Communicateur incendie FireCom – manuel d'installation et de programmation

Manuel d'installation et de programmation du communicateur incendie Trikdis FireCom Ethernet et 4G (EN 54-21, EN 54-4) : alimentation et batterie, raccordement aux sorties ou au bus RS485 de la centrale incendie (ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP, Polon-Alfa 3000), 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-firecom

Sommaire

1. Présentation

1.1 À quoi il sert, comment il fonctionne
1.2 Caractéristiques techniques
1.3 Éléments du communicateur
1.4 Les bornes
1.5 Voyants
1.6 Outillage nécessaire à l'installation

2. Alimentation

2.1 Alimentation principale
2.2 Alimentation de secours
2.3 Contenu de la livraison

3. Installation et raccordement

3.1 Ordre de raccordement
3.2 Raccordement des détecteurs
3.3 Raccordement des détecteurs de fumée
3.4 Raccordement aux sorties de la centrale incendie
3.5 Centrale incendie utilisant le protocole ESPA 4.4.4
3.6 Centrale incendie NSC Solution
3.7 Centrale incendie INIM Smartline
3.8 Centrale incendie C-TEC Cast ZFP
3.9 Centrale incendie Polon-Alfa 3000
3.10 Raccordement d'un capteur de température
3.11 Raccordement d'un relais et d'un indicateur à LED
3.12 Raccordement des entrées de la centrale incendie
3.13 Raccordement des modules d'extension de la série iO
3.14 Mise sous tension du communicateur

4. Configuration rapide avec le logiciel TrikdisConfig

4.1 Configuration pour l'application Protegus 2
4.2 Configuration pour le centre de télésurveillance

5. Commande à distance

5.1 Ajout du FireCom dans Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Configuration et commande par SMS
5.3 Commande des sorties PGM par appel téléphonique

6. Les pages de TrikdisConfig

6.1 La barre d'état
6.2 Page « System Options »
6.3 Page « Reporting to CMS »
6.4 Page « Users & Reporting »
6.5 Page « Modules »
6.6 Page « Zones »
6.7 Page « PGM »
6.8 Page « Sensors »

6.9 Page « System events »
6.10 Page « Events Log »
6.11 Retour aux réglages d'usine
7. Programmation à distance
8. Vérification du fonctionnement
9. Mise à jour du firmware
10. Dépannage et questions fréquentes
11. Consignes de sécurité
Voir aussi

1. Présentation

Le Trikdis FireCom est un communicateur incendie certifié EN 54, avec connexion Ethernet et réseau mobile 4G (deux cartes SIM).

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

Certification	Donnée
Norme	Le FireCom satisfait aux exigences des normes **EN 54-21:2006** et **EN 54-4:1997/AC:1999/A1:2002/A2:2006**, 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-2083** – Systèmes de détection et d'alarme incendie. Équipement de transmission d'alarme et de signalisation de dérangement. Équipement d'alimentation électrique.
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 reliées aux entrées du FireCom (point 3.4).
- Sur le bus RS485 2 : avec les centrales incendie utilisant le protocole **ESPA 4.4.4**, ainsi que les centrales **NSC Solution**, **INIM Smartline**, **C-TEC Cast ZFP** et **Polon-Alfa 3000** (points 3.5–3.9) ; la Polon-Alfa 3000 peut aussi se raccorder via le réseau local (LAN).
- Conformément à l'EN 54, deux sorties relais signalent à la centrale le défaut de la liaison avec le centre de télésurveillance et la bonne réception du message (point 3.12).

Messages vers le centre de télésurveillance

- Il envoie les événements via le module LAN intégré ou le modem mobile 4G.
- Il envoie les événements sur les canaux de communication disponibles, dans l'ordre configuré.
- Tout centre de télésurveillance peut recevoir ses messages s'il dispose d'un récepteur logiciel ou IP Trikdis, ou d'un récepteur IP d'un autre fabricant prenant en charge le protocole IP SIA DC-09.
- La transmission vers le centre de télésurveillance peut être prioritaire : les messages vont d'abord au centre de télésurveillance, et seulement ensuite à Protegus 2.
- Il peut aussi envoyer les événements aux récepteurs de deux sociétés de télésurveillance différentes.
- Il envoie les messages d'événement avec des codes Contact ID ou SIA.

Messages vers les utilisateurs

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

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) pour la configuration : installateur et administrateur.

Entrées et sorties

- 3 sorties relais (1 A, 30 V DC).
- L'entrée **FLOOP** sert au raccordement de détecteurs incendie deux fils.
- 10 bornes I/O, chacune configurable en entrée (IN) ou en sortie (OUT). Types possibles en entrée : NC, NO, EOL, EOL_T, ATZ, ATZ_T. Dans les circuits EOL et ATZ, des résistances de différentes valeurs peuvent être utilisées.
- Avec les modules d'extension iO, le nombre d'entrées (IN) peut être porté à 32 et celui des sorties (OUT) à 16.
- Les modules d'extension de la série iO se raccordent au bus **RS485** (**A1**, **B1**).
- La centrale incendie se raccorde au bus **RS485 2** (**A2**, **B2**).

1.2 Caractéristiques techniques

Caractéristique	Valeur
Bandes du modem LTE	EU (Europe) : LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 ; LA (Amérique latine) : LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Tension d'alimentation	15–32 V DC, 2,5 A
Consommation	en veille 50 mA au maximum ; en transmission 300 mA au maximum ; avec la charge maximale possible des appareils externes, 2,5 A au maximum
Source d'alimentation de secours [BAT]	batterie au plomb 12 V, 4 Ah / 7 Ah
Courant de charge de la batterie	500 mA au maximum
Tension et courant pour les appareils externes [AUX]	12 V DC, 1 A au maximum
Protocole de transmission	TRK, SIA DC-09_2007, SIA DC-09_2012, SIA DC-09_IPcom, TL150
Clé de chiffrement	6 caractères
Liaison avec le centre de télésurveillance	TCP/IP ou UDP/IP
Codes d'événement	Contact ID, SIA

Caractéristique	Valeur
Module LAN	oui, intégré
Configuration du réseau LAN	DHCP ou manuelle
Carte SIM	2, format nano
Destinations des messages	récepteurs principal et de secours de deux sociétés de télésurveillance différentes ; cloud Protegus 2, application Protegus 2 iOS et Android ; SMS vers 8 téléphones mobiles ; appel de 8 téléphones mobiles
Canaux d'envoi des événements	4G, Ethernet (LAN), SMS, appel
Chiffrement des messages	oui
Horloge interne	oui
Utilisateurs	40
Bornes à double fonction [I/O]	10 ; la fonction IN ou OUT se choisit lors de la programmation. En IN, types possibles : NC, NO, EOL, EOL_T, ATZ, ATZ_T. En OUT, la borne est à collecteur ouvert (OC), 100 mA au maximum
Nombre de groupes	8
Nombre de zones	10 (20 avec ATZ) ; extensible à 32 avec des modules d'extension
Nombre de sorties PGM	3 à relais (1 A, 30 V DC) ; 13 si vous configurez les bornes I/O en sorties ; extensible à 16 avec des modules d'extension
Mémoire de messages	60 événements
Journal des événements	1000 événements au maximum ; les entrées les plus anciennes sont effacées automatiquement
Configuration	à distance avec le logiciel TrikdisConfig ou sur place avec un câble USB Type-C
Longueur du bus de données 1-Wire [1 WIRE]	30 m au maximum
Capteurs de température compatibles	Maxim® / Dallas® DS18S20, DS18B20 ; série AM2301
Nombre de capteurs de température raccordables au bus de données 1-Wire	8 (Dallas), ou 1 si vous utilisez un capteur de la série AM2301
Bus RS485	2
Longueur du bus RS485	100 m au maximum
Modules pris en charge	module d'extension **iO-8** ; **iO-MO** – émetteur-récepteur radio iO-WL ; module d'extension **iO-LORA** ; module d'extension **iO8-LORA** ; bouton panique **PB-LORA** ; module d'extension **REL-LORA** ; centrale incendie utilisant le protocole **ESPA 4.4.4** ; centrales incendie **NSC Solution**, **INIM Smartline**, **C-TEC Cast ZFP** et **Polon-Alfa 3000**
Environnement de fonctionnement	–10 … +50 °C, humidité relative de 80 % au maximum à +20 °C
Dimensions	235 × 205 × 92 mm
Poids	1,35 kg

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.

Trikdis FireCom Ethernet + 4G transmetteur d'alarme incendie

1.3 Éléments du communicateur

Les numéros de la figure désignent les éléments du circuit imprimé du FireCom. La carte se trouve, avec le bloc d'alimentation, dans un coffret de montage métallique (chapitre 3).

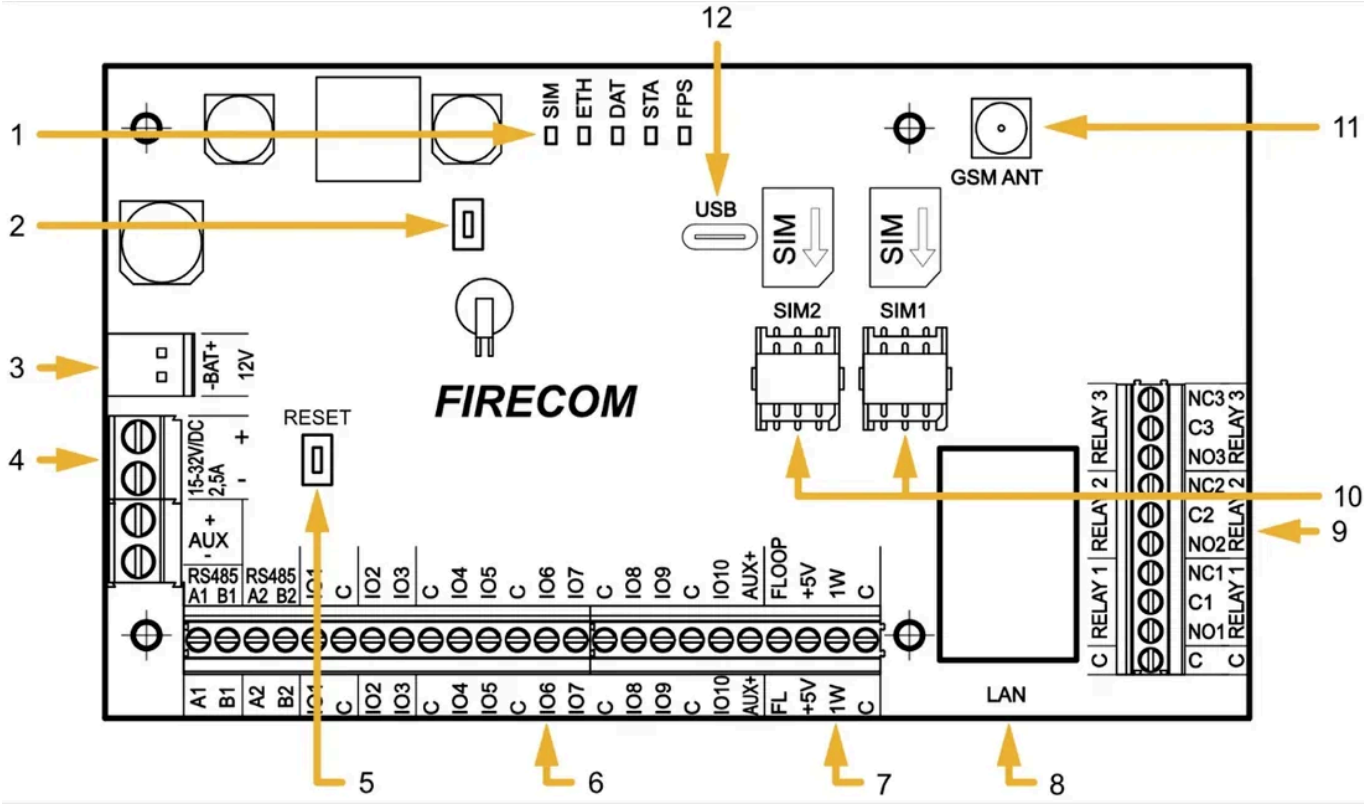


Figure 1. Le circuit imprimé du FireCom.

- 1 les voyants de liaison et de fonctionnement (LED)
- 2 bouton-poussoir – non utilisé
- 3 le bornier de l'alimentation de secours
- 4 le bornier de l'alimentation principale
- 5 bouton RESET
- 6 bornier externe
- 7 le bornier 1-Wire
- 8 connecteur LAN
- 9 le bornier des sorties relais
- 10 supports de carte SIM
- 11 le connecteur de l'antenne réseau mobile (GSM)
- 12 connecteur USB Type-C

1.4 Les bornes

Les noms des bornes sont imprimés sur le circuit imprimé, à côté des borniers.

Borne	Fonction
+ (borne d'alimentation)	borne positive de la tension d'alimentation (15–32 V DC)
– (borne d'alimentation)	borne négative de la tension d'alimentation (15–32 V DC)
BAT+	borne positive de l'alimentation de secours (12 V)
BAT–	borne négative de l'alimentation de secours (12 V)
AUX+	borne d'alimentation positive 12 V pour les appareils externes
AUX–	borne négative commune
A1, **B1** (RS485)	bus RS485 pour le raccordement des modules d'extension iO
A2, **B2** (RS485)	bus RS485 pour le raccordement de la centrale incendie
IO1–IO10	bornes d'entrée et de sortie (en entrée par défaut)
C	borne négative commune
AUX+	borne d'alimentation positive 12 V pour les appareils externes
FLOOP	borne de raccordement d'un détecteur incendie deux fils
+5V	borne d'alimentation positive 5 V, 0,2 A pour les appareils 1-Wire
1W (1 WIRE)	borne du bus de données 1-Wire
C	borne négative commune
NO1 / C1 / NC1	bornes de la sortie relais PGM 1
NO2 / C2 / NC2	bornes de la sortie relais PGM 2
NO3 / C3 / NC3	bornes de la sortie relais PGM 3

1.5 Voyants

Le circuit imprimé comporte cinq voyants (**SIM**, **ETH**, **DAT**, **STA**, **FPS**), la face avant du boîtier en comporte trois (**POWER**, **DATA**, **TROUBLE**). Le tableau décrit ensemble les paires **DAT / DATA**, **STA / TROUBLE** et **FPS / POWER** ; lorsque la signalisation ne concerne que l'un des deux, son nom est indiqué entre parenthèses.

Voyant	Lumière	Signification
SIM	éteint	non connecté au réseau mobile
	clignotement vert	la carte SIM s'enregistre sur le réseau mobile
	vert fixe	la carte SIM est enregistrée sur le réseau mobile
	vert fixe et clignotement jaune	connecté au réseau mobile ; sur le réseau 4G, 3 clignotements jaunes indiquent déjà un niveau de signal suffisant
ETH	clignotement vert	le câble LAN n'est pas branché, ou il y a une erreur DHCP
	vert fixe	connecté au réseau local (LAN)
DAT / DATA	éteint	tous les messages d'événement ont été envoyés
	vert fixe	envoi de message en cours
	jaune fixe (DAT)	des messages d'événement non envoyés se trouvent en mémoire

Voyant	Lumière	Signification
STA / TROUBLE	vert fixe (STA)	pendant la mise sous tension : le communicateur démarre
	clignotement vert (STA)	après le démarrage : aucun défaut de fonctionnement
	éteint (TROUBLE)	aucun défaut de fonctionnement
	1 clignotement rouge	aucune carte SIM insérée
	2 clignotements rouges	le code PIN de la carte SIM est erroné
	3 clignotements rouges	impossible de se connecter au réseau mobile
	4 clignotements rouges	impossible de se connecter au récepteur IP sur le canal principal
	5 clignotements rouges	impossible de se connecter au récepteur IP sur le canal de secours
	6 clignotements rouges	pas de tension d'alimentation DC
	7 clignotements rouges	défaut de la sortie AUX (surintensité ou surtension)
	8 clignotements rouges	défaut batterie
	9 clignotements rouges	le câble LAN n'est pas branché
	10 clignotements rouges	erreur DHCP sur le réseau local (LAN)
FPS / POWER	éteint	l'alimentation n'est pas raccordée
	vert fixe	l'alimentation ne présente aucun problème
	1 clignotement vert	pas de tension secteur (AC)
	2 clignotements verts	la tension de l'alimentation de secours est insuffisante

La signalisation correcte après la mise sous tension et l'évaluation du niveau de signal sont décrites au point 3.14.

1.6 Outillage nécessaire à l'installation

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

1. câble USB Type-C pour la configuration ;
2. câble d'au moins 4 conducteurs pour relier le communicateur et la centrale incendie ;
3. tournevis plat de 2,5 mm ;
4. antenne réseau mobile externe, 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 communicateur.

Les accessoires énumérés sont à acheter séparément – commandez-les auprès de votre revendeur. Si le signal est faible sur le site, utilisez une antenne filaire déportable :

Antenne magnétique Trikdis ME301m avec fil 2,5 m

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

2. Alimentation

2.1 Alimentation principale

Le communicateur doit être alimenté par une source de courant continu (DC). Pour une alimentation sans coupure, une source d'alimentation de secours – une batterie 12 V – doit être raccordée au système. Comme source d'alimentation de secours, une batterie au plomb 12 V de 4 Ah ou 7 Ah convient (point 1.2) ; son choix est abordé dans la remarque du point 3.1.

Batterie gel 12 V 7 Ah pour centrale d'alarme

2.2 Alimentation de secours

En cas de problème sur l'alimentation principale, le communicateur envoie un message d'événement **DC Fault** (défaut DC) et passe automatiquement sur la batterie de secours 12 V. Lorsque la tension de la batterie descend à 11,5 V, un message d'événement **Low Battery** (tension de batterie basse) est généré. Si la tension passe sous 9,5 V, la batterie est déconnectée. Au retour de la tension d'alimentation DC, un message **DC Restore** (DC rétabli) est généré et la charge de la batterie démarre automatiquement. Lorsque la tension de la batterie atteint 12,6 V, un message d'événement **Battery Restore** (batterie rétablie) est généré.

2.3 Contenu de la livraison

Désignation	Quantité
Carte du communicateur FireCom avec antenne, montée dans un boîtier métallique	1 pièce
Boîtier métallique avec bloc d'alimentation à découpage (à impulsions) Mean Well	1 pièce
Résistance de 10 kΩ	20 pièces
Fil de raccordement de la batterie	1 pièce
Contact d'autoprotection (tamper)	1 pièce
Bornier avec fusible 3,15 A	1 pièce
Éléments de fixation (4 vis, 4 chevilles en nylon)	1 jeu

Le câble USB (Type-C) nécessaire à la programmation du communicateur est à acheter séparément.

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.

Le circuit imprimé du communicateur se place dans un coffret de montage dans lequel le bloc d'alimentation DC avec fusible 3,15 A est déjà installé et qui offre aussi de la place pour la batterie de secours. Ce chapitre décrit l'ordre de raccordement, le raccordement des détecteurs, des détecteurs de fumée et des centrales incendie (sorties de la centrale, ou sur le bus RS485 2 les centrales utilisant le protocole ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP et Polon-Alfa 3000), les capteurs de température, le relais et l'indicateur à LED, les entrées de la centrale, les modules d'extension iO et, pour finir, la mise sous tension du communicateur.

Dimensions de la carte FireCom

La figure montre les dimensions de la carte et des trous de fixation (en millimètres), ainsi que l'emplacement des trous.

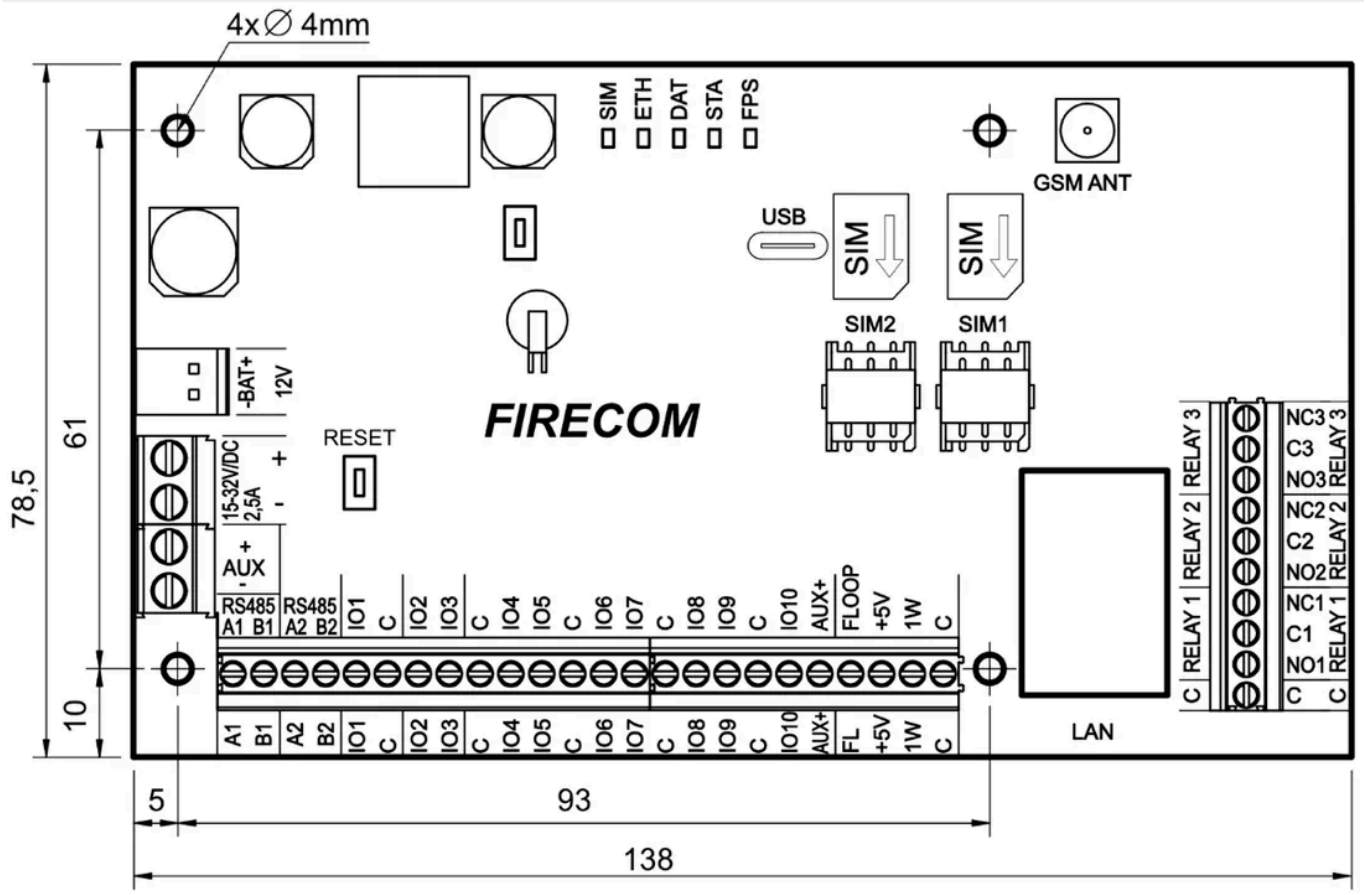


Figure 2. Dimensions de la carte FireCom (mm) : la carte mesure 138 × 78,5 mm ; les quatre trous de fixation de Ø 4 mm sont espacés de 93 mm à l'horizontale et de 61 mm à la verticale, le trou inférieur gauche se trouve à 5 mm du bord gauche et à 10 mm du bord inférieur.

3.1 Ordre de raccordement

Les numéros de la figure correspondent aux numéros des étapes ci-dessous.

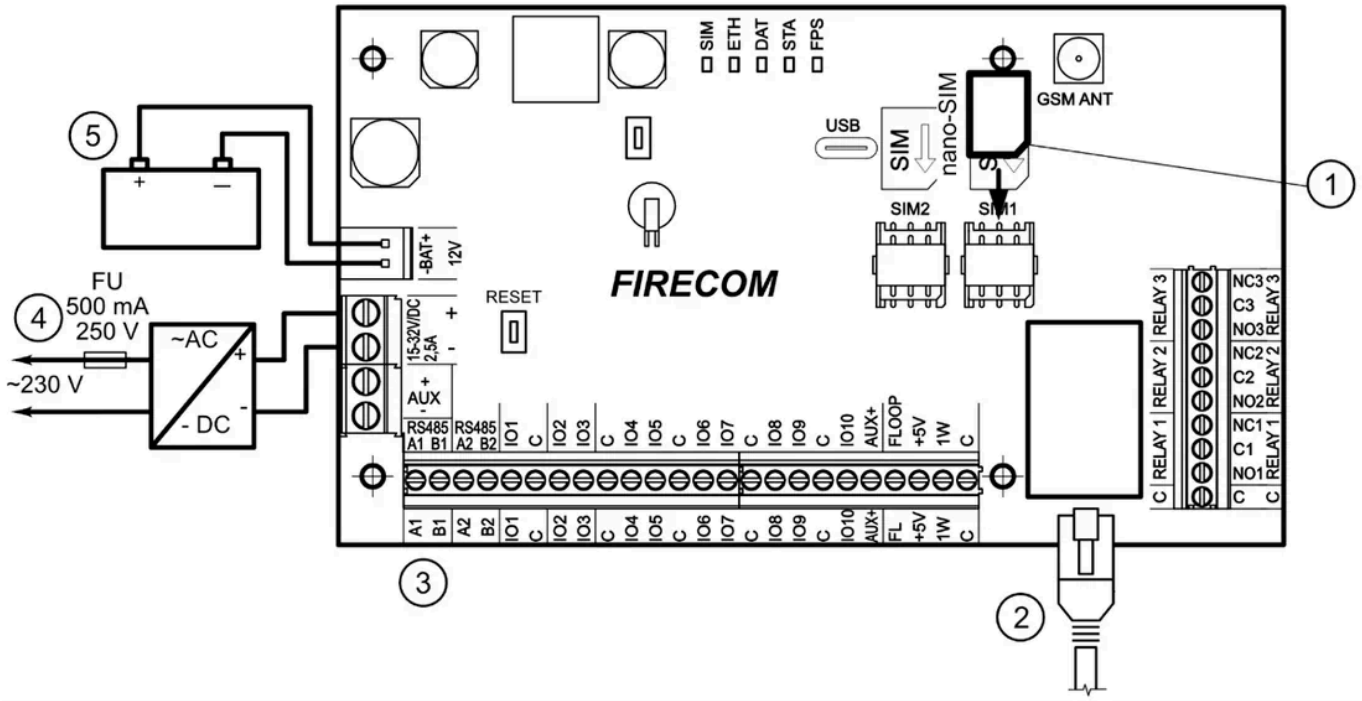


Figure 3. Ordre de raccordement : ① la carte SIM (**nano-SIM**) dans le support **SIM1** ; ② câble LAN (« LAN cable ») ; ③ le bornier ; ④ l'alimentation secteur **~230 V** via le fusible **FU 500 mA 250 V** vers le bloc d'alimentation DC (« DC power supply », 15–32 V, 1,5 A), dont les sorties + et − vont aux bornes + et − de la carte ; ⑤ batterie (« Battery », 12 V, 7 Ah) sur les bornes de batterie, avec la polarité indiquée sur le schéma.

1. Si vous utilisez une carte SIM, insérez la carte SIM activée dans le support de carte SIM.
2. Si vous utilisez le réseau local (LAN), branchez le câble LAN.
3. Raccordez les détecteurs incendie, les indicateurs et les appareils commandés selon les schémas de raccordement fournis et le schéma de raccordement propre à chaque appareil à raccorder.
4. Raccordez les fils d'alimentation secteur (AC) aux bornes.
5. Placez la batterie de secours dans le coffret de montage. Raccordez les pôles de la batterie aux bornes **BAT+** / **BAT−** du communicateur.

Selon les exigences de la norme EN 54, la batterie doit se recharger à 80 % de sa capacité en 24 heures et atteindre le reste au cours des 48 heures suivantes – choisissez une batterie en conséquence.

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

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

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

3.2 Raccordement des détecteurs

Sur la carte du communicateur, 10 bornes (**IO1–IO10**, entrées) servent au raccordement des boucles de détection. Le nombre d'entrées peut être porté à 32 avec des modules d'extension d'entrées (**iO-8**, **iO-MO**, **iO-LORA**, **iO8-LORA**). Chaque borne peut être configurée en entrée et recevoir des propriétés de zone : le type de circuit (NO, NC, EOL, EOL_T, ATZ, ATZ_T) et la sensibilité aux événements transitoires du circuit (point 6.6, page **Zones**).

Voici les schémas de raccordement des détecteurs. Valeurs possibles des résistances (**RT** – autoprotection, **R1** – détecteur 1, **R2** – détecteur 2) :

RT	R1	R2
2,2 kΩ	2,2 kΩ	4,7 kΩ
1 kΩ	1 kΩ	2,2 kΩ
5,6 kΩ	5,6 kΩ	3,3 kΩ
5,6 kΩ	3,3 kΩ	5,6 kΩ
3,3 kΩ	6,8 kΩ	3,3 kΩ
2,2 kΩ	4,7 kΩ	8,2 kΩ
10 kΩ	10 kΩ	5,6 kΩ

Vous indiquez les valeurs utilisées dans le champ **EOL Type** de la page **System Options** (point 6.2).

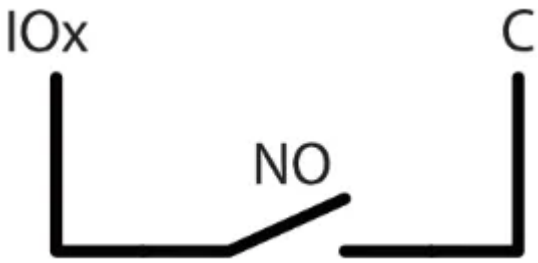


Figure 4. NO – contact normalement ouvert entre l'entrée **IOx** et la borne commune **C**, sans résistance.

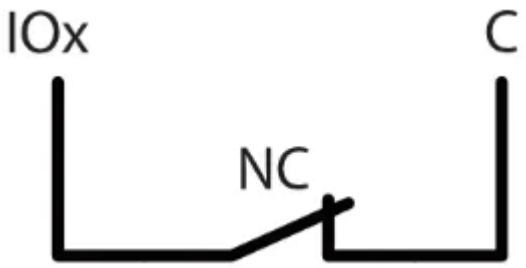


Figure 5. NC – contact normalement fermé entre **IOx** et **C**, sans résistance.

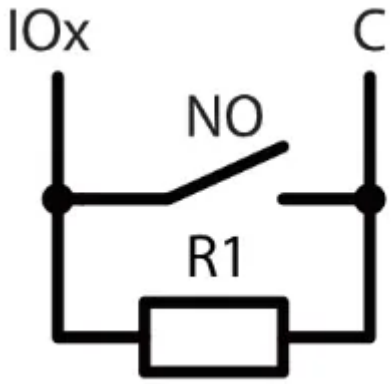


Figure 6. EOL – contact NO avec résistance de fin de ligne : le contact et la résistance **R1** en parallèle entre **IOx** et **C**.

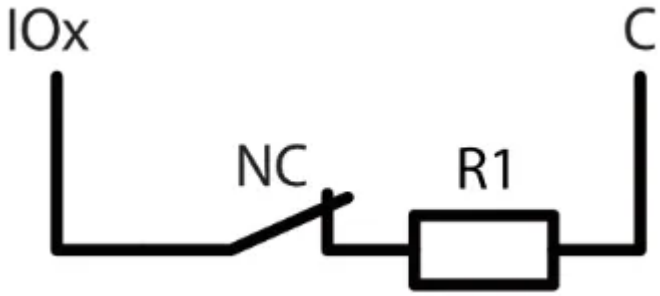


Figure 7. EOL – contact NC avec résistance de fin de ligne : le contact et la résistance **R1** en série.

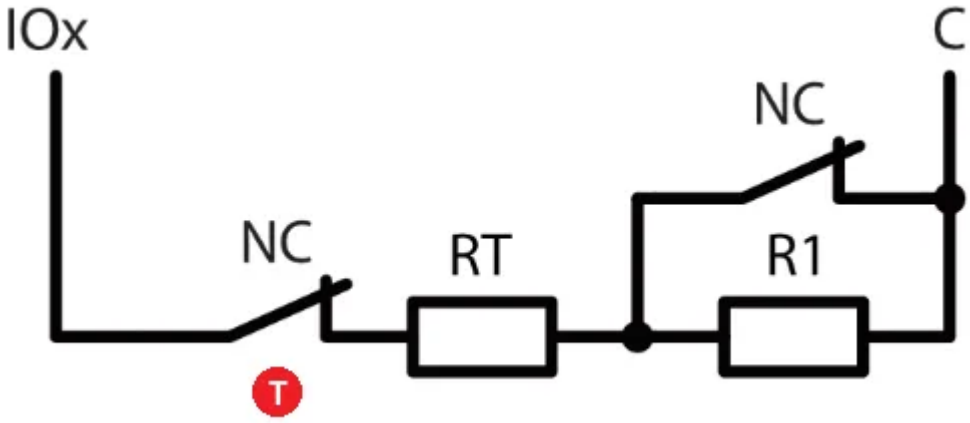


Figure 8. EOL_T – contact NC avec résistance de fin de ligne, avec détection d'autoprotection et de défaut de câblage : depuis **IOx**, le contact d'autoprotection NC et **RT** en série, puis **R1** en parallèle avec le second contact NC, vers **C**.

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

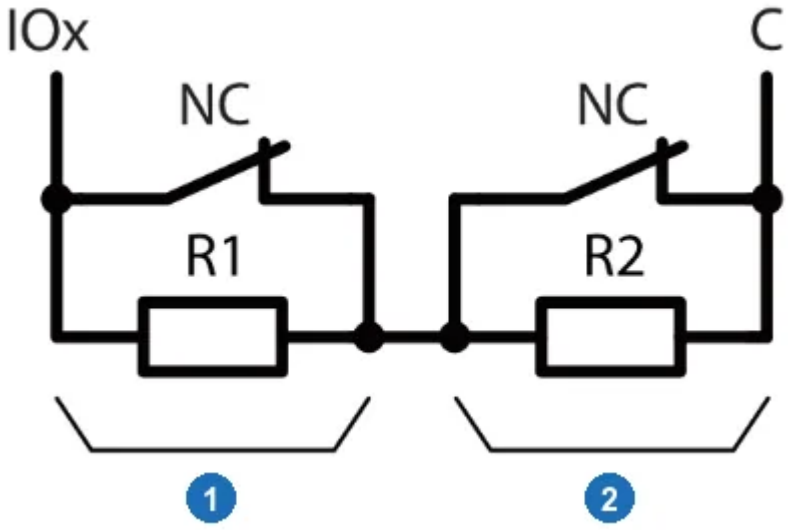


Figure 9. ATZ – deux détecteurs sur une entrée, avec contacts NC, sans surveillance d'autoprotection : le contact NC du détecteur 1 en parallèle avec **R1**, celui du détecteur 2 avec **R2** ; les deux circuits en série entre **IOx** et **C**.

- 1 le circuit du détecteur 1 (« Detector terminal 1 »)
- 2 le circuit du détecteur 2 (« Detector terminal 2 »)

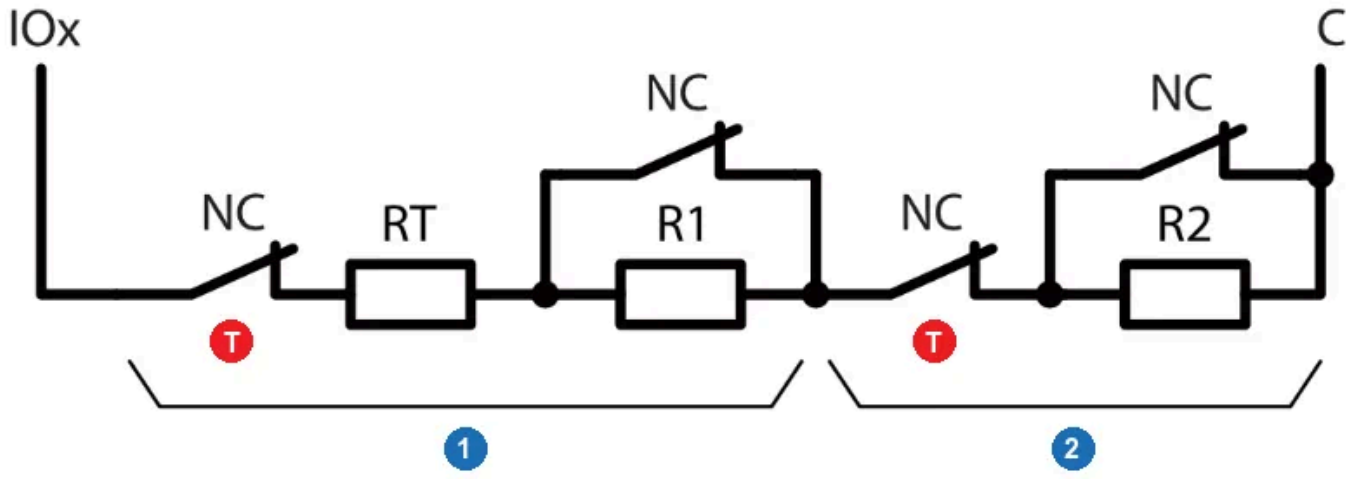


Figure 10. ATZ_T – deux détecteurs sur une entrée, avec contacts NC, fin de ligne, détection d'autoprotection et de défaut de câblage : pour le détecteur 1, le contact d'autoprotection NC et **RT** en série, puis le contact NC en parallèle avec **R1** ; pour le détecteur 2, le contact d'autoprotection NC en série, puis le contact NC en parallèle avec **R2**.

- T contact d'autoprotection (« Tamper »), il signale l'ouverture du capot du détecteur
- 1 le circuit du détecteur 1 (« Detector terminal 1 »)
- 2 le circuit du détecteur 2 (« Detector terminal 2 »)

3.3 Raccordement des détecteurs de fumée

Détecteurs de fumée deux fils sur la borne FLOOP

Si vous utilisez ce raccordement, sélectionnez sur la page **Zones** l'entrée **FC Fire sensor (FLOOP input)** comme entrée (**Input**) de la zone (point 6.6). Le courant d'alarme du détecteur incendie doit être supérieur à 10 mA. 8 détecteurs incendie au maximum peuvent être raccordés à la borne **FLOOP**.

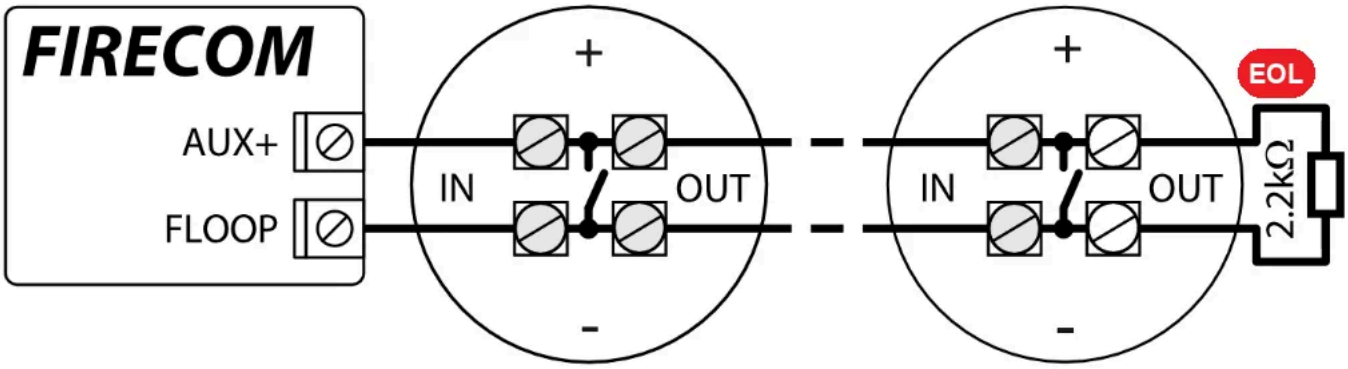


Figure 11. Détecteurs de fumée deux fils sur la borne **FLOOP** : **AUX+** va à la borne **+ IN** du premier détecteur, **FLOOP** à sa borne **– IN** ; les bornes **+ OUT** et **– OUT** de chaque détecteur vont à l'entrée du détecteur suivant ; une résistance de fin de ligne de 2,2 kΩ se place entre les bornes **+ OUT** et **– OUT** du dernier détecteur.

- EOL résistance de fin de ligne de 2,2 kΩ (« End of line resistor »)

Détecteurs de fumée deux fils avec module relais SM1

Si vous raccordez la boucle de détecteurs de fumée à une entrée choisie, l'entrée (**IOx**) doit être activée et le type de circuit doit être réglé (NO, NC, EOL, EOL_T, ATZ, ATZ_T ; point 6.6, page **Zones**). Si vous raccordez le circuit d'alimentation des détecteurs de fumée à la sortie PGM (**IO10**), attribuez la fonction **Fire Sensor Reset** à la sortie (point 6.7, page **PGM**).

Le relais **K1** sert à détecter la coupure du câble et le retrait du détecteur incendie. Si vous n'utilisez pas de relais (**K1**), le contact **K1** doit être court-circuité.

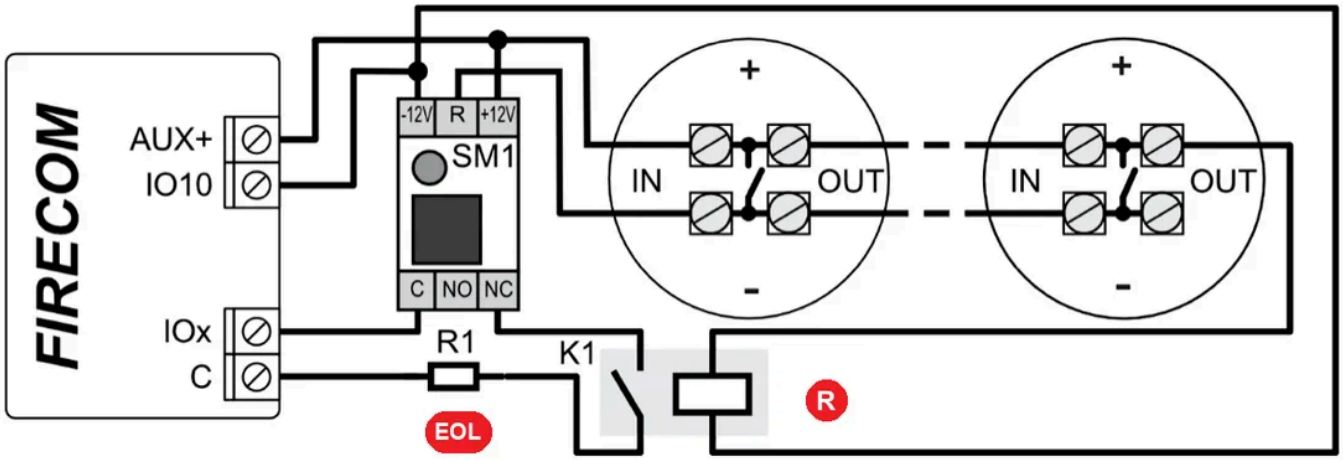


Figure 12. Détecteurs de fumée deux fils avec module relais **SM1** et relais **K1**, avec le contact **NC** du SM1. Alimentation : **AUX+** va aux bornes **+12V** du SM1 et **+ IN** du premier détecteur, **IO10** va à la borne **–12V** du SM1 et à une extrémité de la bobine de K1 ; la borne **R** du SM1 va à la borne **– IN** du premier détecteur ; les deux fils **OUT** continuent vers le second détecteur, dont la borne **+ OUT** va à l'autre extrémité de la bobine de K1, aucun fil ne repart de sa borne **– OUT**. Entrée surveillée : **IOx** va à la borne **C** du SM1, la borne **NC** du SM1 va à la borne **C** du FireCom via le contact de K1 et la résistance de fin de ligne **R1** (en série).

- R relais **K1** (« Relay ») – son rôle est décrit dans la remarque ci-dessus
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

Ou :

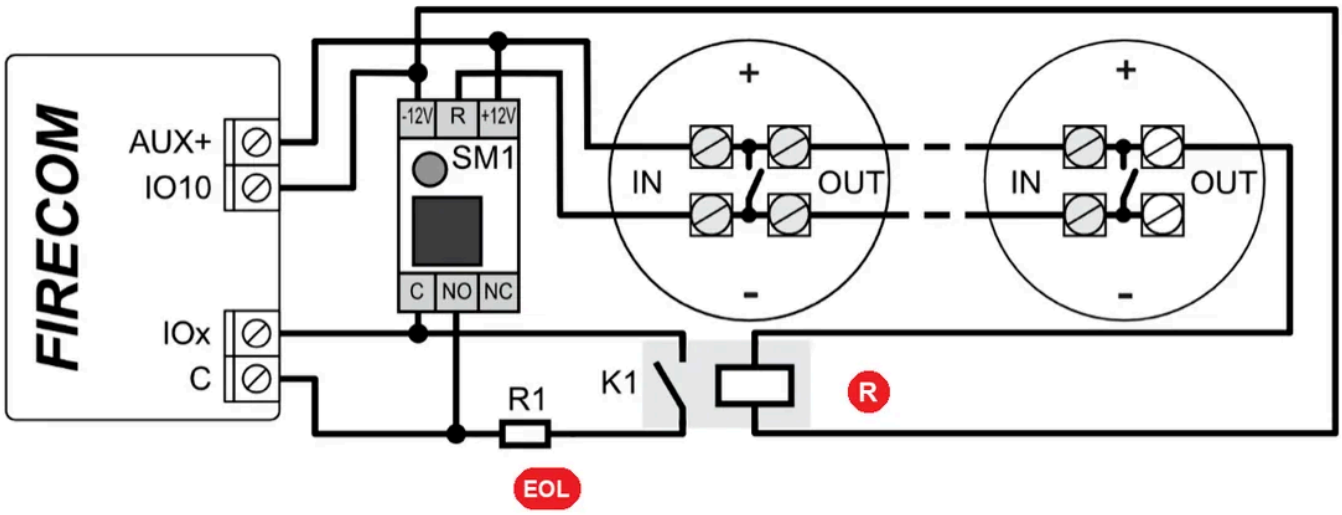


Figure 13. Le même raccordement avec le contact **NO** du SM1 : **IOx** va à la borne **C** du SM1, la borne **NO** du SM1 va à la borne **C** du FireCom ; la branche série formée du contact de K1 et de la résistance de fin de ligne **R1** se trouve entre **IOx** et **C**.

- R relais **K1** (« Relay ») – son rôle est décrit dans la remarque ci-dessus
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

Détecteurs de fumée quatre fils

Si vous raccordez la boucle de détecteurs de fumée à une entrée choisie, l'entrée (**IOx**) doit être activée et le type de circuit doit être réglé (NO, NC, EOL, EOL_T, ATZ, ATZ_T ; point 6.6, page **Zones**). Si vous raccordez le circuit d'alimentation des détecteurs de fumée quatre fils à la sortie PGM (**IO10**), attribuez la fonction **Fire Sensor Reset** à la sortie (point 6.7, page **PGM**).

Ici aussi, le relais **K1** sert à détecter la coupure du câble et le retrait du détecteur incendie. Si vous n'utilisez pas de relais (**K1**), le contact **K1** doit être court-circuité.

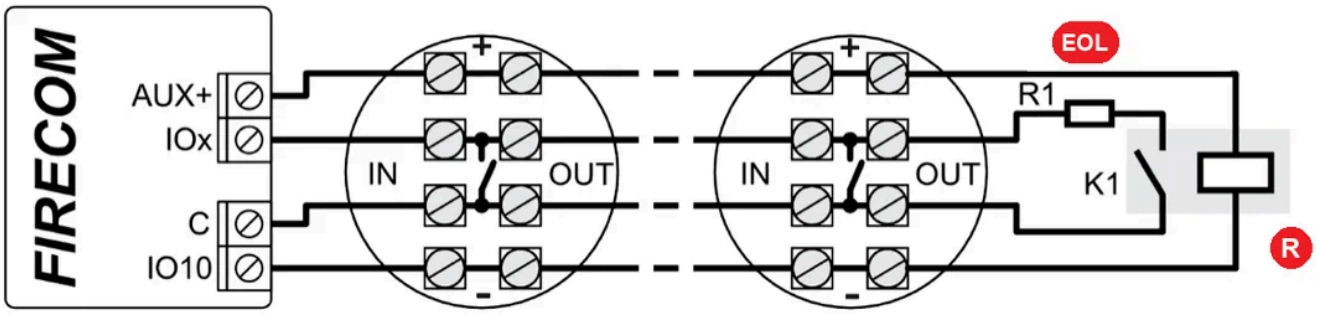


Figure 14. Détecteurs de fumée quatre fils et relais **K1**. Alimentation : **AUX+** va à la borne **+ IN** du premier détecteur, **IO10** à sa borne **– IN** ; les bornes **OUT** vont au second détecteur, entre les bornes **+ OUT** et **– OUT** duquel se place la bobine de K1. Boucle d'alarme : **IOx** et **C** vont à l'entrée du contact du premier détecteur et continuent vers le second détecteur ; le contact de chaque détecteur ponte la paire d'alarme ; entre la dernière paire **OUT** se place la branche série formée de la résistance de fin de ligne **R1** et du contact de K1.

- R relais **K1** (« Relay ») – son rôle est décrit dans la remarque ci-dessus
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

3.4 Raccordement aux sorties de la centrale incendie

Si vous voulez surveiller l'état de la centrale incendie, raccordez les sorties correspondantes de la centrale aux entrées du FireCom. Les sorties de la centrale (**PGM1**, **PGM2**, **PGM3**) doivent être configurées dans la centrale comme sorties d'état (alarme, défaut, etc.). Le schéma existe en deux variantes : lorsque le FireCom

est alimenté par le 24 V de la centrale (sans bloc d'alimentation intégré), et lorsqu'il fonctionne sur son propre bloc d'alimentation intégré.

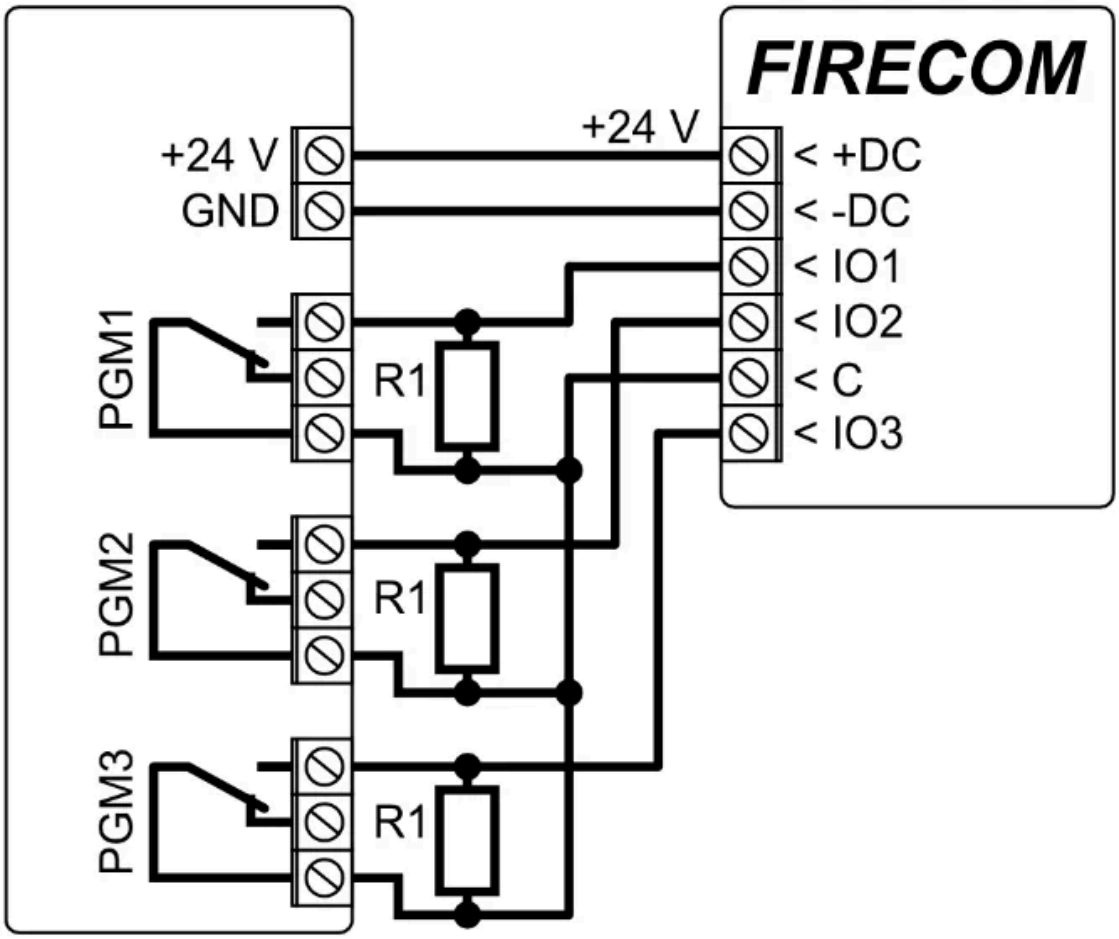


Figure 15. Raccordement aux sorties de la centrale incendie (**Fire control panel**), sans bloc d'alimentation intégré : la borne **+24 V** de la centrale va à la borne **+DC** du FireCom, **GND** à la borne **–DC** ; une borne des sorties **PGM1**, **PGM2** et **PGM3** va respectivement aux entrées **IO1**, **IO2** et **IO3**, l'autre à la borne commune **C** ; une résistance **R1** se place en parallèle entre les deux bornes de chaque sortie (valeurs : point 3.2) ; la borne centrale des sorties PGM n'est pas raccordée.

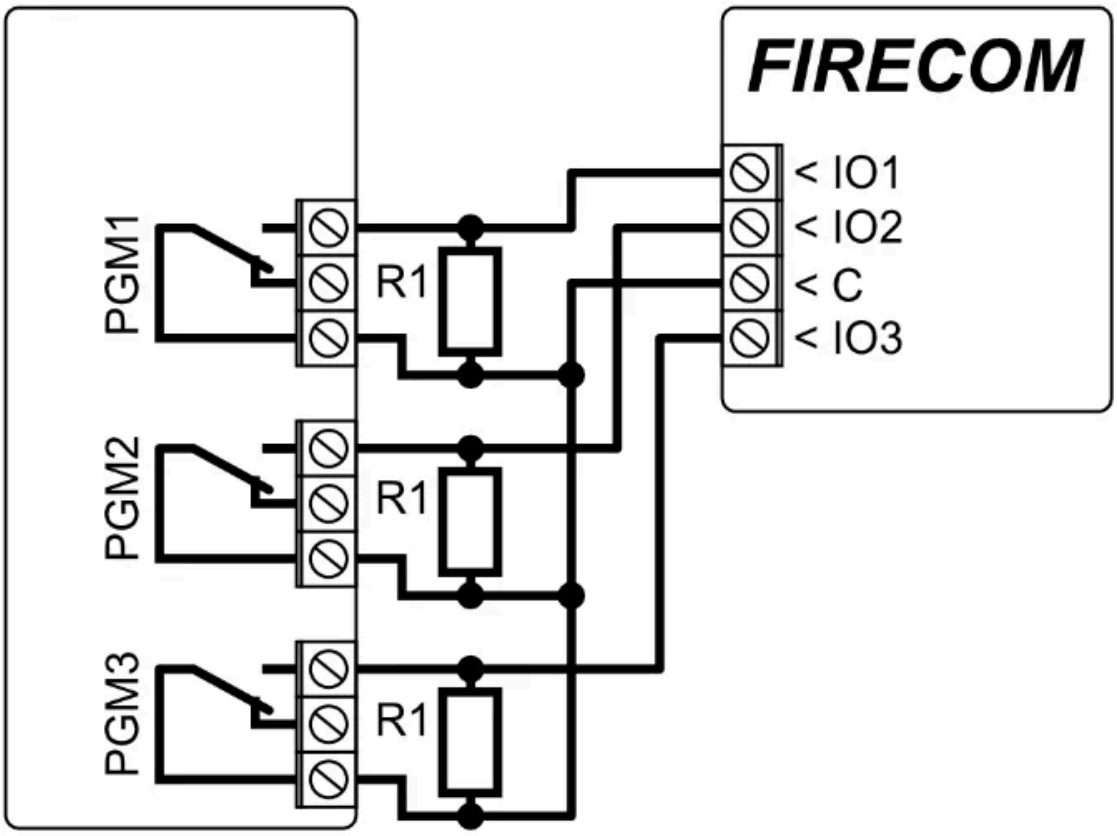


Figure 16. Le même raccordement avec bloc d'alimentation intégré : l'alimentation n'est pas prise sur la centrale ; les sorties **PGM1–PGM3** vont de la même façon aux entrées **IO1–IO3** et à la borne **C**, avec une résistance **R1** en parallèle ; ici non plus, les bornes centrales ne sont pas raccordées.

3.5 Centrale incendie utilisant le protocole ESPA 4.4.4

Raccordez la centrale incendie utilisant le protocole ESPA 4.4.4 au FireCom sur le bus RS485 2 (**A2**, **B2**), selon les schémas ci-dessous.

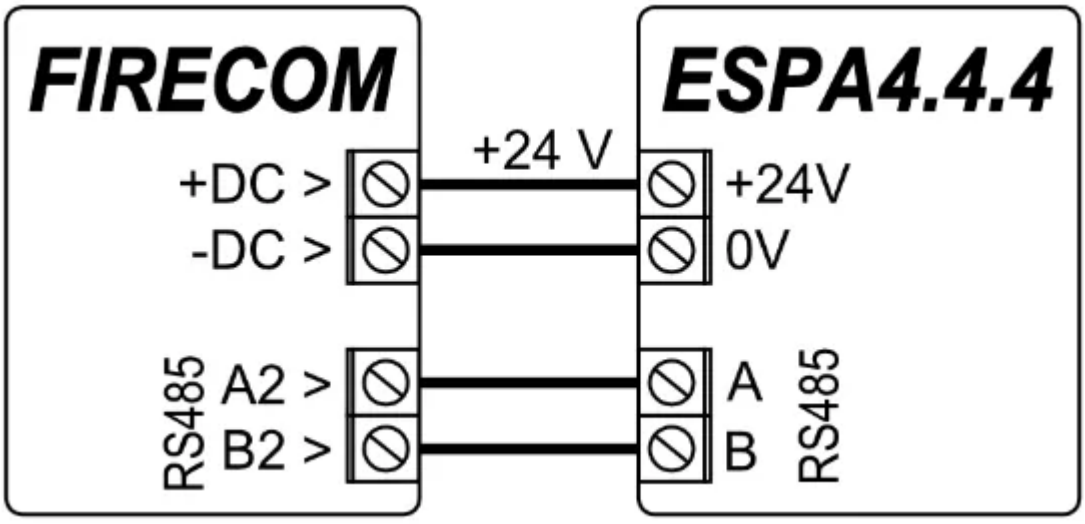


Figure 17. Raccordement de la centrale utilisant le protocole ESPA 4.4.4 (**ESPA4.4.4**) sans bloc d'alimentation intégré : la borne **+24V** de la centrale va à la borne **+DC** du FireCom, **0V** à la borne **–DC** ; RS485 – la borne **A** de la centrale va à **A2**, **B** à **B2**.

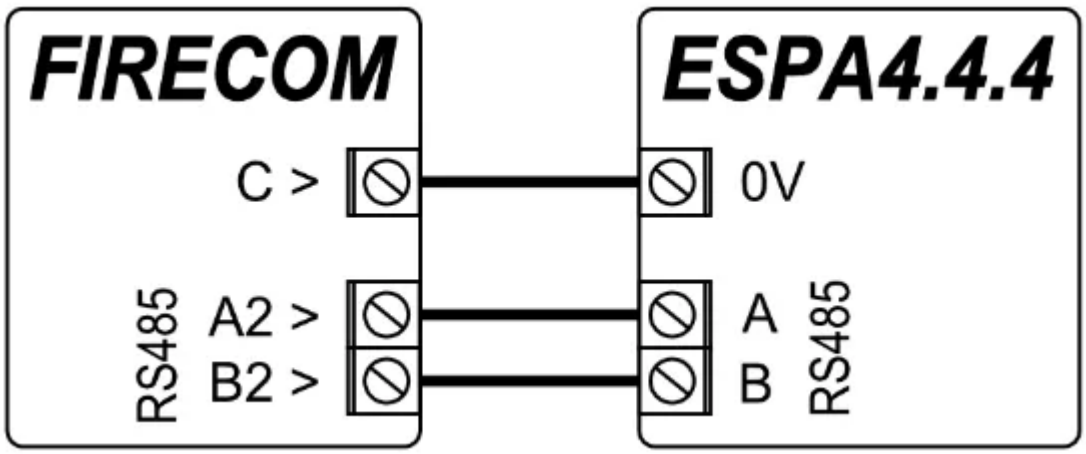


Figure 18. Le même raccordement avec bloc d'alimentation intégré : la borne **0V** de la centrale va à la borne **C** du FireCom ; RS485 – **A** à **A2**, **B** à **B2**.

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

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez le protocole **ESPA 4.4.4**.
2. Sélectionnez le type de liaison (**Connection**).
3. Les paramètres de transmission de données du FireCom et de la centrale incendie doivent être identiques.

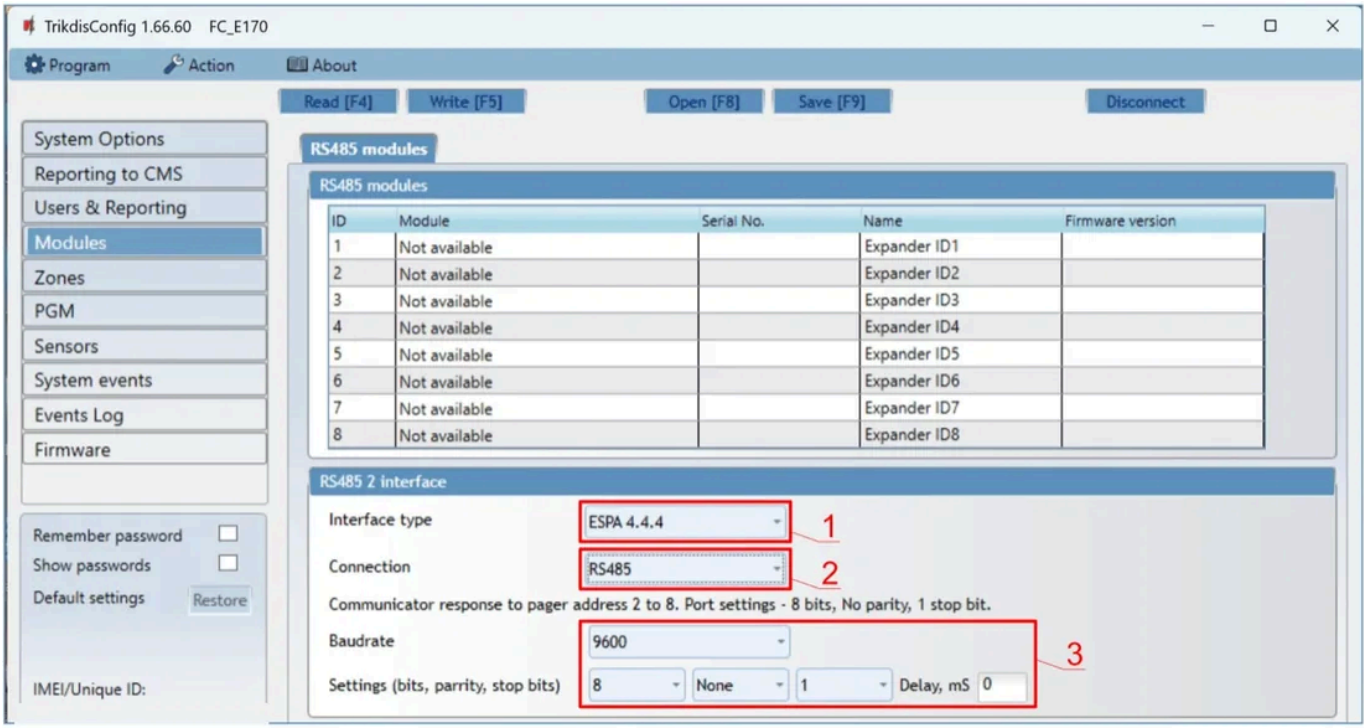


Figure 19. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **ESPA 4.4.4**
- 2 **Connection** – le type de liaison (sur l'image : **RS485**)
- 3 paramètres de transmission de données (sur l'image : **Baudrate** 9600, 8 bits de données, parité **None**, 1 bit d'arrêt, **Delay** 0 ms)

4. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).

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**.

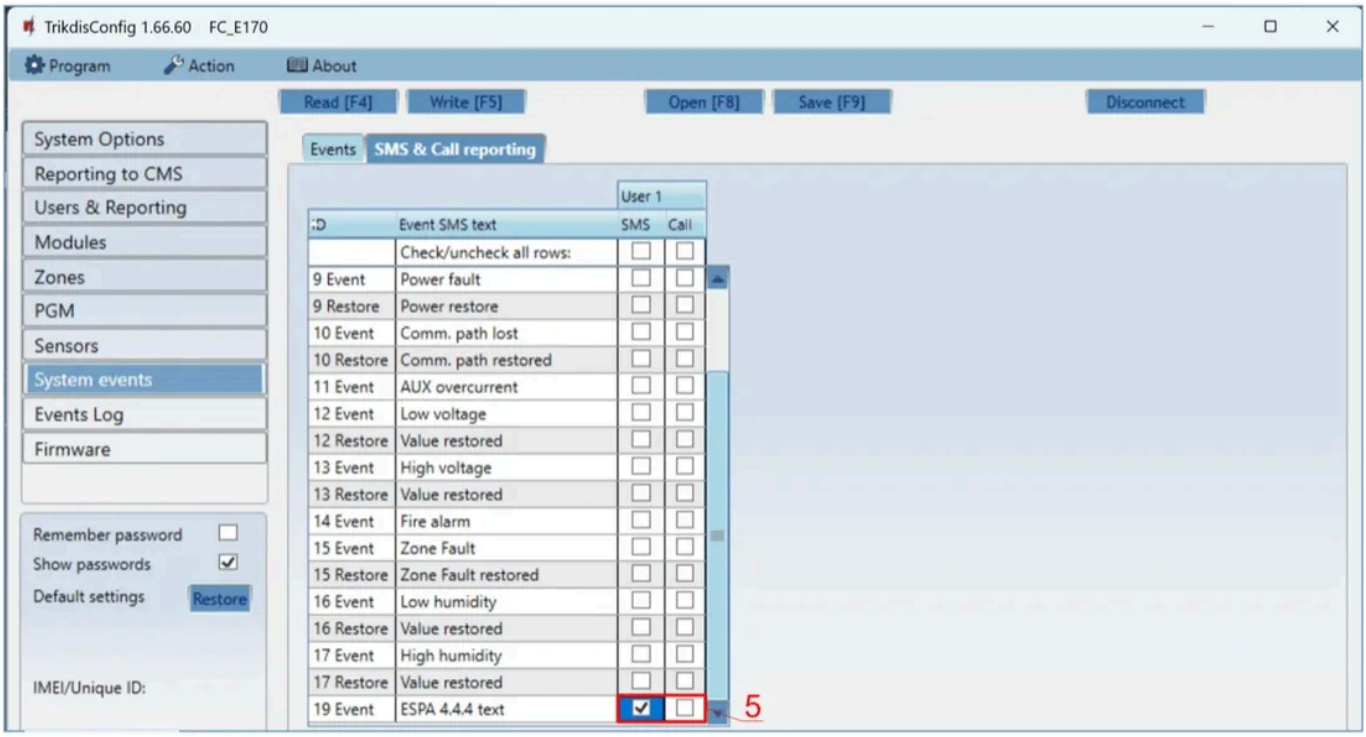


Figure 20. TrikdisConfig – **System events**, onglet **SMS & Call reporting** : pour l'utilisateur 1, à l'événement 19 (**ESPA 4.4.4 text**), **SMS** est coché, **Call** est vide.

- 5 les cases **SMS** et **Call**

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 4.2 et 6.3). 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 FireCom arrivent au centre de télésurveillance et dans Protegus 2.

3.6 Centrale incendie NSC Solution

Raccordez la centrale incendie NSC Solution au FireCom sur le bus RS485 2, selon les schémas ci-dessous.

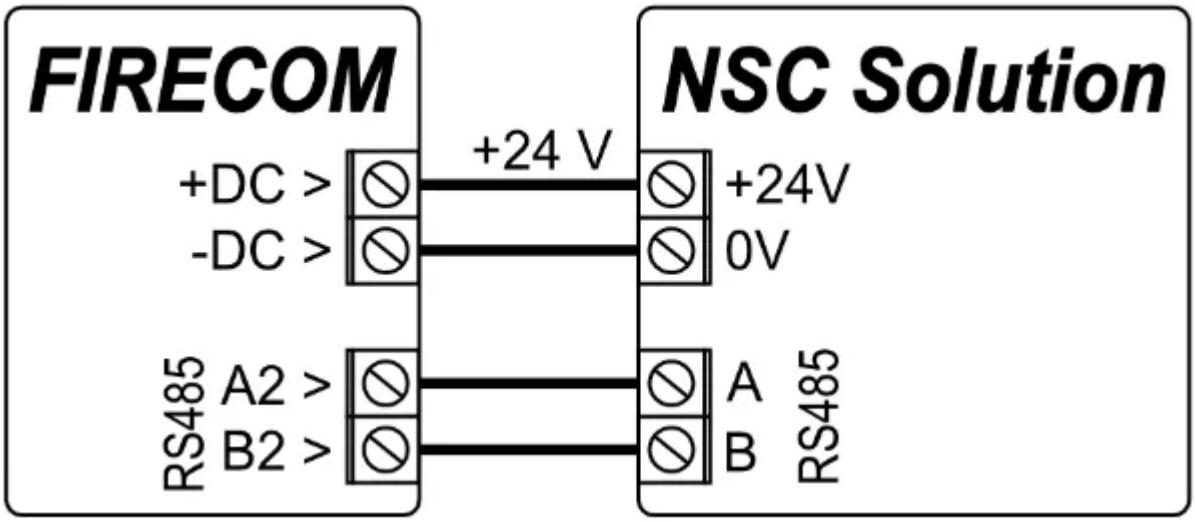


Figure 21. Raccordement de la centrale NSC Solution sans bloc d'alimentation intégré : la borne **+24V** de la centrale va à la borne **+DC** du FireCom, **0V** à la borne **–DC** ; RS485 – **A** à **A2**, **B** à **B2**.

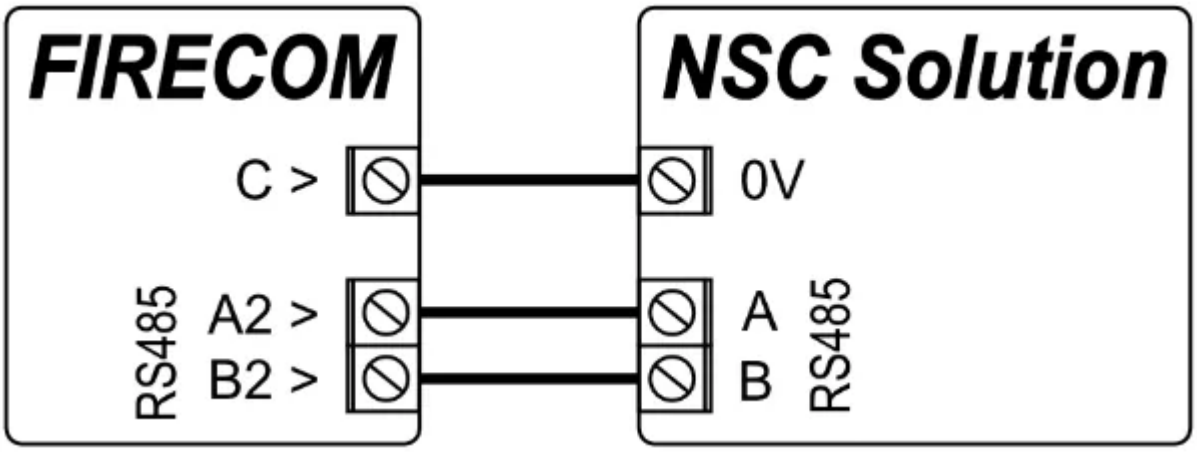


Figure 22. Le même raccordement avec bloc d'alimentation intégré : la borne **0V** de la centrale va à la borne **C** du FireCom ; RS485 – **A** à **A2**, **B** à **B2**.

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

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez la centrale **NSC solution**.
2. L'**NSC slave address** (adresse esclave du communicateur) ne doit pas être identique à l'adresse des modules raccordés à la centrale incendie.

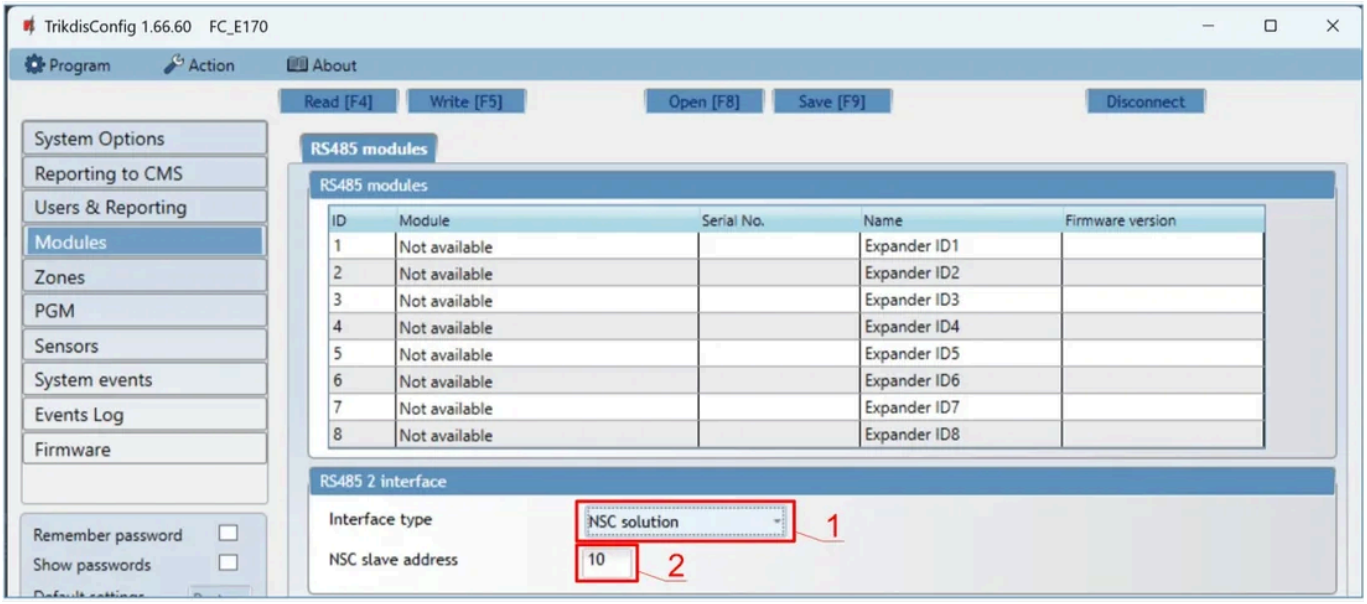


Figure 23. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **NSC solution**
- 2 **NSC slave address** – sur l'image : 10

3. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).
4. Les utilisateurs reçoivent des SMS et des appels 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 ; à côté des 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**).

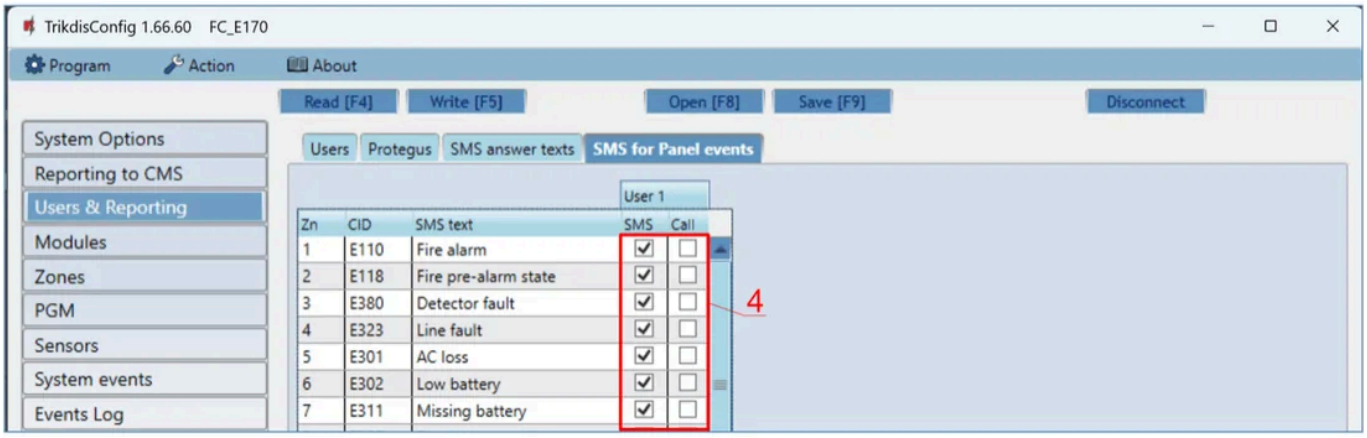


Figure 24. TrikdisConfig – **Users & Reporting**, onglet **SMS for Panel events** : pour l'utilisateur 1, aux événements visibles (**E110** alarme incendie, **E118** préalarme incendie, **E380** défaut de détecteur, **E323** défaut de ligne, **E301** coupure de l'alimentation secteur, **E302** tension de batterie basse, **E311** batterie absente), **SMS** est coché, **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 4.2 et 6.3).

Une fois le FireCom configuré, mettez la centrale incendie sous tension et attendez que son logiciel soit chargé. Il faut ensuite rechercher (scanner) sur la centrale les modules raccordés au bus RS485. Sur la centrale, appuyez sur : **PROG.** > **INSTALLER** > (saisissez le code installateur) **00000 OK** > (sélectionnez) **SETTINGS** >

ENTER > (sélectionnez) **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 FireCom arrivent au centre de télésurveillance et dans Protegus 2.

3.7 Centrale incendie INIM Smartline

Raccordez la centrale incendie INIM Smartline au FireCom sur le bus RS485 2, selon les schémas ci-dessous.

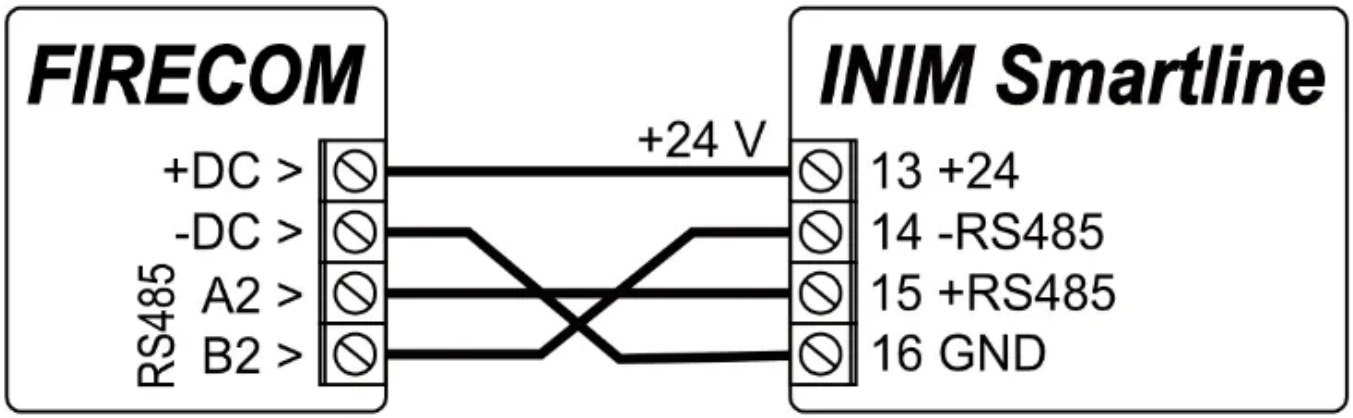


Figure 25. Raccordement de la centrale INIM Smartline sans bloc d'alimentation intégré : la borne **13 +24** de la centrale va à la borne **+DC** du FireCom, **16 GND** à la borne **–DC** ; RS485 – **15 +RS485** à **A2**, **14 –RS485** à **B2**. Les fils qui se croisent ne sont pas en contact.

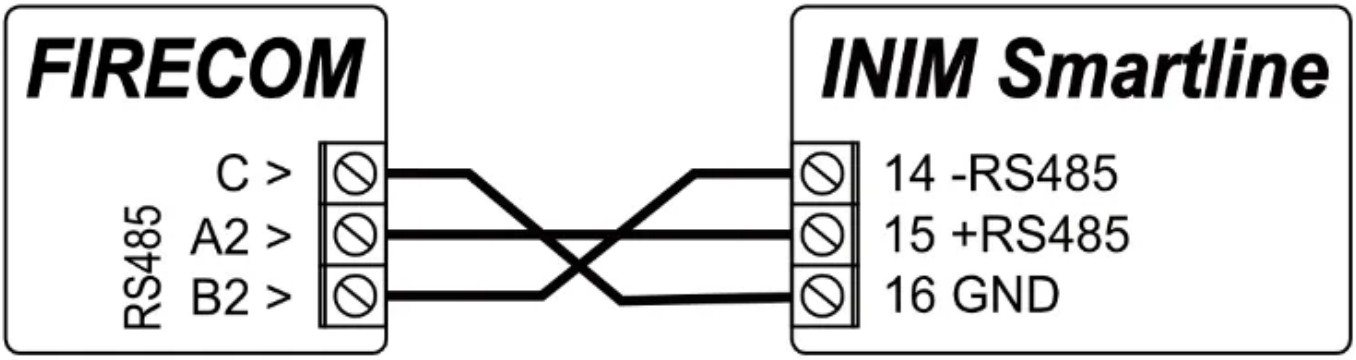


Figure 26. Le même raccordement avec bloc d'alimentation intégré : la borne **16 GND** de la centrale va à la borne **C** du FireCom ; RS485 – **15 +RS485** à **A2**, **14 –RS485** à **B2**.

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

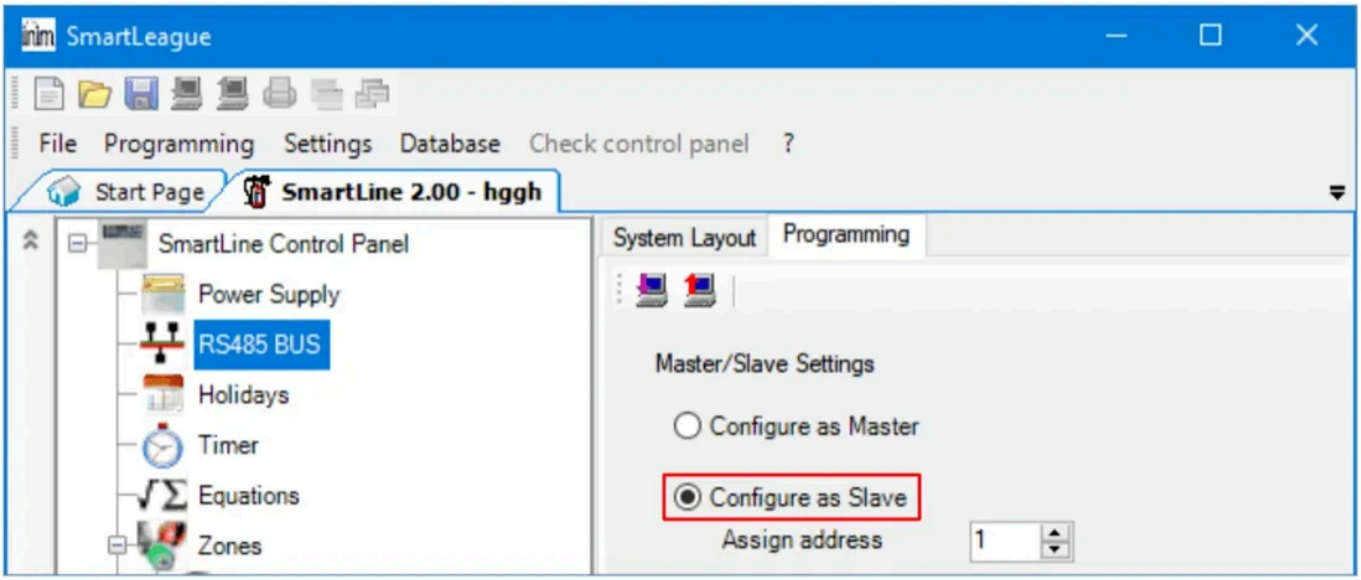


Figure 27. SmartLeague – fenêtre **RS485 Bus Programming** : dans le groupe **Master/Slave Settings**, **Configure as Slave** est sélectionné, **Assign address** : 1.

- Si des répéteurs (repeaters) sont raccordés à la centrale INIM Smartline, le FireCom ne peut pas être raccordé sur le bus RS485.
- Si le FireCom est raccordé à la centrale INIM Smartline sur le bus RS485, les modules d'extension iO ne sont pas pris en charge.

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

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez la centrale **INIM smartline**.

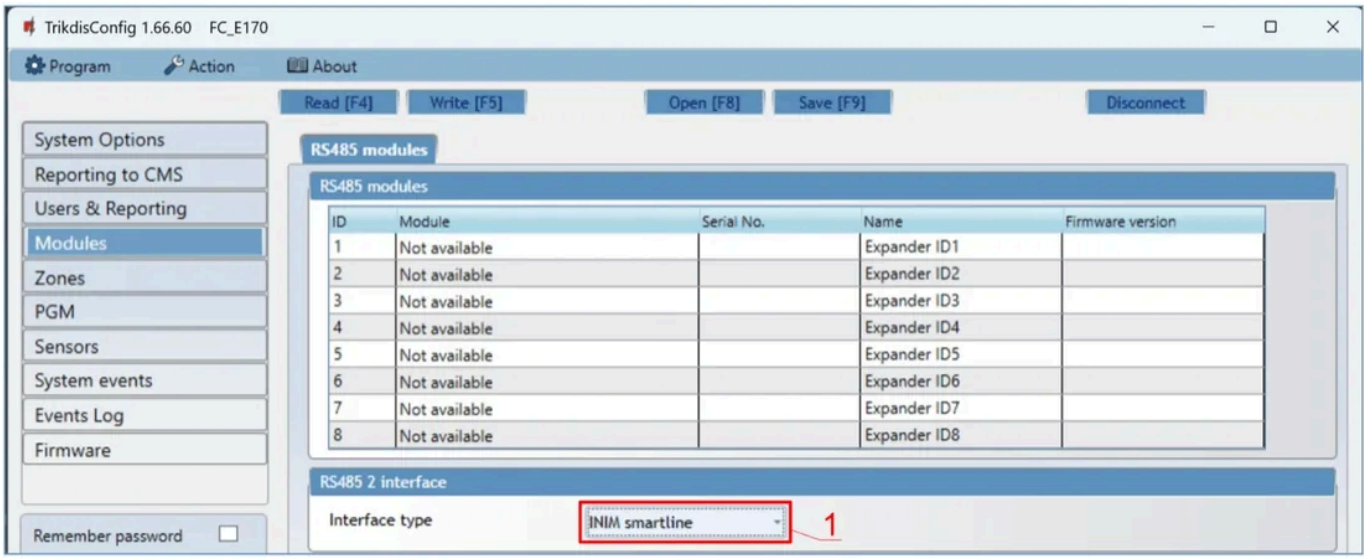


Figure 28. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **INIM smartline**

2. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).
3. Les utilisateurs reçoivent des SMS et des appels pour les événements cochés (page **Users & Reporting**, onglet **SMS for Panel events** ; l'image de l'onglet figure au point 3.6). Dans la colonne **CID**, vous pouvez ajouter d'autres codes d'événement Contact ID ; à côté des 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 4.2 et 6.3).

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

3.8 Centrale incendie C-TEC Cast ZFP

Raccordez la centrale incendie C-TEC Cast ZFP au FireCom sur le bus RS485 2, selon les schémas ci-dessous.

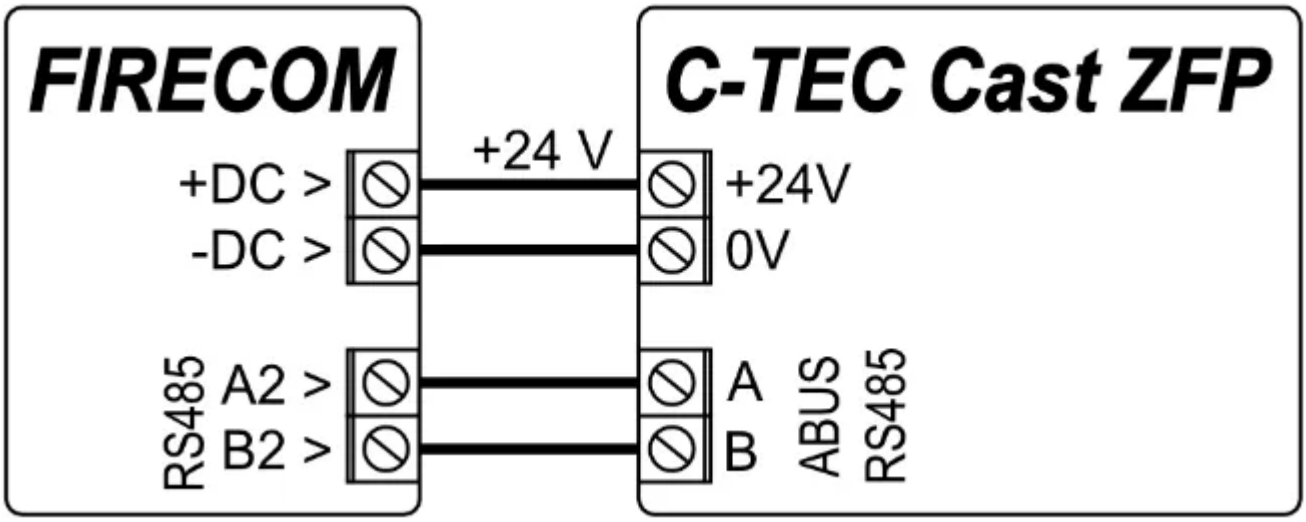


Figure 29. Raccordement de la centrale C-TEC Cast ZFP sans bloc d'alimentation intégré : la borne **+24V** de la centrale va à la borne **+DC** du FireCom, **0V** à la borne **–DC** (le fil positif est repéré +24 V) ; **ABUS RS485** – la borne **A** de la centrale va à **A2**, **B** à **B2**.

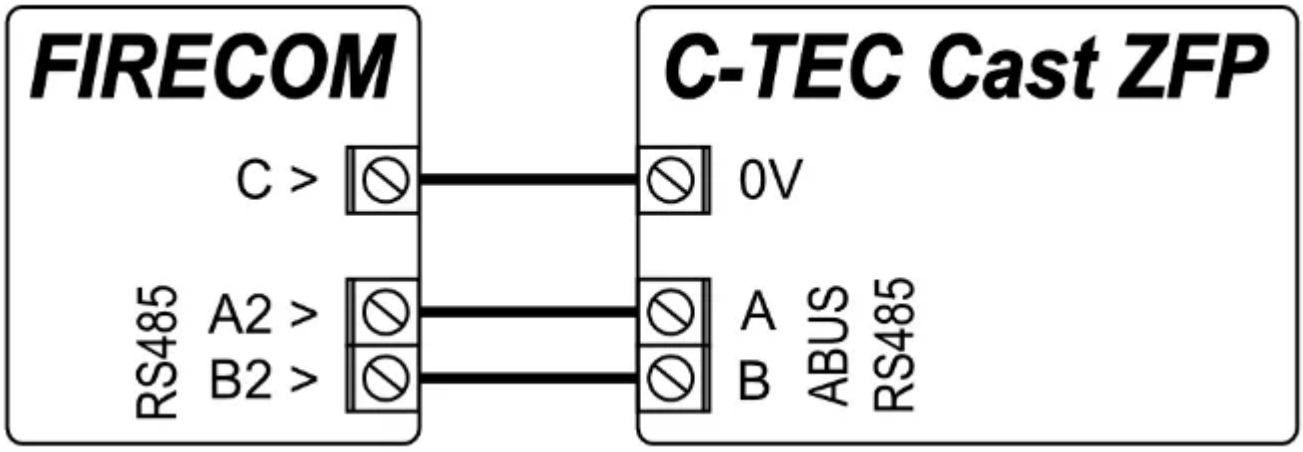


Figure 30. Le même raccordement avec bloc d'alimentation intégré : la borne **0V** de la centrale va à la borne **C** du FireCom ; **ABUS RS485** – **A** à **A2**, **B** à **B2**.

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

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez la centrale **C-TEC Cast ZFP**.

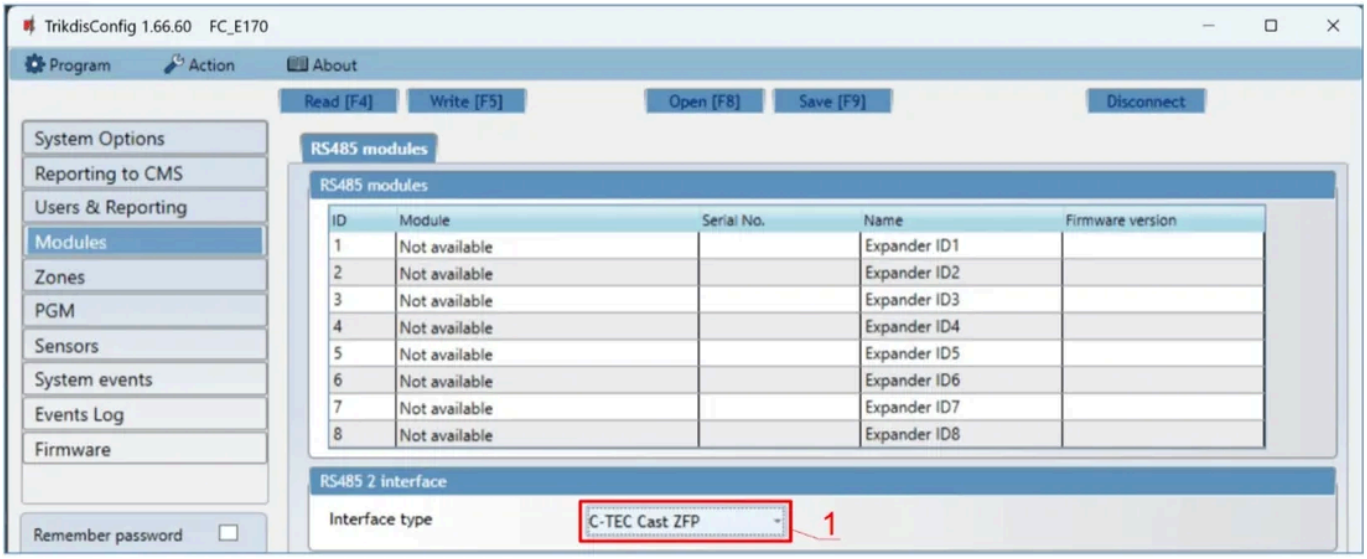


Figure 31. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **C-TEC Cast ZFP**

2. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).
3. Les utilisateurs reçoivent des SMS et des appels pour les événements cochés (page **Users & Reporting**, onglet **SMS for Panel events** ; l'image de l'onglet figure au point 3.6). Dans la colonne **CID**, vous pouvez ajouter d'autres codes d'événement Contact ID ; à côté des 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 4.2 et 6.3).

Configuration de la centrale avec le logiciel 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**. Les numéros des repères sur les images correspondent aux numéros des étapes.

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

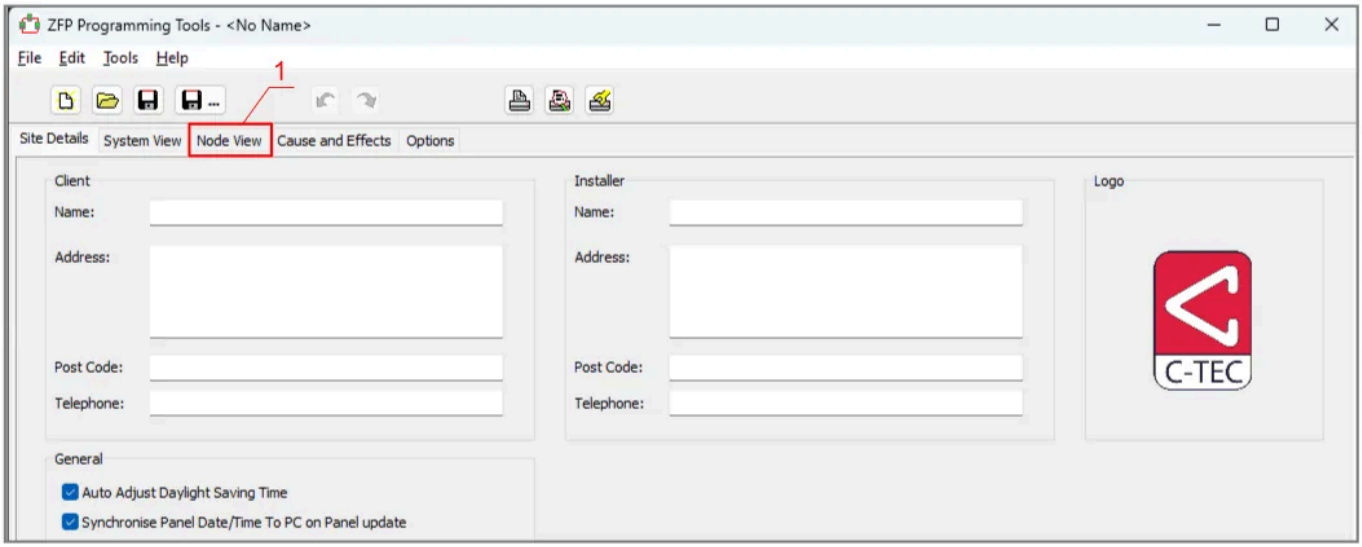


Figure 32. ZFP Programming Tools, fenêtre **Site Details** – l'onglet **Node View**.

- 1 **Node View**

2. Téléchargez les réglages de la centrale sur l'ordinateur.

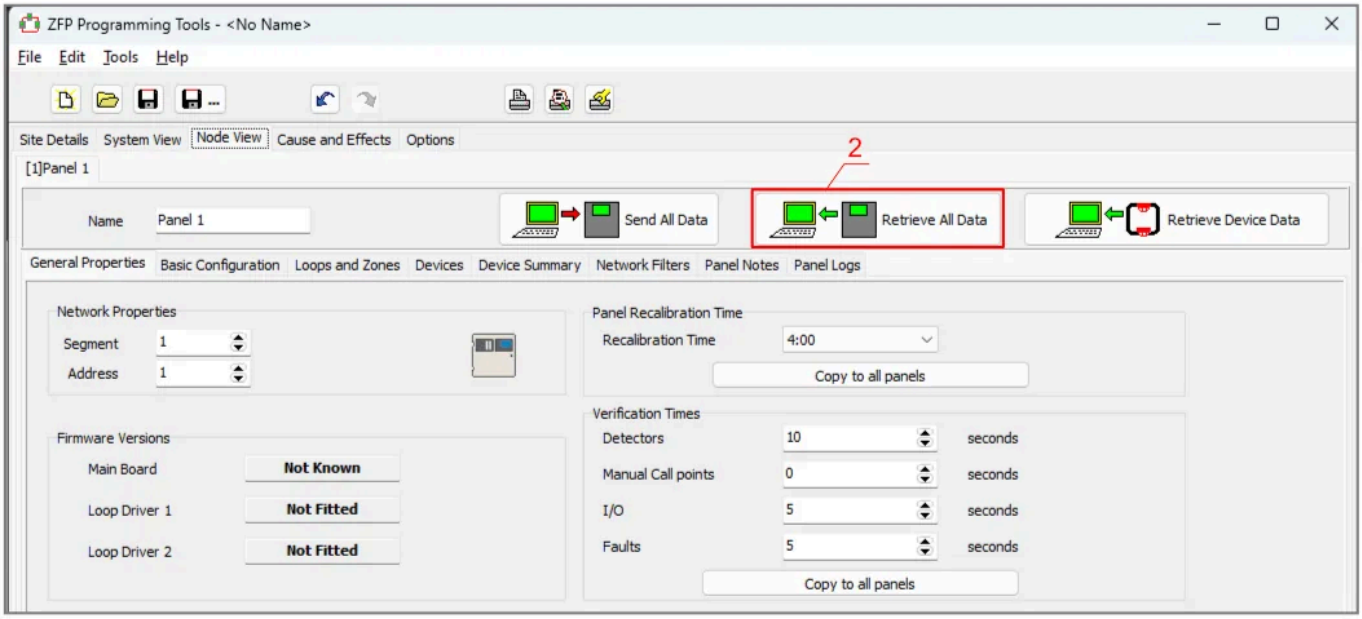


Figure 33. ZFP Programming Tools – **Node View**, **Panel 1**.

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

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

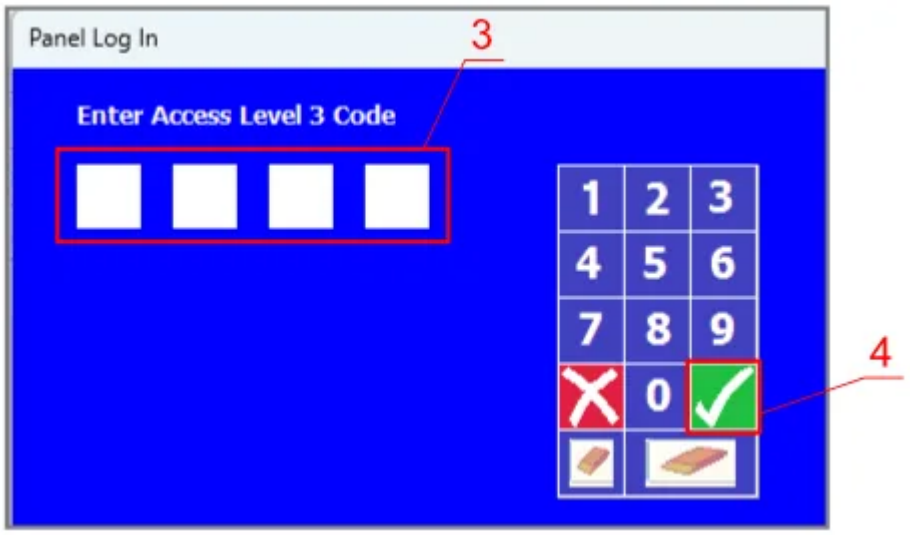


Figure 34. Fenêtre **Panel Log In** : **Enter Access Level 3 Code** – le code du niveau d'accès 3.

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

5. Sélectionnez l'élément **BMS Interface**.
6. Cliquez sur une icône libre.

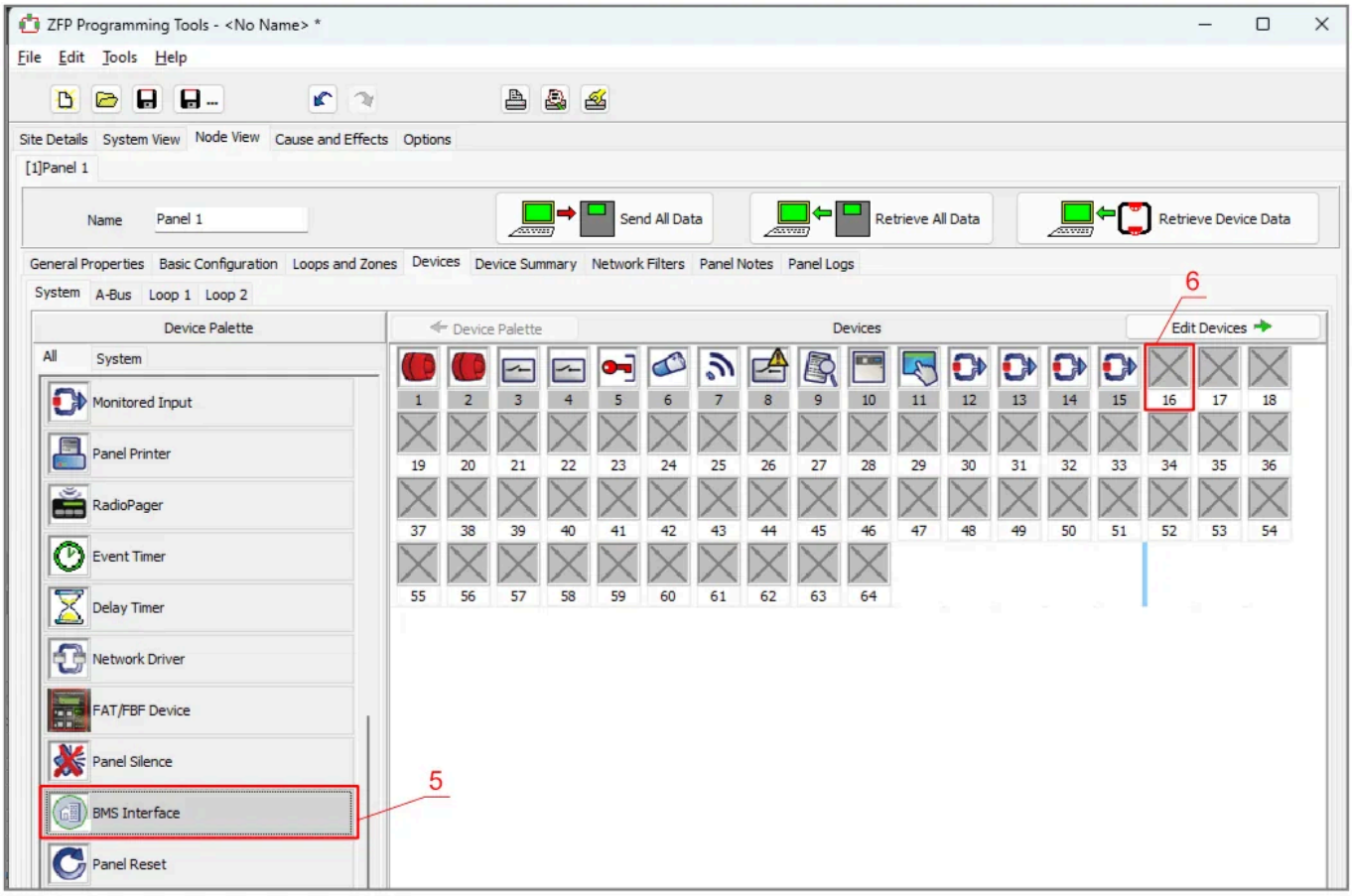


Figure 35. ZFP Programming Tools – **Node View**, **Devices**.

- 5 **BMS Interface** dans la liste **Device Palette**
- 6 emplacement libre dans la partie **Devices** (sur l'image : le 16)

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

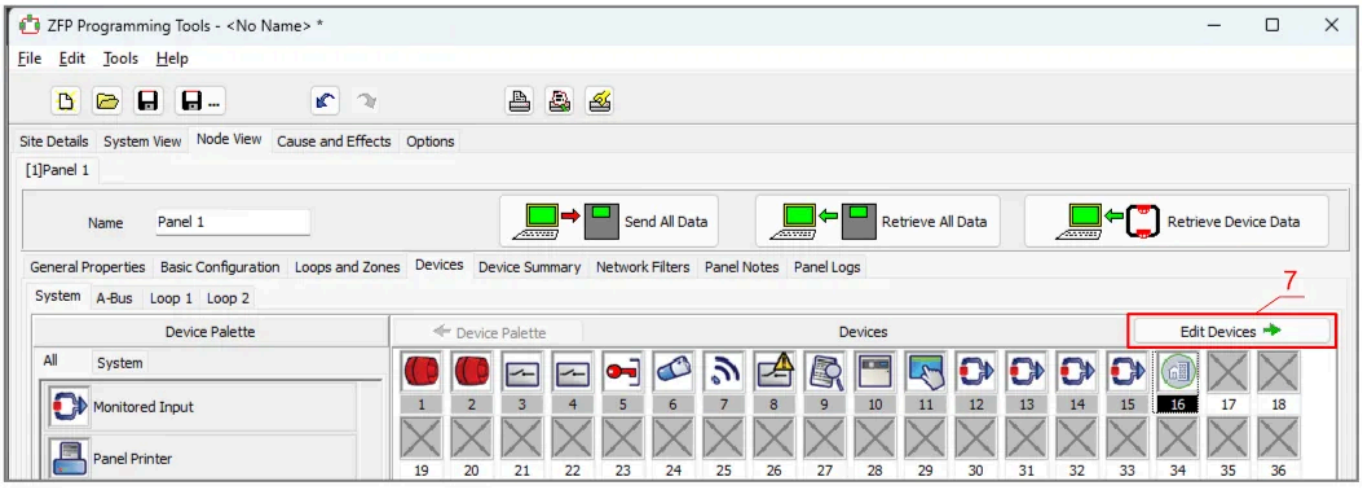


Figure 36. ZFP Programming Tools – l'icône **BMS Interface** est déjà à l'emplacement 16.

- 7 **Edit Devices**

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

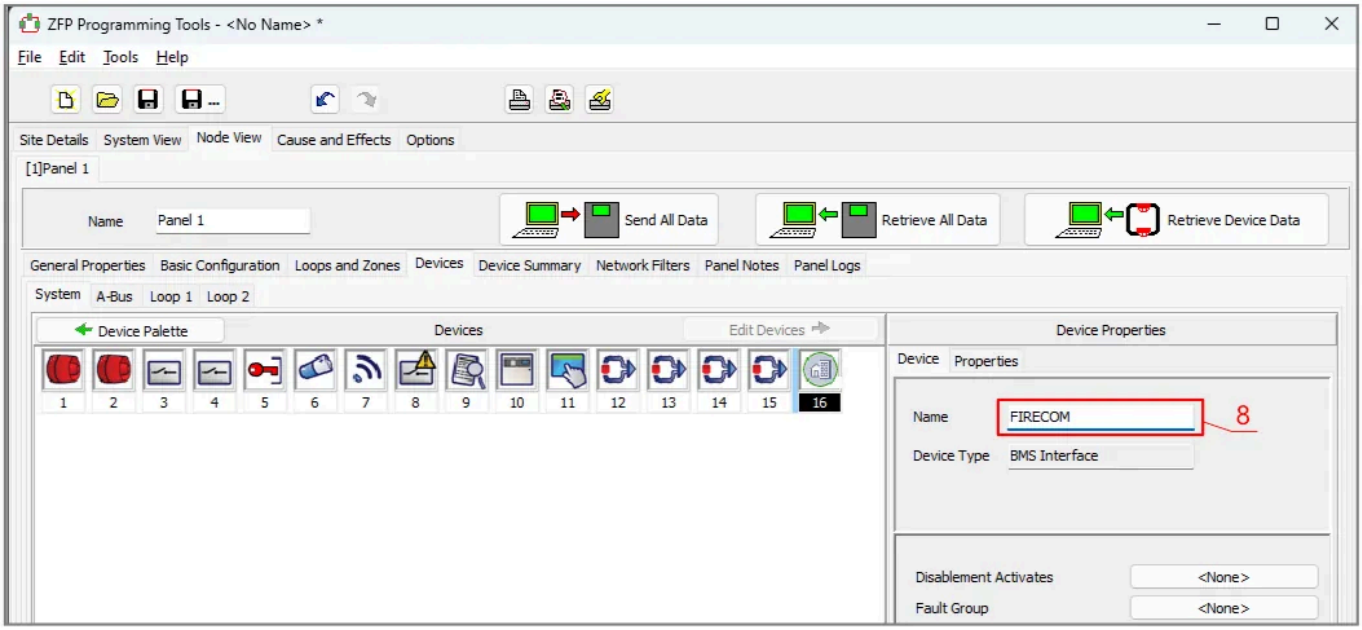


Figure 37. Device Properties, onglet **Device** : **Device Type** : BMS Interface.

- 8 **Name** – le nom du système (sur l'image : FIRECOM)

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

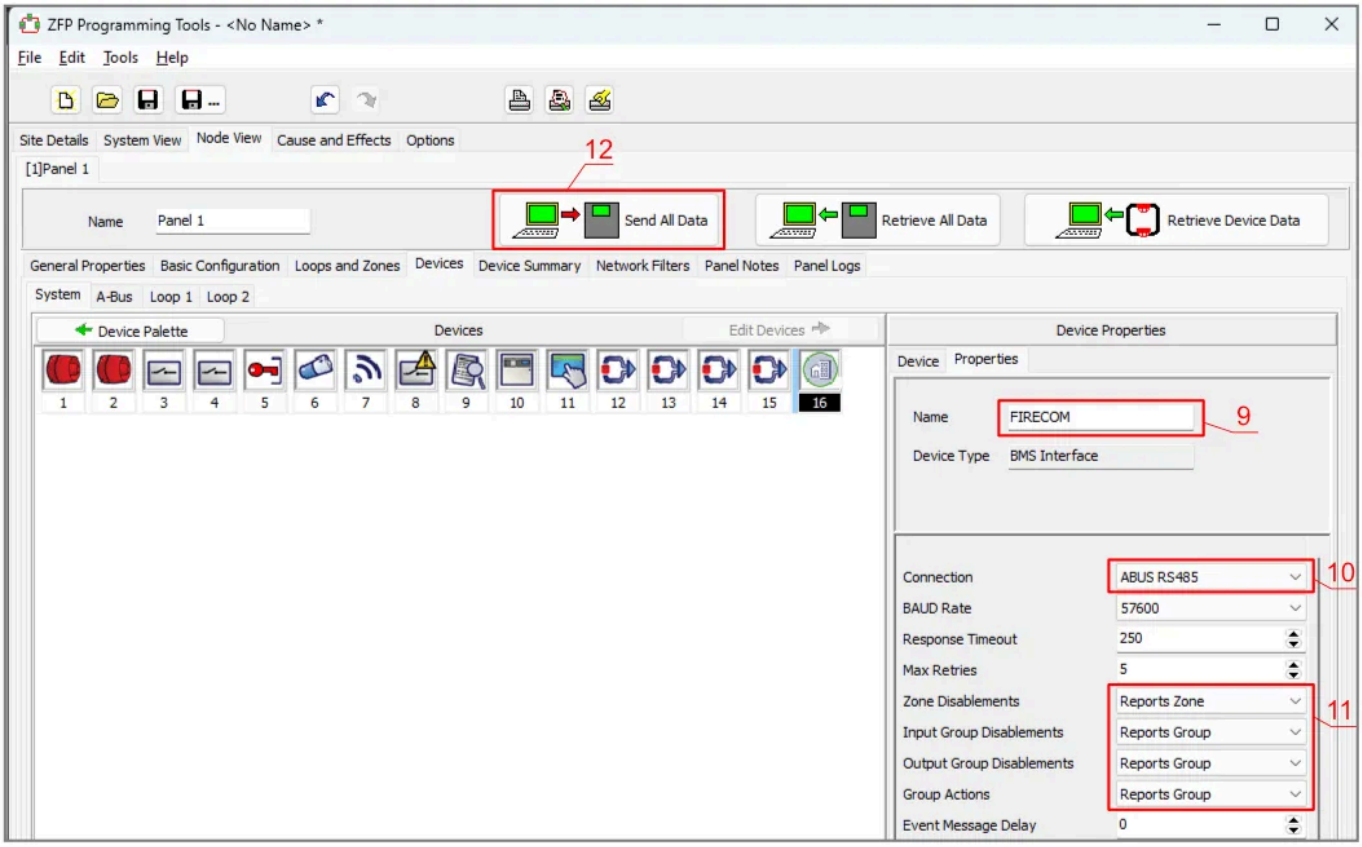


Figure 38. Device Properties, onglet **Properties** ; sur l'image : **BAUD Rate** 57600, **Response Timeout** 250, **Max Retries** 5.

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

13. Saisissez le code (**4444** par défaut).
14. Cliquez sur le bouton **OK** (la fenêtre **Panel Log In** est la même qu'aux étapes 3–4).

La centrale 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 FireCom arrivent au centre de télésurveillance et dans Protegus 2.

3.9 Centrale incendie Polon-Alfa 3000

Raccordement sur le bus RS485

Le FireCom se raccorde à la centrale Polon-Alfa 3000 sur le bus RS485.

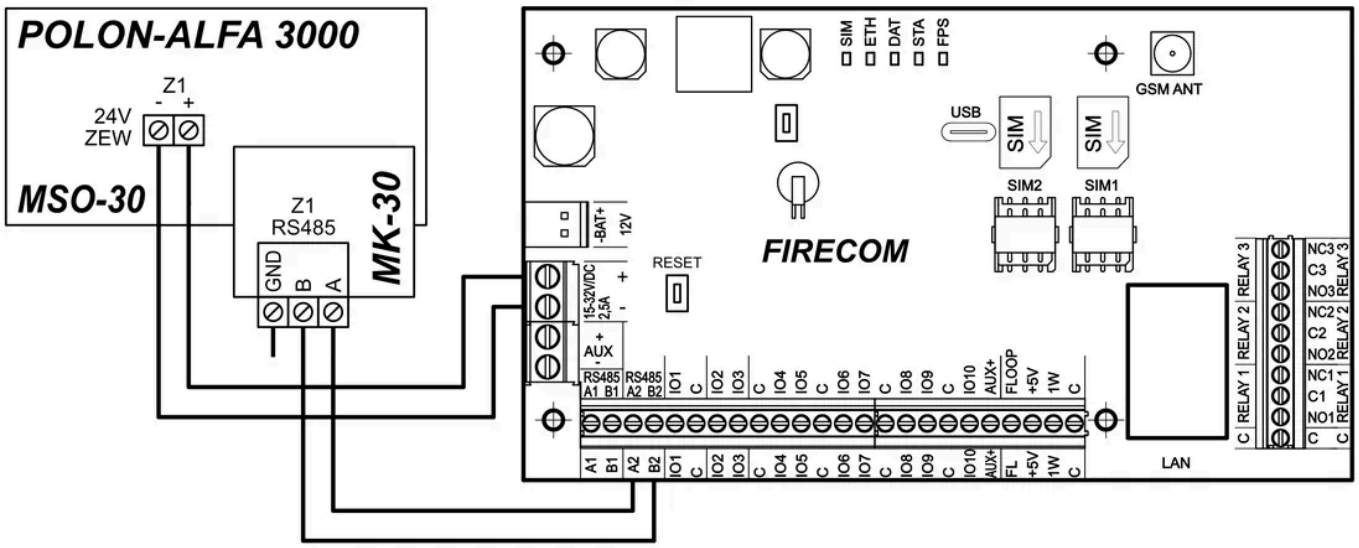


Figure 39. Raccordement de la Polon-Alfa 3000 (modules **MSO-30** et **MK-30**) sur le bus RS485. Alimentation : la borne **Z1 24V ZEW +** du MSO-30 va à la borne **+** du FireCom (15–32 V DC, 2,5 A), **Z1 –** à la borne **–** ; RS485 – la borne **Z1 RS485 A** du MK-30 va à **A2**, **B** à **B2**. La borne **GND** du MK-30 n'est pas raccordée.

Configuration du FireCom dans TrikdisConfig :

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez la centrale **Polon-Alfa 3000**.
2. Comme type de liaison (**Connection**), sélectionnez **RS485**.

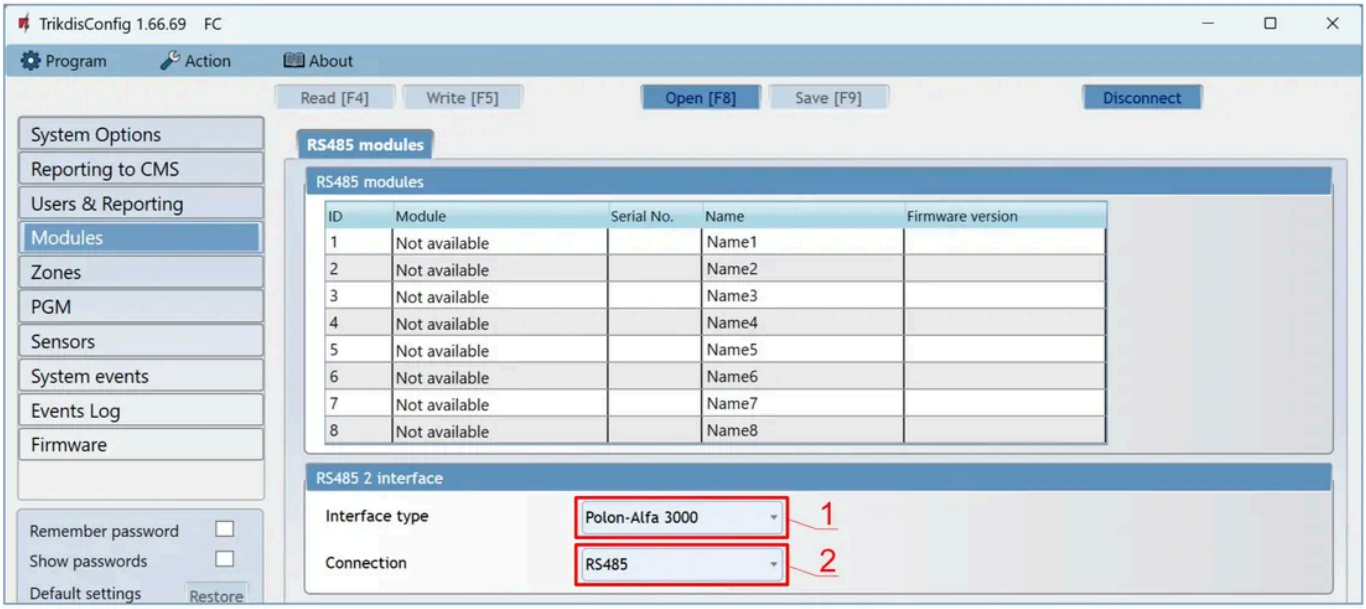


Figure 40. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **Polon-Alfa 3000**
- 2 **Connection** – **RS485**

3. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).
4. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**) (page **System events**, onglet **SMS & Call reporting**, point 6.9).
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 4.2 et 6.3).

La centrale Polon-Alfa 3000 doit être configurée avec le module **MK-30** dans le logiciel **POLON Studio** pour fonctionner avec le protocole **Modbus RTU** (RS485).

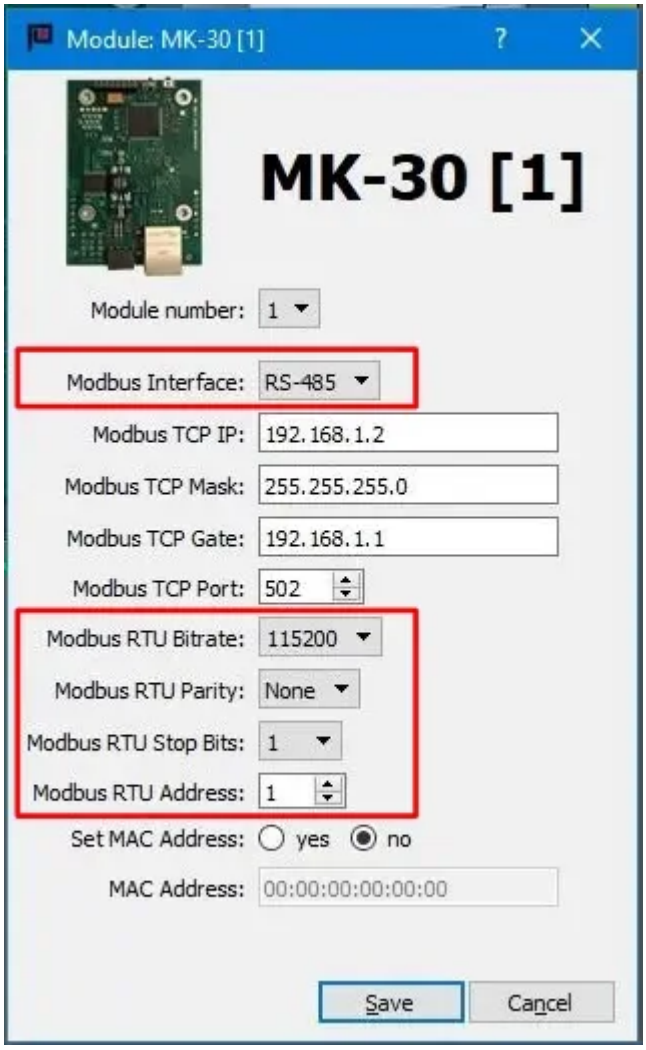


Figure 41. POLON Studio – la fenêtre du module **MK-30 (1)** : **Modbus Interface** : RS-485 ; **Modbus RTU Bitrate** 115200, **Parity** None, **Stop Bits** 1, **Address** 1.

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

Raccordement via le réseau local (LAN)

Le FireCom et la centrale Polon-Alfa 3000 sont raccordés au même réseau local (LAN).

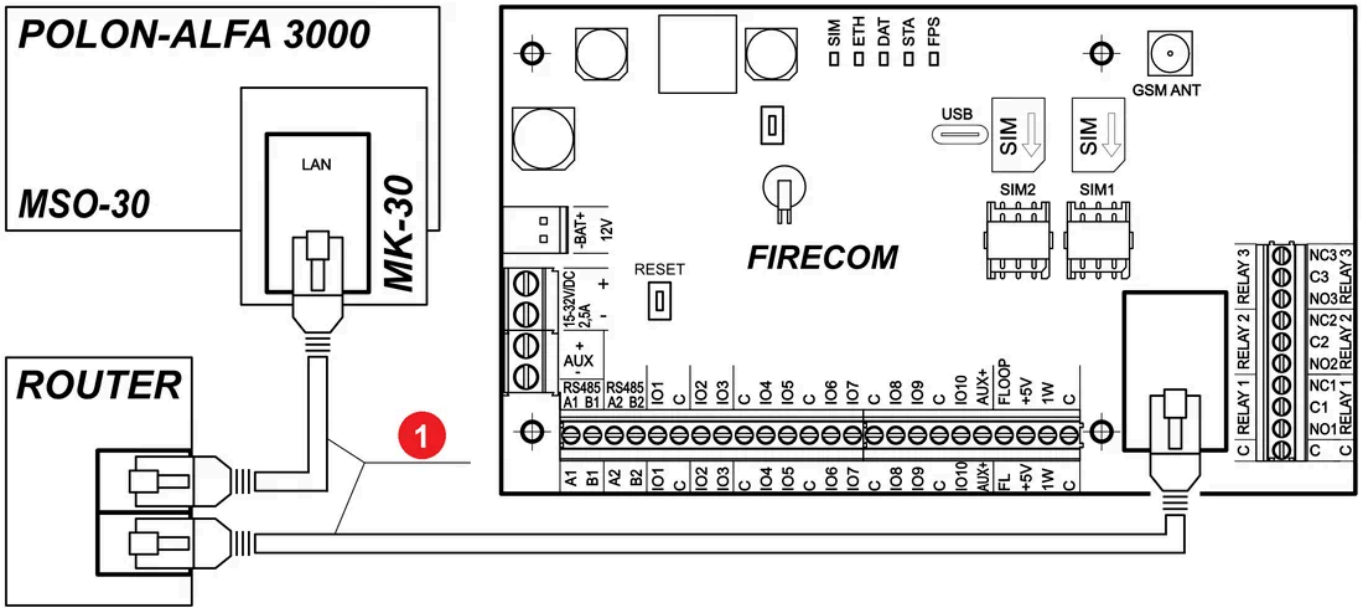


Figure 42. La Polon-Alfa 3000 (**MSO-30** / **MK-30**) et le FireCom sur le même réseau local : le connecteur **LAN** du MK-30 et le connecteur **LAN** du FireCom sont reliés par câble LAN au même routeur (**ROUTER**).

- 1 câble LAN (« LAN cable »)

Configuration du FireCom dans TrikdisConfig :

1. Dans le groupe **RS485 2 interface** de la page **Modules**, sélectionnez la centrale **Polon-Alfa 3000**.
2. Comme type de liaison (**Connection**), sélectionnez **TCP**.
3. Saisissez l'adresse IP (**IP address**) de la centrale Polon-Alfa 3000.

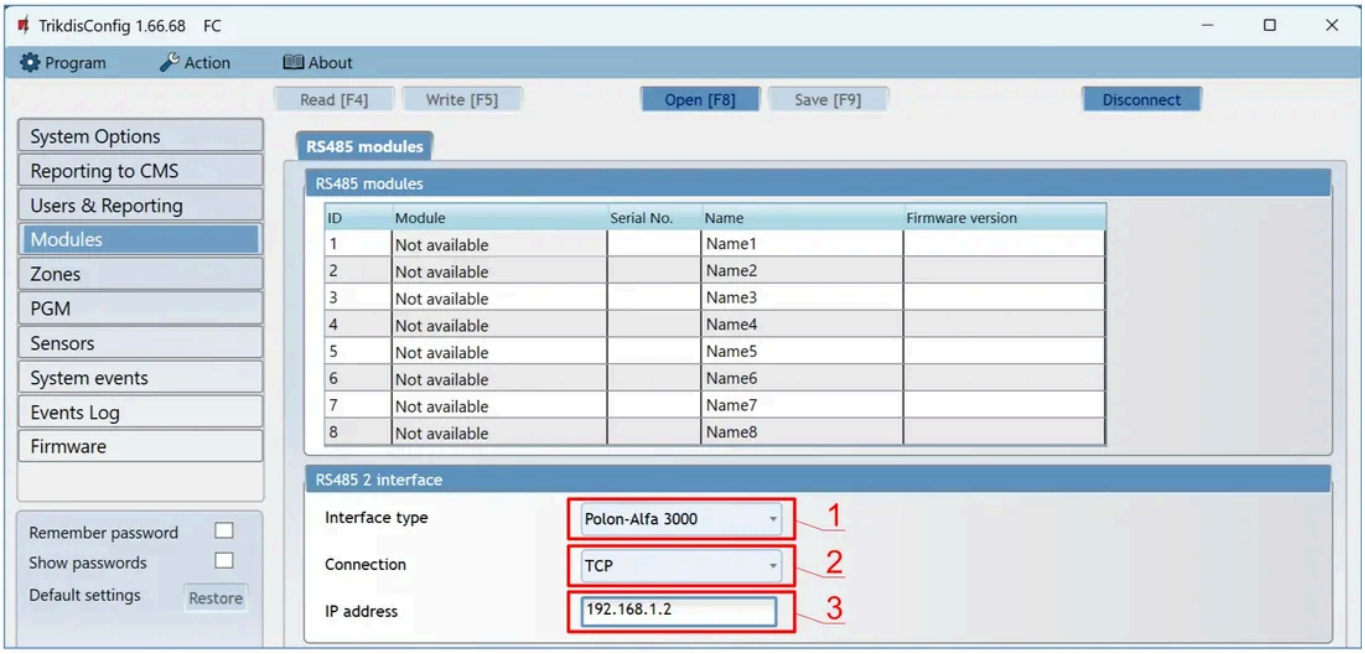


Figure 43. TrikdisConfig – **Modules**, groupe **RS485 2 interface**.

- 1 **Interface type** – sélection de **Polon-Alfa 3000**
- 2 **Connection** – **TCP**
- 3 **IP address** – l'adresse IP de la centrale (sur l'image : 192.168.1.2)

4. Dans l'onglet **Settings** de la page **Reporting to CMS**, groupe **LAN network parameters**, cochez la case **DHCP** (mode d'enregistrement automatique) : le FireCom lit ainsi automatiquement les paramètres réseau (masque de sous-réseau, passerelle) et obtient une adresse IP (point 6.3).

5. Sur la page **Users & Reporting**, indiquez le numéro de téléphone et l'adresse e-mail des utilisateurs qui reçoivent des messages du FireCom (point 6.4).
6. Si vous souhaitez que l'utilisateur reçoive un message (ou un appel) sur les événements, cochez la case **SMS** (ou **Call**) (page **System events**, onglet **SMS & Call reporting**, point 6.9).
7. Si les messages doivent aussi parvenir au récepteur du centre de télésurveillance, configurez le canal de communication sur la page **Reporting to CMS** (points 4.2 et 6.3).

La centrale Polon-Alfa 3000 doit être configurée avec le module **MK-30** dans le logiciel **POLON Studio** pour fonctionner sur le réseau local (LAN). Indiquez les adresses IP du LAN selon les paramètres de votre propre réseau.

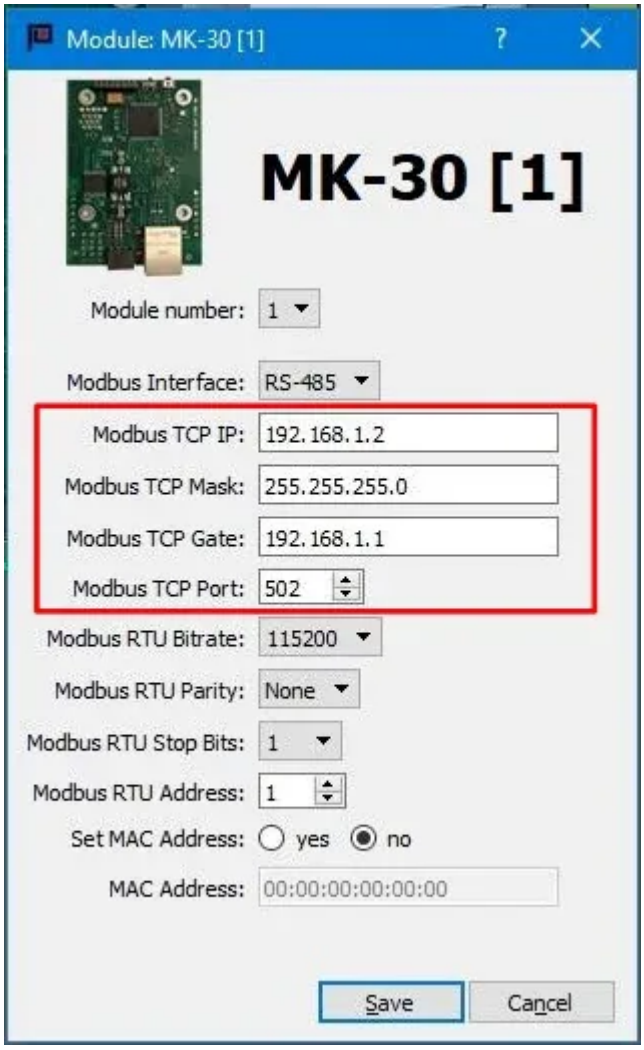


Figure 44. POLON Studio – la fenêtre du module **MK-30 (1)** : **Modbus TCP IP** 192.168.1.2, **Modbus TCP Mask** 255.255.255.0, **Modbus TCP Gate** 192.168.1.1, **Modbus TCP Port** 502.

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

3.10 Raccordement d'un capteur de température

Raccordez les capteurs de température selon les schémas.

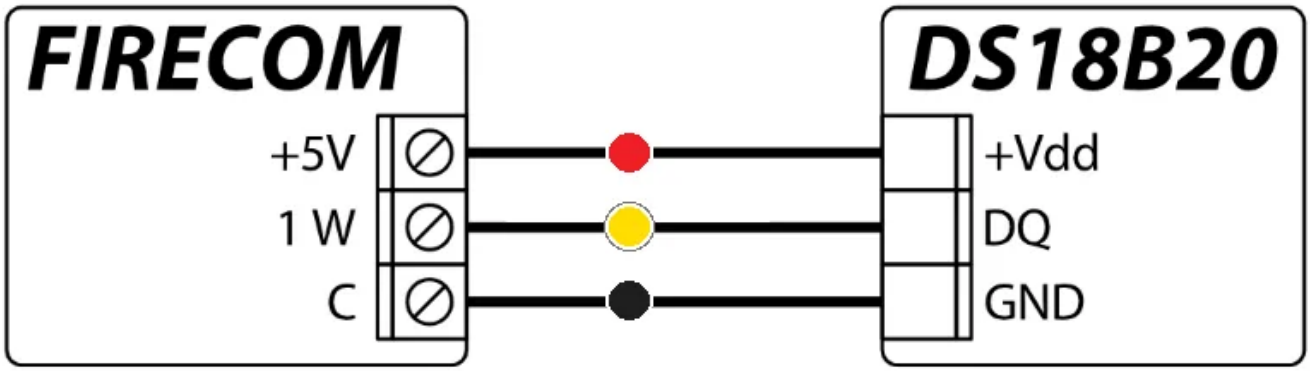


Figure 45. Raccordement du capteur de température **DS18B20** : fil rouge – **+5V** sur la borne **+Vdd** ; jaune – **1W** sur la borne **DQ** ; noir – **C** sur la borne **GND**.

- fil rouge (« Red wire »)
- fil jaune (« Yellow wire »)
- fil noir (« Black wire »)

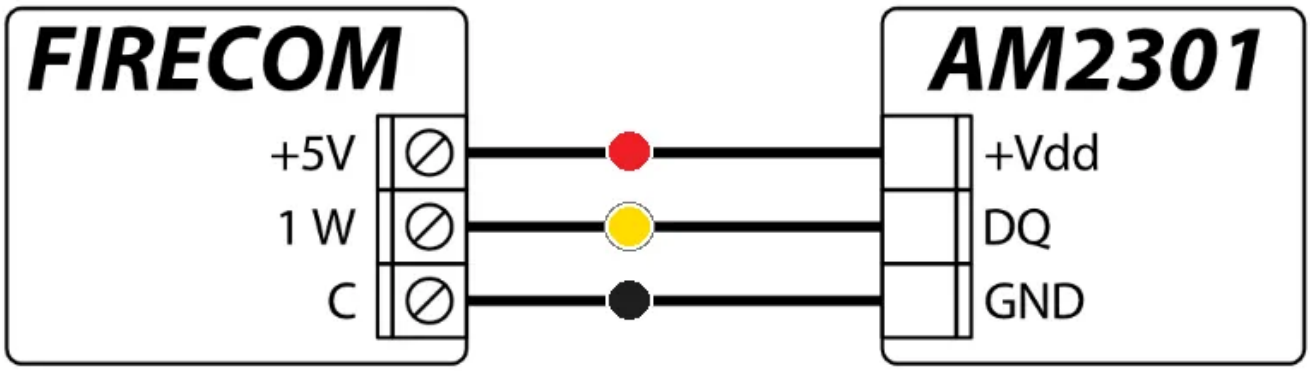


Figure 46. Raccordement du capteur de température et d'humidité **AM2301**, de la même façon : rouge – **+5V** sur **+Vdd** ; jaune – **1W** sur **DQ** ; noir – **C** sur la borne **GND**.

- fil rouge (« Red wire »)
- fil jaune (« Yellow wire »)
- fil noir (« Black wire »)

Au FireCom peuvent être raccordés au maximum 8 capteurs de température Maxim® / Dallas® **DS18S20** ou **DS18B20**, ou au maximum 1 capteur d'humidité et de température **AM2301**. Si vous raccordez le capteur avec un fil de plus de 0,5 m, nous recommandons un câble à paires torsadées (UTP 4×2×0,5 ou STP 4×2×0,5). La borne **+5V** de la carte sert à l'alimentation 5 V DC des appareils raccordés au bus de données 1-Wire ; le courant de sortie maximal est de 0,2 A. La sortie est protégée contre les surcharges : si le courant dépasse la valeur maximale autorisée, l'alimentation se coupe automatiquement. Le communicateur reconnaît et attribue automatiquement les appareils raccordés (l'AM2301 doit être attribué manuellement sur la page **Sensors**, point 6.8).

Capteur de température DS18B20 avec fil 1M

3.11 Raccordement d'un relais et d'un indicateur à LED

Avec les contacts du relais, vous pouvez commuter à distance (marche/arrêt) divers appareils électriques. La borne universelle **I/O** du communicateur doit être configurée en sortie (**OUT**) et recevoir la définition **Remote control** (page **PGM**, **Output definition**, point 6.7).

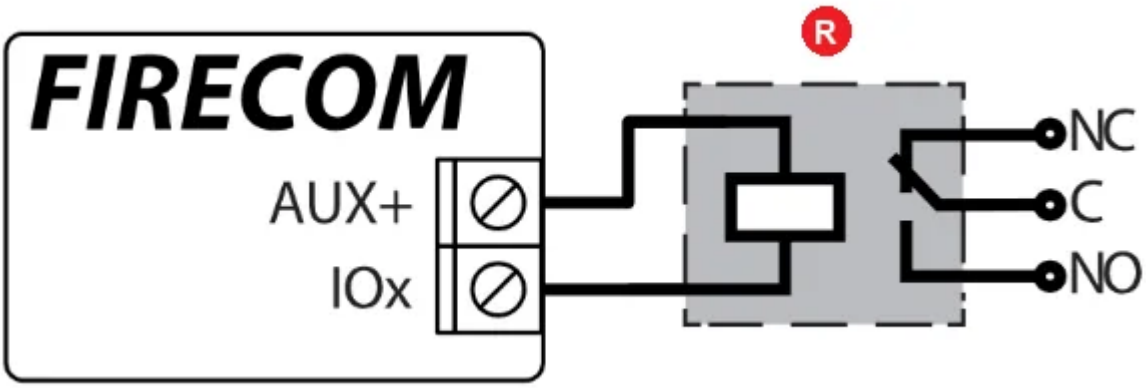


Figure 47. Raccordement d'un relais externe : une extrémité de la bobine va sur **AUX+**, l'autre sur la borne **IOx** ; contacts du relais : **NC**, **C**, **NO**.

- R relais (« Relay »)

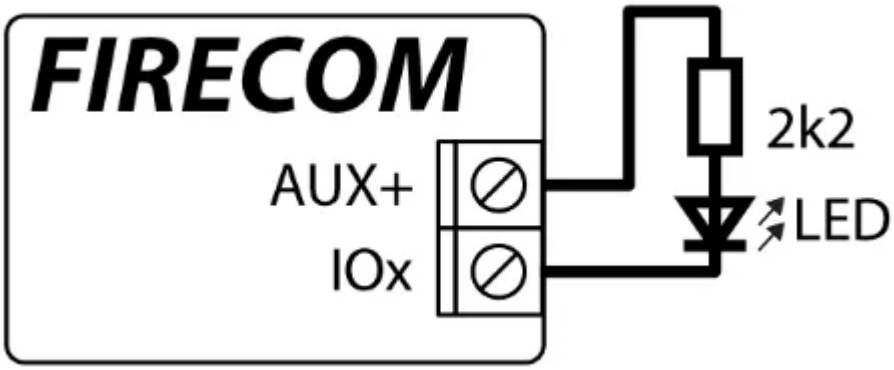


Figure 48. Raccordement d'un indicateur à LED : depuis la borne **AUX+**, via une résistance **2k2** (2,2 kΩ) et la LED, en série, vers la borne **IOx**.

3.12 Raccordement des entrées de la centrale incendie

Selon la norme EN 54, la centrale incendie doit être informée par le communicateur d'un défaut de la liaison avec le centre de télésurveillance, ainsi que de la bonne réception des messages par le centre de télésurveillance. Pour cela, les sorties PGM du communicateur (par exemple les sorties **Relay1** et **Relay2**) doivent être raccordées aux entrées prévues à cet effet sur la centrale incendie. La sortie PGM **Relay1** doit être réglée sur **CMS fail** (défaut de la liaison avec le centre de télésurveillance), **Relay2** sur **ACK received** (acquit reçu) (page **PGM**, point 6.7). La sortie **Relay1** s'active lorsque le canal de communication avec le centre de télésurveillance est interrompu ; la sortie **Relay2** s'active pendant 5 secondes lorsque le message est bien parvenu au centre de télésurveillance.

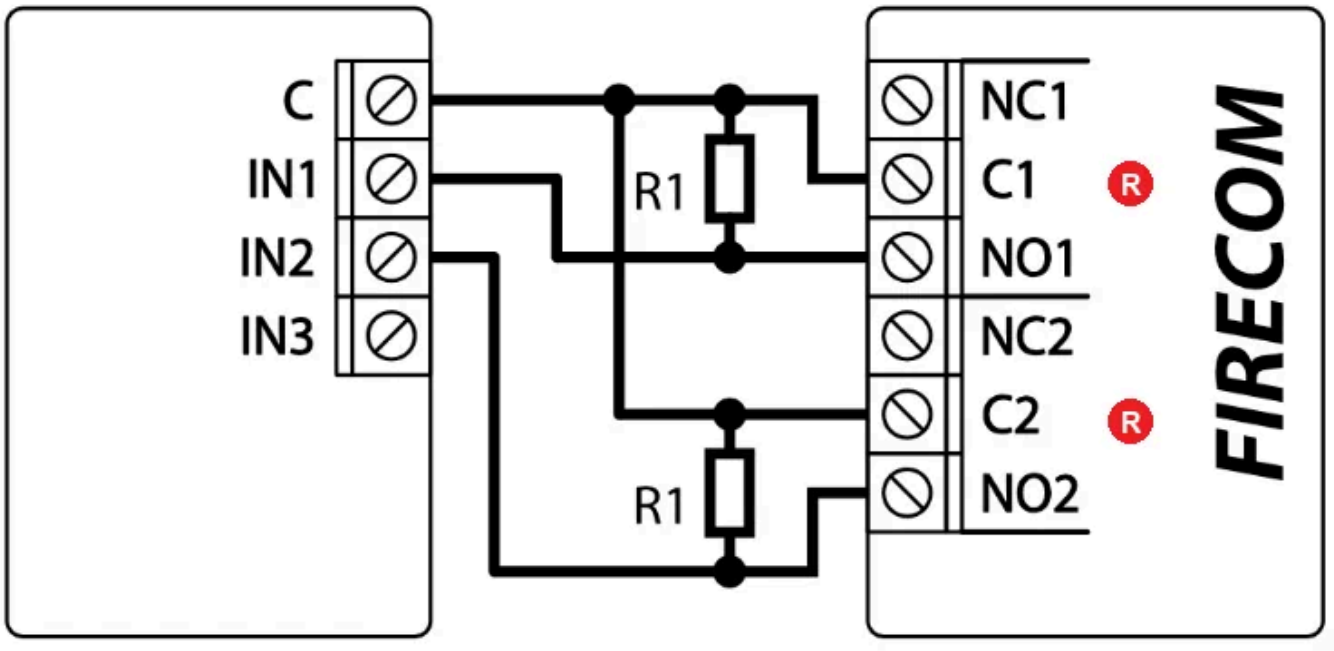


Figure 49. Raccordement des sorties relais du communicateur aux entrées de la centrale incendie (**Fire control panel**). **Relay1** : la borne **C** de la centrale va à **C1**, **IN1** à **NO1**, une résistance **R1** en parallèle entre **C1** et **NO1** ; **Relay2** : **C** va à **C2**, **IN2** à **NO2**, également une résistance **R1** entre **C2** et **NO2**. **IN3**, **NC1** et **NC2** ne sont pas raccordées.

- R sortie relais du communicateur (« Relay ») : en haut **Relay1**, en bas **Relay2**

3.13 Raccordement des modules d'extension de la série iO

Si le FireCom a besoin de davantage d'entrées (IN) ou de sorties (OUT), raccordez-lui un module d'extension d'entrées et de sorties Trikdis de la série iO, filaire ou sans fil. La configuration des modules d'extension dans le FireCom est décrite au point 6.5 (page **Modules**).

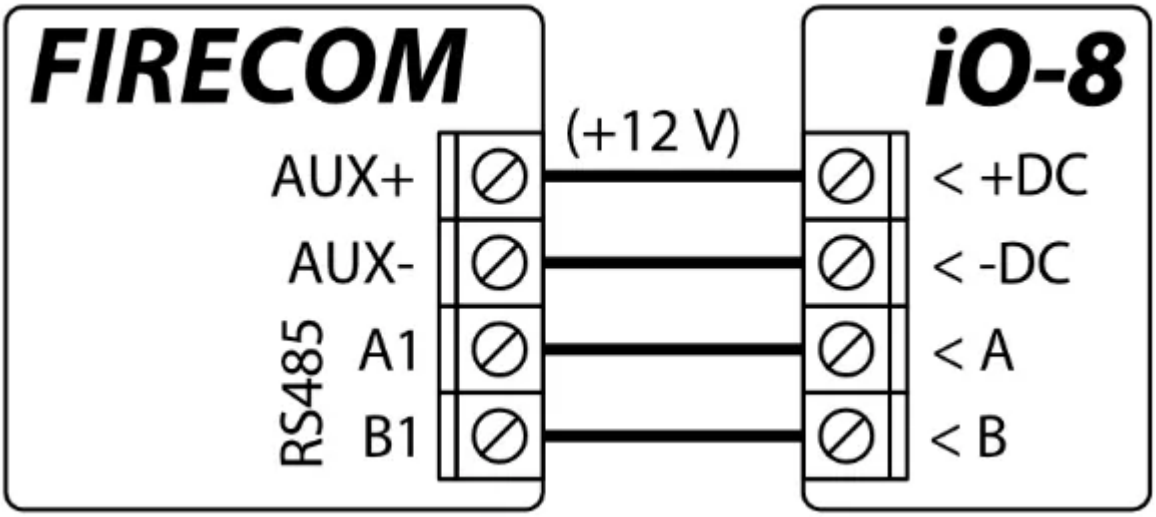


Figure 50. Raccordement de l'**iO-8** : alimentation – **AUX+** (+12 V) va à la borne **+DC** de l'iO-8, **AUX–** à la borne **–DC** ; RS485 – **A1** va à **A**, **B1** à **B**.

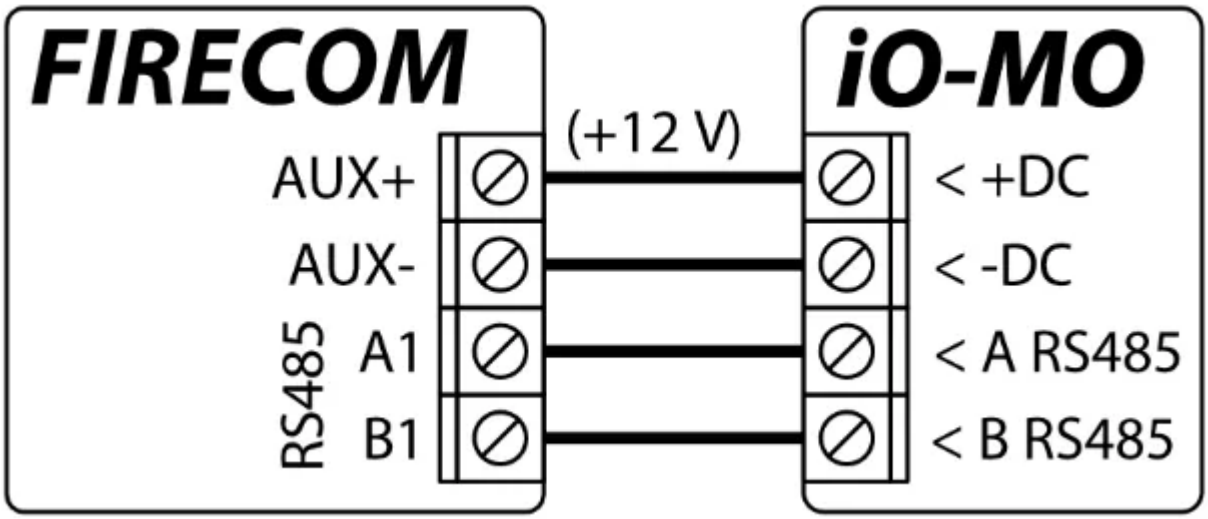


Figure 51. Raccordement de l'**iO-MO** : alimentation – **AUX+** (+12 V) va à la borne **+DC**, **AUX–** à la borne **–DC** ; RS485 – **A1** va à **A RS485**, **B1** à **B RS485**.

Module Trikdis IO8 Wired Expander

Raccordement des modules LORA : l'émetteur-récepteur **RF-LORA** se raccorde au bus RS485 et maintient par radio, jusqu'à 5000 m, la liaison avec les modules d'extension **iO-LORA**, **iO8-LORA** et **REL-LORA** et avec le bouton panique **PB-LORA**.

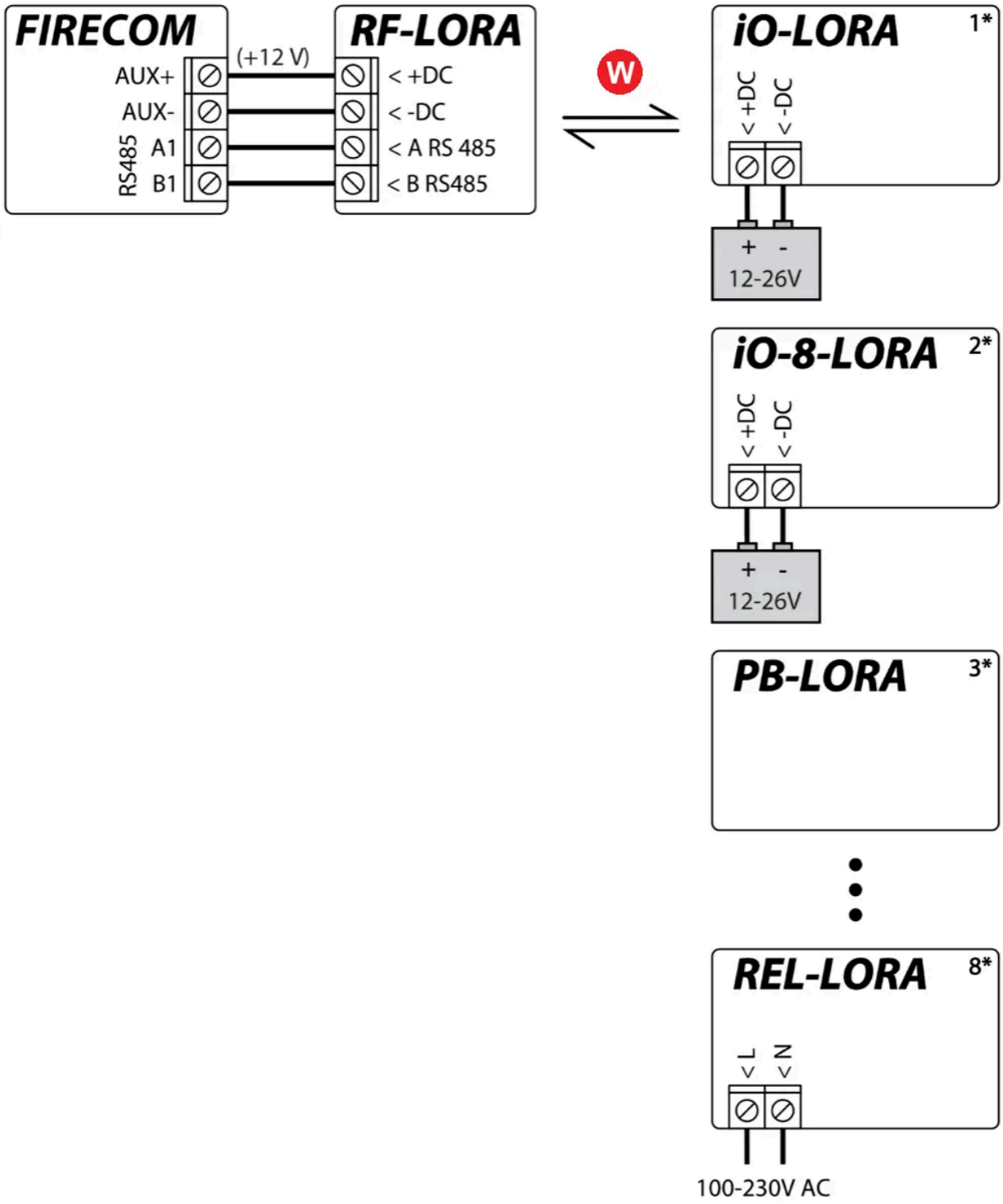


Figure 52. Raccordement des modules LORA : alimentation – **AUX+** (+12 V) va à la borne **+DC** du RF-LORA, **AUX–** à la borne **–DC** ; RS485 – **A1** va à **A RS485**, **B1** à **B RS485**. Liaison radio jusqu'à 5000 m avec les modules **iO-LORA**, **iO8-LORA**, **PB-LORA** et **REL-LORA** (sur le schéma, les noms des modules sont précédés des repères 1, *2*, 3, *8*) ; 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**

3.14 Mise sous tension du communicateur

Pour mettre le communicateur en marche, mettez son alimentation sous tension. Les voyants doivent se comporter ainsi :

- le voyant **STA** est vert fixe pendant la mise sous tension, puis clignote en vert après le démarrage – la tension d'alimentation est correcte ;
- le voyant **SIM** est vert fixe et clignote de temps en temps au moins 3 fois en jaune – la couleur verte indique que la carte SIM s'est bien enregistrée sur le réseau mobile, et le nombre de clignotements jaunes indique le niveau de signal du réseau mobile. Le voyant **ETH** est allumé en vert lorsque le communicateur est connecté au réseau local (LAN).

- Sur le réseau 4G, un niveau de signal de 3 est suffisant (3 clignotements jaunes du voyant **SIM**).
- Si le voyant **SIM** clignote moins souvent en jaune, le niveau de signal du réseau mobile est insuffisant. Choisissez un autre emplacement pour le communicateur, déplacez l'antenne ou utilisez une antenne mobile plus sensible (point 1.6).
- Si les voyants se comportent autrement, recherchez la cause à l'aide du point 1.5 (voyants).
- Si aucun voyant du FireCom ne s'allume, vérifiez l'alimentation et le raccordement.

4. Configuration rapide avec le logiciel TrikdisConfig

Ce chapitre décrit les réglages grâce auxquels le FireCom envoie les événements à l'application Protegus 2 (point 4.1) ou au centre de télésurveillance (point 4.2). Les autres réglages du FireCom se trouvent au chapitre 6.

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. Téléchargez le logiciel TrikdisConfig (avec le bouton ci-dessus, ou sur le site www.trikdis.com en saisissant « TrikdisConfig » dans le champ de recherche), puis installez-le.
2. Reliez le FireCom à l'ordinateur avec un câble **USB Type-C**.
3. Lancez TrikdisConfig. Le logiciel reconnaît automatiquement l'appareil raccordé et ouvre la fenêtre de programmation du FireCom.
4. Cliquez sur le bouton **Read [F4]** : le logiciel lit et affiche les réglages actuels du FireCom. Si le logiciel demande le code administrateur ou 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

4.1 Configuration pour l'application Protegus 2

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



Figure 53. TrikdisConfig – **System Options**, onglet **System general**, groupe **SIM** (deux champs de chaque : sur l'image, 1234 dans les deux champs PIN, internet dans les deux champs APN).

- 1 **SIM card PIN** – le code PIN de la carte SIM
- 2 **APN** – le point d'accès de l'Internet mobile

1. Indiquez le code PIN de la carte SIM (**SIM card PIN**).
2. 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 français et européens : Réglage de l'APN – liste des opérateurs mobiles européens.

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

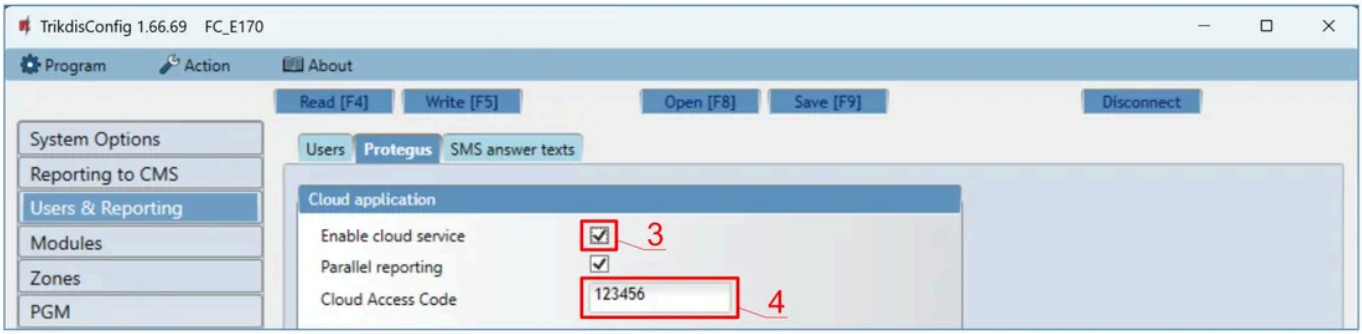


Figure 54. TrikdisConfig – **Users & Reporting**, onglet **Protegus**, groupe **Cloud application** (sur l'image, **Parallel reporting** est également coché).

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

3. Cochez la case **Enable cloud service**.
4. Si vous souhaitez que les utilisateurs doivent saisir le code lors de l'ajout du système dans Protegus 2, modifiez la valeur de **Cloud Access Code** (`123456` par défaut).

Dans l'onglet **Settings** de la page **Reporting to CMS** :

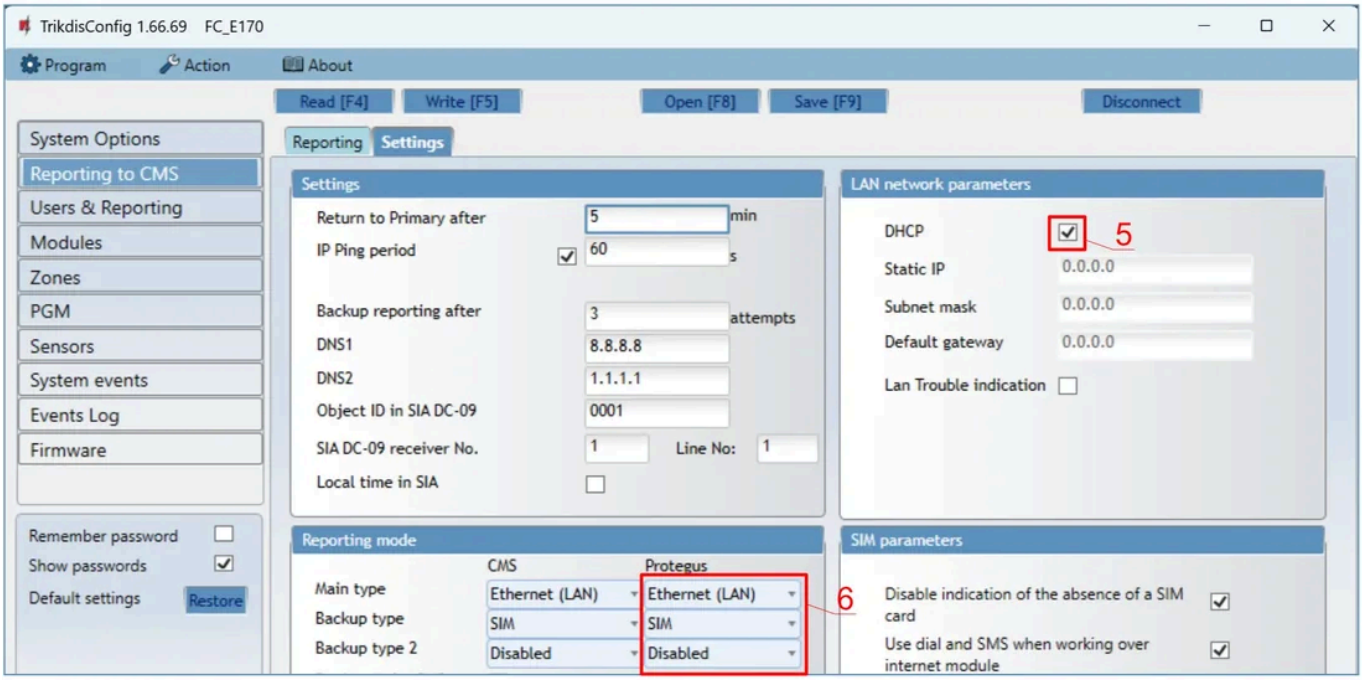


Figure 55. TrikdisConfig – **Reporting to CMS**, onglet **Settings**.

- 5 **DHCP** – configuration réseau automatique
- 6 **Protegus reporting mode** – l'ordre des types de liaison utilisés vers Protegus 2 (sur l'image : **Main type** : Ethernet (LAN), **Backup type** : SIM, **Backup type 2** : Disabled)

5. Si un câble LAN est raccordé au communicateur, cochez la case **DHCP** (mode d'enregistrement automatique) : le FireCom lit ainsi automatiquement les paramètres réseau (masque de sous-réseau, passerelle) et obtient une adresse IP.
6. C'est ici que vous réglez la manière dont le communicateur envoie les messages à Protegus 2. Les types de liaison se succèdent dans l'ordre : si la liaison échoue avec le type de liaison principal, le communicateur passe au suivant, et ainsi de suite. Si le message a pu parvenir à Protegus 2 par le type de liaison de secours, le communicateur réessaie le type de liaison principal après le délai configuré (**Return to Primary**).
7. Dans l'onglet **Zones settings** de la page **Zones**, cochez la case **Prot.** pour les zones dont les changements d'état doivent être notifiés aux utilisateurs dans Protegus 2 (point 6.6).
8. Dans l'onglet **Outputs** de 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 6.7).
9. Dans l'onglet **Events** de 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 6.9).

Une fois les réglages terminés, cliquez sur le bouton **Write [F5]** et débranchez le câble USB. Ajout du système dans l'application Protegus 2 : point 5.1.

Les autres réglages TrikdisConfig du FireCom sont décrits au chapitre 6.

4.2 Configuration pour le centre de télésurveillance

Dans l'onglet **System general** de la page **System Options** :

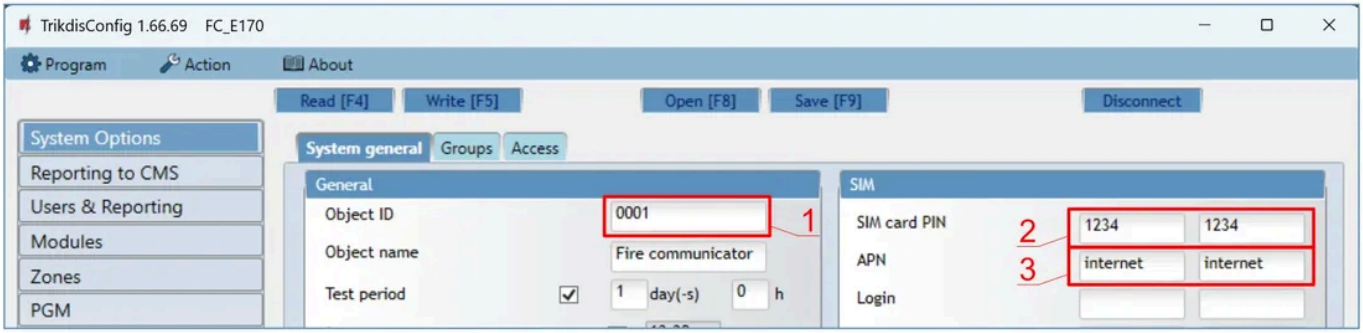


Figure 56. TrikdisConfig – **System Options**, onglet **System general**.

- 1 **Object ID** – identifiant d'objet (sur l'image : 0001)
- 2 **SIM card PIN** – le code PIN de la carte SIM
- 3 **APN** – le point d'accès de l'Internet mobile

1. Indiquez l'identifiant d'objet reçu du centre de télésurveillance (**Object ID**, numéro de client) : 4 caractères, 0–9 et A–F. N'utilisez pas les identifiants FFFE et FFFF.
2. Indiquez le code PIN de la carte SIM (**SIM card PIN**).
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.

Dans l'onglet **Settings** de la page **Reporting to CMS** :

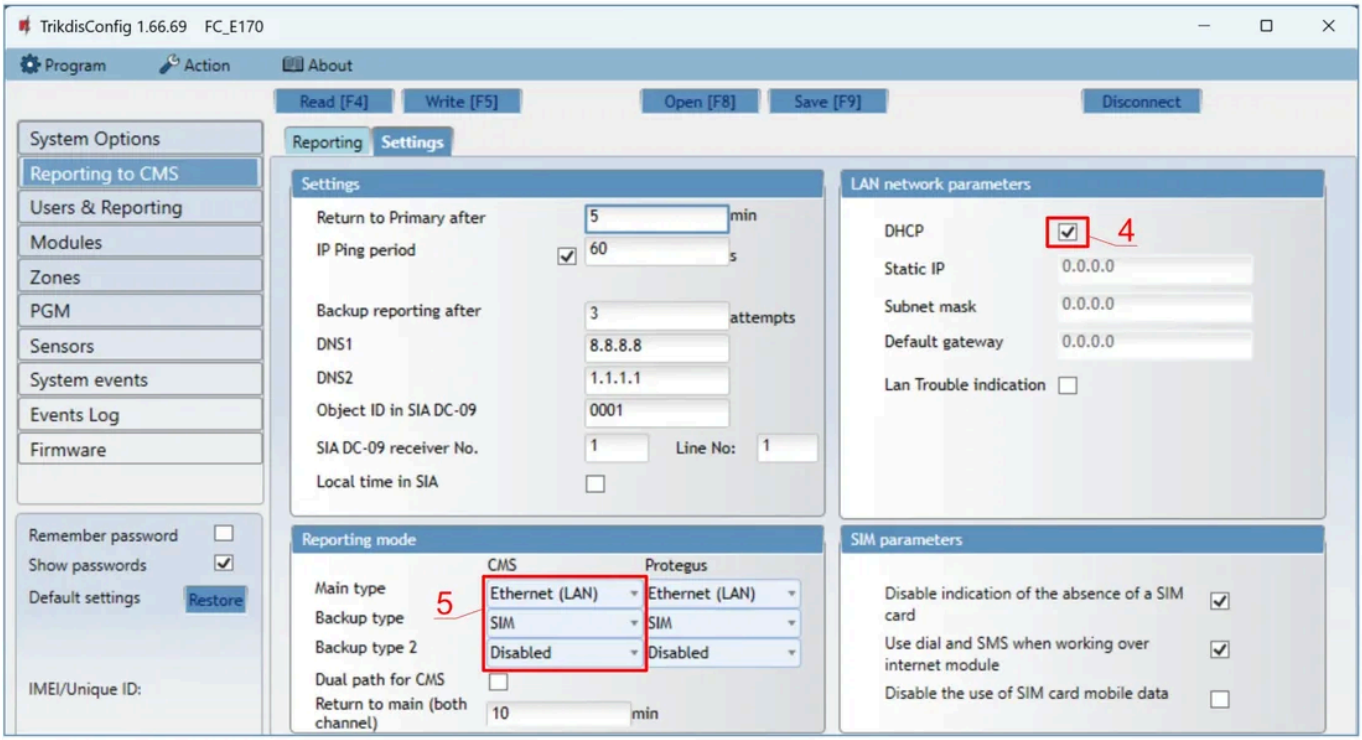


Figure 57. TrikdisConfig – **Reporting to CMS**, onglet **Settings**.

- 4 **DHCP** – configuration réseau automatique
- 5 **CMS reporting mode** – l'ordre des types de liaison utilisés vers le centre de télésurveillance (sur l'image : **Main type** : Ethernet (LAN), **Backup type** : SIM, **Backup type 2** : Disabled)

4. Si un câble LAN est raccordé au communicateur, cochez la case **DHCP** (mode d'enregistrement automatique) : le FireCom lit ainsi automatiquement les paramètres réseau (masque de sous-réseau, passerelle) et obtient une adresse IP.

5. C'est ici que vous réglez la manière dont le communicateur envoie les messages au centre de télésurveillance. Les types de liaison se succèdent dans l'ordre : si la liaison échoue avec le type de liaison principal, le communicateur passe au suivant, et ainsi de suite. Si le message a pu parvenir au centre de télésurveillance par le type de liaison de secours, le communicateur réessaie le type de liaison principal après le délai configuré (**Return to Primary**).

Dans l'onglet **Reporting** de la page **Reporting to CMS** :

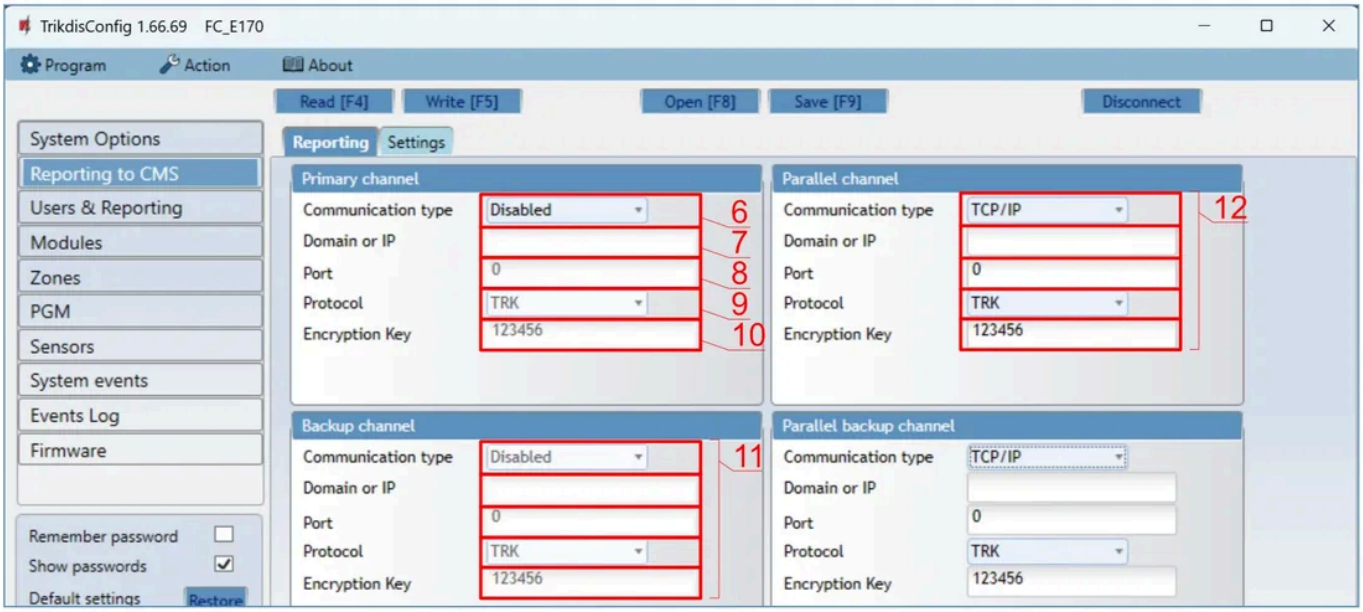


Figure 58. TrikdisConfig – **Reporting to CMS**, onglet **Reporting**.

- 6 **Communication type** – le type de liaison
- 7 **Domain or IP** – l'adresse du récepteur
- 8 **Port** – le port du récepteur
- 9 **Protocol** – protocole de transmission
- 10 **Encryption Key** – clé de chiffrement (sur l'image : 123456)
- 11 **Backup channel** – le canal de secours
- 12 **Parallel channel** – le canal parallèle (sur l'image : TCP/IP)

6. **Communication type** – sélectionnez le type de liaison (TCP ou UDP).
7. **Domain or IP** – saisissez le nom de domaine ou l'adresse IP du récepteur.
8. **Port** – saisissez le port réseau du récepteur.
9. **Protocol** – sélectionnez 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), **TL150** (pour les récepteurs Sur-Gard).
10. **Encryption Key** – saisissez la clé de chiffrement du récepteur.

Si vous choisissez DC-09 comme protocole de transmission, indiquez aussi dans le groupe **Settings** de la page **Reporting to CMS** les numéros d'objet, de ligne et de récepteur (point 6.3).

11. (Recommandé) Configurez le canal de secours (**Backup channel**).
12. Si les messages doivent aussi être envoyés à un second récepteur du centre de télésurveillance, configurez le canal parallèle (**Parallel channel**).

Une fois les réglages terminés, cliquez sur le bouton **Write [F5]** et débranchez le câble USB.

Les autres réglages TrikdisConfig du FireCom sont décrits au chapitre 6.

5. Commande à distance

Le FireCom peut être commandé 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 aussi modifier une partie des réglages.

5.1 Ajout du FireCom dans 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, lors de la création du système).

Avant d'ajouter le système

Vous pouvez ajouter le FireCom dans Protegus 2 si :

1. une carte SIM activée y est insérée, et le code PIN a été saisi ou désactivé ;
2. le service Protegus est activé (**Users & Reporting** → **Enable cloud service**, points 4.1 et 6.4 ; par SMS : `CONNECT 123456 PROTEGUS=ON`, point 5.2) ;
3. son alimentation est sous tension (le voyant **STA** clignote en vert) ;
4. il est connecté au réseau (le voyant **SIM** est vert fixe et clignote en jaune, et/ou, en cas de liaison LAN, le voyant **ETH** est allumé en vert).

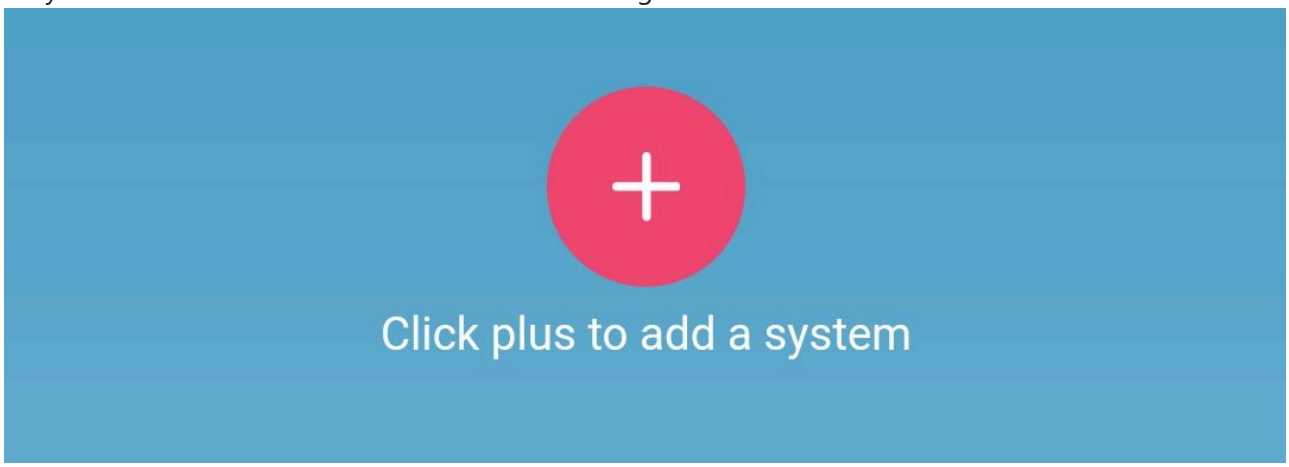
Le voyant **DAT** (sur la face avant : **DATA**) indique si les messages sont partis : s'il est éteint, tous les messages d'événement sont partis ; vert fixe, un envoi de message est en cours ; si **DAT** est jaune fixe, des messages d'événement non envoyés se trouvent en mémoire (point 1.5).

A rendszer létrehozása a Protegus 2 alkalmazásban

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



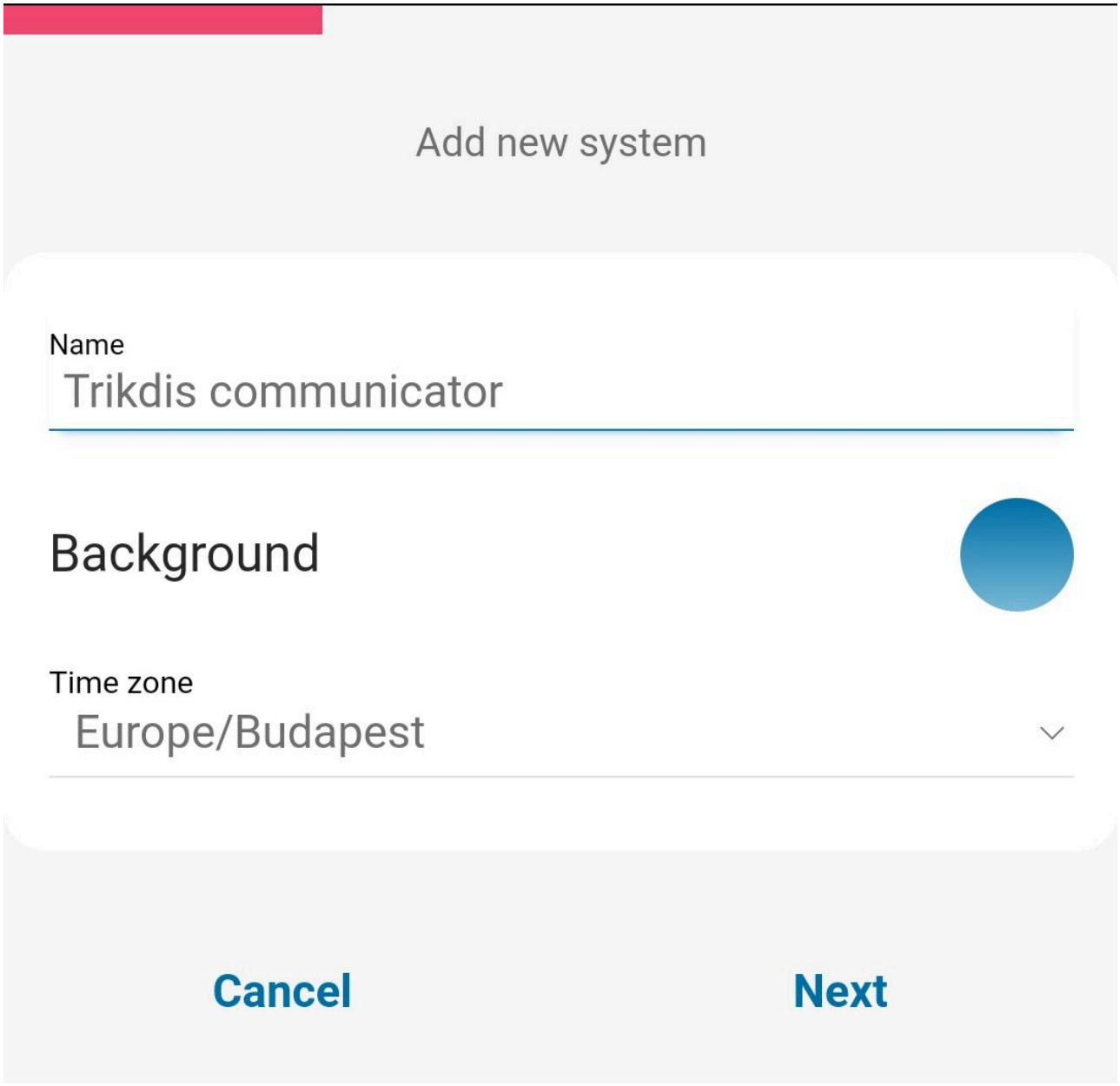
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



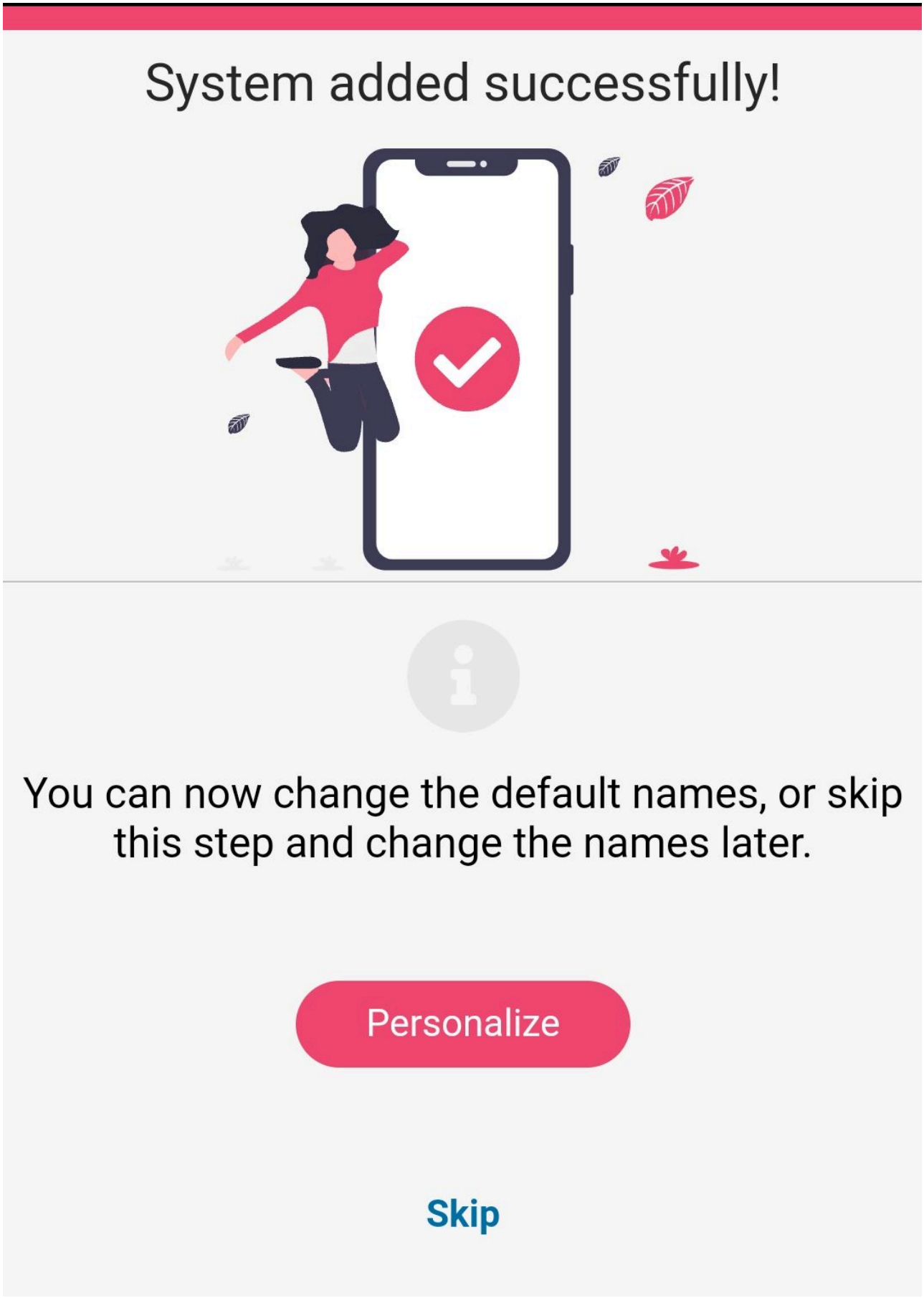
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



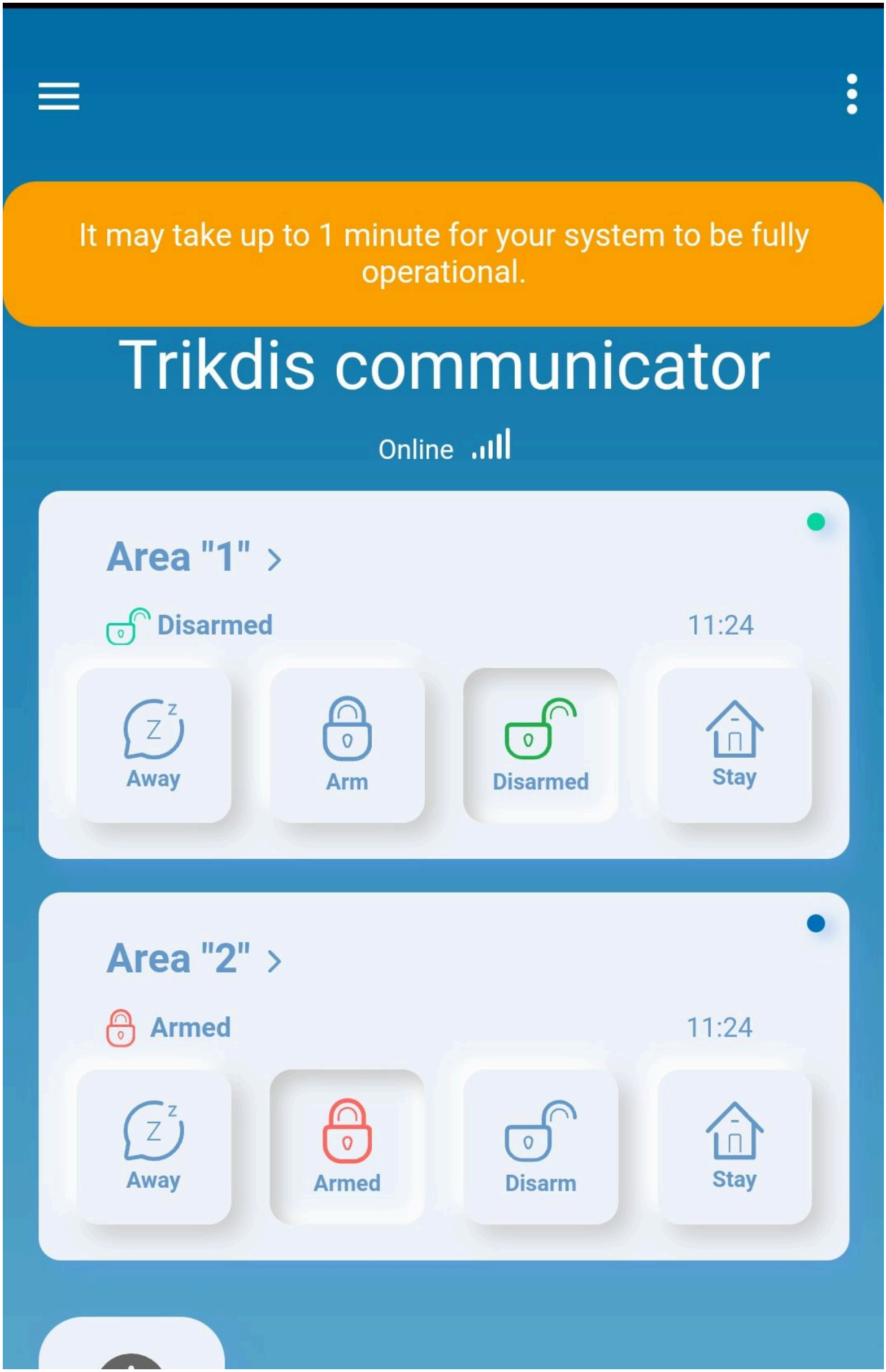
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Pour le FireCom, tenez compte de ces points lors de l'ajout :

1. Après **Créer un système** (**Add new system**), saisissez l'identifiant unique (**Unique ID**) du FireCom, puis cliquez sur le bouton **Next**. L'identifiant figure sur l'étiquette de l'appareil et de la boîte ; en liaison USB, vous le voyez aussi dans la barre d'état de TrikdisConfig (point 6.1).
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 4.1).

5.2 Configuration et commande par SMS

1. Changez 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
```

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

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

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

Partie	Signification
`xxxxxx`	le mot de passe administrateur à 6 caractères
`x`	le numéro d'ordre de l'utilisateur sur la liste (si vous indiquez 1, vous transmettez vos droits d'administrateur à l'autre utilisateur)
`PHONENR`	le numéro de téléphone de l'utilisateur
`NAME`	le nom de l'utilisateur
`EMAIL`	l'adresse e-mail de l'utilisateur

Liste des commandes SMS

Commande	Donnée	Description
`INFO`		Demande d'informations sur le communicateur : la réponse contient le nom de l'objet, l'état de la partition, le numéro IMEI, le niveau de signal du réseau mobile, la version du firmware et le numéro de série. Exemple : `INFO 123456`

Commande	Donnée	Description
`RESET`		Redémarrage de l'appareil. Exemple : `RESET 123456`
`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 de 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 2026/05/09,10:02:00`
`TXTA`	nom de l'objet	Saisie du nom de l'objet. Exemple : `TXTA 123456 House`
`RDR`	`PhoneNR#SMStext`	Transfert d'un SMS vers le numéro indiqué ; le numéro de téléphone doit commencer par le signe « + » 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`
`ASKT`		SMS avec les valeurs de tous les capteurs de température. Exemple : `ASKT 123456`
`FRS`		Réinitialisation (reset) de la sortie détecteur incendie, si la fonction **Fire sensor reset** est attribuée à la sortie OUT (point 6.7). Exemple : `FRS 123456`
`SETN`	`PhoneX=PhoneNR#Name#email`	Ajout d'un numéro de téléphone, d'un nom d'utilisateur et d'une adresse e-mail pour l'utilisateur « x » (« x » est la ligne du numéro de téléphone sur la liste). Le numéro de téléphone doit commencer par le signe « + » 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#jonas@trikdis.lt`
`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 (le nom de la commande est bien `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`

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

5.3 Commande des sorties PGM par appel téléphonique

Si vous voulez commander une sortie PGM à distance :

- L'utilisateur doit avoir le droit de commander les sorties (OUT) (point 6.4), et le type **Remote control** doit être attribué à la sortie (OUT) dans TrikdisConfig (page **PGM**, **Output definition**, point 6.7).
- Appelez le numéro de la carte SIM du FireCom. Le FireCom décroche, 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 6.7). 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 à nouveau la commande.

6. 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 FireCom par câble USB : chapitre 4 ; à distance : chapitre 7.

6.1 La barre d'état

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

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

Libellé	Signification
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 59. La barre d'état du FireCom : **Status: Ready**, **BL** 1.02, **FW** 1.07, **State: USB**, **Role: Administrator** ; à gauche, les champs **IMEI/Unique ID** et numéro de série (**SN**). Pour le FireCom, le champ **Device** doit indiquer le type **FC_xxxx** (sur l'image : FC_E170).

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

6.2 Page « System Options »

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

Onglet System general

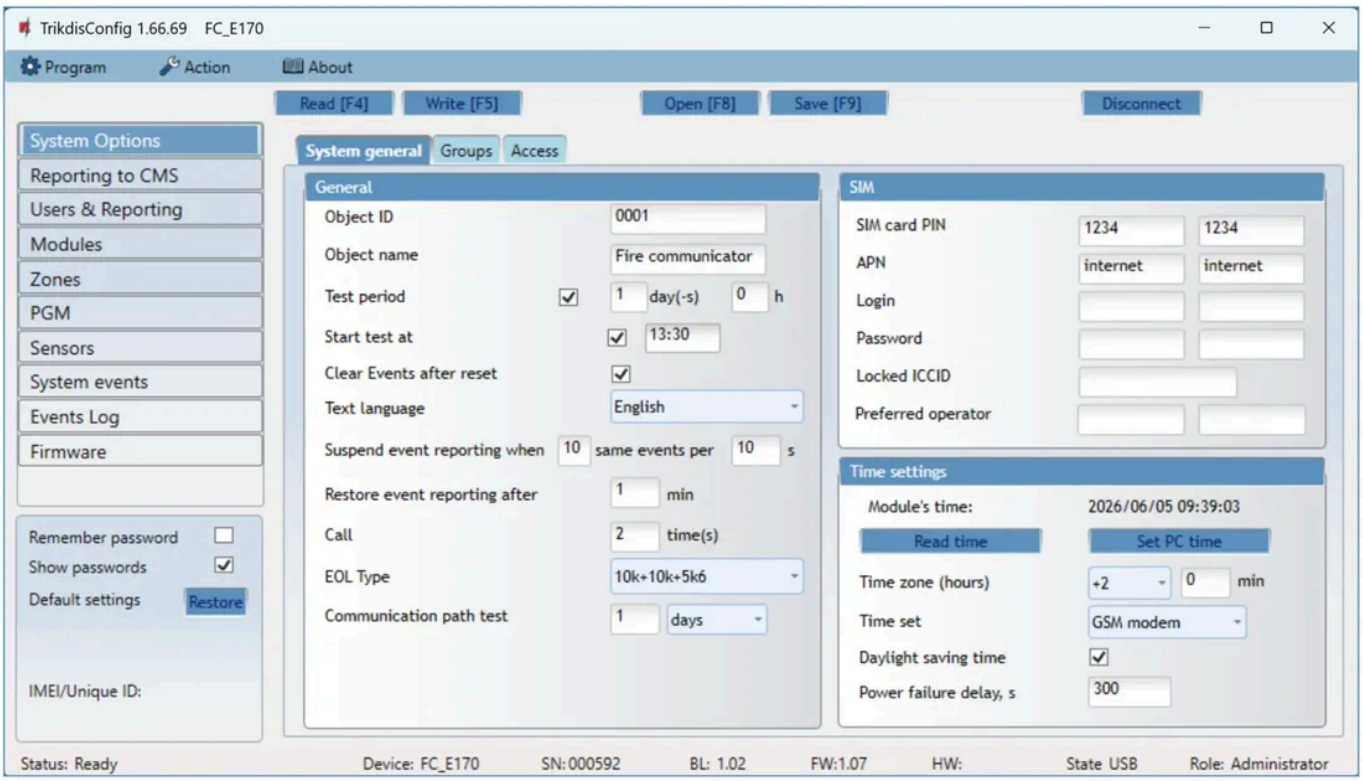


Figure 60. TrikdisConfig – **System Options**, onglet **System general** : les groupes **General**, **SIM** et **Time settings**. Sur l'image : **Object ID** 0001, **Object name** Fire communicator, **Test period** 1 jour 0 heure, **Start test at** 13:30, **Text language** English, suspension après 10 événements identiques / 10 s, rétablissement après 1 minute, **Call** 2 fois, **EOL Type** 10k+10k+5k6, **Communication path test** 1 jour ; **Time set** : GSM modem, **Daylight saving time** coché, **Power failure delay** 300 s.

Groupe General

- **Object ID** – si les événements vont au centre de télésurveillance, saisissez l'identifiant d'objet reçu du 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** – lorsque la case est cochée, le FireCom envoie un message « Test » à l'intervalle configuré.
- **Start test at** – lorsque la case est cochée, vous indiquez ici à quelle heure partent les messages de test.
- **Clear Events after reset** – lorsque la case est cochée, tous les messages d'événement non envoyés sont effacés au 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 en l'espace du 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).
- **Call** – en cas d'événement, le FireCom appelle le ou les utilisateurs ce nombre de fois. Si l'appel est rejeté ou pris, le FireCom arrête d'appeler. Un appel dure 20 secondes.
- **EOL Type** – la valeur nominale des résistances raccordées aux détecteurs (EOL – End Of Line, fin de ligne ; **RT** + **R1** + **R2** : **RT** – autoprotection, **R1** – détecteur 1, **R2** – détecteur 2). Valeurs possibles : point 3.2.
- **Communication path test** – l'intervalle au bout duquel le communicateur vérifie les canaux de communication de secours : il envoie un message au centre de télésurveillance par leur intermédiaire. Une fois les messages envoyés, le communicateur revient au canal principal.

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 l'indiquer si les messages d'événement sont envoyés à l'application Protegus 2 ou au centre de télésurveillance par la liaison de données mobile (GPRS). Les données des opérateurs français et 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.
- **Locked ICCID** – si vous souhaitez que le communicateur ne fonctionne qu'avec une carte SIM donnée, saisissez le numéro ICCID de la carte.
- **Preferred operator** – après la saisie du code de l'opérateur mobile, le communicateur ne se connecte qu'au réseau de l'opérateur choisi. Le code opérateur se compose du code MCC (code pays) et du code MNC (code réseau).

Groupe Time settings

Vous pouvez régler l'heure avec le bouton **Set PC time**. Si le champ **Time set** indique **Disabled**, le communicateur reprend l'heure de l'ordinateur. Si un modem ou un serveur est sélectionné dans le champ **Time set**, le communicateur règle son heure sur celui-ci.

- **Time zone (hours)** – le fuseau horaire du pays (France métropolitaine : +1).
- **Time set** – le serveur sur lequel se règle l'horloge interne du FireCom. La synchronisation a lieu après la mise sous tension du communicateur.

- **Daylight saving time** – lorsque la case est cochée, l'horloge interne du communicateur passe automatiquement à l'heure d'été et à l'heure d'hiver.
- **Power failure delay** – en cas de coupure de l'alimentation principale, la notification de coupure d'alimentation est envoyée après le délai indiqué. Au retour de la tension d'alimentation, la notification de rétablissement est elle aussi envoyée après le délai indiqué.

Onglet Groups



Figure 61. TrikdisConfig – **System Options**, onglet **Groups** : le tableau des groupes (sur l'image, l'identifiant 1, **Group name** : Group 1).

Les zones peuvent être attribuées à des groupes (page **Zones**, colonne **Group**, point 6.6). Le nom de chaque groupe peut être modifié ; les noms de groupe apparaissent dans Protegus 2.

Onglet Access

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

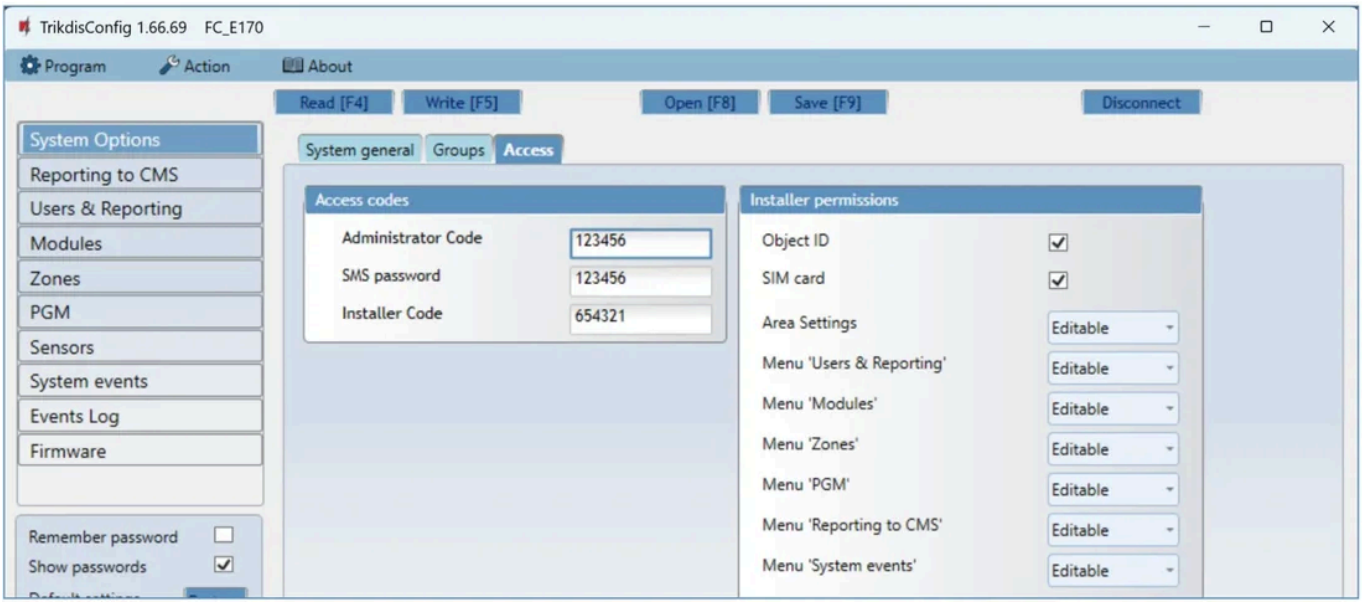


Figure 62. TrikdisConfig – **System Options**, onglet **Access** : le groupe **Access codes** avec les codes par défaut (**Administrator Code** 123456, **SMS password** 123456, **Installer Code** 654321) et le groupe **Installer permissions**. Sur l'image, l'installateur peut modifier les réglages **Object ID** et **SIM card**, et outre **Area Settings**, les pages visibles (**Users & Reporting**, **Modules**, **Zones**, **PGM**, **Reporting to CMS**, **System events**) sont aussi à l'état **Editable** (modifiable).

Groupe Access codes

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

Si le code administrateur par défaut (`123456`) est configuré, le logiciel affiche immédiatement, sans demander de code, les paramètres de fonctionnement actuels de l'appareil après un appui sur **Read [F4]**.

Groupe Installer permissions – c'est ici que l'administrateur règle les paramètres que l'installateur peut modifier.

Pour des raisons de sécurité, changez les codes par défaut. Vous pouvez aussi changer le mot de passe SMS par SMS (`PSW`, point 5.2).

6.3 Page « Reporting to CMS »

Le FireCom envoie les messages au centre de télésurveillance via Internet (IP). Un canal de secours peut être associé au canal principal : l'appareil l'utilise lorsque la liaison est interrompue sur le canal principal. La page comporte deux onglets : **Reporting** et **Settings**.

Onglet Reporting

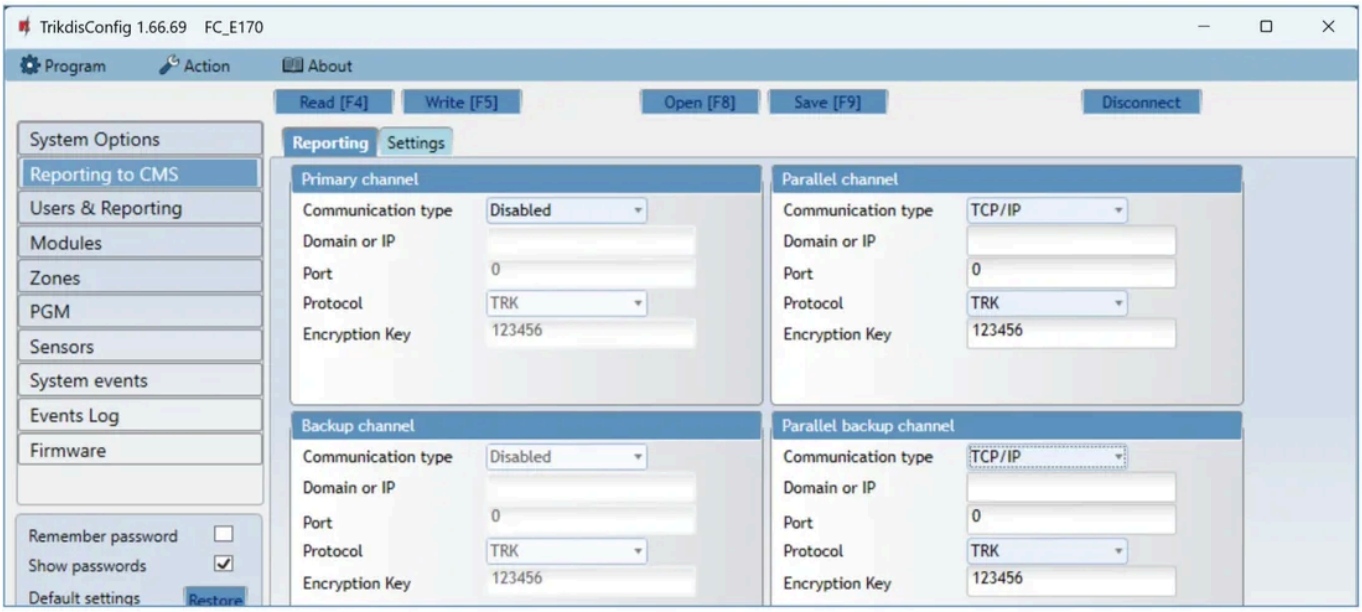


Figure 63. TrikdisConfig – **Reporting to CMS**, onglet **Reporting** : les groupes **Primary channel**, **Backup channel**, **Parallel channel** et **Parallel backup channel**. Sur l'image, le champ **Communication type** des canaux principal et de secours est sur **Disabled**, celui des canaux parallèle et parallèle de secours sur **TCP/IP** ; sur les quatre canaux, **Port** 0, **Protocol** TRK, **Encryption Key** 123456, les champs **Domain or IP** sont vides.

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, il faut un récepteur Trikdis :

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

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

Groupe Primary channel (canal principal) – et de même **Parallel channel** (canal parallèle)

- **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** – le codage avec lequel les événements sont envoyés : **TRK** (pour les récepteurs Trikdis), **DC-09_2007** ou **DC-09_2012** (pour les récepteurs universels ; en choisissant le protocole SIA DC, le format de message SIA-DCS peut aussi être sélectionné), **TL150** (pour les récepteurs Sur-Gard).
- **Encryption Key** – clé de chiffrement à 6 chiffres ; la clé de chiffrement du communicateur doit être identique à celle du récepteur.

Si vous indiquez aussi les paramètres du canal parallèle (**Parallel channel**), les messages sont envoyés simultanément sur les deux canaux. Les deux canaux ne peuvent pas être configurés vers le même récepteur.

Groupe Backup channel (canal de secours) – et de même **Parallel backup channel** (canal parallèle de secours). Activez le canal de secours pour que, en cas d'interruption de la liaison, les messages partent par le canal de secours. Ses réglages sont les mêmes que ci-dessus.

Onglet Settings

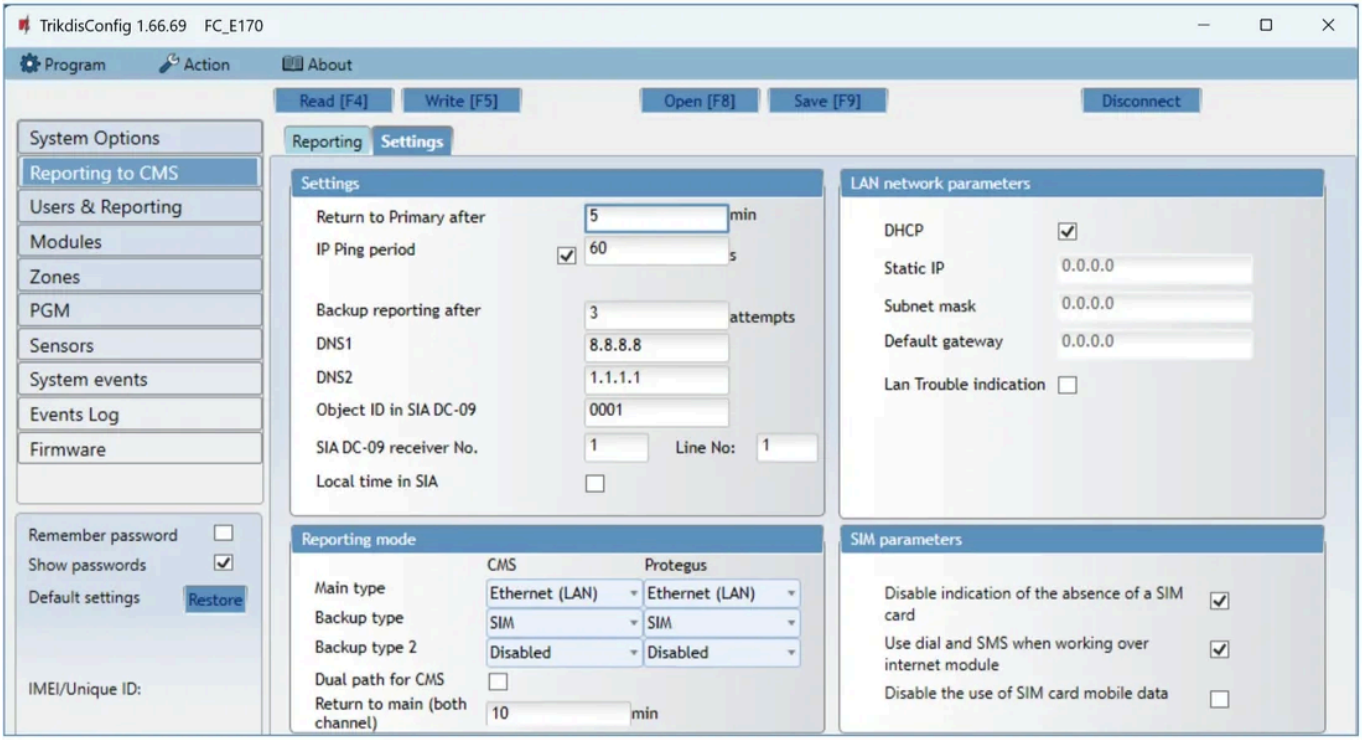


Figure 64. TrikdisConfig – **Reporting to CMS**, onglet **Settings**. Sur l'image : **Return to Primary after** 5 minutes, **IP Ping period** activé à 60 s, **Backup reporting after** 3 tentatives, **DNS1** 8.8.8.8, **DNS2** 1.1.1.1 ; **DHCP** coché ; vers le centre de télésurveillance (**CMS**) comme vers Protegus : **Main type** : Ethernet (LAN), **Backup type** : SIM, **Backup type 2** : Disabled.

Groupe Settings

- **Return to Primary after** – délai au bout duquel le FireCom tente de revenir au canal principal (**Primary channel**).
- **IP PING period** – l'intervalle d'envoi des signaux PING internes qui vérifient 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 configurée.
- **Backup reporting after** – le nombre de tentatives d'envoi infructueuses après lequel le FireCom envoie par le canal de secours (**Backup channel**) : si le message ne part toujours pas par le canal principal (**Primary channel**) après ce nombre de tentatives, l'appareil l'envoie par le canal de secours.

- **DNS1**, **DNS2** – les serveurs DNS (Domain Name System) 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 PING

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

Les champs ci-dessous n'apparaissent 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 d'objet ; avec le protocole DC-09, c'est ce numéro qui figure dans les messages. Saisissez le nombre hexadécimal de 3 à 16 caractères reçu du 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.
- **Local time in SIA** – lorsque la case est cochée, les messages envoyés au centre de télésurveillance contiennent l'heure réglée dans le module.

Groupe Reporting mode

C'est ici que vous réglez la manière dont le communicateur communique sur les canaux de télésurveillance et avec Protegus 2. Les types de liaison se succèdent dans l'ordre : si le communicateur ne peut pas se connecter avec le type de liaison **Main type**, il passe au **Backup type**, et ainsi de suite. Si le message a pu parvenir au centre de télésurveillance par le type de liaison de secours, le communicateur réessaie le type de liaison principal après le délai indiqué (**Return to main**).

- **Main type** – le type de liaison principal (SIM ou Ethernet (LAN)) vers le récepteur du centre de télésurveillance et vers Protegus 2.
- **Backup type** – le type de liaison de secours (SIM ou Ethernet (LAN)) vers le récepteur du centre de télésurveillance et vers Protegus 2.
- **Backup type 2** – le second type de liaison de secours (SIM ou Ethernet (LAN)) vers le récepteur du centre de télésurveillance et vers Protegus 2.
- **Dual path for CMS** – mode double voie : CMS1 fonctionne sur LAN, CMS2 sur SIM. Les deux canaux et voies de communication fonctionnent en parallèle.
- **Return to main (both channel)** – le nombre de minutes au bout duquel le FireCom tente de revenir au canal principal s'il fonctionnait sur un canal de secours.

Groupe LAN network parameters

- **DHCP mode** – le mode d'enregistrement sur le réseau local (LAN) (manuel ou automatique). Lorsque la case est cochée (mode d'enregistrement automatique), le FireCom lit automatiquement les paramètres réseau (masque de sous-réseau, passerelle) et obtient automatiquement 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.
- **LAN Trouble indication** – lorsque la case est cochée, le voyant du communicateur s'allume si la liaison LAN est interrompue.

Groupe SIM parameters

- **Disable indication of the absence of a SIM card** – lorsque la case est cochée, le FireCom ne signale pas l'absence de carte SIM.
- **Use dial and SMS when working over internet module** – lorsque la case est cochée, le communicateur peut aussi être commandé par appel et par SMS. Si la case n'est pas cochée et qu'un réseau LAN est présent, les SMS et les appels ne sont pas utilisés. Si la case n'est pas cochée et qu'il n'y a pas de réseau LAN, le FireCom peut toujours être commandé par appel et par SMS, et il envoie des SMS à l'utilisateur.
- **Disable the use of SIM card mobile data** – lorsque la case est cochée, le FireCom n'utilise pas la liaison de données mobile de la carte SIM : les données ne passent que par le LAN. Si le réseau LAN est temporairement indisponible, le FireCom stocke les données dans sa mémoire et les envoie par le LAN au retour de celui-ci.

6.4 Page « Users & Reporting »

Les réglages des utilisateurs, du cloud Protegus et des réponses SMS, sur trois onglets : **Users**, **Protegus** et **SMS answer texts**. Configuration des SMS et des appels concernant les événements de la centrale incendie (onglet **SMS for Panel events**) : point 3.6.

Onglet Users

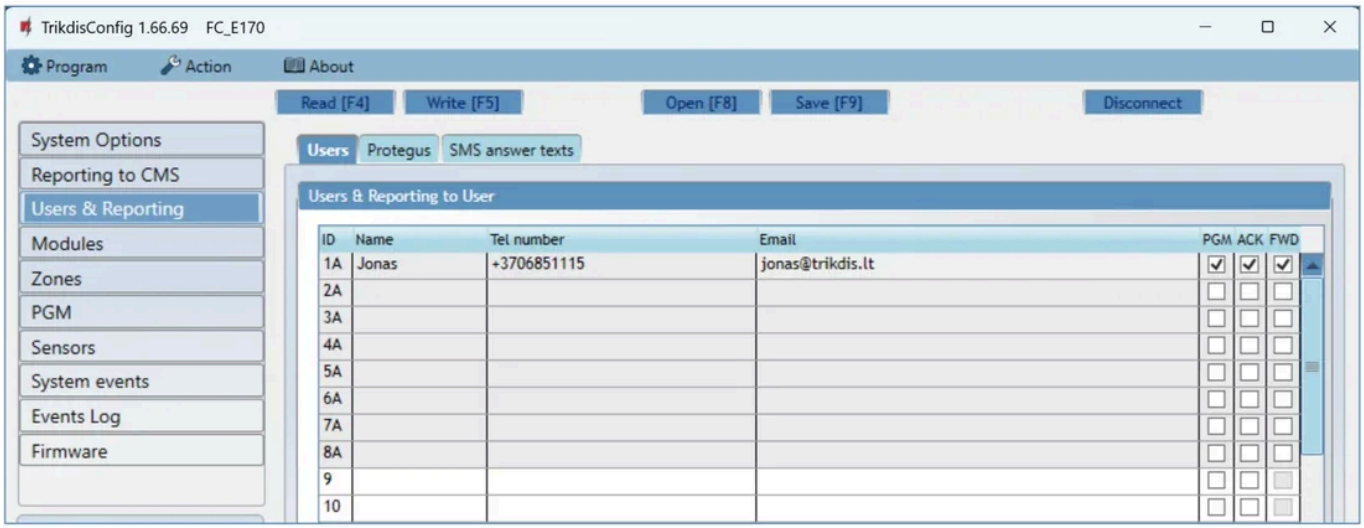


Figure 65. TrikdisConfig – **Users & Reporting**, onglet **Users**, avec des données d'exemple : dans la première ligne (1A) du tableau **Users & Reporting to User**, les champs **Name**, **Tel number** et **Email** sont remplis, les cases **PGM**, **ACK** et **FWD** sont cochées ; les autres lignes visibles sont vides.

Groupe Users & Reporting to User

- **ID** – le numéro d'ordre de l'utilisateur sur la liste.
- **Name** – le nom de l'utilisateur ; c'est ce nom qui figure dans les SMS d'événement et dans l'application.
- **Tel number** – le numéro de téléphone de l'utilisateur, auquel les SMS sont envoyés ; indiquez-le en commençant par l'indicatif international du pays (pour la France : +33…). Les 8 premiers numéros de téléphone reçoivent des messages et des appels sur les événements.
- **E-mail** – l'adresse e-mail de l'utilisateur : il y reçoit une invitation à Protegus 2 pour pouvoir commander le système.
- **PGM** – lorsque la case est cochée, l'utilisateur peut commander les sorties à distance (par appel, par SMS).

- **ACK** – lorsque la case est cochée, le FireCom envoie un SMS de réponse à l'utilisateur après chaque commande SMS reçue (le texte des réponses : onglet **SMS answer texts**).
- **FWD** – lorsque la case est cochée, le FireCom transfère à l'utilisateur les SMS provenant de numéros extérieurs au système (par exemple l'avis de solde de la carte SIM ou des messages publicitaires).

Onglet Protegus

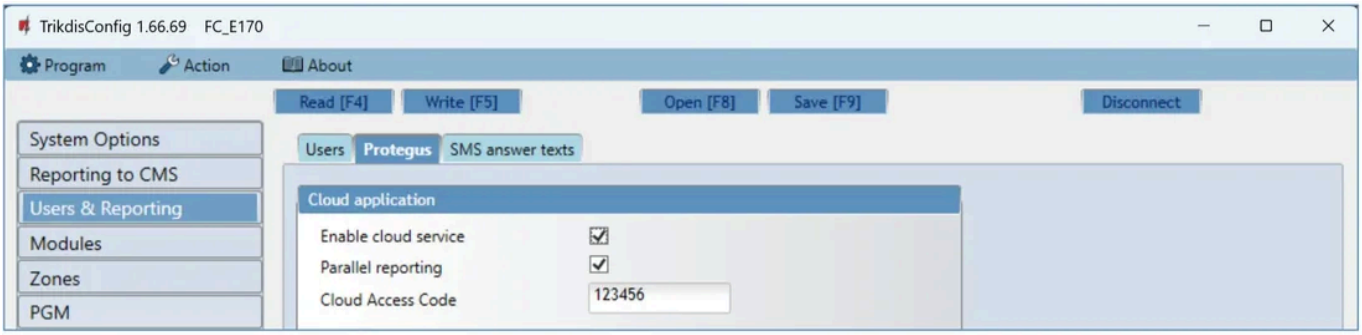


Figure 66. TrikdisConfig – **Users & Reporting**, onglet **Protegus** : dans le groupe **Cloud application**, **Enable cloud service** et **Parallel reporting** sont cochés, **Cloud Access Code** 123456.

Groupe Cloud application

- **Enable cloud service** – activation du service Protegus 2 : le FireCom échange ainsi des données avec l'application Protegus 2 et peut aussi être configuré à distance avec TrikdisConfig (chapitre 7).
- **Parallel reporting** – envoi parallèle : les messages sont envoyés simultanément par le canal principal (**Primary channel**) et à Protegus 2.
- **Cloud Access Code** – code à 6 chiffres pour l'accès à Protegus 2 (`123456` par défaut).

Onglet SMS answer texts

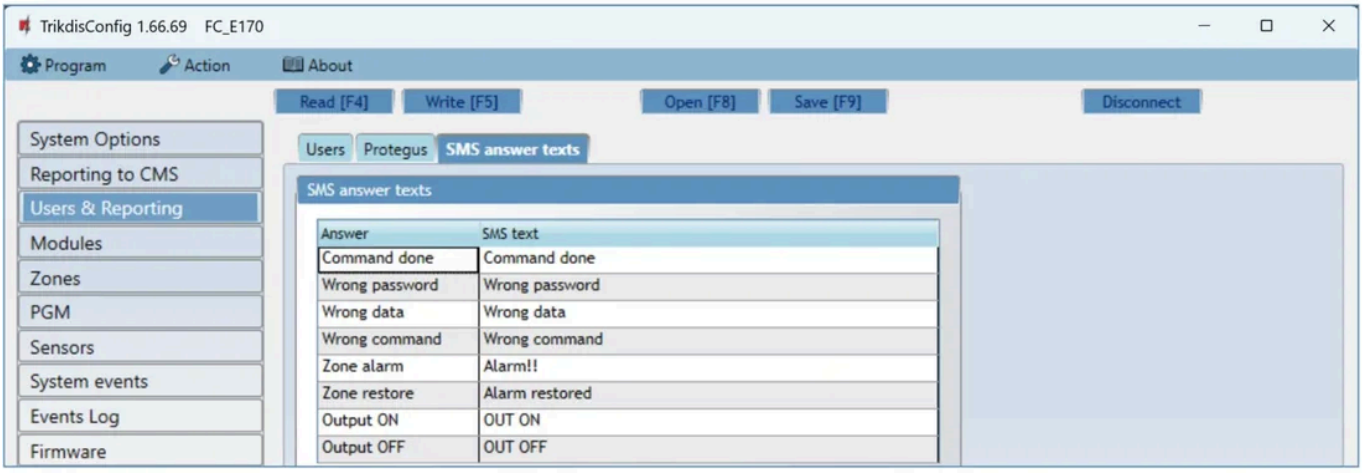


Figure 67. TrikdisConfig – **Users & Reporting**, onglet **SMS answer texts** : **Command done** (commande exécutée), **Wrong password** (mot de passe erroné), **Wrong data** (donnée erronée), **Wrong command** (commande erronée) ; en cas d'alarme de zone (**Zone alarm**) « Alarm!! », au rétablissement de la zone (**Zone restore**) « Alarm restored », à l'activation de la sortie (**Output ON**) « OUT ON », à sa désactivation (**Output OFF**) « OUT OFF ».

Dans la colonne **SMS text**, vous pouvez modifier le texte des réponses envoyées aux commandes SMS. Vous y trouvez aussi les textes des SMS envoyés lors de l'activation des entrées et des sorties.

6.5 Page « Modules »

Les réglages des modules d'extension raccordés au bus RS485 et de la centrale incendie raccordée au bus RS485 2.

Onglet RS485 modules

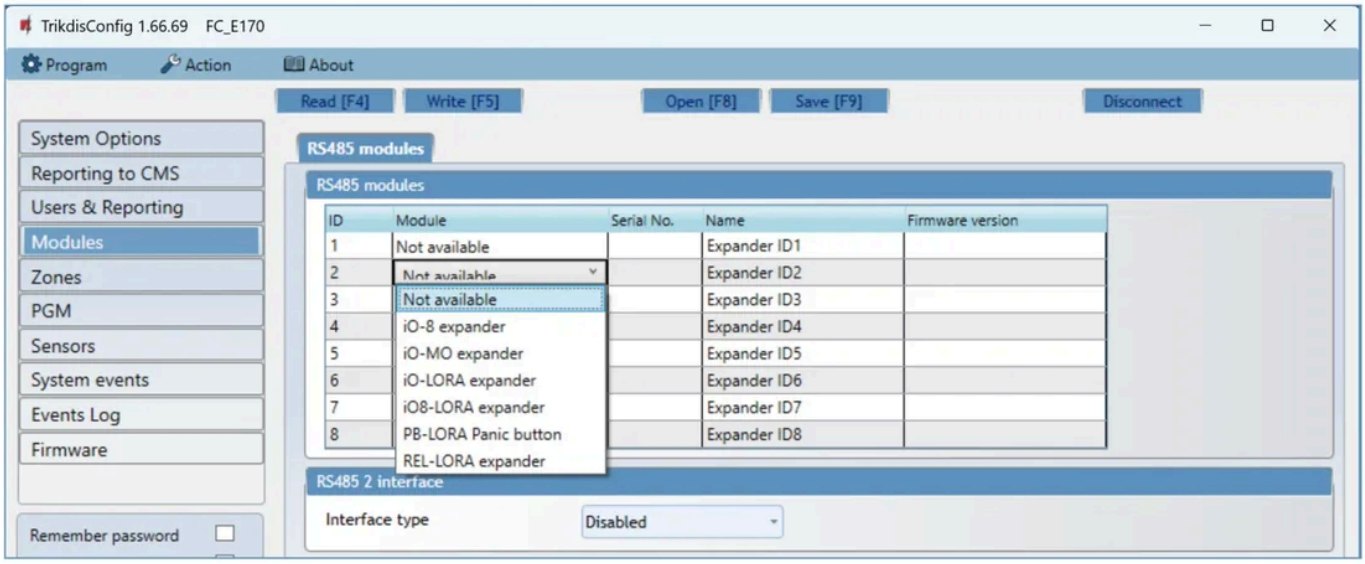


Figure 68. TrikdisConfig – **Modules**, onglet **RS485 modules** : la liste **Module** est dépliée (**Not available**, modules d'extension iO-8, iO-MO, iO-LORA et iO8-LORA, bouton panique PB-LORA, module d'extension REL-LORA) ; les colonnes du tableau : **ID**, **Module**, **Serial No.**, **Name**, **Firmware version**.

Groupe RS485 modules

- **ID** – le numéro d'ordre du module sur la liste.
- **Module** – le module utilisé, choisi dans la liste des modules : iO-8, iO-MO, iO-LORA, iO8-LORA, PB-LORA, REL-LORA (raccordement : point 3.13).
- **Serial No.** – nombre obligatoire à 6 chiffres ; il figure sur le boîtier et l'emballage du module.
- **Name** – le nom du module (libre).
- **Firmware version** – la version du firmware du module ; elle apparaît lorsque le FireCom trouve le module raccordé.

Groupe RS485 2 interface

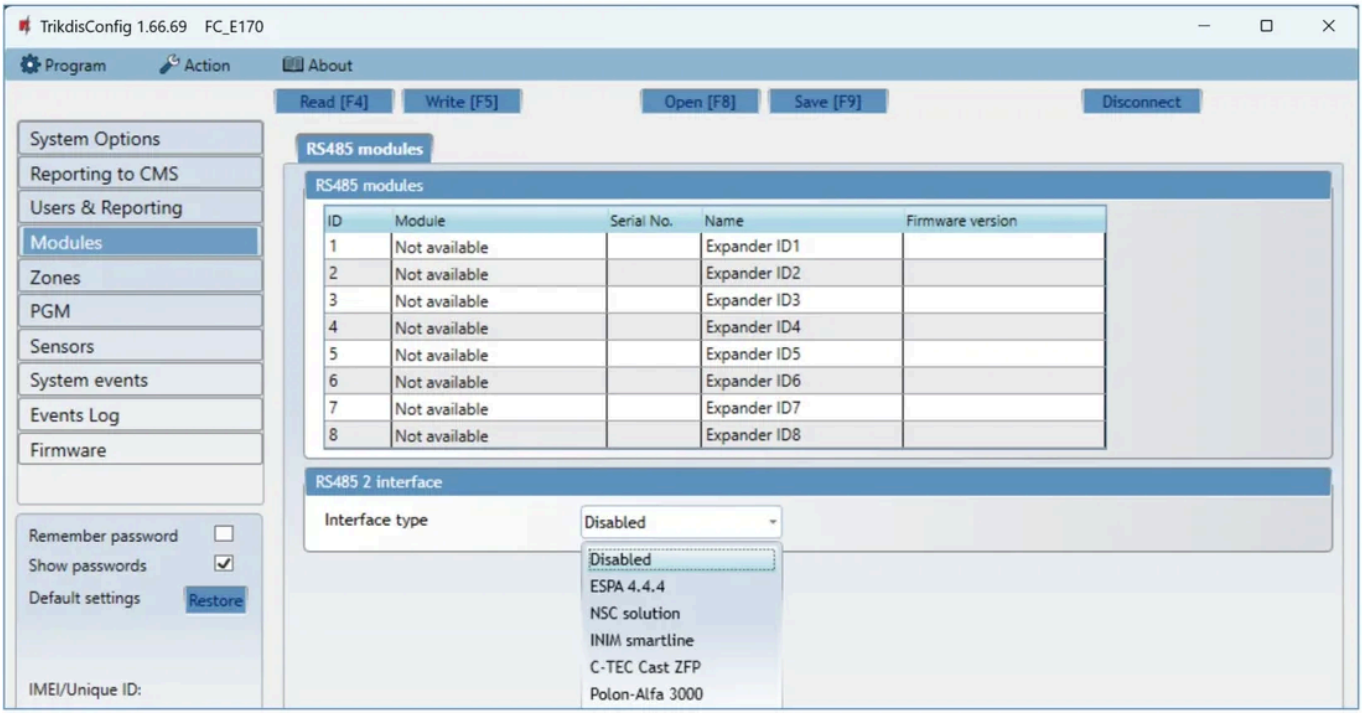


Figure 69. TrikdisConfig – **Modules**, groupe **RS485 2 interface** : la liste **Interface type** est dépliée (**Disabled**, **ESPA 4.4.4**, **NSC solution**, **INIM smartline**, **C-TEC Cast ZFP**, **Polon-Alfa 3000**).

Une centrale incendie peut être raccordée au bus RS485 2 du FireCom : utilisant le protocole ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP ou Polon-Alfa 3000. Le raccordement et la configuration des centrales sont décrits aux points 3.5–3.9.

6.6 Page « Zones »

Les réglages des zones (entrées), sur trois onglets : **Zones settings**, **SMS & Call reporting** et **Zone's codes**.

Onglet Zones settings

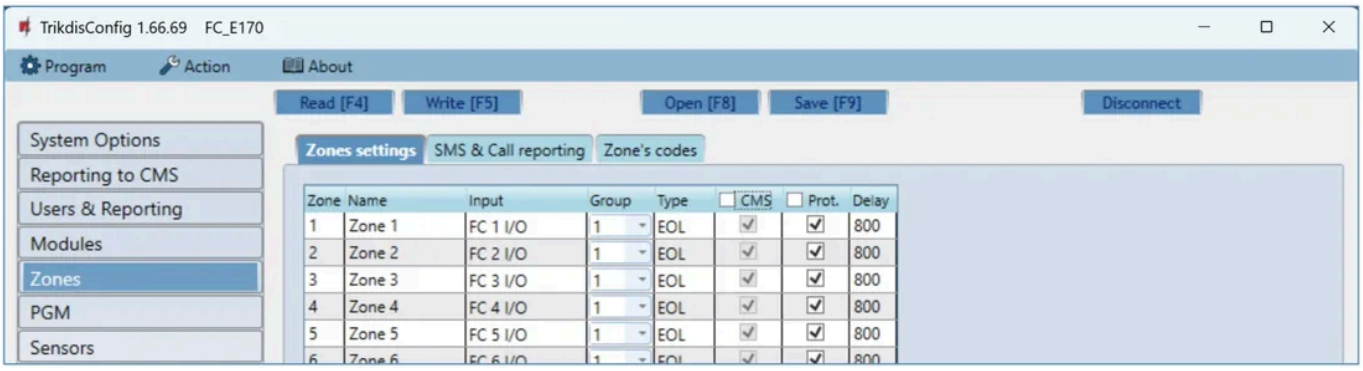


Figure 70. TrikdisConfig – **Zones**, onglet **Zones settings** : sur l'image, les zones 1 à 5 sur les entrées **FC 1 I/O** … **FC 5 I/O**, **Group 1**, type **EOL**, temporisation de 800 ms, cases **CMS** et **Prot.** cochées.

- **Zone No** – le numéro d'ordre de la zone sur la liste.
- **Name** – le nom de la zone ; c'est ce nom qui figure dans les SMS et dans l'application.
- **Input** – l'entrée (IN) du FireCom ou du module d'extension qui appartient à la zone.
- **Group** – l'attribution de la zone à un groupe (les noms de groupe : point 6.2, onglet **Groups**).
- **Type** – le type de circuit raccordé à l'entrée de la zone : **NC** – normalement fermé ; **NO** – normalement ouvert ; **EOL** – avec résistance de fin de ligne ; **EOL_T** – avec résistance de fin de ligne et surveillance d'autoprotection ; **ATZ** – circuit à deux zones normalement fermé, avec résistances de fin de ligne, sans surveillance d'autoprotection (pour l'utiliser, choisissez la seconde zone ATZ dans la liste des entrées) ;

ATZ_T – circuit à deux zones normalement fermé, avec résistances de fin de ligne et surveillance d'autoprotection (pour l'utiliser, choisissez la seconde zone ATZ dans la liste des entrées). Schémas de raccordement : point 3.2.

- **CMS** – lorsque la case est cochée, un message est envoyé au centre de télésurveillance sur les événements de la zone.
- **Prot.** – lorsque la case est cochée, une notification est envoyée à l'application Protegus 2 sur les événements de la zone.
- **Delay** – le temps de réaction de l'entrée (IN) en millisecondes.

Onglet SMS & Call reporting

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

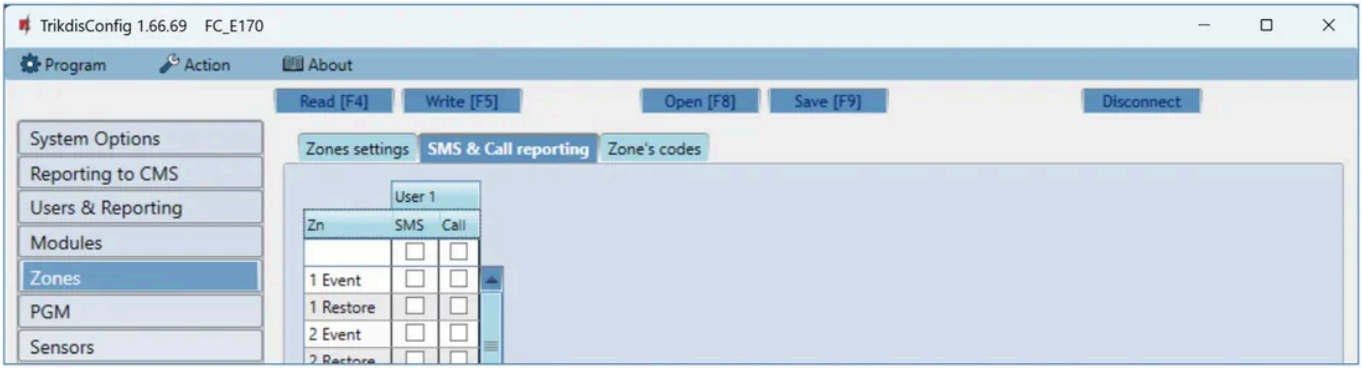


Figure 71. TrikdisConfig – **Zones**, onglet **SMS & Call reporting** : dans le tableau **User 1**, une ligne **Event** et une ligne **Restore** par zone, avec les colonnes **SMS** et **Call** (sur l'image, les cases visibles sont vides).

- **Zn** – le numéro de la zone avec le mot indicateur de l'événement : **Event** (événement) ou **Restore** (rétablissement).
- **User SMS/Call** – pour chaque événement de zone, vous pouvez choisir si l'utilisateur reçoit un SMS et/ou un appel.

Onglet Zone's codes

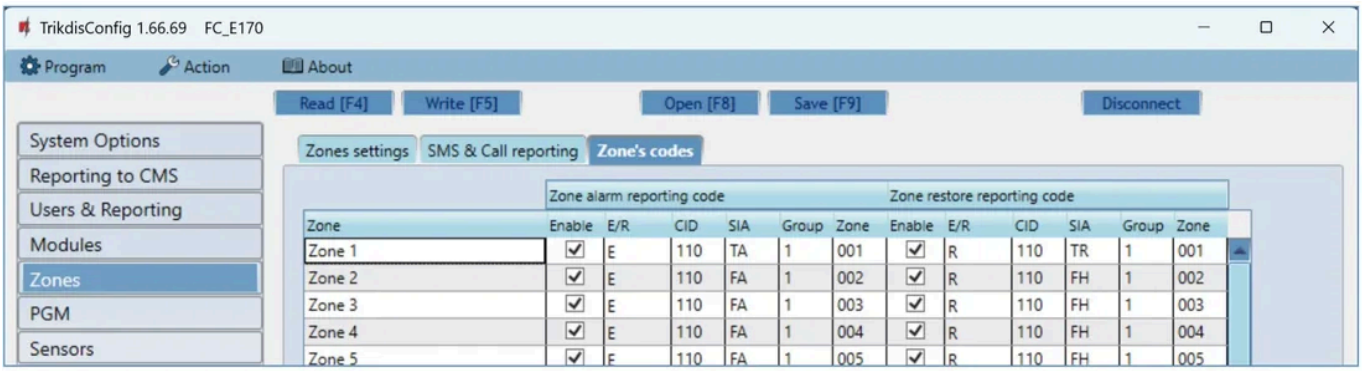


Figure 72. TrikdisConfig – **Zones**, onglet **Zone's codes** : l'alarme (**E/R** : E, **CID** 110, **SIA** TA, **Group** 1, **Zone** 001) et le rétablissement (**E/R** : R, **CID** 110, **SIA** TR) de la zone 1 sont activés ; pour les zones 2 à 5 visibles, le code SIA de l'alarme est FA, celui du rétablissement FH.

Lorsque la zone est déclenchée, le communicateur envoie un message d'événement. Un code Contact ID (SIA) est associé à l'entrée ; c'est lui qui est envoyé au centre de télésurveillance et à Protegus 2.

- **Enable** – les champs d'événement cochés donnent lieu à un message vers le centre de télésurveillance et vers Protegus 2.

- **E/R** – le type d'événement envoyé à l'activation de l'entrée : **Event** (E, événement) ou **Restore** (R, rétablissement).
- **CID** – le code d'événement ; saisissez-le ou laissez la valeur par défaut.
- **SIA** – les codes d'événement SIA.
- **Group** – le numéro de groupe envoyé lorsque l'événement se produit.
- **Zone** – le numéro de zone envoyé lorsque l'événement se produit.

6.7 Page « PGM »

Les réglages des sorties PGM, sur quatre onglets : **Outputs**, **Set Action**, **Scheduler** et **SMS & Call reporting**.

Onglet Outputs

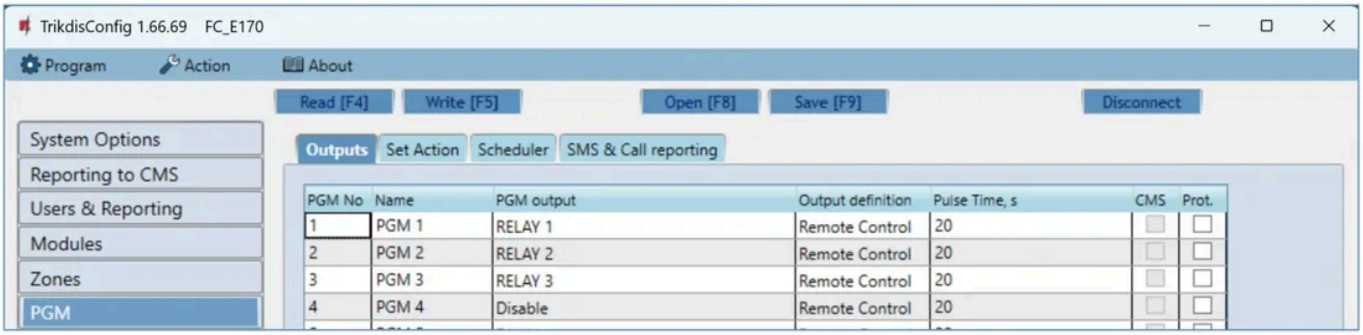


Figure 73. TrikdisConfig – **PGM**, onglet **Outputs** : PGM 1, 2 et 3 sur les sorties **RELAY 1**, **2** et **3**, PGM 4 désactivée (**Disable**) ; sur les quatre lignes visibles, définition de sortie **Remote Control** et durée d'impulsion de 20 s, cases **CMS** et **Prot.** vides.

- **PGM No** – le numéro d'ordre de la sortie PGM sur la liste.
- **Name** – le nom de la sortie PGM.
- **PGM output** – la sortie (OUT) attribuée à la PGM : celle du FireCom ou d'un appareil externe.
- **Output definition** – le mode de fonctionnement de la sortie (OUT) (sur l'image : **Remote Control**).
- **Pulse time, s** – la durée d'activation de la sortie (OUT), 0–9999 secondes.
- **CMS** – lorsque la case est cochée, un message est envoyé au centre de télésurveillance sur les événements sélectionnés.
- **Prot.** – lorsque la case est cochée, une notification est envoyée à l'application Protegus 2 sur les événements de la sortie.

Onglet Set Action

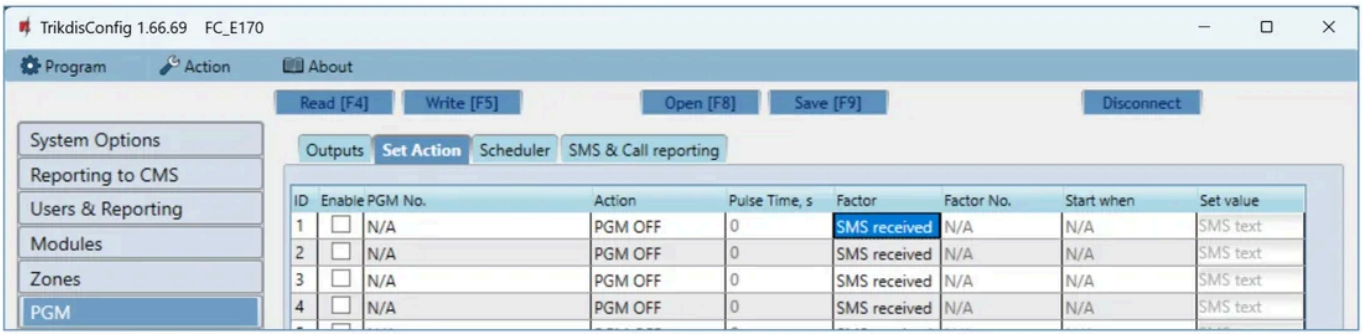


Figure 74. TrikdisConfig – **PGM**, onglet **Set Action** : sur les lignes visibles, la case **Enable** est vide, **PGM No.** : N/A, **Action** : PGM OFF, **Pulse Time** 0 s, **Factor** : SMS received, **Factor No.** et **Start when** : N/A, **Set value** : SMS text.

- **ID** – le numéro d'ordre de la sortie sur la liste.
- **Enable** – activation de l'algorithme de fonctionnement PGM.

- **PGM No.** – la sortie (OUT) que le communicateur commande lorsque survient l'événement décrit dans les colonnes **Factor**, **Factor No.**, **Start when** et **Set value**.
- **Action** – l'action :
  - **PGM OFF** – état de la sortie (OUT) : désactivée (« Off »).
  - **PGM ON** – état de la sortie (OUT) : activée (« On »).
  - **Pulse OFF** – l'état initial de la sortie (OUT) est activé (« On ») ; après la commande, elle se désactive (« Off ») pendant la durée d'impulsion (**Pulse time**), puis revient automatiquement à l'état initial activé.
  - **Pulse ON** – l'état initial de la sortie (OUT) est désactivé (« Off ») ; après la commande, elle s'active (« On ») pendant la durée d'impulsion (**Pulse time**), puis revient automatiquement à l'état initial désactivé.
- **Pulse time, s** – la durée d'impulsion, 0–9999 secondes.
- **Factor** / **Factor No.** – l'événement qui active la sortie (OUT) : zone (**Zone**), réception d'un SMS (**SMS received**) ou autoprotection de zone (**Zone tamper**).
- **Start when** – condition supplémentaire pour l'activation de la sortie (OUT), selon l'événement **Factor**.
- **Set value** – selon la condition choisie dans la colonne **Factor**, vous pouvez indiquer ici une valeur (le texte du SMS reçu). Lorsque le communicateur reconnaît cette valeur, il exécute l'action choisie dans la colonne **Action**. Vous pouvez structurer le texte du SMS avec des signes % : les signes % isolent, dans l'ensemble du SMS reçu, le mot-clé qui change l'état de la sortie.

Modèle	Signification	Exemple
`%…..%`	une partie du texte du SMS reçu doit correspondre au texte écrit entre les signes %	`%hoUSe%` – le SMS doit contenir le texte « hoUSe » ; par exemple `VacationhoUSe25864`
`…..%`	le début du SMS reçu doit correspondre au texte écrit jusqu'au signe %	`hoUSe%` – le SMS doit commencer par le texte « hoUSe » ; par exemple `hoUSeddss`
`%…..`	la fin du SMS reçu doit correspondre au texte écrit après le signe %	`%hoUSe` – le SMS doit se terminer par le texte « hoUSe » ; par exemple `1144hoUSe`

Dans le texte du SMS, les majuscules et les minuscules comptent.

Onglet Scheduler

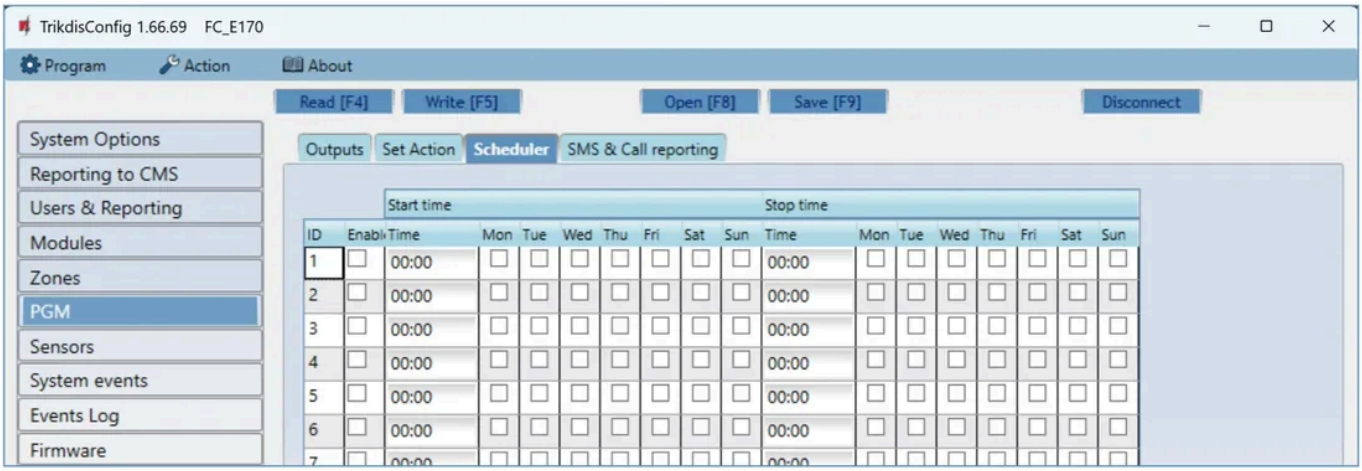


Figure 75. TrikdisConfig – **PGM**, onglet **Scheduler** : les champs **Start time** et **Stop time** du tableau de programmation horaire, chacun avec des cases du lundi au dimanche (sur l'image : 00:00 et cases vides).

- **ID** – le numéro d'ordre de la programmation horaire sur la liste.
- **Enable** – activation de la programmation horaire.

- **Start time** – le moment où la sortie (OUT) s'active – début de la programmation horaire.
- **Stop time** – le moment où la sortie (OUT) se désactive – fin de la programmation horaire.
- **Mon – Sun** – les jours de la semaine où la sortie (OUT) doit s'activer ou se désactiver.

Onglet SMS & Call reporting

Cet onglet n'apparaît que si vous avez indiqué au moins un numéro de téléphone d'utilisateur sur la page **Users & Reporting**. Ces réglages ne peuvent concerner que les 8 premiers utilisateurs.

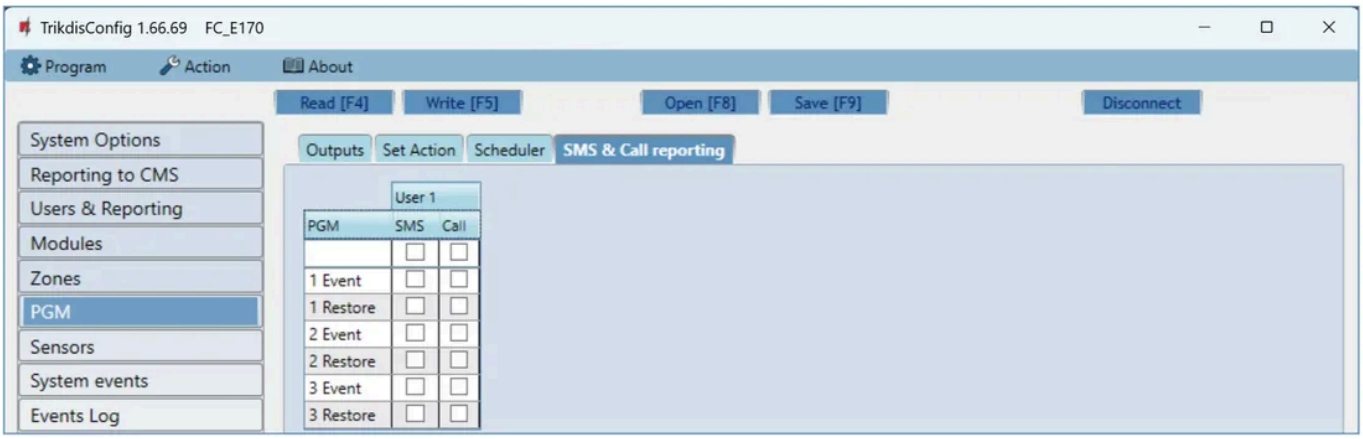


Figure 76. TrikdisConfig – **PGM**, onglet **SMS & Call reporting** : les lignes **Event** et **Restore** des PGM 1, 2 et 3, avec des cases **SMS** et **Call** vides dans la colonne **User 1**.

- **PGM** – le numéro de la sortie (OUT) et le type d'événement : **Event** – activation de la sortie ; **Restore** – désactivation de la sortie.
- **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).

6.8 Page « Sensors »

Les réglages des capteurs de température (raccordement : point 3.10).

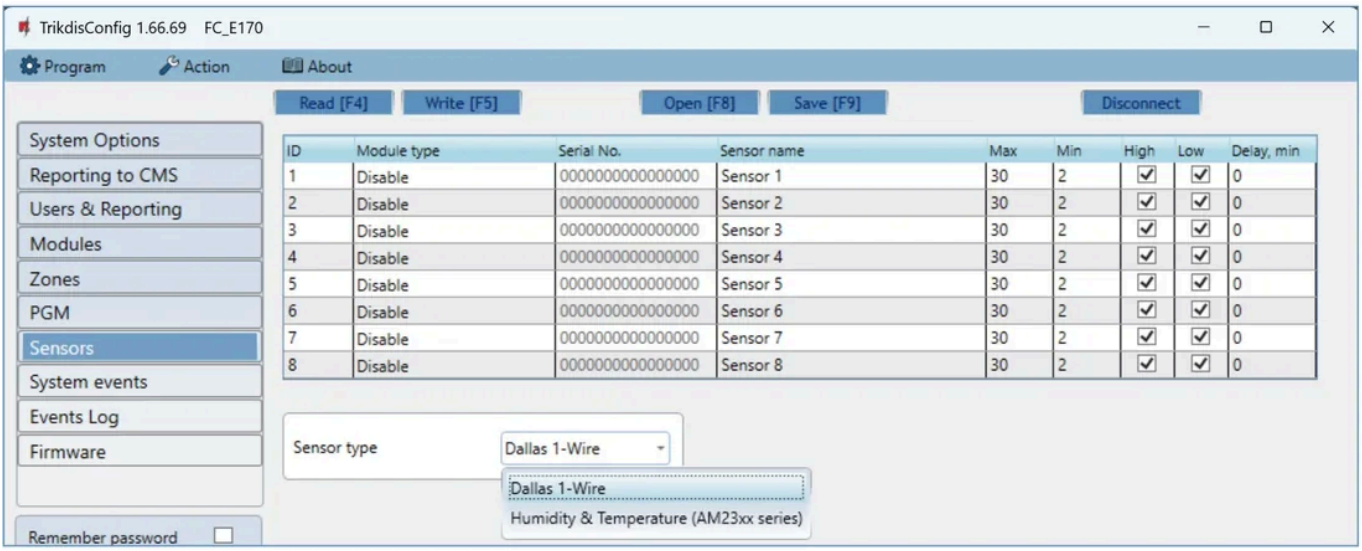


Figure 77. TrikdisConfig – **Sensors** : huit lignes de capteurs (**Module type** : Disable, **Sensor 1** … **Sensor 8**, **Max** 30, **Min** 2, **High** et **Low** cochés, **Delay** 0 minute) ; la liste **Sensor type** est dépliée : **Dallas 1-Wire** et **Humidity & Temperature (AM23xx series)**.

- **ID** – le numéro d'ordre du capteur de température sur la liste.
- **Module type** – le capteur de température attribué à la ligne (ID).

- **Serial No.** – le numéro de série du capteur ; il est lu par le communicateur.
- **Sensor name** – le nom du capteur.
- **Max** – si la température est supérieure à cette valeur, un message d'événement est généré ; pour cela, la case **High** doit être cochée.
- **Min** – si la température est inférieure à cette valeur, un message d'événement est généré ; pour cela, la case **Low** doit être cochée.
- **Delay** – l'événement est envoyé si la valeur mesurée par le capteur dépasse la valeur **Max** ou **Min** pendant la durée configurée. Indiquez la durée en minutes.
- **Sensor type** – le type du capteur de température raccordé : **Dallas 1Wire** – 8 capteurs de ce type au maximum peuvent être raccordés, et le communicateur les attribue automatiquement ; **Humidity & Temperature** – un capteur de température et d'humidité AM2301 peut être raccordé ; si vous l'utilisez, il doit être attribué manuellement dans la colonne **Module type**.

6.9 Page « System events »

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

Onglet Events

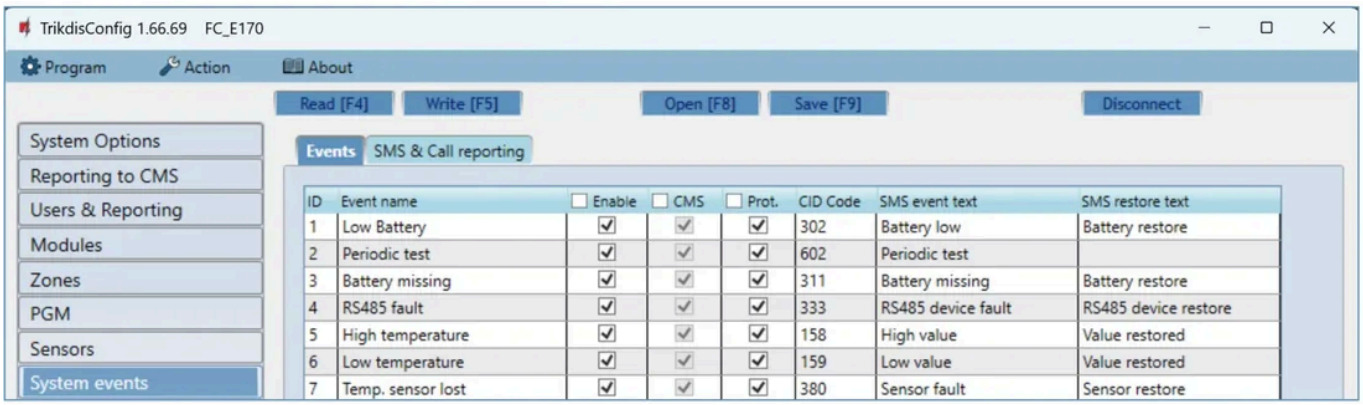


Figure 78. TrikdisConfig – **System events**, onglet **Events** : tension de batterie basse (**Low Battery**, CID 302), test périodique (**Periodic test**, 602), batterie absente (**Battery missing**, 311), défaut RS485 (**RS485 fault**, 333), température haute (**High temperature**, 158), température basse (**Low temperature**, 159) et capteur de température perdu (**Temp. sensor lost**, 380), avec les cases **Enable**, **CMS** et **Prot.** cochées ; à côté, les champs des textes SMS d'événement et de rétablissement.

- **ID** – le numéro d'ordre de l'événement sur la liste.
- **Event name** – le nom de l'événement.
- **Enable** – activation de la surveillance de l'événement.
- **CMS** – un message est envoyé au centre de télésurveillance sur les événements sélectionnés.
- **Prot.** – une notification est envoyée à l'application Protegus 2 sur les événements sélectionnés.
- **CID Code** – le code Contact ID de l'événement.
- **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 indiqué au moins un numéro de téléphone d'utilisateur sur la page **Users & Reporting**.

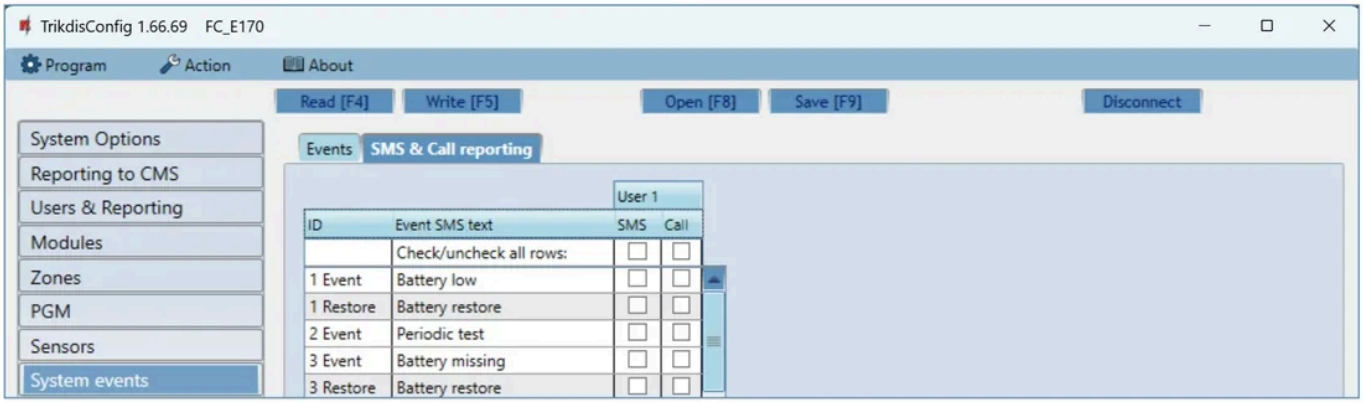


Figure 79. TrikdisConfig – **System events**, onglet **SMS & Call reporting** : dans la colonne **Event SMS text**, par exemple Battery low, Battery restore, Periodic test, Battery missing ; dans la colonne **User 1**, des cases **SMS** et **Call** vides.

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

6.10 Page « Events Log »

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

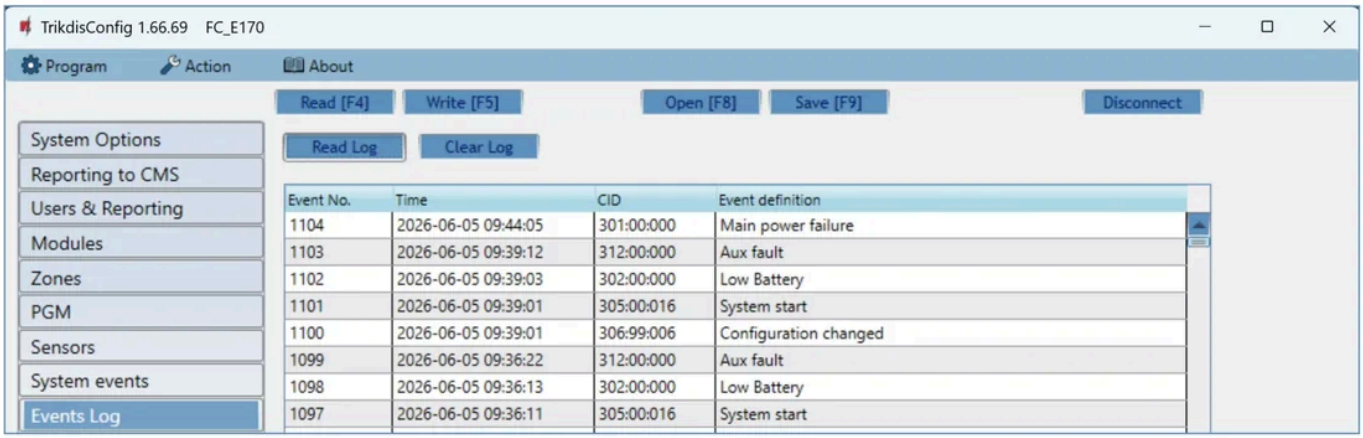


Figure 80. TrikdisConfig – **Events Log** : les boutons **Read Log** et **Clear Log** ; dans le tableau, le numéro d'ordre (**Event No.**), l'heure (**Time**), le code **CID** et la description (**Event definition**) de l'événement – sur l'image, la première entrée est la coupure de l'alimentation principale (**Main power failure**, CID 301:00:000).

- **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 au maximum 1000 événements enregistrés dans la mémoire du FireCom.

6.11 Retour aux réglages d'usine

Pour rétablir les réglages d'usine du FireCom, cliquez sur le bouton **Restore** de TrikdisConfig.

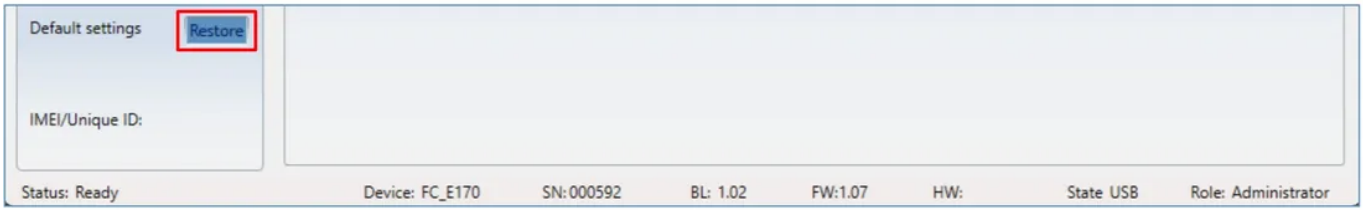


Figure 81. TrikdisConfig – la partie réglages d'usine (**Default settings**), le bouton **Restore** encadré en rouge ; dans la barre d'état, **Ready**, **State: USB**, **Role: Administrator**.

Si vous risquez d'avoir encore besoin des réglages actuels, enregistrez-les dans un fichier avec le bouton **Save [F9]** avant le retour aux réglages d'usine (point 6.1).

7. Programmation à distance

Vous pouvez aussi lire et modifier à distance les réglages du FireCom avec TrikdisConfig via le cloud Protegus – sans vous déplacer sur le site.

Conditions de la programmation à distance

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

1. une carte SIM activée est insérée, et le code PIN a été saisi ou désactivé ;
2. le service Protegus est activé (**Users & Reporting** → **Enable cloud service**, point 6.4) ;
3. son alimentation est sous tension (le voyant **STA** clignote en vert) ;
4. il est connecté au réseau (le voyant **SIM** est vert fixe et clignote en jaune, et/ou, en cas de liaison LAN, le voyant **ETH** est allumé en vert).

Si le voyant **SIM** ou **DAT** est jaune fixe, l'appareil ne parvient pas à se connecter au réseau mobile et/ou à Protegus 2.

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

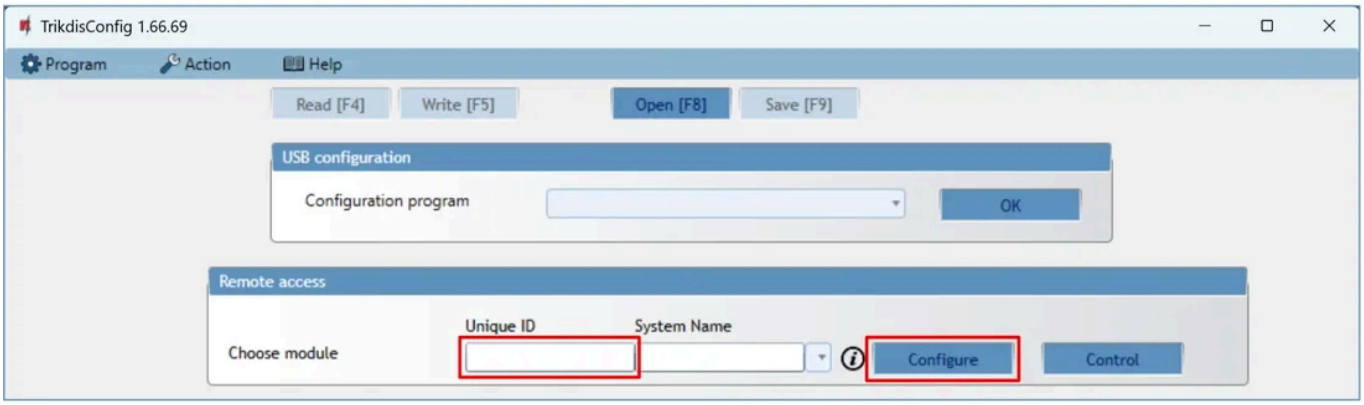


Figure 82. TrikdisConfig – la partie **Remote access** de la fenêtre d'accueil : encadrés en rouge, le champ **Unique ID** vide et le bouton **Configure** ; à côté, le champ **System Name** et le bouton **Control**.

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 installateur.
6. Une fois les réglages terminés, cliquez sur le bouton **Write [F5]**. Lorsque vous avez terminé avec TrikdisConfig, cliquez sur le bouton **Disconnect**.

8. Vérification du fonctionnement

Une fois la configuration et l'installation terminées, testez entièrement le système :

1. Pour vérifier une entrée, activez-la (déclenchez-la). Vérifiez que l'événement est bien 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 bien 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.

Le voyant **DAT** (sur la face avant : **DATA**) indique si les messages sont partis : s'il est éteint, tous les messages d'événement sont partis ; vert fixe, un envoi de message est en cours ; si **DAT** est jaune fixe, des messages d'événement non envoyés se trouvent en mémoire (point 1.5).

Vous pouvez aussi demander par SMS les informations du communicateur, l'état des entrées et des sorties et les valeurs des capteurs de température : `INFO 123456`, `ASKI 123456`, `ASKO 123456`, `ASKT 123456` (remplacez `123456` par votre propre mot de passe SMS ; point 5.2).

9. Mise à jour du firmware

Lorsque vous raccordez le FireCom à TrikdisConfig et qu'un firmware plus récent existe, le logiciel propose de lui-même la mise à jour – pour cela, l'ordinateur doit être connecté à Internet. L'antivirus, le pare-feu ou des réglages d'accès à Internet stricts peuvent bloquer la mise à jour automatique ; dans ce cas, vous devez modifier les réglages de l'antivirus.

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.

Raccordez le FireCom à l'ordinateur avec un câble **USB Type-C**, ou connectez-vous à distance (chapitre 7).

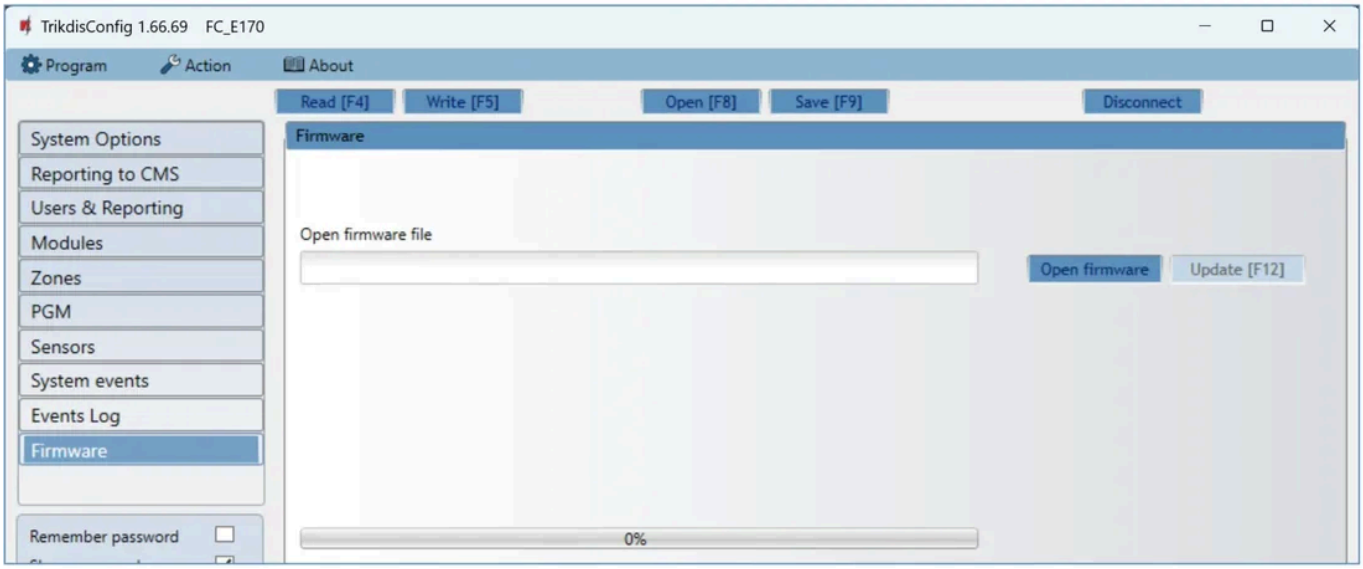


Figure 83. TrikdisConfig – FireCom, page **Firmware** : le champ **Open firmware file**, le bouton **Open firmware**, le bouton **Update [F12]** et l'indicateur de progression.

10. Dépannage et questions fréquentes

Si le communicateur ne fait pas ce que vous attendez, regardez d'abord les voyants (point 1.5), puis les points ci-dessous.

Le voyant STA (sur la face avant : TROUBLE) clignote en rouge – que signifie le nombre de clignotements ?

Le nombre de clignotements indique la cause du défaut : **1** – aucune carte SIM insérée ; **2** – le code PIN de la carte SIM est erroné (**System Options** → **SIM card PIN**, point 6.2) ; **3** – impossible de se connecter au réseau mobile ; **4** – impossible de se connecter au récepteur IP sur le canal principal (**Reporting to CMS**, point 6.3) ; **5** – impossible de se connecter au récepteur IP sur le canal de secours ; **6** – pas de tension d'alimentation DC (point 2.1) ; **7** – défaut de la sortie AUX (surintensité ou surtension) ; **8** – défaut batterie (point 2.2) ; **9** – le câble LAN n'est pas branché ; **10** – erreur DHCP sur le réseau local (**LAN network parameters**, point 6.3).

Le voyant FPS (sur la face avant : POWER) clignote en vert – quel est le problème ?

1 clignotement vert : pas de tension secteur (AC). **2** clignotements verts : la tension de l'alimentation de secours (batterie) est insuffisante (point 2.2). Si le voyant est vert fixe, l'alimentation ne présente aucun problème (point 1.5).

Combien de clignotements jaunes faut-il sur le voyant SIM ?

Le nombre de clignotements jaunes indique le niveau de signal du réseau mobile : sur le réseau 4G, 3 clignotements suffisent déjà. Si vous comptez moins de clignotements jaunes, le niveau de signal est insuffisant : choisissez un autre emplacement pour le communicateur, déplacez l'antenne ou utilisez une antenne mobile plus sensible (points 1.6 et 3.14). Si aucun voyant du FireCom ne s'allume, vérifiez l'alimentation et le raccordement.

Le voyant ETH clignote en vert

Le câble LAN n'est pas branché, ou il y a une erreur DHCP (point 1.5). Vérifiez le câble et le routeur. En attribution automatique des adresses, **DHCP mode** doit être coché ; en configuration manuelle, renseignez les champs **Static IP**, **Subnet mask** et **Default gateway** (**Reporting to CMS → Settings**, **LAN network parameters**, point 6.3). Ce que le réseau doit permettre : point 3.1.

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 6.4), voyant **STA** clignotant en vert, ainsi que voyant **SIM** vert fixe clignotant en jaune et/ou voyant **ETH** vert (point 5.1).
- Si le voyant **SIM** ou **DAT** est jaune fixe, l'appareil ne parvient pas à se connecter au réseau mobile et/ou à Protegus 2 (chapitre 7). Vérifiez le réglage de l'**APN** (point 6.2).
- Si le **Cloud Access Code** n'est pas la valeur par défaut `123456`, saisissez le bon code lors de l'ajout (point 4.1).

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

- La commande par SMS et par appel n'est possible que depuis les numéros de téléphone figurant sur la liste des utilisateurs (point 5.2).
- L'utilisateur doit avoir le droit de commander les sorties (case **PGM**, point 6.4), et la définition **Remote control** doit être attribuée à la sortie (**Output definition**, point 6.7).
- Vérifiez la case **Use dial and SMS when working over internet module** (point 6.3) : si elle n'est pas cochée et qu'un réseau LAN est présent, les appels et les SMS ne sont pas utilisés.

Je ne reçois pas de réponse à mes commandes SMS

Pour le SMS de réponse, la case **ACK** doit être cochée pour l'utilisateur (**Users & Reporting**, point 6.4). Vous pouvez modifier le texte des réponses dans l'onglet **SMS answer texts**.

Les données peuvent-elles passer uniquement par le réseau local (LAN) ?

Oui. Si vous cochez la case **Disable the use of SIM card mobile data**, le FireCom n'utilise pas la liaison de données mobile de la carte SIM : les données ne passent que par le LAN. Si le LAN est temporairement indisponible, le communicateur stocke les données dans sa mémoire et les envoie au retour du LAN. S'il n'y a pas de carte SIM dans le communicateur, vous pouvez désactiver la signalisation de son absence avec la case **Disable indication of the absence of a SIM card** (point 6.3).

Combien de détecteurs de fumée peut-on raccorder à la borne FLOOP ?

Au maximum 8 détecteurs incendie deux fils dont le courant d'alarme est supérieur à 10 mA. Une résistance de fin de ligne de 2,2 kΩ est nécessaire après le dernier détecteur, et sur la page **Zones**, l'entrée **FC Fire sensor (FLOOP input)** doit être choisie comme entrée de la zone (points 3.3 et 6.6). Si vous raccordez les détecteurs à une entrée IO, les schémas de raccordement se trouvent au même endroit.

Quels capteurs de température, et combien, peut-on raccorder ?

Au maximum 8 capteurs de température Maxim® / Dallas® DS18S20 ou DS18B20, ou 1 capteur d'humidité et de température AM2301. Le communicateur attribue automatiquement les capteurs Dallas, l'AM2301 doit être attribué manuellement sur la page **Sensors** (points 3.10 et 6.8). Vous pouvez aussi demander les valeurs par SMS : `ASKT` (point 5.2).

Quelle batterie faut-il ?

Une batterie au plomb 12 V de 4 Ah ou 7 Ah (points 1.2 et 2.1). Selon la norme EN 54, la batterie doit se recharger à 80 % de sa capacité en 24 heures et atteindre le reste au cours des 48 heures suivantes (point 3.1). À 11,5 V, un message **Low Battery** est envoyé ; sous 9,5 V, la batterie est déconnectée (point 2.2).

Comment la centrale incendie sait-elle que le message est parvenu au centre de télésurveillance ?

Selon la norme EN 54, la centrale doit être informée du défaut de la liaison avec le centre de télésurveillance et de la bonne réception des messages. Pour cela, deux sorties PGM du communicateur doivent être raccordées aux entrées prévues à cet effet sur la centrale : la sortie **Relay1**, réglée sur **CMS fail**, s'active lors de l'interruption du canal de communication ; la sortie **Relay2**, réglée sur **ACK received**, s'active pendant 5 secondes lorsque le message est parvenu au centre de télésurveillance (point 3.12).

INIM Smartline : à quoi faut-il faire attention ?

La centrale doit être réglée en mode **slave** dans le logiciel SmartLeague. Si des répéteurs (repeaters) sont raccordés à la centrale, le FireCom ne peut pas être raccordé sur le bus RS485 ; et si le FireCom est raccordé au bus RS485 de la centrale, les modules d'extension iO ne sont pas pris en charge (point 3.7).

NSC Solution : la centrale ne voit pas le communicateur

Une fois le FireCom configuré, il faut rechercher (scanner) sur la centrale les modules raccordés au bus RS485 (**SCAN RS485**, point 3.6). L'**NSC slave address** ne doit pas être identique à l'adresse des modules raccordés à la centrale.

11. Consignes de sécurité

Figyelem!

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

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

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

- Le communicateur ne doit être installé et entretenu que par une personne qualifiée.
- Avant l'installation, lisez attentivement ce manuel afin d'éviter les erreurs pouvant entraîner un mauvais fonctionnement, voire l'endommagement de l'équipement.
- **Avant tout raccordement électrique, coupez la tension d'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

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

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

Produits associés

Trikdis FireCom Ethernet + 4G transmetteur d'alarme 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 **Capteur de température DS18B20 avec fil 1M**

Batterie gel 12 V 7 Ah pour centrale d'alarme

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-firecom