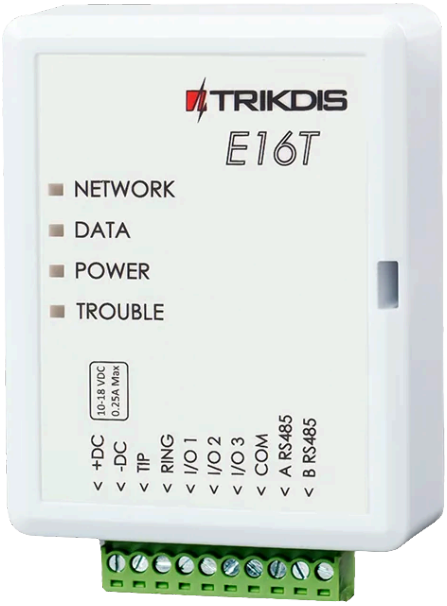
Communicateur E16T – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation du communicateur Ethernet Trikdis E16T : raccordement à la centrale d'alarme, configuration réseau dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2, vérification et dépannage.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-e16t

Sommaire

1. Présentation

1.1 À quoi sert-il, comment fonctionne-t-il ?
1.2 Versions
1.3 Caractéristiques principales
1.4 Éléments du communicateur
1.5 Bornes
1.6 Signalisation des LED
1.7 Caractéristiques techniques

2. Mise en service rapide avec TrikdisConfig

2.1 Préparatifs
2.2 Liaison avec l'application Protegus 2
2.3 Liaison avec le centre de télésurveillance

3. Installation et raccordement

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

4. Programmation de la centrale d'alarme

4.1 Programmation du transmetteur Honeywell Vista
4.2 Centrales d'autres fabricants

5. Commande à distance avec l'application Protegus 2

5.1 Ajout de l'appareil
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armement et désarmement par une sortie
5.3 Armement et désarmement depuis l'application

6. TrikdisConfig – les paramètres en détail

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

7. Programmation à distance

8. Vérification du fonctionnement du communicateur

9. Mise à jour du firmware

10. Dépannage et questions fréquentes

11. Consignes de sécurité

Voir aussi

1. Présentation

L'E16T est le **communicateur Ethernet universel** de Trikdis : il se raccorde à la sortie ligne téléphonique (TIP/RING) de la centrale d'alarme et se comporte comme un central téléphonique. La centrale « compose un numéro » et envoie le message Contact ID en tonalités DTMF ; l'E16T décroche la ligne, décode le message et le transmet, par le réseau local et la connexion Internet filaire, au récepteur du centre de télésurveillance ainsi qu'au cloud Protegus, dans l'application de l'utilisateur. Il peut ainsi être utilisé avec **une centrale de n'importe quelle marque** disposant d'un transmetteur Contact ID – inutile de remplacer la centrale, il suffit de configurer son transmetteur. L'E16T fonctionne par Internet filaire, sans carte SIM ni abonnement.

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

- **Il transmet au centre de télésurveillance.** Il envoie les événements par IP au récepteur logiciel ou matériel Trikdis (protocole TRK ; ces récepteurs fonctionnent avec n'importe quel logiciel de télésurveillance) ou à tout récepteur universel (SIA DC-09 2007/2012, SUR-GARD TL150). Par défaut, il vérifie la liaison toutes les 30 secondes (il envoie un signal de vie, un PING, au récepteur ; l'intervalle est modifiable) et, en cas de défaut, bascule sur le canal de secours.
- **Il informe l'utilisateur.** L'application Protegus 2 signale ce qui s'est passé par notification push (avec un son distinct) et dans la liste des événements ; depuis l'application, l'utilisateur peut armer et désarmer, et commander les équipements raccordés (éclairage, portail, ventilation, chauffage, arrosage, etc.). L'application fonctionne avec la centrale d'alarme de n'importe quel fabricant à laquelle l'E16T est raccordé.
- **Avec la télésurveillance et l'utilisateur, ensemble ou séparément :** il peut être utilisé uniquement avec Protegus 2 (sans télésurveillance), uniquement avec la télésurveillance, ou avec les deux. Si les deux sont configurés, l'événement est d'abord envoyé à la télésurveillance, puis à l'utilisateur.
- **Il a ses propres entrées et sorties.** Trois bornes I/O à double fonction peuvent servir d'entrée (détecteur, autoprotection) ou de sortie commandable (zone à clé, relais). Avec le module d'extension iO-8 raccordé au bus RS485, 8 I/O supplémentaires peuvent être ajoutées au système.
- **Pas d'abonnement.** L'E16T utilise la connexion Internet existante du site : ni carte SIM, ni abonnement mobile, ni antenne ne sont nécessaires, et la force du signal mobile ne compte pas.

La figure ci-dessous montre l'architecture du système : la sortie ligne téléphonique de la centrale d'alarme est raccordée à l'E16T, l'E16T accède à Internet par le routeur local, puis au récepteur du centre de télésurveillance et au cloud Protegus, et l'utilisateur voit le système dans l'application Protegus 2.

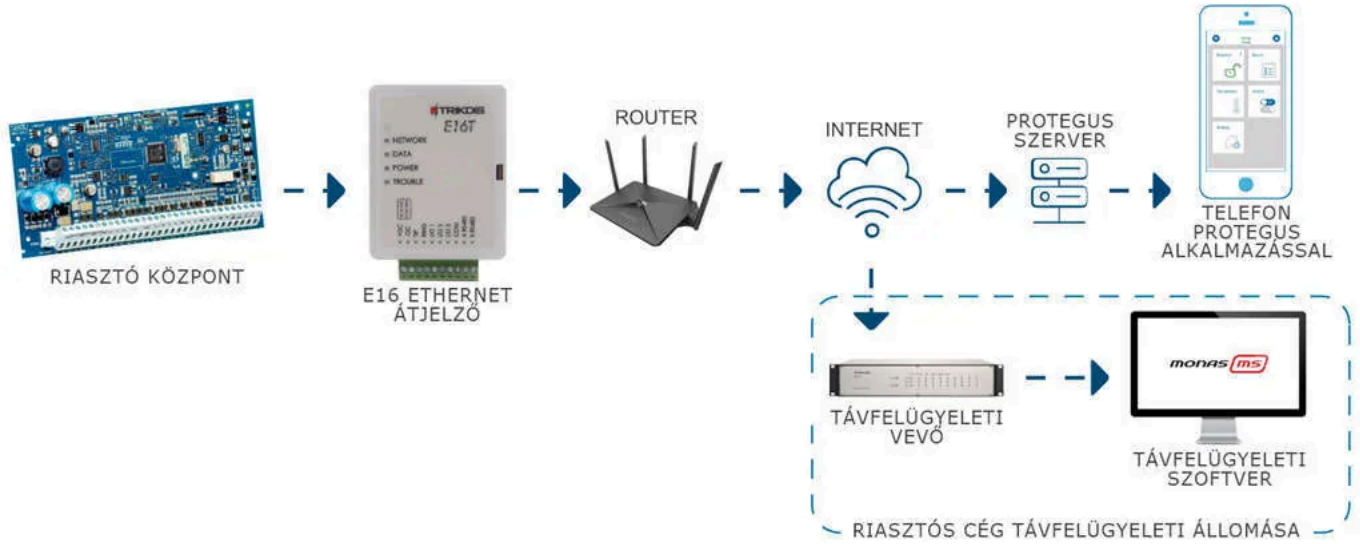


Figure 1. La place de l'E16T dans le système : centrale d'alarme → E16T → routeur → Internet → récepteur du centre de télésurveillance et cloud Protegus → application Protegus 2.

1.2 Versions

Ce manuel a été rédigé pour la **version matérielle actuelle de l'E16T, notée v2** (TrikdisConfig l'affiche sous le nom **E16T_2000**), mais il **s'applique aussi à l'E16T antérieur** : le raccordement, la configuration et le fonctionnement sont en grande partie identiques. Les différences sont résumées dans le tableau ci-dessous ; là où le texte indique une donnée de la v2, tenez compte de ce tableau pour la version antérieure.

	E16T antérieur	**E16T v2 (actuel)**
Entrées/sorties	2 entrées de type au choix (T-1/IN1, R-1/IN2 – NC, NO, EOL ; utilisables aussi pour la supervision de la ligne téléphonique) + 1 sortie à collecteur ouvert (OUT, max. 0,15 A, jusqu'à 30 V ; commandable depuis l'application Protegus)	3 bornes I/O à double fonction (I/O 1, I/O 2, I/O 3), chacune utilisable en entrée (types NC, NO, EOL, DEOL) ou en sortie à collecteur ouvert (max. 0,15 A)
Consommation	0,5 A au maximum	100 mA nominal, 250 mA au maximum pendant l'envoi
LED	NETWORK, DATA, POWER, TROUBLE, LINE (LINE est allumée en vert tant que la centrale a « décroché », c'est-à-dire compose ; les autres signalisations différentes des LED sont listées dans la remarque à la fin de la section 1.6)	NETWORK, DATA, POWER, TROUBLE
Mémoire tampon	100 messages	60 messages
Dimensions	88 × 62 × 25 mm	88 × 65 × 26 mm

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

1.3 Caractéristiques principales

Liaison avec la centrale d'alarme

- Raccordement normal à la sortie ligne téléphonique de la centrale : DC+, DC−, TIP et RING. Si nécessaire, il peut aussi être raccordé avec supervision de ligne (avec les fils T-1 et R-1) : la liaison entre la centrale et le communicateur est alors **supervisée**, le communicateur signale la coupure du câble.
- La centrale envoie les événements au format Contact ID, par numérotation DTMF ; l'E16T transmet l'information complète de l'événement (code, partition, zone ou utilisateur).

Communication avec le centre de télésurveillance

- Liaison IP avec les récepteurs Trikdis (récepteur logiciel IPcom, RL14, RM14) et les récepteurs universels (SIA DC-09, TL150).
- Canal principal, canal de secours et canal parallèle : il peut envoyer simultanément à deux récepteurs, chacun avec son propre canal de secours.
- Communication chiffrée, protégée par mot de passe ; mémoire tampon de 60 messages.

Fonctions utilisateur

- Application mobile et web Protegus 2 : notifications, liste des événements, armement et désarmement, commande des sorties.
- Droits utilisateur à plusieurs niveaux dans l'application (administrateur, installateur, utilisateur).

Installation et configuration

- Les paramètres peuvent être enregistrés dans un fichier et chargés dans un autre communicateur.
- Deux niveaux d'accès : administrateur et installateur – pour la configuration de l'appareil, destinés à l'administrateur du centre de télésurveillance et à l'installateur.
- Configuration et mise à jour à distance avec le logiciel TrikdisConfig.

1.4 Éléments du communicateur

Le circuit imprimé de l'E16T est logé dans un boîtier en plastique blanc ; la face avant est amovible et le bornier est débrochable. Le connecteur réseau (RJ45) se trouve sur le bord supérieur du circuit imprimé et est accessible par l'ouverture du boîtier.

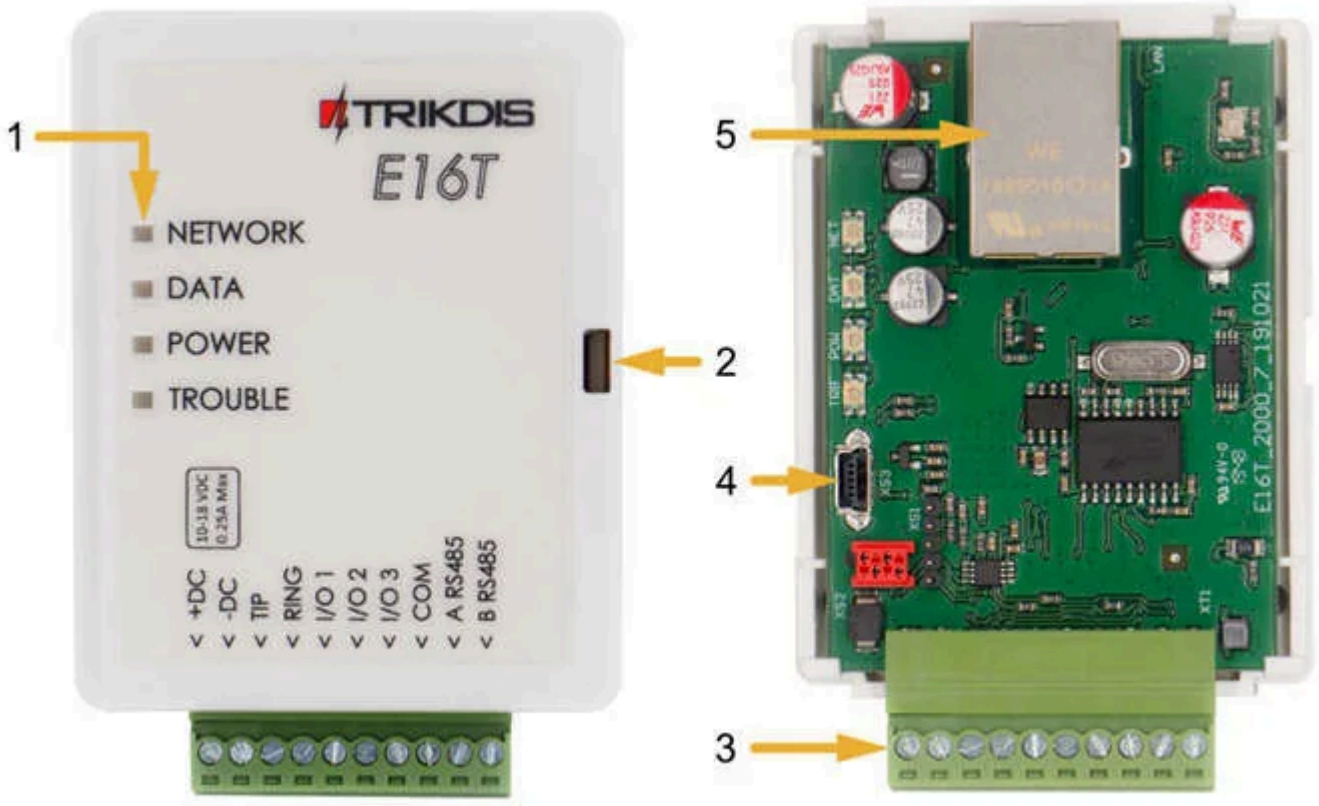


Figure 2. Les éléments de l'E16T, de face et boîtier ouvert.

- 1 Voyants LED (NETWORK, DATA, POWER, TROUBLE)
- 2 Ouverture facilitant le retrait de la face avant (sur le bord supérieur du couvercle)
- 3 Bornier débrochable
- 4 Prise USB Mini-B pour la programmation
- 5 Connecteur Ethernet (RJ45)

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

1.5 Bornes

Borne	Fonction
+DC	Alimentation, +10–18 V DC
–DC	Alimentation, négatif
TIP	Borne TIP de la centrale d'alarme
RING	Borne RING de la centrale d'alarme
I/O 1 (T-1)	Entrée/sortie 1, ou point T-1 de la supervision de la ligne téléphonique
I/O 2 (R-1)	Entrée/sortie 2, ou point R-1 de la supervision de la ligne téléphonique
I/O 3	Entrée/sortie 3
COM	Point commun (négatif) des entrées et sorties
A 485	Fil A du bus RS485 (iO-8 et autres modules d'extension de la série iO)
B 485	Fil B du bus RS485

Le marquage du bornier figure aussi sur la face avant : il n'est donc pas nécessaire de retirer le couvercle pour le câblage.

1.6 Signalisation des LED

Les LED de la face avant sont les outils les plus importants de la mise en service et du dépannage. Lisez-les ensemble : POWER indique l'alimentation, NETWORK la connexion réseau, DATA les messages en attente d'envoi et TROUBLE les défauts.

NETWORK – connexion réseau

Signal	Signification
éteinte	Pas de connexion réseau (pas de câble, port inactif, ou aucune adresse IP obtenue)
allumée en vert	Connecté au réseau local – la liaison fonctionne jusqu'au routeur. Pour savoir si Internet est aussi accessible, regardez la LED DATA (voir ci-dessous).

DATA – trafic de données

Signal	Signification
éteinte	Aucun message en attente d'envoi
allumée en vert	Des messages en attente d'envoi se trouvent dans la mémoire tampon
clignote en vert	Envoi ou réception de données en cours (pendant la programmation)

Vérification rapide

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

POWER – tension d'alimentation

Signal	Signification
éteinte	Pas d'alimentation, ou l'alimentation est coupée
allumée en vert	En marche, la tension d'alimentation est correcte
allumée en jaune	Tension d'alimentation insuffisante (11,5 V au maximum)
allumée en vert, clignote en jaune	Prêt pour la programmation (câble USB branché)
allumée en jaune (pendant la programmation)	Pas de liaison avec l'ordinateur

TROUBLE – défaut

Signal	Signification
éteinte	Aucun défaut
1 clignotement rouge	Pas de liaison physique avec le réseau (PHY link) : câble, connecteur ou port du routeur / switch
2 clignotements rouges	Erreur DHCP : l'appareil n'a pas obtenu d'adresse IP
3 clignotements rouges	Erreur DNS : la résolution de noms ne fonctionne pas
6 clignotements rouges	Pas de liaison avec le récepteur du centre de télésurveillance
7 clignotements rouges	Liaison avec la centrale d'alarme interrompue
clignote en rouge (pendant la programmation)	Erreur mémoire
allumée en rouge (pendant la programmation)	Firmware endommagé

E16T antérieur

Les LED de l'E16T antérieur signalent en partie autre chose : **DATA** est allumée en jaune si un événement en attente d'envoi se trouve dans la mémoire tampon, et clignote en vert pendant que la centrale d'alarme transmet un message au communicateur ; **POWER** clignote en vert si l'alimentation est en marche et la tension correcte, et clignote en jaune si la tension d'alimentation est insuffisante (11,5 V au maximum) ; une lumière rouge fixe de **TROUBLE** signale un défaut de connexion réseau (LAN), éteinte il n'y a aucun défaut ; **LINE** est allumée en vert tant que la centrale a « décroché » (section 1.2).

1.7 Caractéristiques techniques

Paramètre	Valeur
Liaison avec la centrale d'alarme	ligne téléphonique filaire (TIP/RING), Contact ID, DTMF
Entrées/sorties	3 I/O à double fonction (I/O 1, I/O 2, I/O 3) : en entrée NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (résistance de fin de ligne 2,2 kΩ) ; en sortie à collecteur ouvert (OC), max. 0,15 A / 30 V DC
Extension	sur le bus RS485 : module d'extension iO-8 (+8 I/O) et autres modules de la série iO, 4 modules au maximum
Raccordement réseau	Ethernet, IEEE 802.3, 10Base-T, prise RJ45
Configuration réseau	DHCP (usine) ou adresse IP fixe
Tension d'alimentation	10–18 V DC
Consommation	100 mA nominal ; 250 mA au maximum pendant l'envoi
Protocoles de transmission	TRK, DC-09_2007, DC-09_2012, TL150
Mémoire tampon	60 messages
Programmation	TrikdisConfig (Windows) par câble USB Mini-B ou à distance
Environnement de fonctionnement	−10 … +50 °C, humidité relative max. 80 % (à +20 °C)
Dimensions	88 × 65 × 26 mm

Paramètre	Valeur
Poids	80 g

2. Mise en service rapide avec TrikdisConfig

Tous les paramètres de l'E16T se règlent avec le programme Windows **TrikdisConfig** – par câble USB ou à distance. Ce chapitre décrit le chemin le plus court : vous configurez l'appareil sur la table, avant le câblage, puis sur le site il ne reste plus qu'à le raccorder. L'explication détaillée des paramètres se trouve au chapitre 6.

2.1 Préparatifs

Ce dont vous aurez besoin

Câble USB Mini-B (pour la configuration) · câble d'au moins 4 conducteurs jusqu'à la centrale · tournevis plat de 2,5 mm · câble Ethernet (CAT-5 ou supérieur, 100 m au maximum) jusqu'au routeur ou au switch · un port réseau libre · s'il n'y a pas de DHCP sur le réseau : l'adresse IP fixe, le masque, la passerelle et le DNS fournis par l'administrateur réseau · le manuel d'installation de la centrale d'alarme. Ce qui manque peut être commandé séparément auprès du distributeur local.

1. Téléchargez et installez le logiciel TrikdisConfig. Sur le site de Trikdis (www.trikdis.com), saisissez « TrikdisConfig » dans le champ de recherche.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Ouvrez la face avant de l'E16T et reliez-le à l'ordinateur. Insérez un tournevis plat dans l'ouverture située sur le bord supérieur du couvercle et, en faisant levier vers le bas, déclipsez délicatement la face avant, puis branchez le câble USB Mini-B. L'USB fournit suffisamment d'alimentation pour la programmation, aucune alimentation séparée n'est nécessaire.

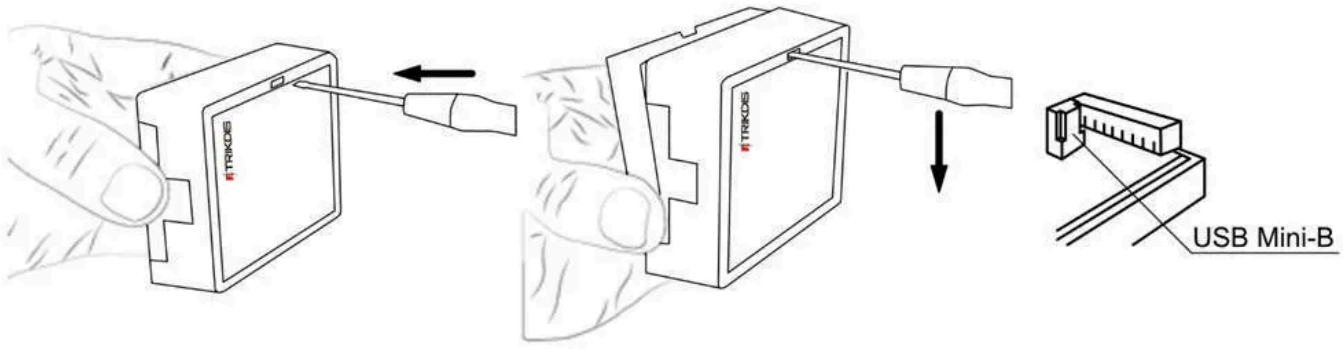


Figure 3. Déclipsage de la face avant et liaison avec l'ordinateur par câble USB Mini-B.

Avertissement

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

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

Les deux sections suivantes décrivent ce qu'il faut configurer pour que la centrale d'alarme puisse être commandée depuis l'application Protegus 2 (2.2) et pour que le communicateur envoie les événements au centre de télésurveillance (2.3).

2.2 Liaison avec l'application Protegus 2

Si l'utilisateur souhaite voir et commander le système depuis l'application Protegus 2, configurez ce qui suit sur la page **User reporting**, onglet **PROTEGUS Cloud**.



Figure 4. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

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

Vérifiez ensuite le type d'interface de la centrale d'alarme sur la page **System settings**.

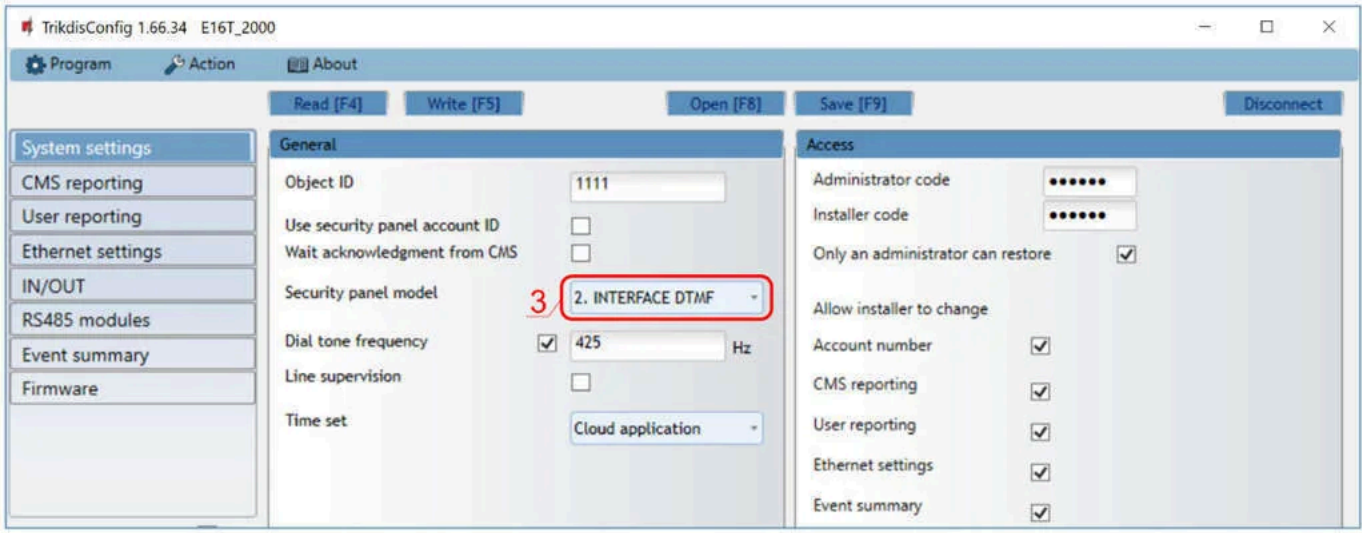


Figure 5. TrikdisConfig – page System settings, groupe General.

- 3 **Security panel model** – laissez **2. INTERFACE DTMF** (liaison par ligne téléphonique, avec numérotation DTMF).

Pour les paramètres réseau, la case **Use DHCP** est cochée en usine sur la page **Ethernet settings** : l'appareil obtient automatiquement une adresse IP du routeur et, dans la plupart des cas, il n'y a rien d'autre à faire. S'il n'y a pas de DHCP sur le réseau, ou s'il faut utiliser une adresse fixe, saisissez ici les paramètres manuels (section 6.5).

Si vous utilisez l'appareil uniquement avec Protegus 2, sans télésurveillance, la configuration est terminée : appuyez sur le bouton **Write [F5]** (écriture), attendez la confirmation et débranchez le câble USB.

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

2.3 Liaison avec le centre de télésurveillance

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

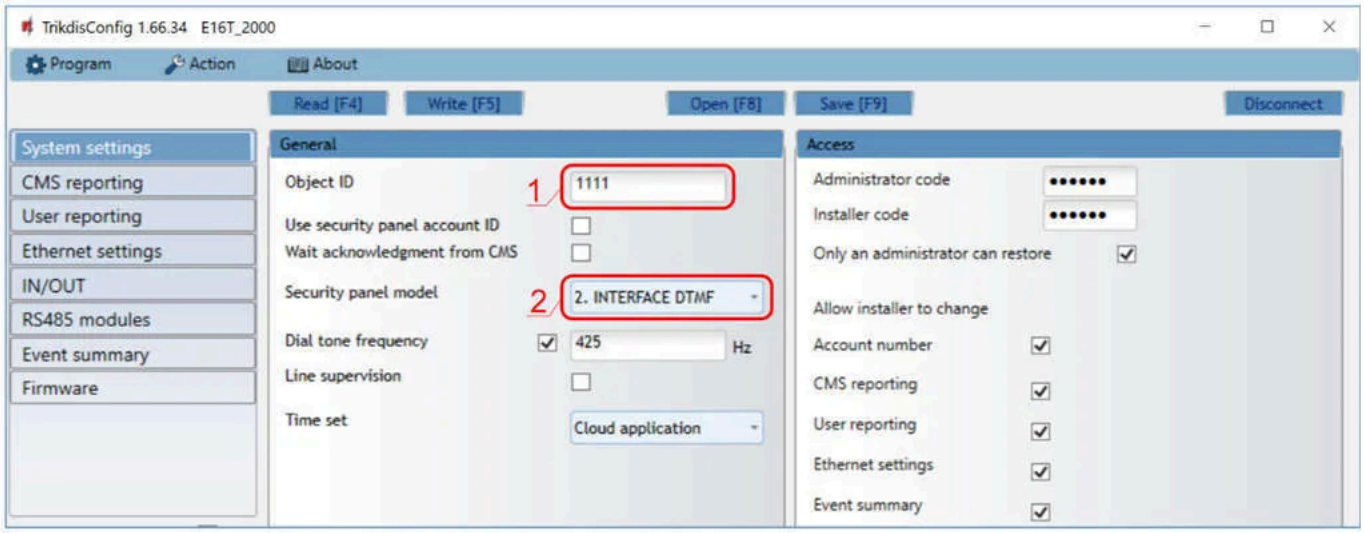


Figure 6. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne sont pas utilisables.
- 2 **Security panel model** – laissez **2. INTERFACE DTMF**.

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

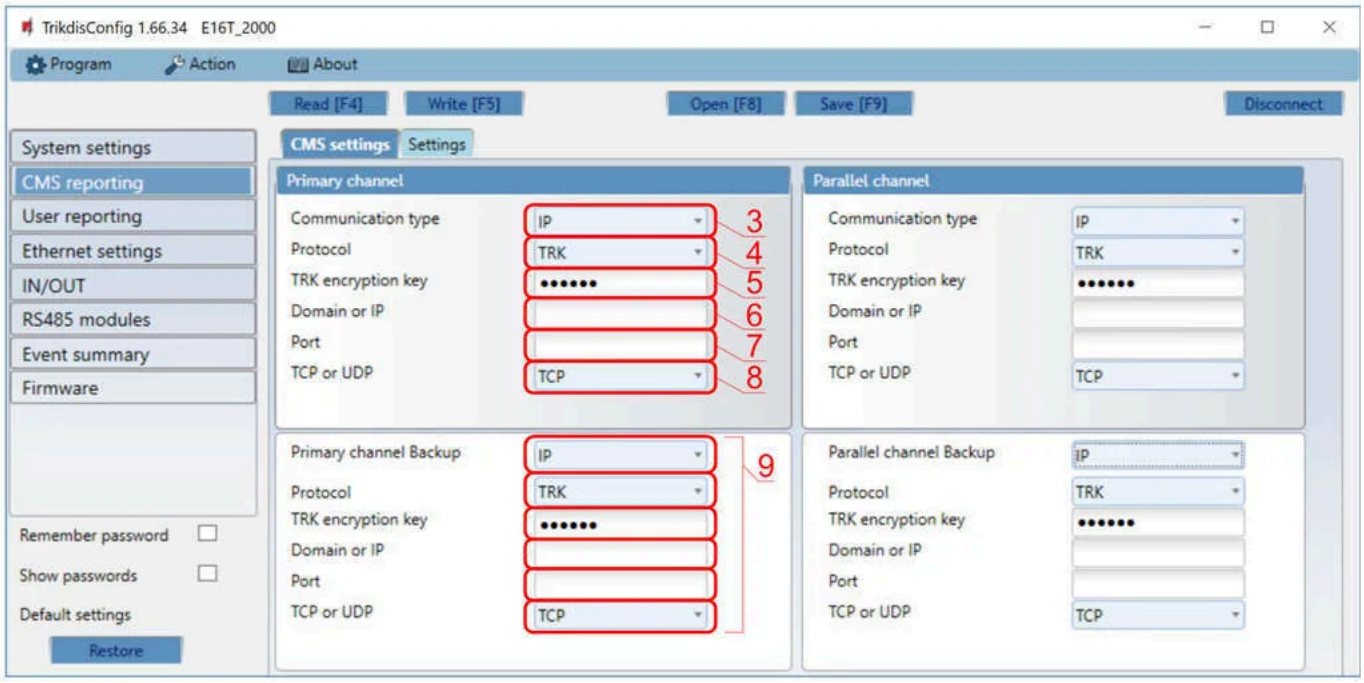


Figure 7. TrikdisConfig – CMS reporting, onglet CMS settings.

- 3 **Communication type** – **IP** (seul choix possible sur l'E16T).
- 4 **Protocol** – **TRK** pour un récepteur Trikdis, **DC-09_2007** ou **DC-09_2012** pour un récepteur universel, **TL150** pour un récepteur SUR-GARD.
- 5 **TRK encryption key** – la clé de chiffrement à 6 chiffres configurée dans le récepteur.
- 6 **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- 7 **Port** – le numéro de port du récepteur.
- 8 **TCP or UDP** – le protocole de transport ; il s'aligne sur la configuration du récepteur.
- 9 **Primary channel Backup** – canal de secours en cas de défaut du canal principal ; remplissez-le de la même façon, il est conseillé de le renseigner.

Avec le protocole **DC-09**, saisissez aussi sur l'onglet **Settings** les numéros d'objet, de ligne et de récepteur DC-09 (section 6.3) ; avec DC-09_2012, le chiffrement peut aussi être activé avec la clé DC-09 configurée dans le récepteur (remarque de la section 6.3). Pour la vérification de la liaison, l'intervalle du signal de vie (PING) se règle sur ce même onglet **Settings** (**IP ping period**, 30 s en usine). Si vous avez saisi le récepteur par son nom de domaine, la résolution de noms nécessite aussi le paramètre DNS de la page **Ethernet settings** (le DNS public de Google y est configuré en usine). Sur l'E16T antérieur, les champs portent d'autres noms (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**) ; la correspondance figure dans la remarque de la section 6.3.

Si l'utilisateur utilise aussi l'application Protegus 2, effectuez également les réglages de la section 2.2 (**User reporting** → **PROTEGUS Cloud**). À la fin de la configuration, appuyez sur le bouton **Write [F5]** (écriture), attendez la confirmation et débranchez le câble USB. L'appareil est alors prêt à être raccordé.

3. Installation et raccordement

Figyelem!

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

3.1 Étapes de l'installation

1. Retirez la face avant (voir la section 2.1) et débrochez le bornier.
2. Sortez le circuit imprimé du fond du boîtier : ouvrez le loquet situé dans le coin.
3. Fixez le fond du boîtier avec des vis à l'emplacement choisi.
4. Remettez le circuit imprimé dans le fond du boîtier et rebranchez le bornier.
5. Branchez le câble Ethernet dans la prise RJ45 (section 3.6).
6. Remettez la face avant.

3.2 Emplacement et réseau

- Placez le communicateur dans un endroit **sec, à l'intérieur**, de préférence près du coffret de la centrale d'alarme, afin que le câblage reste court. Un coffret métallique ne le gêne pas : l'E16T n'a pas d'antenne.
- Le câble Ethernet (CAT-5 ou supérieur) jusqu'au routeur ou au switch peut mesurer **100 m au maximum**.
- Tenez le communicateur et les câbles éloignés du transformateur de la centrale et des câbles secteur.

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.

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

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

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

Coupure de courant

L'E16T est alimenté par la centrale d'alarme ; lors d'une coupure de courant, il continue donc de fonctionner sur la batterie de la centrale – en revanche, le routeur et le modem s'arrêtent généralement, et sans eux il n'y a pas d'Internet. Si ce n'est pas acceptable pour le système, alimentez aussi les équipements réseau par une alimentation sans interruption (onduleur), ou choisissez un communicateur cellulaire (G16T).

3.3 Raccordement à la centrale d'alarme

L'E16T se raccorde à la sortie ligne téléphonique (TIP/RING) de la centrale, et reçoit son alimentation de la sortie d'alimentation auxiliaire 12 V (AUX) de la centrale.

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

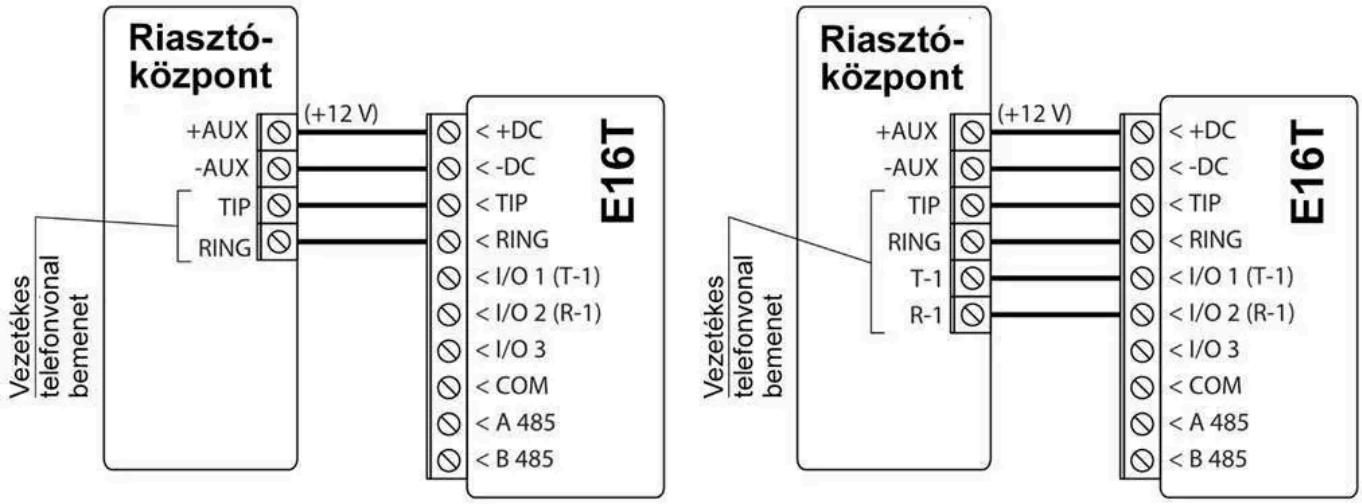


Figure 8. Raccordement à la sortie ligne téléphonique de la centrale : à gauche le raccordement normal, à droite le raccordement avec supervision de ligne.

Pendant l'envoi, l'E16T consomme 250 mA au maximum. Vérifiez que la sortie AUX de la centrale le supporte, avec les autres appareils qui y sont raccordés. Comme l'alimentation est fournie par la centrale, en cas de coupure de courant la batterie de la centrale alimente aussi le communicateur.

3.3.1 Si nécessaire : supervision de ligne

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

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

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

3.4 Raccordement d'une zone à clé

Si vous souhaitez armer et désarmer la centrale à distance, depuis l'application Protegus 2, configurez l'une des bornes I/O du communicateur **en sortie** et raccordez-la à une **zone à clé** de la centrale. Lorsqu'elle est activée, la sortie tire la zone vers COM (le négatif) ; raccordez la résistance de fin de ligne de la zone selon le type de zone de la centrale. Comme l'E16T dispose de trois bornes I/O, jusqu'à trois partitions peuvent être gérées, chacune avec sa propre sortie.

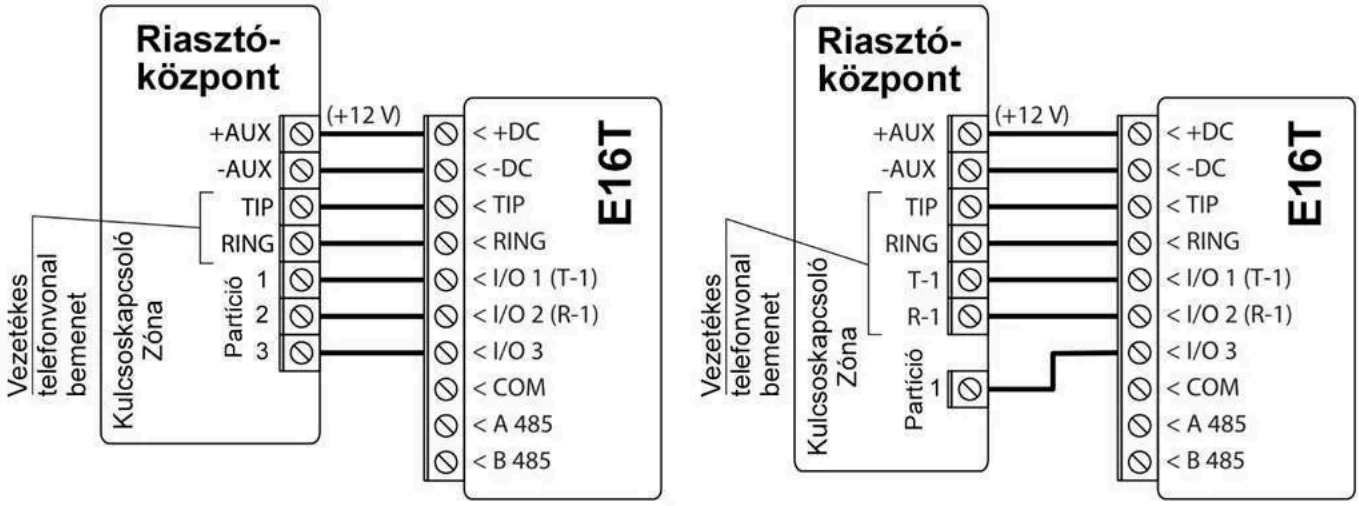


Figure 9. Armement et désarmement par zone à clé : à gauche le raccordement normal, à droite le raccordement avec supervision de ligne (dans ce cas, I/O 3 reste disponible pour la zone à clé).

La zone à clé peut être à impulsion ou à deux états – le même mode doit être configuré dans l'application Protegus 2 (section 5.2). Un article séparé traite des détails et des pièges de l'armement par zone à clé : Armement à distance par zone à clé depuis l'application Protegus 2.

E16T antérieur

Sur l'E16T antérieur (2 entrées + OUT), le type et le mode de la sortie se configurent dans le groupe **System settings** → **Output** de TrikdisConfig : pour l'armement par zone à clé, **OUT type** doit être **Remote Control** et **OUT mode** doit être **Pulse** (avec durée d'impulsion) ou **Level** – selon le type de zone de la centrale.

3.5 Raccordement des entrées

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

Les entrées acceptent les types de circuit suivants : **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La résistance de fin de ligne est de **2,2 kΩ**. Avec une simple fin de ligne (EOL), le court-circuit comme la coupure comptent comme une alarme ; la double fin de ligne (DEOL), avec deux résistances, distingue l'alarme et l'autoprotection (court-circuit ou coupure). Le réglage d'usine est NO (normalement ouvert) ; le type d'entrée se règle sur la page **IN/OUT** de TrikdisConfig, selon le câblage.

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

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

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

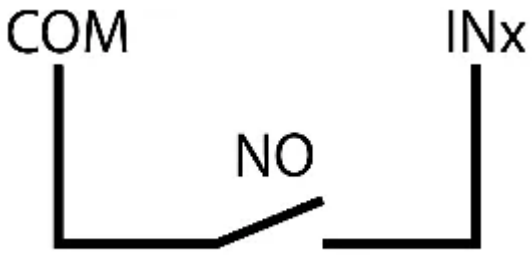


Figure 10. NO – circuit ouvert au repos : fermé – alarme, ouvert – état de repos.

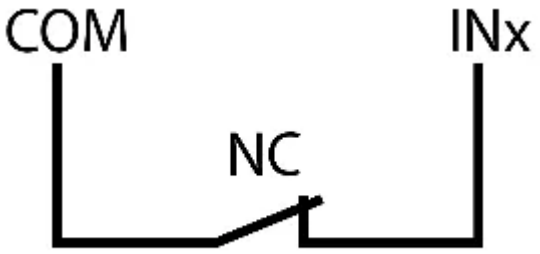


Figure 11. NC – circuit fermé au repos : ouvert – alarme, fermé – état de repos.

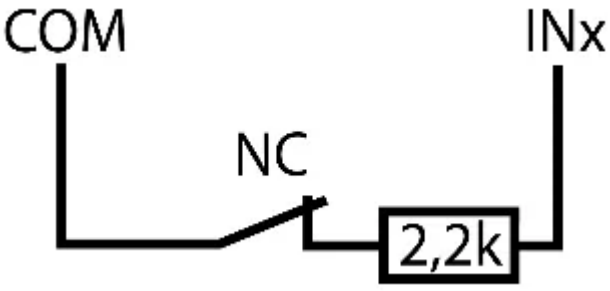


Figure 12. NC/EOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

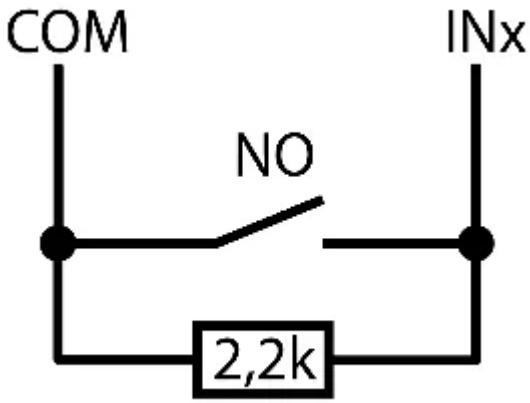


Figure 13. NO/EOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

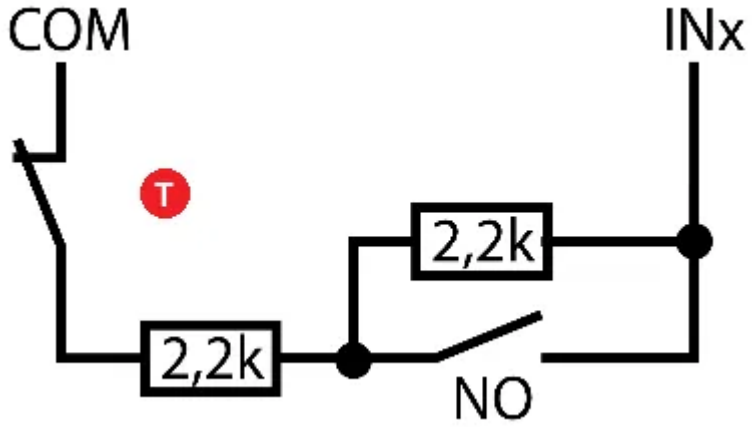


Figure 14. NO/DEOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

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

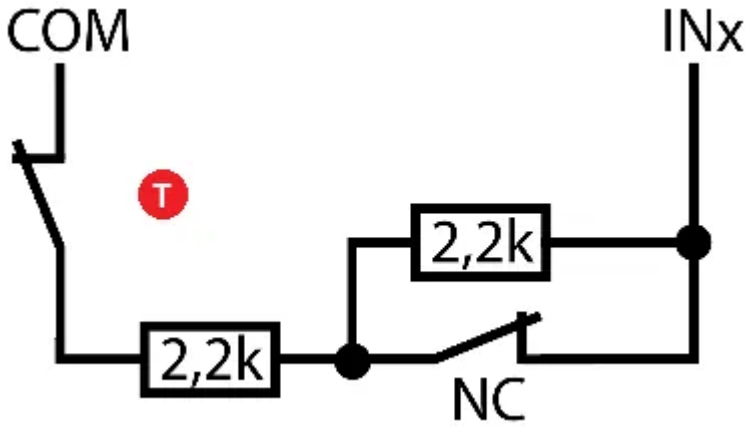


Figure 15. NC/DEOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

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

E16T antérieur

Les deux entrées (IN1, IN2) de l'E16T antérieur (2 entrées + OUT) acceptent un circuit de type NO, NC ou EOL ; le réglage d'usine est NO. Sur cette version, le type d'entrée ne se règle pas sur la page IN/OUT, mais sur la page **Event summary** de TrikdisConfig (remarque de la section 6.6). Le raccordement est le même : raccordez l'entrée selon le type choisi (NO, NC, EOL).

3.6 Raccordement du câble Ethernet

Branchez une extrémité du câble Ethernet dans la prise RJ45 du circuit imprimé de l'E16T, et l'autre dans un port libre du routeur ou du switch. Il faut un câble classique droit (patch) ; le câble entre par l'ouverture supérieure du boîtier. Après la mise sous tension, l'établissement de la connexion réseau est signalé par la lumière verte de la LED **NETWORK**.

3.7 Raccordement d'une sortie avec relais

En sortie, les bornes I/O sont des sorties à collecteur ouvert (OC) : à l'état actif, elles tirent la charge raccordée vers le négatif, avec 0,15 A au maximum, jusqu'à 30 V DC. Commutez un consommateur plus important ou un appareil sur tension secteur **par l'intermédiaire d'un relais** : une extrémité de la bobine du relais va sur +DC, l'autre sur la borne I/O. Une LED témoin peut aussi être raccordée directement à la sortie : depuis +DC, par une résistance série de 2,2 kΩ, vers la LED, et l'autre patte de la LED sur la borne I/O (sur l'E16T antérieur, sur la borne OUT).

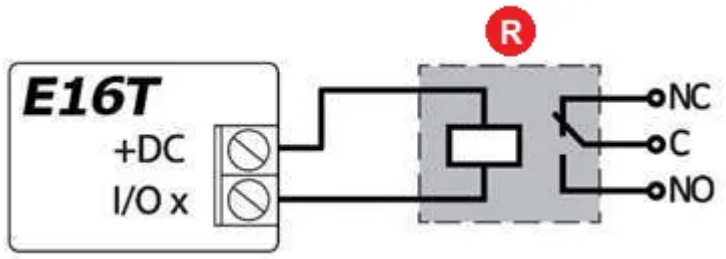


Figure 16. Raccordement d'un relais à la sortie du communicateur : la bobine se place entre +DC et la borne I/O x, les contacts (NC, C, NO) commutent le consommateur.

- R relais (« Relay »)

Vous pouvez commander les sorties depuis l'application Protegus 2 (chapitre 5).

3.8 Raccordement du module d'extension iO-8

Si davantage d'entrées ou de sorties sont nécessaires, jusqu'à quatre modules d'extension **iO-8** peuvent être raccordés au bus RS485 de l'E16T ; chacun ajoute 8 I/O à double fonction. Reliez les bornes A 485 et B 485 aux bornes A et B du module, et prenez l'alimentation du module sur le 12 V de la centrale. Le bus RS485 peut mesurer 100 m au maximum – c'est un maximum théorique, voir la remarque de la section 3.2. Le module doit être ajouté sur la page **RS485 modules** de TrikdisConfig (section 6.7). Les autres membres de la série iO (iO, iO-WL, iO-LO, LO-MOD) peuvent aussi être raccordés ici ; les modules W485 et E485 ne sont pas destinés à l'E16T, puisque l'E16T est lui-même un appareil à Internet filaire.

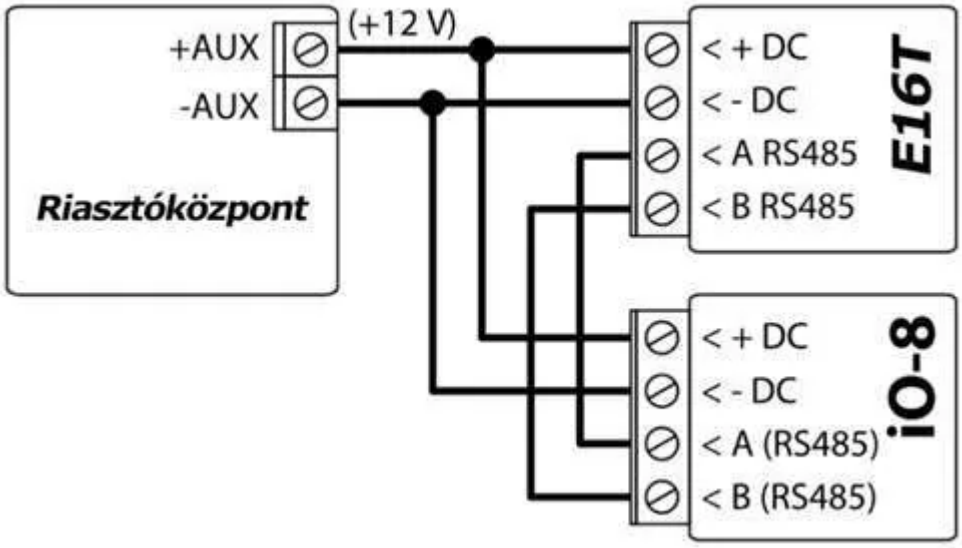


Figure 17. Raccordement du module d'extension iO-8 au bus RS485 de l'E16T ; alimentation depuis la sortie AUX de la centrale d'alarme.

3.9 Mise sous tension et premier contrôle

A TRIKDIS átjelző elindítása

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

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

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

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

- **POWER** allumée en vert – l'alimentation est correcte ;
- **NETWORK** allumée en vert – connecté au réseau local ;
- **TROUBLE** éteinte.

Si TROUBLE clignote, le nombre de clignotements indique la cause (section 1.6) : 1 = pas de liaison physique (câble, port), 2 = aucune adresse IP obtenue (DHCP), 3 = erreur DNS, 6 = le récepteur est injoignable. Si aucune LED ne s'allume, vérifiez l'alimentation et le câblage.

4. Programmation de la centrale d'alarme

Pour que la centrale d'alarme envoie les événements sur sa sortie ligne téléphonique, son transmetteur téléphonique doit être activé et réglé. Les adresses de programmation exactes figurent dans le manuel d'installation de la centrale ; le principe du réglage est le même chez tous les fabricants :

1. **Activez le transmetteur téléphonique (RTC)** dans la centrale.
2. **Saisissez `1234` comme numéro de téléphone** du récepteur de télésurveillance – que le communicateur soit raccordé aux bornes RING/TIP de la centrale ou à la ligne téléphonique. Avec un autre numéro, il arrive que la centrale compose le numéro mais que le communicateur ne reçoive pas les événements : sur une centrale DSC PowerSeries NEO également, la transmission n'a démarré qu'après la modification du numéro en `1234`.
3. **Mode de numérotation :** DTMF (tone), pas à impulsions.
4. **Protocole :** Contact ID.

Si vous souhaitez armer et désarmer la centrale à distance via la sortie du communicateur, la zone raccordée à cette sortie doit être paramétrée dans la centrale comme **zone à clé**.

La zone à clé peut être à impulsion ou à deux états (maintenue). Par défaut, la sortie du communicateur délivre une impulsion de 3 secondes ; vous pouvez modifier la durée de l'impulsion ou passer en mode à deux états dans les réglages de l'application Protegus 2.

4.1 Programmation du transmetteur Honeywell Vista

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

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

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

Adresse	Valeur	Adresse	Valeur	Adresse	Valeur
`*41`	1234 (numéro de téléphone du récepteur)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (numéro d'abonné)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

À la fin de la programmation, quittez le mode programmation avec la commande `*99`.

4.2 Centrales d'autres fabricants

Dans le manuel d'installation de chaque centrale, cherchez les quatre mêmes réglages : l'activation du transmetteur téléphonique, le numéro de téléphone du récepteur, le mode de numérotation (DTMF) et le format de communication (Contact ID). Si la centrale attend une tonalité (dial tone) avant de composer, c'est l'E16T qui la fournit ; si l'appel ne démarre toujours pas, désactivez la détection de tonalité dans la centrale (option « numérotation sans tonalité » ou similaire).

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

5. Commande à distance avec l'application Protegus 2

Avec l'application mobile et web Protegus 2, l'utilisateur voit à distance l'état du système, reçoit des notifications sur les événements, peut armer et désarmer, et commander les sorties du communicateur.

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez :

1. L'E16T est connecté au réseau et accède à Internet : la LED **NETWORK** est allumée en vert, et la LED **DATA** s'éteint après un événement ou un rapport de test.
2. Sur la page **User reporting** → **PROTEGUS Cloud** de TrikdisConfig (section 6.4), **Enable connection** est coché – le cloud Protegus est donc autorisé –, et le **Protegus Cloud access code** est défini (il ne peut plus être modifié une fois le système créé).
3. La LED **POWER** est allumée en vert.

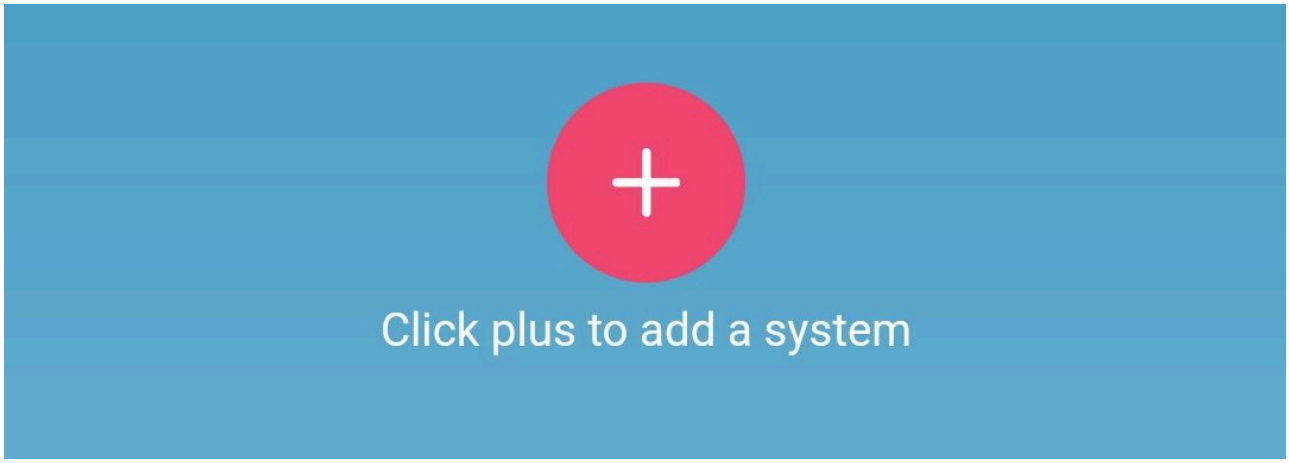
La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur 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



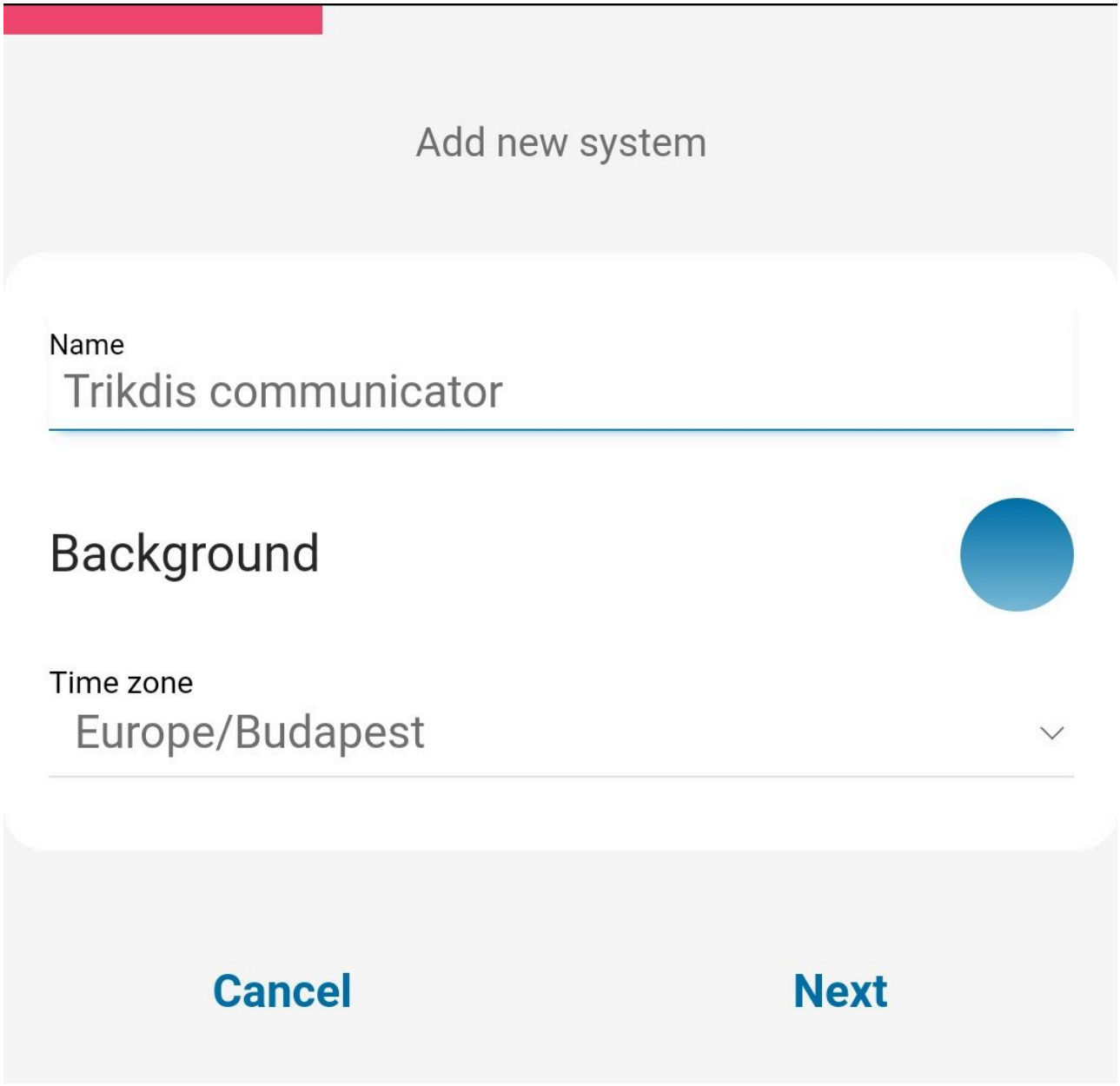
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



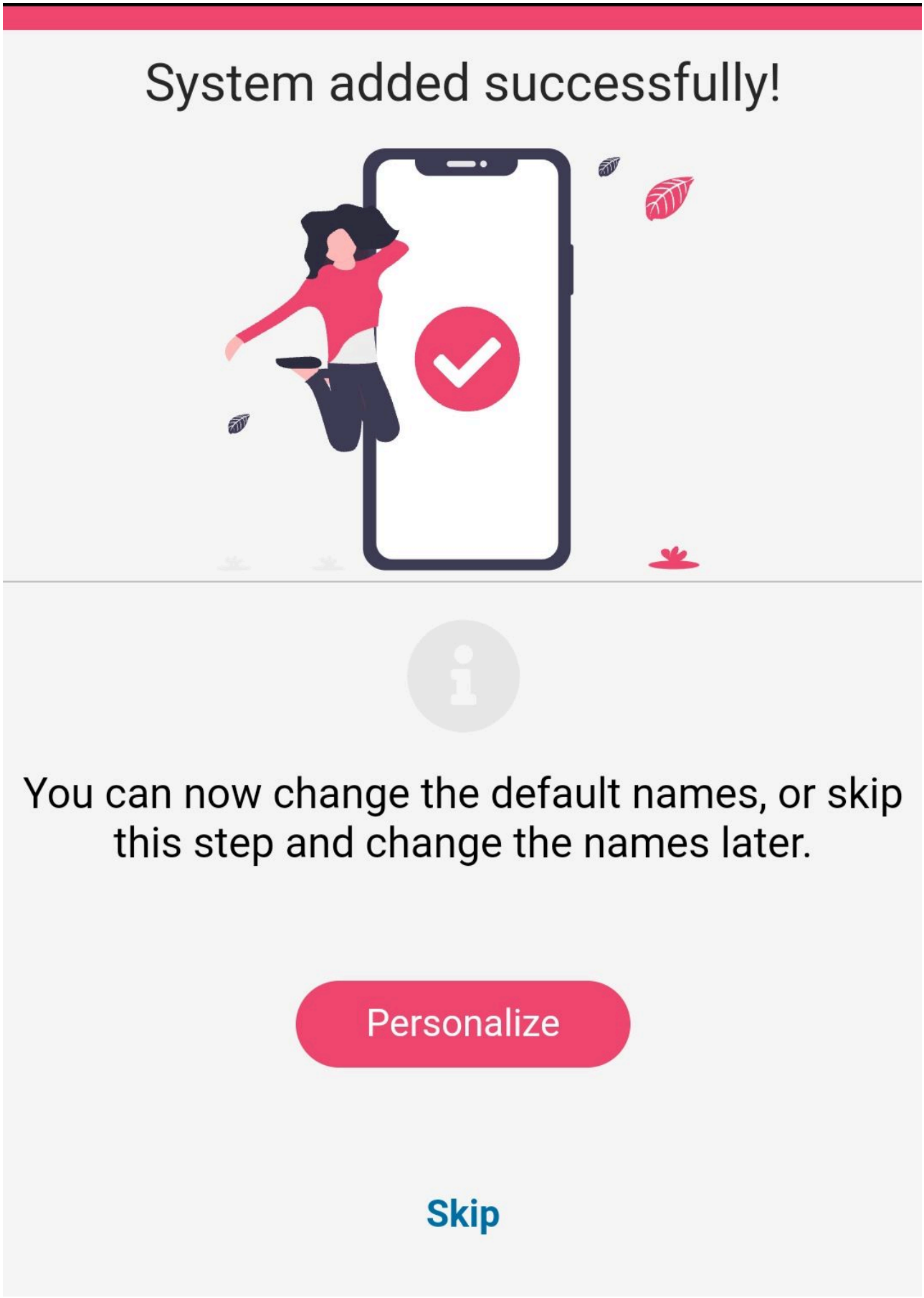
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



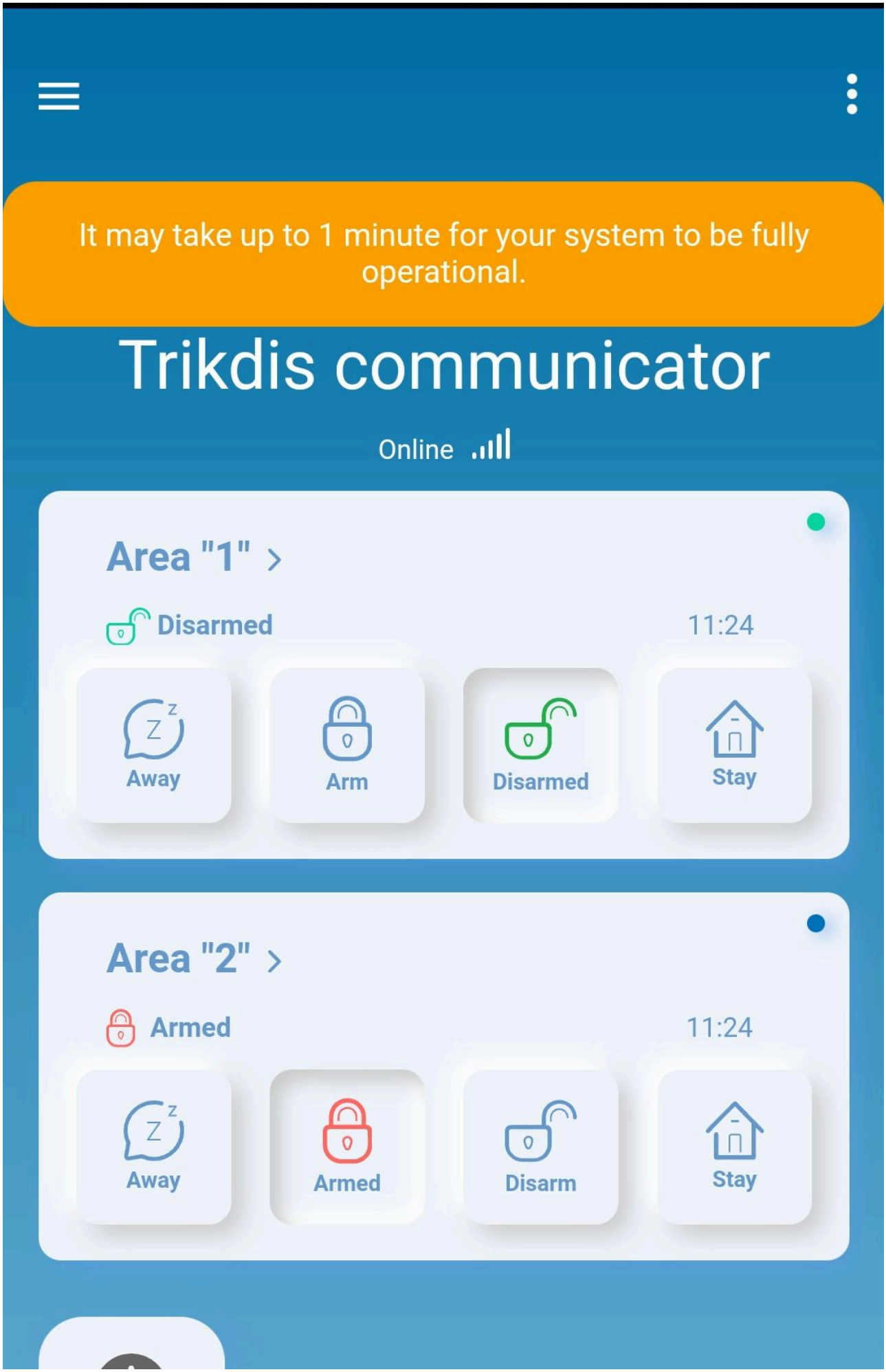
6. Add meg a rendszer nevét és válassz idozónát



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



Sur l'E16T, l'identifiant unique de l'appareil est l'**adresse MAC** : elle figure sur la boîte et au dos de l'appareil, et TrikdisConfig l'affiche aussi (**MAC / Unique ID**).

5.2 Armement et désarmement par une sortie

Si vous souhaitez armer et désarmer la centrale d'alarme via la sortie du communicateur, par l'intermédiaire de la zone à clé de la centrale, indiquez dans l'application Protegus 2, au niveau de la partition, quelle sortie la commande.

La zone de la centrale à laquelle la sortie du communicateur est raccordée doit être programmée dans la centrale comme **zone à clé**, et la centrale doit transmettre les événements d'armement et de désarmement – c'est à partir de ceux-ci que Protegus 2 affiche l'état de la partition.

Le réglage peut se faire lors de la création du système, à l'ajout des partitions, ou ultérieurement dans les réglages du système, en modifiant la partition. Lors de la création du système, l'assistant de Protegus 2 vous guide : cliquez sur le bouton **Continue** (Continuer), saisissez le nom de la partition (**Area name**) et autorisez la commande de la sortie PGM depuis l'application Protegus 2 – cela se fait selon les étapes ci-dessous :

1. Sélectionnez (ou ajoutez) la partition que vous souhaitez commander. Le numéro de partition doit correspondre à celui que la centrale envoie dans les événements (partition 1 = 1, partition 2 = 2).
2. Activez l'option **Commande par PGM** (Control with Protegus2) et, dans le champ **sortie** (Assigned Output), choisissez la sortie du communicateur (PGM1, PGM2 …). Une sortie ne peut commander qu'une seule partition.
3. Choisissez le mode de fonctionnement : **impulsion** (Pulse) ou **deux états** (Level) – le même que celui réglé dans la centrale pour la zone à clé. On utilise généralement le mode impulsion ; la durée de l'impulsion peut aussi être définie (par défaut 3 s).
4. Enregistrez le réglage (**Save**). S'il y a plusieurs partitions, répétez l'opération pour chacune, avec sa propre sortie : dans l'assistant, vous ajoutez une autre partition avec le bouton **Click to add an area** et réglez sa sortie PGM de la même manière. Une fois toutes les partitions réglées, passez à la suite dans l'assistant avec le bouton **Skip**.

Protegus 2 ne peut afficher correctement l'état des partitions que si la centrale envoie les événements d'armement et de désarmement avec le bon numéro de partition. Les détails et les pièges de l'armement par zone à clé font l'objet d'un article séparé : Armement à distance par zone à clé depuis l'application Protegus 2.

5.3 Armement et désarmement depuis l'application

1. Ouvrez le système dans l'application Protegus 2. Sur l'écran d'accueil, chaque partition a sa propre carte et son cadenas : un **cadenas fermé rouge** indique une partition armée, un **cadenas ouvert vert** une partition désarmée.
2. Touchez le cadenas de la partition et choisissez l'opération souhaitée : armement ou désarmement (mise hors service).
3. Si l'application le demande, saisissez le code PIN.

Le cadenas prend l'état réel à la suite de l'événement reçu de la centrale d'alarme ; l'application confirme également dans la liste des événements et par une notification si la centrale a exécuté l'opération.

6. TrikdisConfig – les paramètres en détail

Dans la fenêtre de TrikdisConfig, la liste des pages se trouve à gauche (System settings, CMS reporting, User reporting, Ethernet settings, IN/OUT, RS485 modules, Event summary, Firmware), la barre de boutons en haut (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) et la barre d'état en bas. Ce chapitre passe en revue les paramètres de l'E16T, page par page.

6.1 La barre d'état

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

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

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



Figure 18. La barre d'état de TrikdisConfig avec un E16T lu : à gauche, le bouton de rétablissement des réglages d'usine et la MAC / Unique ID ; en bas, l'état, le type, le numéro de série, les versions, le mode de connexion et le niveau d'accès.

Après **Read [F4]**, le programme lit et affiche les paramètres présents dans l'appareil ; le champ **Device** doit indiquer le type de l'appareil (E16T ; pour la v2, **E16T_2000**). Effectuez les réglages selon les descriptions des pages ci-dessous.

6.2 System settings

La page comporte deux groupes : dans le groupe **General**, vous réglez le fonctionnement de base de l'appareil, dans le groupe **Access**, les niveaux d'accès.

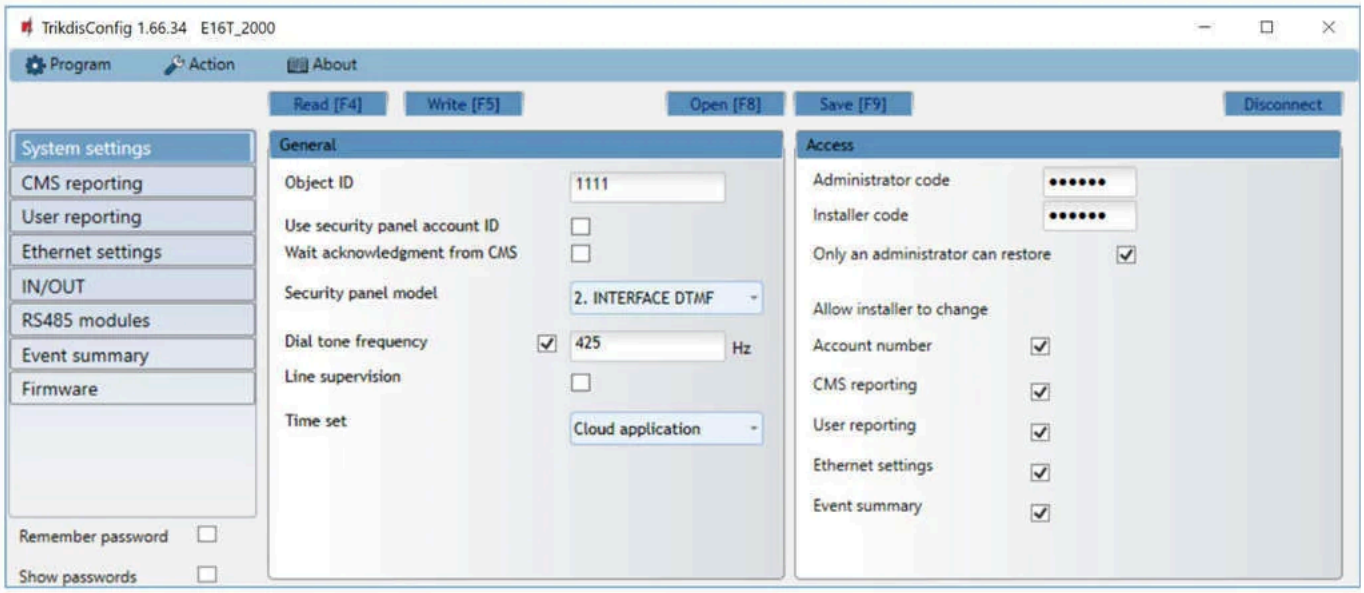


Figure 19. TrikdisConfig – page System settings : groupes General et Access.

- **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux : 0–9, A–F ; `FFFE` et `FFFF` ne peuvent pas être utilisés). Obligatoire si l'appareil transmet aussi à un centre de télésurveillance.
- **Use security panel account ID** – coché, le communicateur n'utilise pas son propre Object ID, mais l'identifiant envoyé par la centrale dans le message Contact ID. Utile si plusieurs partitions transmettent chacune avec leur propre identifiant.
- **Wait acknowledgment from CMS** – coché, le communicateur attend après chaque événement l'acquittement du récepteur, et n'envoie qu'ensuite le signal de fin (kiss-off) à la centrale. Sans acquittement, la centrale renvoie l'événement. Dans un système sans télésurveillance, uniquement avec Protegus 2, laissez-le désactivé (état d'usine).
- **Security panel model** – le type de l'interface ligne téléphonique ; par défaut **2. INTERFACE DTMF**. C'est avec lui que vous activez ou désactivez l'interface ligne téléphonique DTMF du communicateur.
- **Dial tone frequency** – la fréquence de la tonalité que l'E16T fournit à la centrale (par défaut 425 Hz, la tonalité standard dans la plupart des pays européens).
- **Line supervision** – supervision du câble entre la centrale et le communicateur ; nécessite aussi le raccordement des fils T-1 et R-1 (section 3.3.1).
- **Time set** – la source de l'horloge de l'appareil (par défaut **Cloud application**, le cloud Protegus).

E16T antérieur

Sur l'E16T antérieur, la page System settings comporte d'autres groupes :

- **General** → **Test period** – le rapport de test périodique est envoyé à l'intervalle indiqué ici (sur la v2, il se trouve sur l'onglet **CMS reporting** → **Settings**).
- Groupe **Ethernet settings** (sur la v2, page séparée, section 6.5) : **Internal MAC** – l'identifiant unique de l'appareil, l'adresse MAC ; **Use DHCP** – coché, l'appareil s'enregistre automatiquement sur le réseau ; si l'enregistrement automatique échoue, remplissez manuellement les champs **Internal IP address**, **Mask** (masque de sous-réseau), **Gateway** (passerelle) et **DNS**.

- Groupe **Output** (sur la v2, page IN/OUT, section 6.6) : **OUT type** – le fonctionnement de la sortie, à choisir dans la liste : Disabled (désactivée), LAN OK (le réseau est en ordre), Communication Trouble (défaut de communication), Remote Control (commande à distance depuis l'application Protegus) ; **Inverted** – cochée, la sortie fonctionne à l'inverse ; **OUT mode** : **Pulse** – la sortie reste dans le nouvel état pendant la durée (en secondes) indiquée dans le champ **Pulse Time**, **Level** – l'état est maintenu jusqu'à la commande suivante ; **Pulse time** – la durée de l'impulsion en secondes ; en mode Pulse, la sortie commute pour cette durée.

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

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

- **Administrator code** – accès à tous les réglages (mot de passe d'usine : `123456` ; le mot de passe comporte 6 caractères : chiffres ou lettres latines).
- **Installer code** – accès pouvant être restreint (mot de passe d'usine : `654321`).
- **Only an administrator can restore** – case cochée, seul l'administrateur peut lancer la restauration des réglages d'usine.
- **Allow installer to change** – vous sélectionnez ici les groupes de réglages que l'installateur peut modifier : **Account number** (numéro d'abonné), **CMS reporting**, **User reporting**, **SIM card** (appareil mobile) ou **Ethernet settings** (appareil Ethernet), **Event summary**.

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

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

6.3 CMS reporting

Le communicateur envoie les événements au centre de télésurveillance par liaison IP. Les événements peuvent passer par plusieurs canaux : le canal **principal** et le canal **parallèle** fonctionnent simultanément (vers deux récepteurs à la fois), et chacun a un canal **de secours**, qui prend le relais si le canal concerné est interrompu. La communication est chiffrée et protégée par mot de passe ; pour la réception et la retransmission vers le logiciel de télésurveillance, il faut un récepteur Trikdis (récepteur logiciel IPcom pour Windows ou Linux, récepteur matériel IP/SMS RL14, récepteur multicanal RM14) ou un récepteur universel compatible avec le protocole DC-09 / TL150.

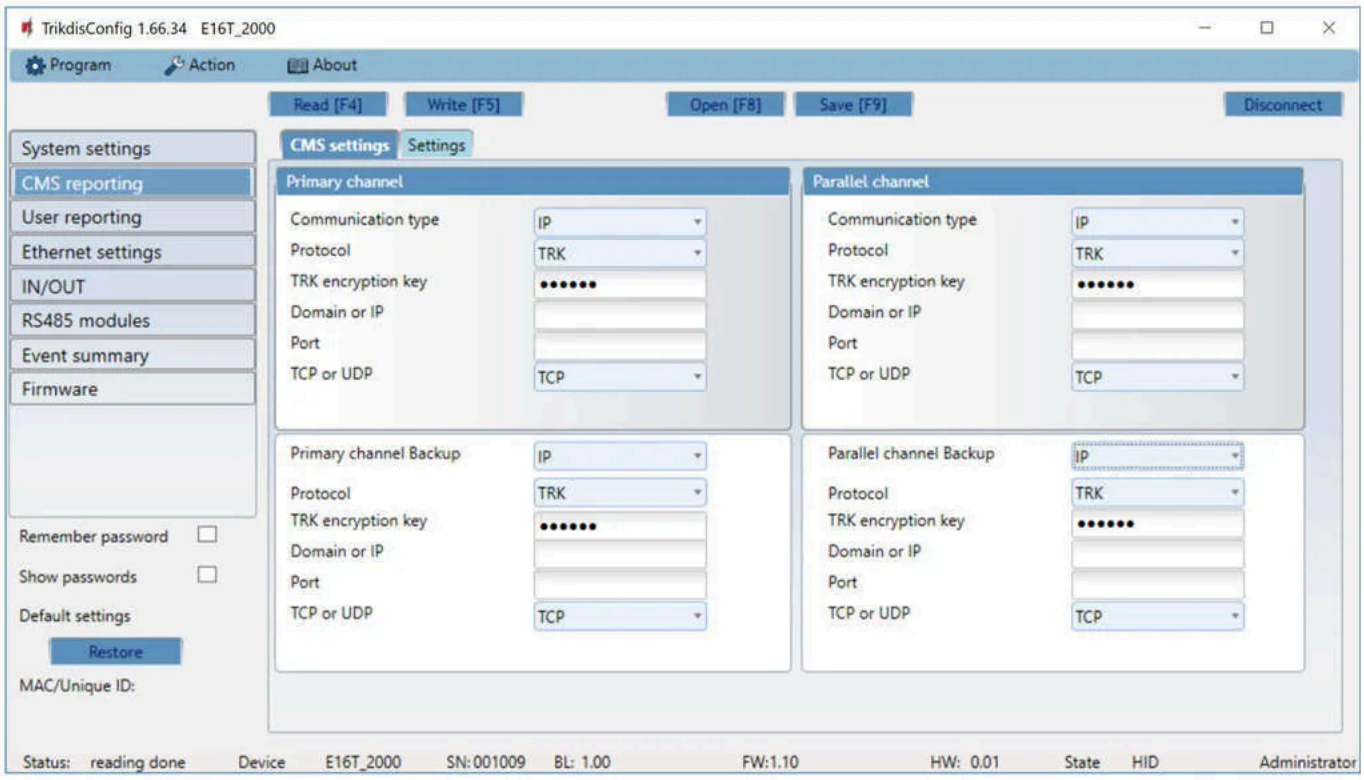


Figure 20. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal, canal de secours et canal parallèle.

Primary channel – canal principal

- **Communication type** – sur l'E16T, seul **IP** peut être choisi.
- **Protocol** – TRK (récepteurs Trikdis), DC-09_2007 ou DC-09_2012 (récepteurs universels), TL150 (SUR-GARD).
- **TRK encryption key** – clé de chiffrement à 6 chiffres ; elle doit être identique dans le communicateur et dans le récepteur.
- **Domain or IP**, **Port** – l'adresse du récepteur (nom de domaine ou adresse IP) et son numéro de port réseau.
- **TCP or UDP** – le protocole de transport : celui par lequel les événements sont envoyés (selon la configuration du récepteur).

Primary channel Backup – canal de secours. Il prend en charge la communication si le canal principal ne fonctionne pas ; ses paramètres sont les mêmes que ci-dessus. Il vaut la peine de le renseigner même sur un appareil filaire – par exemple avec la seconde adresse ou le second port du récepteur –, car le canal de secours pallie aussi une panne côté récepteur.

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

E16T antérieur

Sur l'E16T antérieur, TrikdisConfig affiche la même chose sur l'onglet **CMS Reporting** de la fenêtre **Reporting**, avec d'autres noms de champs :

- Groupe **Primary** : **Enable** – coché, le canal principal vers la télésurveillance est actif ; **Remote Host** – le nom de domaine ou l'adresse IP du récepteur ; **Remote Port** – le numéro de port réseau du récepteur ; **TCP or UDP** – le protocole de transport ; **PING Time** – activez-le et indiquez l'intervalle

entre les signaux de vie (valeur d'usine 30) – il est nécessaire à la supervision de la liaison ; **Encryption key** – clé de chiffrement à 6 chiffres, identique dans le communicateur et dans le récepteur.

- Groupe **Backup** : **Enable** – active le canal de secours, qui envoie si la liaison principale est interrompue ; les autres champs sont les mêmes que pour le canal principal.
- Groupe **Settings** : **TCP protocol** – le codage de l'envoi : TRK (pour un récepteur Trikdis), DC-09_2007 ou DC-09_2012 (pour un récepteur universel).
- Groupe **SIA IP parameter** – modifiable uniquement si le champ **TCP protocol** contient DC-09_2007 ou DC-09_2012 : **Encryption enabled** – avec DC-09_2012, le chiffrement peut être activé ; **DC09-2012 encryption key** – la clé de chiffrement configurée dans le récepteur ; **DC09-2012 receiver No.** – le numéro du récepteur ; **DC-09 line No.** – le numéro de ligne du récepteur ; **Use time stamp** – coché, le message contient aussi l'heure (horodatage).

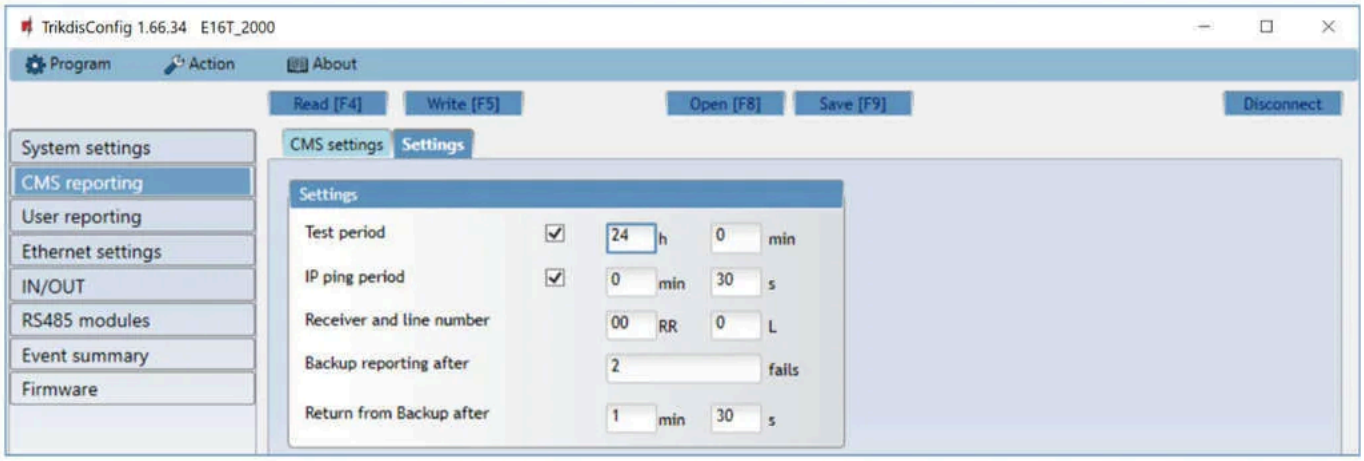


Figure 21. TrikdisConfig – CMS reporting, onglet Settings : rapport de test, PING, numéro de récepteur et de ligne (Receiver and line number : RR = numéro de récepteur, L = numéro de ligne) et temporisations du canal de secours.

Sur l'onglet **Settings**, vous réglez les temporisations ainsi que le numéro de récepteur et de ligne ; le groupe DC-09 n'est nécessaire que si vous envoyez avec le protocole DC-09 (il n'apparaît pas encore sur la capture d'écran de 2022).

- **Test period** – intervalle du rapport de test périodique (par défaut 24 heures). Le rapport de test est envoyé sous forme de message Contact ID à la télésurveillance et à Protegus 2.
- **IP ping period** – intervalle du signal de vie (PING) sur le canal IP (par défaut 30 s). Vous l'activez en cochant la case et saisissez la durée dans les champs minutes (**min**) et secondes (**s**) ; il est nécessaire à la supervision de la liaison. Le récepteur ne transmet pas les PING au logiciel de télésurveillance afin de ne pas le surcharger ; le logiciel ne reçoit un message que si le récepteur ne reçoit aucun PING pendant trois fois la durée réglée. Par exemple, avec une période PING de 3 minutes, la perte de liaison est signalée après la 9e minute.
- **Backup reporting after** – nombre de tentatives d'envoi infructueuses après lequel l'appareil bascule sur le canal de secours (par défaut 2).
- **Return from Backup after** – délai après lequel il revient sur le canal principal (par défaut 1 min 30 s).

Le PING maintient la liaison active entre l'appareil et le récepteur ; l'accès, la commande et la programmation à distance en dépendent également. C'est pourquoi **nous ne recommandons pas une période PING supérieure à 5 minutes**.

DC-09 Settings (à droite de l'onglet) – à remplir uniquement si vous transmettez sur un canal avec le protocole DC-09_2007 ou DC-09_2012 ; le groupe apparaît lorsque DC-09_2007 ou DC-09_2012 est sélectionné dans le champ **Protocol** d'un canal :

- **Object ID in DC-09** – identifiant hexadécimal de 3 à 16 caractères, fourni par la télésurveillance.
- **DC-09 line No** – numéro de ligne.
- **DC-09 receiver No.** – numéro du récepteur.

6.4 User reporting

Sur l'onglet **PROTEGUS Cloud**, vous autorisez le service Protegus. L'E16T n'a ni notification ni commande par SMS ; cette page ne comporte donc que cet onglet.

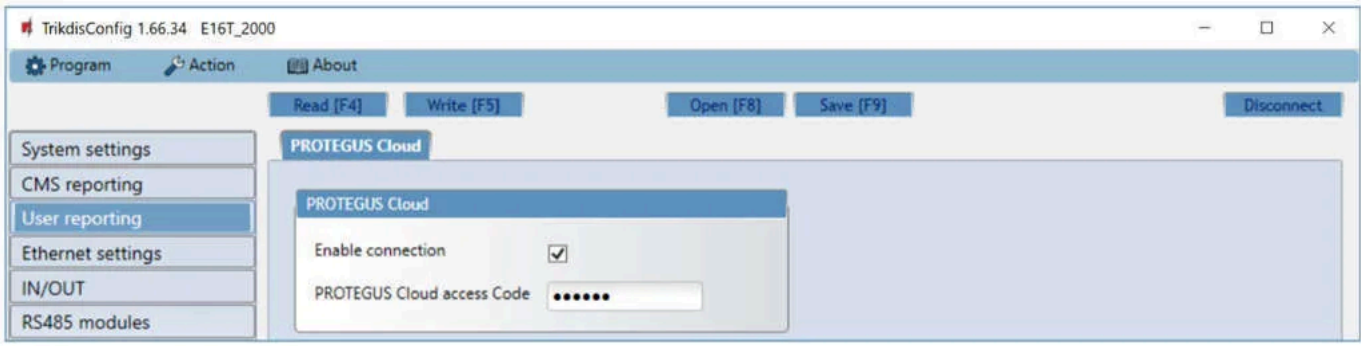


Figure 22. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- **Enable connection** – autorise la connexion au cloud Protegus et l'accès à distance par TrikdisConfig.
- **Protegus Cloud access code** – code à 6 chiffres pour la connexion Protegus (`123456` en usine). Si vous l'avez modifié, c'est lui qu'il faut saisir lors de l'ajout du système dans Protegus 2. Il ne peut être défini qu'avant la création du système dans Protegus 2 ; il ne peut plus être modifié ensuite.

6.5 Ethernet settings

C'est ici que vous indiquez comment l'E16T se connecte au réseau local.



Figure 23. TrikdisConfig – page Ethernet settings ; le DHCP est activé en usine.

- **Use DHCP** – case cochée, l'appareil reçoit automatiquement l'adresse IP, le masque de sous-réseau et la passerelle du serveur DHCP du routeur. C'est le réglage d'usine et, dans la plupart des cas, il n'y a rien d'autre à faire. S'il n'y a pas de DHCP sur le réseau, si la connexion automatique au réseau échoue ou si l'administrateur réseau demande une adresse fixe, décochez la case et remplissez manuellement les champs ci-dessous ainsi que les serveurs de noms :
- **Static IP** – adresse IP fixe de l'appareil sur le réseau local (une adresse qu'aucun autre appareil n'utilise et qui se situe hors de la plage DHCP).
- **Subnet mask** – masque de sous-réseau du réseau.

- **Default gateway** – passerelle par défaut, généralement l'adresse du routeur. Avec une mauvaise passerelle, l'appareil atteint le réseau local, mais pas Internet.
- **DNS 1, DNS 2** – serveurs de noms ; c'est par eux que l'appareil trouve le cloud Protegus et le récepteur indiqué par un nom de domaine. En usine, le DNS public de Google est renseigné ; si le réseau n'autorise vers l'extérieur que son propre serveur de noms, saisissez ici l'adresse du DNS local. 3 clignotements de la LED TROUBLE signalent une erreur DNS.

L'identifiant unique de l'appareil, l'adresse MAC (dans le logiciel **Internal MAC**), ne figure pas sur cette page dans la nouvelle fenêtre TrikdisConfig, mais en bas de la fenêtre, dans le champ **MAC / Unique ID** de la barre d'état.

L'appareil établit uniquement des connexions **sortantes** vers le récepteur et le cloud Protegus ; il n'est donc pas nécessaire d'ouvrir ni de rediriger un port sur le routeur, et aucune adresse IP publique fixe n'est requise.

Sur l'E16T antérieur, l'adresse MAC est affichée dans le champ **Internal MAC** du groupe Ethernet settings de la page **System settings** (remarque de la section 6.2).

6.6 IN/OUT

C'est ici que vous définissez le rôle des trois bornes I/O à double fonction du communicateur : **Disabled** (non utilisée), **IN** (entrée) ou **OUT** (sortie). Pour une entrée, il faut aussi indiquer le type (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

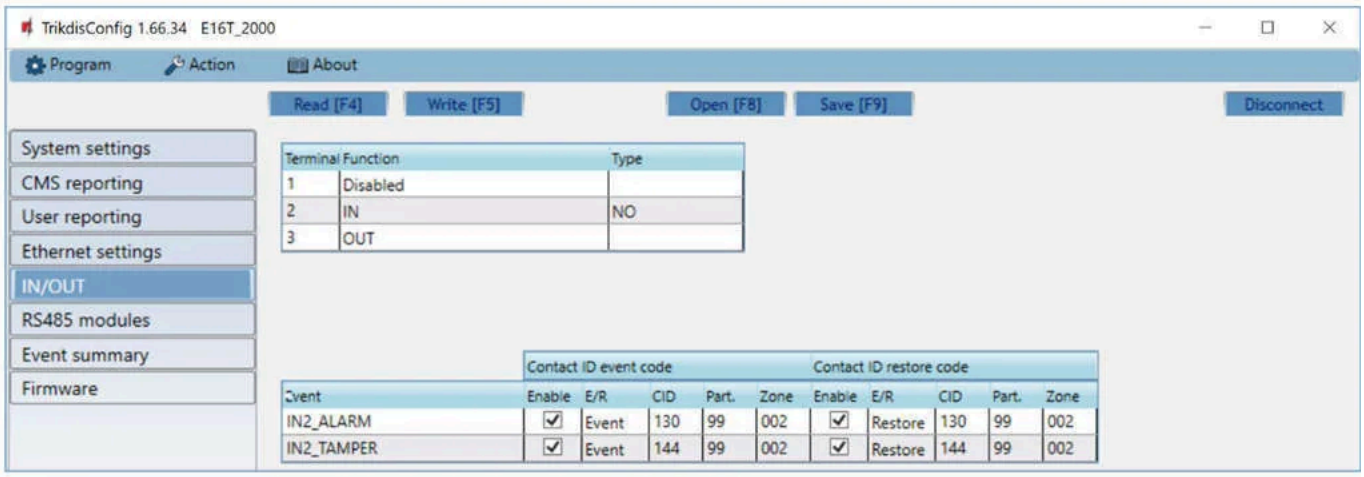


Figure 24. TrikdisConfig – page IN/OUT : fonction des bornes I/O et événements des entrées.

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

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

E16T antérieur

L'E16T antérieur n'a pas de page IN/OUT : le type et les événements des deux entrées se règlent dans le groupe **Input description** de la page **Event summary**. **Partition** – le numéro de partition ; **Contact ID** – le code d'événement (la valeur d'usine peut être conservée) ; lorsque l'entrée est déclenchée, c'est ce code qui est envoyé à Protegus et au centre de télésurveillance ; **Zone No.** – le numéro de zone, transmis dans les messages ; **Type** – le type d'entrée (NO, NC, EOL) ; **Enable / Alarm** – coché, il transmet lorsque l'entrée est déclenchée (événement) ; **Enable / Restore** – coché, il transmet lorsque l'entrée revient au repos. Le réglage de la sortie se trouve dans le groupe **System settings** → **Output** (remarque de la section 6.2).

6.7 RS485 modules

Les modules d'extension iO-8 et autres modules de la série iO raccordés au bus RS485 doivent être ajoutés sur l'onglet **Modules list**.

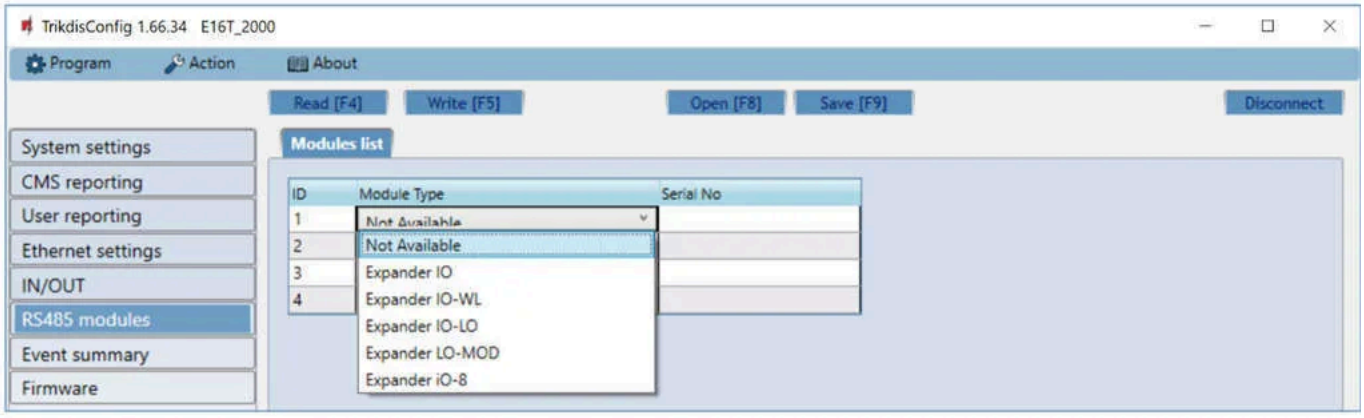


Figure 25. TrikdisConfig – RS485 modules, onglet Modules list : les types de modules disponibles.

- **Module Type** – le type du module raccordé, à choisir dans la liste (Expander iO-8, IO, IO-WL, IO-LO, LO-MOD).
- **Serial No** – le numéro de série à 6 chiffres du module (sur le module et sur sa boîte, SN).

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

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

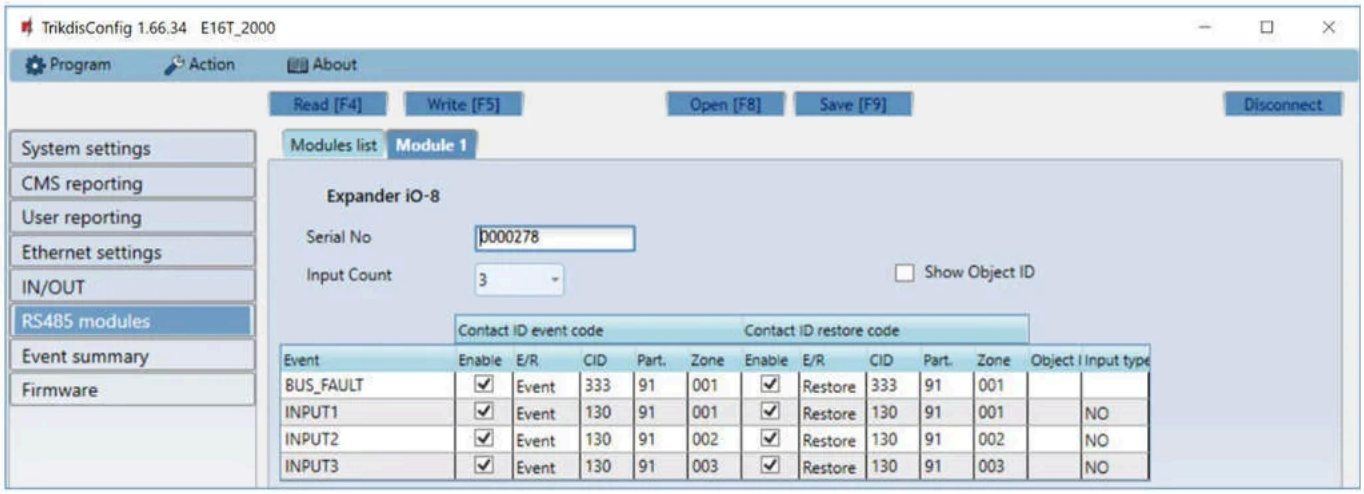


Figure 26. TrikdisConfig – RS485 modules, onglet du module iO-8.

- **Input Count** – le nombre de bornes configurées en entrée ; les autres seront des sorties. Le type d'entrée (**Input type** : NO ou NC) se définit dans le tableau. Le rôle des sorties (armement / désarmement ou commande d'un équipement) se règle dans l'application Protegus 2.
- Dans le tableau, vous pouvez attribuer un code Contact ID au défaut de bus (**BUS_FAULT**, Contact ID 333) et aux événements de déclenchement et de rétablissement des entrées (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Par défaut, le module 1 transmet avec la partition 91, le module 4 avec la partition 94. En cochant **Show Object ID**, un identifiant d'objet différent de celui du communicateur peut être attribué aux entrées.

6.8 Event summary

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

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

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

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

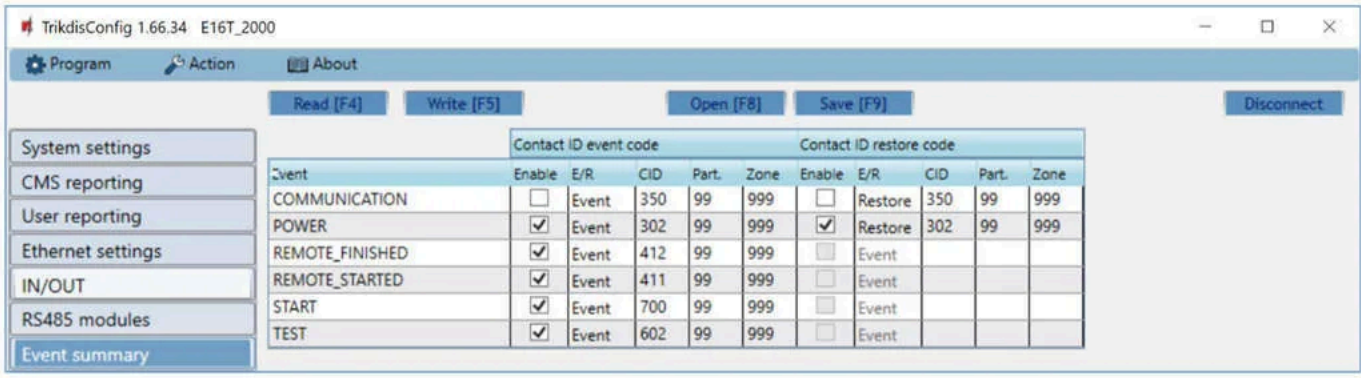


Figure 27. TrikdisConfig – page Event summary : les messages internes de l'appareil.

Sur l'E16T antérieur, le réglage des entrées se trouve aussi sur cette page (remarque de la section 6.6).

6.9 Rétablissement des réglages d'usine

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

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

7. Programmation à distance

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

Conditions requises pour l'accès à distance :

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

Étapes :

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

6. Effectuez les modifications, puis envoyez-les à l'appareil avec le bouton **Write [F5]** (écriture).

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

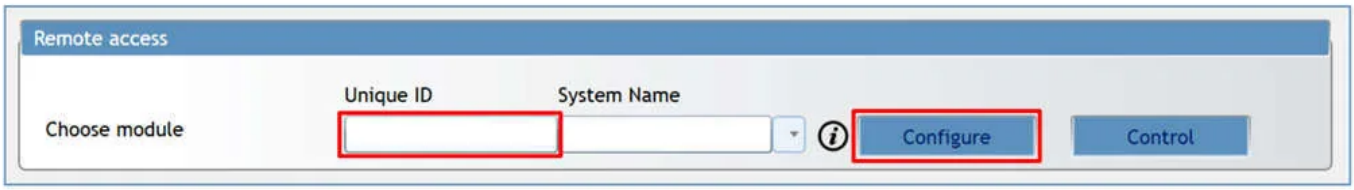


Figure 28. TrikdisConfig – Remote access : identifiant de l'appareil (sur l'E16T, l'adresse MAC), nom du système et bouton Configure.

L'activation du service Protegus est décrite à la section 6.4, le téléchargement de TrikdisConfig à la section 2.1.

8. Vérification du fonctionnement du communicateur

Après la programmation et le raccordement, vérifiez toujours toute la chaîne : centrale d'alarme → communicateur → télésurveillance et/ou Protegus 2.

Vérifiez d'abord que l'alimentation est présente (la LED **POWER** est allumée en vert) et que la connexion réseau est établie (la LED **NETWORK** est allumée en vert).

1. **Déclenchez un événement.** Armez puis désarmez le système depuis le clavier, ou violez une zone sur un système armé pour provoquer une alarme.
2. **Vérifiez la réception.** Contrôlez que l'événement apparaît dans le logiciel de télésurveillance et/ou dans la liste des événements de l'application Protegus 2 – avec les bons numéros de partition et de zone.
3. **Entrées.** Déclenchez le détecteur raccordé à une entrée propre du communicateur et vérifiez l'événement correspondant.
4. **Sorties.** Commutez la sortie depuis l'application Protegus 2 et vérifiez que l'équipement raccordé (relais, zone à clé) se déclenche réellement.
5. **Armement à distance.** Si la centrale peut être commandée à distance, armez-la et désarmez-la également depuis l'application Protegus 2.

9. Mise à jour du firmware

Ha bármikor az USB bedugásakor a program azt jelzi, hogy új firmware verzió jelent meg a Trikdis eszközhöz, fogadd el a frissítést és telepítsd!

Vous pouvez mettre à jour le firmware vous-même – vers une version plus récente et, si nécessaire, vers une version plus ancienne. Après la mise à jour, tous les réglages de l'appareil restent inchangés.

1. Lancez le logiciel TrikdisConfig et connectez l'appareil avec un câble USB, ou accédez à sa programmation à distance.
2. Si un firmware plus récent est disponible, le logiciel propose de le télécharger – acceptez.
3. Sélectionnez l'onglet **Firmware** et cliquez sur le bouton **Open firmware**. Choisissez le fichier de firmware.

4. Appuyez sur le bouton **Update [F12]**, attendez la fin de la mise à jour, puis cliquez sur **OK** dans la fenêtre qui s'affiche. Pendant ce temps, ne débranchez pas le câble et n'interrompez pas la connexion.

Les fichiers de firmware se trouvent dans le dossier d'installation de TrikdisConfig, dans le sous-dossier **Firmwares**, dans le dossier portant le nom de l'appareil. Si ce dossier n'existe pas, soit aucune mise à jour n'est disponible pour l'appareil, soit c'est le logiciel TrikdisConfig lui-même qu'il faut mettre à jour. Les fichiers les plus récents peuvent aussi être téléchargés, en tant qu'utilisateur enregistré, sur le site du fabricant, depuis la page de l'appareil.

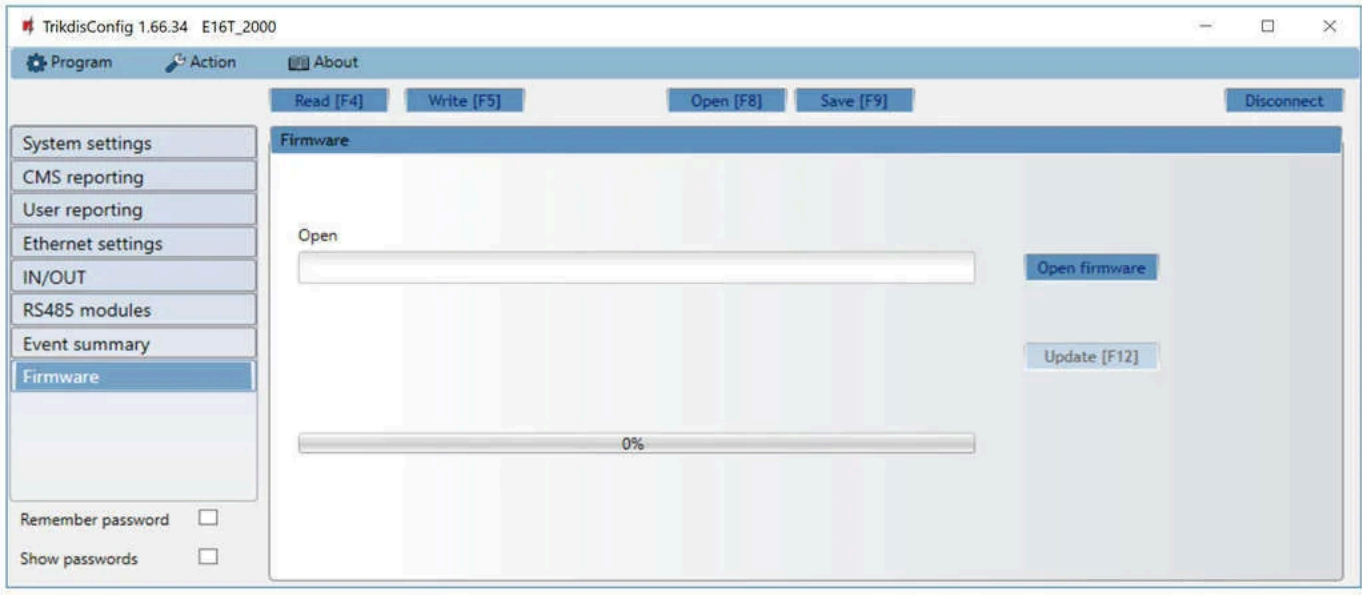


Figure 29. TrikdisConfig – page Firmware : Open firmware et Update [F12].

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

10. Dépannage et questions fréquentes

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

La LED NETWORK ne s'allume pas – pas de réseau

1. Observez les clignotements de la LED **TROUBLE** : 1 = pas de liaison physique, 2 = pas d'adresse IP obtenue (DHCP), 3 = erreur DNS.
2. **1 clignotement :** vérifiez le câble et les connecteurs (le RJ45 est-il enfoncé jusqu'au déclic ?), le port du routeur ou du switch (est-il actif, n'est-il pas désactivé ?), et essayez un autre câble ou un autre port.
3. **2 clignotements :** il n'y a pas de serveur DHCP sur le réseau, ou il ne répond pas : activez-le sur le routeur, ou donnez à l'appareil une adresse IP, un masque et une passerelle fixes sur la page **Ethernet settings** (section 6.5).
4. **3 clignotements :** la résolution de noms ne fonctionne pas : vérifiez les champs DNS 1 / DNS 2 (en usine, le DNS public de Google), et que le réseau autorise le trafic DNS sortant.

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

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

1. 6 clignotements de la LED **TROUBLE** indiquent qu'il n'y a pas de liaison avec le récepteur : vérifiez l'adresse du récepteur, son port, le réglage TCP/UDP et la clé de chiffrement (**CMS reporting**).
2. Si le récepteur est saisi par son nom de domaine, vérifiez le réglage DNS (**Ethernet settings**).
3. Avec une adresse IP fixe, vérifiez la passerelle (**Default gateway**) : avec une mauvaise passerelle, l'appareil atteint le réseau local, mais pas Internet.
4. Sur un réseau d'entreprise ou filtré, le pare-feu peut bloquer la connexion sortante vers le port du récepteur – voyez-le avec l'administrateur réseau (section 3.2).

La centrale n'envoie pas les événements au communicateur

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

Protegus 2 ne voit pas l'appareil

1. Sur la page **User reporting → PROTEGUS Cloud**, **Enable connection** doit être coché.
2. Lors de la création du système, il faut saisir le **Protegus Cloud access code** configuré dans l'appareil ; une fois le système créé, il ne peut plus être modifié dans l'appareil.
3. Saisissez l'adresse MAC exactement, depuis la boîte ou le dos de l'appareil – ou scannez le code QR de l'étiquette avec l'application, ce qui évite toute faute de frappe.
4. La connexion Internet doit fonctionner : la LED NETWORK est verte, et la LED DATA s'éteint après un événement. L'accès au cloud Protegus nécessite aussi un DNS fonctionnel (**Ethernet settings**).

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

1. L'appareil doit être en ligne (LED NETWORK verte, la LED DATA s'éteint après un événement), et la connexion Protegus doit être autorisée.
2. **CMS reporting → Settings → IP ping period** ne doit pas dépasser 5 minutes : c'est le PING qui maintient la connexion nécessaire à l'accès à distance.
3. Vérifiez le mot de passe administrateur ou installateur.

J'ai oublié le mot de passe

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

Faut-il une adresse IP fixe ou une redirection de port sur le routeur ?

Non. L'E16T établit lui-même la connexion sortante vers le récepteur et le cloud Protegus ; il ne faut donc ni adresse IP publique fixe, ni DNS dynamique, ni redirection de port. Sur le réseau local, l'adresse obtenue par DHCP convient aussi ; ne donnez une adresse locale fixe que s'il n'y a pas de DHCP sur le réseau, ou si l'administrateur réseau le demande (section 6.5).

Fonctionne-t-il en Wi-Fi ?

Non : l'E16T ne connaît que la connexion réseau filaire (RJ45). S'il n'y a pas de câble réseau près de la centrale, un pont Wi-Fi jusqu'au routeur peut être installé, ou choisissez le communicateur cellulaire G16T.

Que se passe-t-il en cas de coupure de courant ?

Le communicateur est alimenté par la batterie de la centrale, mais si le routeur et le modem restent sans courant, il n'y a pas d'Internet, et les événements attendent dans la mémoire tampon (la LED DATA est allumée). L'appareil les envoie au retour d'Internet. Si cette interruption n'est pas acceptable, la solution est une alimentation sans interruption pour les équipements réseau, ou un communicateur cellulaire (section 3.2).

11. Consignes de sécurité

Figyelem!

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

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

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

- L'installation et l'entretien d'un équipement de sécurité ne peuvent être effectués que par un installateur qualifié.
- Lisez attentivement le manuel avant l'installation ; le non-respect des instructions peut entraîner un dysfonctionnement ou une panne.
- Avant le raccordement, avant chaque branchement électrique et avant toute intervention de maintenance, mettez l'équipement hors tension.
- Les défauts résultant d'une installation ou d'une utilisation inappropriée, ainsi que les modifications et réparations non autorisées par Trikdis, annulent la garantie.
- Respectez les règles locales de traitement des déchets : ne jetez pas l'appareil défectueux ni ses composants avec les ordures ménagères.

Voir aussi

- Armement à distance par zone à clé depuis l'application Protegus 2 – les détails et les pièges de l'armement par zone à clé.
- Documentation en anglais : docs.trikdis.com.

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

Produits associés

Trikdis E16T Ethernet Universal Communicator - Module IP

Module Trikdis IO8 Wired Expander

Droits d'auteur

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

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

Version toujours à jour de ce manuel : https://trikdis.fr/manuel-e16t