



Moyen de communication GSM G16T

MANUEL D'UTILISATEUR

SARL « TRIKDIS »
17 rue Draugystės,
LT-51229 Kaunas
LITUANIE
Courier : info@trikdis.lt
Site d'Internet : www.trikdis.lt

Contenu

EXIGENCES DE SECURITE	2
1 DESCRIPTION	3
1.1 PARAMÈTRES TECHNIQUES	3
1.2 PANNEAU DU MOYEN DE COMMUNICATION	4
1.3 BUT DES TERMINAUX	4
1.4 INDICATION DE LA LUMIÈRE	4
1.5 CONTENU DE L'EMBALLAGE	5
1.6 AVANT DE COMMENCER	5
2 CONNECTEZ G16T A TRIKDISCONFIG	5
2.1 DESCRIPTION DE LA BARRE D'ÉTAT	7
3 DEFINISSEZ LES PARAMETRES D'OPERATION	7
3.1 FENÊTRE DE CONFIGURATION DU SYSTÈME	7
3.2 FENÊTRE DE RAPPORTS CRA → CHAMP DE RAPPORT CRA.....	8
3.3 FENÊTRE DE RAPPORT CRA → CHAMP DES PARAMÈTRES	8
3.4 FENÊTRE DE RAPPORT DES UTILISATEURS → CHAMP DE SERVICE PROTEGUS	9
3.5 FENÊTRE DE RAPPORTS DES UTILISATEURS → CHAMP DE RAPPORTS LES SMS ET LES APPELS.....	9
3.6 FENÊTRE DE RAPPORT DES UTILISATEURS → CHAMP DE CONTRÔLE SMS	10
3.6.1 <i>Liste des commandes SMS</i>	10
3.6.2 <i>Exemples</i>	10
3.7 FENÊTRE DE LA CARTE SIM	11
3.8 FENÊTRE RÉCAPITULATIVE DE L'ÉVÉNEMENT.....	11
3.9 DÉCONNECTER LE DISPOSITIF :	12
4 PROCESSUS D'INSTALLATION PHYSIQUE.....	13
5 SERVICE PROTEGUS	14
5.1 AJOUTER LE SYSTÈME	14
5.2 ACTIVER/DÉSACTIVER À DISTANCE LE PANNEAU	15
6 TESTEZ LA PERFORMANCE DU MOYEN DE COMMUNICATION.....	15
7 ACCES À DISTANCE	15
8 MISE A JOUR MANUELLE DU MICROPROGRAMME.....	15

Exigences de sécurité

Le système d'alarme de sécurité devrait être installé et entretenu par un personnel qualifié.

Avant l'installation, lisez attentivement ce manuel afin d'éviter les erreurs pouvant entraîner un dysfonctionnement ou même endommager l'équipement.

Débranchez l'alimentation avant de procéder à des connexions électriques.

Les changements, modifications ou réparations non autorisés par le fabricant annulent vos droits en vertu de la garantie.



Veuillez agir conformément à vos règles locales et ne pas disposer de votre système d'alarme inutilisable ou de ses composants avec d'autres ordures ménagères.

1 Description

Communicator G16T est destiné à mettre à niveau n'importe quel panneau d'alarme intrus avec le communicateur de ligne téléphonique (TLC) pour la signalisation d'événement via le réseau cellulaire.

Moyen de communication transmet l'information complète sur les événements au Centre de réception des alarmes (CRA).

Les clients sont informés sur des événements du système de sécurité dans les applications Protegus ou avec des messages SMS. Ils peuvent armer / désarmer le système d'alarme à distance.

Caractéristiques

Connexion

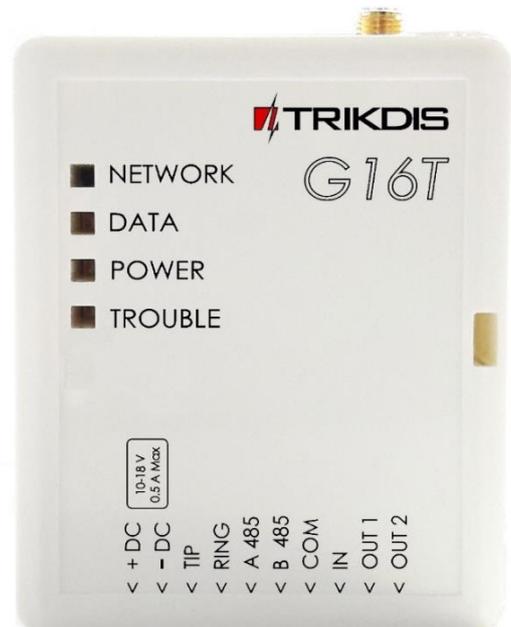
- Connexion aux panneaux de commande via :
 - Connexion du terminal TLC.

Communications

- Modes de communication :
 - GPRS (sur demande 3G)
 - SMS
- 2 Principaux canaux de communication fonctionnant simultanément
- Chaque canal possède un canal de sauvegarde distinct
- Contrôle de connexion avec CRA
- Rapport d'événement simultané à l'application Protegus Mobile / Web, permettant à l'utilisateur de surveiller et de contrôler à distance son système d'alarme
- Les messages d'événement sont transmis dans les codes d'identification de contact
- Rapports d'événements par SMS à 4 utilisateurs différents dans les messages SMS personnalisés par l'utilisateur

Configuration

- Configuration rapide et facile et mises à jour du microprogramme
- L'accès à la configuration de l'appareil est sécurisé avec un mot de passe à deux niveaux



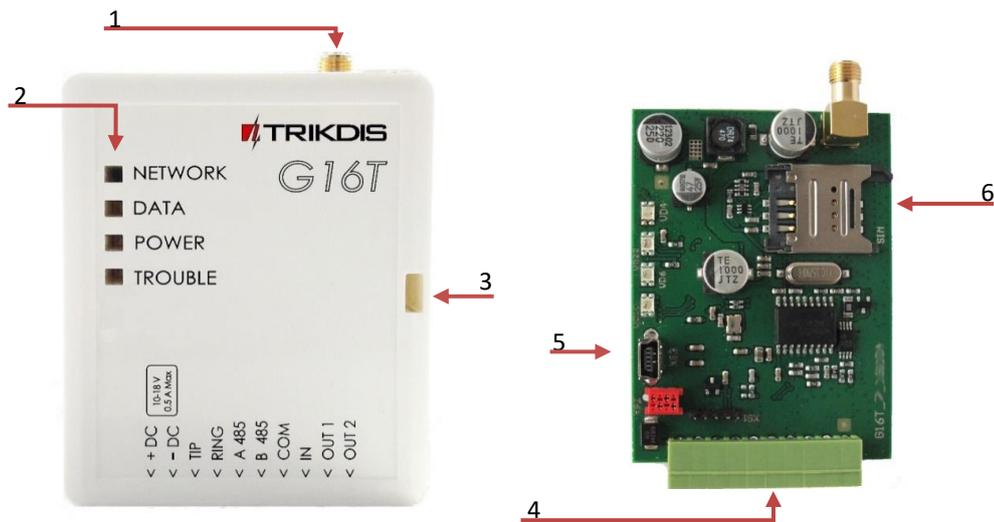
Entrées et sorties

- 2 sorties contrôlées via Mobile/Web application ou SMS
- 1 Entrée, type : NC, NO

1.1 Paramètres techniques

Paramètre	Description
Fréquences de modem GSM	850 / 900 / 1800 / 1900 MHz
Fréquences de modem 3G	800 / 850 / 900 / 1900 / 2100 MHz
Source de courant	DC 10-18V
Consommation de courant	60-100 mA (en attente) Up to 250 mA (lors de l'envoi des données)
Protocoles de transmission	TRK, DC-09_2007, DC-09_2012
Cryptage des messages	AES 128
Mémoire	Jusqu'à 60 messages
Entrées	1, NC/NO type
Sorties	2 x OC type, commutant jusqu'à 0,15 A DC, 30 V max
Configuration des paramètres	Localement via le port USB ou à distance
Environnement d'exploitation	Température de -10 °C jusqu'à 50 °C, humidité relative – jusqu'à 80% à +20 °C
Dimensions du moyen de communication	65 x 77 x 25 mm

1.2 Panneau du moyen de communication



- 1. Connecteur SMA d'antenne GSM
- 2. Indicateurs lumineux
- 3. Emplacement d'ouverture du boîtier frontal
- 4. Bloc de bornes
- 5. Port USB Mini-B pour la programmation des moyens de communication
- 6. Emplacement de la carte SIM

1.3 But des terminaux

Terminal	Description
+DC	Source de courant +10 V/+18 V
-DC	Commun (négatif)
TIP	Connexion à la pince TIP du panneau de contrôle de sécurité
RING	Connexion au collier RING du panneau de contrôle de sécurité
A 485	Pour une utilisation future
B 485	Pour une utilisation future
COM	Commun (négatif)
IN	Entrée
OUT1	1 ^{ère} sortie de collecteur ouvert
OUT2	2 ^{ème} sortie de collecteur ouvert

1.4 Indication de la lumière

Indicateur	Statut lumineux	Description
Réseau	Déconnecté	Pas de connexion au réseau GSM
	Jaune clignotant	Connexion au réseau GSM
	Vert solide avec jaune clignotant	Moyen de communication est connecté au réseau GSM. Une intensité de signal GSM suffisante est le niveau 5 (cinq flashes jaunes)
Données	Déconnecté	Pas de messages dans le tampon
	Vert solide	Messages non transmis dans la mémoire du moyen de communication
	Vert clignotant	(Mode de configuration) Les données sont transférées vers / depuis le moyen de communication
Puissance	Déconnecté	Pas de source de courant
	Vert solide	Source de courant est suffisante et le microcontrôleur fonctionne
	Jaune solide	Source de courant est insuffisante ($\leq 11.5V$), le microcontrôleur fonctionne

	Vert solide avec jaune clignotant	(Mode de configuration) Moyen de communication est prêt à être configuré
	Jaune solide	(Mode de configuration) Pas de connexion avec l'ordinateur
Problème	Déconnecté	Aucun problème d'opération
	1 clignotement rouge	Pas de carte SIM
	2 clignotements rouges	Problème de code PIN de la carte SIM (code PIN incorrect)
	3 clignotements rouges	Problème de programmation (pas d'APN)
	4 clignotements rouges	Inscription au problème du réseau GSM
	5 clignotements rouges	Inscription au problème du réseau GPRS / UMTS
	6 clignotements rouges	Pas de connexion avec le récepteur
	7 clignotements rouges	Connexion perdue avec le panneau de commande
	Rouge clignotant	(Mode de configuration) Défaut de mémoire
Rouge solide	(Mode de configuration) Le microprogramme est corrompu	

1.5 Contenu de l'emballage

Moyen de communication G16T	1 pc.
-----------------------------	-------

1.6 Avant de commencer

Avant de commencer, assurez-vous que vous avez le nécessaire :

- 1) Câble USB (type Mini-B) pour la configuration.
- 2) Câble d'au moins 4 fils pour connecter le moyen de communication au panneau de commande.
- 3) Câble CRP2 pour la connexion au port série du panneau Paradox.
- 4) Tournevis à tête plate.
- 5) Gain suffisant GSM antenne

Commandez-les séparément de votre distributeur local.

2 Connectez G16T à TrikdisConfig

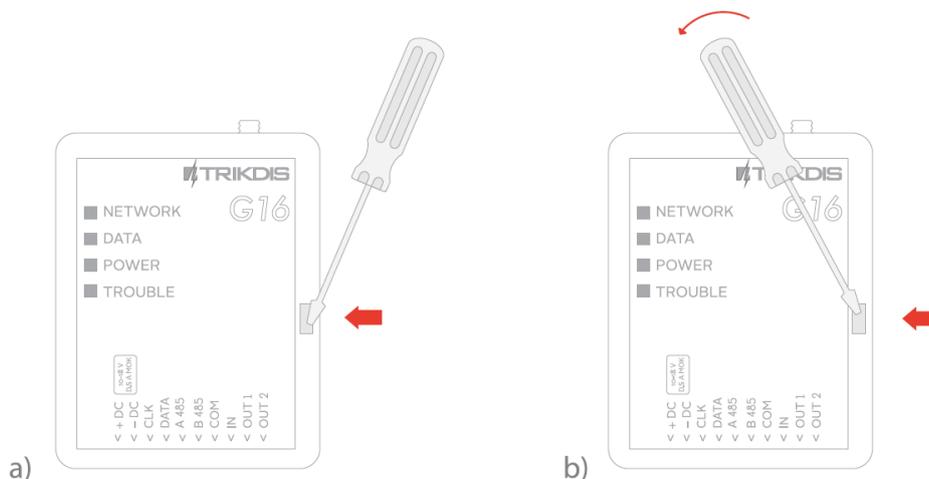
Moyen de communication peut être configuré à l'aide du microprogramme TrikdisConfig pour MS Window OS via un câble USB ou à distance.

IMPORTANT : pour utiliser la fonction de configuration à distance, le service Protegus doit être activé.

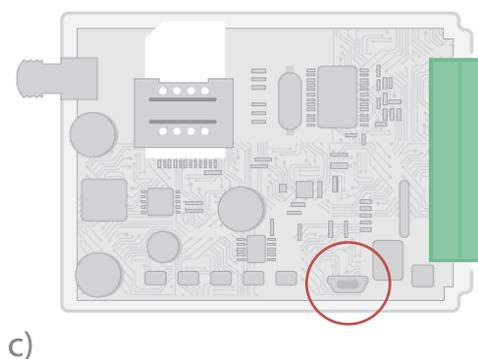
- 1) Téléchargez **TrikdisConfig** de www.trikdis.com (dans le champ de recherche type TrikdisConfig), et installez-le.
- 2) Connectez le communicateur à **TrikdisConfig** :
 - **Utilisation du câble USB** : Ouvrez soigneusement le boîtier avec un tournevis comme indiqué ci-dessous, Pour ouvrir le boîtier, vous aurez besoin d'un tournevis à tête plate :



- Insérer le tournevis dans le trou (flèche rouge). (Il est inutile de mettre la tête du tournevis au bas de l'enveloppe).
- Tenez la partie inférieure du boîtier avec une main et pressez doucement le tournevis sur le côté gauche.



- Branchez le câble USB. Exécutez le microprogramme de configuration **TrikdisConfig**. Le microprogramme reconnaîtra automatiquement le dispositif connecté et ouvrira une fenêtre pour la configuration du communicateur :



- **À distance:** exécuter le programme de configuration **TrikdisConfig**. Dans la section, *Accès à distance*, champ ID unique, entrez l'adresse IMEI du moyen de communication (l'adresse IMEI est fournie sur le paquet du produit). (Facultatif) dans le champ **Nom du système** entrez le nom souhaité au moyen de communication. Appuyez sur **Configurer**.

Remote access	
Choose module	Unique ID
	System Name
	<input type="text"/> <input type="text"/>
	<input type="button" value="Configure"/> <input type="button" value="Control"/>

- 3) Cliquez sur **Lire [F4]** pour lire les paramètres des communicateurs et entrez le code Administrateur ou Installer dans la fenêtre contextuelle. Pour que le programme se souvienne du code, cochez la case à côté de **Mot de passe oublié**.

Remarque: Si le code administrateur est défini par défaut (123456), il n'est pas nécessaire de l'entrer et la fenêtre de demande n'apparaîtra pas.
Pour configurer le communicateur à partir d'un fichier de configuration enregistré, cliquez sur **Ouvrir [F8]** et pCRAourez votre ordinateur pour trouver le fichier de configuration.

2.1 Description de la barre d'état

Une fois que les paramètres du moyen de communication sont lus, la barre d'état affichera des informations sur le dispositif.

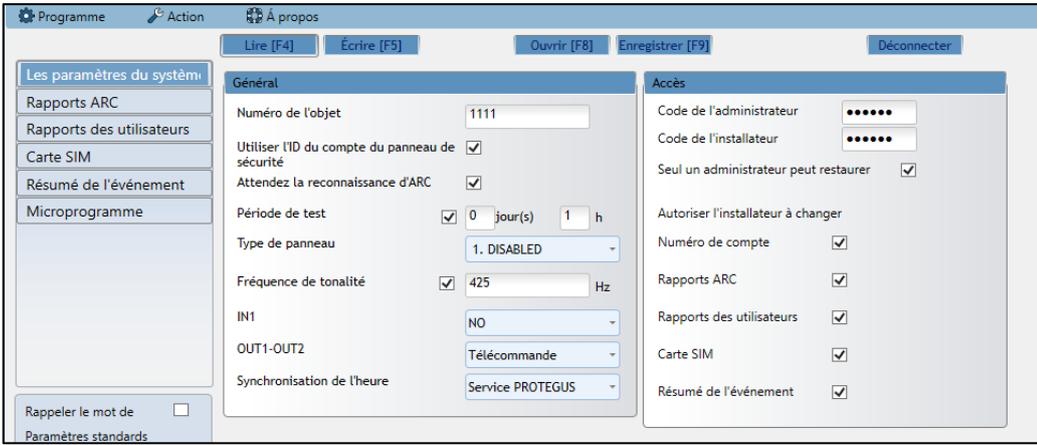
Rappeler le mot de Paramètres standards <input type="checkbox"/> <input type="button" value="Restaurer"/> IMEI / ID unique: 865789023243928										
État : lecture terminé		Dispositif	G16_3G	SN:000001	BL: 1.02	FW:1.07	HW: 0.01	État	HID	Admin

Barre d'état

Nom	Description
IMEI / ID unique	Numéro IMEI de l'appareil
État	Statut de l'action
Dispositif	Type de dispositif (montre G16T ou G16T_3G)
SN	Numéro de série
BL	Version Bootloader
FW	Version du microprogramme
HW	Version du matériel
État	Statut de connexion
Admin	Niveau d'accès (s'affiche après que le code d'accès est confirmé)

3 Définissez les paramètres d'opération

3.1 Fenêtre de configuration du système



The screenshot shows a software interface for configuring a GSM communication device. It features a menu on the left with options like 'Les paramètres du système', 'Rapports ARC', and 'Microprogramme'. The main area is divided into 'Général' and 'Accès' sections. The 'Général' section includes fields for 'Numéro de l'objet' (1111), 'Période de test' (0 days, 1 hour), 'Type de panneau' (1. DISABLED), 'Fréquence de tonalité' (425 Hz), and 'Synchronisation de l'heure' (Service PROTEGUS). The 'Accès' section includes fields for 'Code de l'administrateur' and 'Code de l'installateur', and several checkboxes for permissions like 'Seul un administrateur peut restaurer' and 'Autoriser l'installateur à changer'.

Général

- Écrivez un **Numéro de l'objet** approprié (4 symboles hexadécimaux).
- **Période de test** : Les messages de test périodique seront envoyés selon un intervalle de temps défini dans cette section.
- Pour la communication avec le panneau de commande, le type de panneau doit être sélectionné en Type Panneau.
- Utiliser l'ID du compte du panneau de sécurité - l'ID du compte est définie dans le panneau de contrôle, si elle est activée, elle sera transmise à un G16T.
- Attendez la reconnaissance d'CRA - après une réception réussie d'un message à ARC, le moyen de communication envoie un signal de fusion au panneau de commande. Si le panneau de commande ne reçoit pas la tonalité à temps, il retransmet le message.
- Sélectionnez **Type de panneau** - option INTERFACE DTMF signifie que le moyen de communication est appliqué pour recevoir des informations codées dans le format Contact ID depuis le moyen de communication téléphonique du panneau de commande en tonalités DTMF.
- Activez et écrivez en **Fréquence de tonalité** pour indiquer si la communication fonctionne et si elle est prête à lancer l'appel.

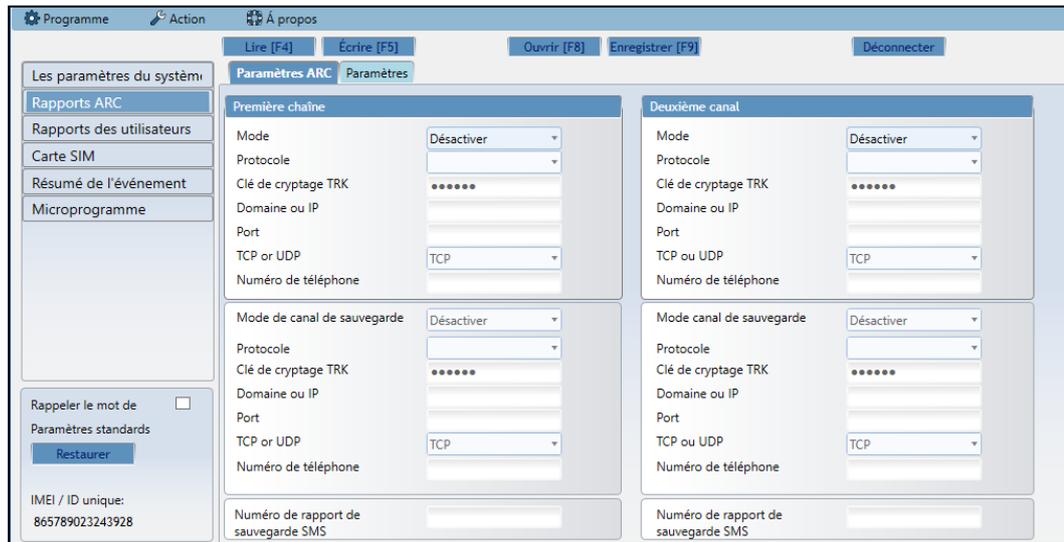
Accès

Le communicateur G16T dispose de deux niveaux d'accès pour la configuration du dispositif :

- **Code d'administrateur** – permet un accès complet à la configuration.
- **Code d'installateur** – permet un accès limité pour installer à la configuration.

Remarque : Les codes de l'administrateur et de l'installateur doivent comporter six symboles et contenir uniquement des chiffres ou des caractères latins.

3.2 Fenêtre de Rapports CRA → Champ de rapport CRA

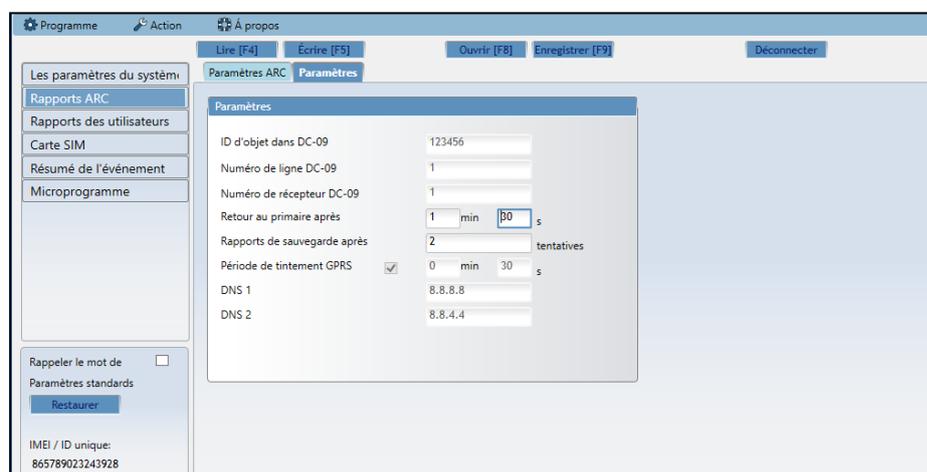


Premier et deuxième canaux (et canaux de sauvegarde)

Les premier et second canaux peuvent fonctionner en parallèle, en permettant au moyen de communication de transmettre simultanément des données via les deux canaux.

- Sélectionnez le **Mode** et le **Protocole** de communication.
 - Si les rapports SMS seront utilisés - entrez la **Clé de cryptage TRK** et le numéro de téléphone des récepteurs.
- Entrez le **Domaine** ou l'adresse **IP** et le **Port** du récepteur.
- Choisissez le protocole de transmission d'événement **TCP ou UDP**.
- Entrez le **Numéro de téléphone** qui recevra des messages (les numéros de téléphone doivent contenir un code de pays, par exemple +370xxxxxxxx, 00370xxxxxxxx, ou 370xxxxxxxx).
- **Numéro de rapport de sauvegarde SMS** – lorsque le mode GPRS est défini dans les canaux de première et de sauvegarde, cette chaîne 1) enverra un message à l'CRA lorsque le moyen de communication commencera à fonctionner et 2) servira de troisième canal de sauvegarde.

3.3 Fenêtre de rapport CRA → Champ des paramètres



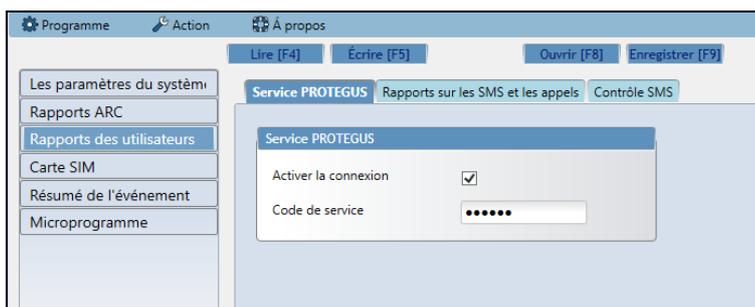
Paramètres

- Écrivez d'**ID d'objet** dans le code **DC-09**, si l'événement est transféré à l'aide du protocole SIA DC-09 (numéro hexadécimal 4-16 symbole).
- Entrez le **numéro de ligne DC-09** requis.
- Entrez le **numéro du récepteur DC-09** requis.
- Après un certain nombre de tentatives de reconnexion échoués, comme défini dans le **rapports de sauvegarde après** le champ.
- Il tentera de revenir à la chaîne principale après une heure, comme défini dans le **Retour au primaire** après le champ.
- **Période de tintement GPRS** – et temps réglé entre les signaux en secondes (requis pour le contrôle de la communication).
- Entrez les adresses **DNS** requises.

3.4 Fenêtre de Rapport des utilisateurs → Champ de Service Protegus

Le service Protegus permet aux utilisateurs de surveiller et de contrôler à distance le moyen de communication. Le service Protegus permet la transmission simultanée de données au serveur Protegus pour une application mobile / Web. Pour plus d'informations sur le service PROTEGUS, visitez www.protegus.eu.

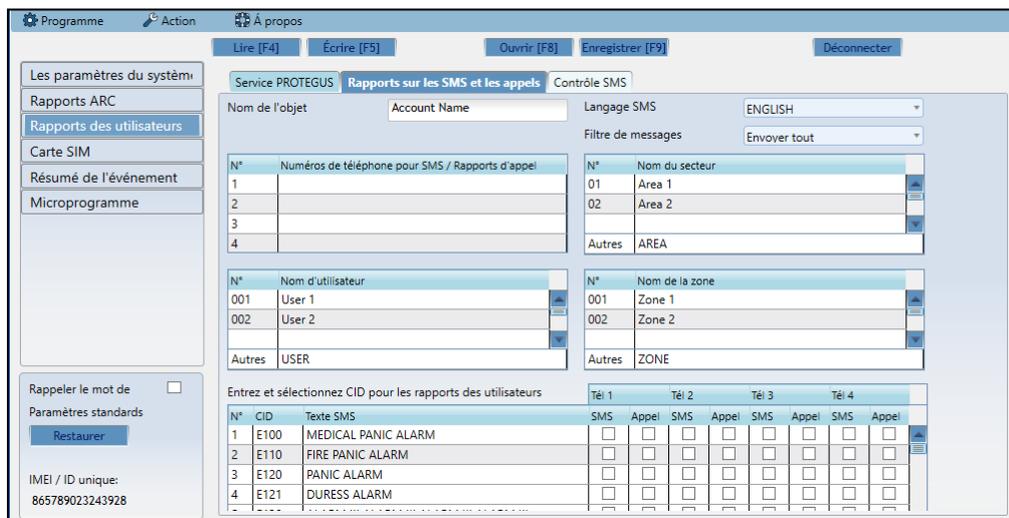
IMPORTANT: Lorsque le service Protegus est utilisé – Le champ de notification des SMS et des appels sera automatiquement désactivé.



Service Protegus

- Activer le service de nuage à la champ de **service PROTEGUS**.
- Entrez le **code de service** (code par défaut - 123456), pour plus de sécurité, changez le code de six symboles.

3.5 Fenêtre de Rapports des utilisateurs → Champ de Rapports les SMS et les appels



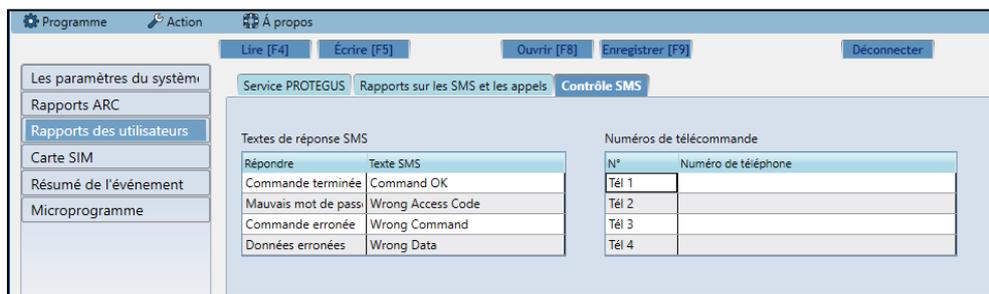
Les messages d'événement reçus et les événements de moyens de communications internes peuvent être signalés aux utilisateurs des téléphones portables par messagerie SMS et appels.

- Chaque message comporte un nom d'objet: entrez le **nom de l'objet** de votre choix dans le champ de texte.

- À partir de la liste déroulante du **langage SMS**, sélectionnez la langue requise (Les messages SMS peuvent être envoyés dans différents jeux de caractères).
- Il est possible de choisir le **mode de Rapport**, par lequel les événements seront signalés à l'utilisateur :
 - **Rapport même les événements non décrits** – rapport tous les événements, même pas décrits, ou
 - **Rapport un événement avec un message texte SMS décrit** - ceux qui ont une zone, des secteurs et des noms d'utilisateur entrés.
- Le message peut être envoyé jusqu'à 4 numéros de téléphone différents. Listez-les dans le tableau des **numéros de téléphone** (les numéros de téléphone doivent contenir un code de pays, par exemple +370xxxxxxx, 00370xxxxxxx, ou 370xxxxxxx).
- Les informations sur les événements reçus en tant que **secteurs, utilisateurs et zones** sont codées en chiffres. Chacun d'entre eux peut être nommé et les noms seront utilisés dans les messages SMS envoyés aux utilisateurs. Écrivez vos noms choisis dans leurs tableaux appropriés.
- Pour recevoir des messages d'événement, spécifiez les événements CID qui seront rapportés. En outre, on peut choisir les numéros de téléphone qui reçoivent des notifications (SMS / Appel) sur les événements.

3.6 Fenêtre de rapport des utilisateurs → Champ de Contrôle SMS

Remarque : Les commandes SMS peuvent être envoyées à partir de n'importe quel numéro de téléphone s'il n'y a pas de numéros décrits dans la liste.



Télécommande

- Les réponses aux commandes SMS peuvent être personnalisées dans un **champ de réponse SMS**.
- Insérez un numéro de téléphone pour la télécommande sur un tableau **Numéro de téléphone pour la télécommande**. SMS, que l'utilisateur reçoit après avoir envoyé une commande (pour recevoir un message de réponse SMS, le **code d'accès** utilisateur doit être correct).

3.6.1 Liste des commandes SMS

Les commandes SMS sont utilisées pour contrôler à distance le dispositif.

Comme le code d'accès utilisez « **Code Administrateur** » ou « **Code Installer** », « _ » représente un espace.

Structure de commande SMS : CodeAcces_Commande_Donnees.

Commande	Données	Description
INFO		Informations sur la demande du dispositif. La réponse comprendra : le type du dispositif, le numéro IMEI, le numéro de série et la version du microprogramme.
RESET		Redémarrez le dispositif.
OUTPUTx	ON	Activez la sortie, où « x » représente la sortie numéro 1 ou 2.
	OFF	Éteignez la sortie, où « x » représente la sortie numéro 1 ou 2.
	PULSE tttt	Activez la sortie pendant un certain nombre de secondes, où « x » représente le numéro de sortie (1) et « tttt » un nombre à quatre chiffres représentant la durée d'impulsion en secondes.

3.6.2 Exemples

Par exemple, le code d'accès est 123456.

Pour recevoir des informations sur le dispositif :

« 123456 INFO »

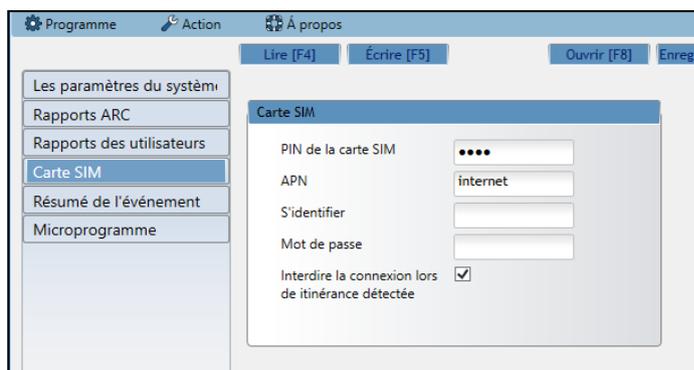
Pour activer la sortie OUT1 :

« 123456 OUTPUT1 ON»

Pour activer la sortie OUT1 pendant 3 secondes :

« 123456 OUTPUT1 PULSE=0003»

3.7 Fenêtre de la Carte SIM



Assurez-vous que la carte SIM fonctionne avant de l'utiliser.

Si une communication GPRS ou 3G est requise, assurez-vous que le service de données mobiles est activé. Pour plus d'informations, comment activer ce service, contactez votre fournisseur de services GSM.

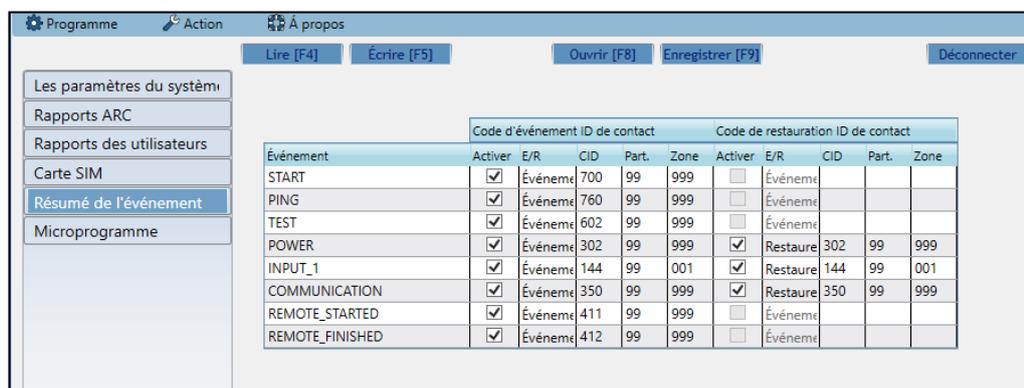
Carte SIM

- Entrez le code **PIN de la carte SIM**, **APN**.
- S'il est nécessaire, entrez le nom et le mot de passe du réseau GSM dans les champs **Connexion**, **Mot de passe**.
- Interdites la connexion lors de roaming détecté (utilisez-la lorsque le système de sécurité est installé près de la frontière du pays, cela garantira que le moyen de communication ne se connecte pas au réseau GSM incorrect).

3.8 Fenêtre récapitulative de l'événement

Le moyen de communication peut générer des **messages de test** périodiques.

Pour activer les messages de repos périodiques à l'échelle mondiale et régler l'heure, accédez à Les paramètres du système → Général → Période de test. Le temps est fixé dans le jour (s) et les heures (maximum 7 jours).



Événement	Code d'événement ID de contact					Code de restauration ID de contact				
	Activer	E/R	CID	Part.	Zone	Activer	E/R	CID	Part.	Zone
START	<input checked="" type="checkbox"/>	Événeme	700	99	999	<input type="checkbox"/>	Événeme			
PING	<input checked="" type="checkbox"/>	Événeme	760	99	999	<input type="checkbox"/>	Événeme			
TEST	<input checked="" type="checkbox"/>	Événeme	602	99	999	<input type="checkbox"/>	Événeme			
POWER	<input checked="" type="checkbox"/>	Événeme	302	99	999	<input checked="" type="checkbox"/>	Restaure	302	99	999
INPUT_1	<input checked="" type="checkbox"/>	Événeme	144	99	001	<input checked="" type="checkbox"/>	Restaure	144	99	001
COMMUNICATION	<input checked="" type="checkbox"/>	Événeme	350	99	999	<input checked="" type="checkbox"/>	Restaure	350	99	999
REMOTE_STARTED	<input checked="" type="checkbox"/>	Événeme	411	99	999	<input type="checkbox"/>	Événeme			
REMOTE_FINISHED	<input checked="" type="checkbox"/>	Événeme	412	99	999	<input type="checkbox"/>	Événeme			

Les changements locaux des messages de test périodique peuvent être effectués dans la **fenêtre récapitulative des événements** :

- Les tests et autres événements internes peuvent être activés / désactivés et leur numéro de contact peut être personnalisé. Pour activer la génération d'événements et définir le numéro d'identification de contact, accédez au tableau récapitulatif des événements.

3.8 Pour écrire de nouveaux paramètres sur le moyen de communication, cliquez sur Ecrire [F5].

Remarque :

Pour restaurer les paramètres par défaut du communicateur, appuyez sur le bouton **Restaurer** sous **Paramètres par défaut** dans le coin inférieur gauche de la fenêtre de configuration.

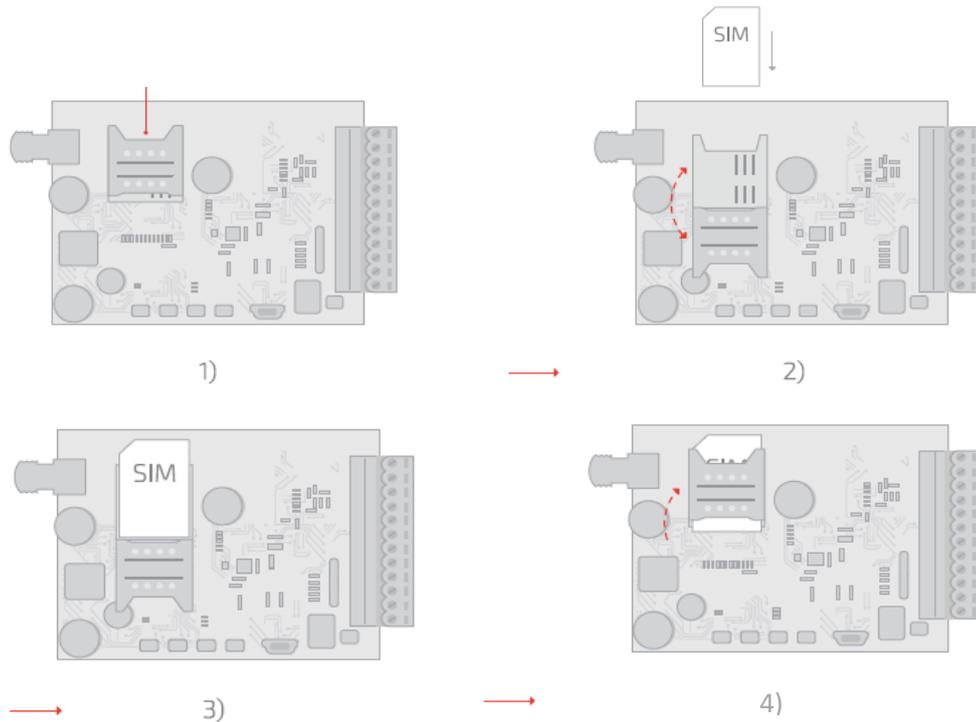
Pour créer un fichier de configuration contenant des paramètres actuels, cliquez sur **Enregistrer [F9]**.

3.9 Déconnecter le dispositif :

- Cliquez sur **Déconnecter** pour vous déconnecter des rôles (installateur ou administrateur) lorsque le moyen de communication est connecté via le câble USB à l'ordinateur.
- Si une configuration est effectuée via un câble USB, débranchez le câble USB, cliquez sur **Déconnecter** pour revenir à la première fenêtre.

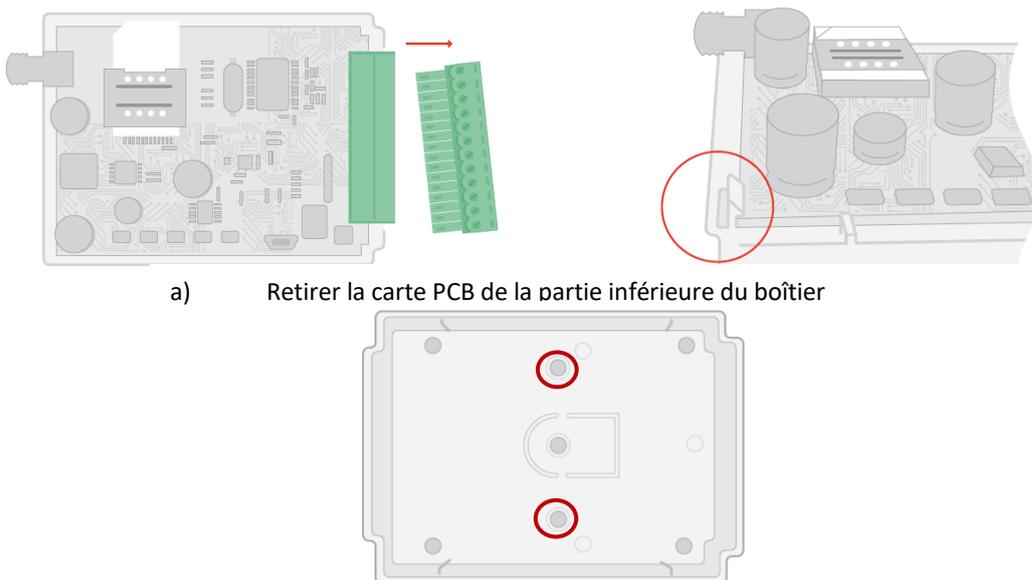
4 Processus d'installation physique

4.1 Insérez la carte SIM dans le support.



- La carte SIM doit déjà être enregistrée sur le réseau GSM, si la communication GPRS est utilisée, assurez-vous d'activer le service de données mobiles.
- Pour configurer le dispositif à distance, insérez une carte SIM avec la fonction de demande de code PIN désactivée.

4.2 Installez le moyen de communication dans un boîtier de montage. Si le montage de la vis est utilisé :



- Fixez ensuite la partie inférieure à sa place avec des vis, remettez la carte PCB dans un support

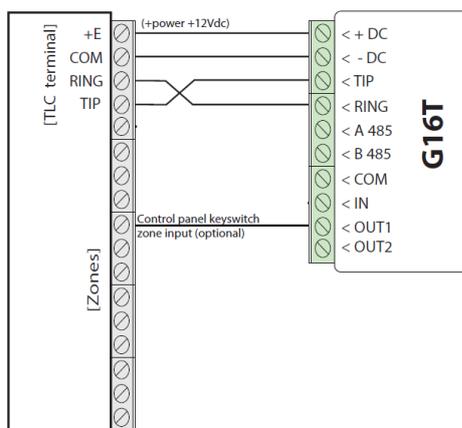
4.3 Fermez le support du moyen de communication.

4.4 Connectez l'antenne GSM.

Remarque : La puissance du signal GSM suffisante est au niveau 5 (cinq flashes jaunes de l'indicateur Réseau). La puissance suffisante du signal 3G est au niveau 3 (trois flashes jaunes de l'indicateur Réseau).

4.5 Suivant les schémas prévus, connectez le panneau de commande, les capteurs et les connexions de sortie.

4.5.1 Schémas de câblage



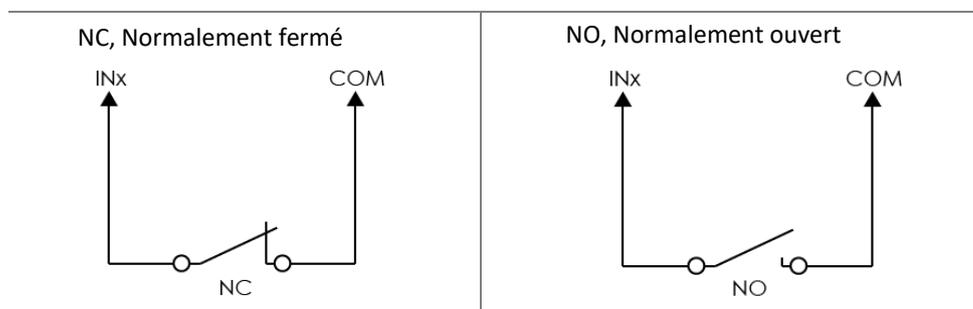
4.5.2 Programmation du panneau de commande de sécurité

Utiliser le manuel de programmation spécifique au panneau de commande de sécurité pour définir les paramètres d'exploitation comme suit :

- 1) Activer le numéroteur PSTN du panneau.
- 2) Choisir le mode DTMF.
- 3) Choisir le format de communication Contact ID.
- 4) Entrer un numéro de téléphone pour la numérotation (vous pouvez utiliser tout numéro avec au minimum 2 chiffres).
- 5) Entrer un numéro de compte à 4 chiffres dans le panneau.

4.5.3 (Facultatif) Connexion d'entrée

Le moyen de communication contient une borne d'entrée (IN1) pour la connexion des capteurs. Pour régler le type de connexion d'entrée, voir **3.8 Fenêtre récapitulative de l'événement**.



4.6 Allumez la source de courant.

5 Service Protegus

5.1 Ajouter le système

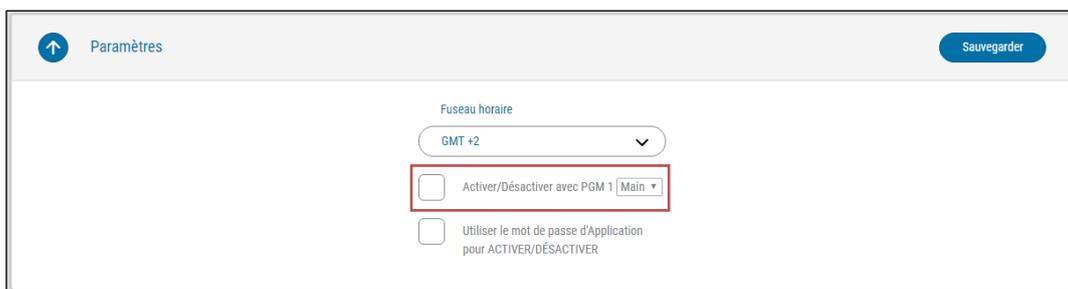
- 1) **Vérifiez que le communicateur soit alimenté et connecté au réseau GSM.**
- 2) Si vous n'avez pas de compte Protegus, créez-en un en complétant le formulaire ici : www.protegus.eu
- 3) Pour ajouter le système à Protegus, appuyez sur "Ajouter un nouveau système +" et entrez les données requises :



5.2 Activer/désactiver à distance le panneau

Pour activer dans l'application Protegus la fonction ACTIVER/DÉSACTIVER à distance le panneau de commande, suivez ces étapes :

- 1) Programmez la zone du panneau d'alarme comme zone de verrouillage à clé de façon momentanée (se référer au manuel de programmation du panneau de contrôle de sécurité)
- 2) Connecter la sortie OUT1 du communicateur à l'entrée de la zone de verrouillage à clé du panneau (un fil, pas de résistance).
- 3) Dans l'application Protegus, puis dans la fenêtre **Paramètres** → **Paramètres**, cochez la case "**Activer/Désactiver avec PGM**". Enregistrer les modifications.



IMPORTANT: Dans l'application Protegus, une sortie PGM peut être affectée à la commande d'une Zone (1 PGM-1 Area, 2 PGM-2 Areas) quel que soit le nombre de zones contrôlées par la même zone de commutateur à clé dans le panneau.

Réglez la zone qui sera contrôlée par Protegus dans le système "Paramètres". Il cochez la case « Arm / Désarmer avec PGM », et le nombre de la zone, que vous souhaitez contrôler.

Dans la fenêtre Protegus "Areas", vous verrez toutes les zones disponibles dans le système, avec des zones contrôlables mises en évidence.

6 Testez la performance du moyen de communication

- 1) Une fois la configuration et l'installation terminées, effectuez un test du système. Activez un événement dans le panneau de contrôle et assurez-vous que l'événement arrive au centre de réception d'alarme ou est reçu dans l'application mobile.
- 2) Pour tester l'entrée du moyen de communication, activez-le et assurez-vous que les messages corrects arrivent aux destinataires.
- 3) Pour tester les sorties du moyen de communication, activez-les à distance. Effectuez des tests de signalisation d'alarme pour vous assurer que le centre de réception d'alarme reçoit correctement les signaux.

7 Acces à distance

Moyen de communication G16T peut être commandé à distance en utilisant TrikdisConfig. Pour ce faire, suivez les étapes indiquées ci-dessous :

- 1) Sur le champ **Acces à distance**, dans le champ **Unique ID** entrez l'adresse IMEI. L'adresse IMEI est fournie sur le paquet du produit.
- 2) (Facultatif) Dans le champ **Nom du système** entrez le nom souhaité au moyen de communication, appuyez sur **Controle**.
- 3) Entrez **Code de libre-service** – c'est le même code utilisé pour le code de service Protegus.
- 4) Dans une nouvelle fenêtre, **Zones tab**, les zones peuvent être contrôlés. De plus, (dans tous les onglets) le temps de rafraîchissement peut être sélectionné.
- 5) Dans l'onglet **Sorties PGM**, les sorties PGM peuvent être contrôlées - désactivées / activées.

8 Mise à jour manuelle du microprogramme

Le microprogramme du moyen de communication peut être mis à jour ou modifié manuellement. Après une mise à jour, tous les paramètres précédents du moyen de communication resteront les mêmes.

Lors de l'écriture manuelle du microprogramme, il peut être changé en version plus récente ou ancienne. Pour mettre à jour :

- 1) Exécutez TrikdisConfig.
- 2) Connectez le moyen de communication via un câble USB à l'ordinateur ou connectez-vous au moyen de communication à distance.
 - Si la version de microprogramme plus récente existe, le microprogramme proposera de télécharger le nouveau fichier de version de microprogramme.

Remarque : S'il existe un logiciel antivirus installé sur votre ordinateur, il peut bloquer l'option de mise à jour automatique du microprogramme. Dans ce cas, vous devez reconfigurer votre logiciel antivirus.

- 3) Sélectionnez la branche du menu Microprogramme.
- 4) Appuyez sur Ouvrir le microprogramme et sélectionnez le fichier de microprogramme requis.
 - Si vous ne possédez pas le fichier, le fichier de microprogramme le plus récent peut être téléchargé par un utilisateur enregistré de www.trikdis.com, dans la section de téléchargement du moyen de communication G16T.
- 5) Appuyez sur **Mise à jour [F12]**.
- 6) Attendez que l'invite concernant la mise à jour terminée apparaisse.
- 7) Cliquez sur **OK** dans la fenêtre d'invite.