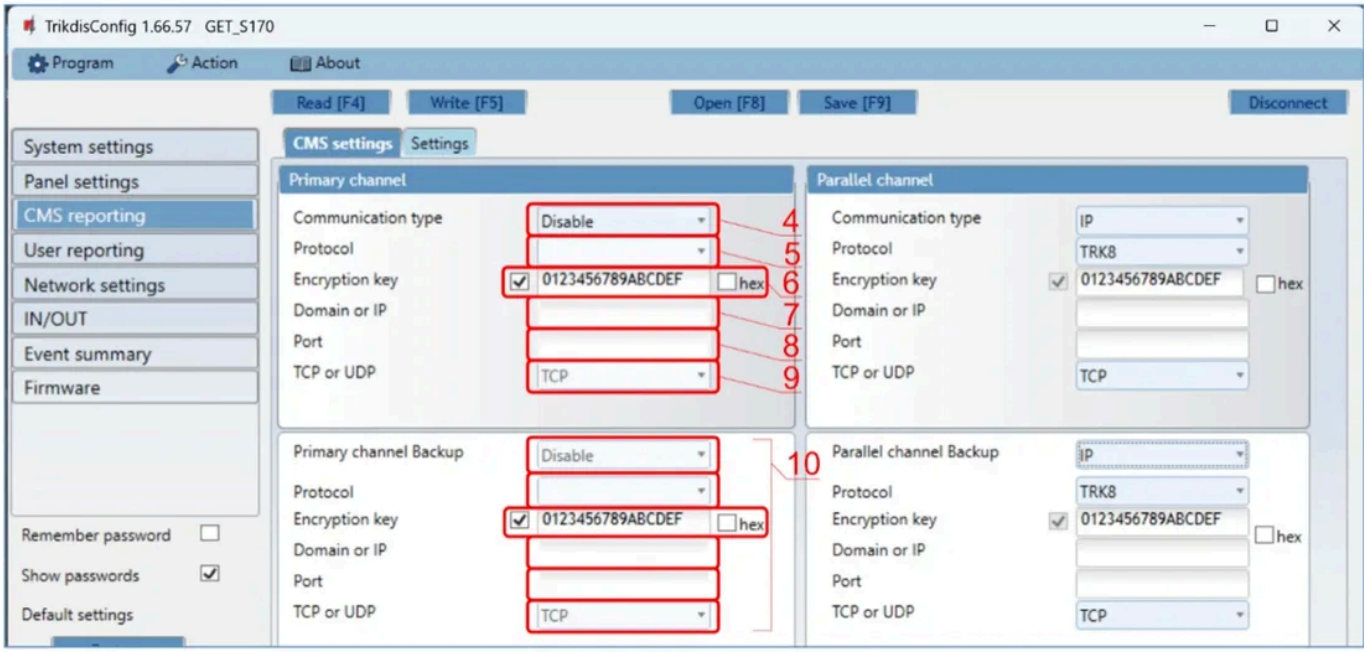


Afbeelding 12. TrikdisConfig – pagina System settings, groep General.

- 1 **Object ID** – het objectnummer dat u van de meldkamer hebt gekregen (6 hexadecimale tekens, 0–9, A–F). `FFFE` en `FFFF` kunnen niet worden gebruikt.

Geef op de pagina **Panel settings** de aansluiting van de centrale op, als u dat in paragraaf 2.2 nog niet hebt gedaan: bij aansluiting op TIP/RING zet u **Communication protocol** op **AUTO**; bij aansluiting op databus of seriële poort kiest u in het veld **Security panel model** het type van de aangesloten centrale (de afbeeldingen in paragraaf 2.2).

Stel daarna op de pagina **CMS reporting**, op het tabblad **CMS settings**, in het deel **Primary channel** (primair kanaal) de gegevens van de ontvanger in. Op de afbeelding ziet u het venster vóór de instelling: het veld **Communication type** van het primaire kanaal staat nog op **Disable**.



Afbeelding 13. TrikdisConfig – CMS reporting, tabblad CMS settings.

- 4 **Communication type** – kies de verbinding **IP**.
- 5 **Protocol** – **TRK8** voor een Trikdis-ontvanger, **DC-09_2007** of **DC-09_2012** voor een universele ontvanger, **TL150** voor een SUR-GARD-ontvanger.
- 6 **Encryption key** – de versleutelingssleutel die in de ontvanger is ingesteld.
- 7 **Domain or IP** – de domeinnaam of het IP-adres van de ontvanger.
- 8 **Port** – het poortnummer van de ontvanger.
- 9 **TCP or UDP** – het transmissieprotocol; dit volgt de instelling van de ontvanger.
- 10 **Primary channel Backup** – reservekanaal bij uitval van het primaire kanaal; vul het op dezelfde manier in, invullen wordt aanbevolen.

Geef op het tabblad **Settings**, in de groep **Reporting mode**, de volgorde van de verbindingen op (**Main type**, **Backup type**, **Backup type 2**), als u dat in paragraaf 2.2 nog niet hebt gedaan – daar vindt u ook de afbeelding en de beschrijving van de werking.

Voer ten slotte op de pagina **Network settings** de netwerkgegevens in, als u dat in paragraaf 2.2 nog niet hebt gedaan: op het tabblad **LAN** het vinkje **Use DHCP**, op het tabblad **SIM1** (en **SIM2**) de gegevens van de kaart (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Bij het **DC-09**-protocol voert u op het tabblad **Settings** ook het lijn- en ontvangernummer in (**Line No.**, **Receiver No.**, paragraaf 6.4.2). De GET meldt alleen via een IP-verbinding – via het bekabelde netwerk of het mobiele internet – naar de meldkamer, hij heeft geen sms-reservekanaal.

Druk aan het einde van de instellingen op de knop **Write [F5]** (schrijven), wacht op de bevestiging en trek de USB-kabel los. Het apparaat is hiermee klaar om te worden aangesloten. Bij aansluiting op de telefoonlijn moet ook hier de kiezer van de alarmcentrale worden ingeschakeld en ingesteld, anders stuurt de centrale geen gebeurtenissen (hoofdstuk 4).

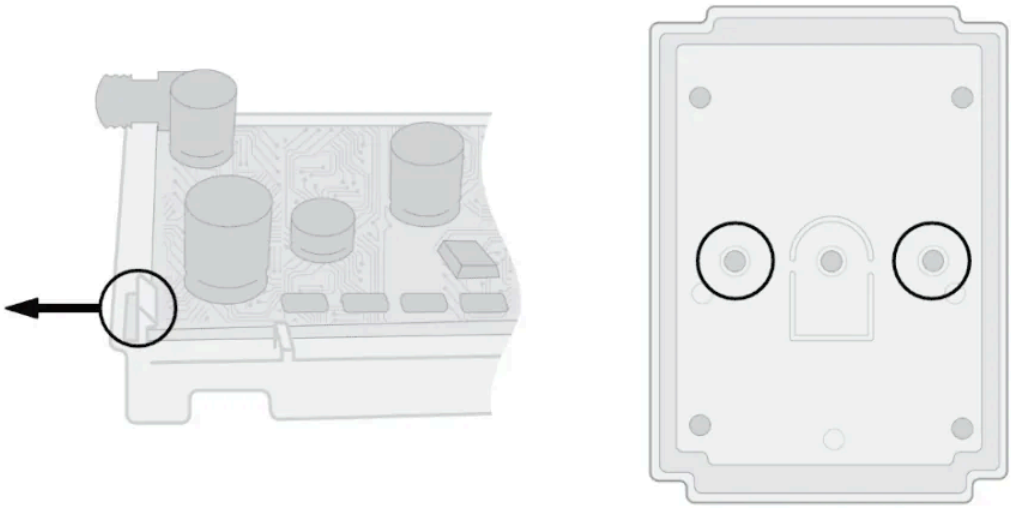
3. Installatie en aansluiting

Figyelem!

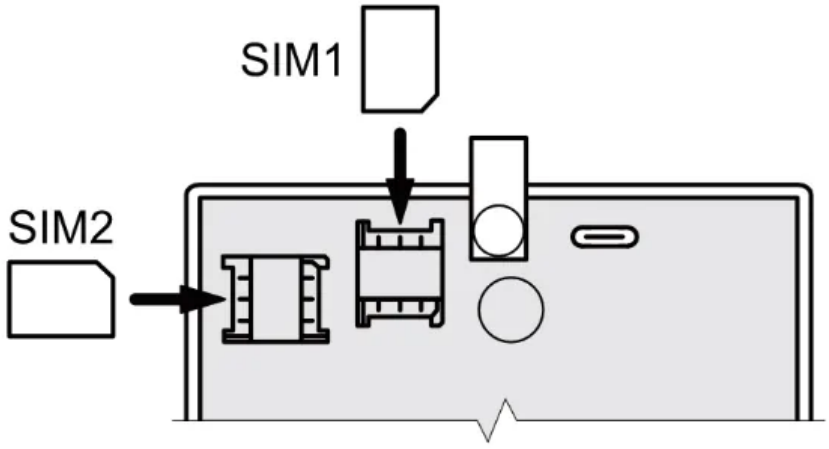
Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

3.1 Stappen van de installatie

1. Verwijder het frontdeksel (zie paragraaf 2.1) en trek de klemmenstrook los.
2. Plaats de nano-simkaart – of allebei – in de houder, als u dat bij de inbedrijfstelling nog niet hebt gedaan.
3. Haal de printplaat uit de achterplaat: open de vergrendeling naast de antenneconnector en til de print eruit (zie de afbeelding).
4. Bevestig de achterplaat met schroeven op de gekozen plaats (op de afbeelding zijn de schroefgaten omcirkeld), of volgens paragraaf 3.2 met de meegeleverde dubbelzijdige tape.
5. Plaats de printplaat terug in de achterplaat en steek de klemmenstrook er weer op.
6. Schroef de mobiele antenne vast.
7. Plaats het frontdeksel terug.
8. Als u de gebeurtenissen ook via het bekabelde netwerk (LAN) naar de meldkamer stuurt, steek dan de netwerkkabel in de LAN-aansluiting van de communicatiemodule.



Afbeelding 14. De printplaat uit de achterplaat halen (links: de vergrendeling en de richting om de print eruit te halen) en de schroefgaten van de achterplaat (rechts).



Afbeelding 15. De plaats van de twee simhouders op de printplaat: SIM1 in het midden van de print, SIM2 aan de linkerrand; de pijlen tonen de richting waarin de kaart wordt geplaatst.

In de communicatiemodule kunnen één of twee simkaarten. De kaart moet actief zijn, en voor IP-gebruik moet de mobiele dataverbinding erop werken. Als u niet wilt dat TrikdisConfig om een pincode vraagt, plaats de kaart dan in een mobiele telefoon en schakel daar de pincodevraag uit.

3.2 Plaatsing in de behuizing van de centrale, antenne

De communicatiemodule moet worden geplaatst in de **behuizing van de alarmcentrale die met een deksel-sabotageschakelaar is beveiligd**. Bevestig hem op de binnenkant van de achterwand van de behuizing met de meegeleverde dubbelzijdige acryl-schuimtape van industriële kwaliteit: plak de tape op een schoon, droog oppervlak en druk stevig aan, zodat hij zeker vastzit. Als de behuizing van de centrale deze veilige bevestiging niet toelaat, kan de communicatiemodule ook in een aparte, tegen sabotage beveiligde behuizing worden gemonteerd.

- **In een metalen behuizing** wordt het mobiele signaal sterk verzwakt. Als de communicatiemodule in de metalen behuizing van de centrale komt, voer de antenne dan naar buiten de behuizing, of gebruik een antenne met een langere kabel.
- **Controleer de signaalsterkte** vóór de definitieve bevestiging: het aantal gele knipperingen van de NETWORK LTE-led moet op 4G minimaal 3 zijn (paragraaf 1.6). Als het minder is, zoek dan een betere plaats voor de antenne, of stap over op een gevoeligere antenne die verder weg kan worden geplaatst.
- Houd de antenne en de communicatiemodule uit de buurt van de transformator van de centrale en van netspanningskabels.
- Voer de LAN-kabel via de kabelinvoer van de behuizing naar de RJ45-aansluiting aan de zijkant van de communicatiemodule; de kabel mag geen trekkracht op de klemmen uitoefenen.



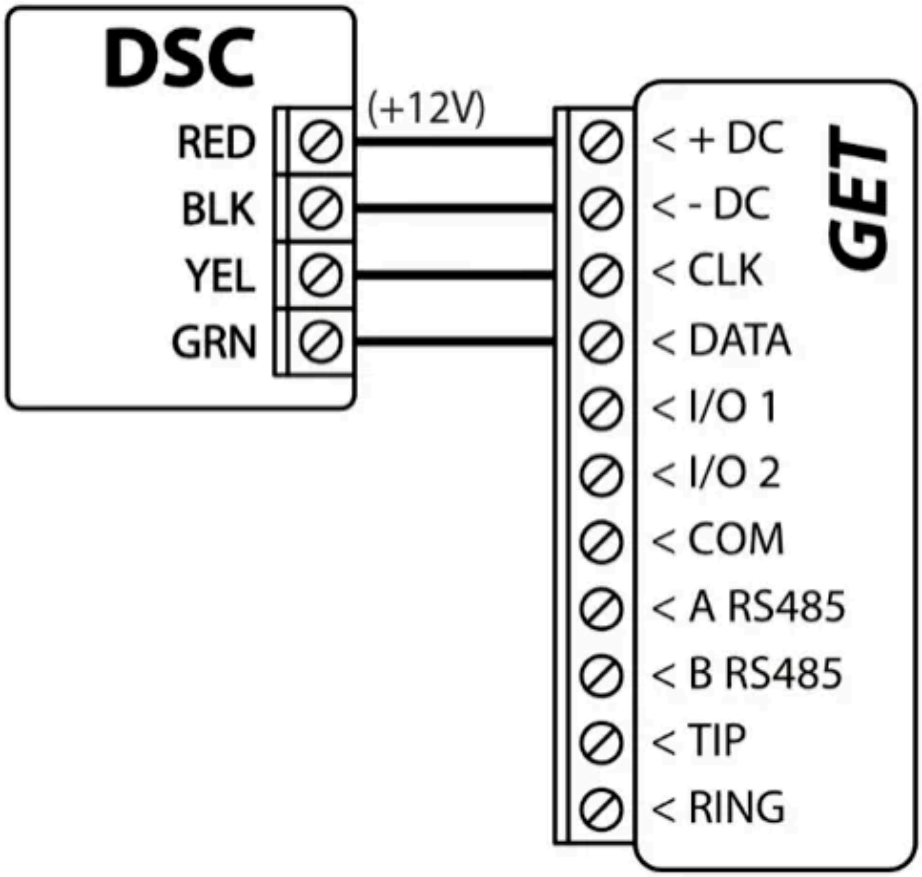
A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna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

3.3 Aansluiting op de alarmcentrale

Volg het schema hieronder dat bij uw centrale past. Op de schema's zijn **+DC** en **–DC** de voedingsklemmen **+12 VDC** / **–12 VDC** van de communicatiemodule, en **A RS485** / **B RS485** de klemmen **A 485** / **B 485** (die hoeven op de GET niet te worden aangesloten). De communicatiemodule krijgt zijn voeding van de hulpvoedingsuitgang (AUX) van de centrale, zodat bij een stroomstoring de accu van de centrale ook de communicatiemodule voedt.

3.3.1 DSC – databus (Keybus)

Sluit de Keybus van de DSC-centrale met vier draden aan op de communicatiemodule: **RED → +DC**, **BLK → –DC**, **YEL → CLK**, **GRN → DATA**.

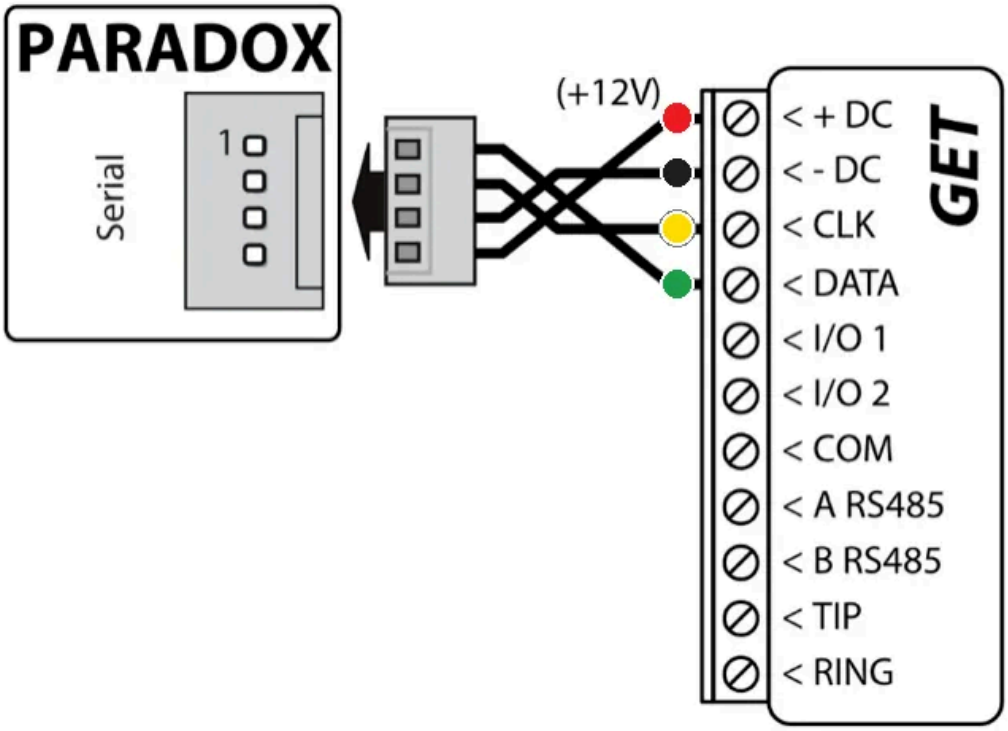


Afbeelding 16. Aansluiting van een DSC-centrale op de databus (Keybus, „Keypad bus"): RED → +DC, BLK → –DC, YEL → CLK, GRN → DATA.

De GET behandelt de DSC-centrale alleen via de databus; het tegelijk aansluiten van de Keybus en de TIP/RING-klemmen kan alleen op de GT+-communicatiemodule. Als hij alleen op de Keybus is aangesloten, krijgt de communicatiemodule van de centrale de algemene status van de zones, maar niet het zonetype (brand, inbraak, waterlekkage enz.), en daarom meldt hij elk alarm als **algemeen alarm, met Contact ID-code E130**. Als de meldkamer de eigen codes van de centrale nodig heeft (bijvoorbeeld brandalarm: E110), kunt u de gebeurtenissen met de telefoonkiezer van de centrale versturen, via aansluiting op TIP/RING (paragraaf 3.3.9 en 4.2); dan is er geen directe besturing.

3.3.2 Paradox – seriële poort

De communicatiemodule wordt op de seriële poort van de Paradox-centrale aangesloten met de apart te bestellen **EX-CRP2.4**-kabel: **rood → +DC**, **zwart → –DC**, **geel → CLK**, **groen → DATA**.



Afbeelding 17. Aansluiting van een Paradox-centrale op de seriële poort met de EX-CRP2.4-kabel (apart te bestellen; „Use the EX-CRP2.4 cable (ordered separately)"): rood → +DC, zwart → −DC, geel → CLK, groen → DATA.

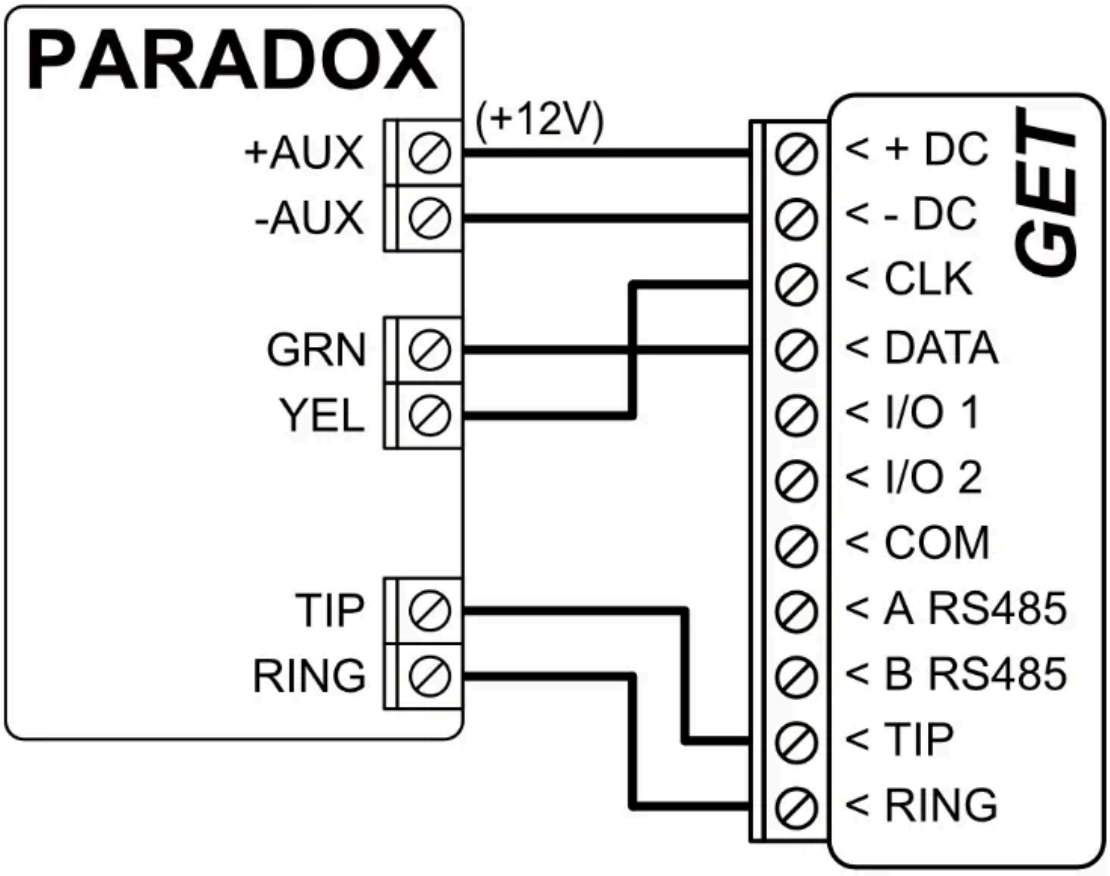
- rode draad („R - red")
- zwarte draad („B - black")
- gele draad („Y - yellow")
- groene draad („G - green")

Op de nieuwere Paradox-centrales (SP+, MG+, EVOHD+) kan de seriële poort af fabriek vergrendeld zijn; over het ontgrendelen gaat paragraaf 4.1.2. Bij de centrales Spectra SP / SP+ en Magellan MG / MG+ kan in plaats van de seriële poort ook de aansluiting uit de volgende paragraaf worden gebruikt.

3.3.3 Paradox SP/MG – Keybus en TIP/RING

De Paradox-centrales Spectra SP, SP+ en Magellan MG, MG+ kunnen in plaats van via de seriële poort ook tegelijk op hun databus (Keybus) en hun TIP/RING-klemmen worden aangesloten: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK**, en ook **TIP** → **TIP**, **RING** → **RING**. Deze aansluiting gebruikt de Keybus van de centrale in plaats van de seriële poort, en daarom is de betaalde ontgrendeling van de seriële poort van Paradox er niet voor nodig.

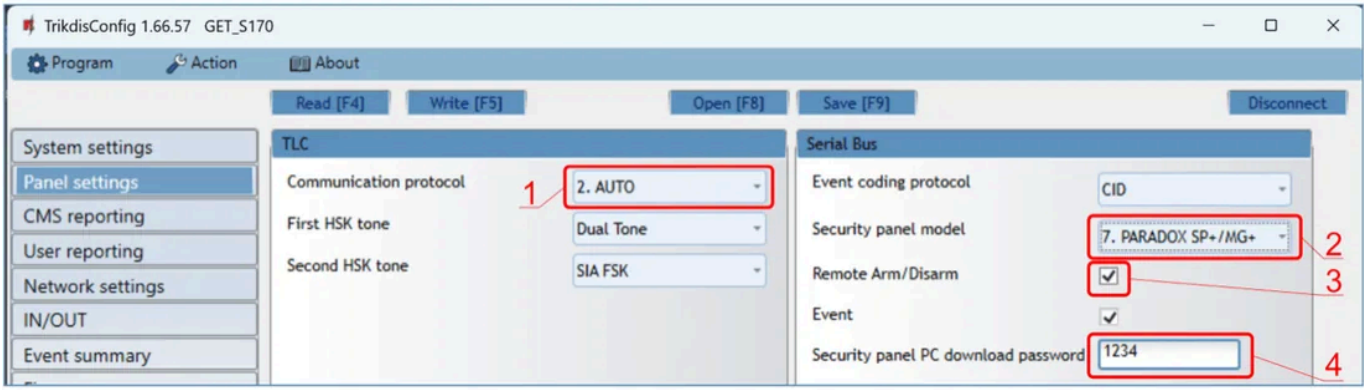
Voor deze aansluiting moet de firmware van de communicatiemodule minimaal **1.21** zijn (het bijwerken staat beschreven in hoofdstuk 9).



Afbeelding 18. Aansluiting van een Paradox SP / SP+ / MG / MG+-centrale tegelijk op de Keybus (databus, „Keypad bus") en op de TIP/RING-klemmen: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Stel voor deze aansluiting op de pagina **Panel settings** van TrikdisConfig het volgende in:

1. **Communication protocol**: **2. AUTO**.
2. **Security panel model**: kies uit de lijst het item **Paradox SP+/MG+ series KeyBus** (op de afbeelding 7. PARADOX SP+/MG+).
3. **Remote Arm/Disarm**: vink dit aan als de gebruikers de centrale vanuit de Protegus 2-app met hun eigen bediendeelcode willen besturen.
4. **Security panel PC download password**: voer voor directe besturing het PC-wachtwoord in dat in de centrale is ingesteld; de twee moeten overeenkomen.



Afbeelding 19. TrikdisConfig – Panel settings voor de aansluiting Keybus + TIP/RING: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm aangevinkt (3), Security panel PC download password ingevuld (4).

In de Protegus 2-app staan dezelfde instellingen op de tabbladen **Panel settings** → **TLF** (Security panel model = Communication protocol) en **Panel settings** → **Serial Bus** (paragraaf 6.3).

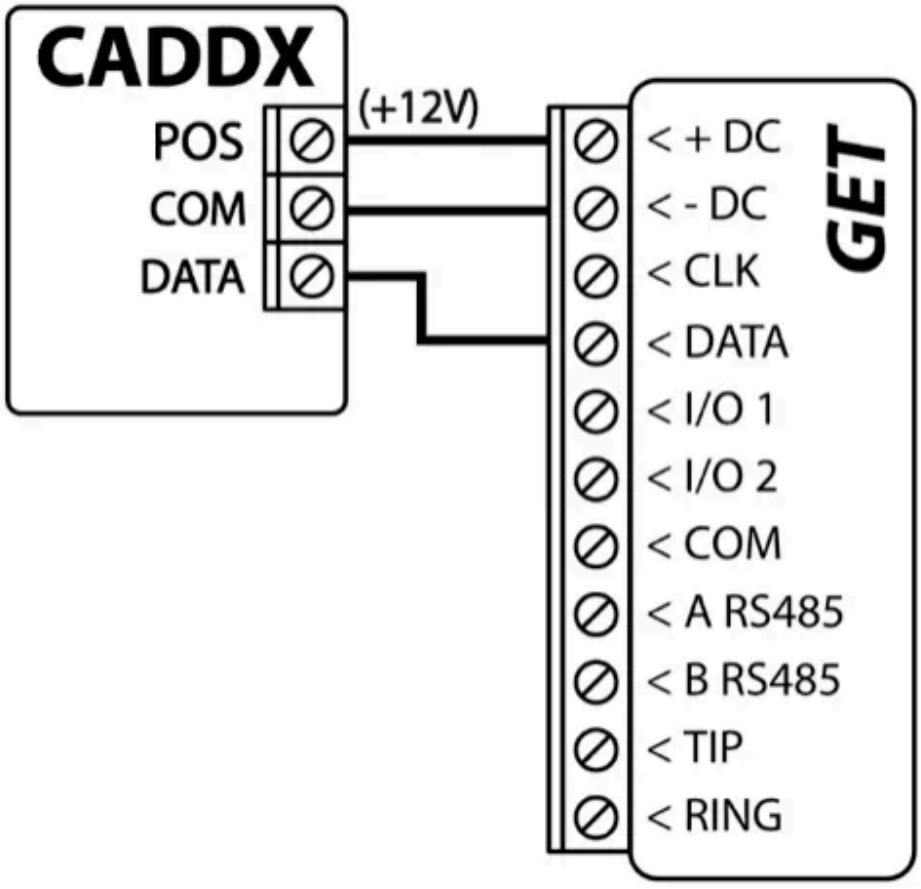
Ook de Paradox-centrale moet worden geprogrammeerd, zodat hij de gebeurtenissen naar de meldkamer stuurt en vanuit Protegus 2 bestuurbaar is – stel op het bediendeel dat op de centrale is aangesloten de volgende secties in:

Sectie	Waarde	Sectie	Waarde
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

Het PC-wachtwoord dat in sectie **911** is geschreven, moet overeenkomen met het veld **Security panel PC download password** van de communicatiemodule (paragraaf 4.1.2).

3.3.4 UTC Interlogix (Caddx) – databus

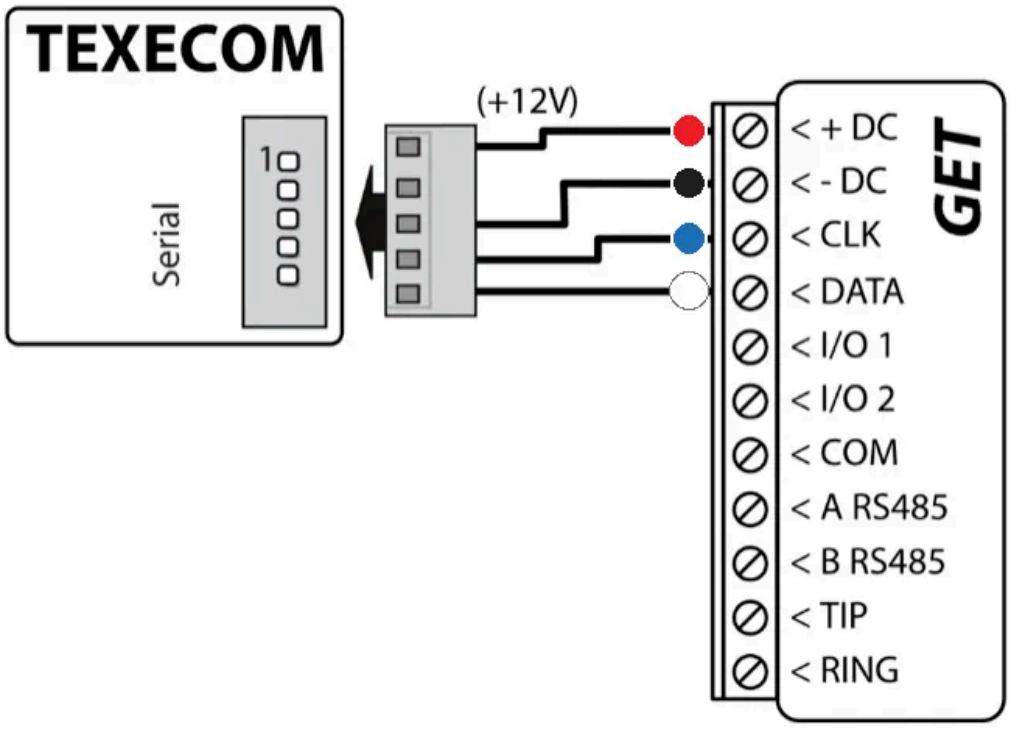
Sluit de databus van de Caddx NetworX-centrale met drie draden aan op de communicatiemodule: **POS** → **+DC**, **COM** → **–DC**, **DATA** → **DATA**. De klemmen CLK, TIP en RING zijn niet nodig.



Afbeelding 20. Aansluiting van een UTC Interlogix (Caddx) NetworX-centrale op de databus („Keypad bus"): POS → +DC, COM → –DC, DATA → DATA.

3.3.5 Texecom – seriële poort

De communicatiemodule wordt op de seriële poort van de Texecom Premier / Premier Elite-centrale aangesloten met de apart te bestellen **EX-CRP4**-kabel: **rood → +DC**, **zwart → –DC**, **blauw → CLK**, **wit → DATA**.

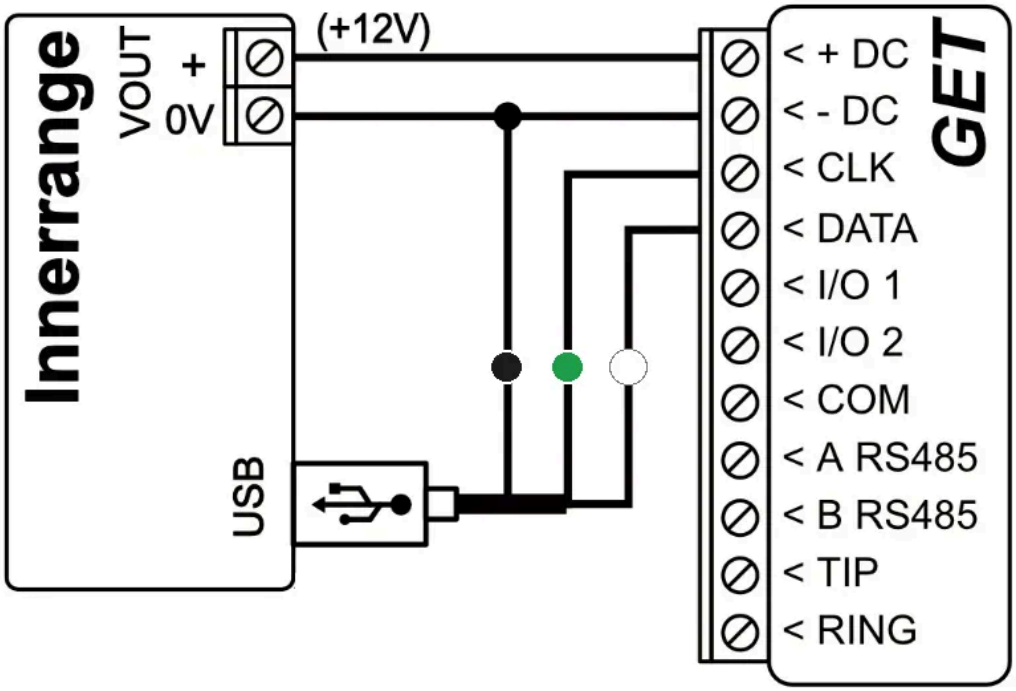


Afbeelding 21. Aansluiting van een Texecom-centrale op de seriële poort met de EX-CRP4-kabel (apart te bestellen; „Use the EX-CRP4 cable (ordered separately)"): rood → +DC, zwart → –DC, blauw → CLK, wit → DATA.

- rode draad („R - red")
- zwarte draad („B - black")
- blauwe draad („BL - blue")
- witte draad („W - white")

3.3.6 InnerRange Inception

De communicatiemodule krijgt zijn voeding van de voedingsuitgang van de Inception-centrale (**VOUT + → +DC**, **VOUT 0V → –DC**), en de dataverbinding komt van de USB-poort van de centrale, met de kabel **993030USB** van Inner Range: **zwart → 0V / –DC**, **groen → CLK**, **wit → DATA**.

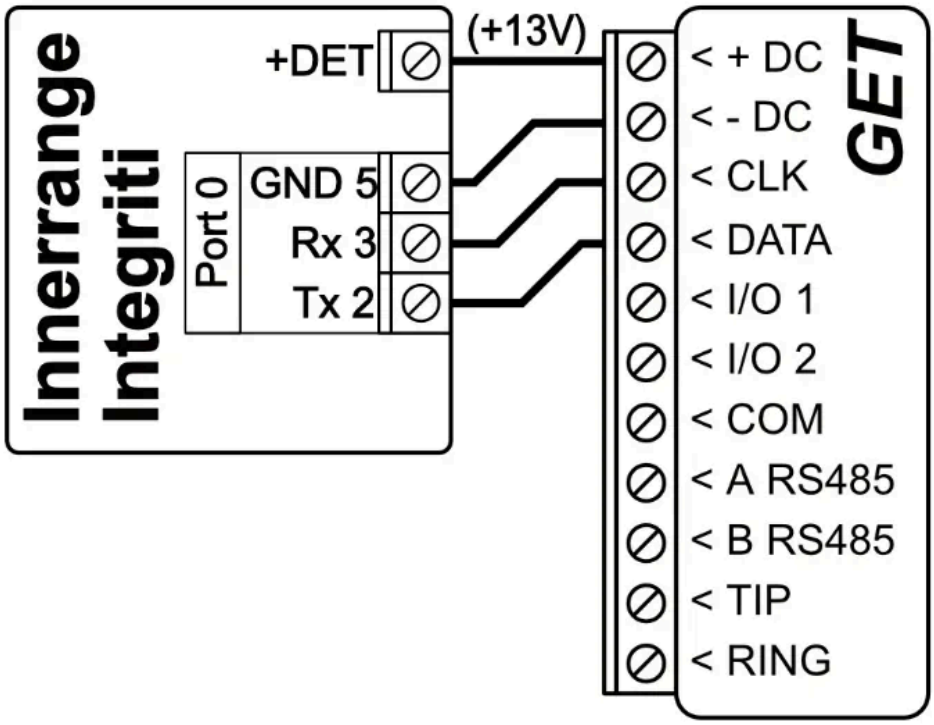


Afbeelding 22. Aansluiting van een InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; vanaf de USB-poort met de kabel 993030USB („Cable, Inner Range part number 993030USB") zwart → −DC, groen → CLK, wit → DATA.

- zwarte draad („Black wire")
- groene draad („Green wire")
- witte draad („White wire")

3.3.7 InnerRange Integriti

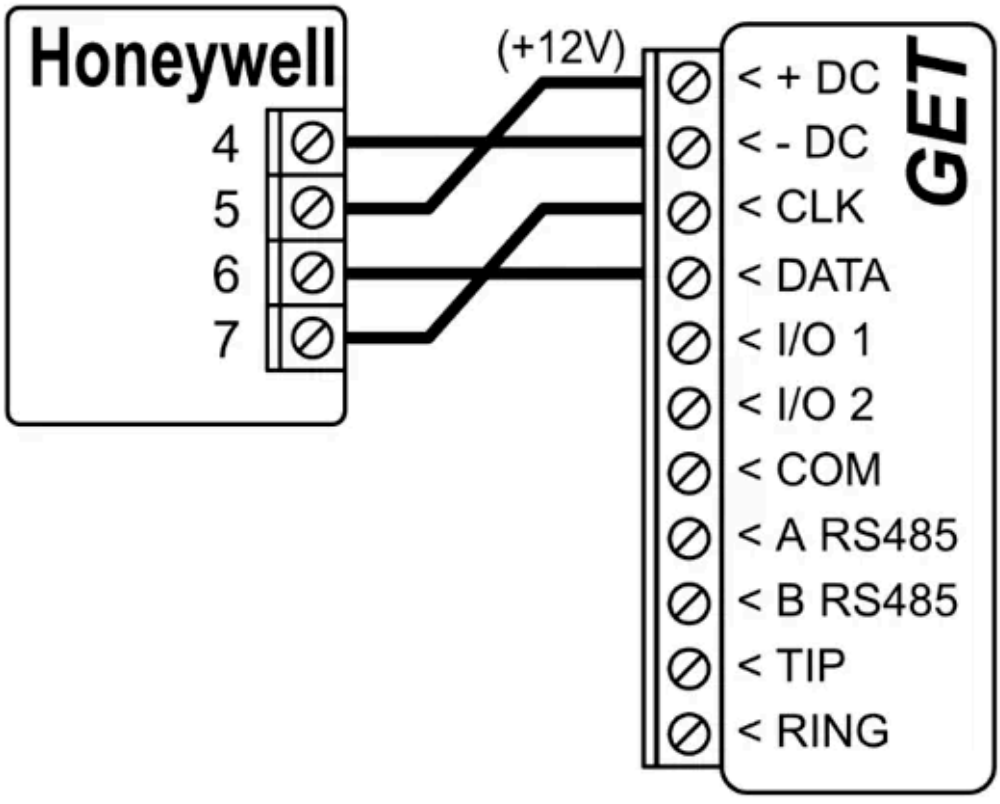
De communicatiemodule wordt op de seriële poort **Port 0** van de Integriti-centrale aangesloten met de kabel **INTG-996795** van Inner Range: **+DET (+13 V)** → **+DC**, **GND (5)** → **−DC**, **Rx (3)** → **CLK**, **Tx (2)** → **DATA**.



Afbeelding 23. Aansluiting van een InnerRange Integriti op Port 0 met de kabel INTG-996795 („Cable, Inner Range part number INTG-996795"): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – databus

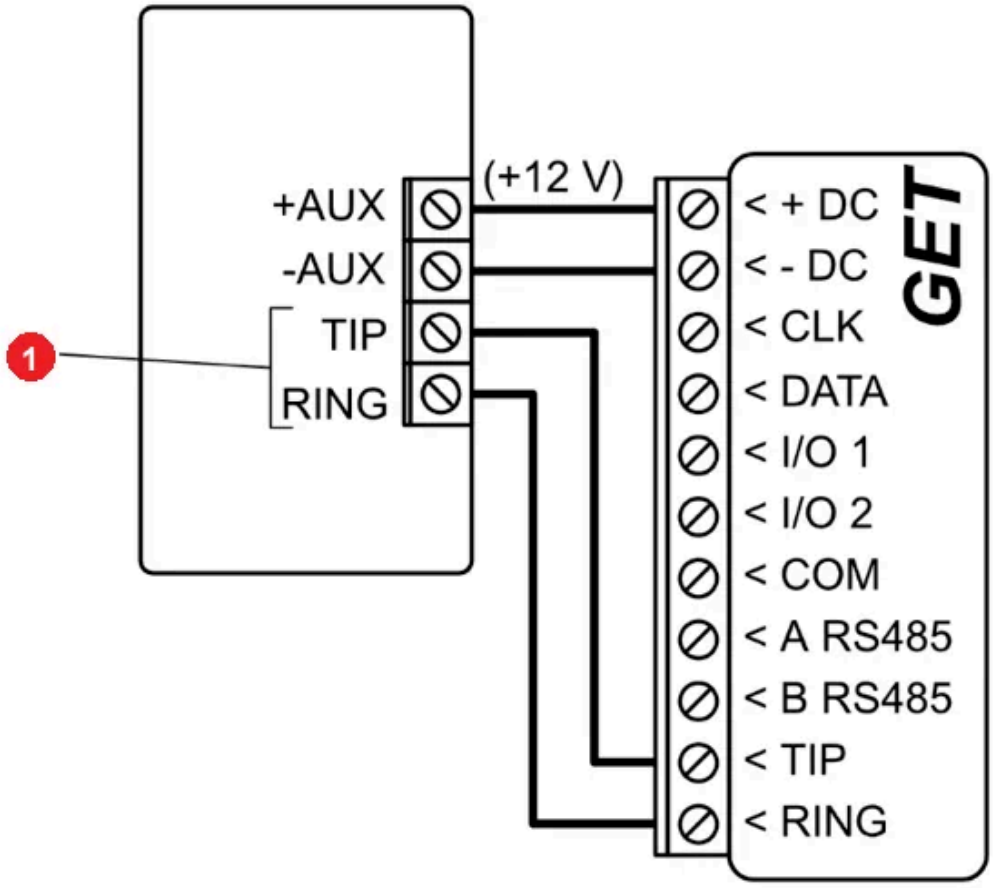
Sluit de bediendeelbus van de Honeywell Ademco Vista-15-, Vista-20- en Vista-48-centrale vanaf de klemmen van de centrale aan op de communicatiemodule: **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.



Afbeelding 24. Aansluiting van een Honeywell Vista-15 / -20 / -48-centrale op de databus („Keypad bus"): klem 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Elke centrale – TIP/RING

Elke andere centrale kan via haar telefoonkiezer worden aangesloten: de voeding van de hulpvoedingsuitgang van de centrale (**+AUX** → **+DC**, **–AUX** → **–DC**), de telefoonlijnuitgang op de klemmen **TIP** en **RING** van de communicatiemodule (**TIP** → **TIP**, **RING** → **RING**). De kiezer van de centrale moet worden ingesteld (paragraaf 4.2).



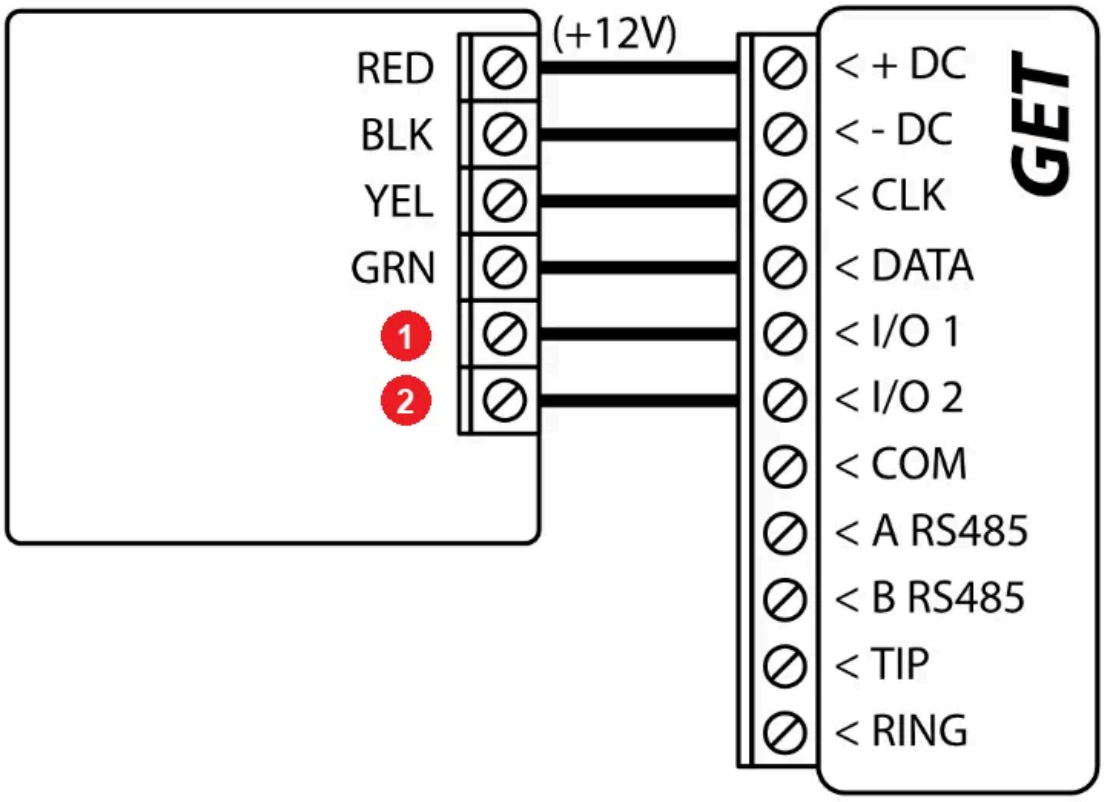
Afbeelding 25. Aansluiting op de telefoonkiezer van de centrale („Control panel"): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 de klemmen van de telefoonkiezer van de centrale („Telephone line communicator terminals")

3.4 Een sleutelschakelaarzone aansluiten

Volg deze aansluiting als u de centrale vanuit de Protegus 2-app wilt in- en uitschakelen doordat de uitgang (PGM) van de communicatiemodule de **sleutelschakelaarzone** van de centrale schakelt. De twee I/O-klemmen met dubbele functie van de communicatiemodule werken als uitgang (OUT, PGM) – op de GET zijn ze af fabriek allebei uitgang –, zodat de twee uitgangen twee partities van het systeem kunnen aansturen: sluit de sleutelschakelaarzone van partitie 1 aan op klem **1 I/O**, die van partitie 2 op klem **2 I/O**. Haal bij zo'n aansluiting op de pagina **Panel settings** van TrikdisConfig het vinkje **Remote Arm/Disarm** weg, zet de klemmen op de pagina **IN/OUT** op de functie **OUT** (paragraaf 6.7), en wijs in de Protegus 2-app de uitgangen volgens paragraaf 5.2 toe aan de partities.

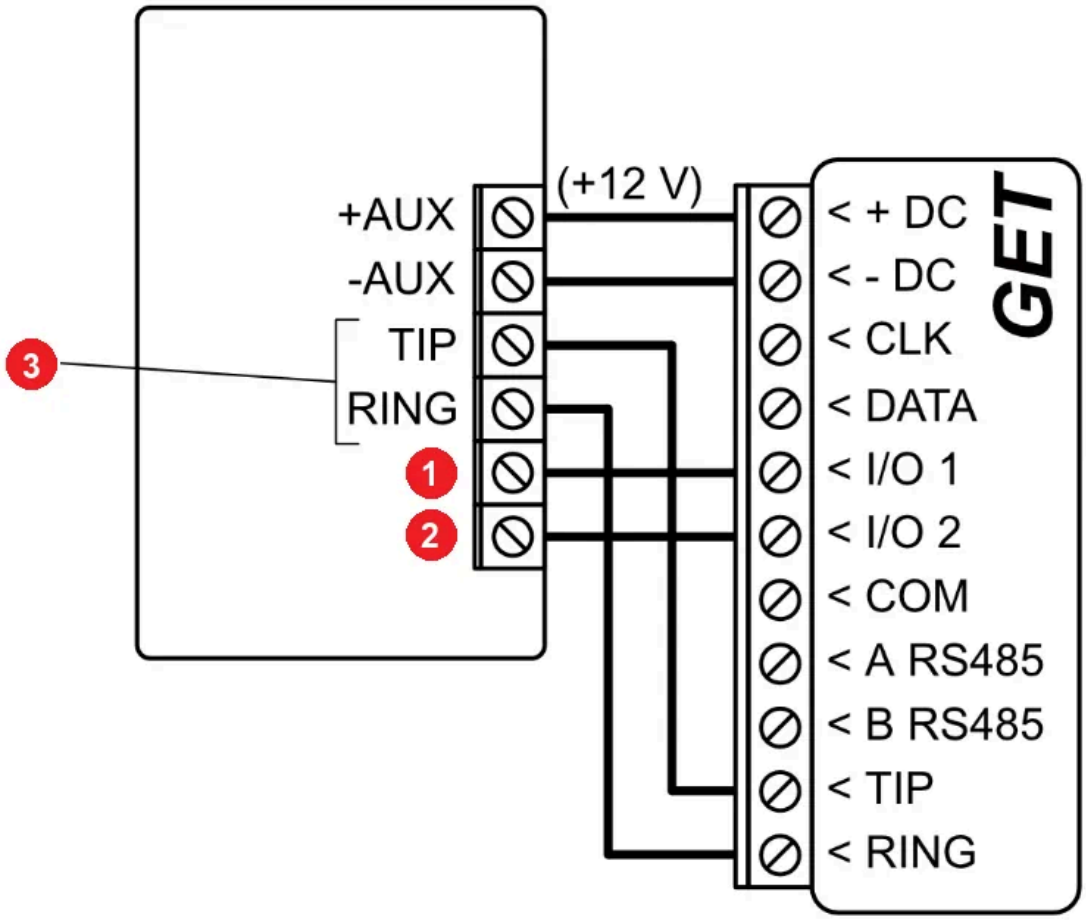
Bij aansluiting op de databus of seriële poort blijft de dataverbinding tussen centrale en communicatiemodule bestaan (de communicatiemodule leest de gebeurtenissen van de bus), het in- en uitschakelen gebeurt via de sleutelschakelaarzone:



Afbeelding 26. In- en uitschakelen met een sleutelschakelaarzone („Zone (keyswitch)"), bij aansluiting op de databus of seriële poort („Keypad bus or Serial port"): klem RED van de alarmcentrale („Control panel") → +DC, BLK → −DC, YEL → CLK, GRN → DATA; de zone van partitie 1 → 1 I/O, die van partitie 2 → 2 I/O.

- 1 de sleutelschakelaarzone van partitie 1 („1-st Area")
- 2 de sleutelschakelaarzone van partitie 2 („2-nd Area")

Bij aansluiting op de telefoonlijn (TIP/RING) stuurt de centrale de gebeurtenissen met haar kiezer, het in- en uitschakelen gebeurt op dezelfde manier via de sleutelschakelaarzone:



Afbeelding 27. In- en uitschakelen met een sleutelschakelaarzone („Zone (keyswitch)"), bij aansluiting op de telefoonlijn: klem +AUX van de alarmcentrale („Control panel") → +DC, −AUX → −DC, TIP → TIP, RING → RING; de zone van partitie 1 → 1 I/O, die van partitie 2 → 2 I/O.

- 1 de sleutelschakelaarzone van partitie 1 („1-st Area")
- 2 de sleutelschakelaarzone van partitie 2 („2-nd Area")
- 3 de klemmen van de telefoonkiezer van de centrale („Telephone line communicator terminals")

De sleutelschakelaarzone kan pulserend of met twee standen werken – in de Protegus 2-app moet dezelfde modus worden ingesteld (paragraaf 5.2). Over de details en valkuilen van het inschakelen met een sleutelschakelaar gaat een apart artikel: Op afstand inschakelen met een sleutelschakelaar vanuit de Protegus 2-app.

3.5 Ingangen aansluiten

De twee I/O-klemmen met dubbele functie van de communicatiemodule kunnen als ingang (IN) ook worden gebruikt voor extra detectoren (bijv. sabotageschakelaar, paniekknop), onafhankelijk van de alarmcentrale. Op de ingang kan een NO-, NC-, NO/EOL-, NC/EOL-, NO/DEOL- of NC/DEOL-kring worden aangesloten. Op de GET zijn de klemmen af fabriek uitgangen: zet de gebruikte klem op de pagina **IN/OUT** van TrikdisConfig op de functie **IN**, en geef in het veld **Type** het type van de aangesloten kring op; in de Protegus 2-app staat hetzelfde op het tabblad **Advanced settings** → **IN/OUT**, in het veld **Type** van klem 1 of 2 (paragraaf 6.7). De ingang moet tussen de gekozen I/O en de klem **COM** worden aangesloten, volgens het gekozen type.

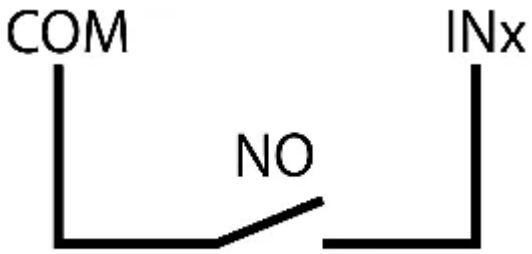
De ingangen accepteren de volgende kringtypen: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. De eindweerstand is **2,2 kΩ**. Bij enkelvoudige afsluiting (EOL) gelden zowel kortsluiting als onderbreking als alarm; dubbele afsluiting (DEOL) met twee weerstanden herkent alarm en sabotage (kortsluiting of

onderbreking) afzonderlijk. De fabrieksinstelling is NO (in rust open); het type ingang stelt u in op de pagina **IN/OUT** van TrikdisConfig, overeenkomstig de aansluiting.

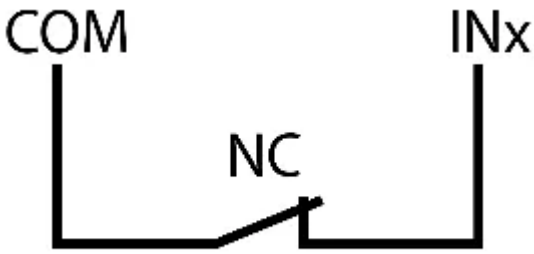
Type	Ruststand	Alarm	Sabotage
NC	gesloten	open	–
NO	open	gesloten	–
NC/EOL	2,2 kΩ	onderbreking of kortsluiting	–
NO/EOL	2,2 kΩ	kortsluiting of onderbreking	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	onderbreking of kortsluiting
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	onderbreking of kortsluiting

Wanneer de ingang wordt geactiveerd, stuurt de communicatiemodule een eigen gebeurtenis naar de meldkamer en naar Protegus 2; de Contact ID-code, het partitie- en zonenummer van de gebeurtenis kunt u op de pagina **IN/OUT** opgeven.

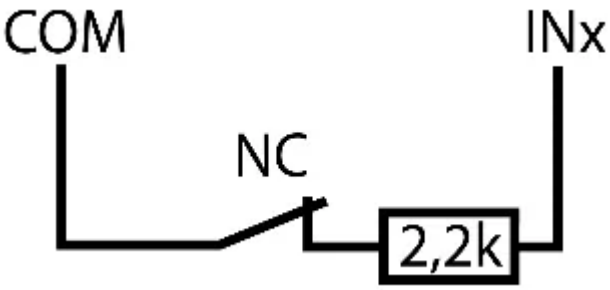
Aansluiting van ingangskringen tussen COM en het punt INx: NO, NC, NC/EOL, NO/EOL, en met sabotagedetectie NO/DEOL en NC/DEOL, met eindweerstanden van 2,2 kΩ; de afzonderlijke toestanden (kortsluiting, onderbreking, 2,2 kΩ, 3,3–5,5 kΩ) worden uitgelegd in de tabel van paragraaf 3.5.



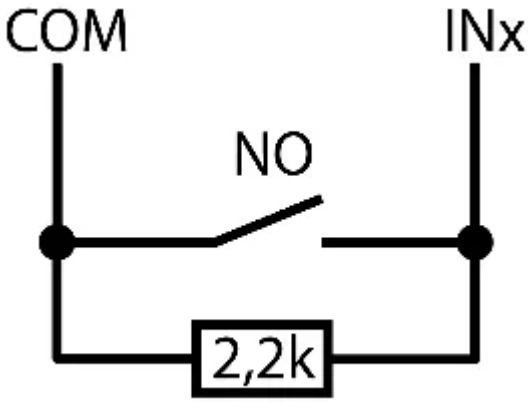
Afbeelding 28. NO – in rust open kring: gesloten – alarm, open – rusttoestand.



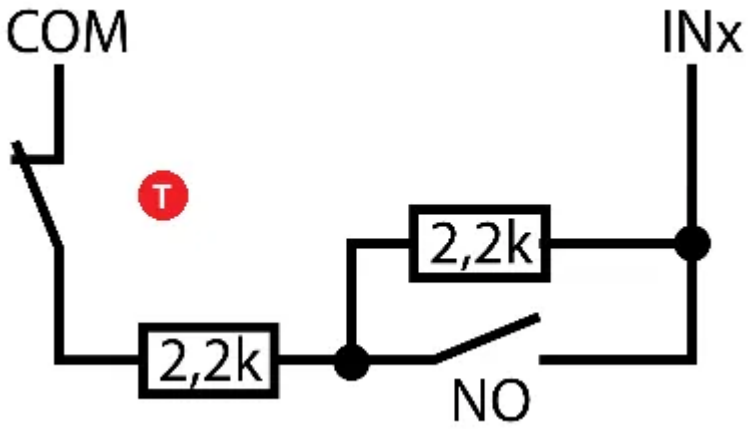
Afbeelding 29. NC – in rust gesloten kring: open – alarm, gesloten – rusttoestand.



Afbeelding 30. NC/EOL – in rust gesloten kring met eindweerstand van 2,2 kΩ: kortsluiting of onderbreking – alarm, 2,2 kΩ – rusttoestand.

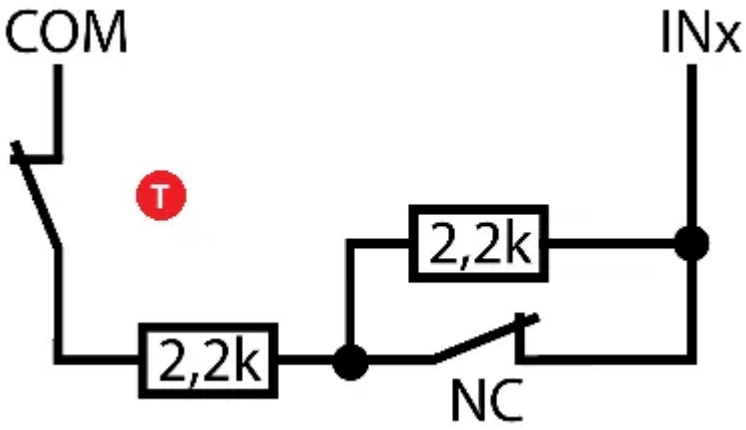


Afbeelding 31. NO/EOL – in rust open kring met eindweerstand van 2,2 kΩ: kortsluiting of onderbreking – alarm, 2,2 kΩ – rusttoestand.



Afbeelding 32. NO/DEOL – in rust open kring met eindweerstand van 2,2 kΩ en sabotagedetectie: kortsluiting of onderbreking – sabotage, 2,2 kΩ – alarm, 3,3–5,5 kΩ – rusttoestand.

- T sabotagecontact („Tamper"), signaleert het openen van de behuizing van de detector

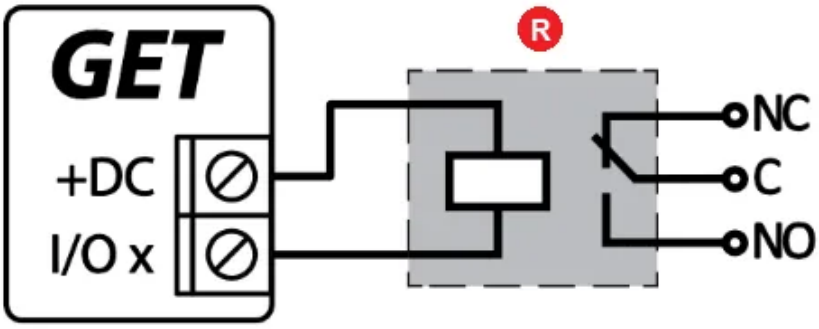


Afbeelding 33. NC/DEOL – in rust gesloten kring met eindweerstand van 2,2 kΩ en sabotagedetectie: kortsluiting of onderbreking – sabotage, 2,2 kΩ – rusttoestand, 3,3–5,5 kΩ – alarm.

- T sabotagecontact („Tamper"), signaleert het openen van de behuizing van de detector

3.6 Een uitgang aansluiten met een relais

Als uitgang zijn de I/O-klemmen open-collectoruitgangen (OC): in actieve toestand trekken ze de aangesloten belasting naar de min, met maximaal 0,15 A, tot 30 V DC. Met de contacten van een relais kunt u allerlei elektrische apparaten in- en uitschakelen: het ene uiteinde van de relaisspoel komt op **+DC**, het andere op de klem **x I/O**, de verbruiker wordt geschakeld door de contacten van het relais (NC, C, NO). De gebruikte I/O-klem moet op de pagina **IN/OUT** van TrikdisConfig (of op het tabblad IN/OUT van de app) een uitgang (**OUT**) zijn – op de GET is dat de fabrieksinstelling.



Afbeelding 34. Een relais aansluiten op de uitgang van de communicatiemodule: de spoel komt tussen +DC en de klem x I/O, de contacten (NC, C, NO) schakelen de verbruiker.

- R relais („Relay")

De uitgangen kunt u schakelen vanuit de Protegus 2-app (hoofdstuk 5).

3.7 Inschakelen en eerste controle

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.

Na het aansluiten start ook de communicatiemodule zodra de voeding van de alarmcentrale wordt ingeschakeld. Op het frontdeksel moet u het volgende zien:

- **POWER** brandt groen – de voeding is in orde;
- **NETWORK LTE** brandt groen en knippert geel – verbonden met het mobiele netwerk; het aantal gele knipperingen is de signaalsterkte: op 4G zijn 3 knipperingen goed; als u er minder telt, is het signaal zwak: zoek een andere plaats voor de communicatiemodule of de antenne, of gebruik een gevoeligere antenne (paragraaf 3.2);
- **NETWORK LAN** brandt groen als u ook een netwerkkabel hebt ingestoken – verbonden met het bekabelde netwerk;
- **TROUBLE** is uit.

Als TROUBLE knippert, geeft het aantal knipperingen de oorzaak aan (paragraaf 1.6); elk ander afwijkend ledsignaal wijst ook op een storing, zoek de oorzaak op aan de hand van de tabellen in paragraaf 1.6. Als geen enkele led brandt, controleer dan de voeding en de aansluiting.

4. De alarmcentrale programmeren

Het instellen van de centrale hangt af van de manier waarop u hem hebt aangesloten: via de databus of de seriële poort (paragraaf 4.1), of via de telefoonkiezer, op de TIP/RING-klemmen (paragraaf 4.2). Bij de aansluiting Keybus + TIP/RING van Paradox SP / SP+ / MG / MG+ staat de instelling van de secties van de centrale in de tabel van paragraaf 3.3.3.

4.1 Aansluiting op databus of seriële poort

Hier beschrijven we hoe de centrale moet worden ingesteld zodat de communicatiemodule haar gebeurtenissen kan lezen en haar op afstand kan besturen. Voor besturing op afstand moet op de pagina **Panel settings** van TrikdisConfig (in de app: **Panel settings** → **Serial Bus**) de optie **Remote Arm/Disarm** zijn aangevinkt (paragraaf 2.2 en 6.3).

4.1.1 DSC

De **DSC PowerSeries**-centrales (de lijst met ondersteunde typen staat in punt 1.2) vereisen geen enkele aparte instelling: de op de Keybus aangesloten communicatiemodule leest de gebeurtenissen direct, en nadat **Remote Arm/Disarm** is aangevinkt, schakelt de gebruiker met zijn eigen bedieningscode in en uit vanuit de app. Over de details van de rechtstreekse bediening – zonestatussen, zone-overbrugging, automatische herkenning van de partities – gaat een apart artikel: Rechtstreekse bediening voor DSC PowerSeries-alarmcentrales.

Met de **DSC PowerSeries NEO**-centrales werkt de communicatiemodule niet: op de bus van de NEO staat de fabrikant geen externe apparaten toe. Voor de NEO is een communicatiemodule voor de telefoonlijn (TIP/RING) geschikt – zie DSC Power Series NEO en Trikdis-communicatiemodules: compatibiliteit en

oplossingen.

4.1.2 Paradox

De **Paradox**-centrales hoeven alleen voor de rechtstreekse bediening geprogrammeerd te worden; voor het lezen van de gebeurtenissen hoeft u niets in te stellen. De firmware van de centrale moet minimaal **V.4** zijn.

Op de nieuwere Paradox-centrales (bijvoorbeeld de SP+-, MG+- en EVOHD+-series) kan de seriële poort **af fabriek vergrendeld** zijn: de communicatiemodule ontvangt geen gegevens totdat u de poort ontgrendelt. Hoe u dat doet: Vergrendelde seriële poort ontgrendelen op Paradox-alarmcentrales.

Voor de bediening moet u het **pc-wachtwoord** (PC password) van de centrale instellen, en hetzelfde wachtwoord ook invullen in het veld **System settings → Security panel PC download password** van TrikdisConfig – de twee moeten overeenkomen.

1. Open op het bedieningspaneel de installateursprogrammering van de centrale.
2. Open de sectie van het pc-wachtwoord: bij de series **MAGELLAN en SPECTRA** sectie **911**, bij de serie **DIGIPLEX EVO** sectie **3012**.
3. Voer een wachtwoord van **4 tekens** in. Het wachtwoord mag niet 0000 zijn en **mag niet met een nul beginnen**.
4. Verlaat de programmering en **start de centrale opnieuw** – een gewijzigd pc-wachtwoord wordt pas na een herstart actief. Vul daarna hetzelfde wachtwoord in TrikdisConfig in.

Veelvoorkomende fouten en oplossingen

- De aan de partitie toegewezen **bedieningscode mag niet de mastercode zijn**: geef de gebruiker een andere code; daarmee werkt het in- en uitschakelen vanuit Protegus 2.
- **Start de communicatiemodule opnieuw na elke wijziging van een bedieningscode** (spanning eraf of de sms-opdracht `RESET`): de codes worden bij het opstarten uitgelezen, latere wijzigingen ziet de module niet.

Op de GET-communicatiemodule staat het veld **Security panel PC download password** op de pagina **Panel settings** van TrikdisConfig, in de groep **Serial bus**; in de Protegus 2-app bij **Panel settings → Serial Bus → PC download password** (paragraaf 2.2 en 6.3).

Aansluiting op Keybus en TIP/RING (SP / SP+ / MG / MG+, paragraaf 3.3.3): de centrale moet daarnaast zo worden geprogrammeerd dat ze de gebeurtenissen naar de meldkamer stuurt en vanuit Protegus 2 bestuurbaar is – de waarden van de secties (801, 811, 812, 815, 911) staan in de tabel van paragraaf 3.3.3.

4.1.3 Texecom

De **Texecom Premier / Premier Elite**-centrales moeten zowel voor het lezen van de gebeurtenissen als voor de bediening worden geprogrammeerd: u stelt het wachtwoord van 4 tekens van de centrale in, **UDL passcode** genaamd, en vult hetzelfde in het veld **System settings → Security panel PC download password** van TrikdisConfig in – de twee moeten overeenkomen.

Met de Texecom-software Wintex: de UDL passcode vindt u op het tabblad **Options** van het venster **Communication Options**.

Via het bedieningspaneel:

1. Voer de 4-cijferige installateurscode in en druk op de toets **[Menu]** om het programmeermenu te openen.
2. Druk direct daarna op de toets **[9]**.
3. Druk op **[7][6]**, daarna op de toets **[2]**, en voer de 4-cijferige UDL passcode in.
4. Druk op de toets **[Yes]** en verlaat daarna de programmering met de toets **[Menu]**.

Op de GET-communicatiemodule staat het veld **Security panel PC download password** op de pagina **Panel settings** van TrikdisConfig, in de groep **Serial bus** (in de app bij **Panel settings** → **Serial Bus** → **PC download password**); de UDL passcode moet hiermee overeenkomen.

4.1.4 UTC Interlogix (Caddx)

De firmware van de **UTC Interlogix (Caddx) NetworX**-centrale moet minimaal **V2** zijn. Op het bedieningspaneel van de centrale stelt u het volgende in:

1. Druk op de toetsen **[*][8]** en voer de installateurscode in (af fabriek **9713**).
2. Voer het **apparaatnummer** in dat aan de communicatiemodule is toegewezen (device address; af fabriek **0**).
3. Programmeer de regels van de onderstaande tabel na elkaar: voer de locatie (location) in, het segmentnummer en daarna de instelling. Met de toets **[*]** gaat u terug naar het vorige veld. `12345678` betekent dat alle acht schakelaars van het segment zijn ingeschakeld (op het display zijn alle cijfers zichtbaar).

Locatie (location)	Segment	Instelling
23	3	12345678
37 (niet strikt noodzakelijk)	3	12345678
37 (niet strikt noodzakelijk)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Als u alle regels hebt geprogrammeerd, drukt u tweemaal op de toets **[Exit]** om de programmering te verlaten.

4.1.5 InnerRange

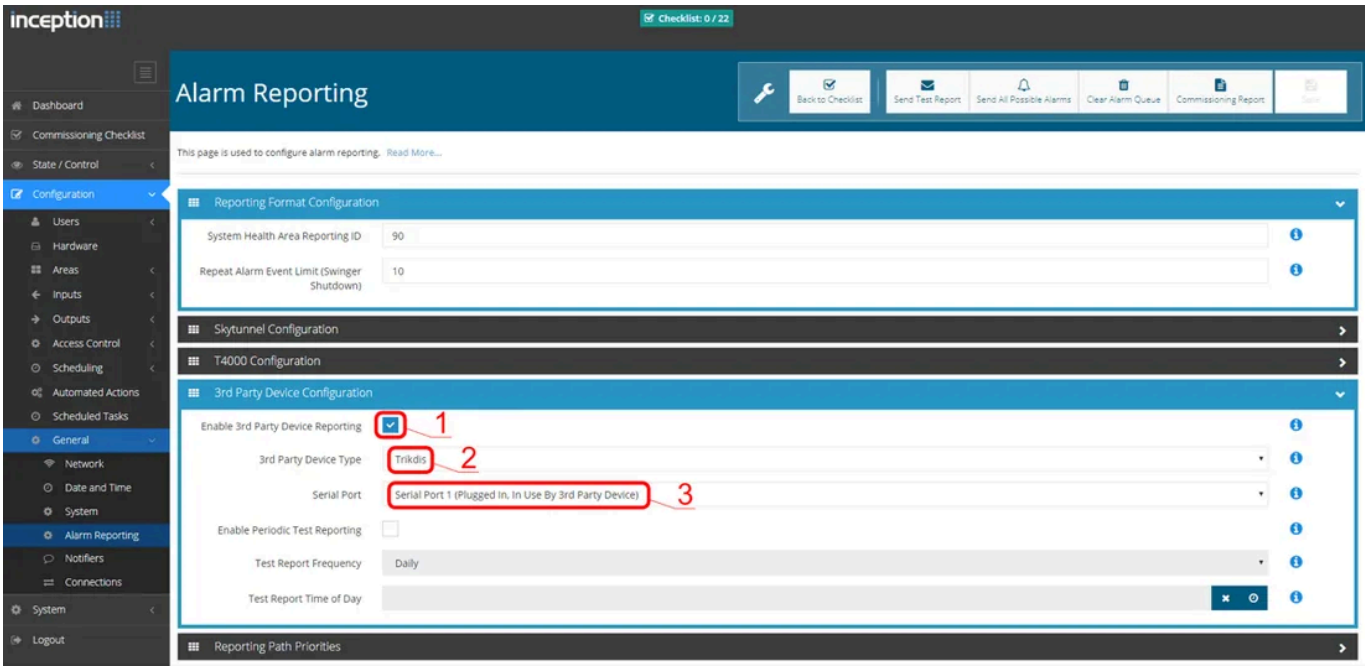
De firmware van de **InnerRange Inception**-centrale moet minimaal **2.3.0.3507-r0** zijn, en de centrale heeft een internetverbinding nodig. De instelling doet u in de webinterface van de centrale:

1. Open in een browser het adres `https://skytunnel.com.au/inception/SERIENUMMER`, waarbij SERIENUMMER het serienummer op de doos van de centrale is. Meld u aan met het installateursaccount.
2. Open de pagina **Configuration** → **General** → **Alarm Reporting**.

3. In de groep **3rd Party Device Configuration**: - vink de optie **Enable 3rd Party Device Reporting** aan; - kies in het veld **3rd Party Device Type** de waarde **Trikdis**; - kies in het veld **Serial Port** de waarde **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Sla de instellingen op en verlaat de interface.

De firmware van de **InnerRange Integriti**-centrale moet minimaal **19.1.0.36608** zijn, en de programmeersoftware (Integriti Professional) minimaal **19.1.0.15396**. De instelling doet u in de programmeersoftware van de centrale:

1. Kies bij de seriële poort (**TTL Port-0**) waarop de communicatiemodule is aangesloten, het communicatieprotocol **Trikdis**.
2. Het dataformaat moet **Contact ID** zijn.
3. Instelling van de poort: **19200, 8, N, 1**.
4. Sla de instellingen op en sluit het programma af.



Afbeelding 35. InnerRange Inception – Configuration → General → Alarm Reporting, groep 3rd Party Device Configuration: Enable 3rd Party Device Reporting aangevinkt, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

De firmware van de **Honeywell Ademco Vista-20**- en **Vista-48**-centrale moet minimaal **V5.3** zijn. De instelling doet u op het bedieningspaneel van de centrale.

De programmering openen – op twee manieren:

- voer de installateurscode in (af fabriek **4112**), gevolgd door de toetsen **[8][0][0]**; of
- zet spanning op de centrale en druk **binnen 50 seconden** tegelijk op de toetsen **[*]** en **[#]** (dit werkt alleen als de programmering eerder met de toetsen [*][9][8] is verlaten).

Instellingen:

1. Schakel het verzenden van Contact ID-gebeurtenissen via de uitgang voor de radio met groot bereik (LRR) in: druk op de toetsen **[*][2][9][1][#]**.
2. Schakel voor de bediening op afstand het gebruik van het **2e AUI-adres** (2nd AUI address) in: druk op de toetsen **[*][1][8][9][1][1][#]**.

De programmering verlaten: druk op de toetsen **[*][9][9]**.

4.2 Aansluiting op de telefoonlijn (TIP/RING)

Om de alarmcentrale de gebeurtenissen via haar telefoonlijnuitgang te laten verzenden, moet de kiezer van de centrale worden ingeschakeld en ingesteld. De precieze programmeerlocaties vindt u in de installatiehandleiding van de centrale; de kern van de instelling is bij elke fabrikant dezelfde:

1. **Schakel de telefoonlijncommunicator (PSTN)** in de centrale in.
2. **Geef als telefoonnummer `1234` op** bij de meldkamerontvanger – ongeacht of de communicatiemodule op de RING/TIP-klemmen van de centrale of op de telefoonlijn is aangesloten. Met een ander nummer kan het gebeuren dat de centrale wel kiest, maar de communicatiemodule de gebeurtenissen toch niet ontvangt: ook bij een DSC PowerSeries NEO-centrale kwam de doormelding pas op gang nadat het nummer in `1234` was gewijzigd.
3. **Kiesmethode:** DTMF (tone), geen pulskiezen.
4. **Protocol:** Contact ID.

Als u de centrale op afstand, met de uitgang van de communicatiemodule, wilt in- en uitschakelen, moet de op de uitgang aangesloten zone in de centrale als **sleutelschakelaarzone** worden ingesteld.

De sleutelschakelaarzone kan pulserend of bistabiel zijn. De uitgang van de communicatiemodule geeft standaard een puls van 3 seconden; de pulsduur of de bistabiele modus kunt u in de instellingen van de Protegus 2-app wijzigen.

De centrales van DSC, Paradox, Caddx, Texecom, InnerRange en Honeywell kunnen ook via hun telefoonlijnuitgang op de communicatiemodule worden aangesloten (paragraaf 3.3.9) – dan moet ook bij deze centrales de kiezer worden ingesteld, en is directe besturing niet beschikbaar.

4.2.1 De kiezer van de Honeywell Vista programmeren

Ga op het bedieningspaneel naar de programmeermodus en stel deze programmeerlocaties in:

Programmeerlocatie	Instelling
`*41`	het telefoonnummer van de meldkamerontvanger: `1234`
`*43`	het objectnummer van de centrale
`*47`	Tone dial = `1`, en het aantal kiespogingen
`*48`	`7` (standaard)
`*49`	`5` (Split/Dual-bericht)
`*50`	vertraging bij het verzenden van een inbraakalarm – standaard `2,0` (30 s); voor direct verzenden `0,0`

Stel bij een **Honeywell Vista 48**-centrale daarnaast de volgende programmeerlocaties in:

Programmeerlocatie	Waarde	Programmeerlocatie	Waarde	Programmeerlocatie	Waarde
`*41`	1234 (telefoonnummer ontvanger)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1

Programmeerlocatie	Waarde	Programmeerlocatie	Waarde	Programmeerlocatie	Waarde
`*43`	1234 (objectnummer)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

Verlaat aan het einde van de programmering de programmeermodus met de opdracht `*99`.

4.2.2 De kiezer van de UTC Interlogix (Caddx) NX

Programmering van de Interlogix NX-4V2-centrale (NX-6V2, NX-8V2) als de communicatiemodule op de TIP/RING-klemmen van de centrale is aangesloten. Voer op het bediendeel na elkaar het volgende in:

Plaats (location)	Toetsen	Opmerking
	`*89713`	De programmering openen (`9713` is de standaard installateurscode)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Alle zone-leds branden (segment 1)
Location 4	`12345678*`	Alle zone-leds branden (segment 2)
Location 4	`12345678*#`	
Location 23	`23#`	Alle zone-leds branden (segment 3)
Location 23	`**`	Alle zone-leds branden (segment 3)
Location 23	`12345678*#`	Alle zone-leds branden (segment 3)
Location 37	`37#`	Alle zone-leds branden (segment 3)
Location 37	`**`	Alle zone-leds branden (segment 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT EXIT`	De programmering verlaten

5. Besturing op afstand met de Protegus 2-app

Met de mobiele en webapp Protegus 2 ziet de gebruiker op afstand de status van het systeem, krijgt hij meldingen over de gebeurtenissen, kan hij in- en uitschakelen en de uitgangen van de communicatiemodule schakelen. De app kan worden gedownload voor Android en iOS (Google Play, App Store), of in de browser worden gebruikt: web.protegus.app. Meld u aan met uw gebruikersnaam en wachtwoord, of registreer een nieuw account. De GET stuurt geen meldingen per sms of telefoonoproep, en ontvangt ook geen sms-commando's: besturing op afstand en meldingen gaan via de app; ook de instellingen van de communicatiemodule zijn bereikbaar vanuit de app (**Settings** → **Advanced settings**, hoofdstuk 6).

5.1 Het apparaat toevoegen

Controleer vóór het toevoegen van het apparaat:

1. De simkaart is actief en de pincode ervan is in het apparaat ingevoerd, of de pincodevraag is uitgeschakeld – **of** de communicatiemodule is met een netwerkkabel (LAN) op het lokale netwerk aangesloten.
2. Op het tabblad **User reporting** → **PROTEGUS Cloud** van TrikdisConfig is **Enable connection** aangevinkt (paragraaf 6.5).
3. De **POWER**-led brandt groen.
4. De **NETWORK LTE**-led brandt groen en knippert geel (het apparaat is op het mobiele netwerk); bij alleen een bekabelde verbinding brandt de **NETWORK LAN**-led groen.

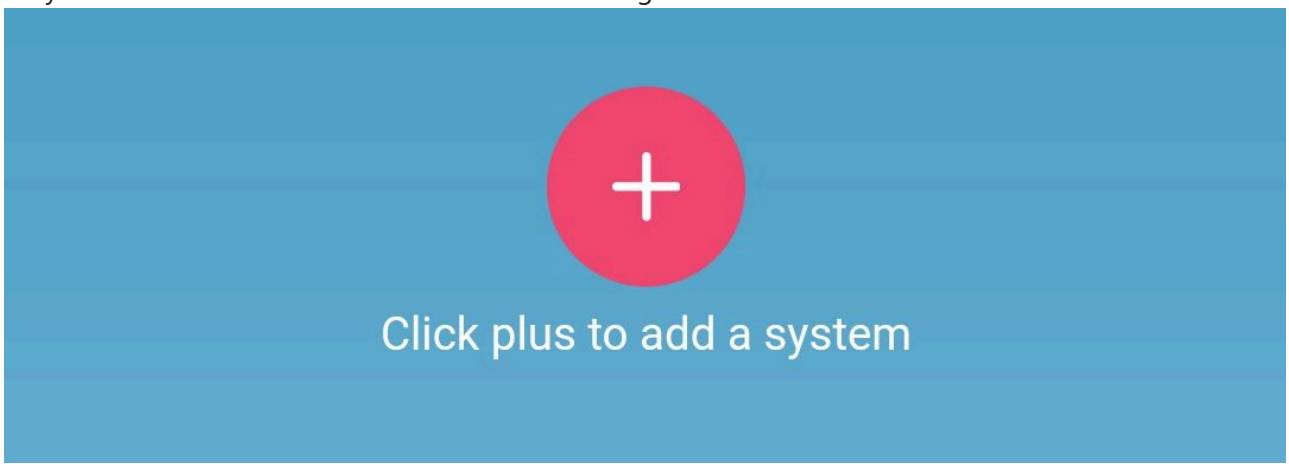
De DATA-led is de eenvoudigste internetcontrole. De DATA-led brandt wanneer er in het geheugen van het apparaat een bericht klaarstaat om te worden verzonden. Het groene licht van de NETWORK-led zegt alleen dat de netwerkverbinding tot stand is gekomen – bij een apparaat met mobiel netwerk heeft het zich aangemeld op het netwerk van de provider, bij een Ethernet-apparaat werkt de verbinding tot aan de router –, maar niet dat het apparaat ook het internet bereikt. Als de NETWORK-led groen is, maar de DATA-led ook na een gebeurtenis of testrapport continu blijft branden, werkt de internetverbinding niet: het bericht kan niet worden verzonden. Op een mobiel netwerk ligt de fout meestal bij de APN of de datadienst van de simkaart, bij Ethernet bij de router, de firewall of de DNS. Als de DATA-led uitgaat, is het bericht verzonden en is de dataverbinding in orde.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



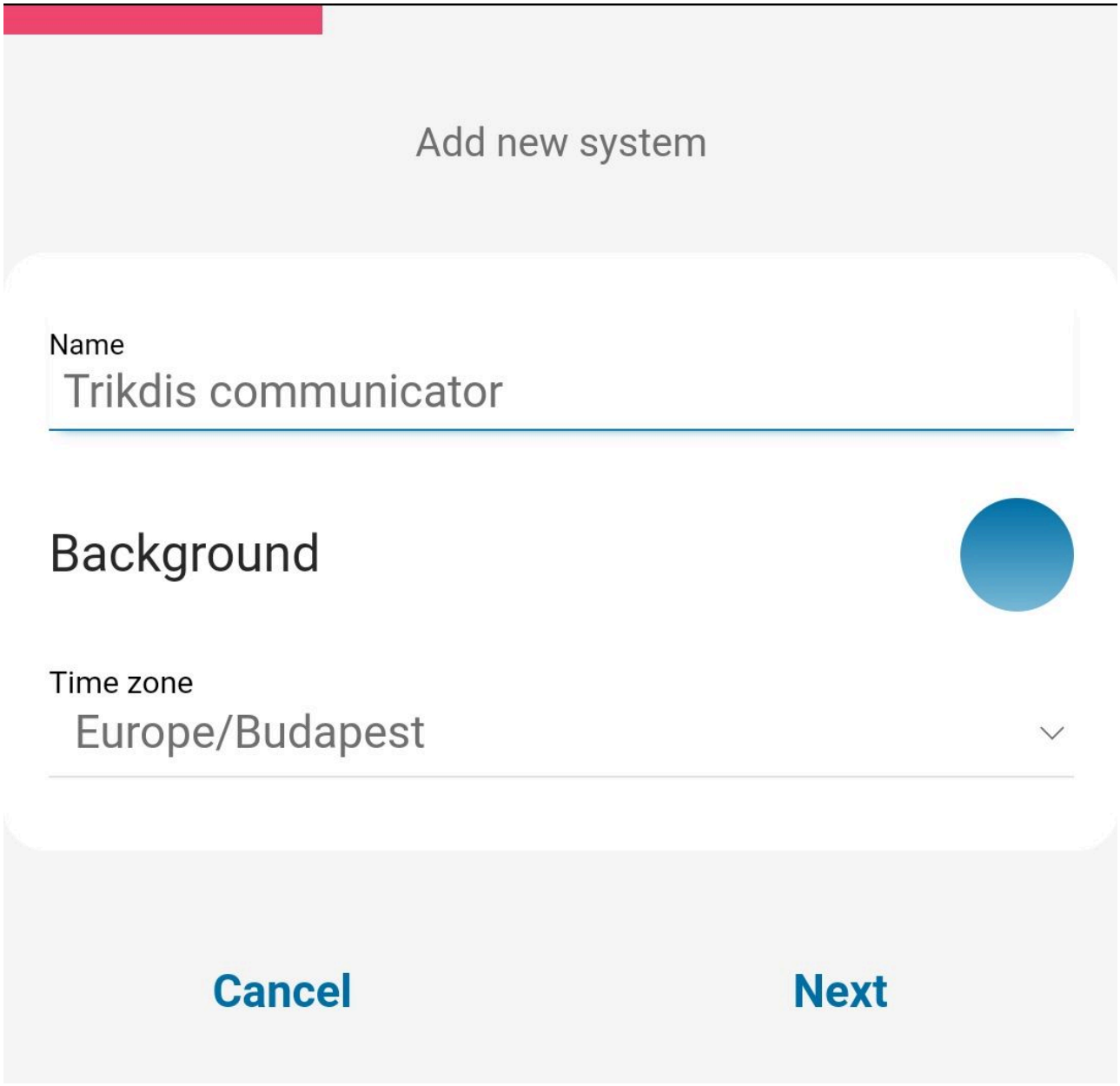
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



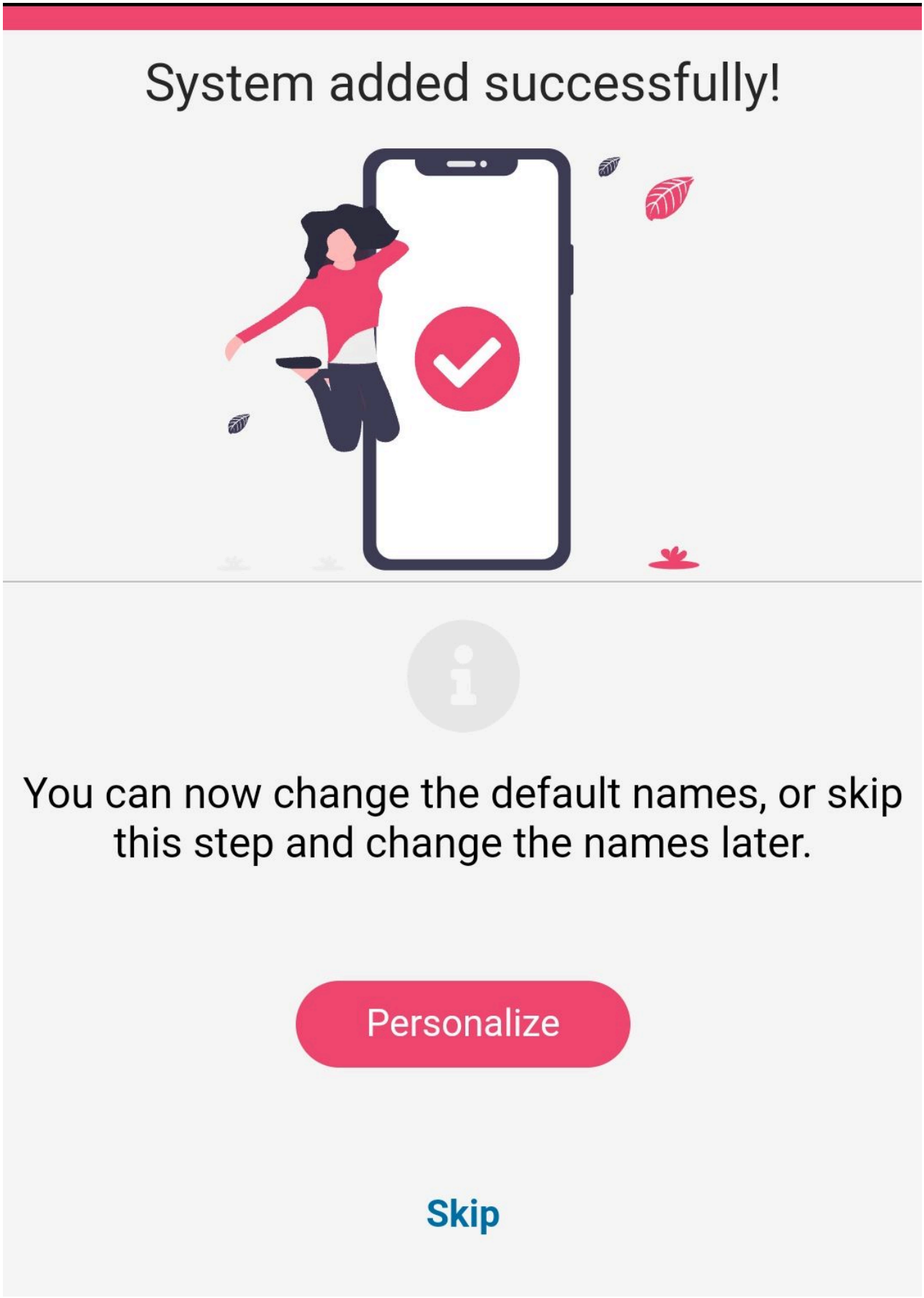
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



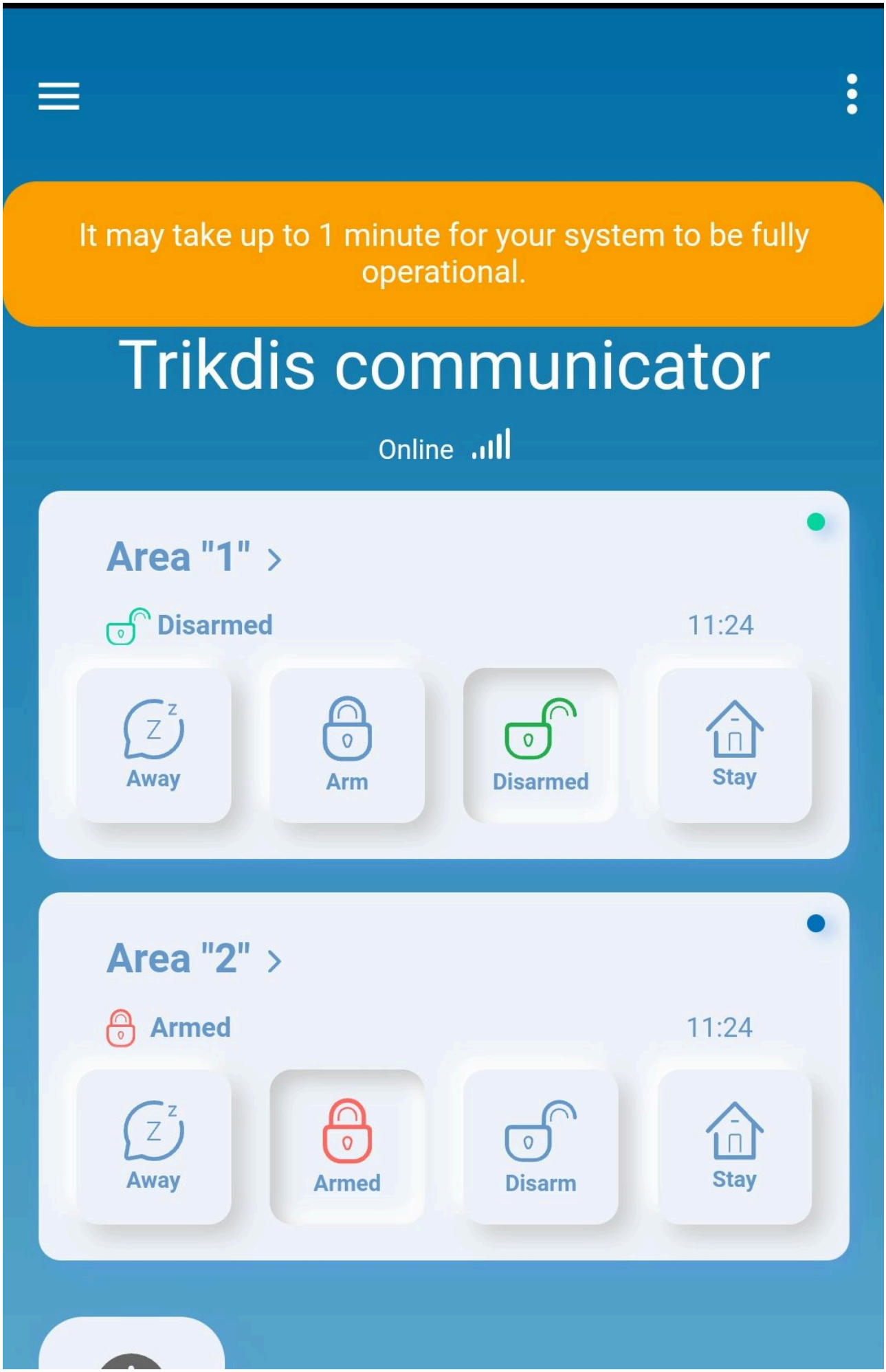
6. Add meg a rendszer nevét és válassz idozónát

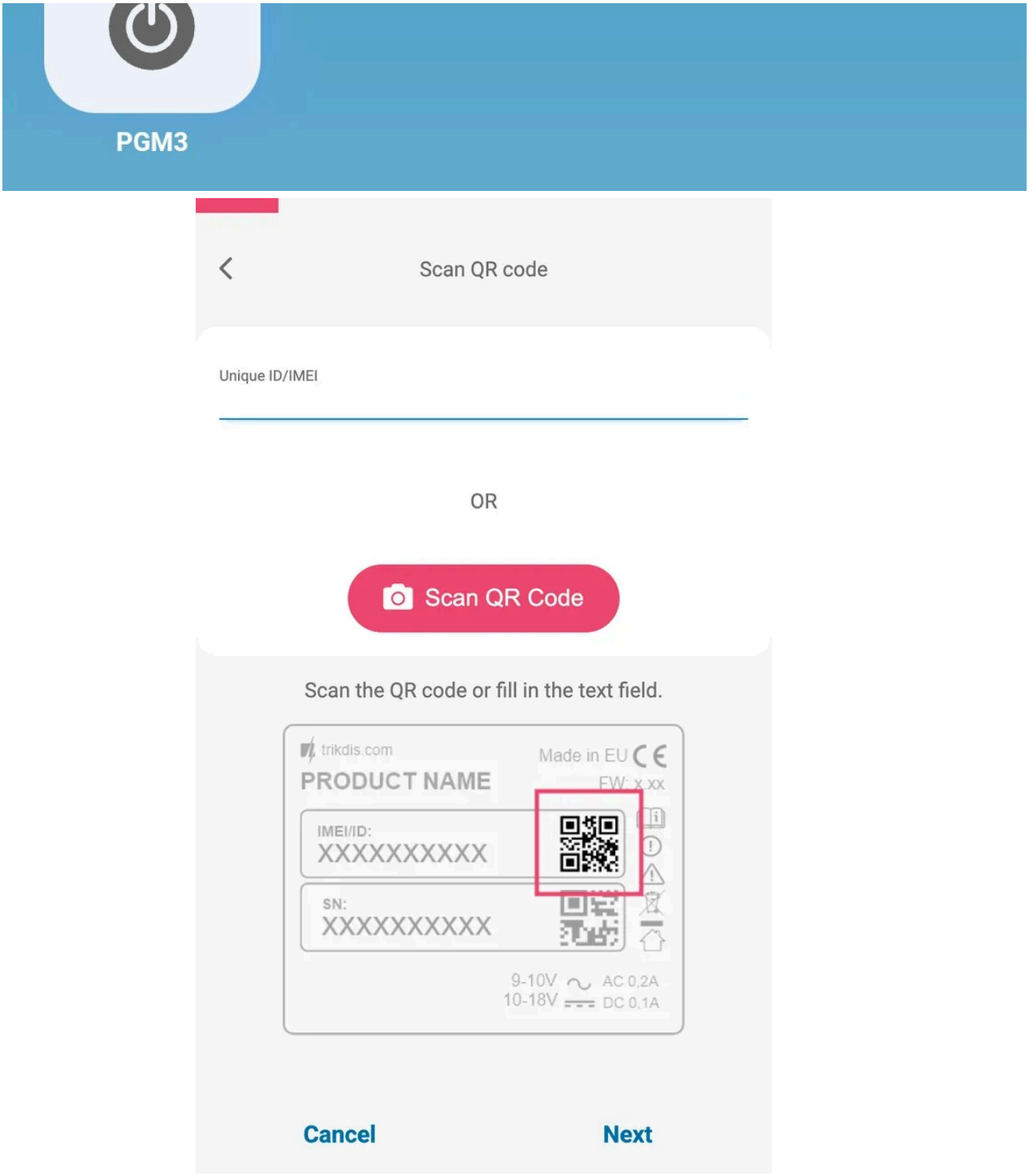


7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.

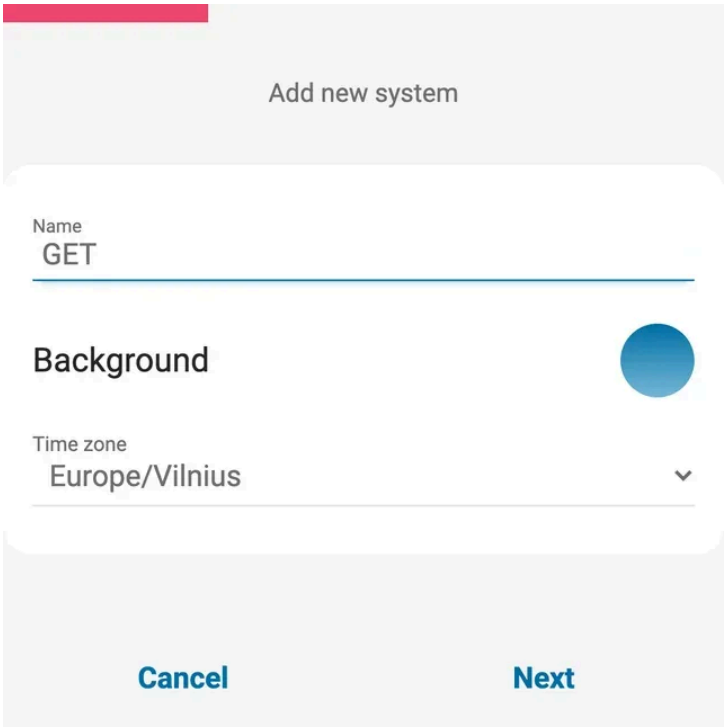


8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


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



Afbeelding 36. Protegus 2 – een nieuw systeem toevoegen: de IMEI / Unique ID invoeren of de QR-code op het label scannen, daarna Next.



Afbeelding 37. Protegus 2 – de naam (Name) van het systeem invoeren, daarna Next.

De unieke identificatie van het apparaat (**IMEI / Unique ID**) staat op het label van het apparaat en op de sticker van de doos, en wordt ook in de statusbalk van TrikdisConfig getoond. Als de **PROTEGUS Cloud access Code** in het apparaat niet de fabriekswaarde is, vraagt de app er bij het toevoegen om.

5.2 In- en uitschakelen met een uitgang

Als u de alarmcentrale met de uitgang van de communicatiemodule, via de sleutelschakelaarzone van de centrale, wilt in- en uitschakelen, geeft u in de Protegus 2-app bij de partitie op welke uitgang haar bedient.

De zone van de centrale waarop de uitgang van de communicatiemodule is aangesloten, moet in de centrale als **sleutelschakelaarzone** zijn geprogrammeerd, en de centrale moet de in- en uitschakelgebeurtenissen melden – op basis daarvan toont Protegus 2 de status van de partitie.

U kunt de instelling uitvoeren bij het aanmaken van het systeem, bij het toevoegen van de partities, of achteraf in de systeeminstellingen, bij het bewerken van de partitie. Bij het aanmaken van het systeem leidt de wizard van Protegus 2 u door de stappen: klik op de knop **Continue** (Doorgaan), geef de naam van de partitie op (**Area name**) en schakel de bediening van de PGM-uitgang vanuit de Protegus 2-app in – dat gaat met de volgende stappen:

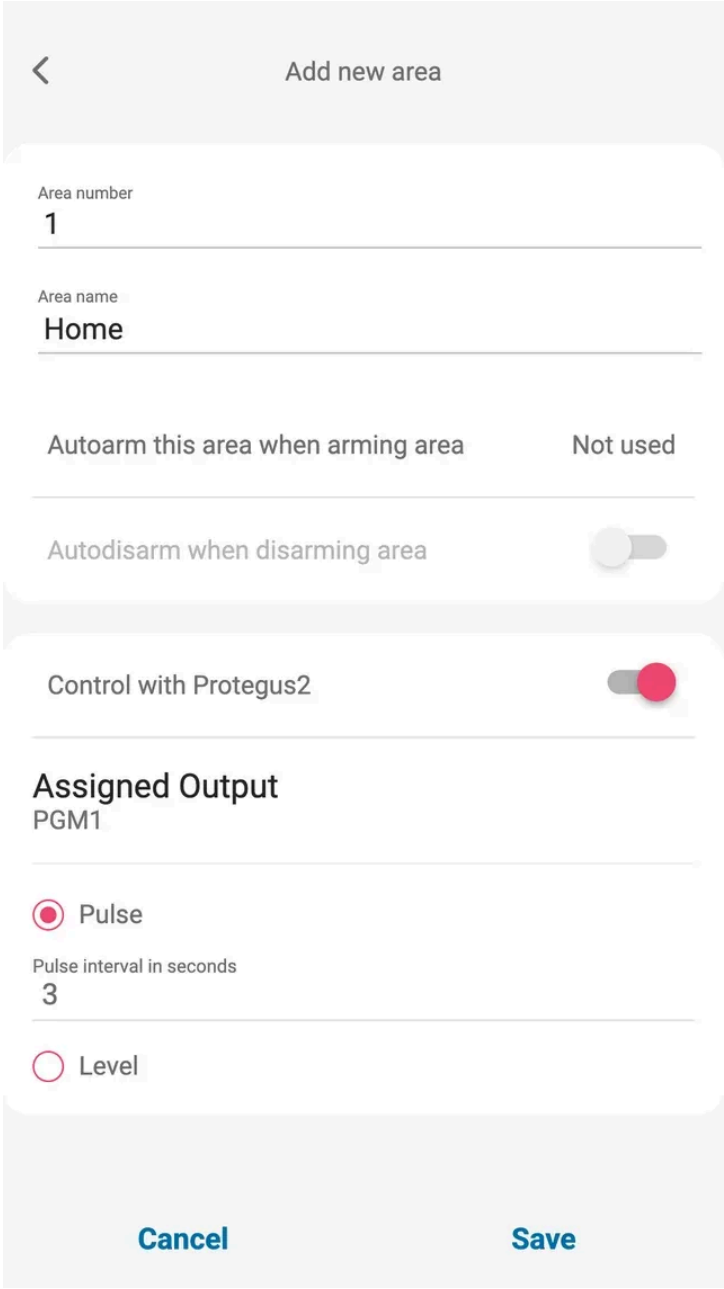
1. Kies (of voeg toe) de partitie die u wilt bedienen. Het nummer van de partitie moet overeenkomen met het nummer dat de centrale in de gebeurtenissen verstuurt (partitie 1 is 1, partitie 2 is 2).
2. Schakel de optie **Bediening met PGM** (Control with Protegus2) in en kies in het veld **uitgang** (Assigned Output) de uitgang van de communicatiemodule (PGM1, PGM2 …). Een uitgang kan maar één partitie bedienen.
3. Kies de werkingsmodus: **pulserend** (Pulse) of **bistabiel** (Level) – dezelfde die u in de centrale bij de sleutelschakelaarzone hebt ingesteld. Meestal gebruiken we de pulserende modus; ook de pulsduur kan worden opgegeven (standaard 3 s).

4. Sla de instelling op (**Save**). Herhaal dit bij meerdere partities voor elke partitie, met haar eigen uitgang: in de wizard voegt u een volgende partitie toe met de knop **Click to add an area** en stelt u haar PGM-uitgang op dezelfde manier in. Als u alle partities hebt ingesteld, gaat u in de wizard verder met de knop **Skip**.

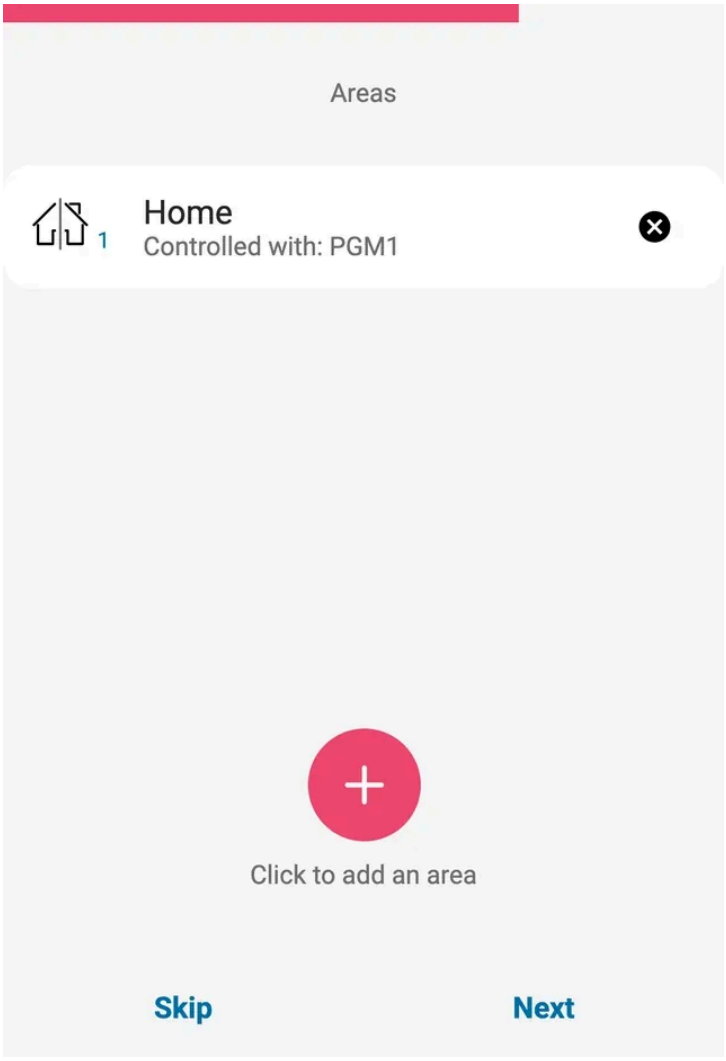
Protegus 2 kan de status van de partities alleen correct weergeven als de centrale de in- en uitschakelgebeurtenissen met het juiste partitienummer verstuurt. Over de details en valkuilen van inschakelen met een sleutelschakelaar gaat een apart artikel: Inschakelen op afstand met een sleutelschakelaar vanuit de Protegus 2-app.



Afbeelding 38. Protegus 2 – het scherm „Het systeem wordt niet op afstand bestuurd" bij het aanmaken van het systeem: met de knop Continue gaat u naar de instelling van de partitie en de PGM-uitgang.



Afbeelding 39. Protegus 2 – een partitie toevoegen (Add new area): Area number, Area name, Control with Protegus2 ingeschakeld, Assigned Output PGM1, Pulse (3 s) of Level, daarna Save.

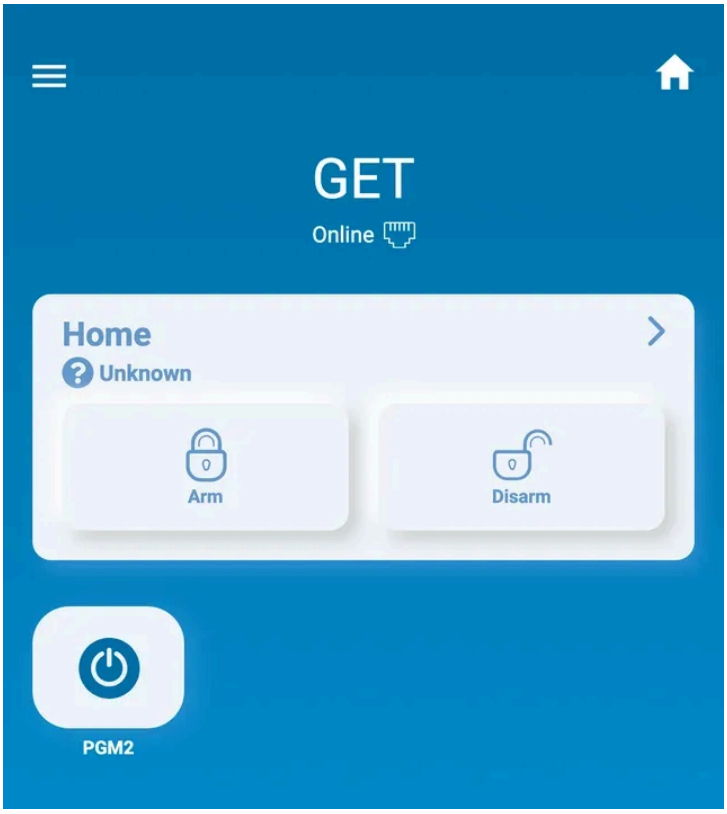


Afbeelding 40. Protegus 2 – de lijst van partities (Areas): de partitie Home wordt aangestuurd door PGM1; nog een partitie met de knop Click to add an area, de wizard kan met de knop Skip worden afgesloten.

5.3 In- en uitschakelen vanuit de app

1. Open het systeem in de Protegus 2-app. Op het startscherm heeft elke partitie een eigen kaart en een eigen slot: een **gesloten, rood slot** betekent een ingeschakelde partitie, een **open, groen slot** een uitgeschakelde.
2. Tik op het slot van de partitie en kies de gewenste handeling: inschakelen of uitschakelen.
3. Voer de pincode in als de app daarom vraagt.

Het slot neemt de werkelijke status aan op basis van de gebeurtenis die van de alarmcentrale binnenkomt; de app geeft ook in de gebeurtenissenlijst en in een melding aan of de centrale de handeling heeft uitgevoerd.



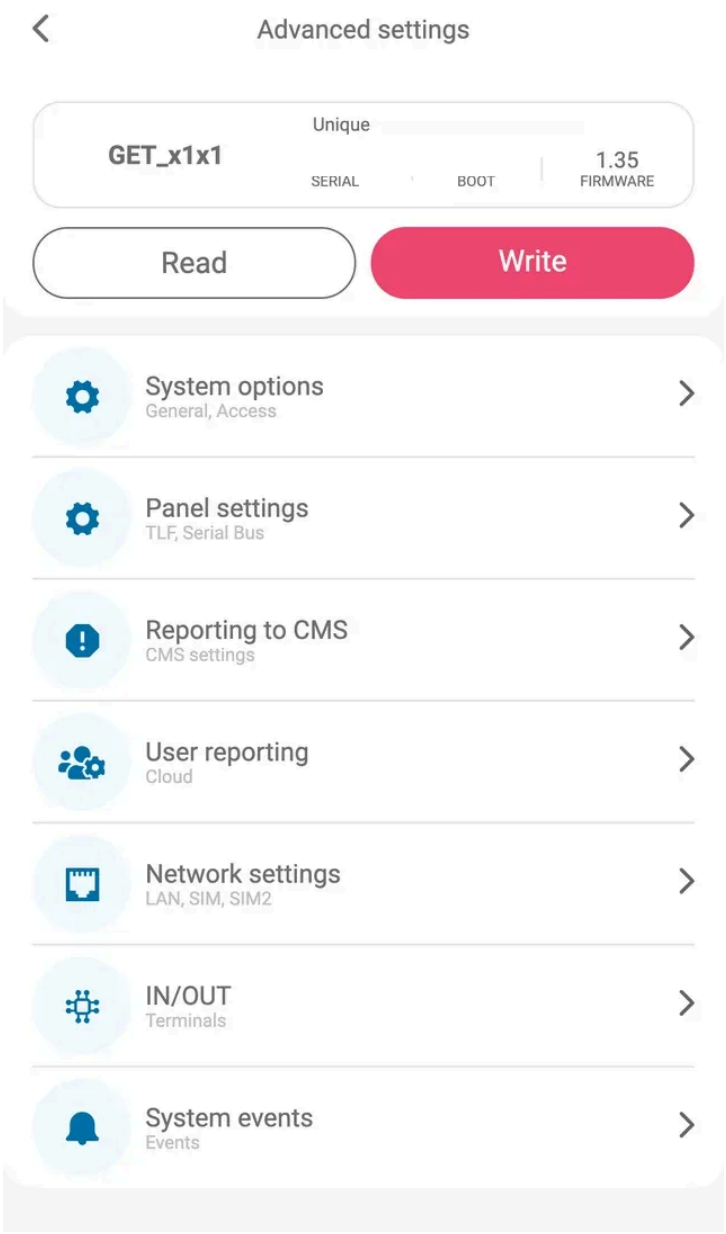
Afbeelding 41. Protegus 2 – het startscherm van het systeem: de status van de partitie, de knoppen Arm en Disarm, daaronder de schakelbare PGM-uitgang.

6. De instellingen in detail

De meeste instellingen van de GET zijn zowel in het Windows-programma **TrikdisConfig** als in de **Protegus 2**-app (**Settings** → **Advanced settings**, paragraaf 2.2) beschikbaar; waar iets alleen in een van de twee zit, geven we dat aan. Elke instelling beschrijven we één keer, en per paragraaf geven we aan waar u die in de twee hulpmiddelen vindt; tussen haakjes staat het opschrift in de app, als dat afwijkt van dat in TrikdisConfig. Links in het TrikdisConfig-venster staat de lijst van pagina's (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), bovenaan de knoppenbalk (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), onderaan de statusbalk.

6.1 Verbinding maken met de communicatiemodule

Protegus 2-app. Open het systeem en ga naar het menu **Settings** → **Advanced settings**. Bovenaan elk scherm staan de gegevens van het verbonden apparaat: **Unique ID** (IMEI), **Serial** (serienummer), **Firmware**- en **Boot**-versie. De groepen instellingen in het menu: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** en **System events**. Na een wijziging schrijft u de instellingen met de knop **Write** naar het apparaat; **Read** leest de actuele waarden opnieuw uit het apparaat.



Afbeelding 42. Protegus 2 – menu Advanced settings: bovenaan de gegevens van het apparaat (type, Unique ID, serienummer, boot- en firmwareversie), de knoppen Read en Write, daaronder de groepen instellingen.

TrikdisConfig. Na het aansluiten van de communicatiemodule en het indrukken van **Read [F4]** toont het programma de gegevens van het apparaat in de statusbalk.

Na het aansluiten en uitlezen van het apparaat (**Read [F4]**) ziet u onderaan het venster de belangrijkste gegevens van het apparaat:

Opschrift	**Betekenis**
IMEI / Unique ID, bij een Ethernet-apparaat **MAC / Unique ID**	De unieke identificatie van het apparaat: bij een apparaat met simkaart de IMEI, bij een Ethernet-apparaat het MAC-adres. Hetzelfde staat op de doos en op de achterkant van het apparaat.
Status	De huidige bedrijfstoestand.

Opschrift	Betekenis
Device	Het type (typeaanduiding) van het apparaat. Controleer of hier het type van uw eigen apparaat staat.
SN	Serienummer.
BL	De versie van de bootloader.
FW	De versie van de firmware.
HW	De versie van de hardware.
State	De verbindingswijze: USB of op afstand (remote).
Administrator / Installer	Het toegangsniveau van degene die programmeert (na invoer van het wachtwoord).

Nadat u de instellingen hebt uitgevoerd, schrijft u ze met de knop **Write [F5]** naar het apparaat; met de knoppen **Open [F8]** en **Save [F9]** kunt u de volledige set instellingen in een bestand opslaan en in een ander apparaat laden. **Save [F9]** slaat de instellingen op in een instellingenbestand, **Open [F8]** opent het opgeslagen bestand; de opgeslagen instellingen kunt u later ook in andere apparaten laden, zodat u meerdere apparaten snel met dezelfde instellingen kunt configureren.

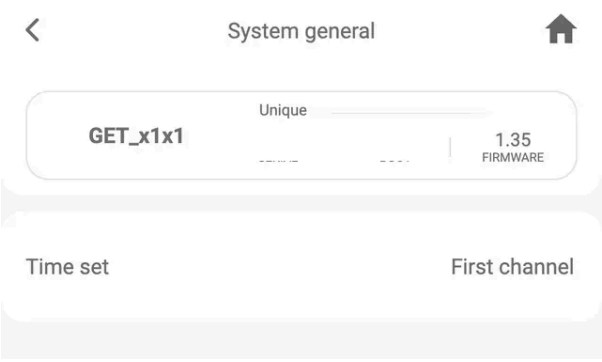


Afbeelding 43. De statusbalk van TrikdisConfig met een uitgelezen GET: identificatie, status, type (Device: GET_S170), serienummer, BL (bootloader), FW- en HW-versie, verbindingswijze en toegangsniveau.

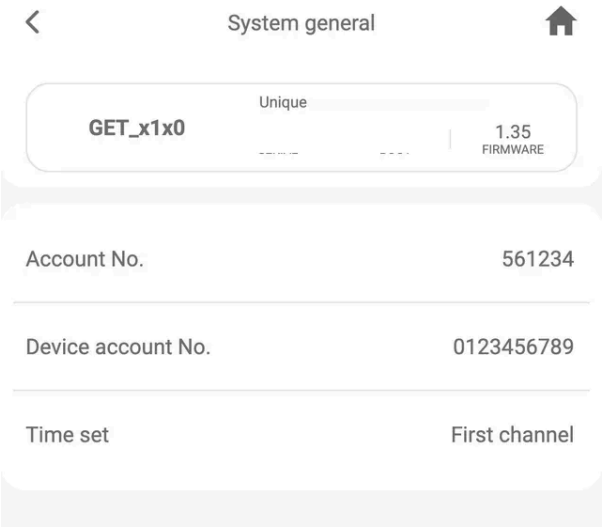
In het veld **Device** moet een GET-typeaanduiding staan (op de afbeelding GET_S170; het letter-cijferachtervoegsel geeft de hardwareversie aan), **BL** is de versie van de bootloader. Na **Read [F4]** leest het programma de in het apparaat ingestelde waarden uit en toont ze; maak de benodigde instellingen volgens de onderstaande beschrijvingen van de pagina's.

6.2 System settings (System options)

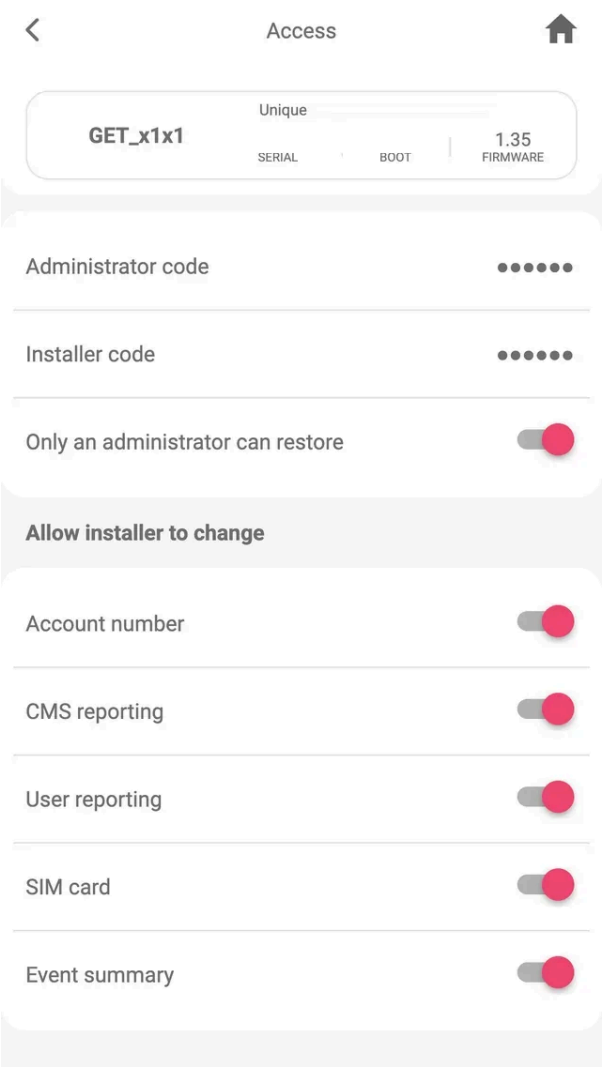
In de app: Advanced settings → System options → System general (identificaties, tijdsynchronisatie) en **System options → Access** (codes en installateursrechten). Waar **Account No.** en **Device account No.** staan, hangt af van de hardwareversie en de firmware: op hardware **x1x1**, met firmware **1.31** of nieuwer, vindt u ze op het tabblad **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.**; op het parallelle kanaal **Parallel Account no.**) en op het tabblad **Reporting to CMS → Settings** (**Device account No.**), op het tabblad System general blijft alleen **Time set** over; anders staan ze allebei op het tabblad System general.



Afbeelding 44. Protegus 2 – System options → System general op hardware x1x1 (firmware 1.35): alleen Time set is zichtbaar, de identificaties staan bij de CMS-instellingen.

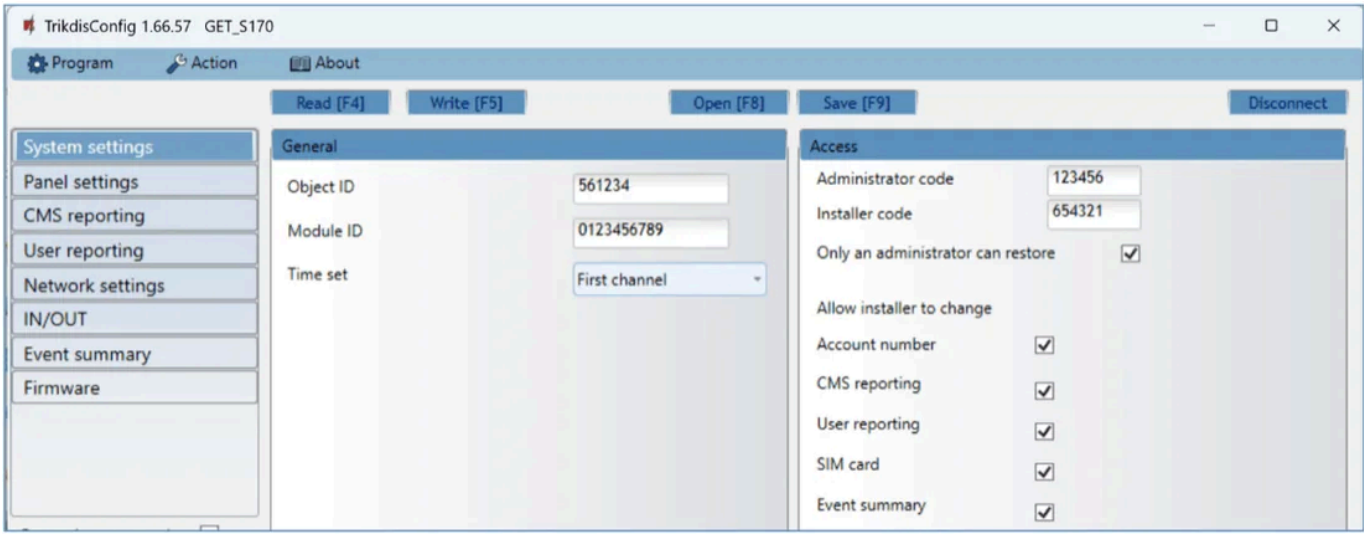


Afbeelding 45. Protegus 2 – System options → System general op hardware x1x0: Account No., Device account No. en Time set.



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

In TrikdisConfig: de pagina **System settings** bestaat uit twee groepen: in de groep **General** stelt u de identificaties van het apparaat in, in de groep **Access** de toegangsniveaus.



Afbeelding 47. TrikdisConfig – pagina System settings: groep General (Object ID, Module ID, Time set) en groep Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – het objectnummer dat u van de meldkamer hebt gekregen (6 hexadecimale tekens: 0–9, A–F; `FFFE` en `FFFF` kunnen niet worden gebruikt). Verplicht als het apparaat ook naar een meldkamer meldt.
- **Module ID** (Device account No.) – het identificatienummer van de module.
- **Time set** – van welke server het apparaat zijn klok synchroniseert.

In de groep **Access** beheert u de toegangsniveaus en wachtwoorden.

Voor de instellingen van het apparaat zijn er twee toegangsniveaus: **beheerder** en **installateur**.

- **Administrator code** – toegang tot alle instellingen (fabriekswachtwoord: `123456`; het wachtwoord bestaat uit 6 tekens: cijfers of Latijnse letters).
- **Installer code** – toegang die kan worden beperkt (fabriekswachtwoord: `654321`).
- **Only an administrator can restore** – met dit vinkje kan alleen de beheerder de fabrieksinstellingen herstellen.
- **Allow installer to change** – hier geeft u aan welke instellingsgroepen de installateur mag wijzigen: **Account number** (objectnummer), **CMS reporting**, **User reporting**, **SIM card** (bij een apparaat met mobiel netwerk) of **Ethernet settings** (bij een Ethernet-apparaat), **Event summary**.

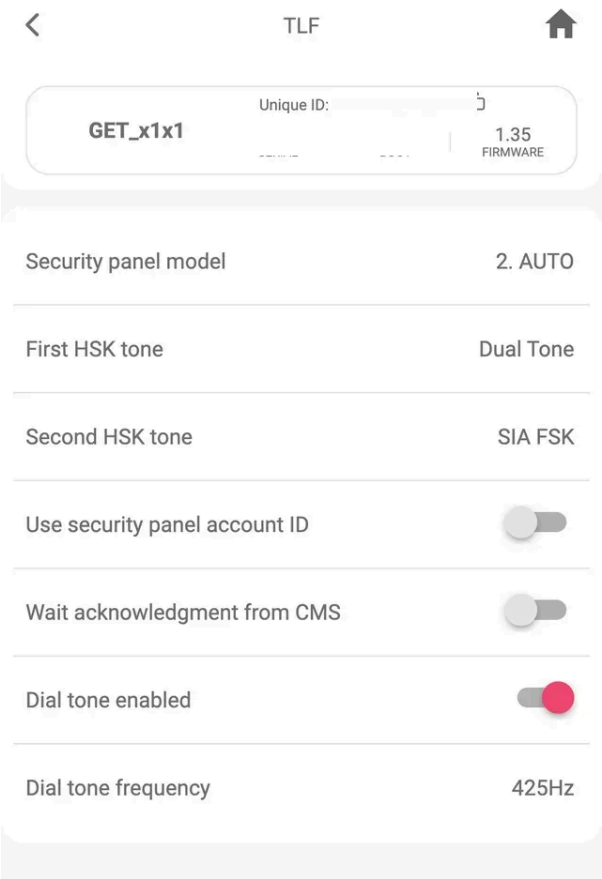
Laat geen fabriekswachtwoorden in het apparaat staan!

Wijzig bij de inbedrijfstelling ten minste het beheerderswachtwoord en noteer het op een veilige plaats. Een vergeten wachtwoord kan ook niet worden gewist door de fabrieksinstellingen te herstellen, want daarvoor is ook een wachtwoord nodig: dan kan alleen de fabrikant of de distributeur het herstellen, nadat het apparaat naar hem is opgestuurd. Uitzondering is een apparaat met een hardwarematige RESET-knop: door de knop 10 seconden ingedrukt te houden worden de fabrieksinstellingen zonder wachtwoord hersteld.

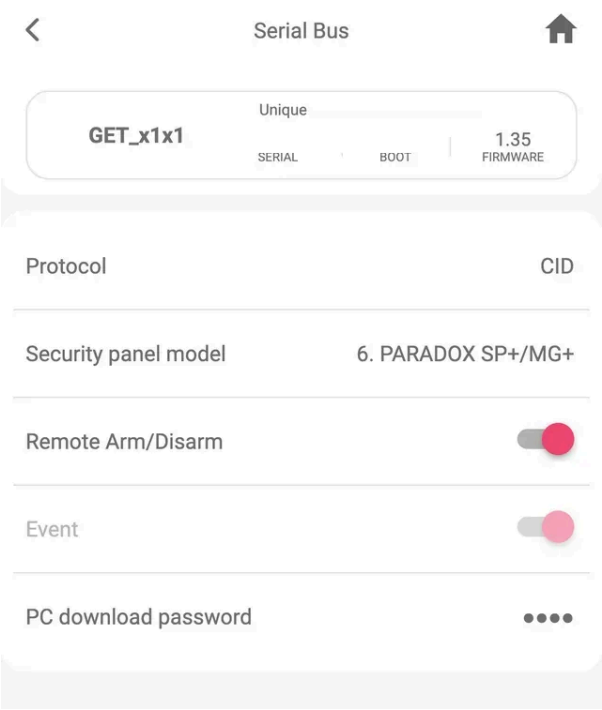
Aanmelden als installateur in de app. Als u de communicatiemodule met de installateurscode opent, verbergt Protegus 2 de velden **Administrator code** en **Only an administrator can restore**, en toont hij de instellingen die de beheerder niet heeft vrijgegeven alleen als leesbaar. In de app geldt het recht **SIM card** ook voor de LAN-instellingen; waar de identificaties bij de CMS-instellingen staan (zie hierboven), geldt daarvoor het recht **CMS reporting**.

6.3 Panel settings

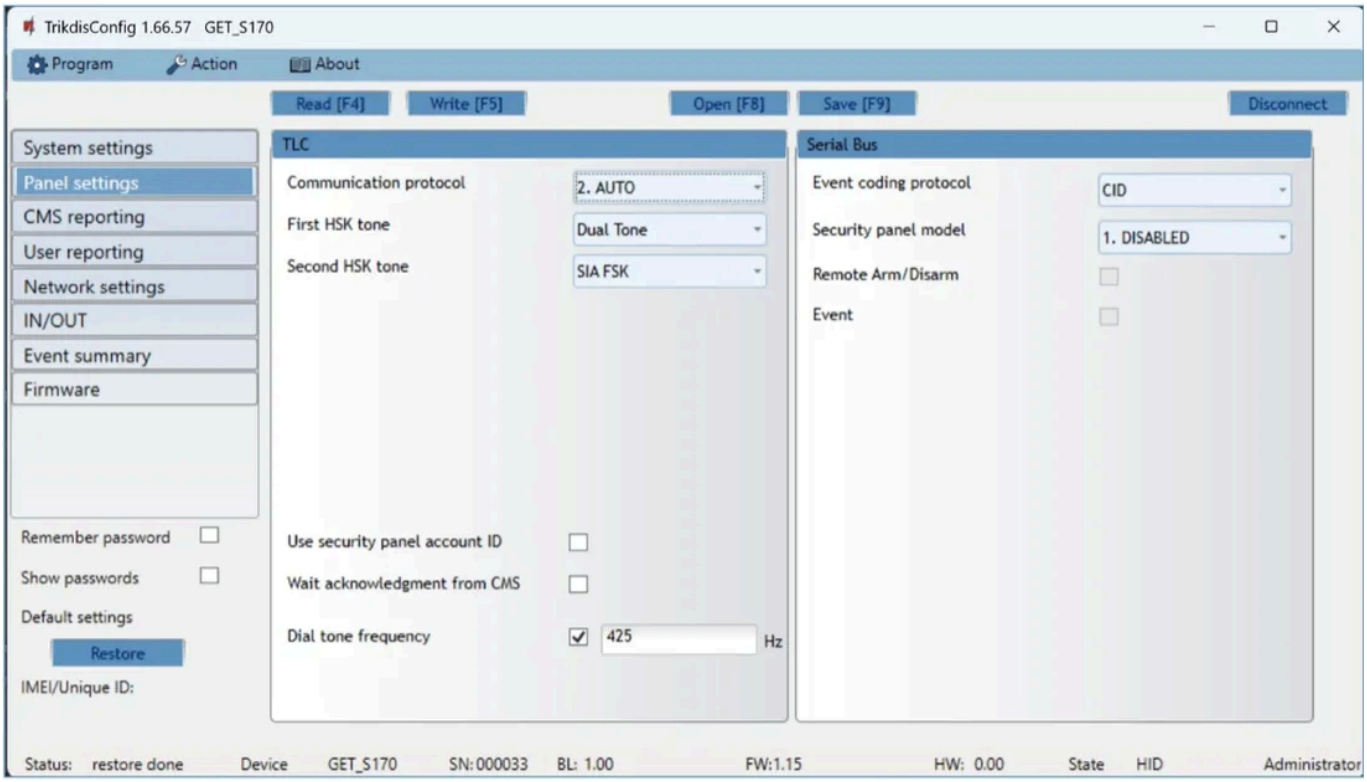
Op deze pagina geeft u aan hoe de communicatiemodule op de alarmcentrale is aangesloten: de groep **TLC** (in de app **TLF**) bevat de instellingen voor aansluiting op de telefoonlijn (TIP/RING), de groep **Serial bus** (**Serial Bus**) die voor aansluiting op de databus of seriële poort. In de app: **Advanced settings** → **Panel settings** → **TLF**, resp. **Panel settings** → **Serial Bus**.



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



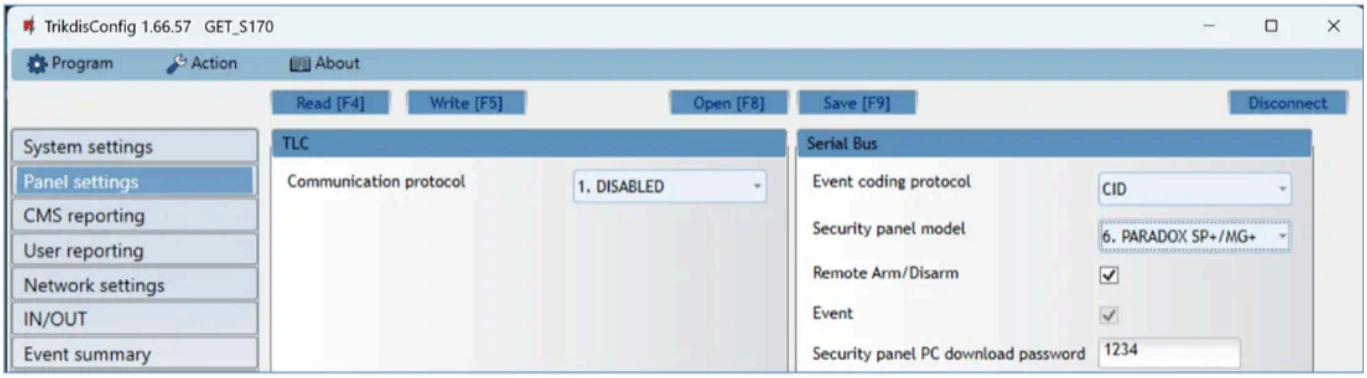
Afbeelding 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm ingeschakeld, Event (alleen leesbaar), PC download password.



Afbeelding 50. TrikdisConfig – Panel settings bij aansluiting op TIP/RING: in de groep TLC Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; de groep Serial bus is dan grijs.

Groep TLC – als de communicatiemodule op de TIP/RING-klemmen van de telefoonkiezer van de centrale is aangesloten:

- **Communication protocol** (Security panel model) – het inschakelen (**2. AUTO**) of uitschakelen (**1. DISABLED**) van de DTMF-telefoonlijninterface van de communicatiemodule. Kies bij aansluiting op TIP/RING de waarde AUTO.
- **First HSK tone**, **Second HSK tone** – de handshaketoon van de centrale, waarmee de communicatiemodule de kiezer van de centrale ontvangt (op de afbeelding Dual Tone en SIA FSK).
- **Use security panel account ID** – aangevinkt stuurt de communicatiemodule niet de waarde van zijn eigen veld **Object ID**, maar het objectnummer dat in de centrale is ingesteld en door de centrale wordt verstuurd.
- **Wait acknowledgment from CMS** – aangevinkt wacht de communicatiemodule na het verzenden van elke gebeurtenis op de bevestiging van de IP-ontvanger dat het bericht is aangekomen; als de bevestiging niet komt, geeft hij de centrale geen „kiss-off"-signaal, en herhaalt de telefoonkiezer van de centrale het bericht.
- **Dial tone frequency** – de frequentie van de kiestoon waarmee de communicatiemodule met de kiezer van de centrale communiceert (standaard 425 Hz, de gangbare Europese kiestoon). Op het tabblad TLF van de app staat daarnaast de schakelaar **Dial tone enabled**: die schakelt de kiestoon in of uit; de frequentie kan alleen bij ingeschakelde kiestoon worden gewijzigd.



Afbeelding 51. TrikdisConfig – Panel settings bij aansluiting op databus of seriële poort: Communication protocol 1. DISABLED; in de groep Serial bus Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm en Event aangevinkt, Security panel PC download password ingevuld.

Groep Serial bus – als de communicatiemodule op de databus of seriële poort van de centrale is aangesloten:

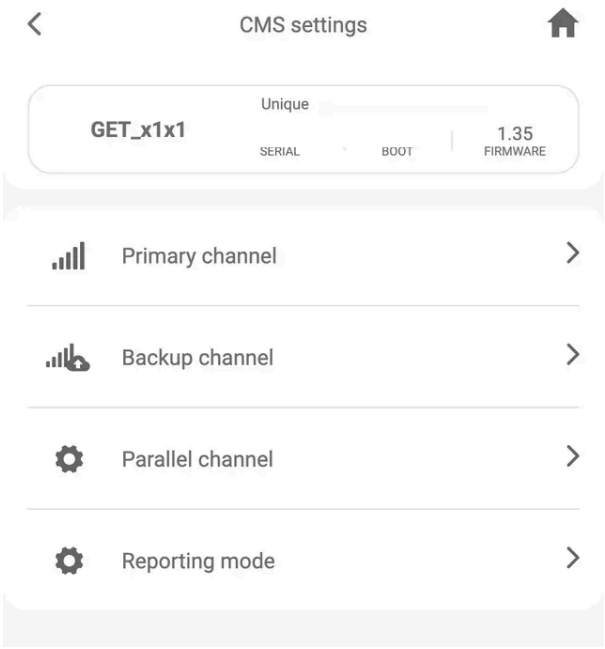
- **Event coding protocol** (Protocol) – het protocol voor de gebeurtenismelding: **CID** of **SIA**.
- **Security panel model** – het type van de aangesloten alarmcentrale uit de lijst (kies voor de aansluiting Keybus + TIP/RING van Paradox SP / SP+ / MG / MG+ het item **Paradox SP+/MG+ series KeyBus**, paragraaf 3.3.3).
- **Remote Arm/Disarm** – aangevinkt bestuurt de communicatiemodule de centrale rechtstreeks (in- en uitschakelen vanuit Protegus 2). Alleen zichtbaar bij de direct bestuurbare centrales. Voor directe besturing moet ook de centrale volgens paragraaf 4.1 worden ingesteld.
- **Event** – aangevinkt stuurt de communicatiemodule de gebeurtenissen van de centrale naar de meldkamer en naar Protegus 2. De app toont deze schakelaar, maar daar kan hij niet worden gewijzigd.
- **Security panel PC download password** (PC download password; bij Texecom de UDL passcode) – voor directe besturing van een Paradox- of Texecom-centrale het PC- resp. UDL-wachtwoord; het moet overeenkomen met het wachtwoord dat in de centrale is ingesteld en waarvan het invoeren in paragraaf 4.1 staat beschreven.

6.4 CMS reporting (Reporting to CMS)

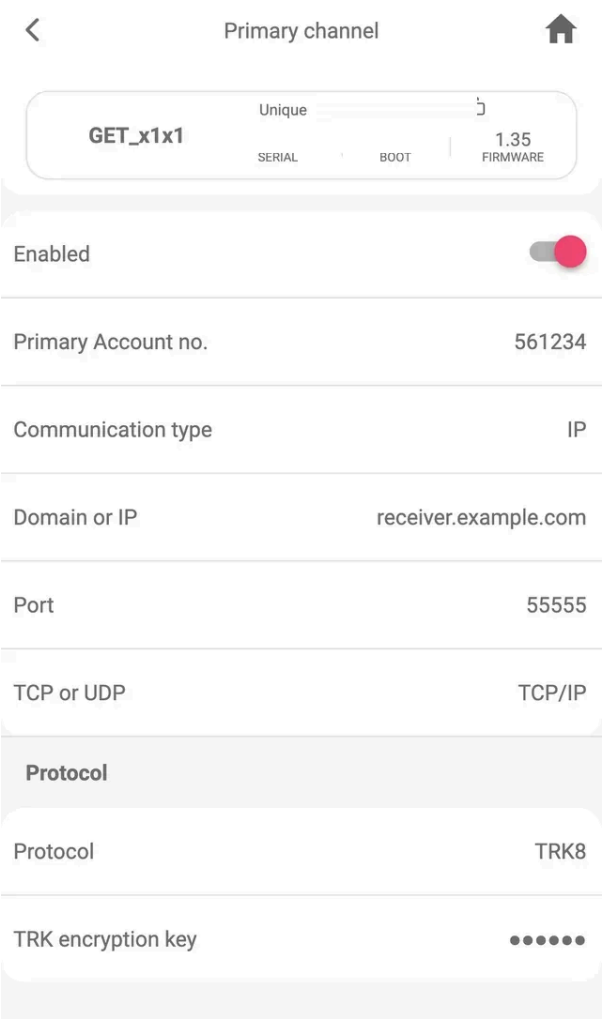
De communicatiemodule stuurt de gebeurtenissen via een IP-verbinding naar de meldkamer – via het bekabelde netwerk (LAN) of via het mobiele netwerk (SIM1, SIM2), in de volgorde die in paragraaf 6.4.2 is ingesteld. De gebeurtenissen kunnen ook via meerdere kanalen gaan: het **primaire** en het **parallelle** kanaal werken tegelijk (naar twee ontvangers tegelijk), en bij elk hoort een **reservekanaal**, dat in werking treedt als het betreffende kanaal uitvalt. De communicatie is versleuteld en met een wachtwoord beveiligd. Voor de TRK-protocollen is een Trikdis-ontvanger nodig, die de gebeurtenissen ontvangt en doorgeeft aan de meldkamersoftware: voor een IP-verbinding de softwareontvanger IPcom (Windows of Linux), de IP/sms-ontvanger RL14 of de meerkanaalsontvanger RM14; de protocollen DC-09 en TL150 zijn bedoeld voor de universele resp. de SUR-GARD-ontvangers (zie hieronder, **Protocol**).

6.4.1 Ontvangerkanalen (CMS settings)

In de app: Advanced settings → Reporting to CMS → CMS settings, daarna **Primary channel**, **Backup channel** of **Parallel channel** (daarbinnen **Parallel primary channel** en **Parallel backup channel**). Door de schakelaar **Enabled** in te schakelen verschijnen de instellingen van het kanaal.

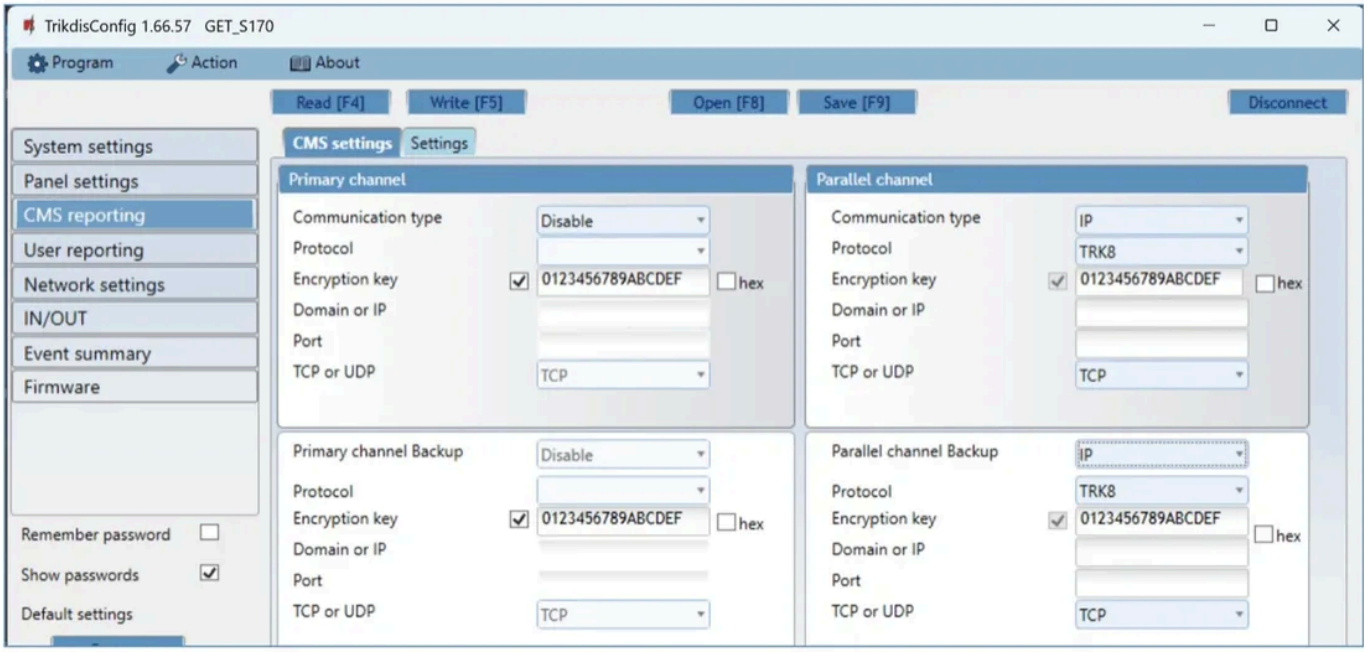


Afbeelding 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel en Reporting mode.



Afbeelding 53. Protegus 2 – Primary channel op hardware x1x1: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 en de TRK encryption key.

In TrikdisConfig: het tabblad **CMS settings** van de pagina **CMS reporting**.



Afbeelding 54. TrikdisConfig – CMS reporting, tabblad CMS settings: primair kanaal en zijn reserve, parallel kanaal en zijn reserve (op de afbeelding het parallelle kanaal met de instelling IP / TRK8 / TCP).

Primary channel – primair kanaal

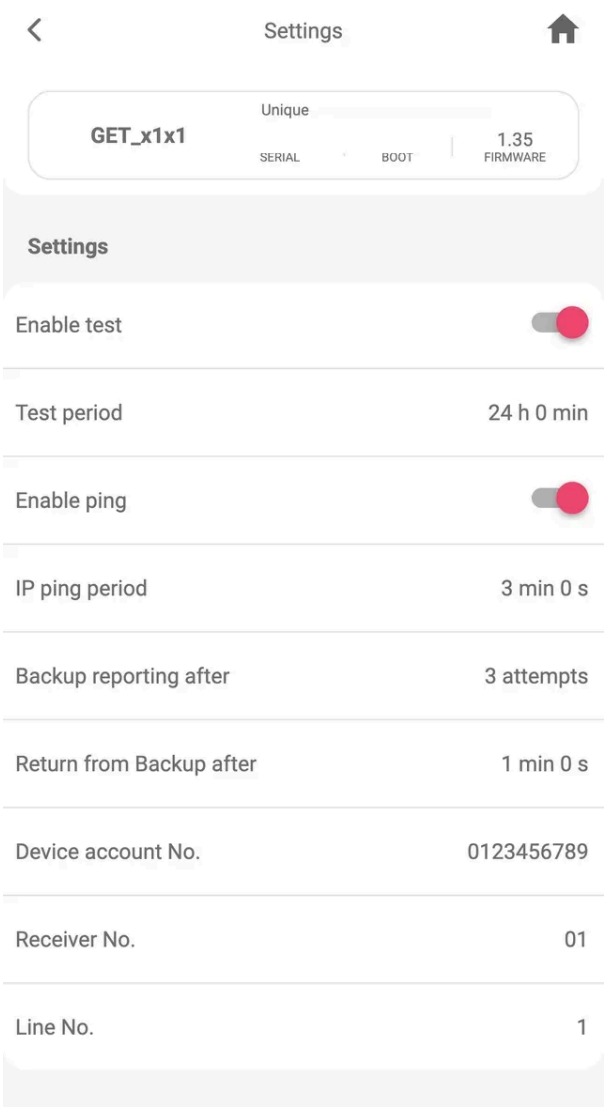
- **Communication type** – de verbindingswijze met de ontvanger: **IP**.
- **Protocol** – **TRK8** (Trikdis-ontvangers), **DC-09_2007** of **DC-09_2012** (universele ontvangers), **TL150** (SUR-GARD-ontvangers).
- **Encryption key** (TRK encryption key; bij de DC-09-protocollen **Enable encryption key** en **DC-09 encryption key**, met de schakelaar **HEX** voor een hexadecimale sleutel) – de versleutelingssleutel van de berichten; die moet in de communicatiemodule en in de ontvanger dezelfde zijn. In de app is de TRK encryption key maximaal 6 tekens, de DC-09 encryption key maximaal 16 tekens (in HEX 32).
- **Domain or IP**, **Port** – de domeinnaam of het IP-adres en de netwerkpoort van de ontvanger.
- **TCP or UDP** – het transmissieprotocol.

Primary channel Backup – reservekanaal. Ingeschakeld neemt het de communicatie over als het primaire kanaal niet werkt; de instellingen zijn gelijk aan de bovenstaande.

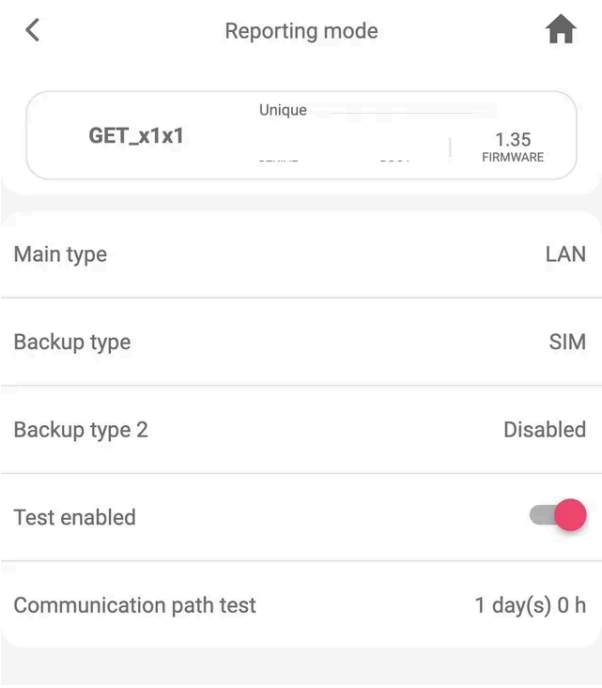
Parallel channel – parallel kanaal. Stuurt naast het primaire kanaal tegelijk naar een tweede ontvanger (bijvoorbeeld naar de lokale en de centrale meldkamer). De instellingen zijn dezelfde als die van het primaire kanaal.

6.4.2 Test, PING en de volgorde van de verbindingen

In de app: Advanced settings → Reporting to CMS → Settings (test, PING, de tijden van het reservekanaal, ontvanger- en lijnnummer) en **Reporting to CMS → CMS settings → Reporting mode** (de volgorde van de verbindingsroutes). In de app staat naast elk interval een schakelaar: **Enable test** voor de Test period, **Enable ping** voor de IP ping period en **Test enabled** voor de Communication path test; op het tabblad Reporting mode heten de verbindingstypes **LAN**, **SIM** (de SIM1) en **SIM2**.

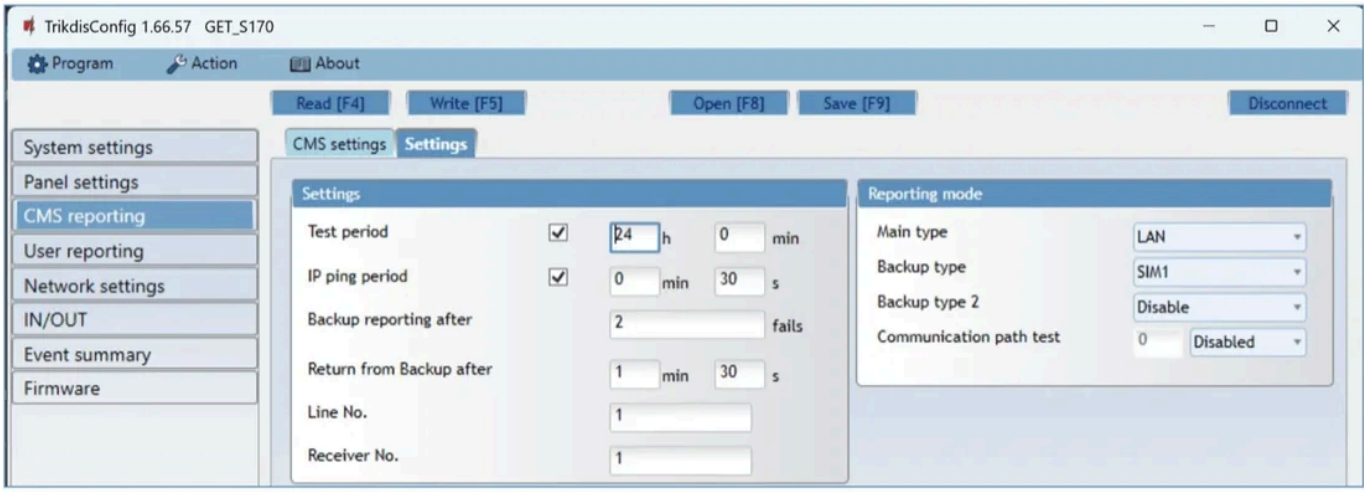


Afbeelding 55. Protegus 2 – Reporting to CMS → Settings op hardware x1x1: Enable test en Test period, Enable ping en IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.



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

In TrikdisConfig: het tabblad **Settings** van de pagina **CMS reporting**.



Afbeelding 57. TrikdisConfig – CMS reporting, tabblad Settings: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; in de groep Reporting mode Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **Test period** – het interval van het periodieke testrapport (standaard 24 uur). Het testrapport gaat als Contact ID-bericht naar de meldkamer en naar Protegus 2.
- **IP ping period** – het interval van het levenssignaal (PING) op het IP-kanaal (standaard 30 s). U schakelt het in met het vinkje en geeft de tijd op in de velden voor minuten (**min**) en seconden (**s**); het is nodig voor de bewaking van de verbinding. De ontvanger stuurt de PING-berichten niet door naar de meldkamersoftware, om die niet te overbelasten; de software krijgt pas een bericht als de ontvanger gedurende driemaal de ingestelde tijd geen PING ontvangt. Is de PING-periode bijvoorbeeld 3 minuten, dan wordt het verbindingsverlies na de 9e minuut gemeld.
- **Backup reporting after** – na dit aantal mislukte verzendpogingen schakelt het apparaat over naar het reservekanaal (standaard 2).

- **Return from Backup after** – na deze tijd keert het apparaat terug naar het primaire kanaal (standaard 1 minuut 30 s).

De PING houdt de actieve verbinding tussen het apparaat en de ontvanger in stand, en daar hangen ook toegang, bediening en programmering op afstand van af. Daarom **raden wij een PING-periode van meer dan 5 minuten af**.

DC-09 Settings (rechts op het tabblad) – hoeft u alleen in te vullen als u op een van de kanalen met het protocol DC-09_2007 of DC-09_2012 verzendt; de groep verschijnt wanneer in het veld **Protocol** van een kanaal DC-09_2007 of DC-09_2012 is geselecteerd:

- **Object ID in DC-09** – hexadecimale identificatie van 3–16 tekens, verstrekt door de meldkamer.
- **DC-09 line No** – het lijnnummer.
- **DC-09 receiver No.** – het ontvangernummer.

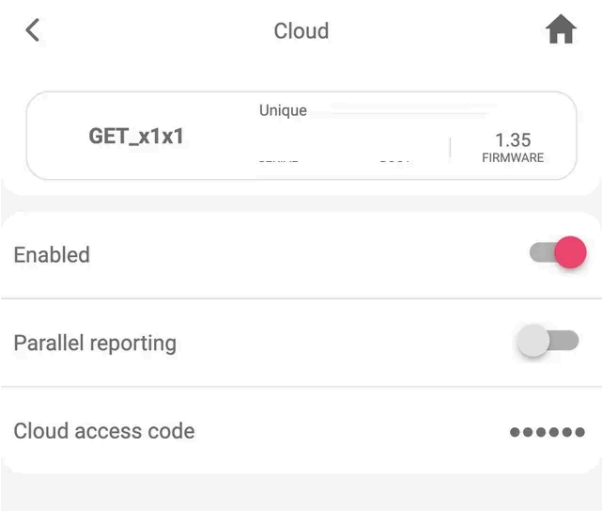
Op het tabblad Settings van de GET staan hier ook de velden **Line No.** (het lijnnummer van de ontvanger) en **Receiver No.** (ontvangernummer); een apart veld „Object ID in DC-09" is er op de GET niet.

Groep Reporting mode – hier geeft u aan via welke route de communicatiemodule met de meldkamerkanalen en met Protegus 2 communiceert. U geeft de verbindingstypes op in volgorde: als de verbinding volgens **Main type** niet tot stand komt, schakelt de communicatiemodule over naar die volgens **Backup type**, enzovoort; als het bericht via de reserveroute kon worden verzonden, probeert hij na de ingestelde tijd (Return from backup after) opnieuw de hoofdroute.

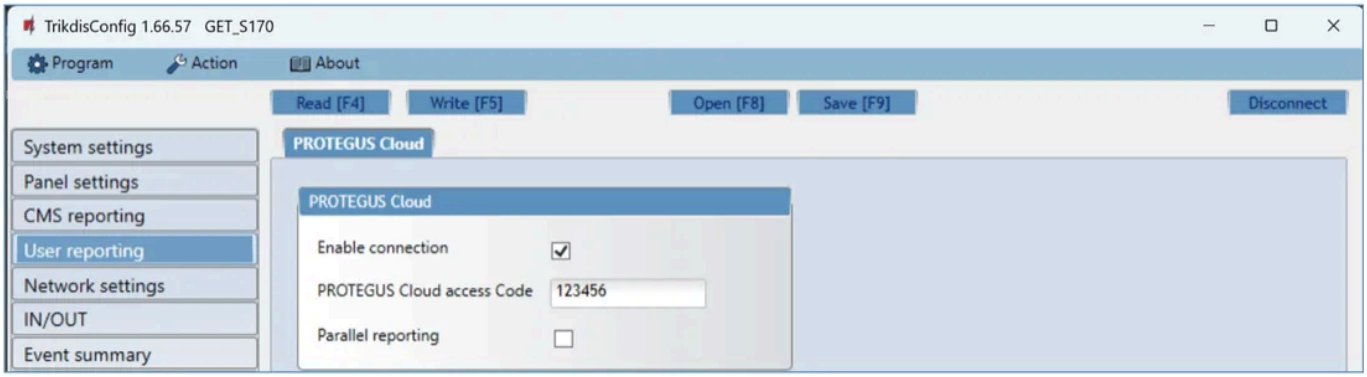
- **Main type** – het type van de hoofdverbinding met de ontvanger en met Protegus 2: **LAN**, **SIM1** of **SIM2**.
- **Backup type** – het type van de reserveverbinding (LAN, SIM1, SIM2).
- **Backup type 2** – het type van de tweede reserveverbinding (LAN, SIM1, SIM2).
- **Communication path test** – met welk interval de communicatiemodule de gekozen verbindingstypes (LAN, SIM1, SIM2) uitprobeert.

6.5 User reporting (Protegus Cloud)

Met de Protegus 2-dienst bewaakt en bestuurt de gebruiker de communicatiemodule en het daarop aangesloten systeem op afstand; details: web.protegus.app. In de app: **Advanced settings** → **User reporting** → **Cloud**; in TrikdisConfig het tabblad **PROTEGUS Cloud** van de pagina **User reporting**.



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



Afbeelding 59. TrikdisConfig – User reporting, tabblad PROTEGUS Cloud: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – schakelt de Protegus 2-dienst in: het apparaat wisselt gegevens uit met de Protegus 2-app, en TrikdisConfig kan het ook op afstand bereiken.
- **PROTEGUS Cloud access Code** (Cloud access code) – 6-cijferige code om verbinding te maken met Protegus 2 (af fabriek `123456`). Als u die in TrikdisConfig wijzigt, moet hij ook in de Protegus 2-app worden aangepast.
- **Parallel reporting** (in de app alleen zichtbaar als de firmware het ondersteunt) – aangevinkt gaan de berichten tegelijk via het primaire kanaal (naar de meldkamer) en naar Protegus 2; Protegus 2 en de gebruikers krijgen het bericht pas nadat het naar de meldkamer is verzonden.

6.6 Network settings

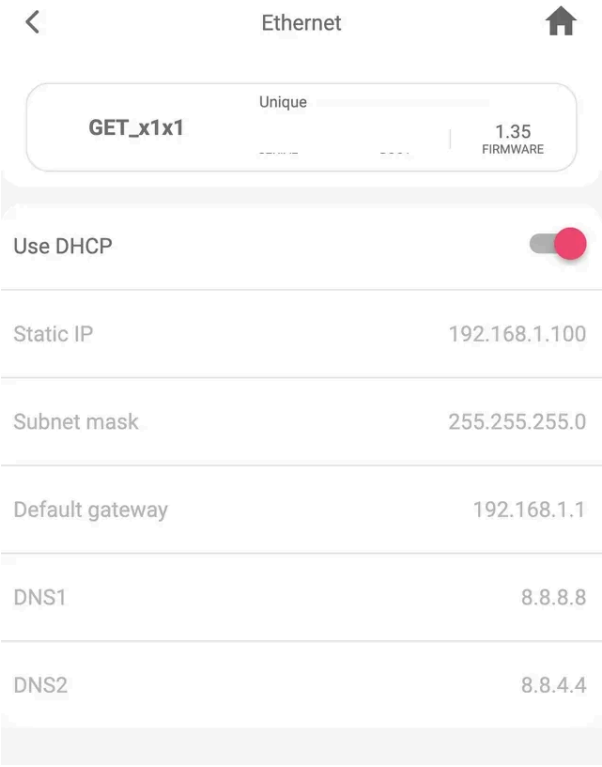
6.6.1 LAN (Ethernet)

Deze instellingen moeten worden opgegeven als de communicatiemodule op het bekabelde lokale netwerk (LAN) is aangesloten. In de app: **Advanced settings** → **Network settings** → **LAN**; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** en **DNS2** kunnen alleen worden gewijzigd als **Use DHCP** is uitgeschakeld. In TrikdisConfig het tabblad **LAN** van de pagina **Network settings**, groep **Ethernet settings**.

Wat moet het netwerk kunnen? De communicatiemodule zet zelf de uitgaande verbinding op naar de meldkamerontvanger en de Protegus-cloud. Daarom hoeft u op de router **geen poort te openen of door te sturen**, en is er ook geen vast openbaar IP-adres of dynamische DNS nodig. Wat wel nodig is:

- een vrije Ethernet-poort op de router of switch;
- DHCP (fabrieksinstelling), of een vast IP-adres, subnetmasker, gateway en DNS die u van de netwerkbeheerder krijgt;
- toestemming voor uitgaand verkeer naar het adres en de poort van de ontvanger (TCP of UDP, afhankelijk van de instelling van de ontvanger), en naar de Protegus-cloud.

Stem dit bij een gefilterd netwerk – van een bedrijf of instelling – vooraf af met de netwerkbeheerder: op thuisrouters zijn standaard alle uitgaande verbindingen toegestaan, maar op een netwerk dat door een firewall wordt beschermd kan een aparte regel nodig zijn.



Afbeelding 60. Protegus 2 – Network settings → LAN: Use DHCP ingeschakeld; de velden Static IP, Subnet mask, Default gateway, DNS1 en DNS2 zijn dan grijs.



Afbeelding 61. TrikdisConfig – Network settings, tabblad LAN, groep Ethernet settings: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

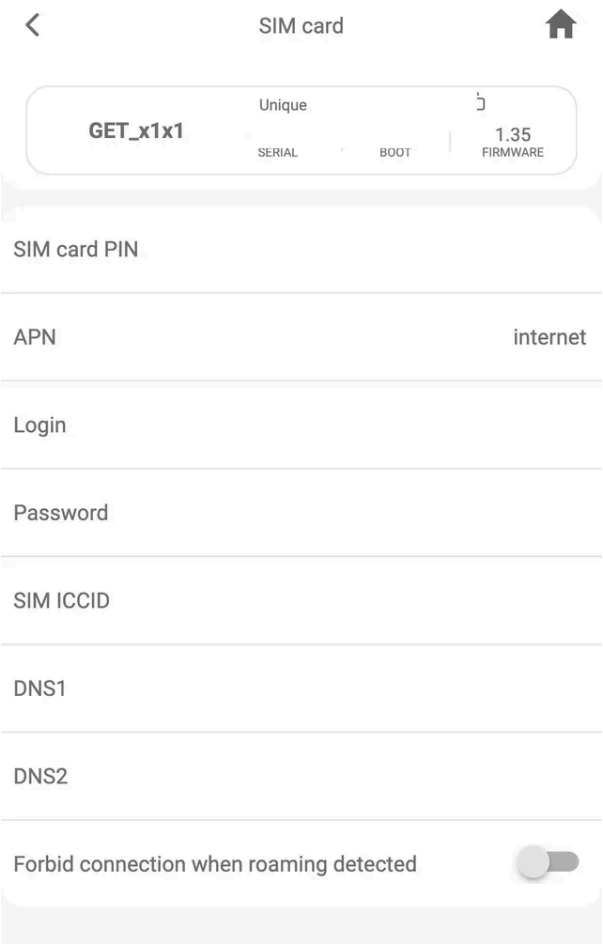
- **Use DHCP** – aangevinkt meldt de communicatiemodule zich automatisch aan op het netwerk (hij krijgt een adres van de DHCP-server van de router). Als het automatisch aanmelden niet lukt, moeten de adressen handmatig worden ingevoerd:
- **Static IP** – het vaste IP-adres van de communicatiemodule bij handmatige instelling.
- **Subnet mask** – subnetmasker bij handmatige instelling.
- **Default gateway** – het adres van de gateway (router) bij handmatige instelling.
- **DNS1, DNS2** – naamservers (DNS, Domain Name System: geeft het IP-adres bij een domeinnaam); die zijn nodig als u de ontvanger in het veld **Domain or IP** van het kanaal met een domeinnaam en niet met een IP-adres hebt opgegeven. Standaard de openbare DNS van Google. Controleer, ongeacht de IP-instellingen, of de DNS-adressen bij uw internetprovider werken.

6.6.2 SIM1 en SIM2

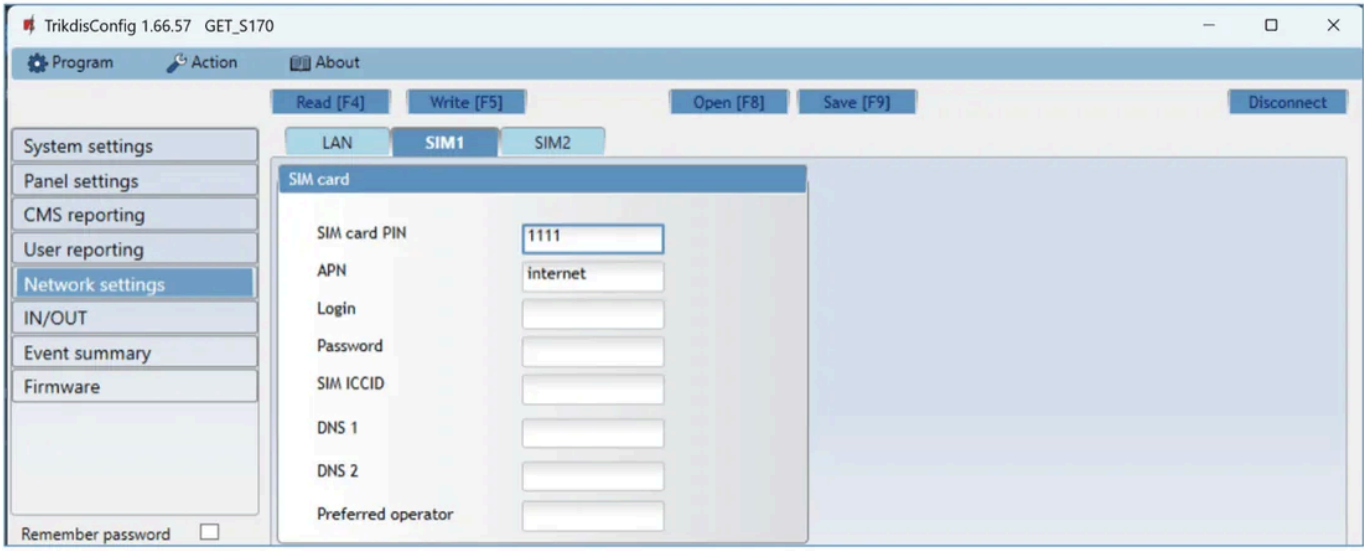
Deze instellingen moeten voor elke geplaatste simkaart apart worden opgegeven; de instellingen van de SIM1- en de SIM2-houder zijn gelijk.

Controleer vóór gebruik of de simkaart actief is en werkt, en of op de kaart ook de mobiele datadienst is ingeschakeld.

In de app: **Advanced settings** → **Network settings** → **SIM** (de SIM1) of **SIM2**. In TrikdisConfig het tabblad **SIM1** resp. **SIM2** van de pagina **Network settings**, groep **SIM card**.



Afbeelding 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 en de schakelaar Forbid connection when roaming detected.



Afbeelding 63. TrikdisConfig – Network settings, tabblad SIM1, groep SIM card: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (het tabblad SIM2 is hetzelfde).

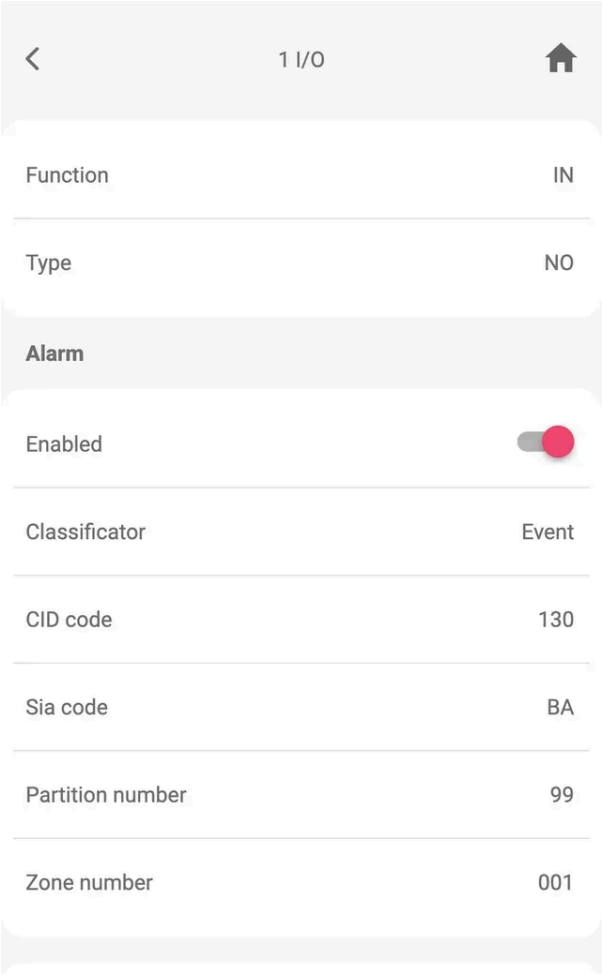
- **SIM card PIN** – de pincode van de kaart. De pincodevraag kunt u uitschakelen door de kaart in een mobiele telefoon te plaatsen en hem daar uit te schakelen; dan kan de fabriekswaarde van het veld blijven staan.
- **APN** – het toegangspunt van de provider (Access Point Name); zonder APN maakt het apparaat geen verbinding met het internet. De waarde vindt u op de website van de provider van de simkaart; `internet` is algemeen geldig en werkt in het netwerk van veel providers. De bekende APN's van de providers staan in het APN-artikel (voor een IoT- / M2M-kaart geeft de provider een aparte APN, zie paragraaf 2.3).
- **Login, Password** – gebruikersnaam en wachtwoord voor de internetverbinding, als de provider daarom vraagt.
- **SIM ICCID** – het ICCID-nummer van de simkaart, als u wilt dat het apparaat alleen met deze kaart werkt.
- **DNS1, DNS2** – naamservers; die zijn nodig als u de ontvanger in het veld **Domain or IP** van het kanaal met een domeinnaam hebt opgegeven. Standaard de openbare DNS van Google; controleer of de DNS-adressen bij uw provider werken.
- **Preferred operator** – de code van de mobiele provider (MCC + MNC); als u die opgeeft, maakt het apparaat alleen verbinding met het netwerk van de gekozen provider. Staat **alleen in TrikdisConfig**.

Op het tabblad SIM van de app staat in plaats van Preferred operator de schakelaar **Forbid connection when roaming detected**: ingeschakeld maakt de communicatiemodule geen verbinding als hij roaming detecteert. Op hardwareversie **M15**, met firmware **1.17** of nieuwer, verschijnen op het tabblad SIM ook de instellingen **Generation** en **Bands**: daarmee kunt u beperken welke mobiele netwerktechnologie en welke frequentiebanden de communicatiemodule gebruikt.

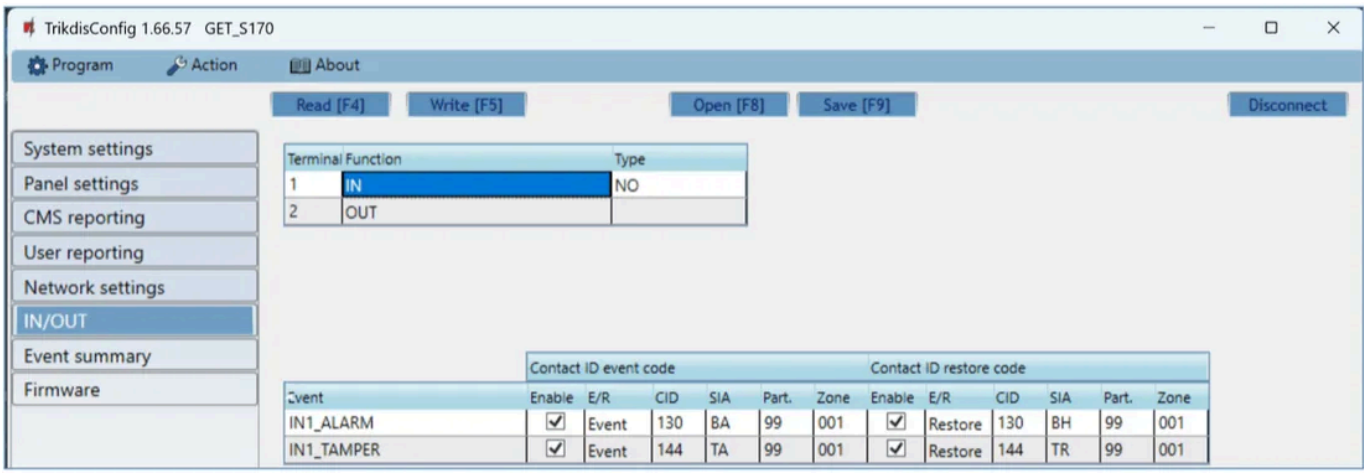
6.7 IN/OUT

Hier geeft u de rol van de twee I/O-klemmen met dubbele functie van de communicatiemodule op: **Disabled** (niet gebruikt), **IN** (ingang) of **OUT** (uitgang; op de GET is dat de fabrieksinstelling). Bij een ingang moet in het veld **Type** ook het type van de aangesloten kring worden opgegeven (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Op de ingangen kunnen extra detectoren worden aangesloten: bij het activeren van de detector stuurt de communicatiemodule een eigen gebeurtenis met de aan de ingang toegewezen Contact ID-code (SIA-code) naar de meldkamer en naar Protegus 2.

In de app: **Advanced settings** → **IN/OUT**, daarna klem **1** of **2**: de **Function** (Disabled, IN, OUT) en bij een ingang de **Type**; in de delen **Alarm** en **Tamper** de gebeurtenis- en herstelberichten die bij het activeren van de ingang worden verstuurd. In TrikdisConfig de pagina **IN/OUT**.



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



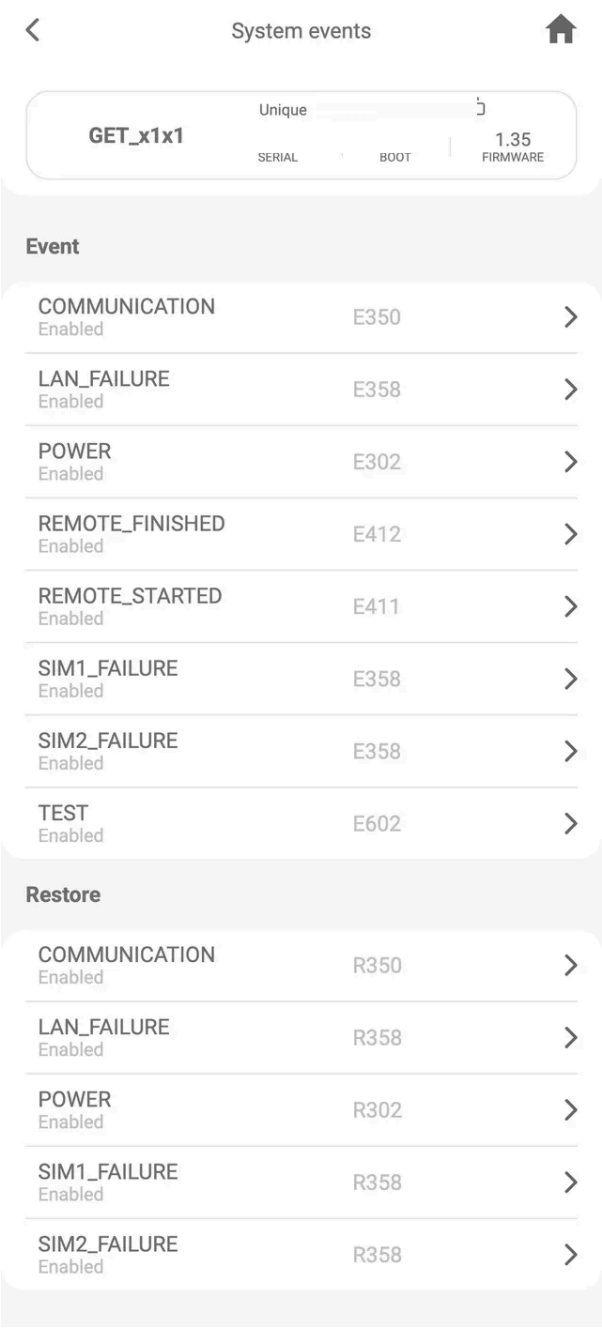
Afbeelding 65. TrikdisConfig – pagina IN/OUT: klem 1 is ingang (IN, NO), klem 2 uitgang (OUT); daaronder de alarm- en sabotagegebeurtenissen van ingang 1 met CID- en SIA-code.

Bij het activeren van de detector op de ingang stuurt de communicatiemodule een alarm (**INx_ALARM**, Contact ID 130, SIA BA; herstel BH), bij het activeren van de sabotagekring een sabotagegebeurtenis (**INx_TAMPER**, 144, SIA TA; herstel TR); in de tabel verschijnen de gebeurtenissen van elke klem die als ingang is ingesteld. De kolommen van de tabel:

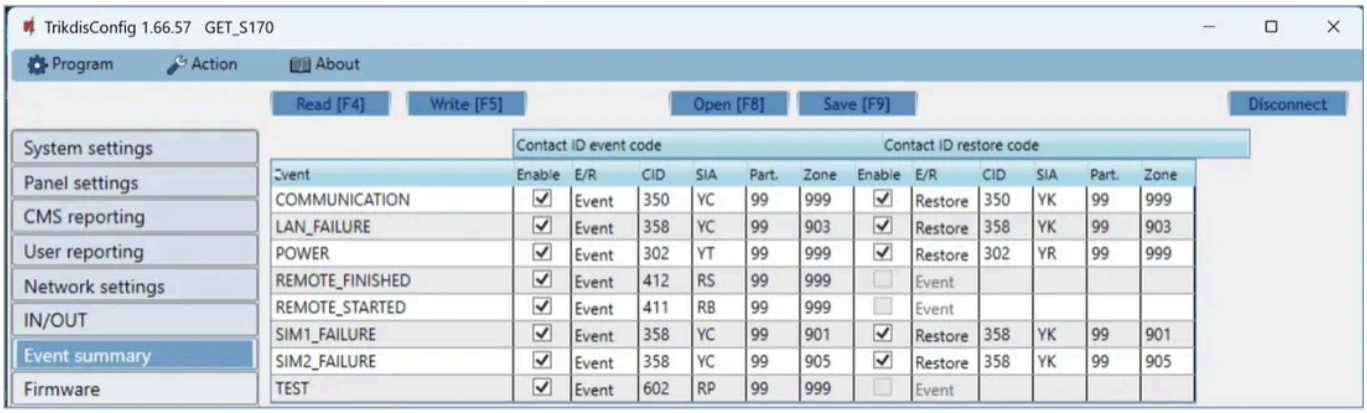
- **Enable** (Enabled) – schakelt het verzenden van het bericht naar de meldkamer en naar Protegus 2 in.
- **E/R** (Classificator) – het type bericht: Event (gebeurtenis) of Restore (herstel).
- **CID** (CID code) – de Contact ID-code (kan worden gewijzigd, of de fabriekswaarde kan blijven staan); bij het activeren van de ingang gaat het bericht met deze code naar Protegus 2 en naar de meldkamer.
- **SIA** (Sia code) – de SIA-code (kan worden gewijzigd, of de fabriekswaarde kan blijven staan).
- **Part.** (Partition number) – het partitienummer in het bericht (zowel bij de gebeurtenis als bij het herstel).
- **Zone** (Zone number) – het zonenummer in het bericht.

6.8 Event summary (System events)

Hier kunt u de eigen, interne berichten van het apparaat inschakelen, uitschakelen en wijzigen. Een bericht dat hier is uitgeschakeld, wordt niet verzonden, ongeacht welke andere instelling ook. In de app: **Advanced settings** → **System events**, de berichten staan in de lijsten **Event** en **Restore**; kies het bericht om het te wijzigen. In TrikdisConfig de pagina **Event summary**.



Afbeelding 66. Protegus 2 – System events: de lijst Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) en de lijst Restore.



Afbeelding 67. TrikdisConfig – pagina Event summary: de interne berichten van het apparaat met CID- en SIA-code, met partitie 99.

De interne berichten van de GET (tussen haakjes de standaard Contact ID-code en zone):

- **COMMUNICATION** (350, zone 999) – storing in de verbinding tussen de centrale en de communicatiemodule; het herstel is een apart bericht.
- **LAN_FAILURE** (358, zone 903) – storing in de bekabelde netwerkverbinding (LAN); het herstel is een apart bericht.
- **POWER** (302, zone 999) – lage voedingsspanning; het herstel is een apart bericht.
- **REMOTE_FINISHED** (412) – einde van het programmeren op afstand met TrikdisConfig (verbinding verbroken).
- **REMOTE_STARTED** (411) – verbinding op afstand om de GET met TrikdisConfig te programmeren.
- **SIM1_FAILURE** (358, zone 901) – storing in de mobiele netwerkverbinding op SIM1; het herstel is een apart bericht.
- **SIM2_FAILURE** (358, zone 905) – storing in de mobiele netwerkverbinding op SIM2; het herstel is een apart bericht.
- **TEST** (602) – periodieke testmelding.

Het inschakelen en het interval van het periodieke TEST-bericht stelt u in het veld **Test period** in (paragraaf 6.4.2).

- **Enable** (Enabled) – aangevinkt is het verzenden van het bericht ingeschakeld.
- Bij elk bericht kunnen de Contact ID-code (SIA-code) en het zone- en partitienummer worden gewijzigd.

6.9 Fabrieksinstellingen herstellen

Vanuit de Protegus 2-app kunnen de fabrieksinstellingen **niet** worden hersteld: daarvoor is de knop **Restore** van TrikdisConfig of de knop **RESET** op het apparaat nodig.

Om de fabrieksinstellingen te herstellen, klikt u linksonder in het TrikdisConfig-venster, in de groep **Default settings**, op de knop **Restore**. Het herstellen wist alle instellingen – ook de wachtwoorden –, daarom is het verstandig de instellingen vooraf in een bestand op te slaan (**Save [F9]**).

Met het installateurswachtwoord is dit alleen mogelijk als de beheerder het niet heeft uitgeschakeld op de pagina **System settings** → **Access**.



Afbeelding 68. TrikdisConfig – de knop Restore in de groep Default settings.

De fabrieksinstellingen kunnen ook op het apparaat zelf worden hersteld, zonder computer: druk bij ingeschakelde voeding op de knop **RESET** op de printplaat (paragraaf 1.4) en houd die **10 seconden** ingedrukt, tot de leds NETWORK, POWER en TROUBLE uitgaan en daarna de POWER-led oplicht. Laat dan de knop los: de fabrieksinstellingen zijn hersteld.

7. Programmeren op afstand

TrikdisConfig bereikt de Trikdis-apparaten niet alleen via een USB-kabel, maar ook **op afstand, via de Protegus-cloud**. Zo kunt u de instellingen van een al gemonteerd apparaat wijzigen zonder ter plaatse te hoeven gaan.

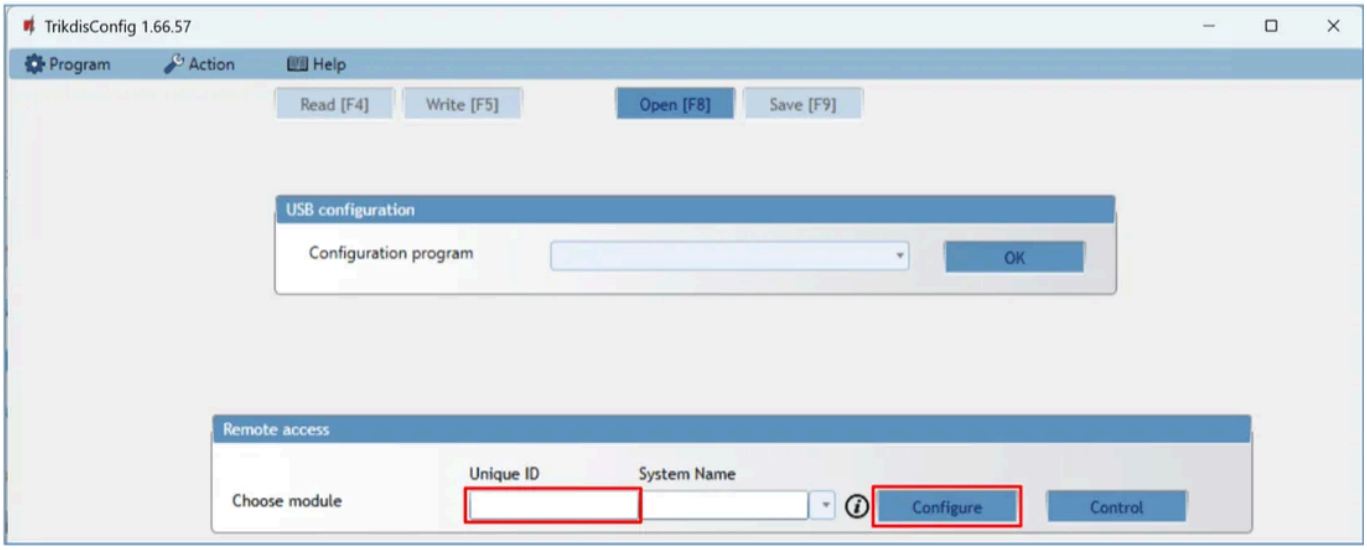
Voor toegang op afstand is nodig:

1. Het apparaat moet ingeschakeld zijn en een netwerkverbinding hebben (de **POWER**- en de **NETWORK**-led branden groen; bij een apparaat met mobiel netwerk knippert de NETWORK-led ook geel). Bij een apparaat met mobiel netwerk moet de geplaatste simkaart actief zijn en moet de pincode ervan in het apparaat zijn ingevoerd, of moet de pincodevraag zijn uitgeschakeld; bij een Ethernet-apparaat moet de netwerkkabel (LAN) zijn aangesloten en moet het apparaat het internet bereiken.
2. Op de pagina **User reporting** → **PROTEGUS Cloud** van TrikdisConfig moet **Enable connection** zijn aangevinkt (stel dit via USB in, bij de eerste inbedrijfstelling).
3. U moet de **unieke identificatie** van het apparaat kennen (IMEI of MAC – te lezen op de doos en op de achterkant van het apparaat) en het beheerders- of installateurswachtwoord.

Stappen:

1. Start de TrikdisConfig-software.
2. Voer in het onderdeel **Remote access**, in het veld **Unique ID**, de unieke identificatie van het apparaat in (IMEI of MAC).
3. Geef desgewenst het systeem een naam in het veld **System name** – het programma onthoudt die, en de volgende keer kunt u hem in de vervolgkeuzelijst kiezen.
4. Druk op de knop **Configure**.
5. Klik in het venster dat opent op de knop **Read [F4]** (lezen) en voer het wachtwoord in. Met het vinkje **Remember password** onthoudt het programma het voor deze sessie.
6. Voer de wijzigingen uit en stuur ze daarna met de knop **Write [F5]** (schrijven) naar het apparaat.

Systemen die eerder op afstand zijn geprogrammeerd en een naam hebben gekregen, slaat het programma op; met de pijl naast het veld **System name** kunt u ze weergeven. Om er een te verwijderen, selecteert u de identificatie in de lijst, drukt u op de toets **Delete** en bevestigt u.



Afbeelding 69. TrikdisConfig – de groep Remote access: het veld Unique ID, de lijst System name en de knop Configure.

De unieke identificatie van de GET is de **IMEI / Unique ID**; die staat op het label van het apparaat en op de sticker van de doos. Toegang op afstand werkt alleen als de simkaart actief is en de pincode ervan is ingevoerd of de pincodevraag is uitgeschakeld – **of** de communicatiemodule met een netwerkkabel (LAN) is aangesloten –; op het tabblad **User reporting** → **PROTEGUS Cloud** is **Enable connection** aangevinkt (paragraaf 6.5); de **POWER**-led brandt groen; de **NETWORK LTE**-led brandt groen en knippert geel (bij alleen een bekabelde verbinding brandt de **NETWORK LAN**-led groen). Het begin en het einde van het programmeren op afstand meldt de communicatiemodule met de berichten REMOTE_STARTED en REMOTE_FINISHED (paragraaf 6.8).

8. De werking van de communicatiemodule controleren

Controleer na het programmeren en aansluiten altijd de volledige keten: alarmcentrale → communicatiemodule → meldkamer en/of Protegus 2.

Controleer vooraf of er voeding is (de **POWER**-led brandt groen) en of er een netwerkverbinding is (de **NETWORK**-led brandt groen).

1. **Genereer een gebeurtenis.** Schakel het systeem in en weer uit op het bedieningspaneel, of verstoor een zone bij een ingeschakeld systeem, zodat er een alarm ontstaat.
2. **Controleer de ontvangst.** Kijk of de gebeurtenis is verschenen in de meldkamersoftware en/of in de gebeurtenissenlijst van de Protegus 2-app – met het juiste partitie- en zonenummer.
3. **Ingangen.** Activeer de detector die op een eigen ingang van de communicatiemodule is aangesloten, en controleer de bijbehorende gebeurtenis.
4. **Uitgangen.** Schakel de uitgang vanuit de Protegus 2-app en controleer of het aangesloten apparaat (relais, sleutelschakelaarzone) daadwerkelijk in werking treedt.
5. **Inschakelen op afstand.** Als de centrale op afstand bediend kan worden, schakel haar dan ook vanuit de Protegus 2-app in en uit.

Als de communicatiemodule zowel via het bekabelde netwerk als via het mobiele netwerk meldt (paragraaf 6.4.2, Reporting mode), is het de moeite waard de test via beide routes uit te voeren: trek de LAN-kabel los, veroorzaak een gebeurtenis, en controleer of die ook via de simkaart bij de meldkamer aankomt; steek daarna de kabel er weer in.

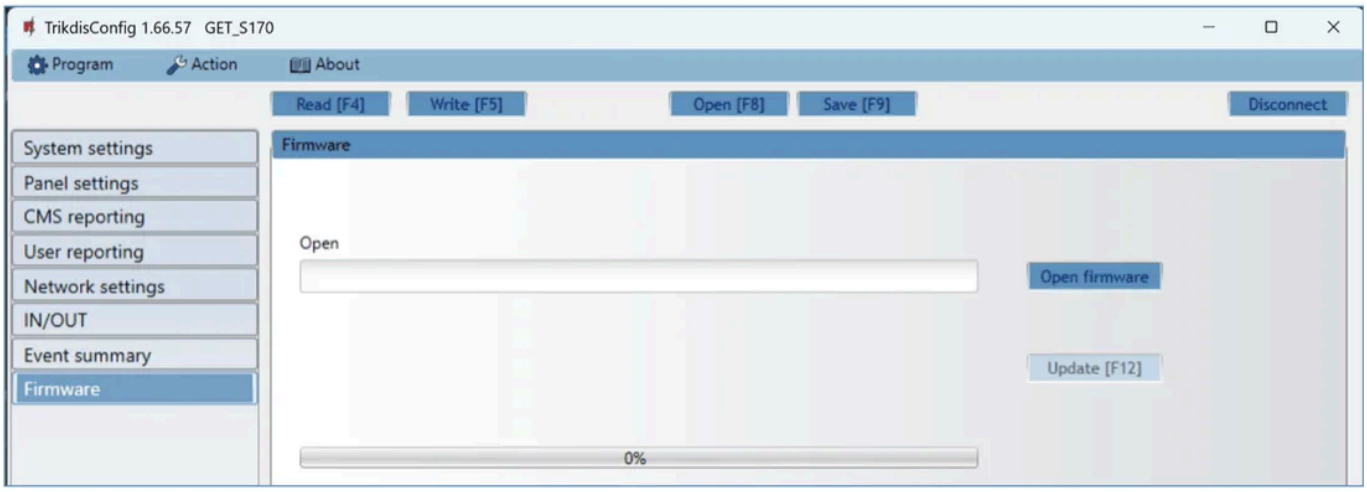
9. Firmware bijwerken

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

U kunt de firmware zelf bijwerken – naar een nieuwere en zo nodig ook naar een oudere versie. Na de update blijven alle instellingen van het apparaat ongewijzigd.

1. Start de TrikdisConfig-software en sluit het apparaat aan met een USB-kabel, of open de programmering ervan op afstand.
2. Als er nieuwere firmware is, biedt het programma aan deze te downloaden – accepteer dat.
3. Kies de pagina **Firmware** en klik op de knop **Open firmware**. Selecteer het firmwarebestand.
4. Druk op de knop **Update [F12]**, wacht tot de update is voltooid en klik daarna in het pop-upvenster op **OK**. Trek intussen de kabel niet los en onderbreek de verbinding niet.

De firmwarebestanden staan in de installatiemap van TrikdisConfig, in de submap **Firmwares**, in de map met de naam van het apparaat. Als er geen zo'n map is, is er ofwel geen update voor, ofwel moet de TrikdisConfig-software zelf worden bijgewerkt. De nieuwste bestanden kunt u als geregistreerde gebruiker ook downloaden van de website van de fabrikant, op de pagina van het apparaat.



Afbeelding 70. TrikdisConfig – pagina Firmware: de knop Open firmware, de knop Update [F12] en de voortgangsbalk.

Voor het bijwerken is een internetverbinding nodig. Een virusscanner, firewall of strenge instelling voor internettoegang kan het automatisch bijwerken van de firmware verhinderen; in dat geval moeten de instellingen van de virusscanner worden aangepast.

Voor sommige functies van de GET is een bepaalde firmwareversie nodig:

- **1.08** of nieuwer: instellen vanuit de Protegus 2-app (Advanced settings, paragraaf 2.2 en hoofdstuk 6);
- **1.17** of nieuwer, op hardwareversie **M15**: de instellingen **Generation** en **Bands** op het tabblad SIM van de app (paragraaf 6.6.2);
- **1.21** of nieuwer: de aansluiting Keybus + TIP/RING van Paradox SP / SP+ / MG / MG+ (paragraaf 3.3.3);
- **1.31** of nieuwer, op hardwareversie **x1x1**: de identificaties (Account No., Device account No.) staan in de app bij de CMS-instellingen (paragraaf 6.2).

10. Storingen zoeken en veelgestelde vragen

De meest voorkomende vragen en storingen, uitgaande van de ledsignalen. Als het antwoord naar het uitgebreide hoofdstuk verwijst, vindt u daar de precieze plaats van de instelling.

De NETWORK LTE-led brandt niet – geen mobiel netwerk

1. Kijk naar de knipperingen van de **TROUBLE**-led: 2 = storing van de SIM1-kaart, 3 = storing van de SIM2-kaart (paragraaf 1.6).
2. Controleer of de simkaart actief is, er een datadienst op zit, en of hij goed in de houder zit (SIM1 in het midden van de print, SIM2 aan de linkerrand; paragraaf 3.1).
3. Als de pincodevraag op de kaart is ingeschakeld, voer dan de pincode in op het tabblad **Network settings** → **SIM1** (of **SIM2**), of schakel de pincodevraag uit in een telefoon.
4. Controleer de APN (paragraaf 2.3): voor een IoT- / M2M-kaart geeft de provider een aparte APN.
5. Controleer de antenne: hij is vastgeschroefd, zit niet in een metalen behuizing, en de signaalsterkte is voldoende (de NETWORK LTE-led knippert minimaal 3 keer geel; paragraaf 1.6 en 3.2).
6. Als de communicatiemodule via het bekabelde netwerk meldt, legt het ontbreken van het mobiele netwerk hem op zich niet stil: volgens de volgorde in **Reporting mode** (paragraaf 6.4.2) stuurt hij via de volgende beschikbare route – maar zo ontbreekt de reserveroute, en het is de moeite waard dat in orde te brengen.

De NETWORK LAN-led brandt niet – geen bekabeld netwerk

1. 1 knippering van de **TROUBLE**-led wijst op een storing in de fysieke verbinding van het bekabelde netwerk: controleer de LAN-kabel aan beide uiteinden, en of de poort van de router of switch actief is (paragraaf 1.6).
2. Als de kabel in orde is, kijk dan op het tabblad **Network settings** → **LAN**: bij DHCP moet de router een adres geven; bij een vast adres moeten Static IP, Subnet mask en Default gateway bij het lokale netwerk passen (paragraaf 6.6.1).
3. Als u de ontvanger met een domeinnaam hebt opgegeven, moeten ook de DNS-adressen in het netwerk werken (DNS1, DNS2).

Er is netwerk, maar de meldkamer ontvangt geen gebeurtenissen

De DATA-led is de eenvoudigste internetcontrole. De DATA-led brandt wanneer er in het geheugen van het apparaat een bericht klaarstaat om te worden verzonden. Het groene licht van de NETWORK-led zegt alleen dat de netwerkverbinding tot stand is gekomen – bij een apparaat met mobiel netwerk heeft het zich aangemeld op het netwerk van de provider, bij een Ethernet-apparaat werkt de verbinding tot aan de router –, maar niet dat het apparaat ook het internet bereikt. Als de NETWORK-led groen is, maar de DATA-led ook na een gebeurtenis of testrapport continu blijft branden, werkt de internetverbinding niet: het bericht kan niet worden verzonden. Op een mobiel netwerk ligt de fout meestal bij de APN of de datadienst van de simkaart, bij Ethernet bij de router, de firewall of de DNS. Als de DATA-led uitgaat, is het bericht verzonden en is de dataverbinding in orde.

1. Controleer het adres, de poort, de TCP/UDP-instelling, het protocol en de versleutelingssleutel van de ontvanger (**CMS reporting** → **CMS settings**, paragraaf 6.4.1); de sleutel moet in de communicatiemodule en in de ontvanger dezelfde zijn.
2. Kijk naar de instelling van **Reporting mode** (paragraaf 6.4.2): **Main type** moet een route zijn die ter plaatse echt beschikbaar is (er is een LAN-kabel, resp. er zit een simkaart in de opgegeven houder), en er moet ook een reserveroute zijn.

3. Als de ontvanger met een domeinnaam is opgegeven, controleer dan de DNS-instelling op de route waarlangs de communicatiemodule meldt (**Network settings** → **LAN**, resp. **SIM1 / SIM2** → **DNS1, DNS2**).
4. Controleer op het mobiele netwerk of de databundel van de simkaart de benodigde poort niet blokkeert (sommige M2M-kaarten laten alleen bepaalde adressen toe); op het bekabelde netwerk moet de lokale firewall de poort van de ontvanger naar buiten toe doorlaten.
5. Als de centrale geen gebeurtenissen stuurt (de DATA-led gaat niet aan), ligt de oorzaak aan de kant van de centrale: zie het volgende punt.

De TROUBLE-led knippert 7 keer – geen verbinding met de centrale

1. Controleer bij aansluiting op de databus of seriële poort de CLK- en DATA-draad, en of in het veld **Panel settings** → **Security panel model** het type van de aangesloten centrale is gekozen (paragraaf 6.3).
2. Kijk bij een Paradox-centrale of de seriële poort niet vergrendeld is (paragraaf 4.1.2); bij een Texecom- en Paradox-centrale moet het **Security panel PC download password** overeenkomen met dat in de centrale.
3. Bij aansluiting op de telefoonlijn moet de kiezer van de centrale ingeschakeld zijn, in DTMF-modus, met Contact ID-formaat en een ingevuld telefoonnummer (paragraaf 4.2), en **Communication protocol** moet op **2. AUTO** staan (paragraaf 6.3).

Via welke route gaat de gebeurtenis: via LAN of via de sim?

Via de route die de volgorde in **Reporting mode** (paragraaf 6.4.2) aangeeft: via de route volgens **Main type**; als die niet werkt, via die volgens **Backup type**, daarna volgens **Backup type 2**. Als het bericht via de reserveroute is verzonden, probeert de communicatiemodule na de tijd **Return from backup after** opnieuw de hoofdroute, en met het interval van **Communication path test** probeert hij alle routes uit. Ook de verbinding met Protegus 2 gebruikt dezelfde route. Op het bekabelde netwerk wordt geen mobiel dataverkeer verbruikt.

Waarvoor dienen de twee simhouders?

Met kaarten van twee verschillende providers wordt ook het mobiele netwerk tweevoudig: in Reporting mode zijn SIM1 en SIM2 aparte verbindingstypes, en elk ervan kan hoofd- of reserveroute zijn (paragraaf 6.4.2). De twee kaarten moeten apart worden ingesteld (**Network settings** → **SIM1**, **SIM2**: pincode, APN; paragraaf 6.6.2); een storing van SIM2 wordt gemeld door 3 knipperingen van de TROUBLE-led en het bericht SIM2_FAILURE (paragraaf 1.6 en 6.8). De communicatiemodule werkt ook met één kaart.

DSC: elk alarm komt binnen als algemeen alarm E130

Als hij alleen op de Keybus is aangesloten, krijgt de communicatiemodule van de centrale de status van de zones, maar niet het zonetype, en daarom meldt hij elk alarm met code E130 (paragraaf 3.3.1). Het tegelijk aansluiten van de Keybus en TIP/RING kan op de GET niet (dat is een functie van de GT+). Als de meldkamer een code verwacht die bij het zonetype past (bijvoorbeeld brand: E110), sluit de GET dan alleen op de TIP/RING-klemmen van de centrale aan en programmeer de kiezer (paragraaf 3.3.9 en 4.2): zo gaan de eigen Contact ID-codes van de centrale door, maar is er geen directe besturing – voor het inschakelen is een sleutelschakelaarzone nodig (paragraaf 3.4).

Paradox: de seriële poort is vergrendeld, of er is geen verbinding

Op de nieuwere Paradox-centrales (SP+, MG+, EVOHD+) kan de seriële poort af fabriek vergrendeld zijn; over het ontgrendelen gaan paragraaf 4.1.2 en het artikel Een vergrendelde seriële poort ontgrendelen op Paradox-alarmcentrales. Bij de centrales Spectra SP / SP+ en Magellan MG / MG+ kan in plaats van de seriële poort ook de aansluiting Keybus + TIP/RING worden gebruikt (paragraaf 3.3.3), waarvoor geen ontgrendeling nodig is, maar de firmware van de communicatiemodule moet minimaal 1.21 zijn (hoofdstuk 9).

Ik kan niet inschakelen vanuit Protegus 2

1. Bij directe besturing moet **Panel settings** → **Remote Arm/Disarm** zijn aangevinkt, en moet de centrale volgens paragraaf 4.1 zijn ingesteld (Paradox: PC-wachtwoord, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: de beschreven instellingen). Controleer in de tabel van paragraaf 1.3 of de centrale überhaupt direct bestuurbaar is.
2. Bij inschakelen met een sleutelschakelaar (paragraaf 3.4) moet de klem op de pagina **IN/OUT** op **OUT** staan (de fabrieksinstelling van de GET), moet de zone van de centrale een sleutelschakelaarzone zijn, en moet in Protegus 2 de uitgang aan de partitie zijn toegewezen, in dezelfde modus als in de centrale (pulserend of met twee standen; paragraaf 5.2).
3. Protegus 2 toont de status van de partitie aan de hand van de in- en uitschakelgebeurtenissen van de centrale: de centrale moet die melden (Opening/Closing).

Protegus 2 ziet het apparaat niet

1. Op het tabblad **User reporting** → **PROTEGUS Cloud** moet **Enable connection** zijn aangevinkt (paragraaf 6.5).
2. Bij het toevoegen moet de **PROTEGUS Cloud access Code** worden ingevoerd die in het apparaat is ingesteld; als u de code in TrikdisConfig hebt gewijzigd, pas die dan ook in de app aan.
3. Voer de IMEI precies in, vanaf het label van het apparaat of de sticker van de doos (of scan de QR-code).
4. Er moet op minimaal één route werkend internet zijn: de NETWORK LTE-led is groen en knippert geel (simkaart met datadienst en de juiste APN), of de NETWORK LAN-led is groen (LAN-kabel). De DATA-led moet na een gebeurtenis uitgaan.

Ik kan op afstand niet inloggen met TrikdisConfig

1. Het apparaat moet online zijn (NETWORK LTE groen, knippert geel, of NETWORK LAN groen), en de Protegus-verbinding moet zijn ingeschakeld (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** mag niet langer zijn dan 5 minuten: de PING houdt de verbinding in stand die nodig is voor toegang op afstand.
3. Controleer het wachtwoord van de beheerder of de installateur.

Kan ik de communicatiemodule vanuit de app instellen?

Ja: met firmware 1.08 of nieuwer is in het menu **Settings** → **Advanced settings** van Protegus 2 het merendeel van de instellingen beschikbaar (paragraaf 2.2 en hoofdstuk 6). Wat alleen in TrikdisConfig zit: het herstellen van de fabrieksinstellingen (paragraaf 6.9), **Preferred operator** (paragraaf 6.6.2) en het handmatig bijwerken van de firmware (hoofdstuk 9); de schakelaar **Event** van Serial bus wordt door de app getoond, maar niet gewijzigd. Als u met de installateurscode bent aangemeld, kunt u alleen de groepen wijzigen die de beheerder heeft vrijgegeven (paragraaf 6.2).

Ik ben het wachtwoord vergeten

Met TrikdisConfig kan dat niet, want ook het herstellen vereist een wachtwoord. Met de **RESET**-knop van het apparaat wel (paragraaf 6.9): houd hem bij ingeschakelde voeding 10 seconden ingedrukt. Alle instellingen worden gewist. Vanuit de app kan het herstellen niet worden gestart.

Hoeveel dataverkeer gebruikt het apparaat?

De gebeurtenisberichten en de PING's zijn zeer klein; het verkeer hangt vooral af van de PING-periode en de frequentie van de testmeldingen. Bij een gemiddeld huishoudelijk systeem blijft het maandelijkse verkeer doorgaans onder 10 MB. De precieze waarde hangt af van de instellingen en van de factureringseenheid van de provider; bij een kaart met een databundel is het daarom de moeite waard het verkeer van de eerste maand te controleren. Zolang de communicatiemodule via het bekabelde netwerk meldt, wordt er geen dataverkeer van de simkaart verbruikt.

11. Veiligheidsvoorschriften

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.

- Beveiligingsapparatuur mag alleen door een gekwalificeerde installateur worden geïnstalleerd en onderhouden.
- Lees de handleiding vóór de installatie door; het negeren van de instructies kan leiden tot een verkeerde werking of een defect van de apparatuur.
- Koppel de apparatuur los van de voeding vóór het aansluiten, bij elke elektrische verbinding en vóór onderhoud.
- Wijzigingen, aanpassingen en reparaties die niet door de fabrikant zijn toegestaan, maken de garantie ongeldig.
- Houd u aan de plaatselijke voorschriften voor afvalverwerking: gooi het afgedankte apparaat en de onderdelen ervan niet bij het huishoudelijk afval. Het symbool van de doorgekruiste vuilnisbak op wielen (WEEE) op het apparaat geeft aan dat het apart, als elektronisch afval, moet worden ingeleverd.

Zie ook

- Compatibiliteitszoeker – welke Trikdis-communicatiemodule en welke aansluiting bij uw alarmcentrale past.
- Trikdis-communicatiemodule + DSC-alarmcentrale: korte installatiehandleiding – de stappen van de DSC-aansluiting in het kort.
- Trikdis-communicatiemodule + Paradox-alarmcentrale: korte installatiehandleiding – de stappen van de Paradox-aansluiting in het kort.
- DSC Power Series NEO en Trikdis-communicatiemodules: compatibiliteit en oplossingen – waarom de NEO niet op de databus kan worden aangesloten, en wat de oplossing is.

- Een vergrendelde seriële poort ontgrendelen op Paradox-alarmcentrales – het ontgrendelen van de seriële poort van de centrales SP+, MG+ en EVOHD+.
- Op afstand inschakelen met een sleutelschakelaar vanuit de Protegus 2-app – de details en valkuilen van het inschakelen met een sleutelschakelaar.
- APN-instelling – lijst van Europese mobiele providers – de APN's van de providers, ook voor IoT- / M2M-kaarten.
- Engelstalige documentatie: docs.trikdis.com – GET – hier staat ook de omzettingstabel Contact ID → SIA (bijlage).

De handleidingen op docs.trikdis.com zijn in het Engels.

Gerelateerde producten

Trikdis GET Ethernet + 4G communicatiemodule

Trikdis CRP2 seriële poort aansluitkabel voor Paradox alarmpanelen

Trikdis ANT04 GSM zelfklevende antenne met 2,5m kabel

Trikdis ME301M magnetische GSM-antenne met 2,5m kabel

Auteursrecht

Deze handleiding is gemaakt door trikdis.hu en mobilamb.eu. De tekst, de opbouw, onze eigen afbeeldingen en aanvullingen zijn ons intellectueel eigendom en zijn auteursrechtelijk beschermd. Zonder onze toestemming mag ze niet geheel of gedeeltelijk worden gekopieerd, verspreid of op een andere website gepubliceerd. Voor de installatie en het gebruik van het product mag je haar vrij downloaden en afdrukken.

De namen en logo's Trikdis en Protegus zijn handelsmerken van UAB Trikdis.

Altijd actuele versie van deze handleiding: https://nl.mobilamb.eu/get-handleiding