Communicateurs GT et GT+ – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation des communicateurs Trikdis GT et GT+ : raccordement au bus de données, au port série ou à la sortie ligne téléphonique de la centrale d'alarme, programmation de la centrale, configuration dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2.



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

Sommaire

1. Présentation

1.1 À quoi il sert, comment il fonctionne
1.2 Versions : 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 avec TrikdisConfig

2.1 Préparatifs
2.2 Liaison avec l'application Protegus 2
2.3 Liaison avec le centre de télésurveillance

3. Installation et raccordement

3.1 Les étapes de l'installation
3.2 Emplacement et antenne
3.3 Raccordement à la centrale d'alarme
3.3.1 DSC – bus de données (Keybus)
3.3.2 DSC – Keybus et TIP/RING (GT+ uniquement)
3.3.3 Paradox – port série
3.3.4 Paradox SP/MG – Keybus et TIP/RING
3.3.5 UTC Interlogix (Caddx) – bus de données
3.3.6 Texecom – port série
3.3.7 InnerRange Inception
3.3.8 InnerRange Integriti
3.3.9 Honeywell Vista – bus de données
3.3.10 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 Raccordement du module d'extension iO-8
3.8 Mise sous tension et première vérification
A TRIKDIS átjelző elindítása

4. Programmation de la centrale d'alarme

4.1 Raccordement par bus de données ou 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
5.4 Pilotage par SMS

6. TrikdisConfig – les paramètres en détail

6.1 La barre d'état
6.2 System settings
6.3 Panel settings
6.4 CMS reporting
6.5 User reporting
6.6 Network settings
6.7 IN/OUT
6.8 RS485 modules
6.9 Event summary
6.10 Retour aux paramètres 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 GT et le GT+ sont les **communicateurs 4G pour réseau mobile** de Trikdis : ils transmettent les événements de la centrale d'alarme au centre de télésurveillance et à l'application Protegus 2. Ils se raccordent 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) qui envoie les événements au format Contact ID, en tonalités DTMF. Le communicateur transmet l'information complète de l'événement (code, partition, zone ou utilisateur) au centre de télésurveillance. Avec l'application Protegus 2, l'utilisateur pilote le système à distance et reçoit des notifications 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 concerne les communicateurs 4G GT et GT+ ; les différences entre les deux versions 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 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 ; la table de conversion figure en annexe de la documentation Trikdis en anglais. 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 coupé, il bascule sur le canal de secours. Avec un canal parallèle, les événements partent en même temps vers deux récepteurs. Si le service Protegus est aussi activé, l'événement est d'abord reçu par le centre de télésurveillance, et seulement ensuite 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. En plus de Protegus 2, des notifications peuvent aussi être demandées par SMS et par appel téléphonique.
- **Il pilote directement la centrale.** Raccordé sur le bus de données ou le 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 – aucune zone à clé n'est nécessaire. Avec les centrales DSC, le GT+ peut être raccordé en même temps sur le bus de données (Keybus) et sur les bornes TIP/RING : le bus sert au pilotage et aux états, et les événements partent avec les propres codes Contact ID de la centrale (point 3.3.2).
- **Il a ses propres entrées et sorties.** Deux bornes I/O à double fonction s'utilisent comme entrée (IN) ou comme sortie pilotable (OUT). Les sorties se commandent depuis l'application Protegus 2 et par commande SMS. Des modules d'extension iO-8 raccordés au bus RS485 permettent d'ajouter d'autres entrées et sorties.
- **Configuration.** Les paramètres 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 peut aussi être configuré à distance, et son firmware peut 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 par le réseau mobile (LTE), 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 et peut aussi recevoir des SMS et des appels par le réseau mobile.

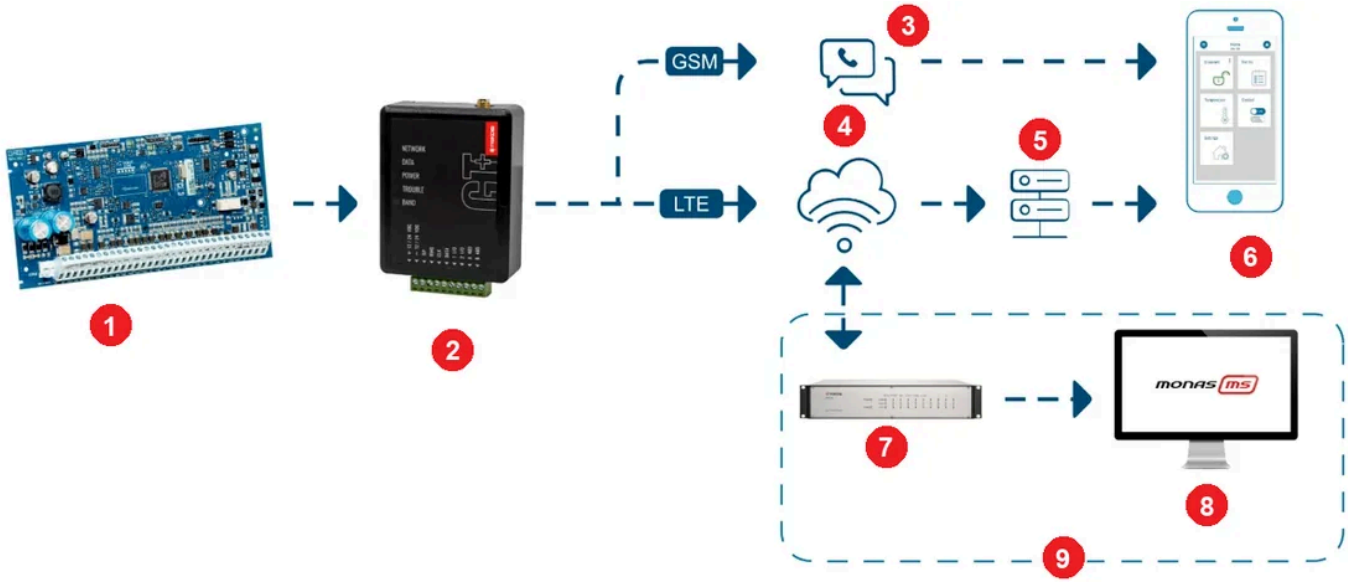


Figure 1. La place du communicateur dans le système : centrale d'alarme → GT / GT+ → réseau mobile → Internet → récepteur du centre de télésurveillance et serveur Protegus → application Protegus 2 ; SMS et appels directement par le réseau mobile.

- 1 centrale d'alarme (« Alarm panel »)
- 2 communicateur LTE GT / GT+ (« LTE communicator »)
- 3 appel et SMS (« Call/SMS »)
- 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 : GT et GT+

Le GT et le GT+ sont le même appareil en deux versions : leur raccordement, leur configuration et leur fonctionnement sont presque identiques, c'est pourquoi nous les décrivons dans un seul manuel. Les différences sont résumées dans le tableau ci-dessous ; là où le texte donne la valeur du GT+, tenez compte de celle-ci pour le GT.

	GT	GT+
Tension d'alimentation	10–18 V DC	10–32 V DC
Marquage des bornes d'alimentation	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Raccordement d'une centrale DSC	uniquement sur le bus de données (Keybus)	sur le bus de données, ou sur le bus de données et les bornes TIP/RING ensemble – ainsi les événements partent avec les propres codes Contact ID de la centrale (p. ex. incendie : E110), et non comme alarme générale (E130)

	GT	GT+
Réglage du raccordement par ligne téléphonique (TIP/RING) dans TrikdisConfig (**Panel settings** → **Communication protocol**)	**2. Dual tone**	**2. AUTO** (la liste propose aussi **3. MANUAL**)
Vérification avec une DSC raccordée en bus + TIP/RING (chapitre 8)	–	l'alarme d'une zone incendie doit arriver en E110
Tout le reste : entrées/sorties, bus RS485, modem, LED, dimensions, protocoles, Protegus 2, commandes SMS	identique	identique

Les deux versions existent avec trois modems différents ; pour la France et le reste de l'Europe, c'est la version européenne (EU) qui convient. Vous trouverez le type de modem et la version matérielle 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 bus de données ou port série. La colonne « Pilotage direct » indique si l'utilisateur peut armer et désarmer depuis Protegus 2 avec son propre code clavier sans raccordement supplémentaire ; 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	Type	Raccordement	Pilotage direct
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	bus de données (Keybus) ; GT+ : aussi Keybus + TIP/RING	oui
DSC	PC5020	bus de données (Keybus)	non
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

Fabricant	Type	Raccordement	Pilotage direct
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 (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 traité au point 4.1.2. Les centrales Spectra SP / SP+ et Magellan MG / MG+ peuvent aussi être raccordées, au lieu du port série, sur le bus de données (Keybus) et les bornes TIP/RING ensemble – cela ne nécessite pas le déverrouillage payant (point 3.3.4).
- Les centrales de **toutes les autres marques** se raccordent par leur transmetteur téléphonique (TIP/RING), s'il envoie les événements au format Contact ID, en numérotation DTMF ; le pilotage nécessite alors une zone à clé.
- Pour savoir quel communicateur Trikdis et quel raccordement conviennent à votre centrale, consultez l'outil 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 et le bornier est débrochable. La figure ci-dessous montre le GT+ ; le GT est identique, seul le marquage du boîtier est GT, et les bornes d'alimentation sont marquées +12 VDC / −12 VDC.

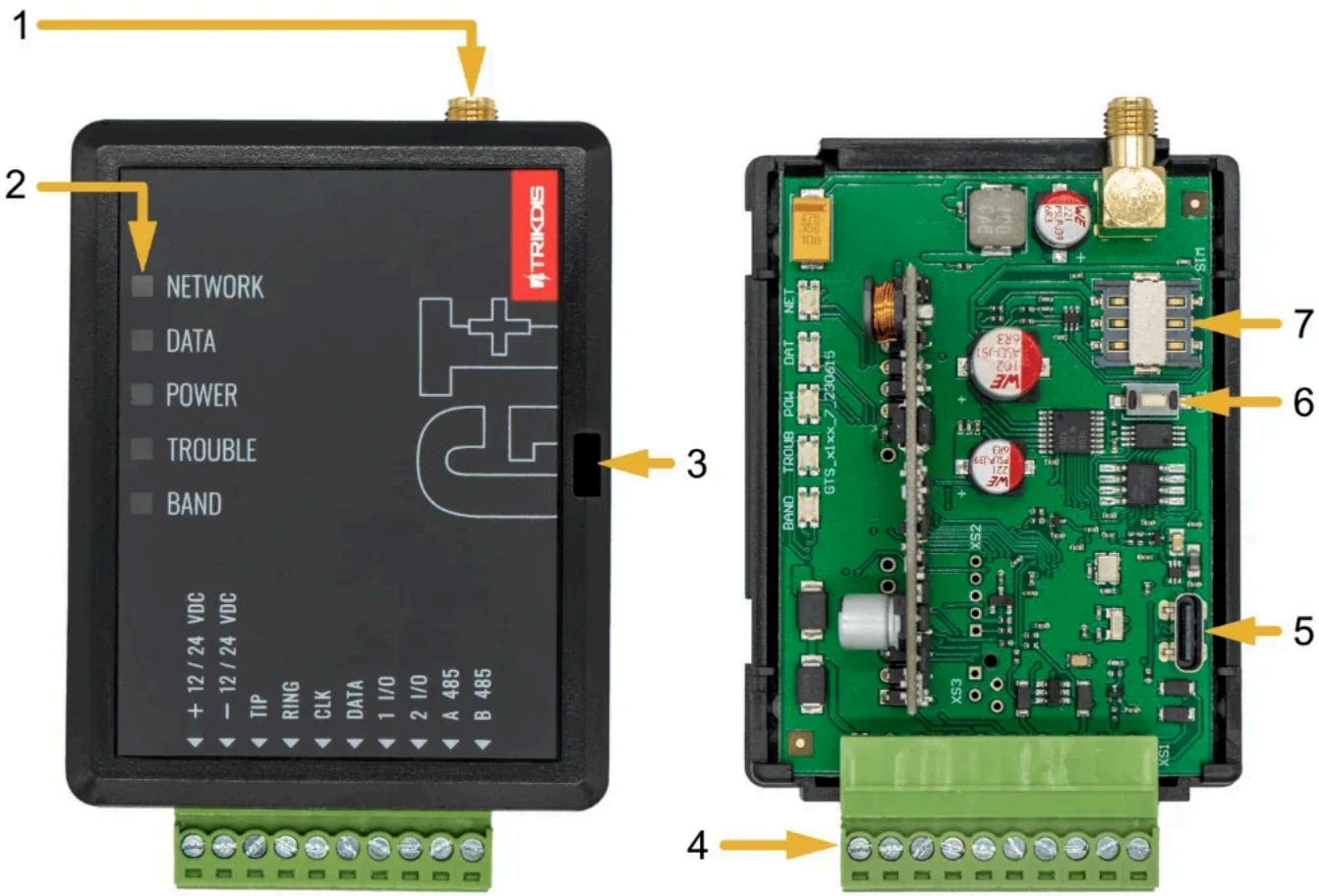


Figure 2. Les éléments du communicateur, vu de face (à gauche) et boîtier ouvert (à droite).

- 1 Connecteur SMA de l'antenne mobile
- 2 Voyants LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Ouverture facilitant le déclipsage de la face avant
- 4 Bornier débrochable pour les raccordements externes
- 5 Prise USB-C pour la programmation
- 6 Bouton RESET
- 7 Support de la carte nano-SIM

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 raccordement, et pour la programmation par USB, l'appareil peut être apporté jusqu'à l'ordinateur.

1.5 Bornes

Borne (GT)	Borne (GT+)	Fonction
+12 VDC	**+12 / 24 VDC**	Alimentation, positif : +10–18 V DC (GT), +10–32 V DC (GT+)
–12 VDC	**–12 / 24 VDC**	Alimentation, 0 V
TIP	**TIP**	Borne TIP du transmetteur téléphonique de la centrale d'alarme
RING	**RING**	Borne RING du transmetteur téléphonique de la centrale d'alarme
CLK	**CLK**	Bus série ou bus de données (horloge) pour le raccordement direct de la centrale
DATA	**DATA**	Bus série ou bus de données (données) pour le raccordement direct de la centrale
1 I/O	**1 I/O**	Entrée/sortie 1 (réglage d'usine : entrée, NO)
2 I/O	**2 I/O**	Entrée/sortie 2 (réglage d'usine : entrée, NO)

Borne (GT)	Borne (GT+)	Fonction
A 485	**A 485**	Fil A du bus RS485
B 485	**B 485**	Fil B du bus RS485

Sur les schémas de raccordement, les bornes d'alimentation sont uniformément marquées **+DC** et **−DC** (sur le GT, ce sont les bornes +12 VDC / −12 VDC, sur le GT+ les bornes +12 / 24 VDC / −12 / 24 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 le réseau, TROUBLE les défauts, BAND le type de réseau.

NETWORK – connexion au réseau

Signal	Signification
éteinte	Pas de connexion au réseau mobile
clignote en jaune	Connexion au réseau mobile en cours
verte fixe, 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

DATA – transfert de données

Signal	Signification
éteinte	Aucun événement en attente d'envoi
verte fixe	Des événements en attente d'envoi sont 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

Signal	Signification
éteinte	Pas d'alimentation, ou l'alimentation est déconnectée
verte fixe	Sous tension, la tension d'alimentation est correcte
jaune fixe	Tension d'alimentation insuffisante (11,5 V au maximum)

Signal	Signification
verte fixe, clignote en jaune	Prêt pour la programmation (pendant la programmation)
jaune fixe (pendant la programmation)	Pas de connexion avec l'ordinateur

TROUBLE – défaut

Signal	Signification
éteinte	Aucun défaut
1 clignotement rouge	Pas de carte SIM
2 clignotements rouges	Erreur de code PIN de la SIM (code PIN incorrect)
3 clignotements rouges	Erreur de programmation (pas d'APN)
4 clignotements rouges	Impossible de s'enregistrer sur le réseau mobile (erreur d'enregistrement)
5 clignotements rouges	Impossible de se connecter au réseau de données (GPRS/UMTS)
6 clignotements rouges	Pas de connexion avec le récepteur du centre de télésurveillance
7 clignotements rouges	La liaison avec la centrale d'alarme est interrompue
8 clignotements rouges	L'ICCID réglé ne correspond pas à l'ICCID de la carte SIM (point 6.6)
clignote en rouge (pendant la programmation)	Erreur de mémoire
rouge fixe (pendant la programmation)	Firmware endommagé

BAND – type de réseau

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

1.7 Caractéristiques techniques

Paramètre	Valeur
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 de 2,2 kΩ) ; en sortie à collecteur ouvert (OC), max. 0,15 A / 30 V DC. Extensible avec des modules iO-8
Modem	EG915U-EU (Europe), EG915U-LA (Amérique latine) ou BG95-M5 (LTE Cat M1) – les bandes de fréquences sont listées dans le tableau du point 1.2
Tension d'alimentation	GT : 10–18 V DC ; GT+ : 10–32 V DC

Paramètre	Valeur
Consommation	au maximum 100 mA en veille ; au maximum 200 mA pendant l'envoi de données
Protocoles de transmission	TRK8, DC-09_2007, DC-09_2012, TL150
Chiffrement	AES-128
Programmation	TrikdisConfig (Windows) par câble USB-C ou à distance
Environnement de fonctionnement	−10 … +50 °C, humidité relative max. 80 % (à +20 °C)
Dimensions	92 × 62 × 26 mm
Poids	80 g

2. Mise en service rapide avec TrikdisConfig

Tous les paramètres du communicateur se règlent avec le logiciel **TrikdisConfig**, qui fonctionne sous Windows – par câble USB-C ou à distance. Ce chapitre décrit le chemin le plus court : vous configurez l'appareil sur le bureau, avant le raccordement, et sur le site il ne reste plus qu'à le raccorder. Nous indiquons quels paramètres sont nécessaires pour que le communicateur envoie les événements au centre de télésurveillance et pour que le système puisse être piloté depuis l'application Protegus 2 ; l'explication détaillée des paramètres se trouve au chapitre 6.

2.1 Préparatifs

Ce dont vous aurez besoin

Câble USB-C pour la programmation · câble d'au moins 4 conducteurs entre le communicateur et la centrale · pour le port série Paradox, un câble CRP2.4 · tournevis plat de 2,5 mm · antenne mobile à gain adapté si la couverture est faible sur le site · carte SIM active (la demande de code PIN peut être désactivée) · le manuel d'installation de la centrale d'alarme.

Commandez séparément les accessoires nécessaires auprès du distributeur.

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

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Ouvrez le boîtier du communicateur avec un tournevis plat : insérez le tournevis en haut, dans la fente à côté de l'antenne, et faites levier vers l'extérieur, puis en bas, au niveau de l'ouverture, vers le bas. La figure montre aussi l'emplacement de la prise USB-C sur le bord du circuit imprimé.

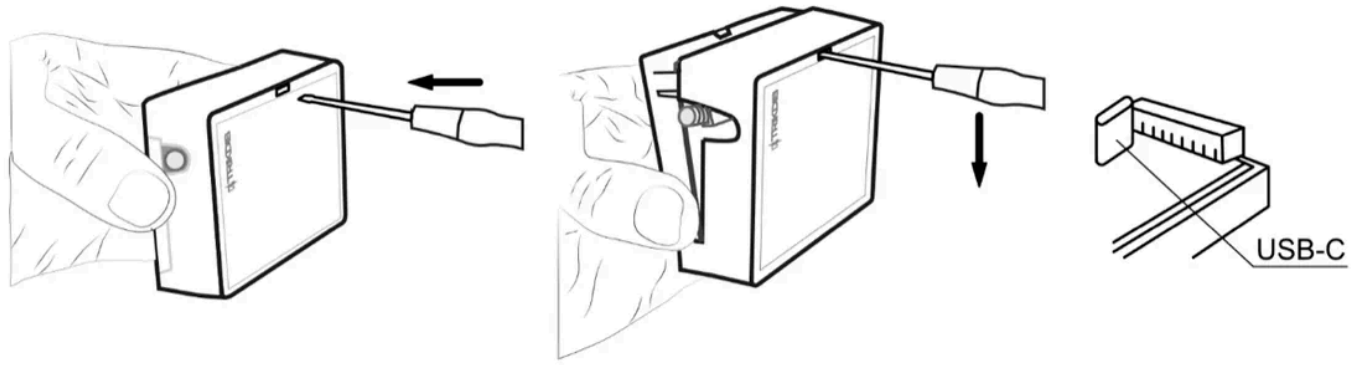


Figure 3. Déclipsage de la face avant avec un tournevis plat ; le détail agrandi montre l'emplacement de la prise USB-C.

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

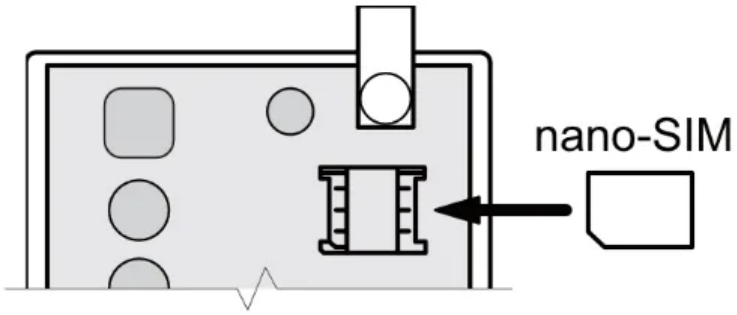


Figure 4. Emplacement de la carte nano-SIM sur le circuit imprimé.

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 paramètres actuels de l'appareil. S'il demande un mot de passe, saisissez le code à 6 chiffres administrateur (`123456` par défaut) ou installateur (`654321` par défaut).

2.2 Liaison avec l'application Protegus 2

Commencez par indiquer, à 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 : dans le champ **Communication protocol**, choisissez la valeur **AUTO** (sur le GT, le deuxième élément de la liste est **Dual tone** – choisissez celui-ci).

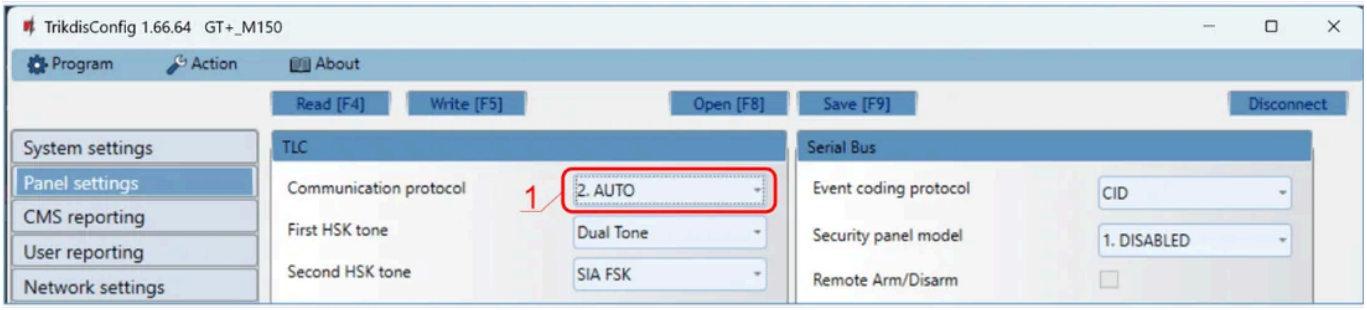


Figure 5. TrikdisConfig – Panel settings, groupe TLC (réglage du GT+ sur l'image).

- 1 **Communication protocol** – pour un raccordement TIP/RING, **2. AUTO** (GT : **2. Dual tone**).

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



Figure 6. TrikdisConfig – Panel settings, groupe Serial bus.

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

GT+, centrale DSC sur le bus de données et sur les bornes TIP/RING ensemble : le **Communication protocol** doit être **AUTO**, le **Security panel model** le type DSC, et cochez l'option **Remote Arm/Disarm** si la centrale doit être pilotée depuis Protegus 2 (point 3.3.2).

Pour le pilotage direct, la centrale d'alarme doit elle 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, à la page **User reporting**, dans l'onglet **PROTEGUS Cloud**, autorisez la liaison avec le cloud.

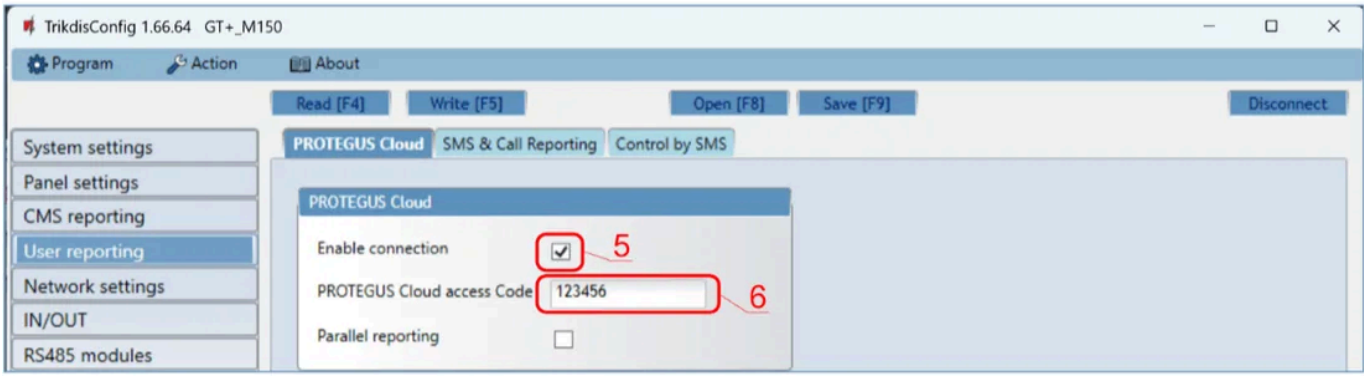


Figure 7. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- 5 **Enable connection** – cochez cette case : elle autorise la liaison avec le cloud Protegus.
- 6 **PROTEGUS Cloud access Code** – le code d'accès à Protegus 2 (`123456` par défaut). Modifiez-le si vous voulez que l'utilisateur doive le saisir lors de l'ajout du système dans l'application. Important : si vous modifiez le code plus tard dans TrikdisConfig, il faut aussi le changer dans l'application Protegus 2.

Enfin, à la page **Network settings**, dans l'onglet **SIM1**, saisissez les données de la carte.

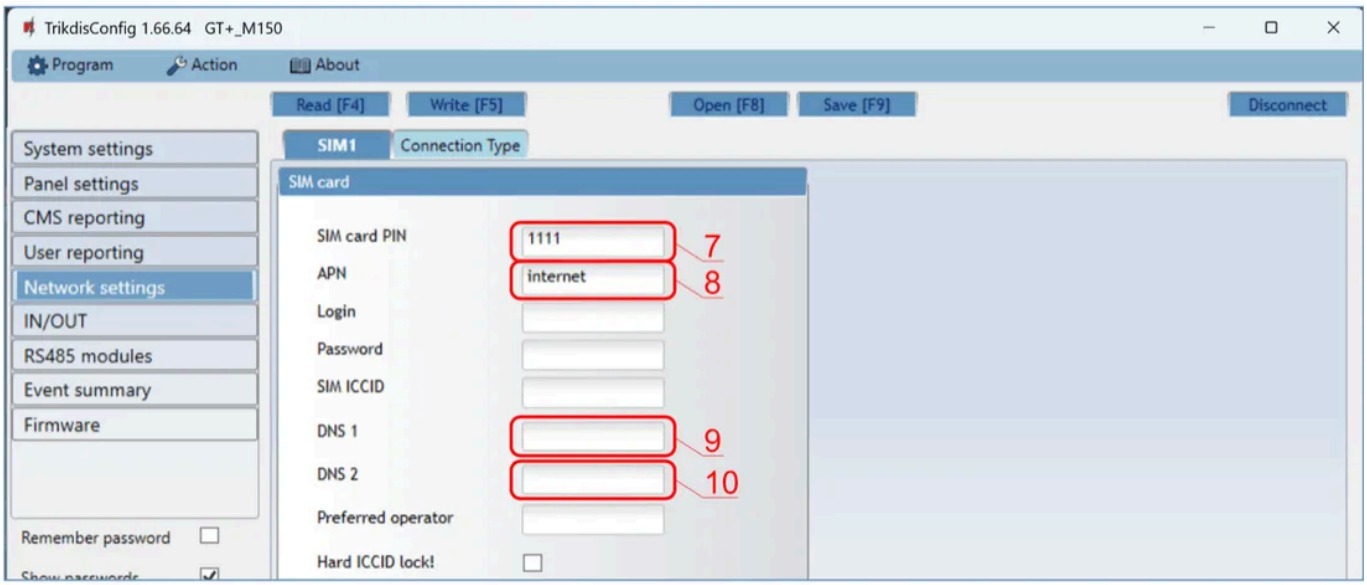


Figure 8. TrikdisConfig – Network settings, onglet SIM1.

- 7 **SIM card PIN** – le code PIN de la carte (si la demande de code PIN est désactivée, la valeur d'usine peut rester).
- 8 **APN** – le point d'accès aux données de l'opérateur (voir ci-dessous).
- 9 **DNS 1** – serveur de noms principal ; par défaut celui de Google. Indépendamment des paramètres IP, vérifiez que les adresses DNS fonctionnent chez votre opérateur.
- 10 **DNS 2** – serveur de noms secondaire (par défaut 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. Vous trouverez la valeur exacte 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 (entre machines), l'opérateur fournit généralement **un APN différent de celui des cartes grand public** – avec l'APN grand public, l'appareil ne se connecte pas. Vous trouverez aussi cette valeur dans l'article sur les APN, ou demandez-la à l'opérateur ; s'il fournit aussi un nom d'utilisateur et un mot de passe, saisissez-les également.

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 Liaison avec le centre de télésurveillance

Si l'appareil transmet aussi vers un récepteur de centre de télésurveillance, commencez par saisir l'identifiant de l'objet à la page **System settings**.

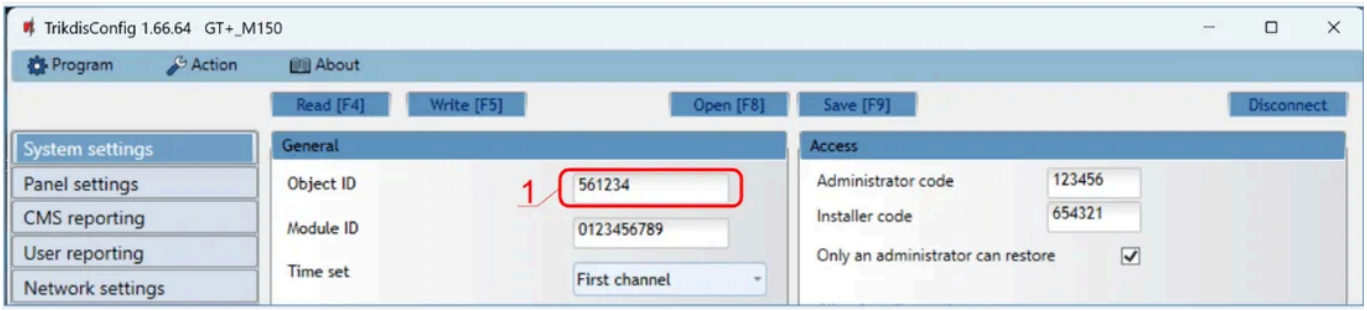


Figure 9. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – l'identifiant de l'objet fourni par le centre de télésurveillance (6 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne peuvent pas être utilisés.

À 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** (GT : **Dual tone**) ; pour un raccordement par bus de données ou port série, choisissez le type de la centrale raccordée dans le champ **Security panel model** (figures du point 2.2).

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

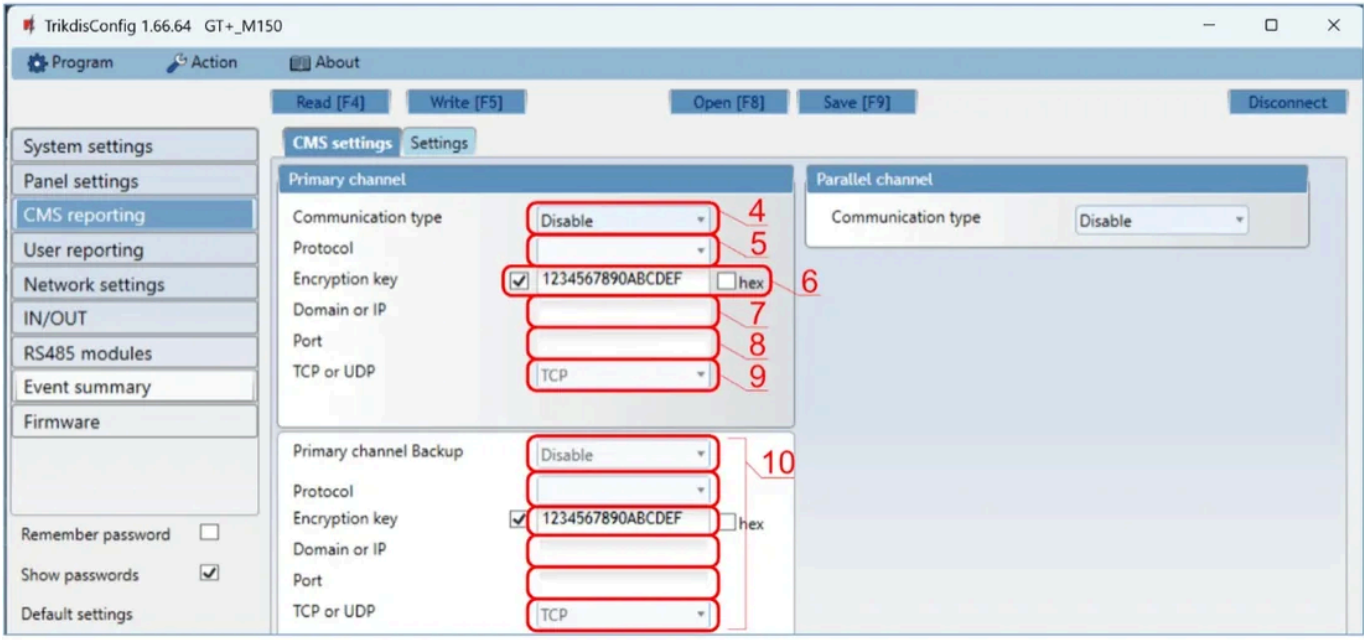


Figure 10. TrikdisConfig – CMS reporting, onglet CMS settings.

- 4 **Communication type** – choisissez la liaison **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 manière, il est recommandé de le renseigner.

Enfin, à la page **Network settings**, dans l'onglet **SIM1**, saisissez les données de la carte (**SIM card PIN**, **APN**, **DNS 1, DNS 2**) si vous ne l'avez pas encore fait au point 2.2.

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). Le GT et le GT+ ne transmettent au centre de télésurveillance que par liaison IP ; ils n'ont pas de canal de secours par SMS.

À la fin de la configuration, 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 dans son support 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 la figure).
4. Fixez le fond du boîtier avec des vis à l'emplacement choisi (les trous de fixation sont entourés sur la figure).
5. Remettez le circuit imprimé dans le fond du boîtier et rebranchez le bornier.
6. Vissez l'antenne mobile.
7. Remettez la face avant.

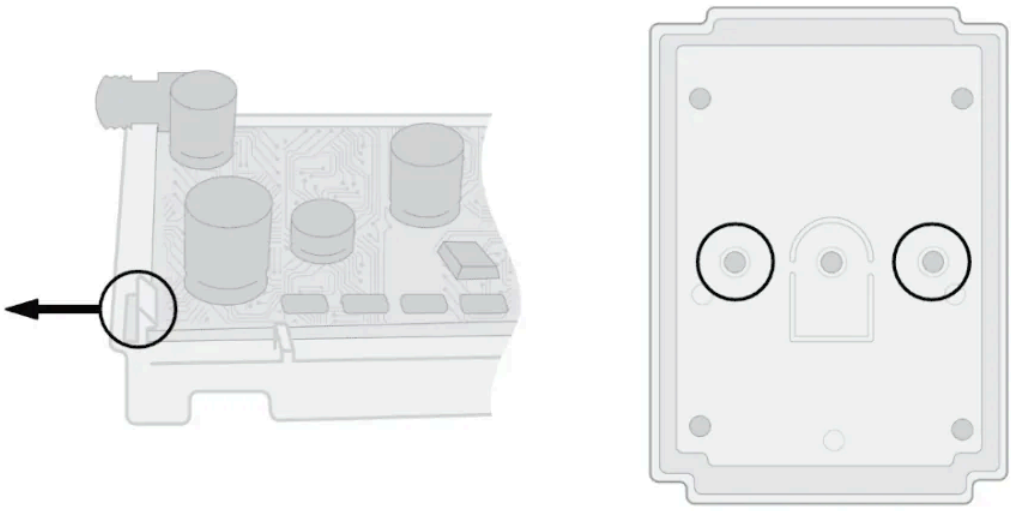


Figure 11. Retrait du circuit imprimé du fond du boîtier (à gauche : le loquet et le sens de retrait) et trous de fixation du fond du boîtier (à droite).

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

3.2 Emplacement et antenne

- Placez le communicateur dans un endroit **sec, à l'intérieur**, de préférence près du coffret de la centrale d'alarme, afin que le câblage reste court.
- Dans un **coffret métallique**, le signal mobile est fortement atténué. Si le communicateur est placé dans le boîtier métallique de la centrale, sortez l'antenne à l'extérieur du coffret ou utilisez une antenne à câble plus long.
- Avant la fixation définitive, **vérifiez le niveau de signal** : en 4G, le nombre de clignotements jaunes de la LED NETWORK doit être d'au moins 3 (point 1.6). S'il est inférieur, cherchez un meilleur emplacement ou passez à une antenne plus sensible, pouvant être placée plus loin.
- Tenez l'antenne et le communicateur éloignés du transformateur de la centrale et des câbles secteur.



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

3.3 Raccordement à la centrale d'alarme

Suivez parmi les schémas ci-dessous celui qui correspond à votre centrale. Sur les schémas, **+DC** et **–DC** désignent les bornes d'alimentation du communicateur (GT : +12 VDC / −12 VDC, GT+ : +12 / 24 VDC / −12 / 24 VDC), et **A RS485** / **B RS485** les bornes A 485 / B 485. 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. Les schémas montrent le GT+ ; le raccordement du GT est identique.

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**.

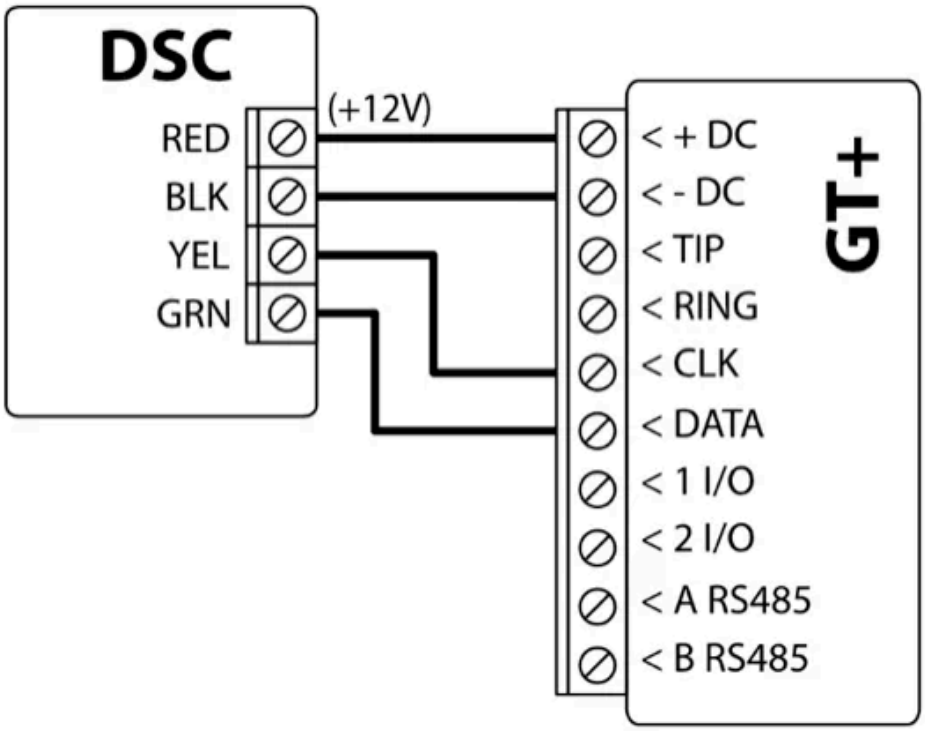


Figure 12. Raccordement d'une centrale DSC sur le bus de données (Keybus, « Keypad bus ») : RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Raccordé uniquement au Keybus, le communicateur reçoit de la centrale l'état général des zones, mais ne connaît pas le type de la zone (incendie, intrusion, fuite d'eau, etc.). Il transmet donc chaque alarme comme **alarme générale, avec le code Contact ID E130**, et certains centres de télésurveillance la traitent autrement que le type de zone réellement déclenché. Si vous voulez envoyer les événements avec les propres codes Contact ID de la centrale (par exemple alarme incendie : E110), raccordez aussi les bornes TIP/RING sur le GT+ (point 3.3.2).

3.3.2 DSC – Keybus et TIP/RING (GT+ uniquement)

Le GT+ peut être raccordé à la centrale DSC à la fois sur le bus de données et sur la sortie ligne téléphonique : en plus des fils du Keybus, reliez aussi les bornes **TIP** → **TIP** et **RING** → **RING** de la centrale à celles du communicateur.

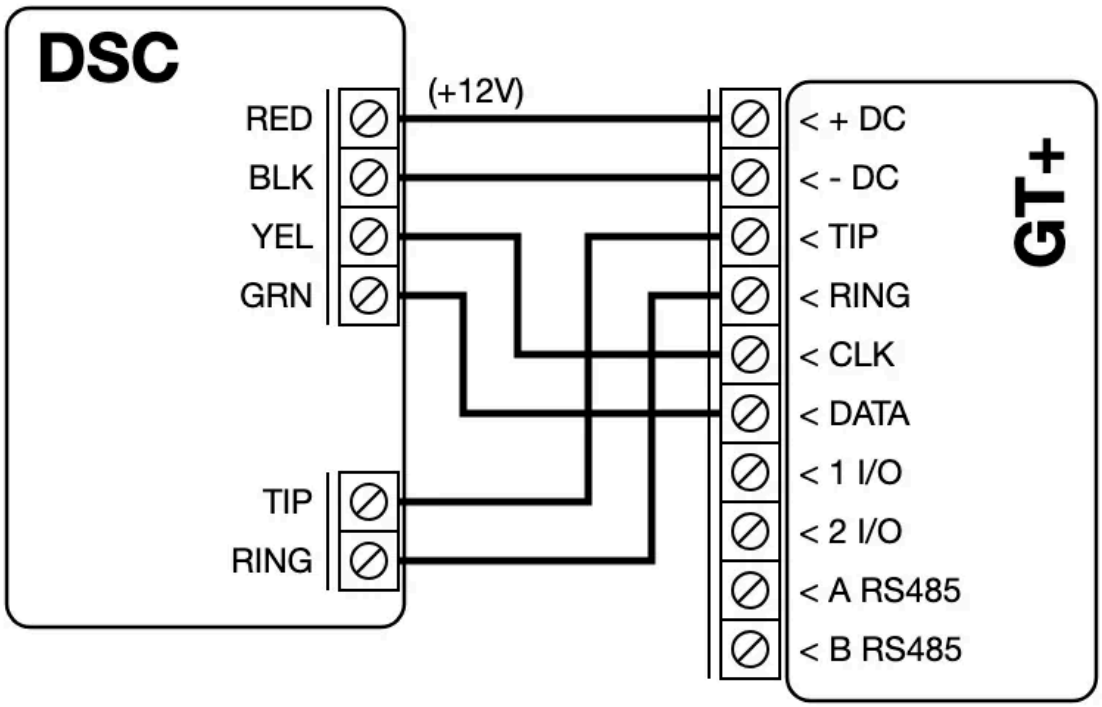


Figure 13. Raccordement d'une centrale DSC sur le bus de données (« Keypad bus ») et sur les bornes TIP/RING ensemble (GT+) : RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA, ainsi que TIP → TIP, RING → RING.

Dans ce cas, le Keybus sert au pilotage et aux états (armement et désarmement à distance, états des partitions et des zones), et les événements sont envoyés par le transmetteur téléphonique de la centrale sur les bornes TIP/RING ; ils partent donc avec les propres codes Contact ID de la centrale. Tant que le raccordement TIP/RING fonctionne, le communicateur n'envoie pas une seconde fois les événements arrivant par le Keybus.

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

1. **Communication protocol** : **AUTO**.
2. **Security panel model** : le type de la centrale DSC.
3. **Remote Arm/Disarm** : cochez cette case si les utilisateurs veulent piloter la centrale depuis l'application Protegus 2.

Le transmetteur téléphonique de la centrale DSC doit aussi être programmé pour qu'il envoie les événements – c'est décrit au point 4.1.1.

3.3.3 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**.

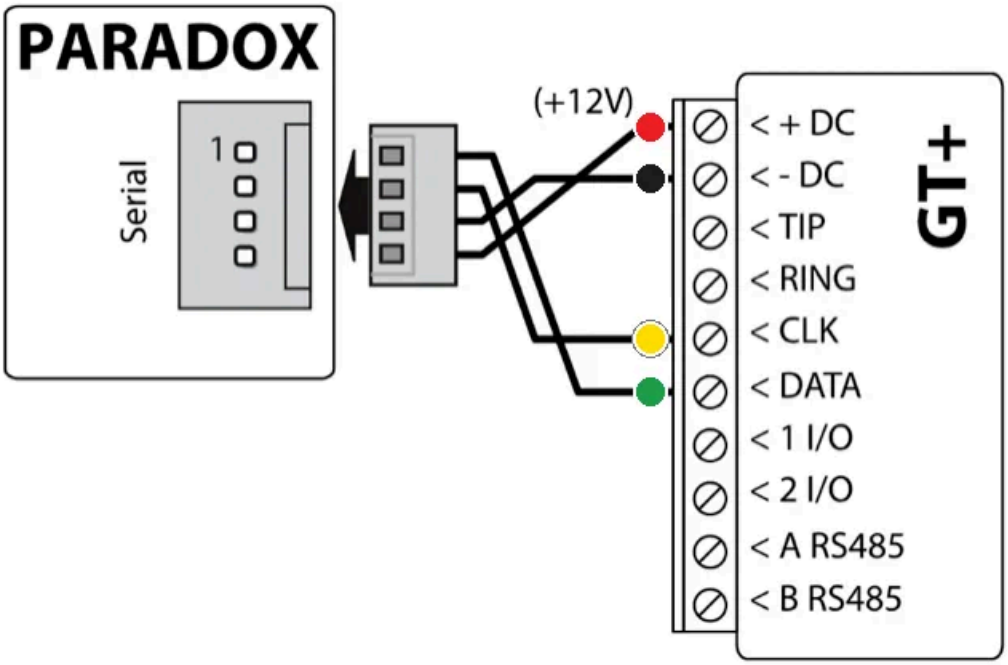


Figure 14. Raccordement d'une centrale Paradox sur le port série avec le câble EX-CRP2.4 (à commander séparément ; « Use the EX-CRP2.4 cable (ordered separately) ») : rouge → +DC, noir → −DC, jaune → CLK, vert → DATA.

- 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 traité 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.

3.3.4 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, sur leur bus de données (Keybus) et leurs bornes TIP/RING ensemble : **+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.

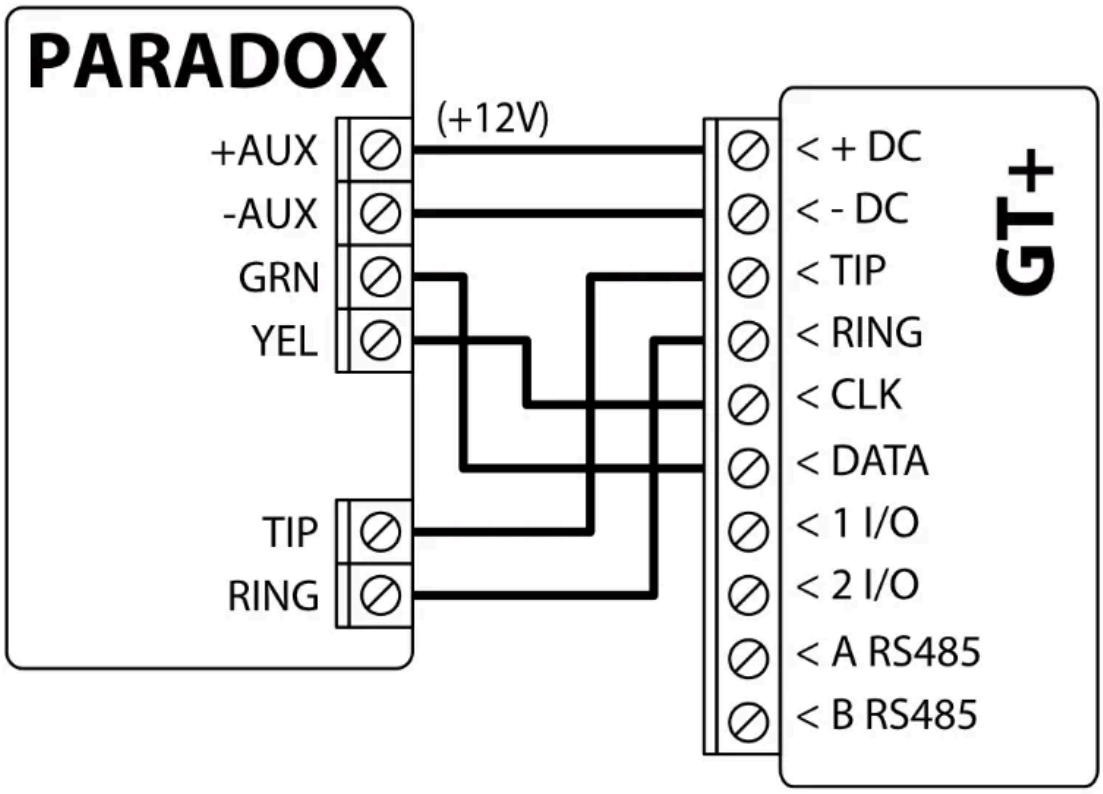


Figure 15. Raccordement d'une centrale Paradox SP / SP+ / MG / MG+ sur le Keybus (bus de données, « Keypad bus ») et sur les bornes TIP/RING ensemble : +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

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

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

1. **Communication protocol** : **AUTO** (GT : **Dual tone**).
2. **Security panel model** : **7. Paradox SP+/MG+ series KeyBus**.
3. **Remote Arm/Disarm** : cochez cette case si les utilisateurs veulent 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 16. TrikdisConfig – Panel settings pour le raccordement Keybus + TIP/RING : Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm coché, PC download password renseigné.

La centrale Paradox doit aussi être programmée pour envoyer les événements au centre de télésurveillance et pour pouvoir être pilotée depuis Protegus 2 – c'est décrit au point 4.1.2.

3.3.5 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 TIP, RING et CLK ne sont pas utilisées.

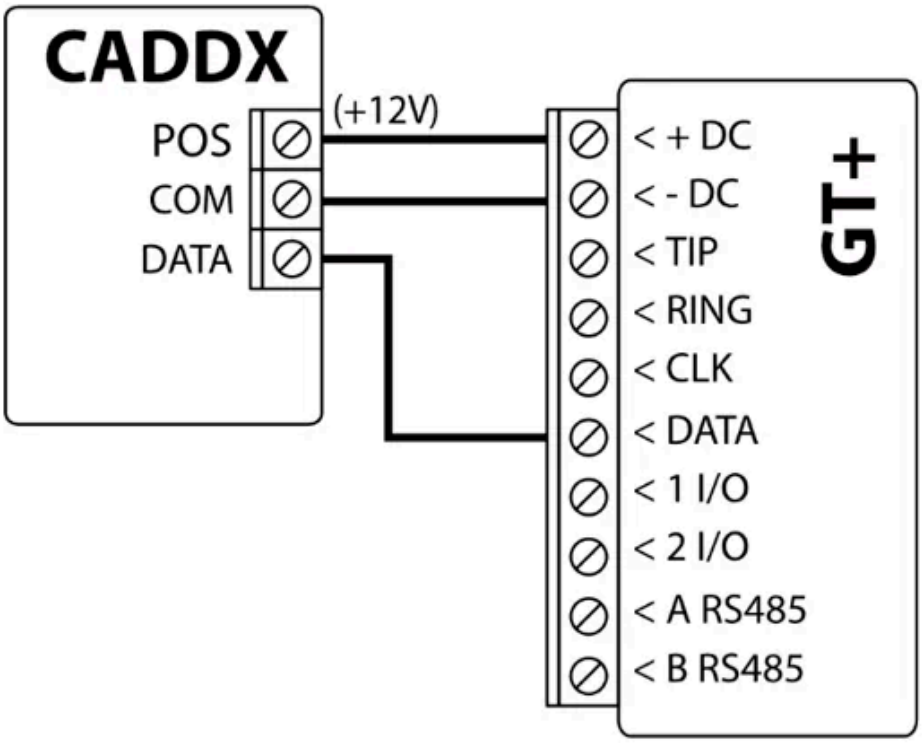


Figure 17. Raccordement d'une centrale UTC Interlogix (Caddx) NetworX sur le bus de données (« Keypad bus ») : POS → +DC, COM → −DC, DATA → DATA.

3.3.6 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**.

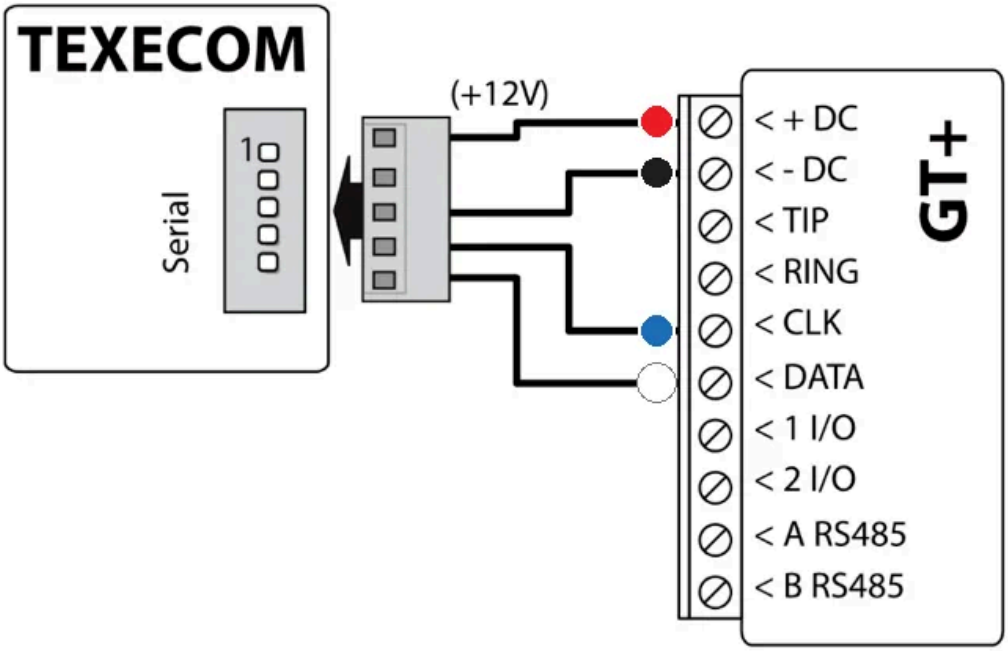


Figure 18. Raccordement d'une centrale Texecom sur le port série avec le câble EX-CRP4 (à commander séparément ; « Use the EX-CRP4 cable (ordered separately) ») : rouge → +DC, noir → −DC, bleu → CLK, blanc → DATA.

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

3.3.7 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 vient du port USB de la centrale, avec le câble Inner Range **993030USB** : **noir → 0V / −DC**, **vert → CLK**, **blanc → DATA**.

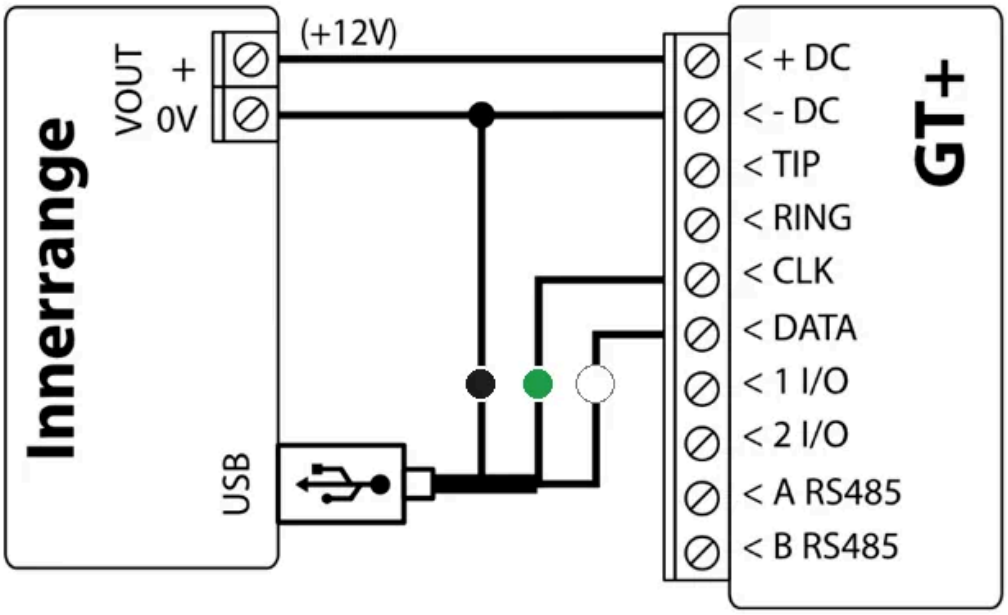


Figure 19. Raccordement d'une centrale InnerRange Inception : VOUT + → +DC, VOUT 0V → −DC ; depuis le port USB avec le câble 993030USB (« Cable, Inner Range part number 993030USB ») noir → −DC, vert → CLK, blanc → DATA.

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

3.3.8 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**.

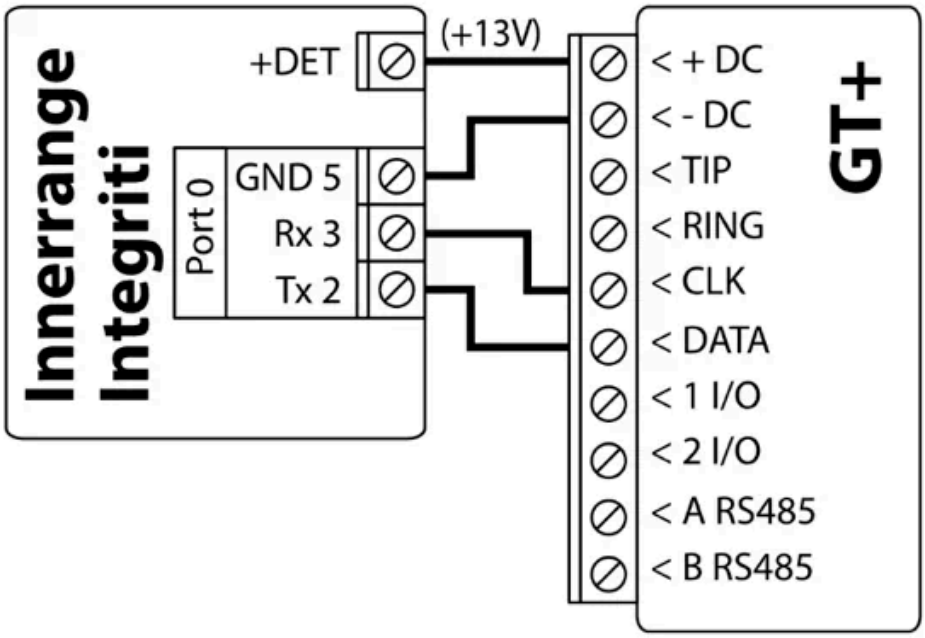


Figure 20. Raccordement d'une centrale InnerRange Integriti au Port 0 avec le câble INTG-996795 (« Cable, Inner Range part number INTG-996795 ») : +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – bus de données

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

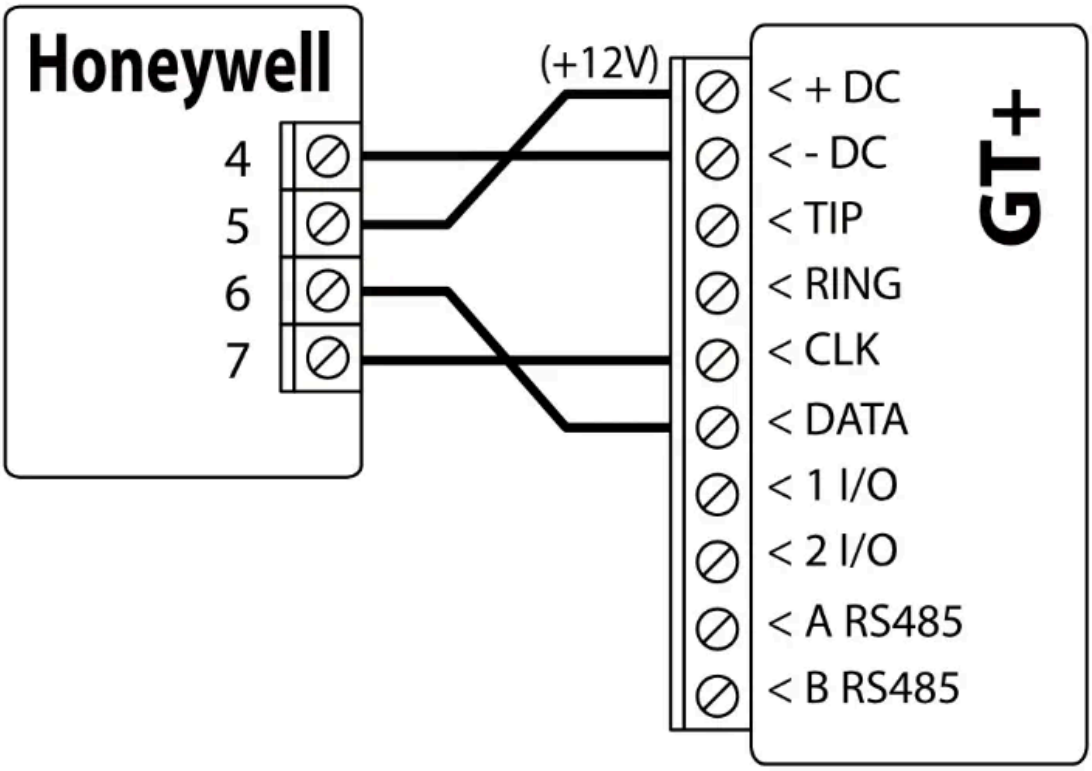


Figure 21. Raccordement d'une centrale Honeywell Vista-15 / -20 / -48 sur le bus de données (« Keypad bus ») : borne 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.10 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).

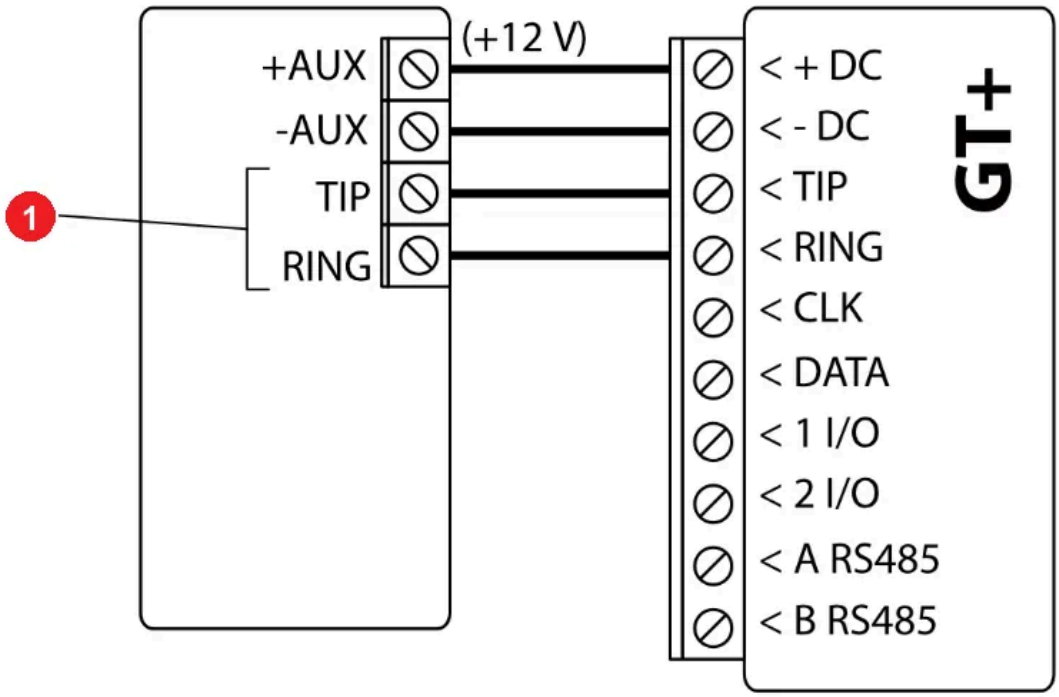


Figure 22. Raccordement sur le transmetteur téléphonique de la centrale (« Control panel ») : +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

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

3.4 Raccordement d'une zone à clé

Si vous voulez armer et désarmer la centrale depuis l'application Protegus 2 de sorte 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 peuvent être réglées en sortie (OUT, PGM) ; les deux sorties peuvent ainsi commander deux partitions du système : raccordez la zone à clé de la partition 1 à la borne **1 I/O**, et celle de la partition 2 à la borne **2 I/O**. Pour ce raccordement, décochez **Remote Arm/Disarm** à la page **Panel settings** de TrikdisConfig, réglez les bornes sur la fonction **OUT** à la page **IN/OUT** (point 6.7), et dans l'application Protegus 2, affectez les sorties aux partitions comme indiqué au point 5.2.

Avec un raccordement par bus de données ou 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 :

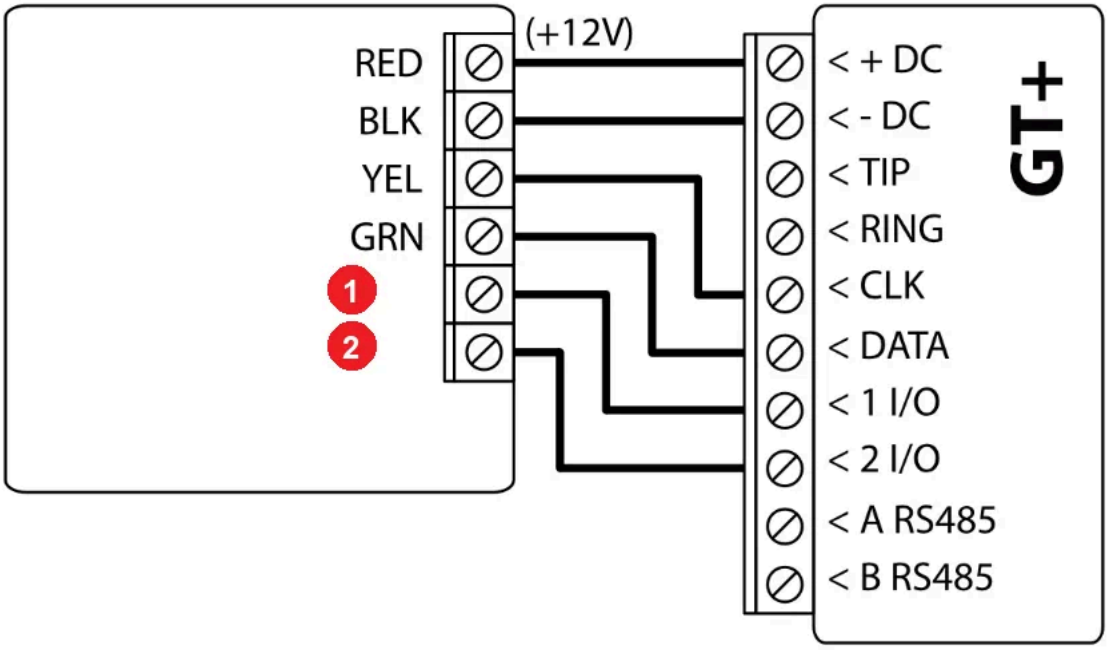


Figure 23. Armement et désarmement par zone à clé (« Zones (keyswitch) »), avec un raccordement par bus de données ou port série (« Keypad bus or serial ») : borne RED de la centrale d'alarme (« Control panel terminals ») → +DC, BLK → −DC, YEL → CLK, GRN → DATA ; zone de la partition 1 → 1 I/O, celle 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, et l'armement et le désarmement se font de la même manière par la zone à clé :

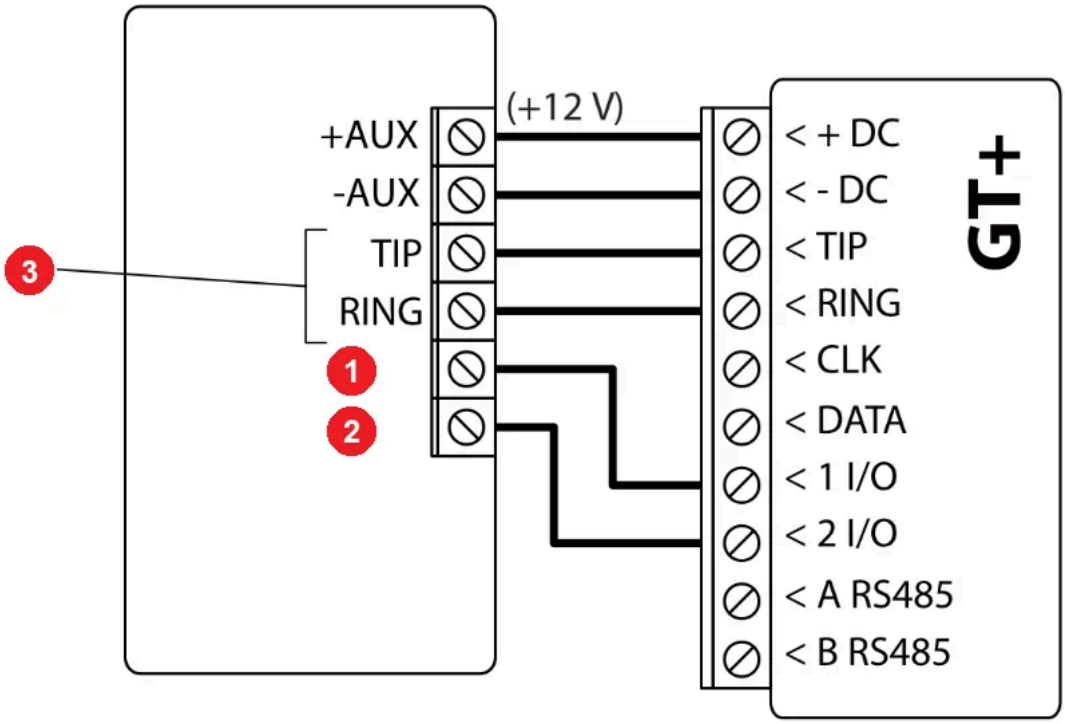


Figure 24. Armement et désarmement par zone à clé (« Zone (keyswitch) »), avec un raccordement par ligne téléphonique : borne +AUX de la centrale d'alarme (« Control panel ») → +DC, −AUX → −DC, TIP → TIP, RING → RING ; zone de la partition 1 → 1 I/O, celle de la partition 2 → 2 I/O.

- 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 bistable – le même mode doit être réglé dans l'application Protegus 2 (point 5.2). Les détails et les pièges de l'armement par zone à clé sont traités dans un article séparé : 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 en entrée (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 sur l'entrée ; le réglage d'usine des deux bornes est entrée, NO. Le type d'entrée se règle à la page **IN/OUT** de TrikdisConfig, dans le champ **Type**. L'entrée se raccorde entre la borne I/O choisie et la borne **−DC** (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	–

Type	État de repos	Alarme	Autoprotection
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.

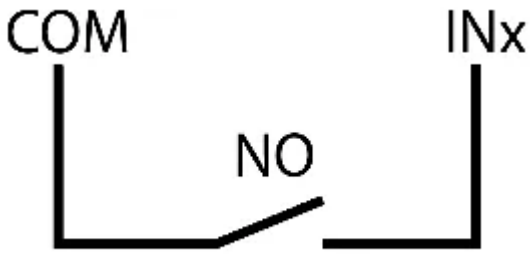


Figure 25. NO – circuit ouvert au repos : fermé – alarme, ouvert – état de repos.

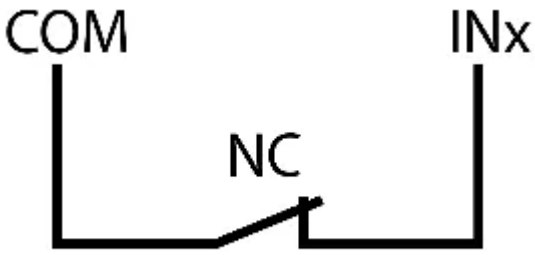


Figure 26. NC – circuit fermé au repos : ouvert – alarme, fermé – état de repos.

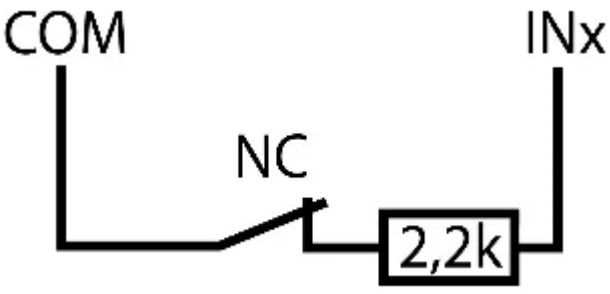


Figure 27. NC/EOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

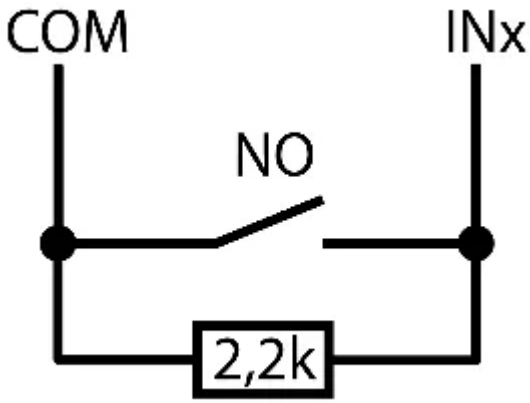


Figure 28. NO/EOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

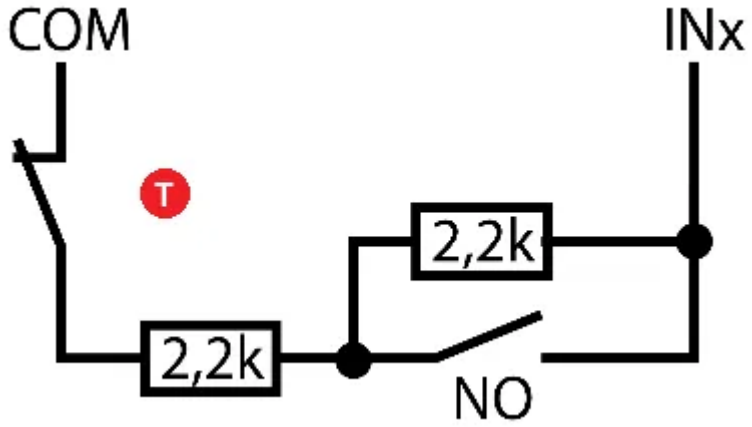


Figure 29. NO/DEOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

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

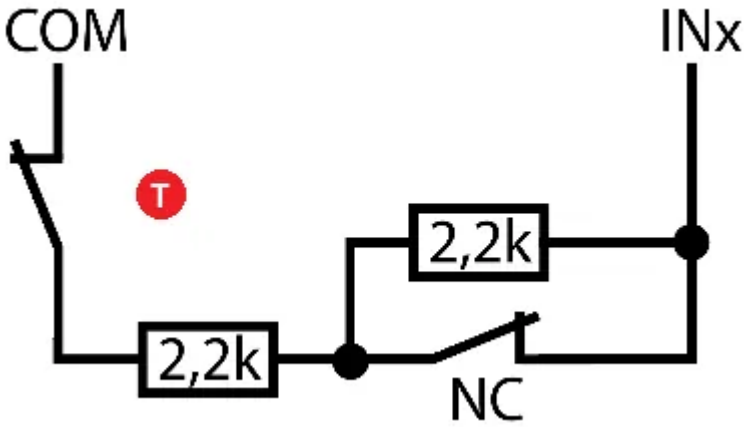


Figure 30. NC/DEOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

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

Si vous avez besoin de davantage d'entrées ou de sorties, raccordez au communicateur un module d'extension Trikdis **iO-8** (point 3.7) ; son raccordement est aussi décrit dans le manuel de l'iO-8.

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 allumer et éteindre différents appareils électriques : une extrémité de la bobine du relais se raccorde 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 réglée en sortie (**OUT**) à la page **IN/OUT** de TrikdisConfig.

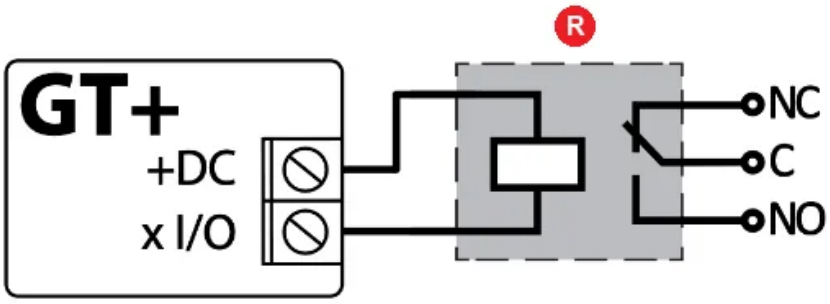


Figure 31. Raccordement d'un relais sur la sortie du communicateur : la bobine se place entre +DC et la borne x I/O, les contacts (NC, C, NO) commutent le consommateur.

- R relais (« Relay »)

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

3.7 Raccordement du module d'extension iO-8

Si vous avez besoin de davantage d'entrées ou de sorties, jusqu'à quatre modules d'extension **iO-8** peuvent être raccordés au bus RS485 du communicateur ; chacun ajoute 8 I/O à double fonction supplémentaires. Reliez les bornes **A 485** et **B 485** aux bornes **A (RS485)** et **B (RS485)** du module ; le communicateur et le module d'extension sont tous deux alimentés par la sortie d'alimentation auxiliaire de la centrale (**+AUX** → **+DC**, **–AUX** → **–DC** sur les deux appareils). Le module d'extension doit être ajouté et configuré à la page **RS485 modules** de TrikdisConfig (point 6.8).

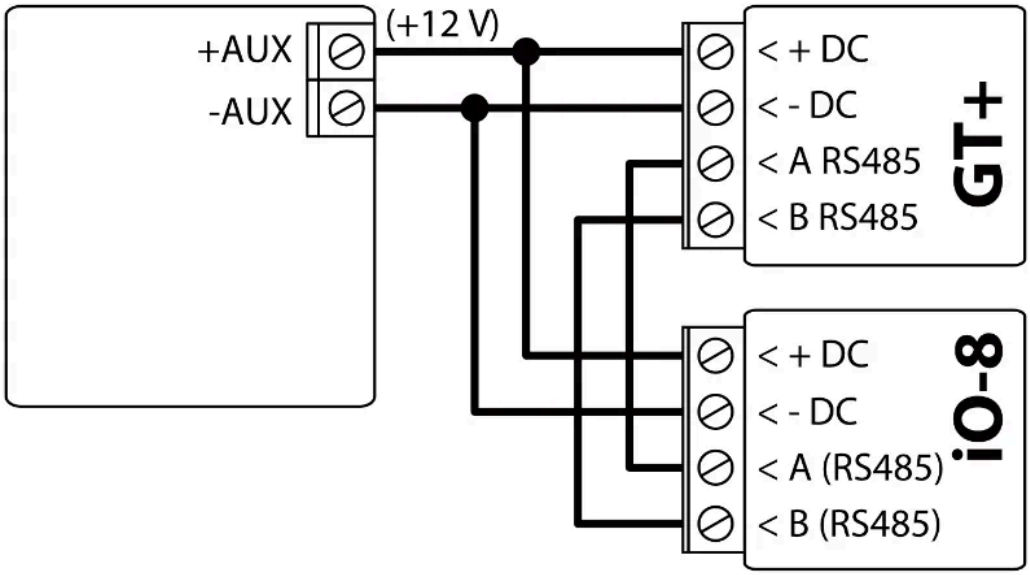


Figure 32. Raccordement du module d'extension iO-8 au bus RS485 du communicateur ; alimentation depuis la sortie AUX de la centrale d'alarme (« Control panel »), pour les deux appareils.

3.8 Mise sous tension et première vérification

A TRIKDIS átjelző elindítása

1. SIM kártyás átjelző esetén a SIM kártyát az elindítás előtt helyezd be a készülékbe.
2. Ethernetes eszköz esetén az Ethernet kábelt elindítás előtt vagy utána is csatlakoztathatod
3. Az indításhoz húzd ki az USB kábelt és csatlakoztasd a lehúzott sorkapcsot

Akkor léphetsz tovább a következő fejezetre, ha az eszköz megfelelően elindul és nem jelez hibát.

- A Power LED zölden világít
- A Trouble LED nem villog pirosan
- A Network LED zölden világít (ha közben sárgán villog az rendben van)
- Ha Data LED nem alszik ki, az azt jelenti, hogy az eszköz nem tud elküldeni valamilyen eseményt. Ez internet / adat kapcsolat hibára utal.

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

- **POWER** verte fixe – l'alimentation est correcte ;
- **NETWORK** verte fixe et clignote en jaune – connecté au réseau ; 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 utilisez une antenne plus sensible (point 3.2) ;
- **TROUBLE** éteinte.

Si la LED TROUBLE clignote, le nombre de clignotements en indique la cause (point 1.6) ; toute autre signalisation des LED indique également 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 manière dont vous l'avez raccordée : sur le bus de données ou le port série (point 4.1), ou sur son transmetteur téléphonique, par les bornes TIP/RING (point 4.2). Sur le GT+, le raccordement DSC Keybus + TIP/RING nécessite les deux : les réglages du raccordement Keybus et la programmation du transmetteur de la centrale (point 4.1.1).

4.1 Raccordement par bus de données ou 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 à la page **Panel settings** de TrikdisConfig (point 2.2).

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.

GT+, raccordement Keybus et TIP/RING (point 3.3.2) : le transmetteur téléphonique de la centrale doit être programmé pour qu'il envoie les événements. Le tableau ci-dessous concerne la centrale DSC PowerSeries PC1616 (PC1832, PC1864). Sur le clavier raccordé à la centrale, entrez en programmation : **[*][8] [code installateur]**, puis saisissez le numéro de la section.

Section	Valeur
[301] Premier numéro de téléphone	N'importe quel numéro de plus de quatre chiffres, **sans D** au début (par exemple `5555555`). Le D signifie l'attente de la tonalité ; sans lui, la centrale numérote plus vite. Le communicateur accepte tous les appels
[310] Identifiant de l'objet du système	L'identifiant de l'objet à 4 chiffres, suivi de `FF` (par exemple `1234FF`). Utilisez le `A` hexadécimal à la place du chiffre 0
[311] Identifiant de l'objet de la partition 1	L'identifiant de l'objet à 4 chiffres ; `A` hexadécimal à la place du 0
[350] Format du transmetteur	`03` (Contact ID) pour le numéro de téléphone 1
[351]–[376] Directions d'appel	Activez pour le numéro de téléphone 1 les groupes d'événements nécessaires : Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Vérifiez séparément le groupe Opening/Closing : sur certaines centrales DSC, il est désactivé d'usine
[380] Option du transmetteur 1	Option 1 **ON** (transmetteur activé) ; option 3 **OFF** (numérotation DTMF)
[381] Option du transmetteur 2	Option 7 **OFF** (la centrale génère automatiquement les codes de rapport Contact ID)

Section	Valeur
[320]–[349] Codes de rapport	Pour les événements à transmettre, n'importe quelle valeur, sauf `00`
[015] Option système 3	Option 7 **OFF** (surveillance de la ligne téléphonique, TLM, désactivée)

Désactivez la surveillance de la ligne téléphonique (TLM) : si elle reste activée, la centrale peut signaler un défaut de ligne téléphonique. Le délai du défaut TLM se règle dans la section **[377]**.

Les numéros de section ci-dessus concernent les centrales PC1616, PC1832 et PC1864 (manuel d'installation v4.x). Sur d'autres types de DSC, les numéros de section peuvent être différents – consultez le manuel de programmation de la centrale.

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 les communicateurs GT et GT+, le champ **Security panel PC download password** se trouve à la page **Panel settings** de TrikdisConfig, dans le groupe **Serial bus** (points 2.2 et 6.3).

Raccordement Keybus et TIP/RING (SP / SP+ / MG / MG+, point 3.3.4) : la centrale doit en outre être programmée pour envoyer les événements au centre de télésurveillance et pour pouvoir être pilotée depuis Protegus 2 :

Section	Valeur	Section	Valeur
801	`********`	**815**	`123456`

Section	Valeur	Section	Valeur
811	`1111`	**911**	`1234`
812	`2222`		

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 les communicateurs GT et GT+, le champ **Security panel PC download password** se trouve à la page **Panel settings** de TrikdisConfig, dans le groupe **Serial bus** ; 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.

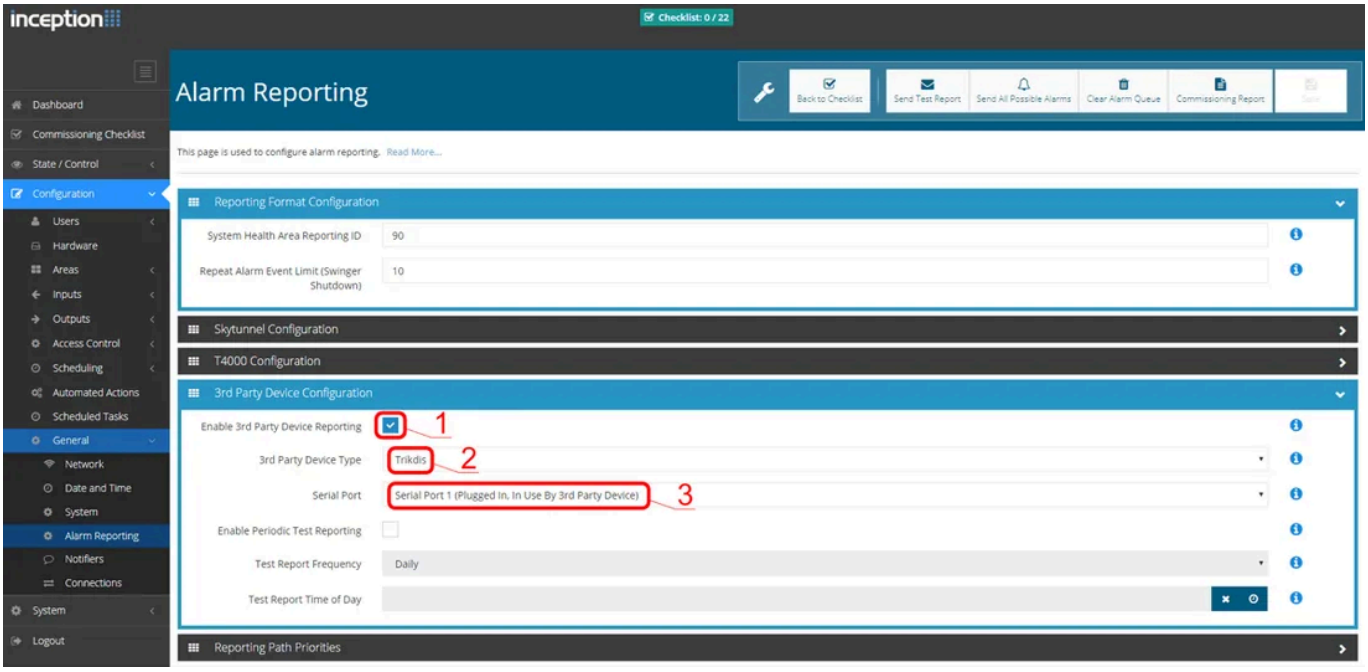


Figure 33. InnerRange Inception – Configuration → General → Alarm Reporting, groupe 3rd Party Device Configuration : Enable 3rd Party Device Reporting coché, 3rd Party Device Type : Trikdis, Serial Port : Serial Port 1.

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 3.3.10) – dans ce cas, c'est aussi leur 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)

Adresse	Réglage
`*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
`*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. Saisissez successivement sur le clavier :

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)

Emplacement (location)	Touches	Remarque
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 des notifications 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 depuis un navigateur : web.protegus.app. Connectez-vous avec votre nom d'utilisateur et votre mot de passe, ou créez un nouveau compte.

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez :

1. La carte SIM est active et la liaison de données mobile y fonctionne ; son code PIN est saisi dans l'appareil, ou la demande de code PIN est désactivée.
2. À la page **User reporting** → **PROTEGUS Cloud** de TrikdisConfig, **Enable connection** est coché (point 6.5).
3. La LED **POWER** est verte fixe.
4. La LED **NETWORK** est verte fixe et clignote en jaune (l'appareil est sur le réseau).

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

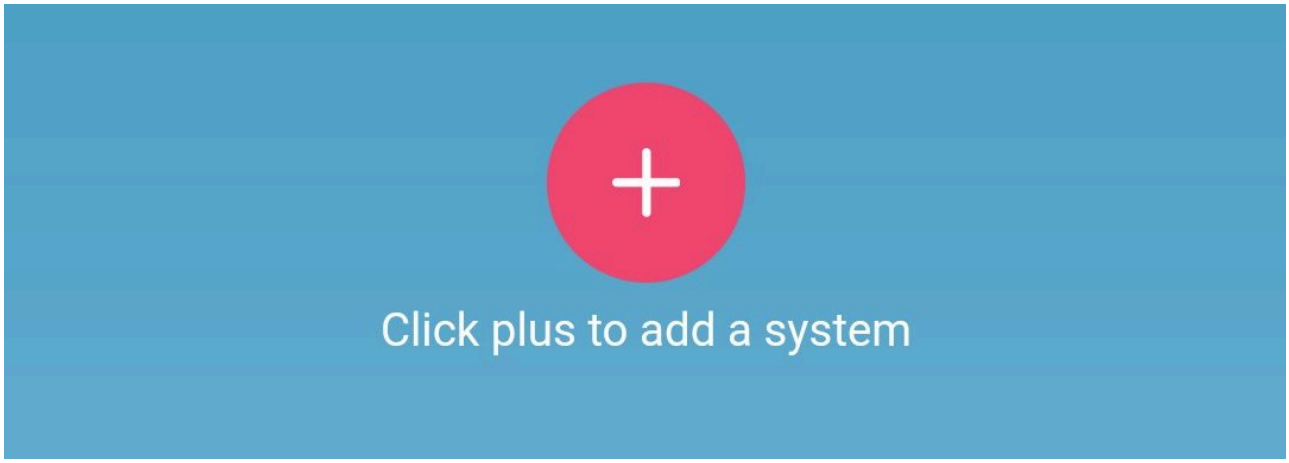








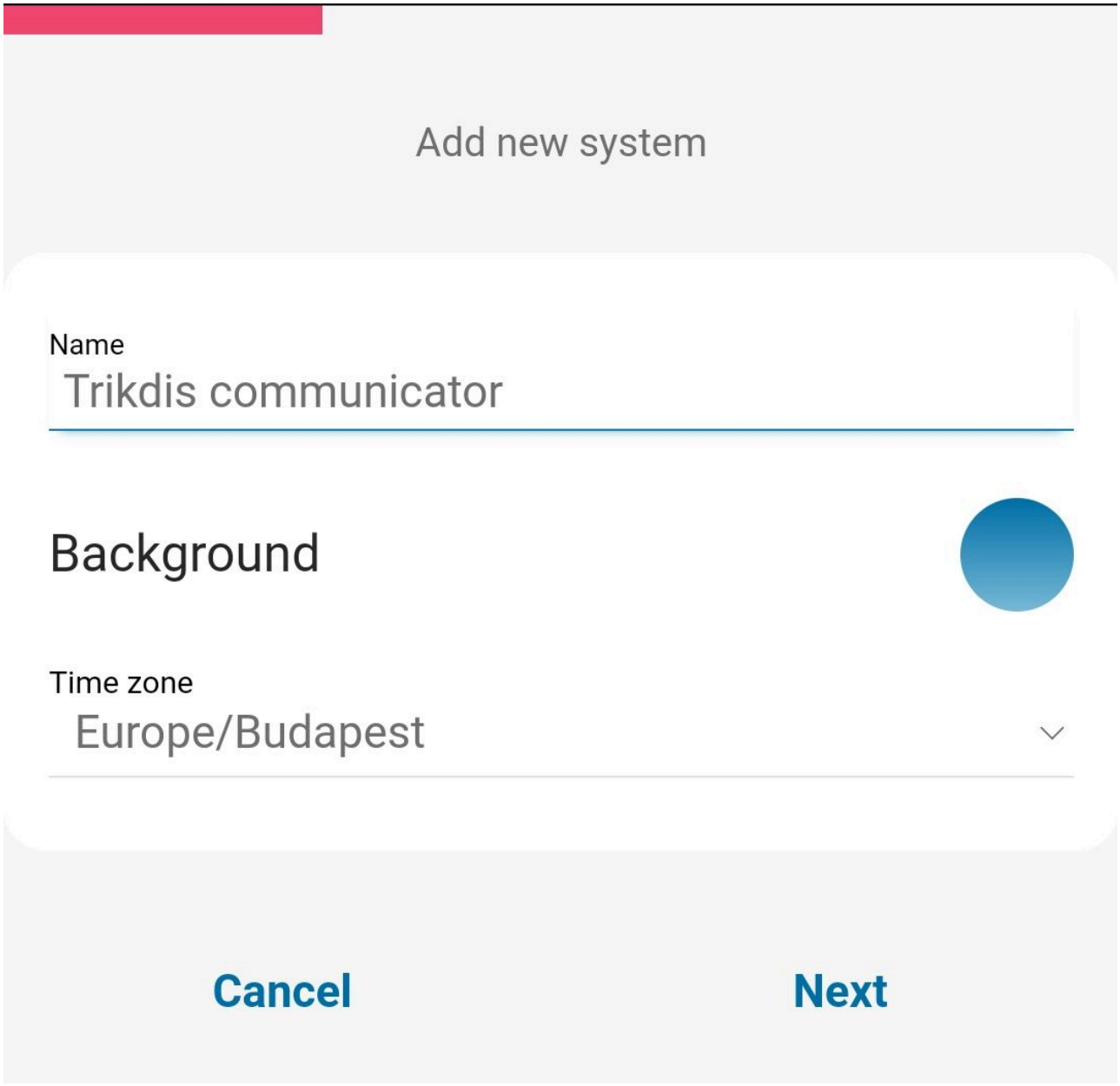
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



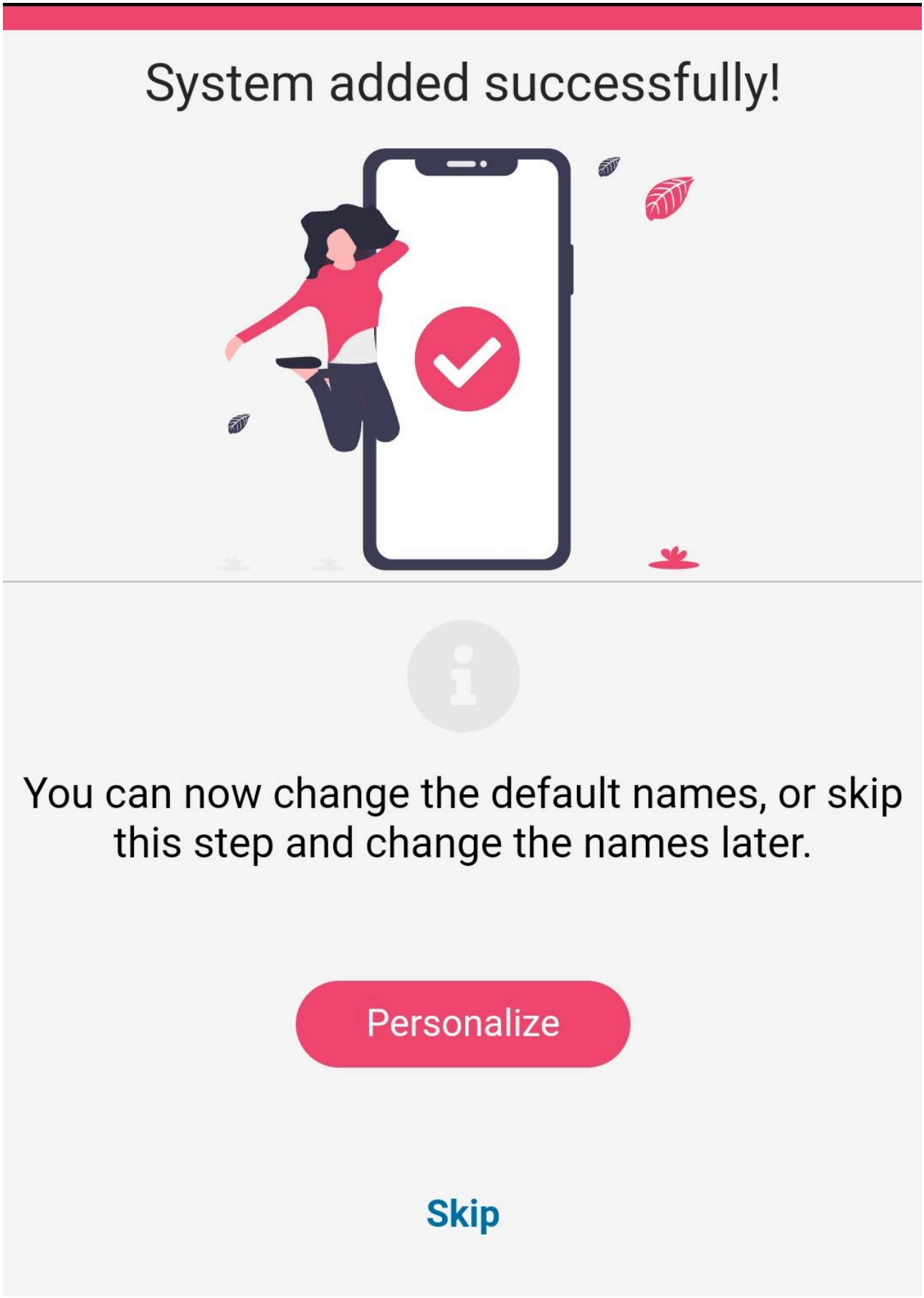
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



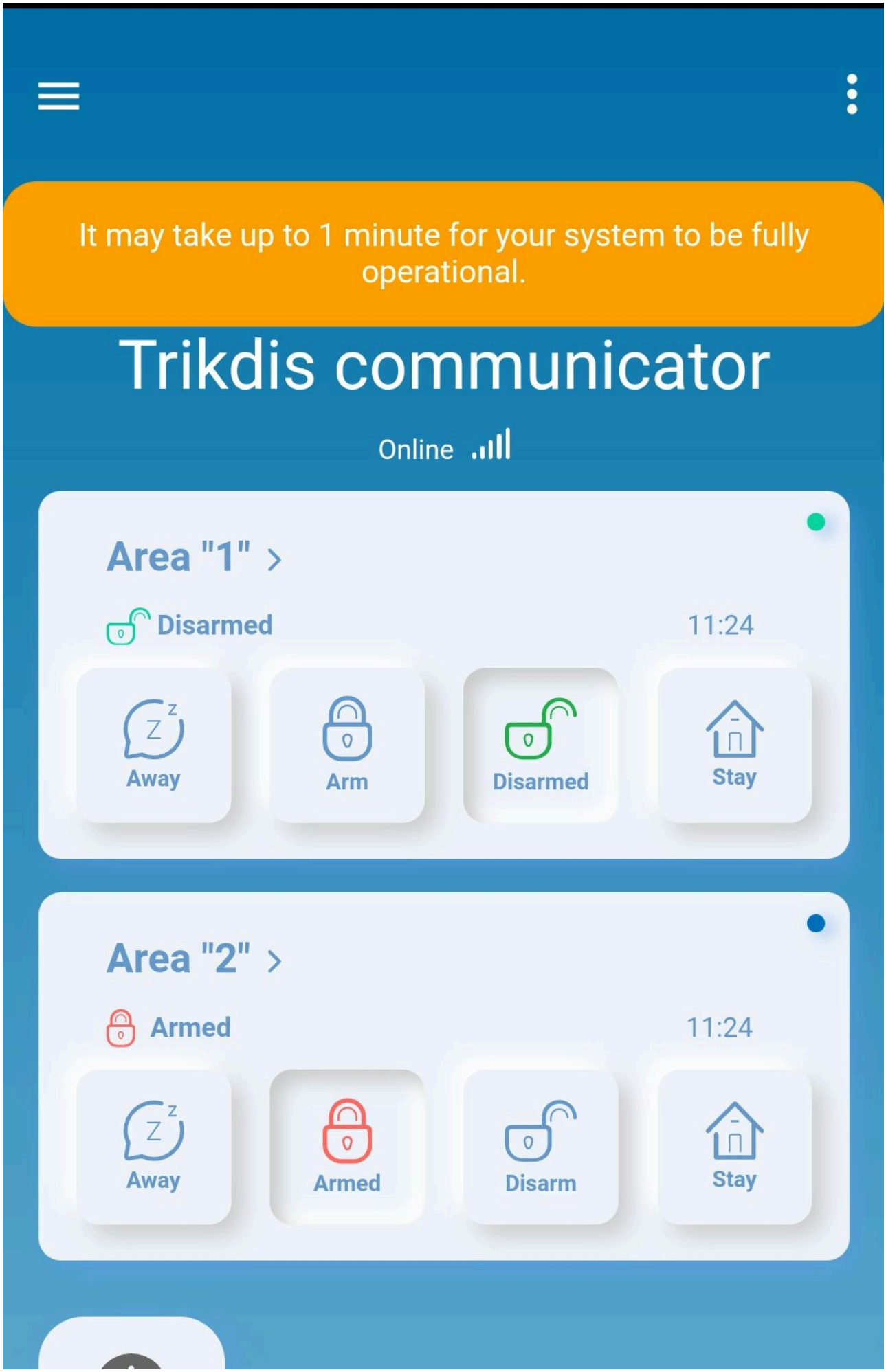
6. Add meg a rendszer nevét és válassz idozónát



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

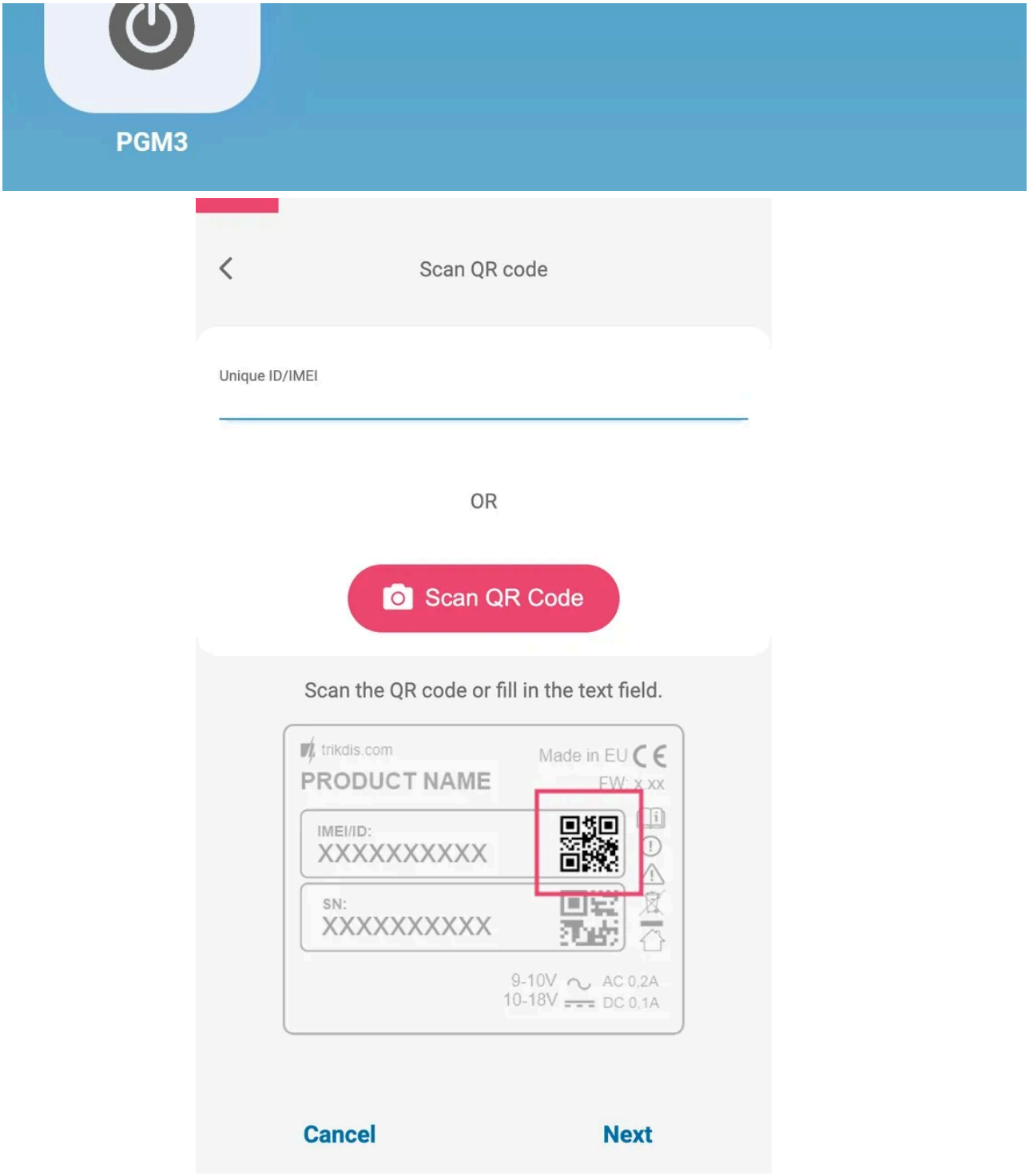


Figure 34. Protegus 2 – ajout d'un nouveau système : saisie de l'IMEI / Unique ID ou lecture du code QR de l'étiquette, puis Next.

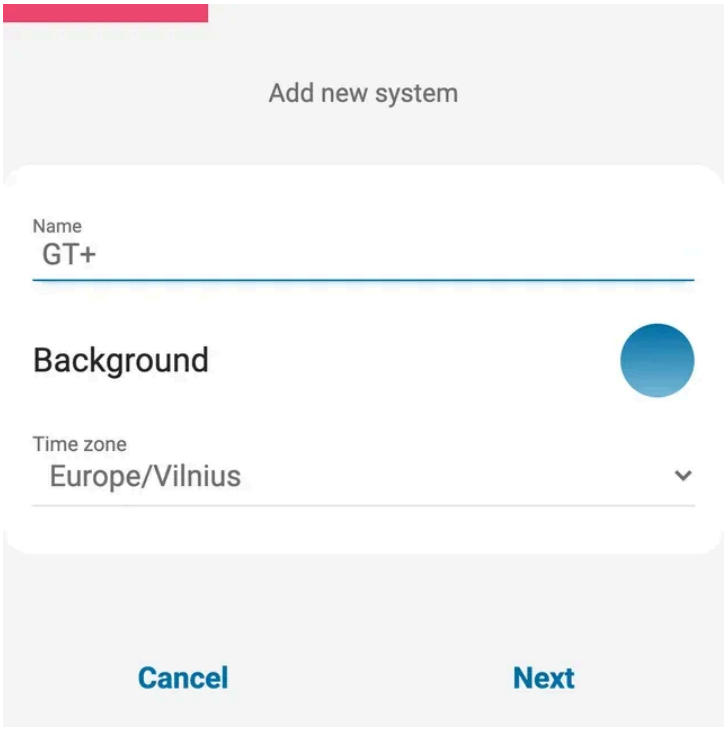


Figure 35. Protegus 2 – saisie du nom du système (Name), puis Next.

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 36. Protegus 2 – 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.

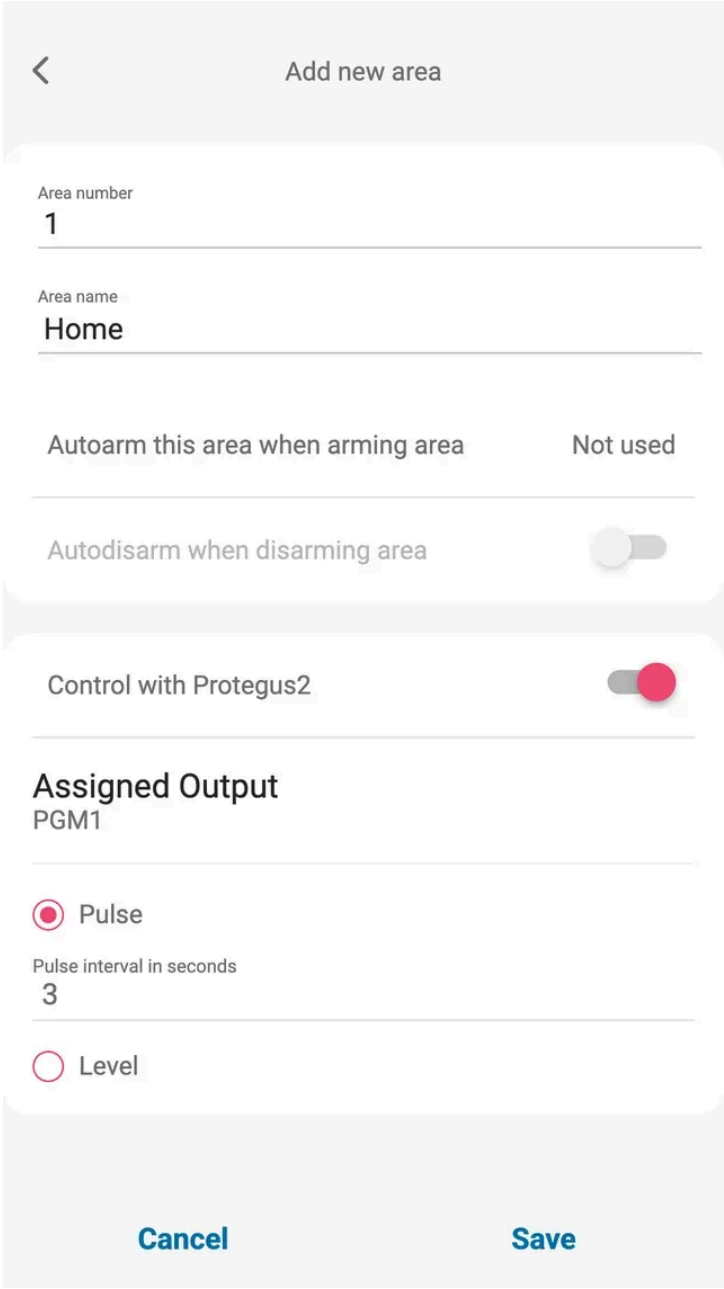


Figure 37. Protegus 2 – ajout d'une partition (Add new area) : Area number, Area name, Control with Protegus2 activé, Assigned Output PGM1, Pulse (3 s) ou Level, puis Save.

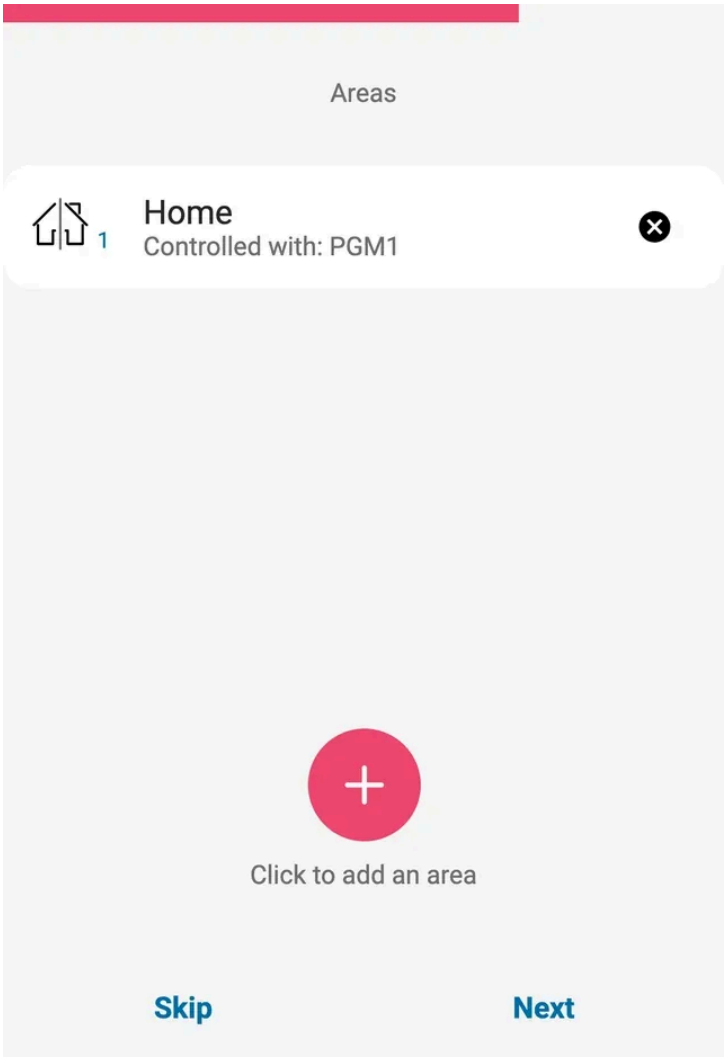


Figure 38. Protegus 2 – la liste des partitions (Areas) : la partition Home est commandée par PGM1 ; une autre partition s'ajoute avec le bouton Click to add an area, l'assistant se ferme avec le bouton Skip.

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.

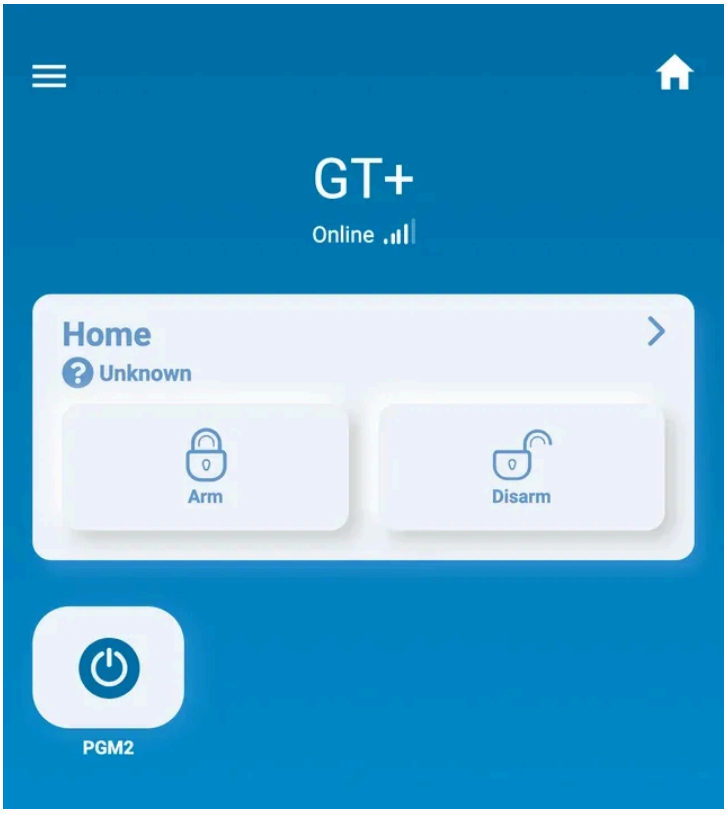


Figure 39. Protegus 2 – l'écran d'accueil du système : l'état de la partition, les boutons Arm et Disarm, et en dessous la sortie PGM commandable.

5.4 Pilotage par SMS

Le communicateur peut aussi être piloté par commandes SMS. Structure du message : `MotDePasse Commande Données` (séparés par des espaces). Comme mot de passe, vous pouvez utiliser le code **administrateur** (`123456` par défaut) pour les commandes `INFO`, `RESET` et `OUTPUTx`, et le code **installateur** (`654321` par défaut) pour les commandes `INFO` et `OUTPUTx`.

Commande	Données	Ce qu'elle fait	Exemple
`INFO`	–	Demande des informations sur l'appareil. La réponse : le type de l'appareil, son numéro IMEI, son numéro de série et sa version de firmware.	`123456 INFO`
`RESET`	–	Redémarre l'appareil (uniquement avec le code administrateur).	`123456 RESET`
`OUTPUTx`	`ON`	Active la sortie x (x = 1 ou 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Désactive la sortie x.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Active la sortie en mode impulsion pendant la durée indiquée ; `tttt` est la durée de l'impulsion en secondes, sur quatre chiffres.	`123456 OUTPUT2 PULSE=0002`

La sortie ne peut être commandée que si la borne I/O concernée est réglée en sortie (**OUT**) à la page **IN/OUT** de TrikdisConfig. Vous pouvez limiter les numéros de téléphone depuis lesquels l'appareil accepte des commandes dans l'onglet **User reporting** → **Control by SMS** (point 6.5).

6. TrikdisConfig – les paramètres en détail

Sur la gauche de la fenêtre de TrikdisConfig se trouve la liste des pages (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, RS485 modules, Event summary, Firmware), en haut la barre de boutons (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), en bas la barre d'état. Ce chapitre passe en revue, page par page, les paramètres du GT et du GT+ ; là où les deux versions diffèrent, nous le signalons séparément.

6.1 La barre d'état

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

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

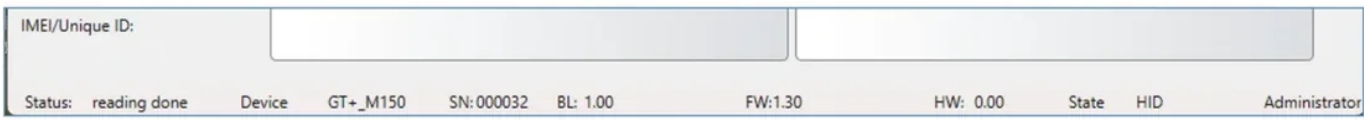


Figure 40. La barre d'état de TrikdisConfig avec un GT+ lu : identifiant, état, type (Device : GT+_M150), numéro de série, versions, mode de connexion et niveau d'accès.

Dans le champ **Device**, le type doit être GT pour le GT et GT+ pour le GT+ (sur l'image GT+_M150 ; le suffixe lettre-chiffre indique la version matérielle). Après **Read [F4]**, le logiciel lit et affiche les valeurs réglées dans l'appareil ; effectuez les réglages nécessaires selon les descriptions de pages ci-dessous.

6.2 System settings

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

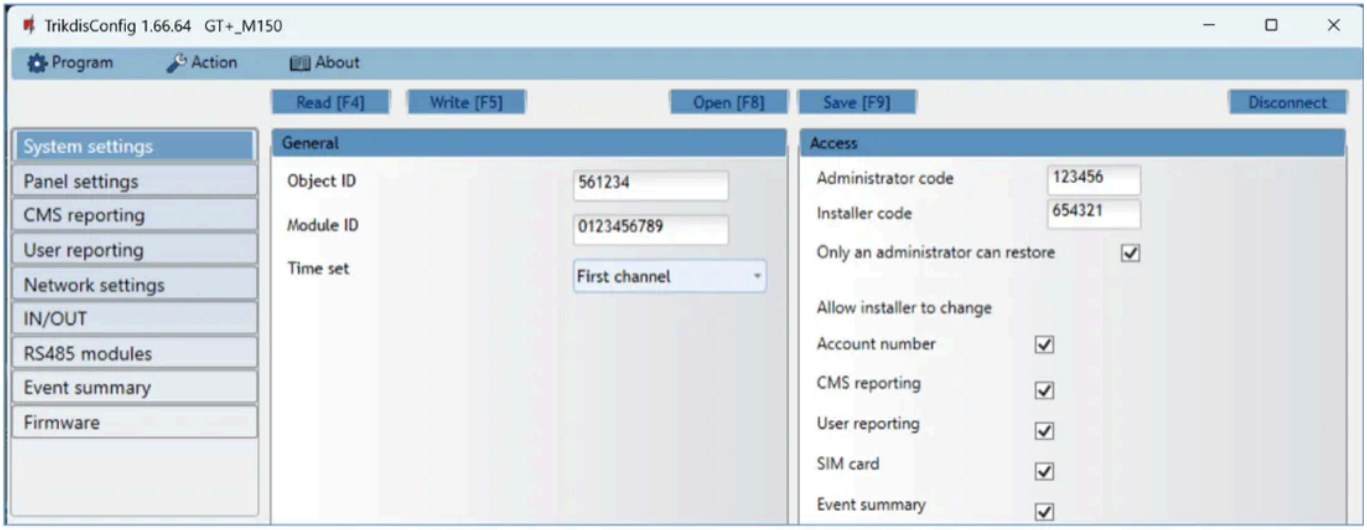


Figure 41. TrikdisConfig – page System settings : groupes General et Access.

- **Object ID** – l'identifiant de l'objet fourni par le 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** – 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.

6.3 Panel settings

Sur cette page, vous indiquez comment le communicateur est raccordé à la centrale d'alarme : le groupe **TLC** contient les réglages du raccordement par ligne téléphonique (TIP/RING), le groupe **Serial bus** ceux du raccordement par bus de données ou port série. On y trouve aussi les réglages communs concernant le traitement des événements de la centrale.

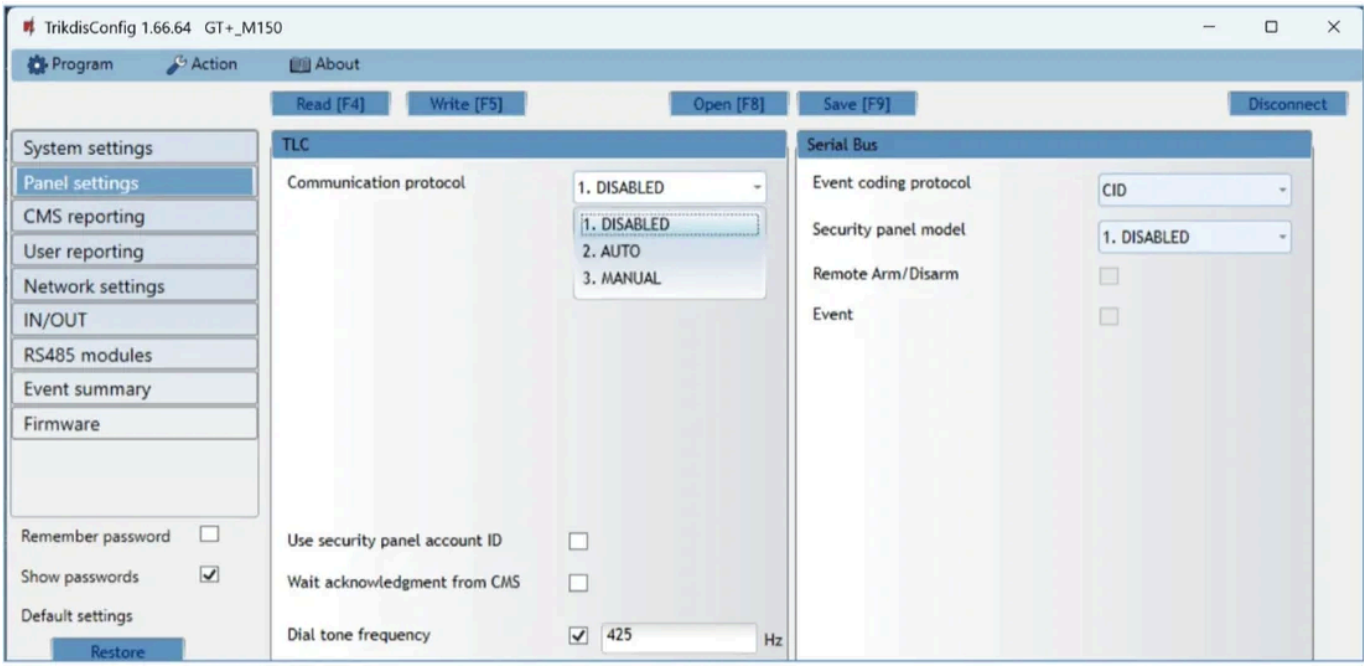


Figure 42. TrikdisConfig – Panel settings sur le GT+ : la liste Communication protocol du groupe TLC (1. DISABLED, 2. AUTO, 3. MANUAL), en dessous le groupe Serial bus et les réglages communs.

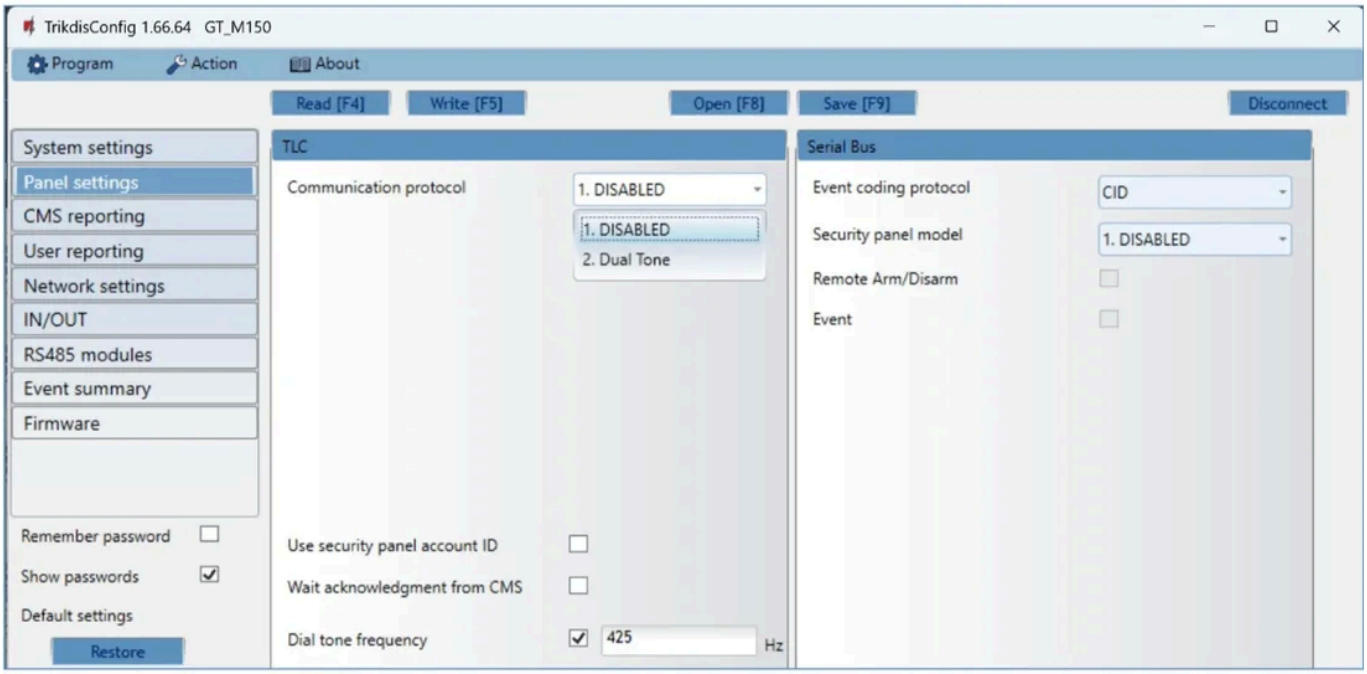


Figure 43. TrikdisConfig – Panel settings sur le GT : la liste Communication protocol propose ici 1. DISABLED et 2. Dual tone.

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

- **Communication protocol** – activation ou désactivation de l'interface ligne téléphonique DTMF du communicateur. GT+ : **1. DISABLED** (désactivé), **2. AUTO**, **3. MANUAL** ; GT : **1. DISABLED**, **2. Dual tone**. Pour un raccordement TIP/RING, choisissez la valeur AUTO (GT : Dual tone).

Réglages situés sous le groupe, valables pour les deux raccordements :

- **Use security panel account ID** – si cette case est cochée, le communicateur n'utilise pas son propre Object ID, mais l'identifiant de l'objet réglé dans la centrale et envoyé par celle-ci.

- **Wait acknowledgment from CMS** – si cette case est cochée, le communicateur attend après chaque événement l'acquittement du récepteur (kiss-off), et seulement ensuite acquitte vers la centrale ; si l'acquittement n'arrive pas à temps, il renvoie le message. Si l'appareil ne transmet pas vers un centre de télésurveillance, laissez cette option désactivée.
- **Dial tone frequency** – la fréquence de la tonalité avec laquelle le communicateur communique avec le transmetteur de la centrale (valeur par défaut 425 Hz, la fréquence de tonalité utilisée dans la plupart des pays européens).



Figure 44. TrikdisConfig – Panel settings, groupe Serial bus : Event coding protocol CID, Security panel model (sur l'image Paradox SP/MG), Remote Arm/Disarm et Event cochés, Security panel PC download password renseigné.

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

- **Event coding protocol** – le protocole de codage des événements (CID).
- **Security panel model** – le type de la centrale d'alarme raccordée, à choisir dans la liste (pour le raccordement Keybus + TIP/RING des Paradox SP / SP+ / MG / MG+, choisissez l'élément **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – si cette case est cochée, 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 chapitre 4.
- **Security panel PC download password** – pour le pilotage direct des centrales Paradox et 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 chapitre 4.

6.4 CMS reporting

Le communicateur envoie les événements au centre de télésurveillance par la liaison de données mobile (IP). 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 coupé. La communication est chiffrée et protégée par mot de passe ; pour la réception et la transmission des événements au logiciel de télésurveillance, il faut un récepteur Trikdis (récepteur logiciel IPcom – Windows ou Linux –, récepteur IP/SMS RL14 ou récepteur multicanal RM14) ou un récepteur universel compatible avec les protocoles DC-09 / TL150. Le GT et le GT+ ne transmettent au centre de télésurveillance que par canal IP ; ils n'ont pas de canal SMS.

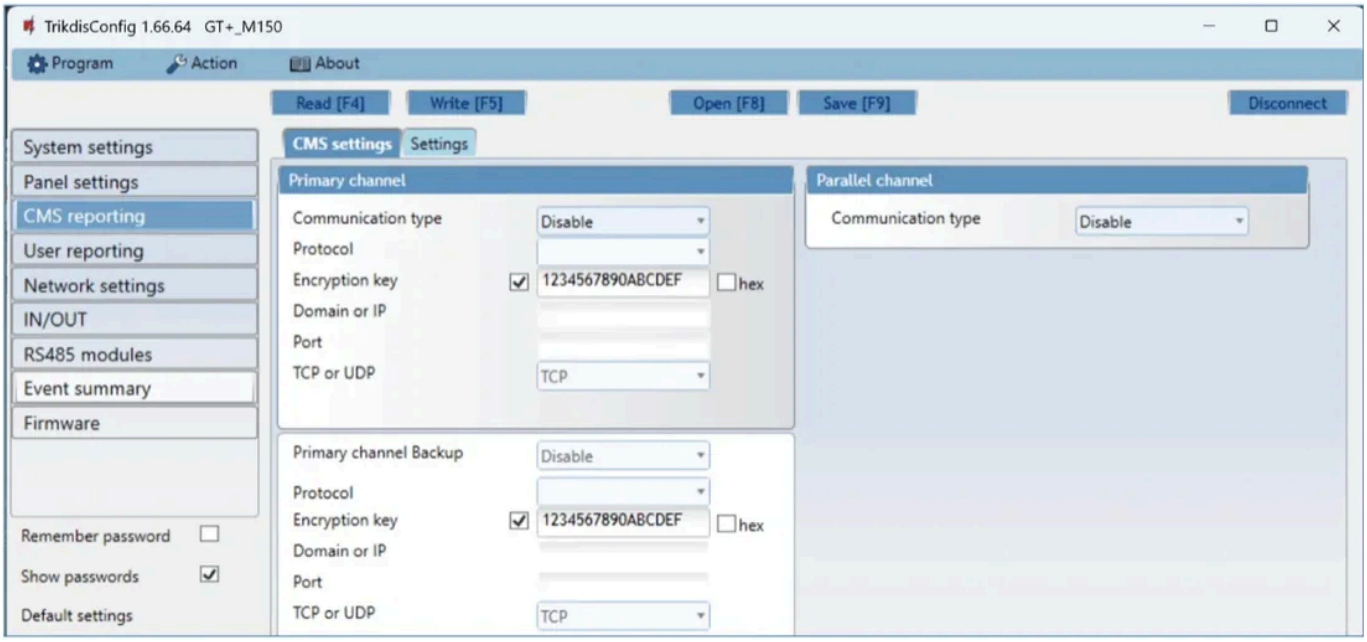


Figure 45. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal, canal de secours et canal parallèle.

Primary channel – canal principal

- **Communication type** – le mode de liaison avec le récepteur : **IP**.
- **Protocol** – **TRK8** (récepteurs Trikdis), **DC-09_2007** ou **DC-09_2012** (récepteurs universels), **TL150** (récepteurs SUR-GARD).
- **Encryption key** – la clé de chiffrement des messages ; elle doit être la même dans le communicateur et dans le récepteur.
- **Domain or IP**, **Port** – le nom de domaine ou l'adresse IP du récepteur et son port.
- **TCP or UDP** – le protocole de transport.

Parallel channel – canal parallèle. En plus du canal principal, il envoie en même temps vers un second récepteur (par exemple vers le centre de télésurveillance local et le centre principal). Ses paramètres sont les mêmes que ceux du canal principal.

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

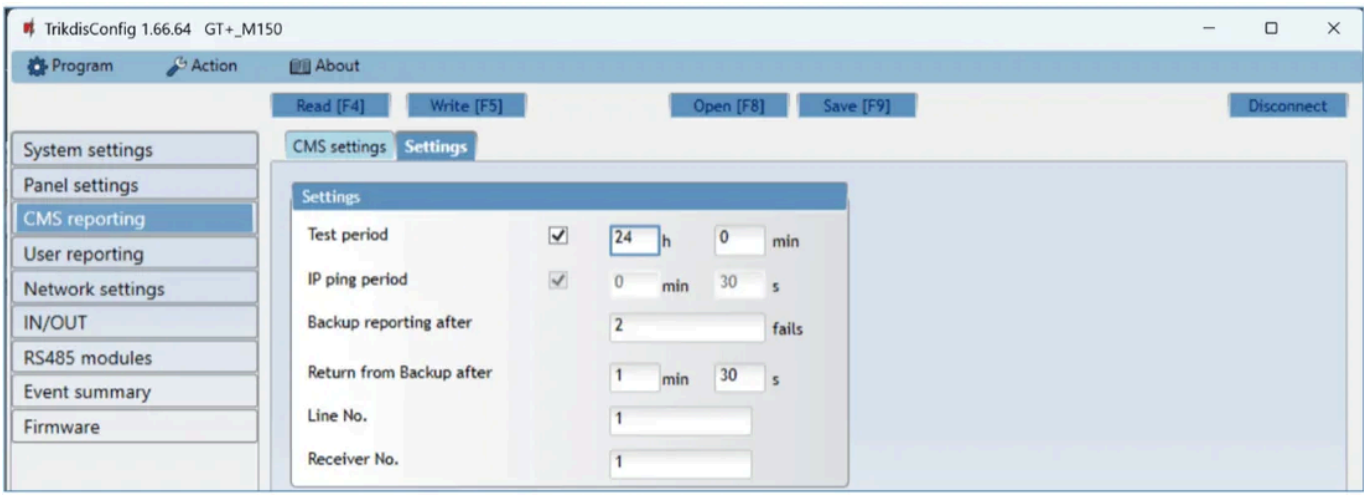


Figure 46. TrikdisConfig – CMS reporting, onglet Settings : rapport de test, PING, temporisations du canal de secours et données DC-09.

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

- **Test period** – intervalle du rapport de test périodique (par défaut 24 heures). Le rapport de test est envoyé sous forme de message Contact ID à la télésurveillance et à Protegus 2.
- **IP ping period** – intervalle du signal de vie (PING) sur le canal IP (par défaut 30 s). Vous l'activez en cochant la case et saisissez la durée dans les champs minutes (**min**) et secondes (**s**) ; il est nécessaire à la supervision de la liaison. Le récepteur ne transmet pas les PING au logiciel de télésurveillance afin de ne pas le surcharger ; le logiciel ne reçoit un message que si le récepteur ne reçoit aucun PING pendant trois fois la durée réglée. Par exemple, avec une période PING de 3 minutes, la perte de liaison est signalée après la 9e minute.
- **Backup reporting after** – nombre de tentatives d'envoi infructueuses après lequel l'appareil bascule sur le canal de secours (par défaut 2).
- **Return from Backup after** – délai après lequel il revient sur le canal principal (par défaut 1 min 30 s).

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

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

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

Dans l'onglet Settings du GT et du GT+, le groupe DC-09 comporte les champs **Line No.** (numéro de ligne) et **Receiver No.** (numéro de récepteur) ; le groupe apparaît si DC-09_2007 ou DC-09_2012 est sélectionné dans le champ **Protocol** de l'un des canaux.

6.5 User reporting

Dans l'onglet **PROTEGUS Cloud**, vous activez le service Protegus, avec lequel l'utilisateur surveille et pilote à distance le communicateur et le système qui y est raccordé ; détails : www.protegus.app.

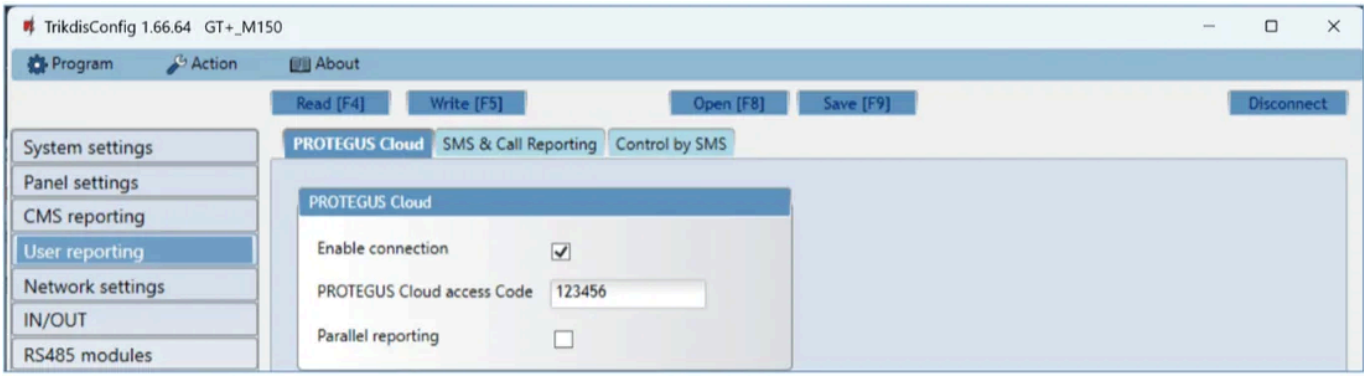


Figure 47. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- **Enable connection** – active le service Protegus : l'appareil échange des données avec l'application Protegus 2, et TrikdisConfig peut aussi y accéder à distance.
- **PROTEGUS Cloud access Code** – code à 6 chiffres pour la connexion à Protegus 2 (`123456` par défaut). Si vous le modifiez dans TrikdisConfig, il faut aussi le changer dans l'application Protegus 2.
- **Parallel reporting** – si cette case est cochée, les messages partent en même temps sur le canal principal (vers le centre de télésurveillance) et vers Protegus 2.

Dans l'onglet **SMS & Call Reporting**, l'utilisateur peut aussi être averti des événements par SMS ou par appel téléphonique.

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

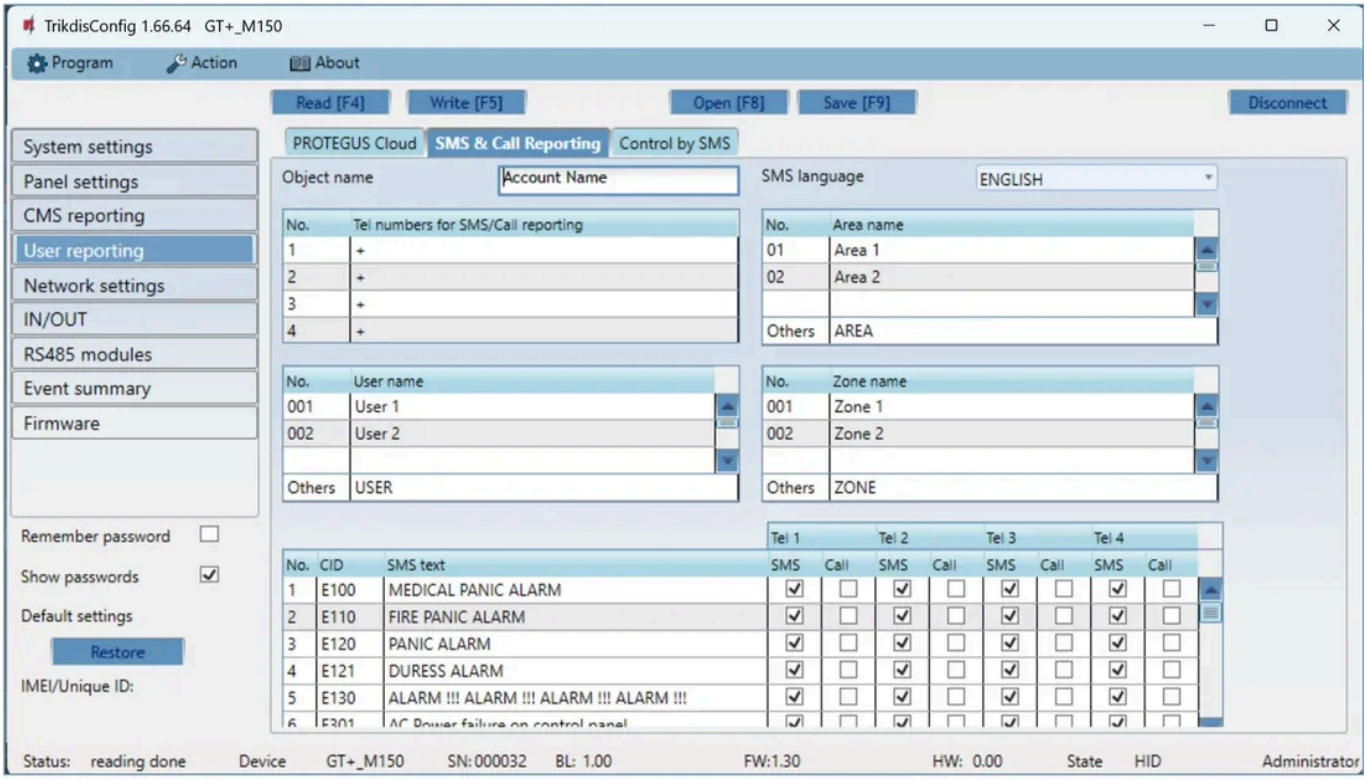


Figure 48. TrikdisConfig – User reporting, onglet SMS & Call Reporting.

- **Object name** – le nom du système ; il figure dans chaque SMS.
- **SMS language** – la langue des SMS (les messages peuvent aussi être envoyés avec les caractères propres à la langue).
- **Tel numbers for SMS/Call reporting** – jusqu'à 4 numéros de téléphone qui reçoivent un SMS ou un appel lors des événements ; saisissez-les avec l'indicatif du pays (par exemple `+33…`, `0033…` ou `33…`).
- **Area name, User name, Zone name** – les noms des partitions, des utilisateurs et des zones ; l'appareil les utilise dans le texte des SMS. Dans le tableau correspondant, saisissez le numéro de la partition, de l'utilisateur ou de la zone, et à côté son nom.
- **CID event table** – pour chaque événement, vous pouvez régler quel numéro reçoit un SMS ou un appel. Le texte SMS et le code Contact ID des événements par défaut peuvent être modifiés, et un nouvel événement peut être ajouté avec sa description.

Dans l'onglet **Control by SMS**, vous réglez la réception des commandes SMS : les commandes permettent de commander les sorties et de demander des informations sur l'appareil (les commandes sont décrites au point 5.4).

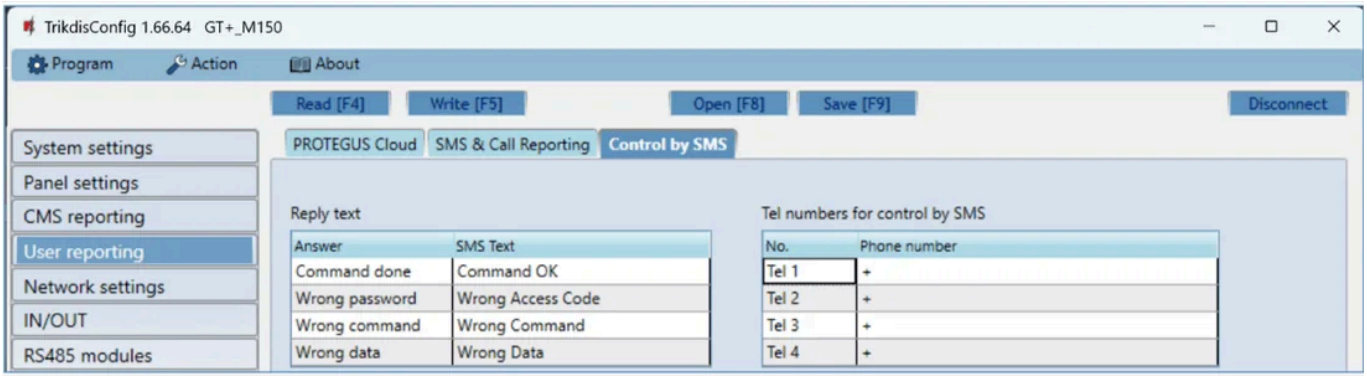


Figure 49. TrikdisConfig – User reporting, onglet Control by SMS.

- **Reply text** – le texte des messages de réponse à une commande SMS : commande réussie (Command done), mot de passe incorrect (Wrong password), commande incorrecte (Wrong command), données incorrectes (Wrong data). Les textes sont modifiables.
- **Tel numbers for control by SMS** – les numéros de téléphone depuis lesquels l'appareil accepte des commandes.

Si aucun numéro de téléphone n'est saisi ici, l'appareil accepte les commandes depuis n'importe quel numéro. La sécurité est alors assurée par le fait que le mot de passe administrateur ou installateur est obligatoire dans la commande.

6.6 Network settings

Avant utilisation, assurez-vous que la carte SIM est active et fonctionne. Si vous envoyez les événements par canal IP ou vers Protegus 2 par l'Internet mobile, le service de données mobiles doit aussi être activé sur la carte.

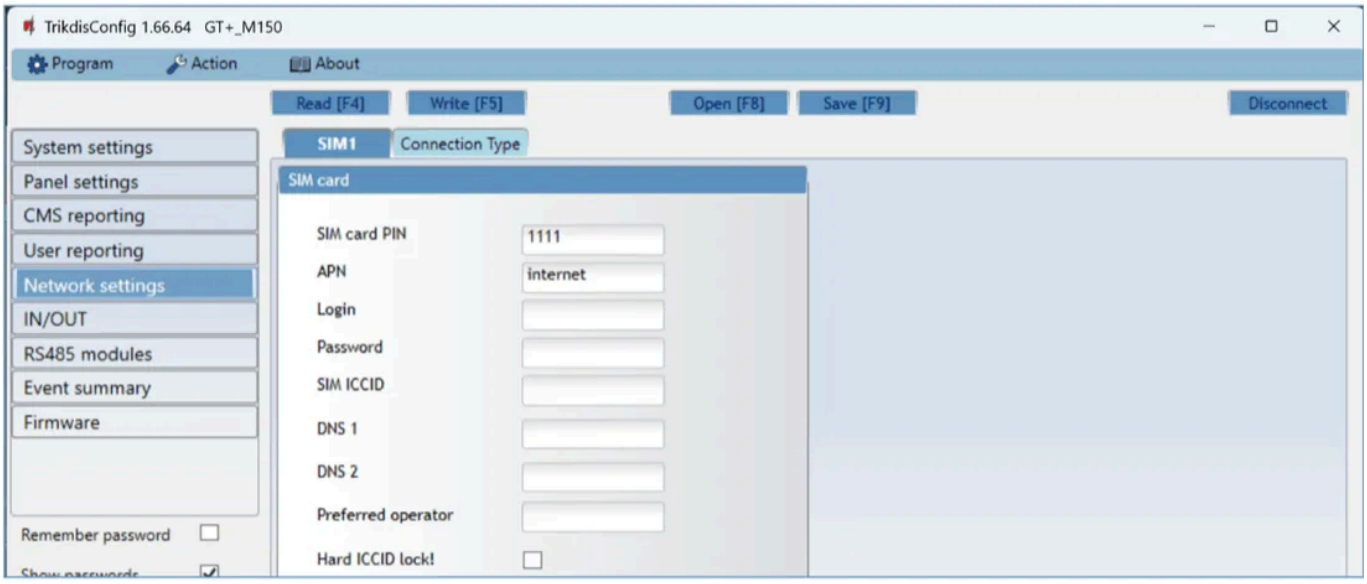


Figure 50. TrikdisConfig – Network settings, onglet SIM1 : les données de la carte SIM.

Onglet SIM1, groupe SIM card

- **SIM card PIN** – le code PIN de la carte. Vous pouvez désactiver la demande de code PIN en plaçant la carte dans un téléphone mobile et en l'y 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. Vous trouverez la valeur 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 listés dans

l'article sur les APN (pour une carte IoT / M2M, l'opérateur fournit un APN distinct, voir le point 2.2).

- **Login, Password** – nom d'utilisateur et mot de passe pour la connexion Internet, si l'opérateur les demande.
- **SIM ICCID** – le numéro ICCID de la carte SIM, si vous voulez que l'appareil ne fonctionne qu'avec cette carte. Si l'ICCID de la carte insérée ne correspond pas, la LED TROUBLE clignote 8 fois (point 1.6).
- **DNS 1, DNS 2** – serveurs de noms (DNS, Domain Name System : il fournit l'adresse IP correspondant au nom de domaine) ; ils sont nécessaires si vous avez saisi le récepteur dans le champ **Domain or IP** par un nom de domaine et non par une adresse IP. Par défaut, le DNS public de Google. Indépendamment des paramètres IP, 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.
- **Hard ICCID lock** – si cette case est cochée, et après le redémarrage de l'appareil, le communicateur est strictement lié à la carte SIM portant le numéro ICCID indiqué.

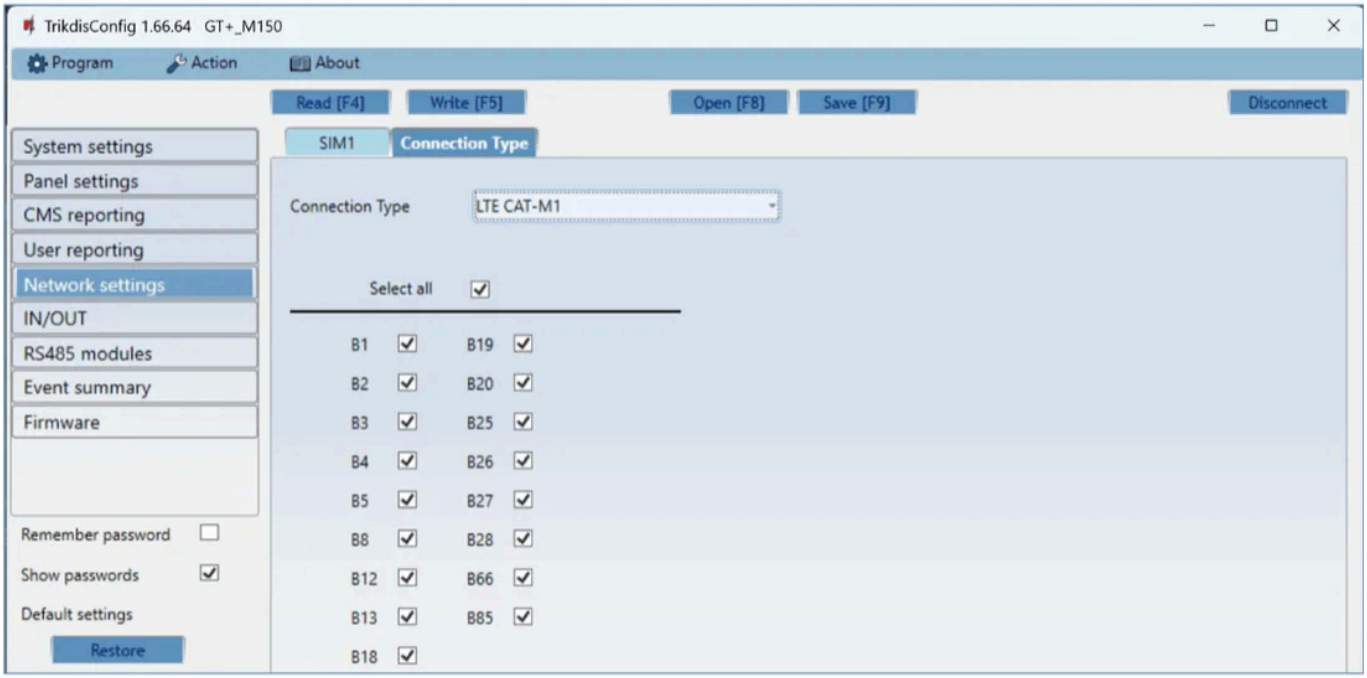


Figure 51. TrikdisConfig – Network settings, onglet Connection Type : sélection des bandes LTE de la version à modem CAT-M1.

Onglet Connection Type – valable uniquement pour la version à modem CAT-M1 (BG95-M5) : vous pouvez y indiquer sur quelles bandes de fréquences LTE le modem de l'appareil doit fonctionner (**Select all** = toutes).

6.7 IN/OUT

Vous indiquez ici le rôle des deux bornes I/O à double fonction du communicateur : **Off** (non utilisée), **IN** (entrée) ou **OUT** (sortie). Pour une entrée, il faut aussi indiquer dans le champ **Type** le type du circuit raccordé (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

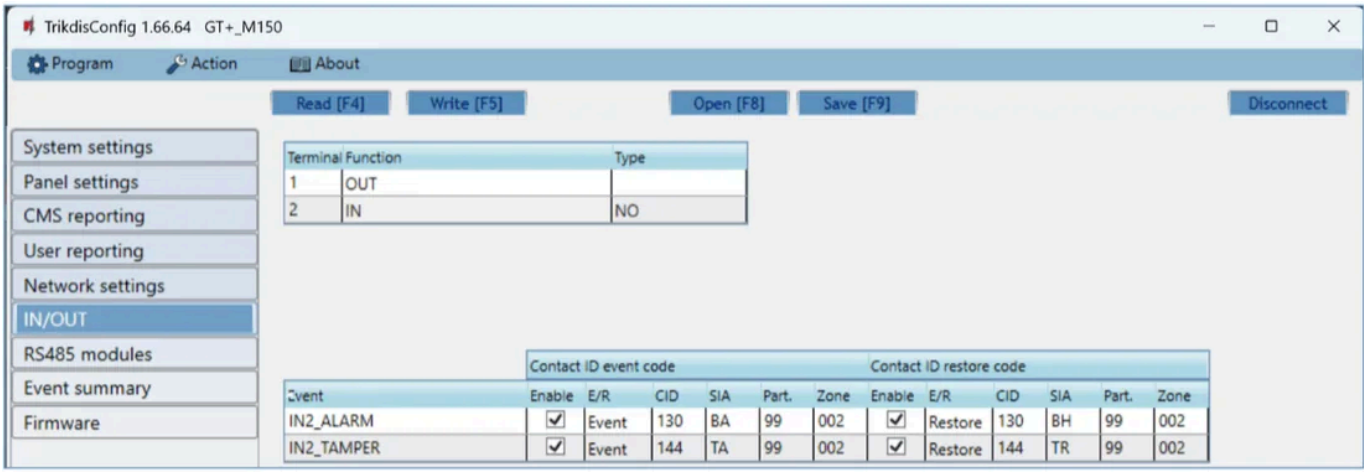


Figure 52. TrikdisConfig – page IN/OUT : la borne 1 en sortie (OUT), la borne 2 en entrée (IN, NO) ; en dessous, les événements d'alarme et d'autoprotection de l'entrée 2 avec leurs codes CID et SIA.

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

- **Enable** – autorise l'envoi du message au centre de télésurveillance et à Protegus 2.
- **E/R** – le type du message : Event (événement) ou Restore (rétablissement).
- **CID** – le code Contact ID (modifiable, ou la valeur d'usine peut rester).
- **SIA** – le code SIA (modifiable, ou la valeur d'usine peut rester).
- **Part.** – le numéro de la partition dans le message.
- **Zone** – le numéro de la zone dans le message.

6.8 RS485 modules

Des modules d'extension **iO-8** raccordés au bus RS485 permettent d'ajouter des entrées et des sorties au communicateur. Les modules d'extension raccordés doivent être ajoutés dans l'onglet **Modules list**.

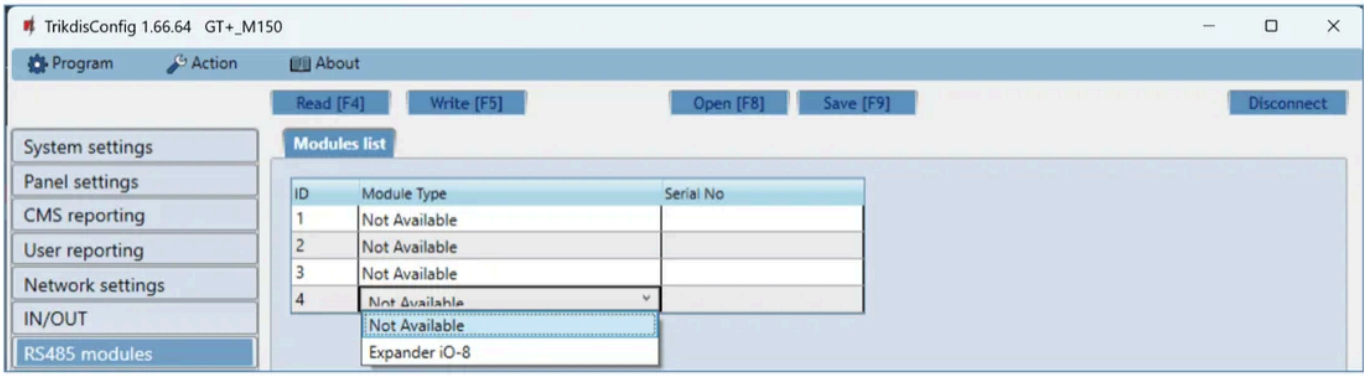


Figure 53. TrikdisConfig – RS485 modules, onglet Modules list : à la 4e position, la liste Module type (Not Available, Expander iO-8).

- **Module type** – le type du module raccordé au bus, à choisir dans la liste (**Expander iO-8**).
- **Serial No** – le numéro de série à 6 chiffres du module (sur le boîtier du module et sur l'autocollant de l'emballage).

Après avoir choisi le module et saisi le numéro de série, passez à l'onglet **RS485 modules** → **Module** : le module ajouté dispose de son propre onglet numéroté (Module 1 …) avec ses paramètres.

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

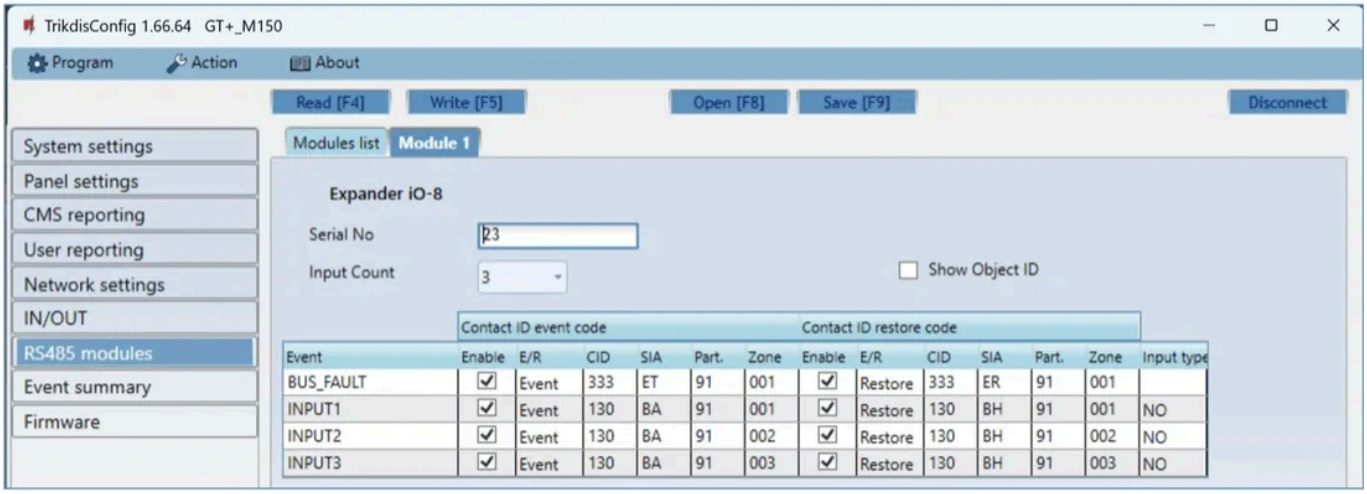


Figure 54. TrikdisConfig – RS485 modules, onglet Module 1 (iO-8) : Input Count, Show Object ID, et les événements BUS_FAULT, INPUT1–INPUT3 avec leurs codes CID et SIA, avec la partition 91.

- **Input Count** – le nombre de bornes en entrée (IN) ; les autres seront des sorties (OUT). Le rôle des sorties (armement / désarmement ou commande d'un équipement) se règle directement dans l'application Protegus 2.
- Dans le tableau, vous pouvez affecter un code d'événement et de rétablissement au défaut du bus (**BUS_FAULT**, Contact ID 333) et aux entrées (**INPUTx**, 130) ; lorsqu'une entrée est déclenchée, le communicateur envoie un événement avec le code réglé au récepteur du centre de télésurveillance et à Protegus 2. Colonnes des lignes d'événement (Contact ID event code) et de rétablissement (Contact ID restore code) : **Enable** (activation), **E/R** (Event ou Restore), **CID** (code Contact ID), **SIA** (code SIA), **Part.** (la partition – elle dépend automatiquement du numéro du module : 91 pour le module 1, 94 pour le module 4), **Zone** (le numéro de la zone).
- **Object ID** – un identifiant d'objet différent de celui du communicateur peut aussi être saisi pour l'entrée (la colonne apparaît quand **Show Object ID** est coché).
- **Input type** – le type de l'entrée : NO, NC ou EOL.

6.9 Event summary

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

Message	Contact ID	Quand est-il généré
COMMUNICATION	350	La communication entre le communicateur et la centrale d'alarme est interrompue (désactivé en usine). Un communicateur raccordé au bus ou au port série la détecte directement ; un communicateur sur ligne téléphonique uniquement si **Line supervision** est activé.
POWER	302	Tension d'alimentation incorrecte (trop basse) ; son rétablissement fait l'objet d'un message distinct.
REMOTE_STARTED	411	Une programmation à distance avec TrikdisConfig a commencé.
REMOTE_FINISHED	412	La programmation à distance est terminée.

Message	Contact ID	Quand est-il généré
START	700	L'appareil s'est connecté au réseau (démarrage).
TEST	602	Rapport de test périodique.
PING	760	Le message de signal de vie PING. Il ne figure pas dans la liste de tous les appareils : il apparaît sur l'écran de l'ancienne version matérielle, mais la page Event summary des versions plus récentes ne comporte pas cette ligne. Son intervalle se règle dans le champ **CMS reporting → Settings → IP ping period**.

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

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

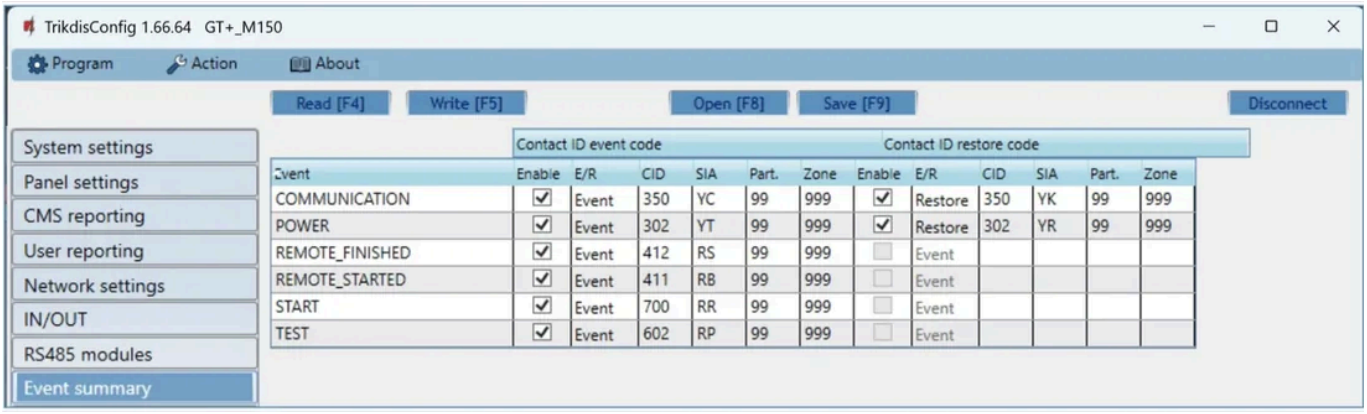


Figure 55. TrikdisConfig – page Event summary : les messages internes de l'appareil avec leurs codes CID et SIA (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

La liste du GT et du GT+ comporte les messages **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** et **TEST**, chacun accompagné aussi de son code SIA. Le message COMMUNICATION signale un défaut de la liaison entre la centrale et le communicateur : avec un raccordement par bus de données ou port série, le communicateur le détecte directement (la LED TROUBLE clignote 7 fois).

6.10 Retour aux paramètres d'usine

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

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



Figure 56. TrikdisConfig – le bouton Restore du groupe Default settings.

Les paramètres d'usine peuvent aussi être rétablis sur l'appareil lui-même, 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 paramètres 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.

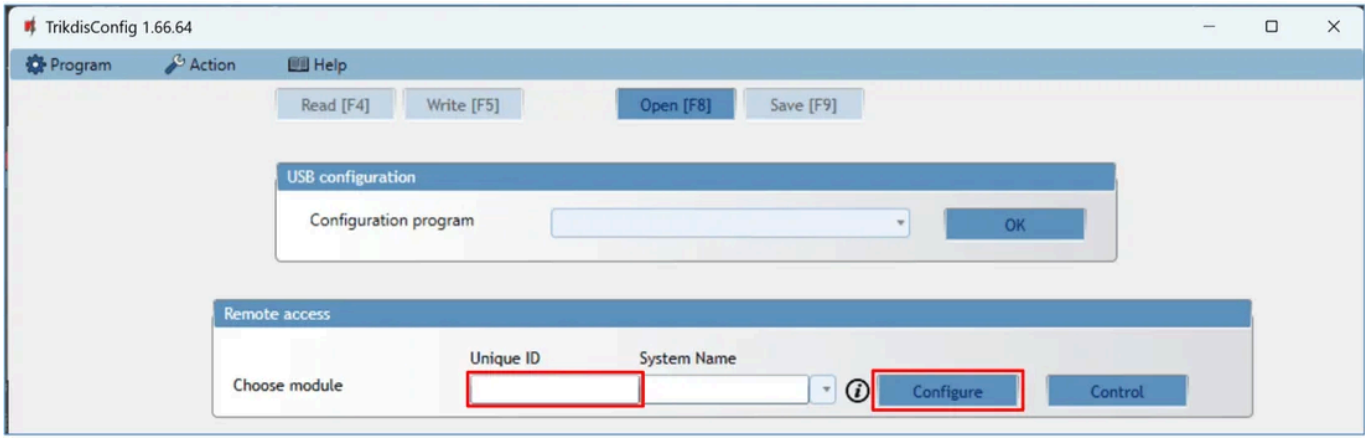


Figure 57. TrikdisConfig – le groupe Remote access : le champ Unique ID, la liste System name et le bouton Configure.

L'identifiant unique du GT et du GT+ est l'**IMEI** ; il figure sur l'étiquette de l'appareil et sur l'autocollant de la boîte. Pour l'accès à distance, la carte SIM doit être active, son code PIN saisi ou la demande de code PIN désactivée ; à la page **User reporting** → **PROTEGUS Cloud**, **Enable connection** doit être coché (point 6.5) ; la LED **POWER** doit être verte fixe, la LED **NETWORK** verte fixe et clignoter en jaune.

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.
6. **Centrale DSC raccordée en Keybus + TIP/RING (GT+).** Armez le système et déclenchez une alarme sur une zone incendie. Le centre de télésurveillance doit recevoir l'événement avec le code Contact ID correspondant au type de la zone (par exemple E110 – alarme incendie), et non comme alarme générale (E130).

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.

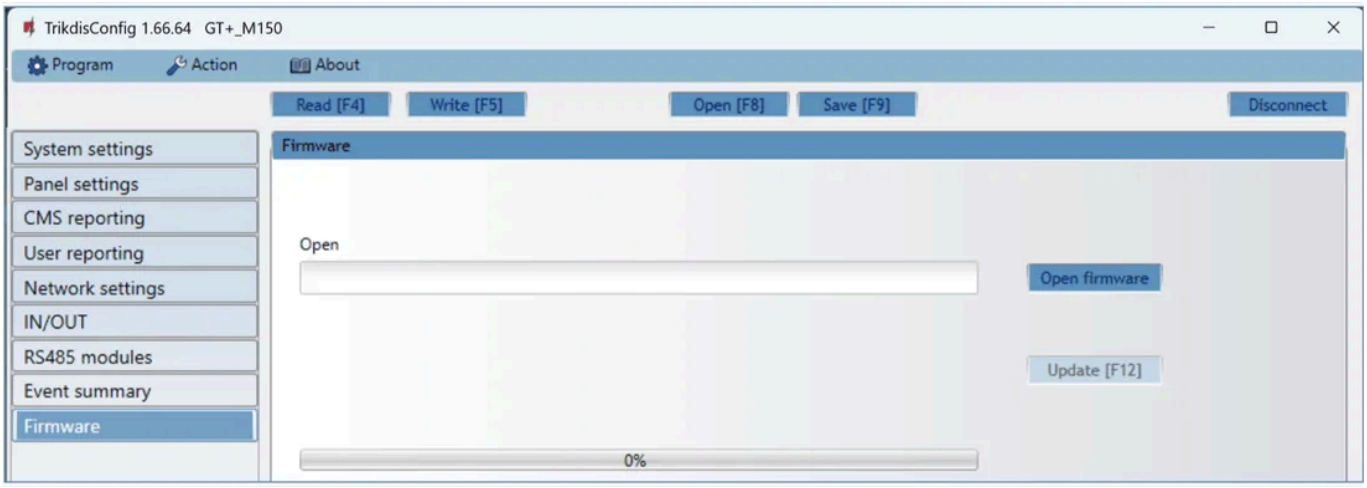


Figure 58. TrikdisConfig – page Firmware : bouton Open firmware, bouton Update [F12] et barre de progression.

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 ; il faut alors modifier les réglages de l'antivirus. Le raccordement Keybus + TIP/RING des Paradox SP / SP+ / MG / MG+ (point 3.3.4) nécessite un firmware 1.21 au minimum.

10. Dépannage et questions fréquentes

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

La LED NETWORK est éteinte – pas de réseau

1. Regardez les clignotements de la LED **TROUBLE** : 1 = pas de SIM, 2 = code PIN incorrect, 3 = pas d'APN, 4 = impossible de s'enregistrer sur le réseau mobile, 5 = impossible de se connecter au réseau de données (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 support.
3. Si la demande de code PIN est activée sur la carte, saisissez le code PIN dans l'onglet **Network settings** → **SIM1**, ou désactivez la demande de code PIN dans un téléphone.

4. Vérifiez l'APN (point 2.2) : pour une carte IoT / M2M, l'opérateur fournit un APN distinct.
5. Vérifiez l'antenne : elle est vissée, elle n'est pas dans un coffret métallique, le niveau de signal est suffisant (la LED NETWORK clignote au moins 3 fois en jaune ; points 1.6 et 3.2).

Le réseau est là, mais le centre de télésurveillance ne reçoit pas d'événements

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

1. 6 clignotements de la LED **TROUBLE** indiquent qu'il n'y a pas de liaison avec le récepteur : vérifiez l'adresse du récepteur, son port, le réglage TCP/UDP, le protocole et la clé de chiffrement (**CMS reporting**).
2. Si le récepteur est saisi par un nom de domaine, vérifiez le réglage DNS (**Network settings** → **SIM1** → **DNS 1, DNS 2**).
3. Vérifiez que le forfait de données de la carte SIM ne bloque pas le port nécessaire (certaines cartes M2M n'autorisent que des adresses déterminées).

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

1. Avec un raccordement par bus de données ou port série, vérifiez les fils CLK et DATA, et que le type de la centrale raccordée est sélectionné dans le champ **Panel settings** → **Security panel model** (point 6.3).
2. Avec une centrale Paradox, vérifiez que le port série n'est pas verrouillé (point 4.1.2) ; avec les centrales Texecom et Paradox, le **Security panel PC download password** doit être identique à celui réglé dans la centrale.
3. Avec 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 AUTO (GT : Dual tone).

La LED TROUBLE clignote 8 fois – ICCID différent

Le numéro saisi dans le champ **Network settings** → **SIM1** → **SIM ICCID** ne correspond pas à l'ICCID de la carte SIM insérée : l'appareil ne fonctionne qu'avec la carte indiquée. Remettez la carte d'origine, ou modifiez (effacez) l'ICCID ; avec **Hard ICCID lock**, redémarrez l'appareil après la modification (point 6.6).

DSC : toutes les alarmes arrivent en E130, alarme générale

Raccordé uniquement au Keybus, le communicateur reçoit de la centrale l'état des zones, mais pas le type de la zone ; il transmet donc chaque alarme avec le code E130 (point 3.3.1). Si le centre de télésurveillance attend le code correspondant au type de la zone (par exemple incendie : E110) : raccordez le **GT+** aux bornes TIP/RING en plus du Keybus, et programmez le transmetteur de la centrale (points 3.3.2 et 4.1.1). Le GT ne permet pas ce double raccordement ; avec lui, les propres codes de la centrale passent par le transmetteur de la centrale, avec un raccordement TIP/RING seul, mais il n'y a alors pas de pilotage direct, et 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 traité 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 3.3.4) ; il ne nécessite pas de déverrouillage, mais le firmware du communicateur doit être au moins en version 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 si la centrale est bien pilotable directement.
2. Pour l'armement par zone à clé (point 3.4), la borne doit être réglée sur **OUT** à la page **IN/OUT**, la zone de la centrale doit être une zone à clé, et dans Protegus 2, la sortie doit être affectée à la partition, dans le même mode que celui de la centrale (à impulsion ou bistable ; 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. À la page **User reporting** → **PROTEGUS Cloud**, **Enable connection** doit être coché.
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, modifiez-le aussi dans l'application.
3. Saisissez l'IMEI exactement, depuis l'étiquette de l'appareil ou l'autocollant de la boîte (ou lisez le code QR).
4. Le service de données de la carte SIM et l'APN doivent être corrects (la LED NETWORK est verte, et la LED DATA s'éteint après un événement).

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

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

J'ai oublié le mot de passe

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 6.10) : appareil sous tension, maintenez-le enfoncé 10 secondes. Tous les paramètres sont effacés.

GT ou GT+ – lequel choisir ?

Le raccordement, la configuration et le fonctionnement des deux versions sont identiques ; les différences sont résumées dans le tableau du point 1.2. Le GT+ fonctionne aussi sur une alimentation de 10–32 V DC (y compris dans les systèmes en 24 V), et il permet aussi le raccordement Keybus + TIP/RING avec les centrales DSC, de sorte que les événements partent avec les propres codes Contact ID de la centrale. Si vous n'en avez pas besoin, le GT fait la même chose.

Quel volume de données l'appareil consomme-t-il ?

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

11. Consignes de sécurité

Figyelem!

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- Seul un installateur qualifié peut installer et entretenir un équipement de sécurité.
- Avant l'installation, lisez 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) apposé 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 sur le 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 – la page du GT et du GT+ contient aussi la table de conversion des codes Contact ID → SIA (annexe). Les manuels de docs.trikdis.com sont en anglais.

Produits associés

Trikdis GT 4G Communicateur Intelligent | **Trikdis GT+ 4G Communicateur Intelligent**

Module Trikdis IO8 Wired Expander

Droits d'auteur

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

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

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