Communicateur incendie G17F – manuel d'installation et de programmation

Manuel d'installation et de programmation du communicateur incendie cellulaire Trikdis G17F (EN 54-21) : raccordement aux sorties ou au bus RS485 de la centrale incendie (ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP), configuration dans TrikdisConfig, télésurveillance, Protegus 2, commande par SMS et par appel.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-g17f

Sommaire

1. Présentation

1.1 À quoi il sert, comment il fonctionne
1.2 Versions
1.3 Caractéristiques techniques
1.4 Éléments de l'appareil
1.5 Les bornes
1.6 Voyants
1.7 Matériel nécessaire à l'installation

2. Configuration rapide avec le logiciel TrikdisConfig

2.1 Configuration pour l'application Protegus 2
2.2 Configuration pour le centre de télésurveillance

3. Installation et raccordement

3.1 Fixation et insertion de la carte SIM
3.2 Raccordement aux sorties de la centrale incendie
3.3 Centrale incendie à protocole ESPA 4.4.4
3.4 Centrale incendie NSC Solution
3.5 Centrale incendie INIM Smartline
3.6 Centrale incendie C-TEC Cast ZFP
3.6.1 Configuration de la centrale C-TEC (ZFPtools)
3.7 Raccordement des entrées
3.8 Modules d'extension de la série iO
3.9 Module d'extension iO-8
3.10 Modules d'extension de la série LORA
3.11 Module WiFi W485
3.12 Module Ethernet E485
3.13 Mise sous tension du communicateur

4. Commande à distance

4.1 Ajout du G17F à Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.2 Configuration et commande par SMS
4.3 Commande des sorties PGM par appel téléphonique

5. Les pages de TrikdisConfig

5.1 La barre d'état
5.2 Page « System Options »
5.3 Page « Reporting to CMS »
5.4 Page « Users & Reporting »
5.5 Page « Modules »
5.6 Page « Zones »
5.7 Page « PGM »
5.8 Page « System events »
5.9 Page « Events Log »
5.10 Rétablissement des réglages d'usine

6. Programmation à distance

7. Vérification du fonctionnement

8. Mise à jour du firmware

9. Dépannage et questions fréquentes

10. Consignes de sécurité

Voir aussi

1. Présentation

Le **G17F** est un communicateur incendie qui permet de transmettre par le réseau mobile les événements de n'importe quel équipement ou centrale de détection incendie. Lorsqu'une entrée (zone) est violée, c'est-à-dire lorsqu'une alarme incendie arrive, l'événement est transmis aux destinataires configurés, par exemple aux pompiers et au centre de télésurveillance. En outre, le propriétaire est lui aussi informé de l'événement dans l'application mobile et web **Protegus 2**.

Le G17F transmet les messages de la centrale incendie par le réseau mobile. **Principe de fonctionnement :** lorsqu'une entrée (zone) du communicateur est violée, le G17F envoie un message d'événement par l'Internet mobile au récepteur du centre de télésurveillance ou à l'application Protegus 2 ; il peut en outre envoyer un SMS et passer un appel téléphonique. Le communicateur est disponible avec un modem 2G ou 4G. Vous effectuez les réglages avec le logiciel **TrikdisConfig**, par câble USB ou à distance.

Certification	Donnée
Norme	Le G17F satisfait aux exigences de la norme **EN 54-21:2006** et remplit les exigences de performance prescrites à l'annexe A de l'EN 54-21 pour un système de transmission de **type 1**.
Certificat	**1922-CPR-1974** – Systèmes de détection et d'alarme incendie. Matériel de transmission d'alarme et de signalisation de dérangement.
Organisme de certification	Organisme notifié de certification de produits n° 1922 « Dedal » – Nesebar, Mladost str. 50, 8230 Bulgarie
Assistance technique Trikdis	support@trikdis.lt, +37067422877

1.1 À quoi il sert, comment il fonctionne

Liaison avec la centrale incendie

- Raccordé aux sorties de la centrale : les sorties d'état de la centrale (alarme, défaut, etc.) sont raccordées aux entrées du G17F (point 3.2).
- Par le bus RS485 : avec les centrales incendie à protocole **ESPA 4.4.4**, **NSC Solution**, **INIM Smartline** et **C-TEC Cast ZFP** (points 3.3–3.6).

Messages au centre de télésurveillance

- Il envoie les événements aux récepteurs logiciels et matériels de Trikdis, qui fonctionnent avec n'importe quel logiciel de télésurveillance.
- Il peut aussi envoyer les événements à des récepteurs SIA DC-09.
- Si la liaison est interrompue sur le canal principal, les messages partent automatiquement vers le récepteur de secours.
- Il peut aussi signaler les événements au centre de télésurveillance par SMS – c'est extrêmement utile, car cela fonctionne même lorsque la liaison IP tombe sur le réseau de l'opérateur mobile.
- Il détecte le brouillage du réseau mobile (jamming).
- Il peut transmettre simultanément au centre de télésurveillance et à l'application Protegus 2 ; la transmission au centre de télésurveillance peut être prioritaire.
- Il envoie les messages d'événement avec des codes Contact ID.

Messages aux utilisateurs

- Il appelle les numéros de téléphone choisis (8 utilisateurs au maximum).
- Il envoie des SMS sur les événements.
- Il envoie des notifications push et des notifications d'événement avec une sonnerie spéciale dans l'application Protegus 2.

Commande à distance des sorties

- depuis l'application Protegus 2 ;
- en appelant le numéro de téléphone de l'appareil ;
- par SMS.

Configuration et installation

- Configuration par câble USB ou à distance, avec le logiciel TrikdisConfig.
- Mise à jour du firmware à distance.
- Deux niveaux d'accès (types de compte) aux réglages : installateur et administrateur.

Entrées et sorties

- 3 entrées, type au choix : NO, NC, EOL (4,7 kΩ, 10 kΩ).
- 3 bornes à double usage, configurables en entrée (IN) ou en sortie (OUT) ; en entrée, type au choix : NO, NC, EOL (4,7 kΩ, 10 kΩ).
- Bus RS485 pour les modules d'extension de la série iO.
- Avec les modules d'extension de la série iO, le nombre d'entrées (IN) ou de sorties (OUT) peut être porté à 12.

1.2 Versions

Le G17F est disponible en deux versions cellulaires : avec un modem 2G ou 4G. Ce manuel s'applique aux deux ; la différence réside dans le modem et les bandes du réseau mobile.

Version	Modem	Bandes
G17F-4G	4G (LTE)	700 / 800 / 900 / 1800 / 2100 / 2600 MHz
G17F-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis G17F 4G GSM / IP communicateur incendie

Trikdis G17F 2G GSM / IP communicateur incendie

En raison de l'arrêt progressif des réseaux 2G, nous recommandons la version 4G pour toute nouvelle installation.

1.3 Caractéristiques techniques

Caractéristique	Valeur
Bandes du modem 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Bandes du modem 4G (LTE)	700 / 800 / 900 / 1800 / 2100 / 2600 MHz

Caractéristique	Valeur
Tension d'alimentation	9–32 V DC
Consommation	100 mA
Protocole de transmission	TRK, SIA DC-09_2007, SIA DC-09_2012
Clé de chiffrement	6 caractères
Liaison avec le centre de télésurveillance	TCP/IP ou UDP/IP, SMS
Codes d'événement	Contact ID
Mémoire de messages	60 messages au maximum
Entrées et sorties	3 entrées : NO, NC, EOL (4,7 kΩ, 10 kΩ) ; 3 bornes à double usage (IN/OUT) : en entrée NO, NC, EOL (4,7 kΩ, 10 kΩ), en sortie à collecteur ouvert (OC), 100 mA au maximum
Journal des événements	1000 événements au maximum
Configuration	à distance avec le logiciel TrikdisConfig ou sur place par câble USB Mini-B ; à distance par SMS
Longueur du bus RS485	100 m au maximum
Modules pris en charge	module d'extension **iO** ; **iO-WL** – **iO-MOD** – émetteur-récepteur radio iO-WL ; module d'extension **iO-8** ; module Ethernet **E485** ; module WiFi **W485 (W17u)** ; module d'extension **iO-LORA** ; module d'extension **iO8-LORA** ; bouton panique **PB-LORA** ; module d'extension **REL-LORA** ; centrales incendie **INIM Smartline**, **NSC Solution** et **C-TEC Cast ZFP** ; centrales incendie à protocole **ESPA 4.4.4**
Environnement de fonctionnement	–10 … +50 °C, humidité relative de 80 % au maximum à +20 °C
Dimensions	92 × 62 × 25 mm
Poids	80 g

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.

1.4 Éléments de l'appareil

Les numéros de la figure désignent les éléments de l'appareil : à gauche la face avant, à droite le circuit imprimé, face avant retirée.

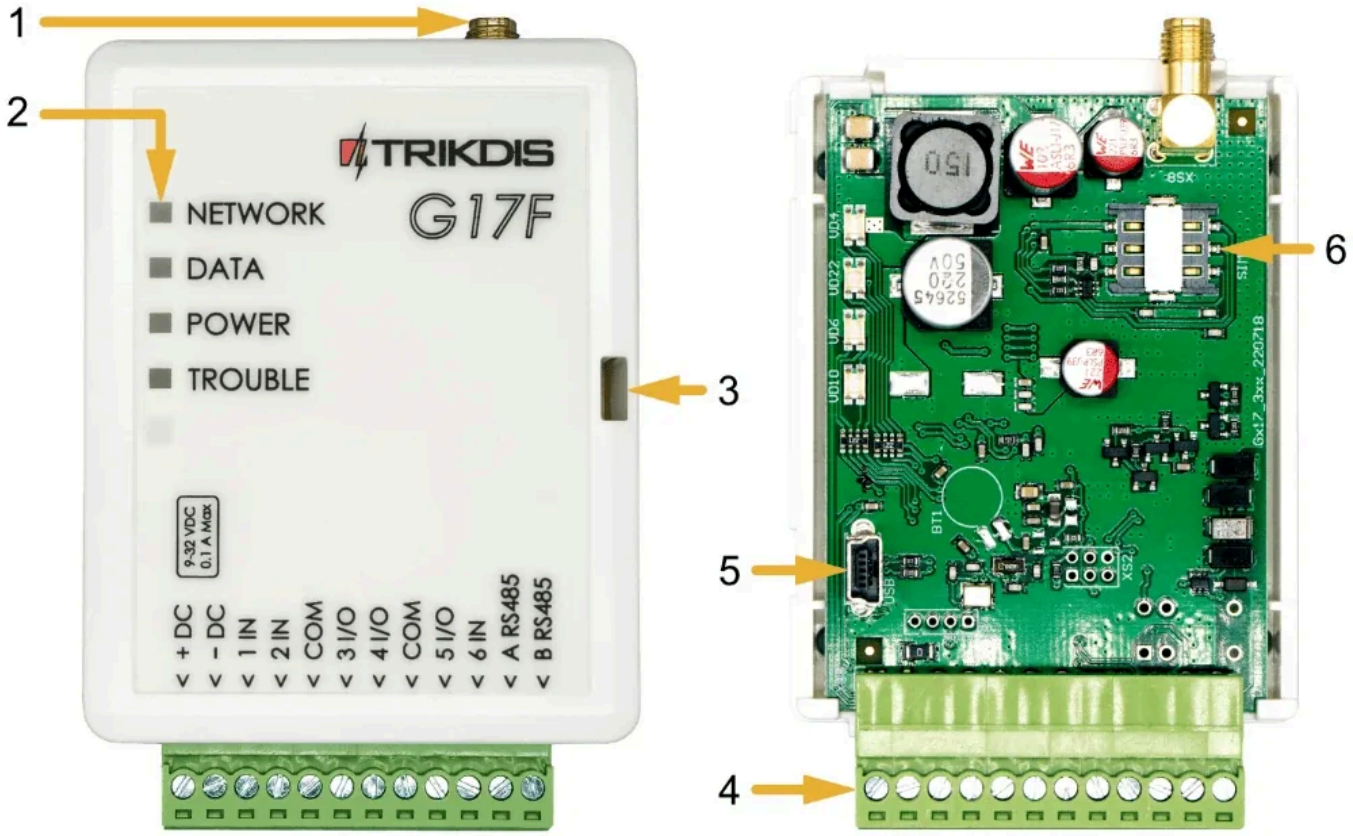


Figure 1. Les éléments du G17F.

- 1 connecteur SMA de l'antenne du réseau mobile
- 2 voyants (LED)
- 3 ouverture servant à retirer la face avant
- 4 bornier pour le raccordement des fils
- 5 connecteur USB Mini-B pour la programmation
- 6 support de la carte nano-SIM

1.5 Les bornes

Les noms des bornes figurent sur la face avant, au-dessus du bornier (de gauche à droite).

Borne	Fonction
+DC	alimentation : pôle positif 9–32 V DC
–DC	alimentation : pôle négatif 9–32 V DC
1 IN	entrée 1, type au choix : NO, NC, EOL (par défaut EOL, 10 kΩ)
2 IN	entrée 2, type au choix : NO, NC, EOL (par défaut EOL, 10 kΩ)
COM	borne commune (négative)
3 I/O	borne 3 à double usage (IN/OUT) : en entrée NO, NC, EOL (par défaut EOL, 10 kΩ), en sortie à collecteur ouvert (OC), 100 mA au maximum
4 I/O	borne 4 à double usage (IN/OUT) : en entrée NO, NC, EOL (par défaut EOL, 10 kΩ), en sortie à collecteur ouvert (OC), 100 mA au maximum
COM	borne commune (négative)
5 I/O	borne 5 à double usage (IN/OUT) : en entrée NO, NC, EOL (par défaut EOL, 10 kΩ), en sortie à collecteur ouvert (OC), 100 mA au maximum

Borne	Fonction
6 IN	entrée 6, type au choix : NO, NC, EOL (par défaut EOL, 10 kΩ)
A RS485, **B RS485**	bus RS485 : pour raccorder les modules d'extension iO, les centrales incendie INIM Smartline, NSC Solution et C-TEC Cast ZFP, les centrales incendie à protocole ESPA 4.4.4, ainsi que les modules E485 et W485

1.6 Voyants

Voyant	Lumière	Signification
NETWORK	éteint	non connecté au réseau mobile
	vert fixe et clignotement jaune	connecté au réseau mobile ; le nombre de clignotements jaunes indique le niveau du signal : sur un réseau 2G (GPRS), 5 clignotements suffisent, sur un réseau 4G, 3 clignotements suffisent
DATA	vert fixe	envoi d'un message en cours
	jaune fixe	des événements non envoyés se trouvent en mémoire
POWER	clignotement vert	la tension d'alimentation est correcte
	clignotement jaune	la tension d'alimentation n'est pas correcte
	clignotement vert et jaune	mode configuration
TROUBLE	éteint	aucun défaut de fonctionnement
	1 clignotement	pas de carte SIM
	2 clignotements	le code PIN de la carte SIM est erroné
	3 clignotements	impossible de se connecter au réseau mobile
	4 clignotements	impossible de se connecter au récepteur IP sur le canal principal
	5 clignotements	impossible de se connecter au récepteur IP sur le canal de secours
	6 clignotements	l'horloge interne du G17F n'est pas réglée
	7 clignotements	la tension d'alimentation n'est pas correcte
	9 clignotements	défaut de liaison avec le module RS485

La signalisation correcte après la mise sous tension et l'évaluation du niveau du signal sont décrites au point 3.13.

1.7 Matériel nécessaire à l'installation

Avant de commencer l'installation, vérifiez que vous avez tout sous la main :

1. câble USB Mini-B pour la configuration ;
2. câble d'au moins 4 conducteurs pour relier le G17F à la centrale incendie ;
3. tournevis plat de 2,5 mm ;
4. antenne externe pour réseau mobile, si le signal est faible sur le site ;
5. carte nano-SIM activée (la demande de code PIN peut être désactivée) ;
6. le manuel de la centrale incendie à laquelle vous raccordez le G17F.

Les accessoires énumérés doivent être achetés séparément – commandez-les auprès de votre revendeur. Si le signal est faible sur le site, utilisez une antenne filaire déportée :

Antenne magnétique Trikdis ME301m avec fil 2,5 m

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

2. Configuration rapide avec le logiciel TrikdisConfig

Ce chapitre décrit les réglages qui permettent au G17F d'envoyer les événements à l'application Protegus 2 (point 2.1) ou au centre de télésurveillance (point 2.2). Les autres réglages du G17F se trouvent au chapitre 5.

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!

1. Retirez la face avant du G17F avec un tournevis plat, comme le montre la figure.



Figure 2. Retrait de la face avant : insérez le tournevis dans l'ouverture latérale et poussez-le vers le bas, le couvercle se détache ; en dessous se trouve le connecteur USB Mini-B.

2. Reliez le G17F à l'ordinateur avec un câble **USB Mini-B**.
3. Lancez TrikdisConfig. Le logiciel reconnaît automatiquement l'appareil raccordé et ouvre la fenêtre de programmation du G17F.
4. Cliquez sur le bouton **Read [F4]** : le logiciel lit et affiche les réglages actuels du G17F. Si le logiciel demande le code administrateur ou le code installateur, saisissez le code à 6 chiffres.

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

2.1 Configuration pour l'application Protegus 2

Dans le groupe **Cloud application** de la page **Users & Reporting** :

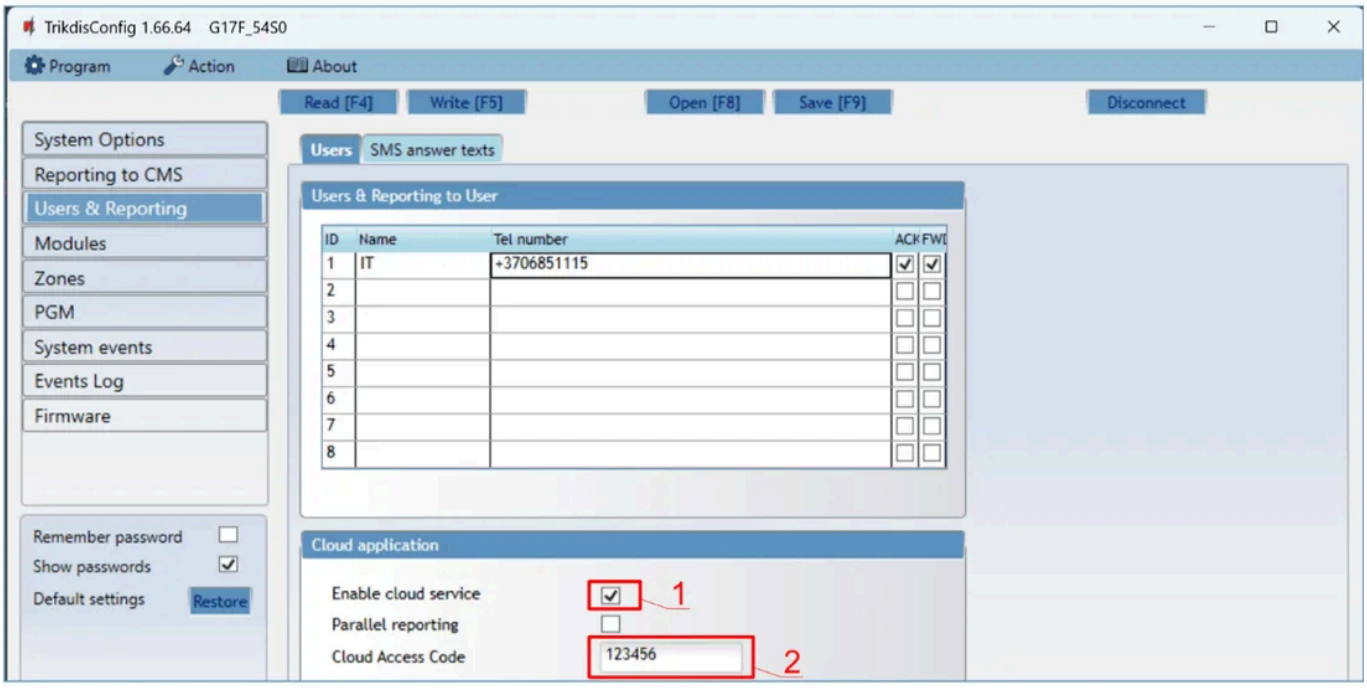


Figure 3. TrikdisConfig – **Users & Reporting**, groupe **Cloud application**.

- 1 **Enable cloud service** – activation du cloud Protegus
- 2 **Cloud Access Code** – le code d'accès au cloud (par défaut `123456`)

1. Cochez la case **Enable cloud service**.
2. Si vous souhaitez que les utilisateurs doivent saisir le code lorsqu'ils ajoutent le système dans Protegus 2, modifiez la valeur du **Cloud Access Code** (par défaut `123456`).

Dans le groupe **SIM** de la page **System Options** :

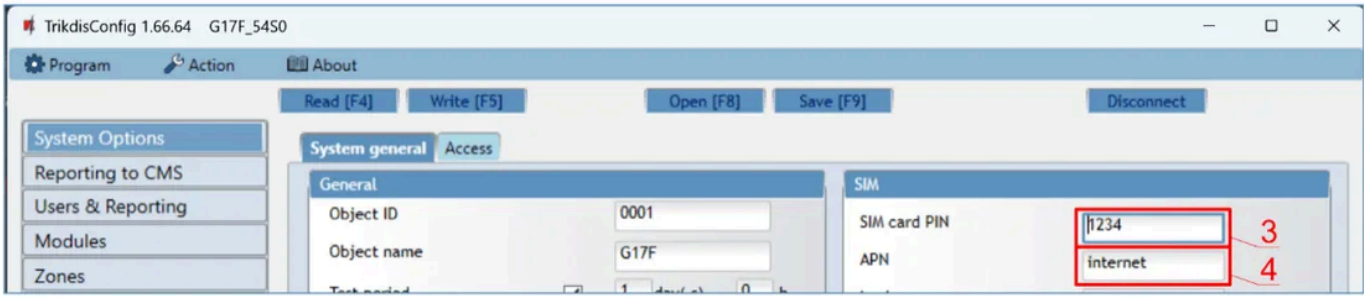


Figure 4. TrikdisConfig – **System Options**, groupe **SIM**.

- 3 **SIM card PIN** – le code PIN de la carte SIM
- 4 **APN** – le point d'accès à l'Internet mobile

3. Saisissez le code PIN de la carte SIM (**SIM card PIN**).
4. Si nécessaire, modifiez le champ **APN**. Vous trouverez l'APN sur le site de l'opérateur mobile ; « internet » est générique et fonctionne sur le réseau de la plupart des opérateurs. Les données des opérateurs de votre pays et des autres opérateurs européens : Réglage de l'APN – liste des opérateurs mobiles européens.
5. Sur la page **Zones**, cochez la case **Prot.** pour les zones dont les changements d'état doivent être notifiés aux utilisateurs dans Protegus 2 (point 5.6).
6. Sur la page **PGM**, cochez la case **Prot.** pour les sorties PGM dont les changements d'état doivent être notifiés aux utilisateurs dans Protegus 2 (point 5.7).

7. Sur la page **System events**, cochez la case **Prot.** pour les événements internes du communicateur dont les changements d'état doivent être notifiés aux utilisateurs dans Protegus 2 (point 5.8).

À la fin des réglages, cliquez sur le bouton **Write [F5]** et débranchez le câble USB. Ajout du système à l'application Protegus 2 : point 4.1.

2.2 Configuration pour le centre de télésurveillance

Les réglages de télésurveillance se trouvent sur deux pages. Sur la page **System Options** :

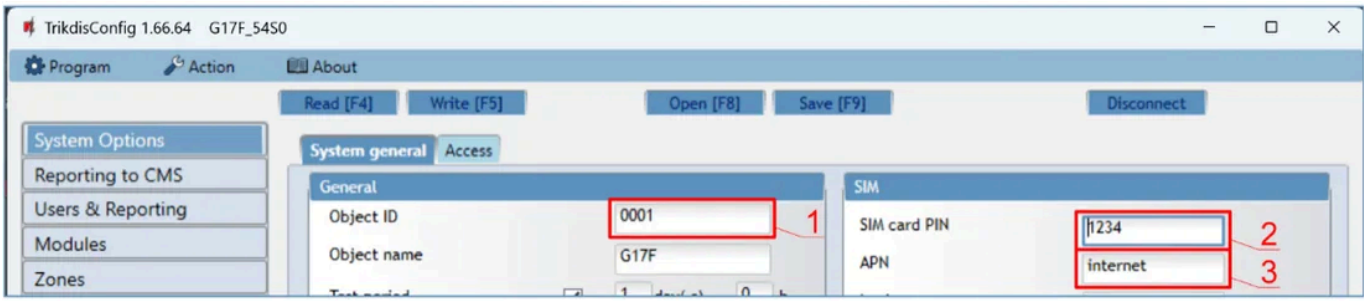


Figure 5. TrikdisConfig – **System Options**.

- 1 **Object ID** – identifiant de l'objet
- 2 **SIM card PIN** – le code PIN de la carte SIM
- 3 **APN** – le point d'accès à l'Internet mobile

1. Saisissez l'identifiant de l'objet (**Object ID**) fourni par le centre de télésurveillance : 4 caractères, 0–9 et A–F. N'utilisez pas les identifiants FFFE et FFFF.
2. Saisissez le code PIN de la carte SIM.
3. Si nécessaire, modifiez le champ **APN**. Vous trouverez l'APN sur le site de l'opérateur mobile ; « internet » est générique et fonctionne sur le réseau de la plupart des opérateurs.

Sur la page **Reporting to CMS** :

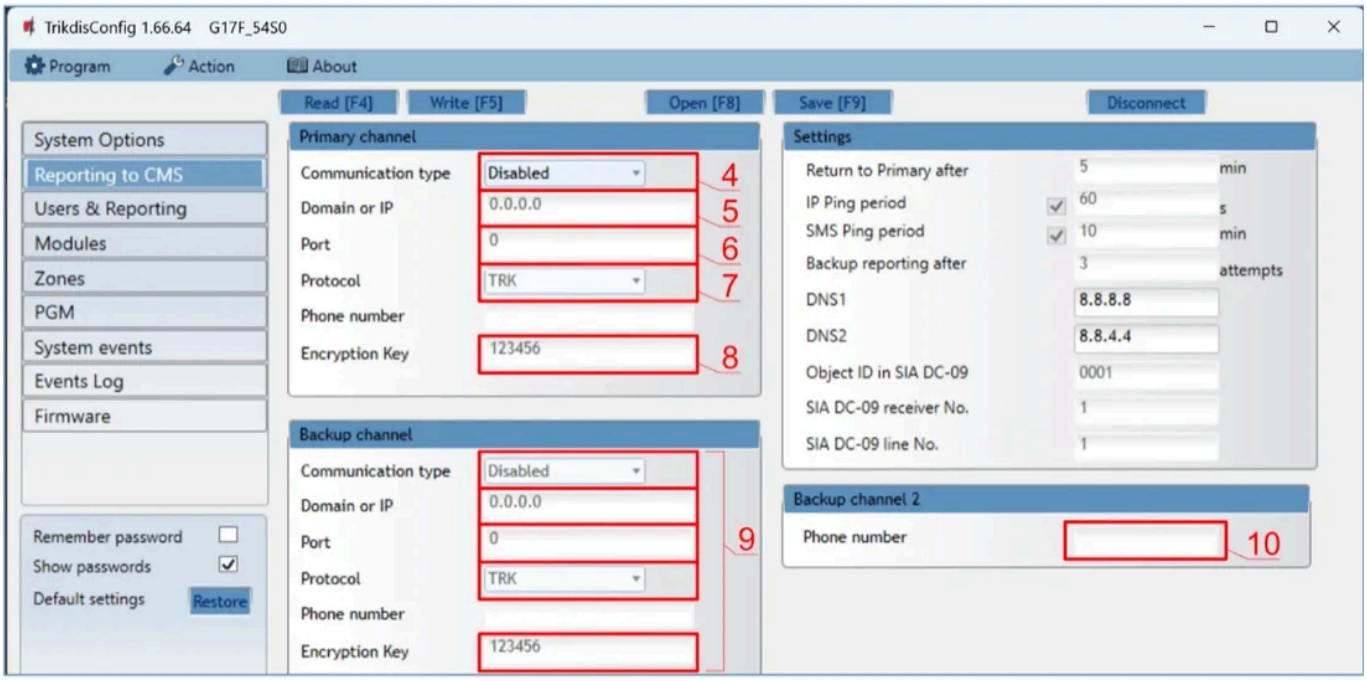


Figure 6. TrikdisConfig – **Reporting to CMS**.

- 4 **Communication type** – le type de liaison
- 5 **Domain or IP** – l'adresse du récepteur
- 6 **Port** – le port du récepteur
- 7 **Protocol** – protocole de transmission
- 8 **Encryption Key** – clé de chiffrement
- 9 **Backup channel** – le canal de secours
- 10 **Backup channel 2** – le numéro de téléphone du récepteur SMS

4. **Communication type** – choisissez le type de liaison (nous ne recommandons pas le SMS sur le canal principal).
5. **Domain or IP** – saisissez le nom de domaine ou l'adresse IP du récepteur.
6. **Port** – saisissez le port réseau du récepteur.
7. **Protocol** – choisissez le protocole avec lequel l'appareil envoie les messages : **TRK** (pour les récepteurs Trikdis), **DC-09_2007** ou **DC-09_2012** (pour les récepteurs universels).
8. **Encryption Key** – saisissez la clé de chiffrement du récepteur.

Si vous transmettez au centre de télésurveillance par SMS, il suffit de remplir les champs **Encryption Key** et **Phone number**. Les SMS sont reçus par le récepteur IP/SMS **RL14**, le récepteur multicanal **RM14** et le récepteur SMS **GM14** de Trikdis. Si vous choisissez DC-09 comme protocole de transmission, indiquez aussi le numéro d'objet, de ligne et de récepteur dans le groupe **Settings** de la page **Reporting to CMS** (point 5.3).

9. (Recommandé) Configurez le canal de secours (**Backup channel**).
10. (Recommandé) Saisissez le numéro de téléphone du **Backup channel 2**.

À la fin des réglages, cliquez sur le bouton **Write [F5]** et débranchez le câble USB. Les autres réglages du G17F sont décrits au chapitre 5.

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.

Ce chapitre décrit la fixation du G17F, le raccordement de la centrale incendie (aux sorties de la centrale ou, par le bus RS485, aux centrales à protocole ESPA 4.4.4, NSC Solution, INIM Smartline et C-TEC Cast ZFP), le raccordement des entrées et des modules d'extension (iO, iO-8, LORA, W485, E485) et enfin la mise sous tension du communicateur. Sur les schémas, les noms des bornes du G17F correspondent aux inscriptions de l'appareil (point 1.5).

3.1 Fixation et insertion de la carte SIM

1. Avant l'installation, assurez-vous que le niveau du signal du réseau mobile est suffisant à l'emplacement de montage du G17F.
2. Retirez la face avant et débranchez le bornier.
3. Retirez le circuit imprimé.
4. Fixez le fond du boîtier à l'emplacement voulu avec des vis.
5. Remettez en place le circuit imprimé et le bornier.
6. Vissez l'antenne du réseau mobile.
7. Insérez la carte nano-SIM. La carte SIM doit être enregistrée sur un réseau mobile, et ses services doivent être activés et fonctionner : elle doit pouvoir appeler, envoyer et recevoir des SMS, et disposer de données mobiles. Renseignez-vous auprès de l'opérateur mobile de la carte SIM pour activer les services souhaités.

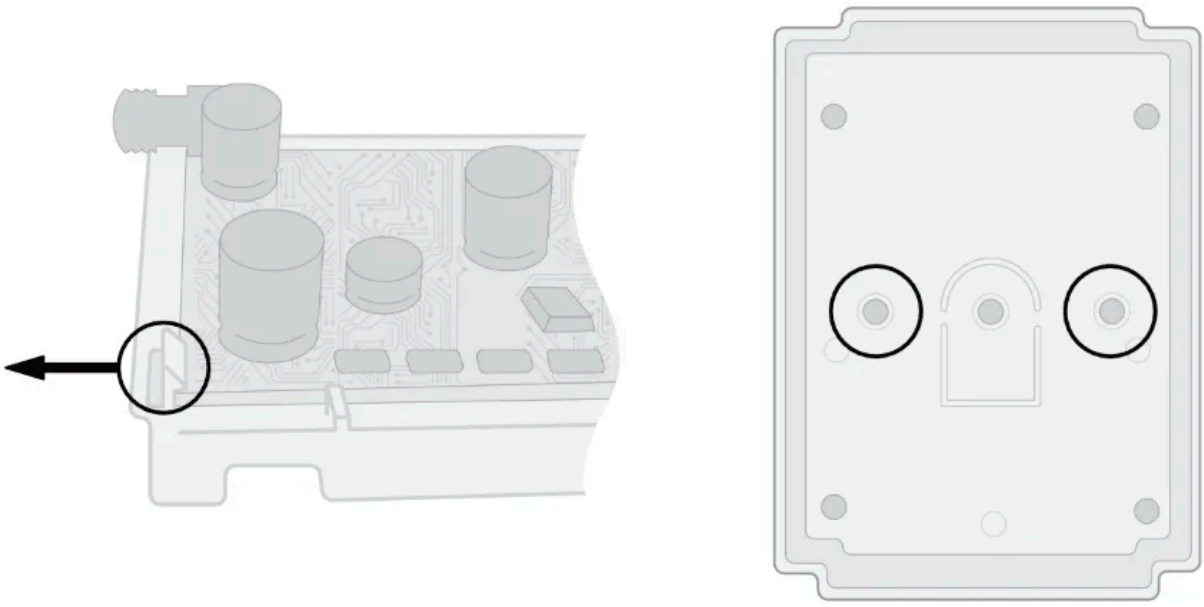


Figure 7. À gauche, l'ergot de fixation du circuit imprimé sur le bord gauche de la carte (il permet de libérer la carte du boîtier) ; à droite, les deux trous de vis du fond du boîtier.

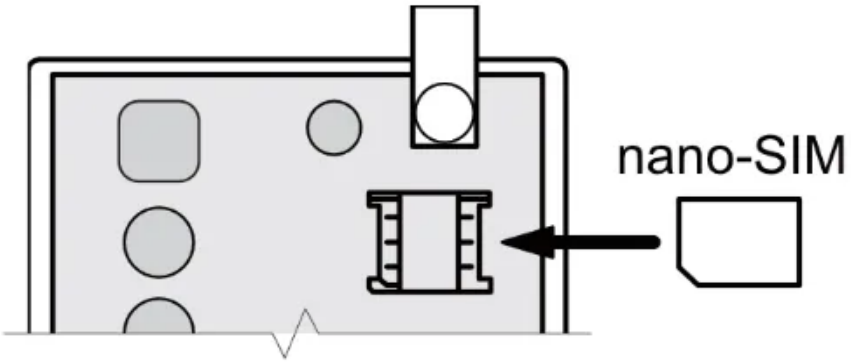


Figure 8. Insertion de la carte nano-SIM par la droite dans le support situé sur le circuit imprimé.

- Vérifiez que la carte SIM est activée.
- Si vous communiquez aussi par un canal IP ou avec l'application Protegus 2, vérifiez que les données mobiles sont activées.
- Si vous ne voulez pas saisir le code PIN dans TrikdisConfig, insérez la carte SIM dans un téléphone et désactivez la demande de code PIN.

8. Pour configurer le G17F à distance, insérez une carte SIM dont la demande de code PIN est désactivée et mettez le communicateur sous tension. Si le G17F n'a pas encore été configuré avec TrikdisConfig et que le service Protegus n'est pas activé, envoyez-lui ce SMS :

```
CONNECT 123456 PROTEGUS=ON,APN=INTERNET
```

9. Le réglage des paramètres à distance est décrit au chapitre 6.
10. Remettez la face avant en place.

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

3.2 Raccordement aux sorties de la centrale incendie

Si vous souhaitez surveiller l'état de la centrale incendie, raccordez les sorties correspondantes de la centrale aux entrées du G17F. Les sorties de la centrale (**PGM1**, **PGM2**, **PGM3**) doivent être configurées dans la centrale comme sorties d'état (alarme, défaut, etc.).

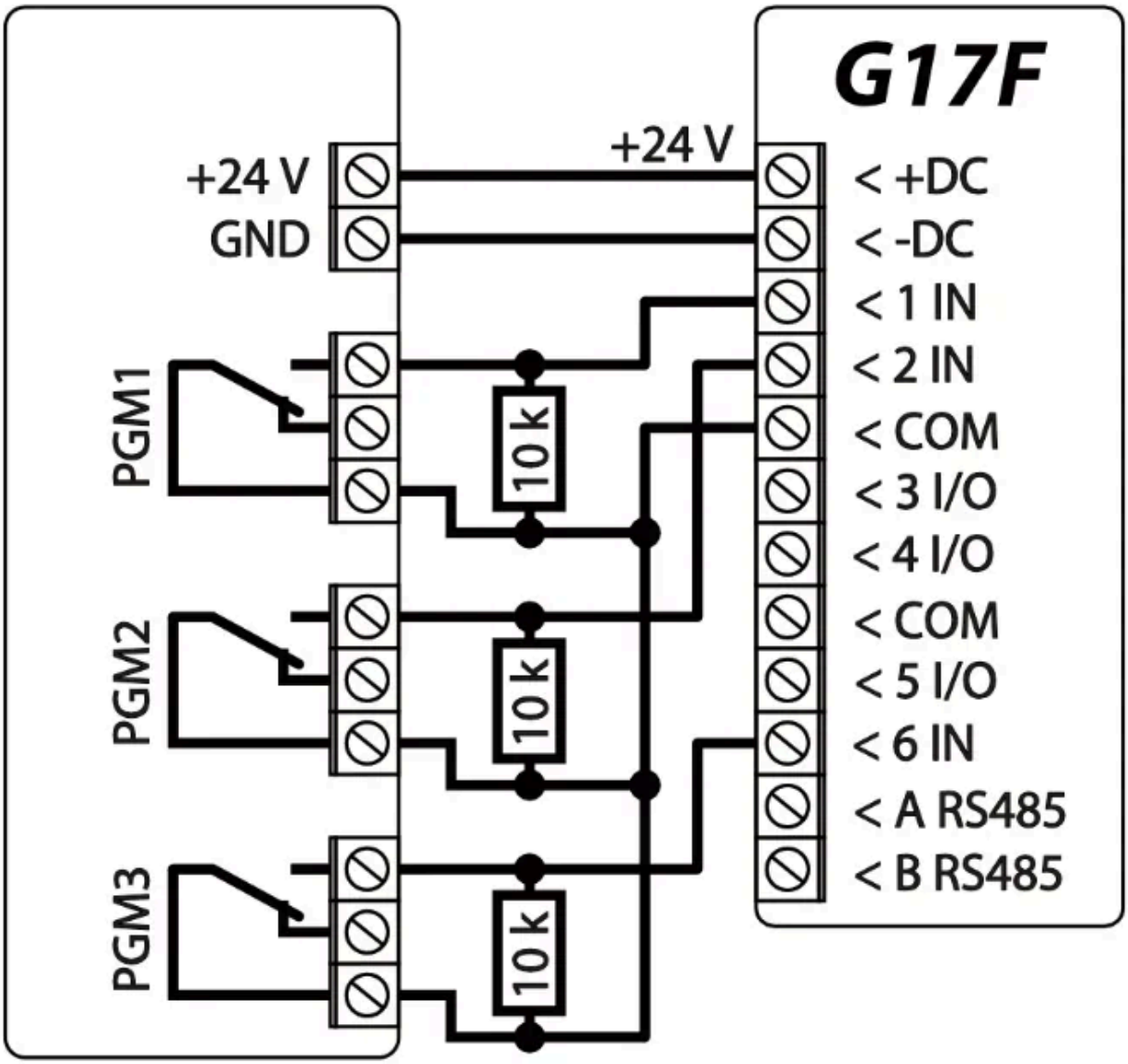


Figure 9. Raccordement du G17F aux sorties de la centrale incendie (**Fire control panel**). Inscriptions du schéma : la borne **+24 V** de la centrale va sur la borne **+DC** du G17F, la borne **GND** sur la borne **–DC** ; l'un des fils des sorties **PGM1**, **PGM2** et **PGM3** va respectivement sur l'entrée **1 IN**, **2 IN** et **6 IN** du G17F, l'autre sur la borne **COM** ; une résistance de **10 k** (10 kΩ) est placée en parallèle entre les deux fils de chaque sortie.

3.3 Centrale incendie à protocole ESPA 4.4.4

Raccordez la centrale incendie à protocole ESPA 4.4.4 au G17F par le bus RS485, selon le schéma ci-dessous.

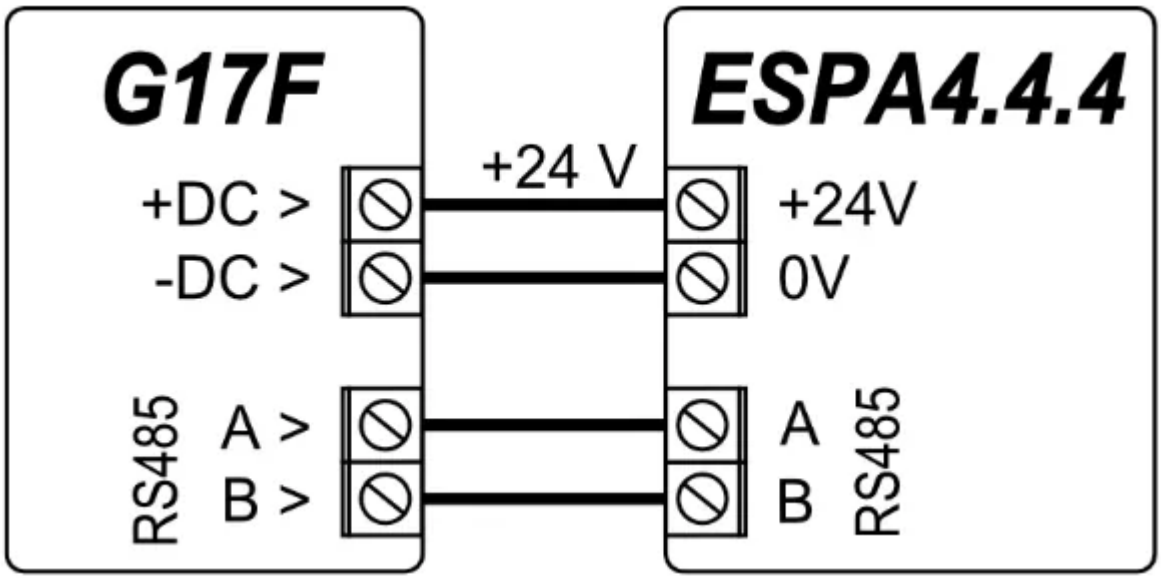


Figure 10. Liaison entre le G17F et la centrale incendie à protocole ESPA 4.4.4. Inscriptions du schéma : alimentation – la borne **+DC** du G17F va sur la borne **+24V** de la centrale, la borne **–DC** sur la borne **0V** ; RS485 – la borne **A** du G17F va sur la borne **A** de la centrale, la borne **B** sur la borne **B**.

Configuration du G17F dans TrikdisConfig lorsqu'il est raccordé à une centrale incendie à protocole ESPA 4.4.4 :

1. Sur la page **Modules**, choisissez le protocole **ESPA 4.4.4**.
2. Choisissez la vitesse de transmission de l'interface (**Baudrate**).
3. Les paramètres de transmission du G17F et de la centrale incendie doivent être identiques.

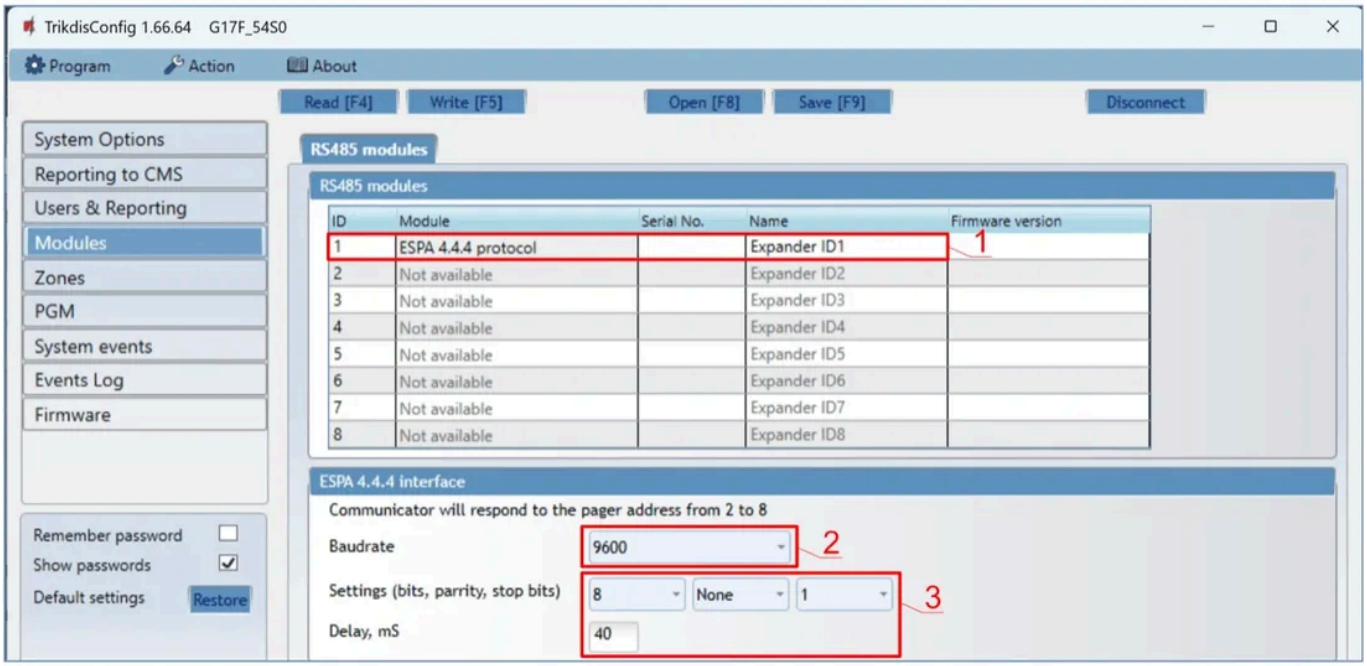


Figure 11. TrikdisConfig – **Modules** : le module RS485 n° 1 est **ESPA 4.4.4 protocol**. Inscription du groupe **ESPA 4.4.4 interface** : « Communicator will respond to the pager address from 2 to 8 » – le communicateur répond aux adresses de récepteur de radiomessagerie (pager address) 2 à 8.

- 1 sélection de **ESPA 4.4.4 protocol**
- 2 **Baudrate** – vitesse de transmission (9600 sur l'image)
- 3 bits de données, parité, bits d'arrêt et délai (8, None, 1, 40 ms sur l'image)

4. Sur la page **Users & Reporting**, saisissez les numéros de téléphone des utilisateurs qui reçoivent des messages du G17F (point 5.4).
5. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**) dans l'onglet **SMS & Call reporting** de la page **System events**.

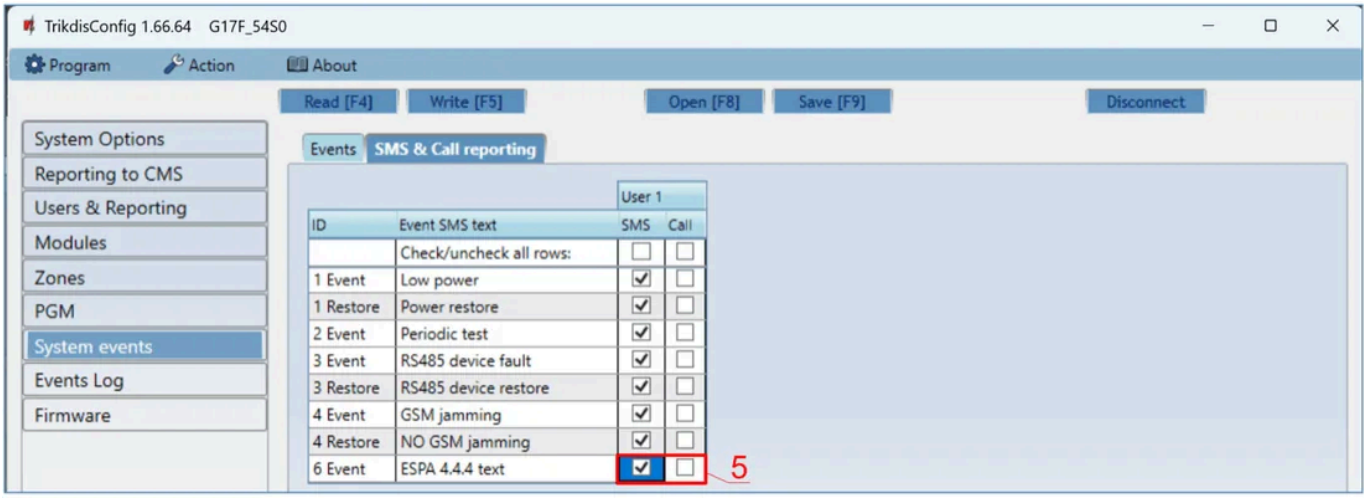


Figure 12. TrikdisConfig – **System events**, onglet **SMS & Call reporting** : pour l'utilisateur 1, la case **SMS** est cochée pour l'événement **ESPA 4.4.4 text**.

- 5 les cases **SMS** et **Call** de l'événement **ESPA 4.4.4 text**

6. Si les messages doivent aussi parvenir au récepteur du centre de télésurveillance, configurez le canal de communication sur la page **Reporting to CMS** (points 2.2 et 5.3). Les messages d'événement sont envoyés avec le protocole **SIA DC-09**.

Testez le système : déclenchez une alarme incendie et vérifiez que les messages du G17F arrivent au centre de télésurveillance et dans Protegus 2.

3.4 Centrale incendie NSC Solution

Raccordez la centrale incendie NSC Solution au G17F par le bus RS485, selon le schéma ci-dessous.

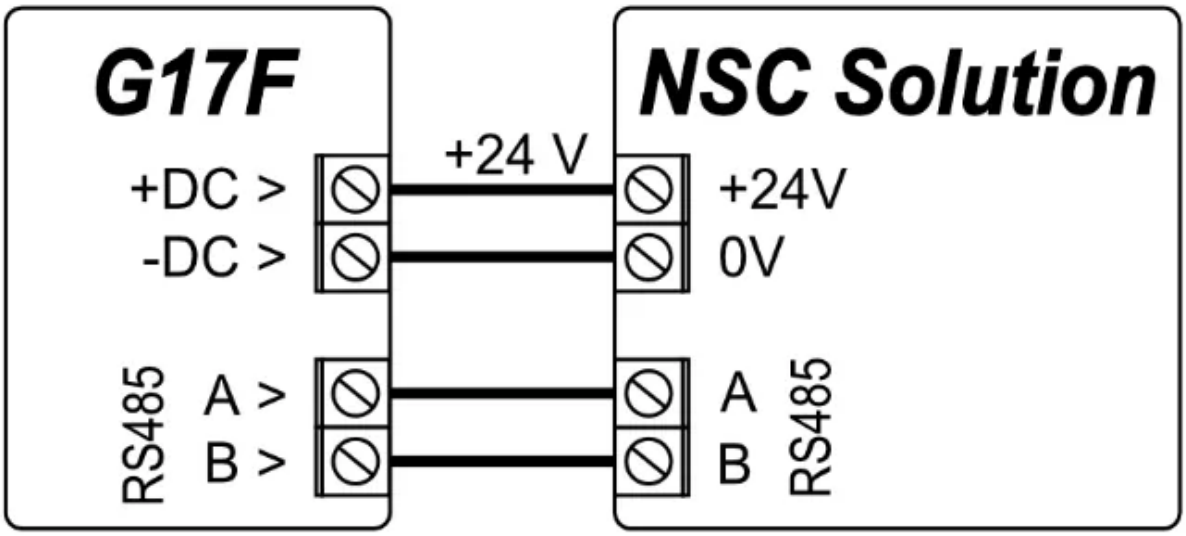


Figure 13. Liaison entre le G17F et la centrale incendie NSC Solution. Inscriptions du schéma : alimentation – la borne **+DC** du G17F va sur la borne **+24V** (+24 V) de la centrale, la borne **−DC** sur la borne **0V** ; RS485 – **A** sur **A**, **B** sur **B**.

Configuration du G17F dans TrikdisConfig lorsqu'il est raccordé à une centrale incendie NSC Solution :

1. Sur la page **Modules**, choisissez le module **NSC Solution**.
2. L'adresse **NSC slave address** (adresse esclave du communicateur) ne doit pas être identique à l'adresse des modules raccordés à la centrale incendie.

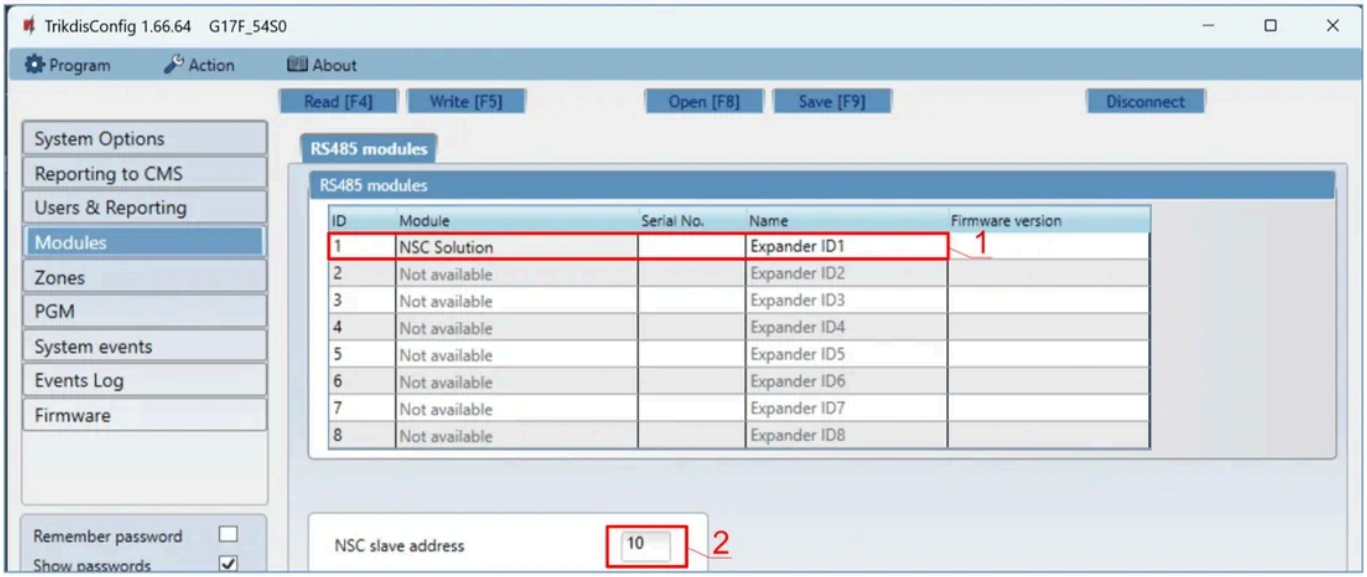


Figure 14. TrikdisConfig – **Modules** : le module RS485 n° 1 est **NSC Solution** (nom **Expander ID1**).

- 1 sélection de **NSC Solution**
- 2 **NSC slave address** – 10 sur l'image

3. Sur la page **Users & Reporting**, saisissez les numéros de téléphone des utilisateurs qui reçoivent des messages du G17F (point 5.4).
4. Les utilisateurs reçoivent un SMS et un appel pour les événements cochés (page **Users & Reporting**, onglet **SMS for Panel events**). Dans la colonne **CID**, vous pouvez ajouter d'autres codes d'événement Contact ID ; pour les nouveaux codes, vous devez aussi saisir le texte du SMS. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**).

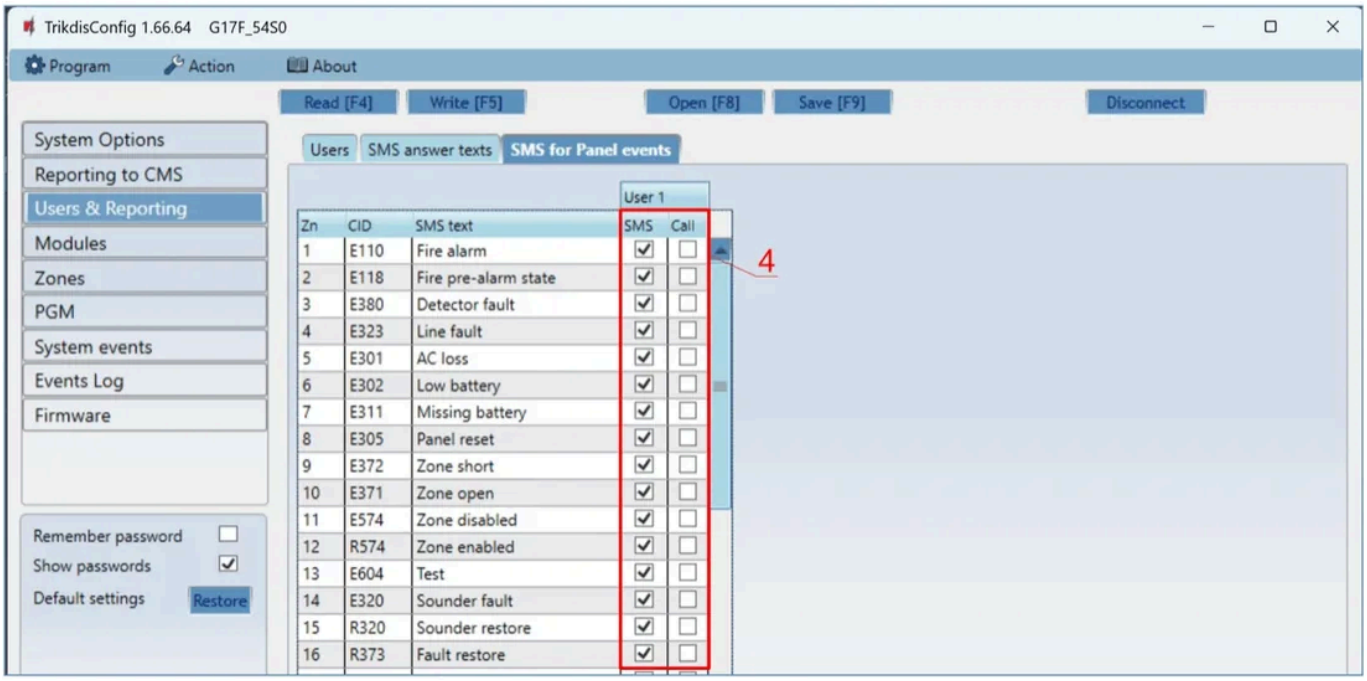


Figure 15. TrikdisConfig – **Users & Reporting**, onglet **SMS for Panel events** : pour l'utilisateur 1, la case **SMS** est cochée pour les 16 événements visibles (de l'alarme incendie **E110 Fire alarm** au rétablissement de défaut **R373 Fault restore**), la case **Call** est vide.

- 4 les colonnes **SMS** et **Call** de l'utilisateur 1

5. Si les messages doivent aussi parvenir au récepteur du centre de télésurveillance, configurez le canal de communication sur la page **Reporting to CMS** (points 2.2 et 5.3).

Après avoir configuré le G17F, mettez la centrale incendie sous tension et attendez que son logiciel soit chargé. Ensuite, il faut rechercher (scanner) sur la centrale les modules raccordés au bus RS485. Sur la centrale, appuyez sur : **PROG.** > **INSTALLER** > (saisissez le code installateur) **00000 OK** > (choisissez) **SETTINGS** > **ENTER** > (choisissez) **SCAN RS485** > **ENTER**. Attendez la fin de la recherche, puis revenez à l'écran principal en appuyant deux fois sur le bouton **CANCEL**.

Testez le système : déclenchez une alarme incendie et vérifiez que les messages du G17F arrivent au centre de télésurveillance et dans Protegus 2.

3.5 Centrale incendie INIM Smartline

Raccordez la centrale incendie INIM Smartline au G17F par le bus RS485, selon le schéma ci-dessous.

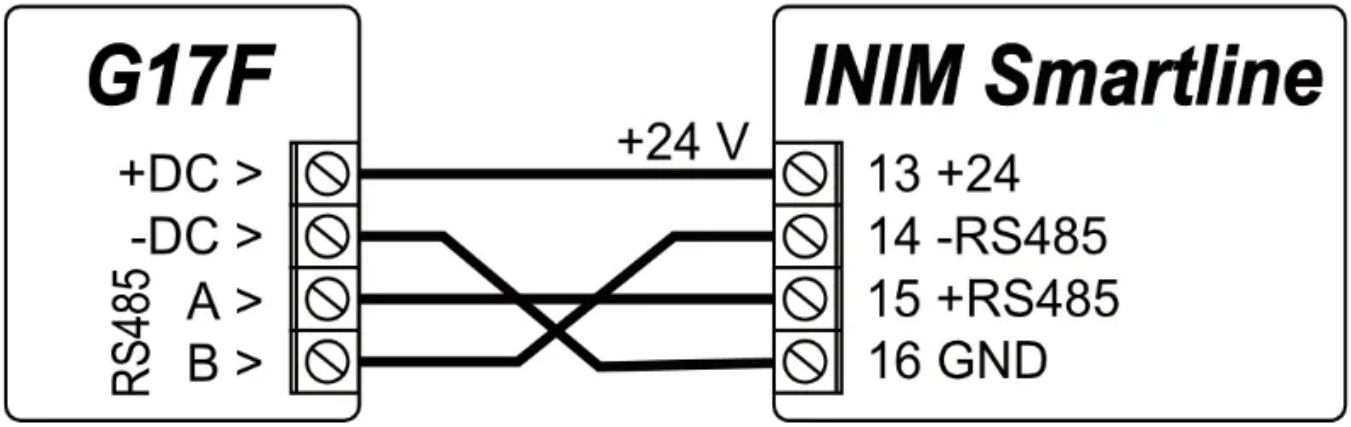


Figure 16. Liaison entre le G17F et la centrale incendie INIM Smartline. Inscriptions du schéma : alimentation – la borne **+DC** du G17F va sur la borne **13 +24** (+24 V) de la centrale, la borne **–DC** sur la borne **16 GND** ; RS485 – la borne **A** va sur la borne **15 +RS485**, la borne **B** sur la borne **14 –RS485**. Les fils qui se croisent ne sont pas en contact.

Si vous raccordez la centrale INIM Smartline au G17F par le bus RS485, la centrale doit être mise en mode **slave** (esclave) – vous pouvez le faire dans le logiciel SmartLeague de la centrale.

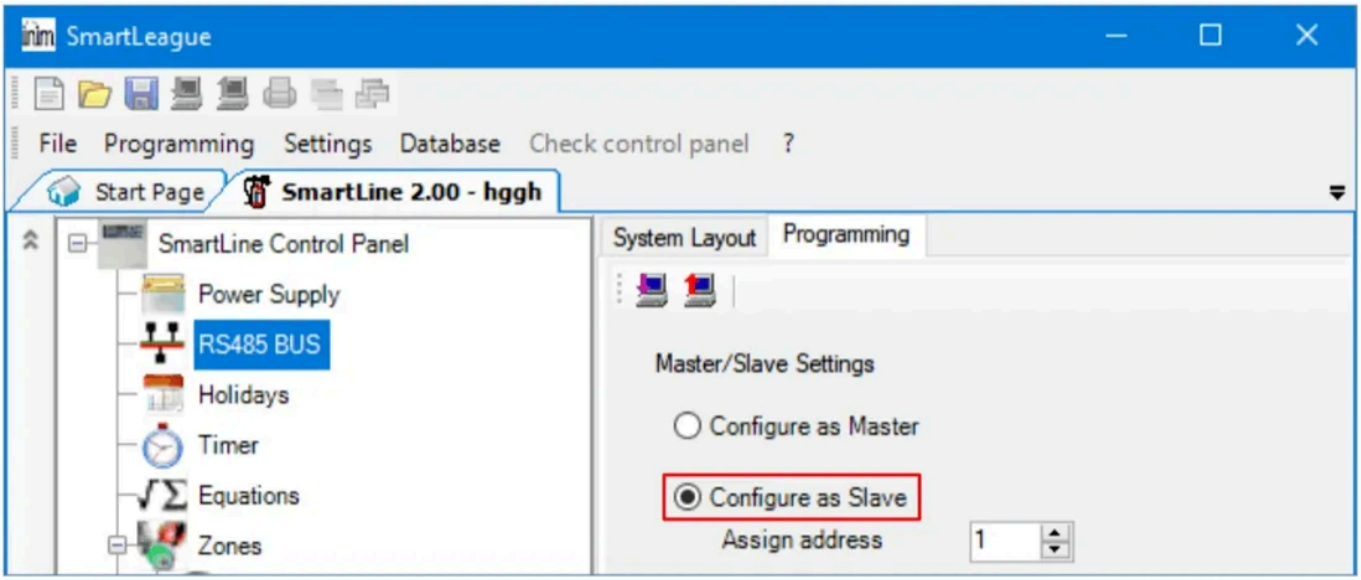


Figure 17. SmartLeague – fenêtre **RS485 Bus Programming** : dans le groupe **Master/Slave Settings**, **Configure as Slave** est sélectionné, **Assign address** : 1.

- Si des répéteurs sont raccordés à la centrale INIM Smartline, le G17F ne peut pas être raccordé par le bus RS485.
- Si le G17F est raccordé au bus RS485 de la centrale INIM Smartline, les modules d'extension iO du communicateur ne sont pas pris en charge.

Configuration du G17F dans TrikdisConfig lorsqu'il est raccordé à une centrale incendie INIM Smartline :

1. Sur la page **Modules**, choisissez le module **Inim Smartline**.

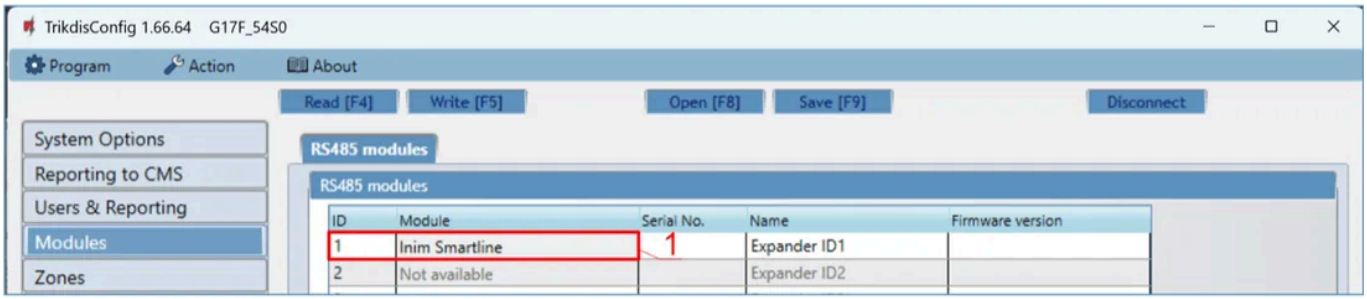


Figure 18. TrikdisConfig – **Modules** : le module RS485 n° 1 est **Inim Smartline** (nom **Expander ID1**).

- 1 sélection de **Inim Smartline**

2. Sur la page **Users & Reporting**, saisissez les numéros de téléphone des utilisateurs qui reçoivent des messages du G17F (point 5.4).
3. Les utilisateurs reçoivent un SMS et un appel pour les événements cochés (page **Users & Reporting**, onglet **SMS for Panel events** – l'image de l'onglet se trouve aux points 3.4 et 5.4). Dans la colonne **CID**, vous pouvez ajouter d'autres codes d'événement Contact ID ; pour les nouveaux codes, vous devez aussi saisir le texte du SMS. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**).
4. Si les messages doivent aussi parvenir au récepteur du centre de télésurveillance, configurez le canal de communication sur la page **Reporting to CMS** (points 2.2 et 5.3).

Testez le système : déclenchez une alarme incendie et vérifiez que les messages du G17F arrivent au centre de télésurveillance et dans Protegus 2.

3.6 Centrale incendie C-TEC Cast ZFP

Raccordez la centrale incendie C-TEC Cast ZFP au G17F par le bus ABUS RS485, selon le schéma ci-dessous.

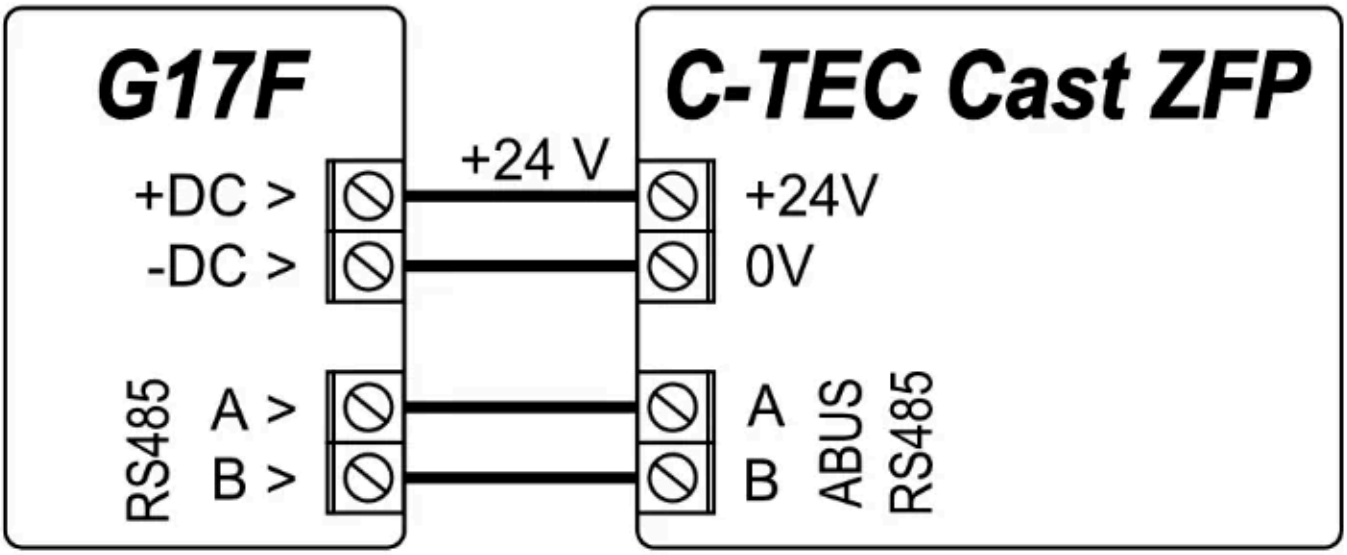


Figure 19. Liaison entre le G17F et la centrale incendie C-TEC Cast ZFP. Inscriptions du schéma : alimentation – la borne **+DC** du G17F va sur la borne **+24V** (+24 V) de la centrale, la borne **–DC** sur la borne **0V** ; **ABUS RS485** – **A** sur **A**, **B** sur **B**.

Configuration du G17F dans TrikdisConfig lorsqu'il est raccordé à une centrale incendie C-TEC Cast ZFP :

1. Sur la page **Modules**, choisissez la centrale incendie **C-TEC Cast ZFP**.

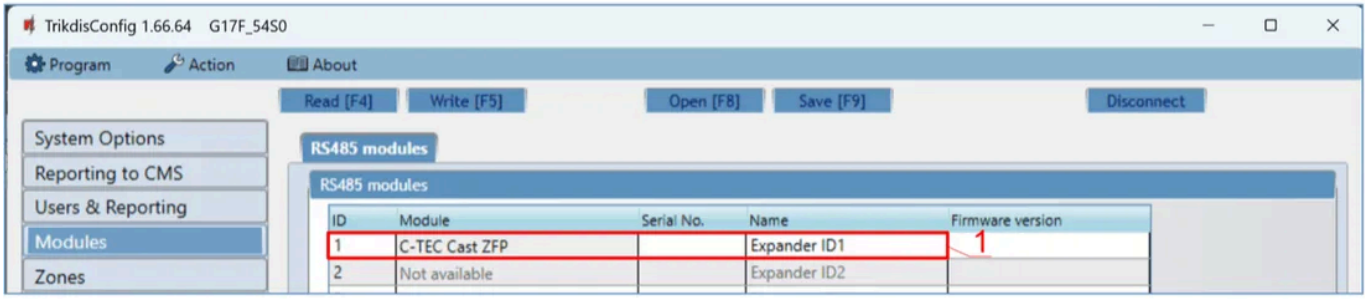


Figure 20. TrikdisConfig – **Modules** : le module RS485 n° 1 est **C-TEC Cast ZFP** (nom **Expander ID1**).

- 1 sélection de **C-TEC Cast ZFP**

2. Sur la page **Users & Reporting**, saisissez les numéros de téléphone des utilisateurs qui reçoivent des messages du G17F (point 5.4).
3. Les utilisateurs reçoivent un SMS et un appel pour les événements cochés (page **Users & Reporting**, onglet **SMS for Panel events** – l'image de l'onglet se trouve aux points 3.4 et 5.4). Dans la colonne **CID**, vous pouvez ajouter d'autres codes d'événement Contact ID ; pour les nouveaux codes, vous devez aussi saisir le texte du SMS. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**).
4. Si les messages doivent aussi parvenir au récepteur du centre de télésurveillance, configurez le canal de communication sur la page **Reporting to CMS** (points 2.2 et 5.3).

3.6.1 Configuration de la centrale C-TEC (ZFPtools)

Installez le logiciel **ZFPtools** sur l'ordinateur et lancez-le. Mettez la centrale incendie sous tension et attendez que son logiciel soit chargé. Reliez la centrale à l'ordinateur avec un câble **USB 2.0 A-B**.

1. Ouvrez l'onglet **Node View**.

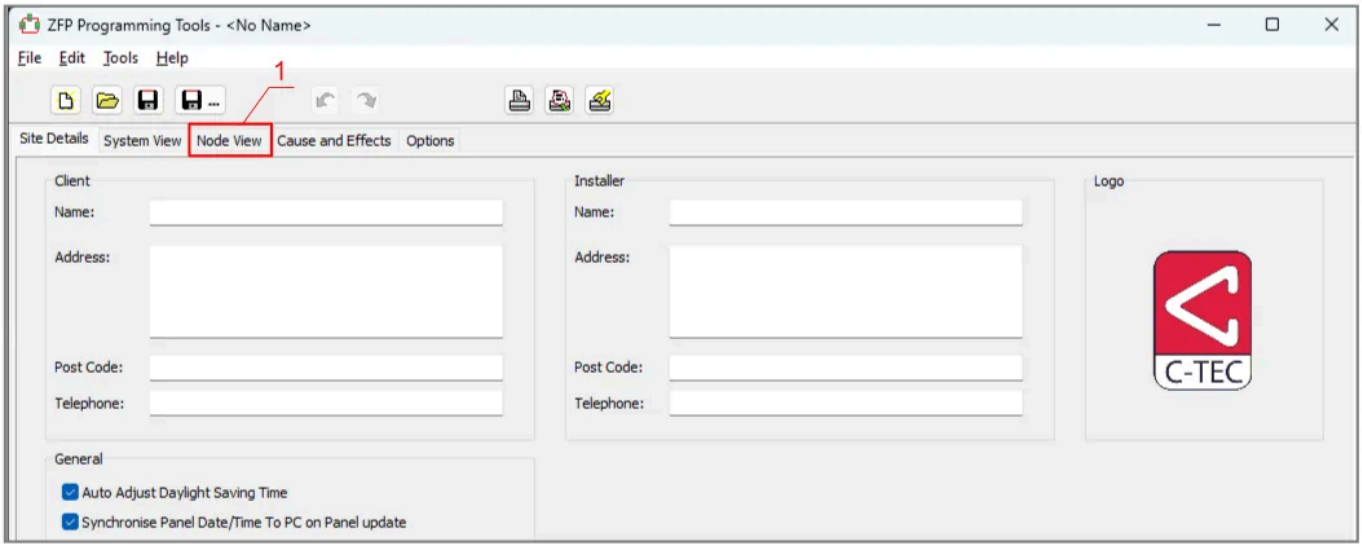


Figure 21. ZFP Programming Tools – fenêtre **Site Details**.

- 1 l'onglet **Node View**

2. Téléchargez les réglages de la centrale incendie sur l'ordinateur (**Retrieve All Data**).

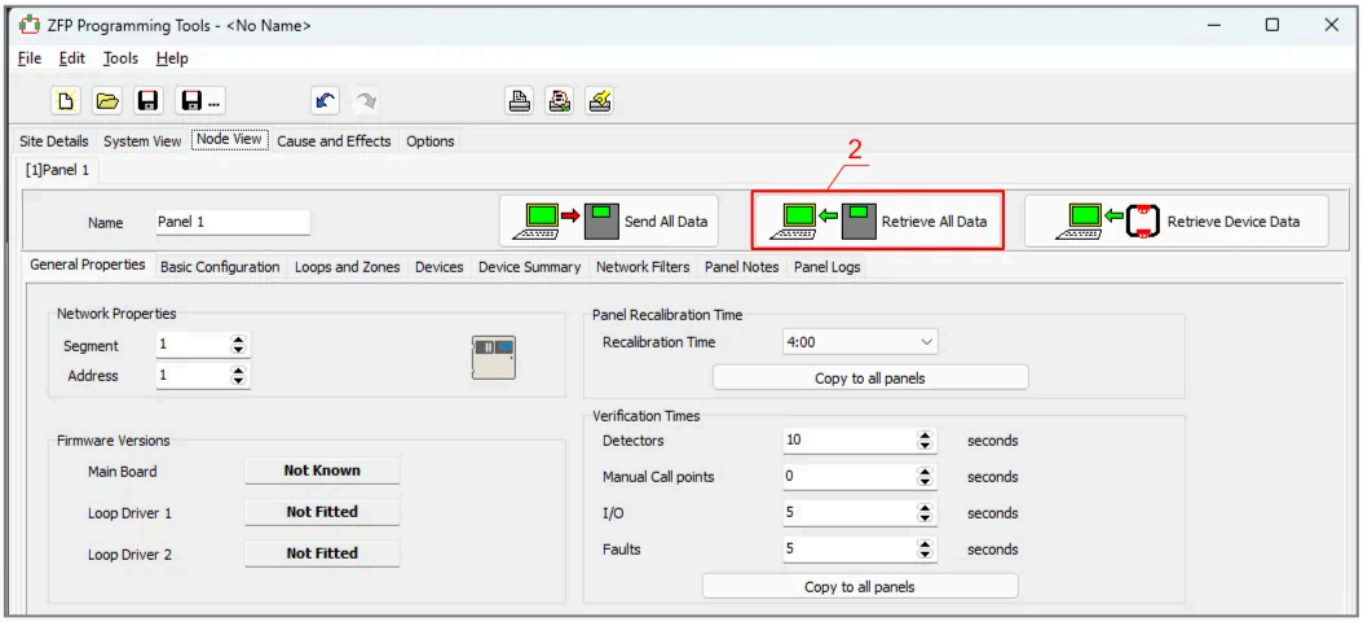


Figure 22. ZFP Programming Tools – **Node View**, **Panel 1** : le bouton **Retrieve All Data**.

- 2 **Retrieve All Data** – téléchargement des réglages de la centrale

3. Saisissez le code (par défaut `4444`).
4. Cliquez sur le bouton **OK** (la coche verte).

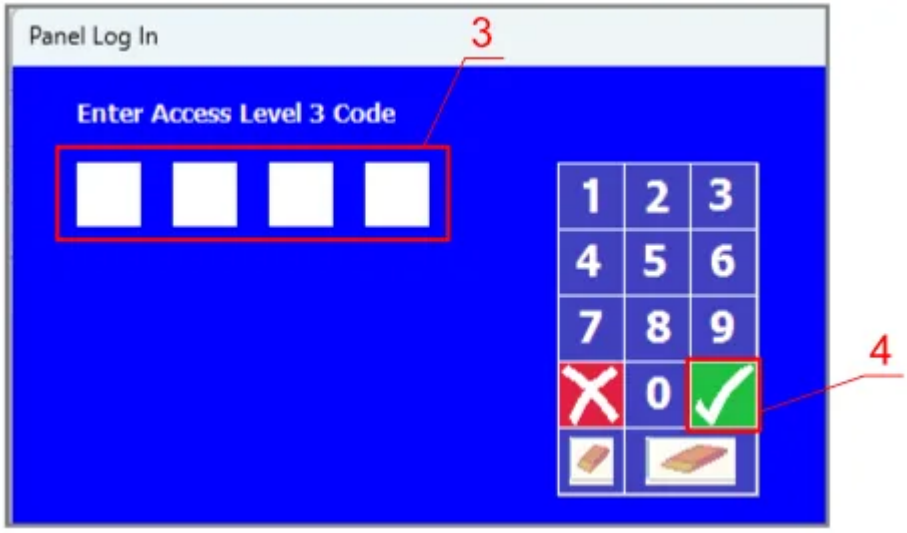


Figure 23. ZFP Programming Tools – fenêtre **Panel Log In** : **Enter Access Level 3 Code** – le code du niveau d'accès 3.

- 3 les quatre champs du code
- 4 le bouton **OK** (coche verte)

5. Choisissez l'équipement **BMS Interface** (**Device Palette**).
6. Cliquez sur un emplacement d'icône libre.

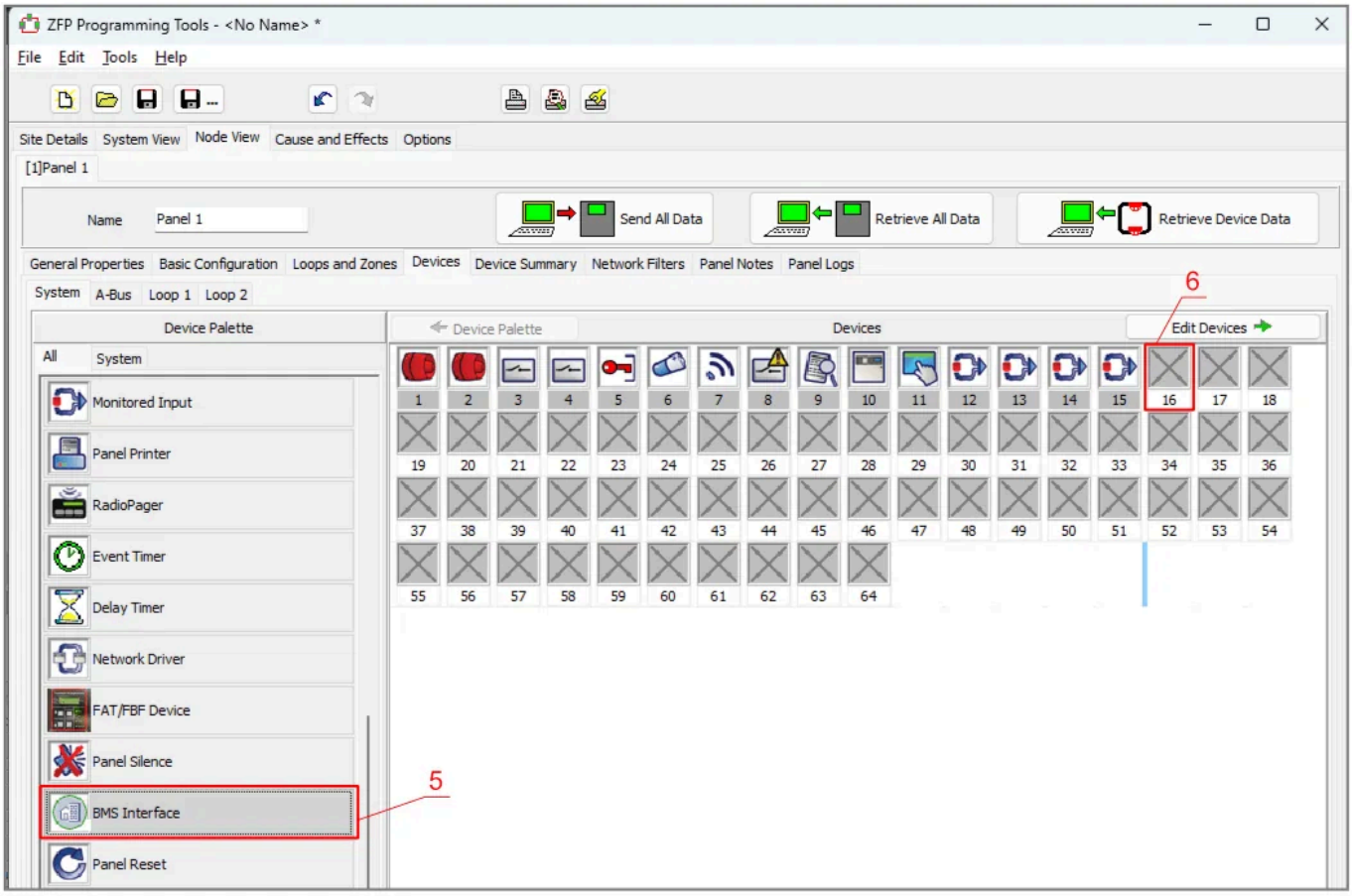


Figure 24. ZFP Programming Tools – **Node View**, **Devices** : dans la liste **Device Palette**, **BMS Interface** est sélectionné.

- 5 **BMS Interface** dans la liste **Device Palette**
- 6 emplacement d'icône libre (le 16e sur l'image)

7. Cliquez sur le bouton **Edit Devices**.

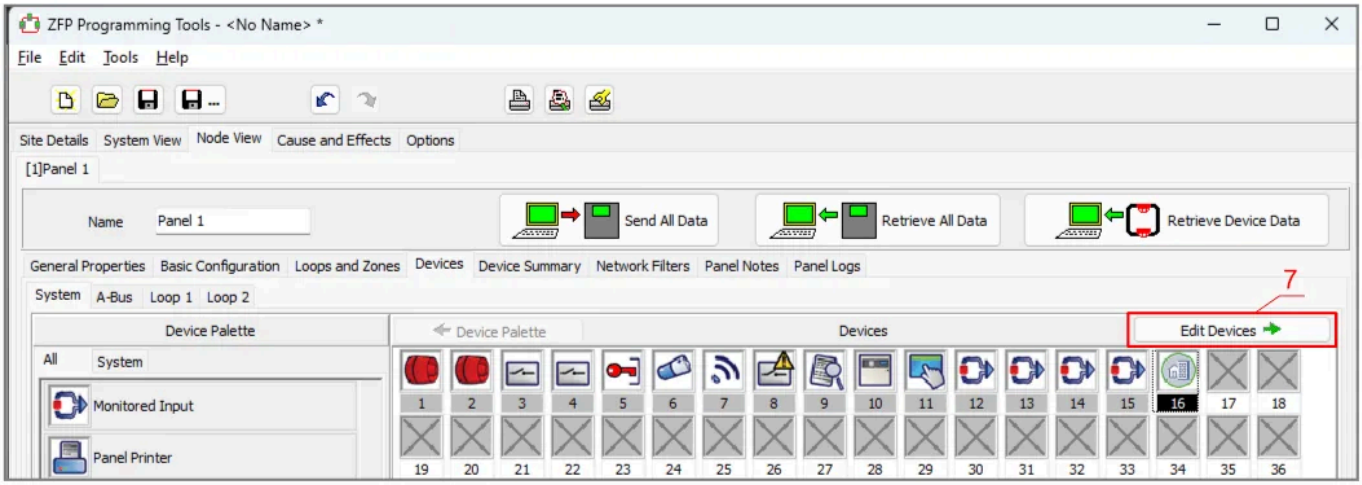


Figure 25. ZFP Programming Tools – **Node View**, **Devices** : **BMS Interface** à l'emplacement 16 ; le bouton **Edit Devices**.

- 7 **Edit Devices**

8. Dans l'onglet **Device**, saisissez le nom du système.

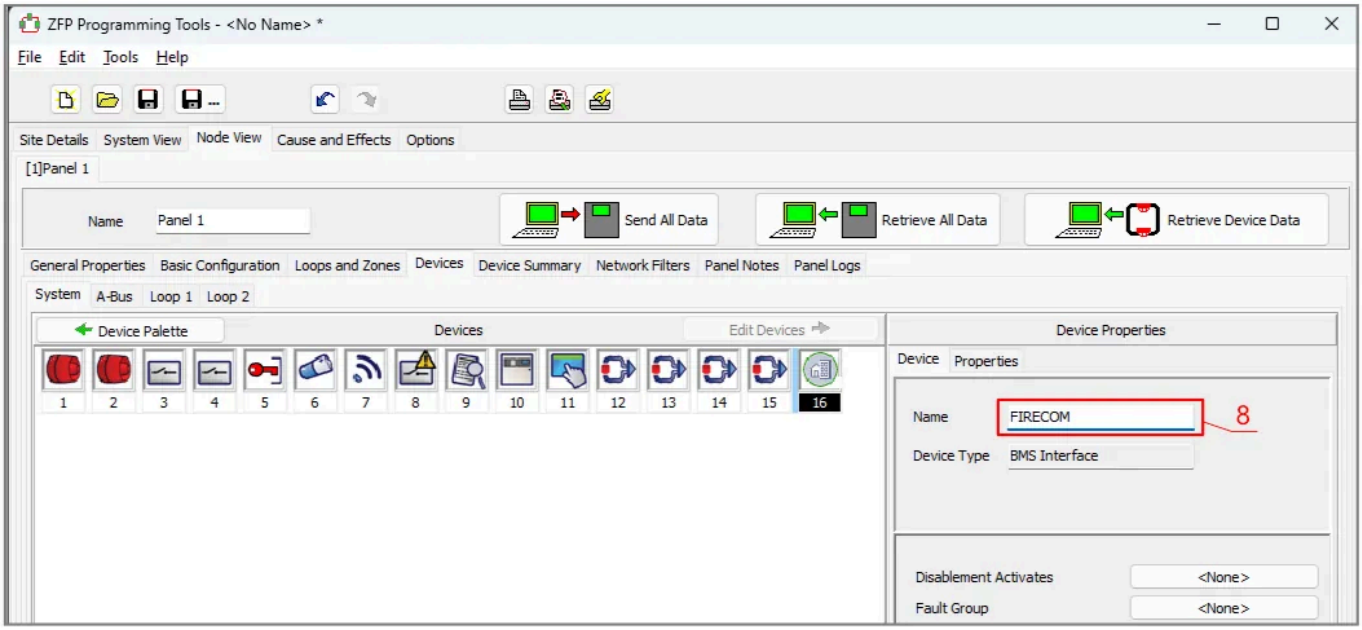


Figure 26. ZFP Programming Tools – **Device Properties**, onglet **Device** : **Name** : FIRECOM, **Device Type** : BMS Interface.

- 8 **Name** – le nom du système

9. Dans l'onglet **Properties**, saisissez le nom du système.
10. Indiquez le bus **ABUS RS485** auquel le G17F est raccordé.
11. Configurez les messages.
12. Écrivez les réglages dans la centrale incendie (**Send All Data**).

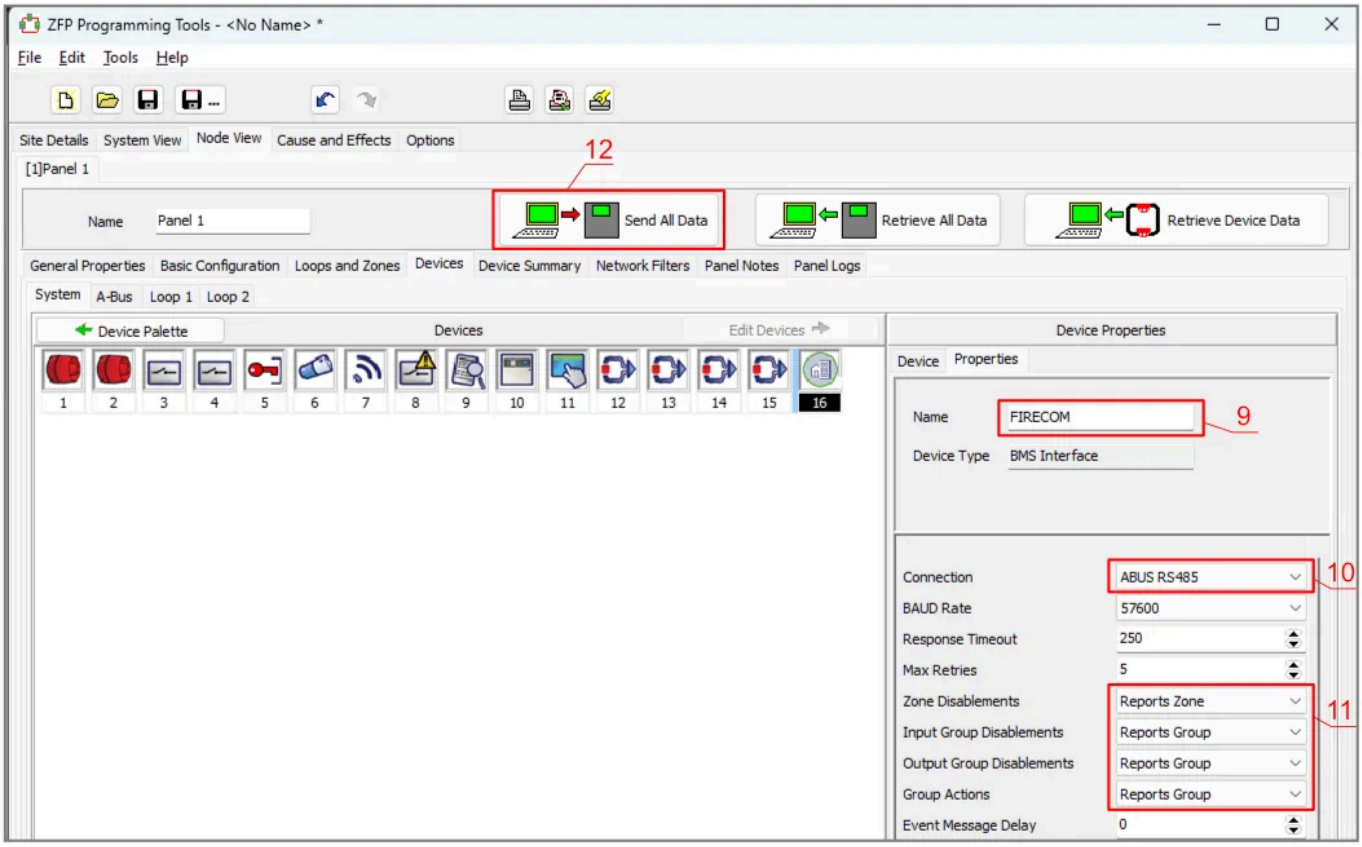


Figure 27. ZFP Programming Tools – **Device Properties**, onglet **Properties**. Sur l'image : **BAUD Rate** 57600, **Response Timeout** 250, **Max Retries** 5.

- 9 **Name** – le nom du système (FIRECOM)
- 10 **Connection** – **ABUS RS485**
- 11 les messages : **Zone Disablements** – **Reports Zone** ; **Input Group Disablements**, **Output Group Disablements** et **Group Actions** – **Reports Group**
- 12 **Send All Data** – écriture des réglages dans la centrale

13. Saisissez le code (par défaut `4444`) – dans la même fenêtre **Panel Log In** qu'à l'étape 3.
14. Cliquez sur le bouton **OK**.

La centrale incendie est programmée. Débranchez le câble USB 2.0 A-B de la centrale.

Testez le système : déclenchez une alarme incendie et vérifiez que les messages du G17F arrivent au centre de télésurveillance et dans Protegus 2.

3.7 Raccordement des entrées

Le communicateur dispose de six bornes d'entrée (**1 IN** – **6 IN** ; dont trois à double usage, IN/OUT), auxquelles vous pouvez raccorder des circuits de type NO, NC et EOL (4,7 kΩ, 10 kΩ). Par défaut, les entrées surveillent un circuit de type EOL ; vous pouvez choisir un autre type sur la page **Zones** de TrikdisConfig (point 5.6).

Raccordement	Repos (rétablissement)	Alarme
NO – contact normalement ouvert	ouvert	court-circuit
NC – contact normalement fermé	court-circuit	ouvert

Raccordement	Repos (rétablissement)	Alarme
NO + EOL – contact ouvert, avec une résistance de 10 kΩ en parallèle	10 kΩ	court-circuit ou ouvert
NC + EOL – contact fermé, avec une résistance de 10 kΩ en série	10 kΩ	court-circuit ou ouvert

Schémas des quatre modes de raccordement ; le contact est placé entre la borne **COM** et la borne **INx**, **10k** est la résistance de fin de ligne de 10 kΩ.

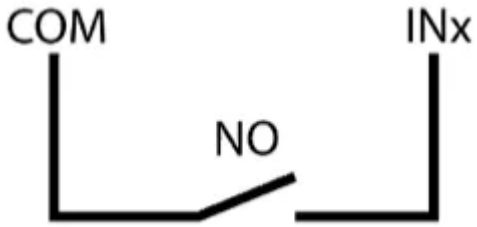


Figure 28. NO – contact normalement ouvert.

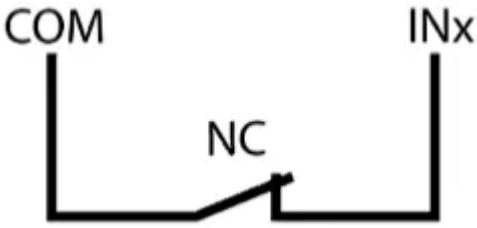


Figure 29. NC – contact normalement fermé.

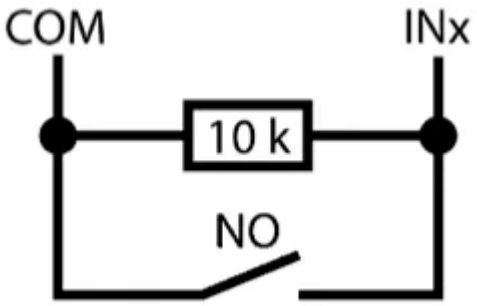


Figure 30. NO + EOL (EOL10k) – contact normalement ouvert avec une résistance de 10 kΩ en parallèle.

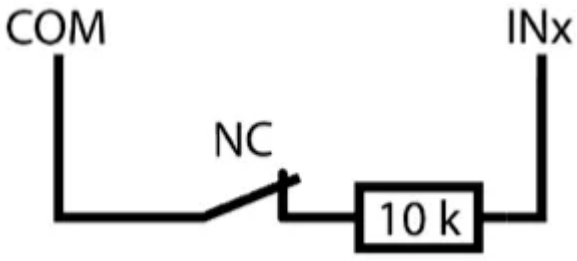


Figure 31. NC + EOL (EOL10k) – contact normalement fermé avec une résistance de 10 kΩ en série.

3.8 Modules d'extension de la série iO

Si le communicateur a besoin de plus d'entrées (IN) ou de sorties (OUT), raccordez-lui un module d'extension d'entrées et de sorties filaire ou sans fil de la série iO de Trikdis.

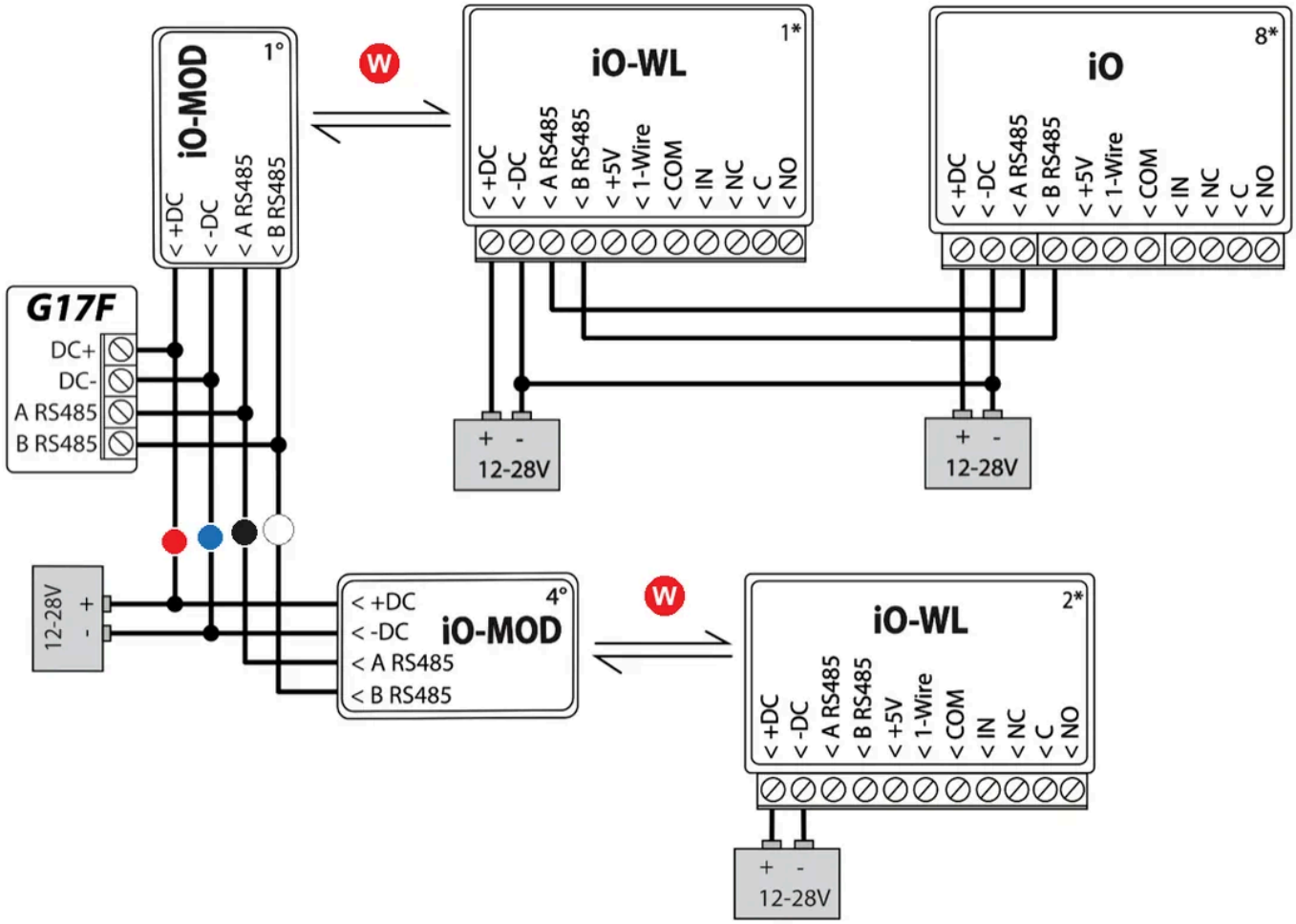


Figure 32. Modules iO-MOD, iO-WL et iO sur le G17F : la borne **DC+** du G17F va sur la borne **+DC** de l'iO-MOD (fil rouge), **DC–** sur **–DC** (bleu), **A RS485** sur **A RS485** (noir), **B RS485** sur **B RS485** (blanc) ; alimentation commune 12–28 V ; 4 modules iO-MOD au maximum (« up to 4 iO-MOD modules », repérés par ° sur le schéma) ; chaque iO-MOD est relié par radio à un iO-WL, jusqu'à 300 m ; l'iO-WL est raccordé au module iO par le bus RS485 (A–A, B–B) (« RS485 connection »), jusqu'à 300 m (« up to 300 m ») ; 8 modules d'extension système au maximum (« up to 8 system expansion modules », repérés par * sur le schéma) ; le pôle négatif de l'alimentation 12–28 V de l'iO-WL et du module iO est commun, l'autre iO-WL reçoit sa propre alimentation 12–28 V.

- fil rouge (« Red wire »)
- fil bleu (« Blue wire »)
- fil noir (« Black wire »)
- fil blanc (« White wire »)
- W liaison sans fil (« Wireless connection »), jusqu'à 300 m (« up to 300 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.

3.9 Module d'extension iO-8

Si le communicateur a besoin de plus d'entrées (IN) ou de sorties (OUT), raccordez-lui un module d'extension filaire **iO-8**. Description détaillée du module d'extension : Extension d'entrées et de sorties iO8 – manuel d'installation.

Module Trikdis IO8 Wired Expander

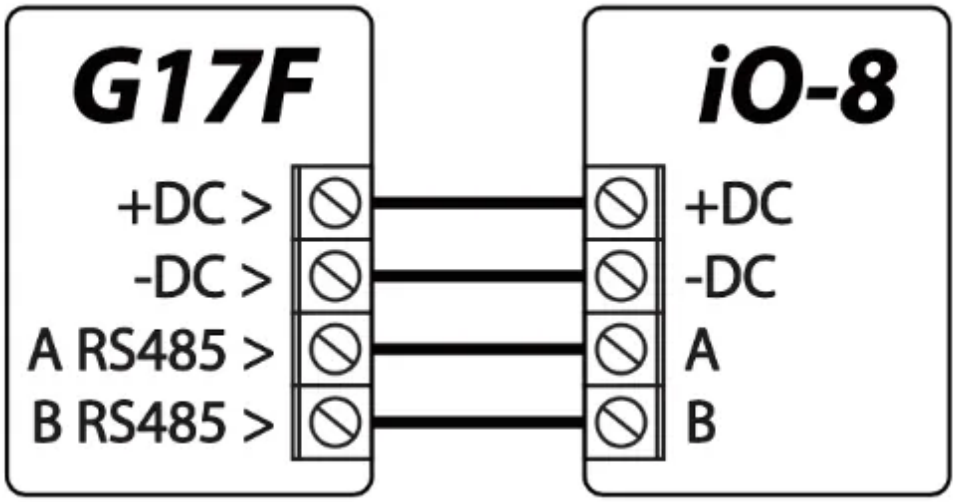


Figure 33. Raccordement du module d'extension iO-8 : la borne **+DC** du G17F va sur la borne **+DC** de l'iO-8, **–DC** sur **–DC**, **A RS485** sur **A**, **B RS485** sur **B**.

3.10 Modules d'extension de la série LORA

Les modules LORA sont reliés au G17F par radio : l'émetteur-récepteur **RF-LORA** est placé sur le bus RS485 et maintient la liaison, jusqu'à 5000 m, avec les modules d'extension **iO-LORA**, **iO8-LORA** et **REL-LORA** et avec le bouton panique **PB-LORA**. Vous ajoutez les modules sur la page **Modules** de TrikdisConfig (point 5.5).

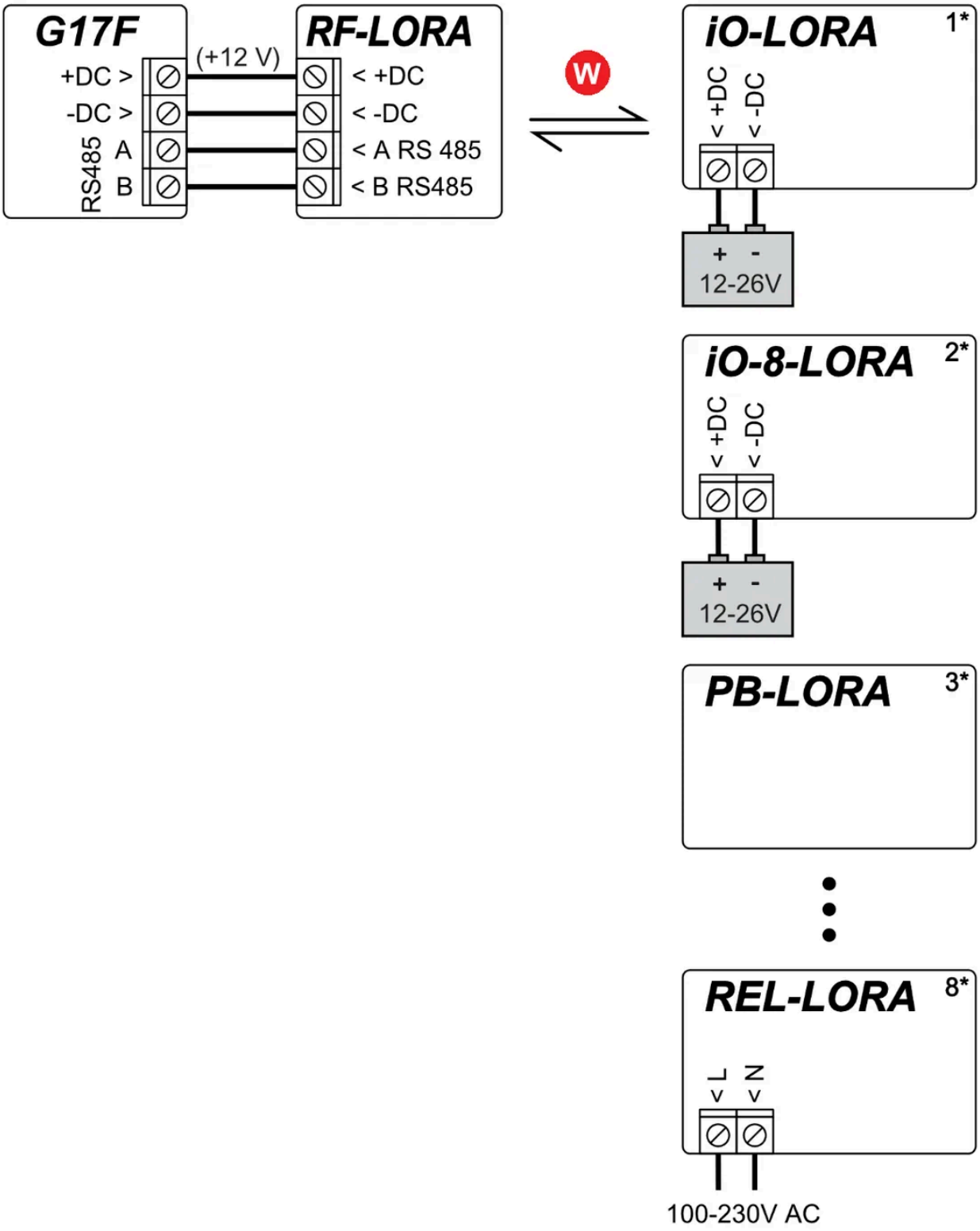


Figure 34. Raccordement des modules LORA : la borne **+DC** du G17F va sur la borne **+DC** (+12 V) du RF-LORA, la borne **–DC** sur la borne **–DC** ; RS485 – la borne **A** du G17F va sur la borne **A RS 485** du RF-LORA, la borne **B** sur la borne **B RS485** ; liaison radio jusqu'à 5000 m avec les modules **iO-LORA**, **iO8-LORA**, **PB-LORA** … **REL-LORA** (repères 1, *2*, 3* … 8* dans le coin des modules) ; l'iO-LORA et l'iO8-LORA reçoivent leur propre alimentation 12–26 V (**+DC**, **–DC**), le REL-LORA une alimentation secteur 100–230 V AC (**L**, **N**).

- W liaison sans fil (« Wireless connection »), jusqu'à 5000 m (« up to 5000 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.

Module d'expanneur sans fil Trikdis RF-Lora | **Module d'expanneur sans fil Trikdis Io-Lora**

Module d'expanneur sans fil Trikdis Io8-Lora | **Bouton de panique sans fil Trikdis PB-Lora**

3.11 Module WiFi W485

Le module **W485** envoie les messages du G17F par WiFi, via le routeur Internet, au centre de télésurveillance et à l'application Protegus 2. Tant que la liaison WiFi existe, le G17F envoie les messages d'événement par le W485 ; si la liaison WiFi est interrompue, il les envoie par le réseau mobile (GPRS), et lorsque la liaison WiFi est rétablie, il revient au W485. Cette fonction est disponible à partir du firmware **1.08** du G17F. **Avec le W485, le G17F peut aussi être utilisé sans carte SIM.** Configuration du W485 pour le G17F : point 5.5.

Module WiFi Trikdis W485 (RS485)

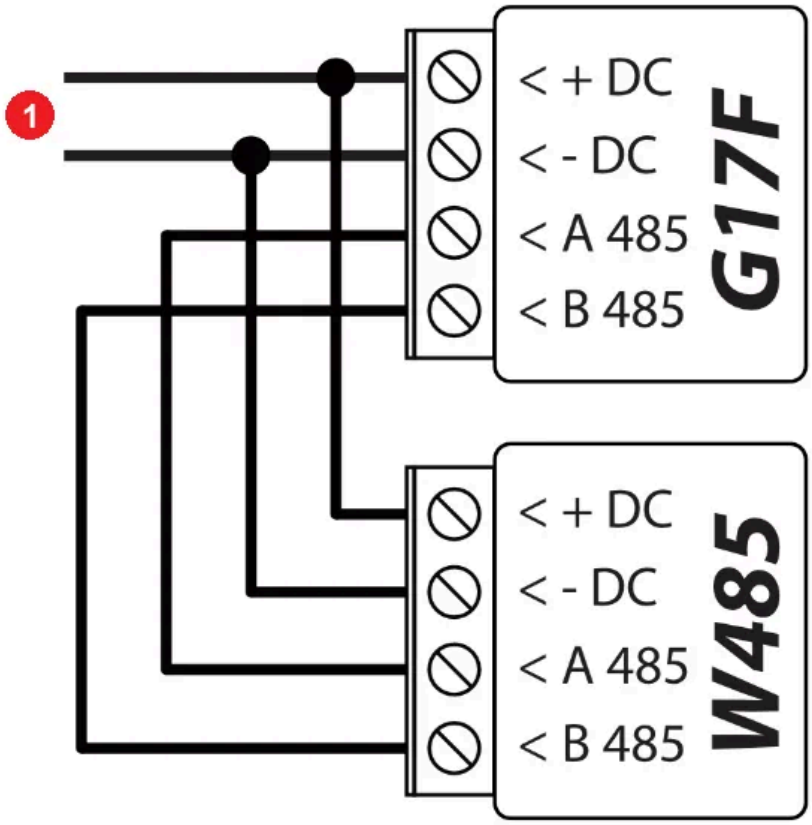


Figure 35. Raccordement du module W485 : le pôle positif de l'alimentation va sur la borne **+DC** du G17F et du W485, le pôle négatif sur la borne **–DC** ; liaison RS485 (« RS485 connection »), jusqu'à 100 m (« up to 100 m ») : la borne **A 485** du G17F va sur la borne **A 485** du W485, la borne **B 485** sur la borne **B 485**.

- 1 alimentation (« Power supply »), 12 V DC, 0,5 A

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.

3.12 Module Ethernet E485

Le module **E485** envoie les messages du G17F par une connexion Internet filaire au centre de télésurveillance et à l'application Protegus 2. Avec l'E485, les messages passent par l'Internet filaire, le G17F n'utilise pas l'Internet mobile. Si la connexion Internet filaire est interrompue, le G17F envoie les messages par l'Internet mobile, puis de nouveau par l'E485 lorsque la connexion filaire est rétablie. Cette fonction est disponible à partir du firmware **1.08** du G17F. **Avec l'E485, le G17F peut aussi être utilisé sans carte SIM.** Configuration de l'E485 pour le G17F : point 5.5.

Module Ethernet Trikdis E485 (RS485)

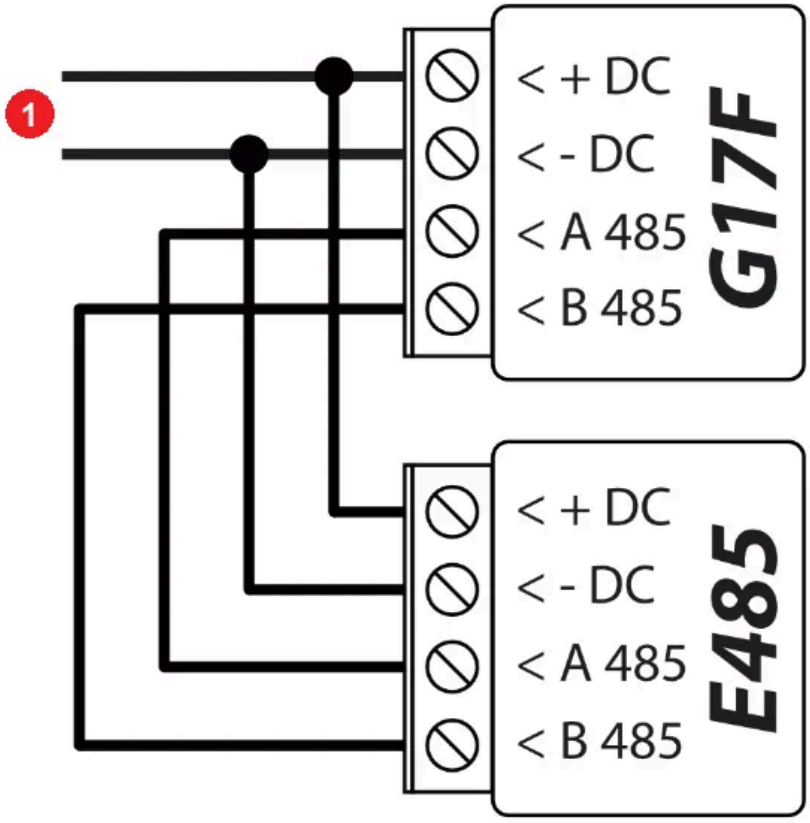


Figure 36. Raccordement du module E485 : le pôle positif de l'alimentation va sur la borne **+DC** du G17F et de l'E485, le pôle négatif sur la borne **–DC** ; liaison RS485 (« RS485 connection »), jusqu'à 100 m (« up to 100 m ») : la borne **A 485** du G17F va sur la borne **A 485** de l'E485, la borne **B 485** sur la borne **B 485**.

- 1 alimentation (« Power supply »), 12 V DC, 0,5 A

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.

3.13 Mise sous tension du communicateur

Pour mettre le communicateur sous tension, vous devez d'abord assurer l'alimentation de la centrale incendie (sur les schémas, le G17F est alimenté par la sortie 24 V de la centrale). Si le communicateur fonctionne correctement, les voyants suivants s'allument :

- la LED **POWER** clignote en vert (la tension d'alimentation est correcte) ;

- la LED **NETWORK** est allumée en vert et clignote en jaune lorsque le communicateur s'est connecté au réseau.

- Niveau de signal du réseau mobile suffisant : 5 sur un réseau 2G (cinq clignotements jaunes de la LED **NETWORK**), 3 sur un réseau 4G (trois clignotements jaunes).
- Si vous comptez moins de 3 clignotements jaunes sur la LED **NETWORK**, le niveau du signal est insuffisant : choisissez un autre emplacement d'installation ou utilisez une antenne plus sensible (point 1.7).
- Si la signalisation est différente, vous trouverez l'explication au point 1.6.
- Si aucun voyant du G17F ne s'allume, vérifiez l'alimentation et le raccordement.

4. Commande à distance

Le G17F se commande depuis l'application **Protegus 2**, par **commande SMS** et par **appel téléphonique** (pendant l'appel, avec le clavier du téléphone). Dans l'application, les utilisateurs voient aussi l'état du système et reçoivent des notifications sur les événements du système ; par SMS, l'administrateur peut également modifier une partie des réglages.

4.1 Ajout du G17F à Protegus 2

Dans Protegus 2, les utilisateurs voient l'état du système et reçoivent des notifications sur les événements du système. L'application est disponible sur téléphone et dans le navigateur (les liens de téléchargement figurent ci-dessous, à la création du système).

Avant d'ajouter le système

Vous pouvez ajouter le G17F à Protegus 2 si :

1. une carte SIM activée y est insérée et que vous avez saisi ou désactivé le code PIN ;
2. le service Protegus est activé (**Users & Reporting** → **Enable cloud service**, point 5.4 ; par SMS : `CONNECT 123456 PROTEGUS=ON`, point 4.2) ;
3. il est sous tension (la LED **POWER** clignote en vert) ;
4. il est connecté au réseau (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

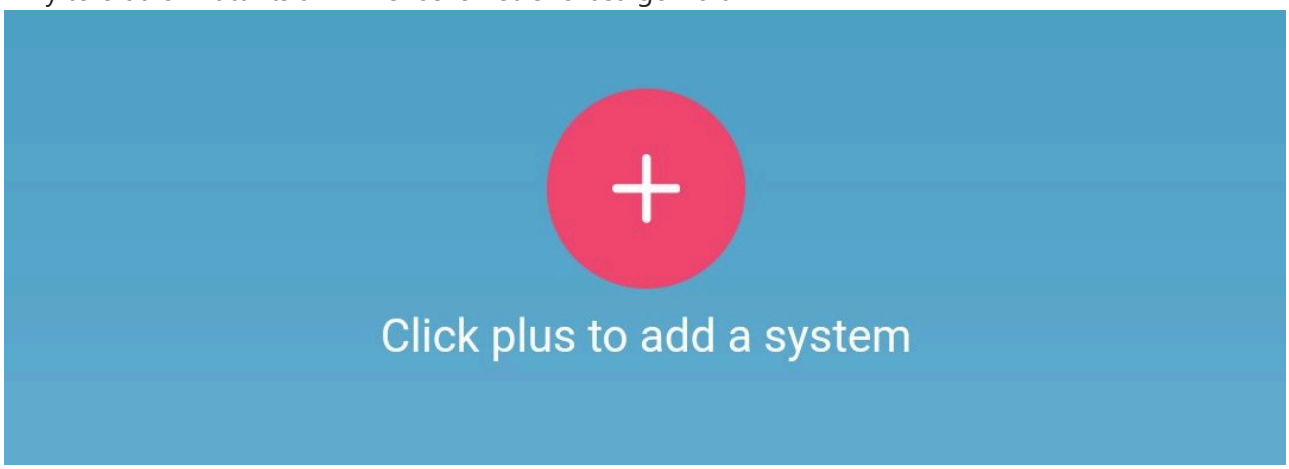
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

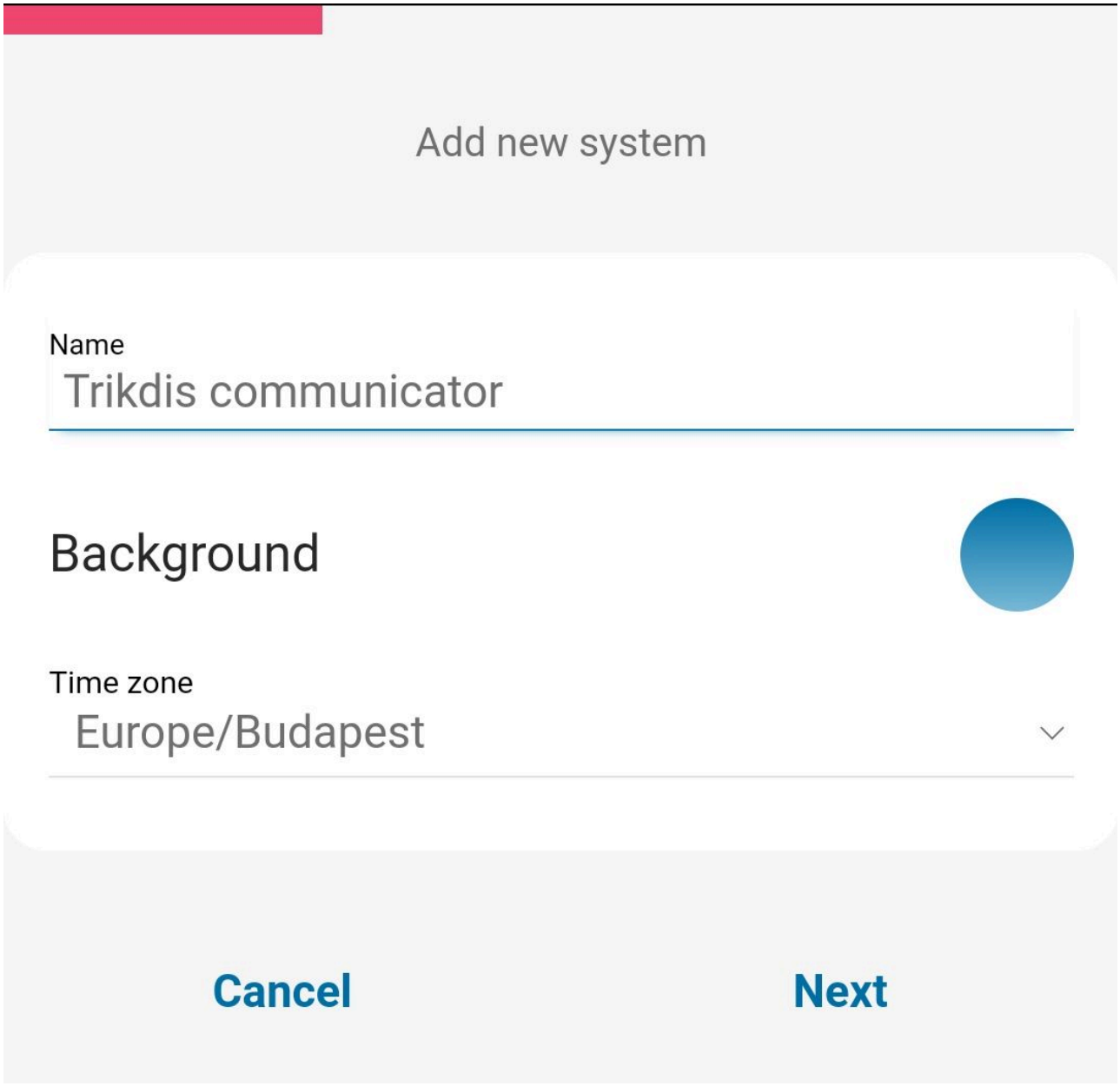
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



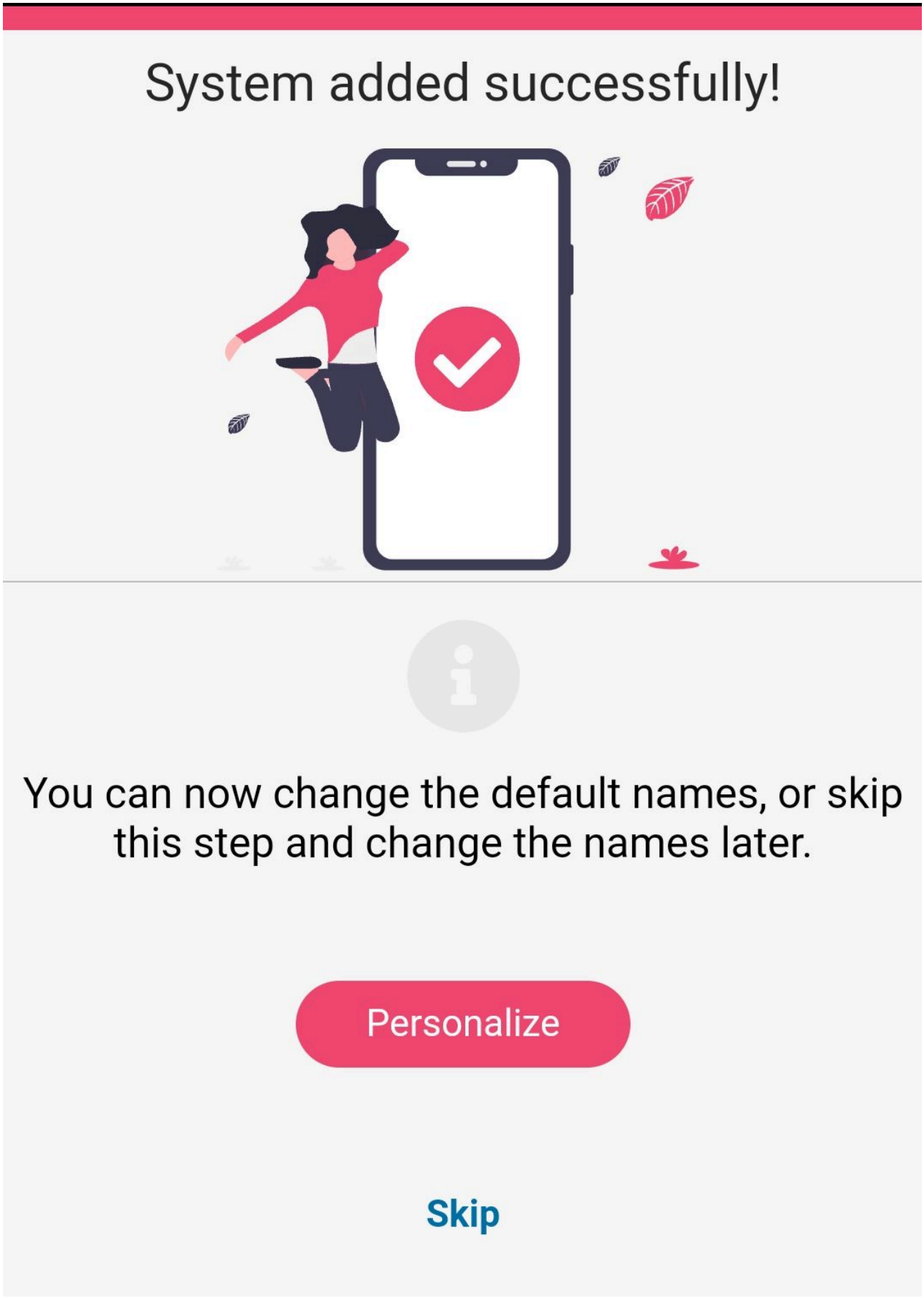
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



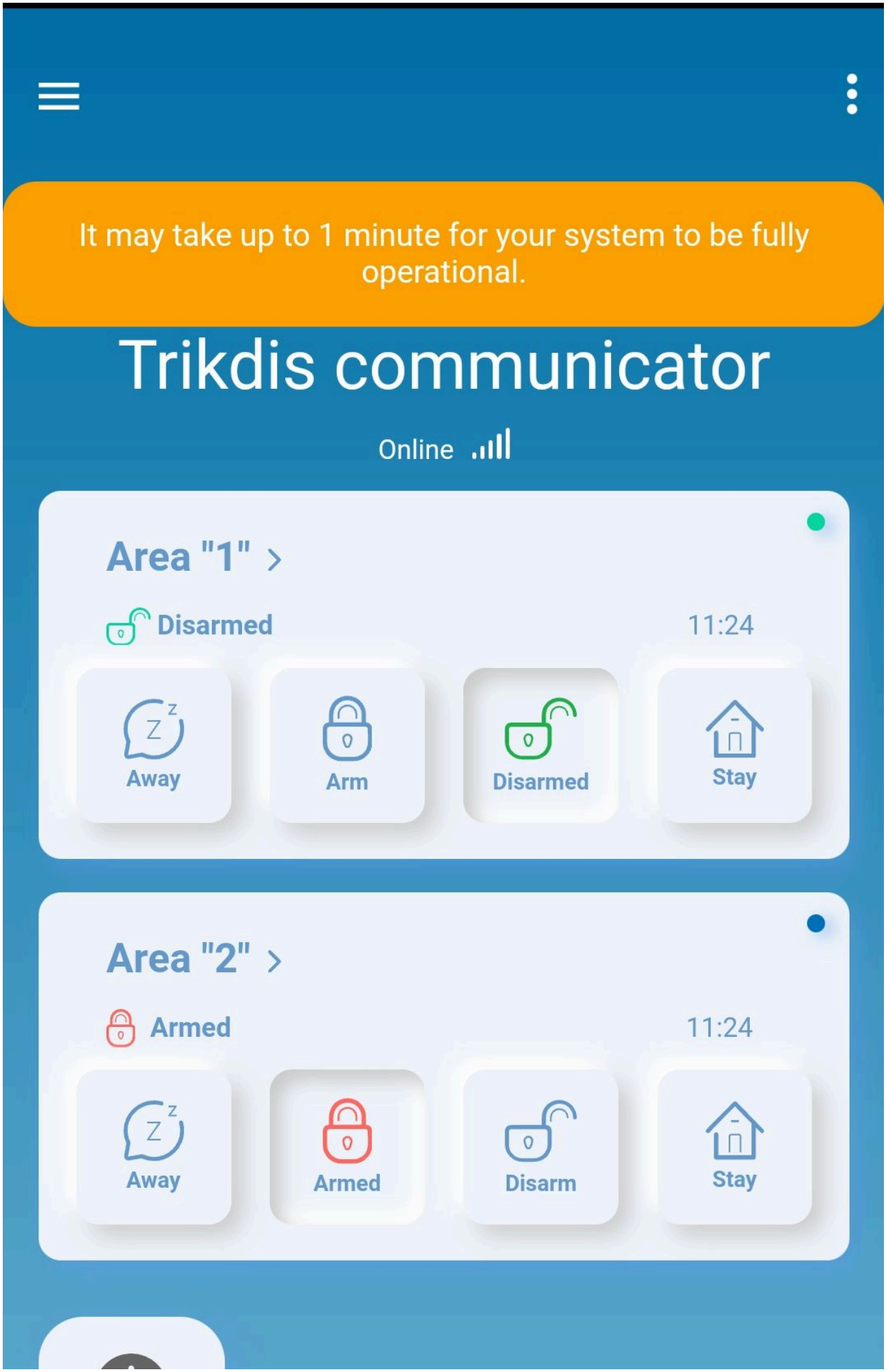
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Pour le G17F, faites attention aux points suivants lors de l'ajout :

1. Après avoir saisi l'identifiant unique (**Unique ID**), cliquez sur le bouton **Next**. Vous trouverez l'identifiant sur l'étiquette de l'appareil et de la boîte ; avec une connexion USB, vous le voyez aussi dans la barre d'état de TrikdisConfig (**IMEI/Unique ID**, point 5.1).
2. Si l'installateur a modifié la valeur par défaut `123456` du **Cloud Access Code**, l'application demande le code lors de l'ajout (point 2.1).

4.2 Configuration et commande par SMS

1. Modifiez le mot de passe administrateur. Pour des raisons de sécurité, remplacez le mot de passe SMS administrateur par défaut. Envoyez un SMS sous cette forme :

```
PSW 123456 xxxxxx
```

Élément	Signification
`123456`	le mot de passe administrateur par défaut
`xxxxxx`	le nouveau mot de passe administrateur à 6 caractères

2. Autorisez la commande pour d'autres utilisateurs. Par SMS et par appel téléphonique, le système ne peut être commandé que depuis les numéros de téléphone figurant dans la liste des utilisateurs. Depuis le téléphone de l'administrateur, envoyez un SMS avec le numéro de téléphone et le nom des autres personnes, afin qu'elles puissent elles aussi commander le système :

```
SETN xxxxxx PHONEx=+PHONENR#NAME
```

Élément	Signification
`xxxxxx`	le mot de passe administrateur à 6 caractères
`x`	le numéro d'ordre de l'utilisateur dans la liste (si vous saisissez 1, vous transférez vos droits d'administrateur à l'autre utilisateur)
`PHONENR`	le numéro de téléphone de l'utilisateur
`NAME`	le nom de l'utilisateur

Liste des commandes SMS

Commande	Donnée	Description
`INFO`		Demande d'informations sur le communicateur : la réponse contient le type du communicateur, son numéro IMEI, son numéro de série et sa version de firmware. Exemple : `INFO 123456`
`RESET`		Redémarrage de l'appareil. Exemple : `RESET 123456`

Commande	Donnée	Description
`OUTPUTx`	`ON`	Activation d'une sortie ; « x » est le numéro de la sortie. Exemple : `OUTPUT1 123456 ON`
`OUTPUTx`	`OFF`	Désactivation d'une sortie ; « x » est le numéro de la sortie. Exemple : `OUTPUT1 123456 OFF`
`OUTPUTx`	`PULSE=ttt`	Activation d'une sortie pendant quelques secondes : « x » est le numéro de la sortie OUT, « ttt » un nombre à trois chiffres, la durée d'impulsion en secondes. Exemple : `OUTPUT1 123456 PULSE=002`
`PSW`	nouveau mot de passe	Changement du mot de passe. Exemple : `PSW 123456 654123`
`TIME`	`YYYY/MM/DD,12:00:00`	Réglage de la date et de l'heure. Exemple : `TIME 123456 2025/05/09,10:23:00`
`TXTA`	nom de l'objet	Saisie du nom de l'objet. Exemple : `TXTA 123456 House`
`TXTE`	`Z1=` … `Z12=`	Saisie du texte SMS d'alarme de zone ; Z1…Z12 est le numéro de la zone d'entrée. Exemple : `TXTE 123456 Z1=ALARM in Zone1`
`TXTR`	`Z1=` … `Z12=`	Saisie du texte SMS de rétablissement de zone ; Z1…Z12 est le numéro de la zone d'entrée. Exemple : `TXTR 123456 Z1=Restore Zone1`
`RDR`	`PhoneNR#SMStext`	Transfert d'un SMS vers le numéro indiqué ; le numéro de téléphone doit commencer par « + » et l'indicatif international du pays. Exemple : `RDR 123456 +37061234567#forwarded text`
`ASKI`		Demande par SMS de l'état des entrées (IN). Exemple : `ASKI 123456`
`ASKO`		Demande par SMS de l'état des sorties (OUT). Exemple : `ASKO 123456`
`SETN`	`PhoneX=PhoneNR#Name`	Ajout d'un numéro de téléphone et d'un nom d'utilisateur pour l'utilisateur « x » (« x » est la ligne du numéro de téléphone dans la liste). Le numéro de téléphone doit commencer par « + » et l'indicatif international du pays ; le numéro de téléphone et le nom d'utilisateur sont séparés par le signe #. Exemple : `SETN 123456 PHONE5=+37061234567#JOHN`
`SETN`	`PhoneX=DEL`	Suppression du numéro de téléphone et du nom de l'utilisateur du système. Exemple : `SETN 123456 PHONE5=DEL`
`UUSD`	`*Uusd code#`	Envoi d'un code USSD à l'opérateur (la commande s'appelle effectivement `UUSD`). Exemple : `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON`	Connexion au service cloud Protegus. Exemple : `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`Protegus=OFF`	Déconnexion du service cloud Protegus. Exemple : `CONNECT 123456 PROTEGUS=OFF`
`CONNECT`	`Code=123456`	Le code du service cloud Protegus. Exemple : `CONNECT 123456 CODE=123456`
`CONNECT`	`IP=0.0.0.0:8000`	L'adresse IP TCP et le port du canal de liaison du serveur principal. Exemple : `CONNECT 123456 IP=0.0.0.0:8000`
`CONNECT`	`IP=0`	Désactivation du canal principal. Exemple : `CONNECT 123456 IP=0`
`CONNECT`	`ENC=123456`	La clé de chiffrement TRK. Exemple : `CONNECT 123456 ENC=123456`
`CONNECT`	`APN=Internet`	Le nom de l'APN. Exemple : `CONNECT 123456 APN=INTERNET`
`CONNECT`	`USER=user`	Le nom d'utilisateur de l'APN. Exemple : `CONNECT 123456 USER=User`

Commande	Donnée	Description
`CONNECT`	`PSW=password`	Le mot de passe de l'APN. Exemple : `CONNECT 123456 PSW=Password`

4.3 Commande des sorties PGM par appel téléphonique

Si aucun utilisateur n'a encore été ajouté au système, la première personne qui appelle le G17F devient l'administrateur du système, et elle seule peut commander le G17F par appel et par commandes SMS. Si vous voulez autoriser la commande par appel pour d'autres utilisateurs, ajoutez-les dans TrikdisConfig (point 5.4) ou donnez-leur le droit par commande SMS (point 4.2).

Si vous voulez commander une sortie PGM à distance :

- L'utilisateur doit avoir le droit de commander les sorties (OUT) (point 5.4), et le type **Remote control** doit être affecté à la sortie (OUT) dans TrikdisConfig (page **PGM**, **Output definition**, point 5.7).
- Appelez le numéro de la carte SIM du G17F. Le G17F prend l'appel, et vous pouvez saisir des commandes avec le clavier du téléphone selon le tableau.

Touches	Fonction	Description
`[sortie]*[état]#`	commande de la sortie (OUT) choisie	Commute la sortie PGM indiquée. État : **0** – sortie désactivée ; **1** – sortie activée ; **2** – désactivée pendant la durée d'impulsion ; **3** – activée pendant la durée d'impulsion (la durée d'impulsion se règle dans le tableau **PGM** de TrikdisConfig, point 5.7). Le **#** marque la fin de la commande. Exemples : activation de la sortie 1 : `1*1#` ; désactivation de la sortie 1 : `1*0#` ; activation de la sortie 2 pendant la durée d'impulsion indiquée dans le tableau **PGM** : `2*3#`
`#`	recommencer la commande	Si vous vous êtes trompé dans la commande, appuyez sur la touche **#** du téléphone et saisissez de nouveau la commande.

5. Les pages de TrikdisConfig

Ce chapitre décrit les pages de la fenêtre de programmation de TrikdisConfig, dans l'ordre où elles se suivent dans le menu de gauche. Raccordement du G17F par câble USB : chapitre 2 ; à distance : chapitre 6.

5.1 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.

Libellé	Signification
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 37. La barre d'état du G17F : **Status: Ready**, **Device: G17F_54S0**, **BL** 2.03, **FW** 1.18, **State: USB**, **Role: Administrator** ; à gauche, le champ **IMEI/Unique ID** et le champ du numéro de série. Pour le G17F, le champ **Device** doit indiquer le type **G17F**.

En cliquant sur le bouton **Read [F4]**, le logiciel lit et affiche les réglages actuels enregistrés dans le G17F. Réglez les paramètres nécessaires à l'aide des descriptions de pages qui suivent.

5.2 Page « System Options »

Les réglages généraux de l'appareil, sur deux onglets : **System general** et **Access**.

Onglet System general

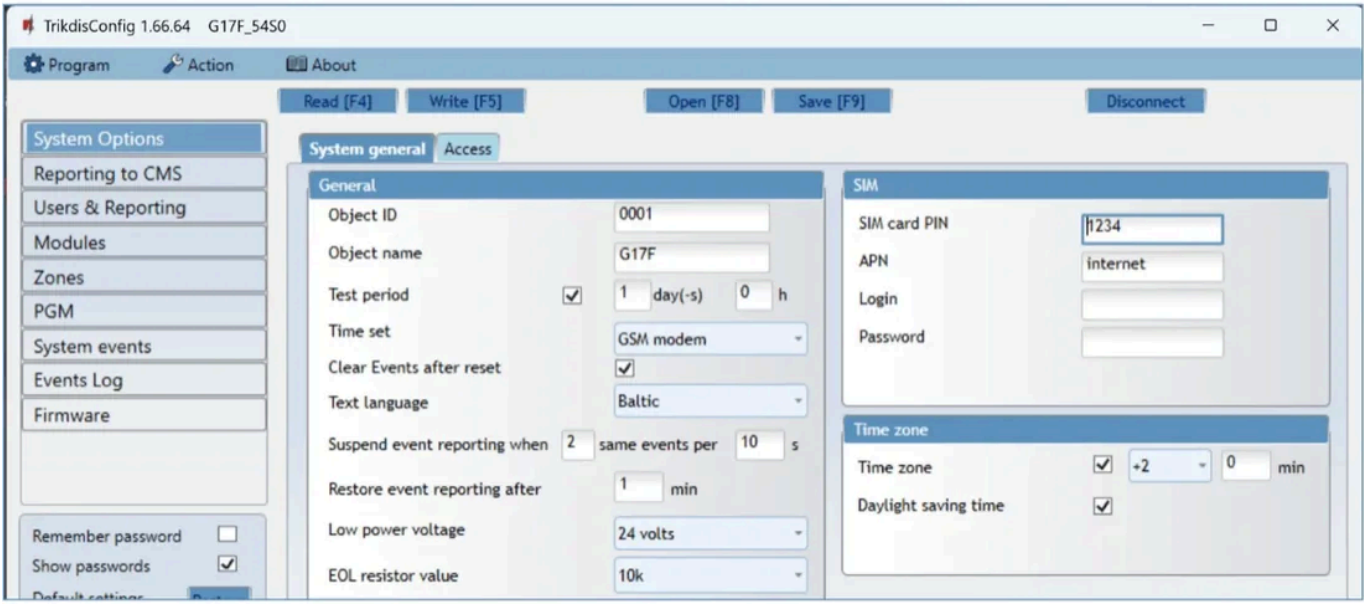


Figure 38. TrikdisConfig – **System Options**, onglet **System general** : les groupes **General**, **SIM** et **Time zone**. En bas du groupe **General**, le champ **EOL resistor value** est également visible (10k sur l'image).

Groupe General

- **Object ID** – si les événements sont envoyés au centre de télésurveillance, saisissez l'identifiant de l'objet fourni par le centre de télésurveillance (nombre hexadécimal à 4 caractères, 0–9, A–F). N'utilisez pas les identifiants FFFE et FFFF.
- **Object name** – le nom de l'objet ; ce nom figure dans les SMS envoyés aux utilisateurs.
- **Test period** – si la case est cochée, le G17F envoie un message « Test » à l'intervalle réglé.
- **Time set** – la source de synchronisation de l'heure. **IP server** : l'heure se cale sur celle du récepteur IP ; **Cellular modem** (**GSM modem** sur l'image) : sur celle du serveur de l'opérateur mobile.
- **Clear Events after reset** – si la case est cochée, tous les messages d'événement non envoyés sont effacés lors du redémarrage (reset).
- **Text language** – la langue des SMS : l'appareil utilise dans les SMS les caractères spécifiques de la langue choisie.
- **Suspend event reporting when … same events per … s** – suspension de l'envoi des événements lorsque le nombre indiqué d'événements identiques se répète dans le nombre de secondes indiqué.
- **Restore event reporting after … min** – délai au bout duquel la suspension de l'envoi des événements prend fin (0–999 minutes).
- **Low power voltage** – indiquez la tension d'alimentation (12 V ou 24 V) de l'appareil ; les messages de tension d'alimentation basse s'y adaptent.

Groupe SIM

- **SIM card PIN** – le code PIN de la carte SIM.
- **APN** – le nom du point d'accès à l'Internet mobile de l'opérateur mobile. Vous devez le saisir si les messages d'événement sont envoyés par la liaison de données mobile à l'application Protegus 2 ou au centre de télésurveillance. Les données des opérateurs de votre pays et des autres opérateurs européens : Réglage de l'APN – liste des opérateurs mobiles européens.
- **Login**, **Password** – le nom d'utilisateur et le mot de passe de l'APN, si l'opérateur mobile les demande.

Groupe Time zone

- **Time zone** – le fuseau horaire du pays (France : +1).
- **Daylight saving time** – si la case est cochée, l'horloge interne de l'appareil passe automatiquement à l'heure d'été et à l'heure d'hiver.

Onglet Access

Dans l'onglet **Access**, vous réglez les codes d'accès et les droits de l'installateur.

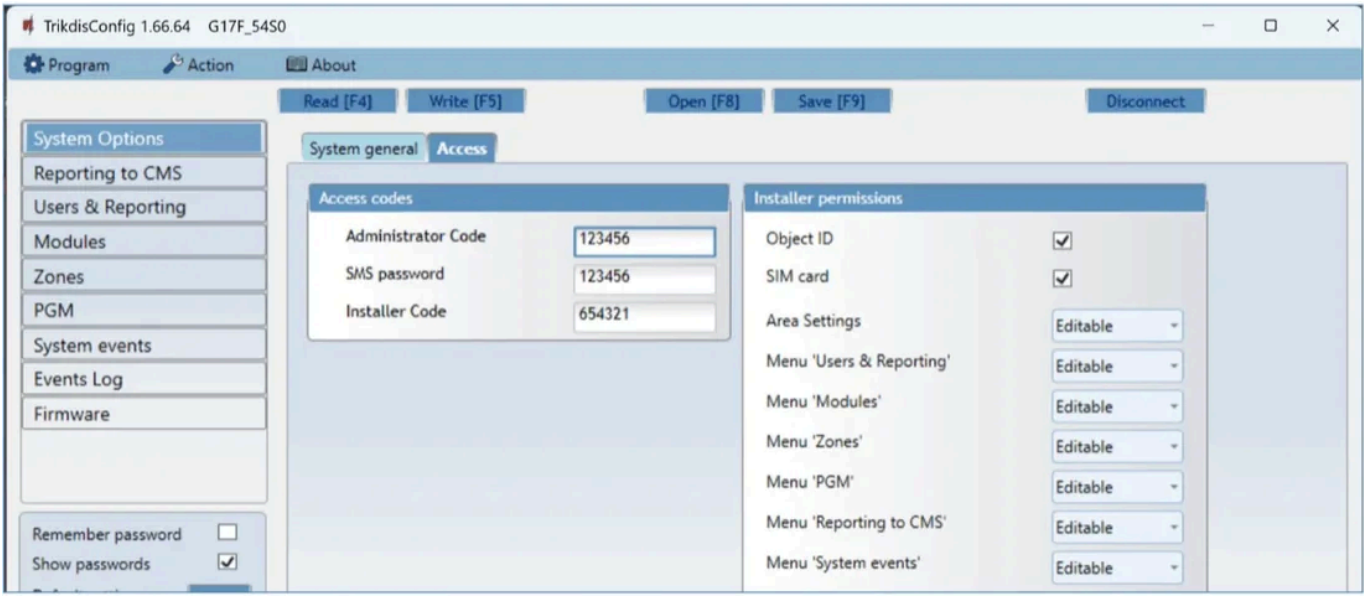


Figure 39. TrikdisConfig – **System Options**, onglet **Access** : le groupe **Access codes** avec les codes par défaut et le groupe **Installer permissions**, dans lequel l'administrateur désigne les réglages que l'installateur peut modifier.

Groupe Access codes

- **Administrator Code** – accès complet aux réglages (par défaut `123456`).
- **SMS password** – mot de passe pour la commande et la programmation à distance par SMS (par défaut `123456`).
- **Installer Code** – accès limité à la modification des réglages (par défaut `654321`).

Groupe Installer permissions – l'administrateur règle ici quels paramètres l'installateur peut modifier.

Pour des raisons de sécurité, modifiez les codes par défaut. Vous pouvez aussi changer le mot de passe SMS par SMS (`PSW`, point 4.2).

5.3 Page « Reporting to CMS »

Le G17F envoie les messages au centre de télésurveillance par l'Internet mobile (IP) ou par SMS. Un canal de secours peut être associé au canal principal : l'appareil l'utilise lorsque la liaison est interrompue sur le canal principal.

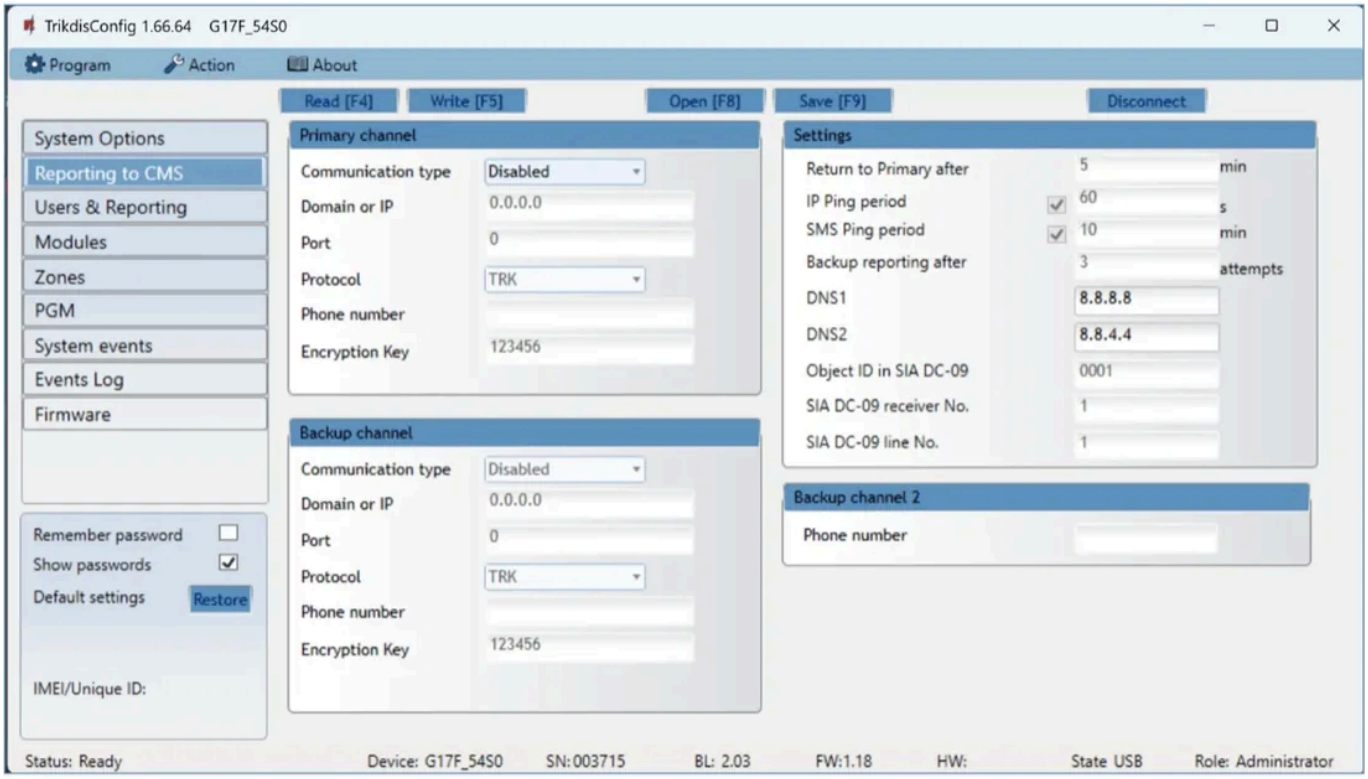


Figure 40. TrikdisConfig – **Reporting to CMS** : les groupes **Primary channel**, **Backup channel**, **Settings** et **Backup channel 2**. Sur l'image : **Communication type: Disabled**, **Return to Primary after** 5 minutes, **IP Ping period** 60 s, **SMS Ping period** 10 minutes, **Backup reporting after** 3 tentatives, **DNS1** 8.8.8.8, **DNS2** 8.8.4.4.

Les messages envoyés au centre de télésurveillance sont codés et protégés par mot de passe. Pour recevoir les messages et les transmettre au logiciel de télésurveillance, un récepteur Trikdis est nécessaire :

- pour les messages IP : le logiciel récepteur **IPcom** (Windows ou Linux), le récepteur matériel IP/SMS **RL14** ou le récepteur multicanal **RM14** ;
- pour les SMS : le récepteur matériel IP/SMS **RL14**, le récepteur multicanal **RM14** ou le récepteur SMS **GM14**.

Récepteur logiciel Trikdis IPcom v5 Windows **Récepteur logiciel Trikdis IPcom v5 Linux**

La liaison SMS est extrêmement utile comme canal de secours, car elle fonctionne même lorsque la connexion Internet tombe sur le réseau de l'opérateur mobile. Nous ne recommandons pas le SMS comme canal principal.

Groupe Primary channel (canal principal)

- **Communication type** – le mode de liaison avec le récepteur du centre de télésurveillance.
- **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- **Port** – le port réseau du récepteur.
- **Protocol** – les récepteurs IP Trikdis reçoivent les messages envoyés avec le protocole **TRK** ; pour les récepteurs IP capables de recevoir des messages SIA DC-09, choisissez le protocole **DC-09_2007** ou **DC-09_2012**.
- **Phone number** – (uniquement pour les SMS) le numéro de téléphone du récepteur SMS Trikdis, commençant par l'indicatif du pays (par exemple 33xxxxxxxx).
- **Encryption Key** – clé de chiffrement à 6 chiffres ; elle doit être identique à la clé de chiffrement du récepteur.

Groupe Backup channel (canal de secours) – activez-le pour que le G17F envoie les messages par le canal de secours lorsque la liaison est interrompue. Ses réglages sont les mêmes que ceux du canal principal.

Groupe Settings

- **Return to Primary after** – délai au bout duquel le G17F tente de revenir au canal principal.
- **IP Ping period** – l'intervalle d'envoi des signaux PING internes qui contrôlent la liaison. Les signaux PING ne passent que par le canal IP ; le récepteur ne les transmet pas au logiciel de télésurveillance, ils ne le surchargent donc pas. Le logiciel n'est averti que si le récepteur ne reçoit pas de PING de l'appareil pendant la durée réglée.
- **SMS Ping period** – l'intervalle, en minutes, du signal PING envoyé par le canal SMS. Pour utiliser ce canal, cochez la case et indiquez l'intervalle.
- **Backup reporting after** – le nombre de tentatives d'envoi infructueuses après lequel le G17F envoie par le canal de secours (**Backup channel**).
- **DNS1**, **DNS2** – les serveurs DNS qui traduisent le nom de domaine en adresse IP. Ils sont nécessaires si vous avez saisi un nom de domaine (et non une adresse IP) dans le champ **Domain or IP** du canal. Par défaut, ce sont les serveurs DNS de Google.

L'intervalle de PING

Par défaut, le récepteur envoie un message « Connection lost » (liaison interrompue) au logiciel de télésurveillance s'il ne reçoit pas de PING pendant trois fois l'intervalle d'envoi de PING de l'appareil : avec un **IP Ping period** de 3 minutes, par exemple, au bout de 9 minutes. Les messages PING maintiennent aussi active la liaison entre l'appareil et le récepteur – la liaison active est nécessaire pour la configuration et la commande à distance. Nous recommandons de régler l'intervalle de PING sur 5 minutes au maximum.

Les champs ci-dessous ne sont visibles que si vous avez choisi le protocole **DC-09_2007** ou **DC-09_2012** dans le champ **Protocol** du canal :

- **Object ID in SIA DC-09** – le numéro de l'objet ; avec le protocole DC-09, c'est ce numéro qui figure dans les messages. Saisissez le nombre hexadécimal de 3 à 16 caractères fourni par le centre de télésurveillance.
- **SIA DC-09 receiver No.** – le numéro du récepteur.
- **SIA DC-09 line No.** – le numéro de la ligne dans le récepteur.

Groupe Backup channel 2

- **Phone number** – (uniquement pour les SMS) le numéro de téléphone du récepteur SMS Trikdis, commençant par l'indicatif du pays (par exemple 33xxxxxxxxx).

5.4 Page « Users & Reporting »

Les réglages des utilisateurs, du cloud Protegus et des réponses SMS, sur trois onglets : **Users**, **SMS answer texts** et **SMS for Panel events**.

Onglet Users

Dans l'onglet **Users**, vous indiquez les utilisateurs qui reçoivent des SMS et des appels, et vous y activez le cloud Protegus.

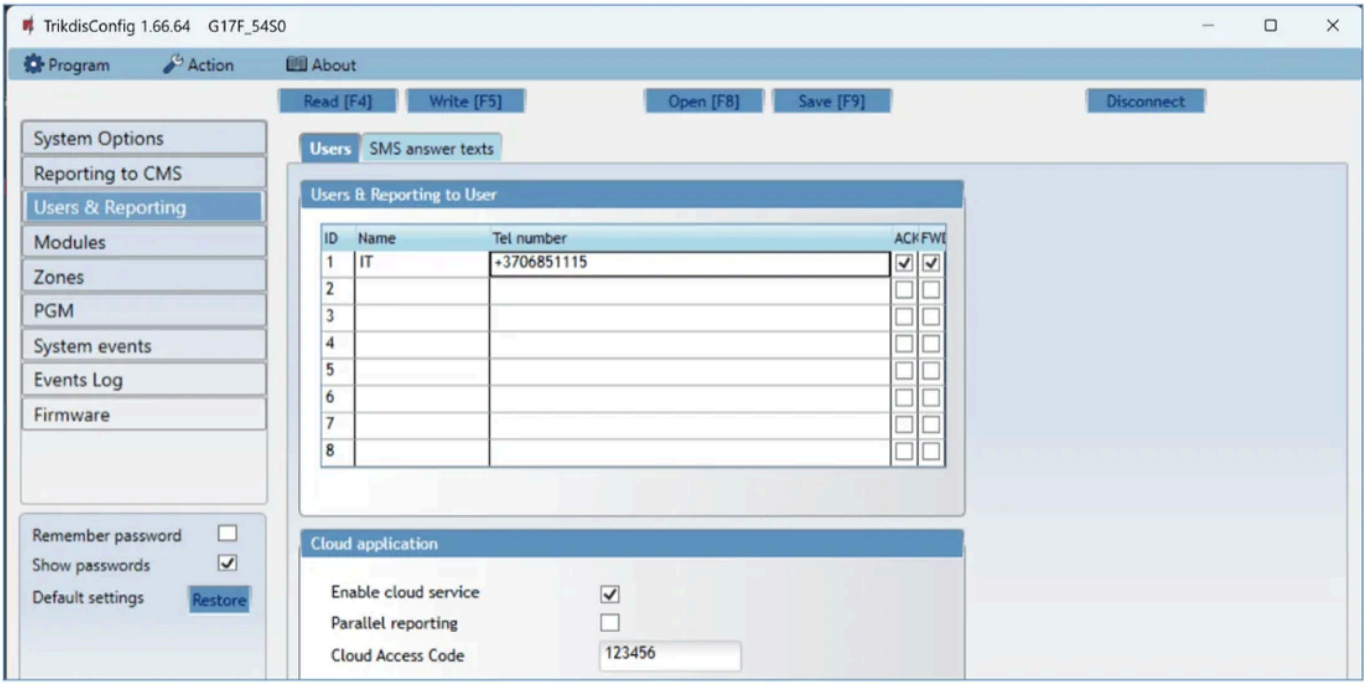


Figure 41. TrikdisConfig – **Users & Reporting**, onglet **Users** : le tableau **Users & Reporting to User** (**ID**, **Name**, **Tel number**, **ACK**, **FWD**) et le groupe **Cloud application** (**Enable cloud service**, **Parallel reporting**, **Cloud Access Code**).

Groupe Users & Reporting to User

- **ID** – le numéro d'ordre de l'utilisateur dans la liste.
- **Name** – le nom de l'utilisateur ; ce nom figure dans les SMS d'événement.
- **Tel number** – le numéro de téléphone de l'utilisateur auquel les SMS sont envoyés ; saisissez-le au format international (+33…).
- **PGM** – si la case est cochée, l'utilisateur peut commander les sorties à distance (cette colonne n'est pas visible sur l'image ci-dessus).
- **ACK** – si la case est cochée, le G17F envoie un SMS de réponse à l'utilisateur après chaque commande SMS reçue (texte des réponses : onglet **SMS answer texts**).
- **FWD** – si la case est cochée, le G17F transfère à l'utilisateur les SMS provenant de numéros extérieurs au système (par exemple la notification de solde de la carte SIM ou des messages publicitaires).

Groupe Cloud application

- **Enable cloud service** – activation du service Protegus : le G17F échange ainsi des données avec l'application Protegus 2 et peut aussi être configuré à distance avec TrikdisConfig (chapitre 6).
- **Parallel reporting** – envoi parallèle : les messages partent simultanément par le canal principal et vers Protegus 2.
- **Cloud Access Code** – code à 6 chiffres pour l'accès à Protegus 2 (par défaut `123456`).

Onglet SMS answer texts

Dans la colonne **SMS text**, vous pouvez modifier le texte des réponses envoyées aux commandes SMS.

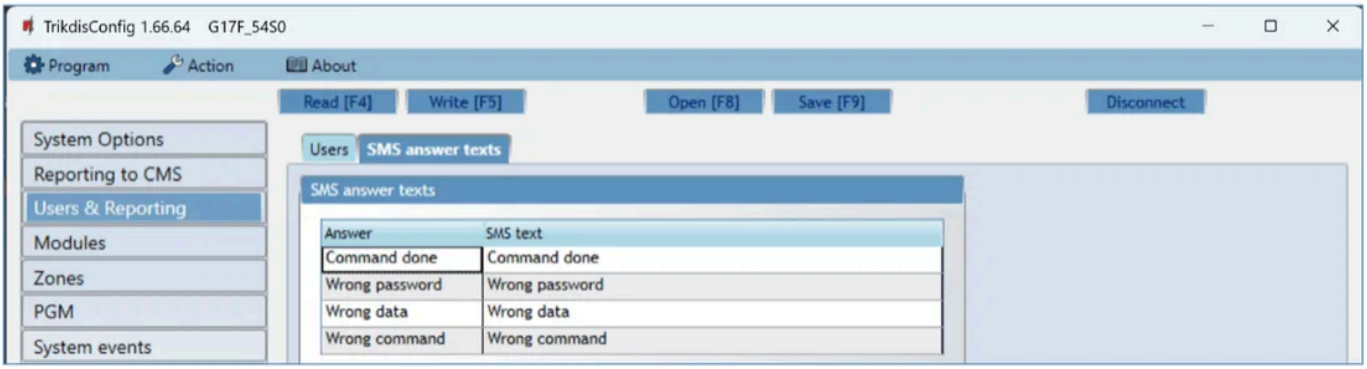


Figure 42. TrikdisConfig – **Users & Reporting**, onglet **SMS answer texts** : **Command done** (commande exécutée), **Wrong password** (mot de passe erroné), **Wrong data** (donnée erronée), **Wrong command** (commande erronée).

Onglet SMS for Panel events

Cet onglet n'apparaît que si vous avez saisi au moins un numéro de téléphone d'utilisateur dans l'onglet **Users**. Vous y réglez si les utilisateurs reçoivent un SMS et/ou un appel pour les événements de la centrale incendie.

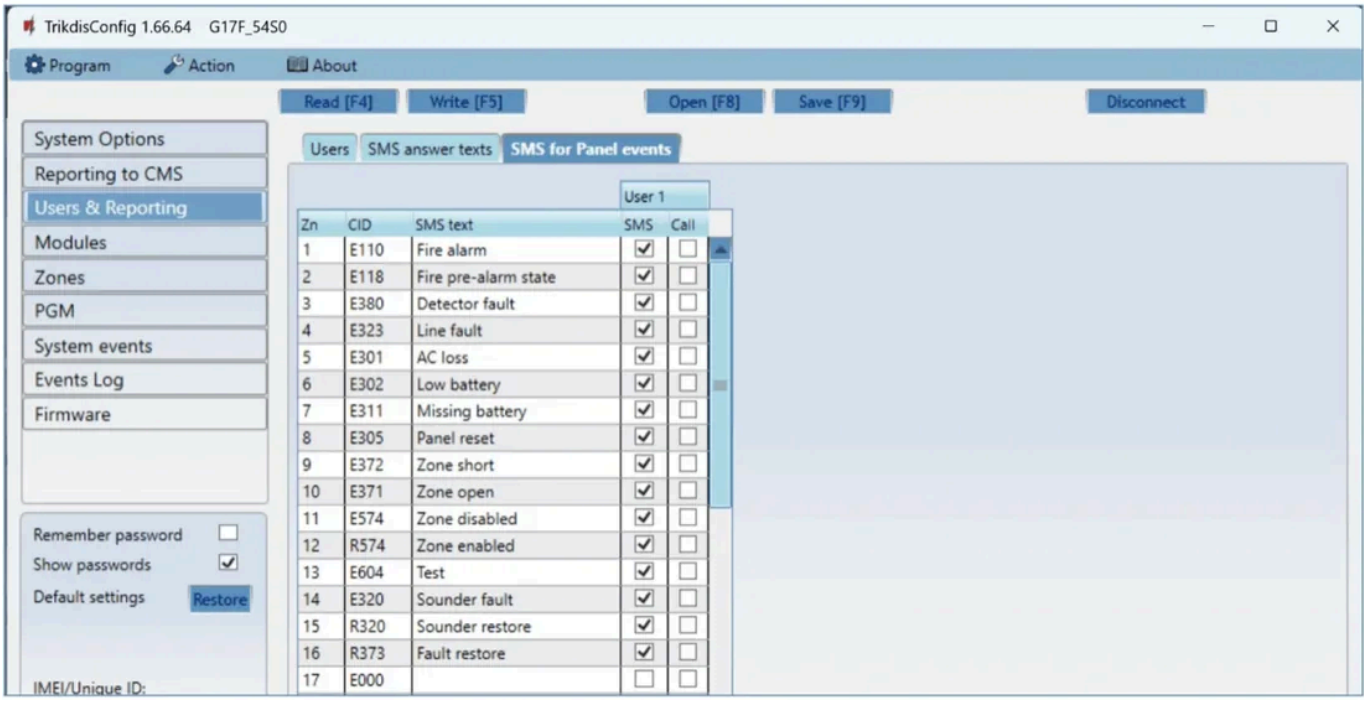


Figure 43. TrikdisConfig – **Users & Reporting**, onglet **SMS for Panel events** : les événements de la centrale avec leur code Contact ID, par exemple E110 alarme incendie (**Fire alarm**), E118 pré-alarme (**Fire pre-alarm state**), E380 défaut de détecteur (**Detector fault**), E301 coupure de l'alimentation secteur (**AC loss**), E302 tension de batterie basse (**Low battery**) ; dans la colonne **User 1**, les cases **SMS** et **Call**.

- **Zn** – le numéro d'ordre de l'événement dans la liste.
- **CID** – le code Contact ID de l'événement.
- **SMS text** – le texte SMS de l'événement.
- **User SMS/Call** – pour chaque événement, vous pouvez choisir si l'utilisateur reçoit un SMS et/ou un appel.

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.

5.5 Page « Modules »

La liste des modules et des centrales incendie raccordés au bus RS485, ainsi que les réglages des modules W485 et E485.

Onglet RS485 modules

Dans la liste, vous indiquez un module ou une centrale incendie par ligne (8 au maximum).

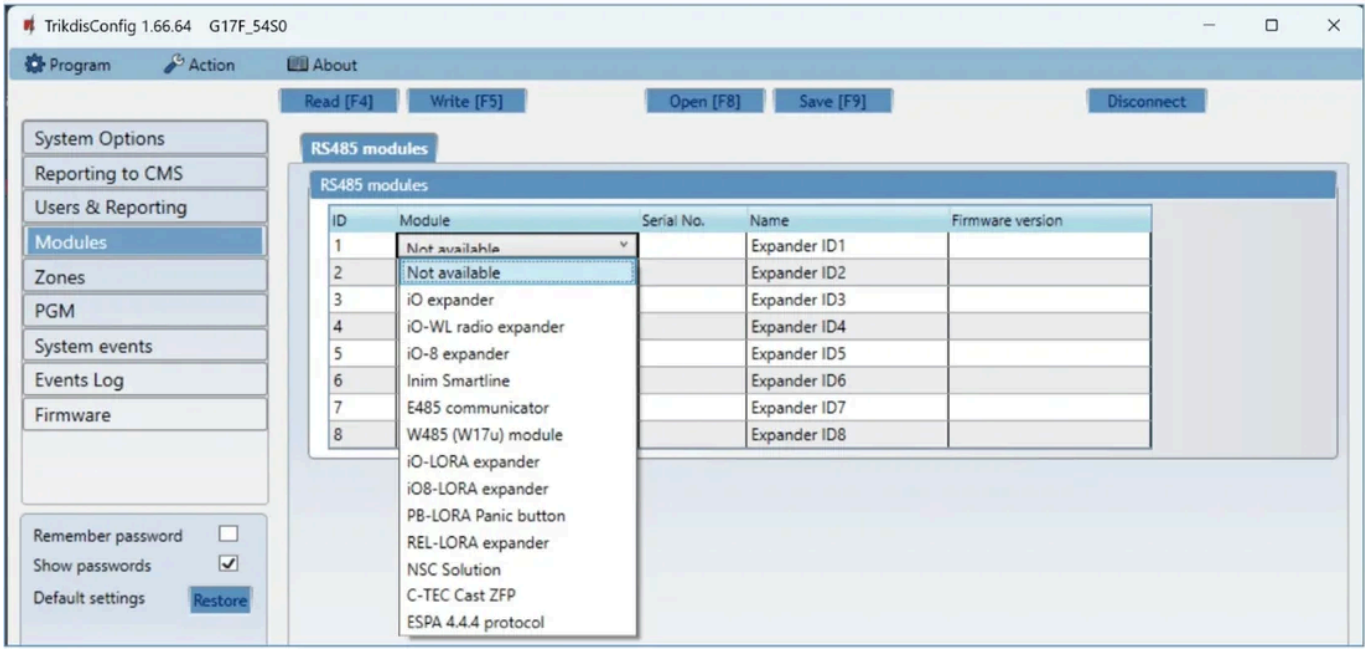


Figure 44. TrikdisConfig – **Modules**, onglet **RS485 modules** : huit lignes (ID 1–8) ; sur la première ligne, la liste **Module** est déroulée avec les modules et les centrales incendie disponibles.

- **ID** – le numéro d'ordre du module dans la liste.
- **Module** – le module ou la centrale utilisé : iO, iO-WL, iO-8, INIM Smartline, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, NSC Solution, C-TEC Cast ZFP, ESPA 4.4.4.
- **Serial No.** – nombre obligatoire à 6 chiffres ; vous le trouverez sur le boîtier et l'emballage du module.
- **Name** – le nom du module (libre).
- **Firmware version** – la version de firmware du module ; elle apparaît lorsque le G17F trouve le module raccordé.

Onglet W485 settings

Les réglages du module WiFi W485 (W17u) (raccordement : point 3.11).

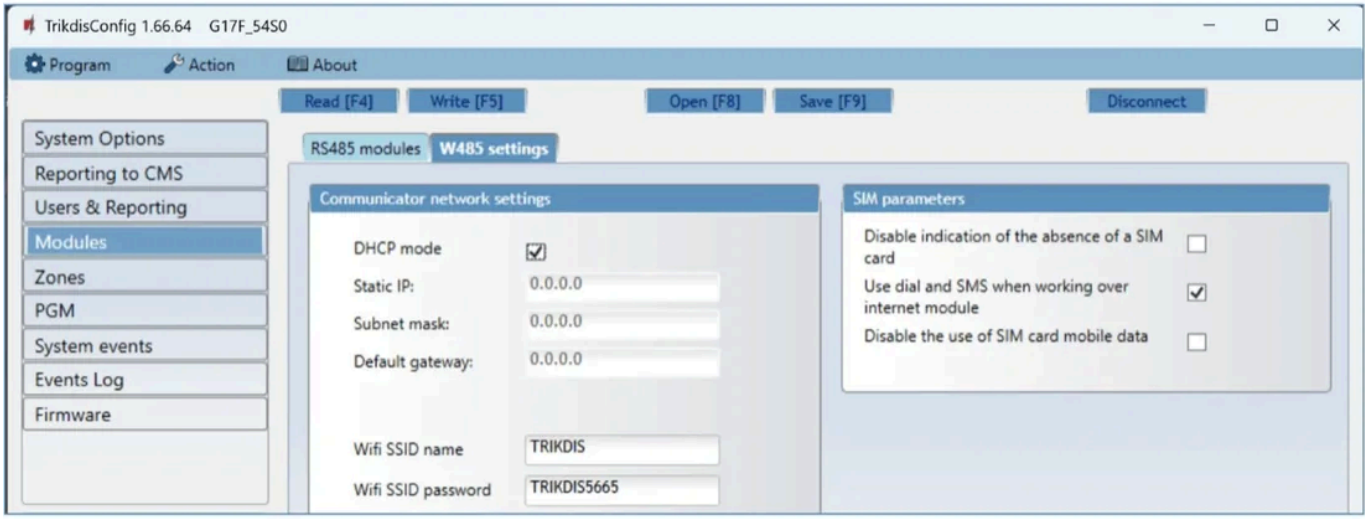


Figure 45. TrikdisConfig – **Modules**, onglet **W485 settings** : le groupe **Communicator network settings** (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**, **Wifi SSID name**, **Wifi SSID password**) et le groupe **SIM parameters**.

Groupe Communicator network settings

- **DHCP mode** – le mode d'enregistrement réseau du module WiFi (manuel ou automatique). Si la case est cochée (mode automatique), le module reconnaît automatiquement les paramètres réseau (masque de sous-réseau, passerelle) et obtient une adresse IP.
- **Static IP** – adresse IP statique en mode manuel.
- **Subnet mask** – masque de sous-réseau en mode manuel.
- **Default gateway** – passerelle par défaut en mode manuel.
- **Wifi SSID name** – le nom du réseau WiFi auquel le W485 (W17u) se connecte.
- **Wifi SSID password** – le mot de passe du réseau WiFi.

Groupe SIM parameters

- **Disable indication of the absence of a SIM card** – si la case est cochée, le G17F ne signale pas l'absence de carte SIM.
- **Use dial and SMS when working over internet module** – si la case est cochée, le G17F peut aussi être commandé par appel et par SMS. Si la case n'est pas cochée et que le réseau WiFi est disponible, l'appel et le SMS ne sont pas utilisés ; si la case n'est pas cochée et que le réseau WiFi n'est pas disponible, le G17F gère les appels et les SMS et envoie un SMS à l'utilisateur.
- **Disable the use of SIM card mobile data** – si la case est cochée, le G17F n'utilise pas la liaison de données mobile de la carte SIM : les données passent uniquement par le module W485. Si le réseau WiFi est interrompu, le G17F conserve les données dans sa mémoire et les envoie par le module W485 lorsque le WiFi revient.

Onglet E485 settings

Les réglages du module Ethernet E485 (raccordement : point 3.12).

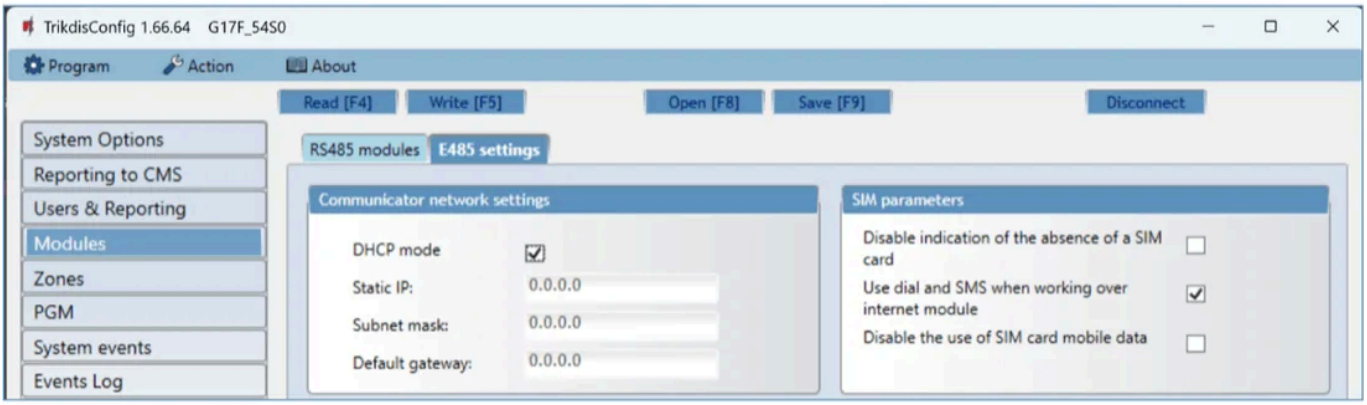


Figure 46. TrikdisConfig – **Modules**, onglet **E485 settings** : le groupe **Communicator network settings** (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**) et le groupe **SIM parameters**.

Groupe Communicator network settings

- **DHCP mode** – le mode d'enregistrement réseau du module Ethernet (manuel ou automatique).
- **Static IP** – adresse IP statique en mode manuel.
- **Subnet mask** – masque de sous-réseau en mode manuel.
- **Default gateway** – passerelle par défaut en mode manuel.

Groupe SIM parameters

- **Disable indication of the absence of a SIM card** – si la case est cochée, le G17F ne signale pas l'absence de carte SIM.
- **Use dial and SMS when working over internet module** – si la case est cochée, le G17F peut aussi être commandé par appel et par SMS. Si la case n'est pas cochée et qu'Internet est disponible, le SMS et l'appel ne sont pas utilisés ; si la case n'est pas cochée et qu'Internet n'est pas disponible, le G17F gère les appels et les SMS et envoie un SMS à l'utilisateur.
- **Disable the use of SIM card mobile data** – si la case est cochée, le G17F n'utilise pas la liaison de données mobile de la carte SIM : les données passent uniquement par le module E485. Si Internet est interrompu, le G17F conserve les données dans sa mémoire et les envoie par le module E485 lorsqu'Internet revient.

5.6 Page « Zones »

Les réglages des zones (entrées), sur deux onglets : **Zones settings** et **SMS & Call reporting**.

Onglet Zones settings

Dans le tableau, vous réglez une zone par ligne.

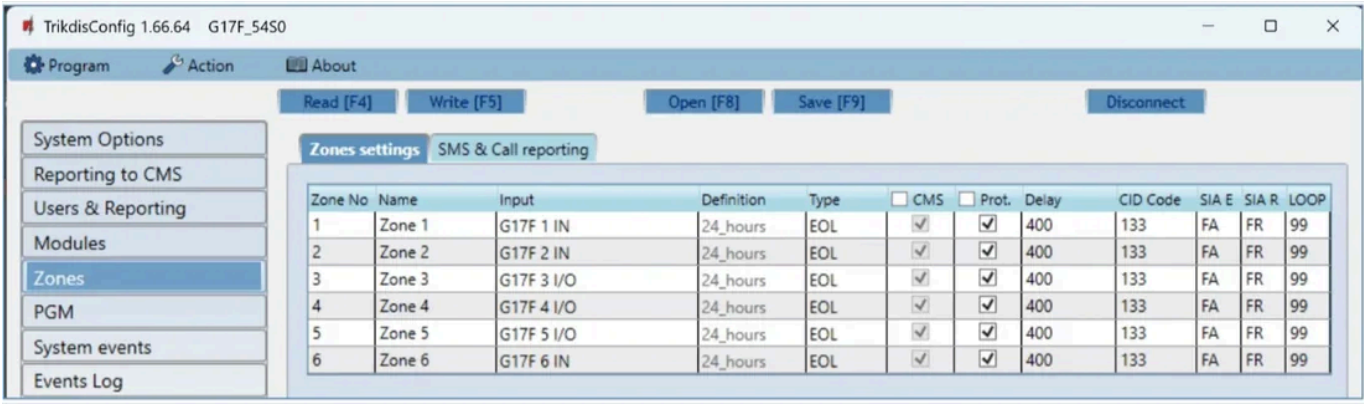


Figure 47. TrikdisConfig – **Zones**, onglet **Zones settings** : sur l'image, six zones sur les six entrées du G17F (**1 IN**, **2 IN**, **3 I/O**, **4 I/O**, **5 I/O**, **6 IN**), chacune avec la définition **24_hours**, le type **EOL**, les cases **CMS** et **Prot.** cochées, un délai de 400 ms et le code CID 133.

- **Zone No** – le numéro d'ordre de la zone dans la liste.
- **Name** – le nom de la zone ; ce nom figure dans les SMS.
- **Input** – l'entrée (IN) du G17F ou du module d'extension qui appartient à la zone.
- **Definition** – toutes les zones ont la définition **24 hours** (24 heures) : lorsque la zone est violée, le message d'événement part immédiatement.
- **Type** – le type de circuit raccordé à l'entrée : **NC** – contact normalement fermé ; **NO** – contact normalement ouvert ; **EOL** – circuit terminé par une résistance de fin de ligne (4,7 kΩ ou 10 kΩ) (point 3.7).
- **CMS** – si la case est cochée, les événements de la zone sont envoyés au centre de télésurveillance.
- **Prot.** – si la case est cochée, une notification est envoyée à l'application Protegus 2 pour les événements de la zone.
- **Delay** – le temps de réaction de l'entrée (IN) en millisecondes.
- **CID Code** – le code Contact ID de l'événement.
- **SIA E** – le code d'événement SIA.
- **SIA R** – le code de rétablissement SIA.
- **LOOP** – le numéro de la boucle ; il figure dans le SMS.

Onglet SMS & Call reporting

Cet onglet n'apparaît que si vous avez saisi au moins un numéro de téléphone d'utilisateur sur la page **Users & Reporting**.

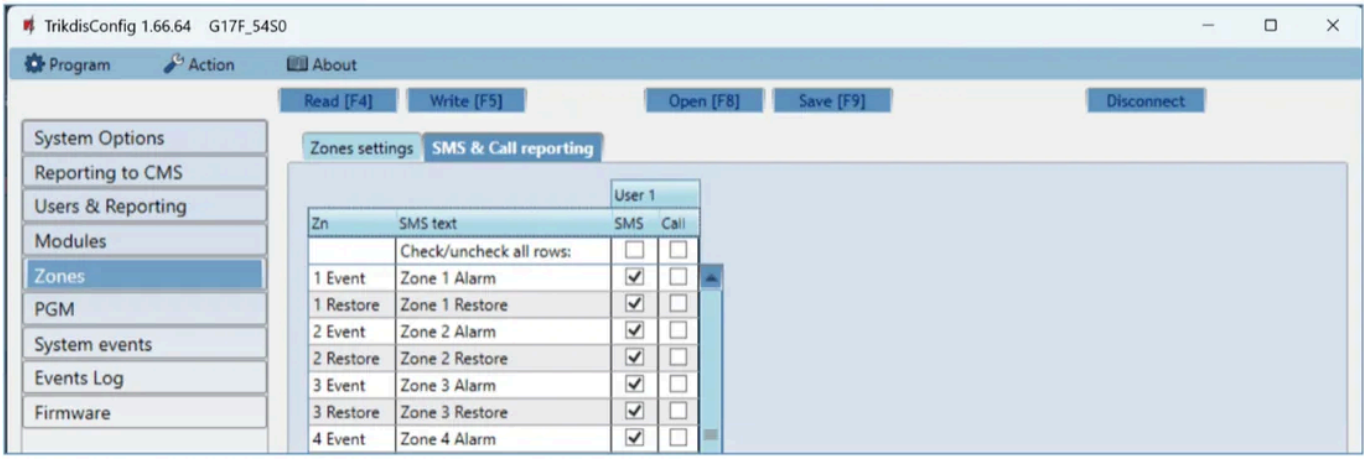


Figure 48. TrikdisConfig – **Zones**, onglet **SMS & Call reporting** : une ligne **Event** et une ligne **Restore** par zone (par exemple Zone 1 Alarm, Zone 1 Restore) ; dans la colonne **User 1**, les cases **SMS** et **Call**.

- **Zn** – le numéro de la zone avec le mot indiquant l'événement : **Event** (événement) ou **Restore** (rétablissement).
- **SMS text** – la description de l'événement de zone ; elle figure dans le SMS d'événement envoyé aux utilisateurs.
- **User SMS/Call** – pour chaque événement de zone, vous pouvez choisir si l'utilisateur reçoit un SMS et/ou un appel.

5.7 Page « PGM »

Les réglages des sorties PGM, sur deux onglets : **Outputs** et **SMS & Call reporting**.

Onglet Outputs

Dans le tableau, vous réglez une sortie PGM par ligne.

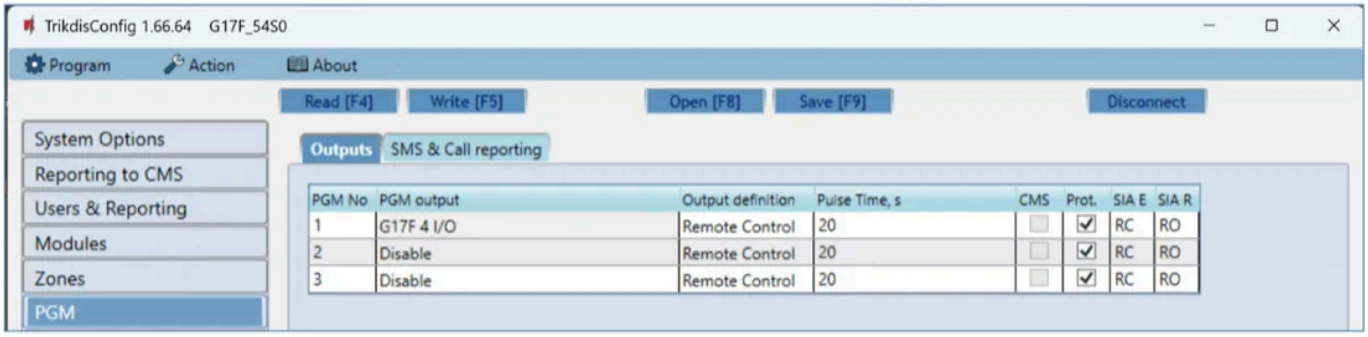


Figure 49. TrikdisConfig – **PGM**, onglet **Outputs** : sur l'image, PGM 1 sur la borne **4 I/O** du G17F, PGM 2 et 3 désactivées (**Disable**) ; sur les trois lignes, la définition de sortie **Remote Control**, une durée d'impulsion de 20 s et la case **Prot.** cochée.

- **PGM No** – le numéro d'ordre de la sortie PGM dans la liste.
- **PGM output** – la sortie (OUT) affectée à la PGM : celle du G17F ou celle d'un équipement externe.
- **Output definition** – le mode de fonctionnement de la sortie (OUT).
- **Pulse time, s** – la durée d'activation de la sortie (OUT), 0–9999 secondes.
- **CMS** – si la case est cochée, les événements choisis sont envoyés au centre de télésurveillance.
- **Prot.** – si la case est cochée, une notification est envoyée à l'application Protegus 2 pour les événements de la sortie.
- **SIA E** – le code d'événement SIA.
- **SIA R** – le code de rétablissement SIA.

Onglet SMS & Call reporting

Cet onglet n'apparaît que si vous avez saisi au moins un numéro de téléphone d'utilisateur sur la page **Users & Reporting**.

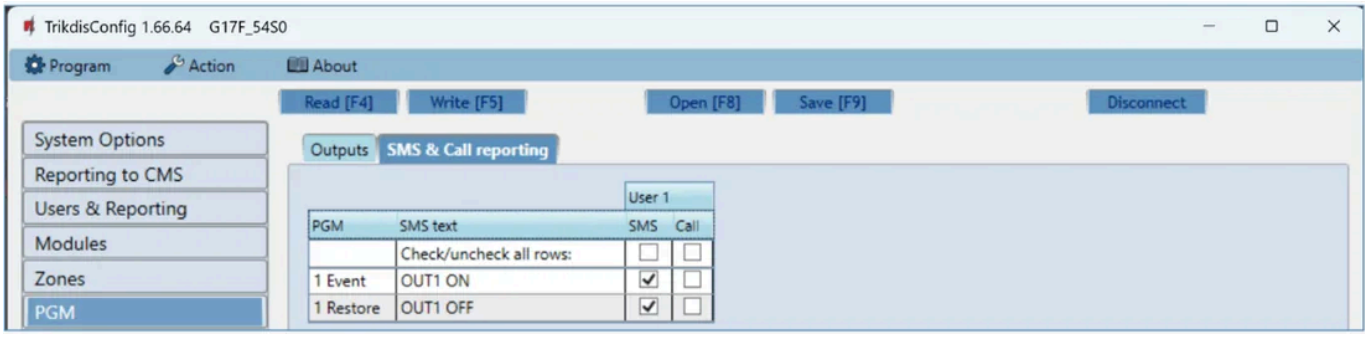


Figure 50. TrikdisConfig – **PGM**, onglet **SMS & Call reporting** : sur la ligne **Event** de la PGM 1, le texte SMS **OUT1 ON**, sur sa ligne **Restore**, le texte SMS **OUT1 OFF** ; dans la colonne **User 1**, la case **SMS** est cochée.

- **PGM** – le numéro de la sortie (OUT) et le type d'événement : **Event** – activation de la sortie ; **Restore** – désactivation de la sortie.
- **SMS text** – le nom de l'événement d'activation ou de désactivation de la sortie ; il figure dans le SMS d'événement.
- **User SMS/Call** – vous pouvez choisir quels utilisateurs reçoivent un SMS et/ou un appel lors de l'activation et de la désactivation de la sortie (OUT).

5.8 Page « System events »

Les réglages des événements propres (système) du communicateur, sur deux onglets : **Events** et **SMS & Call reporting**.

Onglet Events

Dans le tableau, vous réglez un événement système par ligne.

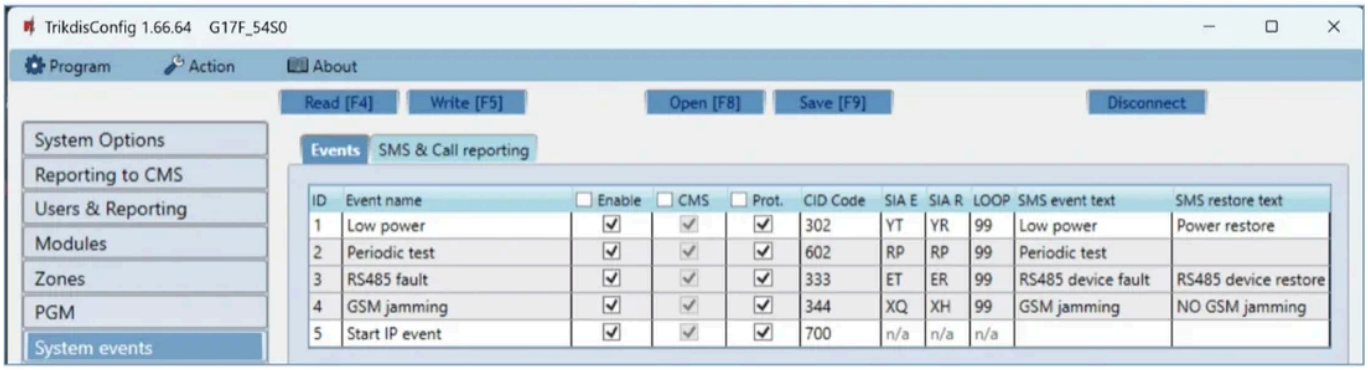


Figure 51. TrikdisConfig – **System events**, onglet **Events** : tension d'alimentation basse (**Low power**, CID 302), test périodique (**Periodic test**, 602), défaut RS485 (**RS485 fault**, 333), brouillage du réseau mobile (**GSM jamming**, 344) et **Start IP event** (700).

- **ID** – le numéro d'ordre de l'événement dans la liste.
- **Event name** – le nom de l'événement.
- **Enable** – activation de la surveillance de l'événement.
- **CMS** – les événements choisis sont envoyés au centre de télésurveillance.
- **Prot.** – une notification est envoyée à l'application Protegus 2 pour les événements choisis.
- **CID Code** – le code Contact ID de l'événement.
- **SIA E** – le code d'événement SIA.
- **SIA R** – le code de rétablissement SIA.
- **LOOP** – le numéro de la boucle ; il figure dans le SMS.
- **SMS event text** – le texte SMS de l'événement.
- **SMS restore text** – le texte SMS du rétablissement.

Onglet SMS & Call reporting

Cet onglet n'apparaît que si vous avez saisi au moins un numéro de téléphone d'utilisateur sur la page **Users & Reporting**.

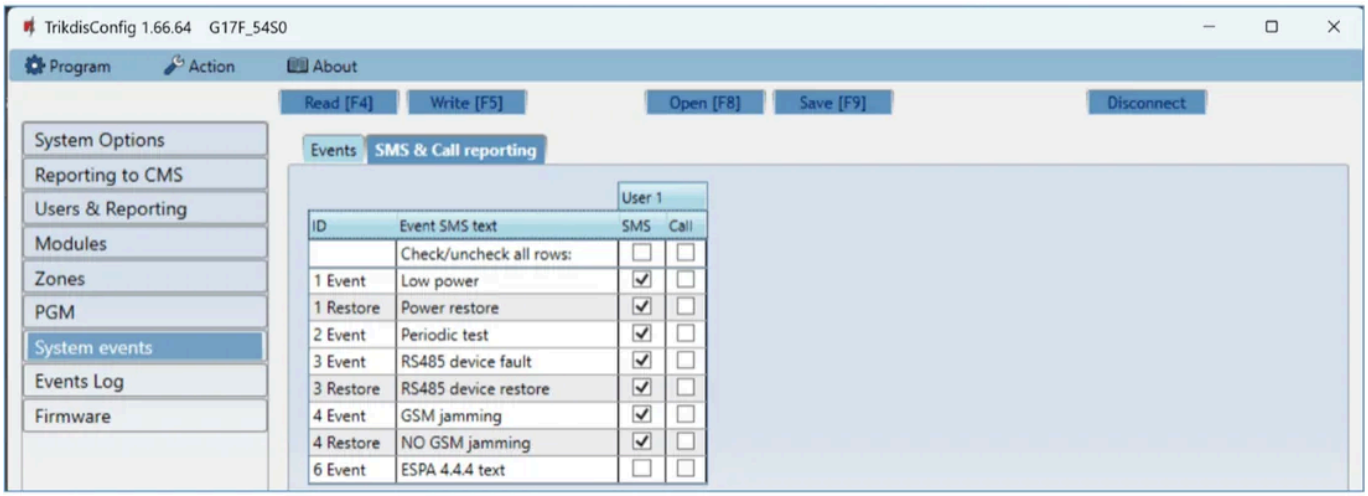


Figure 52. TrikdisConfig – **System events**, onglet **SMS & Call reporting** : les lignes **Event** et **Restore** des événements système (par exemple Low power, Power restore, Periodic test, GSM jamming) ; dans la colonne **User 1**, les cases **SMS** et **Call**.

- **ID** – le numéro d'ordre de l'événement et son mot indicateur (**Event**, **Restore**).
- **Event SMS text** – le texte de l'événement qui figure dans le SMS.
- **User SMS/Call** – pour chaque événement, vous pouvez choisir si l'utilisateur reçoit un SMS et/ou un appel.

5.9 Page « Events Log »

Vous pouvez y lire et effacer le journal des événements de l'appareil.

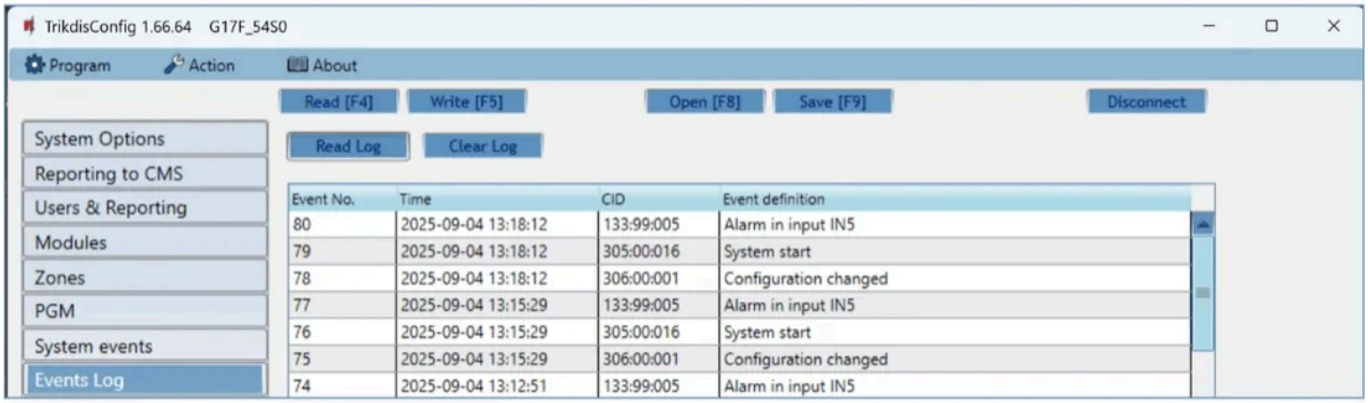


Figure 53. TrikdisConfig – **Events Log** : les boutons **Read Log** et **Clear Log** ; dans le tableau, le numéro d'ordre, l'heure, le code CID et la description de l'événement – sur l'image par exemple une alarme sur l'entrée IN5 (**Alarm in input IN5**), un démarrage du système (**System start**) et une modification de la configuration (**Configuration changed**).

- **Read Log** – le bouton lit le journal des événements dans la mémoire de l'appareil.
- **Clear Log** – le bouton efface les entrées du journal de la mémoire de l'appareil.
- Le tableau affiche le numéro d'ordre (**Event No.**), l'heure (**Time**), le code **CID** et la description (**Event definition**) de l'événement. Le journal affiche jusqu'à 1000 événements enregistrés dans la mémoire du G17F.

5.10 Rétablissement des réglages d'usine

Pour rétablir les réglages d'usine du G17F, cliquez sur le bouton **Restore** de TrikdisConfig (en bas à gauche de la fenêtre de programmation, sur la ligne **Default settings**).



Figure 54. TrikdisConfig – le bouton **Restore** de la ligne **Default settings** ; en dessous, le champ **IMEI/Unique ID** et la barre d'état.

Si vous pouvez avoir besoin plus tard des réglages actuels, enregistrez-les dans un fichier avec le bouton **Save [F9]** avant le rétablissement (point 5.1).

6. Programmation à distance

Vous pouvez aussi lire et modifier les réglages du G17F à distance avec TrikdisConfig, via le cloud Protegus – sans avoir à vous rendre sur le site.

Conditions de la programmation à distance

La configuration à distance ne fonctionne que si, dans le G17F :

1. une carte SIM activée est insérée et que vous avez saisi ou désactivé le code PIN ;
2. le service Protegus est activé (**Users & Reporting** → **Enable cloud service**, point 5.4) ;
3. l'alimentation est présente (la LED **POWER** clignote en vert) ;
4. l'appareil est connecté au réseau (la LED **NETWORK** est allumée en vert et clignote en jaune).

Si la LED **NETWORK** ou **DATA** reste allumée en jaune fixe, l'appareil ne peut pas se connecter au réseau mobile et/ou à Protegus 2.

1. Lancez TrikdisConfig sur l'ordinateur.
2. Dans la partie **Remote access**, saisissez dans le champ **Unique ID** l'identifiant unique du G17F (**Unique ID**). Vous trouverez ce numéro au dos de l'appareil et sur son emballage.

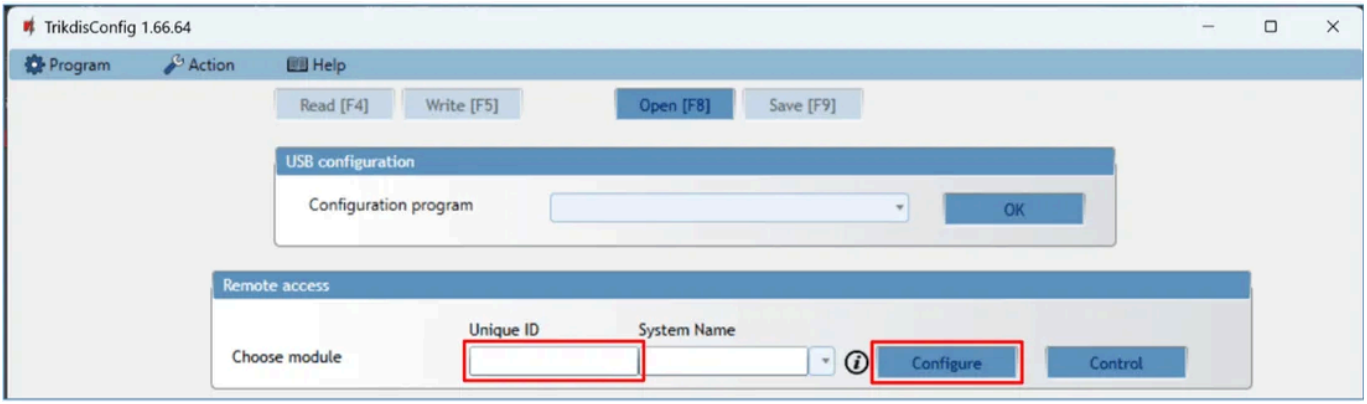


Figure 55. TrikdisConfig – la partie **Remote access** de l'écran d'accueil : le champ **Unique ID**, à côté le champ **System Name**, et le bouton **Configure**.

3. (Facultatif) Dans le champ **System Name**, saisissez un nom pour l'appareil (par exemple le nom de l'objet).
4. Cliquez sur le bouton **Configure**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Read [F4]**. Si le logiciel le demande, saisissez le code administrateur ou le code installateur.

6. À la fin des réglages, cliquez sur le bouton **Write [F5]**. Lorsque vous avez terminé avec TrikdisConfig, cliquez sur le bouton **Disconnect**.

7. Vérification du fonctionnement

À la fin de la configuration et de l'installation, testez tout le système :

1. Pour vérifier une entrée, activez (violez) l'entrée. Vérifiez que l'événement est arrivé au centre de télésurveillance et/ou dans l'application Protegus 2.
2. Pour vérifier les sorties, activez-les à distance et contrôlez leur fonctionnement. Assurez-vous que les événements sont arrivés au centre de télésurveillance et/ou dans l'application Protegus 2.
3. Effectuez un essai d'alarme incendie et vérifiez que le centre de télésurveillance reçoit correctement les événements.

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

Vous pouvez aussi interroger par SMS les données du communicateur ainsi que l'état des entrées et des sorties : `INFO 123456`, `ASKI 123456`, `ASKO 123456` (remplacez `123456` par votre propre mot de passe SMS ; point 4.2).

8. Mise à jour du firmware

Lorsque vous connectez le G17F à TrikdisConfig et qu'un firmware plus récent existe, le logiciel propose de lui-même la mise à jour – l'ordinateur doit pour cela être connecté à Internet. Un antivirus, un pare-feu ou des réglages d'accès à Internet stricts peuvent bloquer la mise à jour automatique.

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.

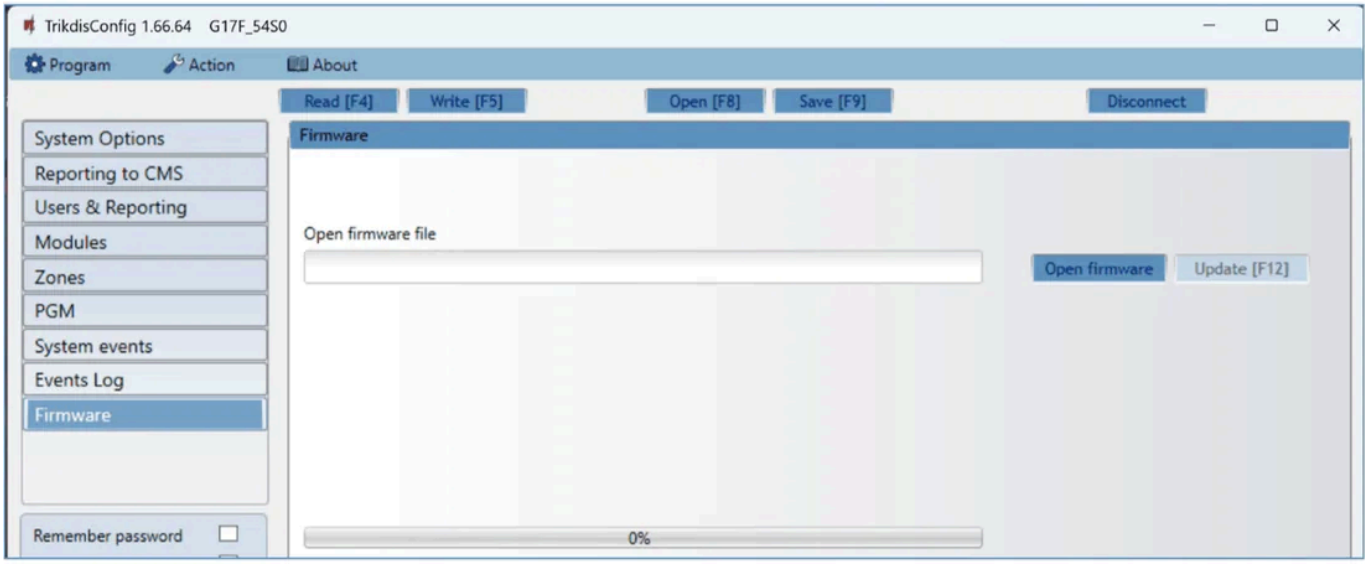


Figure 56. TrikdisConfig – G17F, page **Firmware** : le champ **Open firmware file**, le bouton **Open firmware**, le bouton **Update [F12]** et l'indicateur de progression.

L'utilisation des modules W485 et E485 nécessite au moins le firmware **1.08** du G17F (points 3.11 et 3.12) ; vous voyez la version actuelle dans le champ **FW** de la barre d'état (point 5.1).

9. Dépannage et questions fréquentes

Si le communicateur ne fait pas ce que vous attendez, regardez d'abord les voyants (point 1.6), puis les points ci-dessous.

La LED TROUBLE clignote – que signifie le nombre de clignotements ?

Le nombre de clignotements indique la cause du défaut : **1** – pas de carte SIM ; **2** – le code PIN de la carte SIM est erroné (**System Options** → **SIM card PIN**, point 5.2) ; **3** – impossible de se connecter au réseau mobile ; **4** – impossible de se connecter au récepteur IP sur le canal principal (**Reporting to CMS**, point 5.3) ; **5** – impossible de se connecter au récepteur IP sur le canal de secours ; **6** – l'horloge interne n'est pas réglée (**Time set**, point 5.2 ; par SMS : `TIME`, point 4.2) ; **7** – la tension d'alimentation n'est pas correcte (9–32 V DC ; **Low power voltage**, point 5.2) ; **9** – défaut de liaison avec le module RS485 (raccordement : points 3.3–3.12 ; **Modules**, point 5.5).

Combien de clignotements jaunes faut-il sur la LED NETWORK ?

Le nombre de clignotements jaunes indique le niveau du signal : sur un réseau 2G (GPRS), 5 clignotements suffisent, sur un réseau 4G, 3 clignotements suffisent. Si vous comptez moins de 3 clignotements jaunes, le niveau du signal est insuffisant : choisissez un autre emplacement pour le communicateur ou utilisez une antenne déportée plus sensible (point 1.7). Si les voyants ne s'allument pas du tout, vérifiez l'alimentation et le raccordement (point 3.13).

Protegus 2 ne trouve pas le communicateur

- Vérifiez les conditions d'ajout : carte SIM activée, code PIN saisi ou désactivé, service Protegus activé (**Users & Reporting** → **Enable cloud service**, point 5.4), LED **POWER** clignotant en vert, LED **NETWORK** allumée en vert et clignotant en jaune (point 4.1).
- Si la LED **NETWORK** ou **DATA** reste allumée en jaune fixe, l'appareil ne peut pas se connecter au réseau mobile et/ou à Protegus 2 (chapitre 6). Vérifiez le réglage de l'**APN** (point 5.2).
- Si le **Cloud Access Code** n'est pas la valeur par défaut `123456`, saisissez le bon code lors de l'ajout (point 2.1).

Je ne peux pas commander les sorties par appel ou par SMS

- Par SMS et par appel, la commande n'est possible que depuis les numéros de téléphone figurant dans la liste des utilisateurs (point 4.2). Si aucun utilisateur n'a encore été ajouté, la première personne qui appelle devient l'administrateur (point 4.3).
- L'utilisateur doit avoir le droit de commander les sorties (case **PGM**, point 5.4), et la définition **Remote Control** doit être affectée à la sortie (**Output definition**, point 5.7).
- Avec un module W485 ou E485, vérifiez la case **Use dial and SMS when working over internet module** (point 5.5) : si elle n'est pas cochée et qu'une connexion Internet est disponible, l'appel et le SMS ne sont pas utilisés.

Je ne reçois pas de réponse à mes commandes SMS

Pour recevoir le SMS de réponse, la case **ACK** doit être cochée pour l'utilisateur (**Users & Reporting**, point 5.4). Vous pouvez modifier le texte des réponses dans l'onglet **SMS answer texts**.

Où vont les SMS de l'opérateur (solde, publicité) ?

Si la case **FWD** est cochée pour l'utilisateur, le G17F lui transfère les SMS provenant de numéros extérieurs au système (par exemple la notification de solde de la carte SIM) (point 5.4).

INIM Smartline : à quoi faut-il faire attention ?

La centrale doit être mise en mode **slave** (esclave) dans le logiciel SmartLeague. Si des répéteurs sont raccordés à la centrale, le G17F ne peut pas être raccordé par le bus RS485 ; et si le G17F est raccordé au bus RS485 de la centrale, les modules d'extension iO du communicateur ne sont pas pris en charge (point 3.5).

NSC Solution : la centrale ne voit pas le communicateur

Après la configuration du G17F, il faut rechercher (scanner) sur la centrale les modules raccordés au bus RS485 (**SCAN RS485**, point 3.4). L'adresse **NSC slave address** ne doit pas être identique à l'adresse des autres modules raccordés à la centrale.

Quel intervalle de PING faut-il régler ?

Nous recommandons un intervalle de PING de 5 minutes au maximum. Par défaut, le récepteur signale l'interruption de la liaison au logiciel de télésurveillance au bout de trois fois l'intervalle de PING ; la liaison active est aussi nécessaire pour la configuration et la commande à distance (point 5.3).

Le G17F peut-il être utilisé sans carte SIM ?

Oui, avec le module WiFi W485 ou le module Ethernet E485 (avec au moins le firmware 1.08 du G17F) : dans ce cas, les messages passent par le module (points 3.11 et 3.12). Si le WiFi ou l'Internet filaire tombe, le G17F enverrait par le réseau mobile – ce secours nécessite une carte SIM. Les réglages du module, par exemple la signalisation de l'absence de carte SIM et l'interdiction de la liaison de données mobile : point 5.5.

10. 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.

- Seule une personne qualifiée peut installer et entretenir le communicateur.
- Avant l'installation, lisez attentivement ce manuel afin d'éviter les erreurs pouvant entraîner un dysfonctionnement, voire un endommagement de l'équipement.
- **Avant tout raccordement électrique, coupez l'alimentation.**
- Les changements, modifications ou réparations non approuvés par le fabricant entraînent la perte de la garantie.
- Respectez la réglementation locale sur les déchets : ne jetez pas l'appareil ni ses composants avec les ordures ménagères – remettez l'appareil usagé comme déchet électronique.

Voir aussi

- Extension d'entrées et de sorties iO8 – manuel d'installation – le module d'extension iO-8 pour le G17F.
- Réglage de l'APN – liste des opérateurs mobiles européens – si la liaison de données mobile ne s'établit pas.
- Application Protegus Android / iPhone et web – à propos de l'application.
- Compte professionnel Protegus 2 (Business Account) – gestion de plusieurs systèmes en tant qu'installateur.
- Documentation en anglais : docs.trikdis.com – LTE communicator for fire alarm control panels G17F.

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

Produits associés

Trikdis G17F 4G GSM / IP communicateur incendie

Trikdis G17F 2G GSM / IP communicateur incendie **Module Trikdis IO8 Wired Expander**

Module d'expanneur sans fil Trikdis RF-Lora **Module d'expanneur sans fil Trikdis Io-Lora**

Module d'expanneur sans fil Trikdis Io8-Lora **Bouton de panique sans fil Trikdis PB-Lora**

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

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

Antenne magnétique Trikdis ME301m avec fil 2,5 m

Récepteur logiciel Trikdis IPcom v5 Windows | **Récepteur logiciel Trikdis IPcom v5 Linux**

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-g17f