G16-communicatiemodule – installatie- en gebruikershandleiding

Installatie- en gebruikershandleiding voor de Trikdis G16-communicatiemodule: aansluiting op de databus of seriële poort van de alarmcentrale, programmeren van de centrale, simkaart en instelling in TrikdisConfig, doormelding naar de meldkamer, de Protegus 2-app.



Uitgave: 2026-11-17
Altijd actuele webversie: https://nl.mobilamb.eu/g16-handleiding

Inhoud

1. Overzicht

1.1 Waarvoor dient hij, hoe werkt hij
1.2 Compatibele alarmcentrales
1.3 Versies
1.4 Belangrijkste kenmerken
1.5 Onderdelen van de communicatiemodule
1.6 Aansluitklemmen
1.7 Led-indicaties
1.8 Technische gegevens

2. Snelle inbedrijfstelling met TrikdisConfig

2.1 Voorbereiding
2.2 Type centrale en directe besturing
2.3 Verbinding met de Protegus 2-app
2.4 Verbinding met de meldkamer

3. Installatie en aansluiting

3.1 Installatiestappen
3.2 Plaatsing en antenne
3.3 Aansluiting op de alarmcentrale
3.3.1 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception en Integriti
3.4 Aansluiting van een sleutelschakelaarzone
3.5 Aansluiting van ingangen
3.6 Aansluiting van een uitgang met een relais
3.7 Aansluiting van een iO-8-uitbreiding
3.8 Aansluiting van de W485- en E485-module
3.9 Inschakelen en eerste controle
A TRIKDIS átjelző elindítása

4. Programmeren van de alarmcentrale

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

5. Bediening op afstand met de Protegus 2-app

5.1 Het apparaat toevoegen
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Directe besturing met de bediendeelcode
5.3 Inschakelen met een sleutelschakelaarzone
5.4 In- en uitschakelen vanuit de app
5.5 Bediening met sms-berichten

6. TrikdisConfig – de instellingen in detail

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

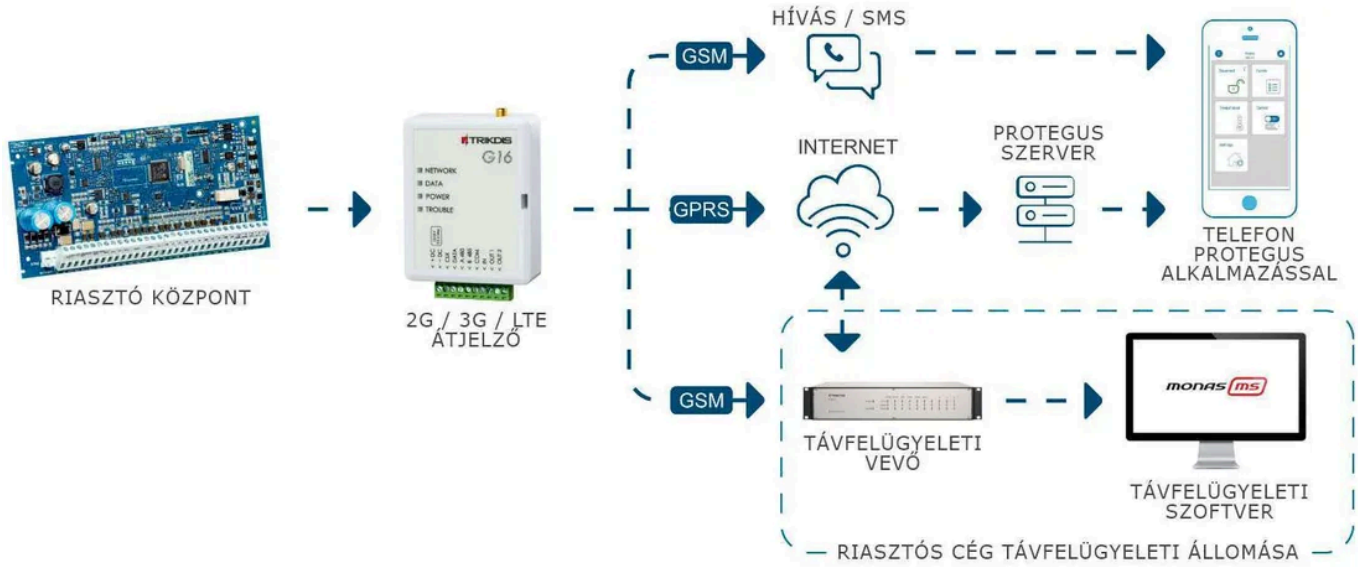
1. Overzicht

De G16 is de **mobiele communicatiemodule met directe aansluiting** van Trikdis: hij wordt niet aangesloten op de telefoonlijnuitgang van de alarmcentrale, maar op de **bediendeelbus of seriële poort** van de centrale. Hij leest de gebeurtenissen rechtstreeks uit de centrale – samen met het zone-, partitie- en gebruikersnummer – en stuurt ze via een mobiele dataverbinding door naar de ontvanger van de meldkamer en naar de Protegus-cloud, in de app van de gebruiker. Hij werkt met de ondersteunde centrales van DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell en Crow; bij de **direct bestuurbare** types schakelt de gebruiker in en uit vanuit de Protegus 2-app met zijn eigen bediendeelcode, zonder aparte sleutelschakelaarzone. De Protegus 2-app kan worden gebruikt met alle alarmcentrales die de G16 ondersteunt, ongeacht het merk. Voor centrales van andere merken die alleen een telefoonlijnuitgang hebben, is de G16T-communicatiemodule (TIP/RING) de juiste keuze.

1.1 Waarvoor dient hij, hoe werkt hij

- **Hij leest de centrale rechtstreeks uit.** Op de bus van de centrale komt elke gebeurtenis meteen bij de communicatiemodule aan, met de eigen nummering van de centrale; de kiezer van de centrale hoeft niet te worden ingesteld en er is ook geen Contact ID-kiezen.
- **Hij meldt door naar de meldkamer.** Hij stuurt de gebeurtenissen via een IP-verbinding naar een software- of hardwareontvanger van Trikdis (TRK-protocol) – die werken samen met elke meldkamersoftware – of naar elke universele ontvanger (SIA DC-09 2007/2012, SUR-GARD TL150). Aan een SUR-GARD-ontvanger geeft hij de Contact ID-codes van de centrale omgezet in SIA-codes door. Standaard controleert hij de verbinding elke 30 seconden (of met het interval dat u instelt), en bij een storing schakelt hij over naar het reservekanaal.
- **Hij waarschuwt de gebruiker.** De Protegus 2-app toont wat er is gebeurd in een pushmelding – met een apart geluid dat bij de gebeurtenis past – en in de gebeurtenissenlijst; vanuit de app kan de gebruiker in- en uitschakelen en de aangesloten apparaten schakelen (verlichting, poort, ventilatie, verwarming, beregening enz.). De gebruiker kan ook per sms en telefoonoproep worden gewaarschuwd.
- **Samen of afzonderlijk** werkt hij met de meldkamer en de gebruiker: hij kan alleen met Protegus 2 worden gebruikt (zonder meldkamer), alleen met een meldkamer, of met allebei. Als beide zijn ingesteld, stuurt hij de gebeurtenis eerst naar de meldkamer en daarna naar de gebruiker.
- **Sms-reserve.** Hij waarschuwt de meldkamer ook per sms als de dataverbinding in het netwerk van de provider niet werkt; hij kan ook parallel naar twee ontvangers sturen, elk met een eigen reservekanaal.
- **Hij heeft eigen in- en uitgangen.** Drie I/O-klemmen met dubbele functie kunnen worden gebruikt als ingang (detector, sabotage) of als bestuurbare uitgang (sleutelschakelaarzone, relais); de uitgangen kunt u schakelen vanuit de Protegus 2-app en met een sms-commando. Op de RS485-bus van de 4G-versie geeft een iO-8-uitbreiding 8 extra I/O's, en met een W485- of E485-module kan hij ook communiceren via WiFi of via een bekabelde internetverbinding – dan is het mobiele netwerk de reserveroute.

De opbouw van het systeem ziet u in de onderstaande afbeelding: de bus van de alarmcentrale is aangesloten op de G16, de G16 bereikt via het mobiele netwerk het internet en daarlangs de ontvanger van de meldkamer en de Protegus-cloud, en de gebruiker ziet het systeem in de Protegus 2-app.



Afbeelding 1. De plaats van de G16 in het systeem: alarmcentrale → G16 → mobiel netwerk → ontvanger van de meldkamer en Protegus-cloud → Protegus 2-app. De gebruiker kan ook sms'en en oproepen ontvangen (GSM), de ontvanger van de meldkamer als reserve sms'en.

- 1 Alarmcentrale (bediendeelbus of seriële poort)
- 2 G16-communicatiemodule (2G / 4G)
- 3 Oproep en sms naar de gebruiker
- 4 Mobiele dataverbinding → internet → Protegus-cloud
- 5 Telefoon met de Protegus 2-app
- 6 Ontvanger van de meldkamer
- 7 Meldkamersoftware (de meldkamer van het beveiligingsbedrijf)

1.2 Compatibele alarmcentrales

De G16 kan worden aangesloten op de onderstaande centrales. Bij de **direct bestuurbare** types gebeurt het in- en uitschakelen vanuit de app met de bediendeelcode; bij de overige met een sleutelschakelaarzone (paragraaf 3.4). Voor directe besturing van Paradox-centrales moet de firmware van de centrale minimaal **V.4** zijn; op de nieuwere Paradox-types (SP+, MG5050+, EVOHD+) is de seriële poort af fabriek vergrendeld en moet die vóór gebruik worden ontgrendeld.

Rechtstreeks bedienbare centrales – de communicatiemodule ontvangt de gebeurtenissen via de databus of de seriële poort, en in- en uitschakelen werkt zonder extra bekabeling:

Fabrikant	Aansluiting	Typen
Paradox	seriële poort	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* boven firmware 7.50)
DSC	databus	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	databus	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	seriële poort	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	databus	Ademco Vista-15, Vista-20, Vista-48

Op de nieuwere Paradox-centrales die met * zijn gemarkeerd, is de seriële poort af fabriek vergrendeld; een extern apparaat kan er pas na ontgrendeling mee communiceren.

Soros port feloldás útmutató

Met sleutelschakelaar bedienbare centrales – de communicatiemodule ontvangt de gebeurtenissen via de databus of de seriële poort; voor de bediening zijn een sleutelschakelaaraansluiting en programmering nodig (punt 3.4):

Fabrikant	Aansluiting	Typen
Paradox	seriële poort	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	databus	PC1404, PC5020
Texecom	seriële poort	Premier 412, 816, 832, 832+
Inner Range	databus	Inception, Integriti
Crow	databus	Runner 4/8, 8/16

De lijst verandert af en toe; de meest actuele stand vindt u in de Compatibiliteitszoeker. Daarnaast kan hij ook worden gebruikt met de centrales **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 en MATRIX 816**, **DSC PC5015** en **Paradox DIGIPLEX EVO96 en NE96**. Met **DSC PowerSeries NEO**-centrales werkt de G16 niet: de fabrikant staat geen externe apparaten toe op de NEO-bus, zie DSC Power Series NEO en Trikdis-communicatiemodules: compatibiliteit en oplossingen.

1.3 Versies

Deze handleiding is geschreven voor **hardwareversie 4** van de G16, maar is **ook bruikbaar voor hardwareversie 3**: aansluiting, instelling en werking van de twee versies zijn grotendeels gelijk. De handleiding geldt evengoed voor de versies met 2G-, 3G- en 4G-modem. De verschillen staan in de onderstaande tabel; waar de tekst de gegevens van versie 4 noemt, houd voor versie 3 rekening met deze tabel.

	Hardware 3 (v3)	Hardware 4 (v4)
Types (in TrikdisConfig)	bv. G16_3210 (2G); er zijn ook versies met 3G- en 4G-modem gemaakt	G16_G410 (2G), G16_54E0 (4G)
In-/uitgangen	1 ingang van instelbaar type (IN) + 2 open-collectoruitgangen (OUT1, OUT2, max. 0,15 A)	3 I/O-klemmen met dubbele functie (I/O 1, I/O 2, I/O 3), elk bruikbaar als ingang of als open-collectoruitgang (max. 0,15 A)
Instellen van de in-/uitgangen	Pagina System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	Pagina **IN/OUT** (paragraaf 6.6)
Stroomverbruik	100 mA; tijdens verzenden maximaal 250 mA	60–100 mA; tijdens verzenden maximaal 500 mA
RS485-bus (iO-8, W485, E485)	alleen op de 3G- en 4G-versie	alleen op de 4G-versie (G16_54E0)

Hardwareversie 4 wordt gemaakt met twee modems:

Type	Modem	Frequenties	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	nee

Type	Modem	Frequenties	RS485 (iO-8, W485, E485)
G16_54E0	4G (LTE)	regioafhankelijke LTE-banden	ja

De hardwareversie vindt u in de statusbalk van TrikdisConfig (**HW**) en op het label op de achterkant van het apparaat. Over de aankondiging van versie 4 gaat een apart artikel: De v4-hardwareversie van de G16- en G16T-GSM-communicatiemodules komt eraan.

1.4 Belangrijkste kenmerken

Verbinding met de alarmcentrale

- Aan te sluiten met maximaal 4 draden (+DC, −DC, CLK, DATA) op de bediendeelbus van de centrale (DSC, Caddx, Crow, Pyronix, Honeywell) of op de seriële poort (Paradox, Texecom, InnerRange); voor de seriële poort is een fabriekskabel verkrijgbaar (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Hij stuurt elke gebeurtenis van de centrale door met de volledige gebeurtenisinformatie (code, partitie, zone of gebruiker); hij meldt het wegvallen van de verbinding (TROUBLE-led, COMMUNICATION-gebeurtenis).
- De direct bestuurbare centrales kunnen vanuit de app met de bediendeelcode worden in- en uitgeschakeld; Protegus 2 toont ook de status van de zones.

Communicatie met de meldkamer

- IP-verbinding met Trikdis-ontvangers (IPcom-softwareontvanger, RL14, RM14) en universele ontvangers (SIA DC-09, TL150).
- Primair, reserve- en parallel kanaal; reservemelding per sms naar de Trikdis-sms-ontvanger (RL14, RM14, GM14).
- Berichtversleuteling AES-128; gebeurtenisbuffer van 60 berichten.

Gebruikersfuncties

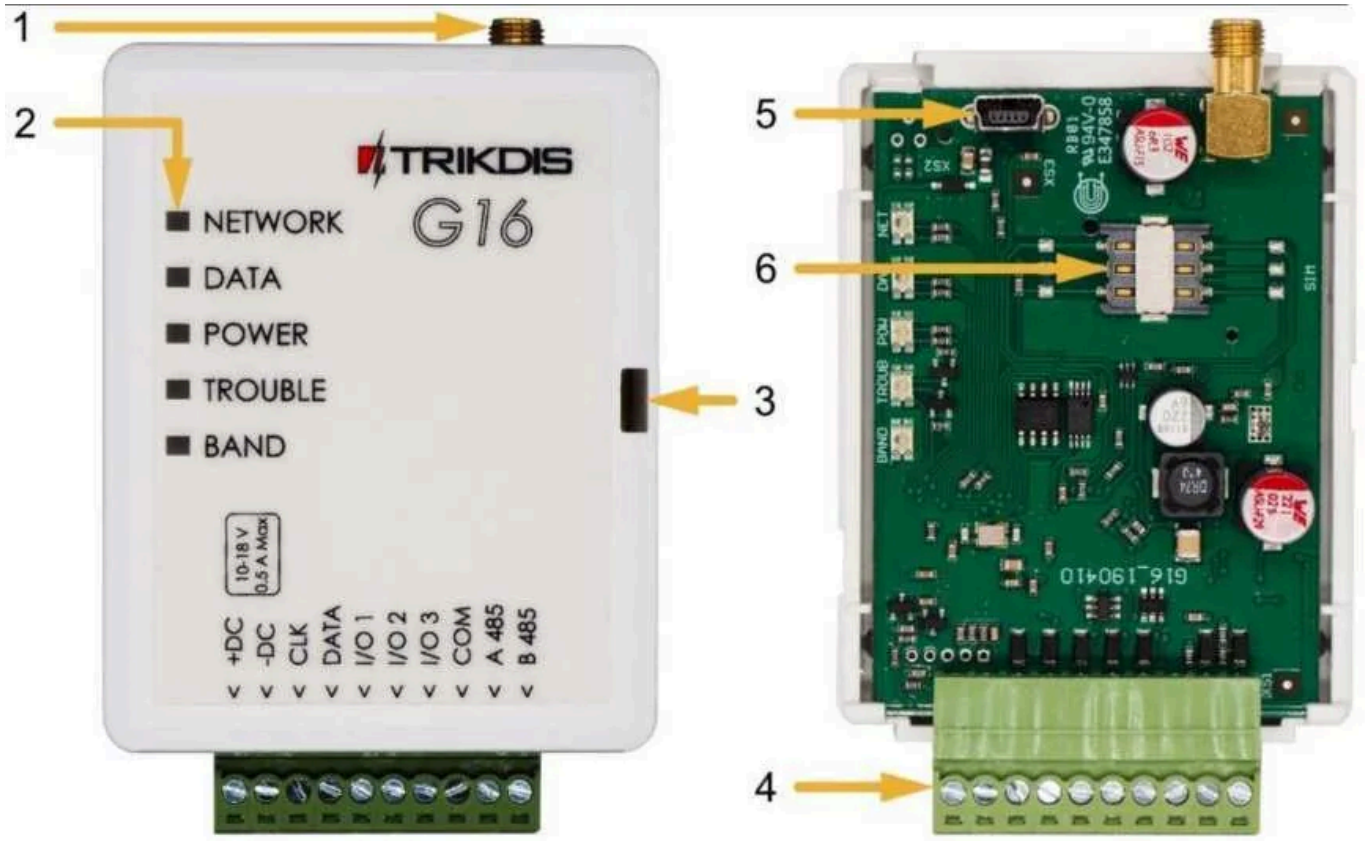
- Protegus 2-app voor mobiel en web: meldingen, gebeurtenissenlijst, in- en uitschakelen, uitgangen schakelen.
- Bediening en basisinstelling ook met sms-commando's.
- Melding ook per sms en telefoonoproep, naar maximaal 4 telefoonnummers.
- Gebruikersrechten op meerdere niveaus in de app (beheerder, installateur, gebruiker).

Installatie en instelling

- De instellingen kunnen in een bestand worden opgeslagen en in een andere communicatiemodule worden geladen.
- Twee toegangsniveaus: beheerder en installateur.
- Op afstand in te stellen en bij te werken met de TrikdisConfig-software.

1.5 Onderdelen van de communicatiemodule

De printplaat van de G16 zit in een witte kunststof behuizing; het frontdeksel kan worden verwijderd en het klemmenblok kan eraf worden getrokken. De onderstaande afbeelding toont de 4G-versie; de 2G-versie heeft geen BAND-led en geen A 485- / B 485-klemmen.



Afbeelding 2. Onderdelen van de G16 (4G-versie) van voren en met geopende behuizing.

- 1 SMA-aansluiting van de GSM-antenne
- 2 Led-indicatoren (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Opening om het frontdeksel te verwijderen
- 4 Afneembaar klemmenblok
- 5 USB Mini-B-aansluiting voor het programmeren
- 6 Houder voor de nano-simkaart

Het klemmenblok kan eraf worden getrokken: zo kunt u het apparaat met één handeling spanningsloos maken of herstarten, is het bij het aansluiten makkelijker te hanteren, en kunt u het apparaat voor programmeren via USB naar de computer meenemen.

1.6 Aansluitklemmen

Klem	Functie
+DC	Voeding, +10–18 V DC
–DC	Voeding, negatief
CLK	Klok- / seriële lijn van de bus van de centrale
DATA	Datalijn van de bus van de centrale
I/O 1	In-/uitgang 1 (fabrieksinstelling: niet gebruikt)
I/O 2	In-/uitgang 2 (fabrieksinstelling: ingang, NO)
I/O 3	In-/uitgang 3 (fabrieksinstelling: uitgang)
COM	Gemeenschappelijk (negatief) punt voor de in- en uitgangen
A 485	A-draad van de RS485-bus (alleen 4G-versie)
B 485	B-draad van de RS485-bus (alleen 4G-versie)

De opschriften van de klemmen staan ook op het frontdeksel, zodat u het deksel bij het aansluiten niet hoeft te verwijderen. Op welke klem van de centrale CLK en DATA worden aangesloten, verschilt per fabrikant – de aansluitschema's staan in paragraaf 3.3.

1.7 Led-indicaties

De leds op het frontdeksel zijn de belangrijkste hulpmiddelen bij inbedrijfstelling en storingzoeken. Lees ze samen: POWER toont de voeding, NETWORK het netwerk, TROUBLE de storing en BAND (alleen 4G) het type netwerk.

NETWORK – netwerkverbinding

Indicatie	Betekenis
uit	Geen verbinding met het mobiele netwerk
knippert geel	Verbinding met het mobiele netwerk wordt gemaakt
brandt groen	Verbonden met het mobiele netwerk
brandt groen, knippert geel	Verbonden; het aantal gele knipperingen is het **signaalniveau**: op 2G betekenen 5 knipperingen, op 4G 3 knipperingen een goed signaal

DATA – dataverkeer

Indicatie	Betekenis
uit	Geen berichten die op verzending wachten
brandt groen	Er staan berichten in de buffer die op verzending wachten
knippert groen	Er worden gegevens verzonden of ontvangen (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

Indicatie	Betekenis
uit	Geen voeding, of de voeding is losgekoppeld
brandt groen	Ingeschakeld, de voedingsspanning is in orde
brandt geel	Ongeschikte voedingsspanning (11,5 V of lager)
brandt groen, knippert geel	Klaar voor programmeren (USB-kabel aangesloten)
brandt geel (tijdens het programmeren)	Geen verbinding met de computer

TROUBLE – storing

Indicatie	Betekenis
uit	Geen storing
1 rode knippering	Geen simkaart
2 rode knipperingen	Sim-pinfout (verkeerde pincode)
3 rode knipperingen	Programmeerfout (geen APN)
4 rode knipperingen	Kan zich niet aanmelden op het mobiele netwerk (registratiefout)
5 rode knipperingen	Kan geen verbinding maken met het datanetwerk (GPRS/UMTS/LTE)
6 rode knipperingen	Geen verbinding met de ontvanger van de meldkamer en/of de Protegus-server (de oorzaak kan ook een storing in de internetverbinding zijn)
7 rode knipperingen	Verbinding met de alarmcentrale verbroken (bus- of seriële verbinding)
knippert rood (tijdens het programmeren)	Geheugenfout
brandt rood (tijdens het programmeren)	Beschadigde firmware

BAND – type netwerk (alleen 4G-versie)

Groene knipperingen	Netwerk
1	geen
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.8 Technische gegevens

Parameter	Waarde
Verbinding met de alarmcentrale	bediendeelbus of seriële poort, afhankelijk van het type centrale (maximaal 4 draden: +DC, −DC, CLK, DATA; op de bus van Caddx en Pyronix wordt CLK niet gebruikt)
In-/uitgangen	3 I/O's met dubbele functie (I/O 1, I/O 2, I/O 3): 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
Uitbreiding	op de RS485-bus (alleen 4G-versie): iO-8-uitbreiding (+8 I/O) en andere uitbreidingen uit de iO-serie; W485 WiFi-, E485 Ethernet-module
2G-modem	850 / 900 / 1800 / 1900 MHz
4G-modem	regioafhankelijke LTE-banden
Voedingsspanning	10–18 V DC
Stroomverbruik	60–100 mA nominaal; maximaal 500 mA tijdens verzenden
Transmissieprotocollen	TRK, DC-09_2007, DC-09_2012, TL150

Parameter	Waarde
Gebeurtenisbuffer	60 berichten
Versleuteling	AES-128
Programmeren	TrikdisConfig (Windows) via een USB Mini-B-kabel of op afstand; sms-commando's
Omgevingsomstandigheden	−10 … +50 °C, max. 80 % relatieve luchtvochtigheid (bij +20 °C)
Afmetingen	92 × 65 × 26 mm
Gewicht	80 g

2. Snelle inbedrijfstelling met TrikdisConfig

Alle instellingen van de G16 gebeuren met het Windows-programma **TrikdisConfig** – via een USB-kabel of op afstand. In dit hoofdstuk beschrijven we de kortste weg: u stelt het apparaat op tafel in, vóór het aansluiten, en ter plaatse hoeft u het daarna alleen nog aan te sluiten. De uitgebreide uitleg van de instellingen staat in hoofdstuk 6.

2.1 Voorbereiding

Wat u nodig hebt

USB Mini-B-kabel · kabel met minimaal 4 aders voor de bus van de centrale – voor de seriële poort van Paradox een **CRP2**- of **CRP2B**-kabel, voor de seriële poort van Texecom een **CRP4**-kabel · platte schroevendraaier van 2,5 mm · mobiele antenne met geschikte versterking (op plaatsen met zwakke dekking een antenne met hogere versterking) · actieve nano-simkaart met mobiele datadienst (de pincodevraag kan worden uitgeschakeld) · de installatiehandleiding van de alarmcentrale. De benodigde accessoires moeten apart bij de leverancier worden besteld.

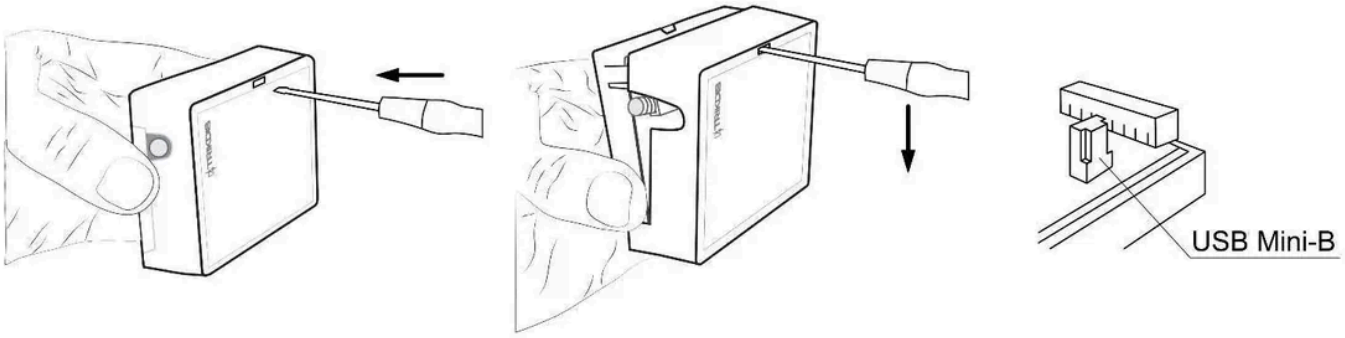
1. Download en installeer de TrikdisConfig-software. Typ op de website van Trikdis (www.trikdis.com) in het zoekveld: „TrikdisConfig”.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

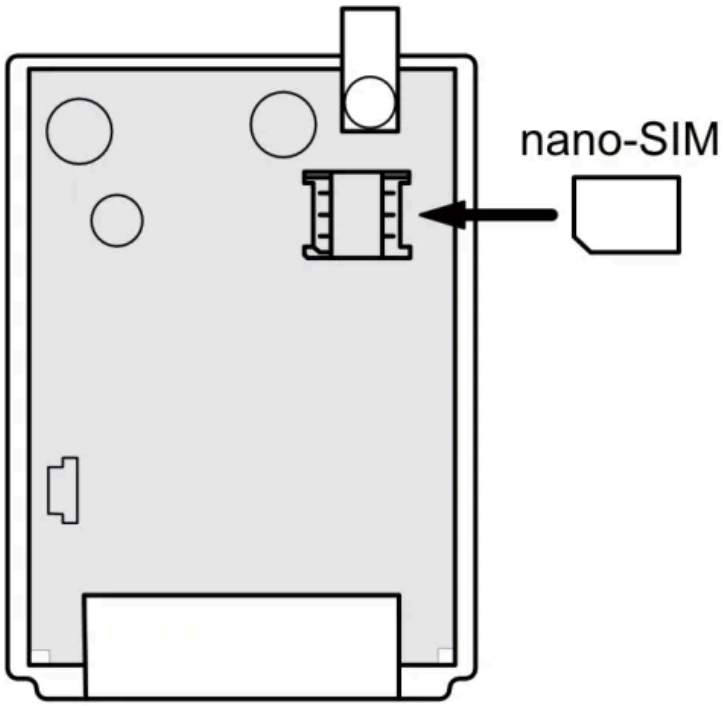
Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

2. Open het frontdeksel van de G16. Steek een platte schroevendraaier in de opening aan de bovenrand van het deksel en wip het frontdeksel voorzichtig naar beneden los. De onderstaande afbeelding toont het openen en de plaats van de USB-aansluiting.



Afbeelding 3. Het frontdeksel loswippen met een platte schroevendraaier (links, midden) en de plaats van de USB Mini-B-aansluiting op de printplaat (rechts).

3. Plaats de nano-simkaart in de houder, in de richting die op de afbeelding te zien is. De kaart moet actief zijn en een mobiele datadienst hebben; schakel zo mogelijk de pincodevraag uit in een telefoon (dan hoeft u in het apparaat geen pincode in te voeren).



Afbeelding 4. De plaats van de nano-simkaart op de printplaat.

4. Verbind de G16 met de computer via een USB Mini-B-kabel. De USB-aansluiting levert voldoende voeding voor het programmeren, een aparte voeding is niet nodig.

Waarschuwing

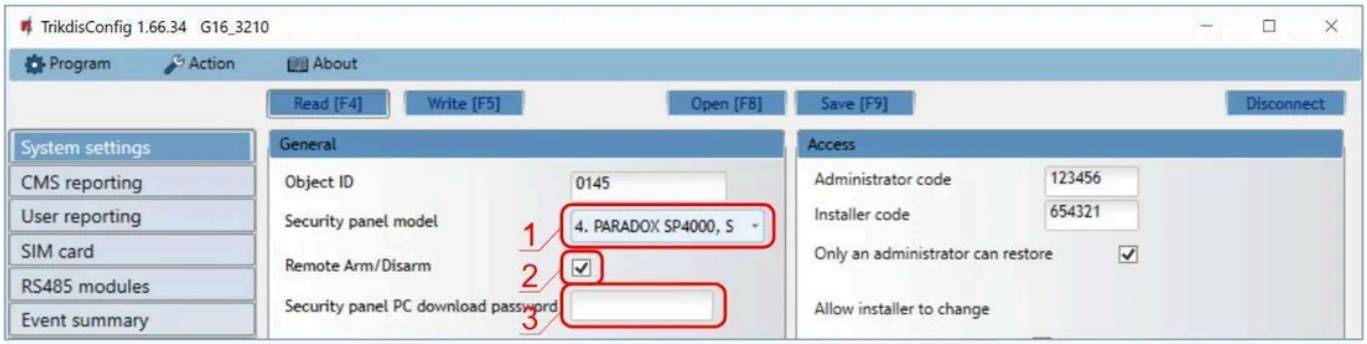
Zolang het apparaat via een USB-kabel met de computer is verbonden, staat het in de programmeermodus: de normale werking stopt, het bewaakt niet, meldt niet, is niet te bedienen, wordt via USB gevoed en start opnieuw op nadat de kabel is losgekoppeld. Het apparaat mag daarom niet vrij toegankelijk zijn: 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 om een wachtwoord wordt gevraagd, voer dan de 6-cijferige beheerderscode (af fabriek `123456`) of installateurscode

(af fabriek `654321`) in.

2.2 Type centrale en directe besturing

Welke werkwijze u ook gebruikt, geef eerst op de pagina **System settings** op op welke centrale de communicatiemodule komt.



Afbeelding 5. TrikdisConfig – pagina System settings, groep General.

- 1 **Security panel model** – het type van de aangesloten alarmcentrale uit de lijst; hiervan hangt af hoe de communicatiemodule de bus uitleest.
- 2 **Remote Arm/Disarm** – vink dit aan als de gebruiker de centrale vanuit de Protegus 2-app met zijn eigen bediendeelcode wil in- en uitschakelen. Verschijnt alleen bij de direct bestuurbare types; bij de overige centrales kan het inschakelen met een sleutelschakelaarzone worden opgelost (paragraaf 3.4) – laat het vakje dan leeg.
- 3 **Security panel PC download password** – bij een Paradox- en Texecom-centrale het pc- resp. UDL-wachtwoord van de centrale (4 tekens); dit moet overeenkomen met het wachtwoord dat in de centrale is ingesteld. Het veld verschijnt nadat Remote Arm/Disarm is aangevinkt.

Bij meerdere centrales is ook een instelling in de centrale nodig: bij Caddx-, Honeywell- en InnerRange-centrales al voor het uitlezen van gebeurtenissen (het vrijgeven van de bus resp. de seriële poort), bij Paradox- en Texecom-centrales voor de directe besturing (pc- resp. UDL-wachtwoord) – hoofdstuk 4 beschrijft dit per fabrikant, samen met het wijzigen van het wachtwoord.

2.3 Verbinding met de Protegus 2-app

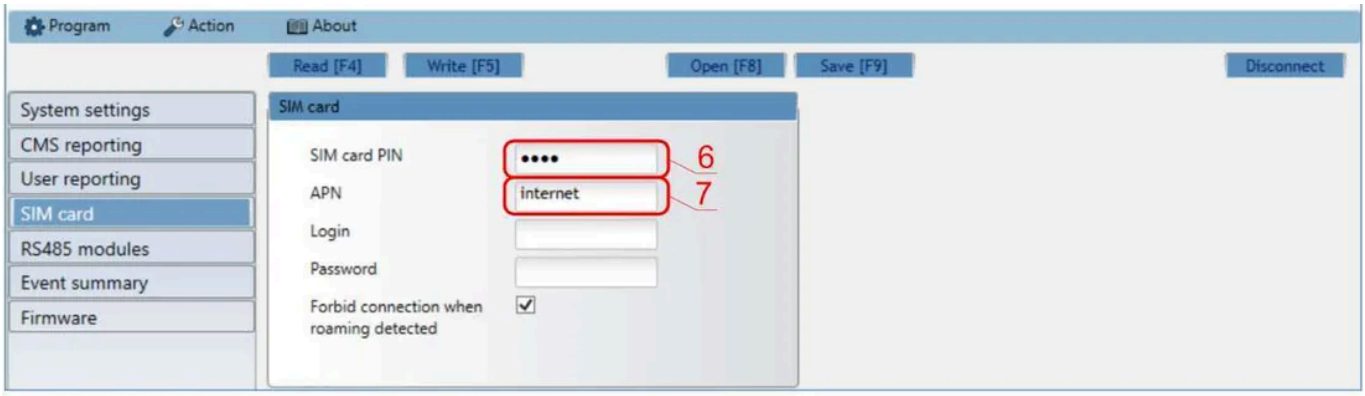
Als de gebruiker het systeem vanuit de Protegus 2-app wil zien en bedienen, stel dan op de pagina **User reporting**, tabblad **PROTEGUS Cloud**, het volgende in.



Afbeelding 6. TrikdisConfig – User reporting, tabblad PROTEGUS Cloud.

- 4 **Enable connection** – vink dit aan: hiermee wordt de verbinding met de Protegus-cloud ingeschakeld.
- 5 **Protegus Cloud access code** – wijzig het fabriekswachtwoord `123456`. Deze code moet later in de app worden ingevoerd bij het aanmaken van het systeem; **na het aanmaken van het systeem kan ze niet meer worden gewijzigd.**

Geef daarna op de pagina **SIM card** de gegevens van de kaart op.



Afbeelding 7. TrikdisConfig – pagina SIM card.

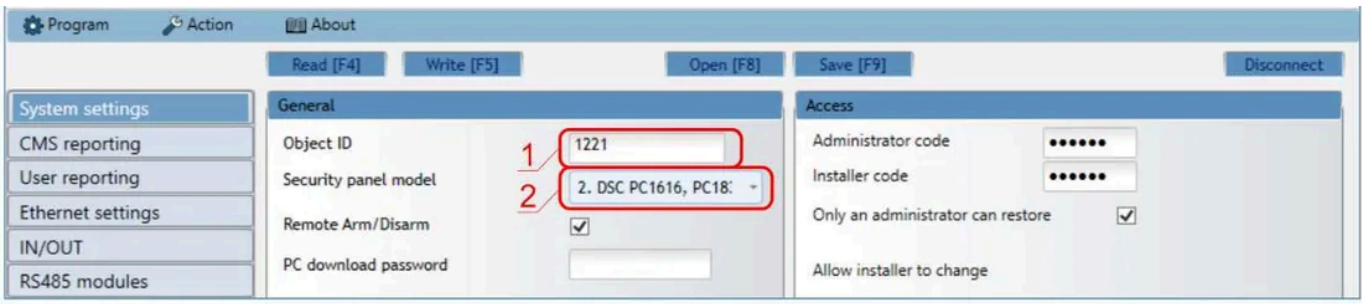
- 6 **SIM card PIN** – de pincode van de kaart (als de pincodevraag is uitgeschakeld, kan de fabriekswaarde blijven staan).
- 7 **APN** – het toegangspunt voor de dataverbinding van de provider (zie hieronder).

De APN (Access Point Name) is het toegangspunt voor de dataverbinding van de mobiele provider; zonder APN kan het apparaat geen verbinding maken met het internet. De juiste waarde krijgt u van de provider van de simkaart, en u vindt ze ook op de website van de provider; de APN „internet" is algemeen en werkt in de netwerken van veel providers. De bekende APN's van Europese providers houden we bij in een apart artikel: APN-instelling – lijst van Europese mobiele providers.

Voor IoT- / M2M-datakaarten (machine-to-machine) 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 ze op bij de provider; als de provider ook een gebruikersnaam en wachtwoord opgeeft, vul die dan eveneens in.

2.4 Verbinding met de meldkamer

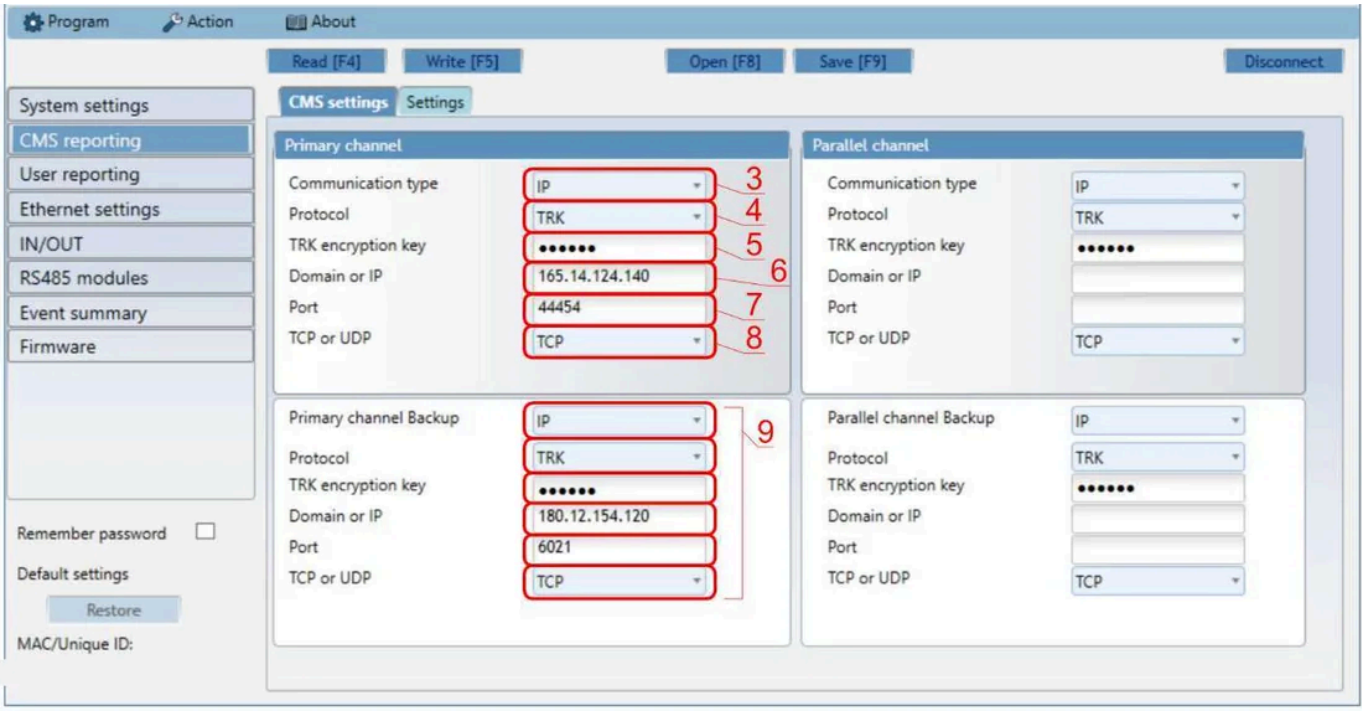
Als het apparaat ook naar een ontvanger van de meldkamer meldt, geef dan op de pagina **System settings** ook het objectnummer op.



Afbeelding 8. TrikdisConfig – pagina System settings, groep General.

- 1 **Object ID** – het objectnummer dat u van de meldkamer hebt gekregen (4 hexadecimale tekens, 0–9, A–F). `FFFE` en `FFFF` kunnen niet worden gebruikt.
- 2 **Security panel model** – het type van de aangesloten alarmcentrale (als u dit in paragraaf 2.2 nog niet hebt ingesteld).

Stel daarna op de pagina **CMS reporting**, in het deel **Primary channel** (primair kanaal), de gegevens van de ontvanger in.

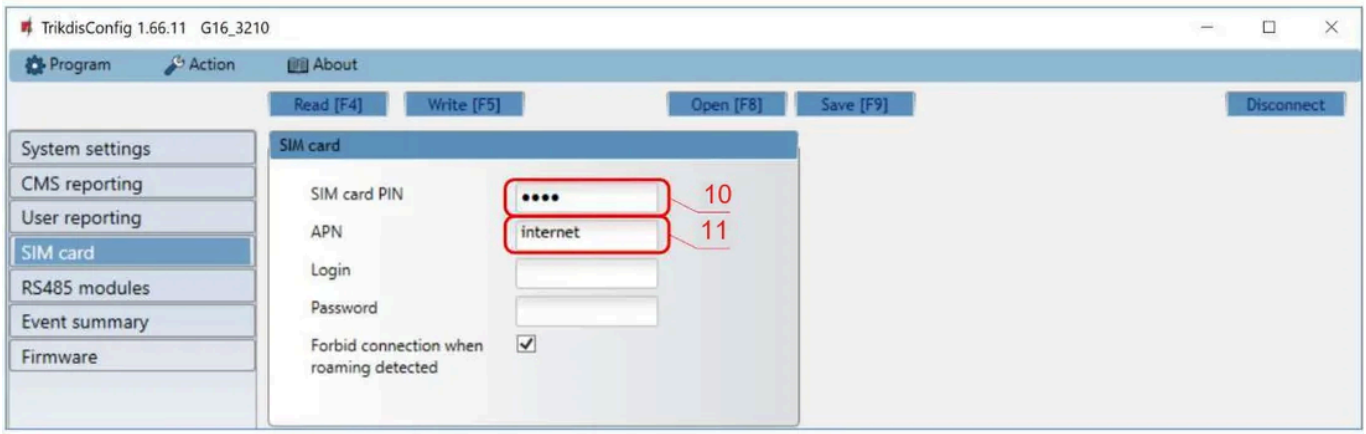


Afbeelding 9. TrikdisConfig – CMS reporting, tabblad CMS settings.

- 3 **Communication type** – kies de **IP**-verbinding (sms wordt als primair kanaal niet aanbevolen).
- 4 **Protocol** – **TRK** voor een Trikdis-ontvanger, **DC-09_2007** of **DC-09_2012** voor een universele ontvanger, **TL150** voor een SUR-GARD-ontvanger.
- 5 **TRK encryption key** – de 6-cijferige versleutelingssleutel die in de ontvanger is ingesteld.
- 6 **Domain or IP** – de domeinnaam of het IP-adres van de ontvanger.
- 7 **Port** – het poortnummer van de ontvanger.
- 8 **TCP or UDP** – het transportprotocol; volgt de instelling van de ontvanger.
- 9 **Primary channel Backup** – reservekanaal bij een storing van het primaire kanaal; vul het op dezelfde manier in, aanbevolen.

Het wordt ook aanbevolen het **Parallel channel** (parallel kanaal) en het bijbehorende reservekanaal in te stellen als de gebeurtenissen door twee ontvangers moeten worden ontvangen; in het veld **Backup SMS reporting number** kunt u – ook dit wordt aanbevolen – het telefoonnummer van de Trikdis-sms-ontvanger invullen: het apparaat stuurt na de eerste start meteen een sms naar dit nummer, en meldt daarna per sms als geen enkel IP-kanaal werkt.

Geef ten slotte op de pagina **SIM card** de gegevens van de kaart op, als u dat in paragraaf 2.3 nog niet hebt gedaan.



Afbeelding 10. TrikdisConfig – pagina SIM card.

- 10 **SIM card PIN** – de pincode van de kaart.
- 11 **APN** – het toegangspunt van de provider (zie paragraaf 2.3).

Melden per sms naar de meldkamer werkt alleen met een Trikdis-ontvanger (RL14 IP/sms-ontvanger, RM14 meerkanaalsontvanger of GM14 sms-ontvanger); dan zijn alleen de versleutelingssleutel en het telefoonnummer nodig. Geef bij het **DC-09**-protocol op het tabblad **Settings** ook het DC-09-object-, lijn- en ontvangernummer op.

Druk aan het einde van de instellingen op de knop **Write [F5]** (schrijven), wacht op de bevestiging en trek de USB-kabel eruit. Het apparaat is nu klaar om te worden aangesloten.

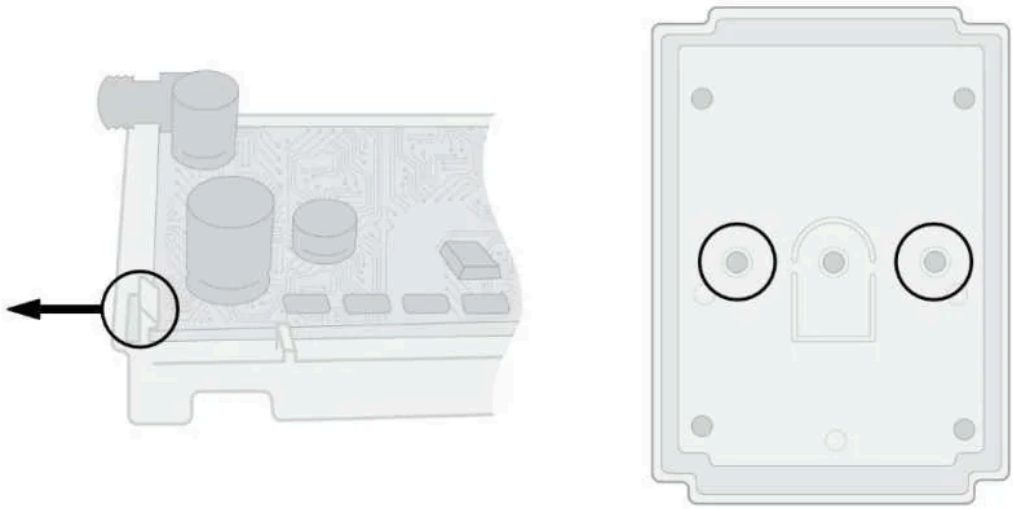
3. Installatie en aansluiting

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 Installatiestappen

1. Verwijder het frontdeksel (zie paragraaf 2.1) en trek het klemmenblok eraf.
2. Plaats de nano-simkaart, als u dat bij de inbedrijfstelling nog niet hebt gedaan.
3. Haal de printplaat uit het achterdeel: open de vergrendeling in de hoek (zie de afbeelding).
4. Bevestig het achterdeel met schroeven op de gekozen plaats.
5. Plaats de printplaat terug in het achterdeel en steek het klemmenblok er weer op.
6. Schroef de GSM-antenne vast.
7. Plaats het frontdeksel terug.



Afbeelding 11. De printplaat uitnemen: de vergrendeling in de hoek openen (links) en de bevestigingsgaten van het achterdeel (rechts, omcirkeld).

De simkaart moet actief zijn, en voor gebruik via IP moet de mobiele dataverbinding erop werken. Als u niet wilt dat TrikdisConfig om een pincode vraagt, schakel dan de pincodevraag op de kaart uit in een telefoon.

3.2 Plaatsing en antenne

- Plaats de communicatiemodule op een **droge plek binnenshuis**, bij voorkeur in de buurt van de behuizing van de alarmcentrale, zodat de busleiding kort blijft.
- In een **metalen behuizing** wordt het mobiele signaal sterk verzwakt. Als de communicatiemodule in de metalen behuizing van de centrale komt, leid de antenne dan naar buiten de behuizing, of gebruik een antenne met een langere kabel.
- **Controleer het signaalniveau** vóór de definitieve bevestiging: het aantal gele knipperingen van de NETWORK-led moet op 2G minimaal 5 en op 4G minimaal 3 zijn (zie paragraaf 1.7). Is het minder, zoek dan een betere plek 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 netspanningsleidingen.



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

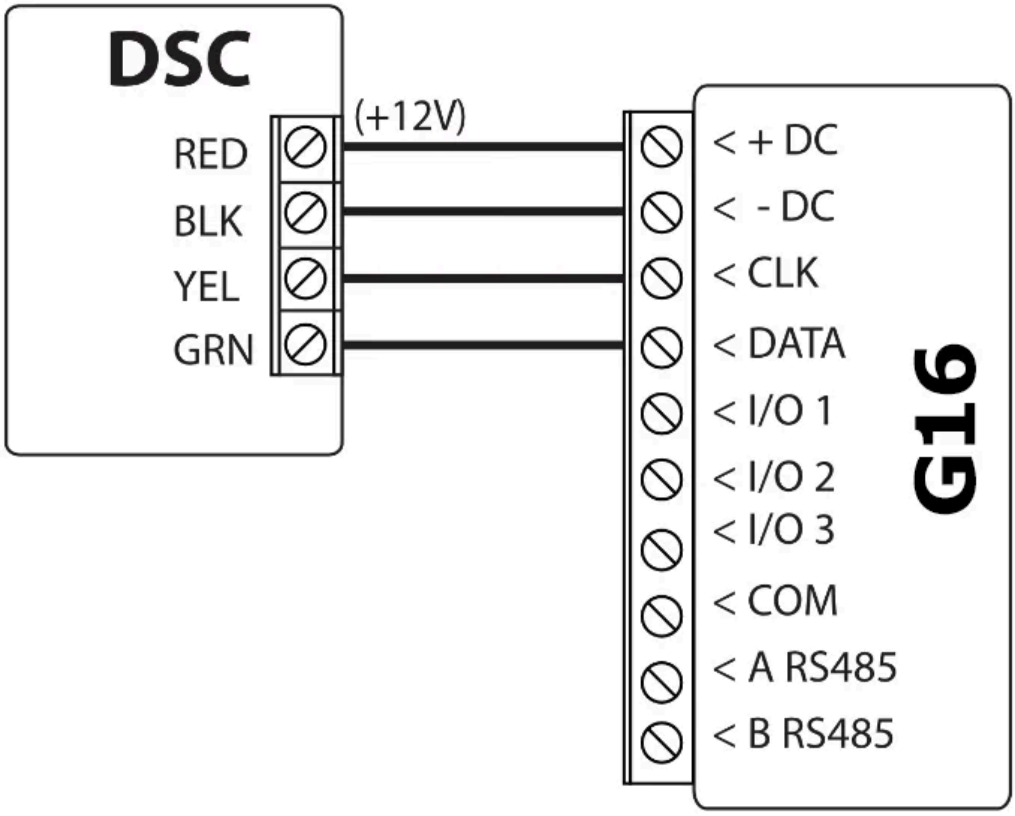
De G16 wordt met **maximaal vier draden** op de centrale aangesloten (op de bus van Caddx en Pyronix wordt CLK niet gebruikt): op de klemmen **+DC** en **–DC** komt de 12 V-hulpvoeding (AUX) van de centrale, op de klemmen **CLK** en **DATA** de twee datadraden van de bediendeelbus of seriële poort van de centrale. Welke klem van de centrale welke is, verschilt per fabrikant – sluit aan volgens de onderstaande schema's. Voor centrales met een seriële poort (Paradox, Texecom) is een fabriekskabel verkrijgbaar, waarvan het ene uiteinde in de connector van de centrale past en het andere op het klemmenblok van de G16 kan worden aangesloten.

De G16 kan tijdens het verzenden tot 500 mA opnemen. Controleer of de AUX-uitgang van de centrale dit aankan, samen met de andere aangesloten apparaten. Omdat de voeding van de centrale komt, voedt de accu van de centrale bij een stroomstoring ook de communicatiemodule. De meeste centrales raken niet beschadigd door verwisselde draden van een apparaat op de bus, maar het verwisselen van **+DC en –DC** kan de communicatiemodule vernielen – controleer de polariteit vóór het aansluiten.

Na het aansluiten moet in TrikdisConfig in het veld **System settings** → **Security panel model** het type van de aangesloten centrale worden gekozen (paragraaf 2.2); bij sommige fabrikanten is ook een instelling in de centrale nodig (hoofdstuk 4).

3.3.1 DSC PowerSeries

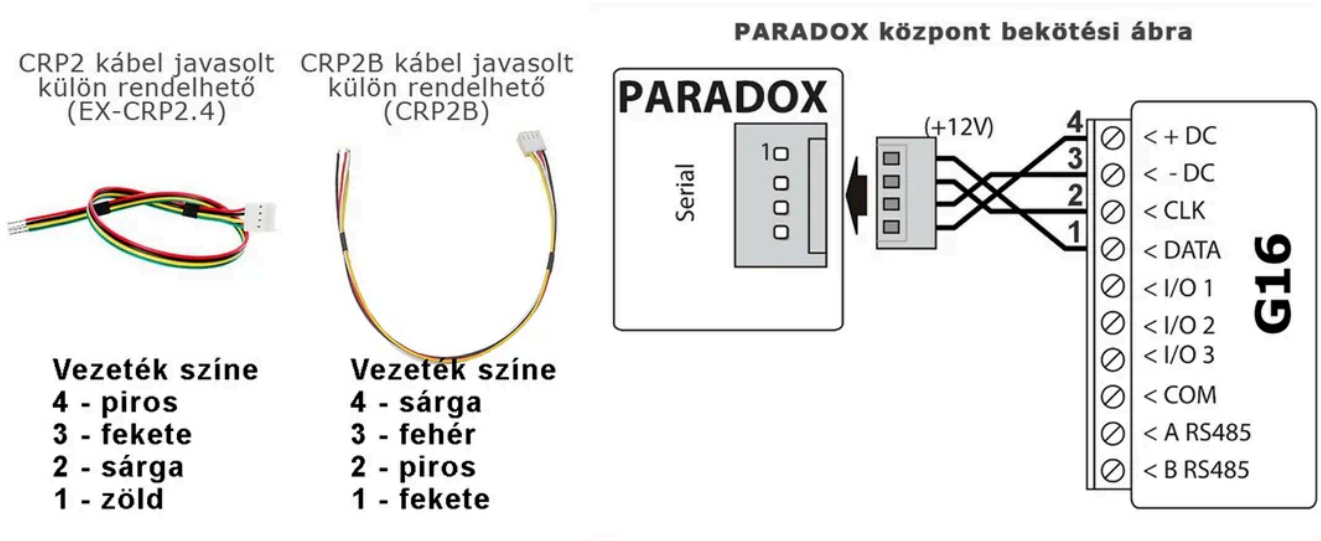
De vier klemmen van de Keybus: **RED** → +DC, **BLK** → –DC, **YEL** → CLK, **GRN** → DATA.



Afbeelding 12. Aansluiting op de Keybus van een DSC PowerSeries-centrale (bediendeelbus, „Keypad bus"): RED → +DC (+12 V), BLK → –DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

De communicatiemodule wordt aangesloten op de **seriële poort** (SERIAL) van Paradox-centrales met de fabriekskabel **CRP2** of **CRP2B**; het uiteinde aan de kant van de centrale past in de seriële connector, het andere uiteinde sluit u aan op het klemmenblok van de G16. De 4 pinnen van de connector: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. De aderkleuren van de twee kabels verschillen – het schema toont de kleurindeling van beide kabels. De aanduiding op de seriële connector van Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

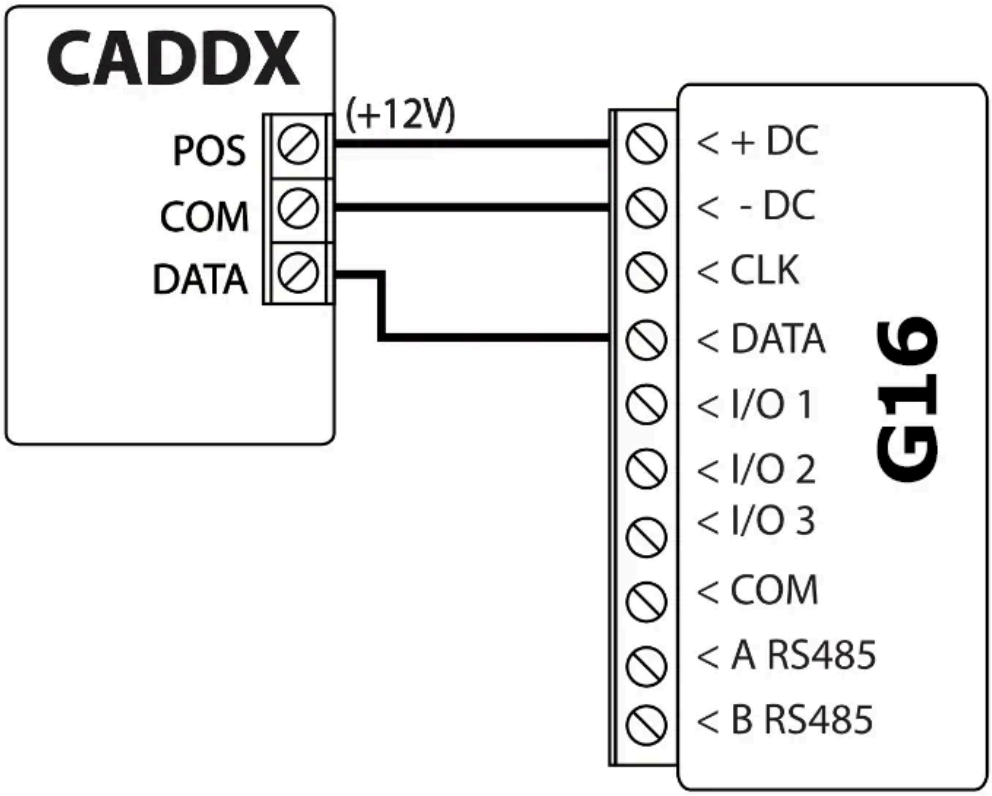


Afbeelding 13. Aansluiting op de seriële poort van een Paradox-centrale met een CRP2- (EX-CRP2.4) of CRP2B-kabel. CRP2: 4 rood → +DC, 3 zwart → −DC, 2 geel → CLK, 1 groen → DATA. CRP2B: 4 geel → +DC, 3 wit → −DC, 2 rood → CLK, 1 zwart → DATA.

Op de nieuwere Paradox-centrales kan de seriële poort af fabriek vergrendeld zijn – de manier van ontgrendelen staat in paragraaf 4.2 en in het artikel Een vergrendelde seriële poort ontgrendelen op Paradox-alarmcentrales.

3.3.3 UTC Interlogix (Caddx) NetworX

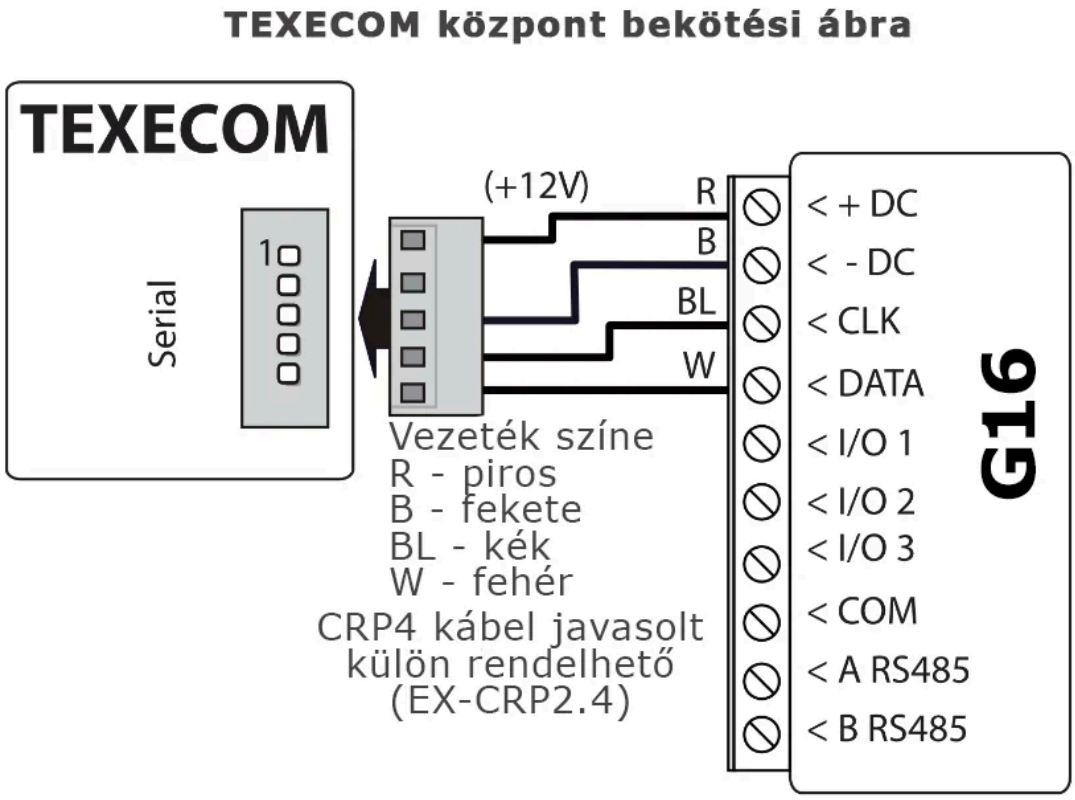
De drie klemmen van de bediendeelbus: **POS** → +DC, **COM** → −DC, **DATA** → DATA. De klem **CLK** wordt niet gebruikt.



Afbeelding 14. Aansluiting op de bediendeelbus van een Caddx NetworX-centrale („Keypad bus"): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK blijft vrij.

3.3.4 Texecom Premier / Premier Elite

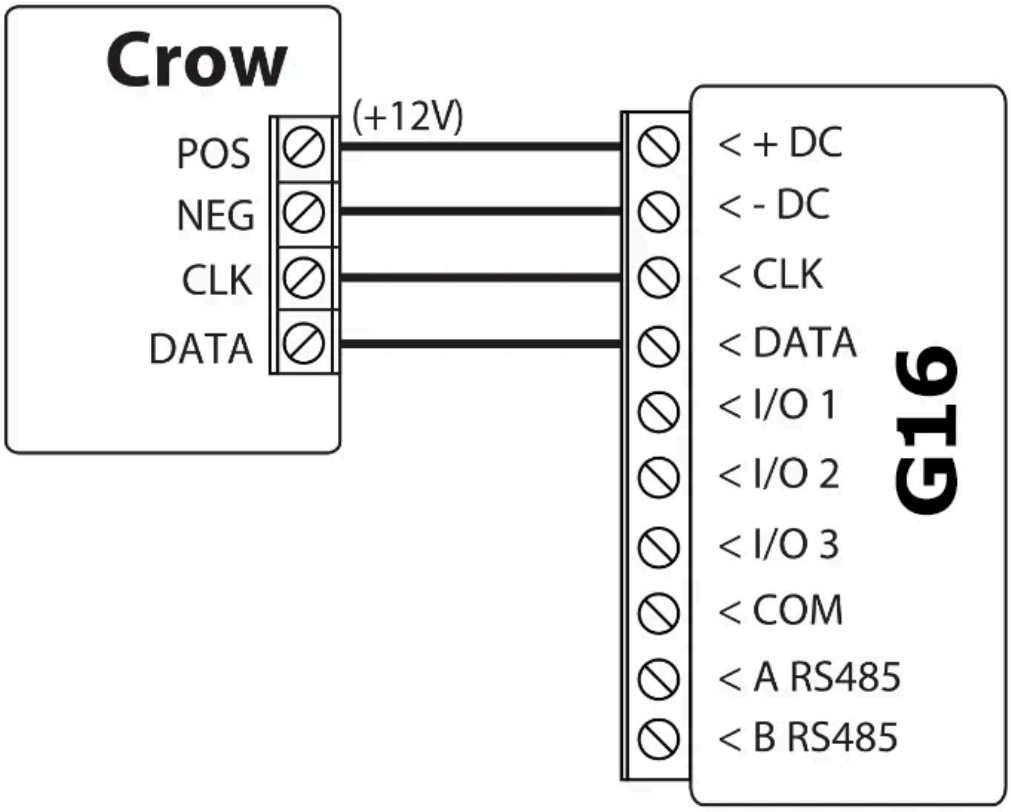
De communicatiemodule wordt met de fabriekskabel **CRP4** op de seriële poort van de centrale aangesloten: **rood (R)** → +DC, **zwart (B)** → −DC, **blauw (BL)** → CLK, **wit (W)** → DATA.



Afbeelding 15. Aansluiting op de seriële poort van een Texecom-centrale met een CRP4-kabel: rood → +DC, zwart → −DC, blauw → CLK, wit → DATA.

3.3.5 Crow Runner

De bediendeelbus van de Crow Runner 4/8 en Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.



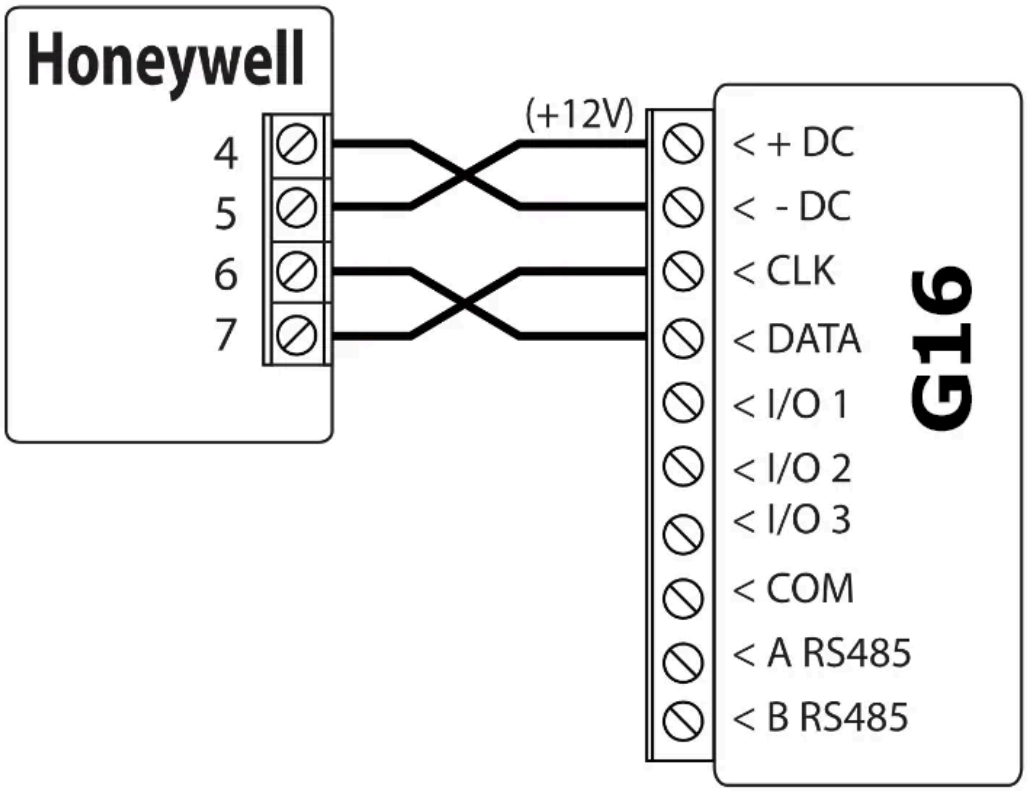
Afbeelding 16. Aansluiting op de bediendeelbus van een Crow Runner 4/8- en Runner 8/16-centrale („Keypad bus"): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

De bediendeelbus van Pyronix-centrales: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. De klem **CLK** wordt niet gebruikt. Maak de centrale na het aansluiten en het instellen van de communicatiemodule spanningsloos en start ze opnieuw, zodat ze de communicatiemodule accepteert (paragraaf 4.5).

3.3.7 Honeywell Ademco Vista

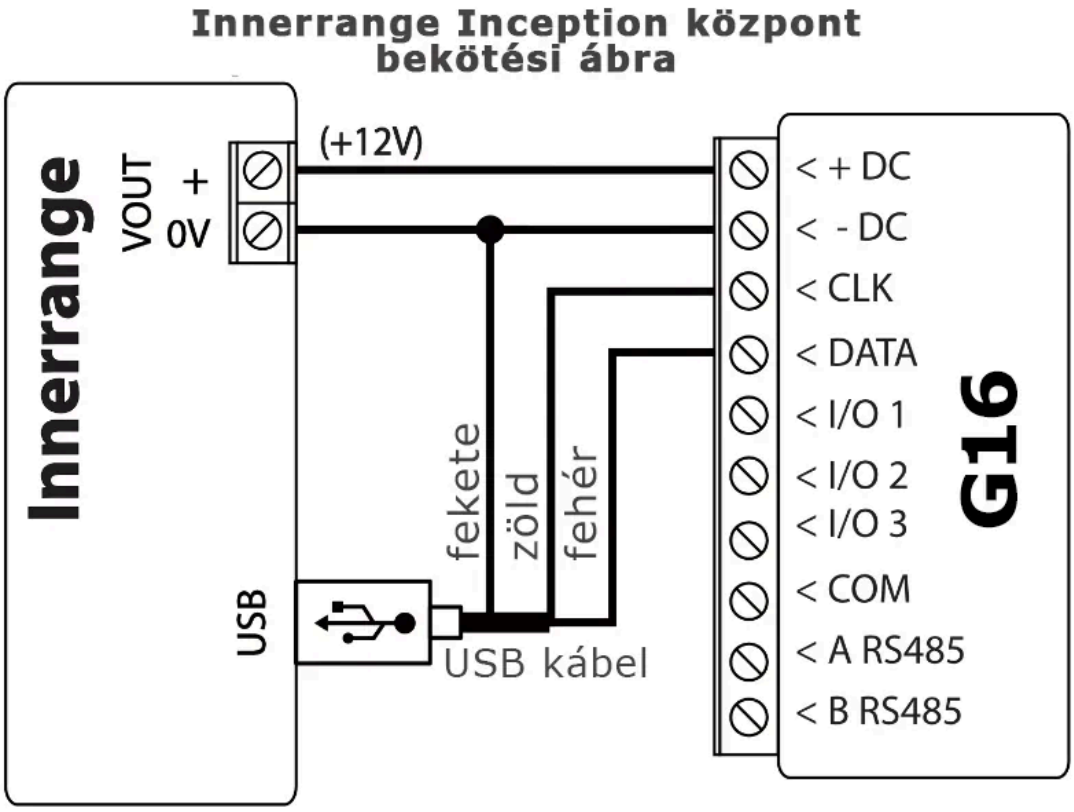
De genummerde klemmen van de bediendeelbus van de Vista-15-, Vista-20- en Vista-48-centrale: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (data-uitgang, geel) → CLK, **6** (data-ingang, groen) → DATA.



Afbeelding 17. Aansluiting op de bediendeelbus van een Honeywell Vista-20- / Vista-48-centrale („Keypad bus"): 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception en Integriti

De communicatiemodule krijgt zijn voeding van de voedingsklemmen van de **Inception**-centrale (**VOUT +** → +DC, **0V** → −DC), en de dataverbinding loopt via de USB-poort van de centrale, met de InnerRange-kabel 993030USB: **zwart** → 0V (−DC), **groen** → CLK, **wit** → DATA. In de centrale moet het gebruik van de seriële poort worden ingeschakeld (paragraaf 4.7).

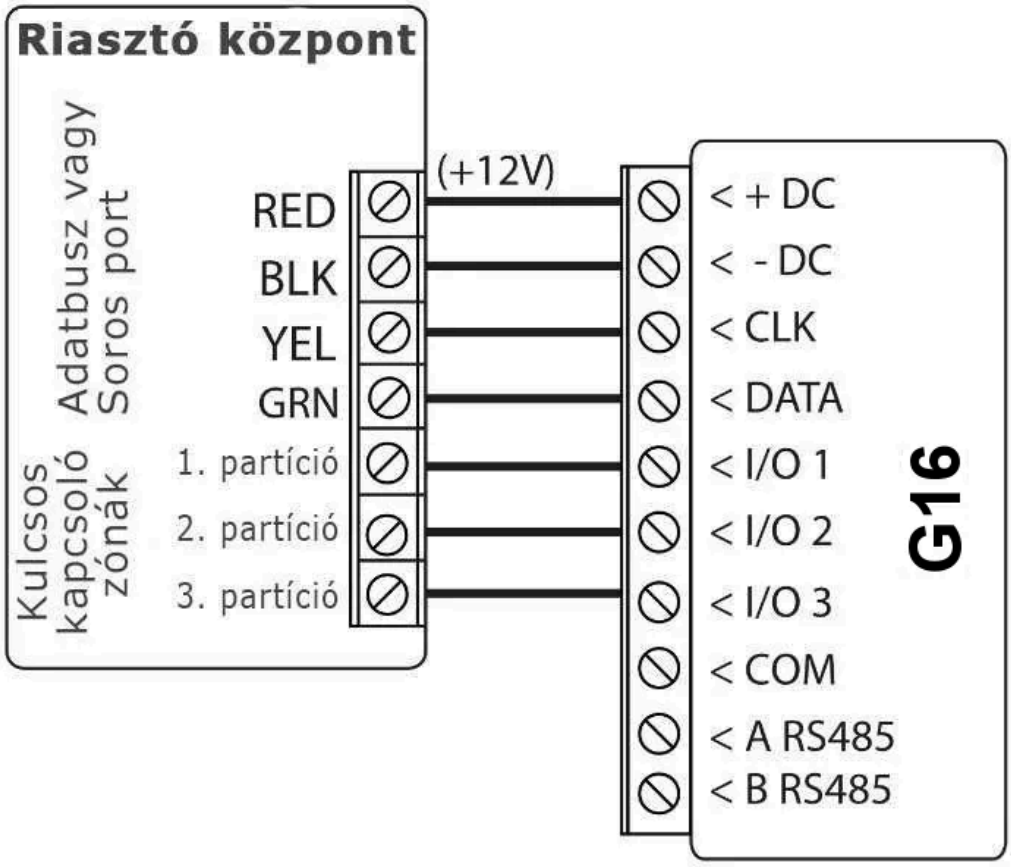


Afbeelding 18. Aansluiting op een InnerRange Inception-centrale: voeding van de klemmen VOUT + en 0V, data van de USB-poort met de 993030USB-kabel (zwart → 0V, groen → CLK, wit → DATA).

Op poort 0 (Port 0) van de **Integriti**-centrale kan hij worden aangesloten met de INTG-996795-kabel: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Aansluiting van een sleutelschakelaarzone

Als de centrale niet tot de direct bestuurbare types behoort, of als u de directe besturing niet wilt gebruiken, kan het in- en uitschakelen op afstand worden opgelost met een **sleutelschakelaarzone**: u stelt een van de I/O-klemmen van de communicatiemodule in als **uitgang** (pagina IN/OUT, paragraaf 6.6) en sluit die aan op een sleutelschakelaarzone van de centrale. Bij activering trekt de uitgang de zone naar COM (negatief); sluit de eindweerstand van de zone aan volgens het zonetype van de centrale. Omdat de G16 drie I/O-klemmen heeft, kunnen tot drie partities elk met een eigen uitgang worden bediend.



Afbeelding 19. In- en uitschakelen met een sleutelschakelaarzone: de communicatiemodule leest de gebeurtenissen van de bus van de centrale, en uitgang I/O 1–3 schakelt de sleutelschakelaarzone van partitie 1–3 van de centrale.

- Op de pagina **System settings** van TrikdisConfig moet **Remote Arm/Disarm leeg** blijven – de twee kunnen niet tegelijk worden gebruikt.
- De sleutelschakelaarzone kan pulserend of tweestandig zijn; in de Protegus 2-app moet dezelfde modus worden ingesteld (paragraaf 5.3).
- Op **hardwareversie 3** kunnen de twee uitgangen (OUT1, OUT2) twee partities bedienen; het veld **System settings** → **Output OUT1 & OUT2 mode** moet op **Remote control** (fabrieksinstelling) staan.

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 Aansluiting van ingangen

De I/O-klemmen van de communicatiemodule kunnen als ingang ook worden gebruikt voor extra detectoren (bv. sabotageschakelaar, paniekknop, temperatuurschakelaar), onafhankelijk van de alarmcentrale. De ingang moet tussen de gekozen I/O-klem en de COM-klem worden aangesloten.

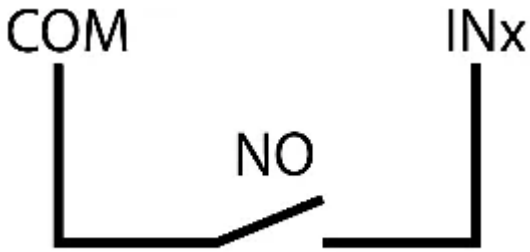
De ingangen accepteren de volgende kringtypen: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. De eindweerstand is **2,2 kΩ**. Bij enkelvoudige afsluiting (EOL) gelden zowel kortsluiting als onderbreking als alarm; dubbele afsluiting (DEOL) met twee weerstanden herkent alarm en sabotage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

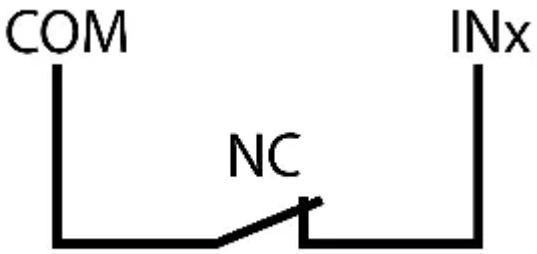
Type	Ruststand	Alarm	Sabotage
NO	open	gesloten	–
NC/EOL	2,2 kΩ	onderbreking of kortsluiting	–
NO/EOL	2,2 kΩ	kortsluiting of onderbreking	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	onderbreking of kortsluiting
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	onderbreking of kortsluiting

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.

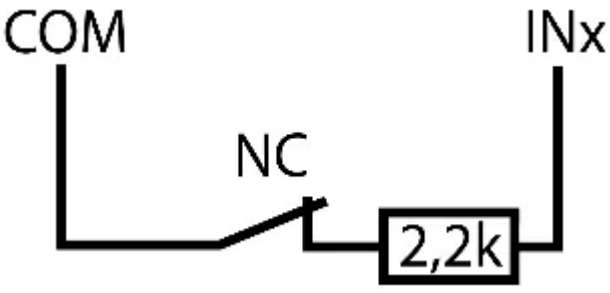
Aansluiting van ingangscircuits: types NO, NC, NC/EOL, NO/EOL, NO/DEOL en NC/DEOL met een eindweerstand van 2,2 kΩ; bij de DEOL-types is ook het sabotagecircuit aangesloten.



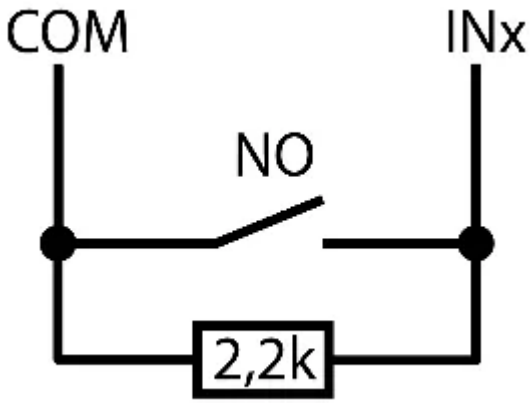
Afbeelding 20. NO – in rust open circuit: gesloten – alarm, open – rusttoestand.



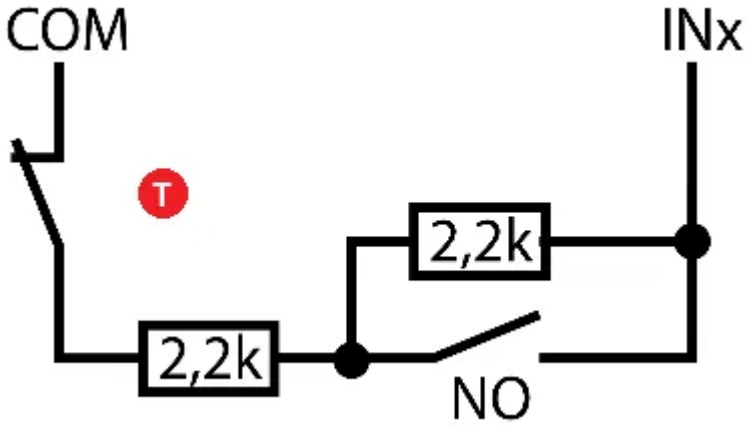
Afbeelding 21. NC – in rust gesloten circuit: open – alarm, gesloten – rusttoestand.



Afbeelding 22. NC/EOL – in rust gesloten circuit met een eindweerstand van 2,2 kΩ: kortsluiting of onderbreking – alarm, 2,2 kΩ – rusttoestand.

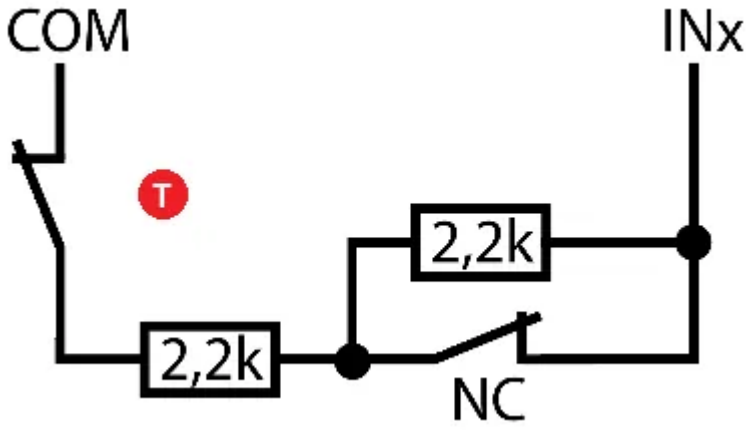


Afbeelding 23. NO/EOL – in rust open circuit met een eindweerstand van 2,2 kΩ: kortsluiting of onderbreking – alarm, 2,2 kΩ – rusttoestand.



Afbeelding 24. NO/DEOL – in rust open circuit met een eindweerstand van 2,2 kΩ en sabotagedetectie: kortsluiting of onderbreking – sabotage, 2,2 kΩ – alarm, 3,3–5,5 kΩ – rusttoestand.

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



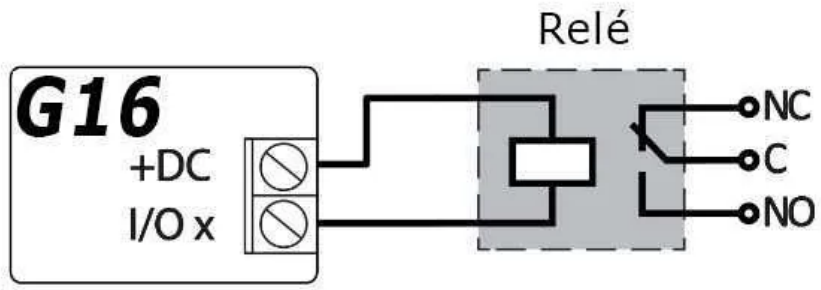
Afbeelding 25. NC/DEOL – in rust gesloten circuit met een eindweerstand van 2,2 kΩ en sabotagedetectie: kortsluiting of onderbreking – sabotage, 2,2 kΩ – rusttoestand, 3,3–5,5 kΩ – alarm.

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

Op **hardwareversie 3** is er één ingang (IN); het type stelt u in het veld **System settings** → **Input IN type** in.

3.6 Aansluiting van een uitgang met een relais

Als uitgang zijn de I/O-klemmen open-collectoruitgangen (OC): in actieve toestand trekken ze de aangesloten belasting naar de negatieve pool, met maximaal 0,15 A, tot 30 V DC. Schakel een grotere verbruiker of een apparaat op netspanning **via een relais**: het ene uiteinde van de relaisspoel komt op +DC, het andere op de I/O-klem. Met de contacten van het relais kunnen allerlei elektrische apparaten worden in- en uitgeschakeld. Hiervoor moet de I/O-klem op de pagina **IN/OUT** van TrikdisConfig als uitgang (**OUT**) worden ingesteld (paragraaf 6.6).

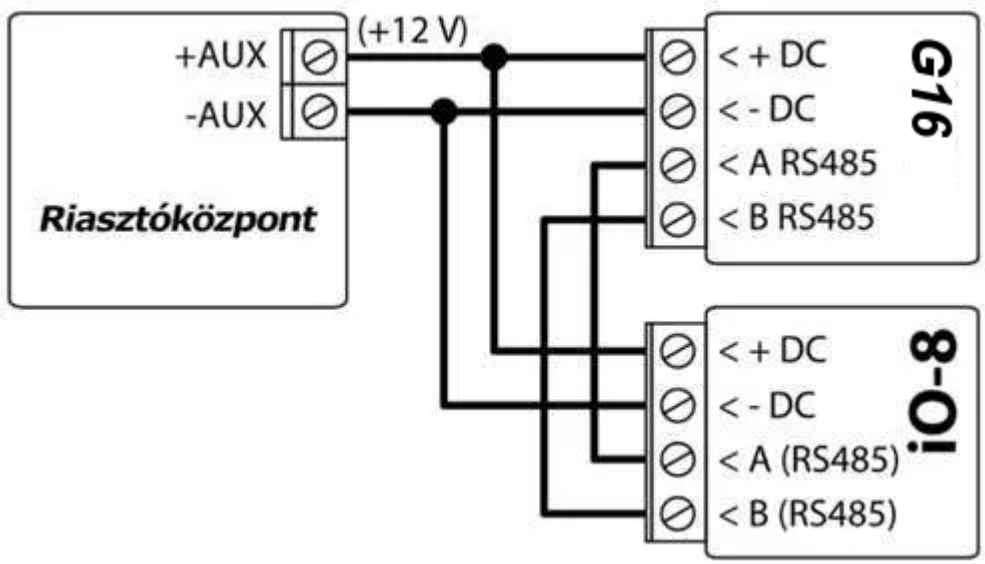


Afbeelding 26. Aansluiting van een relais op de uitgang van de communicatiemodule: de spoel komt tussen de klemmen +DC en I/O x, de contacten (NC, C, NO) schakelen de verbruiker.

De uitgangen kunt u schakelen vanuit de Protegus 2-app of met een sms-commando (hoofdstuk 5).

3.7 Aansluiting van een iO-8-uitbreiding

Als er meer in- of uitgangen nodig zijn, kunnen op de RS485-bus van de **4G-versie** maximaal vier **iO-8**-uitbreidingen worden aangesloten; elke uitbreiding geeft 8 extra I/O's met dubbele functie. Verbind de klemmen A 485 en B 485 met de klemmen A en B van de module, en neem de voeding van de module van de 12 V-AUX-uitgang van de centrale. De manier van aansluiten staat ook in de eigen handleiding van de iO-8. De module moet op de pagina **RS485 modules** van TrikdisConfig worden toegevoegd (paragraaf 6.7); de gebeurtenissen van de ingangen gaan naar de meldkamer en naar Protegus 2, de uitgangen kunnen vanuit de app worden geschakeld.



Afbeelding 27. Aansluiting van een iO-8-uitbreiding op de RS485-bus van de G16 (A 485 → A, B 485 → B); beide apparaten krijgen hun voeding van de AUX-uitgang van de alarmcentrale (+12 V).

De G16 met 2G-modem (G16_G410) heeft geen RS485-bus, daarom kunnen er geen iO-8-, W485- en E485-modules op worden aangesloten.

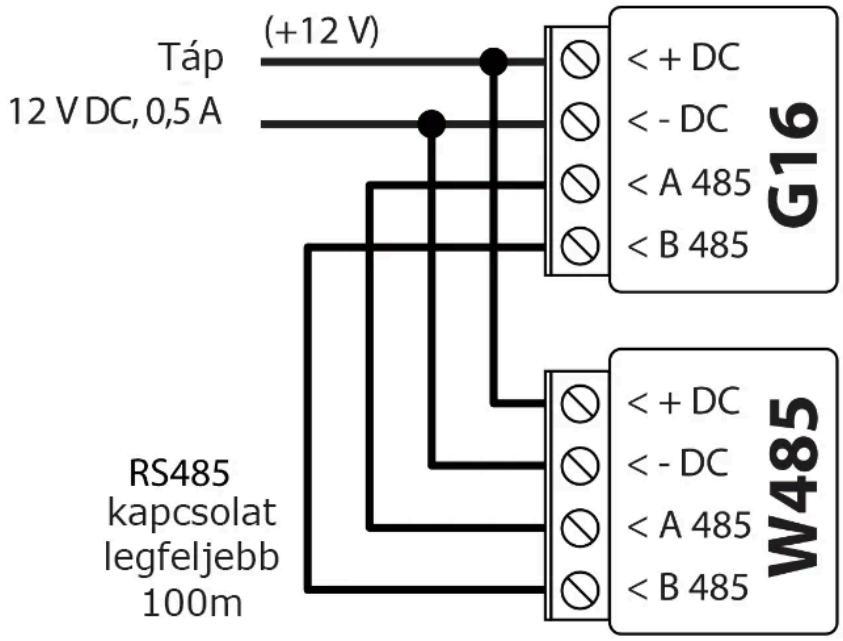
3.8 Aansluiting van de W485- en E485-module

Uitbreiding met Ethernet of wifi – W485 en E485. De communicatiemodule kan worden aangevuld met een W485-wifimodule of een E485-Ethernetmodule: de gebeurtenissen gaan dan via bekabeld internet of wifi naar de meldkamer en naar de Protegus 2-app.

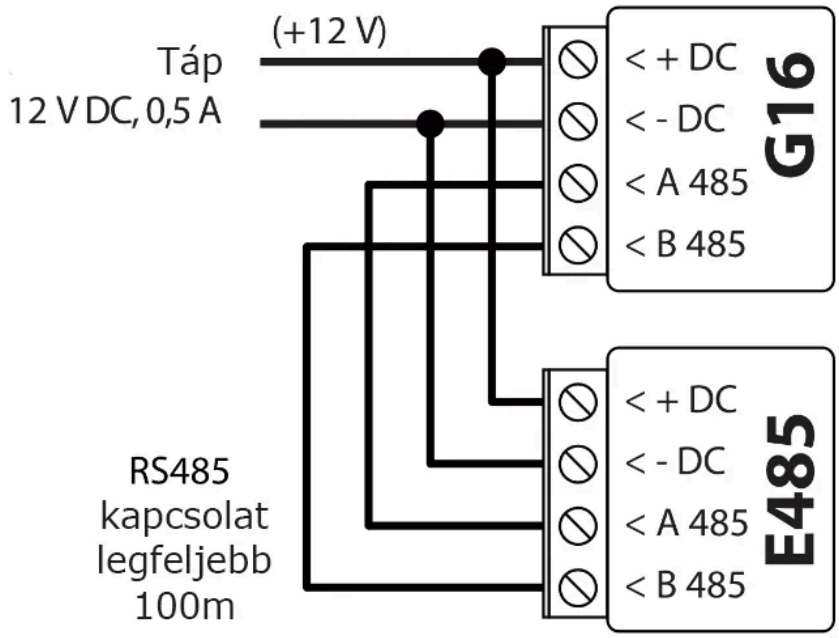
- **Aansluiting:** via de RS485-bus, op dezelfde voeding als de communicatiemodule (voedingsingang van de module 9–28 V DC); een aparte voeding is niet nodig.
- **Internet is het primaire kanaal:** zolang het werkt, gaat alles daarover. Valt het weg, dan schakelt de communicatiemodule vanzelf over op het mobiele netwerk, en zodra het internet terug is, keert ze terug naar IP.
- **Niet alleen doormelding:** ook de Protegus 2-app (meldingen, bediening op afstand) werkt via dit kanaal.
- **E485** – bekabeld Ethernet (RJ45). **W485** – wifi 2,4 GHz (WPA / WPA2), waar geen UTP-kabel is getrokken.
- Indien gewenst ook zonder simkaart te gebruiken. Instellen: met de TrikdisConfig-software, via USB.

Trikdis E485 Ethernet-module (RS485) **Trikdis W485 WiFi module (RS485)**

Zolang de WiFi- resp. Ethernetverbinding actief is, communiceert de G16 daarlangs en gebruikt hij de mobiele dataverbinding niet; als de verbinding wegvalt, schakelt hij over naar de mobiele dataverbinding, en wanneer de verbinding is hersteld, keert hij terug naar de module. Voor de werking van de module **moet er een simkaart in de G16 zitten**.



Afbeelding 28. Aansluiting van de W485 WiFi-module op de G16 via de RS485-bus. Beide apparaten werken op een gemeenschappelijke voeding van 12 V DC (minimaal 0,5 A) (de voedingsingang van de module is 9–28 V DC); de RS485-kabel mag maximaal 100 m lang zijn.



Afbeelding 29. Aansluiting van de E485 Ethernet-module op de G16 via de RS485-bus. Beide apparaten werken op een gemeenschappelijke voeding van 12 V DC (minimaal 0,5 A) (de voedingsingang van de module is 9–28 V DC); de RS485-kabel mag maximaal 100 m lang zijn.

De afstanden "tot ... m" zijn theoretische maximumwaarden die onder ideale omstandigheden haalbaar zijn. In de praktijk zorgen de kwaliteit en het traject van de kabel, storingsbronnen en bij radioverbindingen muren en terrein voor een duidelijk kleiner bereik. Reken met marge en controleer bij lange afstanden de verbinding bij de inbedrijfstelling.

De netwerkinstellingen van de modules doet u op de pagina **RS485 modules** van TrikdisConfig (paragraaf 6.7).

3.9 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 de communicatiemodule mee wanneer de alarmcentrale wordt ingeschakeld. Op het frontdeksel moet u het volgende zien:

- **POWER** brandt groen – de voeding is in orde;
- **NETWORK** brandt groen en knippert geel – verbonden met het netwerk; het aantal knipperingen is het signaalniveau (op 2G is 5, op 4G is 3 goed);
- **TROUBLE** is uit.

Als de NETWORK-led minder gele knipperingen geeft, is het signaalniveau onvoldoende: zoek een andere plek voor de communicatiemodule, of gebruik een gevoeligere antenne (paragraaf 3.2). Elke andere led-indicatie wijst op een storing – stel die vast aan de hand van de tabellen in paragraaf 1.7. Als TROUBLE knippert, geeft het aantal knipperingen de oorzaak aan (paragraaf 1.7). **7 knipperingen** betekent dat er geen verbinding met de centrale is: controleer de CLK- en DATA-draad, het gekozen type centrale en – waar nodig – de programmering van de centrale (hoofdstuk 4). Als geen enkele led brandt, controleer dan de voeding en de bedrading.

4. Programmeren van de alarmcentrale

Dit hoofdstuk beschrijft per fabrikant wat er in de alarmcentrale moet worden ingesteld zodat de G16 de gebeurtenissen kan uitlezen en – waar mogelijk – de centrale op afstand kan besturen. Bij de meeste centrales hoeft voor het uitlezen van gebeurtenissen niets te worden geprogrammeerd; vink voor de **directe besturing** op de pagina **System settings** van TrikdisConfig de optie **Remote Arm/Disarm** aan, en geef bij een Paradox- resp. Texecom-centrale ook het pc- resp. UDL-wachtwoord van de centrale op in het veld **Security panel PC download password** (paragraaf 2.2 en 6.2).

Als u de centrale niet direct, maar via een sleutelschakelaarzone bestuurt (paragraaf 3.4), moet **Remote Arm/Disarm** leeg blijven, en geldt dit hoofdstuk alleen voor de instellingen die nodig zijn voor het uitlezen van gebeurtenissen.

4.1 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.

4.2 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.

4.3 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]**.

4.4 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.

4.5 Crow en Pyronix

De centrales **Crow Runner 4/8** en **Runner 8/16** vereisen geen enkele aparte instelling.

Ook de **Pyronix**-centrales hoeven niet geprogrammeerd te worden, maar **maak de centrale na het instellen en aansluiten van de communicatiemodule spanningsloos** (net en accu) en start haar opnieuw: de centrale accepteert de op haar bus aangesloten communicatiemodule bij het opstarten.

4.6 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]**.

4.7 InnerRange Inception en Integriti

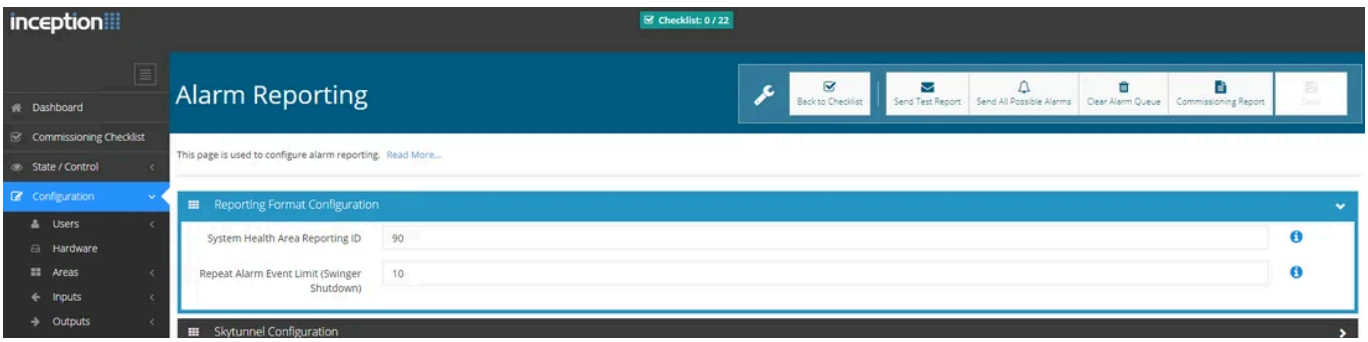
De firmware van de **InnerRange Inception**-centrale moet minimaal **2.3.0.3507-r0** zijn, en de centrale heeft een internetverbinding nodig. De instelling doet u in de webinterface van de centrale:

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.

De Inception en de Integriti geven de gebeurtenissen door aan de communicatiemodule; voor het in- en uitschakelen is een sleutelschakelaarzone nodig (paragraaf 1.2 en 3.4).



Afbeelding 30. Webinterface van de Inception – Configuration → General → Alarm Reporting.



Afbeelding 31. Inception – 3rd Party Device Configuration.

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

5. Bediening op afstand met de Protegus 2-app

Met de Protegus 2-app voor mobiel en web ziet de gebruiker op afstand de status van het systeem, krijgt hij meldingen van gebeurtenissen, kan hij in- en uitschakelen en kan hij de uitgangen van de communicatiemodule schakelen. Bij de G16 kan het inschakelen op twee manieren gebeuren: bij de **direct bestuurbare** centrales met de eigen **bediendeelcode** van de gebruiker, bij centrales die met een sleutelschakelaarzone zijn aangesloten met de **uitgang** van de communicatiemodule.

5.1 Het apparaat toevoegen

Controleer vóór het toevoegen van het apparaat:

1. De simkaart is actief en de mobiele dataverbinding werkt erop; de pincode is in het apparaat ingevoerd, of de pincodevraag is uitgeschakeld.
2. Op het tabblad **User reporting** → **PROTEGUS Cloud** van TrikdisConfig is **Enable connection** aangevinkt en is de **Protegus Cloud access code** ingesteld (na het aanmaken van het systeem kan die niet meer worden gewijzigd).
3. De **POWER**-led brandt groen, de **NETWORK**-led brandt groen en knippert geel.

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

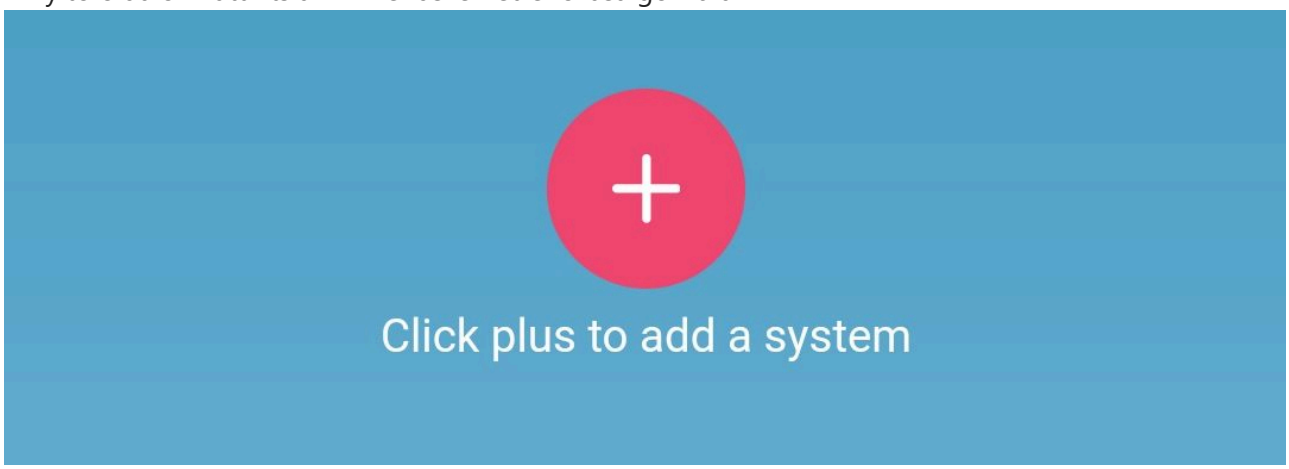
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

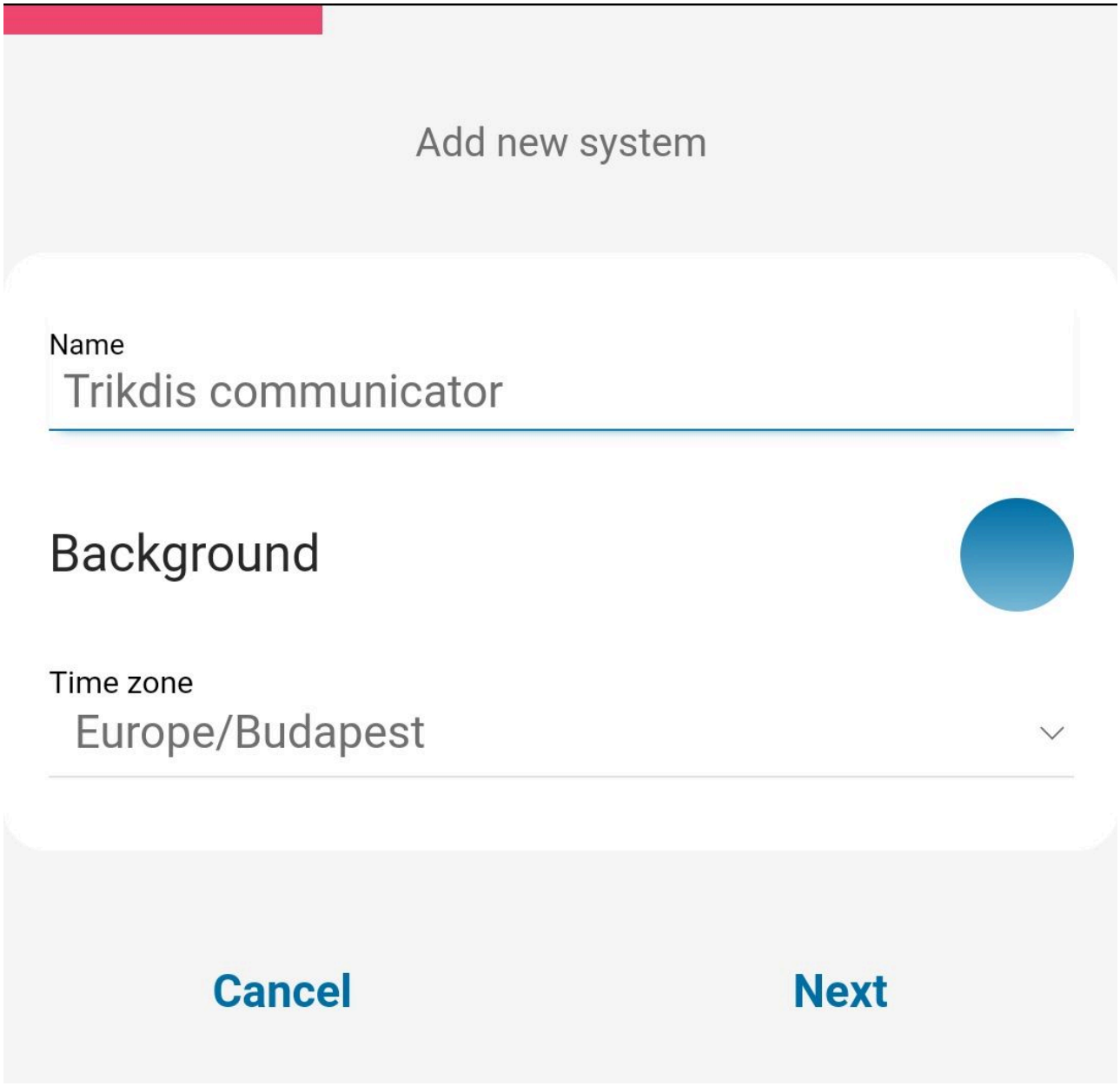
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



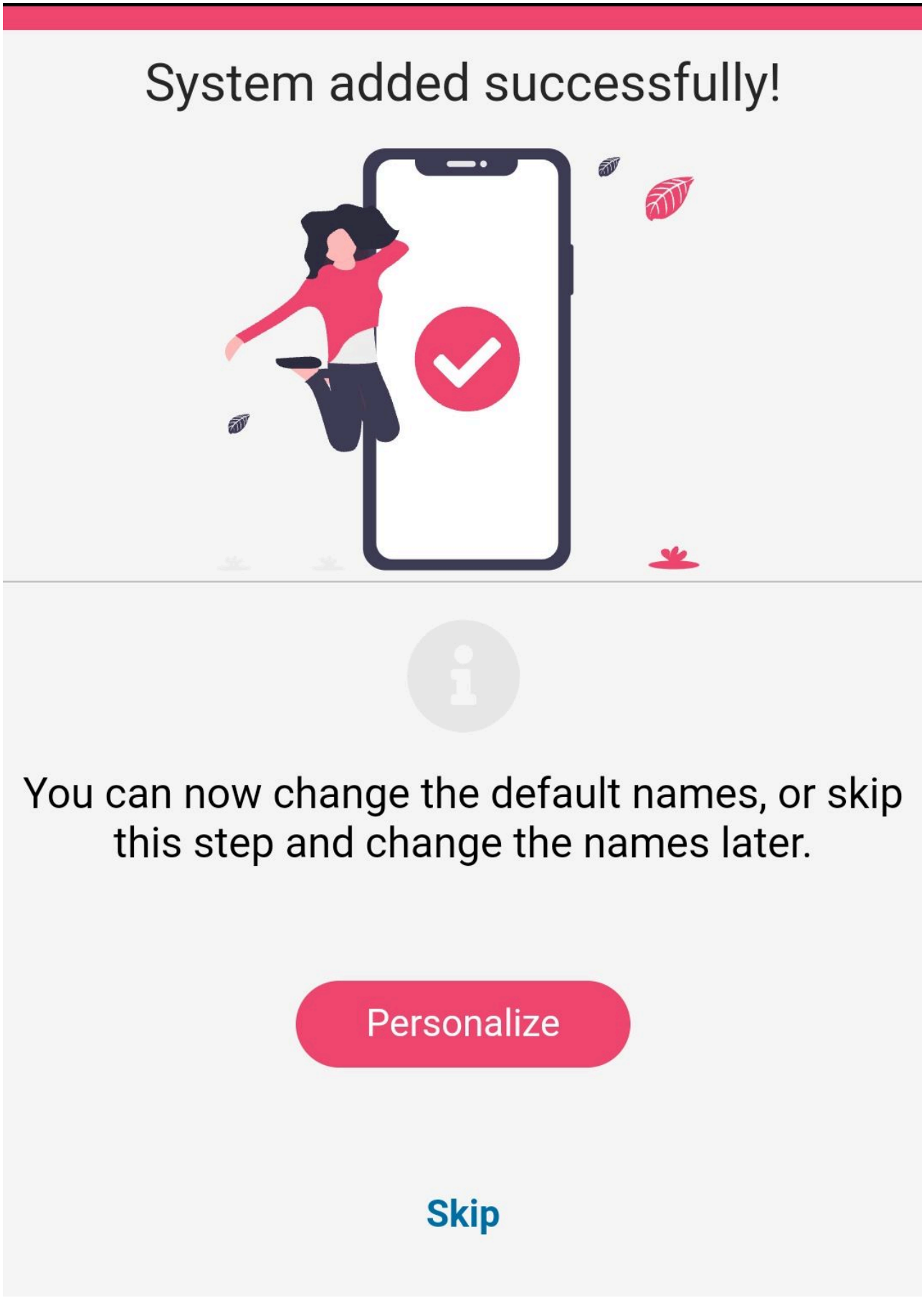
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



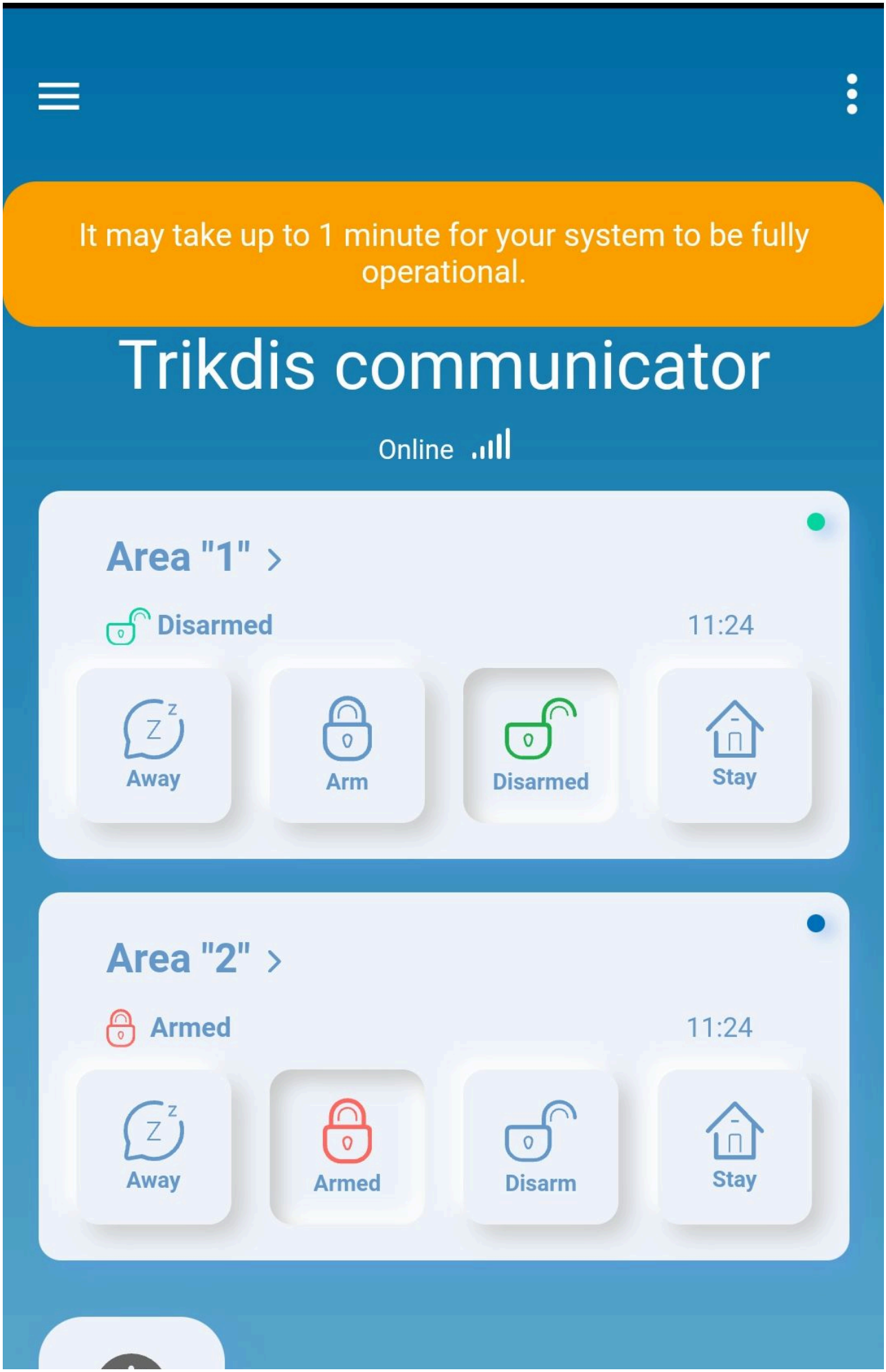
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



De unieke identificatie van het apparaat (**IMEI**) staat op de doos en op de achterkant van het apparaat, en wordt ook in de statusbalk van TrikdisConfig getoond.

5.2 Directe besturing met de bediendeelcode

Als de centrale tot de direct bestuurbare types behoort (paragraaf 1.2) en op de pagina **System settings** van TrikdisConfig **Remote Arm/Disarm** is aangevinkt, toont Protegus 2 de partities van de centrale met de status die van de bus wordt gelezen, en voert de gebruiker voor het in- / uitschakelen **de bediendeelcode van de centrale** in de app in – dezelfde die hij op het bediendeel gebruikt. Een aparte uitgang en sleutelschakelaarzone zijn niet nodig.

- Hiervoor is, afhankelijk van de fabrikant, een instelling in de centrale nodig (Paradox: pc-wachtwoord, Texecom: UDL-wachtwoord; bij Caddx-, Honeywell- en InnerRange-centrales het vrijgeven van de bus resp. de seriële poort, al voor het uitlezen van gebeurtenissen) – zie hoofdstuk 4.
- De bediendeelcode wordt door de centrale gecontroleerd, en ook het gebeurtenissenlogboek van de centrale registreert de gebruiker, niet de communicatiemodule.
- Bij een Paradox-centrale **mag de code van de gebruiker niet de mastercode zijn**; herstart de communicatiemodule na het wijzigen van een code (paragraaf 4.2).
- Bij een DSC PowerSeries-centrale toont de app ook de status van de zones, en is ook het overbruggen van zones mogelijk – details in het artikel over directe besturing van DSC.

Bij het aanmaken van het systeem vraagt Protegus 2 of het inschakelen door de uitgang van de communicatiemodule wordt gestuurd. Wijs bij directe besturing **geen** uitgang toe aan de partitie (**Control with Protegus2** uitgeschakeld): de partitie wordt door de centrale beheerd, de status komt van de bus.

5.3 Inschakelen met een sleutelschakelaarzone

Als de centrale niet direct bestuurbaar is, of als u ze niet zo wilt gebruiken, sluit u een van de uitgangen van de communicatiemodule aan op de sleutelschakelaarzone van de centrale (paragraaf 3.4), blijft **Remote Arm/Disarm** in TrikdisConfig leeg, en wijst u in Protegus 2 de uitgang toe aan de partitie.

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.

5.4 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.

Bij directe besturing vraagt de app om de bediendeelcode van de centrale; bij inschakelen met een sleutelschakelaar – als dat is ingeschakeld – om het wachtwoord van Protegus 2.

5.5 Bediening met sms-berichten

De communicatiemodule kan ook met sms-berichten worden bediend en geprogrammeerd. Opbouw van het bericht:

`WACHTWOORD spatie OPDRACHT spatie GEGEVENS` – bijvoorbeeld `123456 OUTPUT1 ON`

Met het **beheerderswachtwoord** kunnen alle opdrachten worden gebruikt, met het **installateurswachtwoord** de opdrachten INFO, RESET en OUTPUTx. De `x` is het nummer van de uitgang: de als uitgang ingestelde I/O-klem (1, 2 of 3) die u wilt schakelen.

Opdracht	Gegevens	Wat het doet	Voorbeeld
`INFO`	–	Vraagt informatie over het apparaat op: type, IMEI, serienummer, firmwareversie	`123456 INFO`
`RESET`	–	Start het apparaat opnieuw	`123456 RESET`
`OUTPUTx`	`ON`	Schakelt uitgang x in	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Schakelt uitgang x uit	`123456 OUTPUT1 OFF`

Opdracht	Gegevens	Wat het doet	Voorbeeld
`OUTPUTx`	`PULSE=tttt`	Geeft een puls op uitgang x; `tttt` = de pulsduur in seconden, met vier cijfers	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Schakelt de Protegus-verbinding in of uit	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adres:poort`	IP-adres en poort van het primaire kanaal	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=sleutel`	De TRK-coderingssleutel	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=naam`	De APN van de simkaart	`123456 CONNECT APN=internet`
`CONNECT`	`USER=naam`	APN-gebruikersnaam (als de provider daarom vraagt)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=wachtwoord`	APN-wachtwoord (als de provider daarom vraagt)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Kiest het type alarmcentrale met het volgnummer uit de lijst **Security panel model** van TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=cccc` / `DIR=OFF`	Het 4-cijferige wachtwoord voor rechtstreekse bediening (het pc- of UDL-wachtwoord van de centrale); `DIR=OFF` schakelt het uit	`123456 CONNECT DIR=1122`

U kunt beperken van welke telefoonnummers het apparaat opdrachten accepteert: TrikdisConfig → pagina **User reporting** → **Control by SMS**. Als er geen enkel nummer is opgegeven, voert het apparaat elke opdracht met het juiste wachtwoord uit, van welk nummer die ook komt.

6. TrikdisConfig – de instellingen in detail

Links in het TrikdisConfig-venster staat de lijst met pagina's (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), bovenaan de knoppenbalk (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) en onderaan de statusbalk. Dit hoofdstuk behandelt de instellingen van de G16 pagina voor pagina.

6.1 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.
Device	Het type (typeaanduiding) van het apparaat. Controleer of hier het type van uw eigen apparaat staat.

Opschrift	Betekenis
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.

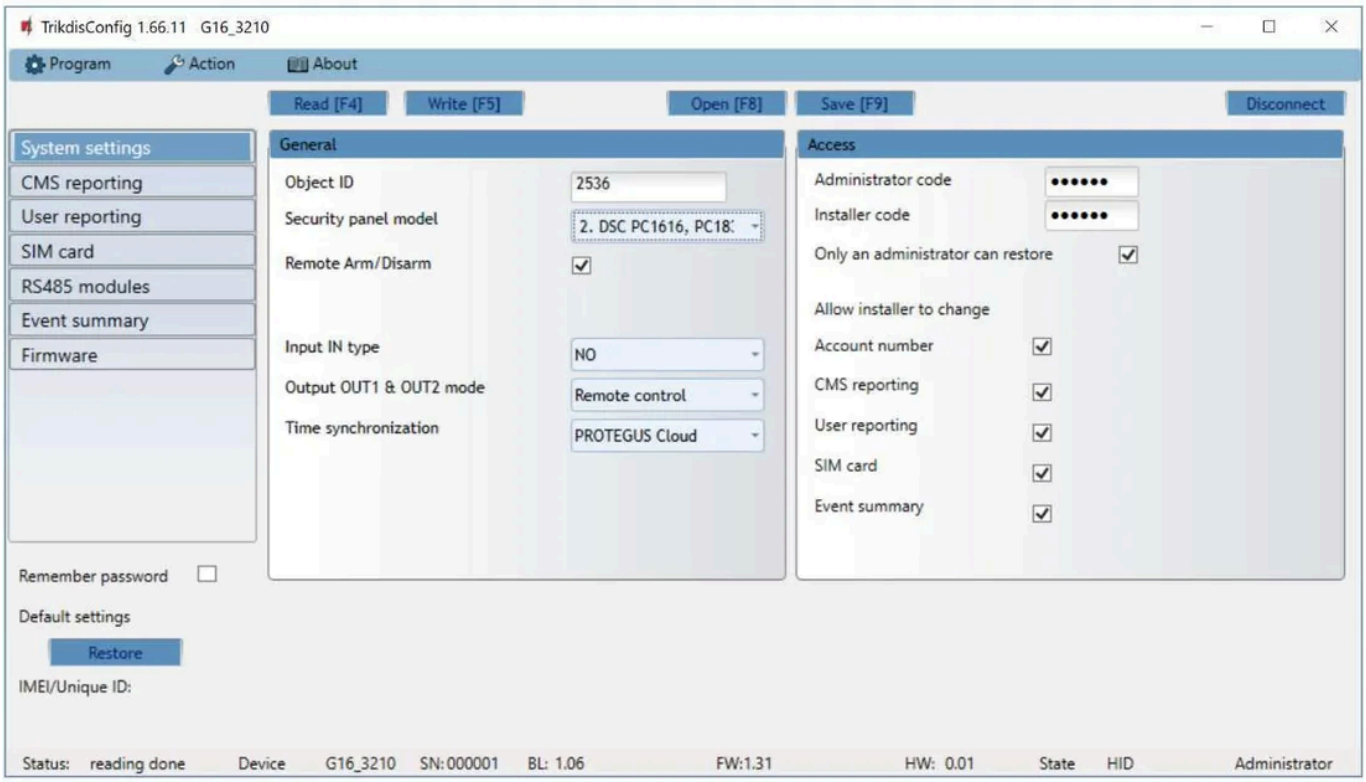
In het veld **Device** moet bij de G16 de typeaanduiding van de G16 staan (bijvoorbeeld G16_G410 of G16_54E0). Na het uitlezen toont het programma de instellingen die in de G16 zijn opgeslagen; stel ze in volgens de onderstaande beschrijvingen per pagina.



Afbeelding 32. De statusbalk van TrikdisConfig met een uitgelezen G16: identificatie, status, type, serienummer, versies, verbindingswijze en toegangsniveau.

6.2 System settings

De pagina bestaat uit twee groepen: in de groep **General** stelt u de basiswerking van het apparaat en de verbinding met de alarmcentrale in, in de groep **Access** de toegangsniveaus.



Afbeelding 33. TrikdisConfig – pagina System settings: groep General en Access (op de afbeelding hardwareversie 3, G16_3210; op versie 4 zijn er geen velden Input IN type en Output OUT1 & OUT2 mode, die staan op de pagina IN/OUT).

- **Object ID** – het objectnummer dat u van de meldkamer hebt gekregen (4 hexadecimale tekens, 0–9, A–F). Verplicht als het apparaat ook naar een meldkamer meldt; `FFFE` en `FFFF` kunnen niet worden gebruikt.
- **Security panel model** – het type van de aangesloten alarmcentrale uit de lijst. Hiervan hangt af hoe de communicatiemodule de bus uitleest, kies daarom het exacte type van de aangesloten centrale.
- **Remote Arm/Disarm** – aangevinkt bestuurt de communicatiemodule de centrale direct: de gebruiker schakelt vanuit Protegus 2 in en uit met zijn bediendeelcode. Verschijnt alleen bij de direct bestuurbare types centrale; afhankelijk van de fabrikant is er een instelling in de centrale voor nodig (hoofdstuk 4). Laat het vakje leeg bij inschakelen met een sleutelschakelaarzone.
- **Security panel PC download password** – voor directe besturing van een Paradox- en Texecom-centrale het pc- resp. UDL-wachtwoord van de centrale (4 tekens); dit moet overeenkomen met het wachtwoord dat in de centrale is ingesteld (paragraaf 4.2 en 4.3).
- **Time set** – de bron van de klok van het apparaat (standaard **Cloud application**, de Protegus-cloud).
- Op **hardwareversie 3** staan hier ook het veld **Input IN type** (het type ingang: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) en het veld **Output OUT1 & OUT2 mode** (de modus van de twee uitgangen; voor inschakelen met een sleutelschakelaar **Remote control**).

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.

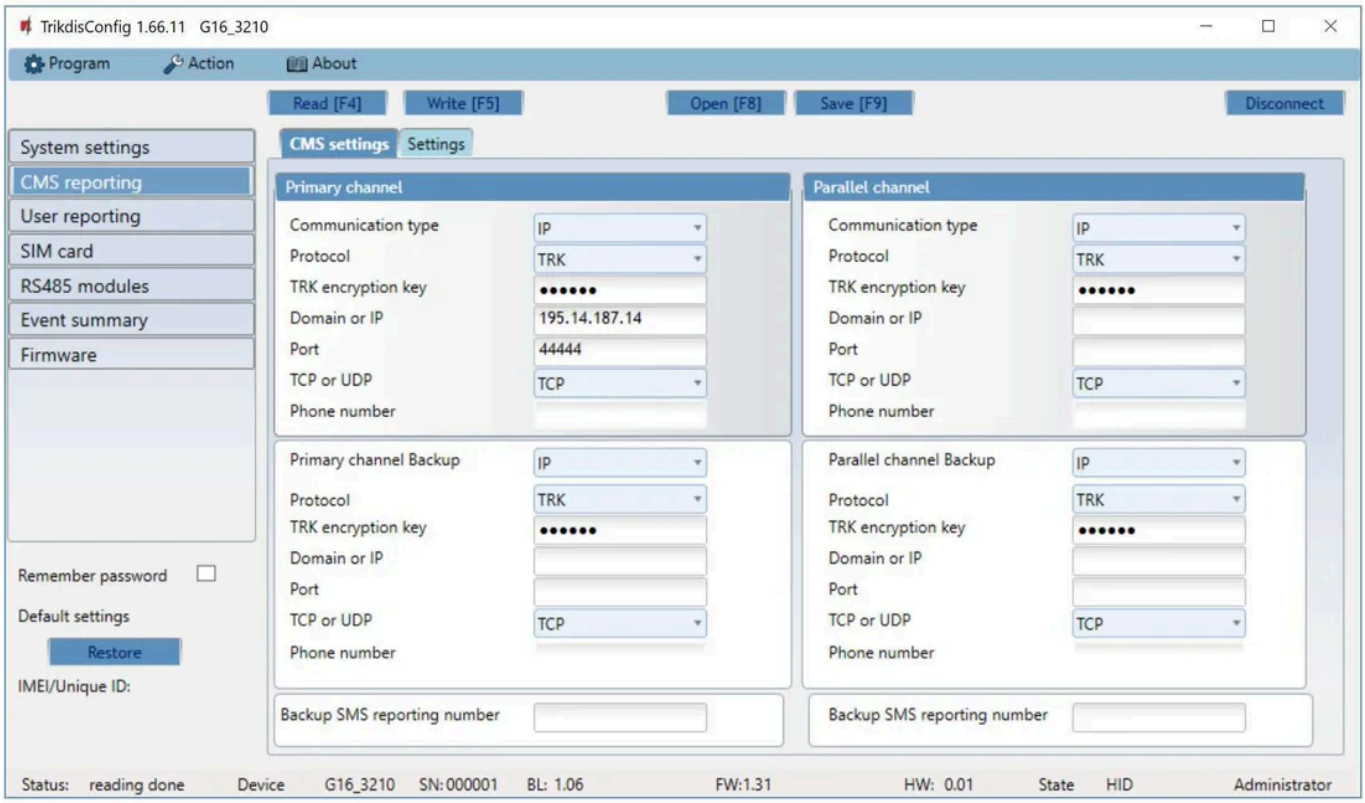
- **Allow installer to change** – hier geeft u aan welke instellingsgroepen de installateur mag wijzigen: **Account number** (objectnummer), **CMS reporting**, **User reporting**, **SIM card** (bij een apparaat met mobiel netwerk) of **Ethernet settings** (bij een Ethernet-apparaat), **Event summary**.

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.

6.3 CMS reporting

De communicatiemodule stuurt de gebeurtenissen via de mobiele dataverbinding (IP) of per sms naar de meldkamer. De gebeurtenissen kunnen 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 wegvalt. De communicatie is versleuteld en met een wachtwoord beveiligd; voor de ontvangst is een Trikdis-ontvanger (IPcom-softwareontvanger, RL14, RM14) of een universele ontvanger die het DC-09- / TL150-protocol kent nodig. De Trikdis-ontvangers sturen de gebeurtenissen door naar de meldkamersoftware: via een IP-verbinding de **IPcom**-softwareontvanger (Windows / Linux), de **RL14** IP/sms-ontvanger of de **RM14** meerkanaalsontvanger; voor het ontvangen van sms de RL14, de RM14 of de **GM14** sms-ontvanger.



Afbeelding 34. TrikdisConfig – CMS reporting, tabblad CMS settings: primair, reserve- en parallel kanaal.

Primary channel – primair kanaal

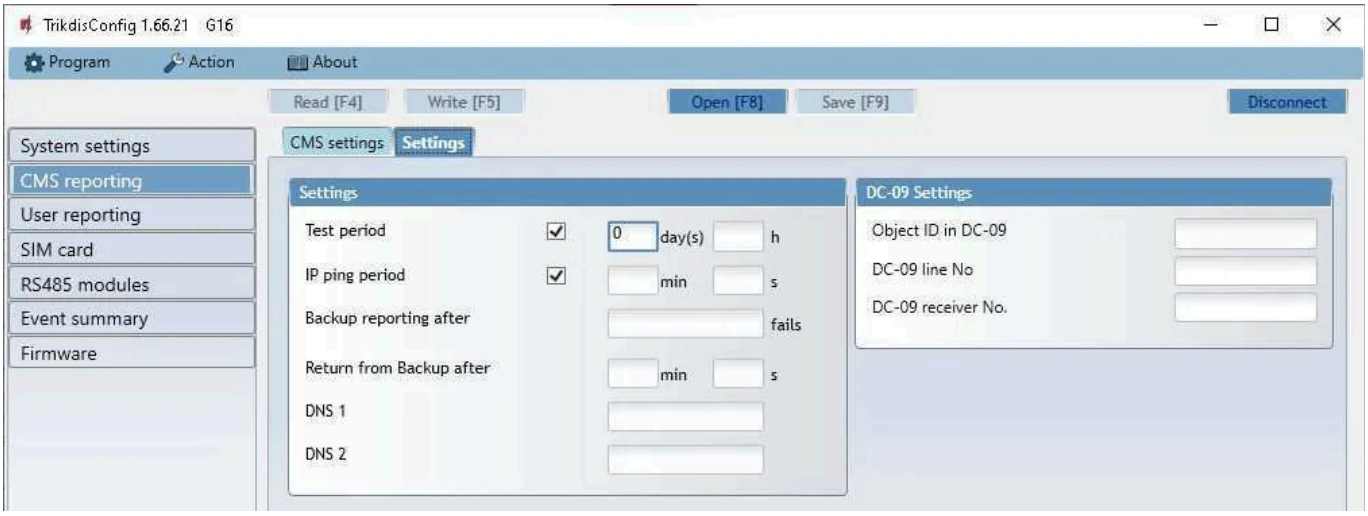
- **Communication type** – IP of sms. Sms is goed als reserve – het werkt ook als er geen mobiele dataverbinding is –, maar wordt als primair kanaal niet aanbevolen.

- **Protocol** – TRK (Trikdis-ontvangers), DC-09_2007 of DC-09_2012 (universele ontvangers), TL150 (SUR-GARD).
- **TRK encryption key** – 6-cijferige versleutelingssleutel; die moet in de communicatiemodule en in de ontvanger gelijk zijn.
- **Domain or IP**, **Port** – het adres en de poort van de ontvanger.
- **TCP or UDP** – het transportprotocol.
- **Phone number** – alleen bij communicatie per sms: het telefoonnummer van de Trikdis-sms-ontvanger met landcode (bv. `CCxxxxxxxxx`, waarbij CC de landcode is).

Primary channel Backup – reservekanaal. Neemt de communicatie over als het primaire kanaal niet werkt; de instellingen zijn dezelfde als hierboven.

Parallel channel – parallel kanaal. Stuurt naast het primaire kanaal tegelijk naar een tweede ontvanger (bijvoorbeeld de lokale en de centrale meldkamer). Heeft een eigen reservekanaal.

Backup SMS reporting number – reserve-sms-nummer. Treedt in werking als verzenden via het primaire, het parallelle en het reservekanaal niet lukt; het is nuttig omdat het ook zonder IP-verbinding werkt. Het is alleen actief als het primaire en het reservekanaal in IP-modus staan. Het apparaat stuurt een sms naar de sms-ontvanger van de meldkamer na de eerste start, en ook als de TCP/IP- of UDP/IP-verbinding op zowel het primaire kanaal als het bijbehorende reservekanaal wegvalt. Vul in het veld het telefoonnummer van de Trikdis-sms-ontvanger van de meldkamer in, met landcode (bv. `CCxxxxxxxxx`, waarbij CC de landcode is).



Afbeelding 35. TrikdisConfig – CMS reporting, tabblad Settings: testmelding, PING, tijden van het reservekanaal, DNS en de DC-09-gegevens.

Op het tabblad **Settings** stelt u de tijden en de DC-09-gegevens in.

- **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**.

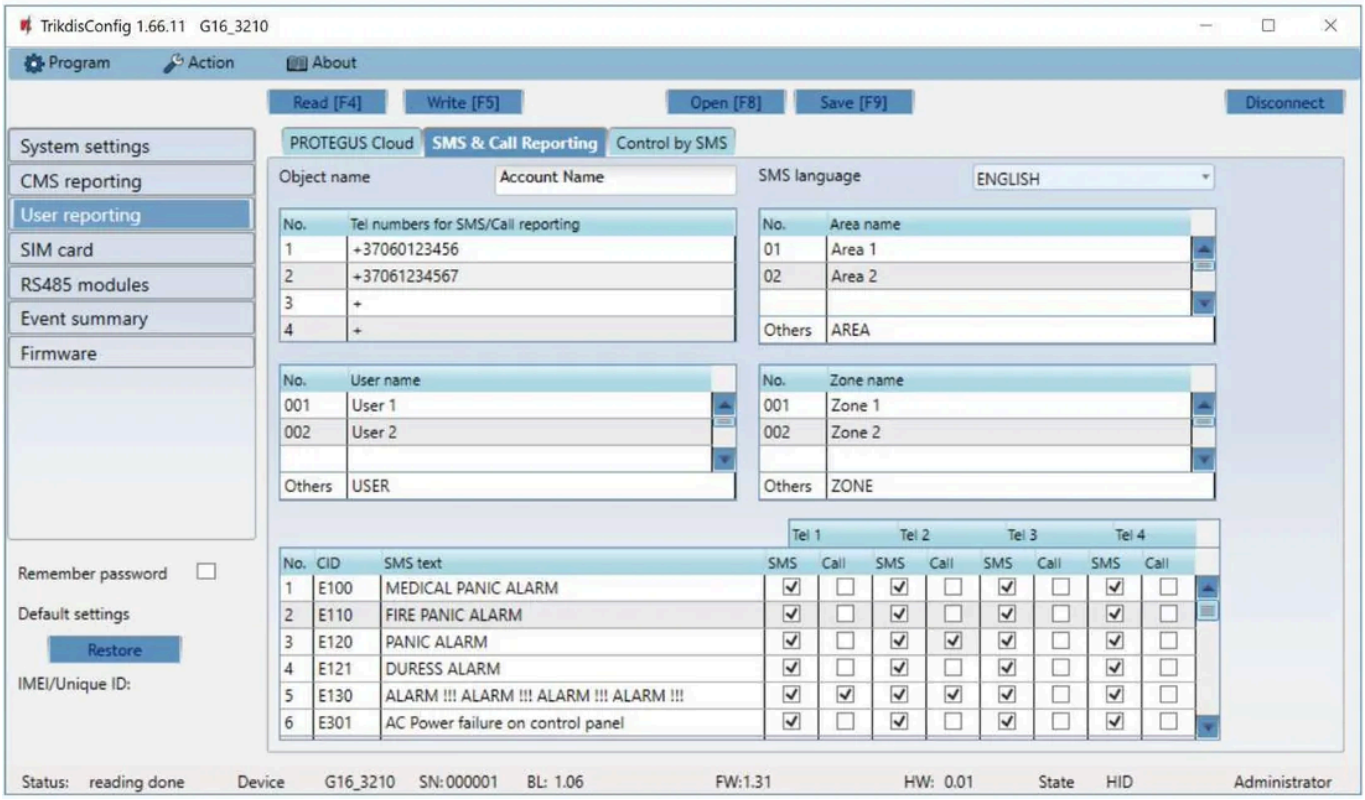
DC-09 Settings (rechts op het tabblad) – hoeft u alleen in te vullen als u op een van de kanalen met het protocol DC-09_2007 of DC-09_2012 verzendt; de groep verschijnt wanneer in het veld **Protocol** van een kanaal DC-09_2007 of DC-09_2012 is geselecteerd:

- **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.

Onderaan het tabblad: **DNS 1, DNS 2** – naamservers; die zijn nodig als u de ontvanger met een domeinnaam en niet met een IP-adres hebt opgegeven. Standaard is dat de openbare DNS van Google. De groep **DC-09 settings** is alleen zichtbaar als op een van de kanalen het DC-09-protocol is ingesteld.

6.4 User reporting

Op het tabblad **PROTEGUS Cloud** schakelt u de Protegus-dienst in. Met de Protegus-dienst kan de gebruiker de communicatiemodule en het systeem op afstand bewaken en bedienen; meer informatie: www.protegus.app.



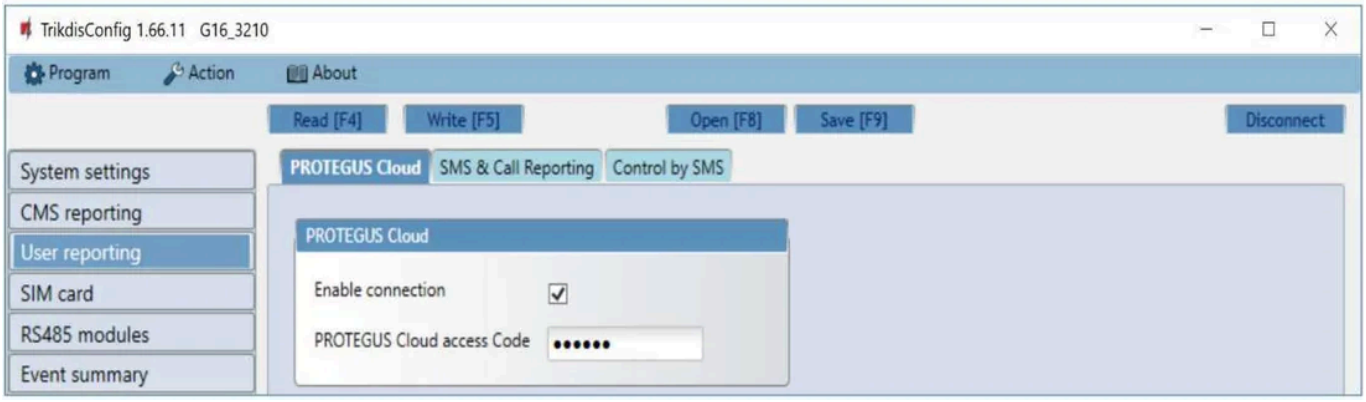
Afbeelding 36. TrikdisConfig – User reporting, tabblad PROTEGUS Cloud.

- **Enable connection** – schakelt de verbinding met de Protegus-cloud en de toegang op afstand van TrikdisConfig in.

- **Protegus Cloud access code** – 6-cijferige code voor de Protegus-verbinding (af fabriek `123456`). Kan alleen vóór het aanmaken van het systeem in Protegus 2 worden ingesteld, achteraf niet meer te wijzigen.

Op het tabblad **SMS & Call Reporting** kan de gebruiker ook per sms of telefoonoproep een melding van de gebeurtenissen krijgen.

Bij een alarm stuurt het apparaat eerst de sms naar alle ingevoerde telefoonnummers en belt het de nummers daarna één voor één, van Tel 1 tot Tel 4. Elk nummer wordt één keer gebeld en gaat 20 seconden over; een gesprek geldt als geslaagd als het nummer overgaat (opnemen of weigeren is ook voldoende). De modem belt via 2G of VoLTE. Waar de provider 2G heeft uitgeschakeld en de modem niet voor VoLTE heeft goedgekeurd, komt de sms wel aan, maar gaat de telefoon niet over. Dit is geen configuratiefout. Gebruik op zulke plaatsen sms en de Protegus 2-app.



Afbeelding 37. TrikdisConfig – User reporting, tabblad SMS & Call Reporting.

- **Object name** – de naam van het systeem; staat in elke sms.
- **SMS language** – de taal van de sms'en (voor de tekens met accenten van die taal).
- **Tel numbers for SMS/Call reporting** – maximaal 4 telefoonnummers met landcode (`+CC…`, `00CC…` of `CC…`, waarbij CC de landcode is).
- **Area name, User name, Zone name** – de namen van de partities, gebruikers en zones; het apparaat gebruikt ze in de tekst van de sms'en. Vul in de juiste tabel het nummer van de partitie, de gebruiker of de zone in, met de naam ernaast. Bij een centrale die via de bus wordt uitgelezen komen de eigen zone- en gebruikersnummers van de centrale binnen; geef bij die nummers de namen op.
- **CID event table** – per gebeurtenis in te stellen welk nummer een sms of oproep krijgt; de berichttekst en de Contact ID-code kunnen ook worden gewijzigd, en er kan een nieuwe gebeurtenis worden toegevoegd.

Op het tabblad **Control by SMS** stelt u het ontvangen van sms-commando's in (de commando's staan beschreven in paragraaf 5.5).

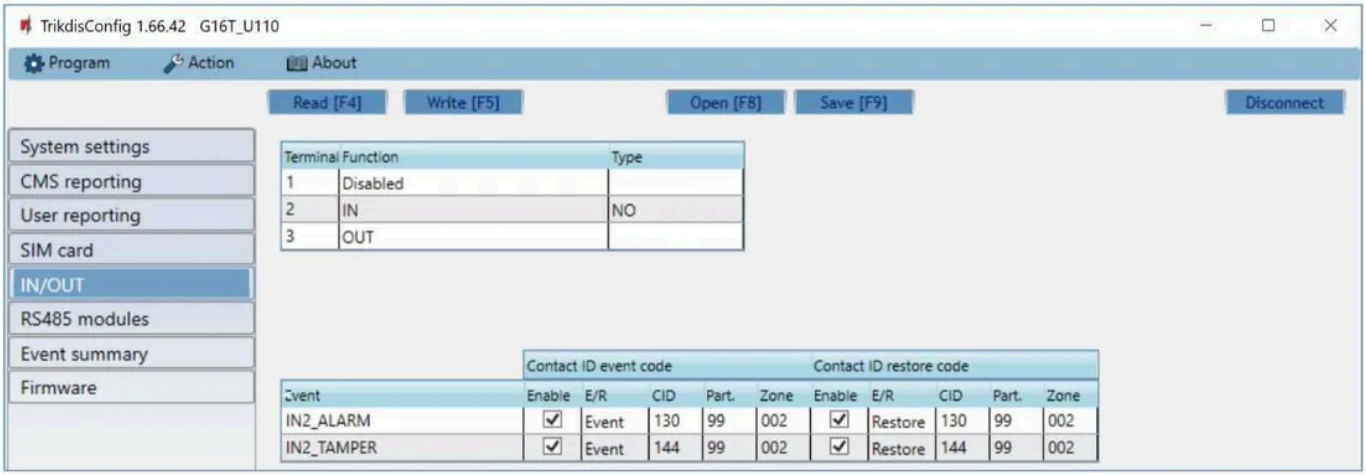


Afbeelding 38. TrikdisConfig – User reporting, tabblad Control by SMS.

- **Reply text** – de tekst van de vier antwoordberichten op een sms-commando: geslaagd commando (Command done), verkeerd wachtwoord (Wrong password), verkeerd commando (Wrong command), verkeerde gegevens (Wrong data).
- **Tel numbers for control by SMS** – maximaal 4 nummers; het apparaat accepteert alleen commando's van deze nummers. Als het veld leeg is, accepteert het een commando met het juiste wachtwoord van elk nummer; de beveiliging zit er dan nog steeds in dat het beheerders- of installateurswachtwoord in het commando verplicht is.

6.5 SIM card

Zonder de gegevens van de simkaart maakt het apparaat geen verbinding met het datanetwerk.



Afbeelding 39. TrikdisConfig – pagina SIM card.

- **SIM card PIN** – de pincode van de kaart. U kunt de pincodevraag uitschakelen door de kaart in een mobiele telefoon te plaatsen en ze daar uit te schakelen. Als de pincodevraag is uitgeschakeld, kan de fabriekswaarde van het veld blijven staan.
- **APN** – het toegangspunt van de provider (Access Point Name); zonder APN kan de communicatiemodule geen verbinding maken met het internet. U vindt ze ook op de website van de provider; de APN „internet" is algemeen en werkt in de netwerken van veel providers. De bekende APN's van de providers staan in het APN-artikel (bij een IoT- / M2M-kaart geeft de provider een aparte APN, zie paragraaf 2.3).
- **Login, Password** – gebruikersnaam en wachtwoord van de APN, als de provider die vraagt.
- **Forbid connection when roaming detected** – nuttig in de buurt van een landsgrens: voorkomt dat het apparaat verbinding maakt met het netwerk van het buurland.

Controleer vóór gebruik of de simkaart actief is en of voor IP-communicatie de mobiele datadienst erop is ingeschakeld.

6.6 IN/OUT

Hier geeft u de rol op van de drie I/O-klemmen met dubbele functie van de communicatiemodule: **Disabled** (niet gebruikt), **IN** (ingang) of **OUT** (uitgang). Bij een ingang moet ook het type worden opgegeven (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Fabrieksinstelling: I/O 1 niet gebruikt, I/O 2 ingang (NO), I/O 3 uitgang.



Afbeelding 40. TrikdisConfig – pagina IN/OUT: de functie van de I/O-klemmen en de gebeurtenissen van de ingangen.

Als de detector op de ingang wordt geactiveerd, stuurt de communicatiemodule een eigen gebeurtenis (**INx_ALARM**, Contact ID 130), en bij het verbreken van het sabotagecircuit een sabotagegebeurtenis (**INx_TAMPER**, 144) naar de meldkamer en naar Protegus 2; in de tabel verschijnen de gebeurtenissen van elke klem die als ingang is ingesteld. De kolommen van de tabel:

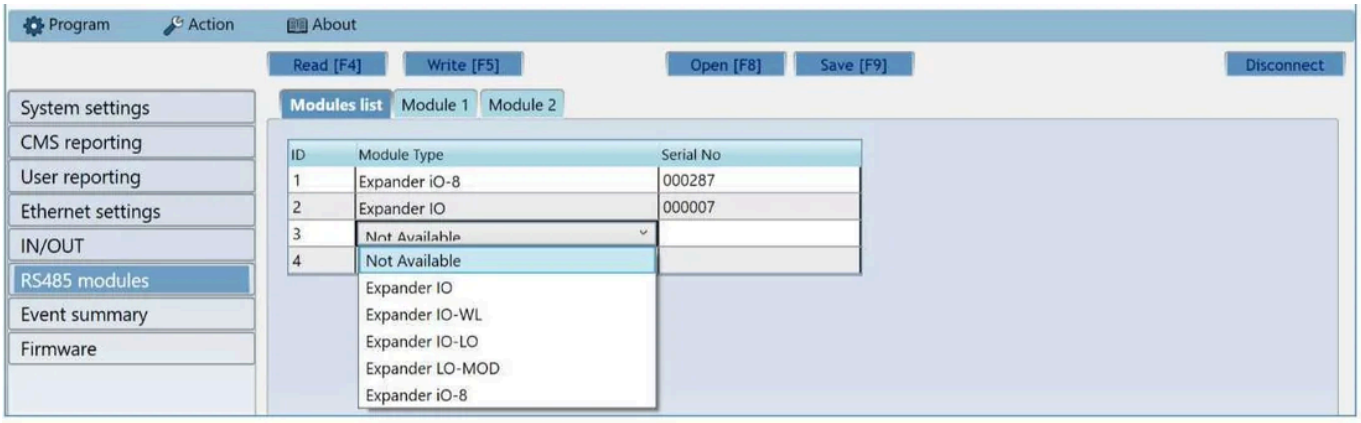
- **Enable** – schakelt het verzenden van het bericht in.
- **E/R** – het type gebeurtenis: Event (alarm) of Restore (herstel).
- **CID** – de Contact ID-code.
- **Part.** – het partitienummer in het bericht.
- **Zone** – het zonenummer in het bericht.

Op **hardwareversie 3** is er geen pagina IN/OUT: het type van de enige ingang stelt u in het veld **System settings → Input IN type** in, de modus van de twee uitgangen in het veld **Output OUT1 & OUT2 mode**, en de gebeurtenissen van de ingang (IN_ALARM, IN_TAMPER) op de pagina **Event summary**.

6.7 RS485 modules

De iO-8-uitbreidingen en W485- / E485-modules die op de RS485-bus zijn aangesloten, moeten op het tabblad **Modules list** worden toegevoegd.

Op de G16 met 2G-modem (G16_G410) kan deze pagina niet worden gebruikt: de 2G-versie heeft geen RS485-bus.

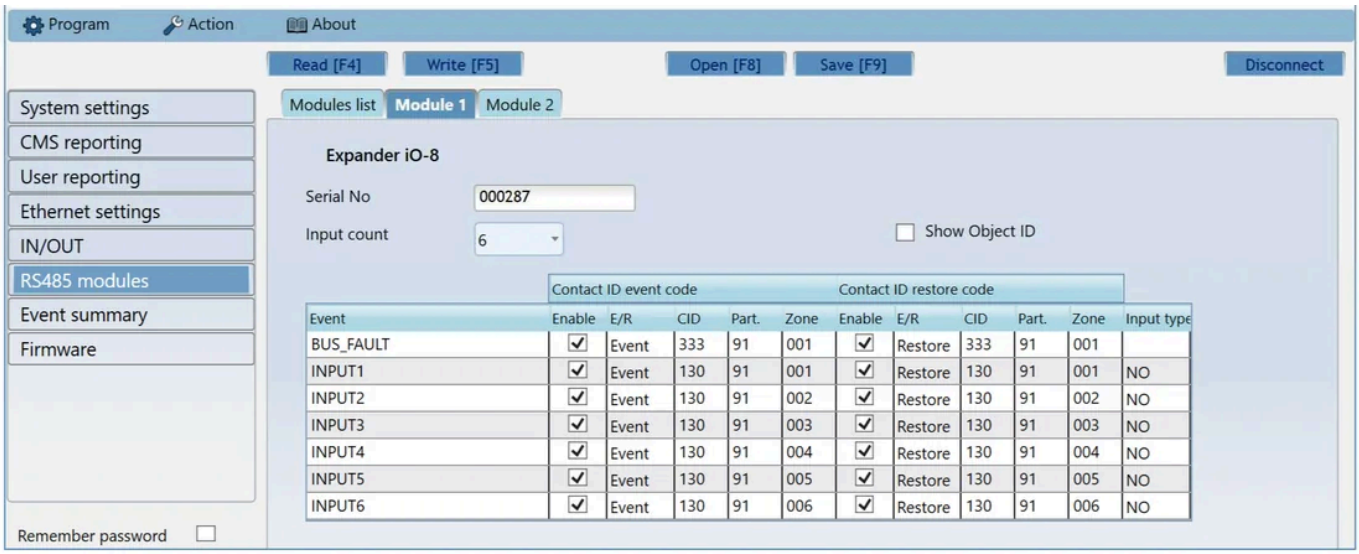


Afbeelding 41. TrikdisConfig – RS485 modules, tabblad Modules list: het type module (Expander iO-8, W17u/W485, E485) en het serienummer.

- **Module Type** – het type van de aangesloten module uit de lijst (Expander iO-8, W17u/W485, E485).
- **Serial No** – het 6-cijferige serienummer van de module (op de module en op de doos, SN).

Druk na het kiezen van de module en het invullen van het serienummer op de knop **Write [F5]**, trek de USB-kabel eruit en wacht een minuut tot de communicatiemodule de module heeft geregistreerd. Steek daarna de kabel er weer in, lees het apparaat uit (**Read [F4]**), en op de pagina RS485 modules verschijnt het eigen, genummerde tabblad van de module.

iO-8-uitbreiding – 8 I/O's met dubbele functie; er kunnen maximaal 4 modules op de communicatiemodule worden aangesloten.



Afbeelding 42. TrikdisConfig – RS485 modules, tabblad van de iO-8-module.

- **Input Count** – hoeveel klemmen ingang moeten zijn; de rest wordt uitgang. Het type ingang (**Input type**: NO of NC) kan in de tabel worden opgegeven. De rol van de uitgangen (in- / uitschakelen met een sleutelschakelaarzone of een apparaat schakelen) stelt u in de Protegus 2-app in.
- In de tabel kunt u een Contact ID-code toewijzen aan de busstoring (**BUS_FAULT**, Contact ID 333) en aan de activerings- en herstelgebeurtenissen van de ingangen (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Bij activering van de ingang stuurt de communicatiemodule met de ingestelde code een gebeurtenis naar de ontvanger van de meldkamer, naar de Protegus 2-app en per sms naar het telefoonnummer van de gebruiker. Standaard meldt module 1 met partitie 91 en module 4 met partitie 94. Door **Show Object ID** aan te vinken kan voor de ingangen ook een ander objectnummer dan dat van de communicatiemodule worden opgegeven.

- Als de gebruiker over de ingangen van de uitbreiding ook een sms of oproep moet krijgen, voeg de aan de ingang toegewezen Contact ID-code dan ook toe aan de gebeurtenissentabel van het tabblad **SMS & Call Reporting**.

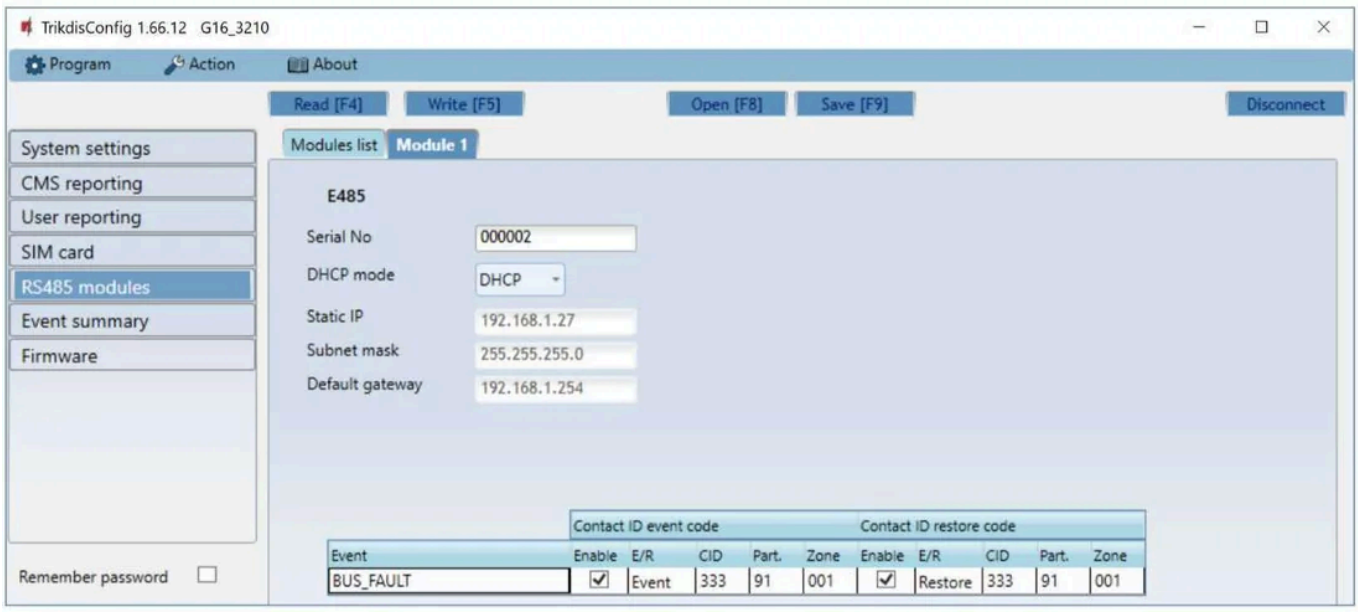
W485 WiFi-module (in de lijst W17u/W485) – de gegevens van het WiFi-netwerk en de netwerkinstellingen.



Afbeelding 43. TrikdisConfig – RS485 modules, tabblad van de W485-module.

- **DHCP mode** – automatische (DHCP) of handmatige (Static) netwerkinstelling.
- **Static IP**, **Subnet mask**, **Default gateway** – bij handmatige instelling.
- **Wifi SSID name**, **Wifi SSID password** – de naam en het wachtwoord van het WiFi-netwerk.
- In de tabel kunt u een Contact ID-code toewijzen aan de storingen van de RS485-bus (wegvallen en herstel van de verbinding tussen de module en de G16); de gebeurtenis wordt ontvangen door de meldkamer en door Protegus 2.

E485 Ethernet-module – dezelfde netwerkinstellingen zonder WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); ook hier kunt u in de tabel een Contact ID-code toewijzen aan de storing van de RS485-bus (wegvallen en herstel van de verbinding tussen de E485 en de G16), die door de meldkamer en door Protegus 2 wordt ontvangen.



Afbeelding 44. TrikdisConfig – RS485 modules, tabblad van de E485-module.

Voor de werking van de W485 en de E485 moet de meldkamer- en/of Protegus-verbinding van de G16 zijn ingesteld (paragraaf 2.3 en 2.4), en moet er een simkaart in de G16 zitten. Zolang de bekabelde of WiFi-verbinding actief is, communiceert de communicatiemodule daarlangs en gebruikt hij de mobiele dataverbinding niet.

6.8 Event summary

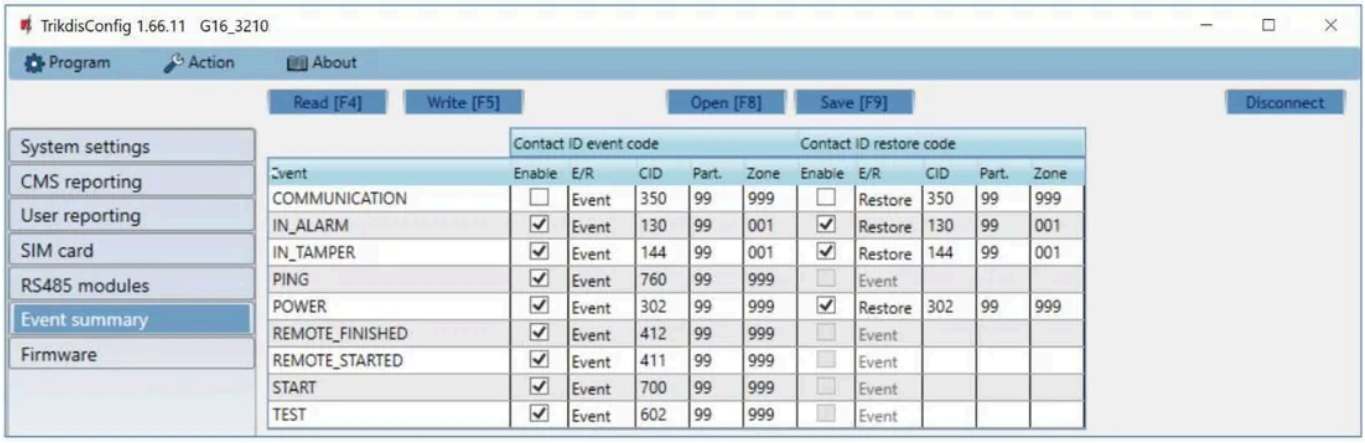
Op deze pagina kunt u de **eigen, interne berichten** van het apparaat in- of uitschakelen en hun Contact ID-code, partitie- en zonenummer wijzigen. Een bericht dat hier is uitgeschakeld, verstuurt het apparaat via geen enkel kanaal. Af fabriek worden de berichten verzonden met partitie 99 en zone 999.

Bericht	Contact ID	Wanneer ontstaat het
COMMUNICATION	350	De communicatie tussen de communicatiemodule en de alarmcentrale is verbroken (af fabriek uitgeschakeld). Een communicatiemodule die op de bus of de seriële poort is aangesloten, detecteert dit rechtstreeks; een communicatiemodule op de telefoonlijn alleen als **Line supervision** is ingeschakeld.
POWER	302	Onvoldoende (lage) voedingsspanning; het herstel is een apart bericht.
REMOTE_STARTED	411	Programmering op afstand met TrikdisConfig is gestart.
REMOTE_FINISHED	412	De programmering op afstand is voltooid.
START	700	Het apparaat heeft verbinding gemaakt met het netwerk (opstarten).
TEST	602	Periodiek testrapport.
PING	760	Het PING-levenssignaal. Het staat niet in de lijst van elk apparaat: op het scherm van de eerdere hardwareversie wel, op de pagina Event summary van de nieuwere versies is er geen zo'n regel. Het interval stelt u in het veld **CMS reporting** → **Settings** → **IP ping period** in.

- **Enable** – schakelt het verzenden van het bericht naar de meldkamer en naar Protegus 2 in.
- **E/R** – het type bericht: Event (gebeurtenis) of Restore (herstel) – de regel staat voor het optreden van de gebeurtenis of voor het herstel ervan.

- **Part.** – het nummer van de partitie (gebied) dat het apparaat bij de interne gebeurtenis en bij het herstel verzendt.
- **Zone** – het zonenummer dat het apparaat bij de interne gebeurtenis en bij het herstel verzendt.
- De **CID**-code, de **partitie** en de **zone** kunnen bij elke gebeurtenis worden gewijzigd; waar er een herstel (Restore) is, kan de code daarvan apart worden opgegeven.

De gebeurtenissen van de eigen ingangen (**INx_ALARM**, **INx_TAMPER**) stelt u in op de pagina **IN/OUT**, de gebeurtenissen van de uitbreidingsmodules (**BUS_FAULT**, **INPUTx**) op de pagina **RS485 modules**, op het tabblad van de module. Het inschakelen en het interval van het testrapport stelt u in het veld **CMS reporting → Settings → Test period** in.



Afbeelding 45. TrikdisConfig – pagina Event summary: de interne berichten van het apparaat (op de afbeelding hardwareversie 3, waarbij de gebeurtenissen IN_ALARM en IN_TAMPER van de ingang en de PING ook hier staan; op versie 4 staan de gebeurtenissen van de ingangen op de pagina IN/OUT).

6.9 Fabrieksinstellingen herstellen

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**.

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:

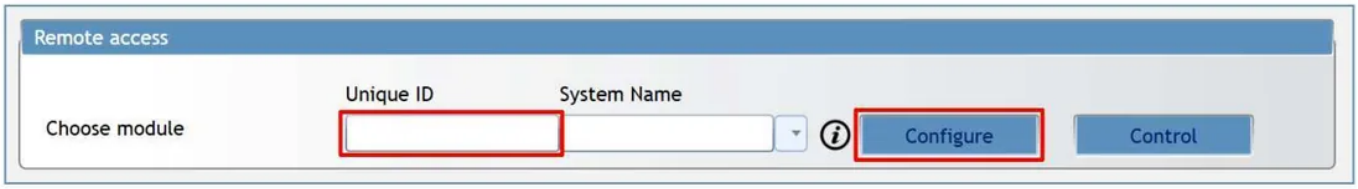
1. Het apparaat moet ingeschakeld zijn en een netwerkverbinding hebben (de **POWER**- en de **NETWORK**-led branden groen; bij een apparaat met mobiel netwerk knippert de NETWORK-led ook geel). Bij een apparaat met mobiel netwerk moet de geplaatste simkaart actief zijn en moet de pincode ervan in het 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 46. TrikdisConfig – Remote access: de identificatie van het apparaat, de naam van het systeem en de knop Configure.

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.

Controleer bij een centrale die op de bus is aangesloten ook of de communicatiemodule echt uit de centrale leest: schakel de centrale op het bediendeel in en uit, en kijk of de gebeurtenis in de gebeurtenissenlijst van Protegus 2 (en bij de meldkamer) met het juiste partitie- en gebruikersnummer verschijnt. Voer bij directe besturing ook een proefinschakeling uit vanuit de app, met de bediendeelcode van de gebruiker.

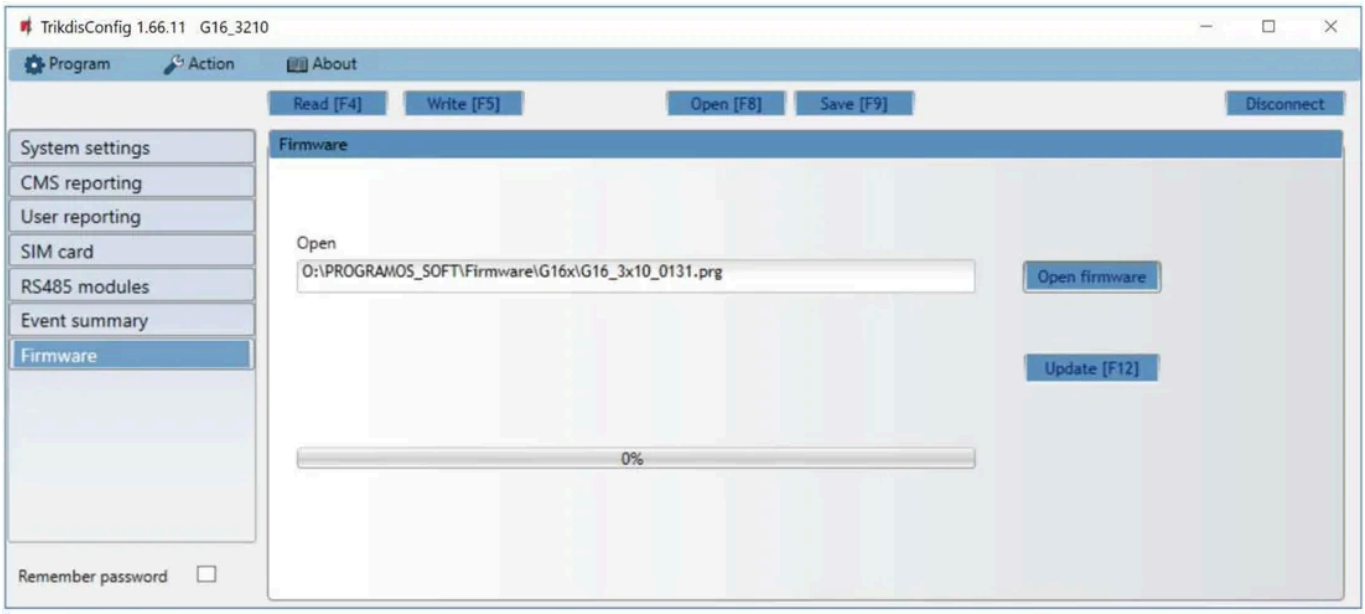
9. Firmware bijwerken

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 47. TrikdisConfig – pagina Firmware: Open firmware en Update [F12].

Voor het bijwerken is een internetverbinding nodig. Een virusscanner, firewall of strenge netwerkinstelling kan het automatisch downloaden van de firmware verhinderen; pas in dat geval de virusscanner aan (sta TrikdisConfig internettoegang toe), of download het bestand handmatig en open het op de pagina Firmware.

10. Storingen zoeken en veelgestelde vragen

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

De NETWORK-led brandt niet – geen netwerk

1. Kijk naar de knipperingen van de **TROUBLE**-led: 1 = geen simkaart, 2 = verkeerde pincode, 3 = geen APN, 4 = kan geen verbinding maken met het mobiele netwerk, 5 = kan geen verbinding maken met het datanetwerk.
2. Controleer of de simkaart actief is, een datadienst heeft en goed in de houder zit.
3. Als de pincodevraag op de kaart is ingeschakeld, vul de pincode dan in op de pagina **SIM card**, of schakel de pincodevraag uit in een telefoon.
4. Controleer de antenne: vastgeschroefd, niet in een metalen behuizing, het signaalniveau is voldoende (paragraaf 1.7 en 3.2).

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. 6 knipperingen van de **TROUBLE**-led betekenen dat er geen verbinding met de ontvanger is: controleer het adres, de poort, de TCP/UDP-instelling en de versleutelingssleutel van de ontvanger (**CMS reporting**).
2. Als de ontvanger met een domeinnaam is opgegeven, controleer dan de DNS-instelling (**CMS reporting** → **Settings**).
3. Kijk of de databundel van de simkaart de benodigde poort niet blokkeert (sommige M2M-kaarten laten alleen bepaalde adressen toe).

De TROUBLE-led knippert zeven keer – de communicatiemodule ziet de centrale niet

1. Controleer de aansluiting volgens het schema in paragraaf 3.3: de meest voorkomende fout is een verwisselde **CLK**- en **DATA**-draad, of een datalijn die op de verkeerde klem van de centrale is aangesloten.
2. In het veld **System settings** → **Security panel model** van TrikdisConfig moet het exacte type van de aangesloten centrale zijn gekozen.
3. Bij Texecom-, Caddx-, Honeywell- en InnerRange-centrales is ook een instelling in de centrale nodig (hoofdstuk 4) – zonder die instelling geeft de centrale geen gegevens op de bus.
4. Bij een Paradox-centrale kan de seriële poort af fabriek vergrendeld zijn – zo ontgrendelt u die.
5. Maak een Pyronix-centrale na het aansluiten spanningsloos en start ze opnieuw, zodat ze de communicatiemodule accepteert.
6. Met een DSC PowerSeries **NEO**-centrale werkt de G16 niet (op de NEO-bus zijn geen externe apparaten toegestaan) – daar is een communicatiemodule voor de telefoonlijn nodig.

De gebeurtenissen komen binnen, maar ik kan niet inschakelen vanuit de app

Bij directe besturing:

1. Op de pagina **System settings** moet **Remote Arm/Disarm** zijn aangevinkt.
2. Bij een Paradox- en Texecom-centrale moet het **Security panel PC download password** overeenkomen met het pc- resp. UDL-wachtwoord van de centrale (paragraaf 4.2 en 4.3).

3. Bij een Paradox-centrale moet de firmware van de centrale minimaal **V.4** zijn; de code van de gebruiker mag niet de mastercode zijn; herstart de communicatiemodule na het wijzigen van een code.
4. Bij een Honeywell Vista-centrale moet het 2e AUI-adres zijn ingeschakeld (paragraaf 4.6).
5. In Protegus 2 mag **geen** uitgang aan de partitie zijn toegewezen (Control with Protegus2 uitgeschakeld).

Met een sleutelschakelaarzone:

1. **Remote Arm/Disarm** moet leeg zijn, de I/O-klem moet op de pagina **IN/OUT** op **OUT** staan.
2. De zone van de centrale moet van het type sleutelschakelaar zijn, en in Protegus 2 moet de juiste uitgang aan de partitie zijn toegewezen, in de pulserende of tweestandige modus die bij de zone past (paragraaf 5.3).

Protegus 2 ziet het apparaat niet

1. Op het tabblad **User reporting** → **PROTEGUS Cloud** moet **Enable connection** zijn aangevinkt.
2. Bij het aanmaken van het systeem moet de **Protegus Cloud access code** worden ingevoerd die in het apparaat is ingesteld; na het aanmaken van het systeem kan die in het apparaat niet meer worden gewijzigd.
3. Voer de IMEI exact in, van de doos of van de achterkant.
4. De datadienst van de simkaart en de APN moeten in orde zijn (de NETWORK-led is groen en de DATA-led gaat na een gebeurtenis uit).

Ik kan niet op afstand inloggen met TrikdisConfig

1. Het apparaat moet online zijn (NETWORK-led groen), en de Protegus-verbinding moet zijn ingeschakeld.
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 de toegang op afstand.
3. Controleer het beheerders- of installateurswachtwoord.

Ik ben het wachtwoord vergeten

Een vergeten wachtwoord kan niet worden opgevraagd en ook niet worden gewist door de fabrieksinstellingen te herstellen, want ook daarvoor is een wachtwoord nodig. Dan kan alleen de fabrikant of de distributeur het herstellen: het apparaat moet naar hem worden opgestuurd. Noteer de ingestelde wachtwoorden daarom op een veilige plaats.

Waarom zie ik de pagina RS485 modules niet, of waarom werkt de iO-8 niet?

De G16 met 2G-modem (G16_G410) heeft geen RS485-bus; iO-8, W485 en E485 kunnen alleen op de 4G-versie (G16_54E0) worden aangesloten. Voor de W485- en E485-module moet er ook een simkaart in de G16 zitten.

Ik heb een 2G-apparaat – hoe lang werkt het nog?

Het uitfaseren van 2G-netwerken verloopt per provider in een ander tempo; voor gebruik op lange termijn raden we de 4G-versie aan, die ook via de RS485-bus kan worden uitgebreid.

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.

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 aandachtig door; het negeren van de instructies kan leiden tot een verkeerde werking of een defect.
- Koppel de apparatuur los van de voeding vóór het aansluiten, bij elke elektrische verbinding en vóór onderhoud.
- Fouten die het gevolg zijn van onjuiste installatie of onjuist gebruik, evenals wijzigingen en reparaties die niet door de fabrikant zijn toegestaan, maken de garantie ongeldig.
- Houd u aan de plaatselijke voorschriften voor afvalverwerking: gooi het defecte apparaat en de onderdelen ervan niet bij het huishoudelijk afval.

Zie ook

- Compatibiliteitszoeker – welke communicatiemodule bij welke alarmcentrale past.
- G16 – directe besturing voor DSC PowerSeries-alarmcentrales – inschakelen met de bediendeelcode, zonestatus, zones overbruggen.
- DSC Power Series NEO en Trikdis-communicatiemodules: compatibiliteit en oplossingen – waarom de G16 niet op de NEO kan worden aangesloten, en wat de oplossing is.
- Een vergrendelde seriële poort ontgrendelen op Paradox-alarmcentrales – het ontgrendelen van de seriële poort van de nieuwere Paradox-centrales.
- Op afstand inschakelen met een sleutelschakelaar vanuit de Protegus 2-app – de details en valkuilen van het inschakelen met een sleutelschakelaar.
- De v4-hardwareversie van de G16- en G16T-GSM-communicatiemodules komt eraan – wat er is veranderd ten opzichte van versie 3.
- APN-instelling – lijst van Europese mobiele providers – de APN van de simkaart per provider.
- Engelstalige documentatie: docs.trikdis.com.

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

Gerelateerde producten

Trikdis G16 4G GSM communicatiemodule | **Trikdis G16 2G GSM communicatiemodule**

Trikdis CRP2 seriële poort aansluitkabel voor Paradox alarmpanelen

CRP2B seriële poort aansluitkabel voor Paradox alarmpanelen

Trikdis CRP4 seriële kabel voor Texecom bedieningspanelen

Trikdis iO8 bekabelde uitbreidingsmodule

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/g16-handleiding