Contrôleur de portail GV17 GATOR – manuel d'installation et de programmation

Manuel d'installation et de programmation du contrôleur de portail Trikdis GV17 GATOR : câblage, carte SIM et configuration dans TrikdisConfig, utilisateurs et autorisations, commande par appel, par SMS et depuis l'application Protegus 2.



Édition: 2026-11-18
Version web toujours à jour: https://trikdis.fr/manuel-gv17

Sommaire

1. Présentation

1.1 À quoi il sert, comment il fonctionne
1.2 Versions
1.3 Caractéristiques techniques
1.4 Éléments de l'appareil et bornes
1.5 Signalisation des LED
1.6 Contenu de la boîte, outillage

2. Mise en service rapide

2.1 Mise en service en trois étapes
2.2 Seules les personnes autorisées
2.3 Application et télésurveillance

3. Installation et raccordement

3.1 Fixation et insertion de la carte SIM
3.2 Alimentation
3.3 Entrées
3.4 Relais sur la sortie universelle
3.5 Raccordement de la motorisation du portail
3.6 Lecteur RFID (Wiegand 26/34)
3.7 Module WiFi W485
3.8 Module Ethernet E485
3.9 RF-LORA et iO-LORA avec lecteur RFID
3.10 Modules d'extension iO8 et iO8-LORA

4. Commande à distance

4.1 Commande par appel téléphonique
4.2 Commande au clavier du téléphone (DTMF)
4.3 Commande depuis l'application Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.4 Widget sur l'écran d'accueil du téléphone
4.5 Utilisateurs dans l'application
4.6 Commande par SMS
4.7 Programmation par SMS

5. Configuration dans TrikdisConfig

5.1 La barre d'état
5.2 Page « System Options »
5.3 Page « IN/OUT »
5.3.1 Onglet IN/OUT – entrées et sorties
5.3.2 Scheduler – horaires des sorties
5.3.3 Onglet Holidays – jours fériés
5.4 Page « Modules »
5.4.1 Onglet Modules
5.4.2 Onglet Parameters – module WiFi W485
5.4.3 Onglet Parameters – module Ethernet E485
5.5 Page « IP Reporting »
5.6 Page « User list »

5.6.1 Onglet Users – les utilisateurs
5.6.2 Enregistrer une carte RFID (badge)
5.6.3 Scheduler – horaires des utilisateurs
5.6.4 Onglet Black list – liste noire
5.7 Page « System events »
5.8 Page « Events Log »
5.9 Retour aux réglages d'usine
5.10 Signalisation de l'état du portail
6. Programmation à distance
7. Vérification du fonctionnement
8. Mise à jour du firmware
9. Dépannage et questions fréquentes
10. Consignes de sécurité
Voir aussi

1. Présentation

Le **GV17 GATOR** est le contrôleur de portail cellulaire de Trikdis : il est conçu pour la commande à distance de portails électriques, de barrières levantes, de portes de garage et d'autres équipements. L'utilisateur le commande par **appel téléphonique**, par **SMS** ou depuis l'application **Protegus 2** ; l'appareil gère les numéros de téléphone (cartes RFID, adresses e-mail) de **7 administrateurs** et de **1000 utilisateurs** au maximum, et pour chaque utilisateur vous pouvez régler une restriction horaire (programmation horaire, durée de validité) et un compteur distincts. Le GATOR signale les changements d'état des entrées et des sorties (activation et rétablissement) par SMS et dans l'application – c'est vous qui définissez le texte des SMS –, et il transmet aussi les événements au centre de télésurveillance au format Contact ID. Avec un module WiFi **W485** ou Ethernet **E485**, la commande et la transmission fonctionnent aussi par Internet, sans données mobiles ; avec un émetteur-récepteur **RF-LORA**, vous pouvez y associer jusqu'à 8 modules d'extension sans fil **iO-LORA** et un module d'extension **iO8-LORA** : un seul appareil commande ainsi jusqu'à 8 portails ou barrières éloignés les uns des autres, chacun avec son propre lecteur RFID (les lecteurs RFID raccordés aux modules iO-LORA peuvent commuter au maximum 8 sorties – un lecteur ne commande toujours qu'une seule sortie de son propre module d'extension –, ce qui nécessite le firmware 2.13 ou plus récent sur le GATOR). Vous effectuez les réglages avec le logiciel **TrikdisConfig**, par câble USB ou à distance.



Figure 1. Le contrôleur de portail GV17 GATOR : à l'avant les voyants NETWORK, DATA, POWER et TROUBLE, en haut le connecteur d'antenne, en bas le bornier débrochable.

1.1 À quoi il sert, comment il fonctionne

Usages principaux

- **Ouverture à distance de portails, barrières et portes de garage** pour la famille, une copropriété, les salariés d'une entreprise ou les locataires d'un parking : l'utilisateur appelle le numéro de la carte SIM du GATOR et le portail s'ouvre – l'appareil rejette l'appel, l'appel est donc gratuit. Il peut faire la même chose depuis l'application d'un seul bouton, avec un widget placé sur l'écran d'accueil du téléphone ou par SMS.
- **Contrôle d'accès par carte RFID et par code** : avec un ou deux lecteurs Wiegand 26/34 (entrée et sortie), bouton-poussoir de sortie, programmation horaire par utilisateur (qui peut entrer et quand), durée de validité et compteur d'accès ; à partir des entrées et des sorties, Protegus 2 peut aussi établir un **relevé du temps de travail** – un article séparé y est consacré : GV17 – système de contrôle d'accès et/ou de suivi du temps de travail.
- **Mise en marche et arrêt à distance de tout autre équipement**, en mode impulsionnel ou bistable, y compris selon une programmation horaire : éclairage, arrosage, pompe, chauffage.
- **Plusieurs portails dans un même système** : sans fil avec les modules RF-LORA et iO-LORA, jusqu'à 8 sites, chacun avec son propre relais, sa propre entrée et son propre lecteur RFID – Contrôle d'accès sans fil flexible avec le système GATOR RF-LoRa.

Comment il fonctionne

- **Commande** : par appel téléphonique (par défaut n'importe qui l'appelant ; avec une liste d'utilisateurs, uniquement les personnes autorisées), pendant l'appel avec le clavier du téléphone (DTMF), par commande SMS, depuis l'application mobile et web Protegus 2, avec un widget Android, par carte RFID et par code.
- **Notification de l'utilisateur** : par SMS aux administrateurs (événements des entrées et des sorties, test, nouvel utilisateur), par notification push dans l'application Protegus 2.
- **Transmission au centre de télésurveillance** : avec des codes d'événement Contact ID vers les récepteurs IP logiciels et matériels de Trikdis, qui fonctionnent avec n'importe quel logiciel de télésurveillance ; récepteur principal et de secours (si la liaison avec le récepteur principal est interrompue, les messages partent automatiquement vers le récepteur de secours), secours par SMS ; les événements peuvent aller simultanément au centre de télésurveillance et dans Protegus 2.
- **Entrées et sorties** : 2 entrées (NO, NC ou EOL 10 kΩ), 2 bornes universelles (entrée ou sortie à collecteur ouvert, 50 mA), 1 sortie relais (1 A / 30 V DC, 0,5 A / 125 V AC). Chaque module d'extension iO-LORA ajoute 1 entrée et 1 sortie relais au système (8 modules d'extension au maximum, soit 8 entrées et 8 sorties supplémentaires au total), le module d'extension iO8 ou iO8-LORA ajoute d'autres entrées et sorties (un seul peut être associé au GATOR).
- **Installation et configuration** : prêt à fonctionner en sortie d'usine ; vous ajoutez et supprimez les utilisateurs depuis l'application Protegus 2 (en tant qu'administrateur), par SMS ou avec le logiciel TrikdisConfig ; la configuration se fait par câble USB Mini-B ou à distance ; le firmware peut aussi être mis à jour à distance ; deux niveaux d'accès (installateur et administrateur).

1.2 Versions

Le GATOR existe en deux versions cellulaires ; leur raccordement, leur configuration et leur commande sont identiques, seul le modem diffère. Dans la barre d'état de TrikdisConfig, vous voyez le type exact sous la forme **GV17_xxxx** (point 5.1).

Version	Modem	Bandes
GV17-4G	4G (LTE)	en Europe LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 (pour l'Amérique latine, il existe une version avec une autre répartition des bandes)

Version	Modem	Bandes
GV17-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis GV17 - GATOR contrôleur de portail intelligent 4G GSM / IP

Trikdis GV17 – GATOR contrôleur de portail intelligent 2G GSM / IP

En raison de l'arrêt progressif des réseaux 2G, nous recommandons la version 4G pour toute nouvelle installation. Sur les appareils de type **GV17_2E70** et **GV17_2S70**, la commande au clavier pendant l'appel (DTMF) ne fonctionne pas (point 4.2) ; la commande par appel, par SMS et depuis l'application y fonctionne de la même façon.

1.3 Caractéristiques techniques

Caractéristique	Valeur
Bandes du modem 2G (GSM)	850 / 900 / 1800 / 1900 MHz
Bandes du modem 4G (LTE)	Europe : LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 ; Amérique latine : LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Tension d'alimentation	9–32 V DC ou 12–24 V AC
Consommation	100 mA
Entrées	2, type au choix : NC, NO, EOL = 10 kΩ
Entrées/sorties universelles	2 ; en entrée NC, NO, EOL = 10 kΩ, en sortie à collecteur ouvert (OC), 50 mA au maximum
Sortie	1 relais, 1 A / 30 V DC, 0,5 A / 125 V AC
Mémoire des événements non envoyés	jusqu'à 60 événements
Journal des événements	jusqu'à 5000 événements
Utilisateurs recevant les messages et autorisés à commander (administrateurs)	7
Utilisateurs autorisés à commander	1000
Environnement de fonctionnement	–20 … +50 °C, humidité relative de 80 % au maximum à +20 °C
Dimensions	92 × 62 × 26 mm
Poids	80 g

1.4 Éléments de l'appareil et bornes

Les numéros de la figure désignent les éléments de l'appareil ; le tableau donne la fonction des bornes.

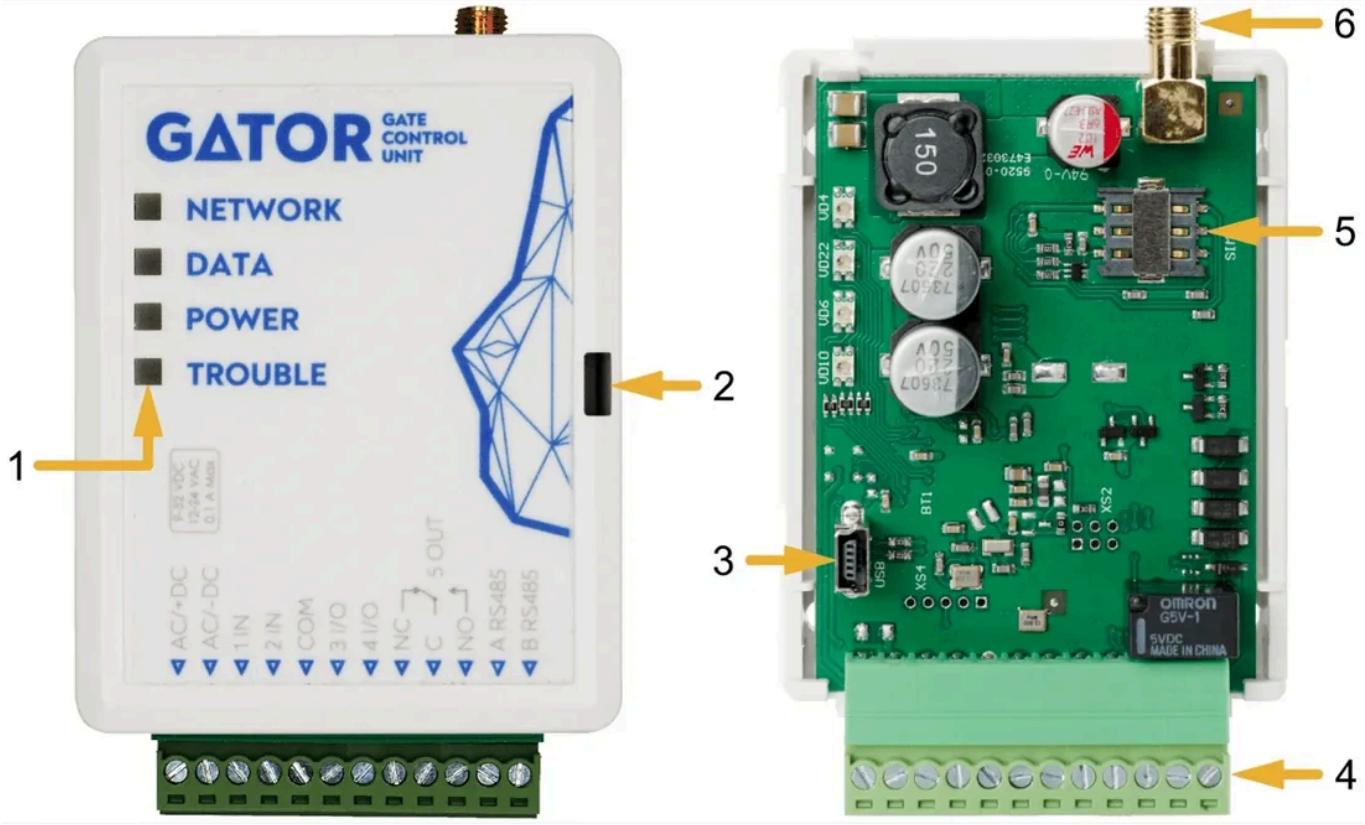


Figure 2. Les éléments du GATOR.

- 1 voyants LED
- 2 fente servant à retirer la face avant
- 3 connecteur USB Mini-B pour la programmation
- 4 bornier débrochable
- 5 logement de la carte nano-SIM
- 6 connecteur SMA de l'antenne cellulaire

Borne	Fonction
AC/+DC	alimentation : pôle positif 9–32 V DC ou 12–24 V AC
AC/−DC	alimentation : pôle négatif 9–32 V DC ou 12–24 V AC
1 IN	entrée 1, type NO, NC ou EOL (par défaut : entrée NO)
2 IN	entrée 2, type NO, NC ou EOL (par défaut : désactivée)
COM	point commun des entrées
3 I/O	entrée ou sortie (par défaut : désactivée)
4 I/O	entrée ou sortie (par défaut : désactivée)
NC	contact normalement fermé du relais
C	contact commun du relais
NO	contact normalement ouvert du relais
A RS485	fil A du bus RS485
B RS485	fil B du bus RS485

Le logiciel et les commandes SMS désignent la sortie relais par **5 OUT** (OUTPUT5), et les deux bornes universelles utilisées en sortie par **3 OUT** et **4 OUT**. Le bornier à 12 pôles se débranche de l'appareil et est aussi disponible séparément :

1.5 Signalisation des LED

Voyant	Lumière	Signification
NETWORK	vert, fixe	connecté au réseau mobile
	jaune clignotant	niveau du signal du réseau mobile, de 0 à 5 clignotements ; 3 suffisent
DATA	vert, fixe	envoi d'un message en cours
	jaune, fixe	des événements en attente d'envoi se trouvent en mémoire
POWER	vert clignotant	la tension d'alimentation est correcte
	jaune clignotant	la tension d'alimentation n'est pas correcte
	rouge et jaune clignotant	mode configuration
TROUBLE	éteint	aucun défaut de fonctionnement
	1 clignotement	pas de carte SIM
	2 clignotements	le code PIN de la carte SIM est erroné
	3 clignotements	impossible de se connecter au réseau mobile
	4 clignotements	impossible de se connecter au cloud Protegus ou au récepteur IP principal
	5 clignotements	impossible de se connecter au récepteur IP de secours
	6 clignotements	l'horloge interne n'est pas réglée
	7 clignotements	la tension d'alimentation n'est pas correcte

Si aucune LED ne s'allume, vérifiez la tension d'alimentation et le raccordement.

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

1.6 Contenu de la boîte, outillage

Dans la boîte : 1 contrôleur de portail GV17 GATOR, 1 antenne cellulaire, 3 résistances de 10 kΩ, 1 ruban adhésif double face (5 cm) et 2 vis.

Ce dont vous aurez besoin

Avant de commencer l'installation, vérifiez que vous avez tout sous la main : câble USB Mini-B pour la configuration · câble d'au moins 4 conducteurs pour le raccordement · tournevis plat de 2,5 mm · carte nano-SIM activée (désactivez la demande de code PIN) avec un service de données mobiles, si vous utilisez aussi l'application ou la télésurveillance · antenne externe si le signal est faible sur le site · manuel d'installation de l'équipement commandé (moteur de portail, barrière levante), avec le raccordement de l'entrée de commande et de la sortie d'état du portail. Les accessoires énumérés sont à acquérir séparément – commandez-les auprès de votre revendeur.

En cas de signal faible, dans un coffret métallique ou derrière un mur épais, utilisez à la place de l'antenne fournie une antenne déportable avec un câble de 2,5 m :

Antenne magnétique Trikdis ME301m avec fil 2,5 m

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

2. Mise en service rapide

Le GATOR est prêt à fonctionner en sortie d'usine

Lorsque quelqu'un appelle le numéro de téléphone de la carte SIM insérée dans l'appareil, le GATOR rejette l'appel et active la sortie relais **5 OUT** pendant **3 secondes**. Si ce fonctionnement vous convient, l'appareil peut être mis en service sans aucun autre réglage.

2.1 Mise en service en trois étapes

1. **Insérez la carte nano-SIM** dans le logement du GATOR (point 3.1). Désactivez au préalable la demande de code PIN de la carte dans un téléphone, sinon l'appareil ne se connecte pas au réseau (ou vous devez saisir le code PIN dans TrikdisConfig, point 5.2).
2. **Raccordez l'alimentation et la motorisation du portail** selon les schémas du chapitre 3 : l'alimentation sur les bornes **AC/+DC** et **AC/−DC**, l'entrée de commande de la motorisation sur les contacts **C** et **NO** du relais.
3. **Mettez sous tension.** En fonctionnement correct, la LED **POWER** clignote en vert, la LED **NETWORK** est allumée en vert et clignote entre-temps en jaune selon le niveau du signal. Appelez le numéro de la carte SIM : l'appareil rejette l'appel et le relais s'enclenche pendant 3 secondes.

2.2 Seules les personnes autorisées

Par défaut, **n'importe qui** appelant son numéro peut commander le GATOR. Si vous voulez réserver la commande à certaines personnes, envoyez un SMS avec le numéro de téléphone des utilisateurs (envoyez la commande depuis votre propre téléphone, car la première personne qui appelle l'appareil ou lui envoie un SMS en devient l'administrateur, point 4.1) :

```
SETU 123456 +33612345678#Pierre#pierre@exemple.fr
```

Une fois le premier numéro enregistré, le GATOR ne réagit plus qu'aux appels provenant des numéros de la liste et ignore les autres. Vous pouvez ajouter d'autres utilisateurs de la même façon, un par un ; l'ensemble des commandes SMS est décrit au point 4.7, et vous pouvez aussi gérer la liste dans TrikdisConfig et dans l'application Protegus 2 (points 5.6 et 4.5).

Changez le mot de passe administrateur

Avec le mot de passe par défaut `123456`, toute personne connaissant le numéro de l'appareil peut reprogrammer le GATOR. Lors de la première mise en service, remplacez-le par SMS (`PSW 123456 nouveaumotdepasse`, 6 caractères) ou dans TrikdisConfig (**System Options** → **Administrator Code**).

2.3 Application et télésurveillance

- **Application Protegus 2 :** dans TrikdisConfig, sur la page **IP Reporting**, activez le service cloud (**Enable cloud service**, point 5.5) et changez le code par défaut `123456` du **Cloud Access Code** ; la même chose par SMS : `CONNECT 123456 PROTEGUS=ON`. Le système peut ensuite être ajouté à l'application selon le point 4.3. Il faut pour cela un service de données mobiles sur la carte SIM (ou un module W485 / E485).
- **Télésurveillance :** sur la page **IP Reporting**, saisissez l'adresse, le port et la clé de chiffrement du récepteur, et sur la page **System Options** l'identifiant d'objet (points 5.2 et 5.5).
- **Ordre recommandé des réglages dans TrikdisConfig :** mot de passe administrateur et données de la SIM (APN) → fonction des entrées et des sorties, durée d'impulsion → utilisateurs, cartes RFID, programmation horaire → cloud et télésurveillance → vérification selon le chapitre 7.

Si vous souhaitez modifier les réglages d'usine ou activer d'autres fonctions de l'appareil, le chapitre 5 décrit les réglages du logiciel TrikdisConfig.

3. Installation et raccordement

Figyelem!
Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

Ce chapitre décrit la fixation du GATOR, l'alimentation, le raccordement des entrées, du relais et de la motorisation du portail, puis le branchement des lecteurs RFID et des modules d'extension (W485, E485, RF-LORA + iO-LORA, iO8 / iO8-LORA). Sur les schémas, les noms des bornes du GATOR correspondent aux inscriptions de l'appareil (point 1.4).

3.1 Fixation et insertion de la carte SIM

1. Retirez la face avant (introduisez le tournevis dans la fente latérale et déclipsez-la), puis débranchez le bornier.
2. Sortez le circuit imprimé du boîtier : appuyez sur la languette de fixation et soulevez-le.
3. Fixez le fond du boîtier à l'endroit voulu avec des vis (ou avec le ruban adhésif double face fourni).
4. Remettez en place le circuit imprimé et le bornier.
5. Vissez l'antenne cellulaire sur le connecteur SMA.
6. Insérez la carte nano-SIM dans son logement.
7. Remettez en place la face avant.

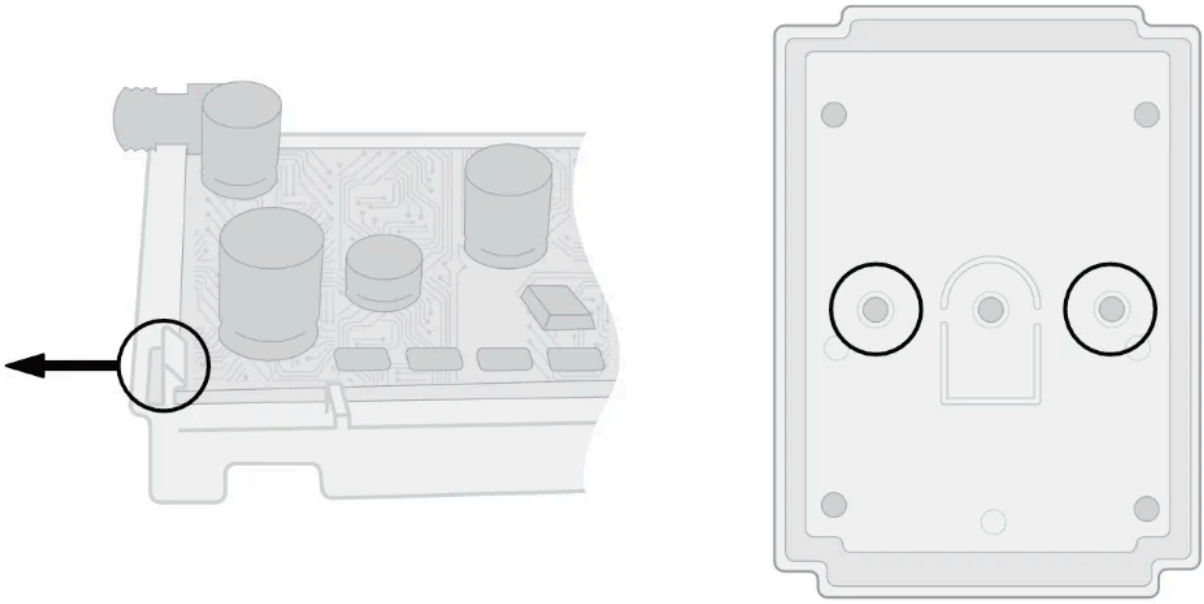


Figure 3. À gauche, la languette de fixation du circuit imprimé (en appuyant dans le sens de la flèche, la carte se libère), à droite les deux trous de vis du fond du boîtier.

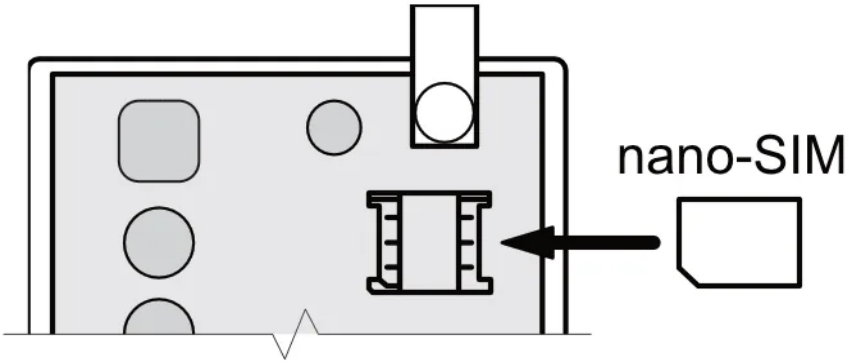


Figure 4. Insertion de la carte nano-SIM dans le sens de la flèche, dans le logement situé sur le circuit imprimé.

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

3.2 Alimentation

Le GATOR fonctionne sur une alimentation **9–32 V DC** ou **12–24 V AC** ; les deux bornes d'alimentation (**AC/+DC**, **AC/−DC**) acceptent les deux types d'alimentation. Dans la plupart des cas, la sortie d'alimentation des accessoires de l'unité de commande du moteur de portail (généralement 24 V AC ou DC) suffit, et aucun bloc d'alimentation séparé n'est nécessaire. Avec une alimentation propre, il faut un transformateur ~230 V / 16 V d'au moins 10 VA (avec un fusible de 125 mA côté 230 V) ou un bloc d'alimentation continue de 9–32 V d'au moins 0,2 A. L'appareil n'a pas de batterie de secours : si le portail doit pouvoir s'ouvrir aussi pendant une coupure de courant, alimentez-le par une alimentation sans interruption. Raccordez les fils selon le schéma ci-dessous.

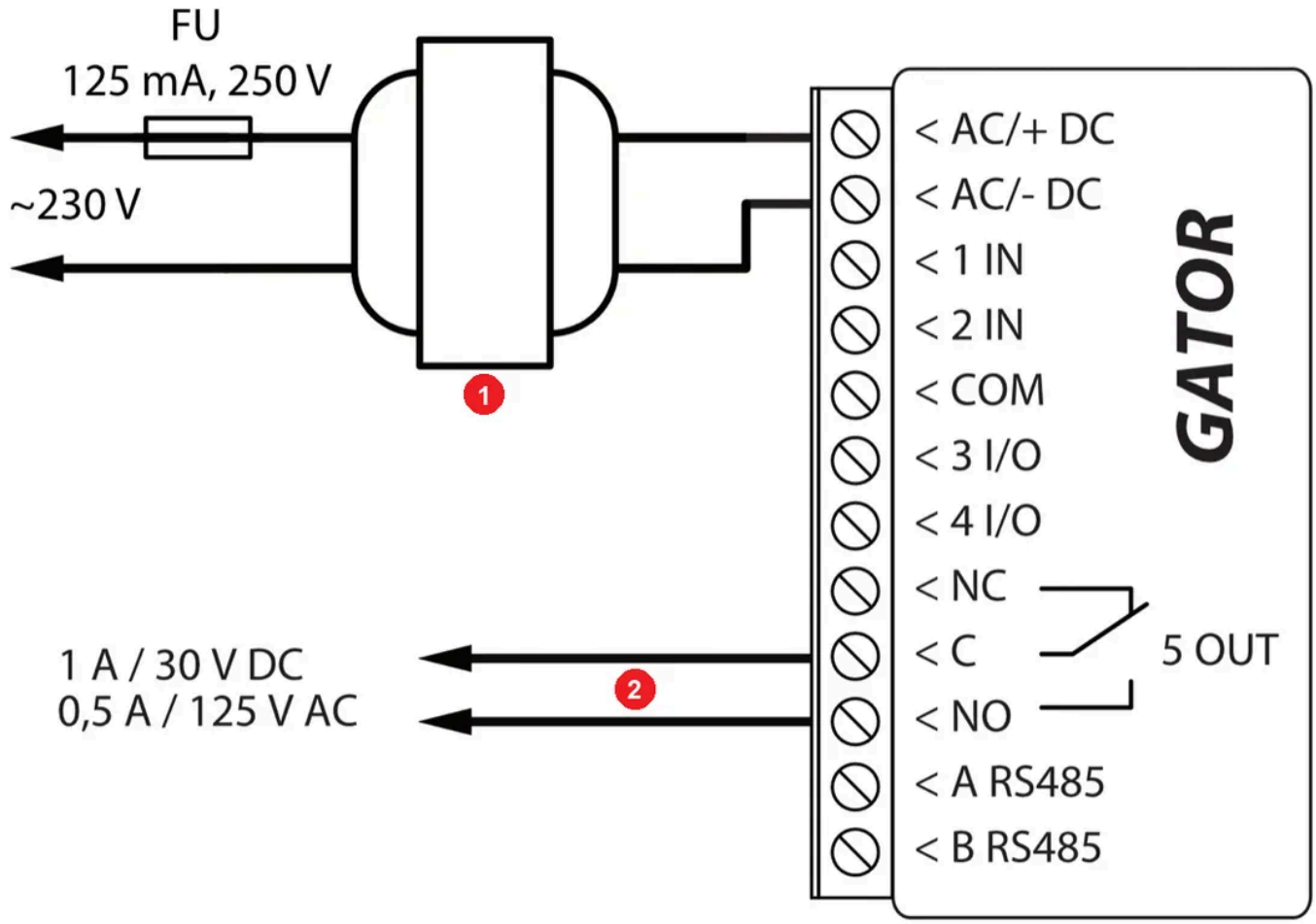


Figure 5. Raccordement de l'alimentation et de la motorisation du portail : alimentation secteur par un transformateur ~230 V / 16 V, 10 VA, 50 Hz (fusible 125 mA, 250 V) ou par un bloc d'alimentation continue 9–32 V, 0,2 A, sur les bornes AC/+DC et AC/−DC ; l'entrée de commande de la motorisation sur les contacts C et NO du relais ; pouvoir de coupure du relais 1 A / 30 V DC ou 0,5 A / 125 V AC.

- 1 transformateur, ~230 V / 16 V, 10 VA, 50 Hz (« Transformer »), ou bloc d'alimentation continue, 9–32 V, 0,2 A (« or DC power supply source »)
- 2 commande du portail (« Gate control ») – l'entrée de commande de la motorisation

Sur les schémas, l'alimentation des lecteurs RFID, des relais et des modules d'extension est prise sur la borne **AC/+DC** : cela n'est possible qu'avec une alimentation **continue** (sur les schémas 9–16 V DC, 0,5 A, pour les modules W485 / E485 et iO8 10–28 V DC). Avec une alimentation alternative, le lecteur et le module ont besoin d'un bloc d'alimentation DC séparé.

3.3 Entrées

Le GATOR a **quatre entrées** : **1 IN** et **2 IN** sont toujours des entrées, **3 I/O** et **4 I/O** sont des bornes universelles, configurables en entrée ou en sortie. Chacune fonctionne par rapport à la borne **COM** et peut être de type **NO**, **NC** ou **EOL** (avec résistance de fin de ligne de 10 kΩ) ; trois résistances de fin de ligne sont fournies dans l'emballage. Sur une entrée, vous pouvez raccorder le fin de course du portail ou sa sortie d'état (signalisation de l'état du portail, points 3.5 et 5.10), un bouton-poussoir de sortie (point 3.6), ou tout détecteur ou contact dont vous voulez être averti des changements par SMS ou notification push, ou avec lequel vous voulez commuter une sortie (**CTRL by IN**, point 5.3). Vous réglez le type et le temps de réaction sur la page **IN/OUT** de TrikdisConfig ; par défaut, seule l'entrée 1 IN est active (NO). Raccordez les entrées selon le type réglé (NC, NO, EOL), conformément au schéma ci-dessous.

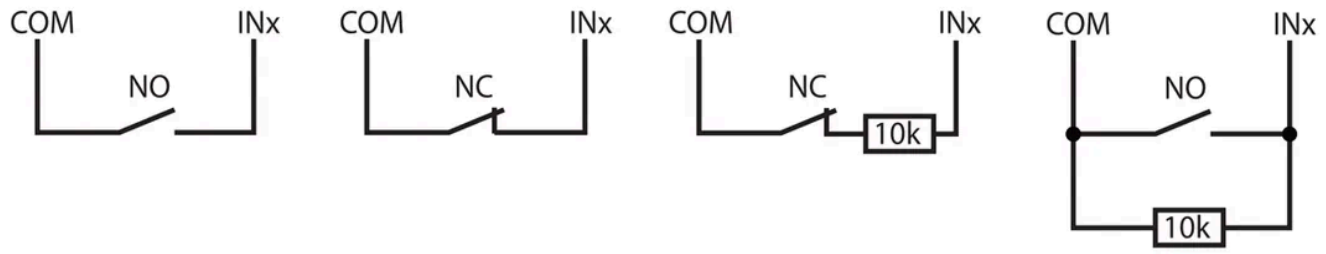


Figure 6. Les quatre modes de raccordement des entrées entre la borne COM et la borne IN. De gauche à droite : **NO** – contact normalement ouvert – fermeture = alarme, ouverture = rétablissement ; **NC** – contact normalement fermé – ouverture = alarme, fermeture = rétablissement ; **NC + EOL** – contact normalement fermé avec une résistance de 10 kΩ en série – court-circuit et coupure = alarme, 10 kΩ = repos ; **NO + EOL** – contact normalement ouvert avec une résistance de 10 kΩ en parallèle – court-circuit et coupure = alarme, 10 kΩ = repos.

3.4 Relais sur la sortie universelle

Utilisées en sortie, les bornes **3 I/O** et **4 I/O** sont à collecteur ouvert, avec un pouvoir de coupure de **50 mA** au maximum : elles ne peuvent commuter directement que la bobine d'un petit relais. Avec les contacts du relais, n'importe quel équipement peut être mis en marche et arrêté à distance. Le schéma vaut pour une alimentation continue : une extrémité de la bobine va sur la borne **AC/+DC**, l'autre sur la sortie ; dans TrikdisConfig, la fonction de la borne doit être réglée sur **Output** (point 5.3).

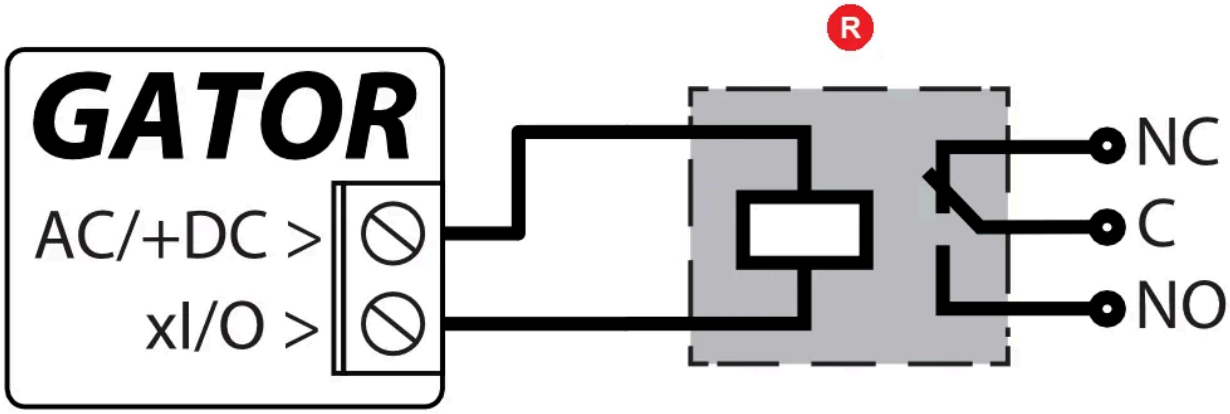


Figure 7. Relais externe sur la sortie universelle : la bobine entre la borne AC/+DC et la borne 3 I/O ou 4 I/O réglée en sortie ; les contacts NC, C et NO du relais commutent l'équipement.

- R relais (« Relay »)

3.5 Raccordement de la motorisation du portail

Effectuez toujours le raccordement hors tension. Les bornes de l'unité de commande de la motorisation et leur tension nominale sont décrites dans la documentation du moteur de portail – le schéma ne montre que la disposition type.

Le portail s'ouvre par les bornes (de commande) **IN** et **COM** de la motorisation : c'est là que se raccordent les contacts **C** et **NO** du relais du GATOR ; l'impulsion du relais fait la même chose que le bouton de la télécommande. La plupart des motorisations disposent d'une **sortie d'état du portail** (OUT), qui indique si le portail est ouvert ou fermé ; il peut s'agir d'une sortie en tension ou d'une sortie relais. Sur le schéma, le relais auxiliaire K1 est raccordé à une motorisation à sortie en tension : portail ouvert, on mesure ~230 V entre les bornes OUT et N de la motorisation, le relais K1 s'enclenche et active l'entrée **1 IN** du GATOR. L'état de

l'entrée 1 IN suit ainsi exactement la position du portail, ce que montrent aussi Protegus 2 et l'icône du widget – le réglage correspondant se trouve au point 5.10. Avec une motorisation à sortie relais, le K1 n'est pas nécessaire : le contact d'état peut être raccordé directement entre 1 IN et COM.

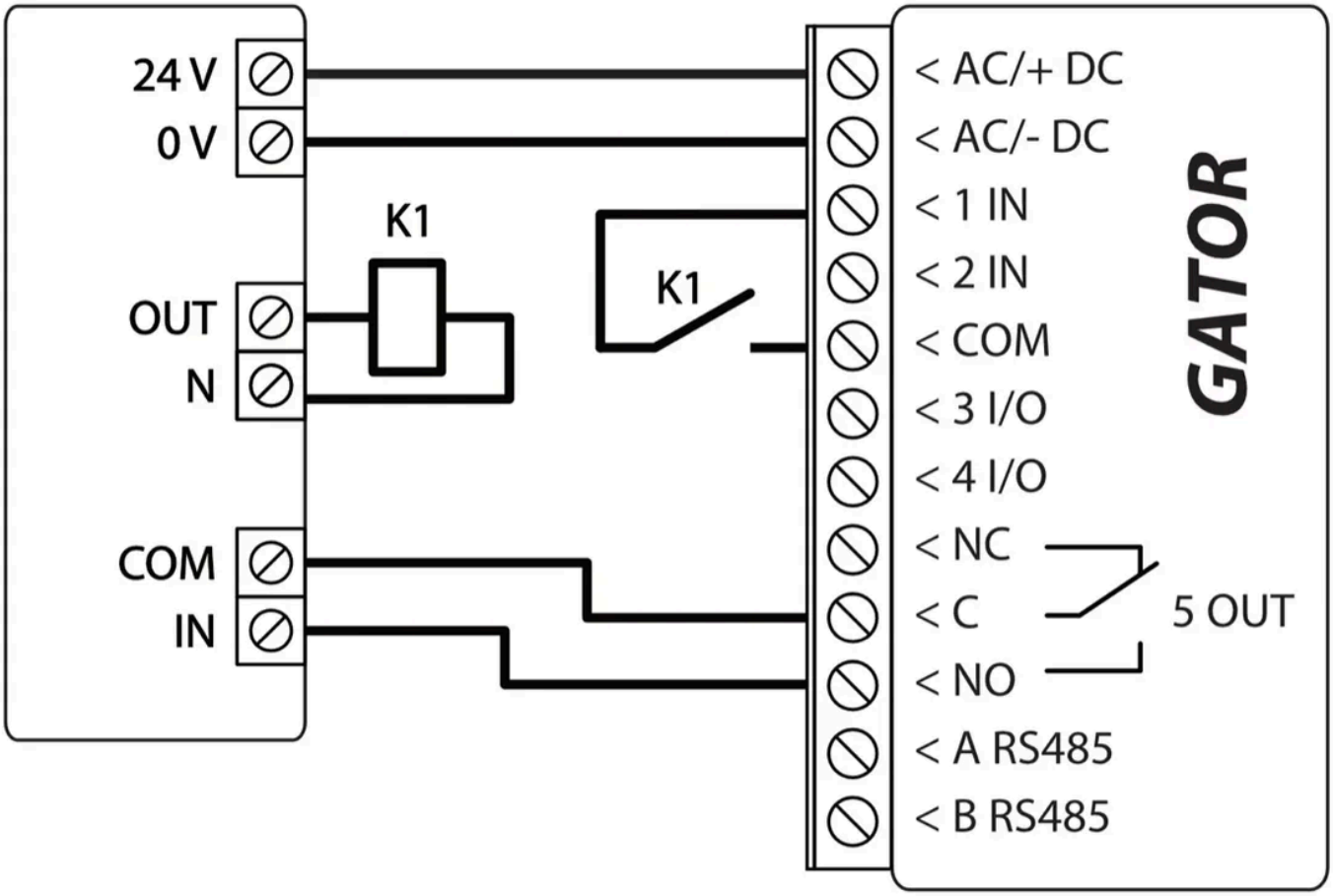


Figure 8. Liaison entre l'unité de commande de la motorisation (« Gate control unit ») et le GATOR avec le relais auxiliaire K1. Alimentation (« Power ») : la sortie d'alimentation 24 V de la motorisation sur la borne AC/+DC du GATOR, le 0 V sur la borne AC/−DC ; état du portail (« Gate status ») : les bornes OUT et N de la motorisation sur la bobine du relais K1, le contact du K1 entre les bornes 1 IN et COM du GATOR ; commande du portail (« Gate control ») : la borne COM de la motorisation sur le contact C de 5 OUT du GATOR, la borne IN sur le contact NO de 5 OUT.

3.6 Lecteur RFID (Wiegand 26/34)

Le GATOR accepte un ou deux lecteurs RFID au protocole **Wiegand 26/34** (lecteurs à carte comme lecteurs à clavier à code). Avec les cartes et les codes enregistrés dans la liste des utilisateurs, le lecteur commute la sortie **5 OUT** (l'autorisation, la programmation horaire et le compteur propres à chaque utilisateur s'appliquent aussi au lecteur). Le lecteur se règle sur la page **IN/OUT** de TrikdisConfig (point 5.3), les cartes s'enregistrent sur la page **User list** (point 5.6) ; le code couleur des fils suit la norme Wiegand : rouge +U, noir GND, vert D0, blanc D1.

Un lecteur : D0 va sur la borne **1 IN**, D1 sur la borne **2 IN**, le bouton-poussoir de sortie entre **COM** et **3 I/O**. Dans le logiciel, réglez **Wiegand reader mode** sur **Single Reader** et, s'il y a un bouton de sortie, cochez la case **IO3 as exit button (5 OUT)** : lorsqu'on appuie sur le bouton, 5 OUT s'active pendant la durée d'impulsion réglée. S'il n'y a pas de bouton, laissez la case décochée.

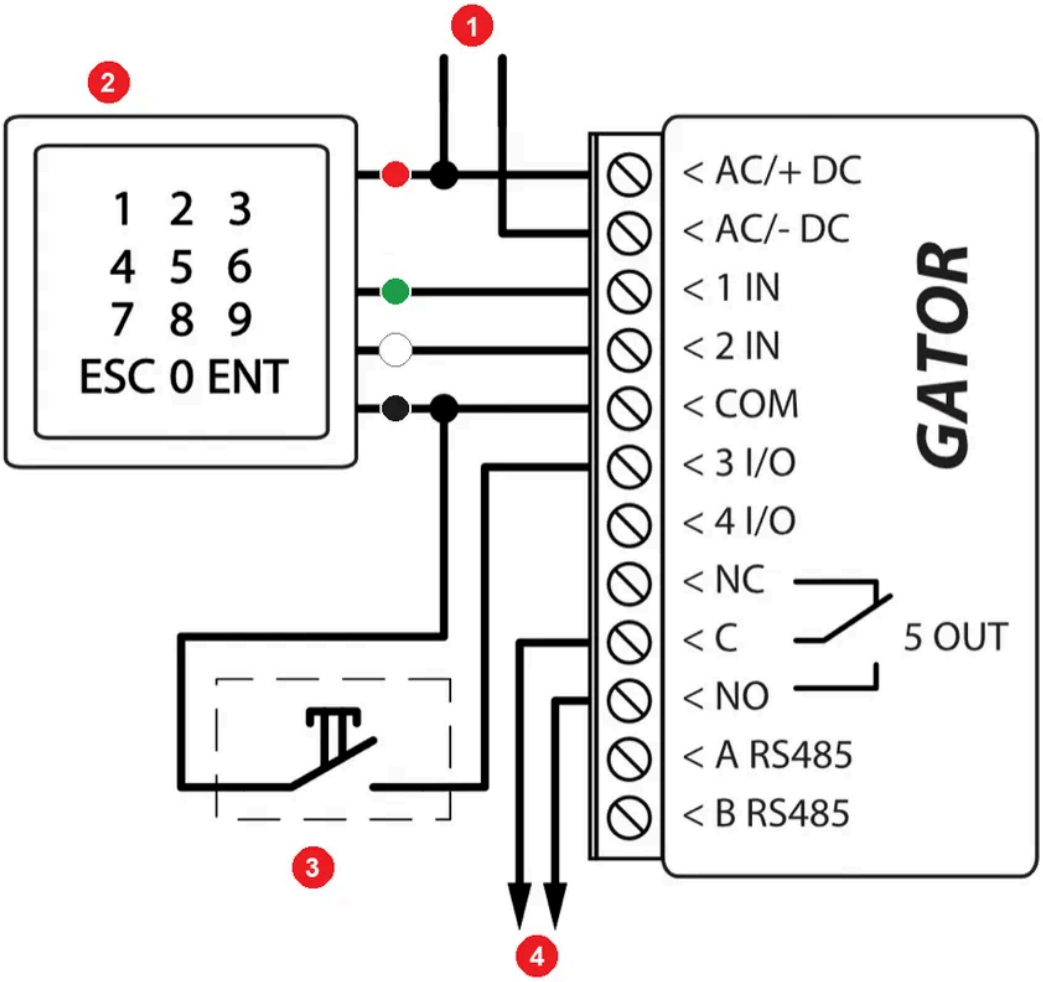


Figure 9. Raccordement d'un lecteur Wiegand 26/34 et d'un bouton de sortie : alimentation continue, 9–16 V, 0,5 A, sur les bornes AC/+DC et AC/−DC ; le fil rouge (+U) du lecteur d'entrée sur AC/+DC, le vert (D0) sur 1 IN, le blanc (D1) sur 2 IN, le noir (GND) sur la borne COM ; le bouton-poussoir de sortie entre les bornes COM et 3 I/O ; la motorisation sur les contacts C et NO du relais (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 bloc d'alimentation continue (« DC power supply »), 9–16 V, 0,5 A
- 2 lecteur d'entrée (« Entry reader ») – lecteur RFID avec clavier, Wiegand 26/34 (« RFID reader with keypad (Wiegand 26/34) »)
- 3 bouton-poussoir de sortie (« »Exit« button »)
- 4 commande du portail (« Gate control ») – l'entrée de commande de la motorisation ; pouvoir de coupure du relais 1 A / 30 V DC, 0,5 A / 125 V AC
- fil rouge, +U (« R - red (+U) »)
- fil noir, GND (« B - black (GND) »)
- fil blanc, D1 (« W - white (D1) »)
- fil vert, D0 (« G - green (D0) »)

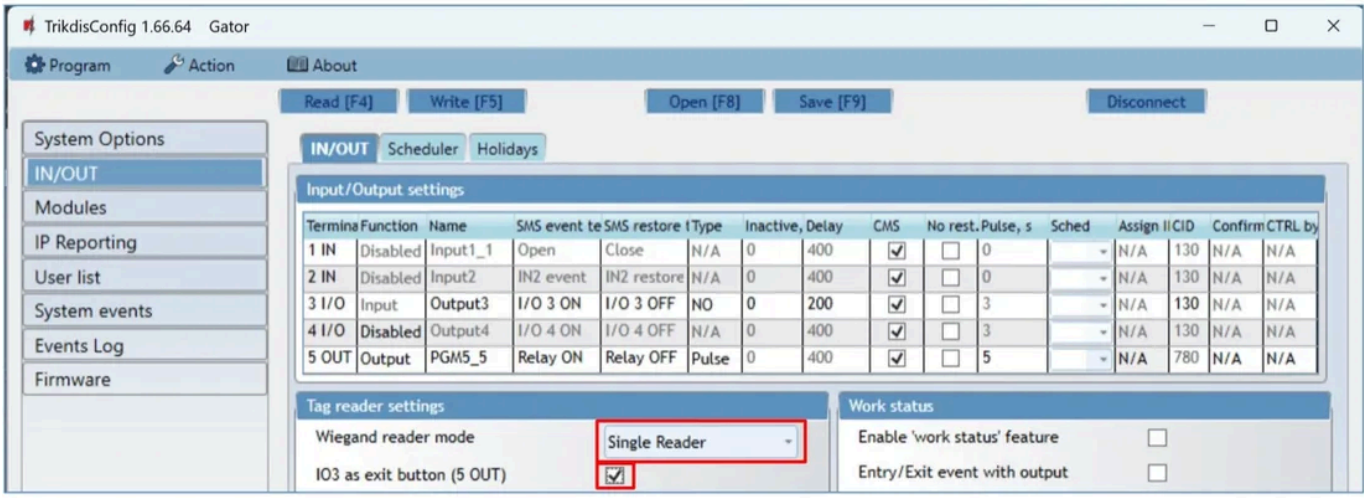


Figure 10. TrikdisConfig – IN/OUT, **Tag reader settings** : avec un lecteur, **Wiegand reader mode = Single Reader**, avec bouton de sortie **IO3 as exit button (5 OUT)** coché.

Deux lecteurs (entrée et sortie) : les fils D0 / D1 du premier lecteur vont sur les bornes **1 IN** / **2 IN**, ceux du second sur les bornes **3 I/O** / **4 I/O** ; dans le logiciel, **Wiegand reader mode = Dual Reader**. Avec deux lecteurs, la borne 3 I/O est occupée et aucun bouton de sortie ne peut y être raccordé.

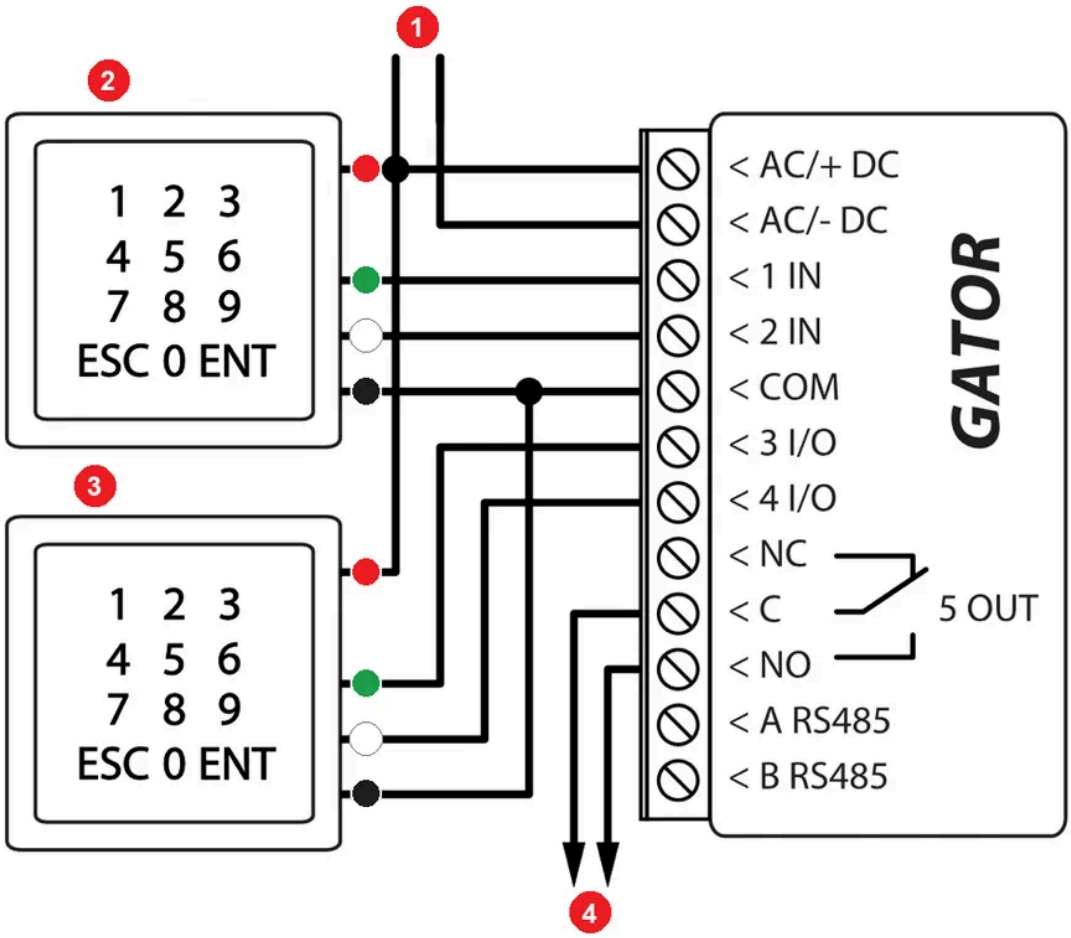


Figure 11. Raccordement de deux lecteurs Wiegand 26/34, tous deux des lecteurs RFID avec clavier (« RFID reader with keypad (Wiegand 26/34) ») : alimentation continue, 9–16 V, 0,5 A ; le fil vert (D0) du lecteur d'entrée sur 1 IN, le blanc (D1) sur 2 IN ; le fil vert (D0) du lecteur de sortie sur 3 I/O, le blanc (D1) sur 4 I/O ; le fil rouge (+U) des deux lecteurs sur AC/+DC, le noir (GND) sur la borne COM ; la motorisation sur les contacts C et NO du relais (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 bloc d'alimentation continue (« DC power supply »), 9–16 V, 0,5 A
- 2 lecteur d'entrée (« Entry reader »)
- 3 lecteur de sortie (« Exit reader »)
- 4 commande du portail (« Gate control ») – l'entrée de commande de la motorisation ; pouvoir de coupure du relais 1 A / 30 V DC, 0,5 A / 125 V AC
- fil rouge, +U (« R - red (+U) »)
- fil noir, GND (« B - black (GND) »)
- fil blanc, D1 (« W - white (D1) »)
- fil vert, D0 (« G - green (D0) »)

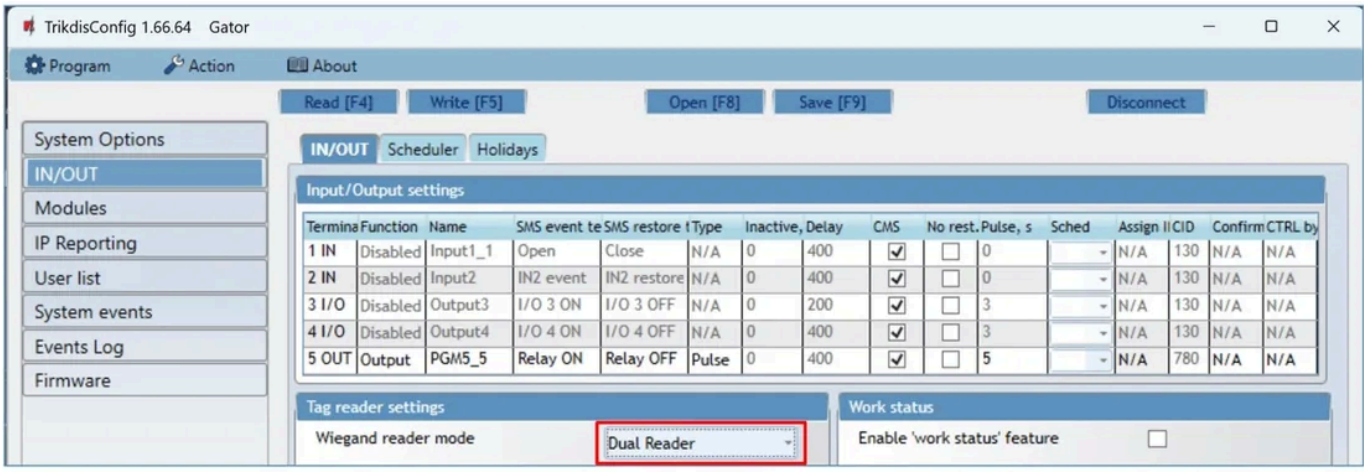


Figure 12. TrikdisConfig – IN/OUT, **Tag reader settings** : avec deux lecteurs, **Wiegand reader mode = Dual Reader**.

Si le lecteur a une sortie en 5 V (basse tension), cochez la case **Low voltage reader** ; si le lecteur émet des impulsions très courtes et que la carte n'est pas reconnue, désactivez le filtre interne avec la case **Disable reader filter** (point 5.3).

3.7 Module WiFi W485

Le module **W485** envoie les messages du GATOR au centre de télésurveillance et à l'application Protegus 2 par le réseau WiFi local, via le routeur Internet : les données mobiles ne sont donc pas consommées. Si le WiFi est interrompu, l'appareil bascule de lui-même sur le réseau mobile et revient sur le W485 au retour du WiFi. La fonction est disponible à partir du firmware **1.06** du GATOR. Le module se raccorde au bus **RS485** (A–A, B–B), avec un câble d'alarme jusqu'à **100 m au maximum**, et fonctionne sur une alimentation 10–28 V DC commune avec le GATOR. **Avec le W485, le GATOR s'utilise aussi sans carte SIM** – il ne se commande alors que depuis l'application, sans appel ni SMS. La configuration du module est décrite au point 5.4.

Module WiFi Trikdis W485 (RS485)

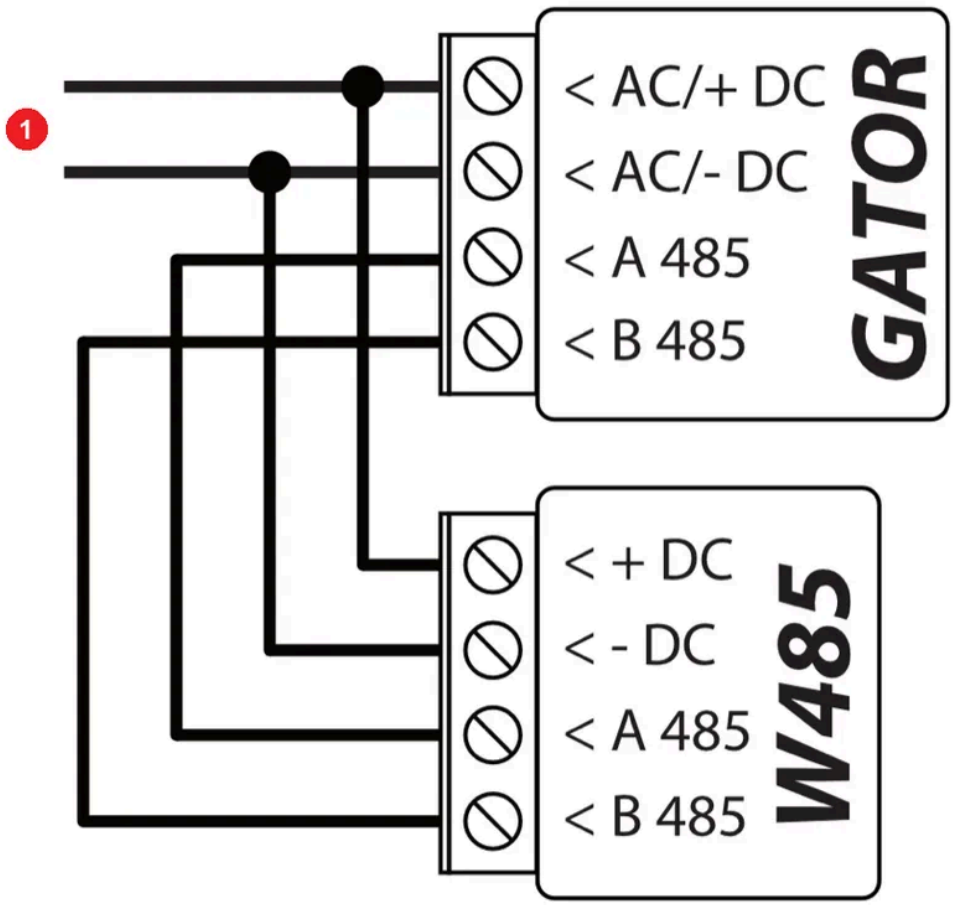


Figure 13. Raccordement du module W485 : le pôle positif du bloc d'alimentation 10–28 V DC, 0,5 A sur la borne AC/+DC du GATOR et la borne +DC du W485, le pôle négatif sur les bornes AC/−DC et −DC ; liaison RS485 (« RS485 connection »), jusqu'à 100 m (« up to 100m ») : A 485 – A 485, B 485 – B 485.

- 1 bloc d'alimentation (« Power supply »), 10–28 V DC, 0,5 A

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

3.8 Module Ethernet E485

Le module **E485** fait la même chose par Internet filaire : les messages du GATOR vers le centre de télésurveillance et l'application Protegus 2 passent par le câble Ethernet branché sur le routeur, l'appareil n'utilise pas l'Internet mobile, et le réseau mobile ne sert que de secours : si l'Internet filaire est interrompu, il envoie les messages par l'Internet mobile, puis de nouveau par l'E485 au retour de la liaison filaire. À partir du firmware **1.06** ; bus RS485 jusqu'à 100 m au maximum ; alimentation 10–28 V DC commune ; utilisable aussi sans carte SIM. Configuration au point 5.4.

Module Ethernet Trikdis E485 (RS485)

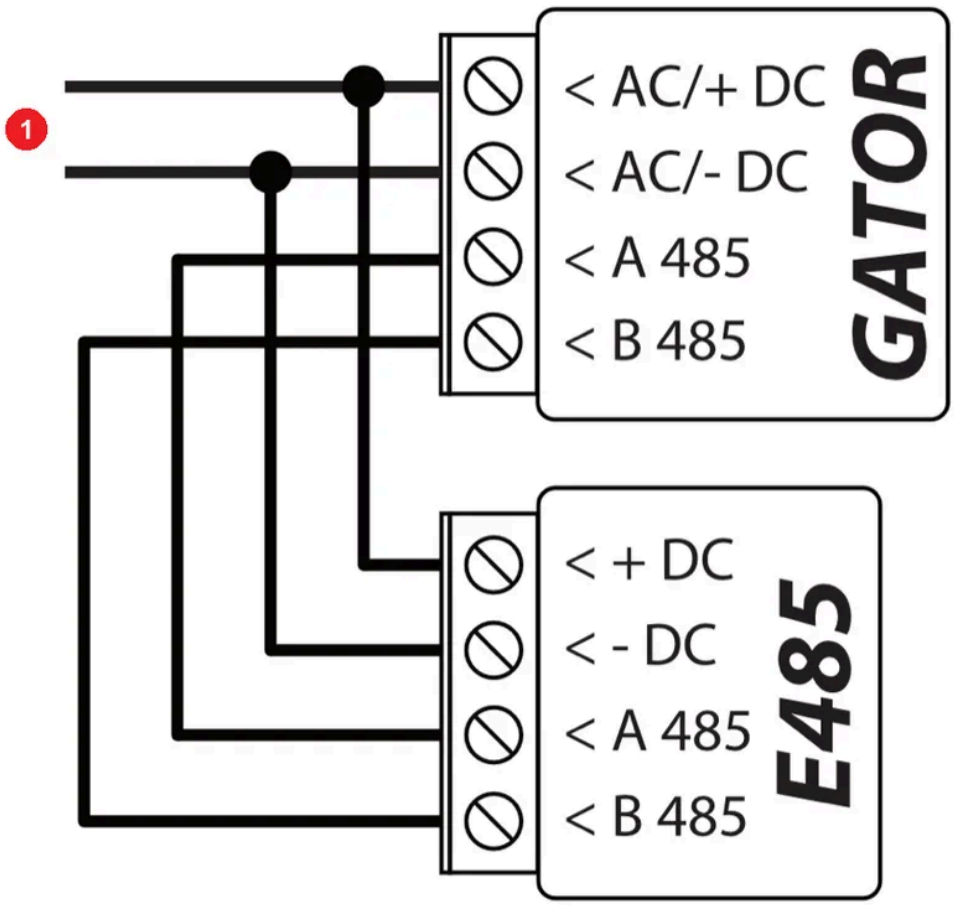


Figure 14. Raccordement du module E485 : le pôle positif du bloc d'alimentation 10–28 V DC, 0,5 A sur la borne AC/+DC du GATOR et la borne +DC de l'E485, le pôle négatif sur les bornes AC/−DC et −DC ; liaison RS485 (« RS485 connection »), jusqu'à 100 m (« up to 100m ») : A 485 – A 485, B 485 – B 485.

- 1 bloc d'alimentation (« Power supply »), 10–28 V DC, 0,5 A

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

3.9 RF-LORA et iO-LORA avec lecteur RFID

À partir du firmware **2.13** du GATOR, le système peut être étendu sans fil : l'émetteur-récepteur **RF-LORA** se raccorde au bus RS485 et maintient par radio la liaison avec jusqu'à **8 modules d'extension iO-LORA** (jusqu'à 5000 m en champ libre). Chaque module iO-LORA ajoute une entrée et une sortie relais au GATOR, et un lecteur RFID Wiegand 26/34 propre peut y être raccordé : le lecteur ne commute **que la sortie relais de son propre module**, aucune sortie distante. Un seul GATOR peut ainsi commander jusqu'à 8 portails ou barrières éloignés les uns des autres, chacun avec son propre lecteur de cartes et son propre bouton de sortie – détails de la solution : Contrôle d'accès sans fil flexible avec le système GATOR RF-LoRa.

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

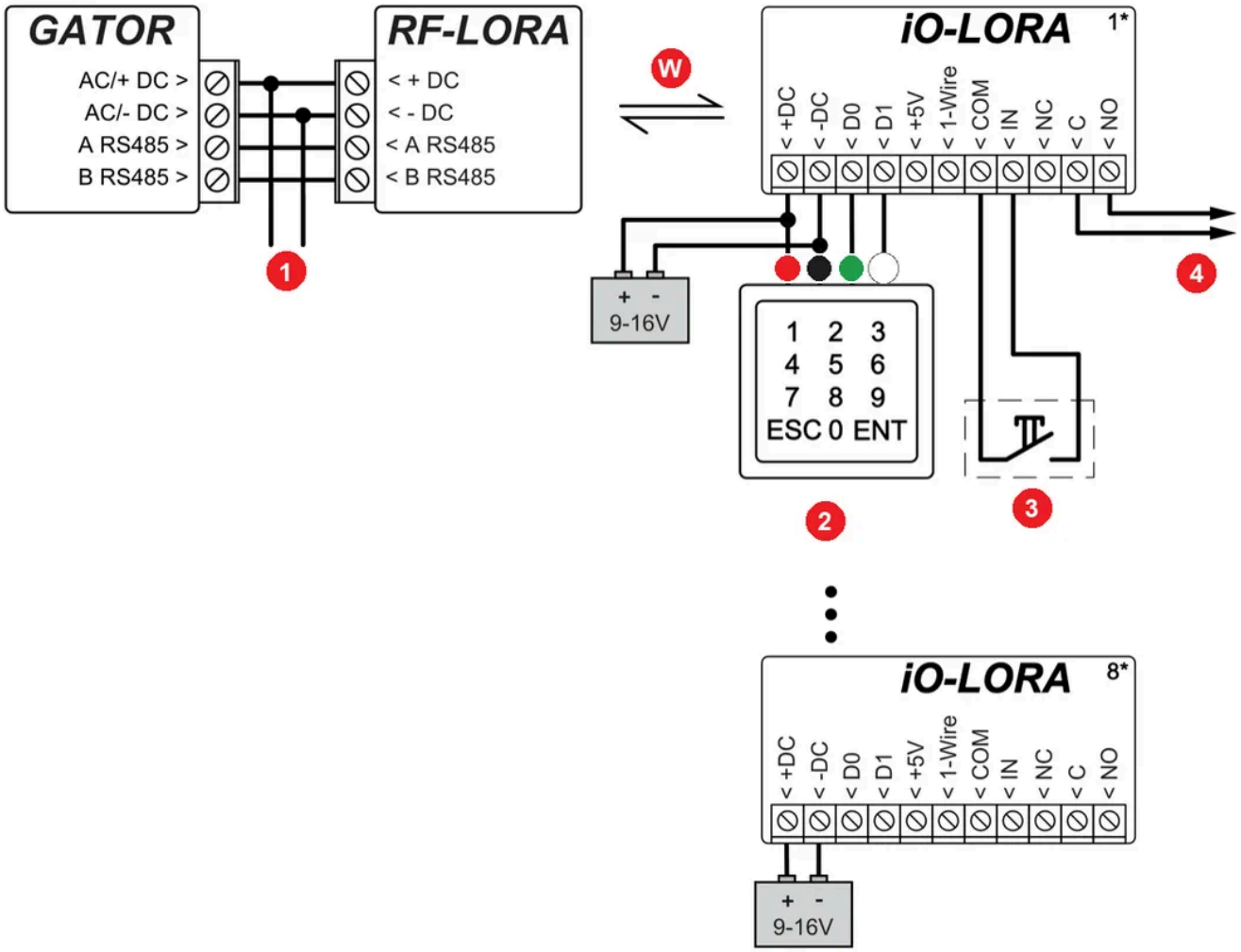


Figure 15. Émetteur-récepteur RF-LORA sur le GATOR et modules d'extension iO-LORA avec lecteur RFID : alimentation commune 9–16 V DC, 0,5 A pour le GATOR et le RF-LORA (AC/+DC – +DC, AC/−DC – −DC) ; RS485 : A–A, B–B ; liaison radio entre le RF-LORA et les modules iO-LORA 1…8, jusqu'à 5000 m ; chaque iO-LORA a sa propre alimentation 9–16 V ; le lecteur sur l'iO-LORA : rouge (+U) sur +DC, noir (GND) sur −DC, vert sur D0, blanc sur la borne D1 ; bouton-poussoir de sortie entre les bornes COM et IN de l'iO-LORA ; la motorisation sur les contacts C et NO du relais de l'iO-LORA (2 A / 230 V AC).

- 1 bloc d'alimentation continue (« DC power supply »), 9–16 V, 0,5 A
- W liaison sans fil (« Wireless connection »), jusqu'à 5000 m (« up to 5000 m »)
- 2 lecteur RFID avec clavier, Wiegand 26/34 (« RFID reader with keypad (Wiegand 26/34) »)
- 3 bouton-poussoir de sortie (« »Exit« button »)
- 4 commande du portail (« Gate control ») – l'entrée de commande de la motorisation ; pouvoir de coupure du relais de l'iO-LORA 2 A / 230 V AC
- fil rouge, +U (« R - red (+U) »)
- fil noir, GND (« B - black (GND) »)
- fil vert, D0 (« G - green (D0) »)
- fil blanc, D1 (« W - white (D1) »)

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.

Configuration dans TrikdisConfig (la description des fenêtres se trouve au chapitre 5) :

1. Lancez TrikdisConfig, raccordez le GATOR à l'ordinateur avec un câble USB Mini-B, ou connectez-vous à distance, et lisez les réglages (**Read [F4]** – le logiciel affiche les réglages actuels de l'appareil). Si le logiciel le demande, saisissez le code administrateur ou installateur à 6 chiffres dans la fenêtre qui

s'ouvre. Sur la page **Modules**, choisissez dans la liste l'élément **iO-LORA controller** et saisissez dans le champ **Serial No.** le numéro de série à six chiffres du module d'extension (sur l'étiquette du module). Le RF-LORA n'a pas besoin d'être ajouté séparément.



Figure 16. TrikdisConfig – Modules : le module d'extension iO-LORA est sélectionné, le numéro de série se saisit dans le champ **Serial No.**.

2. Pour chaque module iO-LORA ajouté, une entrée (par exemple **6 IN iO-LORA 1**) et une sortie (**7 OUT iO-LORA 1**) apparaissent dans la liste de la page **IN/OUT**. Réglez la fonction de l'entrée sur **Exit button** (c'est là que les bornes IN et COM du module raccordent le bouton de sortie) : lorsqu'on appuie dessus, le relais du module (dans l'exemple **7 OUT**) s'active pendant la durée d'impulsion réglée. Le type de la sortie est **Pulse**, la durée d'impulsion correspond à la motorisation (dans l'exemple 3 s).

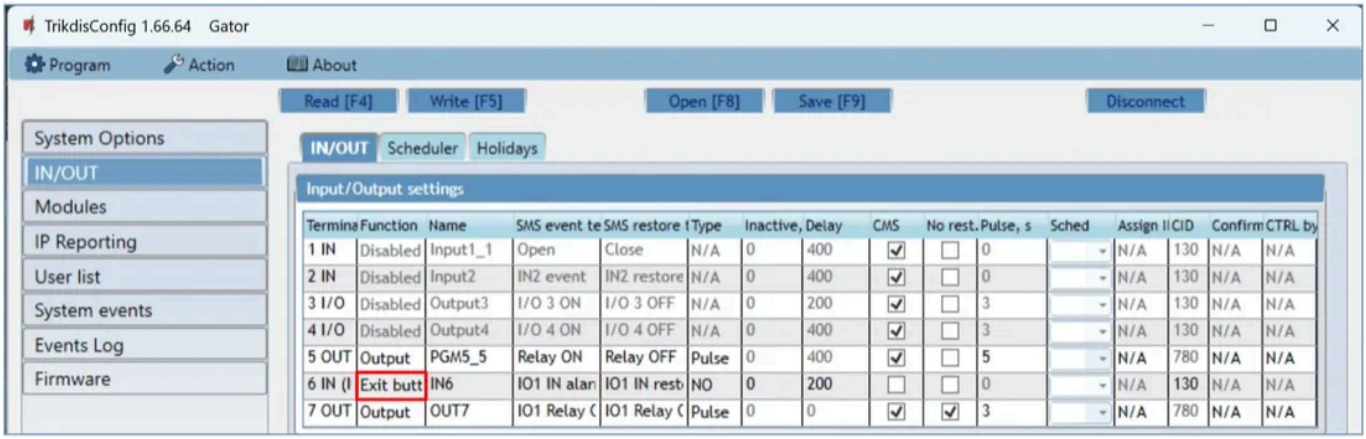


Figure 17. TrikdisConfig – IN/OUT : la fonction de **6 IN** est **Exit button**, la sortie **7 OUT** est de type **Pulse**, avec une impulsion de 3 s.

3. Sur la page **User list**, saisissez le nom de l'utilisateur, le numéro de la carte RFID (**Phone/RFID**), le code pour un lecteur à code, cochez la case **En** et indiquez la sortie qu'il peut commander (dans l'exemple la 7). Écrivez les réglages (**Write [F5]**), attendez la fin de la mise à jour, puis **Disconnect** et débranchez le câble USB.

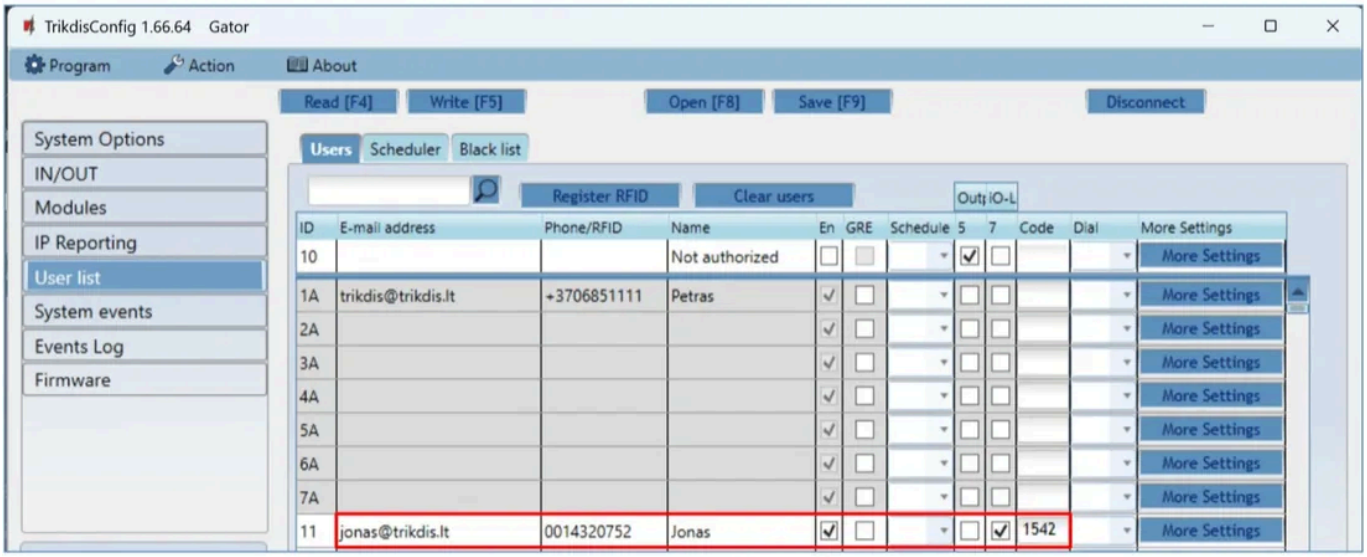


Figure 18. TrikdisConfig – User list : pour l'utilisateur, le numéro RFID, le nom et le code sont renseignés, **En** est coché, la sortie 7 est cochée.

4. **Vérification :** activez la sortie avec la carte ou le code, puis appuyez sur le bouton de sortie – les deux fois, le relais doit s'enclencher pendant la durée d'impulsion réglée.

3.10 Modules d'extension iO8 et iO8-LORA

Si vous avez besoin de davantage d'entrées ou de sorties en un même endroit, vous pouvez associer au GATOR **un seul** module d'extension **iO8** (filaire, RS485) ou **iO8-LORA** (sans fil, via le RF-LORA). Les entrées et sorties du module apparaissent dans la liste de la page **IN/OUT** et se gèrent comme celles du GATOR ; le module doit être ajouté sur la page **Modules** avec son numéro de série (point 5.4).

Module Trikdis IO8 Wired Expander **Module d'expanneur sans fil Trikdis Io8-Lora**

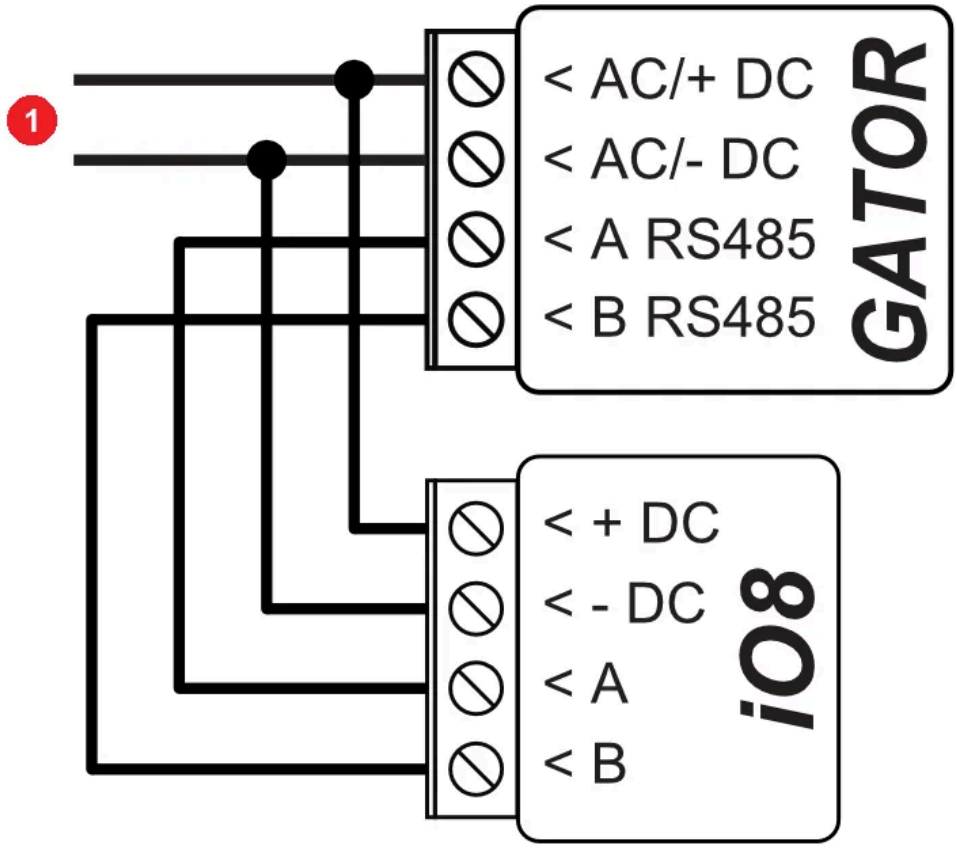


Figure 19. Raccordement du module d'extension iO8 : le pôle positif du bloc d'alimentation 10–28 V DC, 0,5 A sur la borne AC/+DC du GATOR et la borne +DC de l'iO8, le pôle négatif sur les bornes AC/−DC et −DC ; liaison RS485 (« RS485 connection »), jusqu'à 100 m (« up to 100m ») : la borne A RS485 du GATOR sur la borne A de l'iO8, B RS485 sur la borne B.

- 1 bloc d'alimentation (« Power supply »), 10–28 V DC, 0,5 A

L'iO8 fonctionne sur 10–26 V DC : si le bloc d'alimentation fournit une tension supérieure à 26 V, l'iO8 reçoit un bloc d'alimentation séparé, les pôles négatifs des deux alimentations étant reliés.

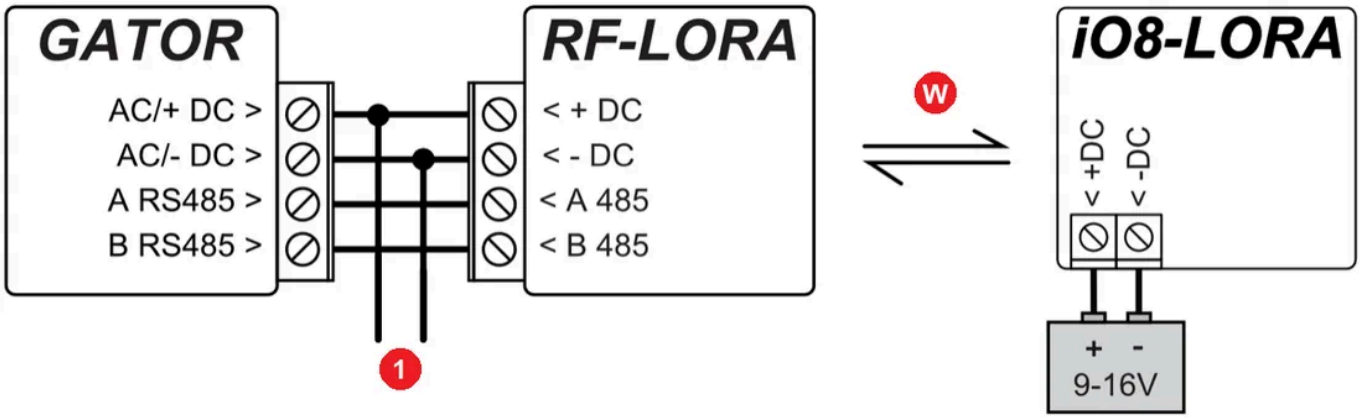


Figure 20. Le module d'extension iO8-LORA via l'émetteur-récepteur RF-LORA : alimentation 9–16 V DC, 0,5 A pour le GATOR et le RF-LORA (AC/+DC – +DC, AC/−DC – −DC) ; RS485 : A RS485 – A 485, B RS485 – B 485 ; liaison radio entre le RF-LORA et l'iO8-LORA, jusqu'à 5000 m ; l'iO8-LORA a sa propre alimentation 9–16 V.

- 1 bloc d'alimentation continue (« DC power supply »), 9–16 V, 0,5 A
- 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.

4. Commande à distance

Vous pouvez commander le GATOR de quatre façons : par **appel téléphonique** (gratuit, car l'appareil ne décroche pas), pendant l'appel avec le **clavier du téléphone** (DTMF), depuis l'application **Protegus 2** ou avec un **widget** placé sur l'écran d'accueil du téléphone, et par **commande SMS**. Dans les quatre cas, c'est la liste des utilisateurs (point 5.6) qui détermine qui peut faire quoi ; avec les commandes SMS, l'administrateur peut aussi modifier les réglages.

4.1 Commande par appel téléphonique

Appelez le numéro de la carte SIM insérée dans le GATOR. L'appareil **rejette automatiquement** l'appel et active la sortie relais **5 OUT** pendant **3 secondes** – l'appel ne coûte rien. Par défaut, toute personne connaissant son numéro peut ainsi commander l'appareil.

- **Uniquement les personnes autorisées** : dès que vous enregistrez ne serait-ce qu'un seul numéro dans la liste des utilisateurs (par SMS : `SETU …`, point 4.7 ; dans TrikdisConfig ou dans l'application), le GATOR ne réagit plus qu'aux appels provenant des numéros de la liste. Dans TrikdisConfig, la même chose se commande avec la case **En** de l'entrée n° 10 de la **User list**, nommée **Not authorized** (point 5.6) : cochée, n'importe qui peut appeler ; décochée, seuls les membres de la liste.
- **Quelle sortie s'ouvre** : si un utilisateur peut commander plusieurs sorties, ce sont les sorties cochées dans la colonne **Dial** qui commutent lors de l'appel, puis l'appareil raccroche.
- **Durée de l'appel** : avec la valeur 0 dans **System Options** → **Hang-up after**, l'appareil rejette immédiatement l'appel ; avec une valeur plus élevée, il décroche et raccroche au bout du temps indiqué – c'est nécessaire pour la commande au clavier (point 4.2).

La **première** personne qui appelle le GATOR dans son état d'usine, ou qui lui envoie le premier SMS, en devient l'**administrateur** : par la suite, elle seule peut le gérer par commandes SMS. Passez donc le premier appel depuis le téléphone du propriétaire ou de l'installateur.

4.2 Commande au clavier du téléphone (DTMF)

Si le GATOR décroche (**Hang-up after** supérieur à 0), l'utilisateur peut commuter plusieurs sorties avec le clavier du téléphone :

1. Appelez le numéro de la carte SIM du GATOR – l'appareil décroche.
2. Tapez la commande sur le clavier du téléphone selon le tableau.

Code DTMF	Fonction	Description
`SORTIE*ÉTAT#`	commande d'une sortie	**SORTIE** – le numéro de la sortie. **ÉTAT** – 0 : désactivation ; 1 : activation ; 2 : désactivation pendant la durée d'impulsion ; 3 : activation pendant la durée d'impulsion (la durée d'impulsion se règle dans le tableau **IN/OUT** de TrikdisConfig). **#** – fin de la commande. Exemple – activation de la sortie 5 : `5*1#` ; activation de la sortie 4 pendant la durée d'impulsion : `4*3#`
`#`	fin de la commande	si vous vous êtes trompé dans la commande, appuyez sur la touche **#** et tapez-la de nouveau

La commande au clavier (DTMF) ne fonctionne pas sur les appareils de type **GV17_2E70** et **GV17_2S70**. Vous voyez le type exact dans la barre d'état de TrikdisConfig (point 5.1).

4.3 Commande depuis l'application Protegus 2

Dans Protegus 2, l'utilisateur ouvre le portail depuis n'importe où, voit l'état du système et l'état du portail (si l'état du portail est raccordé, points 3.5 et 5.10), reçoit tous les événements du système par notification push et, en tant qu'administrateur, gère aussi les utilisateurs. L'application est gratuite ; sur téléphone, vous la téléchargez depuis les boutiques d'applications, dans un navigateur elle s'ouvre à l'adresse https://web.protegus.app.

Avant d'ajouter le système

Dans TrikdisConfig, sur la page **IP Reporting**, la case **Enable cloud service** doit être cochée (point 5.5 ; par SMS : `CONNECT 123456 PROTEGUS=ON`), l'alimentation doit être correcte (la LED **POWER** clignote en vert) et l'appareil doit être connecté au réseau (la LED **NETWORK** est allumée en vert et clignote en jaune). La carte SIM doit disposer d'un service de données mobiles, ou un module W485 / E485 doit être présent.

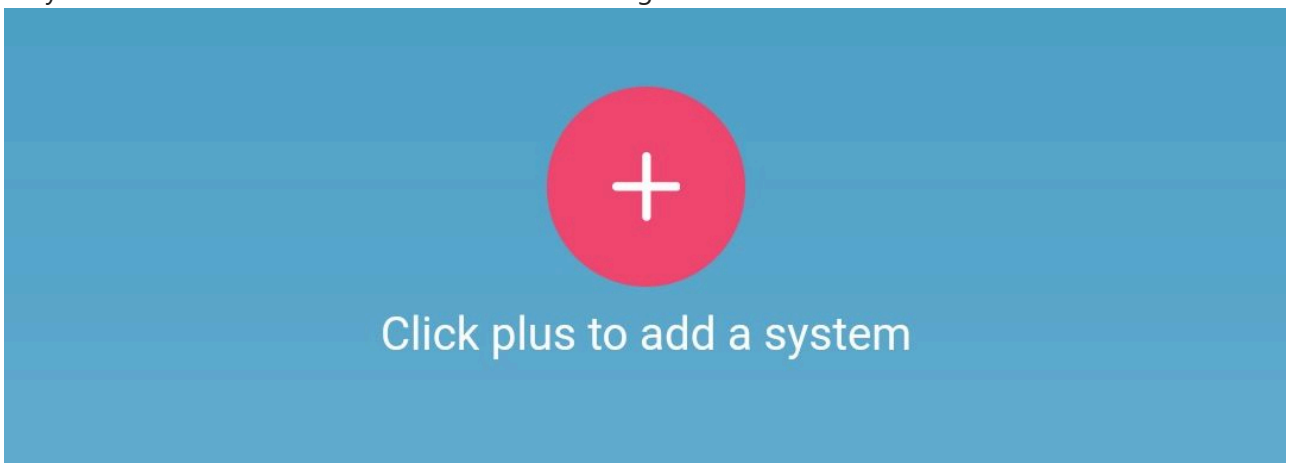
La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur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

A rendszer létrehozása a Protegus 2 alkalmazásban

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



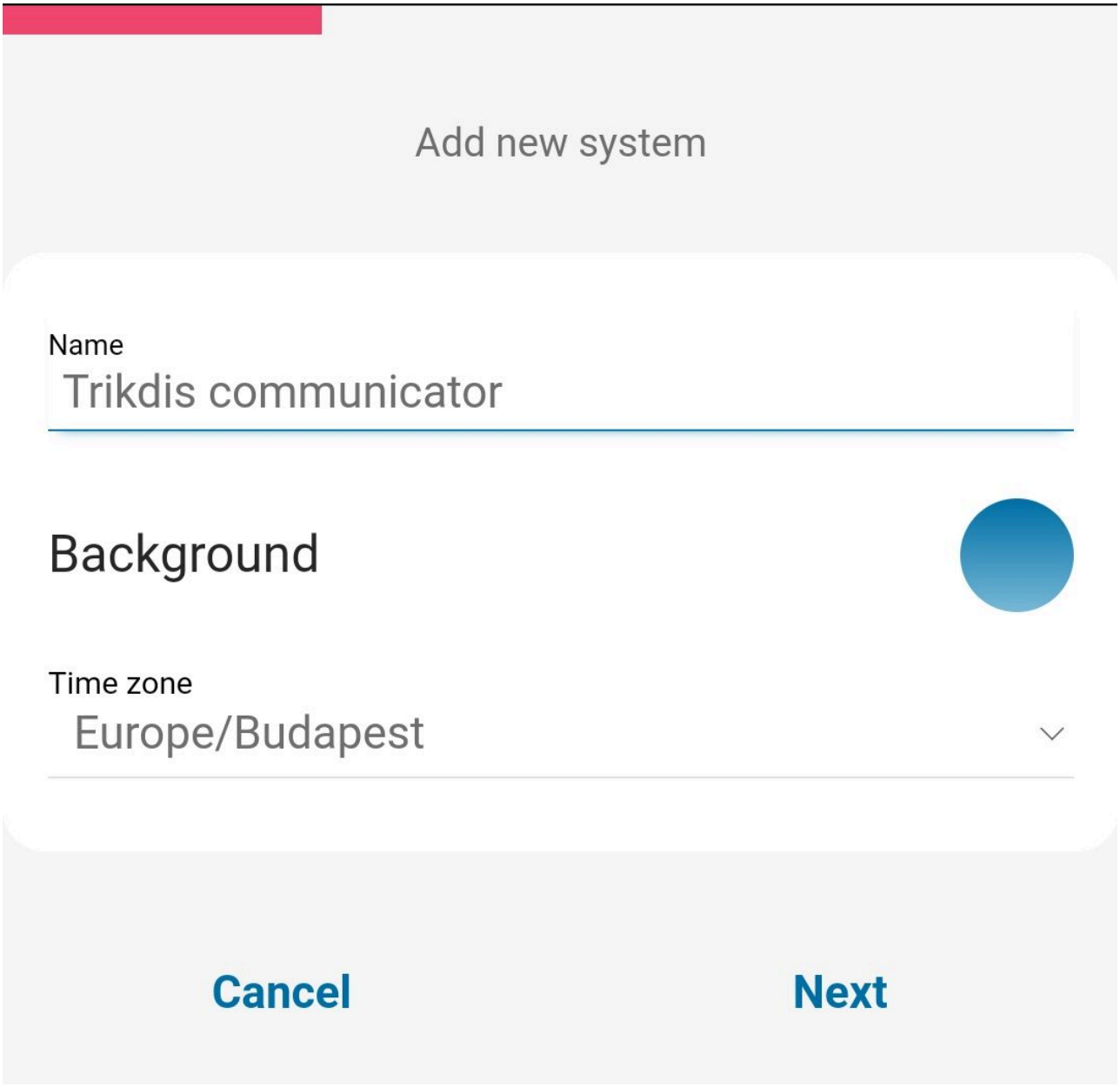
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



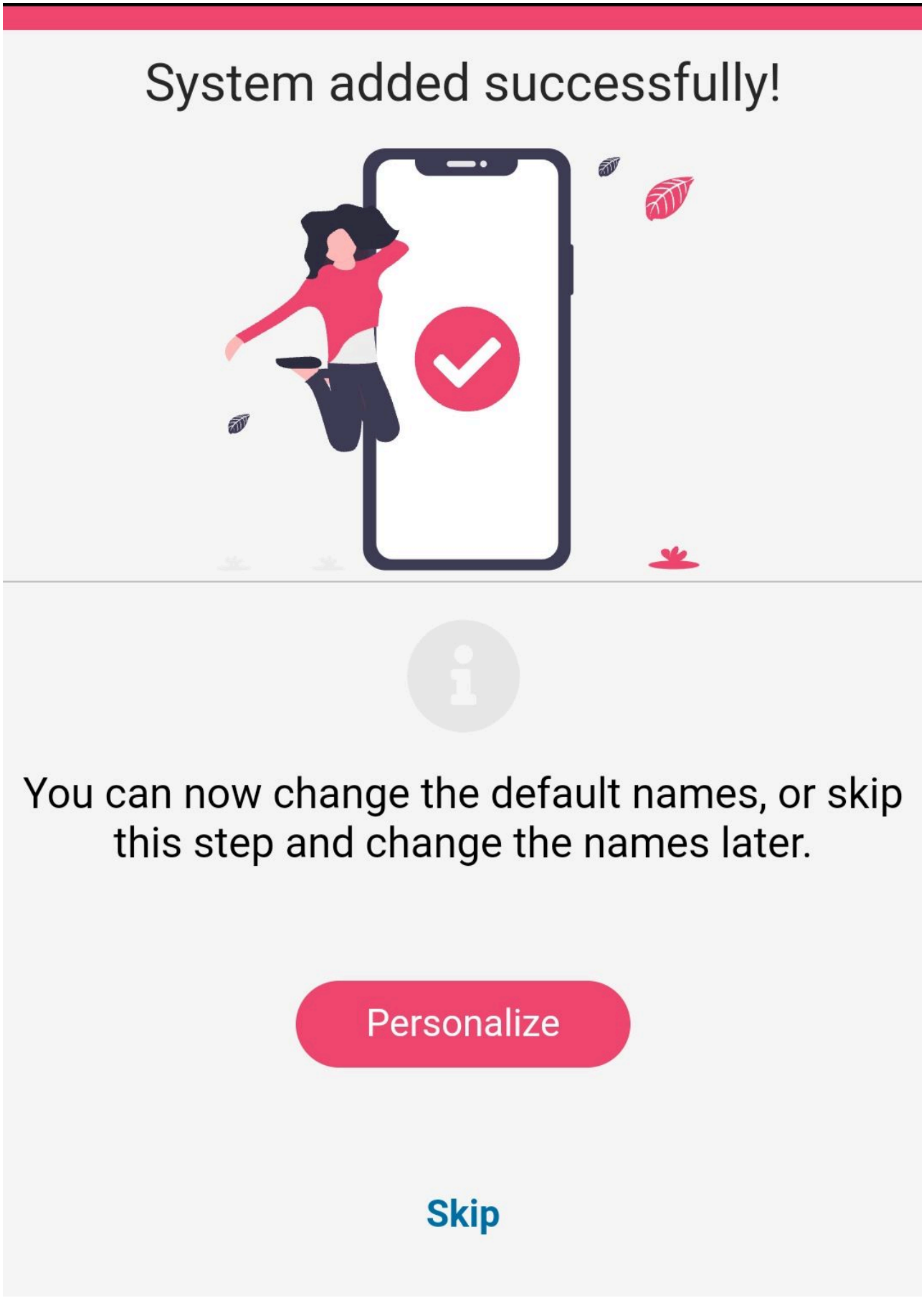
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



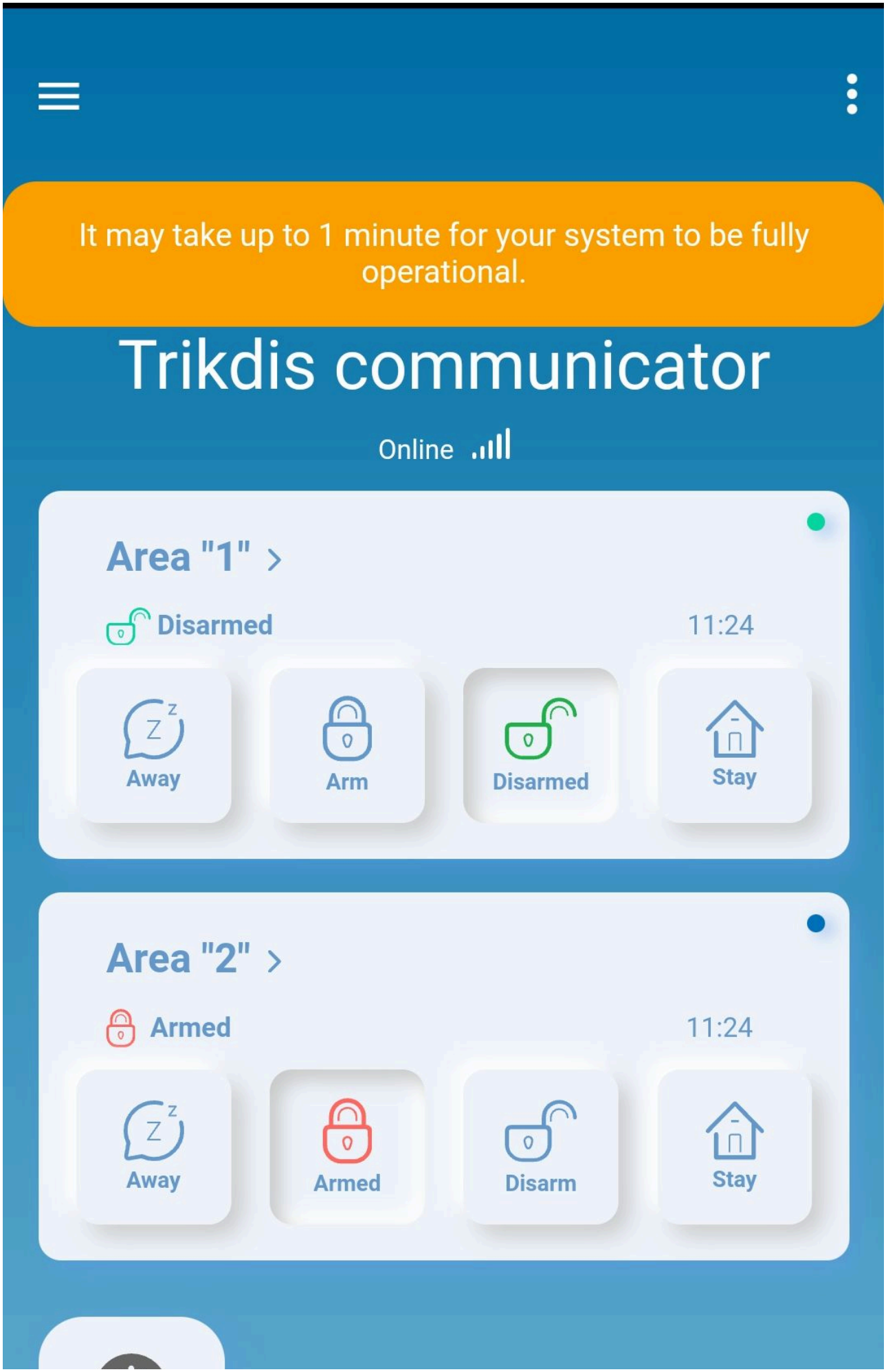
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Pour le GATOR, lors de l'ajout, tenez compte des points suivants :

1. L'identifiant unique est le numéro **IMEI** du GATOR : il figure sur l'étiquette sous l'appareil et sur la boîte, et vous le voyez aussi dans la barre d'état de TrikdisConfig ; vous pouvez également lire le QR code de l'étiquette avec l'appareil photo du téléphone. Si l'installateur a modifié la valeur par défaut `123456` du **Cloud Access Code**, l'application la demande aussi.
2. Après avoir saisi le nom du système, vous pouvez passer l'étape **Personalize** avec le bouton **Skip** : vous pourrez renommer les sorties et les entrées plus tard.
3. Attendez que le bandeau sur fond jaune disparaisse – le système devient opérationnel en 1 minute au maximum.

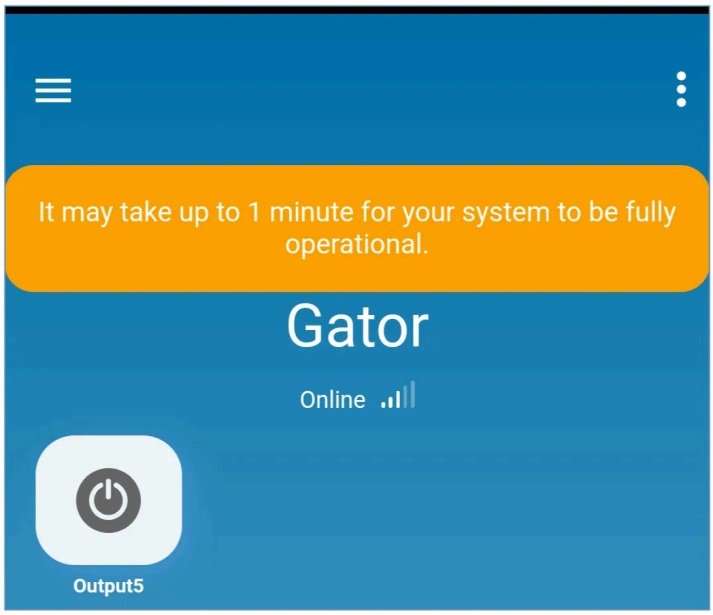


Figure 21. Le GATOR dans Protegus 2 après l'ajout : le système est **Online**, le bandeau jaune indique qu'il faut attendre 1 minute au maximum avant le fonctionnement complet.

4. Vous ouvrez le portail avec le bouton **Output5**. **Astuce :** appuyez longuement sur le bouton, choisissez la modification, puis touchez l'icône pour choisir une icône adaptée à l'usage (portail, barrière, garage), et enregistrez. Si l'état du portail est raccordé, l'icône montre aussi l'état ouvert ou fermé du portail.

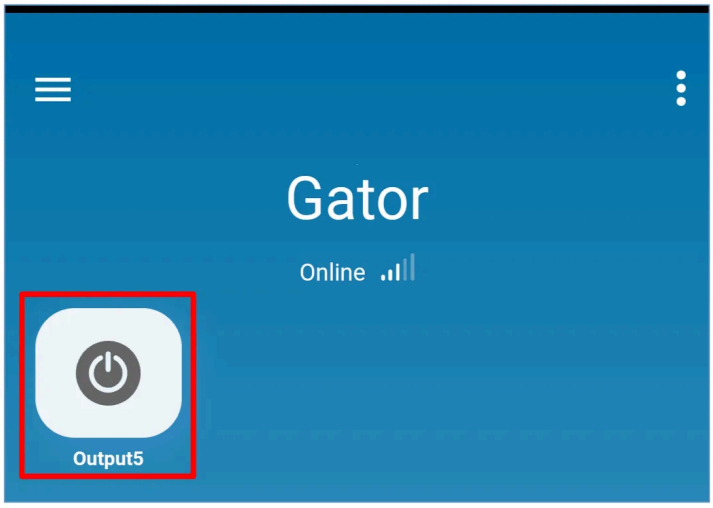


Figure 22. L'écran d'accueil du système avec le bouton **Output5** – c'est lui qui commute le relais du GATOR.

Voir aussi

Le dispositif d'automatisation de portail GV17 fonctionne avec Protegus 2 · Application Protegus Android / iPhone et web · Notifications push dans le navigateur avec l'application Protegus 2

4.4 Widget sur l'écran d'accueil du téléphone

Vous pouvez aussi placer le bouton d'ouverture du portail sur l'écran d'accueil du téléphone : vous ouvrez ainsi d'une seule touche, sans ouvrir l'application. Cela fonctionne **uniquement sous Android** ; la façon de placer le widget peut légèrement varier d'un téléphone à l'autre. Le GATOR doit être ajouté à Protegus 2 et vous devez être connecté à l'application ; fermez ensuite la fenêtre de l'application.

1. Appuyez longuement sur une partie vide de l'écran d'accueil et, dans la barre qui apparaît, choisissez l'élément **Widgets**.
2. Cherchez **Protegus 2** dans la liste et choisissez le widget **Switch Protegus 2**.
3. Choisissez la sortie à commander (par exemple **Gator Output5**) et appuyez sur le bouton **ADD WIDGET**.
4. Le bouton apparaît sur l'écran d'accueil. Essayez-le : revenez à l'écran d'accueil et appuyez sur le bouton – après l'appui, un indicateur circulaire montre que la sortie s'est activée ; si l'état du portail est raccordé, la couleur du bouton montre l'état ouvert ou fermé du portail.



Figure 23. Étape 1 – l'option de menu **Widgets** après un appui long sur l'écran d'accueil.

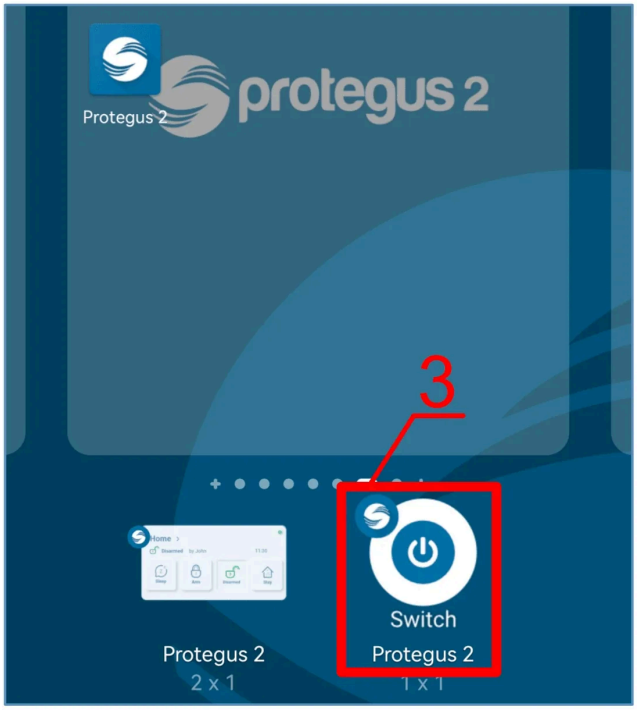


Figure 24. Étape 2 – parmi les widgets de Protegus 2, **Switch Protegus 2**.



Figure 25. Étape 3 – choix de la sortie **Gator Output5** et bouton **ADD WIDGET**.



Figure 26. Étape 4 – le widget **Output5** sur l'écran d'accueil ; le bouton vert indique la sortie activée (portail ouvert).

4.5 Utilisateurs dans l'application

En tant qu'administrateur, vous pouvez aussi ajouter et supprimer des utilisateurs dans Protegus 2 ; l'utilisateur ajouté voit et ouvre le portail depuis son propre compte, et il peut aussi recevoir des notifications par SMS (si le message de bienvenue **HELLO** est activé, il reçoit un SMS l'informant de son ajout).

1. Lancez l'application Protegus 2 sur votre téléphone et connectez-vous avec votre nom d'utilisateur et votre mot de passe. Sur l'écran du système, ouvrez le menu **Settings** (paramètres), puis l'option **System configuration**.
2. Choisissez la liste **Users** (utilisateurs) et appuyez sur le bouton **+** (**Add new user** – nouvel utilisateur).
3. Saisissez l'**adresse e-mail**, le **nom** et le **numéro de téléphone** de l'utilisateur (ou le numéro de la carte RFID, point 5.6), pour un lecteur à code son **code** à 4 chiffres, et indiquez la sortie qu'il peut commander (**Output5**).
4. Appuyez sur le bouton **Add user** (ajouter l'utilisateur) : le nouvel utilisateur apparaît dans la liste. Le bouton **Back** vous ramène à la fenêtre principale.

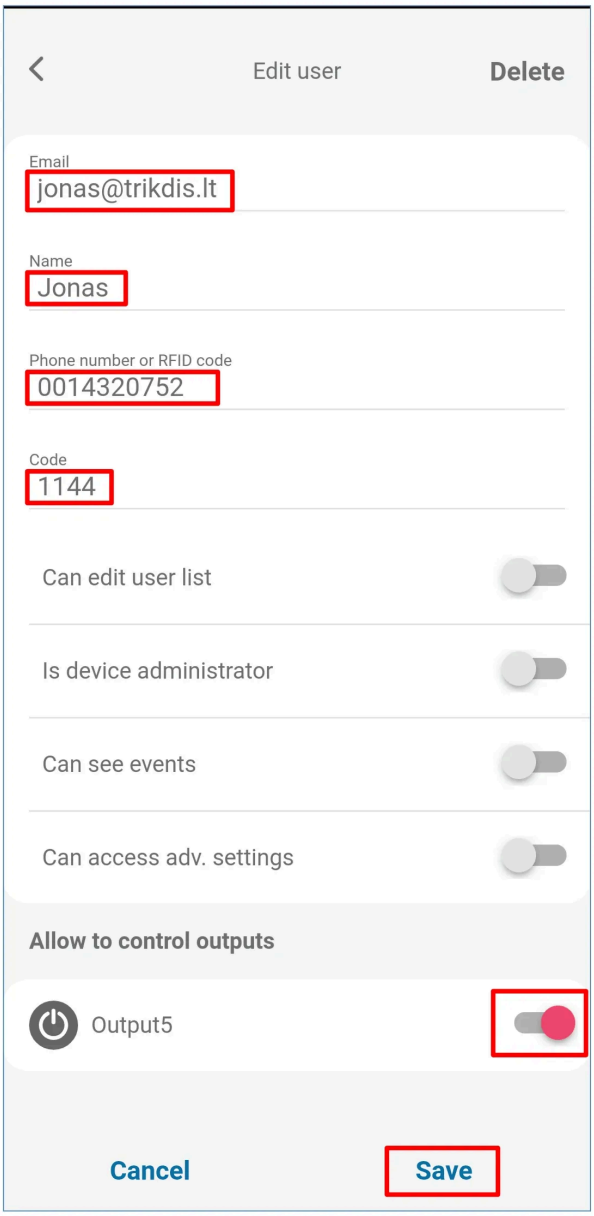


Figure 27. Modification d'un utilisateur dans Protegus 2 : adresse e-mail, nom, numéro de téléphone ou numéro de carte RFID, code, et autorisation de commander **Output5**.

4.6 Commande par SMS

Vous commutez la sortie relais (**OUTPUT5**) avec ces commandes SMS ; `xxxxxx` est le mot de passe administrateur à 6 chiffres (par défaut `123456`). Vous pouvez aussi commuter d'autres sorties par SMS, mais elles doivent d'abord être réglées en sortie dans TrikdisConfig (point 5.3).

Commande	Paramètre	Description
`OUTPUTx xxxxxx ON`	ON	activation de la sortie ; **x** est le numéro de la sortie. Exemple : `OUTPUT5 123456 ON`
`OUTPUTx xxxxxx OFF`	OFF	désactivation de la sortie. Exemple : `OUTPUT5 123456 OFF`
`OUTPUTx xxxxxx PULSE=ttt`	PULSE=ttt	activation de la sortie pendant **ttt** secondes (1–999, sur trois chiffres). Exemple : `OUTPUT5 123456 PULSE=002`

4.7 Programmation par SMS

L'appareil n'accepte les commandes SMS que depuis les numéros **administrateurs** (1A–7A) ; chaque commande contient le mot de passe administrateur à 6 chiffres. L'appareil envoie un SMS de réponse sur l'exécution si l'option **ACK for SMS message** est activée pour l'administrateur (point 5.6).

Changement du mot de passe administrateur – pour des raisons de sécurité, ce doit être votre première action :

```
PSW 123456 xxxxxx
```

`123456` – le mot de passe par défaut ; `xxxxxx` – le nouveau mot de passe de 6 caractères.

Commande réservée aux personnes autorisées – envoyez les données des utilisateurs depuis le téléphone de l'administrateur :

```
SETU xxxxxx +PHONENO#NAME#EMAIL
```

`PHONENO` – le numéro de téléphone de l'utilisateur au format international (+33…) ; `NAME` – son nom ; `EMAIL` – son adresse e-mail (pour Protegus 2). Une fois le premier numéro enregistré, le GATOR ne réagit plus qu'aux appels provenant des numéros de la liste.

Droits d'administrateur pour une autre personne – les autres administrateurs reçoivent les messages du système et peuvent ajouter des utilisateurs :

```
SETA xxxxxx Nox=+PHONENO#NAME#EMAIL
```

`Nox` – le numéro d'ordre de l'administrateur dans la liste (1–7) ; si vous indiquez **1**, vous transférez vos propres droits d'administrateur.

Liste des commandes SMS (dans chacune, le mot de passe suit le mot de commande ; dans les exemples, le mot de passe par défaut `123456`) :

Commande	Paramètre	Description
`INFO`	–	informations sur l'appareil : type, IMEI, niveau du signal, tension d'alimentation, version du firmware, numéro de série, date et heure. Exemple : `INFO 123456`
`ASKI`	–	état des entrées. Exemple : `ASKI 123456`
`ASKO`	–	état des sorties. Exemple : `ASKO 123456`
`SETA`	`NoX=numéro de téléphone#nom#e-mail`	ajout d'un administrateur à la ligne X (1A–7A) ; le numéro doit commencer par le signe + et l'indicatif du pays, les champs sont séparés par #. Exemple : `SETA 123456 No3=+33612345678#Jean#jean@exemple.fr`
`SETA`	`NoX=DEL`	suppression de l'administrateur X. Exemple : `SETA 123456 No2=DEL`
`SETU`	`numéro de téléphone#nom#e-mail`	ajout d'un nouvel utilisateur (lignes 11–1010) ; ici aussi, le numéro doit commencer par le signe + et l'indicatif du pays, les champs sont séparés par #. Exemple : `SETU 123456 +33612345678#Pierre#pierre@exemple.fr`
`DELU`	`numéro de téléphone` ou `nom`	suppression d'un utilisateur d'après son numéro de téléphone ou son nom. Exemple : `DELU 123456 +33612345678`, `DELU 123456 Pierre`

Commande	Paramètre	Description
`SETB`	`e-mail` ou `numéro de téléphone`	ajout à la liste noire (adresse e-mail ou numéro de téléphone). Exemple : `SETB 123456 jean@exemple.fr`, `SETB 123456 +33612345678`
`DELB`	`ALL`	suppression de toute la liste noire. Exemple : `DELB 123456 ALL`
`DELB`	`e-mail` ou `numéro de téléphone`	suppression d'une entrée de la liste noire (pour une adresse e-mail, les majuscules et minuscules comptent). Exemple : `DELB 123456 jean@exemple.fr`, `DELB 123456 +33612345678`
`RESET`	–	redémarrage de l'appareil. Exemple : `RESET 123456`
`PSW`	`nouveau mot de passe`	changement du mot de passe administrateur. Exemple : `PSW 123456 654123`
`TXTA`	`nom de l'objet`	réglage du nom de l'objet. Exemple : `TXTA 123456 Maison`
`TXTE`	`N1=texte` … `N5=texte`	texte du SMS envoyé à l'activation de l'entrée ou de la sortie ; N1…N5 est le numéro de la borne. Exemple : `TXTE 123456 N1=Portail ouvert`
`TXTR`	`N1=texte` … `N5=texte`	texte du SMS envoyé au rétablissement. Exemple : `TXTR 123456 N5=Relais desactive`
`SETD`	`IDx=yy`	durée d'inactivité de l'entrée x en minutes (0–2880) : après une activation, l'appareil envoie une notification et ne réagit pas aux nouveaux changements de l'entrée pendant cette durée ; 0 = désactivé. Exemple : `SETD 123456 ID1=30`
`RESD`	`IDx`	annulation de la durée d'inactivité déjà en cours de l'entrée x. Exemple : `RESD 123456 ID1`
`TIME`	`AAAA/MM/JJ,HH:MM:SS`	réglage de la date et de l'heure. Exemple : `TIME 123456 2026/10/30,12:23:00`
`RDR`	`numéro de téléphone#texte`	transfert d'un SMS vers le numéro indiqué (par exemple recharge de crédit auprès de l'opérateur). Exemple : `RDR 123456 +33612345678#Recharge 10 EUR`
`HELLO`	`ON` / `OFF`	notification par SMS du nouvel utilisateur lors de son ajout (utilisateur ajouté depuis l'application ou par SMS) activée / désactivée. Exemple : `HELLO 123456 ON`
`NATH`	`ON` / `OFF`	activation et désactivation du mode **Not authorized** (n'importe qui peut appeler) sans modifier les autres réglages ; avec plusieurs sorties, en énumérant les sorties commutées par appel (active le mode **Not authorized** et les sorties énumérées, désactive les autres sorties). Exemple : `NATH 123456 ON`, `NATH 123456 ON=5,7,22`, `NATH 123456 OFF`
`UUSD`	`*code#`	envoi d'un code USSD à l'opérateur mobile (consultation du crédit, recharge). Exemple : `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON` / `Protegus=OFF`	connexion au cloud Protegus ou déconnexion. Exemple : `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`APN=nom`, `USER=nom`, `PSW=mot de passe`	nom d'APN, nom d'utilisateur et mot de passe de la liaison de données mobile. Exemple : `CONNECT 123456 APN=INTERNET`
`CONNECT`	`Code=mot de passe`	changement du code d'accès au cloud Protegus (**Cloud Access Code**). Exemple : `CONNECT 123456 Code=123456`

Remplacez l'indicatif du pays et l'adresse e-mail des exemples par vos propres données. Dans les SMS, évitez les lettres accentuées si le réglage **System Options → Text language** n'est pas réglé sur le jeu de caractères adapté (point 5.2). Liste des APN : Réglage de l'APN – liste des opérateurs mobiles européens.

5. Configuration dans TrikdisConfig

Tous les réglages du GATOR sont accessibles avec le logiciel **TrikdisConfig**, qui fonctionne sous Windows – par câble USB ou à distance (chapitre 6). Avec les réglages d'usine, l'appareil ouvre sur appel (chapitre 2) ; le logiciel est nécessaire lorsque vous configurez des utilisateurs, des cartes RFID, une programmation horaire, des textes SMS, des modules, le cloud Protegus ou la télésurveillance.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

1. Retirez la face avant du GATOR avec un tournevis plat, comme sur la figure.
2. Reliez le GATOR à l'ordinateur avec un câble **USB Mini-B**.
3. Lancez TrikdisConfig. Le logiciel reconnaît l'appareil et ouvre la fenêtre de programmation du GATOR.
4. Cliquez sur le bouton **Read [F4]** : le logiciel lit les réglages actuels de l'appareil. S'il le demande, saisissez le code **administrateur** ou **installateur** à 6 chiffres dans la fenêtre qui s'ouvre (le code administrateur par défaut est `123456`).



Figure 28. Retrait de la face avant : en introduisant le tournevis dans la fente latérale et en le poussant vers le bas, le couvercle se déclipse ; dessous se trouve le connecteur USB Mini-B.

Avertissement

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

Le bouton **Restore**, en bas à gauche de la fenêtre de programmation, ramène aux réglages d'usine (point 5.9).

5.1 La barre d'état

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

Libellé	Signification
IMEI / Unique ID, pour un appareil Ethernet **MAC / Unique ID**	Identifiant unique de l'appareil : IMEI pour un appareil à carte SIM, adresse MAC pour un appareil Ethernet. Le même identifiant figure sur la boîte et au dos de l'appareil.
Status	État de fonctionnement actuel.
Device	Type de l'appareil (référence). Vérifiez que c'est bien le type de votre appareil qui figure ici.
SN	Numéro de série.
BL	Version du bootloader.
FW	Version du firmware.
HW	Version du matériel.
State	Mode de connexion : USB ou à distance (remote).
Administrator / Installer	Niveau d'accès de la personne qui programme (après saisie du mot de passe).

Une fois les réglages effectués, vous les écrivez dans l'appareil avec le bouton **Write [F5]** ; les boutons **Open [F8]** et **Save [F9]** permettent d'enregistrer l'ensemble des réglages dans un fichier et de le charger dans un autre appareil. **Save [F9]** enregistre les réglages dans un fichier de configuration, **Open [F8]** ouvre le fichier enregistré ; vous pourrez ensuite charger les réglages enregistrés dans d'autres appareils et configurer ainsi rapidement plusieurs appareils avec des réglages identiques.



Figure 29. La barre d'état du GATOR : dans le champ de gauche **IMEI/Unique ID**, en bas **Status: reading done**, **Device: GV17_2200** (le code de type), le numéro de série, les versions **BL** et **FW**, le mode de connexion (USB). Pour le GATOR, le champ **Device** doit avoir la forme **GV17_xxxx**.

5.2 Page « System Options »

Les réglages généraux de l'appareil : identifiant, heure, code administrateur, réponse aux appels, test, carte SIM et fuseau horaire.

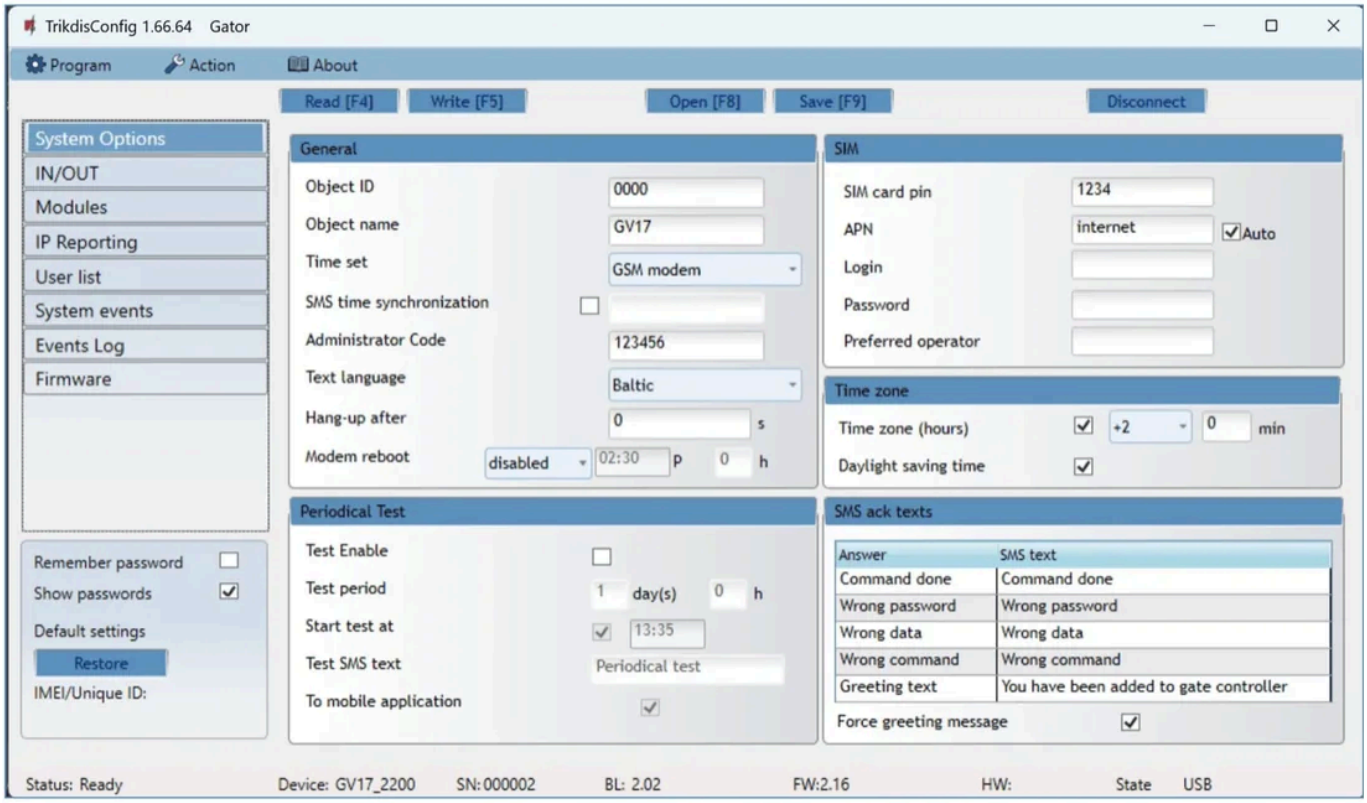


Figure 30. TrikdisConfig – **System Options** : les groupes **General**, **Periodical test**, **SIM**, **Time zone** et **SMS ack texts**.

Groupe General

- **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (nombre hexadécimal à 4 chiffres, 0–9, A–F). N'utilisez pas les valeurs FFFE et FFFF.
- **Object name** – l'appareil envoie chaque événement avec ce nom.
- **Time set** – la source de synchronisation de l'heure (par exemple le réseau mobile).
- **SMS time synchronization** – cochez la case et saisissez le numéro de la carte SIM du GATOR au format international (+33…) si l'heure est synchronisée par SMS.
- **Administrator Code** – le code administrateur : il permet de modifier tous les paramètres du GATOR (par défaut `123456` – changez-le).
- **Text language** – le jeu de caractères des SMS.
- **Hang-up after** – à 0, l'appareil rejette l'appel (il ouvre sur appel) ; avec une autre valeur, il décroche et raccroche au bout du nombre de secondes indiqué – pour la commande au clavier (DTMF) (point 4.2).
- **Modem reboot** – redémarrage quotidien du modem à l'heure indiquée.

Groupe Periodical test

- **Test Enable** – case cochée, l'appareil envoie un rapport de test périodique.
- **Test period** – l'intervalle entre les rapports de test.
- **Start test at** – l'heure du premier test.
- **Test SMS text** – le texte du SMS de test.
- **To mobile application** – case cochée, le rapport de test est aussi envoyé à l'application Protegus 2.

Groupe SIM

- **SIM card PIN** – le code PIN de la carte SIM, si vous n'avez pas désactivé la demande.

- **APN** – le point d'accès de la liaison de données mobile. Avec la case **Auto**, l'appareil choisit un APN dans la liste intégrée (données de plusieurs opérateurs internationaux et nationaux), et n'utilise la valeur saisie dans le champ que s'il ne trouve pas l'opérateur. Si la liaison de données ne s'établit pas, saisissez l'APN de l'opérateur : 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 les demande.
- **Preferred operator** – si vous indiquez un code d'opérateur (MCC + MNC), le GATOR ne se connecte qu'à ce réseau ; c'est utile pour les cartes SIM internationales (itinérance).

Groupe Time zone – c'est ici que vous réglez l'heure exacte du pays : indiquez le fuseau horaire et précisez si le pays applique l'heure d'été.

- **Time zone (hours)** – cochez la case et indiquez le fuseau horaire du pays (France : +1).
- **Daylight saving time** – cochez la case si le pays applique l'heure d'été.

Groupe SMS ack texts – le texte des SMS de réponse que l'utilisateur reçoit après les commandes SMS.

- **Force greeting message** – case cochée, l'appareil envoie un SMS de bienvenue au nouvel utilisateur ajouté par SMS ou depuis Protegus 2 (par SMS : `HELLO 123456 OFF` le désactive).

5.3 Page « IN/OUT »

Les réglages des entrées et sorties, des lecteurs RFID et du relevé du temps de travail, sur trois onglets : **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 Onglet IN/OUT – entrées et sorties

Le tableau comporte une borne par ligne ; c'est ici que vous décidez laquelle est une entrée et laquelle est une sortie, et comment elles signalent.

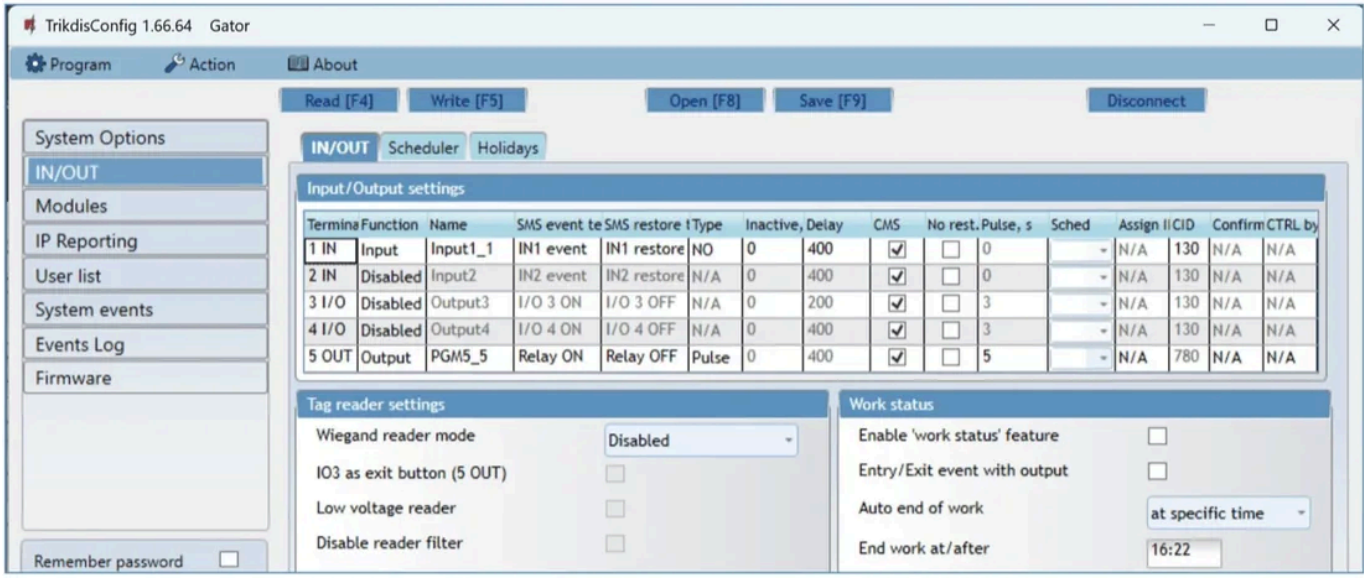


Figure 31. TrikdisConfig – **IN/OUT** : le tableau **Input/Output settings** (par défaut l'entrée 1 IN ; 2 IN, 3 I/O, 4 I/O désactivées ; 5 OUT sortie de type **Pulse**), en dessous les groupes **Tag reader settings** et **Work status**.

Groupe Input/Output settings

- **Terminal** – le numéro des bornes du GATOR (1 IN … 5 OUT ; les bornes des modules d'extension se trouvent en fin de liste).
- **Function** – la fonction de la borne : **Input** (entrée), **Output** (sortie) ou **Disabled** (désactivée).

- **Name** – le nom de l'entrée ou de la sortie (c'est ainsi qu'elle apparaît dans l'application et dans les SMS).
- **SMS event text** – le texte du SMS envoyé à l'activation.
- **SMS restore text** – le texte du SMS envoyé au rétablissement.
- **Type** – pour une entrée, le type de circuit (**NC**, **NO**, **EOL = 10 kΩ**) ; pour une sortie, le fonctionnement : **Pulse** (impulsion) ou **Level** (bistable).
- **Inactive** – après la première activation, l'entrée ne signale plus pendant cette durée ; 0 = désactivé.
- **Delay** – le temps de réaction de l'entrée en millisecondes (par défaut 400 ms).
- **CMS** – case cochée, l'événement est envoyé au centre de télésurveillance et aussi dans Protegus 2.
- **No rest.** – ne pas envoyer d'événement de rétablissement.
- **Pulse** – la durée de l'impulsion en secondes, si la sortie est de type **Pulse** (par défaut 3 s sur 5 OUT ; pour une motorisation de portail, 1–3 s suffisent généralement).
- **Sched** – le numéro de la programmation horaire qui commande la sortie (de l'onglet **Scheduler**).
- **Assign IN** – l'entrée associée à la sortie : au lieu de l'état de la sortie, l'application affiche l'état réel de l'entrée (du portail) (point 5.10).
- **CID** – le code Contact ID de l'événement.
- **Confirm** – le numéro de l'entrée dont l'état actif conditionne la commutation de la sortie.
- **CTRL by IN** – l'activation de l'entrée choisie commute la sortie (automatisme local, fonctionne aussi sans réseau).

Groupe Tag reader settings – les réglages des lecteurs RFID (raccordement au point 3.6)

- **Wiegand reader mode** – le nombre de lecteurs Wiegand raccordés : **Single Reader** ou **Dual Reader**.
- **IO3 as exit button (5 OUT)** – cochez la case si le bouton-poussoir de sortie est raccordé à la borne 3 I/O : lorsqu'on appuie dessus, 5 OUT s'active pendant la durée d'impulsion réglée.
- **Low voltage reader** – pour un lecteur basse tension (niveau de signal de 5 V).
- **Disable reader filter** – désactive le filtre interne des impulsions courtes, si l'appareil ne reconnaît pas les signaux du lecteur.

Groupe Work status – relevé du temps de travail dans Protegus 2 (détails : GV17 – système de contrôle d'accès et/ou de suivi du temps de travail)

- **Enable "work status" feature** – active la signalisation de l'état de travail dans l'application.
- **Entry/Exit event with output** – case cochée, un événement d'entrée / de sortie est aussi généré lors de la commutation à distance de la sortie.
- **Auto end of work** – le mode de clôture automatique du temps de travail.
- **End work at/after** – l'heure de la clôture ou le temps écoulé jusqu'à la clôture, selon le réglage précédent.

5.3.2 Scheduler – horaires des sorties

Les sorties peuvent aussi commuter d'elles-mêmes selon une programmation horaire (par exemple portail ouvert pendant les heures de travail, fermé le soir). Vous associez la programmation horaire dans la colonne **Sched** de la sortie.

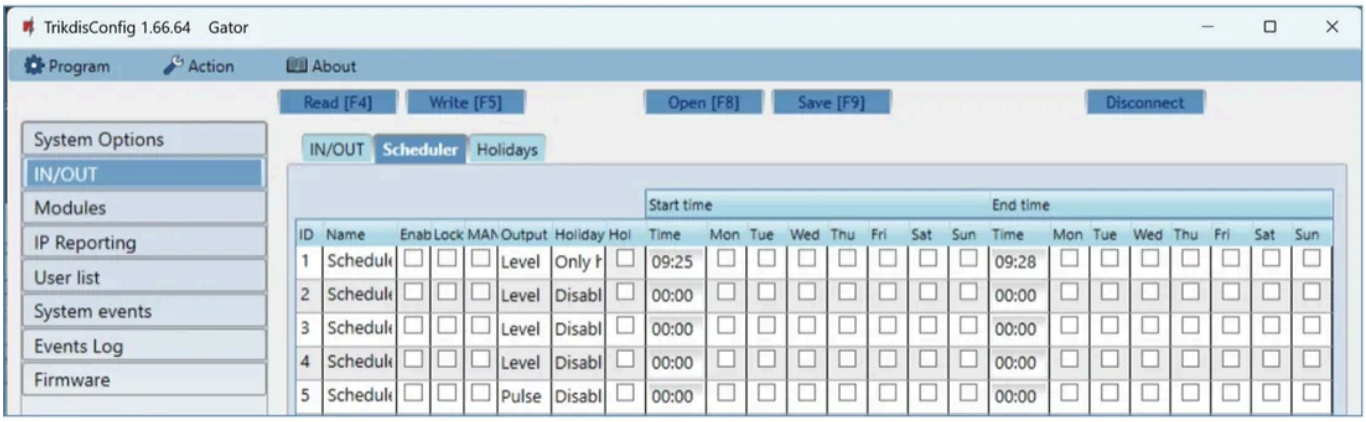


Figure 32. TrikdisConfig – IN/OUT, onglet **Scheduler** : pour chaque programmation horaire, activation, verrouillage, mode de sortie, mode jour férié, heure de début et de fin avec les jours de la semaine.

- **Name** – le nom de la programmation horaire.
- **Enable** – activation de la programmation horaire.
- **Lock** – case cochée, pendant la période active de la programmation horaire, la sortie ne peut pas être commutée d'une autre façon (par appel, depuis l'application).
- **MANUAL** – case cochée, la sortie ne commute pas d'elle-même au début de la programmation horaire ; la programmation démarre lorsque l'utilisateur active la sortie.
- **Output mode** – le fonctionnement de la sortie pendant la programmation horaire : **Level** – la sortie reste activée pendant toute la durée indiquée ; **Pulse** – la sortie commute pendant la durée d'impulsion réglée au début et à la fin de la programmation horaire.
- **Holiday mode** – comment la programmation horaire fonctionne les jours fériés ; **Hol** – cochez la case si, les jours fériés, elle utilise les horaires des jours fériés.
- **Start time** – les jours de la semaine et l'heure à partir de laquelle la sortie s'active.
- **End time** – les jours de la semaine et l'heure jusqu'à laquelle la sortie reste activée.

Si le mode de la sortie est **Level** et que seul **End time** est indiqué, la sortie se désactive à l'heure indiquée si elle était activée jusque-là.

5.3.3 Onglet Holidays – jours fériés

C'est ici que vous indiquez les jours du calendrier pendant lesquels la programmation horaire fonctionne avec les horaires des jours fériés.

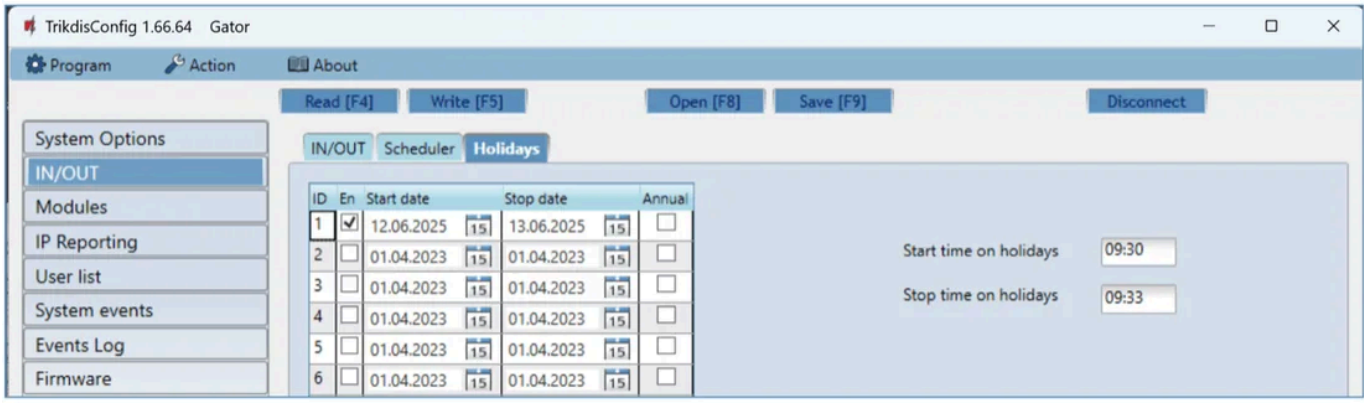


Figure 33. TrikdisConfig – IN/OUT, onglet **Holidays** : périodes de jours fériés avec date de début et de fin, heure de début et de fin pour les jours fériés.

- **En.** – activation de la période de jours fériés.
- **Start date**, **Stop date** – le premier et le dernier jour de la période.

- **Annual** – jour férié qui se répète chaque année : l'appareil ne tient compte que du mois et du jour.
- **Start time on holidays**, **Stop time on holidays** – l'heure de début et de fin pour les jours fériés.

5.4 Page « Modules »

5.4.1 Onglet Modules

Les modules suivants peuvent être associés au GATOR par le bus RS485 ou par radio : module WiFi **W485**, module Ethernet **E485**, module d'extension sans fil **iO-LORA** (via l'émetteur-récepteur RF-LORA, 8 au maximum ; les lecteurs RFID raccordés aux modules iO-LORA peuvent ainsi commuter au maximum 8 sorties supplémentaires, un lecteur ne commandant toujours qu'une seule sortie de son propre module – à partir du firmware 2.13 du GATOR, point 3.9), module d'extension filaire **iO8** et sans fil **iO8-LORA** (via le RF-LORA ; un seul des deux au total). L'émetteur-récepteur RF-LORA n'a pas besoin d'être ajouté à la liste. Si le site dispose du WiFi ou d'Internet filaire, le GATOR envoie, avec un module W485 ou E485, les messages par Internet vers le cloud Protegus et le centre de télésurveillance : les données mobiles ne sont pas consommées (le trafic de données de la carte SIM peut même être désactivé), et le GATOR peut même être utilisé sans carte SIM, commandé uniquement depuis l'application.

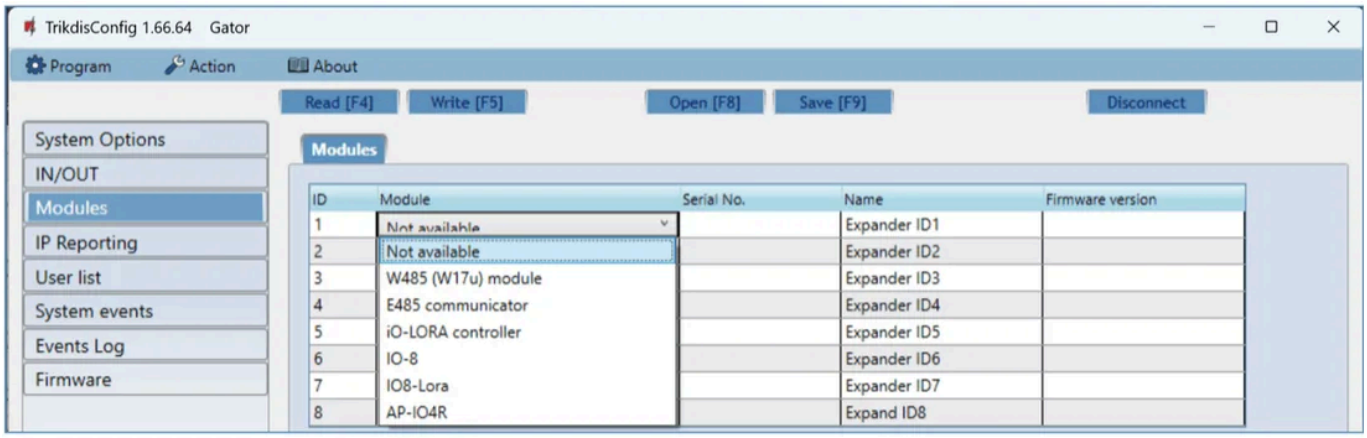


Figure 34. TrikdisConfig – **Modules** : dans la liste déroulante **Module**, les modules W485, E485, iO-LORA, iO8, iO8-LORA et **AP-IO4R** (iO4R) ; à côté, les colonnes **Serial No.**, **Name** et **Firmware version**.

- **Module** – choisissez dans la liste le module raccordé.
- **Serial No.** – le numéro de série à 6 chiffres du module (sur l'étiquette du boîtier et de la boîte du module).

Une fois le module choisi et le numéro de série saisi, l'onglet **Parameters** apparaît avec les réglages propres au module.

Module d'extension à relais iO4R

L'**AP-IO4R** figurant dans la liste est le module d'extension à relais **iO4R** : il sert à surveiller les capteurs de sécurité de l'automatisme de portail et à les shunter à distance, ainsi qu'à compter les cycles du portail. Sa configuration se fait dans l'application Protegus 2, en mode **Advanced Gator Monitoring**, que l'on peut choisir lors de l'ajout du contrôleur de portail – voir le manuel de l'iO4R.

5.4.2 Onglet Parameters – module WiFi W485

Après avoir choisi le W485, vous saisissez ici les données du réseau WiFi et le mode d'utilisation de la carte SIM.

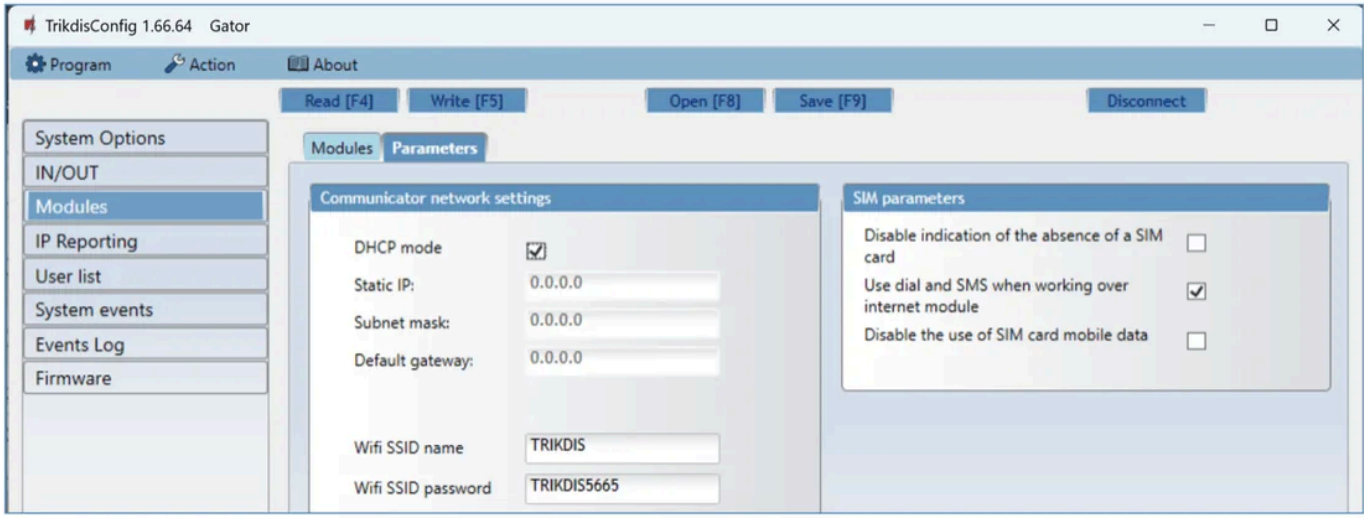


Figure 35. TrikdisConfig – Modules, onglet **Parameters** pour le W485 : **Communicator network settings** (DHCP, adresse IP, nom et mot de passe du réseau WiFi) et **SIM parameters**.

Groupe Communicator network settings

- **DHCP mode** – case cochée, le module reçoit automatiquement du routeur les paramètres réseau (adresse IP, masque de sous-réseau, passerelle) ; décochée, vous les saisissez manuellement.
- **Static IP**, **Subnet mask**, **Default gateway** – l'adresse IP fixe, le masque de sous-réseau et l'adresse de la passerelle en réglage manuel.
- **Wifi SSID name** – le nom du réseau WiFi auquel le W485 se connecte (réseau 2,4 GHz).
- **Wifi SSID password** – le mot de passe du réseau WiFi.

Groupe SIM parameters

- **Disable indication of the absence of a SIM card** – case cochée, l'appareil ne signale pas l'absence de carte SIM comme un défaut (utilisation sans SIM, uniquement par Internet).
- **Use dial and SMS when working over internet module** – case cochée, la commande par appel et par SMS fonctionne aussi avec le module. Décochée, tant que la connexion Internet fonctionne, l'appareil n'utilise ni l'appel ni le SMS ; si Internet est interrompu, l'appel et le SMS fonctionnent de nouveau, et l'appareil envoie un SMS aux utilisateurs.
- **Disable the use of SIM card mobile data** – case cochée, l'appareil n'utilise pas les données mobiles de la carte SIM, les données passent uniquement par le W485. Si le WiFi est interrompu, l'appareil mémorise les événements et les envoie au retour de la liaison.

5.4.3 Onglet Parameters – module Ethernet E485

Après avoir choisi l'E485, vous saisissez ici les données du réseau filaire et le mode d'utilisation de la carte SIM.

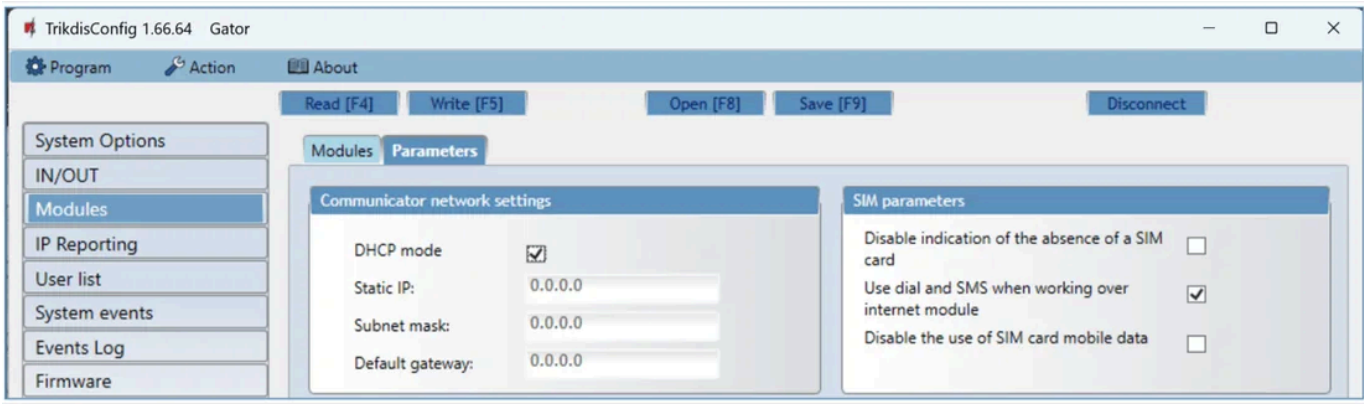


Figure 36. TrikdisConfig – Modules, onglet **Parameters** pour l'E485 : paramètres réseau (DHCP ou adresse IP fixe) et **SIM parameters**.

- **DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway** – comme pour le W485 : réglage réseau automatique ou manuel.
- **SIM parameters** – les trois cases ont la même signification que celle décrite pour le W485 ; avec les données mobiles désactivées, les données passent uniquement par l'E485, et pendant une coupure d'Internet l'appareil mémorise les événements.

5.5 Page « IP Reporting »

Le GATOR envoie les événements au récepteur IP du centre de télésurveillance et au cloud Protegus ; c'est sur cette page que vous activez le cloud.

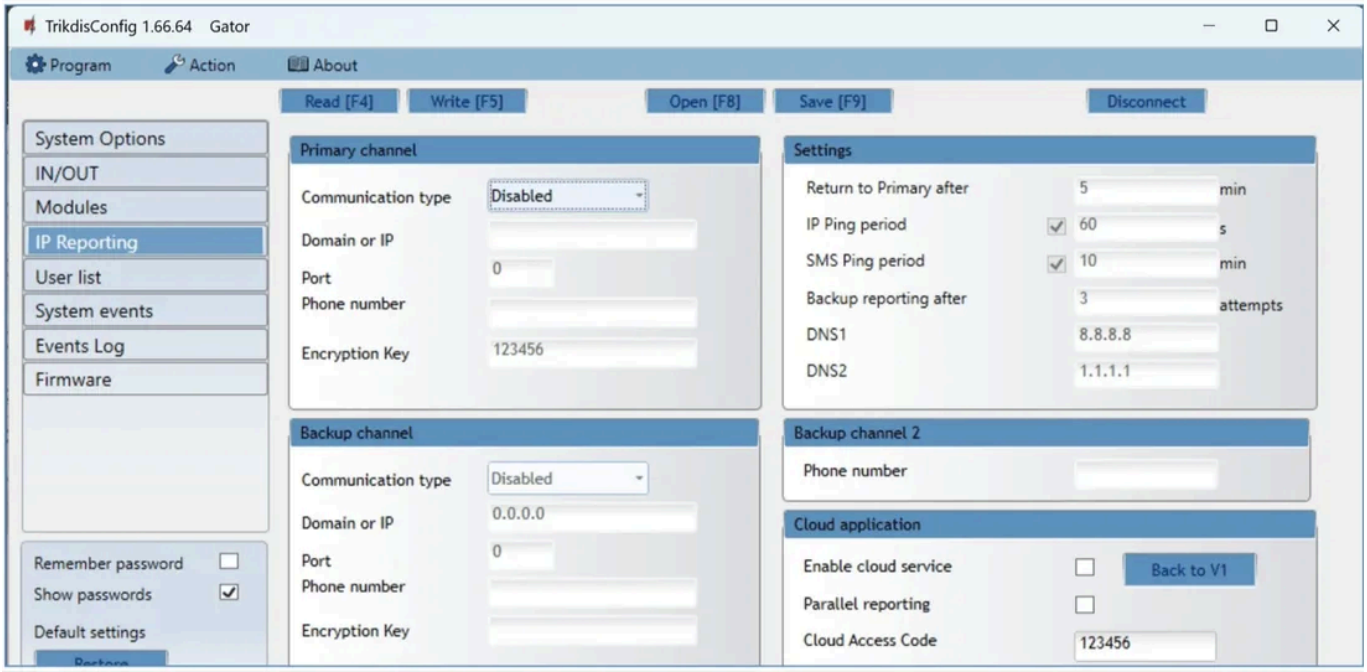


Figure 37. TrikdisConfig – **IP Reporting** : **Primary channel** et **Backup channel** (désactivés par défaut), **Settings**, le canal SMS de secours et le groupe **Cloud application** avec la case **Enable cloud service** et le code **Cloud Access Code**.

Groupe Primary channel

- **Communication type** – le type de liaison avec le récepteur du centre de télésurveillance : **IP** ou **SMS** ; **Disabled** = pas de transmission.
- **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- **Port** – le port réseau du récepteur.

- **Phone number** – le numéro de téléphone du récepteur SMS du centre de télésurveillance (+33…), si le type est SMS.
- **Encryption Key** – clé de chiffrement à 6 chiffres, qui doit être identique à celle réglée dans le récepteur.

Groupe Backup channel – le récepteur de secours, avec les mêmes réglages que le principal.

Groupe Settings

- **Return to primary after** – au bout de ce délai, l'appareil essaie de revenir du canal de secours au canal principal.
- **IP Ping period** – activation et intervalle des signaux PING qui maintiennent la liaison.
- **SMS Ping period** – la même chose sur le canal SMS.
- **Backup reporting after** – après ce nombre de tentatives infructueuses, l'appareil bascule sur le canal de secours.
- **DNS1**, **DNS2** – l'adresse IP des serveurs de noms.

Groupe Backup channel 2

- **Phone number** – le numéro du récepteur SMS du centre de télésurveillance. L'appareil y envoie un SMS lorsque le message ne peut être envoyé ni par le canal IP principal ni par le canal IP de secours ; cela fonctionne aussi lorsque la liaison IP tombe dans le réseau de l'opérateur mobile. Ce canal n'est actif que si les deux canaux IP passent par le réseau mobile ; le récepteur SMS reçoit un message à la première mise sous tension de l'appareil et lors de la perte de la liaison TCP/IP ou UDP/IP.

Groupe Cloud application

- **Enable cloud service** – activation du cloud Protegus : le GATOR communique avec l'application et peut aussi être programmé à distance avec TrikdisConfig (chapitre 6).
- **Parallel reporting** – case cochée, les événements partent simultanément vers le centre de télésurveillance, Protegus 2 et les utilisateurs ; décochée, l'application et les utilisateurs ne les reçoivent qu'après l'acquittement du centre de télésurveillance.
- **Cloud Access Code** – code à 6 chiffres pour la connexion à Protegus 2 (par défaut `123456`) ; c'est ce code que l'application demande lors de l'ajout du système, s'il ne s'agit pas du code par défaut.

5.6 Page « User list »

La liste des administrateurs et des utilisateurs, l'enregistrement des cartes RFID, les programmations horaires des utilisateurs et la liste noire – sur quatre onglets.

5.6.1 Onglet Users – les utilisateurs

Le tableau comporte un administrateur ou un utilisateur par ligne, avec ses autorisations.

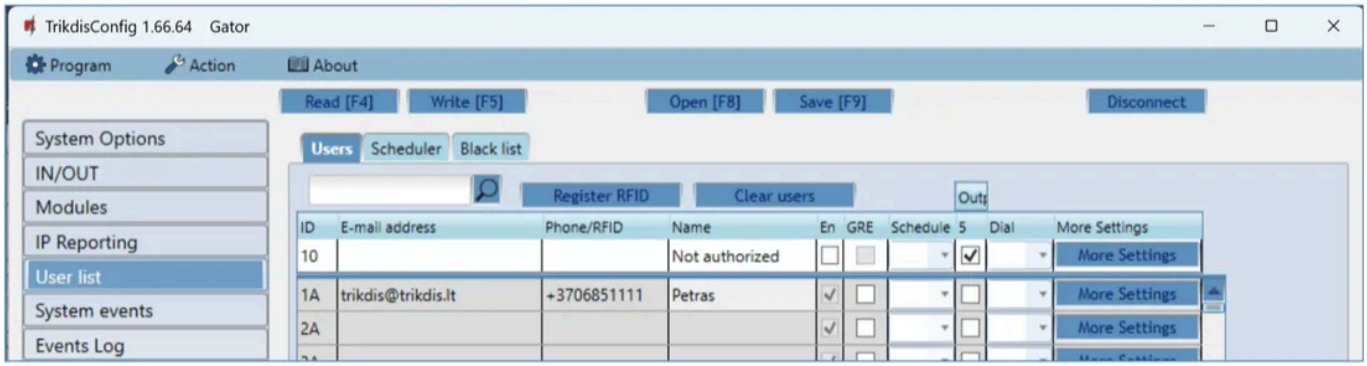


Figure 38. TrikdisConfig – **User list**, onglet **Users** : en haut les boutons **Register RFID** et **Clear users** ; dans le tableau les colonnes **ID**, **E-mail address**, **Phone/RFID**, **Name**, **En**, **GRE**, **Schedule**, **Dial** et le bouton **More settings** ; la ligne 10 est l'entrée **Not authorized**.

- **ID** – le numéro d'ordre de l'utilisateur. Les lignes avec la lettre **A** (**1A–7A**) sont les administrateurs : ils peuvent configurer l'appareil, commuter les sorties, et ce sont eux qui reçoivent les messages. Les lignes numérotées **11–1010** sont les utilisateurs : ils peuvent seulement commuter les sorties.
- **E-mail address** – l'adresse e-mail de l'utilisateur (pour Protegus 2).
- **Phone/RFID** – le numéro de téléphone au format international (+33…) ou le numéro d'identification de la carte RFID.
- **Name** – le nom de l'utilisateur.
- **En** – activation de l'utilisateur : case cochée, l'utilisateur peut commuter les sorties.
- **GRE** – envoi d'un SMS de bienvenue à l'utilisateur.
- **Schedule** – le numéro de la programmation horaire selon laquelle l'utilisateur peut commander (point 5.6.3).
- **Output** – la ou les sorties que l'utilisateur peut commander.
- **Code** – pour un lecteur Wiegand à code (à clavier), le code de l'utilisateur.
- **Dial** – la ou les sorties commutées par appel, si l'utilisateur a plusieurs sorties ; après la commutation, l'appareil raccroche.
- **More settings** – la fenêtre des réglages supplémentaires (ci-dessous).

La ligne 10, « Not authorized »

Si la case **En** de l'utilisateur n° 10 nommé **Not authorized** est **cochée**, le GATOR peut être commandé par appel **depuis n'importe quel numéro de téléphone**. Si elle est décochée, seules les personnes de la liste peuvent appeler ; chaque utilisateur commute la sortie cochée dans sa propre colonne **Dial**. Par SMS, c'est la commande `NATH` qui règle la même chose (point 4.7).

Après l'arrêt du réseau 2G, il se peut que certains opérateurs mobiles n'autorisent pas les appels vocaux sur le réseau 4G (VoLTE) pour le modem Quectel EG915U-EU que nous utilisons. Dans ce cas, l'ouverture du portail par appel et la notification par appel téléphonique ne fonctionnent pas. L'envoi de SMS et la connexion de données (application Protegus 2) ne sont pas concernés par cette restriction et continuent de fonctionner.

Réglages supplémentaires – administrateur (1A–7A)

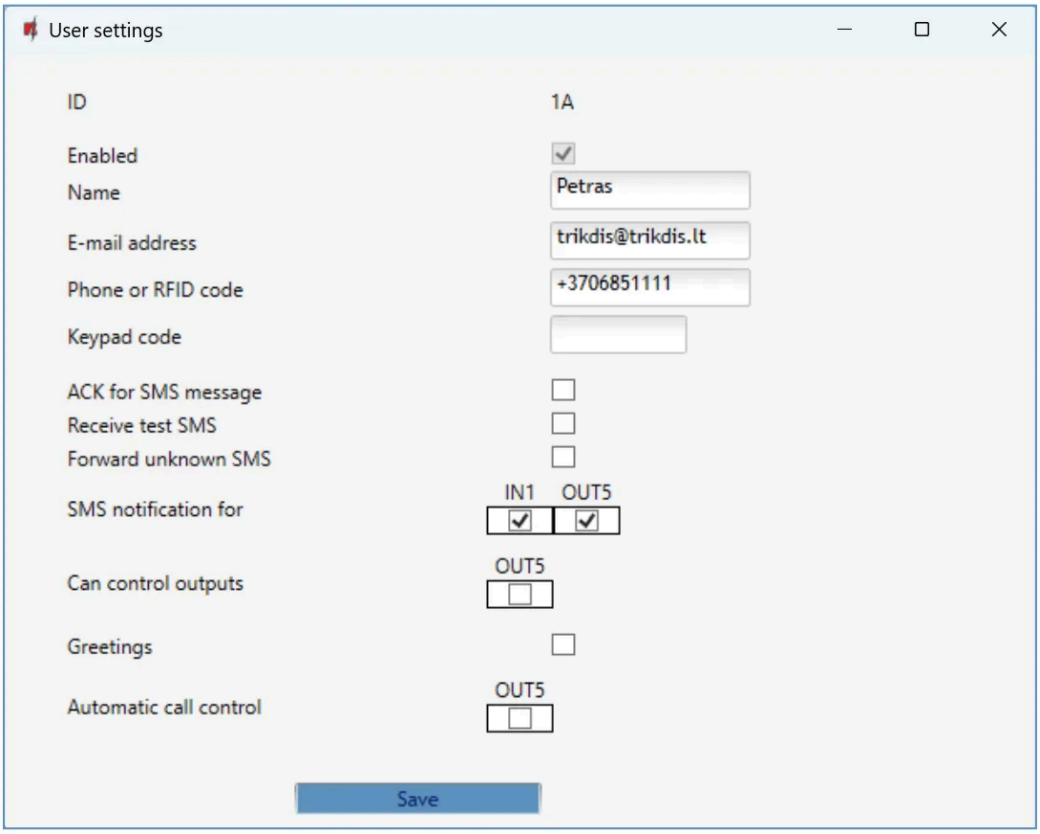


Figure 39. TrikdisConfig – **User settings** pour un administrateur : **Enabled**, les données, **ACK for SMS message**, **Receive test SMS**, **Forward unknown SMS**, **SMS notification for** (IN1, IN2, OUT3, OUT4, OUT5), **Can control output**, **Greetings** et **Automatic call control**.

- **ID**, **Enabled**, **Name**, **E-mail address**, **Phone or RFID code**, **Keypad code** – les données correspondant aux colonnes de la liste.
- **ACK for SMS message** – l'administrateur reçoit un SMS de réponse sur l'exécution des commandes SMS.
- **Receive test SMS** – il reçoit le SMS de test périodique.
- **Forward unknown SMS** – l'appareil lui transfère les SMS provenant de numéros inconnus (par exemple l'avis de solde de l'opérateur).
- **SMS notification for** – les événements (IN1, IN2, OUT3, OUT4, OUT5) dont les changements lui sont signalés par SMS.
- **Can control output** – les sorties qu'il peut commander.
- **Greetings** – envoi d'un SMS de bienvenue.
- **Automatic call control** – les sorties commutées par son appel, puis l'appareil raccroche.

Réglages supplémentaires – utilisateur (11–1010)

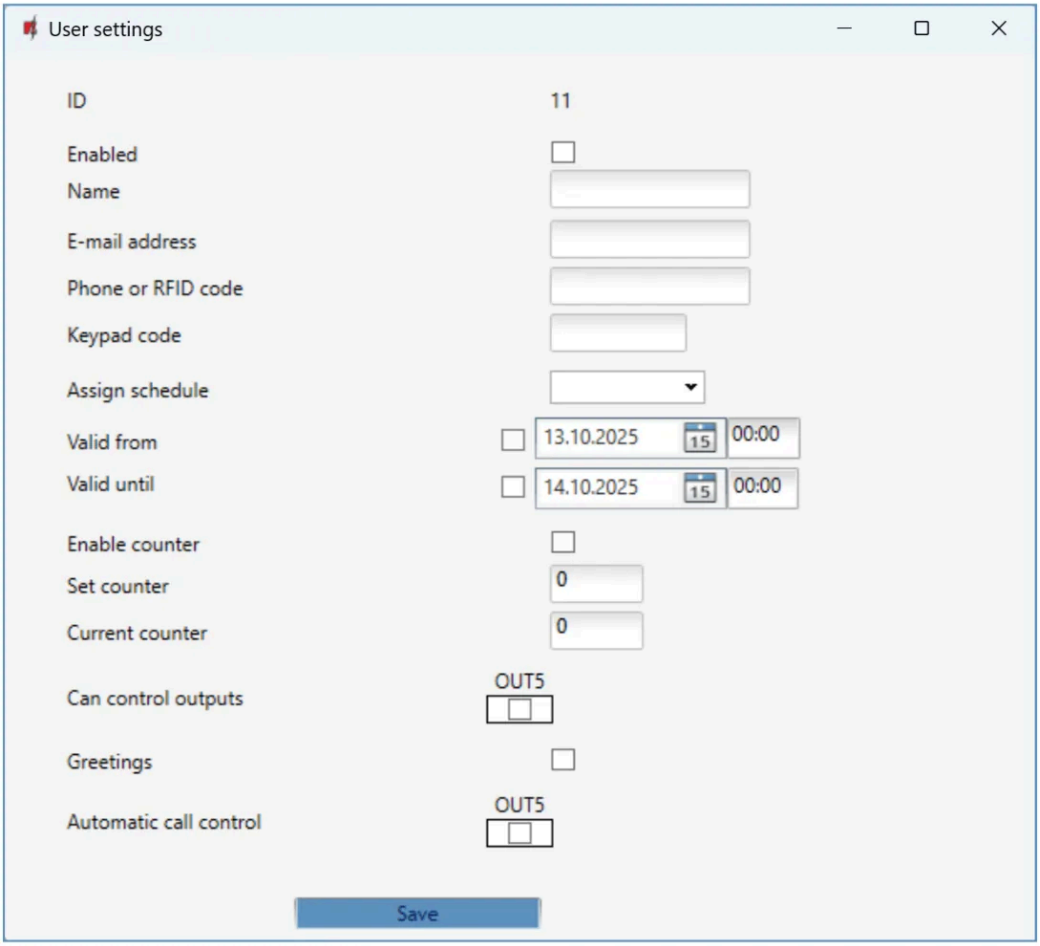


Figure 40. TrikdisConfig – **User settings** pour un utilisateur : **Assign schedule**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs**, **Greetings**, **Automatic call control**.

- **Assign schedule** – la ou les programmations horaires pendant lesquelles l'utilisateur peut commander.
- **Valid from**, **Valid until** – le début et la fin de l'autorisation (date et heure) – par exemple pour un locataire ou un invité.
- **Enable counter** – activation du compteur ; **Set counter** – combien de fois l'utilisateur peut commander pendant la période indiquée ; **Current counter** – le nombre de commutations effectuées jusqu'ici.
- **Can control outputs**, **Greetings**, **Automatic call control** – comme pour l'administrateur.

5.6.2 Enregistrer une carte RFID (badge)

1. Raccordez le lecteur RFID (point 3.6), mettez le GATOR sous tension, lancez TrikdisConfig et connectez-vous par câble USB ou à distance. Sur la page **IN/OUT**, réglez le nombre de lecteurs (**Wiegand reader mode**).
2. Sur la page **User list**, cliquez sur le bouton **Register RFID**.

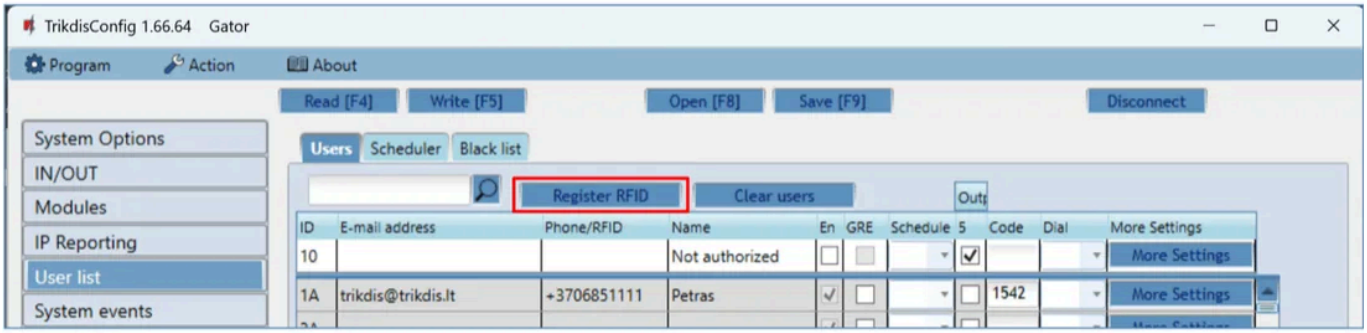


Figure 41. TrikdisConfig – User list : le bouton **Register RFID** au-dessus du tableau des utilisateurs.

3. La fenêtre d'enregistrement s'ouvre (**Add RFID tag/card to reader**).

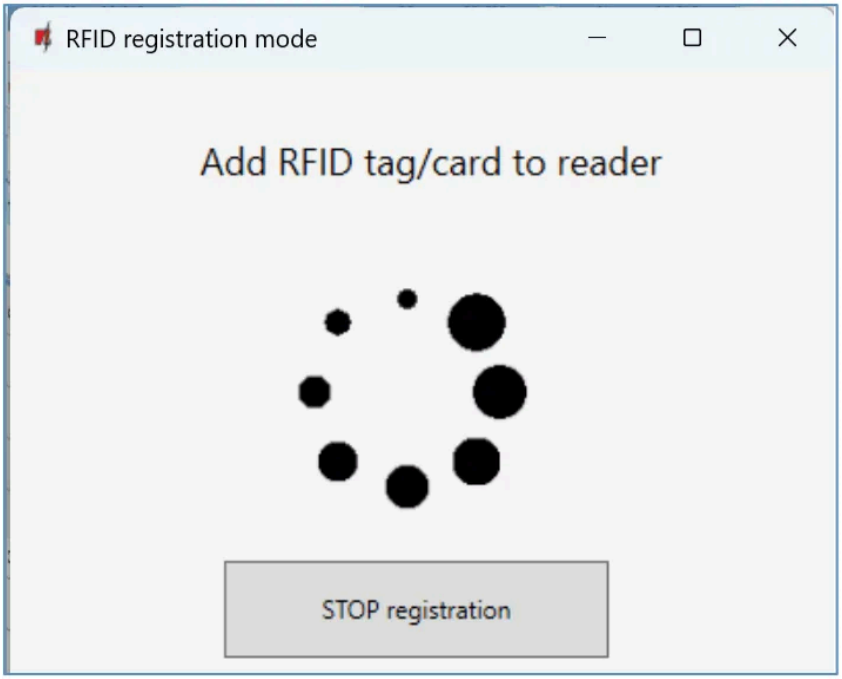


Figure 42. La fenêtre d'enregistrement RFID : la carte doit être présentée au lecteur ; le bouton **STOP registration** clôt l'enregistrement.

4. Présentez la carte au lecteur. Lorsque le lecteur l'a lue, une nouvelle fenêtre s'ouvre : saisissez le nom de l'utilisateur (**Enter user name**), cochez la sortie qu'il peut commander (**User can control PGM Output 5** ; avec la case **Device administrator**, il devient administrateur) et cliquez sur le bouton **ADD**. Répétez l'opération avec les autres cartes, puis appuyez sur le bouton **STOP registration**.
5. Avec le bouton **Write [F5]**, écrivez la liste des cartes dans l'appareil.

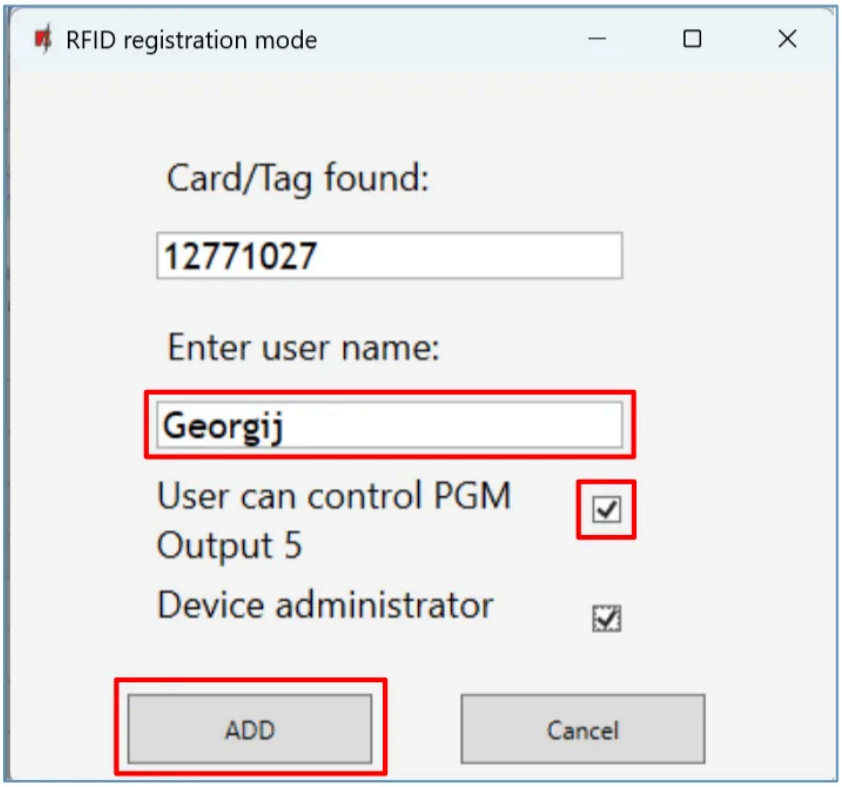


Figure 43. La fenêtre de la carte lue : nom, **User can control PGM Output 5**, **Device administrator**, puis **ADD**.

Ajout d'une carte d'après son numéro : vous pouvez aussi saisir directement dans le champ **Phone/RFID** le numéro d'identification imprimé sur la carte ; indiquez le nom, cochez la case **En** et la sortie commandée, puis **Write [F5]**.

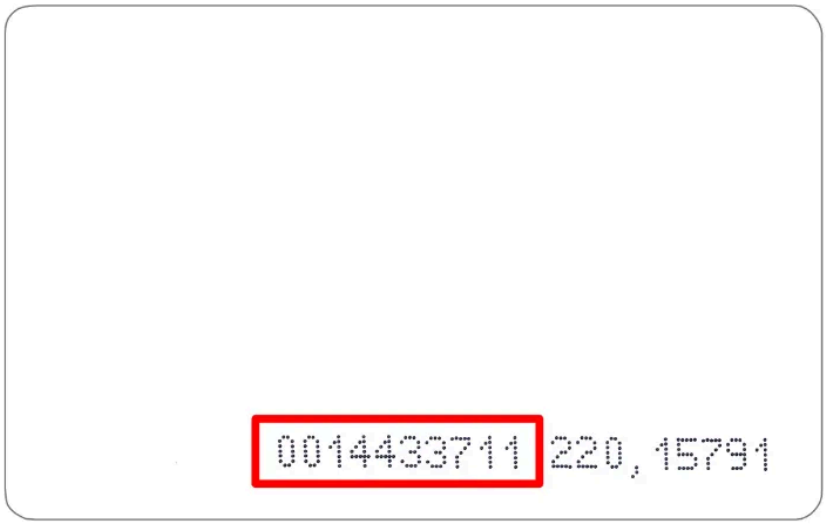


Figure 44. Le numéro d'identification imprimé sur la carte RFID (sur le bord inférieur de la carte).

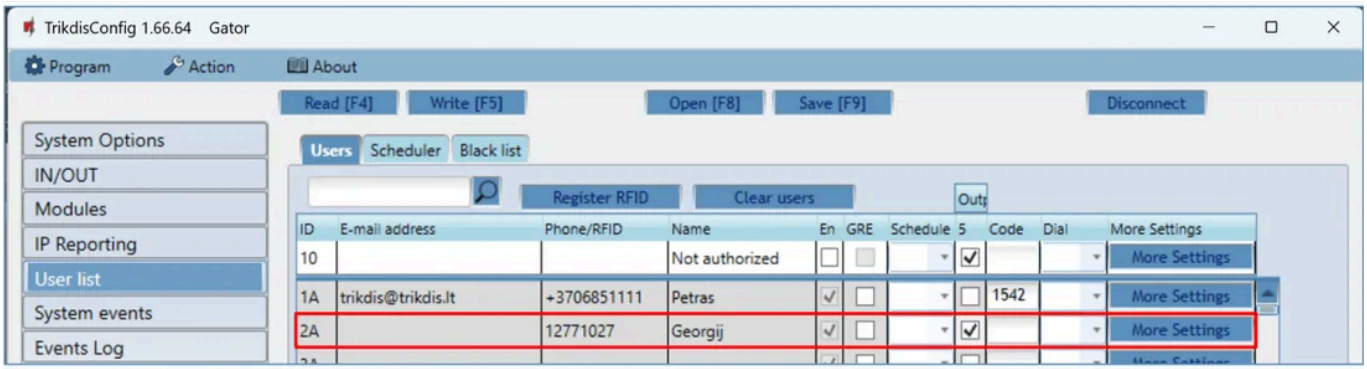


Figure 45. TrikdisConfig – User list : la ligne du nouvel utilisateur avec le numéro de carte dans le champ **Phone/RFID**, le nom, **En** coché, la sortie 5 cochée.

Ajout d'une carte depuis Protegus 2 : dans la liste des utilisateurs, choisissez l'ajout d'un nouvel utilisateur, saisissez l'adresse e-mail, le nom, le numéro d'identification de la carte (dans le champ du numéro de téléphone), pour un lecteur à code le code à 4 chiffres, cochez la sortie et enregistrez (point 4.5).

5.6.3 Scheduler – horaires des utilisateurs

L'utilisateur ne peut commander que pendant la programmation horaire qui lui est attribuée (par exemple la personne chargée du ménage, en semaine entre 6 et 8 heures). Vous attribuez la programmation horaire dans la colonne **Schedule** de l'utilisateur ou dans le champ **More settings** → **Assign schedule**.

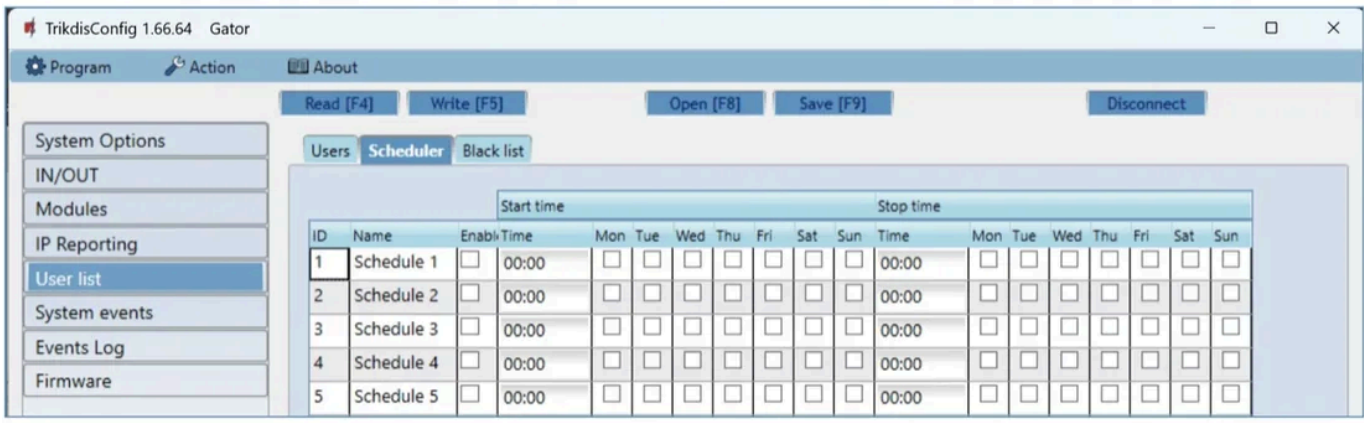


Figure 46. TrikdisConfig – User list, onglet **Scheduler** : cinq programmations horaires, chacune avec **Enable**, heure de début et de fin avec les jours de la semaine.

- **Name** – le nom de la programmation horaire.
- **Enable** – activation de la programmation horaire.
- **Start time** – les jours de la semaine et l'heure à partir de laquelle l'utilisateur peut commander.
- **Stop time** – les jours de la semaine et l'heure jusqu'à laquelle il peut commander.

5.6.4 Onglet Black list – liste noire

Une personne ajoutée ici ne peut commander l'appareil d'aucune façon.

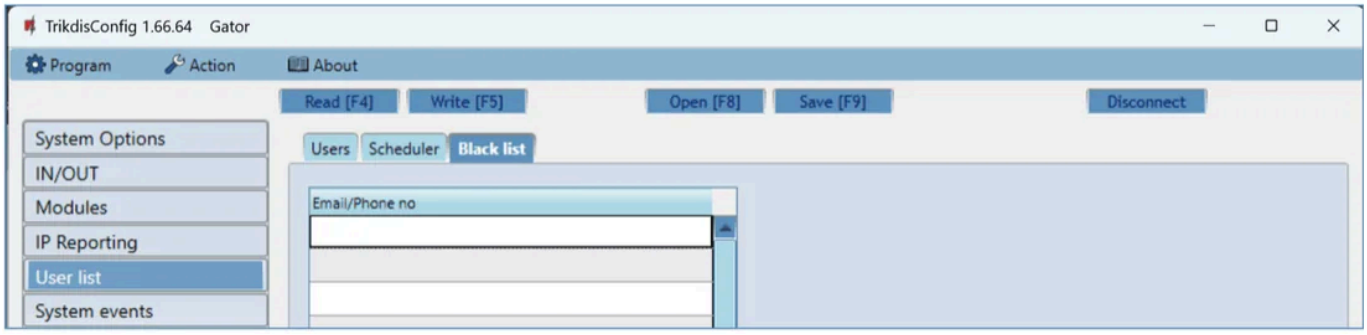


Figure 47. TrikdisConfig – User list, onglet **Black list** : le tableau des adresses e-mail, numéros de téléphone et numéros de carte interdits.

La liste noire contient les adresses e-mail, numéros de téléphone et numéros de carte RFID auxquels la commande du GATOR est interdite. Vous pouvez aussi ajouter une entrée directement depuis le journal des événements : cliquez avec le bouton droit sur le numéro de téléphone, l'adresse e-mail ou le numéro de carte, et choisissez l'option de menu **Add to black list**. Par SMS, les commandes `SETB` et `DELB` gèrent la liste (point 4.7).

5.7 Page « System events »

C'est ici que vous réglez lesquels des événements système propres au GATOR sont envoyés au centre de télésurveillance et à l'application Protegus 2.

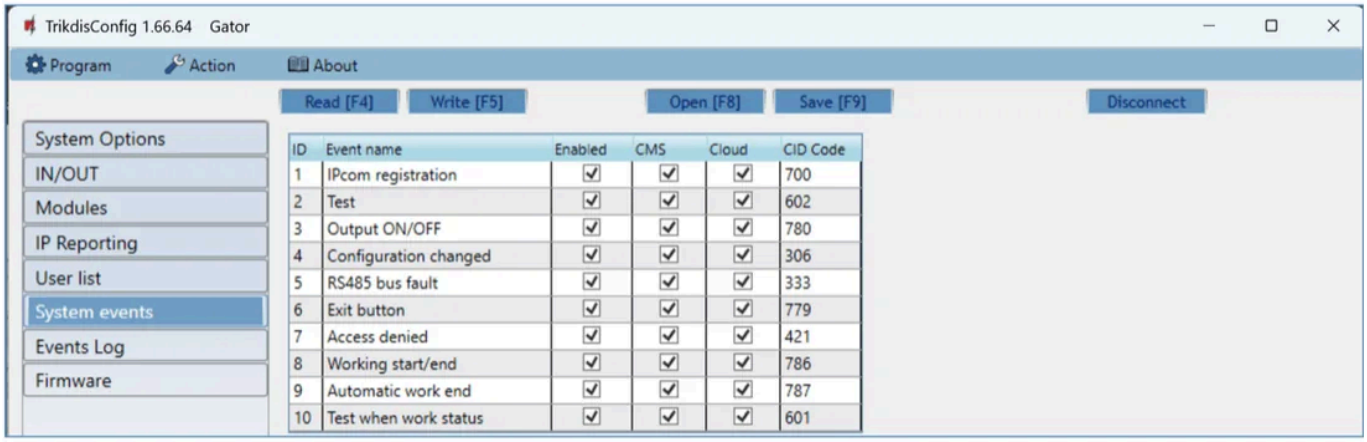


Figure 48. TrikdisConfig – **System events** : la liste des événements avec leur code Contact ID (par exemple IPcom registration 700, Test 602, Output ON/OFF 780, Configuration changed 306, RS485 bus fault 333, Exit button 779, Access denied 421, Working start/end 786, Automatic work end 787), chacun avec les cases **Enabled**, **CMS** et **Cloud**.

- **ID** – le numéro d'ordre de l'événement.
- **Event name** – le nom de l'événement.
- **Enabled** – surveillance de l'événement.
- **CMS** – l'événement est envoyé au centre de télésurveillance.
- **Cloud** – l'événement est envoyé à l'application Protegus 2.
- **CID Code** – le code Contact ID de l'événement.

5.8 Page « Events Log »

Le journal des événements propre à l'appareil – pour le dépannage et pour retrouver les accès.

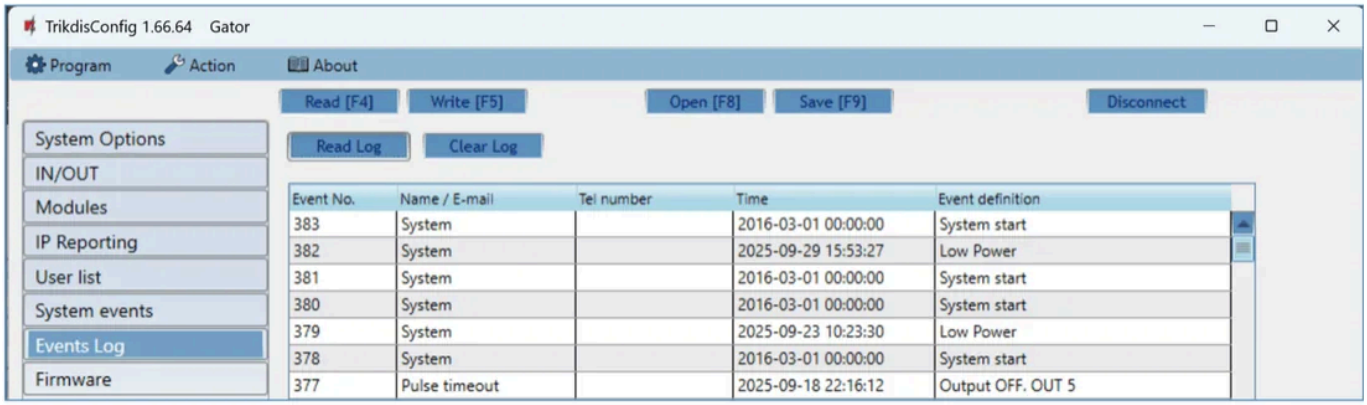


Figure 49. TrikdisConfig – **Events Log** : les boutons **Read Log** et **Clear Log** ; pour chaque événement, le numéro d'ordre, le nom ou l'adresse e-mail de l'utilisateur, le numéro de téléphone, l'heure et la description de l'événement.

Cliquez sur le bouton **Read Log** : le logiciel lit les événements dans la mémoire de l'appareil (5000 au maximum). Le journal montre toutes les opérations et tous les événements internes du GATOR avec des données détaillées : qui a ouvert le portail, quand et par quel moyen (appel, SMS, application, carte), et quelles entrées ont changé. Le bouton **Clear Log** efface le journal.

5.9 Retour aux réglages d'usine

Pour revenir aux réglages d'usine, cliquez sur le bouton **Restore** du groupe **Default settings**, en bas à gauche de la fenêtre de programmation. Le retour aux réglages d'usine efface tous les réglages – y compris la liste des utilisateurs et les mots de passe –, il est donc conseillé d'enregistrer auparavant les réglages dans un fichier (**Save [F9]**).

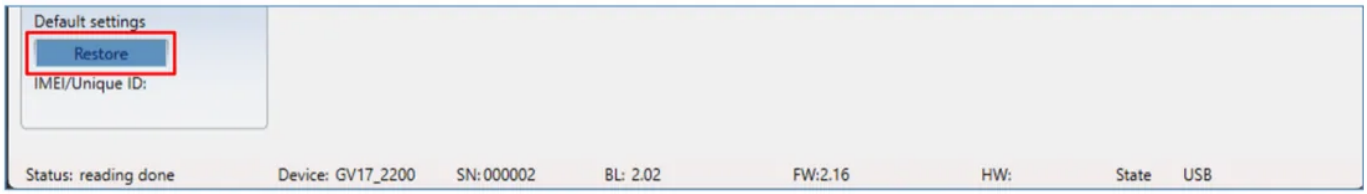


Figure 50. TrikdisConfig – le bouton **Restore** du groupe **Default settings**, au-dessus de la barre d'état.

5.10 Signalisation de l'état du portail

L'application Protegus 2 et le widget peuvent afficher l'état réel du portail (ouvert ou fermé). Pour cela, l'entrée **1 IN** du GATOR doit être raccordée à la sortie d'état de la motorisation ou au fin de course du portail (point 3.5), puis, dans le logiciel, l'entrée doit être associée à la sortie qui commute le portail :

1. Sur la page **IN/OUT**, l'entrée **1 IN** doit avoir la fonction **Input**, avec le type correspondant au contact (dans l'exemple NO). Dans la ligne de **5 OUT**, choisissez l'entrée **1 IN** dans la colonne **Assign IN**.
2. Si vous souhaitez aussi recevoir un SMS à l'ouverture et à la fermeture du portail, saisissez le texte **SMS event text** et **SMS restore text** de 1 IN (par exemple « Portail ouvert » / « Portail fermé »).

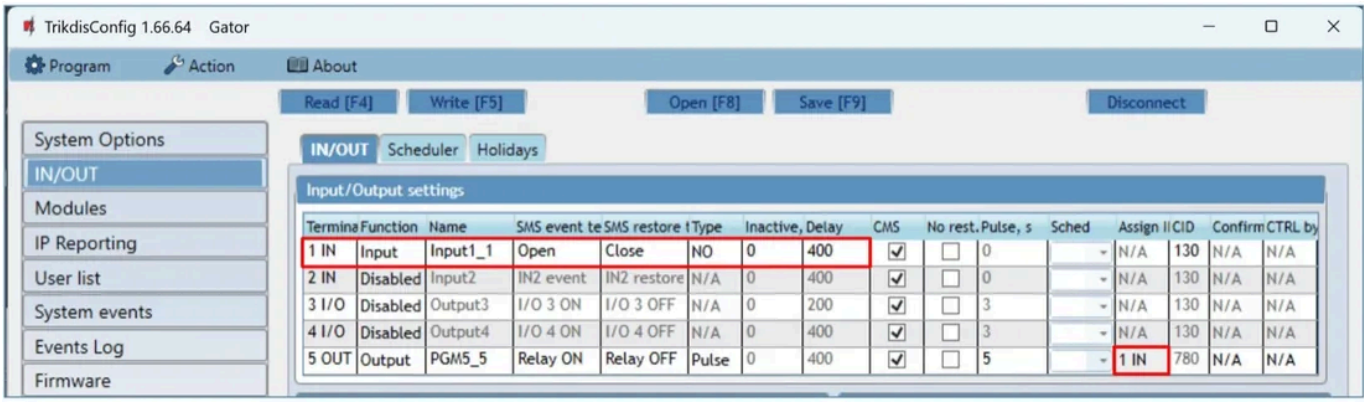


Figure 51. TrikdisConfig – IN/OUT : l'entrée **1 IN** (NO, avec les textes SMS **Open** / **Close**), dans la ligne de **5 OUT** l'entrée **1 IN** dans la colonne **Assign IN**.

3. Sur la page **User list**, dans la ligne de l'utilisateur, cliquez sur le bouton **More settings** et, dans le groupe **SMS notification for**, cochez la case **IN1**, afin que l'utilisateur reçoive un SMS sur l'état du portail. Cliquez sur le bouton **Save**, puis écrivez les réglages (**Write [F5]**).



Figure 52. TrikdisConfig – User list : le bouton **More settings** dans la ligne de l'utilisateur.

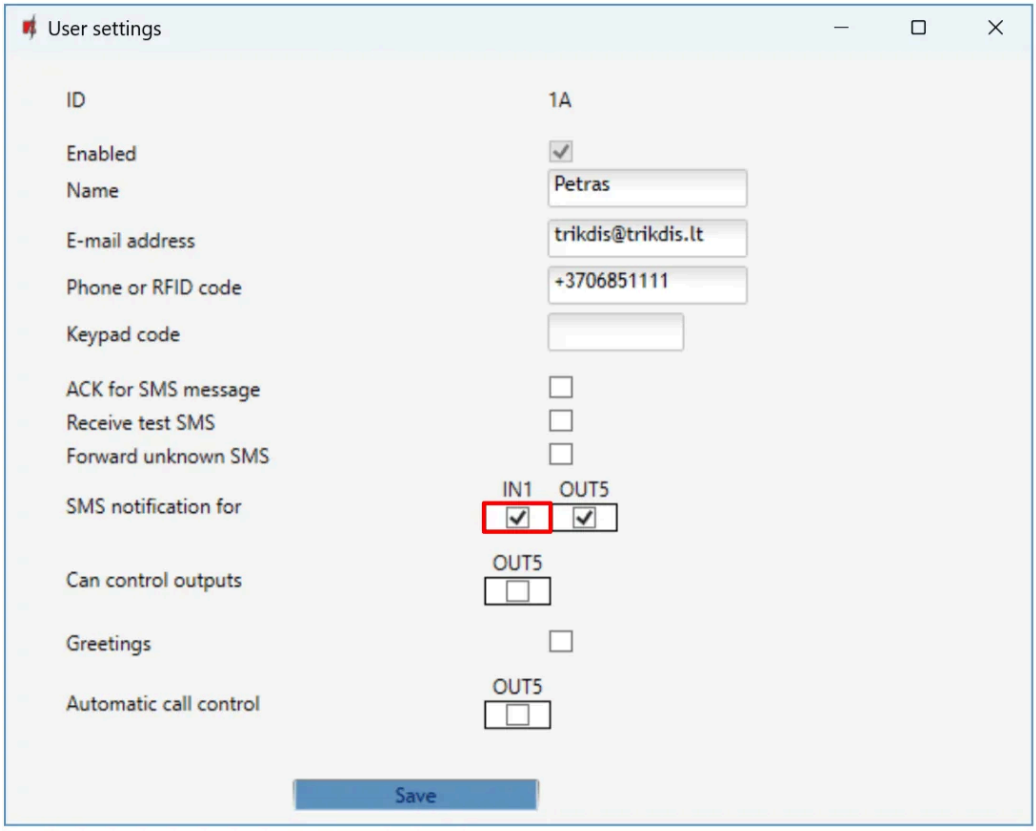


Figure 53. TrikdisConfig – User settings : dans le groupe **SMS notification for**, **IN1** (et **OUT5**) cochés, en bas le bouton **Save**.

6. Programmation à distance

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

Conditions de la programmation à distance

Dans TrikdisConfig, sur la page **IP Reporting**, la case **Enable cloud service** doit être cochée (point 5.5 ; par SMS : `CONNECT 123456 PROTEGUS=ON`), l'alimentation doit être correcte (la LED **POWER** clignote en vert) et l'appareil doit être connecté au réseau (la LED **NETWORK** est allumée en vert et clignote en jaune). Si ces conditions ne sont pas remplies, l'appareil n'est pas accessible à distance.

1. Téléchargez et installez la dernière version de TrikdisConfig depuis le site de Trikdis (https://www.trikdis.com), si elle n'est pas encore sur votre ordinateur.
2. Assurez-vous que le GATOR est connecté à Internet et que le cloud Protegus est activé.
3. Lancez TrikdisConfig. Dans la partie **Remote access** de l'écran d'accueil, saisissez dans le champ **Unique ID** le numéro **IMEI** du GATOR (il figure sur l'étiquette sous l'appareil et sur la boîte ; avec une connexion USB, vous le voyez aussi dans la barre d'état).
4. Dans le champ **System Name**, saisissez un nom quelconque (par exemple le nom de l'objet) et cliquez sur le bouton **Configure**.

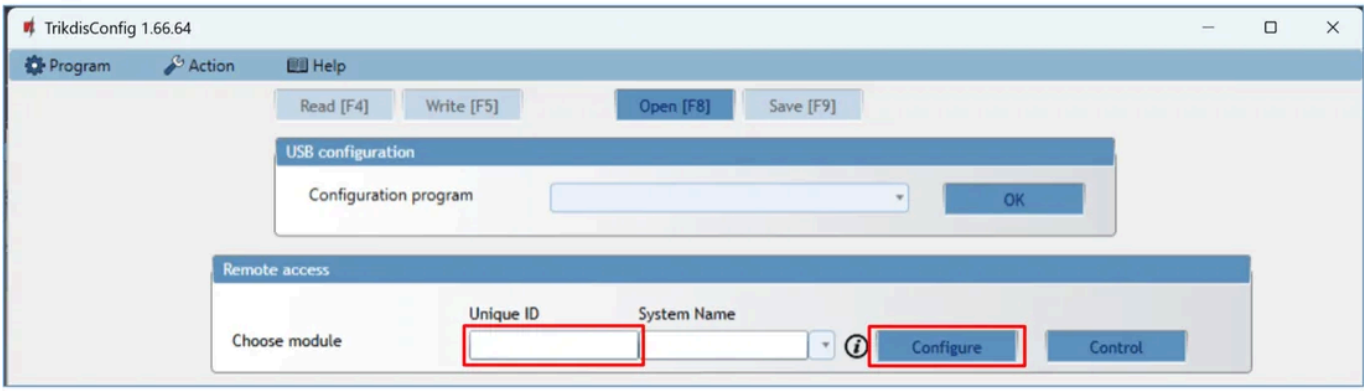


Figure 54. TrikdisConfig – la partie **Remote access** : le champ **Unique ID**, le champ **System Name** et le bouton **Configure**.

5. La fenêtre de programmation du GATOR s'ouvre. Cliquez sur le bouton **Read [F4]** : le logiciel lit les réglages actuels de l'appareil. Si le logiciel demande le code d'accès, saisissez le code **administrateur** à 6 chiffres. Si vous cochez la case **Remember password** et cliquez sur le bouton **Write [F5]**, le logiciel mémorise le code.
6. Effectuez les réglages et écrivez-les avec le bouton **Write [F5]**. À la fin, coupez la liaison avec le bouton **Disconnect** et fermez le logiciel.

La programmation à distance ne nécessite aucune aide sur place : le client vérifie seulement l'alimentation et le réseau grâce aux LED. Pour modifier la liste des utilisateurs, TrikdisConfig n'est même pas nécessaire – l'administrateur la gère aussi depuis Protegus 2 (point 4.5) ou par SMS (point 4.7).

7. Vérification du fonctionnement

À la fin de l'installation et de la configuration, testez tout le système – sur place, avant de le remettre au client :

1. **Alimentation** : la LED **POWER** clignote en vert. Si elle clignote en jaune, la tension d'alimentation n'est pas correcte – mesurez-la sur les bornes d'alimentation (9–32 V DC ou 12–24 V AC).
2. **Réseau** : la LED **NETWORK** est allumée en vert et clignote en jaune selon le niveau du signal (3 clignotements suffisent). Si la LED **TROUBLE** clignote, le nombre de clignotements indique le défaut (point 1.5).
3. **Entrées** : activez l'une après l'autre les entrées raccordées (contact d'état du portail, bouton-poussoir de sortie) et vérifiez que les destinataires reçoivent les bons messages par SMS, dans Protegus 2 et au centre de télésurveillance.
4. **Sorties** : activez les sorties à distance – par appel, depuis l'application, par SMS et avec la carte s'il y a un lecteur – et vérifiez que le portail s'ouvre, que les destinataires reçoivent les messages et que l'état du portail dans l'application correspond aussi à la réalité (point 5.10).

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

Vous pouvez aussi interroger l'état de l'appareil par SMS depuis le téléphone de l'administrateur : en réponse à la commande `INFO 123456`, le GATOR renvoie son type, le niveau du signal, la tension d'alimentation, la version du firmware, la date et l'heure (point 4.7). Si le SMS de réponse n'arrive pas, vérifiez que l'option **ACK for SMS message** est activée pour l'administrateur (point 5.6).

8. Mise à jour du firmware

Lorsque le GATOR est connecté à TrikdisConfig et qu'un firmware plus récent existe, le logiciel propose de lui-même la mise à jour – l'ordinateur doit pour cela être connecté à Internet. Si un antivirus fonctionne sur l'ordinateur, il peut bloquer la mise à jour automatique ; dans ce cas, autorisez TrikdisConfig dans 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.

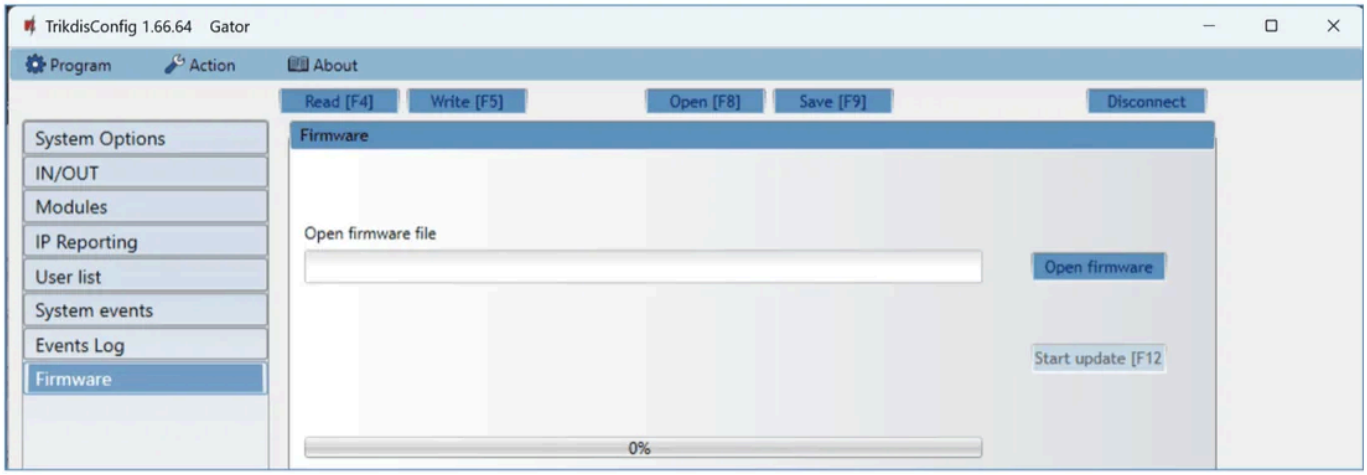


Figure 55. TrikdisConfig – GATOR, page **Firmware** : le bouton **Open firmware**, le champ du fichier choisi, le bouton **Start update [F12]** et l'indicateur de progression.

Pour le GATOR, le bouton qui lance la mise à jour s'intitule **Start update [F12]**. L'utilisation des modules RF-LORA et iO-LORA nécessite au moins le firmware **2.13**, celle des modules W485 et E485 au moins le firmware **1.06** ; vous voyez la version actuelle dans le champ **FW** de la barre d'état (point 5.1).

9. Dépannage et questions fréquentes

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

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

Le nombre de clignotements indique la cause du défaut : **1** – pas de carte SIM (ou mauvais contact : retirez-la et remettez-la) ; **2** – le code PIN de la carte SIM est erroné (désactivez la demande de code PIN dans un téléphone, ou saisissez le bon code PIN dans le champ **System Options** → **SIM card PIN**) ; **3** – impossible de se connecter au réseau mobile (niveau du signal, antenne, la carte SIM est-elle active, carte 2G dans un appareil 4G) ; **4** – impossible de se connecter au cloud Protegus ou au récepteur IP principal (données mobiles sur la SIM, APN, adresse et port du récepteur) ; **5** – impossible de se connecter au récepteur IP de secours ; **6** – l'horloge interne n'est pas réglée (synchronisation de l'heure, commande `TIME`) ; **7** – la tension d'alimentation n'est pas correcte.

J'appelle, mais le GATOR ne réagit pas

- Si la LED **NETWORK** n'est pas allumée en vert, l'appareil n'est pas connecté au réseau : vérifiez la carte SIM (active, code PIN désactivé, apte à recevoir des appels), l'antenne et le niveau du signal (le nombre de clignotements jaunes).
- Si vous avez déjà enregistré des utilisateurs, ou si la case **En** de la ligne **Not authorized** (n° 10) est décochée, l'appareil n'accepte que les appels des numéros de la liste – le numéro de l'appelant doit figurer dans la liste, au format international (+33…), être activé (**En**), avec une programmation horaire et une durée de validité valables (point 5.6).
- Sur le téléphone de l'appelant, le numéro ne doit pas être masqué, sinon l'appareil ne peut pas l'identifier.
- Vérifiez que le numéro ne figure pas dans la liste noire (point 5.6.4).

Il n'ouvre pas sur appel, mais il ouvre depuis l'application

Si un module W485 ou E485 est raccordé à l'appareil, vérifiez sur l'onglet **Modules** → **Parameters**, dans le groupe **SIM parameters**, la case **Use dial and SMS when working over internet module** : décochée, l'appareil n'utilise ni l'appel ni le SMS tant que la connexion Internet fonctionne (point 5.4). Cochez-la si la commande par appel est aussi nécessaire.

Pendant l'appel, je ne parviens pas à commander avec le clavier du téléphone

Pour la commande au clavier (DTMF), la valeur de **System Options** → **Hang-up after** doit être supérieure à 0, sinon l'appareil rejette immédiatement l'appel (point 4.2). Sur les appareils de type **GV17_2E70** et **GV17_2S70**, la commande DTMF ne fonctionne pas – le type est indiqué dans le champ **Device** de la barre d'état.

Protegus 2 ne trouve pas l'appareil, ou celui-ci ne passe pas à l'état Online

- Sur la page **IP Reporting**, la case **Enable cloud service** doit être cochée (par SMS : `CONNECT 123456 PROTEGUS=ON`), et la LED **TROUBLE** ne doit pas clignoter 4 fois.
- La carte SIM doit disposer d'un service de données mobiles, et l'APN doit être correct : dans le champ **System Options** → **APN**, la case **Auto** choisit dans la liste intégrée ; si la liaison ne s'établit pas, saisissez l'APN de l'opérateur (liste).
- Dans l'application, l'IMEI doit être exact et, si le **Cloud Access Code** n'est pas le code par défaut `123456`, saisissez le bon code.
- Si tout est en ordre, attendez 1 minute au maximum après l'ajout (point 4.3).

Le widget ne fonctionne pas, ou je ne le trouve pas

Le widget n'est disponible que sur un téléphone **Android** (point 4.4) ; sur iPhone, vous ouvrez depuis l'écran d'accueil de l'application. Sous Android, le GATOR doit être ajouté aux systèmes et vous devez être connecté ; si le widget reste gris, ouvrez une fois l'application et vérifiez la connexion Internet.

Le lecteur RFID ne lit pas la carte, ou le GATOR n'y réagit pas

- Vérifiez le raccordement selon le schéma du point 3.6 (avec un lecteur **D0** → **1 IN**, **D1** → **2 IN** ; pour le second lecteur **D0** → **3 I/O**, **D1** → **4 I/O** ; point négatif commun), ainsi que l'alimentation du lecteur : avec un lecteur 12 V, le GATOR doit être alimenté en **courant continu** ; avec un lecteur à niveau de signal de 5 V, cochez la case **Low voltage reader**.
- Sur la page **IN/OUT**, **Wiegand reader mode** doit correspondre au nombre de lecteurs (**Single** / **Dual**), et les bornes **3 I/O**, **4 I/O** ne doivent pas être réglées sur une autre fonction.
- Si l'appareil ne reconnaît pas les signaux du lecteur, essayez la case **Disable reader filter**.
- La carte doit figurer dans le tableau **User list** (enregistrée ou saisie par son numéro), être activée, avec la sortie du lecteur (point 5.6.2). Le journal des événements (point 5.8) montre si la lecture a eu lieu et pourquoi elle a été refusée (**Access denied**).

L'application n'affiche pas l'état réel du portail

Pour la signalisation de l'état du portail, la sortie d'état de la motorisation ou le fin de course du portail doit être raccordé à l'entrée **1 IN** (point 3.5), le type de l'entrée doit être réglé sur la page **IN/OUT** selon le contact, et l'entrée **1 IN** doit être choisie dans la colonne **Assign IN** de la ligne de **5 OUT** (point 5.10). Dans l'application, l'icône de la sortie montre ensuite l'état de l'entrée.

L'appareil ne répond pas aux commandes SMS

- Il n'accepte les commandes SMS que depuis les numéros **administrateurs** (1A–7A) ; la première personne qui appelle ou envoie un SMS devient l'administrateur. Si vous ne savez pas de qui il s'agit, lisez le tableau **User list** dans TrikdisConfig.
- Dans la commande, le mot de passe doit suivre le mot de commande, séparé par une espace (`INFO 123456`) ; le nouveau mot de passe comporte 6 caractères.
- Le SMS de réponse n'arrive que si la case **ACK for SMS message** est cochée pour l'administrateur (point 5.6).
- Si l'appareil fonctionne avec un module Internet (W485 / E485) et que la case **Use dial and SMS when working over internet module** est décochée, il ne traite pas les SMS tant que la connexion Internet fonctionne (point 5.4).

J'ai oublié le mot de passe administrateur

Le mot de passe ne peut pas être consulté. Connectez-vous à l'appareil par câble USB et rétablissez les réglages d'usine avec le bouton **Restore**, en bas à gauche de la fenêtre de programmation (point 5.9) – la liste des utilisateurs et tous les réglages sont alors effacés, l'appareil doit donc ensuite être reconfiguré. Si vous avez auparavant enregistré les réglages dans un fichier (**Save [F9]**), vous pouvez les charger après la réinitialisation avec le bouton **Open [F8]**, et il ne vous reste qu'à saisir de nouveau le mot de passe.

Faut-il une carte SIM si j'utilise un module W485 ou E485 ?

Non : avec le module WiFi W485 ou le module Ethernet E485, le GATOR fonctionne aussi sans carte SIM ; la commande se fait alors depuis l'application (et par carte RFID), sans appel ni SMS. Sur l'onglet **Modules** → **Parameters**, cochez la case **Disable indication of the absence of a SIM card**, afin que l'appareil ne signale pas l'absence de carte comme un défaut (point 5.4). Si vous souhaitez aussi le secours par le réseau mobile, insérez une carte SIM et laissez décochée la case **Disable the use of SIM card mobile data**.

Je voudrais commander plusieurs portails depuis un seul appareil

Le relais propre du GATOR commute un seul portail ; les bornes **3 I/O** et **4 I/O** peuvent piloter un relais externe en tant que sorties à collecteur ouvert (50 mA). Pour des portails éloignés les uns des autres, vous pouvez associer, avec l'émetteur-récepteur **RF-LORA**, jusqu'à 8 modules d'extension sans fil **iO-LORA**, chacun avec son propre relais, sa propre entrée et son propre lecteur RFID (point 3.9) ; pour davantage d'entrées et de sorties filaires, un module d'extension **iO8** ou **iO8-LORA** (point 3.10). Pour les utilisateurs, vous indiquez dans le champ **Can control output** la sortie qu'ils peuvent commuter.

10. Consignes de sécurité

Figyelem!

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

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

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

- Seule une personne qualifiée peut installer et entretenir le GATOR.

- Avant l'installation, lisez ce manuel afin d'éviter les erreurs pouvant entraîner un dysfonctionnement ou un endommagement de l'équipement.
- **Avant tout raccordement électrique, coupez l'alimentation** – celle du GATOR comme celle de la motorisation du portail.
- 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

- Le dispositif d'automatisation de portail GV17 fonctionne avec Protegus 2 – le GATOR et l'application ensemble.
- GV17 – système de contrôle d'accès et/ou de suivi du temps de travail – lecteurs RFID, entrée et sortie, temps de travail dans Protegus 2.
- Communication dual-path disponible aussi pour le contrôleur de portail GV17 GATOR – module W485 / E485 pour le GATOR.
- Contrôle d'accès sans fil flexible avec le système GATOR RF-LoRa – modules RF-LORA et iO-LORA, plusieurs portails dans un même système.
- Réglage de l'APN – liste des opérateurs mobiles européens – si la liaison de données mobile ne s'établit pas.
- Application Protegus Android / iPhone et web – à propos de l'application.
- Documentation en anglais : docs.trikdis.com – Cellular gate controller GATOR.

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

Produits associés

Trikdis GV17 - GATOR contrôleur de portail intelligent 4G GSM / IP

Trikdis GV17 – GATOR contrôleur de portail intelligent 2G GSM / IP

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

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

Module Trikdis IO8 Wired Expander **Module d'expanneur sans fil Trikdis Io8-Lora**

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

Antenne magnétique Trikdis ME301m avec fil 2,5 m

Droits d'auteur

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

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

Version toujours à jour de ce manuel : https://trikdis.fr/manuel-gv17