Communicateur GET – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation du communicateur Trikdis GET Ethernet + 4G : raccordement à la centrale d'alarme, configuration LAN et SIM dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2.



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

Sommaire

1. Présentation

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

2. Mise en service rapide

2.1 Préparation
2.2 Connexion à l'application Protegus 2
2.3 Connexion au centre de télésurveillance

3. Installation et raccordement

3.1 Les étapes de l'installation
3.2 Emplacement dans le boîtier de la centrale, antenne
3.3 Raccordement à la centrale d'alarme
3.3.1 DSC – bus de données (Keybus)
3.3.2 Paradox – port série
3.3.3 Paradox SP/MG – Keybus et TIP/RING
3.3.4 UTC Interlogix (Caddx) – bus de données
3.3.5 Texecom – port série
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – bus de données
3.3.9 Toute centrale – TIP/RING
3.4 Raccordement d'une zone à clé
3.5 Raccordement des entrées
3.6 Raccordement d'une sortie avec un relais
3.7 Mise sous tension et première vérification
A TRIKDIS átjelző elindítása

4. Programmation de la centrale d'alarme

4.1 Raccordement au bus de données ou au port série
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Raccordement par ligne téléphonique (TIP/RING)
4.2.1 Programmation du transmetteur Honeywell Vista
4.2.2 Transmetteur des centrales UTC Interlogix (Caddx) NX

5. Pilotage à distance avec l'application Protegus 2

5.1 Ajout de l'appareil
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armement et désarmement par une sortie

5.3 Armement et désarmement depuis l'application

6. Les réglages en détail

6.1 Connexion au communicateur

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Canaux de réception (CMS settings)

6.4.2 Test, PING et ordre des connexions

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 et SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Rétablissement des réglages d'usine

7. Programmation à distance

8. Vérification du fonctionnement du communicateur

9. Mise à jour du firmware

10. Dépannage et questions fréquentes

11. Consignes de sécurité

Voir aussi

1. Présentation

Le GET est le **communicateur Ethernet + 4G** de Trikdis : il transmet les événements de la centrale d'alarme par le réseau local filaire (LAN) ou par le réseau mobile au centre de télésurveillance et à l'application Protegus 2. Il se raccorde à la centrale de deux façons : **directement**, sur le bus de données ou le port série de la centrale (centrales DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange et Honeywell), ou **sur le transmetteur téléphonique de n'importe quelle centrale** (TIP/RING), à condition que celui-ci envoie les événements au format Contact ID, en tonalités DTMF. Le communicateur transmet au centre de télésurveillance toutes les informations de l'événement (code, partition, zone ou utilisateur). Avec l'application Protegus 2, l'utilisateur pilote le système à distance et reçoit une notification des événements ; l'application fonctionne avec toutes les centrales prises en charge par le communicateur, quelle que soit leur marque. La transmission vers le centre de télésurveillance et Protegus 2 peuvent être utilisés en même temps. Ce manuel a été rédigé pour le communicateur GET à modem LTE (4G) ; les différences entre GET, GT et GT+ sont résumées au point 1.2.

1.1 À quoi il sert, comment il fonctionne

- **Il transmet au centre de télésurveillance.** Il envoie les événements par liaison IP, sur le réseau filaire ou le réseau mobile, au récepteur logiciel ou matériel de Trikdis (protocole TRK8) – ceux-ci fonctionnent avec n'importe quel logiciel de télésurveillance –, à un récepteur SIA DC-09 ou à un récepteur SUR-GARD (TL150). Vers un récepteur SUR-GARD, il convertit les codes Contact ID reçus de la centrale en codes SIA ; le tableau de conversion se trouve en annexe de la documentation anglaise de Trikdis. Il vérifie la liaison avec le récepteur toutes les 30 secondes (ou selon l'intervalle réglé) par un message PING ; si le canal principal est interrompu, il bascule sur le canal de secours. Avec un canal parallèle, les événements partent en même temps vers deux récepteurs. Vous pouvez classer les voies de connexion – LAN, SIM1, SIM2 – par ordre de priorité : si la voie principale ne fonctionne pas, le communicateur bascule sur la voie de secours (point 6.4.2). Si le service Protegus est aussi activé, l'événement est reçu d'abord par le centre de télésurveillance, puis seulement par l'application des utilisateurs.
- **Il avertit l'utilisateur.** L'application Protegus 2 signale les événements par notification push et par un son distinct ; depuis l'application, l'utilisateur peut armer et désarmer et commander les équipements raccordés (éclairage, portail, ventilation, chauffage, arrosage, etc.). Dans l'application, les droits de l'administrateur, de l'installateur et de l'utilisateur sont différents. Le GET n'envoie ni SMS ni appel : la notification arrive par l'application Protegus 2.
- **Il pilote directement la centrale.** Raccordé au bus de données ou au port série, le communicateur voit aussi l'état des partitions et des zones de la centrale, et l'utilisateur arme et désarme depuis Protegus 2 avec son propre code clavier – sans zone à clé.
- **Il a ses propres entrées et sorties.** Deux bornes I/O à double fonction s'utilisent comme entrée (IN) ou comme sortie pilotable (OUT) ; d'usine, les deux sont des sorties. Les sorties se commandent depuis l'application Protegus 2. Les bornes **A 485** et **B 485** ne sont pas utilisées sur le GET ; aucun module d'extension RS485 ne peut être raccordé au GET.
- **Il se configure avec deux outils.** Les réglages se font avec le logiciel TrikdisConfig sous Windows (par câble USB-C ou à distance) et – avec le firmware 1.08 ou plus récent – aussi depuis l'application Protegus 2 (Settings → Advanced settings). Les réglages peuvent être enregistrés dans un fichier et écrits dans d'autres communicateurs. Il existe deux niveaux d'accès : celui de l'administrateur du centre de télésurveillance et celui de l'installateur. Le communicateur se configure aussi à distance, et son firmware peut aussi être mis à jour à distance.

Le schéma ci-dessous montre l'architecture du système : la centrale d'alarme se raccorde au communicateur, le communicateur accède à Internet de deux façons – par le réseau mobile (LTE) ou par le routeur (LAN) –, et de là au récepteur du centre de télésurveillance (et à son logiciel) et au serveur Protegus ; l'utilisateur voit le système dans l'application Protegus 2.

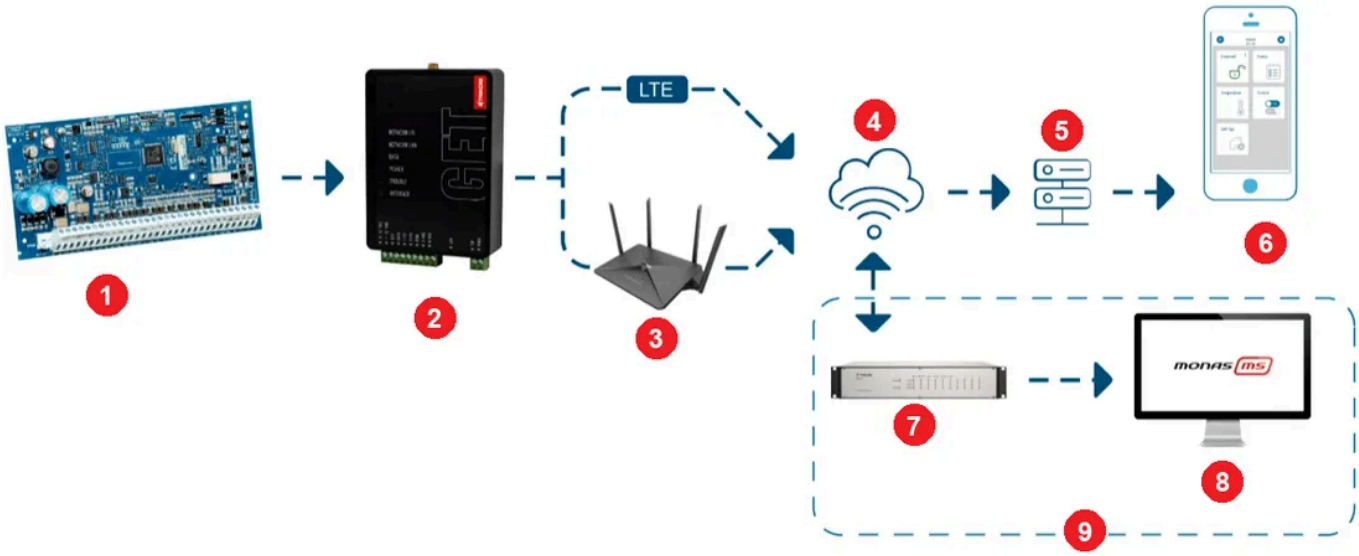


Figure 1. La place du communicateur dans le système : centrale d'alarme → GET → réseau mobile (LTE) ou routeur (LAN) → Internet → récepteur du centre de télésurveillance et serveur Protegus → application Protegus 2.

- 1 centrale d'alarme (« Alarm panel »)
- 2 communicateur LTE GET (« LTE communicator »)
- 3 routeur (« Router »)
- 4 Internet (« Internet »)
- 5 serveur Protegus (« Protegus server »)
- 6 téléphone avec l'application Protegus (« Phone with Protegus software »)
- 7 récepteur du centre de télésurveillance (« Receiver »)
- 8 logiciel de télésurveillance (« Monitoring software »)
- 9 poste de télésurveillance de la société de sécurité (« Monitoring station in security company ») – dans le cadre en pointillés

1.2 Versions : GET, GT et GT+

Le GET est le « frère » à port Ethernet des communicateurs GT et GT+ : le raccordement et la programmation de la centrale d'alarme, la liste des centrales compatibles, le modem, les protocoles de transmission et l'utilisation de Protegus 2 sont identiques ; c'est pourquoi les manuels des trois communicateurs ont aussi le même plan. Le tableau ci-dessous résume les différences.

	GET	GT	GT+
Connexion réseau	**LTE (4G) et Ethernet (LAN, RJ45)** ; l'ordre des voies de connexion est réglable (Main / Backup / Backup 2 : LAN, SIM1, SIM2 ; point 6.4.2)	LTE (4G)	LTE (4G)
Carte SIM	**2 emplacements nano-SIM** (SIM1, SIM2) ; une ou deux cartes peuvent être insérées	1 nano-SIM	1 nano-SIM
Tension d'alimentation	10–18 V DC	10–18 V DC	10–32 V DC

	GET	**GT**	**GT+**
Consommation	au maximum 100 mA en veille, 300 mA pendant l'envoi de données	au maximum 100 / 200 mA	au maximum 100 / 200 mA
Dimensions, poids	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g
Bornes	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485 ; prise **LAN** (RJ45) séparée et TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Réglage d'usine des bornes I/O	sortie (OUT)	entrée (IN, NO)	entrée (IN, NO)
Bus RS485, extension iO-8	les bornes A 485 / B 485 ne sont **pas utilisées** ; aucune extension ne peut être raccordée	jusqu'à 4 iO-8	jusqu'à 4 iO-8
LED	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (non utilisée)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Clignotements de la LED TROUBLE	1 = liaison physique LAN (câble), 2 = défaut SIM1, 3 = défaut SIM2, 7 = centrale	1–8 (SIM, PIN, APN, réseau, récepteur, centrale, ICCID)	1–8
SMS et appel	pas de notification SMS, pas de commande SMS ni d'appel : la notification et le pilotage passent par Protegus 2	notification par SMS et par appel, commandes SMS	notification par SMS et par appel, commandes SMS
Centrale DSC à la fois sur le bus de données et sur les bornes TIP/RING	non	non	oui
Réglage du raccordement TIP/RING (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (**3. MANUAL** peut aussi être choisi)
Configuration depuis l'application Protegus 2	oui (Advanced settings, à partir du firmware 1.08)	TrikdisConfig	TrikdisConfig
Mémoire d'événements	60 événements	pas de données	pas de données
Messages internes (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	comme le GT
Modem, protocoles de transmission (TRK8, DC-09, TL150), chiffrement, centrales compatibles, schémas de raccordement, Protegus 2	identiques	identiques	identiques

Les trois communicateurs sont fabriqués avec les trois mêmes modems ; pour l'Europe, c'est la version européenne (EU) qui convient. Le type de modem et la version matérielle se trouvent dans la barre d'état de TrikdisConfig (**Device**, **HW**) et sur l'étiquette de l'appareil.

Modem	Réseau et bandes de fréquences
EG915U-EU (Europe)	LTE FDD : B1 / B3 / B5 / B7 / B8 / B20 / B28 ; GSM : B2 / B3 / B5 / B8
EG915U-LA (Amérique latine)	LTE FDD : B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66 ; GSM : B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD : B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85 ; EGPRS : 850 / 900 / 1800 / 1900 MHz

1.3 Centrales d'alarme compatibles

Les centrales ci-dessous peuvent être raccordées directement au communicateur, par le bus de données ou le port série. La colonne « Pilotage direct » indique si l'utilisateur peut armer et désarmer depuis Protegus 2 avec son propre code clavier, sans autre raccordement ; là où ce n'est pas possible, le communicateur lit les événements sur le bus, et le pilotage nécessite une zone à clé (point 3.4).

Fabricant	Modèle	Raccordement	Pilotage direct
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	bus de données (Keybus)	oui
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	port série (câble EX-CRP2.4), ou Keybus + TIP/RING	oui
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	port série (câble EX-CRP2.4), ou Keybus + TIP/RING	oui
Paradox	Digiplex EVO192, EVOHD, EVOHD+	port série (câble EX-CRP2.4)	oui
Paradox	Digiplex EVO48	port série (câble EX-CRP2.4)	non
Paradox	Spectra 1727, 1728, 1738 ; Esprit E55	port série (câble EX-CRP2.4)	non
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	bus de données	oui
Texecom	Premier 24, 48, 88, 168, 640 ; Premier Elite 12, 24, 48, 64, 88, 168, 640	port série (câble EX-CRP4)	oui
InnerRange	Inception, Integriti	port série (avec le câble du fabricant de la centrale)	non
Honeywell	Ademco Vista-15, Vista-20, Vista-48	bus de données	oui

- Le firmware des centrales **Paradox** pilotées directement doit être au moins en **V.4**. Sur les centrales Paradox récentes (SP+, MG+, EVOHD+), le port série peut être verrouillé d'usine ; le déverrouillage est décrit au point 4.1.2. Les centrales Spectra SP / SP+ et Magellan MG / MG+ peuvent aussi être raccordées, au lieu du port série, à la fois au bus de données (Keybus) et aux bornes TIP/RING – cela ne nécessite pas le déverrouillage payant, mais le firmware du communicateur doit être au moins en 1.21 (point 3.3.3).
- La centrale de **tout autre fabricant** se raccorde par son transmetteur téléphonique (TIP/RING), s'il envoie les événements au format Contact ID, en numérotation DTMF ; dans ce cas, le pilotage nécessite une zone à clé.

- Pour savoir quel communicateur Trikdis et quel raccordement conviennent à votre centrale, consultez le moteur de recherche de compatibilité.

1.4 Les éléments du communicateur

Le circuit imprimé du communicateur est logé dans un boîtier en plastique noir ; la face avant se déclipse, le bornier est débrochable. La prise LAN et le bornier TIP/RING sont accessibles sur le côté du boîtier, par une ouverture séparée.

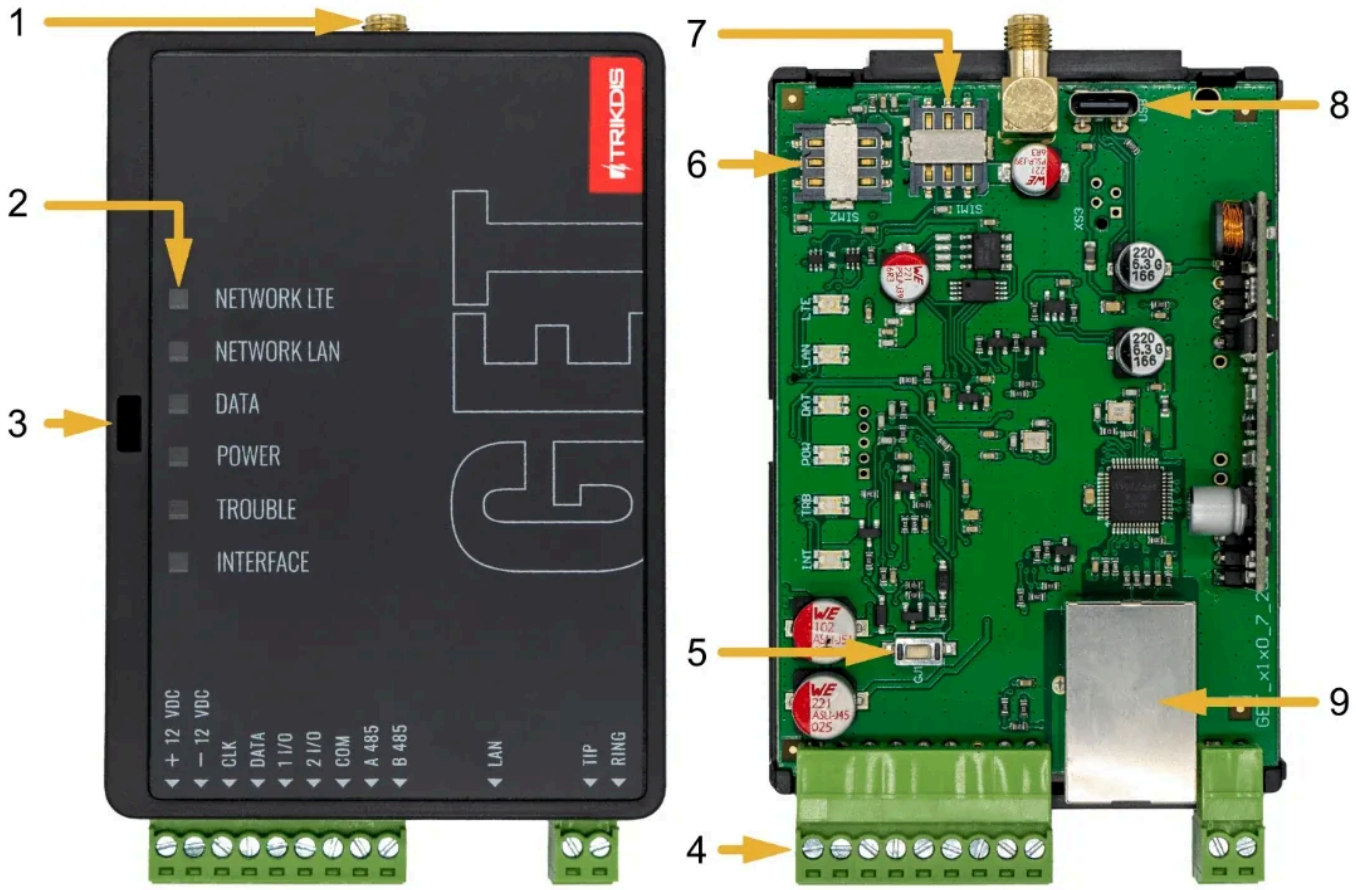


Figure 2. Les éléments du communicateur vus de face (à gauche) et boîtier ouvert (à droite).

- 1 Connecteur SMA de l'antenne mobile
- 2 LED de signalisation (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Encoche facilitant le déclipsage de la face avant
- 4 Bornier débrochable pour les raccordements externes
- 5 Bouton RESET
- 6 Emplacement de la carte SIM2
- 7 Emplacement de la carte SIM1
- 8 Prise USB-C pour la programmation
- 9 Prise Ethernet (LAN) RJ45

Le bornier est débrochable : l'appareil peut ainsi être mis hors tension ou redémarré 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.

1.5 Bornes

Borne	Fonction
+12 VDC	Alimentation, positif : +10–18 V DC

Borne	Fonction
–12 VDC	Alimentation, 0 V
CLK	Bus série ou bus de données (horloge) pour le raccordement direct de la centrale
DATA	Bus série ou bus de données (données) pour le raccordement direct de la centrale
1 I/O	Entrée/sortie 1 (réglage d'usine : sortie, OUT)
2 I/O	Entrée/sortie 2 (réglage d'usine : sortie, OUT)
COM	Point commun (négatif) des entrées et des sorties
A 485	Non utilisée
B 485	Non utilisée (la paire de A 485)
LAN	Prise RJ45 Ethernet (réseau local)
TIP	Borne TIP du transmetteur téléphonique de la centrale d'alarme
RING	Borne RING du transmetteur téléphonique de la centrale d'alarme

Sur les schémas de raccordement, les bornes d'alimentation sont marquées **+DC** et **–DC** (sur l'appareil : +12 VDC / –12 VDC), et les bornes RS485 **A RS485** / **B RS485** (sur l'appareil : A 485 / B 485). Le marquage du bornier figure aussi sur la face avant.

1.6 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 LTE le réseau mobile, NETWORK LAN le réseau filaire, TROUBLE le défaut ; la LED INTERFACE n'a pas de fonction sur le GET.

NETWORK LTE – connexion au réseau mobile

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

NETWORK LAN – connexion au réseau filaire

Signalisation	Signification
éteinte	Pas de connexion au réseau informatique
allumée en vert	Connecté au réseau informatique

DATA – trafic de données

Signalisation	Signification
éteinte	Aucun événement en attente d'envoi
allumée en vert	Des événements en attente d'envoi se trouvent en mémoire
clignote en vert	Transfert de données entre le communicateur et l'ordinateur (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

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

TROUBLE – défaut

Signalisation	Signification
éteinte	Pas de défaut
1 clignotement rouge	Défaut de la liaison physique du réseau filaire (PHY Link) – vérifiez le câble LAN
2 clignotements rouges	Défaut de la carte SIM1
3 clignotements rouges	Défaut de la carte SIM2
7 clignotements rouges	La liaison avec la centrale d'alarme est interrompue (bus série)

INTERFACE – non utilisée sur le GET.

1.7 Caractéristiques techniques

Paramètre	Valeur
Connexion réseau	LTE (4G) et Ethernet (LAN)
Liaison avec la centrale d'alarme	bus série, bus de données (Keybus) ou ligne téléphonique (TIP/RING, Contact ID, DTMF)
Entrées/sorties	2 I/O à double fonction : 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
Modem	EG915U-EU (Europe), EG915U-LA (Amérique latine) ou BG95-M5 (LTE Cat M1) – les bandes de fréquences figurent dans le tableau du point 1.2
Carte SIM	2 emplacements nano-SIM (SIM1, SIM2)
Tension d'alimentation	10–18 V DC
Consommation	au maximum 100 mA en veille ; au maximum 300 mA pendant l'envoi de données

Paramètre	Valeur
Protocoles de transmission	TRK8, DC-09_2007, DC-09_2012, TL150
Chiffrement	AES-128
Mémoire d'événements	60 événements
Programmation	TrikdisConfig (Windows) par câble USB-C ou à distance ; application Protegus 2 (à partir du firmware 1.08)
Environnement de fonctionnement	−10 … +50 °C, humidité relative max. 80 % (à +20 °C)
Dimensions	113 × 70 × 25 mm
Poids	110 g

2. Mise en service rapide

Le communicateur se configure avec deux outils : le logiciel **TrikdisConfig** sous Windows – par câble USB-C ou à distance – et l'**application Protegus 2** (Settings → Advanced settings). Ce chapitre décrit le chemin le plus court : les réglages nécessaires pour que le communicateur envoie les événements au centre de télésurveillance et que le système puisse être piloté depuis l'application Protegus 2. Pour chaque étape, nous indiquons le chemin dans l'application et dans TrikdisConfig ; l'explication détaillée des réglages se trouve au chapitre 6.

2.1 Préparation

Ce dont vous aurez besoin

Câble USB-C pour la programmation · câble d'au moins 4 conducteurs entre le communicateur et la centrale · câble CRP2.4 pour le port série Paradox · tournevis plat de 2,5 mm · antenne mobile avec un gain suffisant si la couverture est faible sur le site · carte SIM active (une ou deux ; la demande de code PIN peut être désactivée) si vous utilisez le réseau mobile · câble Ethernet jusqu'au routeur ou au switch si vous utilisez le réseau filaire · le manuel d'installation de la centrale d'alarme.

Commandez séparément les accessoires nécessaires auprès du distributeur.

Configuration avec TrikdisConfig. Vous configurez l'appareil sur le bureau, avant le raccordement ; sur le site, il ne reste plus qu'à le raccorder.

1. Téléchargez et installez le logiciel TrikdisConfig. Sur le site de Trikdis (www.trikdis.com), saisissez « 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 le boîtier du communicateur avec un tournevis plat : introduisez le tournevis en haut, dans la fente à côté de l'antenne, et faites levier vers l'extérieur, puis en bas, à l'encoche, vers le bas. Le schéma montre aussi l'emplacement de la prise USB-C sur le bord du circuit imprimé.

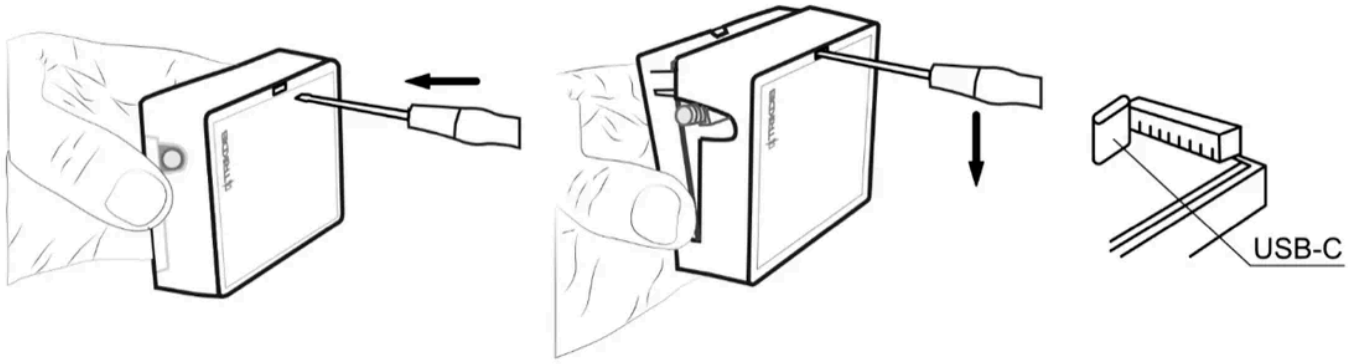


Figure 3. Déclipsage de la face avant avec un tournevis plat ; le détail agrandi montre l'emplacement de la prise USB-C.

3. Insérez la carte nano-SIM (ou les cartes) dans l'emplacement, dans le sens indiqué sur le schéma : l'emplacement SIM1 se trouve au milieu du circuit imprimé, SIM2 sur le bord. La carte doit être active, disposer d'un service de données mobiles et, si possible, désactivez la demande de code PIN dans un téléphone (vous n'aurez ainsi pas à saisir de PIN dans l'appareil). Si vous utilisez le communicateur uniquement sur le réseau filaire, aucune carte SIM n'est nécessaire.

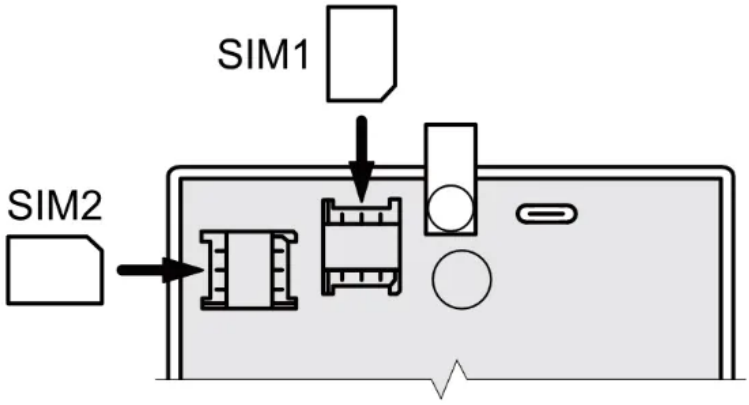


Figure 4. L'emplacement des logements SIM1 et SIM2 sur le circuit imprimé ; les flèches indiquent le sens d'insertion de la carte.

4. Reliez le communicateur à l'ordinateur avec un câble USB-C.

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

Configuration depuis l'application Protegus 2. Vous pouvez configurer depuis l'application si le communicateur est déjà en ligne et que vous l'avez ajouté à votre compte Protegus (point 5.1). Si le communicateur ne peut pas encore se connecter – par exemple parce que la carte SIM demande un code PIN ou que l'opérateur exige un autre APN –, effectuez la première configuration avec TrikdisConfig.

1. Dans l'application, ouvrez le système et allez dans le menu **Settings** → **Advanced settings**.
2. La première fois, l'application affiche un avertissement (**Proceed with Caution**) : ces réglages sont destinés aux professionnels. Appuyez sur **Accept the risk and continue** ; avec la case **Do not show this again**, l'avertissement n'apparaîtra plus.
3. L'application lit les réglages du communicateur. Si elle demande un **Service Access code**, saisissez le code d'accès Protegus Cloud du communicateur (d'usine `123456`).
4. Effectuez les réglages décrits ci-dessous, puis appuyez sur **Write** : l'application les écrit dans le communicateur.

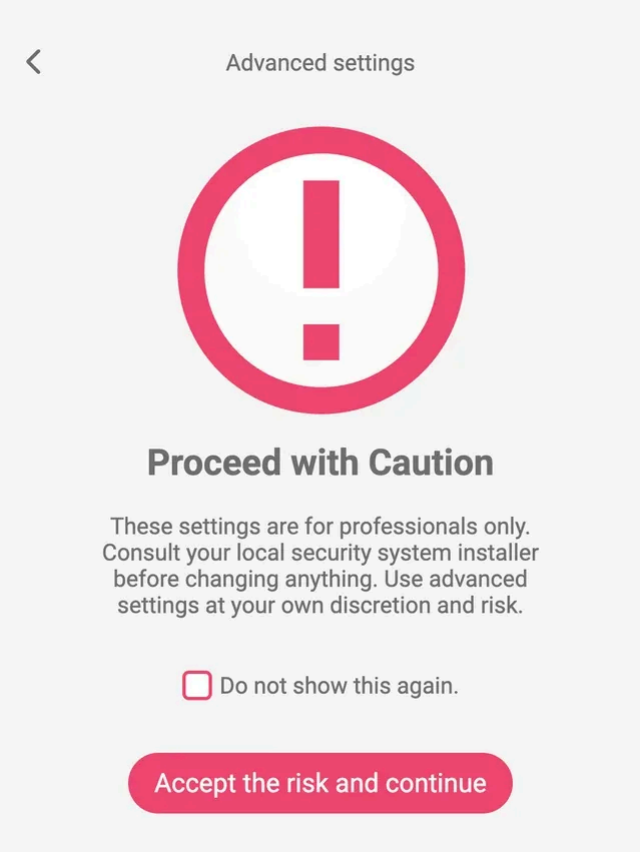


Figure 5. Protegus 2 – l'avertissement affiché à la première ouverture des Advanced settings (Proceed with Caution) et le bouton Accept the risk and continue.

Le GET se configure depuis l'application Protegus 2 **avec le firmware 1.08 ou plus récent** (la mise à jour est décrite au chapitre 9).

2.2 Connexion à l'application Protegus 2

Dans l'application (Settings → Advanced settings) :

1. **Panel settings** → **TLF** – si le communicateur est raccordé aux bornes TIP/RING de la centrale : le **Security panel model** doit être **AUTO**.
2. **Panel settings** → **Serial Bus** – si le communicateur est raccordé au bus de données ou au port série de la centrale : choisissez le modèle de la centrale raccordée dans le champ **Security panel model**.

3. Au même endroit, activez l'option **Remote Arm/Disarm** si les utilisateurs souhaitent piloter la centrale depuis Protegus 2 avec leur propre code clavier. Elle n'apparaît que pour les centrales pilotables directement.
4. Pour le pilotage direct d'une centrale Paradox, saisissez le **PC download password**, pour une centrale Texecom l'**UDL passcode** ; il doit être identique au mot de passe réglé dans la centrale.
5. **User reporting** → **Cloud** : activez l'option **Enabled** et modifiez le **Cloud access code** si vous souhaitez que l'utilisateur doive le saisir lors de l'ajout du système dans l'application (d'usine `123456`).
6. **Network settings** → **LAN** – si le communicateur est raccordé au réseau filaire : activez l'option **Use DHCP**.
7. **Network settings** → **SIM** et **SIM2** – pour chaque carte SIM insérée : saisissez le **SIM card PIN** et l'**APN**, et vérifiez que **DNS1** et **DNS2** fonctionnent chez votre opérateur.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode** : dans les champs **Main type**, **Backup type** et **Backup type 2**, réglez l'ordre dans lequel le communicateur utilise les connexions **LAN**, **SIM** (SIM1) et **SIM2**.
9. Appuyez sur **Write**.

Dans TrikdisConfig. Indiquez d'abord, sur la page **Panel settings**, comment le communicateur est raccordé à la centrale.

Si vous le raccordez à la sortie ligne téléphonique (TIP/RING) de la centrale : choisissez la valeur **AUTO** dans le champ **Communication protocol**.

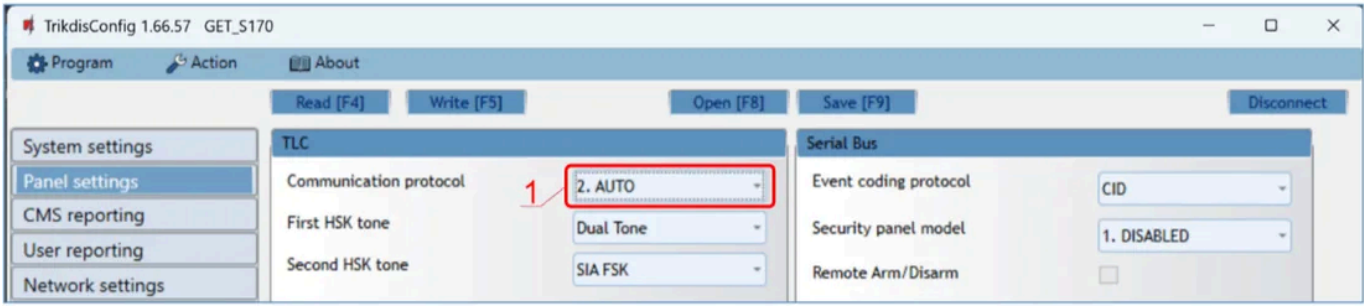


Figure 6. TrikdisConfig – Panel settings, groupe TLC.

- 1 **Communication protocol** – pour un raccordement TIP/RING, **2. AUTO**.

Si vous le raccordez au bus de données ou au port série de la centrale : réglez la centrale dans le groupe **Serial bus**.



Figure 7. TrikdisConfig – Panel settings, groupe Serial bus.

- 2 **Security panel model** – le modèle de la centrale raccordée.
- 3 **Remote Arm/Disarm** – cochez-le si les utilisateurs souhaitent piloter la centrale depuis Protegus 2 avec leur propre code clavier. N'apparaît que pour les centrales pilotables directement.
- 4 **Security panel PC download password** – pour le pilotage direct d'une centrale Paradox ou Texecom, le mot de passe PC ou UDL réglé dans la centrale ; les deux doivent être identiques.

Pour le pilotage direct, la centrale d'alarme doit aussi être configurée – c'est décrit au chapitre 4, où vous trouverez aussi la marche à suivre pour saisir le mot de passe PC ou UDL.

Ensuite, sur la page **User reporting**, dans l'onglet **PROTEGUS Cloud**, autorisez la connexion au cloud.

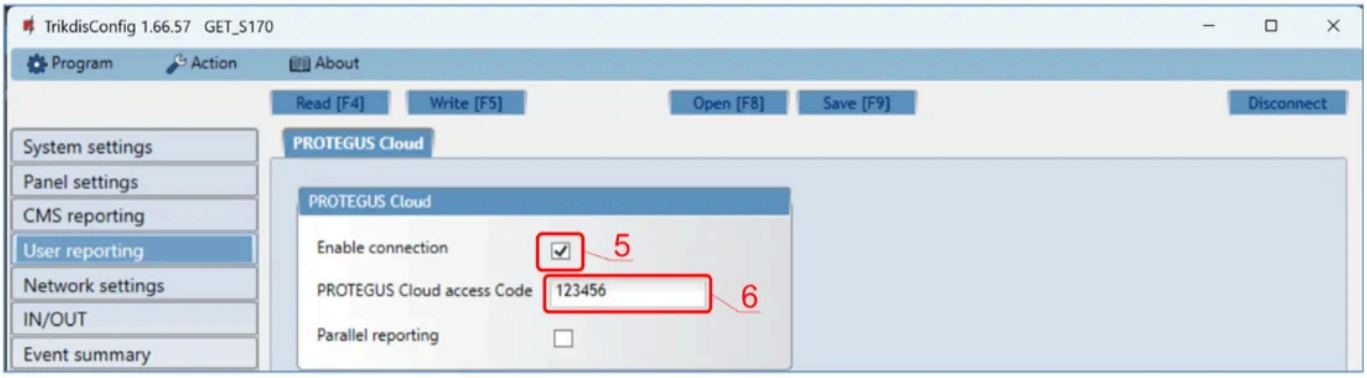


Figure 8. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- 5 **Enable connection** – cochez-le : autorise la connexion au cloud Protegus.
- 6 **PROTEGUS Cloud access Code** – le code d'accès pour Protegus 2 (d'usine `123456`). Modifiez-le si vous souhaitez que l'utilisateur doive le saisir lors de l'ajout du système dans l'application. Si vous modifiez le code plus tard, il faut aussi le changer dans l'application Protegus 2.

Si le communicateur est raccordé au réseau filaire, cochez l'option **Use DHCP** sur la page **Network settings**, onglet **LAN** : le communicateur reçoit automatiquement les réglages du réseau (masque de sous-réseau, passerelle) et une adresse IP.

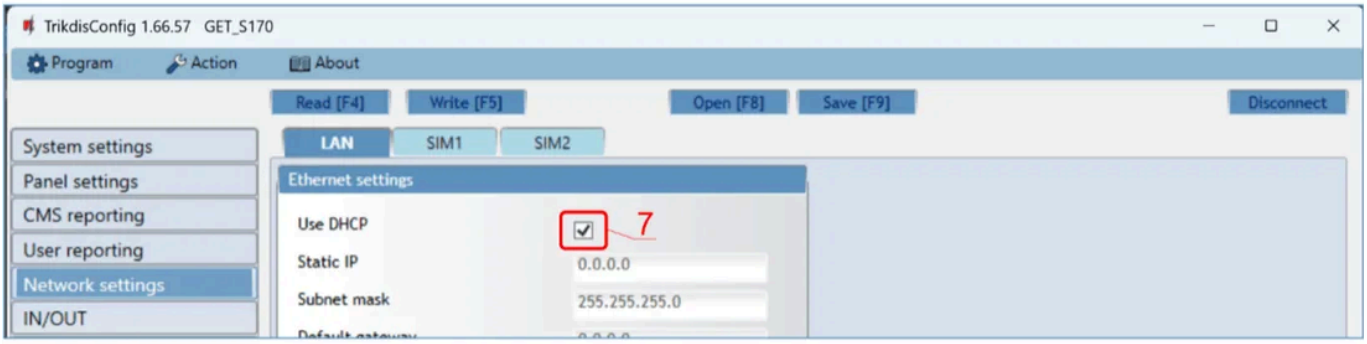


Figure 9. TrikdisConfig – Network settings, onglet LAN (Ethernet settings).

- 7 **Use DHCP** – coché, le communicateur reçoit automatiquement du routeur une adresse IP et les réglages du réseau.

Si le communicateur contient une carte SIM (une ou deux), saisissez les données de la carte dans l'onglet **SIM1** (et **SIM2**).

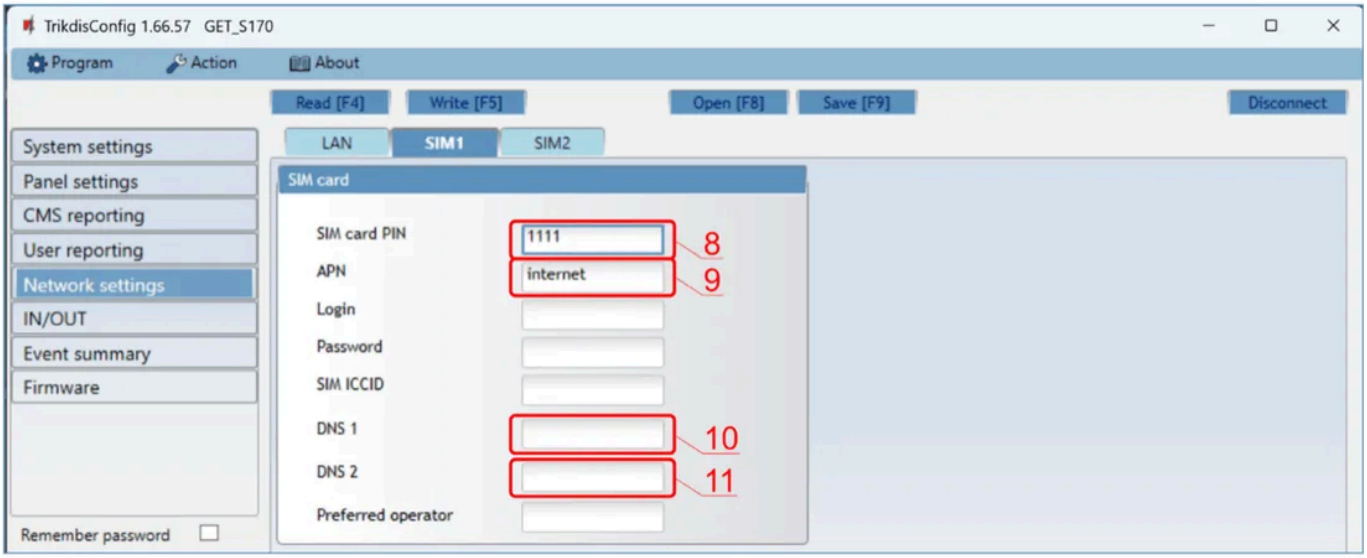


Figure 10. TrikdisConfig – Network settings, onglet SIM1.

- 8 **SIM card PIN** – le code PIN de la carte (si la demande de PIN est désactivée, la valeur d'usine peut rester).
- 9 **APN** – le point d'accès aux données de l'opérateur (voir ci-dessous).
- 10 **DNS 1** – serveur de noms primaire ; d'usine, celui de Google. Indépendamment des réglages IP, vérifiez que les adresses DNS fonctionnent chez votre opérateur.
- 11 **DNS 2** – serveur de noms secondaire (d'usine, également celui de Google).

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 par le réseau mobile. La valeur exacte se trouve sur le site de l'opérateur de la carte SIM. Nous tenons à jour les APN connus des opérateurs européens dans un article séparé : Réglage de l'APN – liste des opérateurs mobiles européens. Si l'opérateur ne vous a pas donné d'autre information, essayez l'APN `internet` : il est générique et fonctionne sur le réseau de nombreux opérateurs.

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.

Enfin, sur la page **CMS reporting**, onglet **Settings**, dans le groupe **Reporting mode**, indiquez l'ordre des connexions : c'est par cette voie que le communicateur envoie les messages au centre de télésurveillance et à Protegus 2.

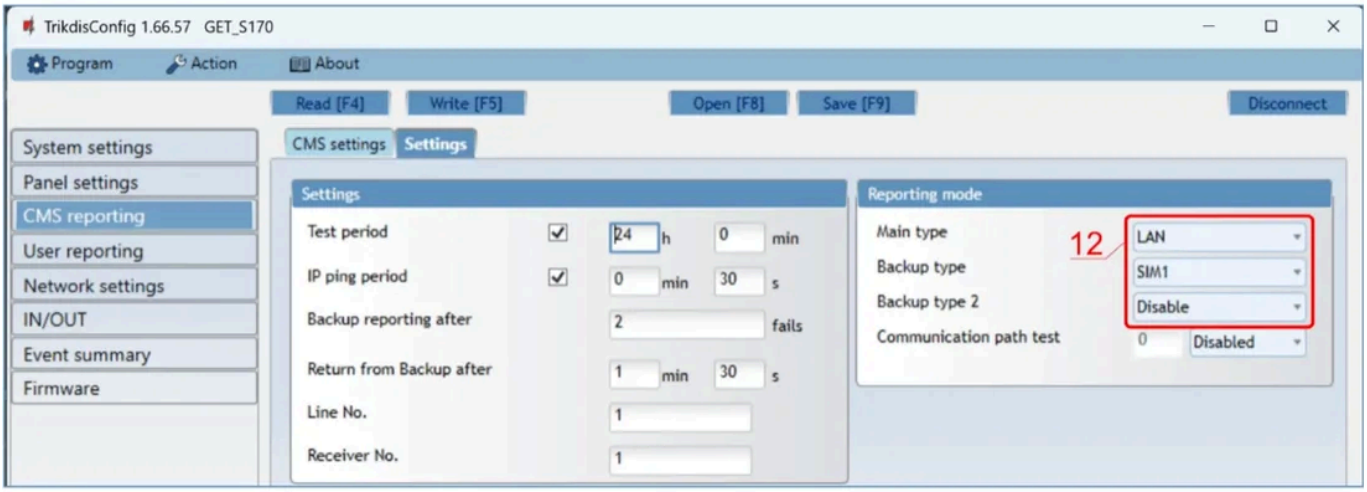


Figure 11. TrikdisConfig – CMS reporting, onglet Settings, groupe Reporting mode (d'usine Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type** : la connexion principale (LAN, SIM1 ou SIM2) ; **Backup type** : la connexion de secours ; **Backup type 2** : la deuxième connexion de secours.

Vous indiquez les types de connexion dans l'ordre. Si le communicateur ne peut pas se connecter avec la connexion **Main type**, il bascule sur **Backup type**, et ainsi de suite. Si la connexion de secours a bien transmis le message au centre de télésurveillance, le communicateur tente de revenir à la connexion principale une fois le délai réglé écoulé (point 6.4.2).

Si l'appareil ne transmet pas vers un centre de télésurveillance, la configuration est terminée : appuyez sur le bouton **Write [F5]** (écriture), attendez la confirmation et débranchez le câble USB.

Pour un raccordement par ligne téléphonique (TIP/RING), n'oubliez pas d'activer et de configurer le transmetteur de la centrale d'alarme, sinon la centrale n'envoie aucun événement ; pour le pilotage direct, les centrales Paradox, Texecom, Caddx, InnerRange et Honeywell doivent aussi être configurées. La configuration de la centrale est décrite au chapitre 4.

2.3 Connexion au centre de télésurveillance

Dans l'application (Settings → Advanced settings) :

1. **System options** → **System general** : saisissez le numéro d'abonné reçu du centre de télésurveillance (**Account No.** ; 0–9, A–F ; `FFFE` et `FFFF` ne peuvent pas être utilisés). Sur la version matérielle **x1x1**, avec le firmware **1.31** ou plus récent, le numéro d'abonné se saisit par canal : **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** Vous le reconnaissez à l'écran : si System general n'affiche que le champ **Time set**, utilisez le réglage du canal.
2. **Panel settings** → **TLF** (raccordement TIP/RING) : le **Security panel model** doit être **AUTO** ; ou **Panel settings** → **Serial Bus** (raccordement au bus de données ou au port série) : choisissez le **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel** : activez l'option **Enabled**, puis saisissez : **Communication type** : **IP** ; l'adresse **Domain or IP** et le **Port** du récepteur ; **TCP or UDP** ; **Protocol** : **TRK8** pour un récepteur Trikdis, **DC-09_2007** ou **DC-09_2012** pour un récepteur universel, **TL150** pour un récepteur SUR-GARD ; et la clé de chiffrement réglée dans le récepteur : pour le protocole TRK dans le champ **TRK encryption key**, pour DC-09 activez l'option **Enable encryption key** et saisissez la **DC-09 encryption key**.
4. (Recommandé) Réglez de la même façon le **Backup channel** (canal de secours).

5. **Reporting to CMS** → **CMS settings** → **Reporting mode** : **Main type**, **Backup type**, **Backup type 2**.
6. **Network settings** → **LAN** (réseau filaire) : activez l'option **Use DHCP**. **Network settings** → **SIM** et **SIM2** (pour chaque carte SIM) : **SIM card PIN**, **APN**, et vérifiez les champs **DNS1**, **DNS2**.
7. Appuyez sur **Write**.

Dans TrikdisConfig. Saisissez d'abord le numéro d'abonné sur la page **System settings**.



Figure 12. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – le numéro d'abonné reçu du centre de télésurveillance (6 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne peuvent pas être utilisés.

Sur la page **Panel settings**, indiquez le raccordement de la centrale si vous ne l'avez pas encore fait au point 2.2 : pour un raccordement TIP/RING, le **Communication protocol** doit être **AUTO** ; pour un raccordement au bus de données ou au port série, choisissez le modèle de la centrale raccordée dans le champ **Security panel model** (schémas du point 2.2).

Ensuite, sur la page **CMS reporting**, onglet **CMS settings**, dans la partie **Primary channel** (canal principal), réglez les données du récepteur. L'image montre la fenêtre avant la configuration : le champ **Communication type** du canal principal est encore sur **Disable**.

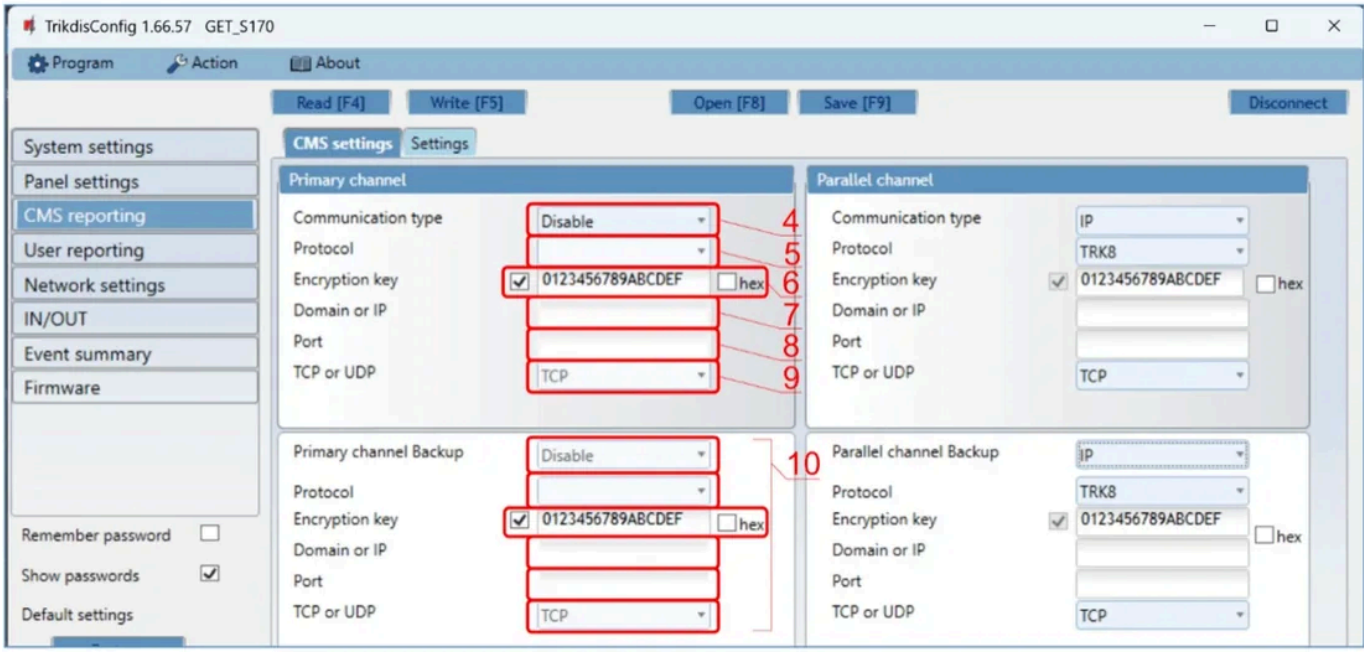


Figure 13. TrikdisConfig – CMS reporting, onglet CMS settings.

- 4 **Communication type** – choisissez la connexion **IP**.
- 5 **Protocol** – **TRK8** pour un récepteur Trikdis, **DC-09_2007** ou **DC-09_2012** pour un récepteur universel, **TL150** pour un récepteur SUR-GARD.
- 6 **Encryption key** – la clé de chiffrement réglée dans le récepteur.
- 7 **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- 8 **Port** – le numéro de port du récepteur.
- 9 **TCP or UDP** – le protocole de transport ; il s'aligne sur le réglage du récepteur.
- 10 **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.

Dans l'onglet **Settings**, groupe **Reporting mode**, indiquez l'ordre des connexions (**Main type**, **Backup type**, **Backup type 2**) si vous ne l'avez pas encore fait au point 2.2 – vous y trouverez aussi le schéma et la description du fonctionnement.

Enfin, sur la page **Network settings**, saisissez les données du réseau si vous ne l'avez pas encore fait au point 2.2 : la case **Use DHCP** dans l'onglet **LAN**, les données de la carte dans l'onglet **SIM1** (et **SIM2**) (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Avec le protocole **DC-09**, saisissez aussi, dans l'onglet **Settings**, le numéro de ligne et le numéro de récepteur (**Line No.**, **Receiver No.**, point 6.4.2). Le GET transmet au centre de télésurveillance uniquement par liaison IP – par le réseau filaire ou l'Internet mobile –, il n'a pas de canal de secours SMS.

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. Pour un raccordement par ligne téléphonique, le transmetteur de la centrale d'alarme doit ici aussi être activé et configuré, sinon la centrale n'envoie aucun événement (chapitre 4).

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 – ou les deux – dans son emplacement, 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 à côté du connecteur d'antenne et soulevez la carte (voir le schéma).
4. Fixez le fond du boîtier avec des vis à l'endroit choisi (les trous de fixation sont entourés sur le schéma), ou avec l'adhésif double face fourni, selon le point 3.2.
5. Remettez le circuit imprimé dans le fond du boîtier et rebranchez le bornier.
6. Vissez l'antenne mobile.
7. Remettez la face avant.
8. Si vous envoyez aussi les événements au centre de télésurveillance par le réseau filaire (LAN), branchez le câble réseau dans la prise LAN du communicateur.

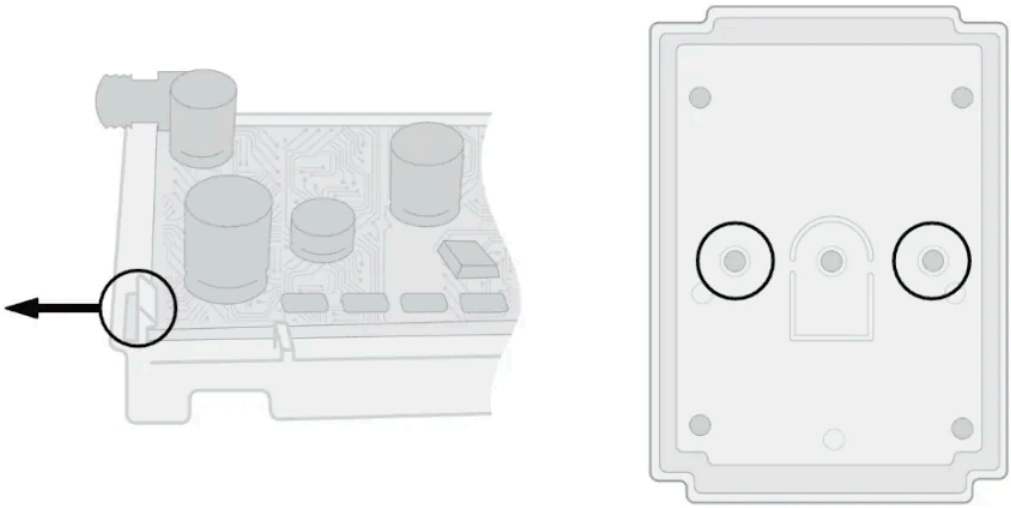


Figure 14. Sortie du circuit imprimé du fond du boîtier (à gauche : le loquet et le sens de sortie) et les trous de fixation du fond du boîtier (à droite).

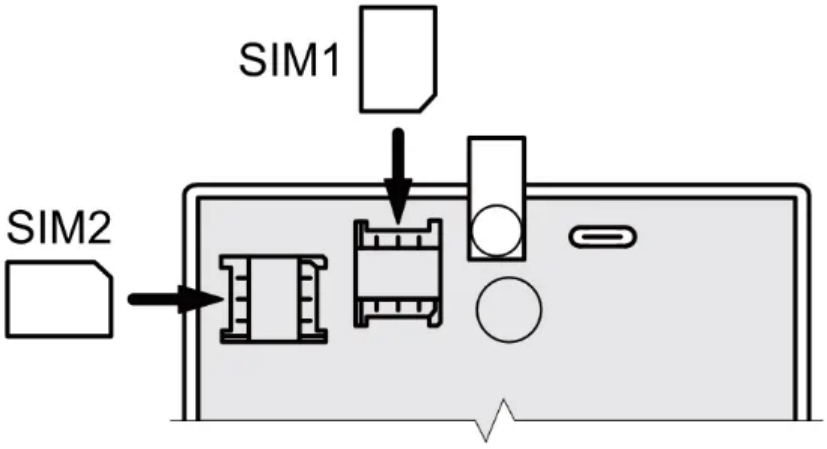


Figure 15. L'emplacement des deux logements SIM sur le circuit imprimé : SIM1 au milieu de la carte, SIM2 sur le bord gauche ; les flèches indiquent le sens d'insertion de la carte.

Le communicateur accepte une ou deux cartes SIM. La carte 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, insérez la carte dans un téléphone mobile et désactivez-y la demande de PIN.

3.2 Emplacement dans le boîtier de la centrale, antenne

Le communicateur doit être installé dans le **boîtier de la centrale d'alarme protégé par un contact d'autoprotection du couvercle**. Fixez-le sur la paroi arrière intérieure du boîtier avec la bande mousse acrylique double face de qualité industrielle fournie : collez la bande sur une surface propre et sèche, en appuyant fortement, pour qu'elle tienne de façon sûre. Si le boîtier de la centrale ne permet pas cette fixation sûre, le communicateur peut aussi être monté dans un boîtier séparé, protégé contre l'ouverture.

- Dans un **boîtier métallique**, le signal mobile est fortement atténué. Si le communicateur est placé dans le boîtier métallique de la centrale, faites sortir l'antenne à l'extérieur du boîtier ou utilisez une antenne à câble plus long.
- Avant la fixation définitive, **vérifiez le niveau de signal** : en 4G, la LED NETWORK LTE doit clignoter en jaune au moins 3 fois (point 1.6). Si c'est moins, cherchez un meilleur emplacement pour l'antenne 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.
- Faites passer le câble LAN par l'entrée de câbles du boîtier jusqu'à la prise RJ45 sur le côté du communicateur ; le câble ne doit pas tirer sur les bornes.



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

Suivez parmi les schémas ci-dessous celui qui correspond à votre centrale. Sur les schémas, **+DC** et **–DC** sont les bornes d'alimentation **+12 VDC** / **–12 VDC** du communicateur, et **A RS485** / **B RS485** les bornes **A 485** / **B 485** (elles n'ont pas à être raccordées sur le GET). Le communicateur est alimenté par la sortie d'alimentation auxiliaire (AUX) de la centrale ; ainsi, en cas de coupure de courant, la batterie de la centrale alimente aussi le communicateur.

3.3.1 DSC – bus de données (Keybus)

Raccordez le Keybus de la centrale DSC au communicateur avec quatre fils : **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

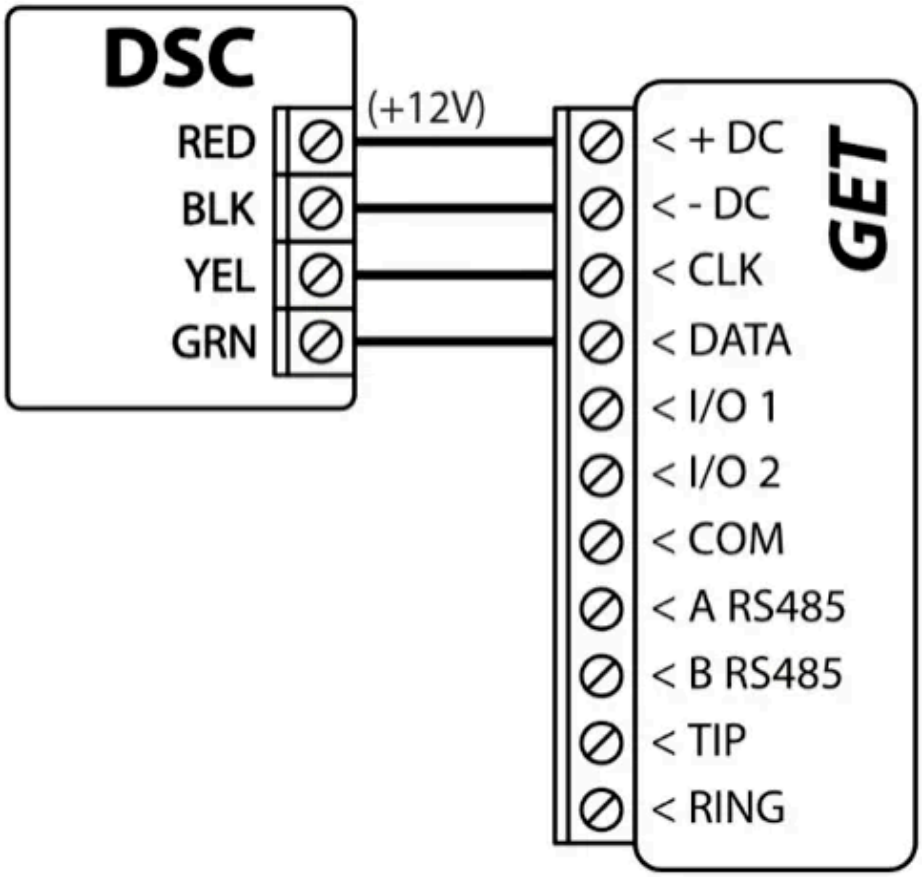


Figure 16. Raccordement d'une centrale DSC sur le bus de données (Keybus, « Keypad bus ») : RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Le GET gère la centrale DSC uniquement sur le bus de données ; le raccordement simultané du Keybus et des bornes TIP/RING n'existe que sur le communicateur GT+. Raccordé uniquement au Keybus, le communicateur reçoit de la centrale l'état général des zones, mais pas le type de zone (incendie, intrusion, fuite d'eau, etc.) ; c'est pourquoi il transmet chaque alarme comme **alarme générale, avec le code Contact ID E130**. Si le centre de télésurveillance a besoin des codes propres à la centrale (par exemple alarme incendie : E110), vous pouvez envoyer les événements par le transmetteur téléphonique de la centrale, avec un raccordement TIP/RING (points 3.3.9 et 4.2) ; dans ce cas, il n'y a pas de pilotage direct.

3.3.2 Paradox – port série

Le communicateur se raccorde au port série de la centrale Paradox avec le câble **EX-CRP2.4**, à commander séparément : **rouge** → **+DC**, **noir** → **–DC**, **jaune** → **CLK**, **vert** → **DATA**.

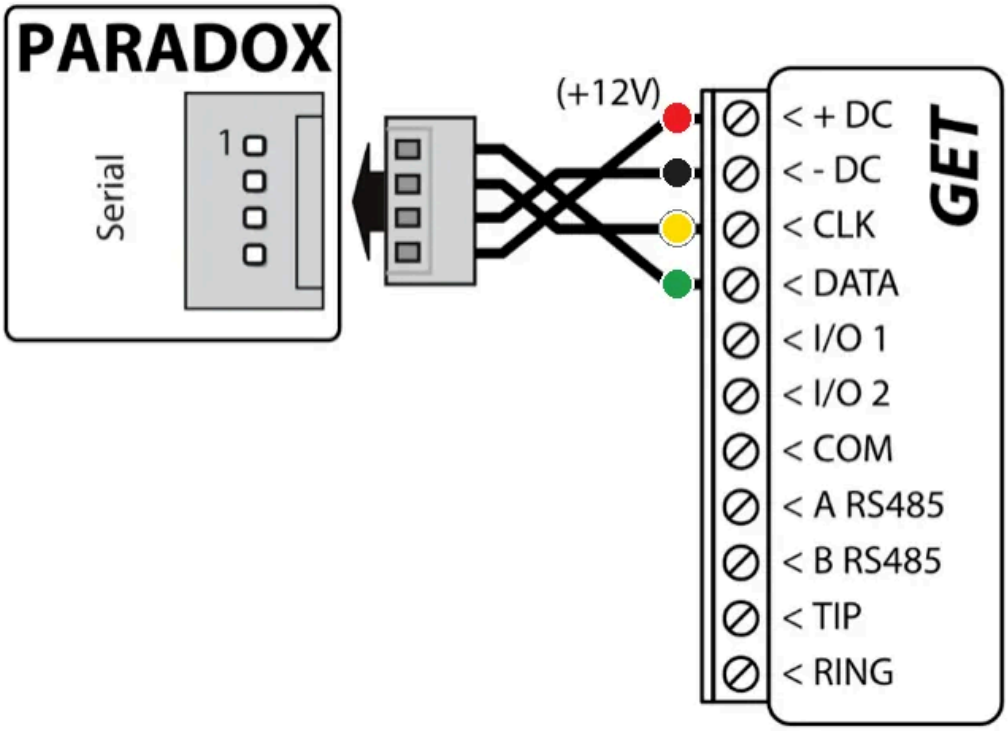


Figure 17. Raccordement d'une centrale Paradox sur le port série avec le câble EX-CRP2.4 (à commander séparément ; « Use the EX-CRP2.4 cable (ordered separately) ») : rouge → +DC, noir → −DC, jaune → CLK, vert → DATA.

- fil rouge (« R - red »)
- fil noir (« B - black »)
- fil jaune (« Y - yellow »)
- fil vert (« G - green »)

Sur les centrales Paradox récentes (SP+, MG+, EVOHD+), le port série peut être verrouillé d'usine ; le déverrouillage est décrit au point 4.1.2. Pour les centrales Spectra SP / SP+ et Magellan MG / MG+, le raccordement décrit au point suivant peut aussi être utilisé à la place du port série.

3.3.3 Paradox SP/MG – Keybus et TIP/RING

Les centrales Paradox Spectra SP, SP+ et Magellan MG, MG+ peuvent aussi être raccordées, à la place du port série, à la fois à leur bus de données (Keybus) et à leurs bornes TIP/RING : **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK**, ainsi que **TIP** → **TIP**, **RING** → **RING**. Ce raccordement utilise le Keybus de la centrale au lieu du port série ; il ne nécessite donc pas le déverrouillage payant du port série Paradox.

Pour ce raccordement, le firmware du communicateur doit être au moins en **1.21** (la mise à jour est décrite au chapitre 9).

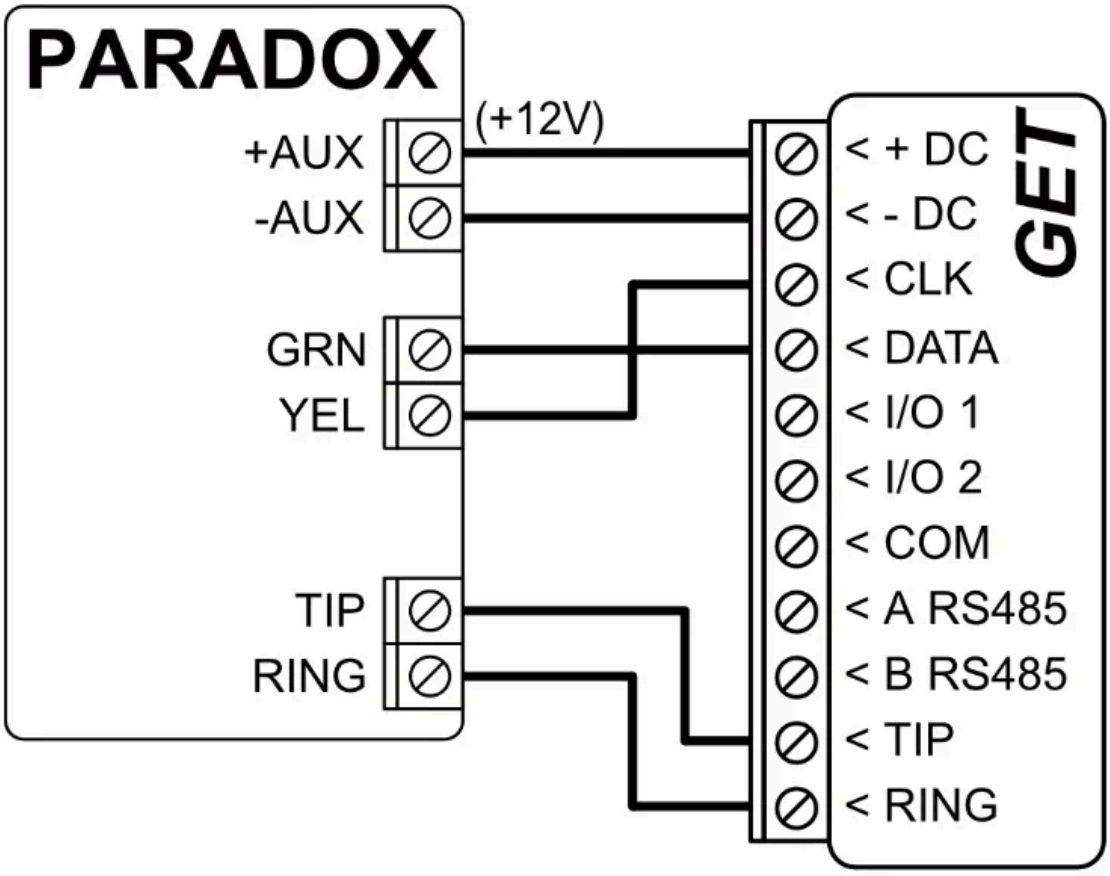


Figure 18. Raccordement d'une centrale Paradox SP / SP+ / MG / MG+ à la fois sur le Keybus (bus de données, « Keypad bus ») et sur les bornes TIP/RING : +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Pour ce raccordement, réglez les éléments suivants sur la page **Panel settings** de TrikdisConfig :

1. **Communication protocol** : **2. AUTO**.
2. **Security panel model** : choisissez dans la liste l'élément **Paradox SP+/MG+ series KeyBus** (sur l'image, 7. PARADOX SP+/MG+).
3. **Remote Arm/Disarm** : cochez-le si les utilisateurs souhaitent piloter la centrale depuis l'application Protegus 2 avec leur propre code clavier.
4. **Security panel PC download password** : pour le pilotage direct, saisissez le mot de passe PC réglé dans la centrale ; les deux doivent être identiques.



Figure 19. TrikdisConfig – Panel settings pour le raccordement Keybus + TIP/RING : Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm coché (3), Security panel PC download password saisi (4).

Dans l'application Protegus 2, les mêmes réglages se trouvent dans les pages **Panel settings** → **TLF** (Security panel model = Communication protocol) et **Panel settings** → **Serial Bus** (point 6.3).

La centrale Paradox doit aussi être programmée pour qu'elle envoie les événements au centre de télésurveillance et qu'elle puisse être pilotée depuis Protegus 2 – sur le clavier raccordé à la centrale, réglez les cellules suivantes :

Cellule	Valeur	Cellule	Valeur
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

Le mot de passe PC saisi dans la cellule **911** doit être identique au champ **Security panel PC download password** du communicateur (point 4.1.2).

3.3.4 UTC Interlogix (Caddx) – bus de données

Raccordez le bus de données de la centrale Caddx NetworX au communicateur avec trois fils : **POS** → **+DC**, **COM** → **−DC**, **DATA** → **DATA**. Les bornes CLK, TIP et RING ne sont pas nécessaires.

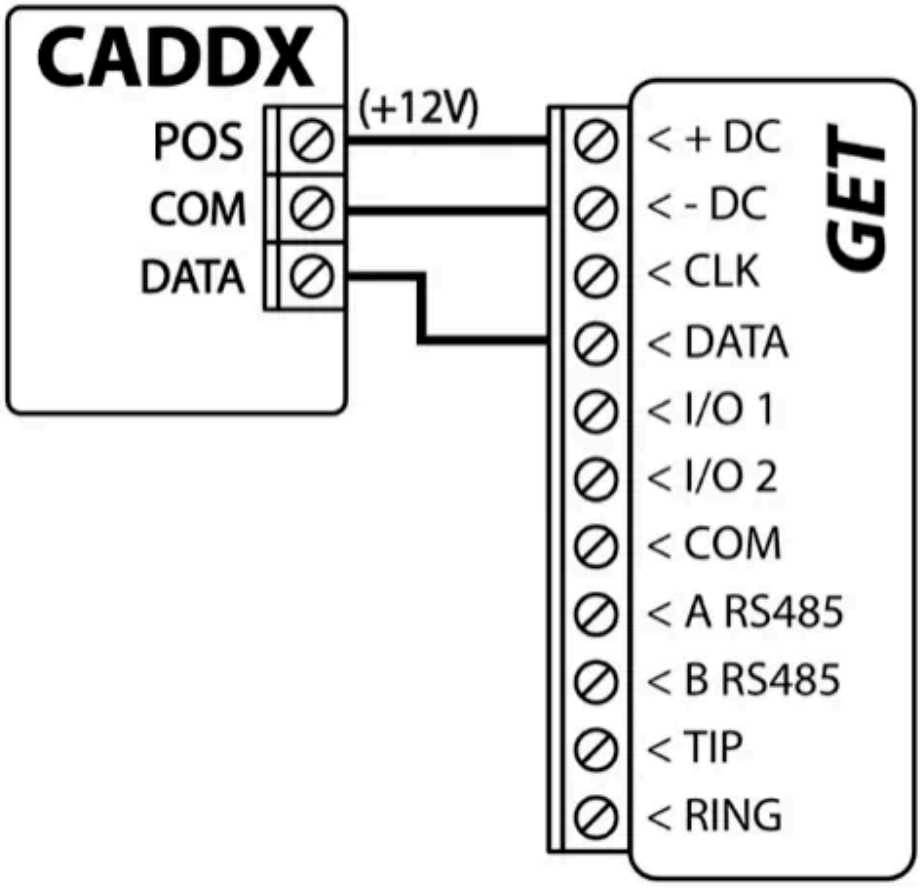


Figure 20. Raccordement d'une centrale UTC Interlogix (Caddx) NetworX sur le bus de données (« Keypad bus ») : POS → +DC, COM → −DC, DATA → DATA.

3.3.5 Texecom – port série

Le communicateur se raccorde au port série de la centrale Texecom Premier / Premier Elite avec le câble **EX-CRP4**, à commander séparément : **rouge** → **+DC**, **noir** → **−DC**, **bleu** → **CLK**, **blanc** → **DATA**.

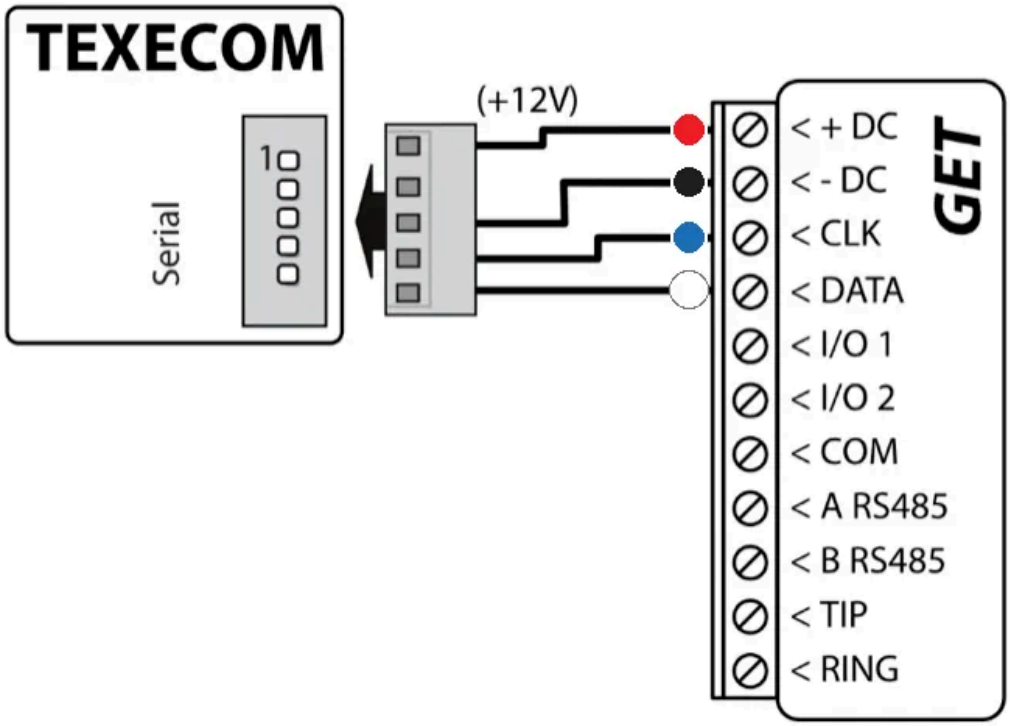


Figure 21. Raccordement d'une centrale Texecom sur le port série avec le câble EX-CRP4 (à commander séparément ; « Use the EX-CRP4 cable (ordered separately) ») : rouge → +DC, noir → −DC, bleu → CLK, blanc → DATA.

- fil rouge (« R - red »)
- fil noir (« B - black »)
- fil bleu (« BL - blue »)
- fil blanc (« W - white »)

3.3.6 InnerRange Inception

Le communicateur est alimenté par la sortie d'alimentation de la centrale Inception (**VOUT + → +DC**, **VOUT 0V → −DC**), et la liaison de données passe par le port USB de la centrale, avec le câble Inner Range **993030USB** : **noir → 0V / −DC**, **vert → CLK**, **blanc → DATA**.

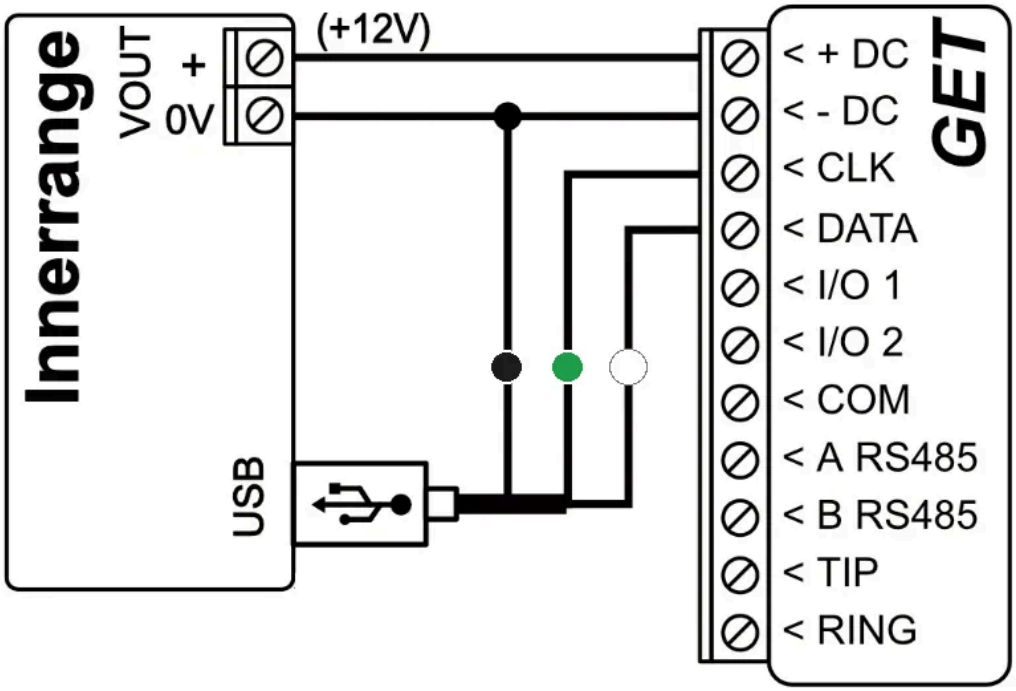


Figure 22. Raccordement d'une centrale InnerRange Inception : VOUT + → +DC, VOUT 0V → −DC ; depuis le port USB, avec le câble 993030USB (« Cable, Inner Range part number 993030USB »), noir → −DC, vert → CLK, blanc → DATA.

- fil noir (« Black wire »)
- fil vert (« Green wire »)
- fil blanc (« White wire »)

3.3.7 InnerRange Integriti

Le communicateur se raccorde au port série **Port 0** de la centrale Integriti avec le câble Inner Range **INTG-996795** : **+DET (+13 V) → +DC**, **GND (5) → −DC**, **Rx (3) → CLK**, **Tx (2) → DATA**.

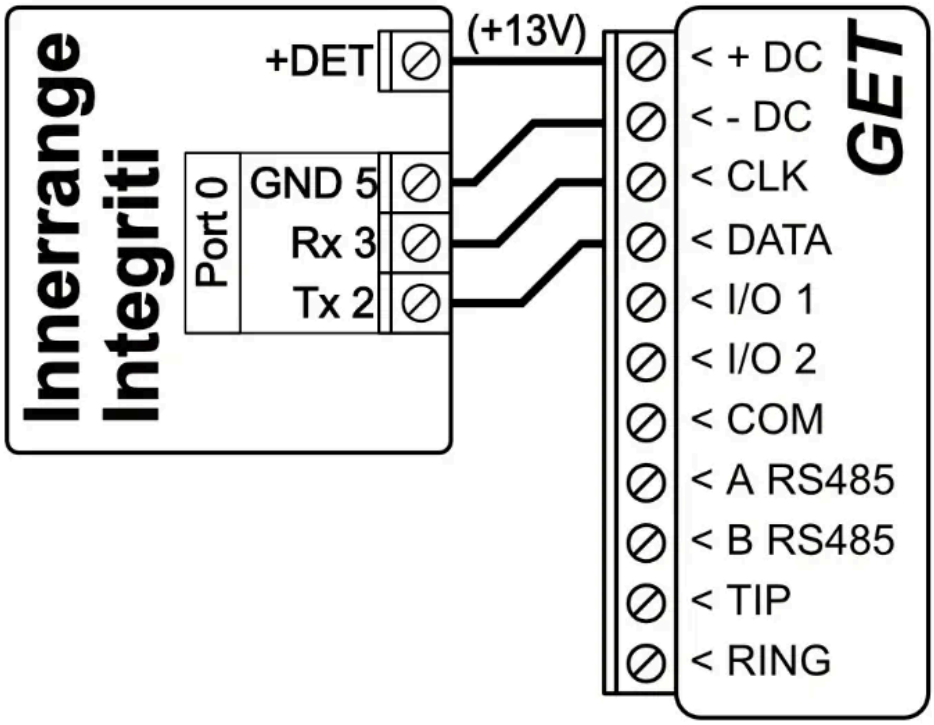


Figure 23. Raccordement d'une centrale InnerRange Integriti sur le Port 0 avec le câble INTG-996795 (« Cable, Inner Range part number INTG-996795 ») : +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – bus de données

Raccordez le bus clavier des centrales Honeywell Ademco Vista-15, Vista-20 et Vista-48 au communicateur depuis les bornes de la centrale : **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.

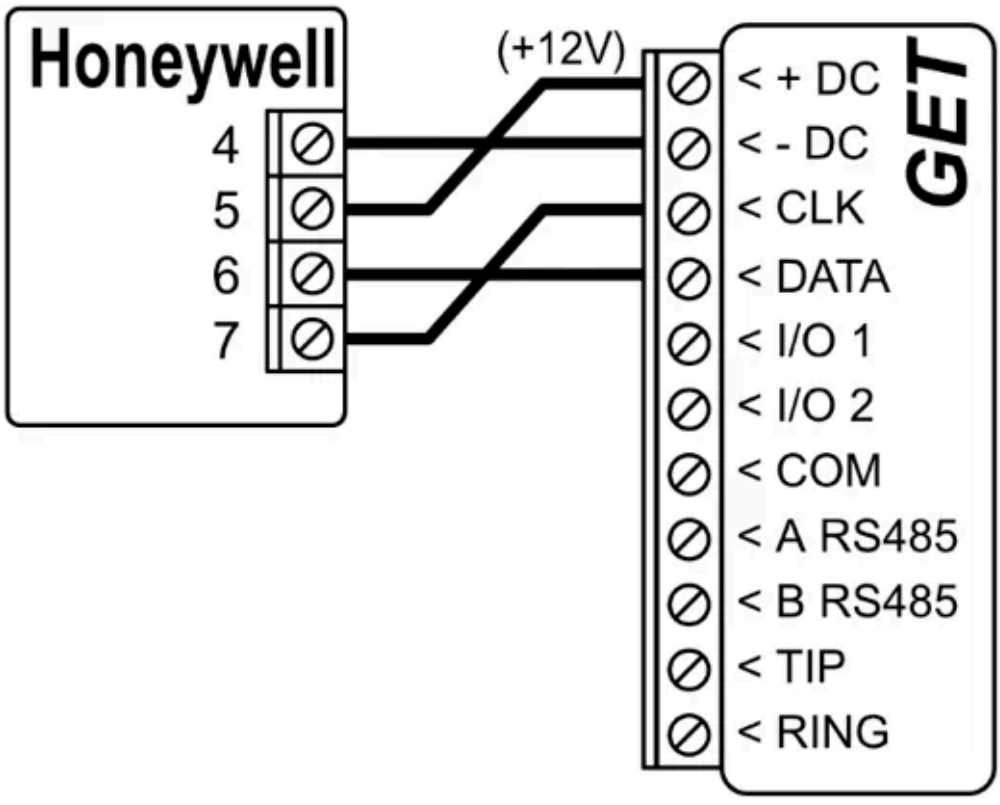


Figure 24. Raccordement d'une centrale Honeywell Vista-15 / -20 / -48 sur le bus de données (« Keypad bus ») : borne 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Toute centrale – TIP/RING

Toute autre centrale peut être raccordée par son transmetteur téléphonique : l'alimentation depuis la sortie d'alimentation auxiliaire de la centrale (**+AUX** → **+DC**, **–AUX** → **–DC**), la sortie ligne téléphonique sur les bornes **TIP** et **RING** du communicateur (**TIP** → **TIP**, **RING** → **RING**). Le transmetteur de la centrale doit être configuré (point 4.2).

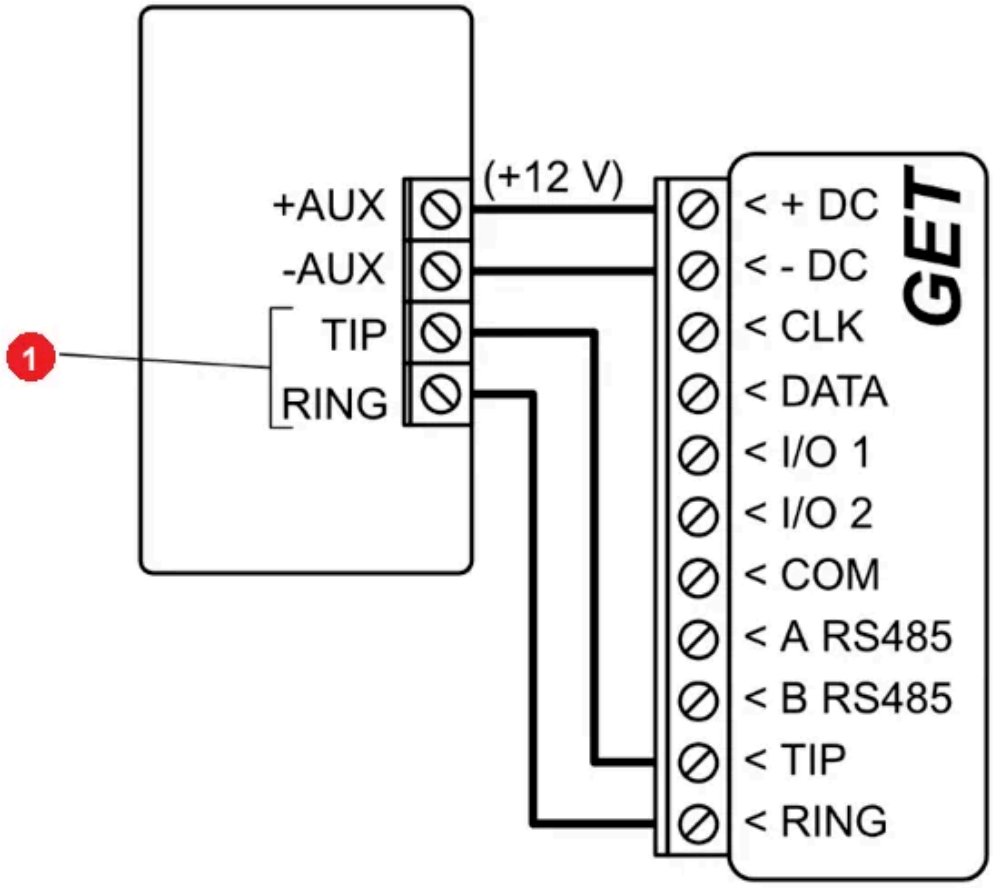


Figure 25. Raccordement au transmetteur téléphonique de la centrale (« Control panel ») : +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 bornes du transmetteur téléphonique de la centrale (« Telephone line communicator terminals »)

3.4 Raccordement d'une zone à clé

Si vous souhaitez armer et désarmer la centrale depuis l'application Protegus 2 de façon que la sortie (PGM) du communicateur commande la **zone à clé** de la centrale, suivez ce raccordement. Les deux bornes I/O à double fonction du communicateur fonctionnent comme sorties (OUT, PGM) – sur le GET, les deux sont des sorties d'usine –, de sorte que les deux sorties peuvent commander deux partitions du système : raccordez la zone à clé de la partition 1 à la borne **1 I/O**, celle de la partition 2 à la borne **2 I/O**. Avec ce raccordement, décochez **Remote Arm/Disarm** sur la page **Panel settings** de TrikdisConfig, les bornes doivent être en fonction **OUT** sur la page **IN/OUT** (point 6.7), et dans l'application Protegus 2, attribuez les sorties aux partitions selon le point 5.2.

Avec un raccordement au bus de données ou au port série, la liaison de données entre la centrale et le communicateur est conservée (le communicateur lit les événements sur le bus), l'armement et le désarmement se font par la zone à clé :

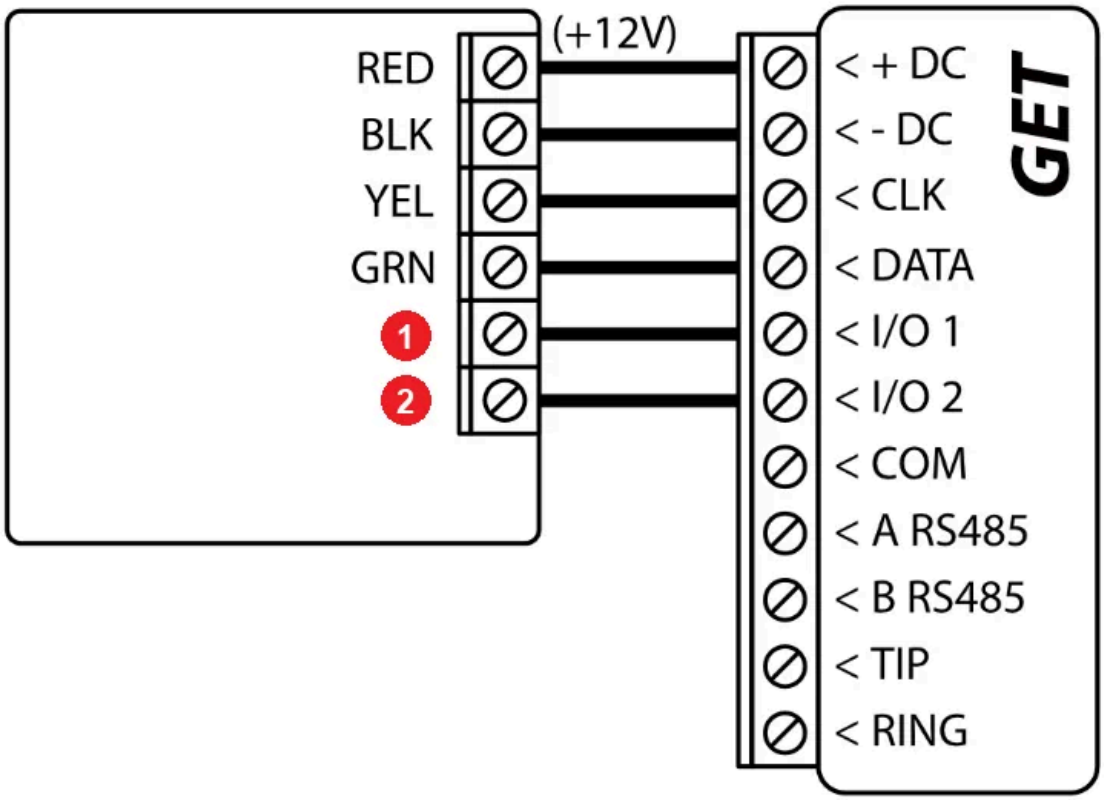


Figure 26. Armement et désarmement par zone à clé (« Zone (keyswitch) »), avec un raccordement au bus de données ou au port série (« Keypad bus or Serial port ») : borne RED de la centrale d'alarme (« Control panel ») → +DC, BLK → −DC, YEL → CLK, GRN → DATA ; zone de la partition 1 → 1 I/O, celle de la partition 2 → 2 I/O.

- 1 zone à clé de la partition 1 (« 1-st Area »)
- 2 zone à clé de la partition 2 (« 2-nd Area »)

Avec un raccordement par ligne téléphonique (TIP/RING), la centrale envoie les événements par son transmetteur ; l'armement et le désarmement se font de la même façon par la zone à clé :

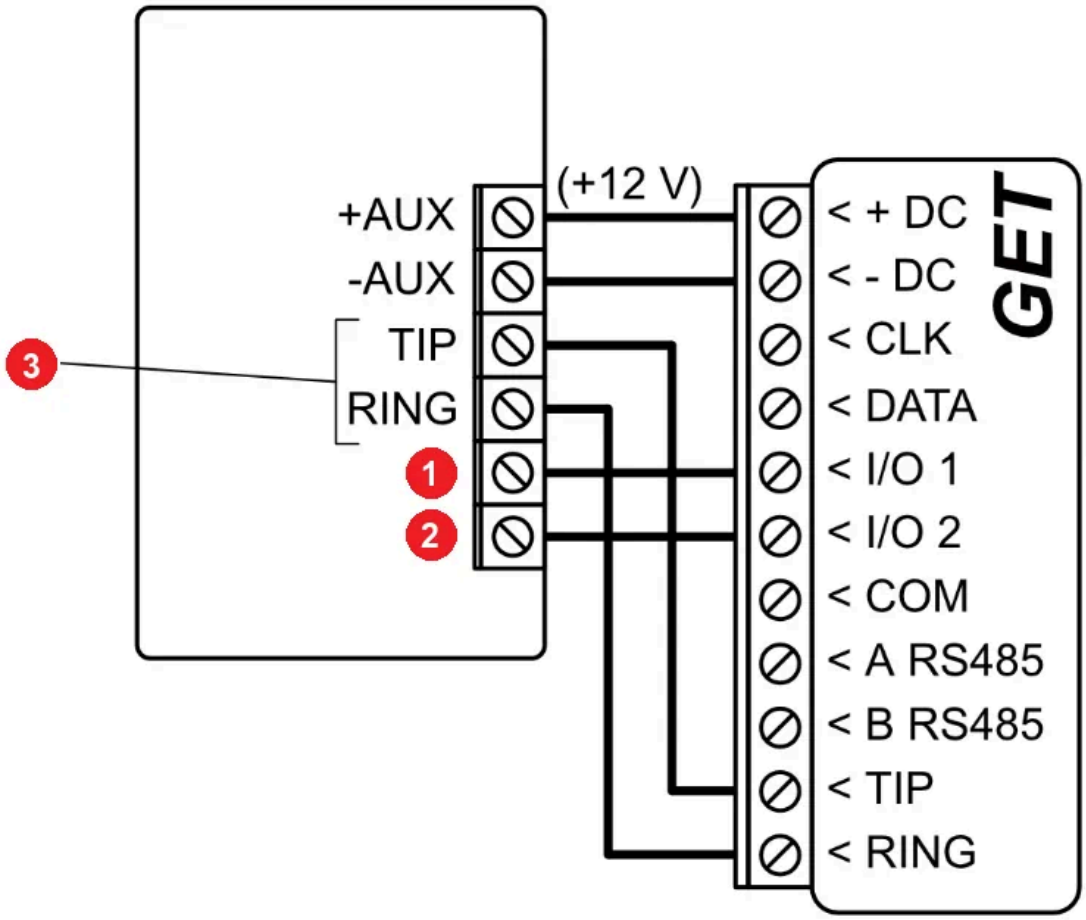


Figure 27. Armement et désarmement par zone à clé (« Zone (keyswitch) »), avec un raccordement par ligne téléphonique : borne +AUX de la centrale d'alarme (« Control panel ») → +DC, −AUX → −DC, TIP → TIP, RING → RING ; zone de la partition 1 → 1 I/O, celle de la partition 2 → 2 I/O.

- 1 zone à clé de la partition 1 (« 1-st Area »)
- 2 zone à clé de la partition 2 (« 2-nd Area »)
- 3 bornes du transmetteur téléphonique de la centrale (« Telephone line communicator terminals »)

La zone à clé peut être à impulsion ou à deux positions – le même mode doit être réglé dans l'application Protegus 2 (point 5.2). Un article séparé traite des détails et des 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

Les deux bornes I/O à double fonction du communicateur peuvent aussi être utilisées comme entrées (IN) pour recevoir d'autres détecteurs (p. ex. contact d'autoprotection, bouton panique), indépendamment de la centrale d'alarme. Un circuit NO, NC, NO/EOL, NC/EOL, NO/DEOL ou NC/DEOL peut être raccordé à l'entrée. Sur le GET, les bornes sont des sorties d'usine : réglez la borne utilisée sur la fonction **IN** sur la page **IN/OUT** de TrikdisConfig, et indiquez le type du circuit raccordé dans le champ **Type** ; dans l'application Protegus 2, le même réglage se trouve dans la page **Advanced settings** → **IN/OUT**, dans le champ **Type** de la borne 1 ou 2 (point 6.7). L'entrée doit être raccordée entre la borne I/O choisie et la borne **COM**, selon le type choisi.

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	–
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 entre COM et le point INx : NO, NC, NC/EOL, NO/EOL, ainsi que, avec détection d'autoprotection, NO/DEOL et NC/DEOL, avec des résistances de fin de ligne de 2,2 kΩ ; les différents états (court-circuit, coupure, 2,2 kΩ, 3,3–5,5 kΩ) sont expliqués dans le tableau du point 3.5.

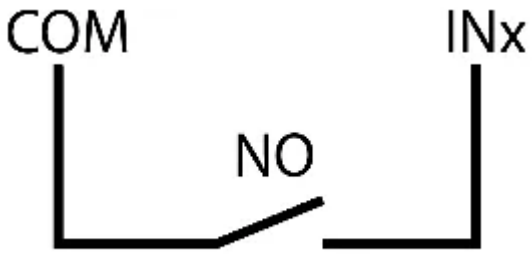


Figure 28. NO – circuit ouvert au repos : fermé – alarme, ouvert – état de repos.

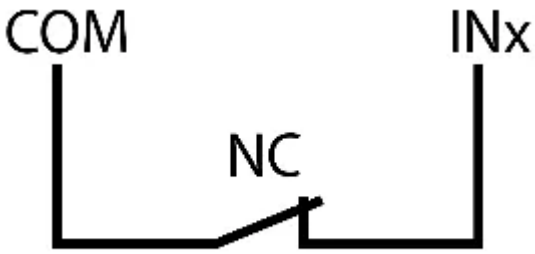


Figure 29. NC – circuit fermé au repos : ouvert – alarme, fermé – état de repos.

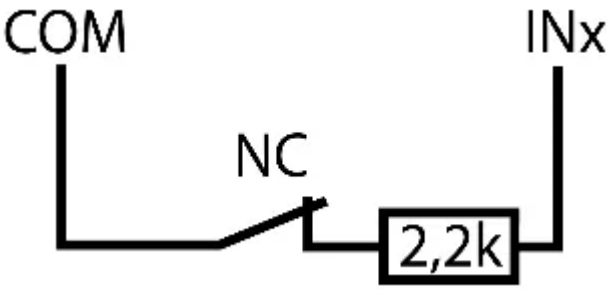


Figure 30. NC/EOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

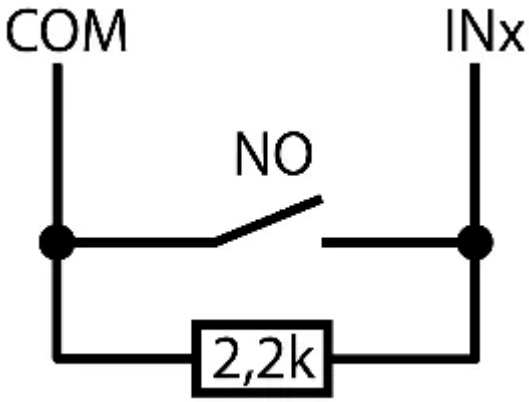


Figure 31. NO/EOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

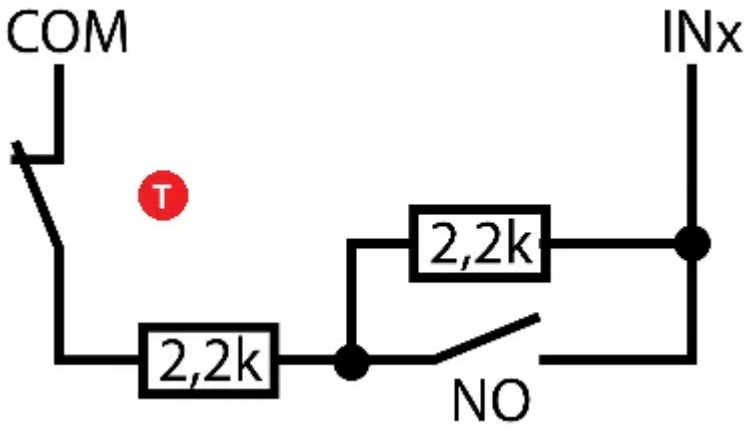


Figure 32. NO/DEOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

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

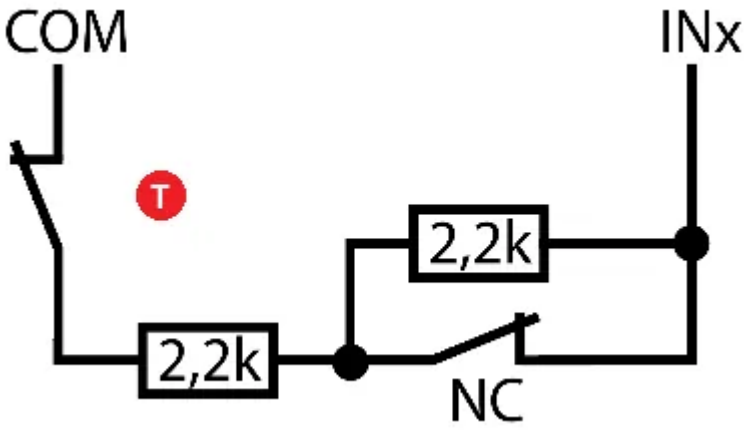


Figure 33. NC/DEOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

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

3.6 Raccordement d'une sortie avec un relais

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 au maximum 0,15 A, jusqu'à 30 V DC. Avec les contacts d'un relais, vous pouvez mettre en marche et arrêter divers appareils électriques : une extrémité de la bobine du relais va sur **+DC**, l'autre sur la borne **x I/O**, et le consommateur est commuté par les contacts du relais (NC, C, NO). La borne I/O utilisée doit être une sortie (**OUT**) sur la page **IN/OUT** de TrikdisConfig (ou dans la page IN/OUT de l'application) – sur le GET, c'est le réglage d'usine.

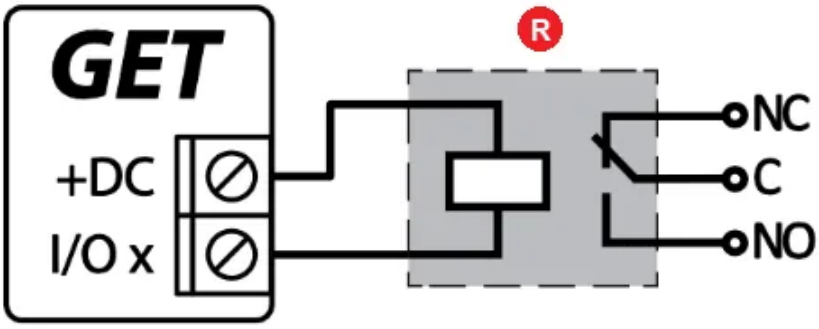


Figure 34. Raccordement d'un relais sur la sortie du communicateur : la bobine se place entre +DC et la borne x I/O, les contacts (NC, C, NO) commutent le consommateur.

- R relais (« Relay »)

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

3.7 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 lui aussi à la mise sous tension de la centrale d'alarme. Voici ce que vous devez voir sur la face avant :

- **POWER** allumée en vert – l'alimentation est correcte ;
- **NETWORK LTE** allumée en vert et clignotant en jaune – connecté au réseau mobile ; le nombre de clignotements jaunes indique le niveau de signal : en 4G, 3 clignotements sont suffisants ; si vous en comptez moins, le signal est faible : cherchez un autre emplacement pour le communicateur ou l'antenne, ou utilisez une antenne plus sensible (point 3.2) ;
- **NETWORK LAN** allumée en vert si vous avez aussi branché un câble réseau – connecté au réseau filaire ;
- **TROUBLE** éteinte.

Si la LED TROUBLE clignote, le nombre de clignotements indique la cause (point 1.6) ; toute autre signalisation des LED indique aussi un défaut, dont vous trouverez la cause à l'aide des tableaux du point 1.6. Si aucune LED ne s'allume, vérifiez l'alimentation et le raccordement.

4. Programmation de la centrale d'alarme

La configuration de la centrale dépend de la façon dont vous l'avez raccordée : par le bus de données ou le port série (point 4.1), ou par son transmetteur téléphonique, sur les bornes TIP/RING (point 4.2). Pour le raccordement Keybus + TIP/RING des centrales Paradox SP / SP+ / MG / MG+, le réglage des cellules de la centrale est donné dans le tableau du point 3.3.3.

4.1 Raccordement au bus de données ou au port série

Nous décrivons ici comment configurer la centrale pour que le communicateur lise ses événements et puisse la piloter à distance. Pour le pilotage à distance, l'option **Remote Arm/Disarm** doit être cochée sur la page **Panel settings** de TrikdisConfig (dans l'application : **Panel settings** → **Serial Bus**) (points 2.2 et 6.3).

4.1.1 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.

4.1.2 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.

Sur le communicateur GET, le champ **Security panel PC download password** se trouve sur la page **Panel settings** de TrikdisConfig, dans le groupe **Serial bus** ; dans l'application Protegus 2 : **Panel settings → Serial Bus → PC download password** (points 2.2 et 6.3).

Raccordement Keybus et TIP/RING (SP / SP+ / MG / MG+, point 3.3.3) : la centrale doit en outre être programmée pour qu'elle envoie les événements au centre de télésurveillance et qu'elle puisse être pilotée depuis Protegus 2 – les valeurs des cellules (801, 811, 812, 815, 911) sont données dans le tableau du point 3.3.3.

4.1.3 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]**.

Sur le communicateur GET, le champ **Security panel PC download password** se trouve sur la page **Panel settings** de TrikdisConfig, dans le groupe **Serial bus** (dans l'application : **Panel settings** → **Serial Bus** → **PC download password**) ; l'UDL passcode doit lui être identique.

4.1.4 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.

4.1.5 InnerRange

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.

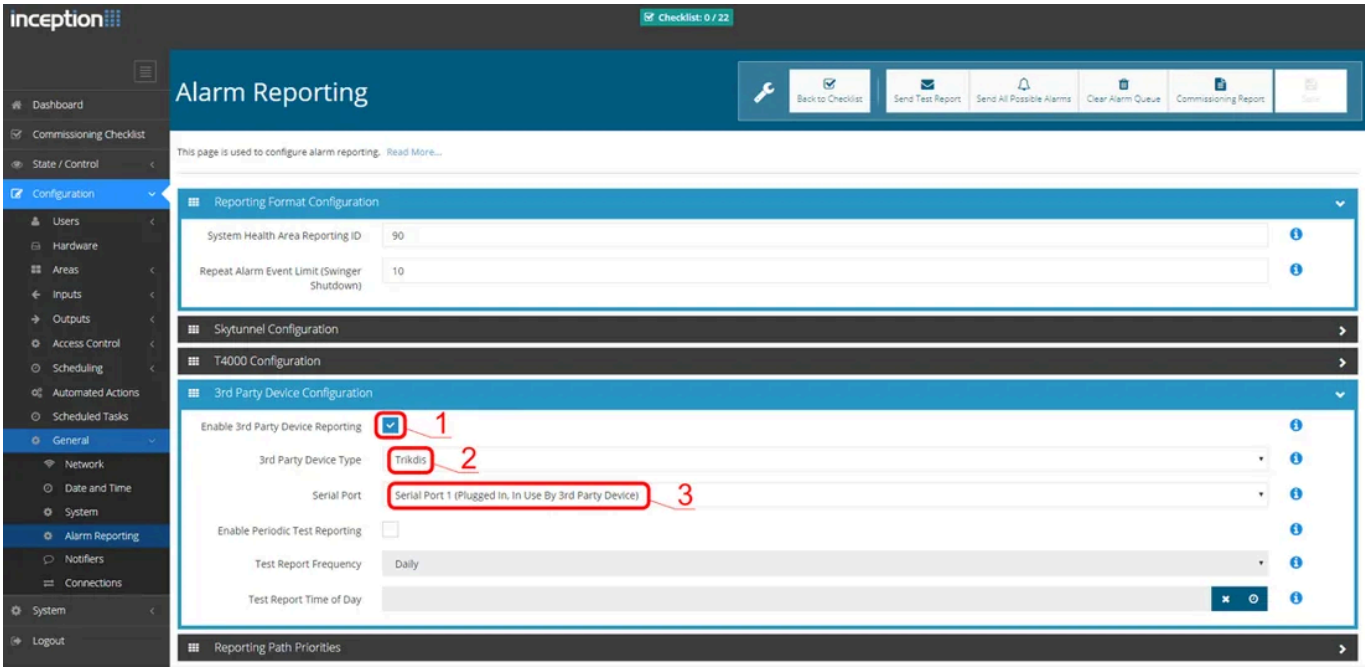


Figure 35. InnerRange Inception – Configuration → General → Alarm Reporting, groupe 3rd Party Device Configuration : Enable 3rd Party Device Reporting coché, 3rd Party Device Type : Trikdis, Serial Port : Serial Port 1.

4.1.6 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]**.

4.2 Raccordement par ligne téléphonique (TIP/RING)

Pour que la centrale d'alarme envoie les événements sur sa sortie ligne téléphonique, son transmetteur téléphonique doit être activé et réglé. Les adresses de programmation exactes figurent dans le manuel d'installation de la centrale ; le principe du réglage est le même chez tous les fabricants :

1. **Activez le transmetteur téléphonique (RTC)** dans la centrale.
2. **Saisissez `1234` comme numéro de téléphone** du récepteur de télésurveillance – que le communicateur soit raccordé aux bornes RING/TIP de la centrale ou à la ligne téléphonique. Avec un autre numéro, il arrive que la centrale compose le numéro mais que le communicateur ne reçoive pas les événements : sur une centrale DSC PowerSeries NEO également, la transmission n'a démarré qu'après la modification du numéro en `1234`.
3. **Mode de numérotation :** DTMF (tone), pas à impulsions.
4. **Protocole :** Contact ID.

Si vous souhaitez armer et désarmer la centrale à distance via la sortie du communicateur, la zone raccordée à cette sortie doit être paramétrée dans la centrale comme **zone à clé**.

La zone à clé peut être à impulsion ou à deux états (maintenue). Par défaut, la sortie du communicateur délivre une impulsion de 3 secondes ; vous pouvez modifier la durée de l'impulsion ou passer en mode à deux états dans les réglages de l'application Protegus 2.

Les centrales DSC, Paradox, Caddx, Texecom, InnerRange et Honeywell peuvent aussi être raccordées au communicateur par leur sortie ligne téléphonique (point 3.3.9) – dans ce cas, c'est aussi le transmetteur qu'il faut configurer, et le pilotage direct n'est pas disponible.

4.2.1 Programmation du transmetteur Honeywell Vista

Sur le clavier, passez en mode programmation et réglez les adresses de programmation suivantes :

Adresse	Réglage
`*41`	numéro de téléphone du récepteur de télésurveillance : `1234`
`*43`	numéro d'abonné (identifiant de site) de la centrale
`*47`	Tone dial = `1`, et nombre de tentatives de numérotation
`*48`	`7` (par défaut)
`*49`	`5` (message Split/Dual)
`*50`	délai d'envoi de l'alarme intrusion – par défaut `2,0` (30 s) ; pour un envoi immédiat `0,0`

Pour une centrale **Honeywell Vista 48**, réglez en outre les adresses de programmation suivantes :

Adresse	Valeur	Adresse	Valeur	Adresse	Valeur
`*41`	1234 (numéro de téléphone du récepteur)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (numéro d'abonné)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1

Adresse	Valeur	Adresse	Valeur	Adresse	Valeur
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

À la fin de la programmation, quittez le mode programmation avec la commande `*99`.

4.2.2 Transmetteur des centrales UTC Interlogix (Caddx) NX

Programmation de la centrale Interlogix NX-4V2 (NX-6V2, NX-8V2) lorsque le communicateur est raccordé aux bornes TIP/RING de la centrale. Sur le clavier, saisissez successivement :

Emplacement (location)	Touches	Remarque
	`*89713`	Entrée en programmation (`9713` est le code installateur d'usine)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Toutes les LED de zone allumées (segment 1)
Location 4	`12345678*`	Toutes les LED de zone allumées (segment 2)
Location 4	`12345678*#`	
Location 23	`23#`	Toutes les LED de zone allumées (segment 3)
Location 23	`**`	Toutes les LED de zone allumées (segment 3)
Location 23	`12345678*#`	Toutes les LED de zone allumées (segment 3)
Location 37	`37#`	Toutes les LED de zone allumées (segment 3)
Location 37	`**`	Toutes les LED de zone allumées (segment 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT EXIT`	Sortie de la programmation

5. Pilotage à distance avec l'application Protegus 2

Avec l'application mobile et web Protegus 2, l'utilisateur voit à distance l'état du système, reçoit une notification des événements, peut armer et désarmer et commander les sorties du communicateur. L'application se télécharge pour Android et iOS (Google Play, App Store), ou s'utilise dans un navigateur :

web.protegus.app. Connectez-vous avec votre nom d'utilisateur et votre mot de passe, ou créez un nouveau compte. Le GET n'avertit ni par SMS ni par appel téléphonique, et il n'accepte pas non plus de commandes SMS : le pilotage à distance et la notification passent par l'application ; les réglages du communicateur sont aussi accessibles depuis l'application (**Settings** → **Advanced settings**, chapitre 6).

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez que :

1. La carte SIM est active, et son code PIN est saisi dans l'appareil ou la demande de PIN est désactivée – **ou** le communicateur est raccordé au réseau local par un câble réseau (LAN).
2. Sur la page **User reporting** → **PROTEGUS Cloud** de TrikdisConfig, **Enable connection** est coché (point 6.5).
3. La LED **POWER** est allumée en vert.
4. La LED **NETWORK LTE** est allumée en vert et clignote en jaune (l'appareil est sur le réseau mobile) ; avec une connexion filaire uniquement, c'est la LED **NETWORK LAN** qui est allumée en vert.

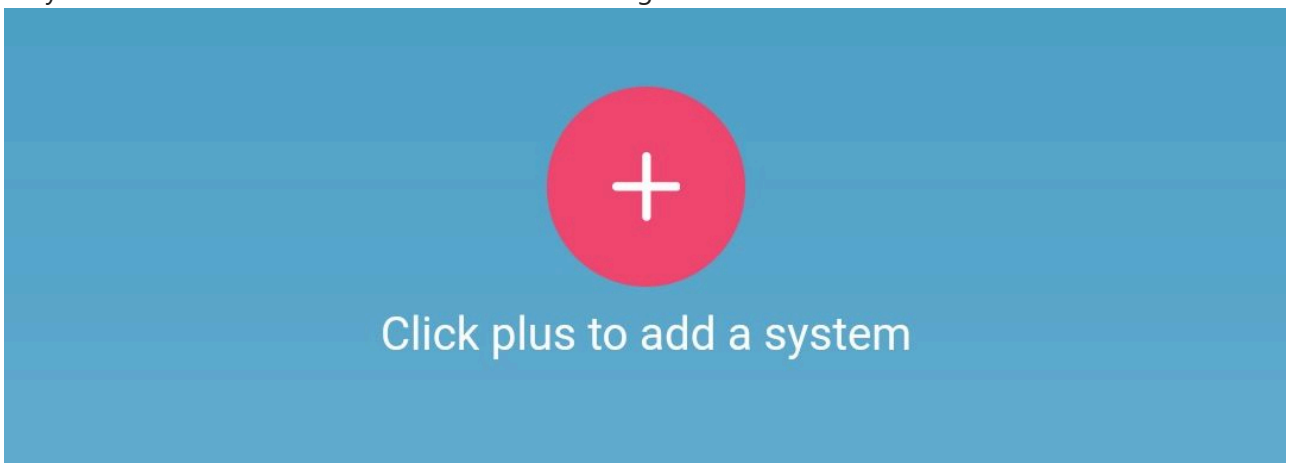
La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur 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



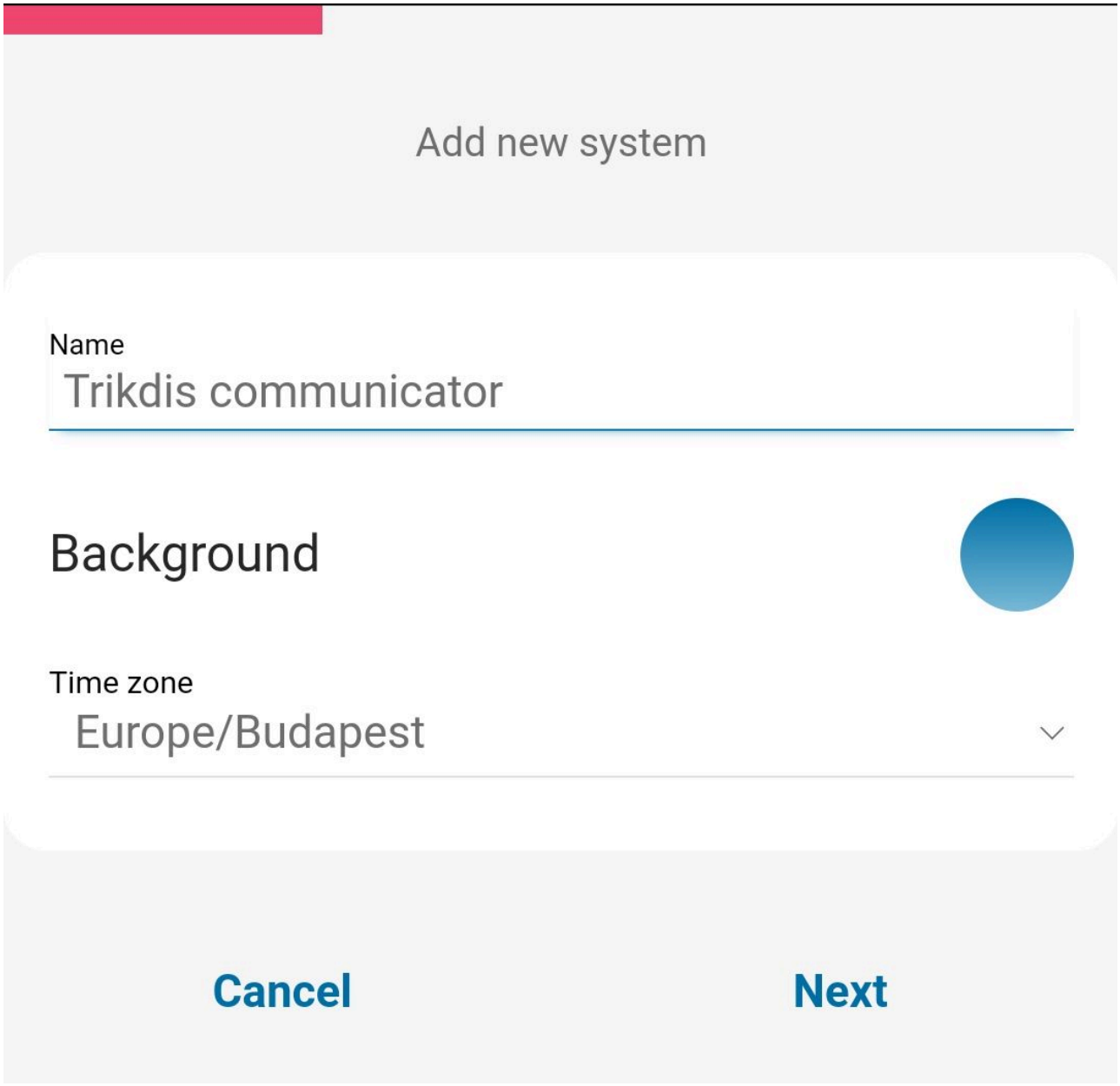
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



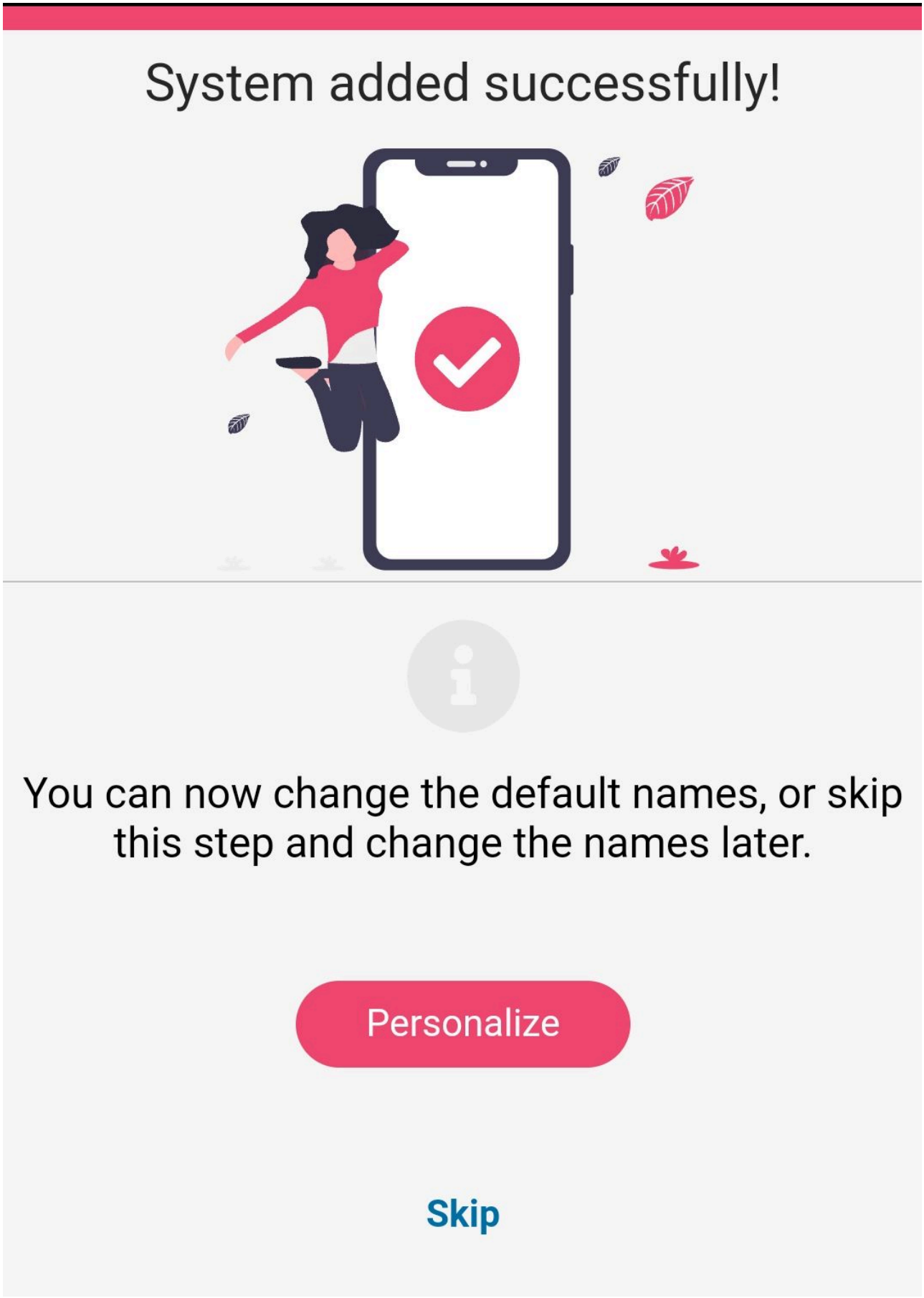
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



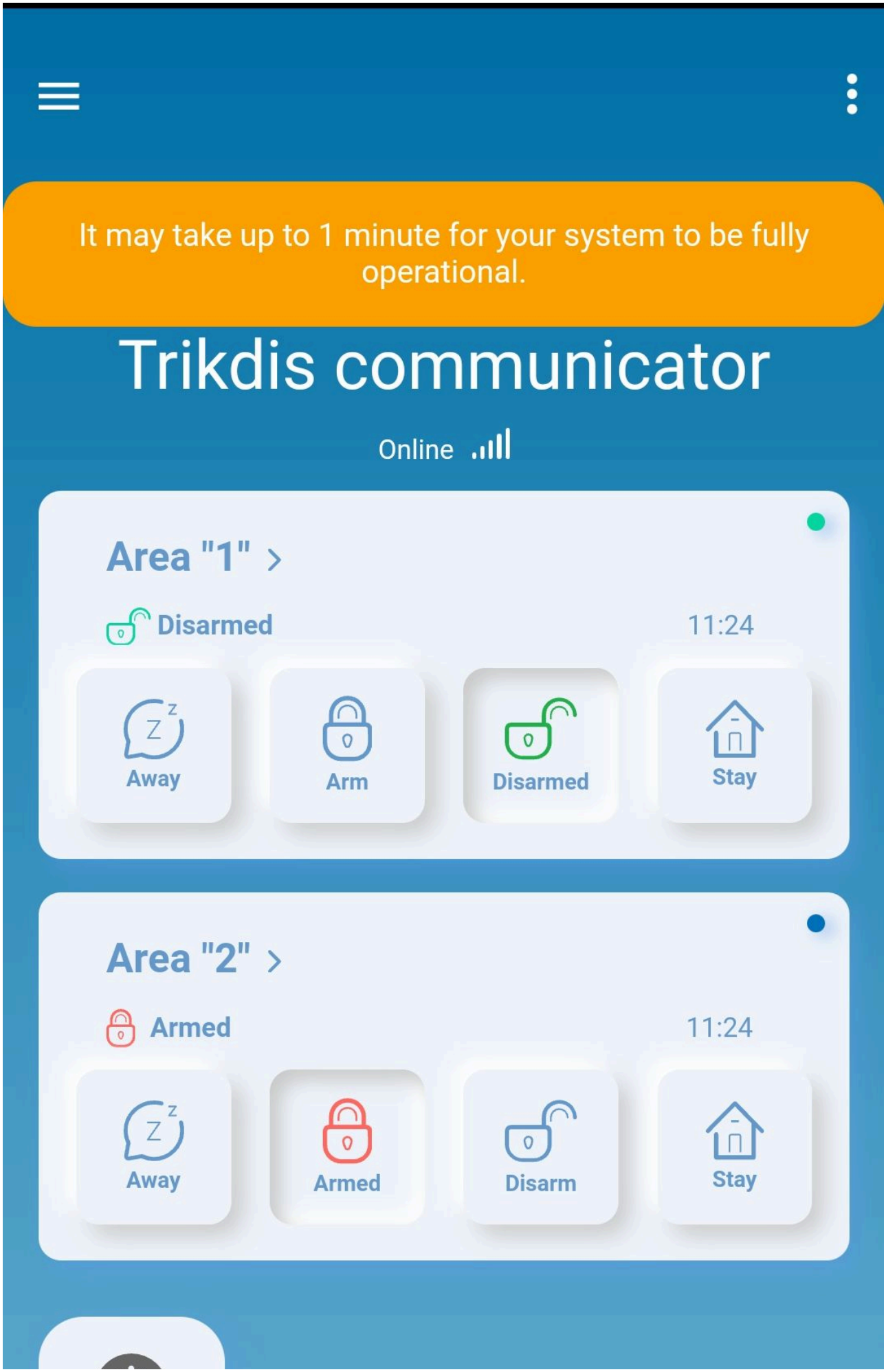
6. Add meg a rendszer nevét és válassz idozónát



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

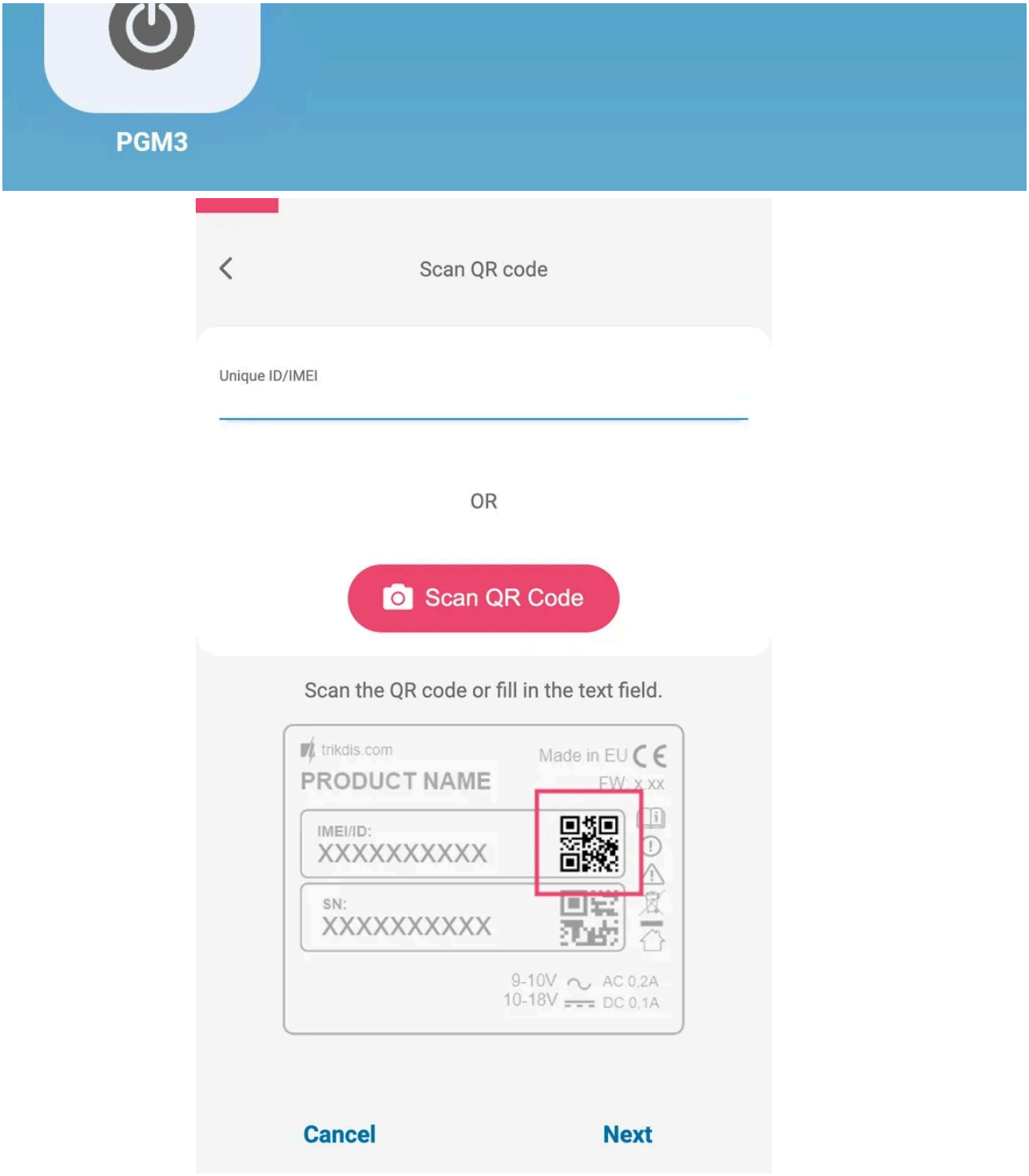


Figure 36. Protegus 2 – ajout d'un nouveau système : saisie de l'IMEI / Unique ID ou lecture du QR code de l'étiquette, puis Next.

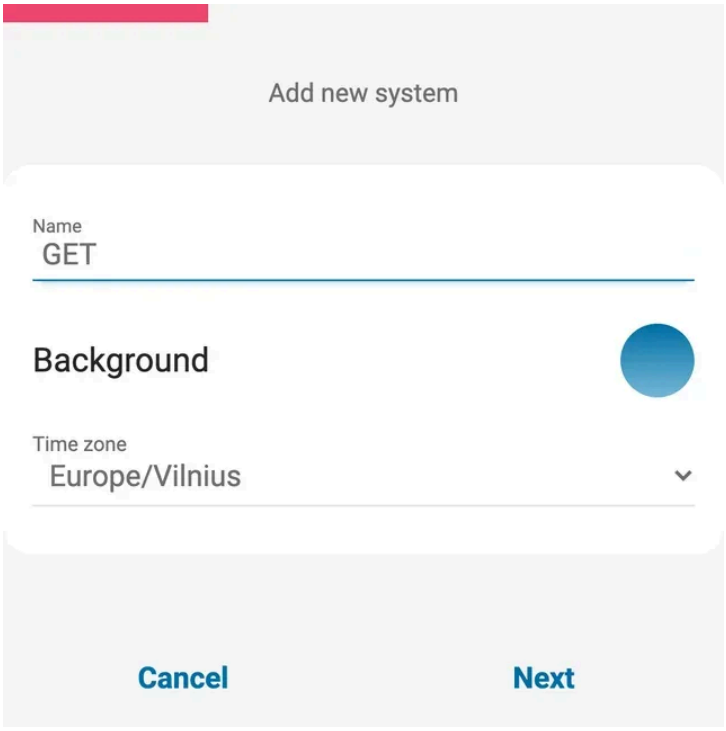


Figure 37. Protegus 2 – saisie du nom du système (Name), puis Next.

L'identifiant unique de l'appareil (**IMEI / Unique ID**) figure sur l'étiquette de l'appareil et sur l'autocollant de la boîte, et la barre d'état de TrikdisConfig l'affiche aussi. Si le **PROTEGUS Cloud access Code** de l'appareil n'est pas celui d'usine, l'application le demande lors de l'ajout.

5.2 Armement et désarmement par une sortie

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.



Figure 38. Protegus 2 – la page « Le système n'est pas piloté à distance » lors de la création du système : le bouton Continue mène au réglage de la partition et de la sortie PGM.

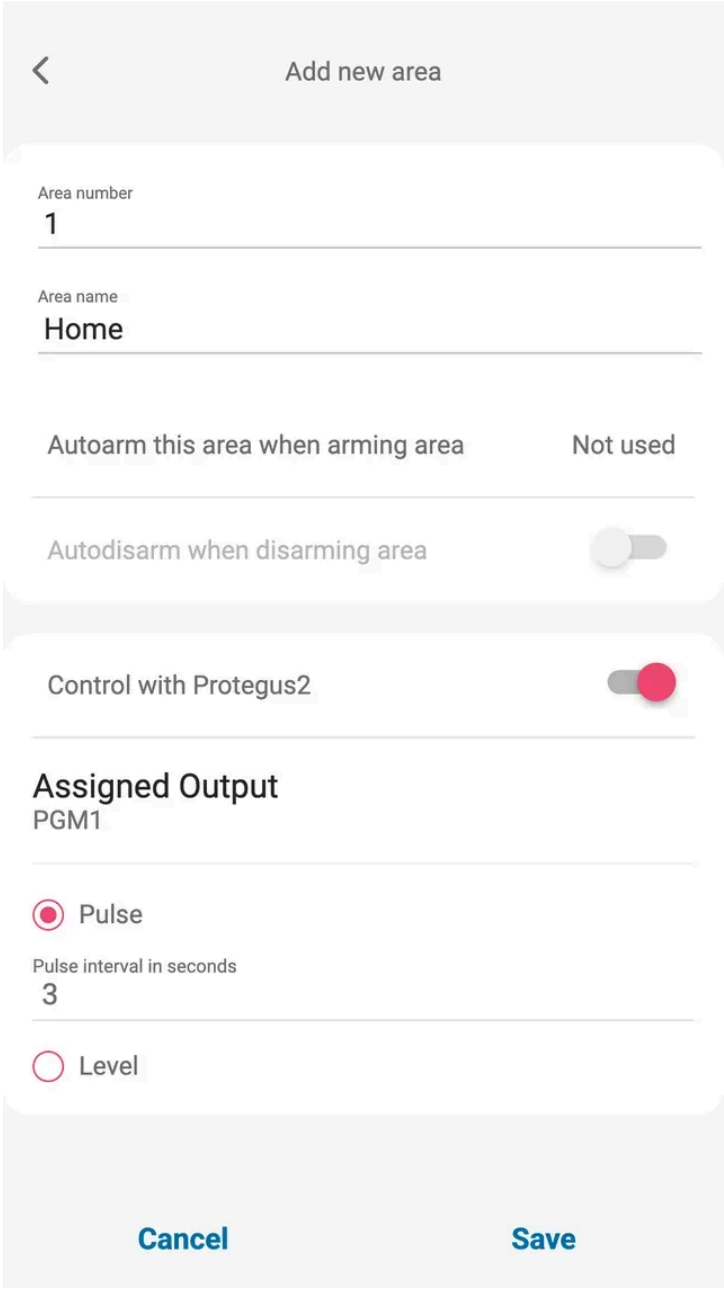


Figure 39. Protegus 2 – ajout d'une partition (Add new area) : Area number, Area name, Control with Protegus2 activé, Assigned Output PGM1, Pulse (3 s) ou Level, puis Save.

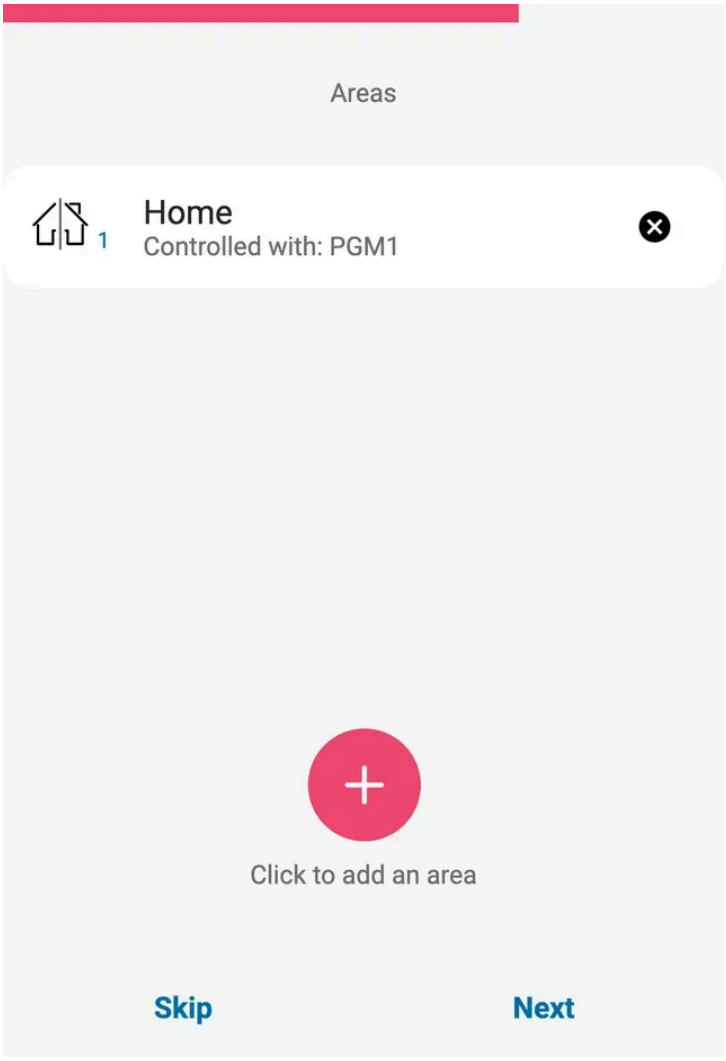


Figure 40. Protegus 2 – la liste des partitions (Areas) : la partition Home est commandée par PGM1 ; une autre partition s'ajoute avec le bouton Click to add an area, l'assistant se ferme avec le bouton Skip.

5.3 Armement et désarmement 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.

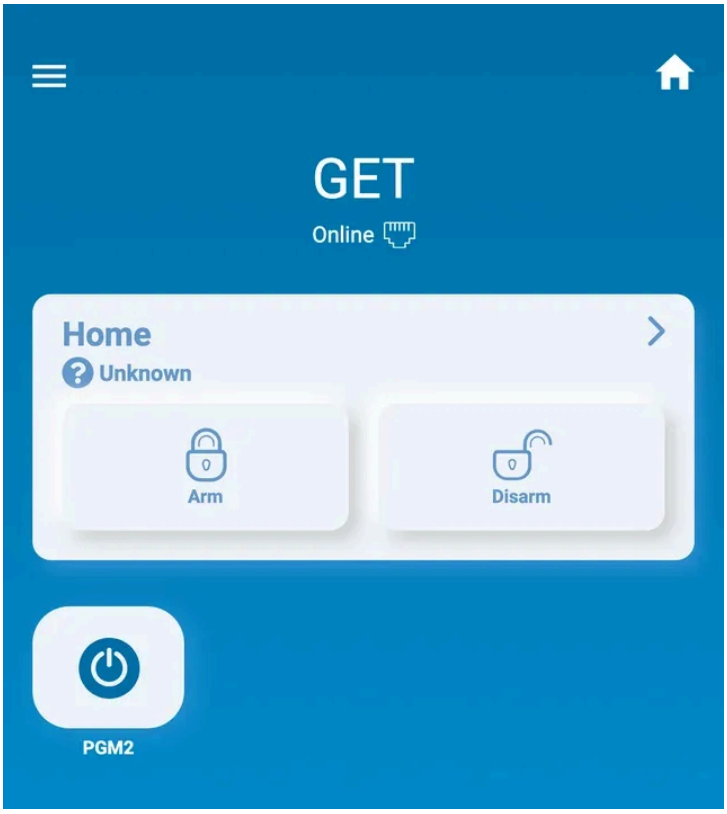


Figure 41. Protegus 2 – l'écran d'accueil du système : l'état de la partition, les boutons Arm et Disarm, et en dessous la sortie PGM commandable.

6. Les réglages en détail

La plupart des réglages du GET sont accessibles à la fois dans le logiciel **TrikdisConfig** sous Windows et dans l'application **Protegus 2** (**Settings** → **Advanced settings**, point 2.2) ; lorsqu'un réglage n'existe que dans l'un des deux, nous le signalons. Chaque réglage n'est décrit qu'une fois, et nous indiquons pour chaque point où le trouver dans les deux outils ; entre parenthèses figure le libellé de l'application lorsqu'il diffère de celui de TrikdisConfig. À gauche de la fenêtre TrikdisConfig se trouve la liste des pages (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), en haut la barre de boutons (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), en bas la barre d'état.

6.1 Connexion au communicateur

Application Protegus 2. Ouvrez le système et allez dans le menu **Settings** → **Advanced settings**. En haut de chaque écran apparaissent les données de l'appareil connecté : **Unique ID** (IMEI), **Serial** (numéro de série), version **Firmware** et **Boot**. Les groupes de réglages du menu sont : **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** et **System events**. Après une modification, le bouton **Write** écrit les réglages dans l'appareil ; **Read** relit les valeurs actuelles dans l'appareil.

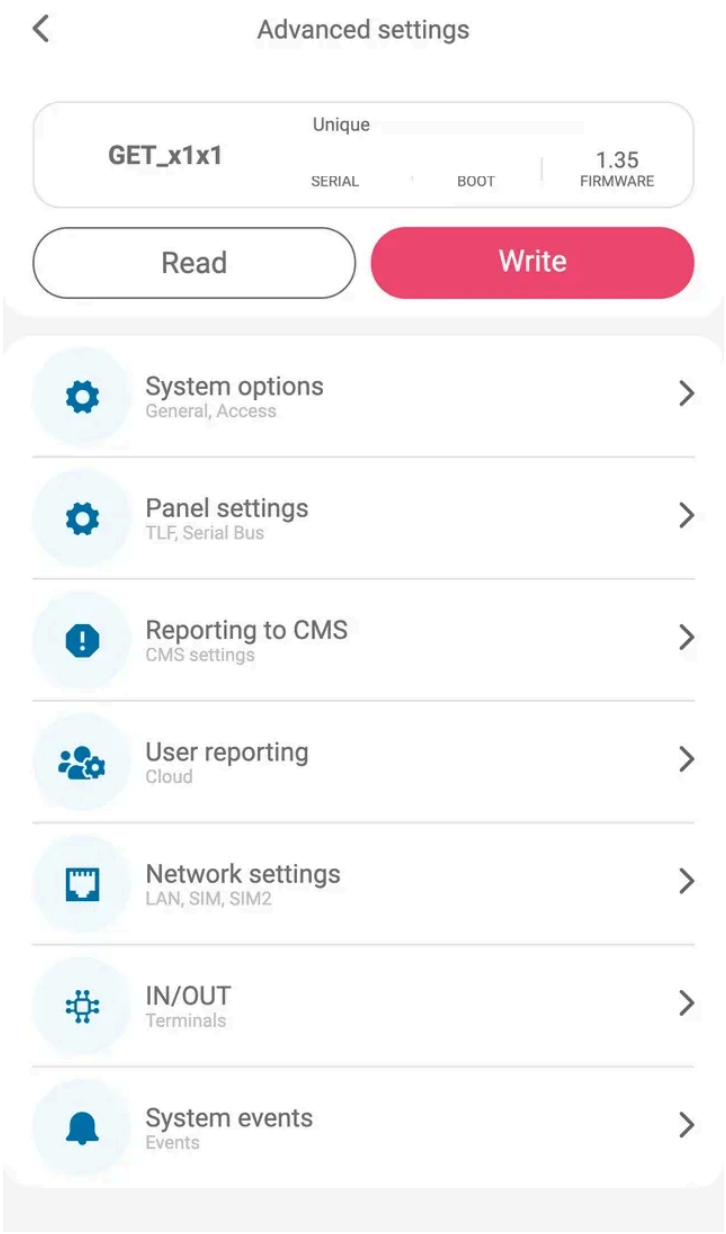


Figure 42. Protegus 2 – menu Advanced settings : en haut les données de l'appareil (type, Unique ID, numéro de série, versions boot et firmware), les boutons Read et Write, en dessous les groupes de réglages.

TrikdisConfig. Après avoir connecté le communicateur et appuyé sur **Read [F4]**, le logiciel affiche les données de l'appareil dans 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.

Libellé	Signification
Device	Type de l'appareil (référence). Vérifiez que c'est bien le type de votre appareil qui figure ici.
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.



Figure 43. La barre d'état de TrikdisConfig avec un GET lu : identifiant, état, type (Device : GET_S170), numéro de série, versions BL (bootloader), FW et HW, mode de connexion et niveau d'accès.

Le champ **Device** doit afficher une référence GET (sur l'image, GET_S170 ; le suffixe lettres-chiffres désigne la version matérielle), **BL** est la version du bootloader. Après **Read [F4]**, le logiciel lit et affiche les valeurs réglées dans l'appareil ; effectuez les réglages nécessaires selon les descriptions des pages ci-dessous.

6.2 System settings (System options)

Dans l'application : Advanced settings → System options → System general (identifiants, synchronisation de l'heure) et **System options → Access** (codes et droits de l'installateur). L'emplacement de l'**Account No.** et du **Device account No.** dépend de la version matérielle et du firmware : sur le matériel **x1x1**, avec le firmware **1.31** ou plus récent, vous les trouvez dans la page **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.** ; sur le canal parallèle **Parallel Account no.**) et dans la page **Reporting to CMS → Settings** (**Device account No.**), la page System general ne gardant que **Time set** ; sinon, les deux se trouvent dans la page System general.

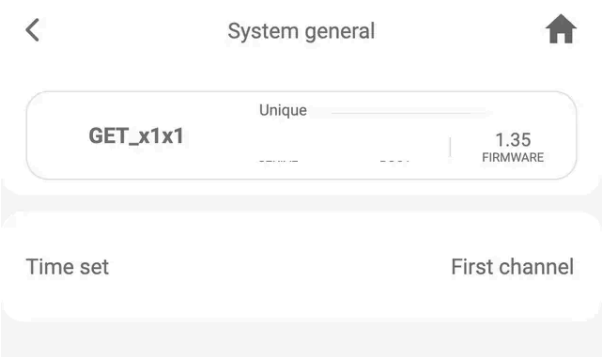


Figure 44. Protegus 2 – System options → System general sur le matériel x1x1 (firmware 1.35) : seul Time set est visible, les identifiants se trouvent parmi les réglages CMS.

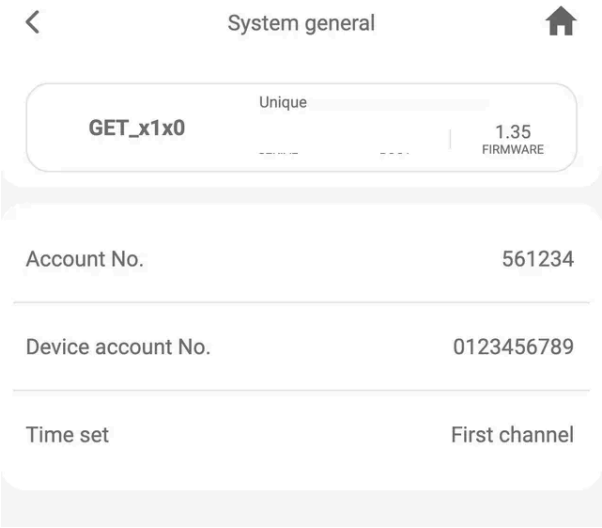


Figure 45. Protegus 2 – System options → System general sur le matériel x1x0 : Account No., Device account No. et Time set.

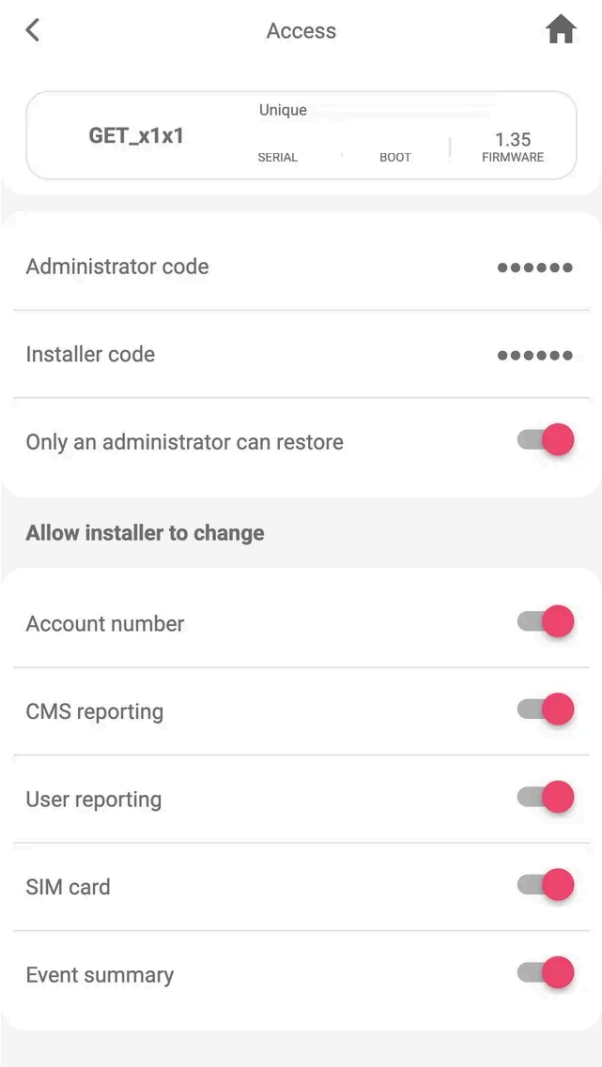


Figure 46. Protegus 2 – System options → Access : Administrator code, Installer code, Only an administrator can restore, et la liste Allow installer to change (Account number, CMS reporting, User reporting, SIM card, Event summary).

Dans TrikdisConfig : la page **System settings** comporte deux groupes : dans le groupe **General**, vous réglez les identifiants de l'appareil, dans le groupe **Access**, les niveaux d'accès.

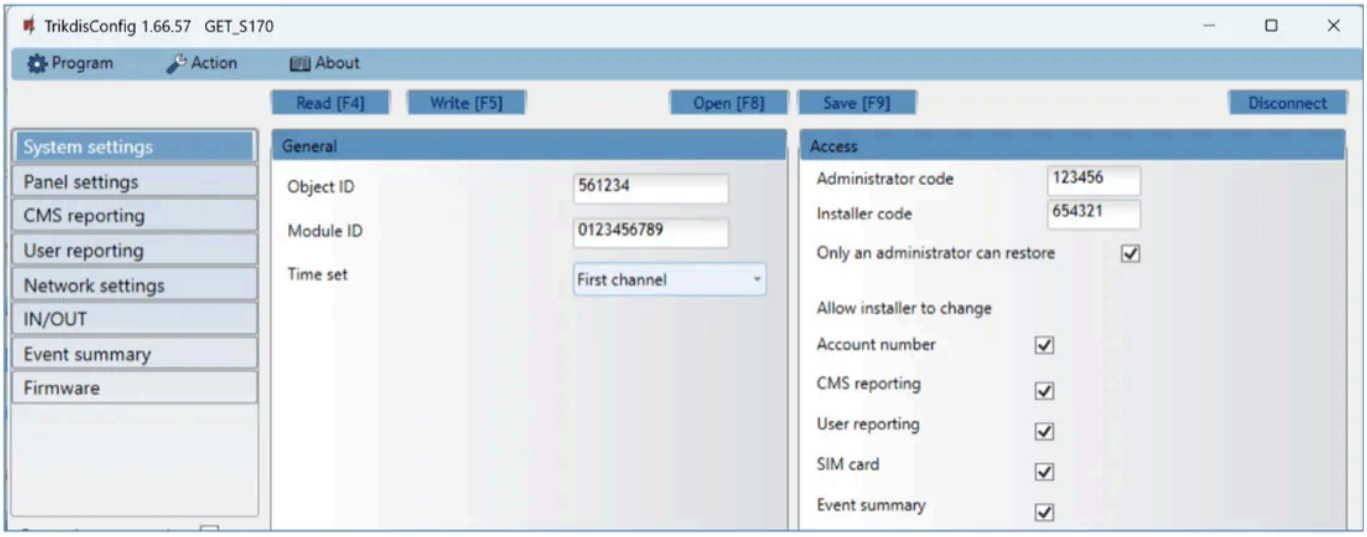


Figure 47. TrikdisConfig – page System settings : groupe General (Object ID, Module ID, Time set) et groupe Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – le numéro d'abonné reçu du centre de télésurveillance (6 caractères hexadécimaux : 0–9, A–F ; `FFFE` et `FFFF` ne peuvent pas être utilisés). Obligatoire si l'appareil transmet aussi vers un centre de télésurveillance.
- **Module ID** (Device account No.) – le numéro d'identification du module.
- **Time set** – le serveur sur lequel l'appareil synchronise son horloge.

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.

Connexion de l'installateur dans l'application. Si vous ouvrez le communicateur avec le code installateur, Protegus 2 masque les champs **Administrator code** et **Only an administrator can restore**, et affiche en lecture seule les réglages que l'administrateur n'a pas autorisés. Dans l'application, le droit **SIM card** s'applique aussi aux réglages LAN ; lorsque les identifiants se trouvent parmi les réglages CMS (voir ci-dessus), c'est le droit **CMS reporting** qui s'y applique.

6.3 Panel settings

Sur cette page, vous indiquez comment le communicateur est raccordé à la centrale d'alarme : le groupe **TLC** (dans l'application **TLF**) contient les réglages du raccordement par ligne téléphonique (TIP/RING), le groupe **Serial bus** (**Serial Bus**) ceux du raccordement au bus de données ou au port série. Dans l'application : **Advanced settings** → **Panel settings** → **TLF**, ou **Panel settings** → **Serial Bus**.

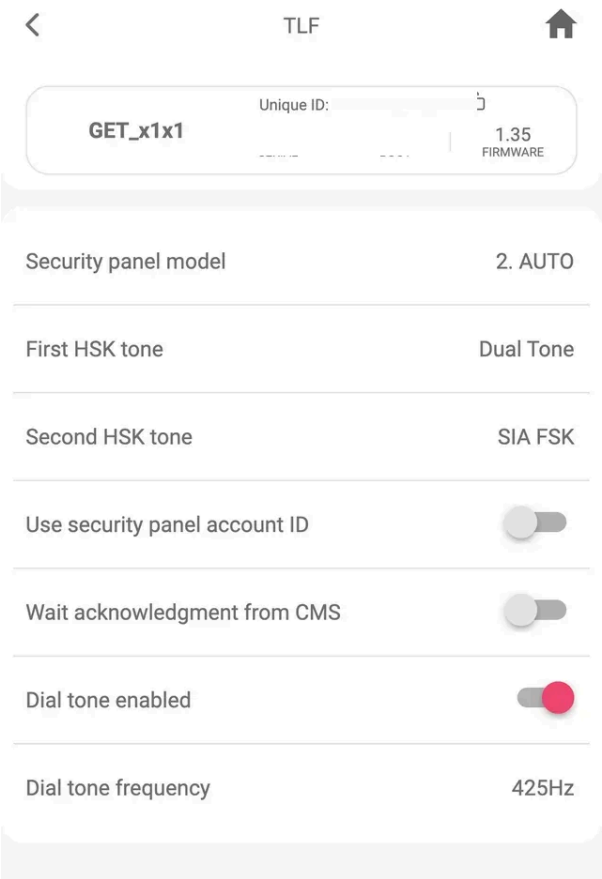


Figure 48. Protegus 2 – Panel settings → TLF : Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.

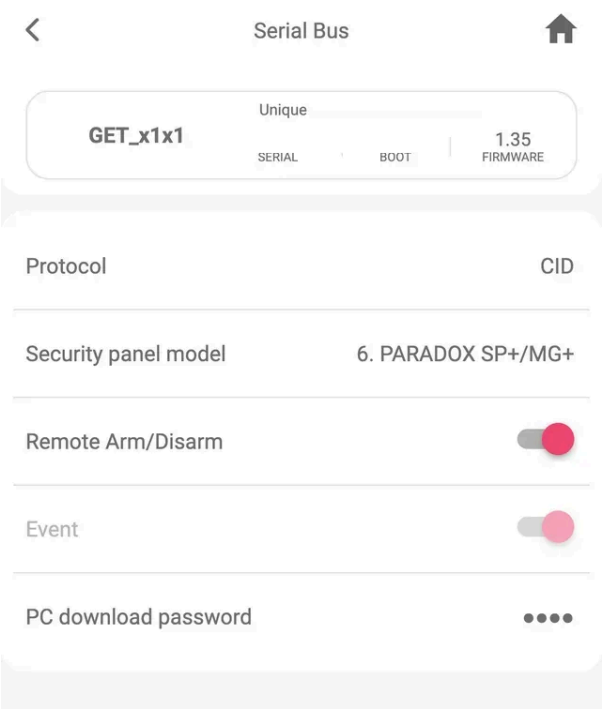


Figure 49. Protegus 2 – Panel settings → Serial Bus : Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm activé, Event (lecture seule), PC download password.

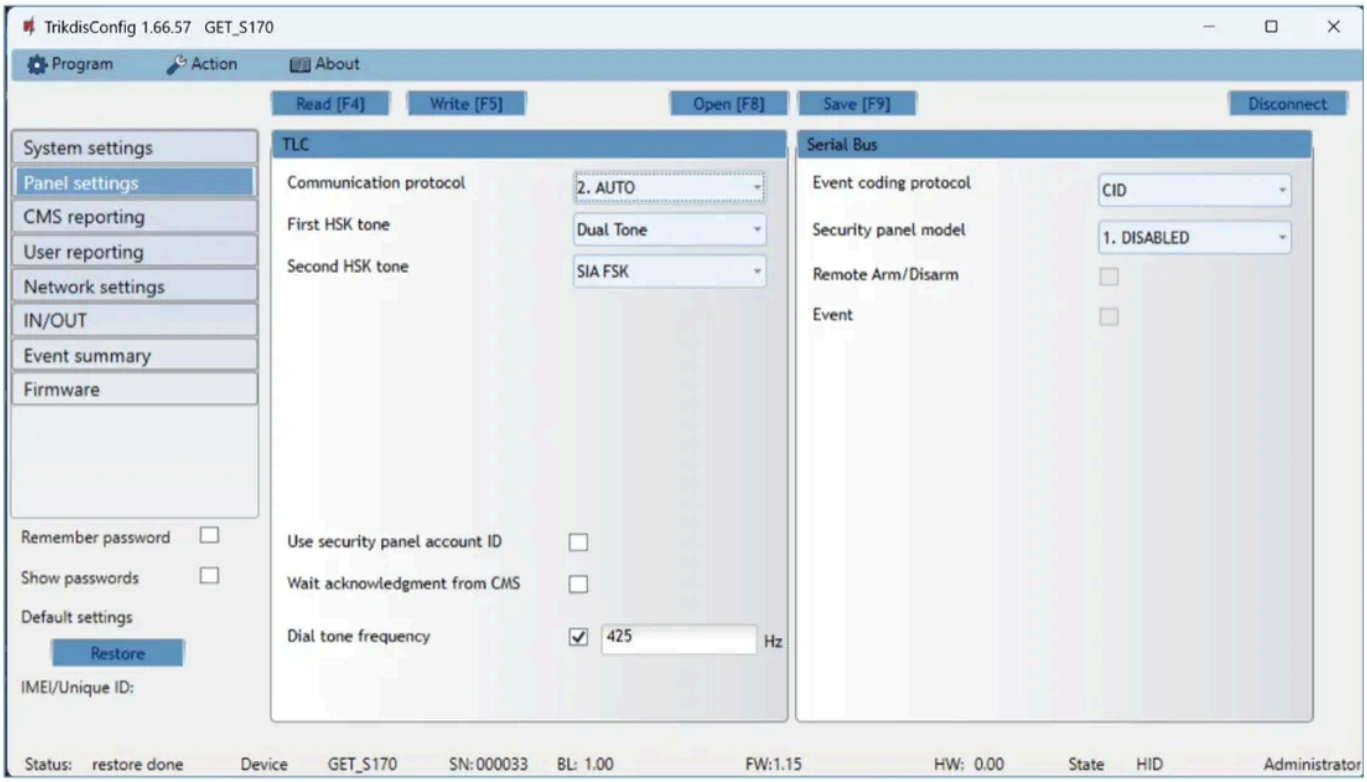


Figure 50. TrikdisConfig – Panel settings pour un raccordement TIP/RING : dans le groupe TLC, Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz ; le groupe Serial bus est alors grisé.

Groupe TLC – si le communicateur est raccordé aux bornes TIP/RING du transmetteur téléphonique de la centrale :

- **Communication protocol** (Security panel model) – activation (**2. AUTO**) ou désactivation (**1. DISABLED**) de l'interface ligne téléphonique DTMF du communicateur. Pour un raccordement TIP/RING, choisissez la valeur AUTO.
- **First HSK tone**, **Second HSK tone** – la tonalité de prise de contact (handshake) de la centrale, par laquelle le communicateur répond au transmetteur de la centrale (sur l'image, Dual Tone et SIA FSK).
- **Use security panel account ID** – coché, le communicateur n'envoie pas la valeur de son propre champ **Object ID**, mais le numéro d'abonné réglé dans la centrale et envoyé par celle-ci.
- **Wait acknowledgment from CMS** – coché, le communicateur attend, après l'envoi de chaque événement, l'acquittement du récepteur IP confirmant que le message est arrivé ; si l'acquittement n'arrive pas, il ne donne pas le signal « kiss-off » à la centrale, et le transmetteur téléphonique de la centrale répète le message.
- **Dial tone frequency** – la fréquence de la tonalité par laquelle le communicateur communique avec le transmetteur de la centrale (par défaut 425 Hz, la tonalité standard dans la plupart des pays européens). Dans la page TLF de l'application se trouve en plus l'interrupteur **Dial tone enabled** : il active ou désactive la tonalité ; la fréquence ne peut être modifiée que si la tonalité est activée.

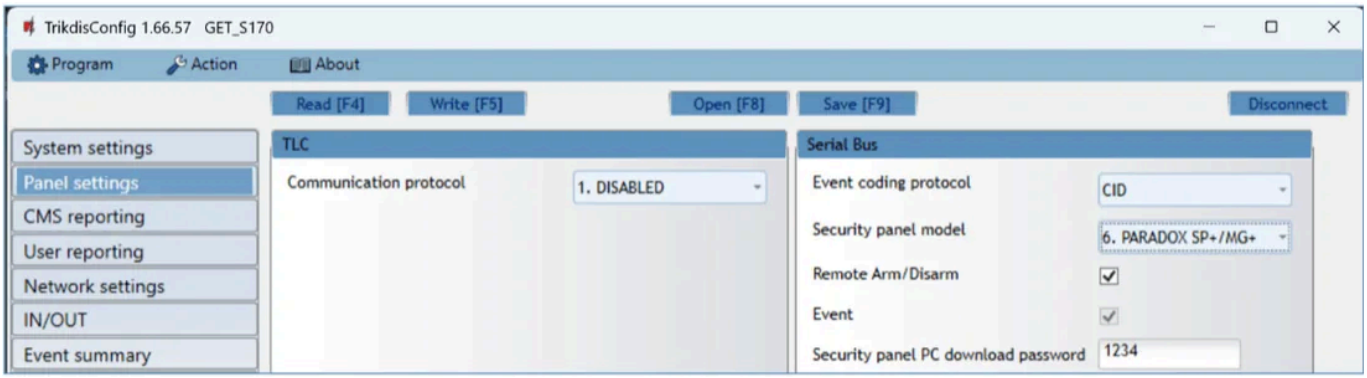


Figure 51. TrikdisConfig – Panel settings pour un raccordement au bus de données ou au port série : Communication protocol 1. DISABLED ; dans le groupe Serial bus, Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm et Event cochés, Security panel PC download password saisi.

Groupe Serial bus – si le communicateur est raccordé au bus de données ou au port série de la centrale :

- **Event coding protocol** (Protocol) – le protocole de transmission des événements : **CID** ou **SIA**.
- **Security panel model** – le modèle de la centrale d'alarme raccordée, choisi dans la liste (pour le raccordement Keybus + TIP/RING des centrales Paradox SP / SP+ / MG / MG+, choisissez l'élément **Paradox SP+/MG+ series KeyBus**, point 3.3.3).
- **Remote Arm/Disarm** – coché, le communicateur pilote directement la centrale (armement et désarmement depuis Protegus 2). Visible uniquement pour les centrales pilotables directement. Pour le pilotage direct, la centrale doit aussi être configurée selon le point 4.1.
- **Event** – coché, le communicateur envoie les événements de la centrale au centre de télésurveillance et à Protegus 2. L'application affiche cet interrupteur, mais il n'y est pas modifiable.
- **Security panel PC download password** (PC download password ; pour Texecom, l'UDL passcode) – pour le pilotage direct d'une centrale Paradox ou Texecom, le mot de passe PC ou UDL ; il doit être identique au mot de passe réglé dans la centrale, dont la saisie est décrite au point 4.1.

6.4 CMS reporting (Reporting to CMS)

Le communicateur envoie les événements au centre de télésurveillance par liaison IP – par le réseau filaire (LAN) ou le réseau mobile (SIM1, SIM2), dans l'ordre réglé au point 6.4.2. Les événements peuvent passer par plusieurs canaux : le canal **principal** et le canal **parallèle** fonctionnent en même temps (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. Les protocoles TRK nécessitent un récepteur Trikdis, qui reçoit les événements et les transmet au logiciel de télésurveillance : pour une liaison IP, le récepteur logiciel IPcom (Windows ou Linux), le récepteur IP/SMS RL14 ou le récepteur multicanal RM14 ; les protocoles DC-09 et TL150 sont destinés respectivement aux récepteurs universels et aux récepteurs SUR-GARD (voir ci-dessous, **Protocol**).

6.4.1 Canaux de réception (CMS settings)

Dans l'application : Advanced settings → Reporting to CMS → CMS settings, puis **Primary channel**, **Backup channel** ou **Parallel channel** (et, à l'intérieur, **Parallel primary channel** et **Parallel backup channel**). Les réglages du canal apparaissent lorsque vous activez l'interrupteur **Enabled**.

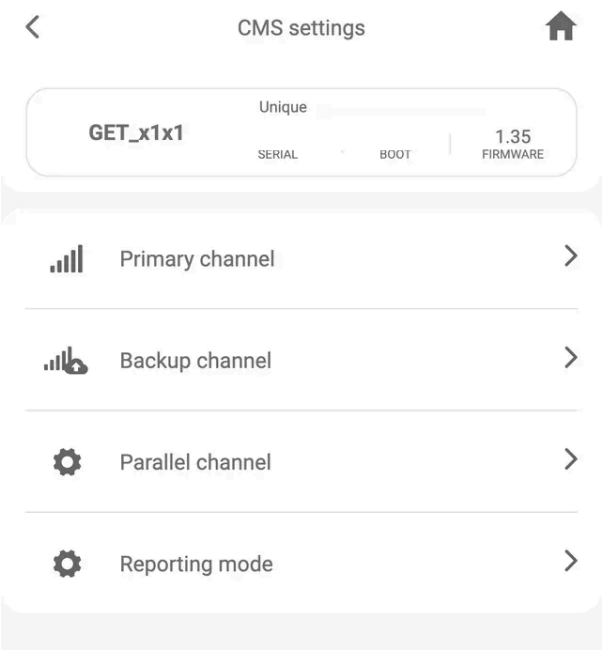


Figure 52. Protegus 2 – Reporting to CMS → CMS settings : Primary channel, Backup channel, Parallel channel et Reporting mode.

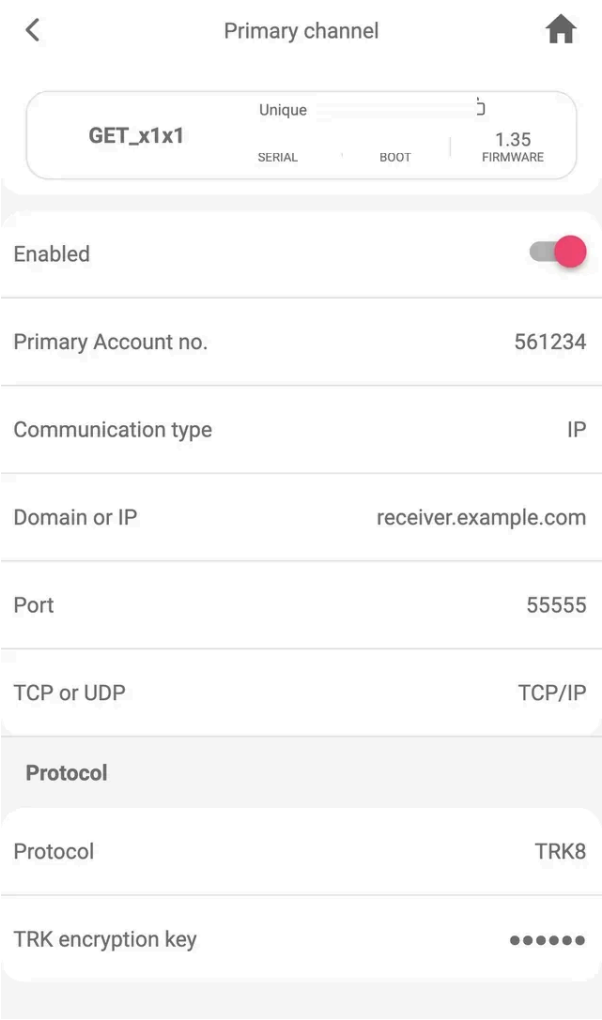


Figure 53. Protegus 2 – Primary channel sur le matériel x1x1 : Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 et la TRK encryption key.

Dans TrikdisConfig : l'onglet **CMS settings** de la page **CMS reporting**.

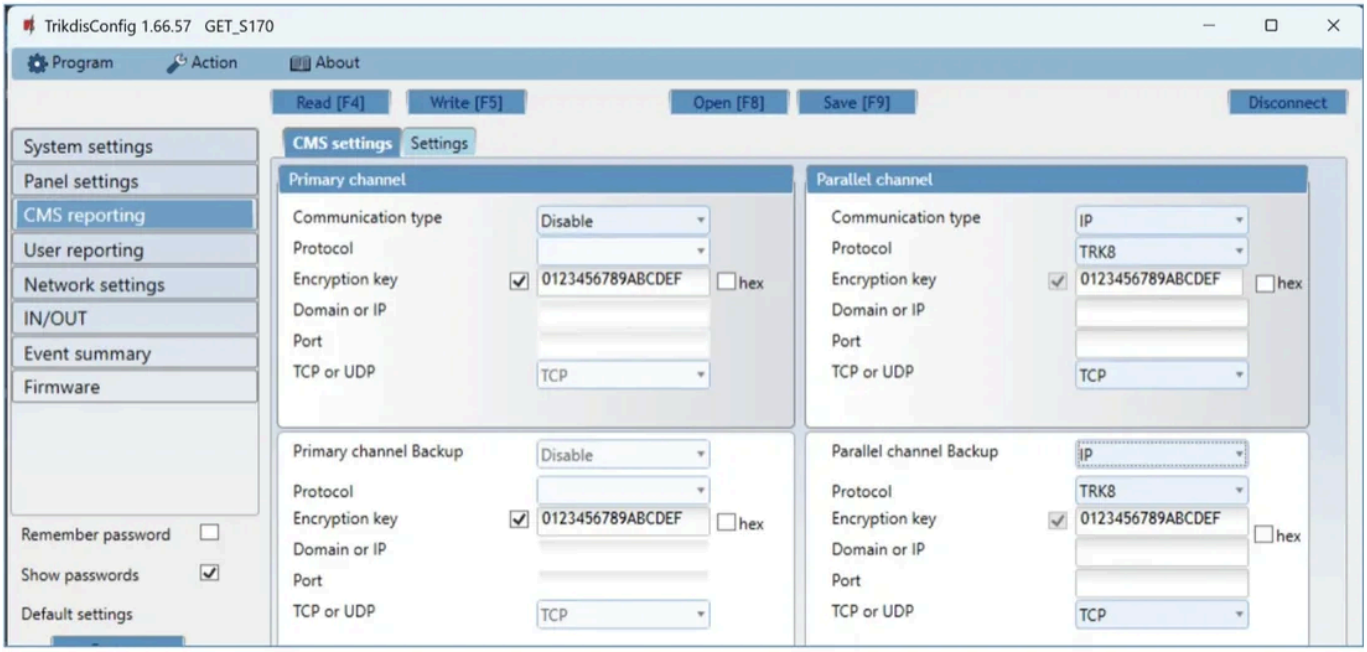


Figure 54. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal et son canal de secours, canal parallèle et son canal de secours (sur l'image, le canal parallèle avec le réglage IP / TRK8 / TCP).

Primary channel – canal principal

- **Communication type** – le mode de connexion avec le récepteur : **IP**.
- **Protocol** – **TRK8** (récepteurs Trikdis), **DC-09_2007** ou **DC-09_2012** (récepteurs universels), **TL150** (récepteurs SUR-GARD).
- **Encryption key** (TRK encryption key ; pour les protocoles DC-09, **Enable encryption key** et **DC-09 encryption key**, avec l'interrupteur **HEX** pour une clé hexadécimale) – la clé de chiffrement des messages ; elle doit être identique dans le communicateur et dans le récepteur. Dans l'application, la TRK encryption key comporte au maximum 6 caractères, la DC-09 encryption key au maximum 16 (32 en HEX).
- **Domain or IP**, **Port** – le nom de domaine ou l'adresse IP du récepteur et son port réseau.
- **TCP or UDP** – le protocole de transport.

Primary channel Backup – canal de secours. Activé, 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 en même temps vers un second récepteur (par exemple le centre de télésurveillance local et le centre de télésurveillance central). Ses réglages sont les mêmes que ceux du canal principal.

6.4.2 Test, PING et ordre des connexions

Dans l'application : Advanced settings → Reporting to CMS → Settings (test, PING, temporisations du canal de secours, numéros de récepteur et de ligne) et **Reporting to CMS → CMS settings → Reporting mode** (ordre des voies de connexion). Dans l'application, chaque intervalle a son interrupteur : **Enable test** pour Test period, **Enable ping** pour IP ping period et **Test enabled** pour Communication path test ; dans la page Reporting mode, les types de connexion s'appellent **LAN**, **SIM** (la SIM1) et **SIM2**.

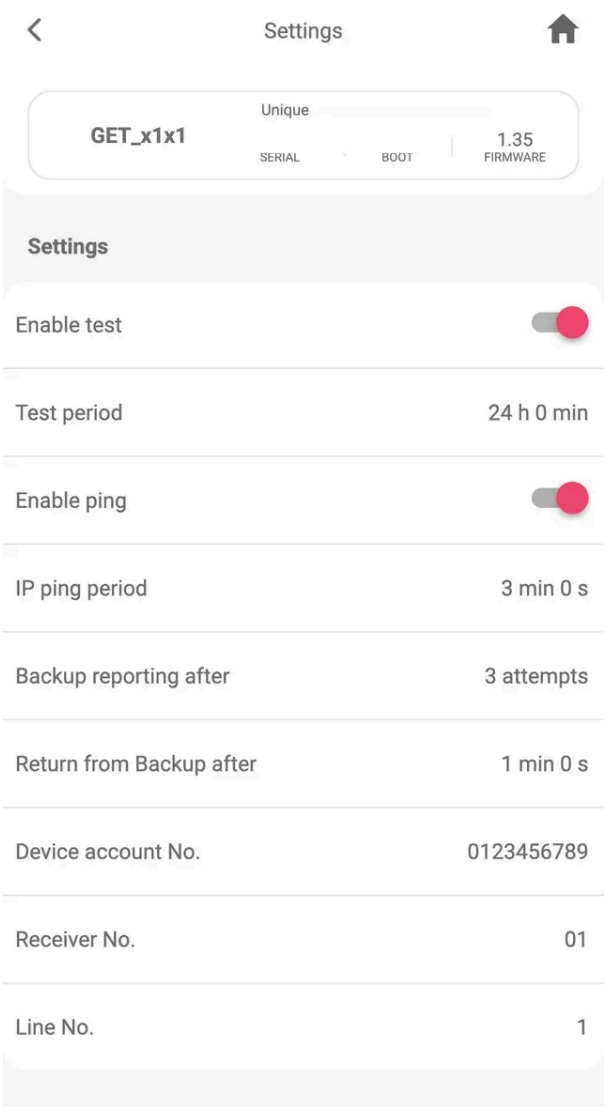


Figure 55. Protegus 2 – Reporting to CMS → Settings sur le matériel x1x1 : Enable test et Test period, Enable ping et IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.

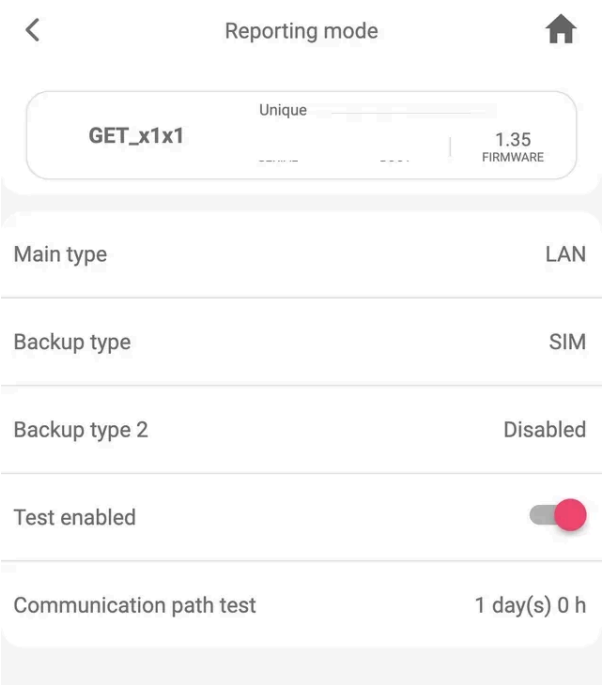


Figure 56. Protegus 2 – CMS settings → Reporting mode : Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled et Communication path test.

Dans TrikdisConfig : l'onglet **Settings** de la page **CMS reporting**.

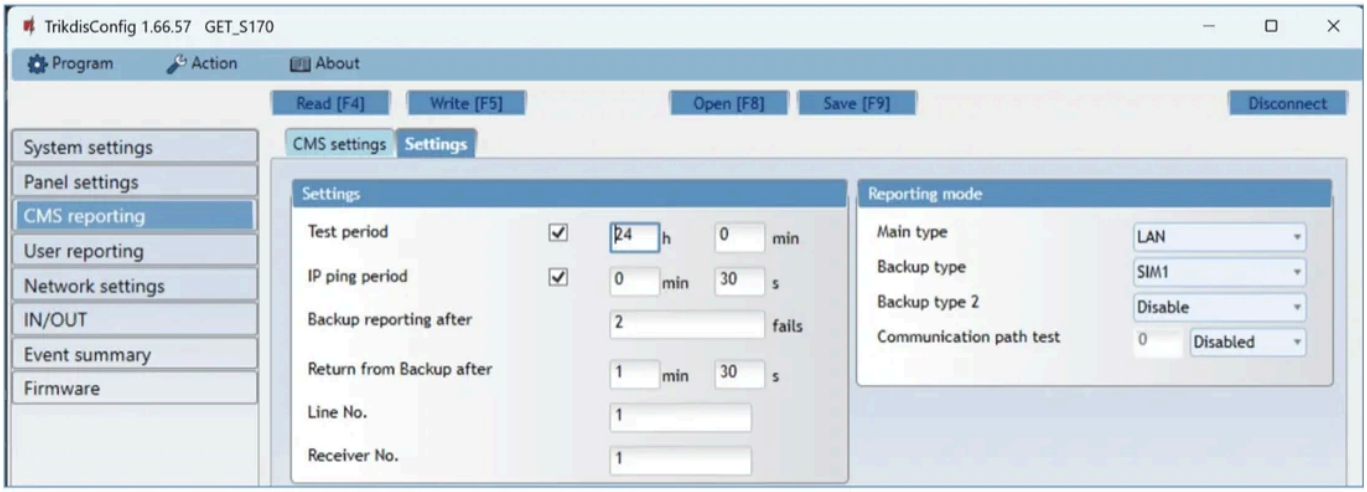


Figure 57. TrikdisConfig – CMS reporting, onglet Settings : Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No. ; dans le groupe Reporting mode, Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **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.

Dans l'onglet Settings du GET se trouvent aussi les champs **Line No.** (numéro de ligne du récepteur) et **Receiver No.** (numéro de récepteur) ; le GET n'a pas de champ séparé « Object ID in DC-09 ».

Groupe Reporting mode – vous indiquez ici par quelle voie le communicateur communique avec les canaux de télésurveillance et avec Protegus 2. Vous indiquez les types de connexion dans l'ordre : si la connexion selon **Main type** ne s'établit pas, le communicateur bascule sur celle selon **Backup type**, et ainsi de suite ; si le message a pu être envoyé par la voie de secours, il retente la voie principale une fois le délai réglé (Return from backup after) écoulé.

- **Main type** – le type de la connexion principale avec le récepteur et Protegus 2 : **LAN**, **SIM1** ou **SIM2**.
- **Backup type** – le type de la connexion de secours (LAN, SIM1, SIM2).
- **Backup type 2** – le type de la deuxième connexion de secours (LAN, SIM1, SIM2).
- **Communication path test** – l'intervalle auquel le communicateur teste les types de connexion choisis (LAN, SIM1, SIM2).

6.5 User reporting (Protegus Cloud)

Avec le service Protegus 2, l'utilisateur surveille et pilote à distance le communicateur et le système qui y est raccordé ; détails : web.protegus.app. Dans l'application : **Advanced settings** → **User reporting** → **Cloud** ; dans TrikdisConfig, l'onglet **PROTEGUS Cloud** de la page **User reporting**.

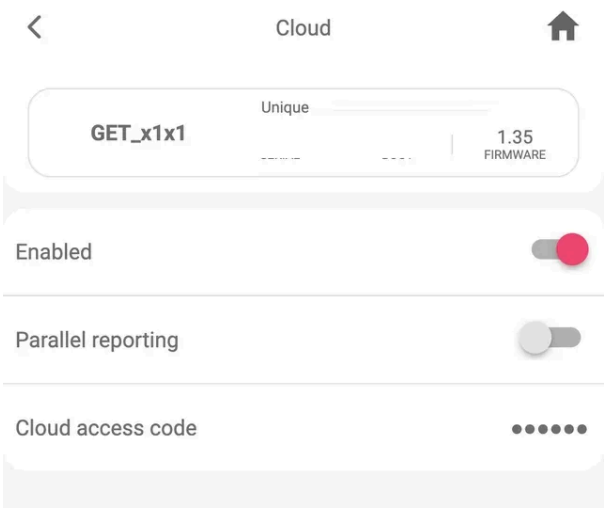


Figure 58. Protegus 2 – User reporting → Cloud : Enabled, Parallel reporting, Cloud access code.

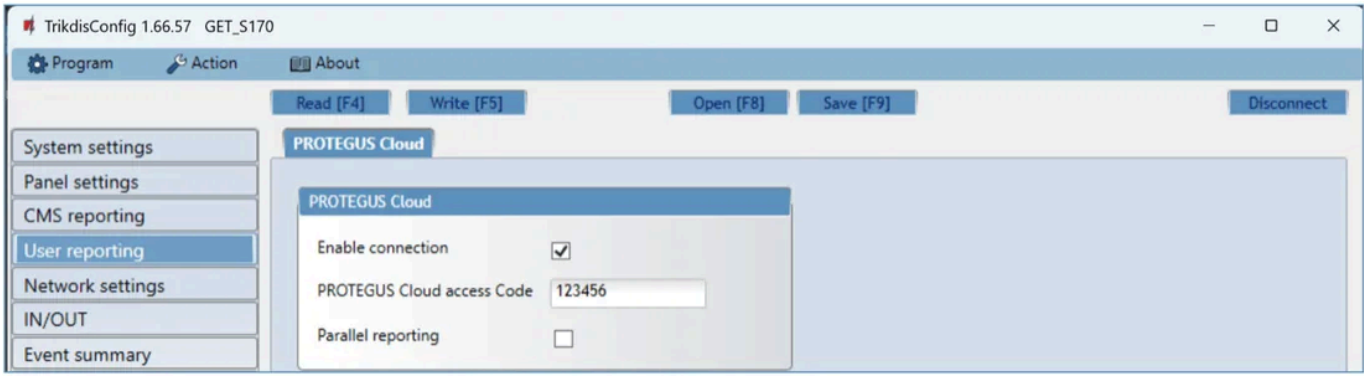


Figure 59. TrikdisConfig – User reporting, onglet PROTEGUS Cloud : Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – active le service Protegus 2 : l'appareil échange des données avec l'application Protegus 2, et TrikdisConfig peut aussi y accéder à distance.
- **PROTEGUS Cloud access Code** (Cloud access code) – code à 6 chiffres pour la connexion à Protegus 2 (d'usine `123456`). Si vous le modifiez dans TrikdisConfig, il faut aussi le changer dans l'application Protegus 2.
- **Parallel reporting** (visible dans l'application uniquement si le firmware le prend en charge) – coché, les messages partent en même temps sur le canal principal (vers le centre de télésurveillance) et vers Protegus 2 ; Protegus 2 et les utilisateurs ne reçoivent le message qu'après son envoi au centre de télésurveillance.

6.6 Network settings

6.6.1 LAN (Ethernet)

Ces réglages sont nécessaires si le communicateur est raccordé au réseau local filaire (LAN). Dans l'application : **Advanced settings → Network settings → LAN** ; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** et **DNS2** ne sont modifiables que si **Use DHCP** est désactivé. Dans TrikdisConfig, l'onglet **LAN** de la page **Network settings**, groupe **Ethernet settings**.

De quoi le réseau a-t-il besoin ? Le communicateur établit lui-même la connexion sortante vers le récepteur de télésurveillance et le cloud Protegus ; il n'est donc **pas nécessaire d'ouvrir ni de rediriger un port** sur le routeur, et ni adresse IP publique fixe ni DNS dynamique ne sont requis. Il faut :

- un port Ethernet libre sur le routeur ou le switch ;
- le DHCP (réglage d'usine), ou une adresse IP fixe, un masque de sous-réseau, une passerelle et un DNS fournis par l'administrateur réseau ;
- l'autorisation du trafic sortant vers l'adresse et le port du récepteur (TCP ou UDP, selon le réglage du récepteur), ainsi que vers le cloud Protegus.

Sur un réseau filtré – d'entreprise ou d'établissement –, convenez-en au préalable avec l'administrateur réseau : sur les routeurs domestiques, toutes les connexions sortantes sont autorisées par défaut, mais sur un réseau protégé par un pare-feu, une règle spécifique peut être nécessaire.

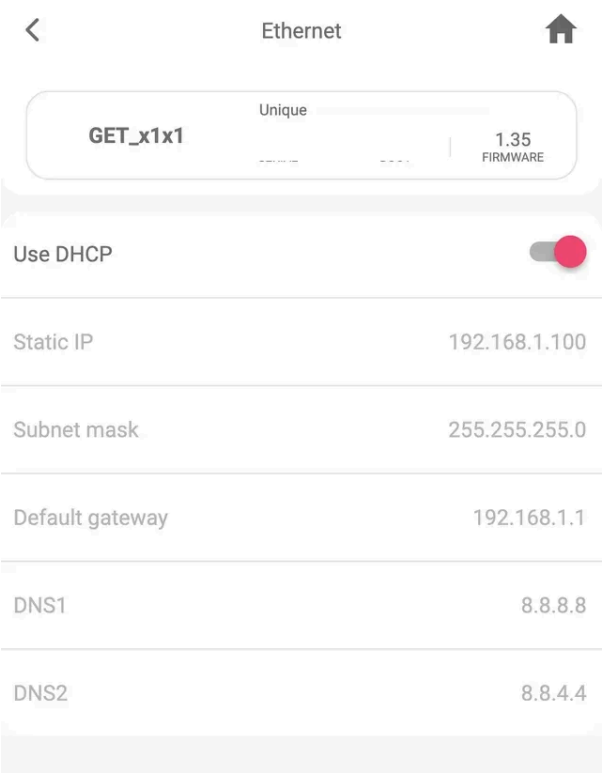


Figure 60. Protegus 2 – Network settings → LAN : Use DHCP activé ; les champs Static IP, Subnet mask, Default gateway, DNS1 et DNS2 sont alors grisés.



Figure 61. TrikdisConfig – Network settings, onglet LAN, groupe Ethernet settings : Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

- **Use DHCP** – coché, le communicateur se connecte automatiquement au réseau (il reçoit une adresse du serveur DHCP du routeur). Si la connexion automatique échoue, les adresses doivent être saisies manuellement :
- **Static IP** – l'adresse IP fixe du communicateur en réglage manuel.
- **Subnet mask** – masque de sous-réseau en réglage manuel.
- **Default gateway** – l'adresse de la passerelle (routeur) en réglage manuel.
- **DNS1, DNS2** – serveurs de noms (DNS, Domain Name System : il fournit l'adresse IP correspondant à un nom de domaine) ; ils sont nécessaires si vous avez saisi le récepteur dans le champ **Domain or IP** du canal par un nom de domaine et non par une adresse IP. Par défaut, le DNS public de Google. Indépendamment des réglages IP, vérifiez que les adresses DNS fonctionnent chez votre fournisseur d'accès à Internet.

6.6.2 SIM1 et SIM2

Ces réglages doivent être effectués séparément pour chaque carte SIM insérée ; les réglages des emplacements SIM1 et SIM2 sont identiques.

Avant utilisation, assurez-vous que la carte SIM est active et fonctionne, et que le service de données mobiles est également activé sur la carte.

Dans l'application : **Advanced settings** → **Network settings** → **SIM** (la SIM1) ou **SIM2**. Dans TrikdisConfig, l'onglet **SIM1** ou **SIM2** de la page **Network settings**, groupe **SIM card**.

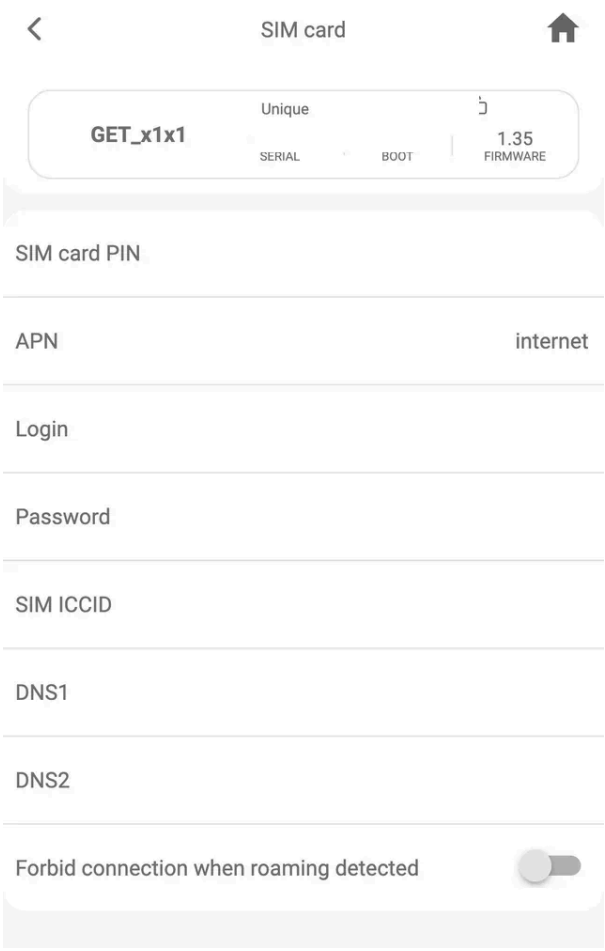


Figure 62. Protegus 2 – Network settings → SIM : SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 et l'interrupteur Forbid connection when roaming detected.

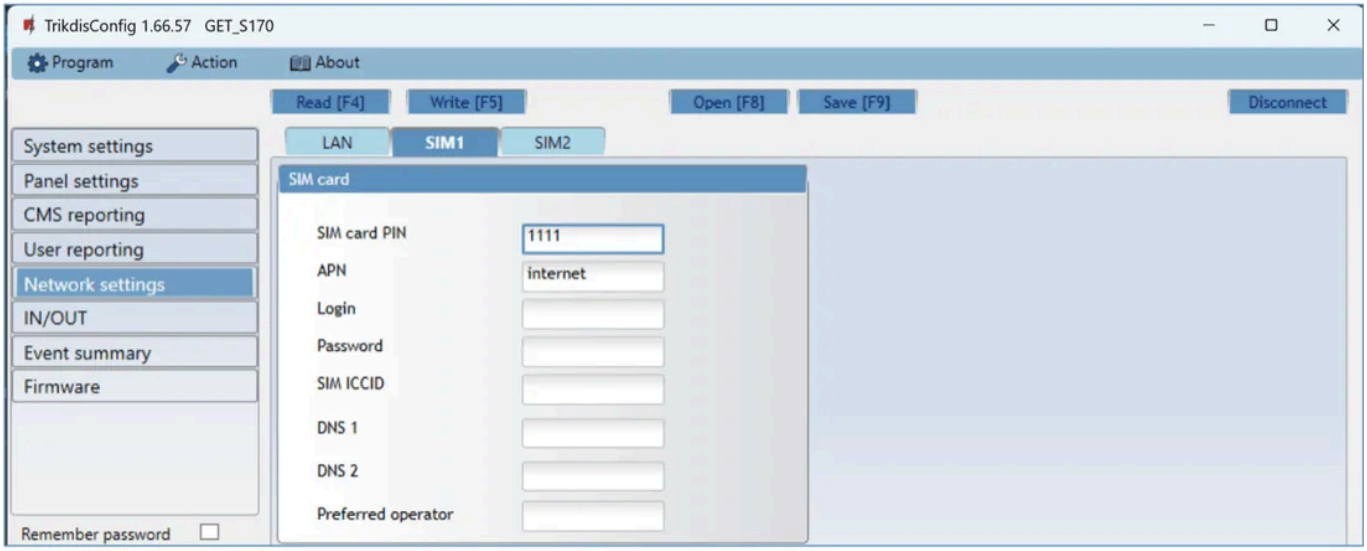


Figure 63. TrikdisConfig – Network settings, onglet SIM1, groupe SIM card : SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (l'onglet SIM2 est identique).

- **SIM card PIN** – le code PIN de la carte. Vous pouvez désactiver la demande de PIN en insérant la carte dans un téléphone mobile et en la désactivant ; la valeur d'usine du champ peut alors rester.
- **APN** – le point d'accès de l'opérateur (Access Point Name) ; sans lui, l'appareil ne se connecte pas à Internet. La valeur se trouve sur le site de l'opérateur de la carte SIM ; `internet` est générique et fonctionne sur le réseau de nombreux opérateurs. Les APN connus des opérateurs sont répertoriés dans l'article sur les APN (pour une carte IoT / M2M, l'opérateur fournit un APN distinct, voir le point 2.3).
- **Login, Password** – nom d'utilisateur et mot de passe pour la connexion Internet, si l'opérateur les exige.
- **SIM ICCID** – le numéro ICCID de la carte SIM, si vous souhaitez que l'appareil ne fonctionne qu'avec cette carte.
- **DNS1, DNS2** – serveurs de noms ; ils sont nécessaires si vous avez saisi le récepteur dans le champ **Domain or IP** du canal par un nom de domaine. Par défaut, le DNS public de Google ; vérifiez que les adresses DNS fonctionnent chez votre opérateur.
- **Preferred operator** – le code de l'opérateur mobile (MCC + MNC) ; si vous le saisissez, l'appareil ne se connecte qu'au réseau de l'opérateur choisi. **Uniquement dans TrikdisConfig**.

Dans la page SIM de l'application, à la place de Preferred operator, se trouve l'interrupteur **Forbid connection when roaming detected** : activé, le communicateur ne se connecte pas s'il détecte une itinérance (roaming). Sur la version matérielle **M15**, avec le firmware **1.17** ou plus récent, les réglages **Generation** et **Bands** apparaissent aussi dans la page SIM : ils permettent de limiter la technologie de réseau mobile et les bandes de fréquences utilisées par le communicateur.

6.7 IN/OUT

Vous indiquez ici le rôle des deux bornes I/O à double fonction du communicateur : **Disabled** (non utilisée), **IN** (entrée) ou **OUT** (sortie ; sur le GET, c'est le réglage d'usine). Pour une entrée, il faut aussi indiquer le type du circuit raccordé dans le champ **Type** (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). D'autres détecteurs peuvent être raccordés aux entrées : lorsque le détecteur est déclenché, le communicateur envoie un événement propre, avec le code Contact ID (SIA) attribué à l'entrée, au centre de télésurveillance et à Protegus 2.

Dans l'application : **Advanced settings** → **IN/OUT**, puis la borne **1** ou **2** : la **Function** (Disabled, IN, OUT) et, pour une entrée, le **Type** ; dans les parties **Alarm** et **Tamper**, les messages d'événement et de rétablissement envoyés lors du déclenchement de l'entrée. Dans TrikdisConfig, la page **IN/OUT**.

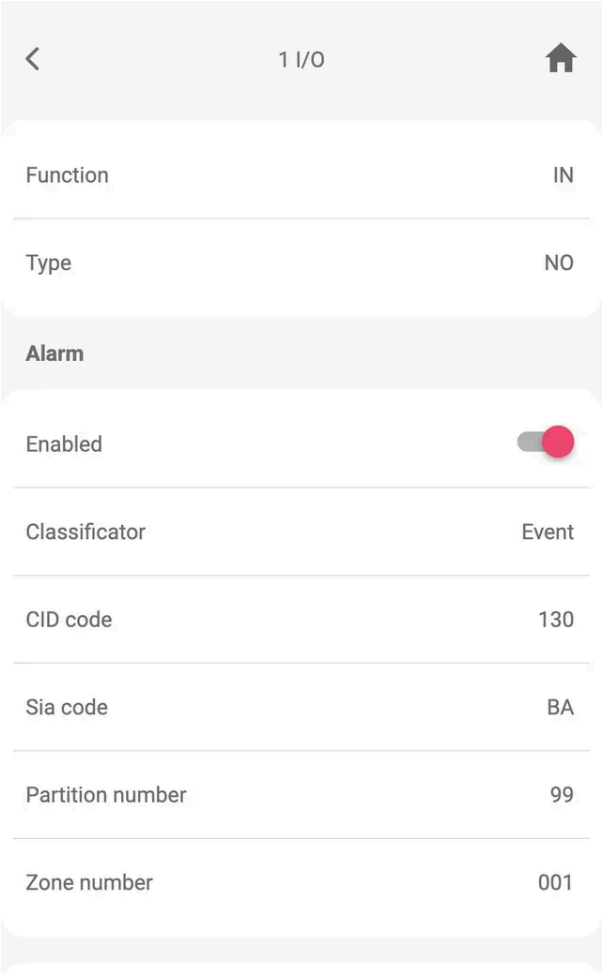


Figure 64. Protegus 2 – IN/OUT, borne 1 : Function IN, Type NO ; l'événement Alarm Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.

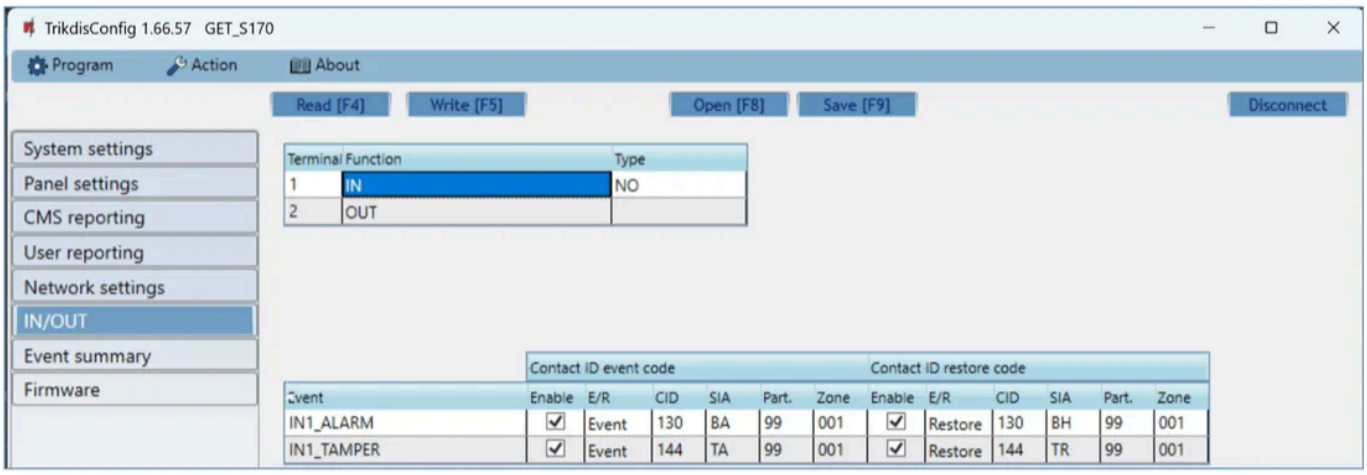


Figure 65. TrikdisConfig – page IN/OUT : la borne 1 en entrée (IN, NO), la borne 2 en sortie (OUT) ; en dessous, les événements d'alarme et d'autoprotection de l'entrée 1 avec leur code CID et SIA.

Lorsque le détecteur raccordé à l'entrée est déclenché, le communicateur envoie une alarme (**INx_ALARM**, Contact ID 130, SIA BA ; rétablissement BH), et lorsque le circuit d'autoprotection est déclenché, un événement d'autoprotection (**INx_TAMPER**, 144, SIA TA ; rétablissement TR) ; le tableau affiche les événements de chaque borne réglée en entrée. Les colonnes du tableau :

- **Enable** (Enabled) – autorise l'envoi du message au centre de télésurveillance et à Protegus 2.
- **E/R** (Classificator) – le type du message : Event (événement) ou Restore (rétablissement).
- **CID** (CID code) – le code Contact ID (modifiable, ou la valeur d'usine peut rester) ; lors du déclenchement de l'entrée, le message part avec ce code vers Protegus 2 et le centre de télésurveillance.
- **SIA** (Sia code) – le code SIA (modifiable, ou la valeur d'usine peut rester).
- **Part.** (Partition number) – le numéro de partition dans le message (pour l'événement comme pour le rétablissement).
- **Zone** (Zone number) – le numéro de zone dans le message.

6.8 Event summary (System events)

Vous pouvez ici autoriser, interdire et modifier les messages internes propres à l'appareil. Un message interdit ici ne part pas, quels que soient les autres réglages. Dans l'application : **Advanced settings** → **System events**, les messages se trouvent dans les listes **Event** et **Restore** ; pour le modifier, sélectionnez le message. Dans TrikdisConfig, la page **Event summary**.

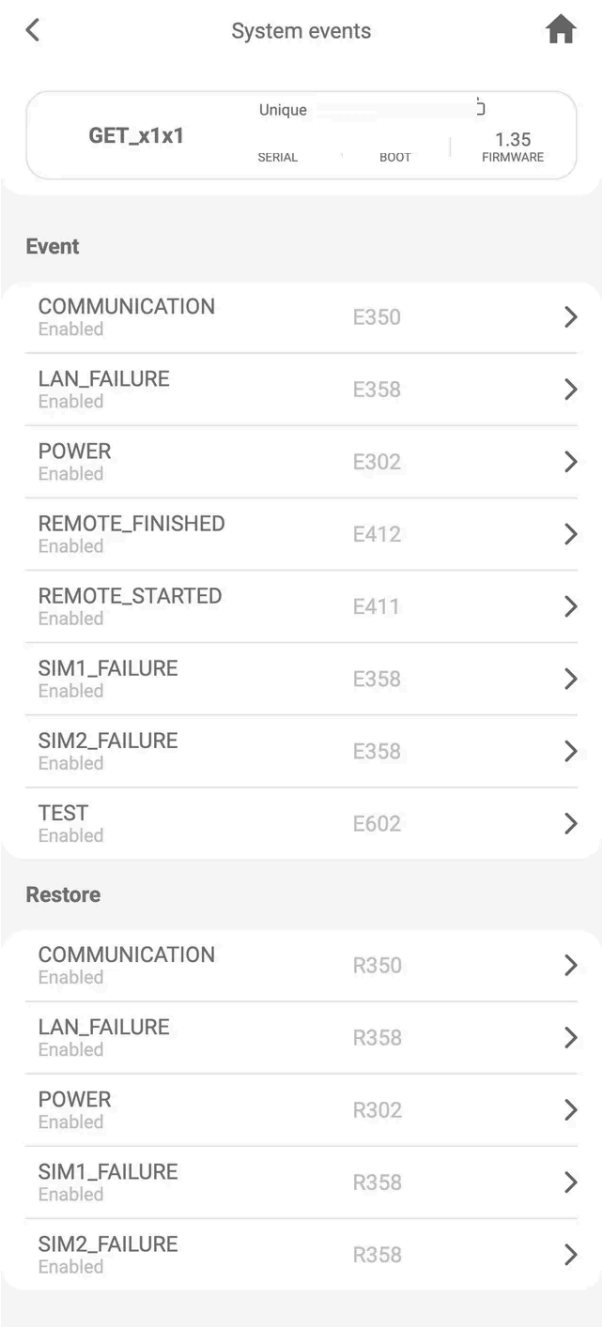


Figure 66. Protegus 2 – System events : la liste Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) et la liste Restore.

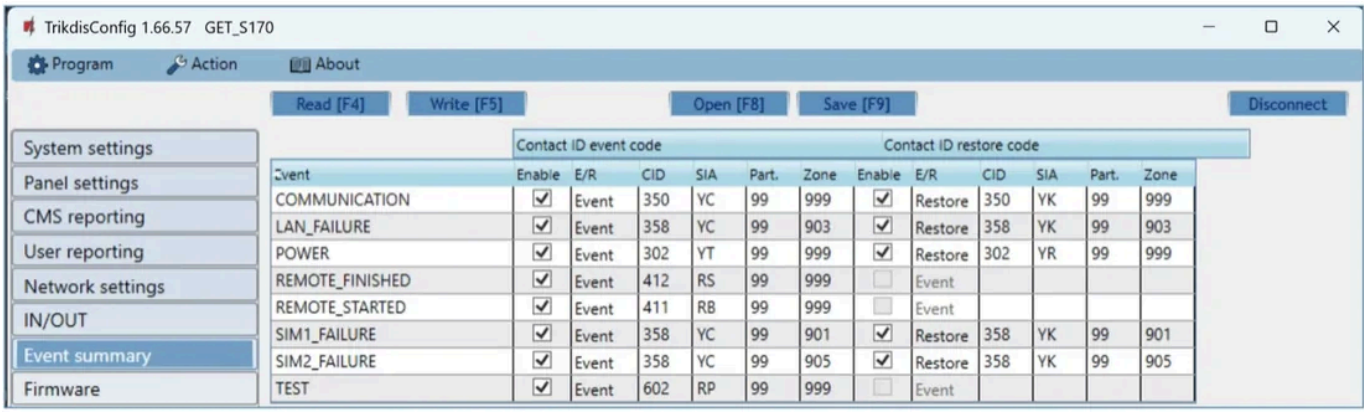


Figure 67. TrikdisConfig – page Event summary : les messages internes de l'appareil avec leur code CID et SIA, avec la partition 99.

Les messages internes du GET (entre parenthèses, le code Contact ID et la zone d'usine) :

- **COMMUNICATION** (350, zone 999) – défaut de la liaison entre la centrale et le communicateur ; son rétablissement est un message distinct.
- **LAN_FAILURE** (358, zone 903) – défaut de la connexion au réseau filaire (LAN) ; son rétablissement est un message distinct.
- **POWER** (302, zone 999) – tension d'alimentation basse ; son rétablissement est un message distinct.
- **REMOTE_FINISHED** (412) – fin de la programmation à distance par TrikdisConfig (déconnexion).
- **REMOTE_STARTED** (411) – connexion à distance pour programmer le GET avec TrikdisConfig.
- **SIM1_FAILURE** (358, zone 901) – défaut de la connexion au réseau mobile sur la SIM1 ; son rétablissement est un message distinct.
- **SIM2_FAILURE** (358, zone 905) – défaut de la connexion au réseau mobile sur la SIM2 ; son rétablissement est un message distinct.
- **TEST** (602) – rapport de test périodique.

L'activation et l'intervalle du message TEST périodique se règlent dans le champ **Test period** (point 6.4.2).

- **Enable** (Enabled) – coché, l'envoi du message est autorisé.
- Pour chaque message, le code Contact ID (SIA) ainsi que le numéro de zone et de partition sont modifiables.

6.9 Rétablissement des réglages d'usine

Les réglages d'usine ne peuvent **pas** être rétablis depuis l'application Protegus 2 : il faut le bouton **Restore** de TrikdisConfig ou le bouton **RESET** de l'appareil.

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**.



Figure 68. TrikdisConfig – le bouton Restore du groupe Default settings.

Les réglages d'usine peuvent aussi être rétablis sur l'appareil, sans ordinateur : appareil sous tension, appuyez sur le bouton **RESET** du circuit imprimé (point 1.4) et maintenez-le enfoncé **pendant 10 secondes**, jusqu'à ce que les LED NETWORK, POWER et TROUBLE s'éteignent, puis que la LED POWER s'allume. Relâchez alors le bouton : les réglages d'usine sont rétablis.

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.

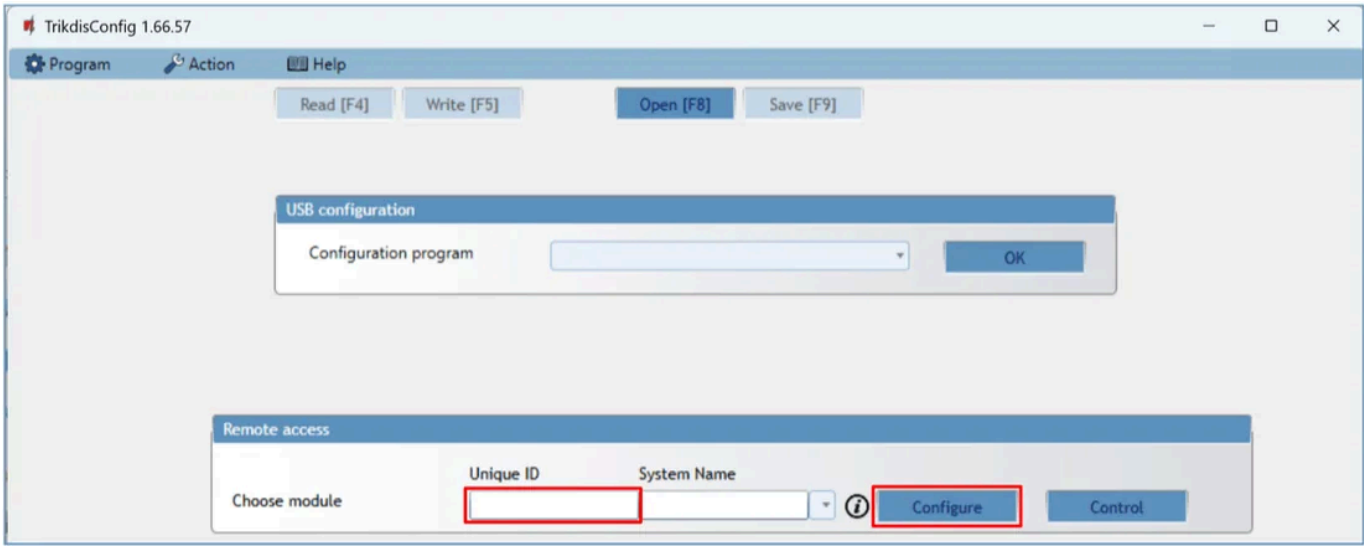


Figure 69. TrikdisConfig – le groupe Remote access : le champ Unique ID, la liste System name et le bouton Configure.

L'identifiant unique du GET est l'**IMEI / Unique ID** ; il figure sur l'étiquette de l'appareil et sur l'autocollant de la boîte. L'accès à distance ne fonctionne que si la carte SIM est active et que son code PIN est saisi ou la demande de PIN désactivée – **ou** que le communicateur est raccordé par un câble réseau (LAN) – ; si, dans la page **User reporting** → **PROTEGUS Cloud**, **Enable connection** est coché (point 6.5) ; si la LED **POWER** est allumée en vert ; si la LED **NETWORK LTE** est allumée en vert et clignote en jaune (avec une connexion filaire uniquement, c'est la LED **NETWORK LAN** qui est allumée en vert). Le communicateur signale le début et la fin de la programmation à distance par les messages REMOTE_STARTED et REMOTE_FINISHED (point 6.8).

8. Vérification du fonctionnement du communicateur

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.

Si le communicateur transmet à la fois par le réseau filaire et par le réseau mobile (point 6.4.2, Reporting mode), il est utile d'effectuer l'essai par les deux voies : débranchez le câble LAN, déclenchez un événement et vérifiez qu'il arrive aussi au centre de télésurveillance par la carte SIM ; rebranchez ensuite le câble.

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.

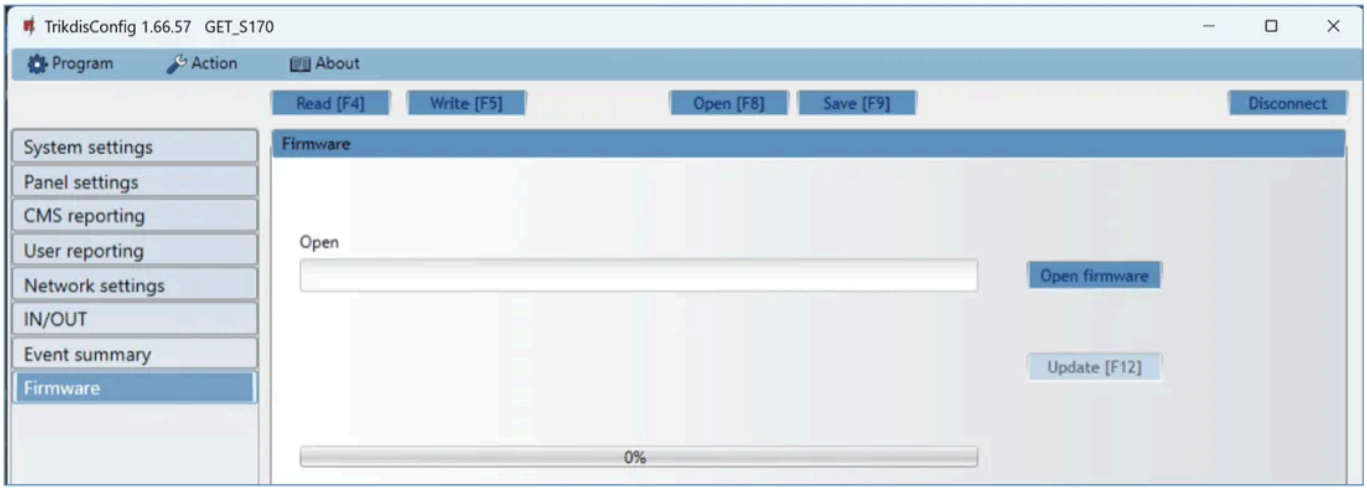


Figure 70. TrikdisConfig – page Firmware : bouton Open firmware, bouton Update [F12] et la barre de progression.

La mise à jour nécessite une connexion Internet. Un antivirus, un pare-feu ou des réglages stricts d'accès à Internet peuvent empêcher la mise à jour automatique du firmware ; dans ce cas, il faut modifier les réglages de l'antivirus.

Certaines fonctions du GET nécessitent une version de firmware déterminée :

- **1.08** ou plus récent : configuration depuis l'application Protegus 2 (Advanced settings, point 2.2 et chapitre 6) ;
- **1.17** ou plus récent, sur la version matérielle **M15** : les réglages **Generation** et **Bands** dans la page SIM de l'application (point 6.6.2) ;
- **1.21** ou plus récent : le raccordement Keybus + TIP/RING des centrales Paradox SP / SP+ / MG / MG+ (point 3.3.3) ;
- **1.31** ou plus récent, sur la version matérielle **x1x1** : dans l'application, les identifiants (Account No., Device account No.) se trouvent parmi les réglages CMS (point 6.2).

10. Dépannage et questions fréquentes

Les questions et défauts les plus fréquents, en partant de la signalisation des LED. Lorsque la réponse renvoie au chapitre détaillé, vous y trouverez l'emplacement exact du réglage.

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

1. Regardez les clignotements de la LED **TROUBLE** : 2 = défaut de la carte SIM1, 3 = défaut de la carte SIM2 (point 1.6).
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 emplacement (SIM1 au milieu de la carte, SIM2 sur le bord gauche ; point 3.1).
3. Si la demande de PIN est activée sur la carte, saisissez le PIN dans l'onglet **Network settings** → **SIM1** (ou **SIM2**), ou désactivez la demande de PIN dans un téléphone.
4. Vérifiez l'APN (point 2.3) : pour une carte IoT / M2M, l'opérateur fournit un APN distinct.
5. Vérifiez l'antenne : elle est vissée, elle n'est pas dans un boîtier métallique, le niveau de signal est suffisant (la LED NETWORK LTE clignote au moins 3 fois en jaune ; points 1.6 et 3.2).
6. Si le communicateur transmet par le réseau filaire, l'absence de réseau mobile ne l'arrête pas à elle seule : il envoie par la voie disponible suivante, selon l'ordre du **Reporting mode** (point 6.4.2) – mais la voie de secours manque alors, il vaut la peine de remettre les choses en ordre.

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

1. 1 clignotement de la LED **TROUBLE** signale un défaut de la liaison physique du réseau filaire : vérifiez le câble LAN aux deux extrémités, ainsi que le bon fonctionnement du port du routeur ou du switch (point 1.6).
2. Si le câble est en ordre, regardez l'onglet **Network settings** → **LAN** : avec DHCP, c'est le routeur qui doit attribuer l'adresse ; avec une adresse fixe, Static IP, Subnet mask et Default gateway doivent correspondre au réseau local (point 6.6.1).
3. Si vous avez saisi le récepteur par un nom de domaine, les adresses DNS doivent aussi fonctionner dans le réseau (DNS1, DNS2).

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

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. Vérifiez l'adresse du récepteur, son port, le réglage TCP/UDP, le protocole et la clé de chiffrement (**CMS reporting** → **CMS settings**, point 6.4.1) ; la clé doit être identique dans le communicateur et dans le récepteur.
2. Regardez le réglage du **Reporting mode** (point 6.4.2) : le **Main type** doit être une voie réellement disponible sur le site (câble LAN présent, ou carte SIM présente dans l'emplacement indiqué), et il doit y avoir aussi une voie de secours.

3. Si le récepteur est saisi par un nom de domaine, vérifiez le réglage DNS sur la voie par laquelle le communicateur transmet (**Network settings** → **LAN**, ou **SIM1 / SIM2** → **DNS1, DNS2**).
4. Sur le réseau mobile, 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) ; sur le réseau filaire, le pare-feu local doit autoriser le port du récepteur en sortie.
5. Si la centrale n'envoie pas d'événement (la LED DATA ne s'allume pas), la cause se trouve du côté de la centrale : voir le point suivant.

La LED TROUBLE clignote 7 fois – pas de liaison avec la centrale

1. Pour un raccordement au bus de données ou au port série, vérifiez les fils CLK et DATA, et que le modèle de la centrale raccordée est bien sélectionné dans le champ **Panel settings** → **Security panel model** (point 6.3).
2. Pour une centrale Paradox, vérifiez que le port série n'est pas verrouillé (point 4.1.2) ; pour les centrales Texecom et Paradox, le **Security panel PC download password** doit être identique à celui réglé dans la centrale.
3. Pour un raccordement par ligne téléphonique, le transmetteur de la centrale doit être activé, en mode DTMF, au format Contact ID, avec un numéro de téléphone saisi (point 4.2), et le **Communication protocol** doit être **2. AUTO** (point 6.3).

Par quelle voie part l'événement : par le LAN ou par la SIM ?

Par celle que donne l'ordre du **Reporting mode** (point 6.4.2) : par la voie selon **Main type** ; si elle ne fonctionne pas, par celle selon **Backup type**, puis selon **Backup type 2**. Si le message est parti par la voie de secours, le communicateur retente la voie principale une fois le délai **Return from backup after** écoulé, et le **Communication path test** teste toutes les voies à intervalles réguliers. La connexion à Protegus 2 utilise aussi cette même voie. Sur le réseau filaire, les données mobiles ne sont pas consommées.

À quoi servent les deux emplacements SIM ?

Avec les cartes de deux opérateurs différents, le réseau mobile devient lui aussi double : dans le Reporting mode, SIM1 et SIM2 sont des types de connexion distincts, chacune pouvant être la voie principale ou de secours (point 6.4.2). Les deux cartes doivent être configurées séparément (**Network settings** → **SIM1**, **SIM2** : PIN, APN ; point 6.6.2) ; le défaut de la SIM2 est signalé par 3 clignotements de la LED TROUBLE et par le message SIM2_FAILURE (points 1.6 et 6.8). Le communicateur fonctionne aussi avec une seule carte.

DSC : toutes les alarmes arrivent comme alarme générale E130

Raccordé uniquement au Keybus, le communicateur reçoit de la centrale l'état des zones, mais pas le type de zone ; c'est pourquoi il transmet chaque alarme avec le code E130 (point 3.3.1). Le raccordement simultané du Keybus et de TIP/RING n'existe pas sur le GET (c'est une fonction du GT+). Si le centre de télésurveillance attend un code correspondant au type de zone (par exemple incendie : E110), raccordez le GET uniquement aux bornes TIP/RING de la centrale et programmez le transmetteur (points 3.3.9 et 4.2) : ce sont alors les codes Contact ID propres à la centrale qui partent, mais il n'y a pas de pilotage direct – l'armement nécessite une zone à clé (point 3.4).

Paradox : le port série est verrouillé, ou il n'y a pas de liaison

Sur les centrales Paradox récentes (SP+, MG+, EVOHD+), le port série peut être verrouillé d'usine ; le déverrouillage est décrit au point 4.1.2 et dans l'article Déverrouillage du port série verrouillé des centrales d'alarme Paradox. Pour les centrales Spectra SP / SP+ et Magellan MG / MG+, le raccordement Keybus +

TIP/RING peut aussi être utilisé à la place du port série (point 3.3.3) ; il ne nécessite pas de déverrouillage, mais le firmware du communicateur doit être au moins en 1.21 (chapitre 9).

Je n'arrive pas à armer depuis Protegus 2

1. Pour le pilotage direct, **Panel settings → Remote Arm/Disarm** doit être coché, et la centrale doit être configurée selon le point 4.1 (Paradox : mot de passe PC, firmware V.4+ ; Texecom : UDL passcode ; Caddx, InnerRange, Honeywell : les réglages décrits). Vérifiez dans le tableau du point 1.3 que la centrale est bien pilotable directement.
2. Pour l'armement par zone à clé (point 3.4), la borne doit être en **OUT** sur la page **IN/OUT** (réglage d'usine du GET), la zone de la centrale doit être une zone à clé, et dans Protegus 2, la sortie doit être attribuée à la partition, dans le même mode que celui de la centrale (impulsion ou deux positions ; point 5.2).
3. Protegus 2 affiche l'état de la partition à partir des événements d'armement et de désarmement de la centrale : la centrale doit les transmettre (Opening/Closing).

Protegus 2 ne voit pas l'appareil

1. Dans la page **User reporting → PROTEGUS Cloud**, **Enable connection** doit être coché (point 6.5).
2. Lors de l'ajout, il faut saisir le **PROTEGUS Cloud access Code** réglé dans l'appareil ; si vous avez modifié le code dans TrikdisConfig, changez-le aussi dans l'application.
3. Saisissez l'IMEI exactement, à partir de l'étiquette de l'appareil ou de l'autocollant de la boîte (ou lisez le QR code).
4. Une connexion Internet doit fonctionner sur au moins une voie : la LED NETWORK LTE est verte et clignote en jaune (carte SIM avec service de données et bon APN), ou la LED NETWORK LAN est verte (câble LAN). Après un événement, la LED DATA doit s'éteindre.

Je n'arrive pas à me connecter à distance avec TrikdisConfig

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

Puis-je configurer le communicateur depuis l'application ?

Oui : avec le firmware 1.08 ou plus récent, la plupart des réglages sont accessibles dans le menu **Settings → Advanced settings** de Protegus 2 (point 2.2 et chapitre 6). Ce qui n'existe que dans TrikdisConfig : le rétablissement des réglages d'usine (point 6.9), le **Preferred operator** (point 6.6.2) et la mise à jour manuelle du firmware (chapitre 9) ; l'interrupteur **Event** du Serial bus est affiché par l'application, mais elle ne le modifie pas. Connecté avec le code installateur, vous ne pouvez modifier que les groupes autorisés par l'administrateur (point 6.2).

J'ai oublié le mot de passe

Ce n'est pas possible avec TrikdisConfig, car la restauration exige aussi un mot de passe. C'est possible en revanche avec le bouton **RESET** de l'appareil (point 6.9) : appareil sous tension, maintenez-le enfoncé 10 secondes. Tous les paramètres sont effacés. Le rétablissement ne peut pas être lancé depuis l'application.

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 utile de vérifier le trafic du premier mois. Tant que le communicateur transmet par le réseau filaire, les données de la carte SIM ne sont pas consommées.

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 ce manuel ; le non-respect des instructions peut entraîner un dysfonctionnement ou une panne de l'équipement.
- Avant le raccordement, lors de chaque branchement électrique et avant toute intervention, mettez l'équipement hors tension.
- Les modifications, transformations 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 devenu inutilisable ni ses composants avec les ordures ménagères. Le symbole de la poubelle sur roues barrée (DEEE) figurant sur l'appareil indique qu'il doit être déposé séparément, comme déchet électronique.

Voir aussi

- Moteur de recherche de compatibilité – quel communicateur Trikdis et quel raccordement conviennent à votre centrale d'alarme.
- Communicateur Trikdis + centrale d'alarme DSC : guide d'installation rapide – les étapes du raccordement DSC en bref.
- Communicateur Trikdis + centrale d'alarme Paradox : guide d'installation rapide – les étapes du raccordement Paradox en bref.
- DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions – pourquoi la NEO ne peut pas être raccordée au bus de données, et quelle est la solution.
- Déverrouillage du port série verrouillé des centrales d'alarme Paradox – déverrouillage du port série des centrales SP+, MG+ et EVOHD+.
- Armement à distance par zone à clé depuis l'application Protegus 2 – les détails et les pièges de l'armement par zone à clé.
- Réglage de l'APN – liste des opérateurs mobiles européens – les APN des opérateurs, y compris pour les cartes IoT / M2M.

- Documentation en anglais : docs.trikdis.com – GET – vous y trouverez aussi le tableau de conversion des codes Contact ID → SIA (annexe).

Les manuels de docs.trikdis.com sont en anglais.

Produits associés

Trikdis GET Ethernet + 4G Communicateur Intelligent

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

Antenne Stick-on GSM Trikdis ANT04 avec fil 2,5 m

Antenne magnétique Trikdis ME301m avec fil 2,5 m

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-get