Communicateur G16 – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation du communicateur Trikdis G16 : raccordement au bus de données ou au port série de la centrale d'alarme, programmation de la centrale, carte SIM et configuration dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-g16

Sommaire

1. Présentation

1.1 À quoi il sert, comment il fonctionne
1.2 Centrales d'alarme compatibles
1.3 Versions
1.4 Caractéristiques principales
1.5 Les éléments du communicateur
1.6 Bornes
1.7 Signalisation des LED
1.8 Caractéristiques techniques

2. Mise en service rapide avec TrikdisConfig

2.1 Préparatifs
2.2 Type de centrale et pilotage direct
2.3 Liaison avec l'application Protegus 2
2.4 Liaison avec le centre de télésurveillance

3. Installation et raccordement

3.1 Les étapes de l'installation
3.2 Emplacement et antenne
3.3 Raccordement à la centrale d'alarme
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 et Integriti
3.4 Raccordement d'une zone à clé
3.5 Raccordement des entrées
3.6 Raccordement d'une sortie avec un relais
3.7 Raccordement du module d'extension iO-8
3.8 Raccordement des modules W485 et E485
3.9 Mise sous tension et première vérification
A TRIKDIS átjelző elindítása

4. Programmation de la centrale d'alarme

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

5. Pilotage à distance avec Protegus 2

5.1 Ajout de l'appareil
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Pilotage direct avec le code clavier
5.3 Armement par zone à clé
5.4 Armer et désarmer depuis l'application
5.5 Pilotage par SMS

6. TrikdisConfig – les réglages en détail

6.1 La barre d'état
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 Retour aux réglages d'usine

7. Programmation à distance

8. Vérification du fonctionnement

9. Mise à jour du firmware

10. Dépannage et questions fréquentes

11. Consignes de sécurité

Voir aussi

1. Présentation

Le G16 est le **communicateur cellulaire à raccordement direct** de Trikdis : il ne se branche pas sur la sortie ligne téléphonique de la centrale d'alarme, mais sur son **bus clavier ou son port série**. Il lit les événements directement dans la centrale – avec les numéros de zone, de partition et d'utilisateur – et les transmet par liaison de données mobile au récepteur du centre de télésurveillance ainsi qu'au cloud Protegus, vers l'application de l'utilisateur. Il fonctionne avec les centrales DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell et Crow prises en charge ; sur les modèles **pilotables directement**, l'utilisateur arme et désarme depuis l'application Protegus 2 avec son propre code clavier, sans zone à clé séparée. L'application Protegus 2 s'utilise avec toutes les centrales d'alarme prises en charge par le G16, quelle que soit leur marque. Pour une centrale d'une autre marque qui ne dispose que d'une sortie ligne téléphonique, c'est le communicateur G16T (TIP/RING) qui convient.

1.1 À quoi il sert, comment il fonctionne

- **Il lit directement la centrale.** Sur le bus de la centrale, chaque événement arrive immédiatement au communicateur, avec la numérotation propre de la centrale ; il n'est pas nécessaire de configurer le transmetteur téléphonique de la centrale, et il n'y a pas de numérotation Contact ID.
- **Il transmet au centre de télésurveillance.** Il envoie les événements par liaison IP au récepteur logiciel ou matériel de Trikdis (protocole TRK) – ceux-ci fonctionnent avec n'importe quel logiciel de télésurveillance – ou à n'importe quel récepteur universel (SIA DC-09 2007/2012, SUR-GARD TL150). Vers un récepteur SUR-GARD, il convertit les codes Contact ID reçus de la centrale en codes SIA. Par défaut, il vérifie la liaison toutes les 30 secondes (ou selon l'intervalle que vous avez réglé) et, en cas de défaut, bascule sur le canal de secours.
- **Il avertit l'utilisateur.** L'application Protegus 2 affiche ce qui s'est passé par notification push – avec un son distinct adapté à l'événement – et dans la liste des événements ; depuis l'application, l'utilisateur peut armer et désarmer et commander les équipements raccordés (éclairage, portail, ventilation, chauffage, arrosage, etc.). Il peut aussi être averti par SMS et par appel téléphonique.
- **Ensemble ou séparément** : il fonctionne avec le centre de télésurveillance et avec l'utilisateur – il s'utilise uniquement avec Protegus 2 (sans télésurveillance), uniquement avec la télésurveillance, ou avec les deux. Si les deux sont configurés, il envoie l'événement d'abord au centre de télésurveillance, puis à l'utilisateur.
- **Secours par SMS.** Il avertit aussi le centre de télésurveillance par SMS si la liaison de données ne fonctionne pas sur le réseau de l'opérateur ; il peut envoyer à deux récepteurs en parallèle, chacun avec son propre canal de secours.
- **Il a ses propres entrées et sorties.** Trois bornes I/O à double fonction s'utilisent comme entrée (détecteur, autoprotection) ou comme sortie pilotable (zone à clé, relais) ; vous pouvez commander les sorties depuis l'application Protegus 2 et par commande SMS. Sur le bus RS485 de la version 4G, un module d'extension iO-8 ajoute 8 I/O, et un module W485 ou E485 permet de communiquer aussi par WiFi ou par Internet filaire – le réseau mobile devient alors la voie de secours.

Le schéma ci-dessous montre l'architecture du système : le bus de la centrale d'alarme se raccorde au G16, le G16 accède à Internet par le réseau mobile, et de là au récepteur du centre de télésurveillance et au cloud Protegus ; l'utilisateur voit le système dans l'application Protegus 2.

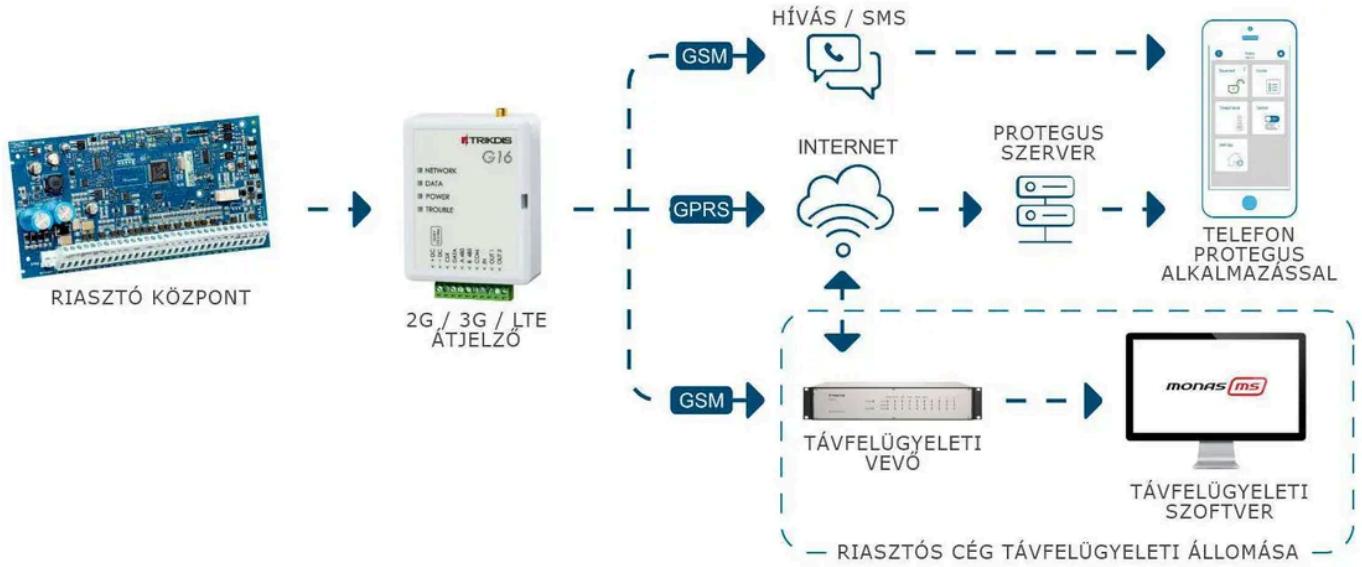


Figure 1. La place du G16 dans le système : centrale d'alarme → G16 → réseau mobile → récepteur du centre de télésurveillance et cloud Protegus → application Protegus 2. L'utilisateur peut aussi recevoir des SMS et des appels (GSM), le récepteur du centre de télésurveillance des SMS en secours.

- 1 Centrale d'alarme (bus clavier ou port série)
- 2 Communicateur G16 (2G / 4G)
- 3 Appel et SMS vers l'utilisateur
- 4 Liaison de données mobile → Internet → cloud Protegus
- 5 Téléphone avec l'application Protegus 2
- 6 Récepteur du centre de télésurveillance
- 7 Logiciel de télésurveillance (poste de télésurveillance de la société de sécurité)

1.2 Centrales d'alarme compatibles

Le G16 peut être raccordé aux centrales ci-dessous. Sur les modèles **pilotables directement**, l'armement et le désarmement se font depuis l'application avec le code clavier ; sur les autres, par une zone à clé (point 3.4). Pour le pilotage direct des centrales Paradox, le firmware de la centrale doit être au moins en **V.4** ; sur les modèles Paradox récents (SP+, MG5050+, EVOHD+), le port série est verrouillé d'usine et doit être déverrouillé avant utilisation.

Centrales à commande directe – le communicateur reçoit les événements par le bus de données ou le port série, et l'armement / le désarmement fonctionnent sans câblage supplémentaire :

Fabricant	Raccordement	Modèles
Paradox	port série	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* firmware supérieur à 7.50)
DSC	bus de données	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	bus de données	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	port série	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	bus de données	Ademco Vista-15, Vista-20, Vista-48

Sur les centrales Paradox plus récentes marquées d'un *, le port série est verrouillé en usine ; l'appareil externe ne communique avec la centrale qu'après son déverrouillage.

Soros port feloldás útmutató

Centrales commandées par zone à clé – le communicateur reçoit les événements par le bus de données ou le port série ; la commande nécessite un raccordement et une programmation en zone à clé (point 3.4) :

Fabricant	Raccordement	Modèles
Paradox	port série	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	bus de données	PC1404, PC5020
Texecom	port série	Premier 412, 816, 832, 832+
Inner Range	bus de données	Inception, Integriti
Crow	bus de données	Runner 4/8, 8/16

La liste change de temps en temps ; l'état le plus récent se trouve dans le moteur de recherche de compatibilité. En plus de celles-ci, il s'utilise aussi avec les centrales **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 et MATRIX 816**, **DSC PC5015** ainsi que **Paradox DIGIPLEX EVO96 et NE96**. Le G16 ne fonctionne pas avec les centrales **DSC PowerSeries NEO** : le fabricant n'autorise aucun appareil externe sur le bus NEO, voir DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions.

1.3 Versions

Ce manuel a été rédigé pour la **version matérielle 4** du G16, mais il **s'applique aussi à la version matérielle 3** : le raccordement, la configuration et le fonctionnement des deux versions sont en grande partie identiques. Le manuel vaut de la même façon pour les versions à modem 2G, 3G et 4G. Le tableau ci-dessous résume les différences ; là où le texte donne une valeur de la version 4, tenez compte de celle-ci pour la version 3.

	Matériel 3 (v3)	Matériel 4 (v4)
Modèles (dans TrikdisConfig)	p. ex. G16_3210 (2G) ; il a aussi existé des versions à modem 3G et 4G	G16_G410 (2G), G16_54E0 (4G)
Entrées / sorties	1 entrée de type paramétrable (IN) + 2 sorties à collecteur ouvert (OUT1, OUT2, max. 0,15 A)	3 bornes I/O à double fonction (I/O 1, I/O 2, I/O 3), chacune utilisable comme entrée ou comme sortie à collecteur ouvert (max. 0,15 A)
Configuration des entrées / sorties	page System settings : **Input IN type**, **Output OUT1 & OUT2 mode**	page **IN/OUT** (point 6.6)
Consommation	100 mA ; jusqu'à 250 mA pendant l'émission	60–100 mA ; jusqu'à 500 mA pendant l'émission
Bus RS485 (iO-8, W485, E485)	uniquement sur les versions 3G et 4G	uniquement sur la version 4G (G16_54E0)

La version matérielle 4 existe avec deux modems :

Modèle	Modem	Fréquences	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	non

Modèle	Modem	Fréquences	RS485 (iO-8, W485, E485)
G16_54E0	4G (LTE)	bandes LTE selon la région	oui

La version matérielle s'affiche dans la barre d'état de TrikdisConfig (**HW**) et figure sur l'étiquette au dos de l'appareil. Un article séparé présente la version 4 : La version matérielle v4 des communicateurs GSM G16 et G16T arrive.

1.4 Caractéristiques principales

Liaison avec la centrale d'alarme

- Se raccorde avec 4 fils au maximum (+DC, −DC, CLK, DATA) au bus clavier de la centrale (DSC, Caddx, Crow, Pyronix, Honeywell) ou à son port série (Paradox, Texecom, InnerRange) ; pour le port série, un câble d'origine est disponible (Paradox : CRP2 / CRP2B, Texecom : CRP4).
- Transmet chaque événement de la centrale avec toutes les informations (code, partition, zone ou utilisateur) ; signale la perte de liaison (LED TROUBLE, événement COMMUNICATION).
- Les centrales pilotables directement s'arment et se désarment depuis l'application avec le code clavier ; Protegus 2 affiche aussi l'état des zones.

Communication avec le centre de télésurveillance

- Liaison IP avec les récepteurs Trikdis (récepteur logiciel IPcom, RL14, RM14) et les récepteurs universels (SIA DC-09, TL150).
- Canal principal, de secours et parallèle ; notification SMS de secours vers le récepteur SMS Trikdis (RL14, RM14, GM14).
- Chiffrement des messages AES-128 ; mémoire de 60 messages.

Fonctions pour l'utilisateur

- Application mobile et web Protegus 2 : notifications, liste des événements, armement et désarmement, commande des sorties.
- Pilotage et configuration de base aussi par commandes SMS.
- Notification aussi par SMS et par appel téléphonique, vers 4 numéros de téléphone au maximum.
- Droits utilisateur à plusieurs niveaux dans l'application (administrateur, installateur, utilisateur).

Installation et configuration

- Les paramètres peuvent être enregistrés dans un fichier et chargés dans un autre communicateur.
- Deux niveaux d'accès : administrateur et installateur.
- Configuration et mise à jour à distance avec le logiciel TrikdisConfig.

1.5 Les éléments du communicateur

Le G16 loge son circuit imprimé dans un boîtier en plastique blanc ; la face avant se retire et le bornier est débrochable. L'image ci-dessous montre la version 4G ; la version 2G n'a pas de LED BAND ni de bornes A 485 / B 485.

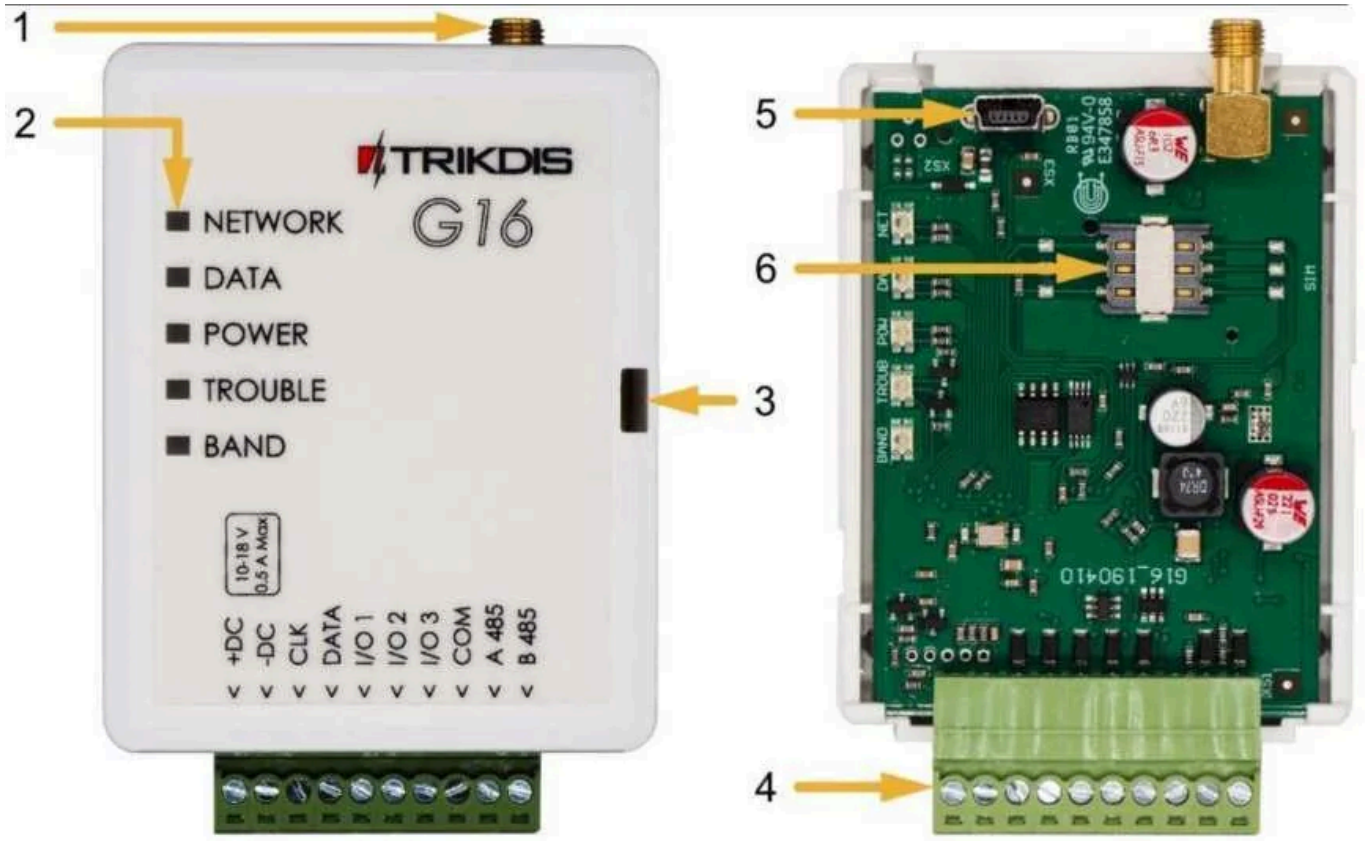


Figure 2. Les éléments du G16 (version 4G), de face et boîtier ouvert.

- 1 Connecteur SMA de l'antenne GSM
- 2 Voyants LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Fente facilitant le retrait de la face avant
- 4 Bornier débrochable
- 5 Prise USB Mini-B pour la programmation
- 6 Support de la carte nano-SIM

Le bornier est débrochable : l'appareil se met ainsi hors tension ou redémarre d'un seul geste, il est plus facile à manipuler lors du câblage, et pour la programmation par USB, l'appareil peut être apporté jusqu'à l'ordinateur.

1.6 Bornes

Borne	Fonction
+DC	Alimentation, +10–18 V DC
−DC	Alimentation, négatif
CLK	Ligne d'horloge / ligne série du bus de la centrale
DATA	Ligne de données du bus de la centrale
I/O 1	Entrée/sortie 1 (réglage d'usine : non utilisée)
I/O 2	Entrée/sortie 2 (réglage d'usine : entrée, NO)
I/O 3	Entrée/sortie 3 (réglage d'usine : sortie)
COM	Point commun (négatif) des entrées et des sorties
A 485	Fil A du bus RS485 (version 4G uniquement)
B 485	Fil B du bus RS485 (version 4G uniquement)

Le marquage du bornier figure aussi sur la face avant : il n'est donc pas nécessaire de retirer le couvercle pour le câblage. La borne de la centrale sur laquelle vont CLK et DATA varie selon le fabricant – les schémas de raccordement se trouvent au point 3.3.

1.7 Signalisation des LED

Les LED de la face avant sont les outils les plus importants pour la mise en service et le dépannage. Lisez-les ensemble : POWER indique l'alimentation, NETWORK le réseau, TROUBLE le défaut, BAND (4G uniquement) le type de réseau.

NETWORK – connexion au réseau

Signal	Signification
éteinte	Pas de connexion au réseau mobile
clignote en jaune	Connexion au réseau mobile en cours
allumée en vert	Connecté au réseau mobile
allumée en vert, clignote en jaune	Connecté ; le nombre de clignotements jaunes indique le **niveau du signal** : en 2G, 5 clignotements, en 4G, 3 clignotements correspondent à un bon signal

DATA – trafic de données

Signal	Signification
éteinte	Aucun message en attente d'envoi
allumée en vert	Des messages en attente d'envoi se trouvent en mémoire
clignote en vert	Envoi ou réception de données en cours (pendant la programmation)

Vérification rapide

La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur le réseau de l'opérateur ; pour un appareil Ethernet, que la liaison jusqu'au routeur fonctionne –, mais pas que l'appareil accède aussi à Internet. Si la LED NETWORK est verte mais que la LED DATA reste allumée en continu après un événement ou un rapport de test, la connexion Internet ne fonctionne pas : le message ne peut pas partir. Sur le réseau mobile, la cause la plus fréquente est l'APN ou le service de données de la carte SIM ; en Ethernet, le routeur, le pare-feu ou le DNS. Si la LED DATA s'éteint, le message est parti et la connexion de données fonctionne.

POWER – tension d'alimentation

Signal	Signification
éteinte	Pas d'alimentation, ou alimentation coupée
allumée en vert	Sous tension, la tension d'alimentation est correcte
allumée en jaune	Tension d'alimentation insuffisante (11,5 V au maximum)
allumée en vert, clignote en jaune	Prêt pour la programmation (câble USB branché)
allumée en jaune (pendant la programmation)	Pas de liaison avec l'ordinateur

TROUBLE – défaut

Signal	Signification
éteinte	Aucun défaut
1 clignotement rouge	Pas de carte SIM
2 clignotements rouges	Erreur de PIN SIM (code PIN erroné)
3 clignotements rouges	Erreur de programmation (pas d'APN)
4 clignotements rouges	Impossible de s'enregistrer sur le réseau mobile (erreur d'enregistrement)
5 clignotements rouges	Impossible de se connecter au réseau de données (GPRS/UMTS/LTE)
6 clignotements rouges	Pas de liaison avec le récepteur du centre de télésurveillance et/ou le serveur Protegus (la cause peut aussi être un défaut de la connexion Internet)
7 clignotements rouges	Liaison avec la centrale d'alarme perdue (liaison bus ou série)
clignote en rouge (pendant la programmation)	Erreur mémoire
allumée en rouge (pendant la programmation)	Firmware endommagé

BAND – type de réseau (version 4G uniquement)

Clignotements verts	Réseau
1	aucun
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.8 Caractéristiques techniques

Paramètre	Valeur
Liaison avec la centrale d'alarme	bus clavier ou port série, selon le type de centrale (4 fils au maximum : +DC, −DC, CLK, DATA ; sur les bus Caddx et Pyronix, CLK n'est pas utilisé)
Entrées / sorties	3 I/O à double fonction (I/O 1, I/O 2, I/O 3) : en entrée NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (résistance de fin de ligne 2,2 kΩ) ; en sortie à collecteur ouvert (OC), max. 0,15 A / 30 V DC
Extension	sur le bus RS485 (version 4G uniquement) : module d'extension iO-8 (+8 I/O) et autres modules de la série iO ; module WiFi W485, module Ethernet E485
Modem 2G	850 / 900 / 1800 / 1900 MHz
Modem 4G	bandes LTE selon la région
Tension d'alimentation	10–18 V DC
Consommation	60–100 mA en nominal ; jusqu'à 500 mA pendant l'émission

Paramètre	Valeur
Protocoles de transmission	TRK, DC-09_2007, DC-09_2012, TL150
Mémoire d'événements	60 messages
Chiffrement	AES-128
Programmation	TrikdisConfig (Windows) par câble USB Mini-B ou à distance ; commandes SMS
Environnement de fonctionnement	−10 … +50 °C, max. 80 % d'humidité relative (à +20 °C)
Dimensions	92 × 65 × 26 mm
Poids	80 g

2. Mise en service rapide avec TrikdisConfig

Tous les réglages du G16 se font avec **TrikdisConfig**, un programme fonctionnant sous Windows – par câble USB ou à distance. Ce chapitre décrit le chemin le plus court : vous configurez l'appareil sur votre bureau, avant le raccordement, et sur place il ne reste plus qu'à le câbler. L'explication détaillée des réglages se trouve au chapitre 6.

2.1 Préparatifs

Ce dont vous aurez besoin

Câble USB Mini-B · câble d'au moins 4 conducteurs pour le bus de la centrale – pour le port série Paradox, câble **CRP2** ou **CRP2B**, pour le port série Texecom, câble **CRP4** · tournevis plat de 2,5 mm · antenne mobile de gain adapté (antenne à gain plus élevé dans les zones de faible couverture) · carte nano-SIM active avec service de données mobiles (la demande de PIN peut être désactivée) · manuel d'installation de la centrale d'alarme. Les accessoires nécessaires se commandent séparément auprès du distributeur.

1. Téléchargez et installez le logiciel TrikdisConfig. Sur le site de Trikdis (www.trikdis.com), tapez « TrikdisConfig » dans le champ de recherche.

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. Ouvrez la face avant du G16. Insérez un tournevis plat dans la fente du bord supérieur du couvercle et, en faisant levier vers le bas, déclipsez doucement la face avant. Le schéma ci-dessous montre l'ouverture et l'emplacement de la prise USB.

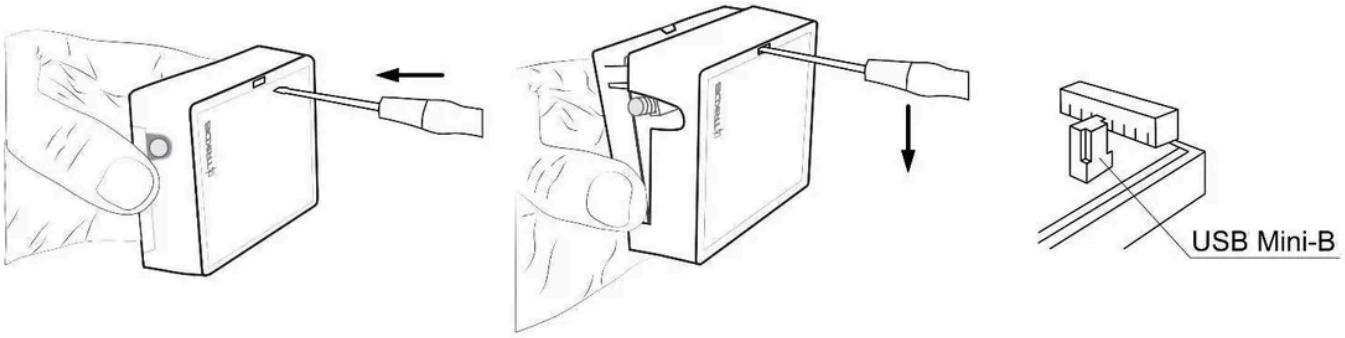


Figure 3. Déclipsage de la face avant avec un tournevis plat (à gauche, au centre) et emplacement de la prise USB Mini-B sur le circuit imprimé (à droite).

3. Insérez la carte nano-SIM dans son support, dans le sens indiqué sur le schéma. La carte doit être active et disposer d'un service de données mobiles ; si possible, désactivez la demande de PIN dans un téléphone (ainsi, il n'est pas nécessaire de saisir le PIN dans l'appareil).

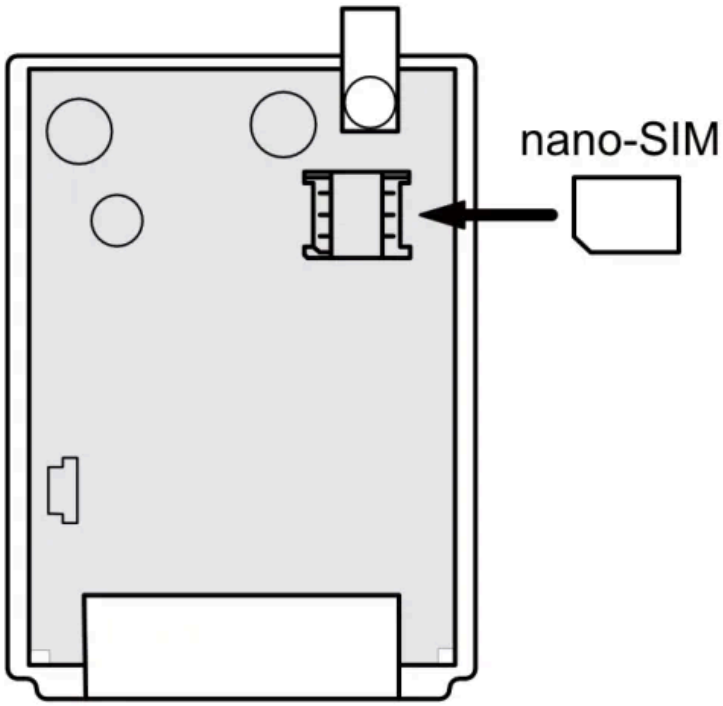


Figure 4. Emplacement de la carte nano-SIM sur le circuit imprimé.

4. Reliez le G16 à l'ordinateur avec un câble USB Mini-B. L'USB fournit assez d'alimentation pour la programmation, une alimentation séparée n'est pas nécessaire.

Avertissement

Tant que l'appareil est relié à l'ordinateur par câble USB, il est en mode programmation : son fonctionnement normal s'arrête, il ne surveille plus, ne transmet plus et ne peut plus être commandé ; il est alimenté par l'USB et redémarre une fois le câble débranché. L'appareil ne doit donc pas être librement accessible : il doit se trouver dans un coffret métallique fermé, avec une protection anti-sabotage (tamper) ou un détecteur de mouvement qui surveille le coffret. Plus de détails dans la FAQ

5. Lancez TrikdisConfig. Le programme reconnaît l'appareil et ouvre la fenêtre de programmation. Cliquez sur le bouton **Read [F4]** (lecture) : le programme lit les réglages actuels de l'appareil. S'il demande un mot de passe, saisissez le code à 6 chiffres administrateur (`123456` d'usine) ou installateur (`654321` d'usine).

2.2 Type de centrale et pilotage direct

Quel que soit le mode utilisé, indiquez d'abord à la page **System settings** à quelle centrale le communicateur sera raccordé.

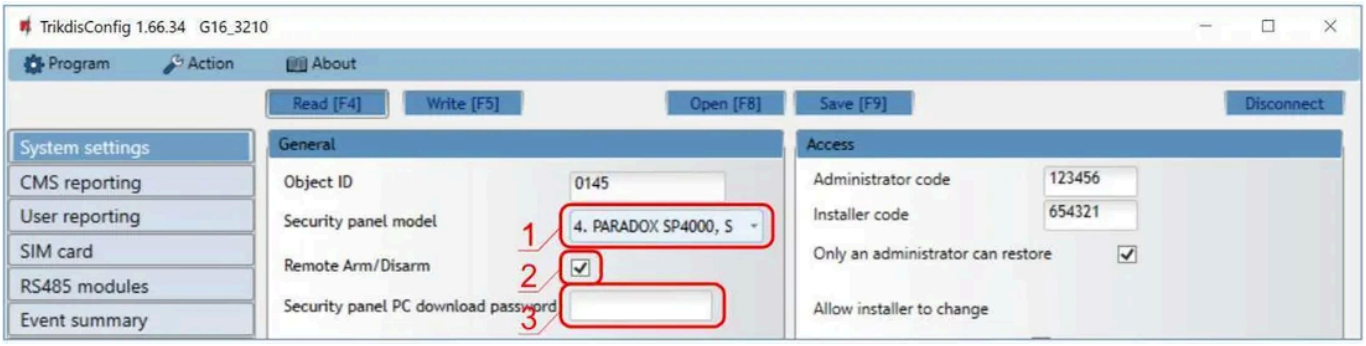


Figure 5. TrikdisConfig – page System settings, groupe General.

- 1 **Security panel model** – le type de la centrale d'alarme raccordée, choisi dans la liste ; c'est de lui que dépend la façon dont le communicateur lit le bus.
- 2 **Remote Arm/Disarm** – cochez cette case si l'utilisateur souhaite armer et désarmer la centrale depuis l'application Protegus 2 avec son propre code clavier. Elle n'apparaît que pour les modèles pilotables directement ; pour les autres centrales, l'armement se fait par une zone à clé (point 3.4) – laissez-la alors décochée.
- 3 **Security panel PC download password** – pour les centrales Paradox et Texecom, le mot de passe PC ou UDL de la centrale (4 caractères) ; il doit être identique à celui réglé dans la centrale. Le champ apparaît après avoir coché Remote Arm/Disarm.

Sur plusieurs centrales, un réglage est aussi nécessaire dans la centrale : pour les centrales Caddx, Honeywell et InnerRange, dès la lecture des événements (activation du bus ou du port série), pour les centrales Paradox et Texecom, pour le pilotage direct (mot de passe PC ou UDL) – le chapitre 4 le décrit par fabricant, y compris la modification du mot de passe.

2.3 Liaison avec l'application Protegus 2

Si l'utilisateur souhaite voir et piloter le système depuis l'application Protegus 2, réglez les points suivants à la page **User reporting**, onglet **PROTEGUS Cloud**.



Figure 6. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- 4 **Enable connection** – cochez : autorise la liaison avec le cloud Protegus.
- 5 **Protegus Cloud access code** – changez le mot de passe d'usine `123456`. C'est ce code qu'il faudra saisir dans l'application lors de la création du système ; **une fois le système créé, il ne peut plus être modifié.**

Ensuite, saisissez les données de la carte à la page **SIM card**.

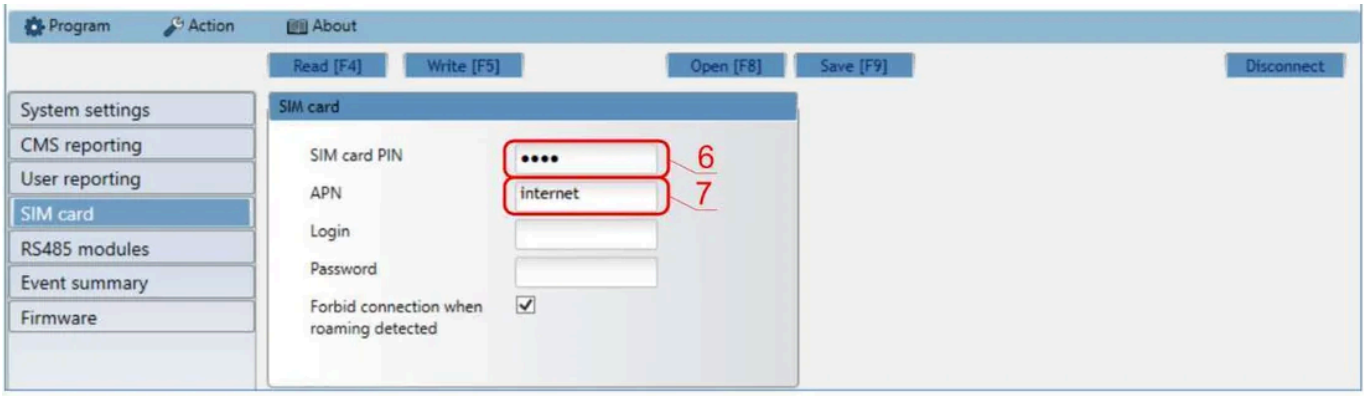


Figure 7. TrikdisConfig – page SIM card.

- 6 **SIM card PIN** – le code PIN de la carte (si la demande de PIN est désactivée, la valeur d'usine peut rester).
- 7 **APN** – le point d'accès aux données de l'opérateur (voir ci-dessous).

L'APN (Access Point Name) est le point d'accès aux données de l'opérateur mobile ; sans lui, l'appareil ne peut pas se connecter à Internet. La valeur exacte vous est fournie par l'opérateur de la carte SIM, et elle se trouve aussi sur le site de l'opérateur ; l'APN « internet » est générique et fonctionne sur le réseau de nombreux opérateurs. Nous tenons à jour les APN connus des opérateurs européens dans un article séparé : Réglage de l'APN – liste des opérateurs mobiles européens.

Pour une carte de données IoT / M2M (de machine à machine), l'opérateur fournit généralement **un APN différent de celui des cartes grand public** – avec l'APN grand public, l'appareil ne se connecte pas. Cette valeur se trouve aussi dans l'article sur les APN, ou demandez-la à l'opérateur ; si l'opérateur fournit aussi un nom d'utilisateur et un mot de passe, saisissez-les également.

2.4 Liaison avec le centre de télésurveillance

Si l'appareil transmet aussi à un récepteur de télésurveillance, saisissez également l'identifiant d'objet à la page **System settings**.

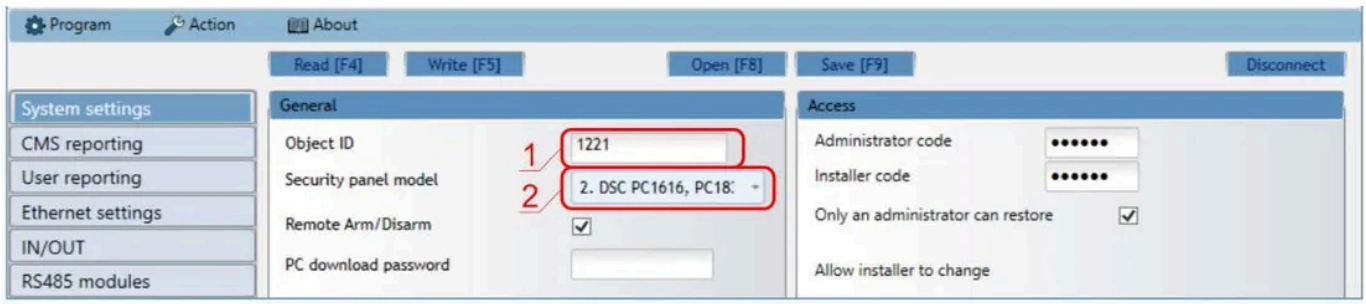


Figure 8. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne peuvent pas être utilisés.
- 2 **Security panel model** – le type de la centrale d'alarme raccordée (si vous ne l'avez pas encore réglé au point 2.2).

Ensuite, à la page **CMS reporting**, dans la partie **Primary channel** (canal principal), réglez les données du récepteur.

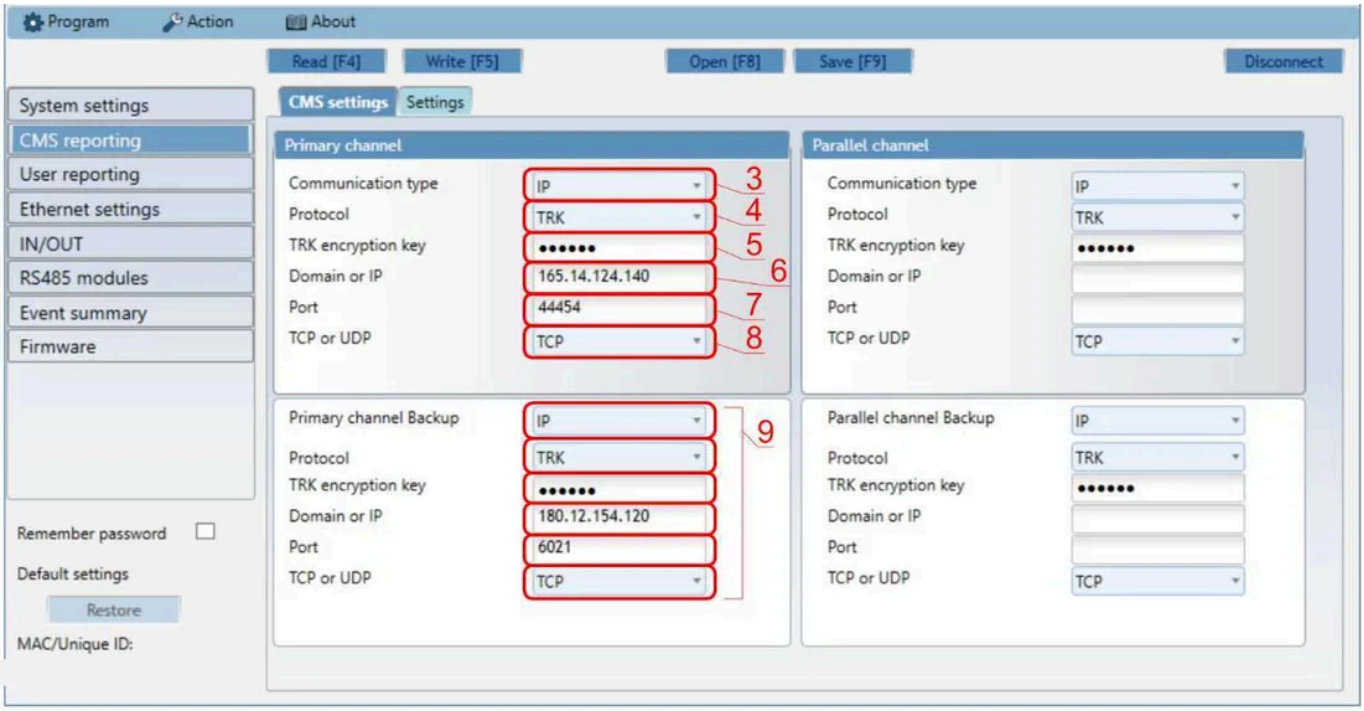


Figure 9. TrikdisConfig – CMS reporting, onglet CMS settings.

- 3 **Communication type** – choisissez la liaison **IP** (le SMS n'est pas recommandé comme canal principal).
- 4 **Protocol** – **TRK** pour un récepteur Trikdis, **DC-09_2007** ou **DC-09_2012** pour un récepteur universel, **TL150** pour un récepteur SUR-GARD.
- 5 **TRK encryption key** – la clé de chiffrement à 6 chiffres réglée dans le récepteur.
- 6 **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- 7 **Port** – le numéro de port du récepteur.
- 8 **TCP or UDP** – le protocole de transport ; il s'aligne sur le réglage du récepteur.
- 9 **Primary channel Backup** – canal de secours en cas de défaut du canal principal ; remplissez-le de la même façon, il est recommandé de le renseigner.

Il est recommandé de régler aussi le **Parallel channel** (canal parallèle) et son canal de secours si les événements doivent parvenir à deux récepteurs ; dans le champ **Backup SMS reporting number** – ce qui est également recommandé – vous pouvez saisir le numéro de téléphone du récepteur SMS Trikdis : l'appareil y envoie un SMS immédiatement après le premier démarrage, puis il transmet par SMS lorsque aucun canal IP ne fonctionne.

Enfin, saisissez les données de la carte à la page **SIM card**, si vous ne l'avez pas encore fait au point 2.3.

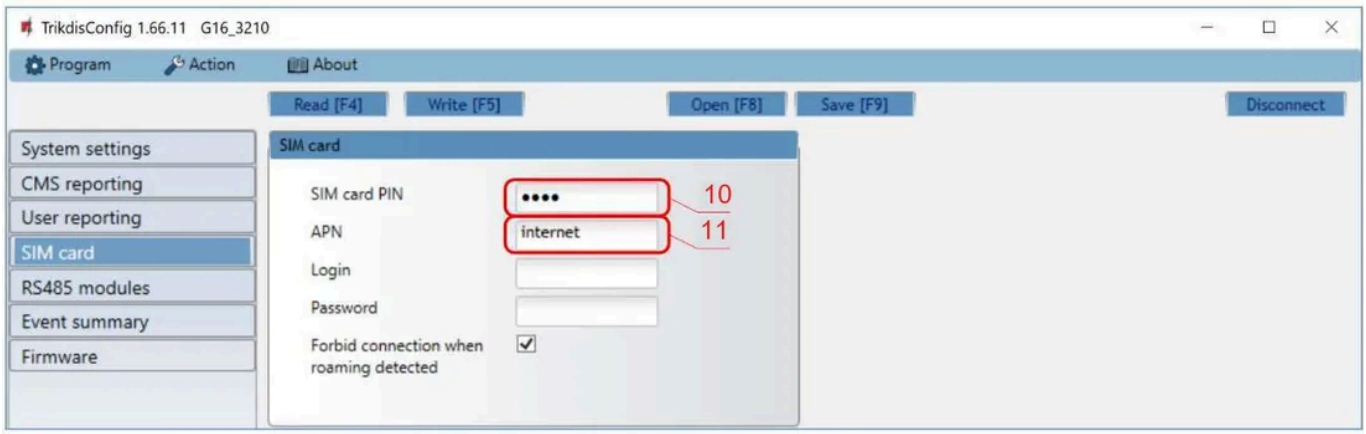


Figure 10. TrikdisConfig – page SIM card.

- 10 **SIM card PIN** – le code PIN de la carte.
- 11 **APN** – le point d'accès de l'opérateur (voir le point 2.3).

La **transmission par SMS** au centre de télésurveillance ne fonctionne qu'avec un récepteur Trikdis (récepteur IP/SMS RL14, récepteur multicanal RM14 ou récepteur SMS GM14) ; dans ce cas, seuls la clé de chiffrement et le numéro de téléphone sont nécessaires. Avec le protocole **DC-09**, saisissez aussi à l'onglet **Settings** les numéros d'objet, de ligne et de récepteur DC-09.

À la fin des réglages, appuyez sur le bouton **Write [F5]** (écriture), attendez la confirmation et débranchez le câble USB. L'appareil est alors prêt à être raccordé.

3. Installation et raccordement

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 Les étapes de l'installation

1. Retirez la face avant (voir le point 2.1) et débrochez le bornier.
2. Insérez la carte nano-SIM, si vous ne l'avez pas encore fait lors de la mise en service.
3. Sortez le circuit imprimé du fond du boîtier : ouvrez le loquet situé dans le coin (voir le schéma).
4. Fixez le fond du boîtier avec des vis à l'emplacement choisi.
5. Remettez le circuit imprimé dans le fond du boîtier et rebranchez le bornier.
6. Vissez l'antenne GSM.
7. Remettez la face avant.

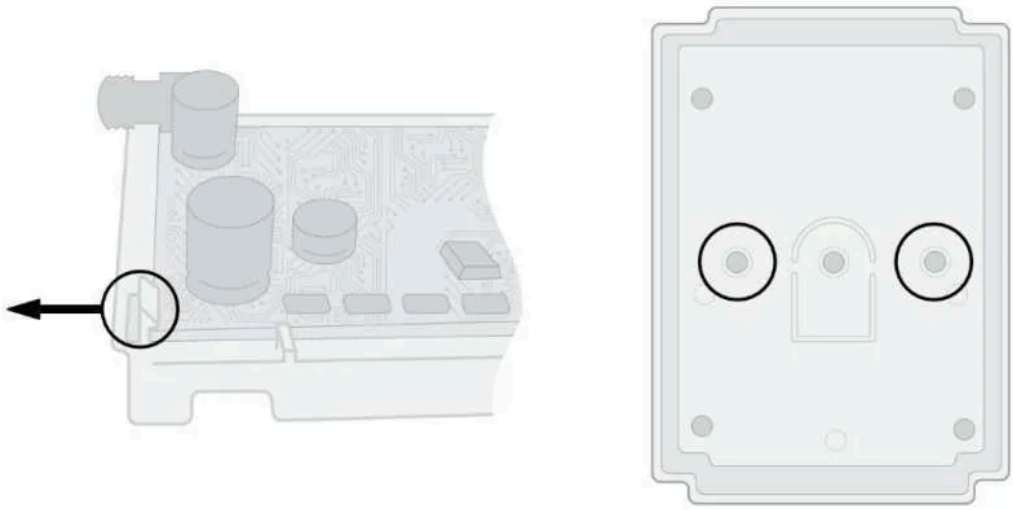


Figure 11. Retrait du circuit imprimé : ouverture du loquet dans le coin (à gauche) et trous de fixation du fond du boîtier (à droite, entourés).

La carte SIM doit être active et, pour une utilisation en IP, la liaison de données mobile doit y fonctionner. Si vous ne souhaitez pas que TrikdisConfig demande un code PIN, désactivez la demande de PIN de la carte dans un téléphone.

3.2 Emplacement et antenne

- Placez le communicateur dans un endroit **sec, à l'intérieur**, de préférence près du coffret de la centrale d'alarme, pour que le câble du bus soit court.
- **Dans un coffret métallique**, le signal mobile est fortement atténué. Si le communicateur est placé dans le boîtier métallique de la centrale, sortez l'antenne à l'extérieur du coffret ou utilisez une antenne à câble plus long.
- Avant la fixation définitive, **vérifiez le niveau du signal** : le nombre de clignotements jaunes de la LED NETWORK doit être d'au moins 5 en 2G et d'au moins 3 en 4G (voir le point 1.7). S'il est inférieur, cherchez un meilleur emplacement ou passez à une antenne plus sensible, pouvant être placée plus loin.
- Tenez l'antenne et le communicateur à l'écart du transformateur de la centrale et des câbles secteur.



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 Raccordement à la centrale d'alarme

Le G16 se raccorde à la centrale avec **quatre fils au maximum** (sur les bus Caddx et Pyronix, CLK n'est pas utilisé) : sur les bornes **+DC** et **−DC** arrive l'alimentation auxiliaire 12 V (AUX) de la centrale, sur les bornes **CLK** et **DATA** les deux fils de données du bus clavier ou du port série de la centrale. La correspondance des bornes de la centrale varie selon le fabricant – raccordez selon les schémas ci-dessous. Pour les centrales à port série (Paradox, Texecom), un câble d'origine est disponible : une extrémité s'enfiche dans le connecteur de la centrale, l'autre se raccorde au bornier du G16.

Pendant l'émission, le G16 peut consommer jusqu'à 500 mA. Vérifiez que la sortie AUX de la centrale le supporte avec les autres appareils qui y sont raccordés. Comme l'alimentation est fournie par la centrale, en cas de coupure de courant, la batterie de la centrale alimente aussi le communicateur. La plupart des centrales ne sont pas endommagées par l'inversion des fils d'un appareil raccordé au bus, mais l'inversion de **+DC et −DC** peut détruire le communicateur – vérifiez la polarité avant le raccordement.

Après le raccordement, il faut choisir le type de la centrale raccordée dans le champ **System settings** → **Security panel model** de TrikdisConfig (point 2.2) ; chez certains fabricants, un réglage est aussi nécessaire dans la centrale (chapitre 4).

3.3.1 DSC PowerSeries

Les quatre bornes du Keybus : **RED** → +DC, **BLK** → −DC, **YEL** → CLK, **GRN** → DATA.

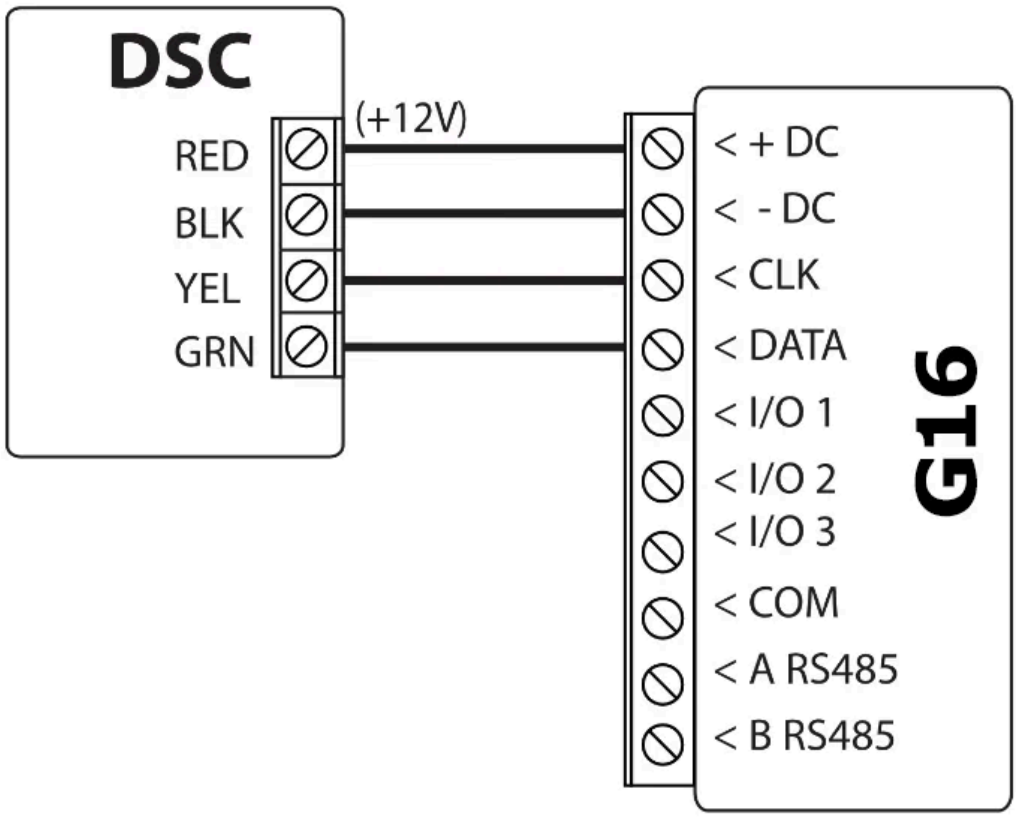


Figure 12. Raccordement au Keybus d'une centrale DSC PowerSeries (bus clavier, « Keypad bus ») : RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Le communicateur se raccorde au **port série** (SERIAL) des centrales Paradox avec le câble d'origine **CRP2** ou **CRP2B** ; l'extrémité côté centrale s'enfiche dans le connecteur série, l'autre extrémité se raccorde au bornier du G16. Les 4 broches du connecteur : **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Les couleurs des conducteurs diffèrent entre les deux câbles – le schéma montre la répartition des couleurs des deux câbles. Marquage du connecteur série Paradox : AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

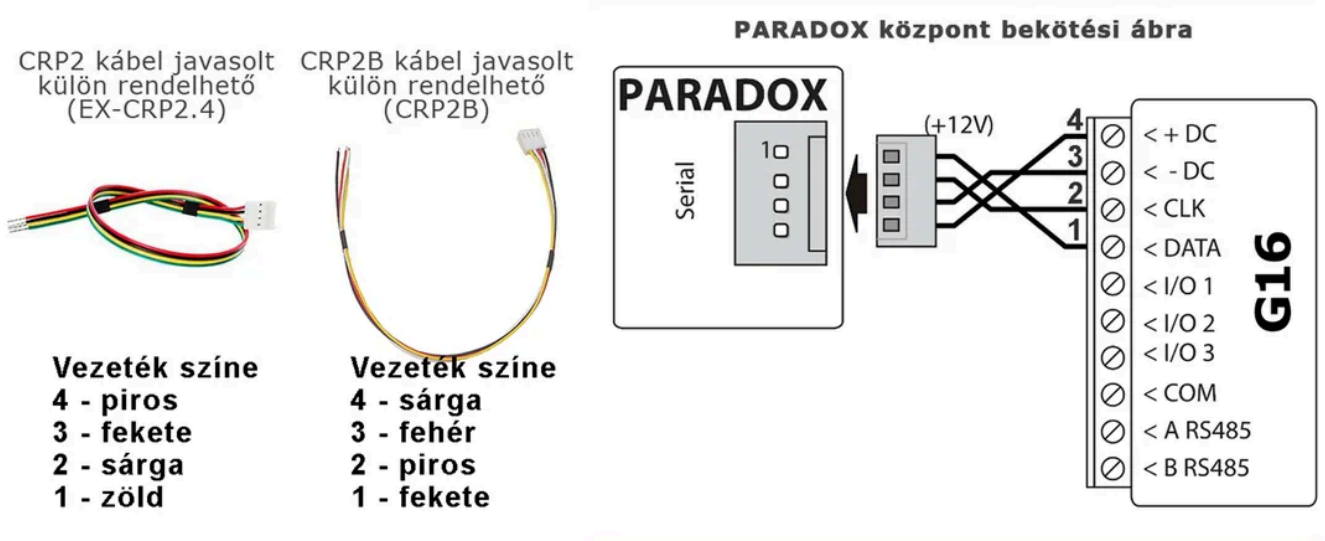


Figure 13. Raccordement au port série d'une centrale Paradox avec le câble CRP2 (EX-CRP2.4) ou CRP2B. CRP2 : 4 rouge → +DC, 3 noir → −DC, 2 jaune → CLK, 1 vert → DATA. CRP2B : 4 jaune → +DC, 3 blanc → −DC, 2 rouge → CLK, 1 noir → DATA.

Sur les centrales Paradox récentes, le port série peut être verrouillé d'usine – la procédure de déverrouillage se trouve au point 4.2 et dans l'article Déverrouillage du port série verrouillé des centrales d'alarme Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

Les trois bornes du bus clavier : **POS** → +DC, **COM** → −DC, **DATA** → DATA. La borne **CLK** n'est pas utilisée.

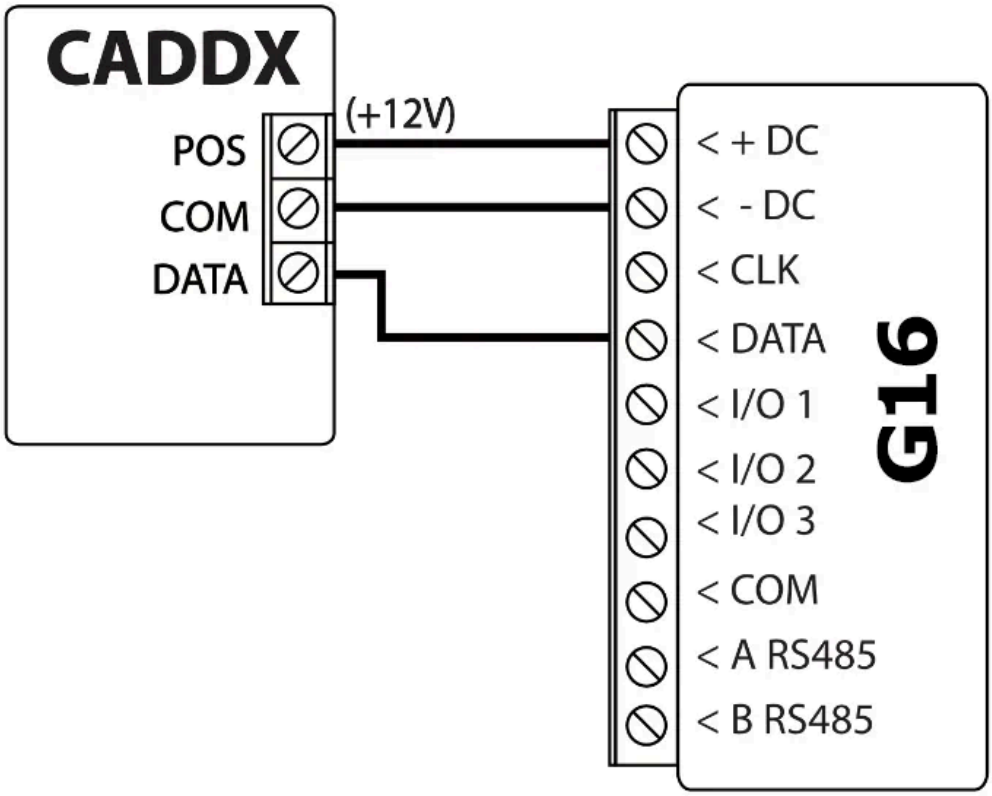


Figure 14. Raccordement au bus clavier d'une centrale Caddx NetworX (« Keypad bus ») : POS → +DC (+12 V), COM → −DC, DATA → DATA ; CLK reste libre.

3.3.4 Texecom Premier / Premier Elite

Le communicateur se raccorde au port série de la centrale avec le câble d'origine **CRP4** : **rouge (R)** → +DC, **noir (B)** → −DC, **bleu (BL)** → CLK, **blanc (W)** → DATA.

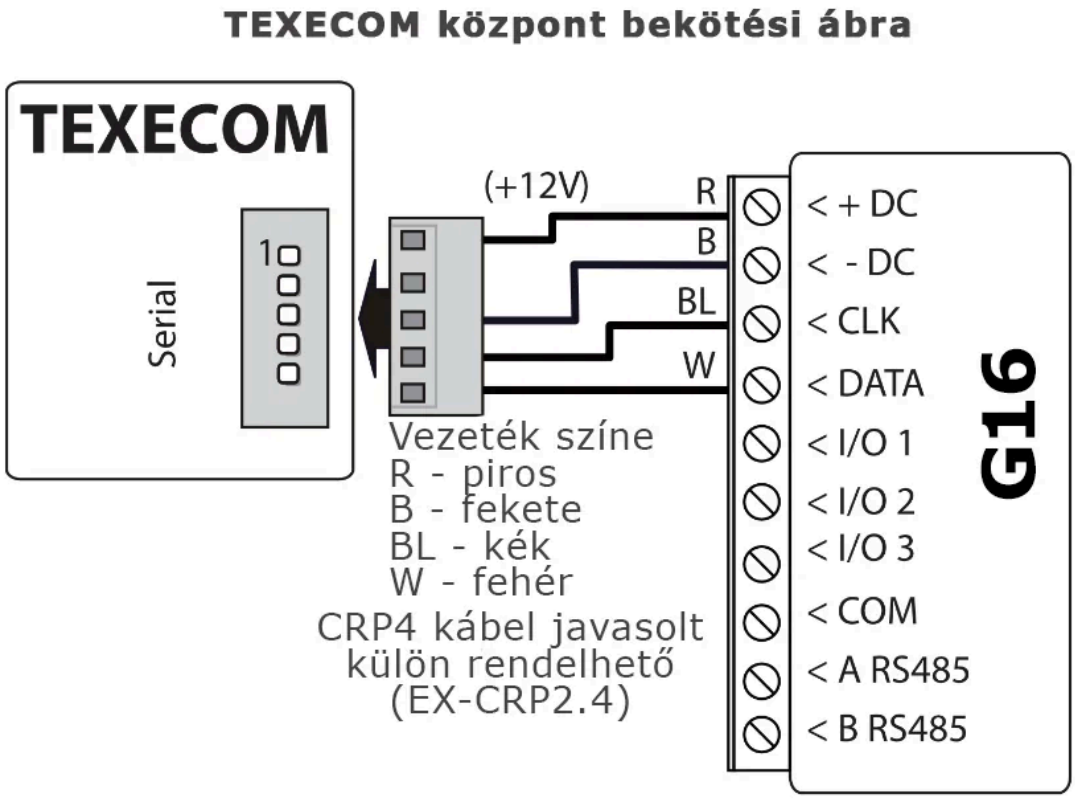


Figure 15. Raccordement au port série d'une centrale Texecom avec le câble CRP4 : rouge → +DC, noir → −DC, bleu → CLK, blanc → DATA.

3.3.5 Crow Runner

Le bus clavier des Crow Runner 4/8 et Runner 8/16 : **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

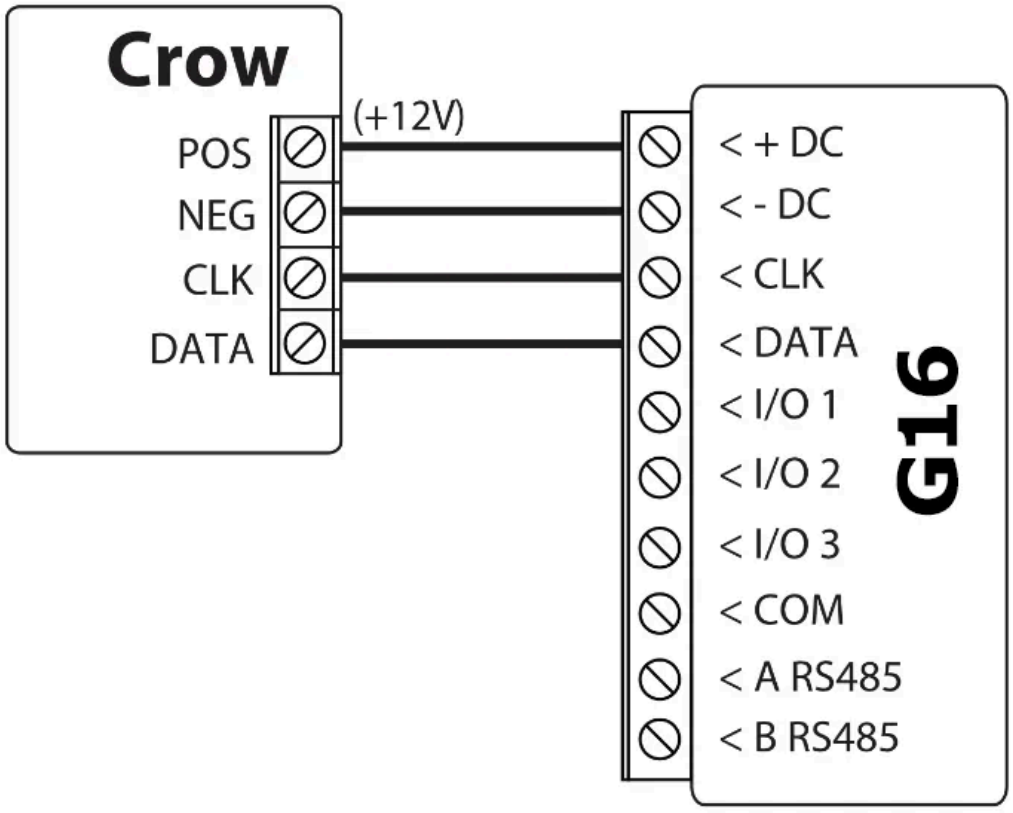


Figure 16. Raccordement au bus clavier d'une centrale Crow Runner 4/8 et Runner 8/16 (« Keypad bus ») : POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Le bus clavier des centrales Pyronix : **+AUX** → +DC, **–AUX** → −DC, **KD** → DATA. La borne **CLK** n'est pas utilisée. Après le raccordement et la configuration du communicateur, mettez la centrale hors tension puis redémarrez-la pour qu'elle accepte le communicateur (point 4.5).

3.3.7 Honeywell Ademco Vista

Les bornes numérotées du bus clavier des centrales Vista-15, Vista-20 et Vista-48 : **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (sortie de données, jaune) → CLK, **6** (entrée de données, vert) → DATA.

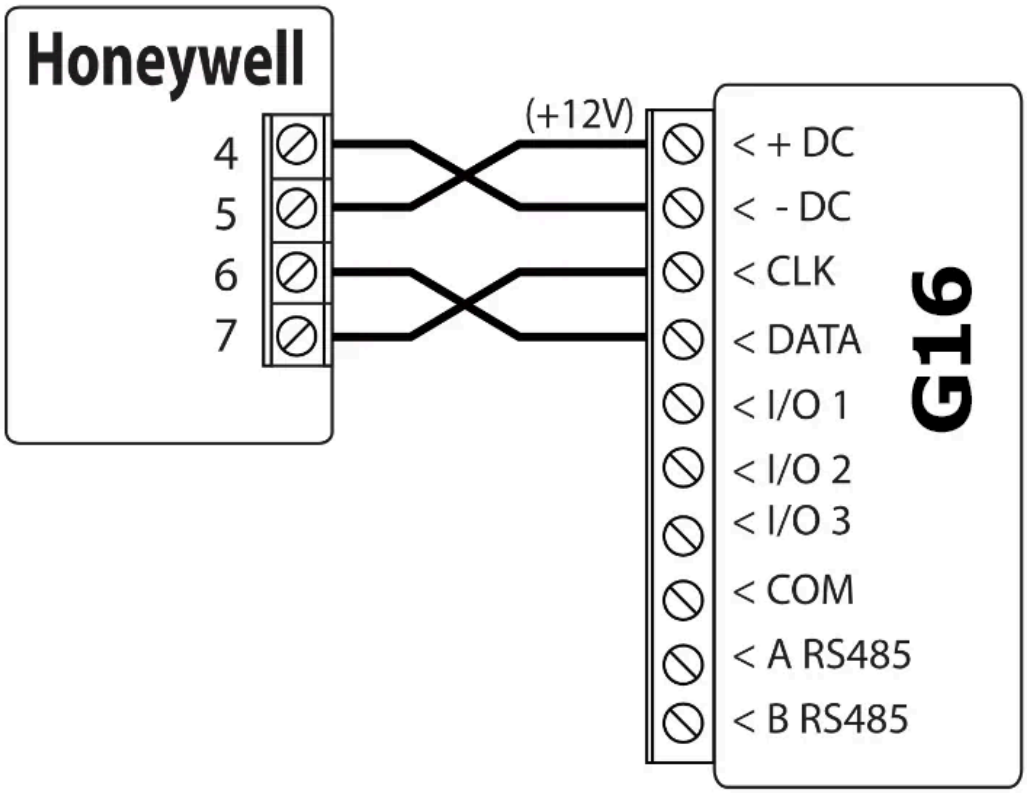


Figure 17. Raccordement au bus clavier d'une centrale Honeywell Vista-20 / Vista-48 (« Keypad bus ») : 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception et Integriti

Le communicateur est alimenté par les bornes d'alimentation de la centrale **Inception** (**VOUT +** → +DC, **0V** → −DC), et la liaison de données se fait par le port USB de la centrale, avec le câble InnerRange 993030USB : **noir** → 0V (−DC), **vert** → CLK, **blanc** → DATA. Dans la centrale, l'utilisation du port série doit être activée (point 4.7).

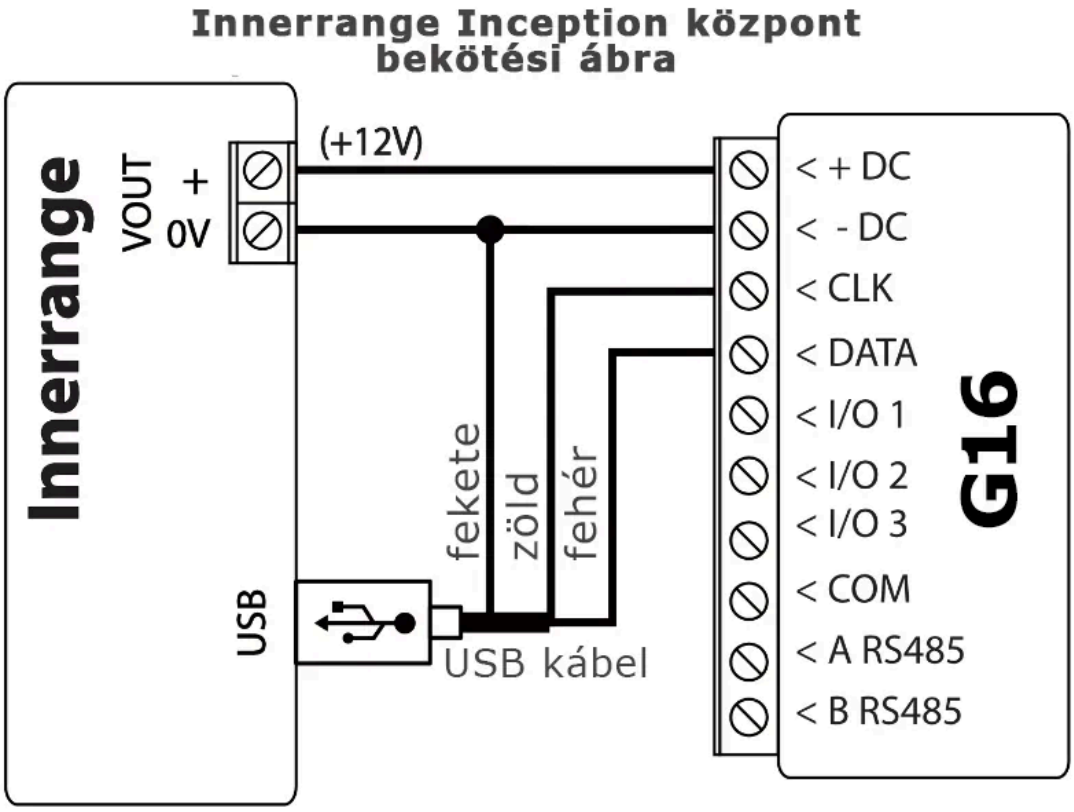


Figure 18. Raccordement à une centrale InnerRange Inception : alimentation depuis les bornes VOUT + et 0V, données depuis le port USB avec le câble 993030USB (noir → 0V, vert → CLK, blanc → DATA).

La centrale **Integriti** se raccorde par son port 0 (Port 0) avec le câble INTG-996795 : **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Raccordement d'une zone à clé

Si la centrale ne fait pas partie des modèles pilotables directement, ou si vous ne souhaitez pas utiliser le pilotage direct, l'armement et le désarmement à distance se font par une **zone à clé** : vous configurez une des bornes I/O du communicateur **en sortie** (page IN/OUT, point 6.6) et vous la raccordez à une zone à clé de la centrale. À l'activation, la sortie tire la zone vers COM (négatif) ; raccordez la résistance de fin de ligne de la zone selon le type de zone de la centrale. Comme le G16 a trois bornes I/O, jusqu'à trois partitions peuvent être gérées avec une sortie chacune.

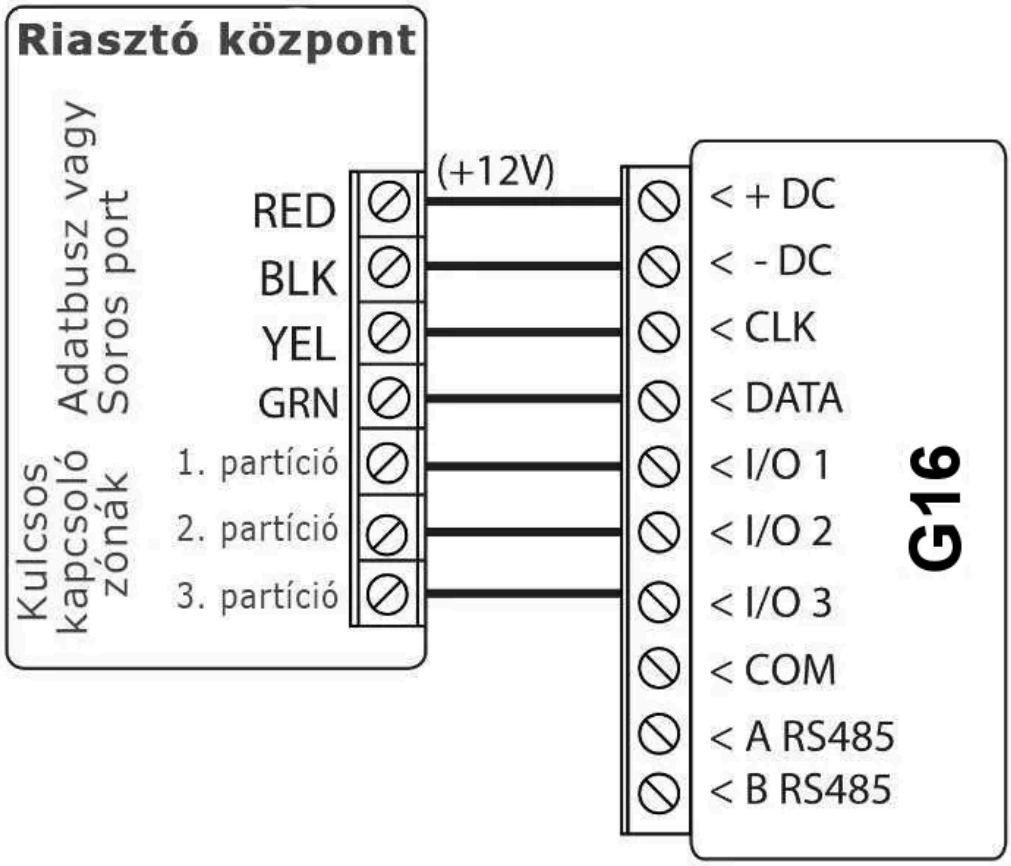


Figure 19. Armement et désarmement par zone à clé : le communicateur lit les événements sur le bus de la centrale, et les sorties I/O 1–3 commandent la zone à clé des partitions 1–3 de la centrale.

- À la page **System settings** de TrikdisConfig, **Remote Arm/Disarm** doit rester **décoché** – les deux ne peuvent pas être utilisés en même temps.
- La zone à clé peut être à impulsion ou à deux positions ; il faut régler le même mode dans l'application Protegus 2 (point 5.3).
- Sur la **version matérielle 3**, les deux sorties (OUT1, OUT2) peuvent gérer deux partitions ; le champ **System settings → Output OUT1 & OUT2 mode** doit être sur **Remote control** (réglage d'usine).

Un article séparé présente les détails et les pièges de l'armement par zone à clé : Armement à distance par zone à clé depuis l'application Protegus 2.

3.5 Raccordement des entrées

Utilisées en entrée, les bornes I/O du communicateur peuvent aussi recevoir des détecteurs supplémentaires (p. ex. contact d'autoprotection, bouton panique, thermostat), indépendamment de la centrale d'alarme. L'entrée se raccorde entre la borne I/O choisie et la borne COM.

Les entrées acceptent les types de circuit suivants : **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La résistance de fin de ligne est de **2,2 kΩ**. Avec une simple fin de ligne (EOL), le court-circuit comme la coupure comptent comme une alarme ; la double fin de ligne (DEOL), avec deux résistances, distingue l'alarme et l'autoprotection (court-circuit ou coupure). Le réglage d'usine est NO (normalement ouvert) ; le type d'entrée se règle sur la page **IN/OUT** de TrikdisConfig, selon le câblage.

Type	État de repos	Alarme	Autoprotection
NC	fermé	ouvert	–

Type	État de repos	Alarme	Autoprotection
NO	ouvert	fermé	–
NC/EOL	2,2 kΩ	coupure ou court-circuit	–
NO/EOL	2,2 kΩ	court-circuit ou coupure	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	coupure ou court-circuit
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	coupure ou court-circuit

Lorsque l'entrée est déclenchée, le communicateur envoie son propre événement à la télésurveillance et à Protegus 2 ; le code Contact ID ainsi que les numéros de partition et de zone de l'événement se définissent sur la page **IN/OUT**.

Raccordement des circuits d'entrée : types NO, NC, NC/EOL, NO/EOL, NO/DEOL et NC/DEOL avec résistance de fin de ligne de 2,2 kΩ ; pour les types DEOL, le circuit d'autoprotection est également raccordé.

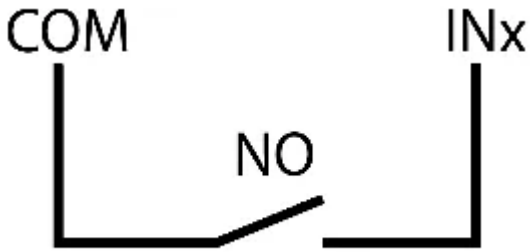


Figure 20. NO – circuit ouvert au repos : fermé – alarme, ouvert – état de repos.

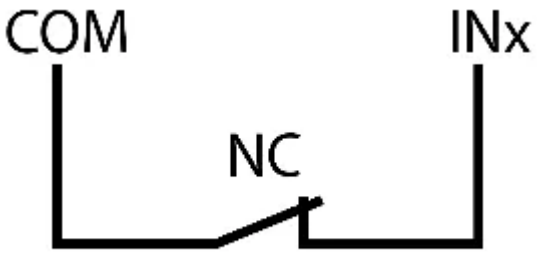


Figure 21. NC – circuit fermé au repos : ouvert – alarme, fermé – état de repos.

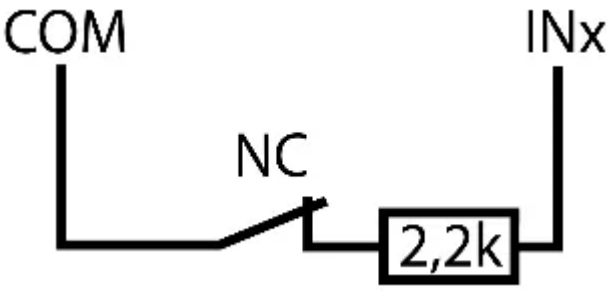


Figure 22. NC/EOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

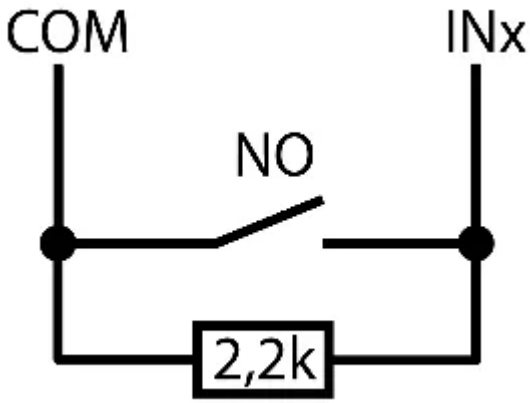


Figure 23. NO/EOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

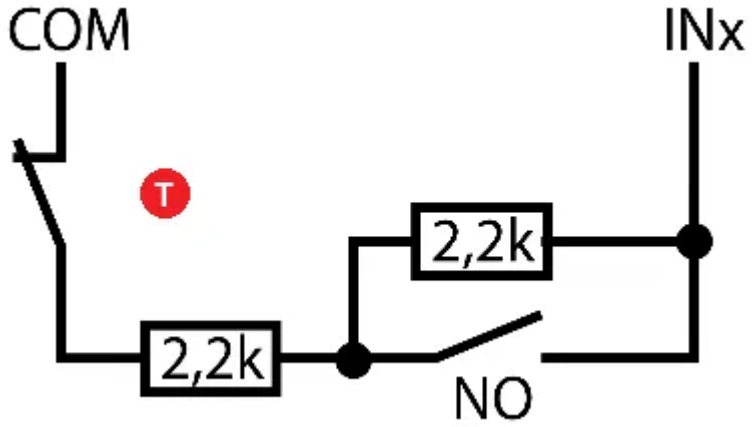


Figure 24. NO/DEOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

- T contact d'autoprotection (« Tamper »), signale l'ouverture du boîtier du détecteur

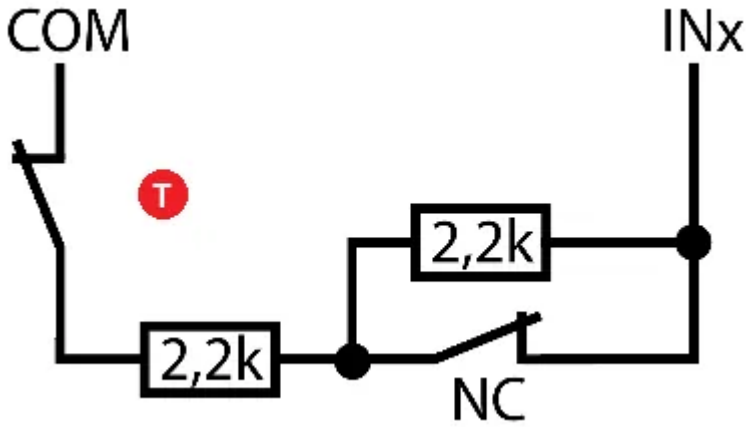


Figure 25. NC/DEOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

- T contact d'autoprotection (« Tamper »), signale l'ouverture du boîtier du détecteur

La **version matérielle 3** a une seule entrée (IN) ; son type se règle dans le champ **System settings → Input IN type**.

3.6 Raccordement d'une sortie avec un relais

Utilisées en sortie, les bornes I/O sont des sorties à collecteur ouvert (OC) : à l'état actif, elles tirent la charge raccordée vers le négatif, avec 0,15 A au maximum, jusqu'à 30 V DC. Commutez un consommateur plus puissant ou un appareil sur tension secteur **par l'intermédiaire d'un relais** : une extrémité de la bobine du relais va sur +DC, l'autre sur la borne I/O. Les contacts du relais permettent d'allumer et d'éteindre différents appareils électriques. Pour cela, la borne I/O doit être réglée en sortie (**OUT**) à la page **IN/OUT** de TrikdisConfig (point 6.6).

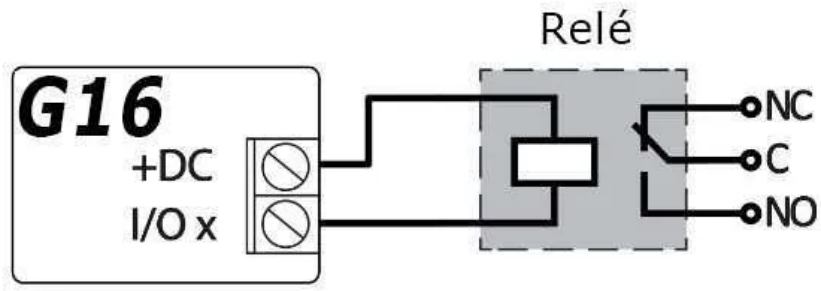


Figure 26. Raccordement d'un relais sur la sortie du communicateur : la bobine se place entre +DC et la borne I/O x, les contacts (NC, C, NO) commutent le consommateur.

Vous pouvez commander les sorties depuis l'application Protegus 2 ou par commande SMS (chapitre 5).

3.7 Raccordement du module d'extension iO-8

Si davantage d'entrées ou de sorties sont nécessaires, jusqu'à quatre modules d'extension **iO-8** peuvent être raccordés sur le bus RS485 de la **version 4G** ; chacun ajoute 8 I/O à double fonction. Reliez les bornes A 485 et B 485 aux bornes A et B du module, et prenez l'alimentation du module sur la sortie AUX 12 V de la centrale. Le manuel propre de l'iO-8 décrit aussi le raccordement. Le module doit être ajouté à la page **RS485 modules** de TrikdisConfig (point 6.7) ; les événements des entrées sont transmis au centre de télésurveillance et à Protegus 2, et les sorties se commandent depuis l'application.

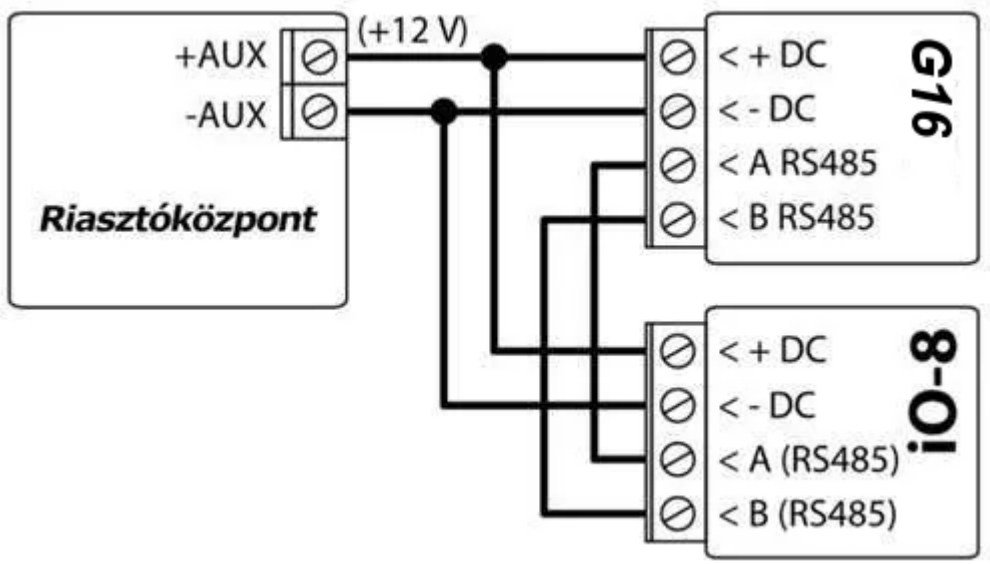


Figure 27. Raccordement du module d'extension iO-8 au bus RS485 du G16 (A 485 → A, B 485 → B) ; les deux appareils sont alimentés par la sortie AUX de la centrale d'alarme (+12 V).

Le G16 à modem 2G (G16_G410) n'a pas de bus RS485 : on ne peut donc pas y raccorder de module iO-8, W485 ou E485.

3.8 Raccordement des modules W485 et E485

Extension Ethernet ou Wi-Fi – W485 et E485. Le communicateur peut être complété par un module Wi-Fi W485 ou Ethernet E485 : les événements sont alors transmis à la télésurveillance et à l'application Protegus 2 par Internet filaire ou par Wi-Fi.

- **Raccordement :** sur le bus RS485, avec une alimentation commune au communicateur (entrée d'alimentation du module 9–28 V DC) ; aucune alimentation séparée n'est nécessaire.
- **Internet est le canal principal :** tant qu'il fonctionne, tout passe par lui. S'il est interrompu, le communicateur bascule automatiquement sur le réseau mobile et, dès le retour d'Internet, revient sur IP.
- **Pas seulement la transmission d'alarmes :** l'application Protegus 2 (notifications, commande à distance) fonctionne également par ce canal.
- **E485** – Ethernet filaire (RJ45). **W485** – Wi-Fi 2,4 GHz (WPA / WPA2), là où aucun câble UTP n'est tiré.
- Si nécessaire, il peut aussi être utilisé sans carte SIM. Configuration : avec le logiciel TrikdisConfig, par USB.

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

Tant que la liaison WiFi ou Ethernet fonctionne, le G16 communique par elle et n'utilise pas la liaison de données mobile ; si la liaison est interrompue, il bascule sur la liaison de données mobile et revient au module lorsque la liaison est rétablie. Pour que le module fonctionne, **une carte SIM doit se trouver dans le G16**.

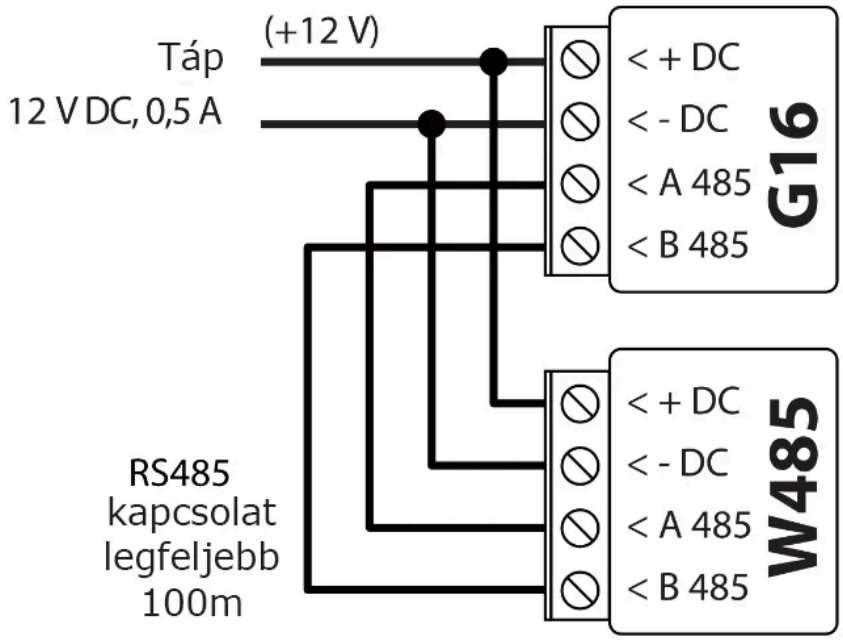


Figure 28. Raccordement du module WiFi W485 au G16 par le bus RS485. Les deux appareils fonctionnent sur une alimentation commune de 12 V DC (au moins 0,5 A) (entrée d'alimentation du module : 9–28 V DC) ; le câble RS485 peut mesurer 100 m au maximum.

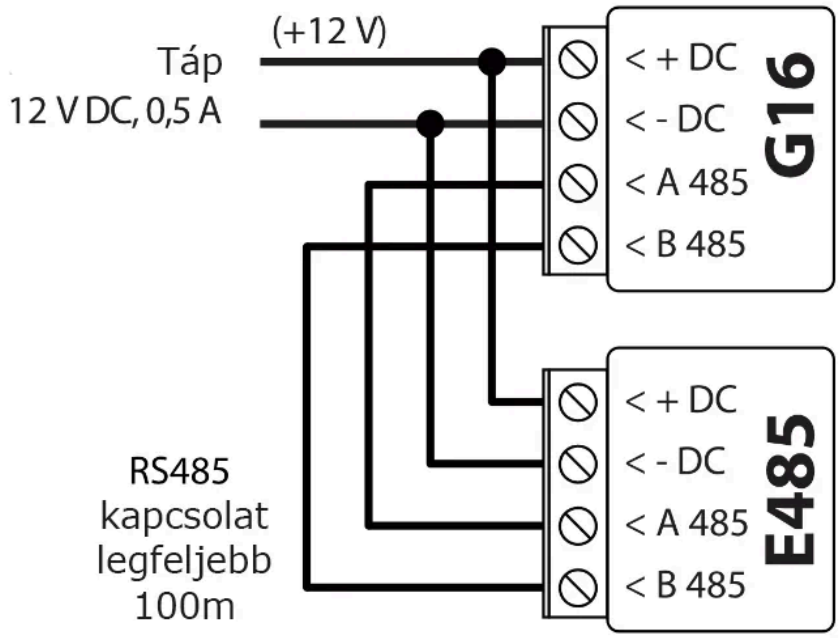


Figure 29. Raccordement du module Ethernet E485 au G16 par le bus RS485. Les deux appareils fonctionnent sur une alimentation commune de 12 V DC (au moins 0,5 A) (entrée d'alimentation du module : 9–28 V DC) ; le câble RS485 peut mesurer 100 m au maximum.

Les distances « jusqu'à … m » sont des maximums théoriques atteignables dans des conditions idéales. En pratique, la qualité et le cheminement du câble, les sources de perturbations et, pour les liaisons radio, les murs et le terrain donnent une portée nettement plus courte. Prévoyez une marge et, sur les longues distances, vérifiez la liaison lors de la mise en service.

Les réglages réseau des modules se font à la page **RS485 modules** de TrikdisConfig (point 6.7).

3.9 Mise sous tension et première vérification

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.

Après le raccordement, le communicateur démarre en même temps que la centrale d'alarme est mise sous tension. Sur la face avant, vous devez voir :

- **POWER** allumée en vert – l'alimentation est correcte ;
- **NETWORK** allumée en vert et clignotant en jaune – connecté au réseau ; le nombre de clignotements indique le niveau du signal (5 en 2G, 3 en 4G correspondent à un bon signal) ;
- **TROUBLE** éteinte.

Si la LED NETWORK donne moins de clignotements jaunes, le niveau du signal est insuffisant : cherchez un autre emplacement pour le communicateur ou utilisez une antenne plus sensible (point 3.2). Toute autre signalisation des LED indique un défaut – identifiez-le à l'aide des tableaux du point 1.7. Si TROUBLE clignote, le nombre de clignotements en indique la cause (point 1.7). **7 clignotements** signalent l'absence de liaison avec la centrale : vérifiez les fils CLK et DATA, le type de centrale choisi et – si nécessaire – la programmation de la centrale (chapitre 4). Si aucune LED ne s'allume, vérifiez l'alimentation et le câblage.

4. Programmation de la centrale d'alarme

Ce chapitre décrit, par fabricant, ce qu'il faut régler dans la centrale d'alarme pour que le G16 lise les événements et – lorsque c'est possible – pilote la centrale à distance. Sur la plupart des centrales, il n'y a rien à programmer pour la lecture des événements ; pour le **pilotage direct**, cochez **Remote Arm/Disarm** à la page **System settings** de TrikdisConfig et, pour une centrale Paradox ou Texecom, saisissez aussi le mot de passe PC ou UDL de la centrale dans le champ **Security panel PC download password** (points 2.2 et 6.2).

Si vous pilotez la centrale non pas directement, mais par une zone à clé (point 3.4), **Remote Arm/Disarm** doit rester décoché, et ce chapitre ne concerne que les réglages nécessaires à la lecture des événements.

4.1 DSC

Les centrales **DSC PowerSeries** (liste des modèles pris en charge au point 1.2) ne nécessitent aucun réglage particulier : le communicateur raccordé au Keybus lit immédiatement les événements et, une fois **Remote Arm/Disarm** coché, l'utilisateur arme et désarme depuis l'application avec son propre code clavier. Les détails de la commande directe – états des zones, exclusion de zones, détection automatique des partitions – font l'objet d'un article séparé : Commande directe des centrales d'alarme DSC PowerSeries.

Le communicateur ne fonctionne pas avec les centrales **DSC PowerSeries NEO** : le fabricant de la centrale n'autorise aucun appareil externe sur le bus NEO. Pour une NEO, il faut un communicateur sur ligne téléphonique (TIP/RING) – voir DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions.

4.2 Paradox

Les centrales **Paradox** ne doivent être programmées que pour la commande directe ; aucun réglage n'est nécessaire pour la lecture des événements. Le firmware de la centrale doit être au moins en version **V.4**.

Sur les centrales Paradox plus récentes (par exemple les séries SP+, MG+ et EVOHD+), le port série peut être **verrouillé en usine** : le communicateur ne reçoit aucune donnée tant que le port n'est pas déverrouillé. Procédure de déverrouillage : Déverrouillage du port série verrouillé sur les centrales d'alarme Paradox.

Pour la commande, il faut régler le **mot de passe PC** (PC password) de la centrale et saisir le même dans le champ **System settings** → **Security panel PC download password** de TrikdisConfig – les deux doivent être identiques.

1. Entrez dans la programmation installateur de la centrale depuis le clavier.
2. Ouvrez la section du mot de passe PC : section **911** pour les séries **MAGELLAN et SPECTRA**, section **3012** pour la série **DIGIPLEX EVO**.
3. Saisissez un mot de passe de **4 caractères**. Le mot de passe ne peut pas être 0000 et **ne doit pas commencer par zéro**.
4. Quittez la programmation et **redémarrez la centrale** – la modification du mot de passe PC prend effet après le redémarrage. Saisissez ensuite le même mot de passe dans TrikdisConfig.

Erreurs fréquentes et solutions

- Le **code clavier attribué à la partition ne peut pas être le code maître** : donnez un autre code à l'utilisateur, et l'armement / le désarmement depuis Protegus 2 fonctionnera avec celui-ci.
- **Après toute modification d'un code clavier, redémarrez le communicateur** (coupure d'alimentation ou commande SMS `RESET`) : il lit les codes au démarrage et ne voit pas les modifications ultérieures.

4.3 Texecom

Les centrales **Texecom Premier / Premier Elite** doivent être programmées aussi bien pour la lecture des événements que pour la commande : il faut régler le mot de passe à 4 caractères de la centrale appelé **UDL passcode** et saisir le même dans le champ **System settings** → **Security panel PC download password** de TrikdisConfig – les deux doivent être identiques.

Avec le logiciel Wintex de Texecom : l'UDL passcode se trouve dans l'onglet **Options** de la fenêtre **Communication Options**.

Depuis le clavier :

1. Saisissez le code installateur à 4 chiffres et appuyez sur la touche **[Menu]** pour entrer dans le menu de programmation.
2. Appuyez immédiatement après sur la touche **[9]**.
3. Appuyez sur **[7][6]**, puis sur la touche **[2]**, et saisissez l'UDL passcode à 4 chiffres.
4. Appuyez sur la touche **[Yes]**, puis quittez la programmation avec la touche **[Menu]**.

4.4 UTC Interlogix (Caddx)

Le firmware de la centrale **UTC Interlogix (Caddx) NetworX** doit être au moins en version **V2**. Les réglages suivants se font sur le clavier de la centrale :

1. Appuyez sur les touches **[*][8]** et saisissez le code installateur (en usine **9713**).
2. Saisissez le **numéro d'appareil** attribué au communicateur (device address ; en usine **0**).
3. Programmez l'une après l'autre les lignes du tableau ci-dessous : saisissez l'emplacement (location), le numéro de segment, puis le réglage. La touche **[*]** permet de revenir au champ précédent. `12345678` signifie que les huit interrupteurs du segment sont activés (tous les chiffres sont visibles à l'écran).

Emplacement (location)	Segment	Réglage
23	3	12345678
37 (pas forcément nécessaire)	3	12345678
37 (pas forcément nécessaire)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Une fois toutes les lignes programmées, appuyez deux fois sur la touche **[Exit]** pour quitter la programmation.

4.5 Crow et Pyronix

Les centrales **Crow Runner 4/8** et **Runner 8/16** ne nécessitent aucun réglage particulier.

Les centrales **Pyronix** ne nécessitent pas non plus de programmation, mais après le réglage et le raccordement du communicateur, **mettez la centrale hors tension** (secteur et batterie) et redémarrez-la : la centrale accepte au démarrage le communicateur raccordé à son bus.

4.6 Honeywell Ademco Vista

Le firmware des centrales **Honeywell Ademco Vista-20** et **Vista-48** doit être au moins en version **V5.3**. Le réglage se fait sur le clavier de la centrale.

Accès à la programmation – de deux façons :

- saisissez le code installateur (en usine **4112**), puis les touches **[8][0][0]** ; ou
- mettez la centrale sous tension et, **dans les 50 secondes**, appuyez simultanément sur les touches **[*]** et **[#]** (cela ne fonctionne que si l'on a quitté la programmation précédente avec les touches [*][9][8]).

Réglages :

1. Activez l'envoi des événements Contact ID sur la sortie radio longue portée (LRR) : appuyez sur les touches **[*][2][9][1][#]**.
2. Pour la commande à distance, autorisez l'utilisation de la **2e adresse AUI** (2nd AUI address) : appuyez sur les touches **[*][1][8][9][1][1][#]**.

Sortie de la programmation : appuyez sur les touches **[*][9][9]**.

4.7 InnerRange Inception et Integriti

Le firmware de la centrale **InnerRange Inception** doit être au moins en version **2.3.0.3507-r0**, et la centrale a besoin d'une connexion Internet. Le réglage se fait dans l'interface web de la centrale :

1. Ouvrez dans un navigateur l'adresse `https://skytunnel.com.au/inception/NUMERODESERIE`, où NUMERODESERIE est le numéro de série figurant sur la boîte de la centrale. Connectez-vous avec le compte installateur.
2. Ouvrez la page **Configuration → General → Alarm Reporting**.
3. Dans le groupe **3rd Party Device Configuration** : - cochez l'option **Enable 3rd Party Device Reporting** ; - dans le champ **3rd Party Device Type**, choisissez la valeur **Trikdis** ; - dans le champ **Serial Port**, choisissez la valeur **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Enregistrez les réglages et quittez l'interface.

Le firmware de la centrale **InnerRange Integriti** doit être au moins en version **19.1.0.36608**, et son logiciel de programmation (Integriti Professional) au moins en version **19.1.0.15396**. Le réglage se fait dans le logiciel de programmation de la centrale :

1. Pour le port série (**TTL Port-0**) auquel le communicateur est raccordé, choisissez le protocole de communication **Trikdis**.
2. Le format de données doit être **Contact ID**.
3. Réglage du port : **19200, 8, N, 1**.
4. Enregistrez les réglages et quittez le logiciel.

L'Inception et l'Integriti transmettent les événements au communicateur ; pour l'armement et le désarmement, une zone à clé est nécessaire (points 1.2 et 3.4).

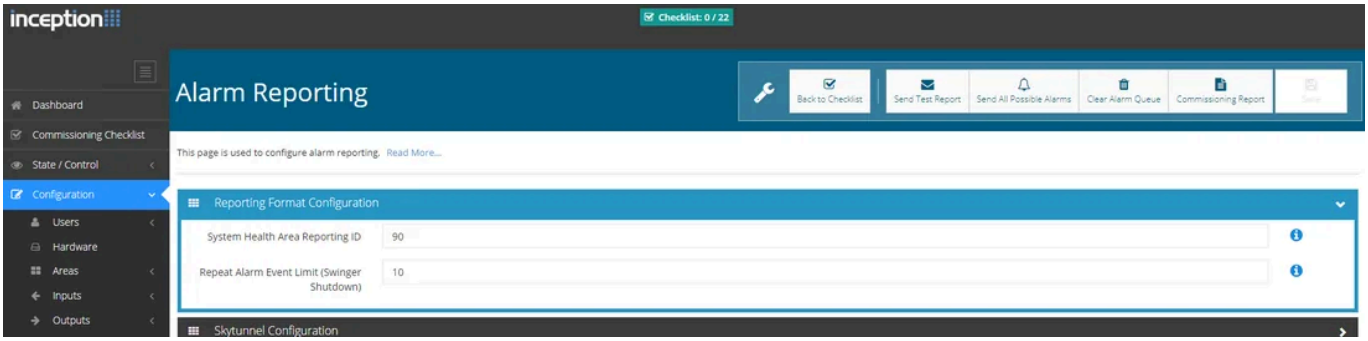


Figure 30. Interface web de l'Inception – Configuration → General → Alarm Reporting.



Figure 31. Inception – 3rd Party Device Configuration.

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

5. Pilotage à distance avec Protegus 2

Avec l'application mobile et web Protegus 2, l'utilisateur voit à distance l'état du système, reçoit des notifications sur les événements, peut armer et désarmer et commander les sorties du communicateur. Avec le G16, l'armement peut se faire de deux façons : sur les centrales **pilotables directement**, avec le **code clavier** propre de l'utilisateur ; sur les centrales raccordées par une zone à clé, avec une **sortie** du communicateur.

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez :

1. La carte SIM est active et la liaison de données mobile y fonctionne ; son code PIN est saisi dans l'appareil, ou la demande de PIN est désactivée.
2. À la page **User reporting** → **PROTEGUS Cloud** de TrikdisConfig, **Enable connection** est coché et le **Protegus Cloud access code** est réglé (une fois le système créé, il ne peut plus être modifié).
3. La LED **POWER** est allumée en vert, la LED **NETWORK** est allumée en vert et clignote en jaune.

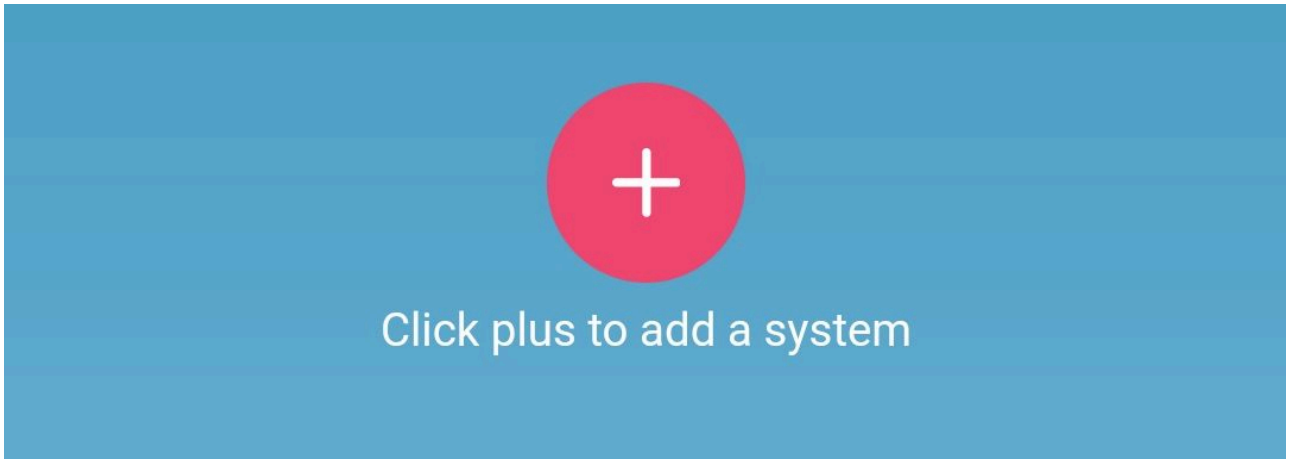
La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur le réseau de l'opérateur ; pour un appareil Ethernet, que la liaison jusqu'au routeur fonctionne –, mais pas que l'appareil accède aussi à Internet. Si la LED NETWORK est verte mais que la LED DATA reste allumée en continu après un événement ou un rapport de test, la connexion Internet ne fonctionne pas : le message ne peut pas partir. Sur le réseau mobile, la cause la plus fréquente est l'APN ou le service de données de la carte SIM ; en Ethernet, le routeur, le pare-feu ou le DNS. Si la LED DATA s'éteint, le message est parti et la connexion de données fonctionne.

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

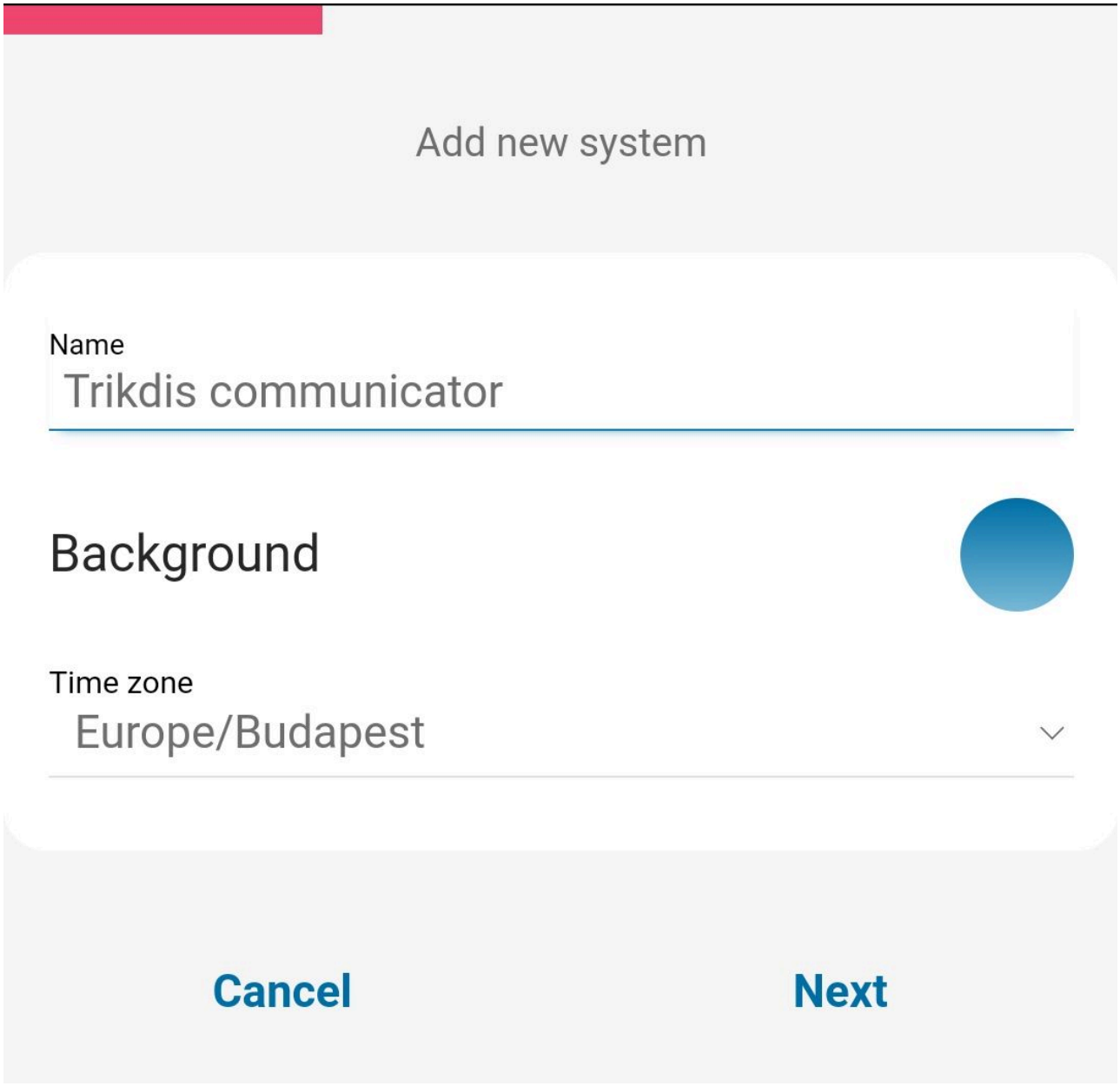
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



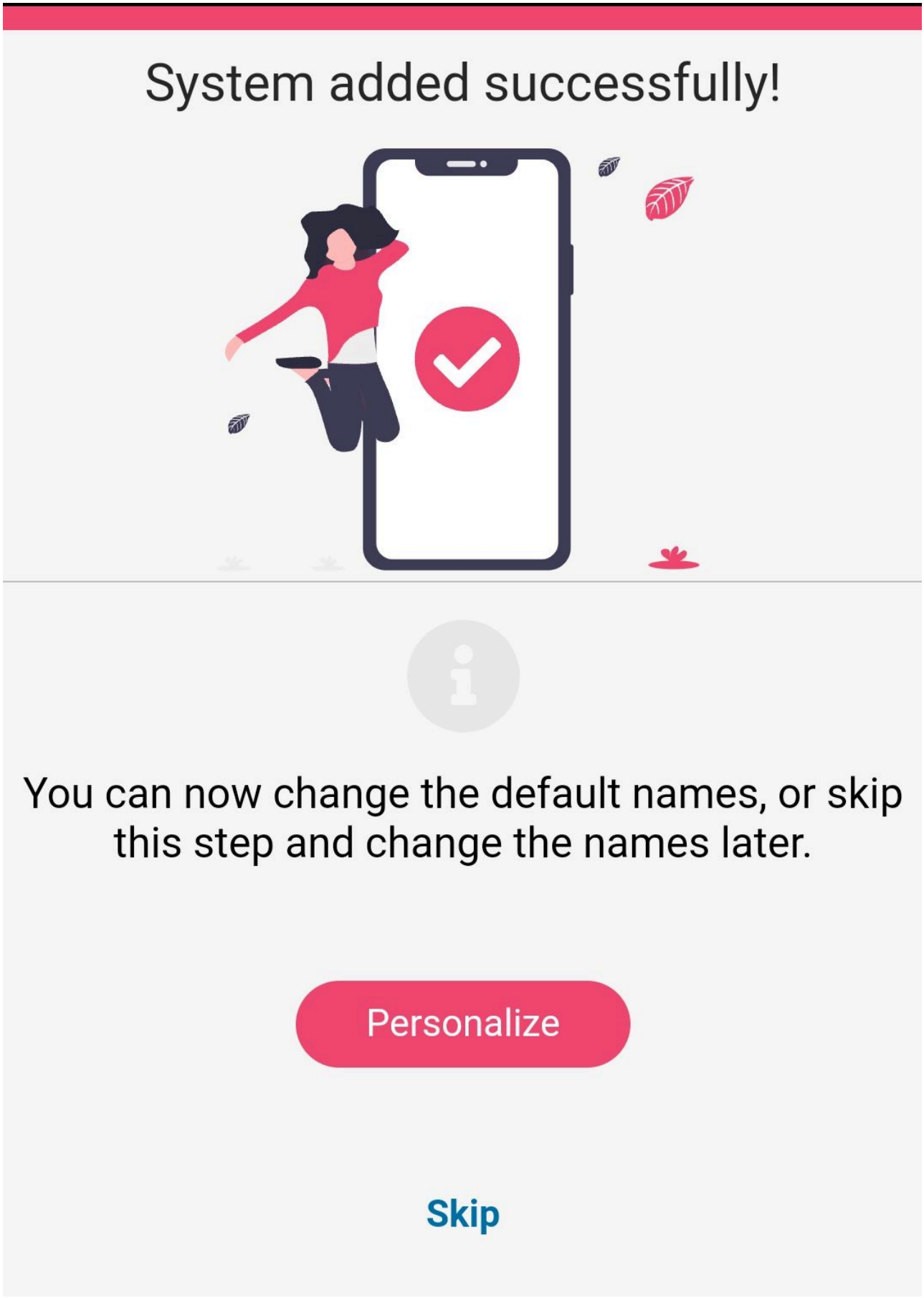
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



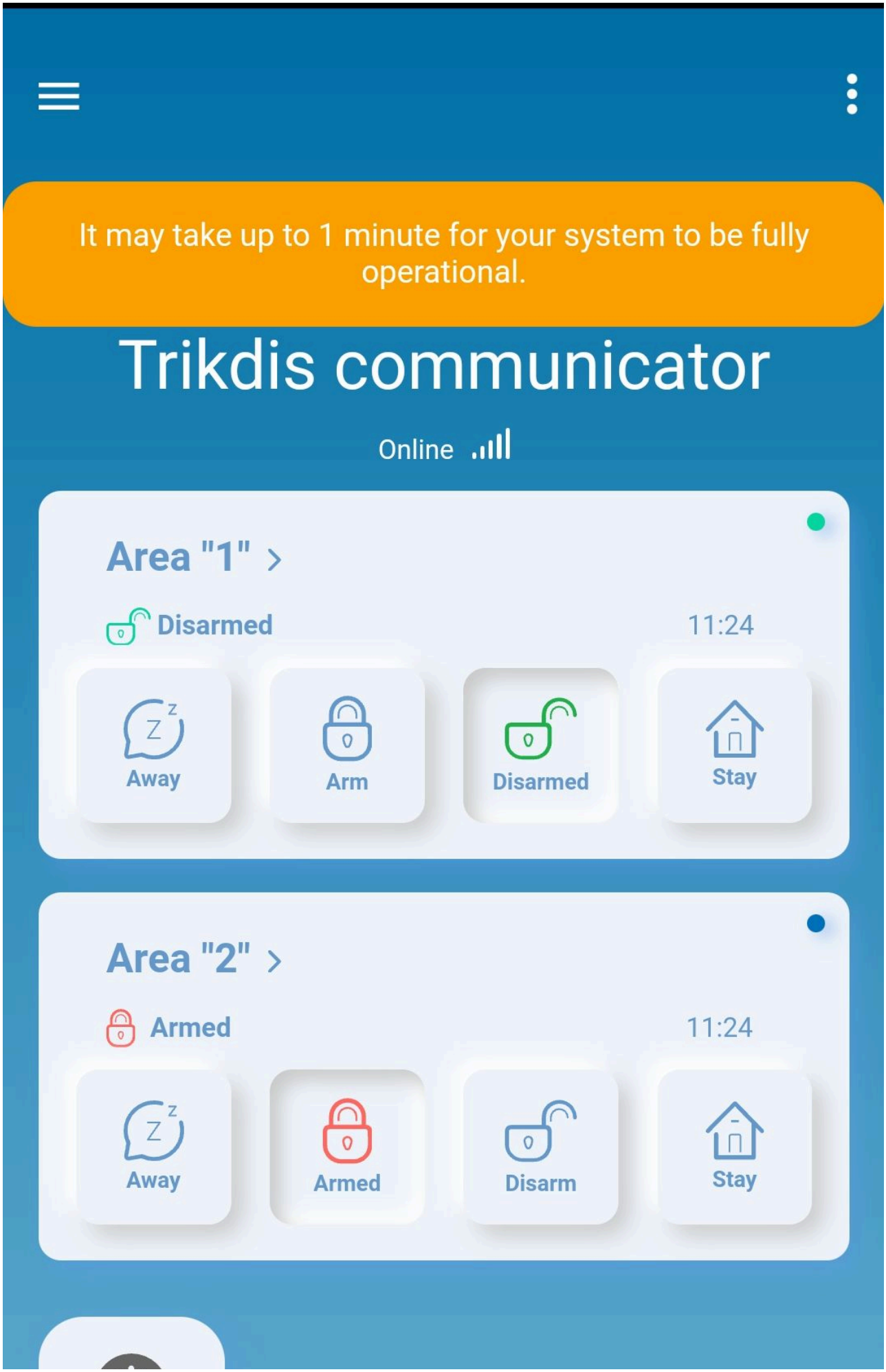
6. Add meg a rendszer nevét és válassz idozónát



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



L'identifiant unique de l'appareil (**IMEI**) figure sur la boîte et au dos de l'appareil, et la barre d'état de TrikdisConfig l'affiche aussi.

5.2 Pilotage direct avec le code clavier

Si la centrale fait partie des modèles pilotables directement (point 1.2) et que **Remote Arm/Disarm** est coché à la page **System settings** de TrikdisConfig, Protegus 2 affiche les partitions de la centrale avec l'état lu sur le bus, et pour armer / désarmer, l'utilisateur saisit dans l'application **le code clavier de la centrale** – le même que celui qu'il utilise sur le clavier. Aucune sortie ni zone à clé séparée n'est nécessaire.

- Selon le fabricant, un réglage est nécessaire pour cela dans la centrale (Paradox : mot de passe PC, Texecom : mot de passe UDL ; pour les centrales Caddx, Honeywell et InnerRange, l'activation du bus ou du port série est déjà nécessaire pour la lecture des événements) – voir le chapitre 4.
- Le code clavier est vérifié par la centrale, et le journal d'événements de la centrale enregistre l'utilisateur, et non le communicateur.
- Sur une centrale Paradox, le code de l'utilisateur **ne peut pas être le code maître** ; après une modification de code, redémarrez le communicateur (point 4.2).
- Sur une centrale DSC PowerSeries, l'application affiche aussi l'état des zones, et l'exclusion de zones est possible – détails dans l'article sur le pilotage direct DSC.

Lors de la création du système, Protegus 2 demande si l'armement est commandé par une sortie du communicateur. En pilotage direct, **n'attribuez pas** de sortie à la partition (**Control with Protegus2** désactivé) : la partition est gérée par la centrale, l'état arrive par le bus.

5.3 Armement par zone à clé

Si la centrale ne peut pas être pilotée directement, ou si vous ne souhaitez pas l'utiliser ainsi, vous raccordez une sortie du communicateur à la zone à clé de la centrale (point 3.4), **Remote Arm/Disarm** reste décoché dans TrikdisConfig, et dans Protegus 2, vous attribuez la sortie à la partition.

Si vous souhaitez armer et désarmer la centrale d'alarme via la sortie du communicateur, par l'intermédiaire de la zone à clé de la centrale, indiquez dans l'application Protegus 2, au niveau de la partition, quelle sortie la commande.

La zone de la centrale à laquelle la sortie du communicateur est raccordée doit être programmée dans la centrale comme **zone à clé**, et la centrale doit transmettre les événements d'armement et de désarmement – c'est à partir de ceux-ci que Protegus 2 affiche l'état de la partition.

Le réglage peut se faire lors de la création du système, à l'ajout des partitions, ou ultérieurement dans les réglages du système, en modifiant la partition. Lors de la création du système, l'assistant de Protegus 2 vous guide : cliquez sur le bouton **Continue** (Continuer), saisissez le nom de la partition (**Area name**) et autorisez la commande de la sortie PGM depuis l'application Protegus 2 – cela se fait selon les étapes ci-dessous :

1. Sélectionnez (ou ajoutez) la partition que vous souhaitez commander. Le numéro de partition doit correspondre à celui que la centrale envoie dans les événements (partition 1 = 1, partition 2 = 2).

2. Activez l'option **Commande par PGM** (Control with Protegus2) et, dans le champ **sortie** (Assigned Output), choisissez la sortie du communicateur (PGM1, PGM2 …). Une sortie ne peut commander qu'une seule partition.
3. Choisissez le mode de fonctionnement : **impulsion** (Pulse) ou **deux états** (Level) – le même que celui réglé dans la centrale pour la zone à clé. On utilise généralement le mode impulsion ; la durée de l'impulsion peut aussi être définie (par défaut 3 s).
4. Enregistrez le réglage (**Save**). S'il y a plusieurs partitions, répétez l'opération pour chacune, avec sa propre sortie : dans l'assistant, vous ajoutez une autre partition avec le bouton **Click to add an area** et réglez sa sortie PGM de la même manière. Une fois toutes les partitions réglées, passez à la suite dans l'assistant avec le bouton **Skip**.

Protegus 2 ne peut afficher correctement l'état des partitions que si la centrale envoie les événements d'armement et de désarmement avec le bon numéro de partition. Les détails et les pièges de l'armement par zone à clé font l'objet d'un article séparé : Armement à distance par zone à clé depuis l'application Protegus 2.

5.4 Armer et désarmer depuis l'application

1. Ouvrez le système dans l'application Protegus 2. Sur l'écran d'accueil, chaque partition a sa propre carte et son cadenas : un **cadenas fermé rouge** indique une partition armée, un **cadenas ouvert vert** une partition désarmée.
2. Touchez le cadenas de la partition et choisissez l'opération souhaitée : armement ou désarmement (mise hors service).
3. Si l'application le demande, saisissez le code PIN.

Le cadenas prend l'état réel à la suite de l'événement reçu de la centrale d'alarme ; l'application confirme également dans la liste des événements et par une notification si la centrale a exécuté l'opération.

En pilotage direct, l'application demande le code clavier de la centrale ; en armement par zone à clé – s'il est activé – le mot de passe Protegus 2.

5.5 Pilotage par SMS

Le communicateur peut aussi être commandé et programmé par SMS. Structure du message :

`MOTDEPASSE espace COMMANDE espace DONNÉE` – par exemple `123456 OUTPUT1 ON`

Avec le mot de passe **administrateur**, toutes les commandes sont utilisables ; avec le mot de passe **installateur**, les commandes INFO, RESET et OUTPUTx. `x` est le numéro de la sortie : la borne E/S configurée en sortie (1, 2 ou 3) que vous souhaitez commuter.

Commande	Donnée	Fonction	Exemple
`INFO`	–	Demande des informations sur l'appareil : type, IMEI, numéro de série, version du firmware	`123456 INFO`
`RESET`	–	Redémarre l'appareil	`123456 RESET`
`OUTPUTx`	`ON`	Active la sortie x	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Désactive la sortie x	`123456 OUTPUT1 OFF`

Commande	Donnée	Fonction	Exemple
`OUTPUTx`	`PULSE=tttt`	Délivre une impulsion sur la sortie x ; `tttt` = durée de l'impulsion en secondes, sur quatre chiffres	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Active ou désactive la connexion Protegus	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adresse:port`	Adresse IP et port du canal principal	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=clé`	Clé de chiffrement TRK	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=nom`	APN de la carte SIM	`123456 CONNECT APN=internet`
`CONNECT`	`USER=nom`	Nom d'utilisateur APN (si l'opérateur le demande)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=motdepasse`	Mot de passe APN (si l'opérateur le demande)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Sélection du type de centrale d'alarme par son numéro d'ordre dans la liste **Security panel model** de TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=nnnn` / `DIR=OFF`	Mot de passe à 4 chiffres de la commande directe (mot de passe PC ou UDL de la centrale) ; `DIR=OFF` la désactive	`123456 CONNECT DIR=1122`

Vous pouvez limiter les numéros de téléphone depuis lesquels l'appareil accepte des commandes : TrikdisConfig → page **User reporting** → **Control by SMS**. Si aucun numéro n'est indiqué, il exécute toute commande comportant le bon mot de passe, quel que soit le numéro d'origine.

6. TrikdisConfig – les réglages en détail

Dans la fenêtre de TrikdisConfig, on voit à gauche la liste des pages (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), en haut la barre de boutons (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) et en bas la barre d'état. Ce chapitre passe en revue les réglages du G16 page par page.

6.1 La barre d'état

Après la connexion et la lecture de l'appareil (**Read [F4]**), les principales données de l'appareil s'affichent en bas de la fenêtre :

Libellé	Signification
IMEI / Unique ID, pour un appareil Ethernet **MAC / Unique ID**	Identifiant unique de l'appareil : IMEI pour un appareil à carte SIM, adresse MAC pour un appareil Ethernet. Le même identifiant figure sur la boîte et au dos de l'appareil.
Status	État de fonctionnement actuel.
Device	Type de l'appareil (référence). Vérifiez que c'est bien le type de votre appareil qui figure ici.

Libellé	Signification
SN	Numéro de série.
BL	Version du bootloader.
FW	Version du firmware.
HW	Version du matériel.
State	Mode de connexion : USB ou à distance (remote).
Administrator / Installer	Niveau d'accès de la personne qui programme (après saisie du mot de passe).

Une fois les réglages effectués, vous les écrivez dans l'appareil avec le bouton **Write [F5]** ; les boutons **Open [F8]** et **Save [F9]** permettent d'enregistrer l'ensemble des réglages dans un fichier et de le charger dans un autre appareil. **Save [F9]** enregistre les réglages dans un fichier de configuration, **Open [F8]** ouvre le fichier enregistré ; vous pourrez ensuite charger les réglages enregistrés dans d'autres appareils et configurer ainsi rapidement plusieurs appareils avec des réglages identiques.

Pour le G16, le champ **Device** doit indiquer la référence du G16 (par exemple G16_G410 ou G16_54E0). Après la lecture, le programme affiche les réglages enregistrés dans le G16 ; réglez-les selon les descriptions des pages ci-dessous.



Figure 32. La barre d'état de TrikdisConfig avec un G16 lu : identifiant, état, modèle, numéro de série, versions, mode de connexion et niveau d'accès.

6.2 System settings

La page comporte deux groupes : dans le groupe **General**, vous réglez le fonctionnement de base de l'appareil et sa liaison avec la centrale d'alarme, dans le groupe **Access**, les niveaux d'accès.

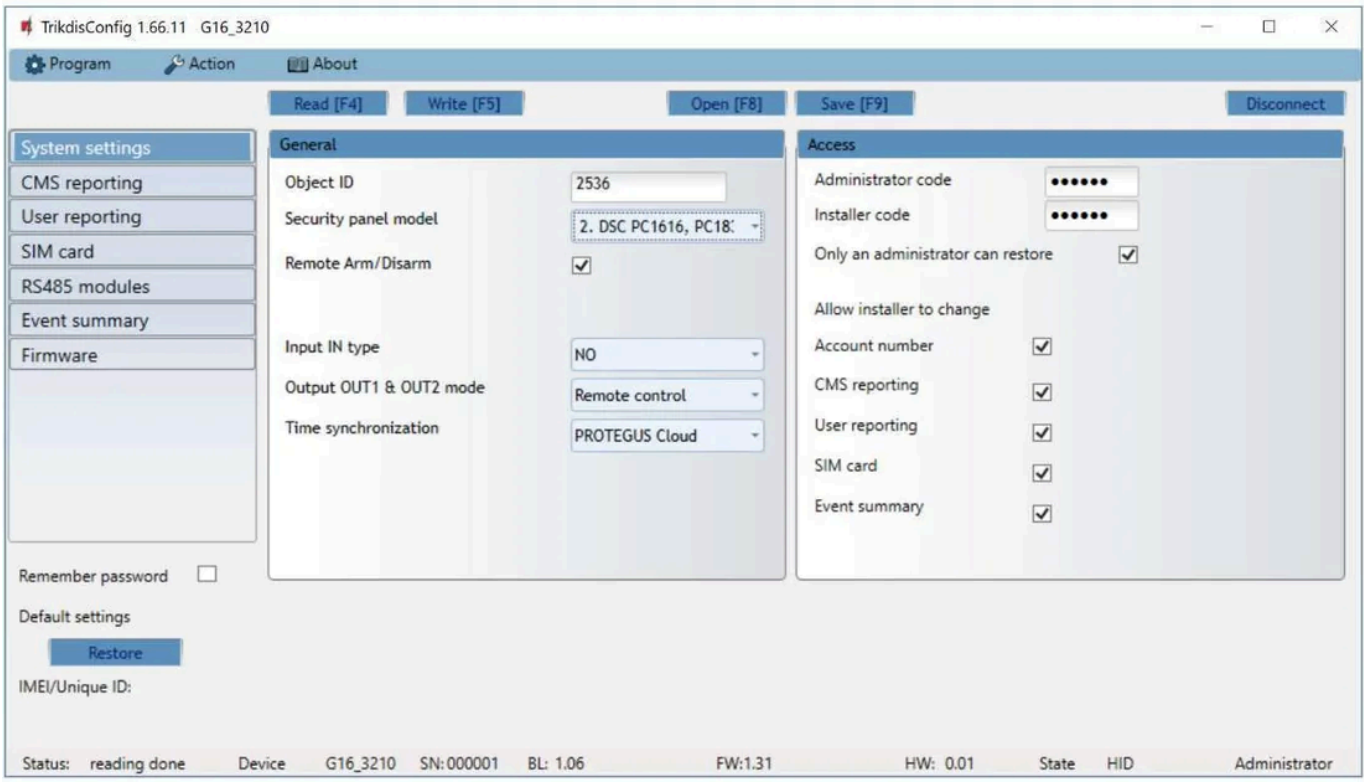


Figure 33. TrikdisConfig – page System settings : groupes General et Access (sur l'image, la version matérielle 3, G16_3210 ; la version 4 n'a pas les champs Input IN type et Output OUT1 & OUT2 mode, qui sont passés à la page IN/OUT).

- **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). Obligatoire si l'appareil transmet aussi au centre de télésurveillance ; `FFFE` et `FFFF` ne peuvent pas être utilisés.
- **Security panel model** – le type de la centrale d'alarme raccordée, choisi dans la liste. C'est de lui que dépend la façon dont le communicateur lit le bus : choisissez donc le type exact de la centrale raccordée.
- **Remote Arm/Disarm** – coché, le communicateur pilote directement la centrale : l'utilisateur arme et désarme depuis Protegus 2 avec son code clavier. N'apparaît que pour les types de centrale pilotables directement ; selon le fabricant, un réglage est nécessaire dans la centrale (chapitre 4). Pour l'armement par zone à clé, laissez-le décoché.
- **Security panel PC download password** – pour le pilotage direct d'une centrale Paradox ou Texecom, le mot de passe PC ou UDL de la centrale (4 caractères) ; il doit être identique à celui réglé dans la centrale (points 4.2 et 4.3).
- **Time set** – la source de l'horloge de l'appareil (par défaut **Cloud application**, le cloud Protegus).
- Sur la **version matérielle 3**, on trouve encore ici les champs **Input IN type** (le type de l'entrée : NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) et **Output OUT1 & OUT2 mode** (le mode des deux sorties ; pour l'armement par zone à clé, **Remote control**).

Dans le groupe **Access**, vous gérez les niveaux d'accès et les mots de passe.

Les réglages de l'appareil disposent de deux niveaux d'accès : **administrateur** et **installateur**.

- **Administrator code** – accès à tous les réglages (mot de passe d'usine : `123456` ; le mot de passe comporte 6 caractères : chiffres ou lettres latines).
- **Installer code** – accès pouvant être restreint (mot de passe d'usine : `654321`).
- **Only an administrator can restore** – case cochée, seul l'administrateur peut lancer la restauration des réglages d'usine.

- **Allow installer to change** – vous sélectionnez ici les groupes de réglages que l'installateur peut modifier : **Account number** (numéro d'abonné), **CMS reporting**, **User reporting**, **SIM card** (appareil mobile) ou **Ethernet settings** (appareil Ethernet), **Event summary**.

Ne laissez pas les mots de passe d'usine dans l'appareil !

Lors de la mise en service, changez au moins le mot de passe administrateur et notez-le en lieu sûr. Un mot de passe oublié ne peut pas être effacé même par la restauration des réglages d'usine, car celle-ci exige aussi un mot de passe : seul le fabricant ou le distributeur peut le réinitialiser, une fois l'appareil envoyé chez lui. Exception : un appareil doté d'un bouton RESET matériel, dont le maintien pendant 10 secondes restaure les réglages d'usine sans mot de passe.

6.3 CMS reporting

Le communicateur envoie les événements au centre de télésurveillance par liaison de données mobile (IP) ou par SMS. Les événements peuvent passer par plusieurs canaux : le canal **principal** et le canal **parallèle** fonctionnent simultanément (vers deux récepteurs à la fois), et chacun dispose d'un canal de **secours**, qui prend le relais si le canal concerné est interrompu. La communication est chiffrée et protégée par mot de passe ; pour la réception, il faut un récepteur Trikdis (récepteur logiciel IPcom, RL14, RM14) ou un récepteur universel connaissant le protocole DC-09 / TL150. Les récepteurs Trikdis transmettent les événements au logiciel de télésurveillance : en liaison IP, le récepteur logiciel **IPcom** (Windows / Linux), le récepteur IP/SMS **RL14** ou le récepteur multicanal **RM14** ; pour la réception des SMS, le RL14, le RM14 ou le récepteur SMS **GM14**.

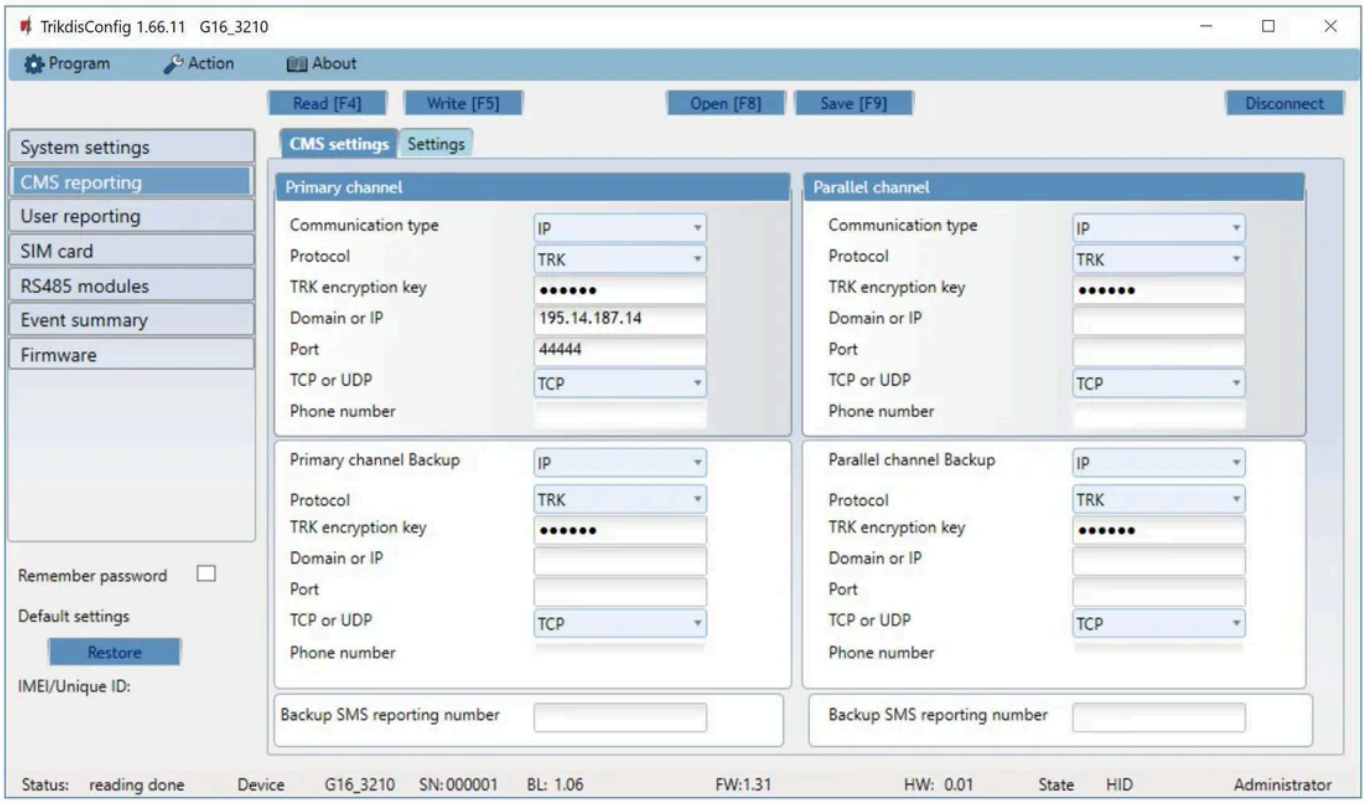


Figure 34. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal, de secours et parallèle.

Primary channel – canal principal

- **Communication type** – IP ou SMS. Le SMS convient comme secours – il fonctionne même sans liaison de données mobile –, mais il n'est pas recommandé comme canal principal.

- **Protocol** – TRK (récepteurs Trikdis), DC-09_2007 ou DC-09_2012 (récepteurs universels), TL150 (SUR-GARD).
- **TRK encryption key** – clé de chiffrement à 6 chiffres ; elle doit être identique dans le communicateur et dans le récepteur.
- **Domain or IP**, **Port** – l'adresse et le port du récepteur.
- **TCP or UDP** – le protocole de transport.
- **Phone number** – uniquement en communication SMS : le numéro de téléphone du récepteur SMS Trikdis avec l'indicatif du pays (p. ex. `CCxxxxxxxxx`, où CC est l'indicatif du pays).

Primary channel Backup – canal de secours. Il prend en charge la communication si le canal principal ne fonctionne pas ; ses réglages sont identiques à ceux ci-dessus.

Parallel channel – canal parallèle. En plus du canal principal, il envoie simultanément à un second récepteur (par exemple au centre de télésurveillance local et au centre principal). Il a son propre canal de secours.

Backup SMS reporting number – numéro SMS de secours. Il entre en jeu si l'envoi échoue sur le canal principal, le canal parallèle et le canal de secours ; il est utile parce qu'il fonctionne aussi sans liaison IP. Il n'est actif que si le canal principal et le canal de secours sont en mode IP. L'appareil envoie un SMS au récepteur SMS du centre de télésurveillance après le premier démarrage, ainsi que si la liaison TCP/IP ou UDP/IP est interrompue à la fois sur le canal principal et sur son canal de secours. Dans ce champ, saisissez le numéro de téléphone du récepteur SMS Trikdis du centre de télésurveillance, avec l'indicatif du pays (p. ex. `CCxxxxxxxxx`).

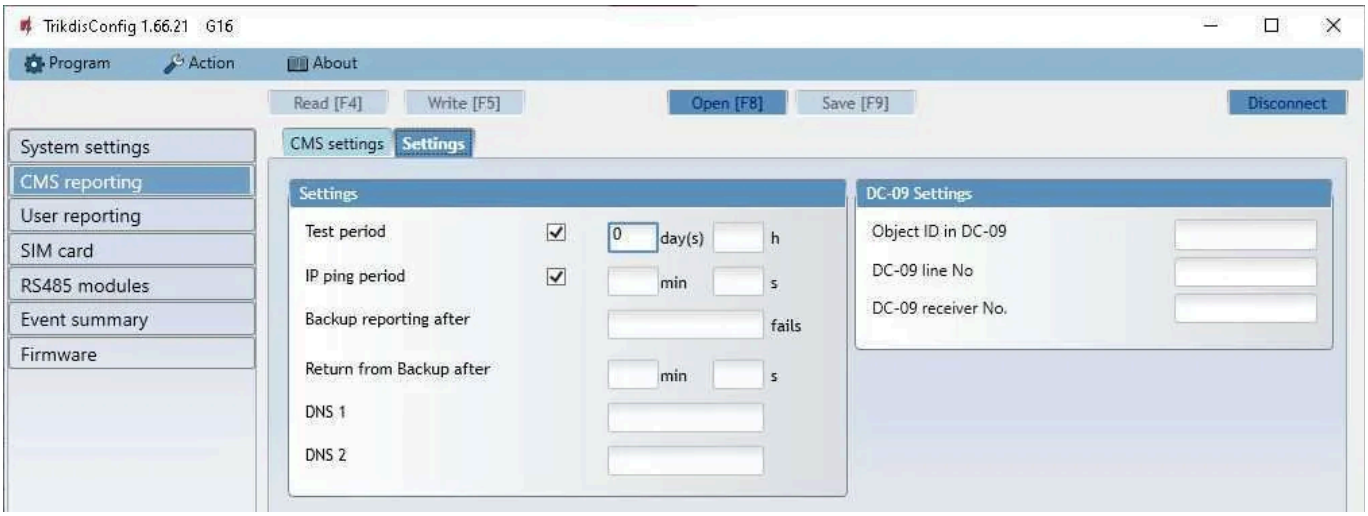


Figure 35. TrikdisConfig – CMS reporting, onglet Settings : rapport de test, PING, temporisations du canal de secours, DNS et données DC-09.

À l'onglet **Settings**, vous réglez les temporisations et les données DC-09.

- **Test period** – intervalle du rapport de test périodique (par défaut 24 heures). Le rapport de test est envoyé sous forme de message Contact ID à la télésurveillance et à Protegus 2.
- **IP ping period** – intervalle du signal de vie (PING) sur le canal IP (par défaut 30 s). Vous l'activez en cochant la case et saisissez la durée dans les champs minutes (**min**) et secondes (**s**) ; il est nécessaire à la supervision de la liaison. Le récepteur ne transmet pas les PING au logiciel de télésurveillance afin de ne pas le surcharger ; le logiciel ne reçoit un message que si le récepteur ne reçoit aucun PING pendant trois fois la durée réglée. Par exemple, avec une période PING de 3 minutes, la perte de liaison est signalée après la 9e minute.
- **Backup reporting after** – nombre de tentatives d'envoi infructueuses après lequel l'appareil bascule sur le canal de secours (par défaut 2).

- **Return from Backup after** – délai après lequel il revient sur le canal principal (par défaut 1 min 30 s).

Le PING maintient la liaison active entre l'appareil et le récepteur ; l'accès, la commande et la programmation à distance en dépendent également. C'est pourquoi **nous ne recommandons pas une période PING supérieure à 5 minutes**.

DC-09 Settings (à droite de l'onglet) – à remplir uniquement si vous transmettez sur un canal avec le protocole DC-09_2007 ou DC-09_2012 ; le groupe apparaît lorsque DC-09_2007 ou DC-09_2012 est sélectionné dans le champ **Protocol** d'un canal :

- **Object ID in DC-09** – identifiant hexadécimal de 3 à 16 caractères, fourni par la télésurveillance.
- **DC-09 line No** – numéro de ligne.
- **DC-09 receiver No.** – numéro du récepteur.

En bas de l'onglet : **DNS 1, DNS 2** – serveurs de noms ; ils sont nécessaires si vous avez indiqué le récepteur par un nom de domaine et non par une adresse IP. Par défaut, il s'agit du DNS public de Google. Le groupe **DC-09 settings** n'est visible que si le protocole DC-09 est réglé sur l'un des canaux.

6.4 User reporting

À l'onglet **PROTEGUS Cloud**, vous activez le service Protegus. Avec le service Protegus, l'utilisateur peut surveiller et piloter à distance le communicateur et le système ; plus d'informations : www.protegus.app.

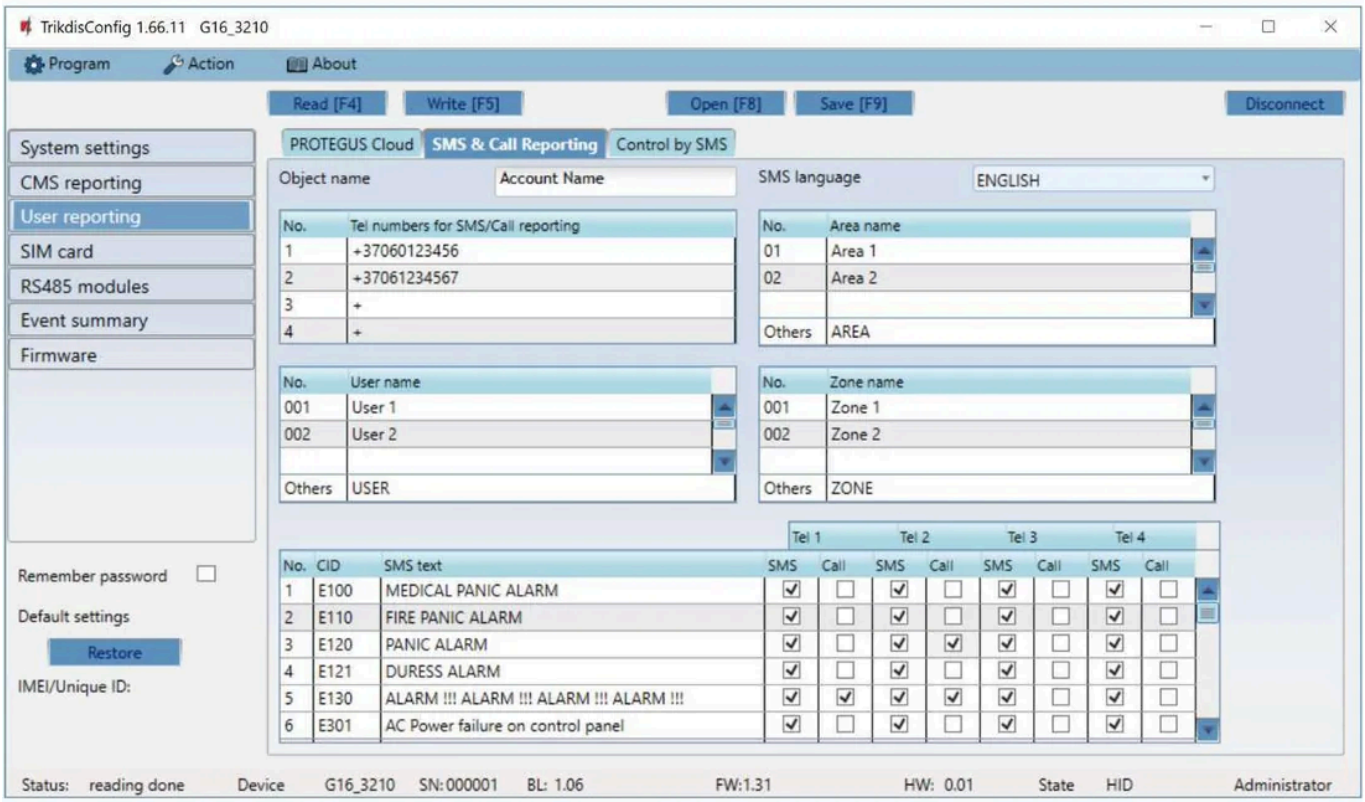


Figure 36. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- **Enable connection** – autorise la liaison avec le cloud Protegus et l'accès à distance de TrikdisConfig.
- **Protegus Cloud access code** – code à 6 chiffres pour la liaison Protegus (`123456` d'usine). Il ne peut être réglé qu'avant la création du système dans Protegus 2 ; il ne peut plus être modifié ensuite.

À l'onglet **SMS & Call Reporting**, l'utilisateur peut aussi recevoir des notifications sur les événements par SMS ou par appel téléphonique.

En cas d'alarme, l'appareil envoie d'abord le SMS à tous les numéros de téléphone saisis, puis les appelle un par un, de Tel 1 à Tel 4. Chaque numéro est appelé une seule fois et sonne pendant 20 secondes ; l'appel est considéré comme réussi si le numéro sonne (décrocher ou refuser suffit aussi). Le modem passe l'appel via la 2G ou la VoLTE. Là où l'opérateur a arrêté la 2G et n'a pas autorisé le modem pour la VoLTE, le SMS arrive, mais le téléphone ne sonne pas. Il ne s'agit pas d'une erreur de configuration. Dans ce cas, utilisez les SMS et l'application Protegus 2.

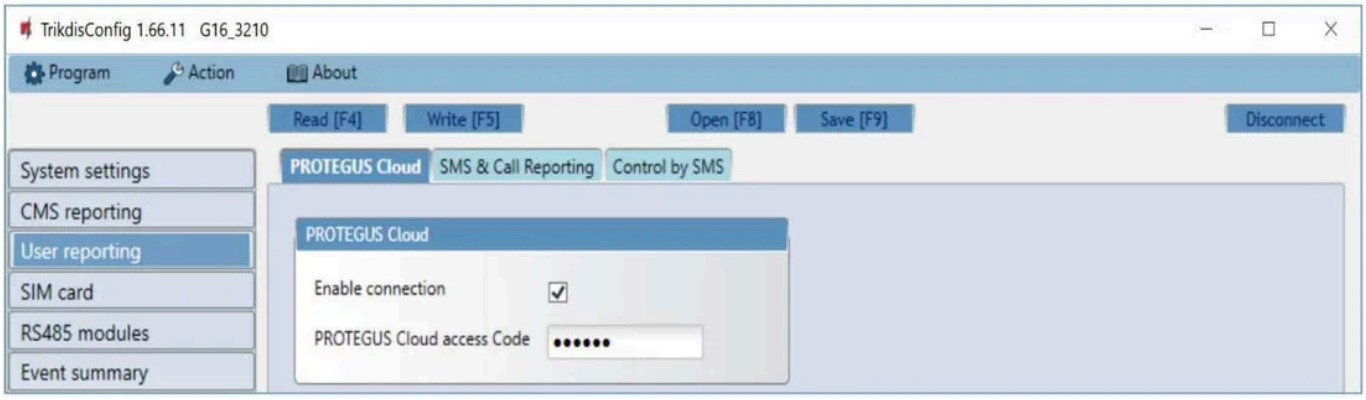


Figure 37. TrikdisConfig – User reporting, onglet SMS & Call Reporting.

- **Object name** – le nom du système ; il figure dans chaque SMS.
- **SMS language** – la langue des SMS (pour les caractères accentués de la langue).
- **Tel numbers for SMS/Call reporting** – jusqu'à 4 numéros de téléphone avec l'indicatif du pays (`+CC…`, `00CC…` ou `CC…`, où CC est l'indicatif du pays).
- **Area name, User name, Zone name** – les noms des partitions, des utilisateurs et des zones ; l'appareil les utilise dans le texte des SMS. Dans le tableau correspondant, saisissez le numéro de la partition, de l'utilisateur ou de la zone, et son nom à côté. Pour une centrale lue sur le bus, ce sont les numéros de zone et d'utilisateur propres à la centrale qui arrivent : indiquez les noms pour ceux-ci.
- **CID event table** – pour chaque événement, vous pouvez régler quel numéro reçoit un SMS ou un appel ; le texte du message et le code Contact ID peuvent aussi être modifiés, et un nouvel événement peut être ajouté.

À l'onglet **Control by SMS**, vous réglez la réception des commandes SMS (les commandes sont décrites au point 5.5).



Figure 38. TrikdisConfig – User reporting, onglet Control by SMS.

- **Reply text** – le texte des quatre messages de réponse à une commande SMS : commande réussie (Command done), mot de passe erroné (Wrong password), commande erronée (Wrong command), données erronées (Wrong data).

- **Tel numbers for control by SMS** – 4 numéros au maximum ; l'appareil n'accepte de commandes que de ces numéros. Si le champ est vide, il accepte de n'importe quel numéro une commande avec le bon mot de passe ; la sécurité est alors assurée par le fait que le mot de passe administrateur ou installateur est obligatoire dans la commande.

6.5 SIM card

Sans les données de la carte SIM, l'appareil ne se connecte pas au réseau de données.

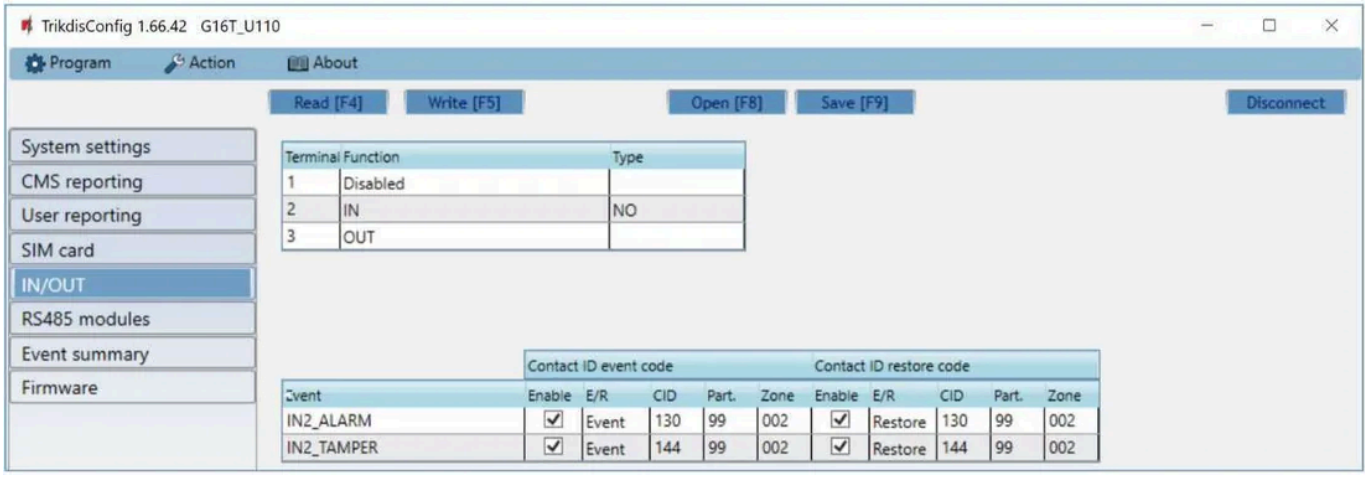


Figure 39. TrikdisConfig – page SIM card.

- **SIM card PIN** – le code PIN de la carte. Vous pouvez désactiver la demande de PIN en plaçant la carte dans un téléphone mobile et en l'y désactivant. Si la demande de PIN est désactivée, la valeur d'usine du champ peut rester.
- **APN** – le point d'accès de l'opérateur (Access Point Name) ; sans lui, le communicateur ne peut pas se connecter à Internet. Il se trouve aussi sur le site de l'opérateur ; l'APN « internet » est générique et fonctionne sur le réseau de nombreux opérateurs. L'article sur les APN recense les APN connus des opérateurs (pour une carte IoT / M2M, l'opérateur fournit un APN spécifique, voir le point 2.3).
- **Login, Password** – nom d'utilisateur et mot de passe de l'APN, si l'opérateur les demande.
- **Forbid connection when roaming detected** – utile près d'une frontière : empêche l'appareil de se connecter au réseau du pays voisin.

Avant utilisation, assurez-vous que la carte SIM est active et que le service de données mobiles y est activé pour la communication IP.

6.6 IN/OUT

C'est ici que vous définissez le rôle des trois bornes I/O à double fonction du communicateur : **Disabled** (non utilisée), **IN** (entrée) ou **OUT** (sortie). Pour une entrée, il faut aussi indiquer le type (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Réglage d'usine : I/O 1 non utilisée, I/O 2 entrée (NO), I/O 3 sortie.



Figure 40. TrikdisConfig – page IN/OUT : fonction des bornes I/O et événements des entrées.

Lorsque le détecteur raccordé à une entrée est déclenché, le communicateur envoie son propre événement (**INx_ALARM**, Contact ID 130), et lorsque le circuit d'autoprotection est déclenché, un événement d'autoprotection (**INx_TAMPER**, 144), au centre de télésurveillance et à Protegus 2 ; les événements de chaque borne réglée en entrée apparaissent dans le tableau. Les colonnes du tableau :

- **Enable** – autorise l'envoi du message.
- **E/R** – le type d'événement : Event (alarme) ou Restore (rétablissement).
- **CID** – le code Contact ID.
- **Part.** – le numéro de partition dans le message.
- **Zone** – le numéro de zone dans le message.

La **version matérielle 3** n'a pas de page IN/OUT : le type de l'unique entrée se règle dans le champ **System settings → Input IN type**, le mode des deux sorties dans le champ **Output OUT1 & OUT2 mode**, et les événements de l'entrée (IN_ALARM, IN_TAMPER) à la page **Event summary**.

6.7 RS485 modules

Les modules d'extension iO-8 et les modules W485 / E485 raccordés au bus RS485 doivent être ajoutés à l'onglet **Modules list**.

Sur le G16 à modem 2G (G16_G410), cette page ne peut pas être utilisée : la version 2G n'a pas de bus RS485.

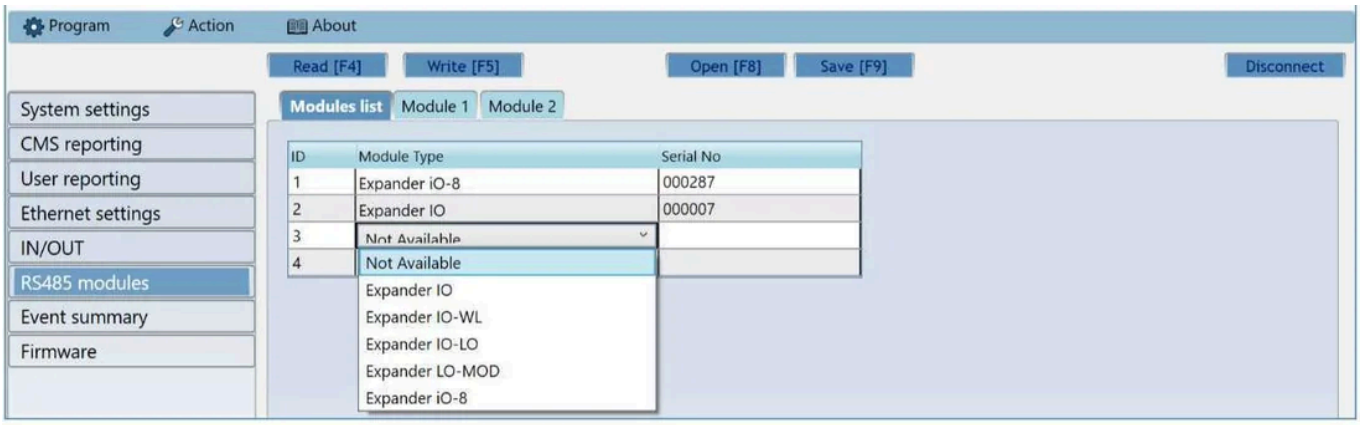


Figure 41. TrikdisConfig – RS485 modules, onglet Modules list : type de module (Expander iO-8, W17u/W485, E485) et numéro de série.

- **Module Type** – le type du module raccordé, choisi dans la liste (Expander iO-8, W17u/W485, E485).
- **Serial No** – le numéro de série à 6 chiffres du module (sur le module et sur sa boîte, SN).

Après avoir choisi le module et saisi le numéro de série, appuyez sur le bouton **Write [F5]**, débranchez le câble USB et attendez une minute que le communicateur enregistre le module. Ensuite, rebranchez le câble, lisez l'appareil (**Read [F4]**) : l'onglet propre du module, numéroté, apparaît à la page RS485 modules.

Module d'extension iO-8 – 8 I/O à double fonction ; jusqu'à 4 modules peuvent être raccordés au communicateur.

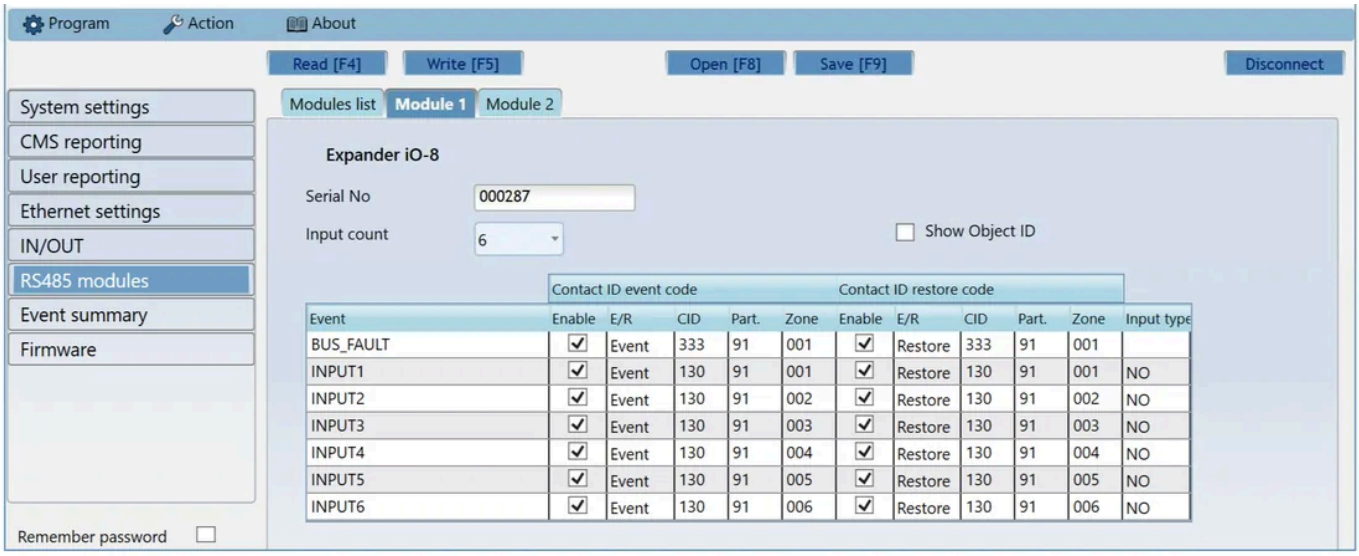


Figure 42. TrikdisConfig – RS485 modules, onglet du module iO-8.

- **Input Count** – le nombre de bornes à utiliser comme entrées ; les autres seront des sorties. Le type d'entrée (**Input type** : NO ou NC) s'indique dans le tableau. Le rôle des sorties (armement / désarmement par zone à clé ou commande d'un équipement) se règle dans l'application Protegus 2.
- Dans le tableau, vous pouvez attribuer un code Contact ID au défaut du bus (**BUS_FAULT**, Contact ID 333) et aux événements de déclenchement et de rétablissement des entrées (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Lorsqu'une entrée est déclenchée, le communicateur envoie un événement avec le code réglé au récepteur du centre de télésurveillance, à l'application Protegus 2 et par SMS au numéro de téléphone de l'utilisateur. Par défaut, le module 1 transmet avec la partition 91, le module 4 avec la partition 94. En cochant **Show Object ID**, vous pouvez aussi indiquer pour les entrées un identifiant d'objet différent de celui du communicateur.
- Si l'utilisateur doit aussi recevoir un SMS ou un appel pour les entrées du module d'extension, ajoutez aussi le code Contact ID attribué à l'entrée dans le tableau des événements de l'onglet **SMS & Call Reporting**.

Module WiFi W485 (dans la liste : W17u/W485) – les données du réseau WiFi et les réglages réseau.



Figure 43. TrikdisConfig – RS485 modules, onglet du module W485.

- **DHCP mode** – réglage réseau automatique (DHCP) ou manuel (Static).
- **Static IP**, **Subnet mask**, **Default gateway** – en réglage manuel.
- **Wifi SSID name**, **Wifi SSID password** – le nom et le mot de passe du réseau WiFi.
- Dans le tableau, vous pouvez attribuer un code Contact ID aux défauts du bus RS485 (interruption et rétablissement de la liaison entre le module et le G16) ; l'événement est reçu par le centre de télésurveillance et par Protegus 2.

Module Ethernet E485 – les mêmes réglages réseau, sans WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**) ; dans le tableau, vous pouvez ici aussi attribuer au défaut du bus RS485 (interruption et rétablissement de la liaison entre l'E485 et le G16) un code Contact ID, reçu par le centre de télésurveillance et par Protegus 2.



Figure 44. TrikdisConfig – RS485 modules, onglet du module E485.

Pour que le W485 et l'E485 fonctionnent, la liaison du G16 avec le centre de télésurveillance et/ou Protegus doit être configurée (points 2.3 et 2.4), et une carte SIM doit se trouver dans le G16. Tant que la liaison filaire ou WiFi fonctionne, le communicateur communique par elle et n'utilise pas la liaison de données mobile.

6.8 Event summary

Sur cette page, vous pouvez activer ou désactiver les **messages internes propres** de l'appareil et modifier leur code Contact ID ainsi que leurs numéros de partition et de zone. Un message désactivé ici n'est envoyé par l'appareil sur aucun canal. En usine, les messages sont envoyés avec la partition 99 et la zone 999.

Message	Contact ID	Quand est-il généré
COMMUNICATION	350	La communication entre le communicateur et la centrale d'alarme est interrompue (désactivé en usine). Un communicateur raccordé au bus ou au port série la détecte directement ; un communicateur sur ligne téléphonique uniquement si **Line supervision** est activé.
POWER	302	Tension d'alimentation incorrecte (trop basse) ; son rétablissement fait l'objet d'un message distinct.
REMOTE_STARTED	411	Une programmation à distance avec TrikdisConfig a commencé.
REMOTE_FINISHED	412	La programmation à distance est terminée.
START	700	L'appareil s'est connecté au réseau (démarrage).
TEST	602	Rapport de test périodique.
PING	760	Le message de signal de vie PING. Il ne figure pas dans la liste de tous les appareils : il apparaît sur l'écran de l'ancienne version matérielle, mais la page Event summary des versions plus récentes ne comporte pas cette ligne. Son intervalle se règle dans le champ **CMS reporting** → **Settings** → **IP ping period**.

- **Enable** – autorise l'envoi du message à la télésurveillance et à Protegus 2.
- **E/R** – type du message : Event (événement) ou Restore (rétablissement) – la ligne correspond à la survenue de l'événement ou à son rétablissement.
- **Part.** – numéro de la partition (secteur) que l'appareil envoie pour l'événement interne et pour le rétablissement.
- **Zone** – numéro de la zone que l'appareil envoie pour l'événement interne et pour le rétablissement.
- Le code **CID**, la **partition** et la **zone** peuvent être modifiés pour n'importe quel événement ; lorsqu'il existe un rétablissement (Restore), son code peut être défini séparément.

Les événements des entrées propres (**INx_ALARM**, **INx_TAMPER**) se règlent sur la page **IN/OUT**, ceux des modules d'extension (**BUS_FAULT**, **INPUTx**) sur la page **RS485 modules**, dans l'onglet du module. L'activation et l'intervalle du rapport de test se règlent dans le champ **CMS reporting** → **Settings** → **Test period**.

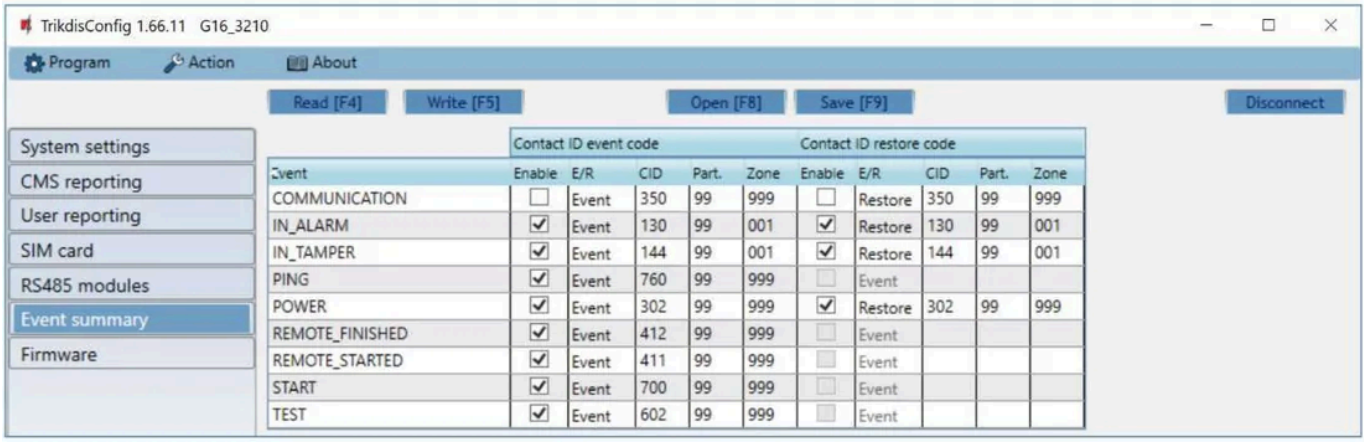


Figure 45. TrikdisConfig – page Event summary : les messages internes de l'appareil (sur l'image, la version matérielle 3, pour laquelle les événements IN_ALARM et IN_TAMPER de l'entrée ainsi que le PING figurent aussi ici ; sur la version 4, les événements des entrées se trouvent à la page IN/OUT).

6.9 Retour aux réglages d'usine

Pour restaurer les réglages d'usine, cliquez sur le bouton **Restore** dans le groupe **Default settings**, en bas à gauche de la fenêtre TrikdisConfig. La restauration efface tous les réglages – y compris les mots de passe –, il est donc conseillé d'enregistrer auparavant les réglages dans un fichier (**Save [F9]**).

Avec le mot de passe installateur, cela n'est possible que si l'administrateur ne l'a pas interdit sur la page **System settings → Access**.

7. Programmation à distance

TrikdisConfig accède aux appareils Trikdis non seulement par câble USB, mais aussi **à distance, via le cloud Protegus**. Vous pouvez ainsi modifier les réglages d'un appareil déjà installé sans vous rendre sur site.

Conditions requises pour l'accès à distance :

1. L'appareil doit être sous tension et disposer d'une connexion réseau (les LED **POWER** et **NETWORK** sont allumées en vert ; sur un appareil mobile, la LED NETWORK clignote aussi en jaune). Sur un appareil mobile, la carte SIM insérée doit être active et son code PIN doit être saisi dans l'appareil, ou la demande de PIN doit être désactivée ; sur un appareil Ethernet, le câble réseau (LAN) doit être branché et l'appareil doit accéder à Internet.
2. Sur la page **User reporting → PROTEGUS Cloud** de TrikdisConfig, **Enable connection** doit être coché (à régler par USB, lors de la première mise en service).
3. Vous devez connaître l'**identifiant unique** de l'appareil (IMEI ou MAC – indiqué sur la boîte et au dos de l'appareil) ainsi que le mot de passe administrateur ou installateur.

Étapes :

1. Lancez le logiciel TrikdisConfig.
2. Dans la partie **Remote access**, saisissez l'identifiant unique de l'appareil (IMEI ou MAC) dans le champ **Unique ID**.
3. Si vous le souhaitez, donnez un nom au système dans le champ **System name** – le logiciel le mémorise et, la fois suivante, vous pourrez le choisir dans la liste déroulante.
4. Appuyez sur le bouton **Configure**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Read [F4]** (lecture) et saisissez le mot de passe. Avec la case **Remember password**, le logiciel le mémorise pour cette session.
6. Effectuez les modifications, puis envoyez-les à l'appareil avec le bouton **Write [F5]** (écriture).

Le logiciel enregistre les systèmes programmés à distance auxquels un nom a été donné ; la flèche à côté du champ **System name** permet de les afficher. Pour en supprimer un, sélectionnez l'identifiant dans la liste, appuyez sur la touche **Delete** et confirmez.

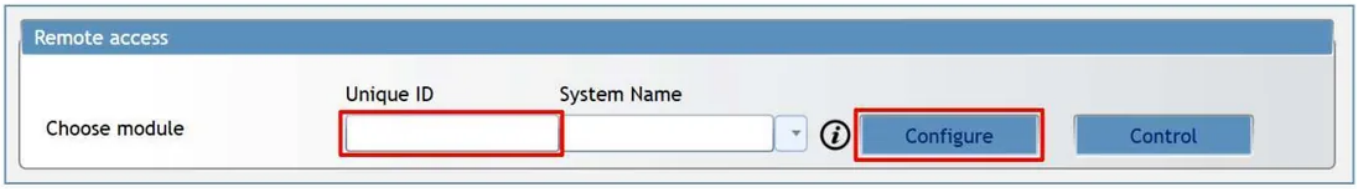


Figure 46. TrikdisConfig – Remote access : l'identifiant de l'appareil, le nom du système et le bouton Configure.

8. Vérification du fonctionnement

Après la programmation et le raccordement, vérifiez toujours toute la chaîne : centrale d'alarme → communicateur → télésurveillance et/ou Protegus 2.

Vérifiez d'abord que l'alimentation est présente (la LED **POWER** est allumée en vert) et que la connexion réseau est établie (la LED **NETWORK** est allumée en vert).

1. **Déclenchez un événement.** Armez puis désarmez le système depuis le clavier, ou violez une zone sur un système armé pour provoquer une alarme.
2. **Vérifiez la réception.** Contrôlez que l'événement apparaît dans le logiciel de télésurveillance et/ou dans la liste des événements de l'application Protegus 2 – avec les bons numéros de partition et de zone.
3. **Entrées.** Déclenchez le détecteur raccordé à une entrée propre du communicateur et vérifiez l'événement correspondant.
4. **Sorties.** Commutez la sortie depuis l'application Protegus 2 et vérifiez que l'équipement raccordé (relais, zone à clé) se déclenche réellement.
5. **Armement à distance.** Si la centrale peut être commandée à distance, armez-la et désarmez-la également depuis l'application Protegus 2.

Pour une centrale raccordée au bus, vérifiez aussi que le communicateur lit réellement la centrale : armez et désarmez la centrale au clavier, et regardez si, dans la liste des événements de Protegus 2 (et au centre de télésurveillance), l'événement apparaît avec le bon numéro de partition et d'utilisateur. En pilotage direct, effectuez aussi un essai d'armement depuis l'application, avec le code clavier de l'utilisateur.

9. Mise à jour du firmware

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

Vous pouvez mettre à jour le firmware vous-même – vers une version plus récente et, si nécessaire, vers une version plus ancienne. Après la mise à jour, tous les réglages de l'appareil restent inchangés.

1. Lancez le logiciel TrikdisConfig et connectez l'appareil avec un câble USB, ou accédez à sa programmation à distance.
2. Si un firmware plus récent est disponible, le logiciel propose de le télécharger – acceptez.
3. Sélectionnez l'onglet **Firmware** et cliquez sur le bouton **Open firmware**. Choisissez le fichier de firmware.
4. Appuyez sur le bouton **Update [F12]**, attendez la fin de la mise à jour, puis cliquez sur **OK** dans la fenêtre qui s'affiche. Pendant ce temps, ne débranchez pas le câble et n'interrompez pas la connexion.

Les fichiers de firmware se trouvent dans le dossier d'installation de TrikdisConfig, dans le sous-dossier **Firmwares**, dans le dossier portant le nom de l'appareil. Si ce dossier n'existe pas, soit aucune mise à jour n'est disponible pour l'appareil, soit c'est le logiciel TrikdisConfig lui-même qu'il faut mettre à jour. Les fichiers les plus récents peuvent aussi être téléchargés, en tant qu'utilisateur enregistré, sur le site du fabricant, depuis la page de l'appareil.

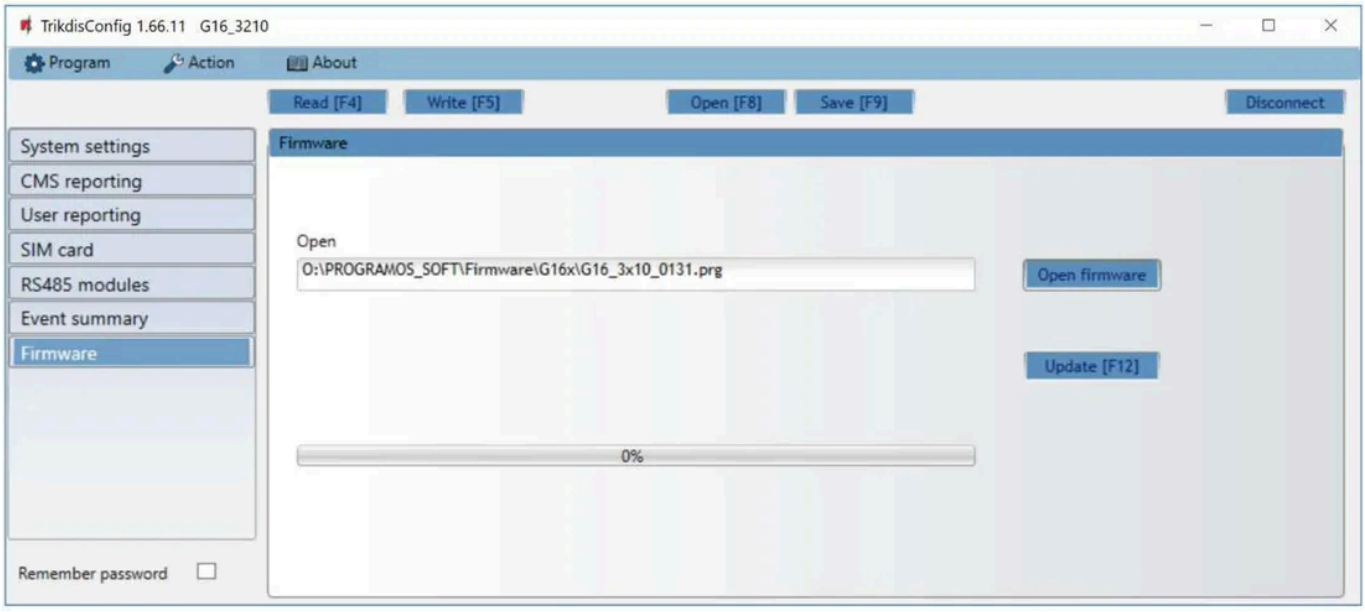


Figure 47. TrikdisConfig – page Firmware : Open firmware et Update [F12].

La mise à jour nécessite une connexion Internet. Un antivirus, un pare-feu ou un réglage réseau strict peut empêcher le téléchargement automatique du firmware ; dans ce cas, modifiez le réglage de l'antivirus (autorisez l'accès Internet de TrikdisConfig), ou téléchargez le fichier manuellement et ouvrez-le à la page Firmware.

10. Dépannage et questions fréquentes

Les questions et défauts les plus fréquents, à partir de la signalisation des LED. Lorsque la réponse renvoie au chapitre détaillé, c'est là que vous trouverez l'emplacement exact du réglage.

La LED NETWORK ne s'allume pas – pas de réseau

1. Regardez les clignotements de la LED **TROUBLE** : 1 = pas de SIM, 2 = PIN erroné, 3 = pas d'APN, 4 = impossible de se connecter au réseau mobile, 5 = impossible de se connecter au réseau de données.
2. Vérifiez que la carte SIM est active, qu'elle dispose d'un service de données et qu'elle est bien en place dans son support.
3. Si la demande de PIN est activée sur la carte, saisissez le PIN à la page **SIM card**, ou désactivez la demande de PIN dans un téléphone.

4. Vérifiez l'antenne : elle est vissée, elle n'est pas dans un coffret métallique, le niveau du signal est suffisant (points 1.7 et 3.2).

Il y a du réseau, mais le centre de télésurveillance ne reçoit pas d'événements

La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur le réseau de l'opérateur ; pour un appareil Ethernet, que la liaison jusqu'au routeur fonctionne –, mais pas que l'appareil accède aussi à Internet. Si la LED NETWORK est verte mais que la LED DATA reste allumée en continu après un événement ou un rapport de test, la connexion Internet ne fonctionne pas : le message ne peut pas partir. Sur le réseau mobile, la cause la plus fréquente est l'APN ou le service de données de la carte SIM ; en Ethernet, le routeur, le pare-feu ou le DNS. Si la LED DATA s'éteint, le message est parti et la connexion de données fonctionne.

1. 6 clignotements de la LED **TROUBLE** signalent l'absence de liaison avec le récepteur : vérifiez l'adresse et le port du récepteur, le réglage TCP/UDP et la clé de chiffrement (**CMS reporting**).
2. Si le récepteur est indiqué par un nom de domaine, vérifiez le réglage DNS (**CMS reporting** → **Settings**).
3. Vérifiez que le forfait de données de la carte SIM ne bloque pas le port nécessaire (certaines cartes M2M n'autorisent que des adresses déterminées).

La LED TROUBLE clignote sept fois – le communicateur ne voit pas la centrale

1. Vérifiez le raccordement selon le schéma du point 3.3 : l'erreur la plus fréquente est l'inversion des fils **CLK** et **DATA**, ou une ligne de données raccordée à la mauvaise borne de la centrale.
2. Dans le champ **System settings** → **Security panel model** de TrikdisConfig, le type exact de la centrale raccordée doit être sélectionné.
3. Pour les centrales Texecom, Caddx, Honeywell et InnerRange, un réglage est aussi nécessaire dans la centrale (chapitre 4) – sans lui, la centrale ne fournit pas de données sur le bus.
4. Sur une centrale Paradox, le port série est peut-être verrouillé d'usine – voici comment le déverrouiller.
5. Après le raccordement, mettez une centrale Pyronix hors tension puis redémarrez-la pour qu'elle accepte le communicateur.
6. Le G16 ne fonctionne pas avec une centrale DSC PowerSeries **NEO** (elle n'autorise aucun appareil externe sur son bus) – il faut ici un communicateur sur ligne téléphonique.

Les événements arrivent, mais je ne peux pas armer depuis l'application

En pilotage direct :

1. À la page **System settings**, **Remote Arm/Disarm** doit être coché.
2. Pour une centrale Paradox ou Texecom, le **Security panel PC download password** doit correspondre au mot de passe PC ou UDL de la centrale (points 4.2 et 4.3).
3. Pour une centrale Paradox, le firmware de la centrale doit être au moins en **V.4** ; le code de l'utilisateur ne doit pas être le code maître ; après une modification de code, redémarrez le communicateur.
4. Pour une centrale Honeywell Vista, la 2e adresse AUI doit être activée (point 4.6).
5. Dans Protegus 2, **aucune** sortie ne doit être attribuée à la partition (Control with Protegus2 désactivé).

Avec une zone à clé :

1. **Remote Arm/Disarm** doit être décoché, et la borne I/O doit être réglée sur **OUT** à la page **IN/OUT**.

2. La zone de la centrale doit être de type zone à clé, et dans Protegus 2, la sortie correspondante doit être attribuée à la partition, en mode impulsion ou deux positions selon la zone (point 5.3).

Protegus 2 ne voit pas l'appareil

1. À la page **User reporting** → **PROTEGUS Cloud**, **Enable connection** doit être coché.
2. Lors de la création du système, il faut saisir le **Protegus Cloud access code** réglé dans l'appareil ; une fois le système créé, il ne peut plus être modifié dans l'appareil.
3. Saisissez l'IMEI exactement, depuis la boîte ou le dos de l'appareil.
4. Le service de données de la carte SIM et l'APN doivent être corrects (la LED NETWORK est verte, et la LED DATA s'éteint après un événement).

Je ne peux pas me connecter à distance avec TrikdisConfig

1. L'appareil doit être en ligne (LED NETWORK verte), et la liaison Protegus doit être activée.
2. **CMS reporting** → **Settings** → **IP ping period** ne doit pas dépasser 5 minutes : c'est le PING qui maintient la liaison nécessaire à l'accès à distance.
3. Vérifiez le mot de passe administrateur ou installateur.

J'ai oublié le mot de passe

Un mot de passe oublié ne peut pas être récupéré, ni effacé par la restauration des réglages d'usine, car celle-ci exige aussi un mot de passe. Dans ce cas, seul le fabricant ou le distributeur peut le réinitialiser : l'appareil doit lui être envoyé. Notez donc les mots de passe définis en lieu sûr.

Pourquoi je ne vois pas la page RS485 modules, ou pourquoi l'iO-8 ne fonctionne pas ?

Le G16 à modem 2G (G16_G410) n'a pas de bus RS485 ; les modules iO-8, W485 et E485 ne peuvent être raccordés qu'à la version 4G (G16_54E0). Pour les modules W485 et E485, une carte SIM doit aussi se trouver dans le G16.

J'ai un appareil 2G – jusqu'à quand fonctionnera-t-il ?

L'arrêt des réseaux 2G progresse à un rythme différent selon l'opérateur ; pour un fonctionnement à long terme, nous recommandons la version 4G, qui peut aussi être étendue par le bus RS485.

Quelle quantité de données l'appareil consomme-t-il ?

Les messages d'événement et les PING sont très petits ; le trafic dépend essentiellement de la période de PING et de la fréquence des rapports de test. Pour un système domestique moyen, le trafic mensuel reste généralement inférieur à 10 Mo. La valeur exacte dépend des réglages et de l'unité de facturation de l'opérateur ; avec une carte à volume de données limité, il est donc conseillé de vérifier le trafic du premier mois.

11. Consignes de sécurité

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.

- Seul un installateur qualifié peut installer et entretenir un équipement de sécurité.
- Avant l'installation, lisez attentivement ce manuel ; le non-respect des instructions peut entraîner un dysfonctionnement ou une panne.
- Avant le raccordement, lors de chaque branchement électrique et avant toute intervention, mettez l'équipement hors tension.
- Les défauts résultant d'une installation ou d'une utilisation incorrecte, ainsi que les modifications et réparations non autorisées par le fabricant, entraînent la perte de la garantie.
- Respectez la réglementation locale sur les déchets : ne jetez pas l'appareil défectueux ni ses composants avec les ordures ménagères.

Voir aussi

- Moteur de recherche de compatibilité – quel communicateur convient à quelle centrale d'alarme.
- G16 – pilotage direct des centrales d'alarme DSC PowerSeries – armement avec le code clavier, état des zones, exclusion de zones.
- DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions – pourquoi le G16 ne peut pas être raccordé à la NEO, et quelle est la solution.
- Déverrouillage du port série verrouillé des centrales d'alarme Paradox – déverrouillage du port série des centrales Paradox récentes.
- Armement à distance par zone à clé depuis l'application Protegus 2 – les détails et les pièges de l'armement par zone à clé.
- La version matérielle v4 des communicateurs GSM G16 et G16T arrive – ce qui a changé par rapport à la version 3.
- Réglage de l'APN – liste des opérateurs mobiles européens – l'APN de la carte SIM selon l'opérateur.
- Documentation en anglais : docs.trikdis.com – les manuels de docs.trikdis.com sont en anglais.

Produits associés

Trikdis G16 4G GSM communicateur intelligent

Trikdis G16 2G GSM communicateur intelligent

Câble de connexion de port série Trikdis CRP2 pour les centrales d'alarme Paradox

Câble de connexion de port série CRP2B pour les centrales d'alarme Paradox

Câble série Trikdis CRP4 pour les panneaux de contrôle Texecom

Module Trikdis IO8 Wired Expander

Droits d'auteur

Ce manuel a été réalisé par trikdis.hu et mobilamb.eu. Son texte, sa structure, nos propres illustrations et ses compléments sont notre propriété intellectuelle et sont protégés par le droit d'auteur. Sans notre autorisation, il ne peut être copié, diffusé ni publié sur un autre site web, ni en totalité ni en partie. Tu peux le télécharger et l'imprimer librement pour installer et utiliser le produit.

Les noms et logos Trikdis et Protegus sont des marques de UAB Trikdis.

Version toujours à jour de ce manuel : https://trikdis.fr/manuel-g16