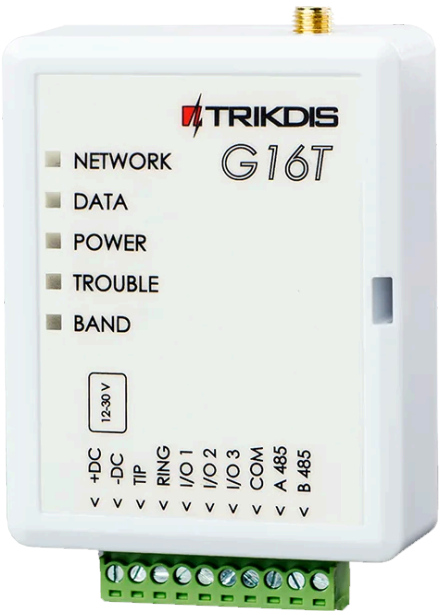
Communicateur G16T – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation du communicateur Trikdis G16T : raccordement à la centrale d'alarme, carte SIM et configuration dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2, vérification et dépannage.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-g16t

Sommaire

1. Présentation

- 1.1 À quoi sert-il, comment fonctionne-t-il ?
- 1.2 Versions
- 1.3 Caractéristiques principales
- 1.4 Composants 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 Connexion à l'application Protegus 2
- 2.3 Connexion au centre de télésurveillance

3. Installation et raccordement

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

4. Programmation de la centrale d'alarme

- 4.1 Programmation du transmetteur Honeywell Vista
- 4.2 Centrales d'autres marques

5. Commande 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 Commande par SMS

6. TrikdisConfig – les réglages en détail

- 6.1 La barre d'état
- 6.2 System settings
- 6.3 CMS reporting
- 6.4 User reporting
- 6.5 SIM card
- 6.6 IN/OUT
- 6.7 RS485 modules
- 6.8 Event summary
- 6.9 Rétablissement des réglages d'usine

7. Programmation à distance

8. Vérification du fonctionnement du communicateur

9. Mise à jour du firmware

10. Dépannage et questions fréquentes

11. Consignes de sécurité

Voir aussi

1. Présentation

Le G16T est le **communicateur universel pour réseau mobile** de Trikdis : il se raccorde à la sortie ligne téléphonique (TIP/RING) de la centrale d'alarme et se comporte comme un central téléphonique. La centrale « compose le numéro » et envoie le message Contact ID en tonalités DTMF ; le G16T prend la ligne, décode le message et le transmet par la connexion de données mobiles au récepteur du centre de télésurveillance ainsi qu'au cloud Protegus, vers l'application de l'utilisateur. Il fonctionne ainsi avec **une centrale de n'importe quelle marque** équipée d'un transmetteur téléphonique Contact ID : inutile de remplacer la centrale, il suffit de configurer son transmetteur. Les communicateurs G16T sont certifiés au niveau de sécurité le plus élevé, **EN 50131 Grade 4**.

1.1 À quoi sert-il, comment fonctionne-t-il ?

- **Transmission vers le centre de télésurveillance.** Il envoie les événements par IP à un récepteur logiciel ou matériel Trikdis (protocole TRK) – ceux-ci fonctionnent avec n'importe quel logiciel de télésurveillance – ou à n'importe quel récepteur universel (SIA DC-09 2007/2012, SUR-GARD TL150). Vers un récepteur SUR-GARD, il convertit les codes Contact ID reçus de la centrale en codes SIA ; la table de conversion figure en annexe de la documentation Trikdis en anglais. Par défaut, il vérifie la connexion toutes les 30 secondes (ou à l'intervalle que vous avez réglé) et bascule sur le canal de secours en cas de défaut.
- **Notification de l'utilisateur.** L'application Protegus 2 signale ce qui s'est passé par notification push, avec un son distinct, et dans la liste des événements ; depuis l'application, l'utilisateur peut armer et désarmer, et commander les équipements raccordés (éclairage, portail, ventilation, chauffage, arrosage, etc.). L'application fonctionne avec toute centrale d'alarme à laquelle le communicateur est raccordé, quelle qu'en soit la marque.
- **Ensemble ou séparément** avec le centre de télésurveillance et avec l'utilisateur : il peut être utilisé uniquement avec Protegus 2 (sans télésurveillance), uniquement avec la télésurveillance, ou avec les deux. Si les deux sont configurés, l'événement est d'abord envoyé au centre de télésurveillance, puis à l'utilisateur.
- **Secours par SMS.** Il informe aussi le centre de télésurveillance par SMS si la connexion de données ne fonctionne pas dans le réseau de l'opérateur ; il peut envoyer en parallèle à deux récepteurs, chacun avec son propre canal de secours.
- **Ses propres entrées et sorties.** Trois bornes I/O à double fonction peuvent servir d'entrées (détecteur, autoprotection) ou de sorties commandables (zone à clé, relais). Sur le bus RS485 de la version 4G, un module d'extension iO-8 ajoute 8 I/O supplémentaires (d'autres modules filaires ou sans fil de la série iO ajoutent d'autres entrées et sorties, un module iO ou iO-WL permet la surveillance de température à distance) ; avec un module W485 ou E485, il peut aussi communiquer par WiFi ou par Internet filaire – le réseau mobile devient alors la voie de secours.

La figure ci-dessous montre l'architecture du système : la sortie ligne téléphonique de la centrale d'alarme est raccordée au G16T, le G16T accède à Internet par le réseau mobile, et de là au récepteur du centre de télésurveillance et au cloud Protegus ; l'utilisateur voit le système dans l'application Protegus 2.

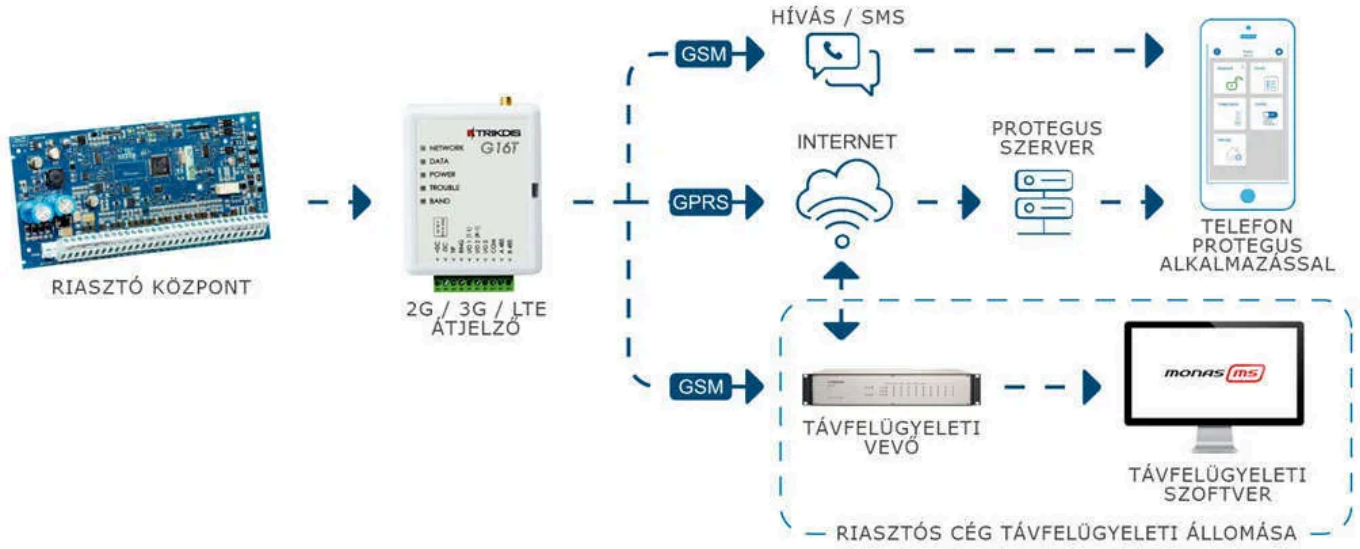


Figure 1. La place du G16T dans le système : centrale d'alarme → G16T → réseau mobile → récepteur du centre de télésurveillance et cloud Protegus → application Protegus 2.

1.2 Versions

Ce manuel est rédigé pour la **version matérielle 4** du G16T, mais il **s'applique aussi à la version matérielle 3** : le raccordement, la configuration et le fonctionnement des deux versions sont en grande partie identiques. Le tableau ci-dessous résume les différences ; lorsque le texte donne une valeur de la version 4, tenez compte de ce tableau pour la version 3.

	Matériel 3 (v3)	**Matériel 4 (v4)**
Types	G16T_321x (2G), G16T_331x (3G), G16T_341x (4G), G16T_3M10 (LTE Cat-M1 + 2G) – tous avec 1 carte SIM	G16T_G410 (2G), G16T_E120 (4G, avec repli 2G)
Entrées / sorties	2 entrées de type sélectionnable (T-1/IN1, R-1/IN2 – utilisables aussi pour la supervision de la ligne téléphonique) + 1 sortie à collecteur ouvert (OUT, max. 0,15 A)	3 bornes I/O à double fonction (I/O 1, I/O 2, I/O 3), chacune utilisable comme entrée ou comme sortie à collecteur ouvert (max. 0,15 A)
Consommation	60–100 mA ; jusqu'à 250 mA pendant l'émission	60–100 mA ; jusqu'à 500 mA pendant l'émission
Fréquences du modem	2G : 850 / 900 / 1800 / 1900 MHz ; 3G : 800 / 850 / 900 / 1900 / 2100 MHz ; 4G : selon la région	2G : 850 / 900 / 1800 / 1900 MHz ; 4G : selon la région
Dimensions	92 × 62 × 26 mm	92 × 65 × 26 mm
Bus RS485 (iO-8, W485, E485)	oui	uniquement sur la version 4G (G16T_E120)

La version matérielle 4 existe avec deux modems :

Type	**Modem**	**Fréquences**	**RS485 (iO-8, W485, E485)**
G16T_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	non
G16T_E120	4G (LTE), avec repli 2G	selon la région	oui

La version matérielle est indiquée dans la barre d'état de TrikdisConfig (**HW**) et sur l'étiquette au dos de l'appareil.

1.3 Caractéristiques principales

Liaison avec la centrale d'alarme

- Raccordement normal à la sortie ligne téléphonique de la centrale : DC+, DC−, TIP et RING. Si nécessaire, il peut aussi être raccordé avec supervision de ligne (avec les fils T-1 et R-1) : la liaison entre la centrale et le communicateur est alors **supervisée**, le communicateur signale la coupure du câble.
- La centrale envoie les événements au format Contact ID, en numérotation DTMF ; le G16T transmet l'information complète de l'événement (code, partition, zone ou utilisateur).

Communication avec le centre de télésurveillance

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

Fonctions utilisateur

- Application mobile et web Protegus 2 : notification push avec un son distinct, liste des événements, armement et désarmement, commande des sorties.
- Surveillance de température à distance (avec un module iO ou iO-WL).
- Commande et configuration de base également par commandes SMS.
- Notification également par SMS et par appel téléphonique, vers 4 numéros de téléphone au maximum.
- Droits utilisateur à plusieurs niveaux dans l'application (administrateur, installateur, utilisateur).

Installation et configuration

- Les réglages peuvent être enregistrés dans un fichier et chargés dans un autre communicateur.
- Deux niveaux d'accès : administrateur (celui du centre de télésurveillance) et installateur.
- Configuration et mise à jour à distance avec le logiciel TrikdisConfig.

1.4 Composants du communicateur

Le circuit imprimé du G16T est logé dans un boîtier en plastique blanc ; la face avant est amovible et le bornier est débrochable. La figure ci-dessous montre la version 4G ; la version 2G n'a ni LED BAND ni bornes A 485 / B 485.

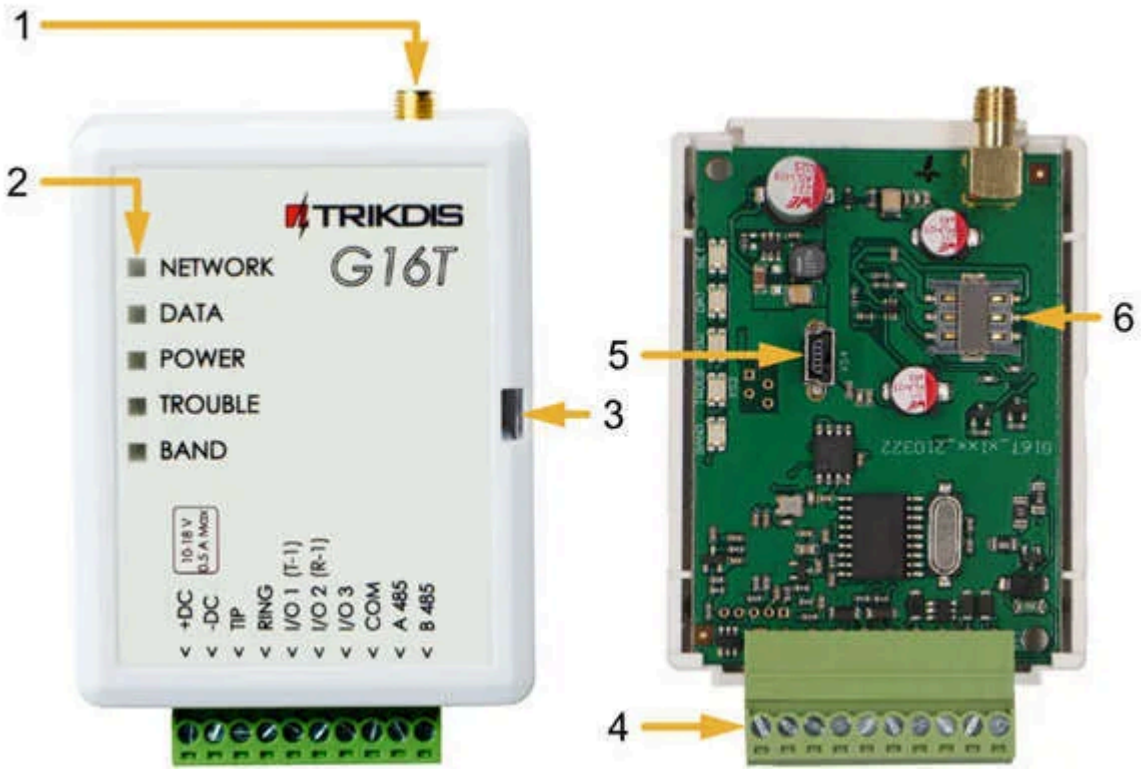


Figure 2. Composants du G16T (version 4G), vue de face et boîtier ouvert.

- 1 Connecteur SMA de l'antenne GSM
- 2 Voyants LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Fente facilitant le retrait de la face avant
- 4 Bornier débrochable
- 5 Prise USB Mini-B pour la programmation
- 6 Logement 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 câblage et, pour la programmation par USB, l'appareil peut être apporté jusqu'à l'ordinateur.

1.5 Bornes

Borne	Fonction
+DC	Alimentation, +10–18 V DC
−DC	Alimentation, négatif
TIP	Borne TIP de la centrale d'alarme
RING	Borne RING de la centrale d'alarme
I/O 1 (T-1)	Entrée / sortie 1, ou point T-1 de la supervision de la ligne téléphonique
I/O 2 (R-1)	Entrée / sortie 2, ou point R-1 de la supervision de la ligne téléphonique
I/O 3	Entrée / sortie 3
COM	Point commun (négatif) des entrées et sorties
A 485	Fil A du bus RS485 (version 4G uniquement)
B 485	Fil B du bus RS485 (version 4G uniquement)

Le marquage du bornier figure aussi sur la face avant : inutile de retirer le couvercle pour le câblage.

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 et BAND (4G uniquement) le type de réseau.

NETWORK – connexion au réseau

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

DATA – trafic de données

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

Vérification rapide

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

POWER – tension d'alimentation

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

TROUBLE – défaut

Signalisation	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/LTE)
6 clignotements rouges	Pas de connexion avec le récepteur du centre de télésurveillance
7 clignotements rouges	Liaison avec la centrale d'alarme interrompue
clignote en rouge (pendant la programmation)	Erreur mémoire
allumée en rouge (pendant la programmation)	Firmware endommagé

BAND – type de réseau (version 4G uniquement)

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

1.7 Caractéristiques techniques

Paramètre	Valeur
Liaison avec la centrale d'alarme	ligne téléphonique filaire (TIP/RING), Contact ID, DTMF
Entrées / sorties	3 I/O à double fonction (I/O 1, I/O 2, I/O 3) : en entrée NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (résistance de fin de ligne 2,2 kΩ) ; en sortie collecteur ouvert (OC), max. 0,15 A / 30 V DC
Extension	sur le bus RS485 (version 4G uniquement) : module d'extension iO-8 (+8 I/O) et autres modules de la série iO ; module WiFi W485, module Ethernet E485
Modem 2G	850 / 900 / 1800 / 1900 MHz
Modem 4G	bandes LTE selon la région
Tension d'alimentation	10–18 V DC
Consommation	60–100 mA en nominal ; jusqu'à 500 mA pendant l'émission
Protocoles de transmission	TRK, DC-09_2007, DC-09_2012, TL150

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

2. Mise en service rapide avec TrikdisConfig

Tous les réglages du G16T se font avec **TrikdisConfig**, un logiciel fonctionnant sous Windows – par câble USB ou à distance. Ce chapitre décrit le chemin le plus court : vous configurez l'appareil sur votre bureau, avant le raccordement, puis sur site il ne reste plus qu'à le câbler. L'explication détaillée des réglages se trouve au chapitre 6.

2.1 Préparatifs

Ce dont vous aurez besoin

Câble USB Mini-B · câble d'au moins 4 conducteurs vers la centrale · tournevis plat de 2,5 mm · antenne mobile de gain adapté (si la couverture est faible sur site) · carte nano-SIM active avec service de données mobiles · 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 www.trikdis.com, saisissez « TrikdisConfig » dans le champ de recherche.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Ouvrez la face avant du G16T. Insérez un tournevis plat dans la fente latérale et déclipsez doucement le couvercle. La figure ci-dessous montre l'emplacement du verrouillage et les trous de fixation du fond du boîtier.

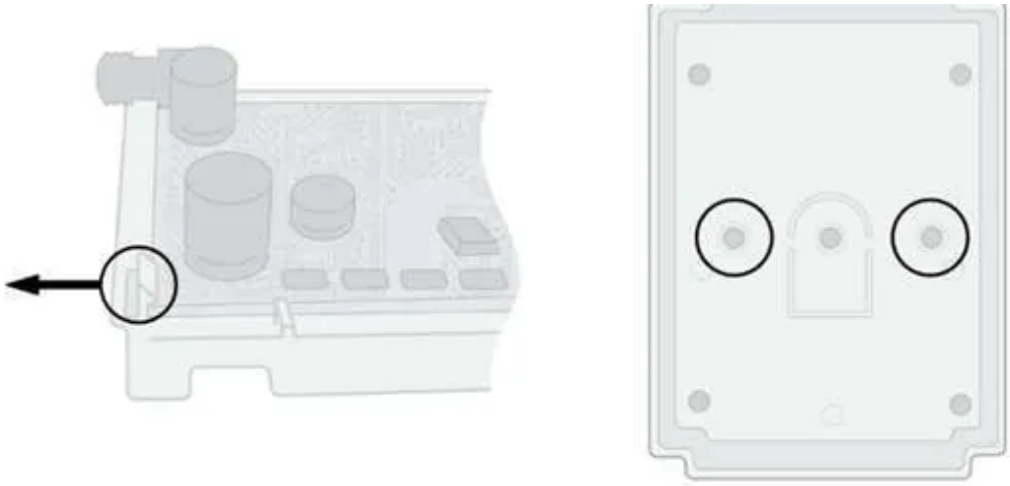


Figure 3. Déclipsage de la face avant (à gauche) et trous de fixation du fond du boîtier (à droite).

3. Insérez la carte nano-SIM dans son logement, 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 (ainsi, vous n'aurez pas à saisir de code PIN dans l'appareil).

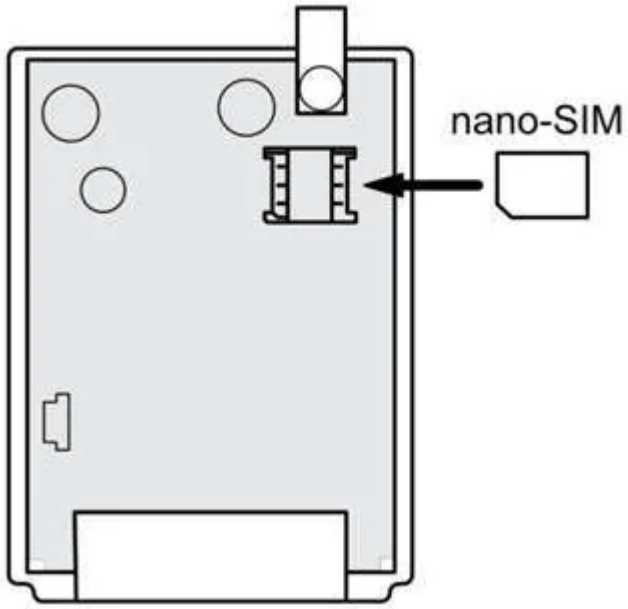


Figure 4. Emplacement de la carte nano-SIM sur le circuit imprimé.

4. Reliez le G16T à l'ordinateur avec un câble USB Mini-B. L'USB fournit assez d'énergie pour la programmation, aucune alimentation séparée n'est nécessaire.



Figure 5. Connexion à l'ordinateur avec un câble USB Mini-B.

Avertissement

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

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

2.2 Connexion à l'application Protegus 2

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

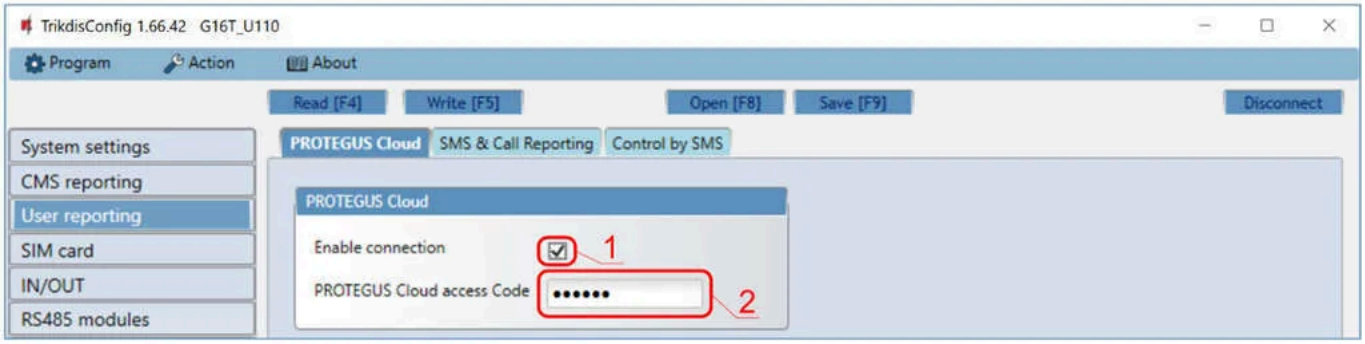


Figure 6. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- 1 **Enable connection** – cochez cette case : elle autorise la connexion au cloud Protegus.
- 2 **Protegus Cloud access code** – changez le mot de passe par défaut `123456`. C'est lui qu'il faudra saisir dans l'application lors de la création du système ; **il ne peut plus être modifié une fois le système créé.**

Saisissez ensuite les données de la carte sur la page **SIM card**.

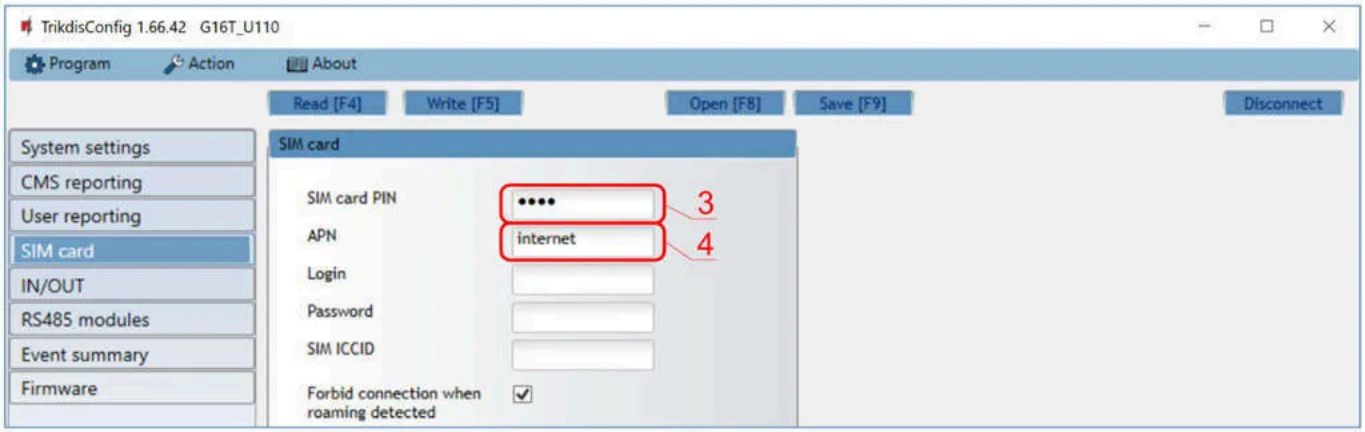


Figure 7. TrikdisConfig – page SIM card.

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

L'APN (Access Point Name) est le point d'accès aux données de l'opérateur mobile ; sans lui, l'appareil ne peut pas se connecter à Internet. Vous obtenez la valeur exacte auprès de l'opérateur de la carte SIM. Les APN connus des opérateurs européens sont regroupés 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 dans les réseaux de nombreux opérateurs.

Pour une carte de données IoT / M2M (communication 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. Cette valeur figure aussi dans l'article sur les APN, ou demandez-la à l'opérateur ; si l'opérateur fournit aussi un nom d'utilisateur et un mot de passe, saisissez-les également.

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.

N'oubliez pas d'activer et de configurer le transmetteur téléphonique de la centrale d'alarme, sinon la centrale n'enverra aucun événement. La configuration de la centrale est décrite au chapitre 4.

2.3 Connexion au centre de télésurveillance

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

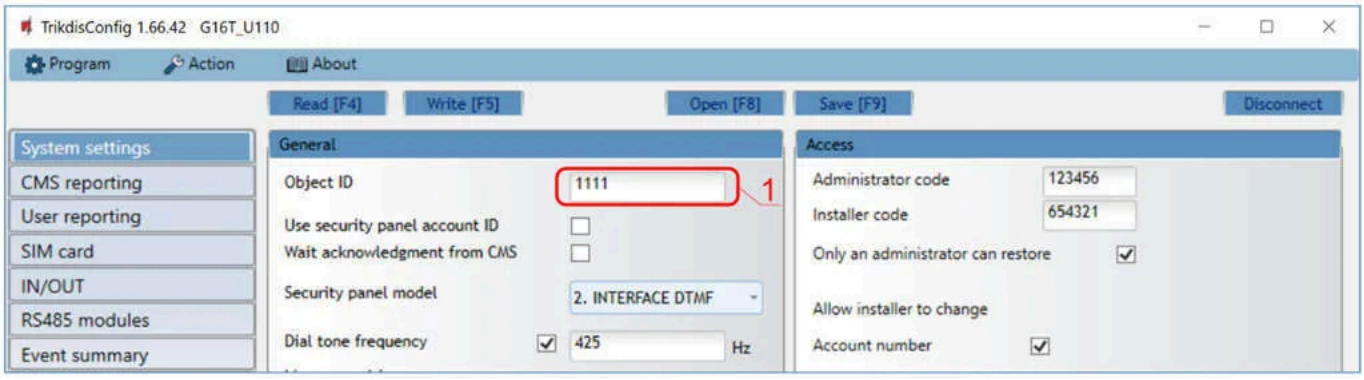


Figure 8. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne sont pas utilisables.

Réglez ensuite les données du récepteur sur la page **CMS reporting**, dans la partie **Primary channel** (canal principal).

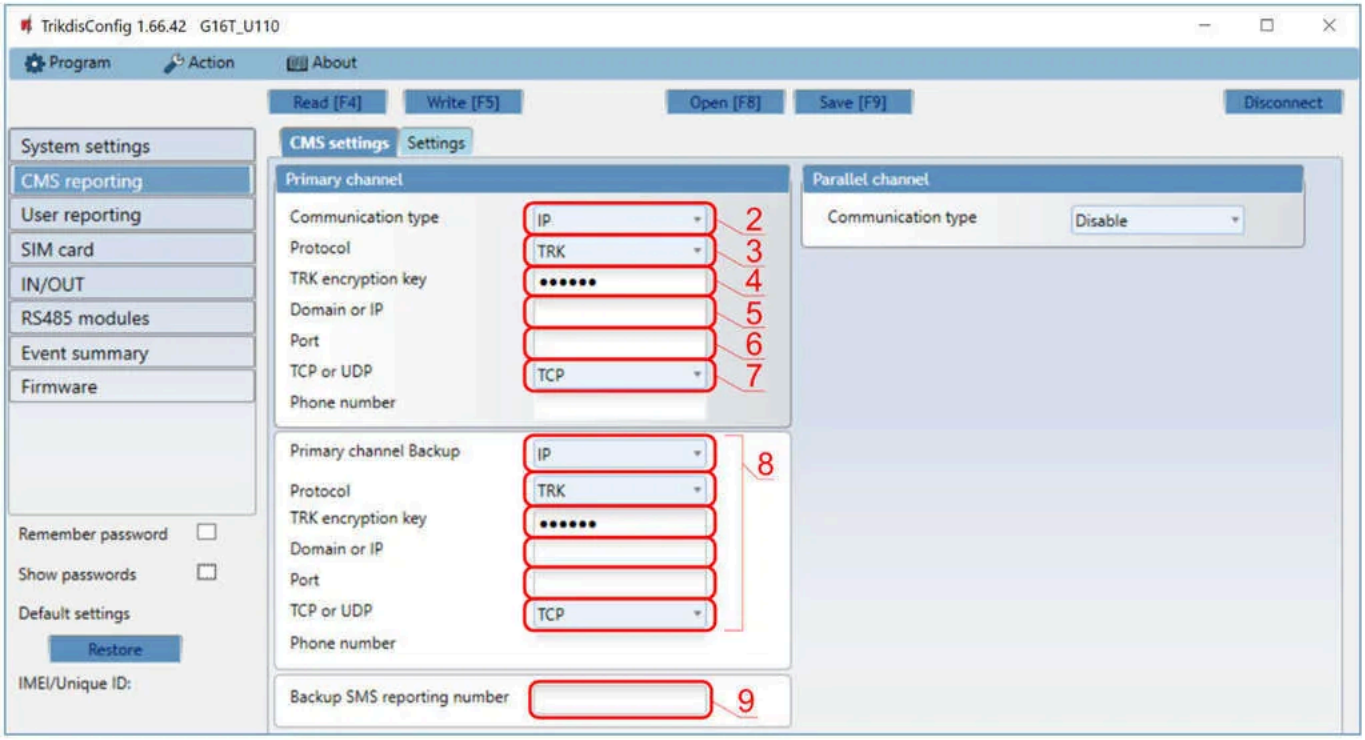


Figure 9. TrikdisConfig – CMS reporting, onglet CMS settings.

- 2 **Communication type** – choisissez la connexion **IP** (le SMS n'est pas recommandé comme canal principal).
- 3 **Protocol** – **TRK** pour un récepteur Trikdis, **DC-09_2007** ou **DC-09_2012** pour un récepteur universel, **TL150** pour un récepteur SUR-GARD.
- 4 **TRK encryption key** – la clé de chiffrement à 6 chiffres réglée dans le récepteur.
- 5 **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- 6 **Port** – le numéro de port du récepteur.
- 7 **TCP or UDP** – le protocole de transport ; il doit correspondre au réglage du récepteur.
- 8 **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.
- 9 **Backup SMS reporting number** – si vous disposez d'un récepteur SMS Trikdis, saisissez ici son numéro de téléphone : l'appareil y envoie un SMS immédiatement après le premier démarrage, puis transmet par SMS lorsqu'aucun canal IP ne fonctionne.

Enfin, saisissez les données de la carte sur la page **SIM card**, si vous ne l'avez pas encore fait au point 2.2.

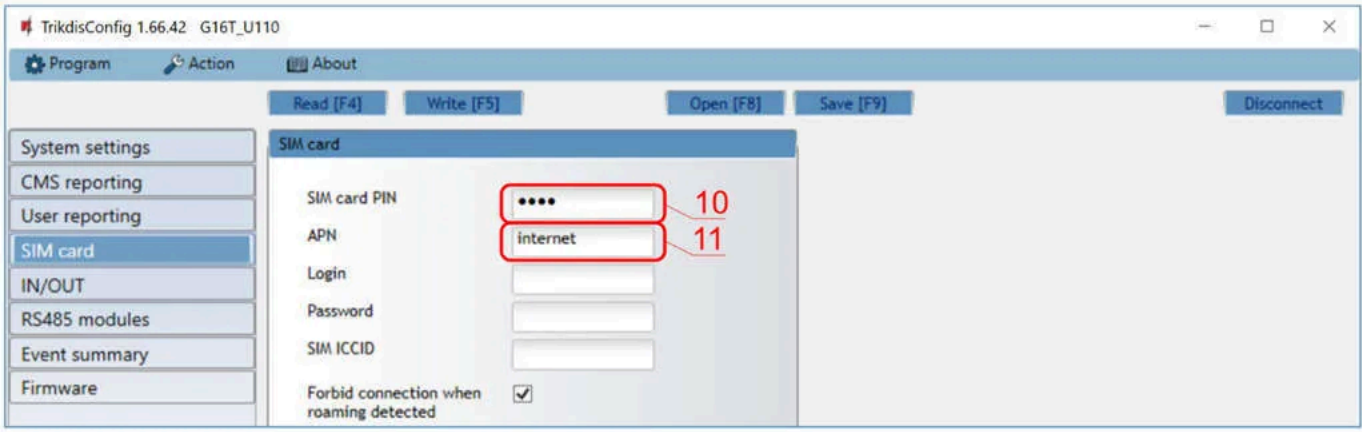


Figure 10. TrikdisConfig – page SIM card.

- 10 **SIM card PIN** – le code PIN de la carte.
- 11 **APN** – le point d'accès de l'opérateur (voir le point 2.2).

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

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. Là aussi, le transmetteur téléphonique de la centrale d'alarme doit être activé et configuré, sinon la centrale n'enverra 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 Étapes de l'installation

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

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

3.2 Emplacement et antenne

- Placez le communicateur dans un endroit **sec, à l'intérieur**, de préférence près du boîtier de la centrale d'alarme, afin que le câblage soit court.
- Dans un **boîtier métallique**, le signal mobile est fortement atténué. Si le communicateur est placé dans le boîtier métallique de la centrale, faites sortir l'antenne du boîtier ou utilisez une antenne à câble plus long.
- Avant la fixation définitive, **vérifiez le niveau du signal** : le nombre de clignotements jaunes de la LED NETWORK doit être d'au moins 5 en 2G et d'au moins 3 en 4G (voir le point 1.6). 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

Le G16T se raccorde à la sortie ligne téléphonique (TIP/RING) de la centrale et est alimenté par la sortie d'alimentation auxiliaire 12 V (AUX) de la centrale.

Raccordement recommandé, normal : DC+, DC−, TIP et RING. Dans ce cas, le communicateur ne détecte pas la coupure du câble.

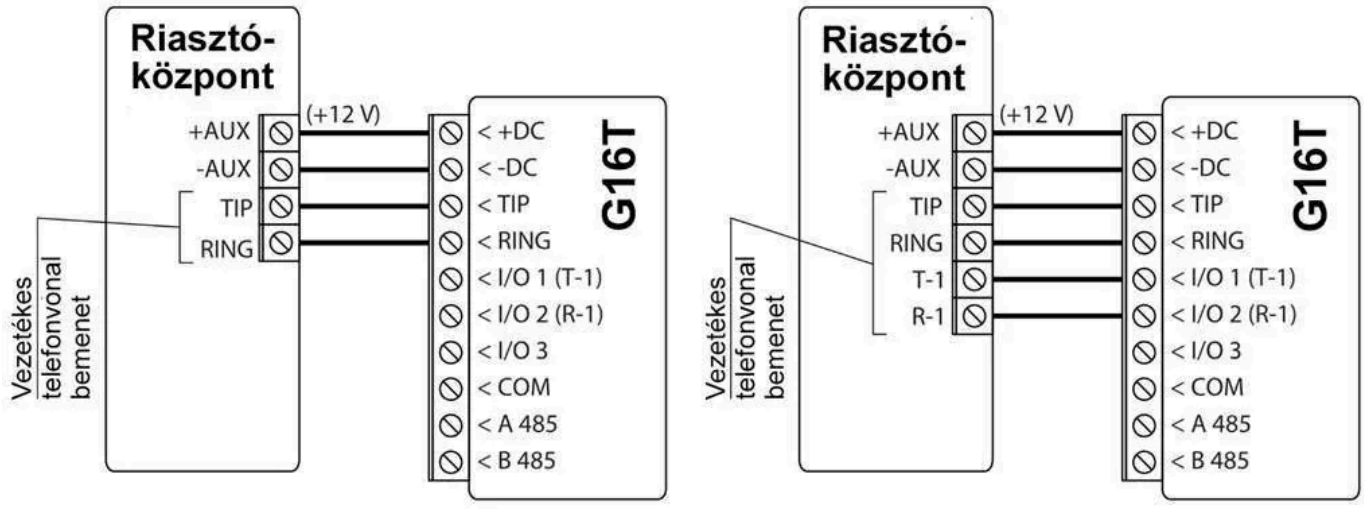


Figure 11. Raccordement à la sortie ligne téléphonique de la centrale : à gauche le raccordement normal, à droite le raccordement avec supervision de ligne.

Pendant l'émission, le G16T peut consommer jusqu'à 500 mA. Vérifiez que la sortie AUX de la centrale le supporte avec tous les autres appareils qui y sont raccordés. Comme l'alimentation est fournie par la centrale, en cas de coupure secteur la batterie de la centrale alimente aussi le communicateur.

3.3.1 Si nécessaire : supervision de ligne

Uniquement si la supervision de ligne est requise : le communicateur signale alors la coupure de la liaison entre lui et la centrale d'alarme.

1. En plus du raccordement normal, raccordez aussi ces deux fils : la borne **T-1** de la centrale sur la borne **I/O 1 (T-1)** du communicateur, la borne **R-1** de la centrale sur la borne **I/O 2 (R-1)**.
2. Sur la page **System settings** de TrikdisConfig, activez l'option **Line supervision**.
3. Vérifiez les réglages nécessaires côté centrale d'alarme dans le manuel d'installation de la centrale.

Dans ce cas, I/O 1 et I/O 2 ne peuvent pas être utilisées à d'autres fins.

3.4 Raccordement d'une zone à clé

Si vous souhaitez armer et désarmer la centrale à distance depuis l'application Protegus 2, configurez l'une des bornes I/O du communicateur comme **sortie** et raccordez-la à une **zone à clé** de la centrale. À l'activation, la sortie tire la zone vers COM (le négatif) ; raccordez la résistance de fin de ligne de la zone selon le type de zone de la centrale. Comme le G16T dispose de trois bornes I/O, jusqu'à trois partitions peuvent être commandées, chacune avec sa propre sortie. Réglez la borne utilisée pour la zone à clé sur la fonction **OUT** dans la page **IN/OUT** de TrikdisConfig (point 6.6). Le matériel version 3 possède une sortie programmable (OUT), qui peut commander une partition ; le champ **Output OUT1 mode** de la page **System settings** doit alors être réglé sur **Remote control** (réglage par défaut).

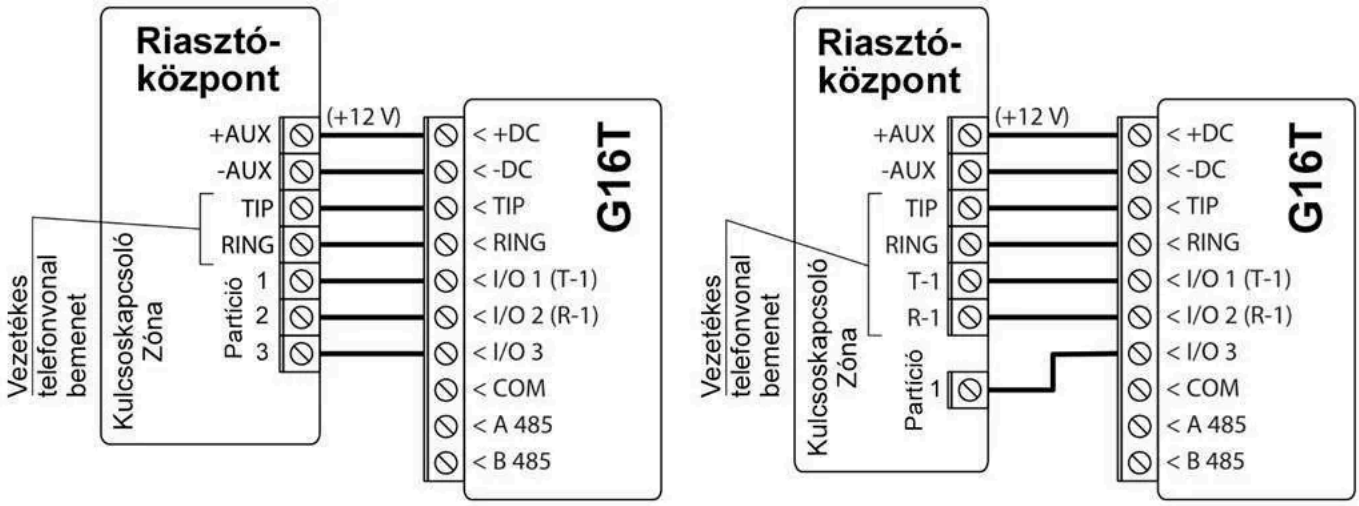


Figure 12. Armement et désarmement par zone à clé : à gauche le raccordement normal, à droite le raccordement avec supervision de ligne (dans ce cas, I/O 3 reste disponible pour la zone à clé).

La zone à clé peut être de type impulsionnel ou bistable – il faut régler le même mode dans l'application Protegus 2 (point 5.2). 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.

3.5 Raccordement des entrées

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

Les entrées acceptent les types de circuit suivants : **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La résistance de fin de ligne est de **2,2 kΩ**. Avec une simple fin de ligne (EOL), le court-circuit comme la coupure comptent comme une alarme ; la double fin de ligne (DEOL), avec deux résistances, distingue l'alarme et

l'autoprotection (court-circuit ou coupure). Le réglage d'usine est NO (normalement ouvert) ; le type d'entrée se règle sur la page **IN/OUT** de TrikdisConfig, selon le câblage.

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

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

Raccordement des circuits d'entrée : types NC, NO, EOL et DEOL avec résistance de fin de ligne de 2,2 kΩ, avec boucle d'autoprotection pour les types DEOL.

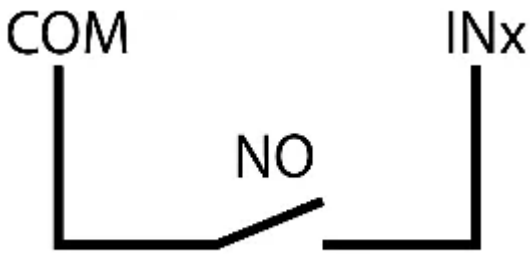


Figure 13. NO – circuit normalement ouvert : fermé – alarme, ouvert – état de repos.

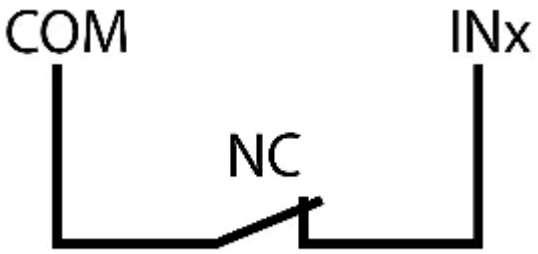


Figure 14. NC – circuit normalement fermé : ouvert – alarme, fermé – état de repos.

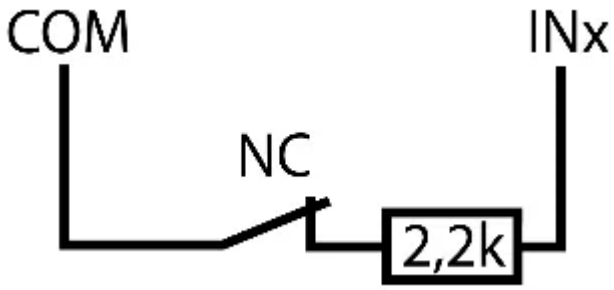


Figure 15. NC/EOL – circuit normalement fermé avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

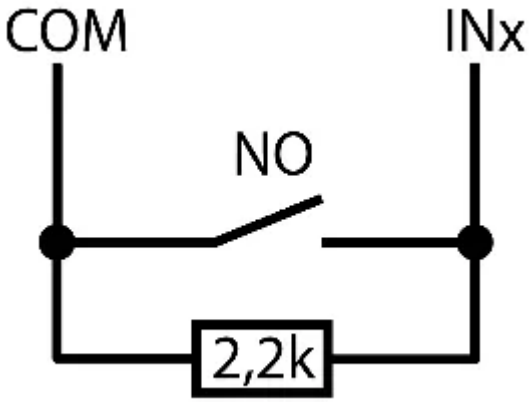


Figure 16. NO/EOL – circuit normalement ouvert avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

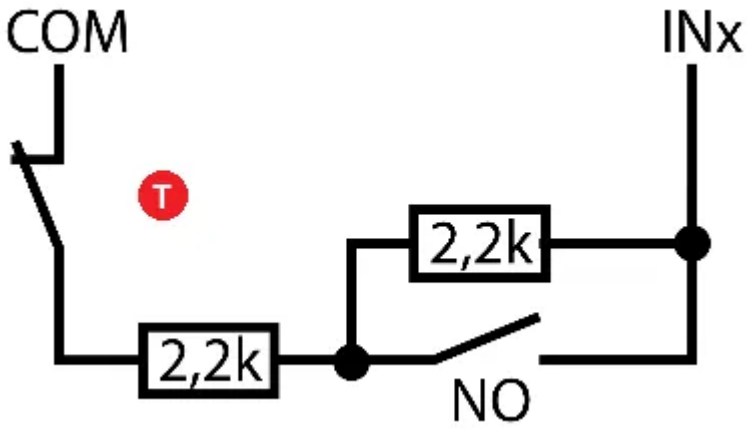


Figure 17. NO/DEOL – circuit normalement ouvert avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

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

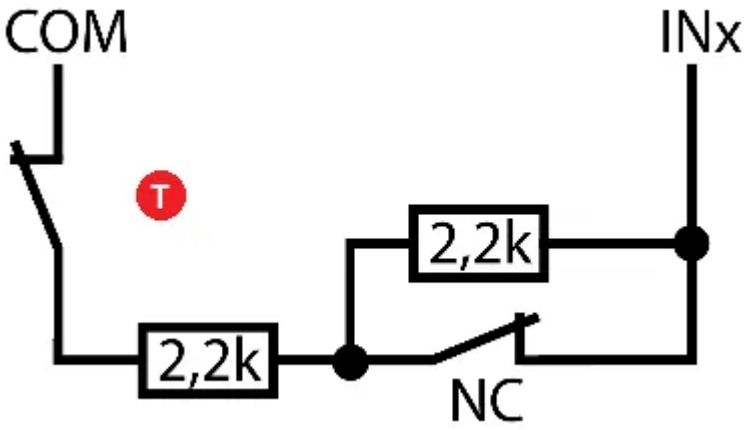


Figure 18. NC/DEOL – circuit normalement fermé avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

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

3.6 Raccordement d'une sortie avec un relais

En sortie, les bornes I/O sont des sorties à collecteur ouvert (OC) : à l'état actif, elles tirent la charge raccordée vers le négatif, avec 0,15 A au maximum, jusqu'à 30 V DC. Commandez un consommateur plus important ou un appareil sous tension secteur **par l'intermédiaire d'un relais** : une extrémité de la bobine du relais va sur +DC, l'autre sur la borne I/O.

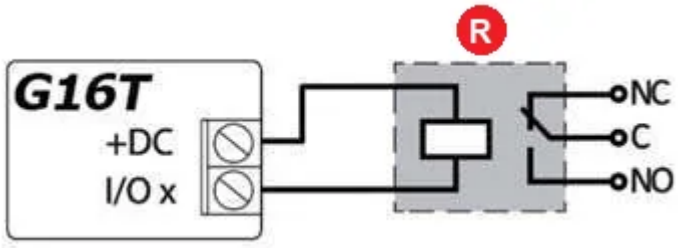


Figure 19. Raccordement d'un relais à la sortie du communicateur : la bobine se place entre +DC et la borne I/O x, les contacts (NC, C, NO) commandent le consommateur.

- 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 plus d'entrées ou de sorties, vous pouvez raccorder jusqu'à quatre modules d'extension **iO-8** au bus RS485 de la **version 4G** ; chacun ajoute 8 I/O à double fonction supplémentaires. Les autres modules d'extension filaires ou sans fil de la série iO de Trikdis peuvent aussi être raccordés à ce même bus, par exemple si vous souhaitez brancher une sonde de température : le module **iO** possède 1 entrée, 1 sortie relais et un bus 1-Wire pour sondes de température (configuration au point 6.7). Reliez les bornes A 485 et B 485 aux bornes A et B du module, et alimentez le module par le 12 V de la centrale. Le module doit être ajouté sur la page **RS485 modules** de TrikdisConfig (point 6.7).

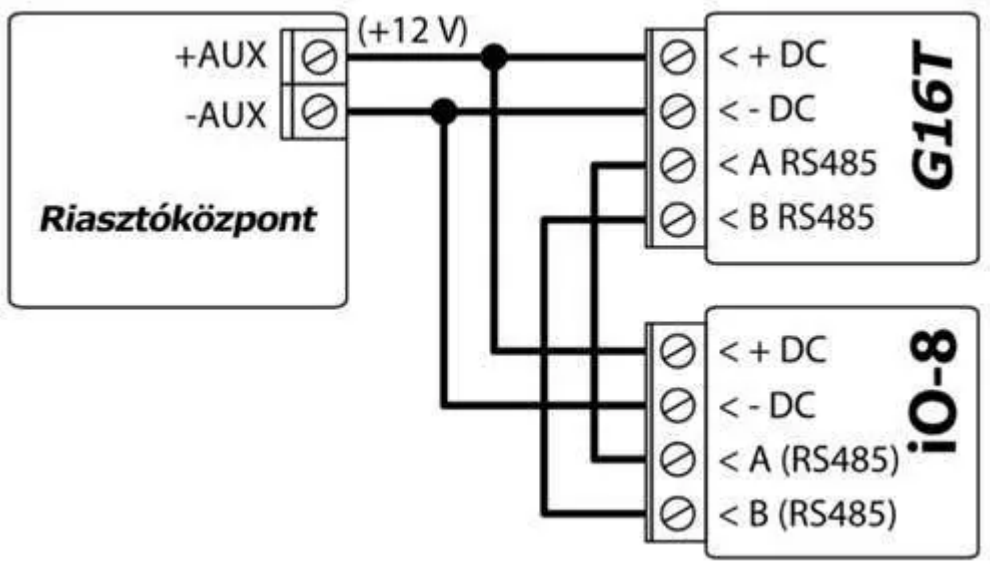


Figure 20. Raccordement du module d'extension iO-8 au bus RS485 du G16T ; alimentation par la sortie AUX de la centrale d'alarme.

Le G16T à modem 2G (G16T_G410) n'a pas de bus RS485 : aucun module iO-8, W485 ou E485 ne peut donc y être raccordé.

3.8 Raccordement des modules W485 et E485

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

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

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

Tant que la connexion WiFi ou Ethernet est active, le G16T communique par elle (les messages vers le centre de télésurveillance et vers Protegus passent par le routeur WiFi ou par l'Internet filaire ; la connexion de données mobiles n'est alors pas utilisée) ; si elle est interrompue, il bascule sur les données mobiles et revient au module lorsque la connexion est rétablie. Pour que le module fonctionne, **une carte SIM doit être présente dans le G16T**.

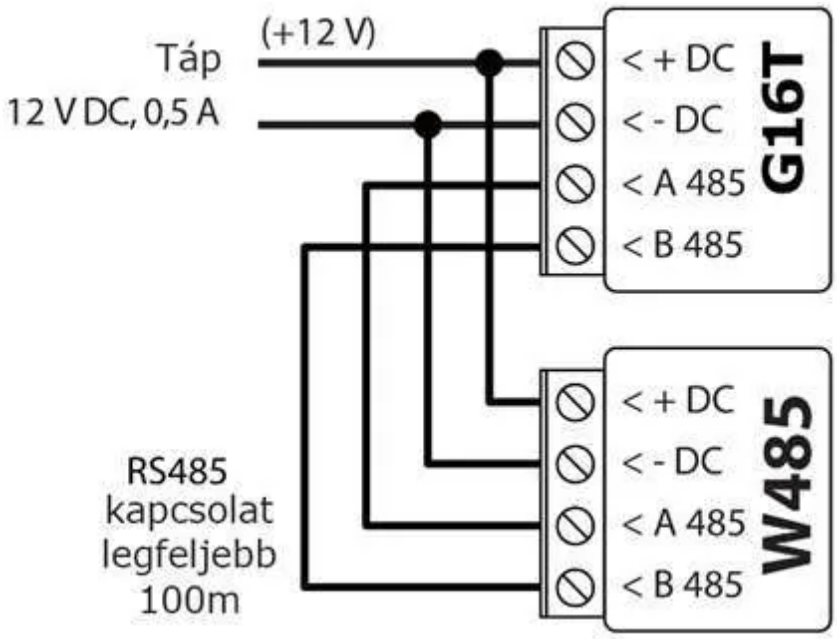


Figure 21. Raccordement du module WiFi W485 au G16T par le bus RS485. Les deux appareils sont alimentés par une alimentation commune de 12 V DC (au moins 0,5 A) (entrée d'alimentation du module 9–28 V DC) ; le câble RS485 peut mesurer jusqu'à 100 m.

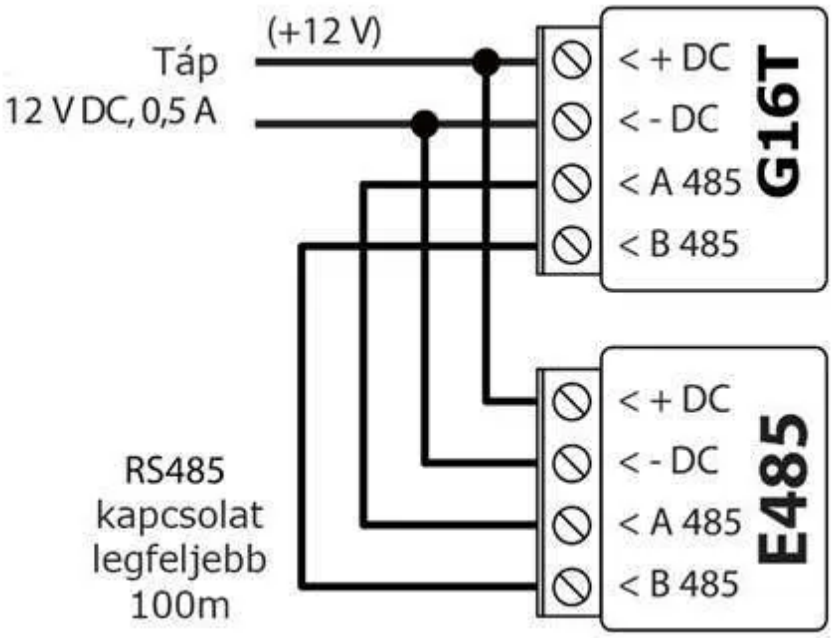


Figure 22. Raccordement du module Ethernet E485 au G16T par le bus RS485. Les deux appareils sont alimentés par une alimentation commune de 12 V DC (au moins 0,5 A) (entrée d'alimentation du module 9–28 V DC) ; le câble RS485 peut mesurer jusqu'à 100 m.

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

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

3.9 Mise sous tension et première vérification

A TRIKDIS átjelző elindítása

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

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

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

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

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

4. Programmation de la centrale d'alarme

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.

4.1 Programmation du transmetteur Honeywell Vista

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

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

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

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

Dans le manuel d'installation de chaque centrale, recherchez les quatre mêmes réglages : l'activation du transmetteur téléphonique, le numéro de téléphone du récepteur, le mode de numérotation (DTMF) et le format de communication (Contact ID). Si la centrale attend une tonalité (dial tone) avant de composer le numéro, le G16T la fournit ; si l'appel ne démarre toujours pas, désactivez la détection de tonalité dans la centrale (« numérotation sans tonalité » ou option similaire).

Si la centrale signale une erreur en fin d'appel alors que l'événement est bien arrivé, vérifiez le réglage **Wait acknowledgment from CMS** sur la page **System settings** de TrikdisConfig : lorsqu'il est activé, le communicateur ne termine l'appel (kiss-off) qu'après l'acquittement du récepteur de télésurveillance. Dans un système sans télésurveillance, uniquement avec Protegus 2, laissez-le désactivé (c'est l'état par défaut), car aucun récepteur ne peut acquitter.

5. Commande 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 sur les événements, peut armer et désarmer, et commander les sorties du communicateur.

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez :

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

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

A rendszer létrehozása a Protegus 2 alkalmazásban

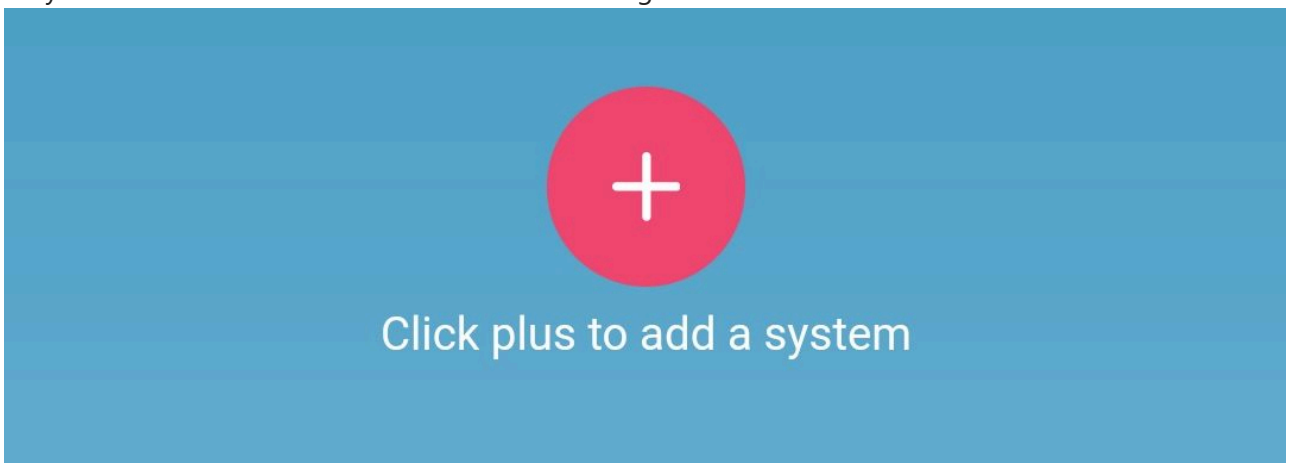
1. Töltsd le a Protegus 2 alkalmazást a telefonodra vagy nyisd meg egy böngészőben

protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

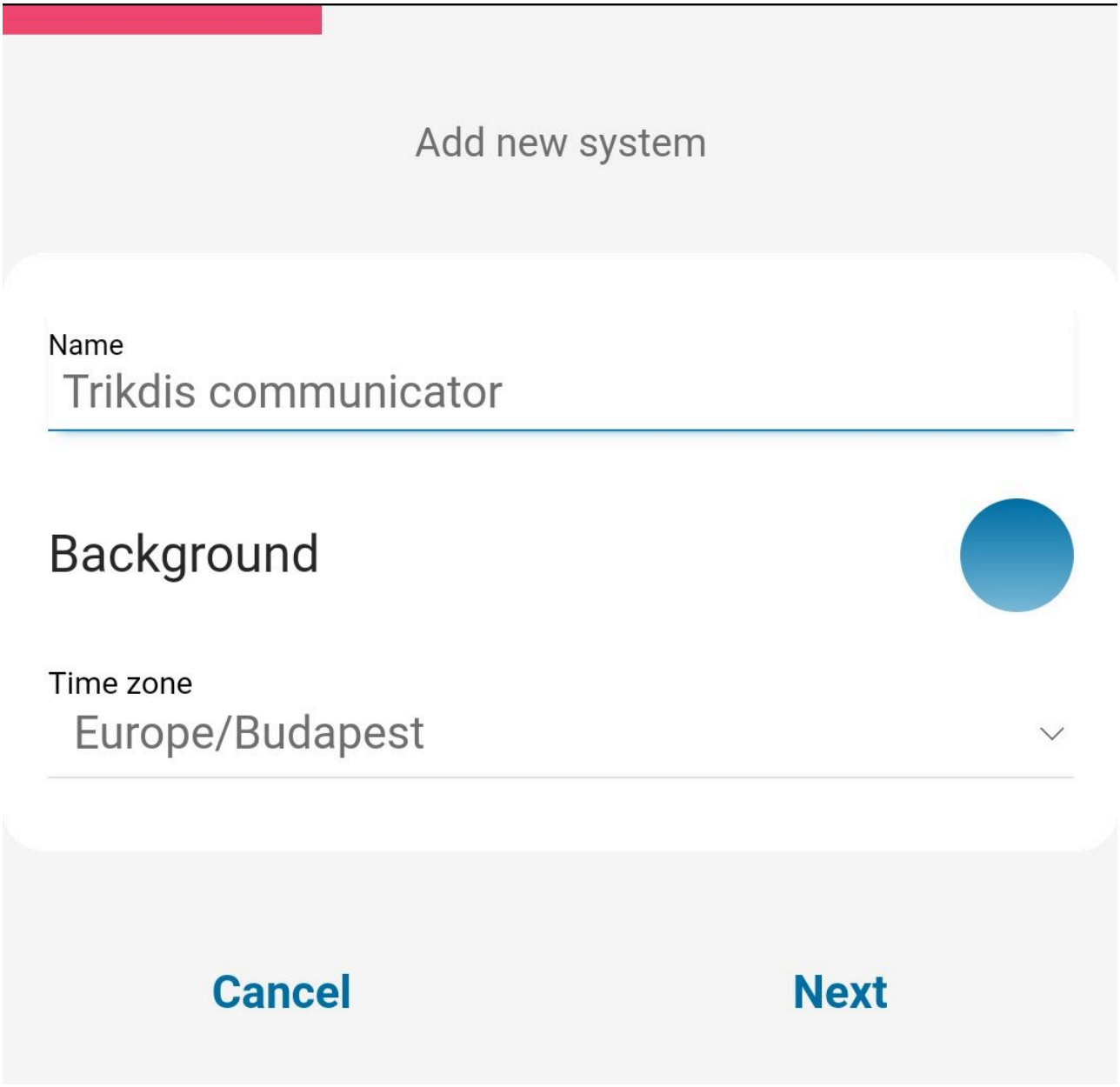
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



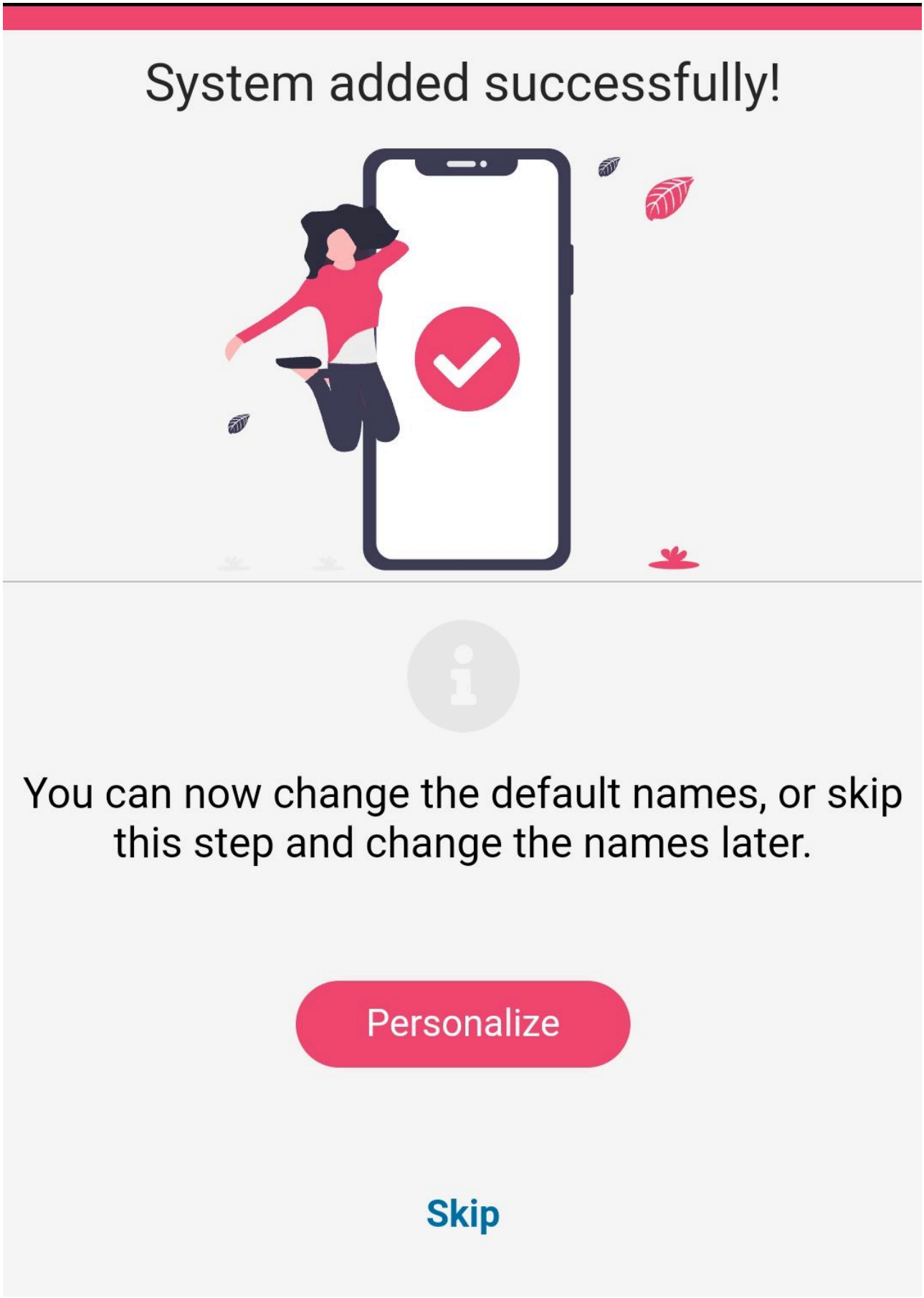
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



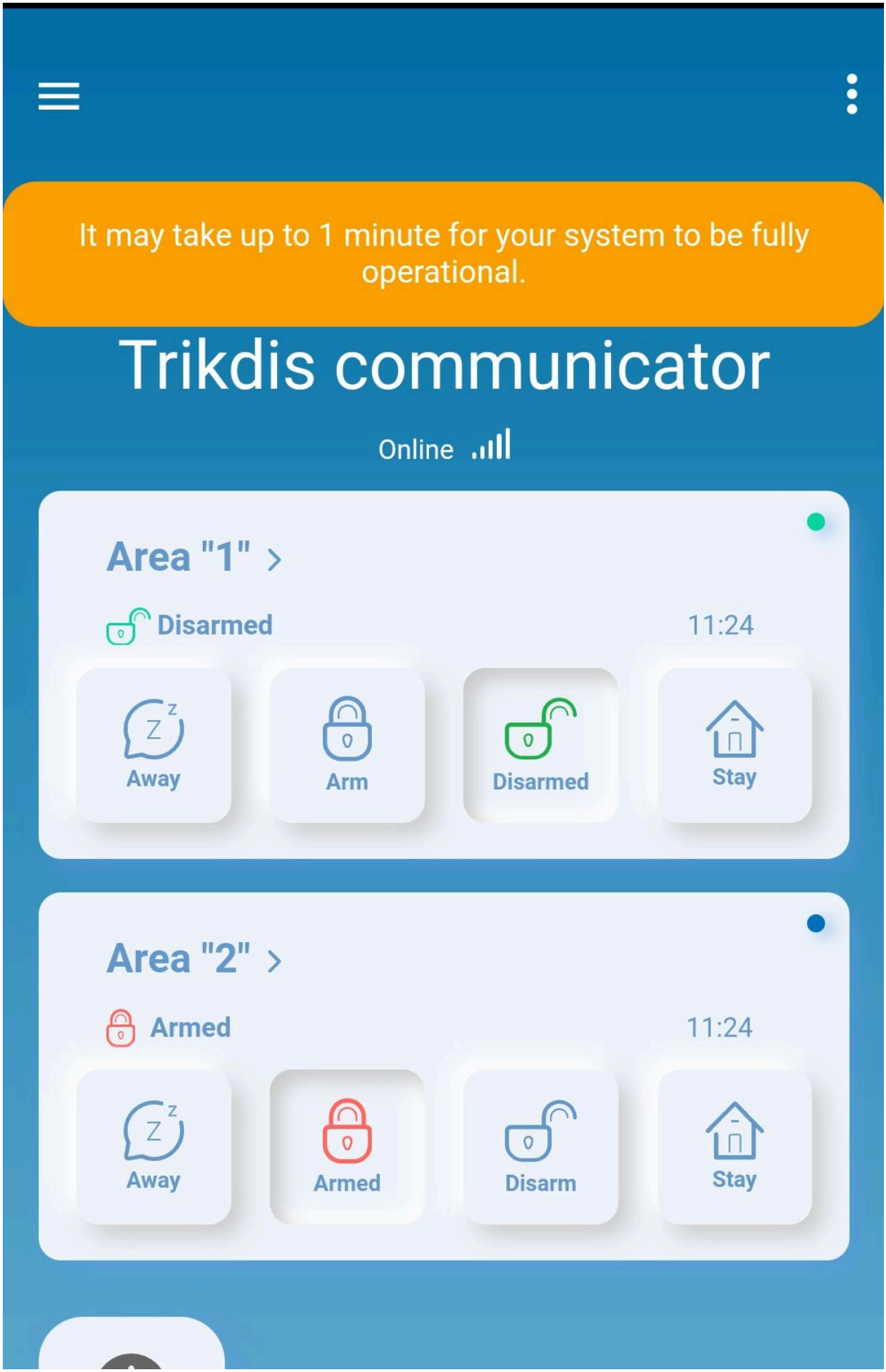
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



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

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.

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.

5.4 Commande par SMS

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

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

Avec le mot de passe **administrateur**, toutes les commandes sont utilisables ; avec le mot de passe **installateur**, les commandes INFO, RESET et OUTPUTx.

Commande	Donnée	Fonction	Exemple
`INFO`	–	Demande des informations sur l'appareil : type, IMEI, numéro de série, version du firmware	`123456 INFO`
`RESET`	–	Redémarre l'appareil	`123456 RESET`
`OUTPUTx`	`ON`	Active la sortie x	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Désactive la sortie x	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Délivre une impulsion sur la sortie x ; `tttt` = durée de l'impulsion en secondes, sur quatre chiffres	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Active ou désactive la connexion Protegus	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=adresse:port`	Adresse IP et port du canal principal	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=clé`	Clé de chiffrement TRK	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=nom`	APN de la carte SIM	`123456 CONNECT APN=internet`
`CONNECT`	`USER=nom`	Nom d'utilisateur APN (si l'opérateur le demande)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=motdepasse`	Mot de passe APN (si l'opérateur le demande)	`123456 CONNECT PASS=password`

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

Sur le G16T, la commande `CONNECT` a un paramètre supplémentaire : `CP=1` désactive, `CP=2` active l'interface ligne téléphonique du communicateur. Exemple : `123456 CONNECT CP=2`.

6. TrikdisConfig – les réglages en détail

La fenêtre de TrikdisConfig affiche à gauche la liste des pages (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), en haut la barre de boutons (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) et en bas la barre d'état. Ce chapitre passe en revue, page par page, les réglages du G16T.

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 23. La barre d'état de TrikdisConfig avec un G16T lu : identifiant, état, type, numéro de série, versions, mode de connexion et niveau d'accès.

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 le fonctionnement de base de l'appareil, dans le groupe **Access**, les niveaux d'accès.

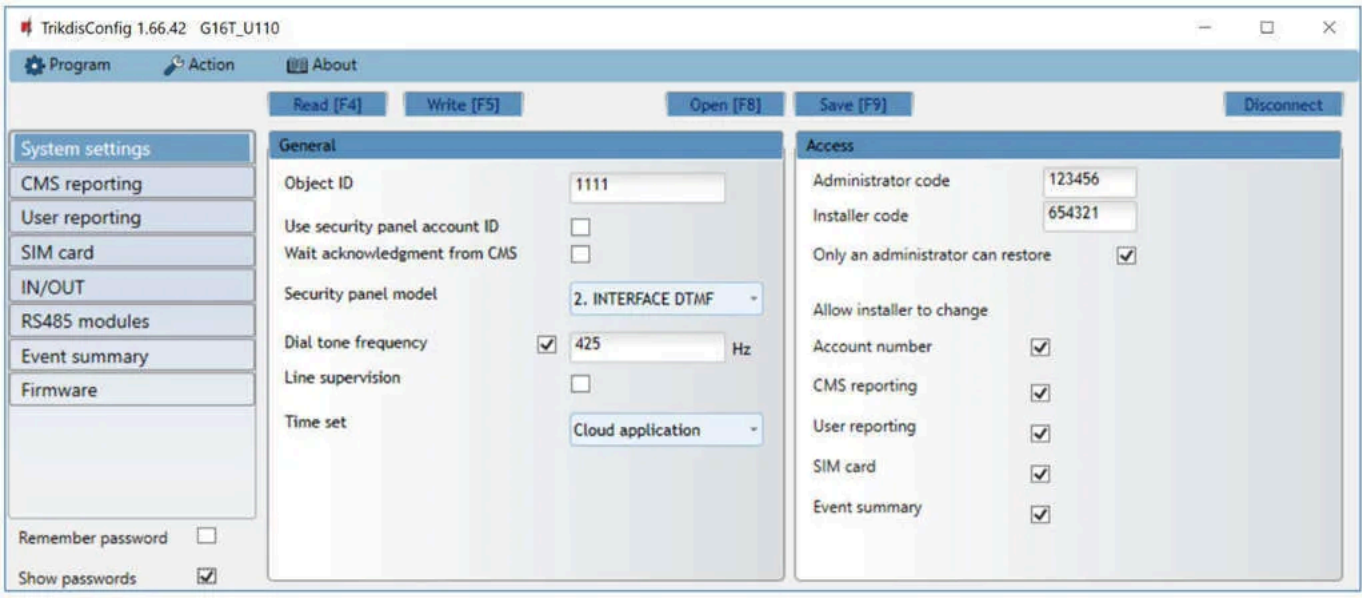


Figure 24. TrikdisConfig – page System settings : groupes General et Access.

- **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux : 0–9, A–F ; `FFFE` et `FFFF` ne sont pas utilisables). Obligatoire si l'appareil transmet aussi vers un centre de télésurveillance.
- **Use security panel account ID** – si cette case est cochée, le communicateur n'utilise pas son propre Object ID, mais l'identifiant envoyé par la centrale dans le message Contact ID. Utile lorsque plusieurs partitions transmettent avec des identifiants différents.
- **Wait acknowledgment from CMS** – si cette case est cochée, le communicateur attend, après chaque événement, l'acquittement du récepteur, et n'envoie qu'ensuite le signal de fin (kiss-off) à la centrale. En l'absence d'acquittement, la centrale renvoie l'événement. Dans un système sans télésurveillance, uniquement avec Protegus 2, laissez-la décochée (état par défaut).
- **Security panel model** – le type d'interface ligne téléphonique (ce réglage active ou désactive l'interface ligne téléphonique DTMF du communicateur) ; par défaut **2. INTERFACE DTMF**.
- **Dial tone frequency** – la fréquence de la tonalité que le G16T fournit à la centrale (par défaut 425 Hz, la tonalité utilisée dans la plupart des pays européens).
- **Line supervision** – supervision du câble entre la centrale et le communicateur ; nécessite aussi le raccordement des fils T-1 et R-1 (section 3.3.1).
- Sur le matériel version 4, le type des entrées et le rôle des sorties se règlent sur la page **IN/OUT** (point 6.6). Sur le matériel version 3, ces deux champs se trouvent ici : **Input IN1-IN2 type** – le type d'entrée dans la liste (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) ; **Output OUT1 mode** – le mode de fonctionnement de la sortie dans la liste.
- **Time set** – la source de l'horloge de l'appareil (par défaut **Cloud application**, le cloud Protegus).

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

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

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

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

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

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

6.3 CMS reporting

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

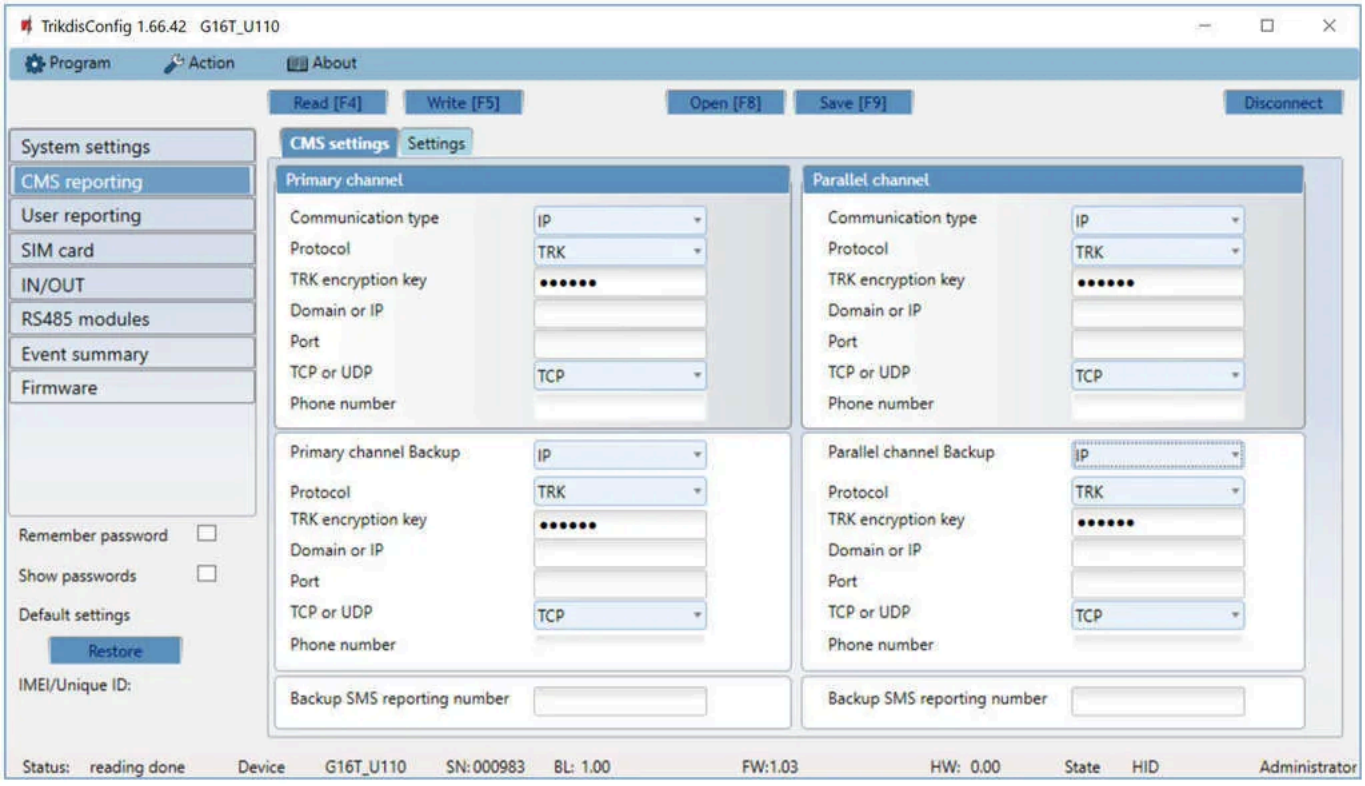


Figure 25. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal, de secours et parallèle.

Primary channel – canal principal

- **Communication type** – IP ou SMS.
- **Protocol** – TRK (récepteurs Trikdis), DC-09_2007 ou DC-09_2012 (récepteurs universels), TL150 (SUR-GARD).

- **TRK encryption key** – clé de chiffrement à 6 chiffres ; elle doit être identique dans le communicateur et dans le récepteur.
- **Domain or IP**, **Port** – l'adresse et le port du récepteur.
- **TCP or UDP** – le protocole de transport.
- **Phone number** – uniquement pour la communication par SMS : le numéro de téléphone du récepteur SMS Trikdis avec l'indicatif pays (par ex. `33xxxxxxxxx` pour un numéro français).

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

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

Backup SMS reporting number – numéro SMS de secours. Il entre en action si l'envoi échoue sur le canal principal, sur le canal parallèle et sur le canal de secours ; il est utile parce qu'il fonctionne sans connexion IP. Il n'est actif que si le canal principal et le canal de secours sont en mode IP. L'appareil envoie un SMS au récepteur SMS du centre de télésurveillance après le premier démarrage, ainsi que lorsque la connexion TCP/IP ou UDP/IP est interrompue à la fois sur le canal principal et sur son canal de secours. Saisissez le numéro de téléphone du récepteur SMS Trikdis avec l'indicatif pays (par ex. `33xxxxxxxxx` pour un numéro français).

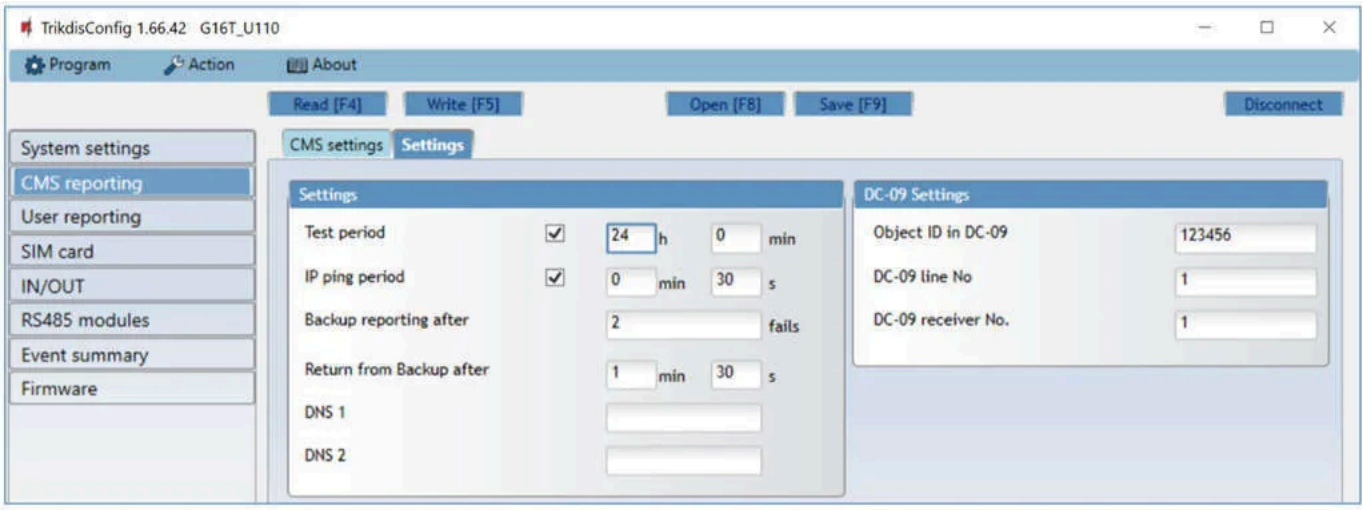


Figure 26. TrikdisConfig – CMS reporting, onglet Settings : rapport de test, PING, temporisations du canal de secours, DNS et données DC-09.

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.

En bas de l'onglet : **DNS 1, DNS 2** – serveurs de noms (DNS, Domain Name System : il fournit l'adresse IP correspondant à un nom de domaine) ; ils sont nécessaires si vous avez saisi le récepteur par son nom de domaine et non par son adresse IP. Par défaut, le DNS public de Google.

6.4 User reporting

Dans l'onglet **PROTEGUS Cloud**, vous activez le service Protegus. Avec le service Protegus, l'utilisateur peut surveiller et commander à distance le communicateur et le système qui y est raccordé ; détails : www.protegus.app.

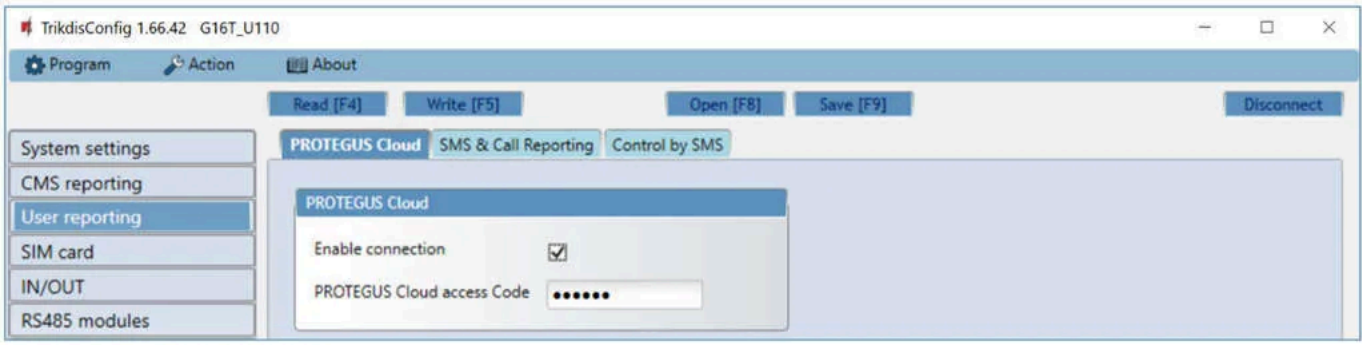


Figure 27. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

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

Dans l'onglet **SMS & Call Reporting**, l'utilisateur peut aussi être informé 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.

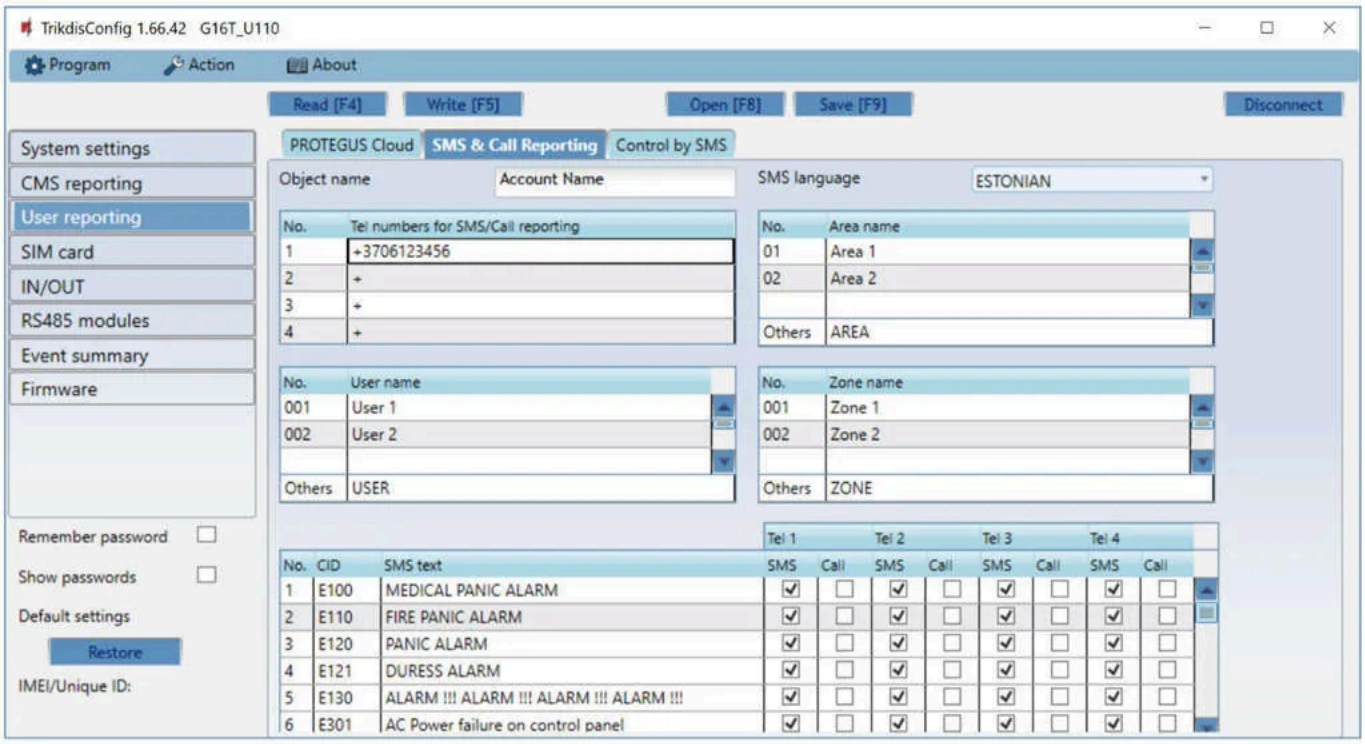


Figure 28. TrikdisConfig – User reporting, onglet SMS & Call Reporting.

- **Object name** – le nom du système ; il figure dans chaque SMS.
- **SMS language** – la langue des SMS (pour les caractères accentués de la langue).
- **Tel numbers for SMS/Call reporting** – jusqu'à 4 numéros de téléphone avec l'indicatif pays (par ex. pour un numéro français `+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 son nom à côté.
- **CID event table** – pour chaque événement, vous pouvez choisir quel numéro reçoit un SMS ou un appel ; le texte du message et le code Contact ID sont aussi modifiables, et vous pouvez ajouter un nouvel événement.

Dans l'onglet **Control by SMS**, vous réglez la réception des commandes SMS (les commandes sont décrites au point 5.4).

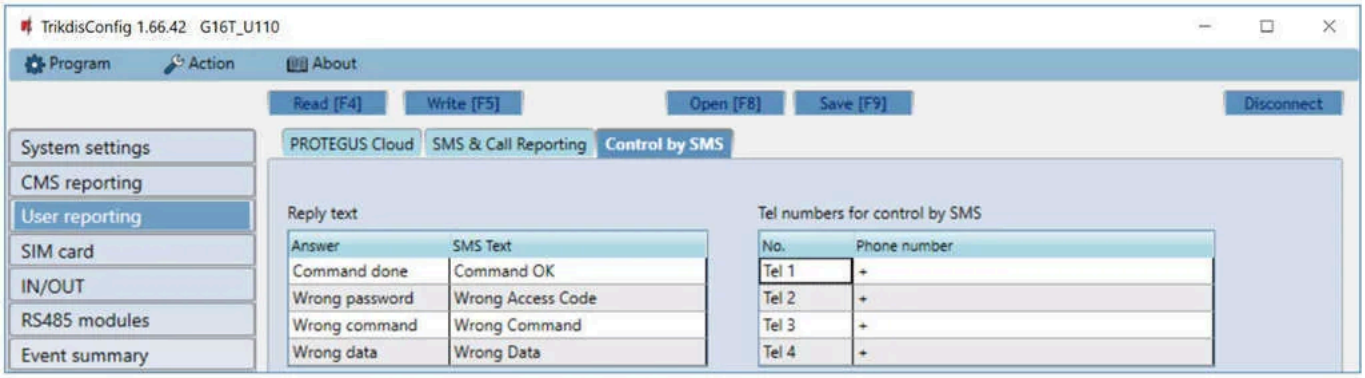


Figure 29. TrikdisConfig – User reporting, onglet Control by SMS.

- **Reply text** – le texte des quatre messages de réponse à une commande SMS : commande réussie (Command done), mot de passe incorrect (Wrong password), commande incorrecte (Wrong command), données incorrectes (Wrong data). Les textes de réponse sont modifiables.

- **Tel numbers for control by SMS** – jusqu'à 4 numéros ; l'appareil n'accepte de commandes que de ces numéros. Si la liste est vide, il accepte une commande avec le bon mot de passe 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.

6.5 SIM card

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



Figure 30. TrikdisConfig – page SIM card.

- **SIM card PIN** – le code PIN de la carte. Pour désactiver la demande de code PIN, placez la carte dans un téléphone mobile et désactivez-la à cet endroit. Si la demande de code PIN est désactivée, la valeur par défaut du champ peut rester.
- **APN** – le point d'accès de l'opérateur ; les APN connus des opérateurs sont répertoriés dans l'article sur les APN (pour une carte IoT / M2M, l'opérateur fournit un APN spécifique, voir le point 2.2). L'APN est nécessaire à la connexion Internet de l'appareil ; si vous n'avez pas d'autre information, essayez l'APN `internet`, qui est générique et fonctionne dans les réseaux de nombreux opérateurs.
- **Login, Password** – nom d'utilisateur et mot de passe de l'APN, si l'opérateur les exige.
- **Forbid connection when roaming detected** – utile près d'une frontière : empêche l'appareil de se connecter au réseau du pays voisin.

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

6.6 IN/OUT

C'est ici que vous définissez le rôle des trois bornes I/O à double fonction du communicateur : **Disabled** (non utilisée), **IN** (entrée) ou **OUT** (sortie). Pour une entrée, il faut aussi indiquer le type (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Sur le matériel version 3, ces réglages se trouvent sur la page **System settings** (point 6.2).

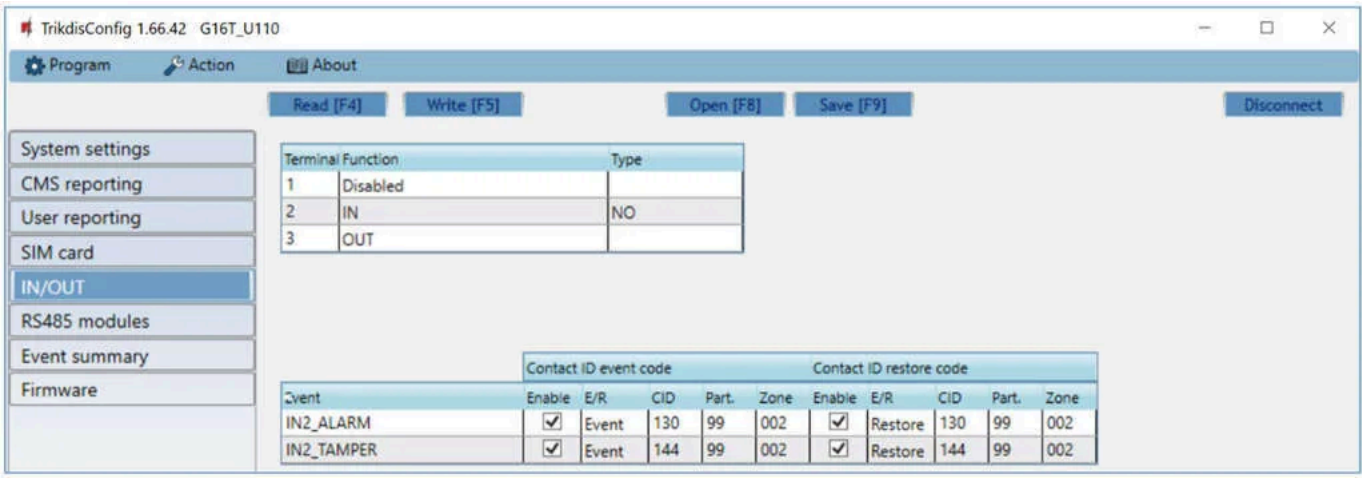


Figure 31. TrikdisConfig – page IN/OUT : fonction des bornes I/O et événements des entrées.

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

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

6.7 RS485 modules

Les modules d'extension de la série iO permettent d'ajouter au communicateur des entrées, des sorties et un bus série pour sondes de température. Les modules d'extension iO-8 (et les autres modules de la série iO) ainsi que les modules W485 / E485 raccordés au bus RS485 doivent être ajoutés dans l'onglet **Modules list**.

Sur le G16T à modem 2G (G16T_G410), cette page n'est pas utilisable : la version 2G n'a pas de bus RS485.

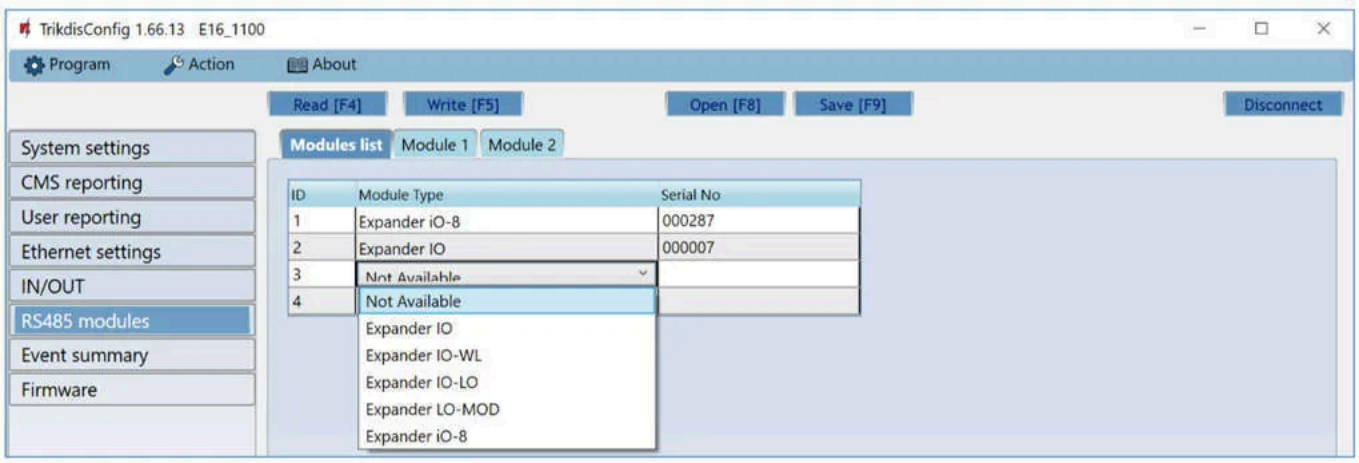


Figure 32. TrikdisConfig – RS485 modules, onglet Modules list.

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

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

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

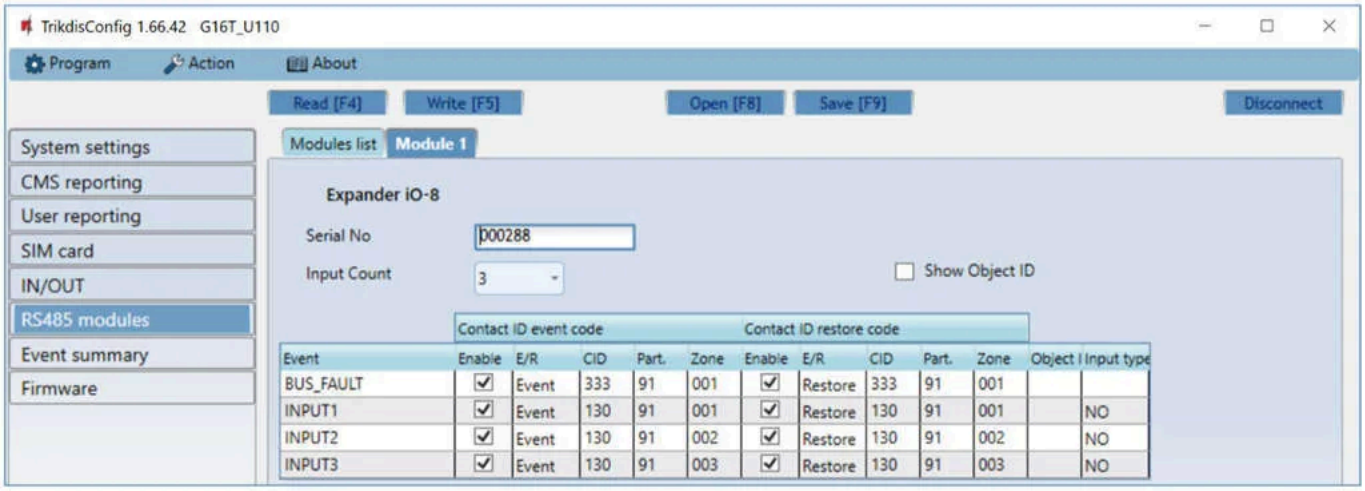


Figure 33. TrikdisConfig – RS485 modules, onglet du module iO-8.

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

Module d'extension iO – 1 entrée, 1 sortie relais (contacts de relais) et un bus série 1-Wire pour sondes de température. La sortie relais peut aussi être commandée selon des conditions logiques (SI … ALORS).

- **Input IN1 type** – le type d'entrée (NO ou NC).
- **Max °C (T1)** – si la température dépasse cette valeur, l'appareil envoie un événement ; pour cela, l'événement doit être activé dans le tableau.
- **Min °C (T2)** – si la température descend sous cette valeur, l'appareil envoie un événement ; pour cela, l'événement doit être activé dans le tableau.
- Dans le tableau, vous pouvez attribuer à l'entrée un code Contact ID d'événement et de rétablissement, comme pour le module iO-8 ; au déclenchement de l'entrée, le communicateur envoie un événement avec le code réglé au récepteur de télésurveillance et à Protegus 2.

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

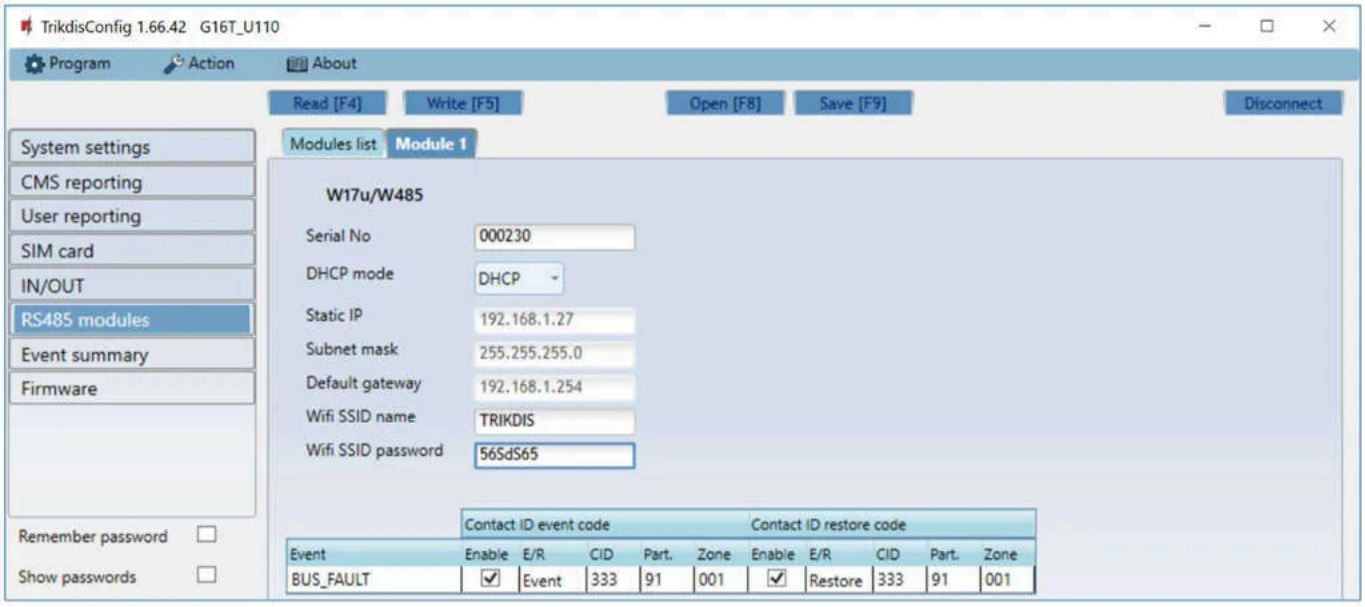


Figure 34. TrikdisConfig – RS485 modules, onglet du module W485.

- **DHCP mode** – réglage réseau automatique ou manuel.
- **Static IP**, **Subnet mask**, **Default gateway** – pour le réglage manuel.
- **Wifi SSID name**, **Wifi SSID password** – le nom et le mot de passe du réseau WiFi.
- Dans le tableau, vous pouvez attribuer un code Contact ID aux défauts du bus RS485 (interruption et rétablissement de la liaison entre le module et le G16T) ; le centre de télésurveillance et Protegus 2 reçoivent tous deux l'événement.

Module Ethernet E485 – les mêmes réglages réseau, sans WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**) ; vous pouvez de la même façon attribuer un code Contact ID aux défauts du bus RS485 (interruption et rétablissement de la liaison entre le module et le G16T) ; le centre de télésurveillance et Protegus 2 reçoivent tous deux l'événement.

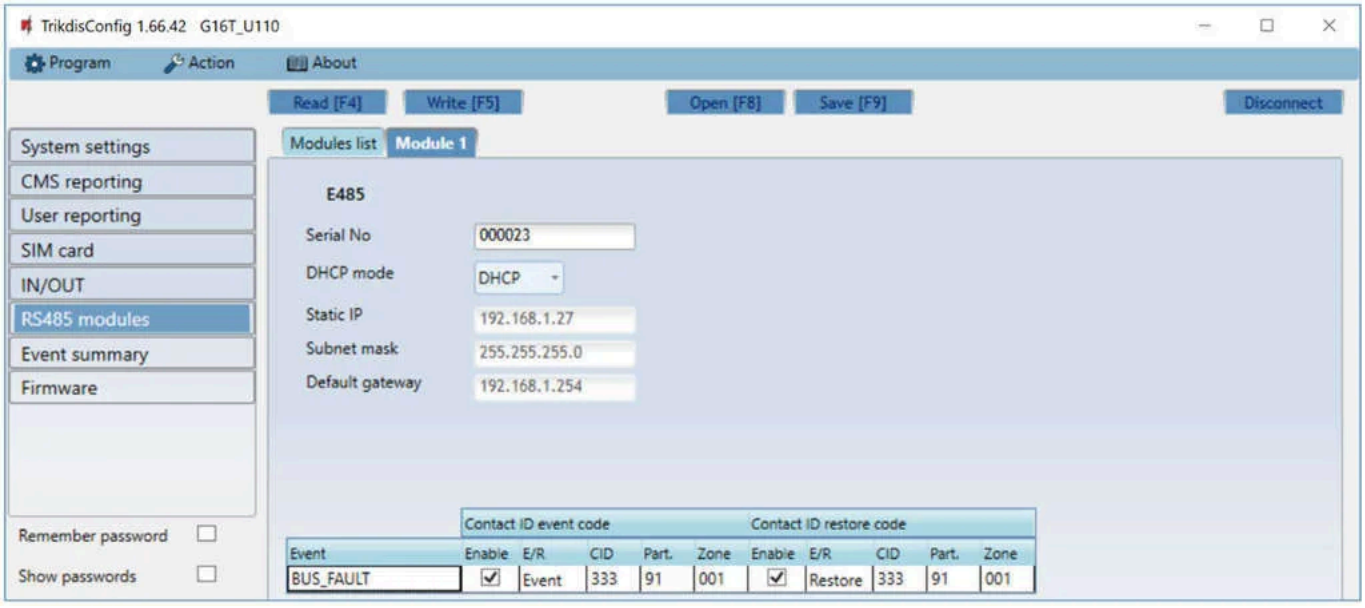


Figure 35. TrikdisConfig – RS485 modules, onglet du module E485.

Pour que le W485 et l'E485 fonctionnent, la connexion du G16T au centre de télésurveillance et/ou à Protegus doit être configurée (points 2.2 et 2.3) et, en règle générale, une carte SIM doit aussi être présente dans le G16T (si besoin, le fonctionnement sans carte SIM est possible : cette fonction a été ajoutée ultérieurement par Trikdis, sur demande).

6.8 Event summary

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

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

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

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

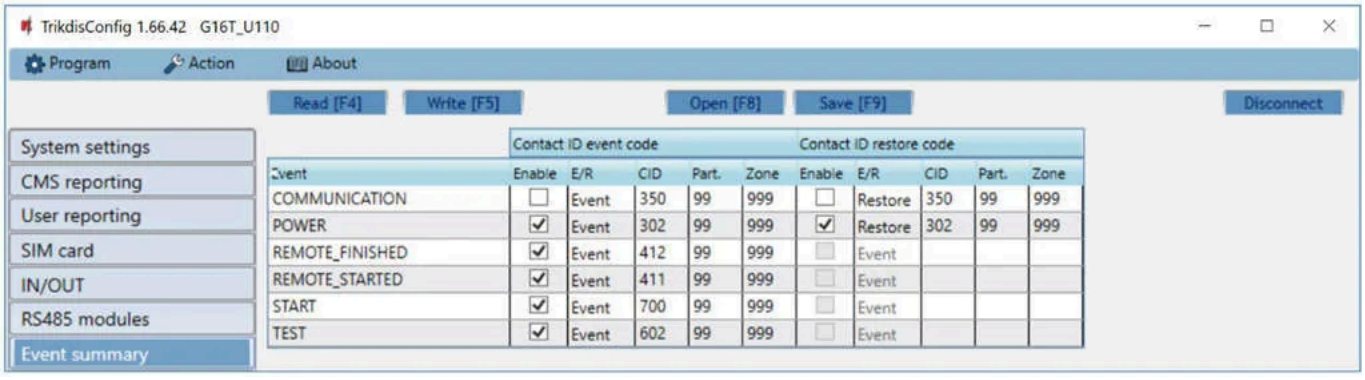


Figure 36. TrikdisConfig – page Event summary : messages internes de l'appareil.

6.9 Rétablissement des réglages d'usine

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

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

7. Programmation à distance

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

Conditions requises pour l'accès à distance :

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

Étapes :

1. Lancez le logiciel TrikdisConfig.
2. Dans la partie **Remote access**, saisissez l'identifiant unique de l'appareil (IMEI ou MAC) dans le champ **Unique ID**.
3. Si vous le souhaitez, donnez un nom au système dans le champ **System name** – le logiciel le mémorise et, la fois suivante, vous pourrez le choisir dans la liste déroulante.
4. Appuyez sur le bouton **Configure**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Read [F4]** (lecture) et saisissez le mot de passe. Avec la case **Remember password**, le logiciel le mémorise pour cette session.
6. Effectuez les modifications, puis envoyez-les à l'appareil avec le bouton **Write [F5]** (écriture).

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

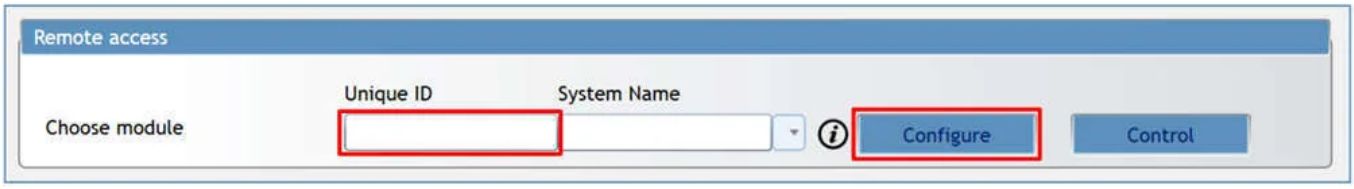


Figure 37. TrikdisConfig – Remote access : l'identifiant de l'appareil, le nom du système et le bouton Configure.

L'activation du cloud Protegus est décrite au point 6.4.

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.

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.

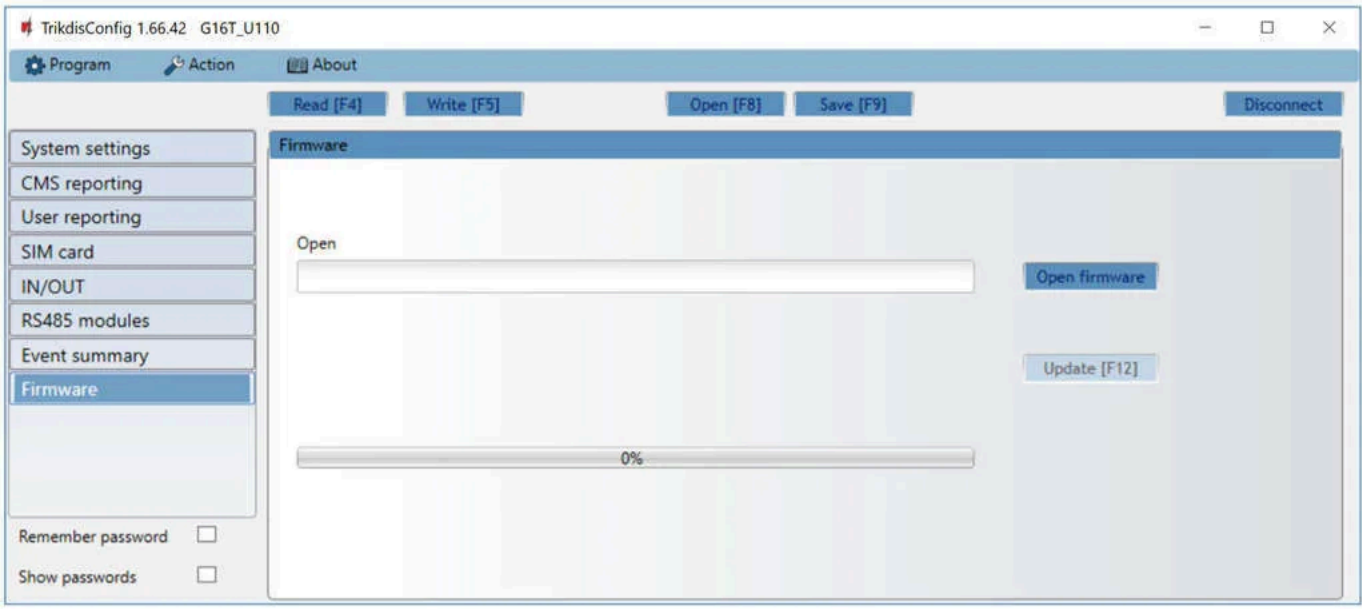


Figure 38. TrikdisConfig – page Firmware : Open firmware et Update [F12].

La mise à jour nécessite une connexion Internet. Un antivirus, un pare-feu ou des réglages réseau stricts peuvent empêcher le téléchargement automatique du firmware ; dans ce cas, téléchargez le fichier manuellement et ouvrez-le sur la page Firmware.

10. Dépannage et questions fréquentes

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

La LED NETWORK est éteinte – pas de réseau

1. Observez les clignotements de la LED **TROUBLE** : 1 = pas de SIM, 2 = code PIN incorrect, 3 = pas d'APN, 4 = impossible de se connecter au réseau GSM, 5 = impossible de se connecter au réseau de données.
2. Vérifiez que la carte SIM est active, qu'elle dispose d'un service de données et qu'elle est bien en place dans son logement.
3. Si la demande de code PIN est activée sur la carte, saisissez le code PIN sur la page **SIM card**, ou désactivez la demande de code PIN dans un téléphone.
4. Vérifiez l'antenne : elle est vissée, elle n'est pas dans un boîtier métallique, le niveau du signal est suffisant (points 1.6 et 3.2).

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

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

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

La centrale n'envoie pas les événements au communicateur

1. Le transmetteur de la centrale doit être activé, en mode DTMF, au format Contact ID, avec un numéro de téléphone saisi (chapitre 4).
2. Vérifiez le raccordement TIP/RING ; 7 clignotements de la LED **TROUBLE** signalent l'absence de liaison avec la centrale (en cas de raccordement avec supervision de ligne).
3. Si la centrale attend une tonalité et ne lance pas l'appel, désactivez la détection de tonalité dans la centrale.
4. Si la centrale signale une « erreur de communication » alors que l'événement est bien arrivé, vérifiez le réglage **Wait acknowledgment from CMS** (point 6.2).

Protegus 2 ne voit pas l'appareil

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

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

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

J'ai oublié le mot de passe

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

Pourquoi la page RS485 modules n'apparaît-elle pas, ou pourquoi l'iO-8 ne fonctionne-t-il pas ?

Le G16T à modem 2G (G16T_G410) n'a pas de bus RS485 ; les modules iO-8, W485 et E485 ne peuvent être raccordés qu'à la version 4G (G16T_E120). En règle générale, le module W485 ou E485 nécessite aussi une carte SIM dans le G16T ; si besoin, il peut aussi fonctionner sans carte SIM (fonction ajoutée ultérieurement par Trikdis, sur demande).

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

L'arrêt des réseaux 2G avance à un rythme différent selon les opérateurs ; pour un fonctionnement à long terme, nous recommandons la version 4G, qui dispose aussi d'un repli 2G. La version 4G peut en outre être étendue par le bus RS485.

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

Les messages d'événement et les PING sont très petits ; le trafic dépend 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.

- L'installation et la maintenance d'un équipement de sécurité ne doivent être effectuées que par un installateur qualifié.
- Lisez le manuel avant l'installation ; le non-respect des instructions peut entraîner un dysfonctionnement ou une panne.
- Avant le câblage, avant chaque raccordement électrique et avant toute intervention, déconnectez l'équipement de son alimentation.
- Les défauts résultant d'une installation ou d'une utilisation incorrecte, ainsi que les modifications et réparations non autorisées par le fabricant, annulent la garantie.
- Respectez la réglementation locale relative aux déchets : ne jetez pas l'appareil défectueux ni ses composants avec les ordures ménagères.

Voir aussi

- Armement à distance par zone à clé depuis l'application Protegus 2 – détails et pièges de l'armement par zone à clé.
- La version matérielle 4 des communicateurs GSM G16 et G16T arrive – ce qui a changé par rapport à la version précédente.
- Nouveautés du communicateur G16T v3 – l'annonce du produit.
- Documentation en anglais : docs.trikdis.com.

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

Produits associés

Trikdis G16T 4G GSM communicateur intelligent (TIP-RING)

Trikdis G16T 2G GSM communicateur intelligent (TIP-RING)

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-g16t