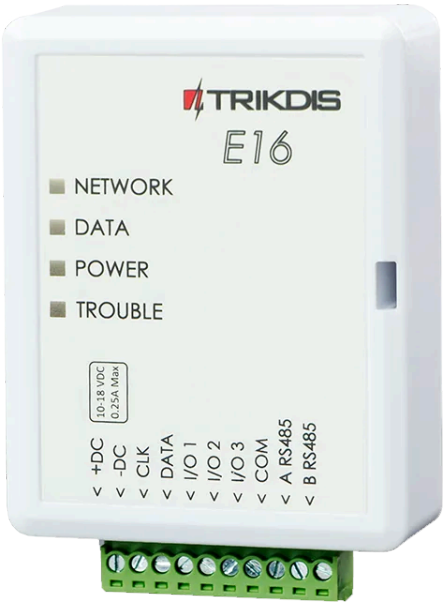
Communicateur E16 – manuel d'installation et d'utilisation

Manuel d'installation et d'utilisation du communicateur Ethernet Trikdis E16 : raccordement au bus de données ou au port série de la centrale d'alarme, programmation de la centrale, configuration réseau dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-e16

Sommaire

1. Présentation

1.1 À quoi sert-il, comment fonctionne-t-il ?
1.2 Centrales d'alarme compatibles
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 Type de centrale et commande directe
2.3 Liaison avec l'application Protegus 2
2.4 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 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception et Integriti
3.4 Raccordement d'une zone à clé
3.5 Raccordement des entrées
3.6 Raccordement d'une sortie avec relais
3.7 Raccordement du module d'extension iO-8
3.8 Raccordement du câble Ethernet
3.9 Mise sous tension et premier contrôle
A TRIKDIS átjelző elindítása

4. Programmation de la centrale d'alarme

4.1 DSC
4.2 Paradox
4.3 Texecom
4.4 UTC Interlogix (Caddx)
4.5 Crow et Pyronix
4.6 Honeywell Ademco Vista
4.7 InnerRange Inception et Integriti

5. Commande à distance avec l'application Protegus 2

5.1 Ajout de l'appareil
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Commande directe avec le code clavier

5.3 Armement par zone à clé
5.4 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'E16 est le **communicateur Ethernet à raccordement direct** de Trikdis : il ne se branche pas sur la sortie ligne téléphonique de la centrale d'alarme, mais sur son **bus clavier ou son port série**. Il lit les événements directement dans la centrale – avec le numéro de zone, de partition et d'utilisateur – et les 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 fonctionne avec les centrales DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell et Crow prises en charge ; sur les modèles **à commande directe**, l'utilisateur arme et désarme depuis l'application Protegus 2 avec son propre code clavier, sans zone à clé séparée. Pour une centrale d'une autre marque qui ne dispose que d'une sortie ligne téléphonique, il faut le communicateur Ethernet E16T (TIP/RING) ; là où il n'y a pas d'Internet filaire, le communicateur cellulaire G16.

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

- **Il lit directement la centrale.** Sur le bus de la centrale, chaque événement arrive immédiatement au communicateur, avec la numérotation propre de la centrale ; inutile de configurer le transmetteur téléphonique de la centrale, et il n'y a pas de numérotation Contact ID.
- **Il transmet au centre de télésurveillance.** Il envoie les événements par IP au récepteur logiciel ou matériel Trikdis (protocole TRK ; les récepteurs Trikdis fonctionnent avec n'importe quel logiciel de télésurveillance) ou à tout récepteur universel (SIA DC-09 2007/2012, SUR-GARD TL150). Avec un récepteur SUR-GARD, le communicateur convertit en codes SIA les codes Contact ID reçus de la centrale ; la table de conversion figure en annexe de la documentation Trikdis en anglais. Par défaut, il vérifie la liaison toutes les 30 secondes (l'intervalle est modifiable, section 6.3) et, en cas de défaut, bascule sur le canal de secours ; avec le canal parallèle, les événements peuvent être envoyés simultanément à deux récepteurs.
- **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, chauffage, ventilation, arrosage, etc.). Protegus 2 fonctionne avec les centrales de toutes les marques prises en charge par l'E16.
- **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.
- **Ni carte SIM ni abonnement mobile.** L'appareil utilise la connexion Internet existante du site : il se raccorde au routeur ou au switch par un câble Ethernet, obtient son adresse par DHCP en configuration d'usine et n'établit que des connexions sortantes ; il n'est donc pas nécessaire d'ouvrir de port sur le routeur.
- **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.

La figure ci-dessous montre l'architecture du système : le bus de la centrale d'alarme est raccordé à l'E16, l'E16 accède à Internet par le routeur, puis au cloud Protegus et au récepteur du centre de télésurveillance, et l'utilisateur voit le système dans l'application Protegus 2.

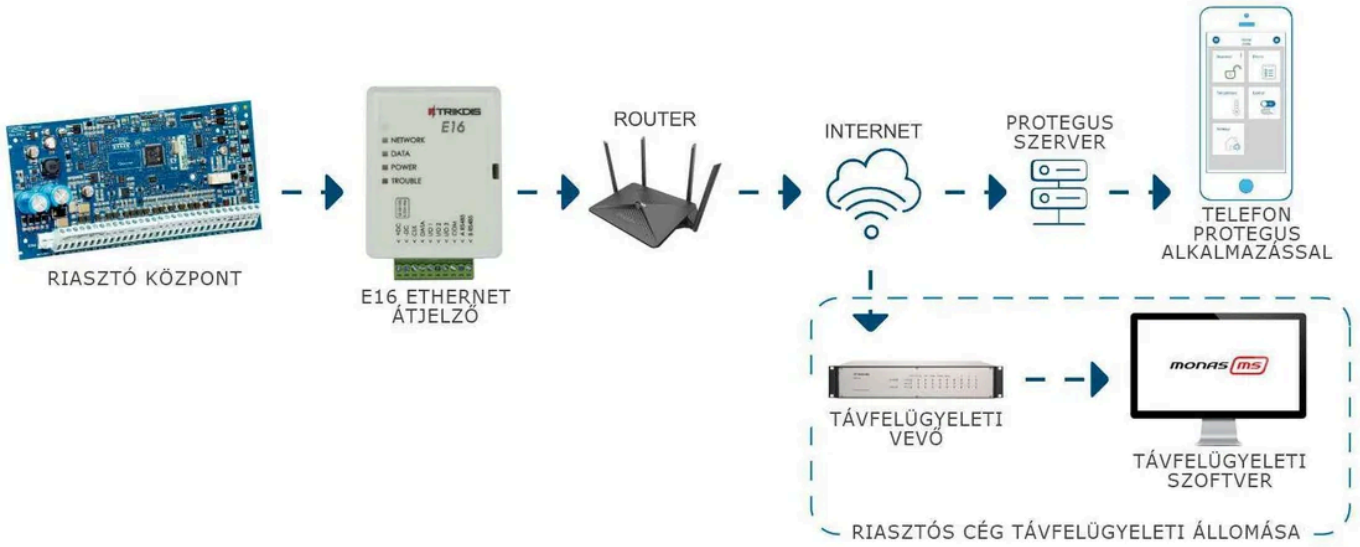


Figure 1. La place de l'E16 dans le système : centrale d'alarme (bus clavier ou port série) → communicateur Ethernet E16 → routeur → Internet → cloud Protegus et récepteur du centre de télésurveillance → téléphone de l'utilisateur avec l'application Protegus 2, ou logiciel de télésurveillance de la société de sécurité.

1.2 Centrales d'alarme compatibles

L'E16 peut être raccordé aux centrales ci-dessous. Sur les modèles **à commande directe**, l'armement et le désarmement se font depuis l'application avec le code clavier ; sur les autres, par une zone à clé (section 3.4). Pour la commande directe des centrales Paradox, le firmware de la centrale doit être au moins en **V.4** ; sur les modèles Paradox récents (SP+, MG5050+, EVOHD+), le port série est verrouillé en usine et doit être déverrouillé avant utilisation.

Centrales à commande directe – le communicateur reçoit les événements par le bus de données ou le port série, et l'armement / le désarmement fonctionnent sans câblage supplémentaire :

Fabricant	Raccordement	Modèles
Paradox	port série	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* firmware supérieur à 7.50)
DSC	bus de données	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	bus de données	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	port série	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	bus de données	Ademco Vista-15, Vista-20, Vista-48

Sur les centrales Paradox plus récentes marquées d'un *, le port série est verrouillé en usine ; l'appareil externe ne communique avec la centrale qu'après son déverrouillage.

Soros port feloldás útmutató

Centrales commandées par zone à clé – le communicateur reçoit les événements par le bus de données ou le port série ; la commande nécessite un raccordement et une programmation en zone à clé (point 3.4) :

Fabricant	Raccordement	Modèles
Paradox	port série	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	bus de données	PC1404, PC5020
Texecom	port série	Premier 412, 816, 832, 832+
Inner Range	bus de données	Inception, Integriti
Crow	bus de données	Runner 4/8, 8/16

Il peut en outre être utilisé avec les centrales **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 et MATRIX 816**, ainsi que **Paradox DIGIPLEX NE96 et EVO96**.

La liste évolue de temps en temps ; vous trouverez l'état le plus récent dans le moteur de recherche de compatibilité. L'E16 ne fonctionne pas avec les centrales **DSC PowerSeries NEO** : DSC n'autorise pas d'appareil externe sur le bus NEO, voir DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions.

1.3 Caractéristiques principales

Liaison avec la centrale d'alarme

- Se raccorde avec 4 fils au maximum (+DC, −DC, CLK, DATA) au bus clavier (DSC, Caddx, Crow, Pyronix, Honeywell) ou au port série (Paradox, Texecom, InnerRange) de la centrale ; un câble d'origine est disponible pour le port série (Paradox : CRP2 / CRP2B, Texecom : CRP4).
- Transmet chaque événement de la centrale avec l'information complète (code, partition, zone ou utilisateur) ; signale la perte de liaison (LED TROUBLE, événement COMMUNICATION).
- Les centrales à commande directe peuvent être armées et désarmées depuis l'application avec le code clavier ; Protegus 2 affiche aussi l'état des zones.

Connexion réseau

- Raccordement Ethernet (IEEE 802.3, 10Base-T, RJ45) au réseau local ; l'adresse est obtenue par DHCP en configuration d'usine, une adresse IP fixe peut aussi être définie.
- N'établit que des connexions sortantes vers le récepteur et le cloud Protegus : pas de port à ouvrir, ni adresse IP publique ni carte SIM nécessaires.

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, chacun avec son propre récepteur de secours ; avec le canal parallèle, les événements partent simultanément vers deux récepteurs.
- Messages chiffrés (AES-128) ; 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.
- Configuration et mise à jour à distance avec le logiciel TrikdisConfig.

1.4 Éléments du communicateur

Le circuit imprimé de l'E16 est logé dans un boîtier en plastique blanc ; la face avant est amovible et le bornier est débrochable. Le connecteur Ethernet se trouve sur le circuit imprimé, le câble entre par l'ouverture du boîtier.

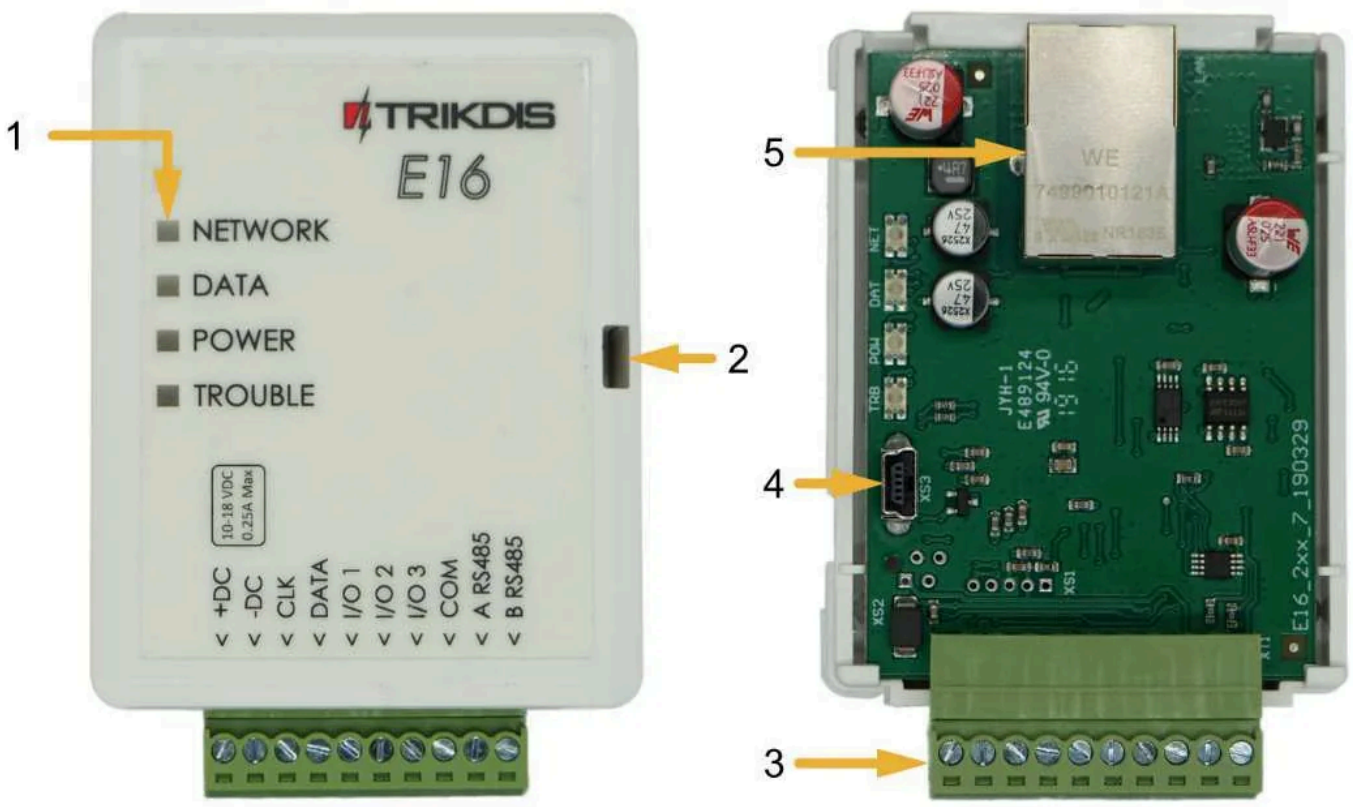


Figure 2. Les éléments de l'E16, de face et boîtier ouvert.

- 1 Voyants LED (NETWORK, DATA, POWER, TROUBLE)
- 2 Ouverture facilitant le retrait de la face avant
- 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
CLK	Ligne d'horloge / ligne série du bus de la centrale

Borne	Fonction
DATA	Ligne de données du bus de la centrale
I/O 1	Entrée/sortie 1 (réglage d'usine : entrée, NO)
I/O 2	Entrée/sortie 2 (réglage d'usine : entrée, NO)
I/O 3	Entrée/sortie 3 (réglage d'usine : sortie)
COM	Point commun (négatif) des entrées et sorties
A RS485	Fil A du bus RS485
B RS485	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. La borne de la centrale à laquelle vont CLK et DATA varie selon le fabricant – les schémas de raccordement se trouvent à la section 3.3.

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 le trafic et TROUBLE les défauts.

NETWORK – connexion réseau

Signal	Signification
éteinte	Pas de connexion au réseau (câble, routeur ou adresse IP manquant – la LED TROUBLE indique lequel)
allumée en vert	Connecté au réseau

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) : le câble n'est pas branché, ou le port du routeur / switch est inactif
2 clignotements rouges	Erreur DHCP : l'appareil n'a pas obtenu d'adresse IP
3 clignotements rouges	Erreur DNS : impossible de résoudre le nom de domaine du récepteur ou du cloud Protegus
6 clignotements rouges	Pas de liaison avec le récepteur du centre de télésurveillance et/ou le serveur Protegus (la cause peut aussi être la connexion Internet ou le pare-feu)
7 clignotements rouges	Liaison avec la centrale d'alarme interrompue (liaison bus ou série)
clignote en rouge (pendant la programmation)	Erreur mémoire
allumée en rouge (pendant la programmation)	Firmware endommagé

1.7 Caractéristiques techniques

Paramètre	Valeur
Liaison avec la centrale d'alarme	bus clavier ou port série, selon le type de centrale (4 fils : +DC, −DC, CLK, DATA)
Raccordement réseau	Ethernet, IEEE 802.3, 10Base-T, prise RJ45
Configuration réseau	DHCP (usine) ou adresse IP fixe, masque de sous-réseau, passerelle, DNS
Entrées/sorties	3 I/O à double fonction : 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	jusqu'à 4 modules iO-8 sur le bus RS485 (+8 I/O par module)
Tension d'alimentation	10–18 V DC
Consommation	100 mA nominal (en veille) ; 250 mA au maximum pendant l'envoi
Protocoles de transmission	TRK, DC-09_2007, DC-09_2012, TL150
Chiffrement des messages	AES-128
Mémoire tampon	60 messages
Programmation	TrikdisConfig (Windows) par câble USB Mini-B ou à distance

Paramètre	Valeur
Environnement de fonctionnement	−10 … +50 °C, humidité relative max. 80 % (à +20 °C)
Dimensions	88 × 65 × 26 mm
Poids	80 g

2. Mise en service rapide avec TrikdisConfig

Tous les paramètres de l'E16 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 · câble d'au moins 4 conducteurs pour le bus de la centrale – pour le port série Paradox, câble **CRP2** ou **CRP2B**, pour le port série Texecom, câble **CRP4** · tournevis plat de 2,5 mm · câble Ethernet (CAT-5 ou supérieur, 100 m au maximum) jusqu'au routeur ou au switch · manuel d'installation de la centrale d'alarme. Les câbles et accessoires sont à commander séparément auprès du distributeur.

1. Téléchargez et installez le logiciel TrikdisConfig.

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'E16. 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. La figure ci-dessous montre l'ouverture et l'emplacement de la prise USB.

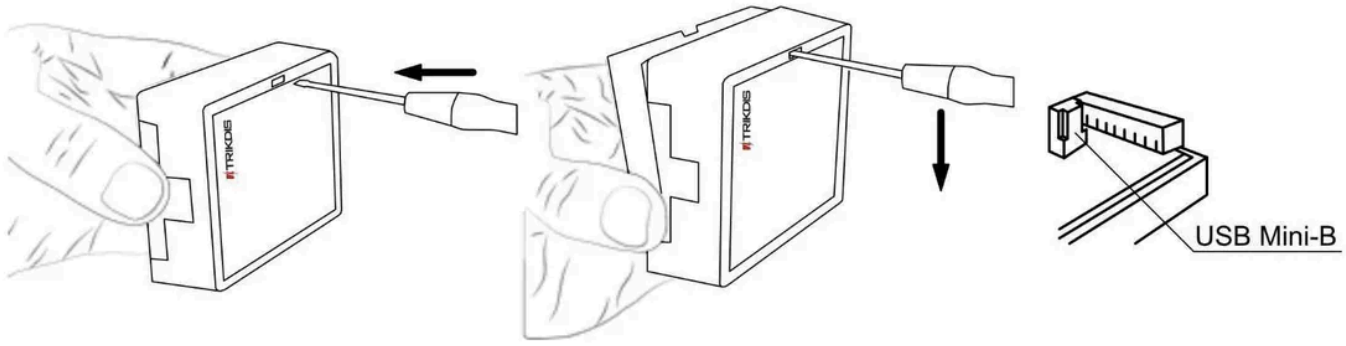


Figure 3. Déclipsage de la face avant avec un tournevis plat (à gauche, au centre) et emplacement de la prise USB Mini-B sur le circuit imprimé (à droite).

3. Reliez l'E16 à l'ordinateur avec un câble USB Mini-B. L'USB fournit suffisamment d'alimentation pour la programmation, aucune alimentation séparée n'est nécessaire.

Avertissement

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

4. 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).

2.2 Type de centrale et commande directe

Quel que soit le mode de fonctionnement utilisé, indiquez d'abord sur la page **System settings** sur quelle centrale le communicateur sera installé.

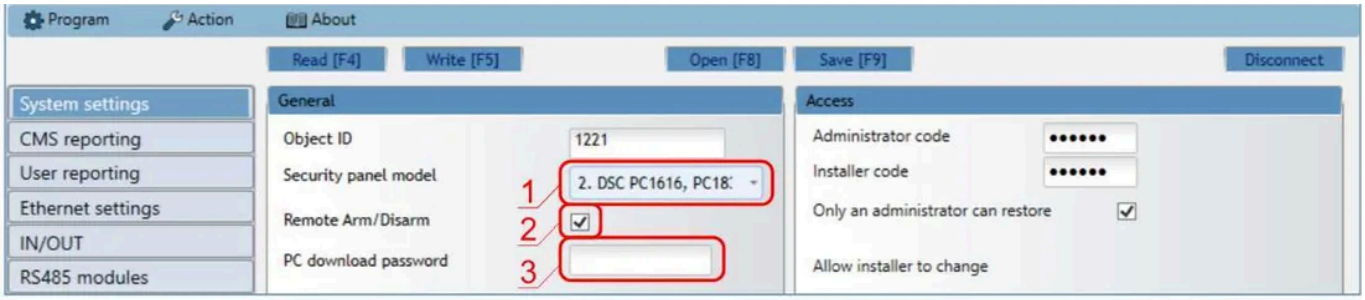


Figure 4. TrikdisConfig – page System settings, groupe General.

- 1 **Security panel model** – le type de la centrale d'alarme raccordée, à choisir dans la liste ; c'est de lui que dépend la façon dont le communicateur lit le bus.
- 2 **Remote Arm/Disarm** – cochez-le si l'utilisateur souhaite armer et désarmer la centrale depuis l'application Protegus 2 avec son propre code clavier. Il n'apparaît que pour les modèles à commande directe ; sur les autres centrales, l'armement se fait par une zone à clé (section 3.4) – dans ce cas, laissez-le décoché.
- 3 **Security panel PC download password** – pour les centrales Paradox et Texecom, le mot de passe PC ou UDL de la centrale (4 caractères) ; il doit être identique à celui configuré dans la centrale. Le champ apparaît une fois Remote Arm/Disarm coché.

Pour plusieurs centrales, un réglage est aussi nécessaire dans la centrale elle-même : pour Caddx, Honeywell et InnerRange dès la lecture des événements (activation du bus ou du port série), pour Paradox et Texecom pour la commande directe (mot de passe PC ou UDL) – le chapitre 4 le décrit par fabricant, y compris le changement du mot de passe.

2.3 Liaison avec l'application Protegus 2

Si l'utilisateur souhaite voir et commander le système depuis l'application Protegus 2, réglez les points suivants sur la page **User reporting**, onglet **PROTEGUS Cloud**.



Figure 5. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- 4 **Enable connection** – cochez-le : il autorise la connexion au cloud Protegus.
- 5 **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 ; **il ne peut plus être modifié une fois le système créé.**

Pour les paramètres réseau, l'option **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. Si le réseau n'a pas de DHCP, ou s'il faut utiliser une adresse fixe, saisissez ici les paramètres manuels (section 6.5).

L'E16 n'établit que des connexions **sortantes** vers le cloud Protegus et le récepteur ; il n'est donc pas nécessaire d'ouvrir ou de rediriger un port sur le routeur. Sur un réseau d'entreprise filtré par un pare-feu, convenez du trafic sortant avec l'administrateur système (section 3.2).

Si l'appareil fonctionne 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. S'il transmet aussi à un centre de télésurveillance, poursuivez avec la section 2.4.

2.4 Liaison avec le centre de télésurveillance

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

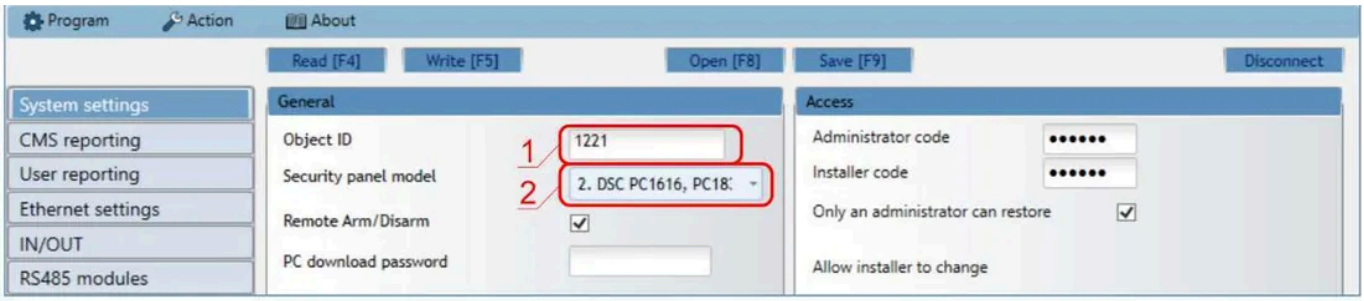


Figure 6. TrikdisConfig – page System settings, groupe General.

- 1 **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). `FFFE` et `FFFF` ne peuvent pas être utilisés.
- 2 **Security panel model** – le type de la centrale d'alarme raccordée (si vous ne l'avez pas encore réglé à la section 2.2).

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

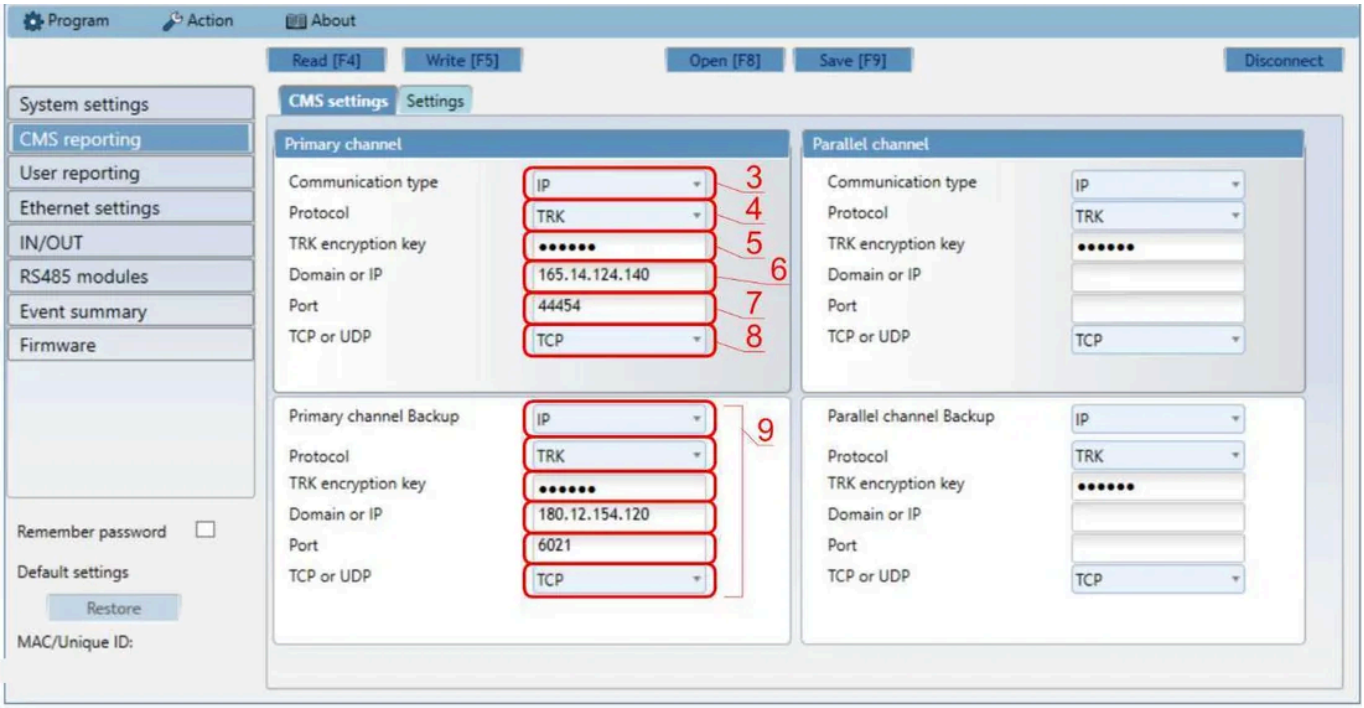


Figure 7. TrikdisConfig – CMS reporting, onglet CMS settings.

- 3 **Communication type** – **IP** (c'est la seule possibilité sur l'E16).
- 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 recommandé de le définir.

Il est recommandé de configurer aussi le **Parallel channel** (canal parallèle) et son canal de secours, si les événements doivent parvenir à deux récepteurs.

Avec le protocole **DC-09**, indiquez aussi sur l'onglet **Settings** les numéros d'objet, de ligne et de récepteur DC-09. Si vous saisissez le récepteur par son nom de domaine, une adresse DNS fonctionnelle doit être définie sur la page **Ethernet settings** (en usine, le serveur de noms public de Google).

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 3.8).
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 câble du bus reste court. Un coffret métallique ne le gêne pas : l'E16 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'E16 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 (G16).

3.3 Raccordement à la centrale d'alarme

L'E16 se raccorde à la centrale avec **quatre fils au maximum** (sur le bus Caddx et Pyronix, CLK n'est pas utilisé) : sur les bornes **+DC** et **−DC** arrive l'alimentation auxiliaire 12 V (AUX) de la centrale, sur les bornes **CLK** et **DATA** les deux fils de données du bus clavier ou du port série de la centrale. La correspondance des bornes de la centrale varie selon le fabricant – raccordez selon les schémas ci-dessous. Pour les centrales à port série (Paradox, Texecom), un câble d'origine est disponible : une extrémité s'enfiche dans le connecteur de la centrale, l'autre se raccorde au bornier de l'E16.

Pendant l'envoi, l'E16 peut consommer jusqu'à 250 mA. 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. La plupart des centrales ne

sont pas endommagées par l'inversion des fils d'un appareil raccordé au bus, mais l'inversion de **+DC et −DC** peut détruire le communicateur – vérifiez la polarité avant le raccordement.

Après le raccordement, il faut choisir le type de la centrale raccordée dans le champ **System settings** → **Security panel model** de TrikdisConfig (section 2.2) ; chez certains fabricants, un réglage est aussi nécessaire dans la centrale (chapitre 4).

3.3.1 DSC PowerSeries

Les quatre bornes du Keybus : **RED** → +DC, **BLK** → −DC, **YEL** → CLK, **GRN** → DATA.

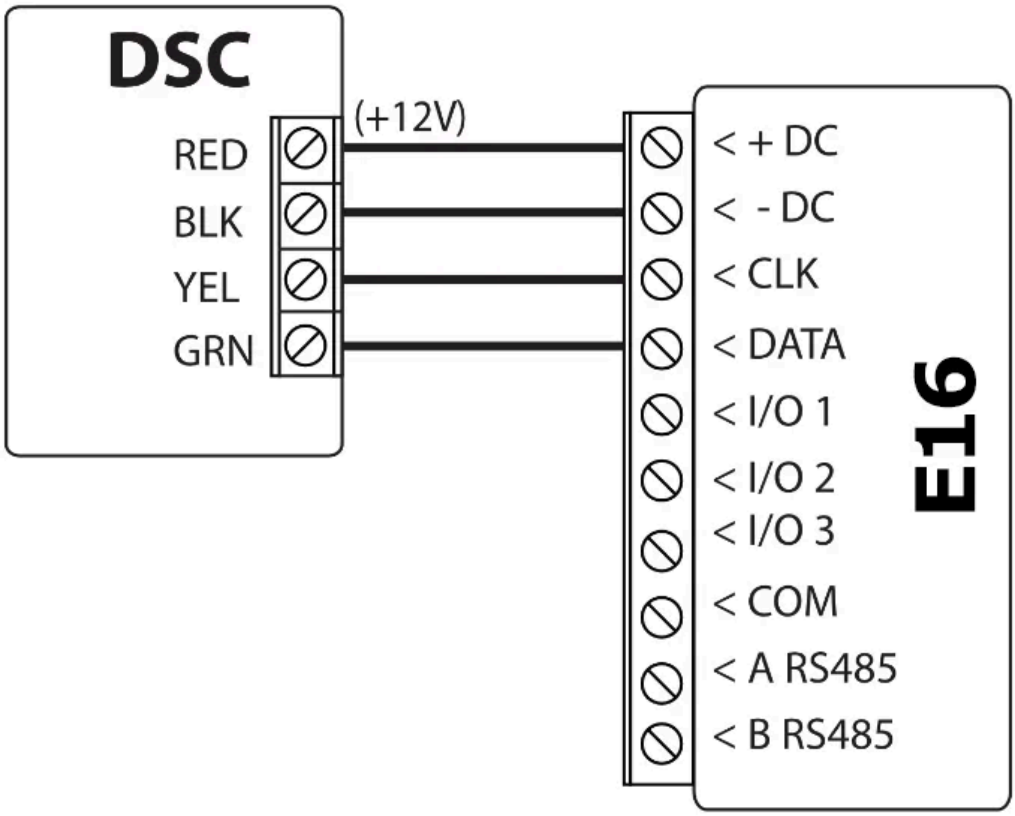


Figure 8. Raccordement au Keybus d'une centrale DSC PowerSeries (bus clavier, « Keypad bus ») : RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Le communicateur se raccorde au **port série** (SERIAL) des centrales Paradox avec le câble d'origine **CRP2** ou **CRP2B** ; l'extrémité côté centrale s'enfiche dans le connecteur série, l'autre extrémité se raccorde au bornier de l'E16. Les 4 broches du connecteur : **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Les couleurs des conducteurs diffèrent entre les deux câbles – le schéma montre la répartition des couleurs des deux câbles. Marquage du connecteur série Paradox : AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

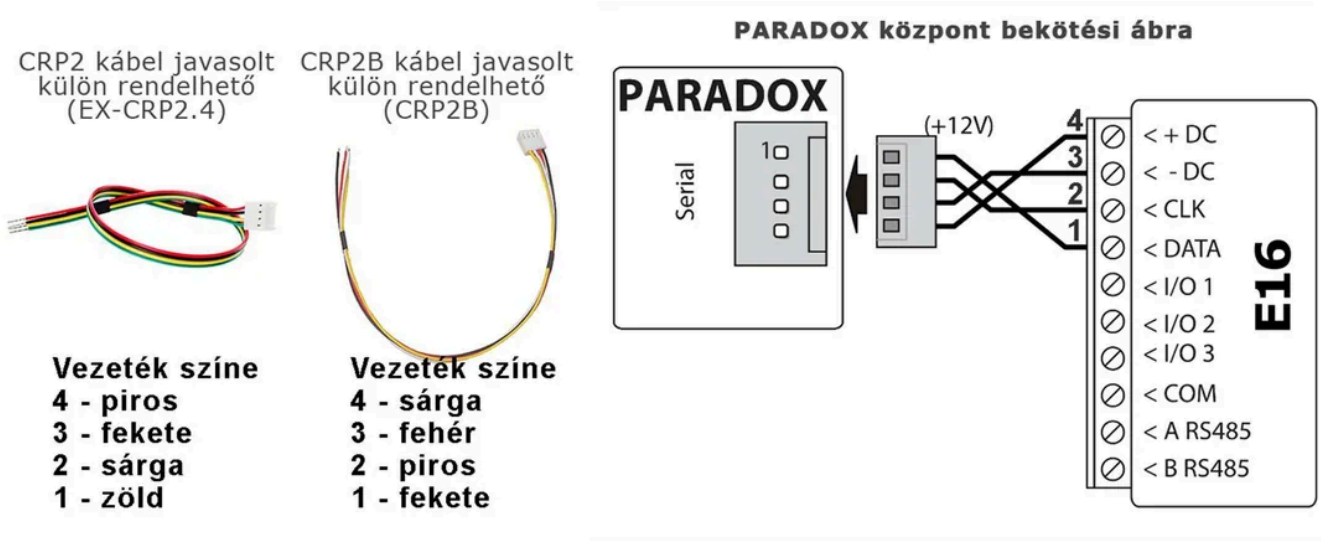


Figure 9. Raccordement au port série d'une centrale Paradox avec le câble CRP2 (EX-CRP2.4) ou CRP2B. CRP2 : 4 rouge → +DC, 3 noir → −DC, 2 jaune → CLK, 1 vert → DATA. CRP2B : 4 jaune → +DC, 3 blanc → −DC, 2 rouge → CLK, 1 noir → DATA.

Sur les centrales Paradox récentes, le port série peut être verrouillé en usine – la procédure de déverrouillage est décrite à la section 4.2 et dans l'article Déverrouillage du port série verrouillé des centrales d'alarme Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

Les trois bornes du bus clavier : **POS** → +DC, **COM** → −DC, **DATA** → DATA. La borne **CLK** n'est pas utilisée.

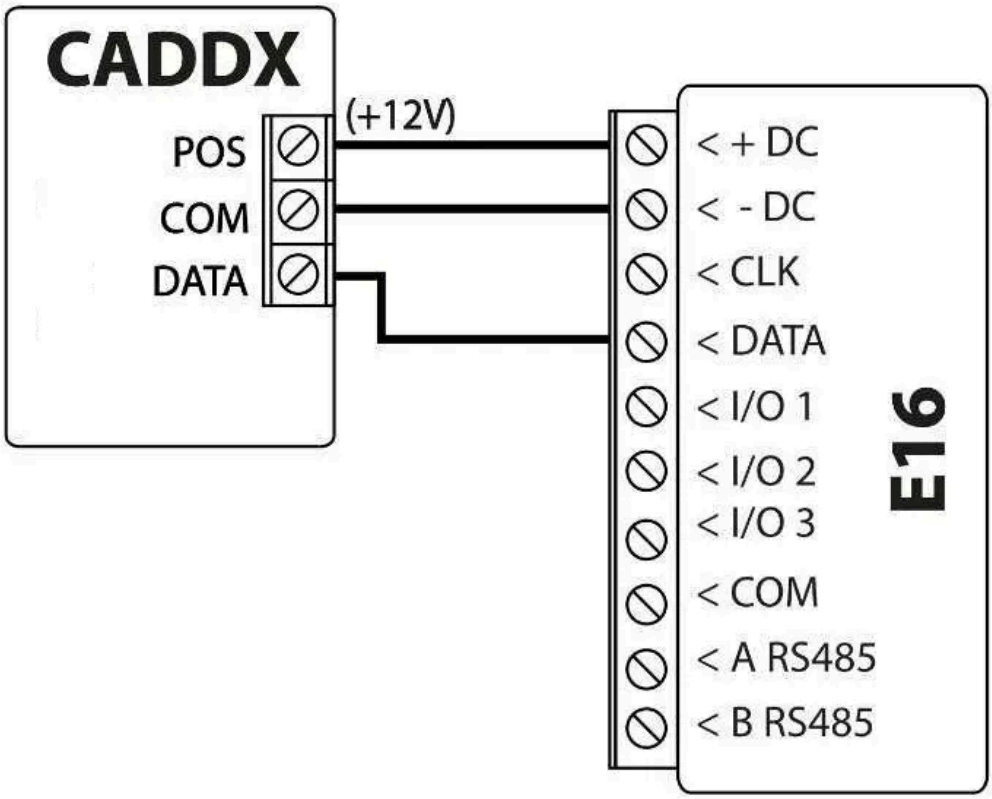


Figure 10. Raccordement au bus clavier d'une centrale Caddx NetworX (« Keypad bus ») : POS → +DC (+12 V), COM → −DC, DATA → DATA ; CLK reste libre.

3.3.4 Texecom Premier / Premier Elite

Le communicateur se raccorde au port série de la centrale avec le câble d'origine **CRP4** : **rouge (R)** → +DC, **noir (B)** → −DC, **bleu (BL)** → CLK, **blanc (W)** → DATA.

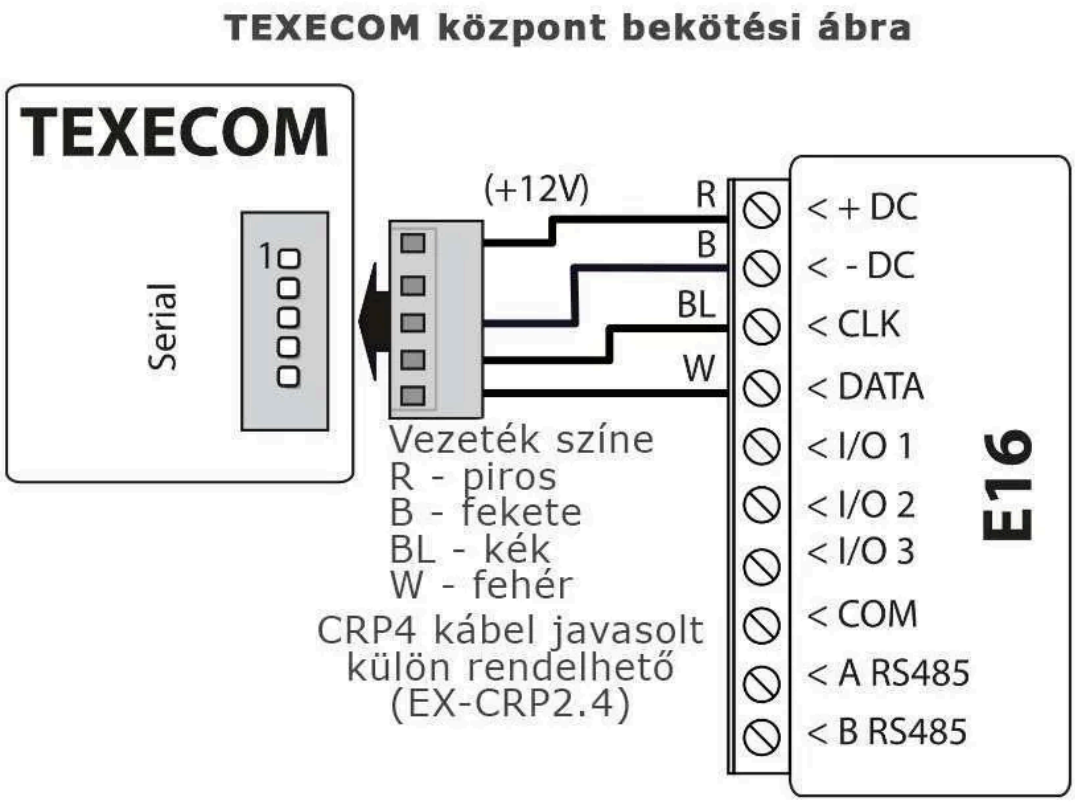


Figure 11. Raccordement au port série d'une centrale Texecom avec le câble CRP4 : rouge → +DC, noir → −DC, bleu → CLK, blanc → DATA.

3.3.5 Crow Runner

Bus clavier des Crow Runner 4/8 et Runner 8/16 : **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

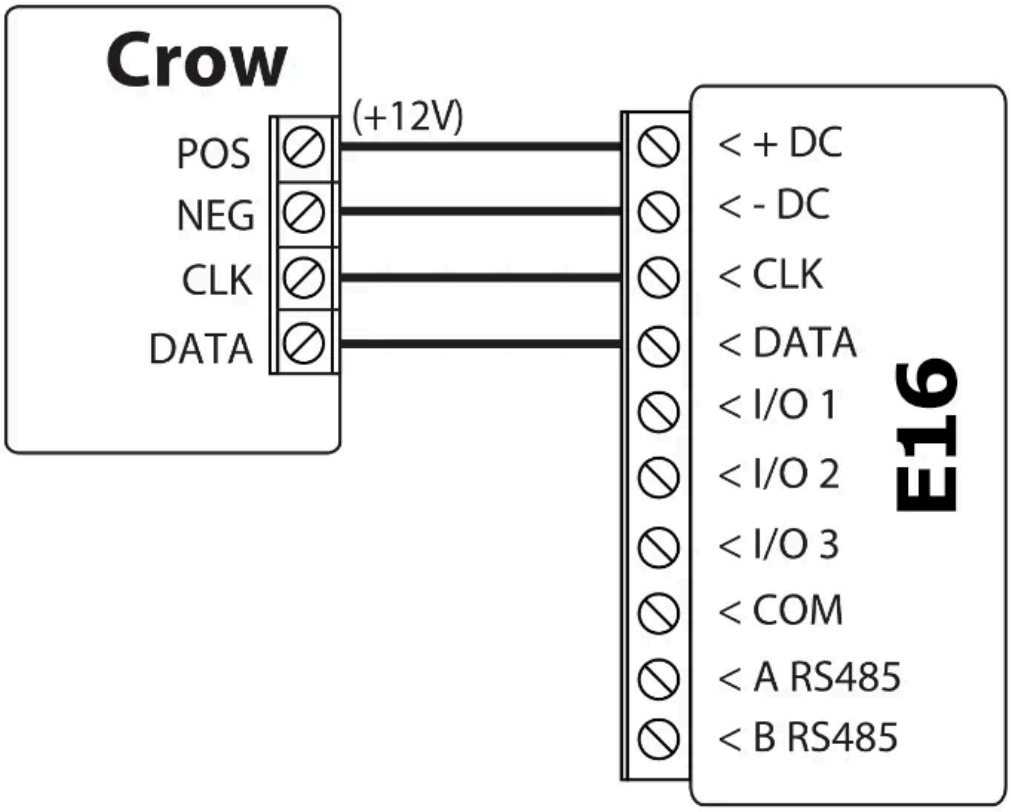


Figure 12. Raccordement au bus clavier d'une centrale Crow Runner 4/8 et Runner 8/16 (« Keypad bus ») : POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Bus clavier des centrales Pyronix : **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. La borne **CLK** n'est pas utilisée. Après le raccordement et la configuration du communicateur, mettez la centrale hors tension puis redémarrez-la pour qu'elle accepte le communicateur (section 4.5).

3.3.7 Honeywell Ademco Vista

Les bornes numérotées du bus clavier des centrales Vista-15, Vista-20 et Vista-48 : **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (sortie de données, jaune) → CLK, **6** (entrée de données, vert) → DATA.

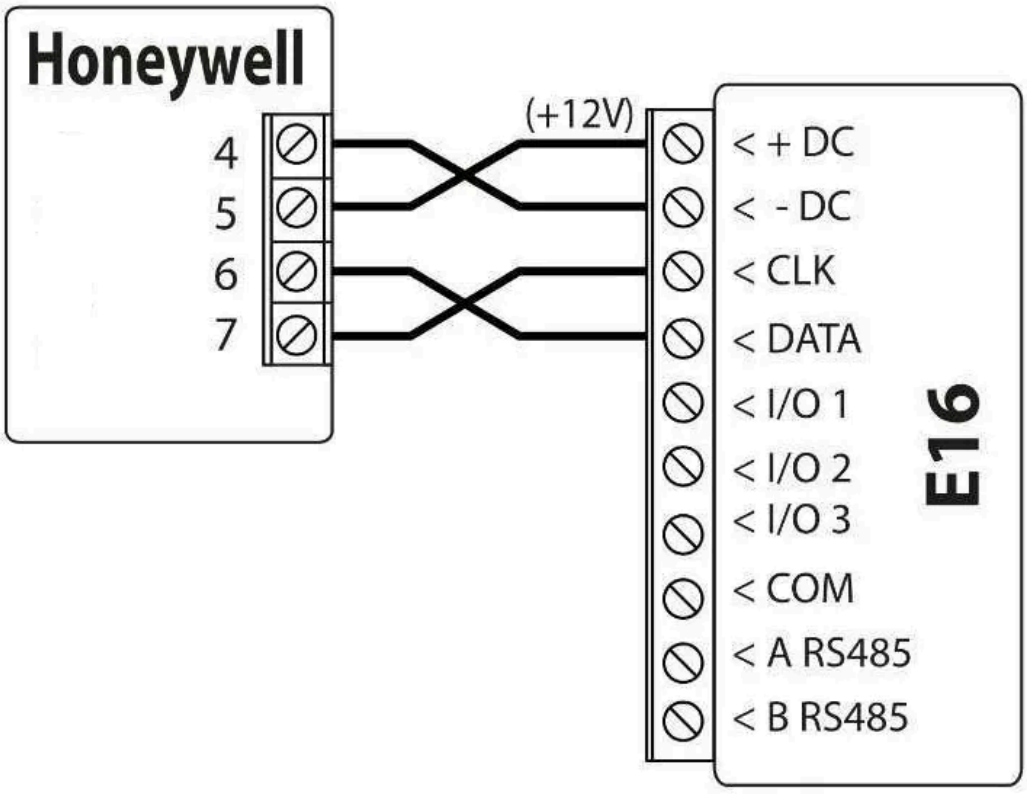


Figure 13. Raccordement au bus clavier d'une centrale Honeywell Vista-20 / Vista-48 (« Keypad bus ») : 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception et Integriti

Le communicateur est alimenté par les bornes d'alimentation de la centrale **Inception** (**VOUT +** → +DC, **0V** → −DC), et la liaison de données se fait depuis le port USB de la centrale, avec le câble InnerRange 993030USB : **noir** → 0V (−DC), **vert** → CLK, **blanc** → DATA. L'utilisation du port série doit être activée dans la centrale (section 4.7).

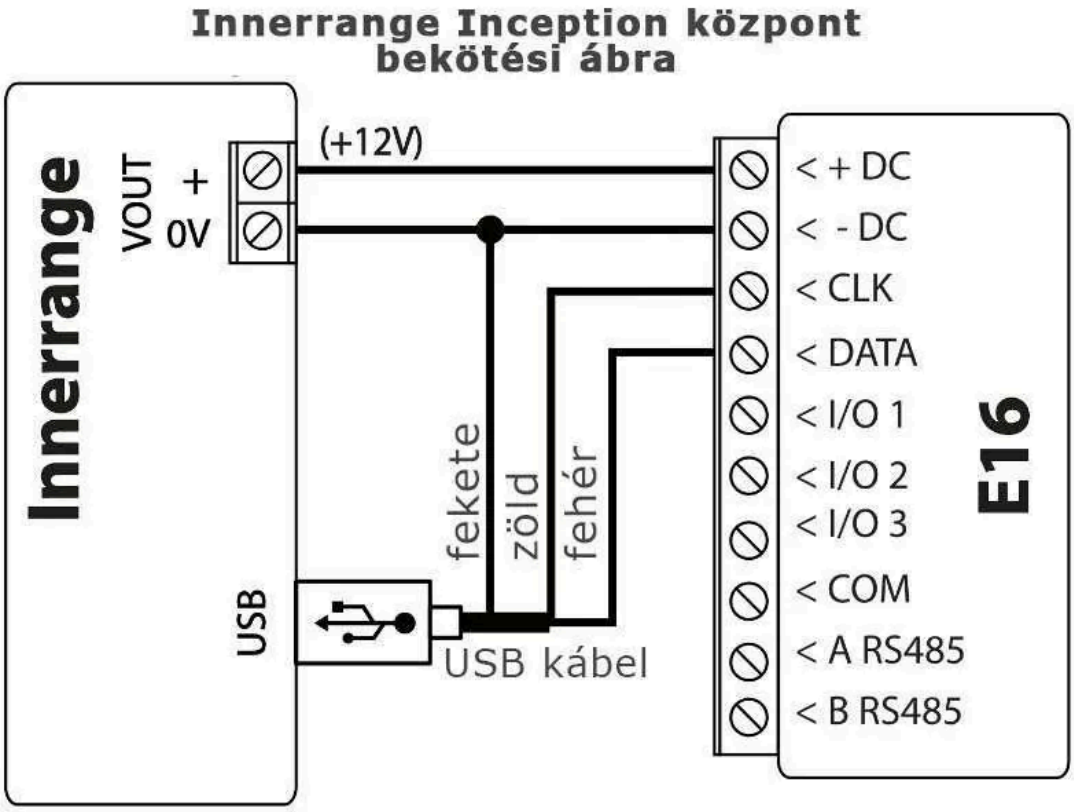


Figure 14. Raccordement à une centrale InnerRange Inception : alimentation depuis les bornes VOUT + et 0V, données depuis le port USB avec le câble 993030USB (noir → 0V, vert → CLK, blanc → DATA).

Sur la centrale **Integriti**, le raccordement se fait au port 0 (Port 0) avec le câble INTG-996795 : **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA. Le port série de la centrale doit être réglé sur le protocole Trikdis (section 4.7).

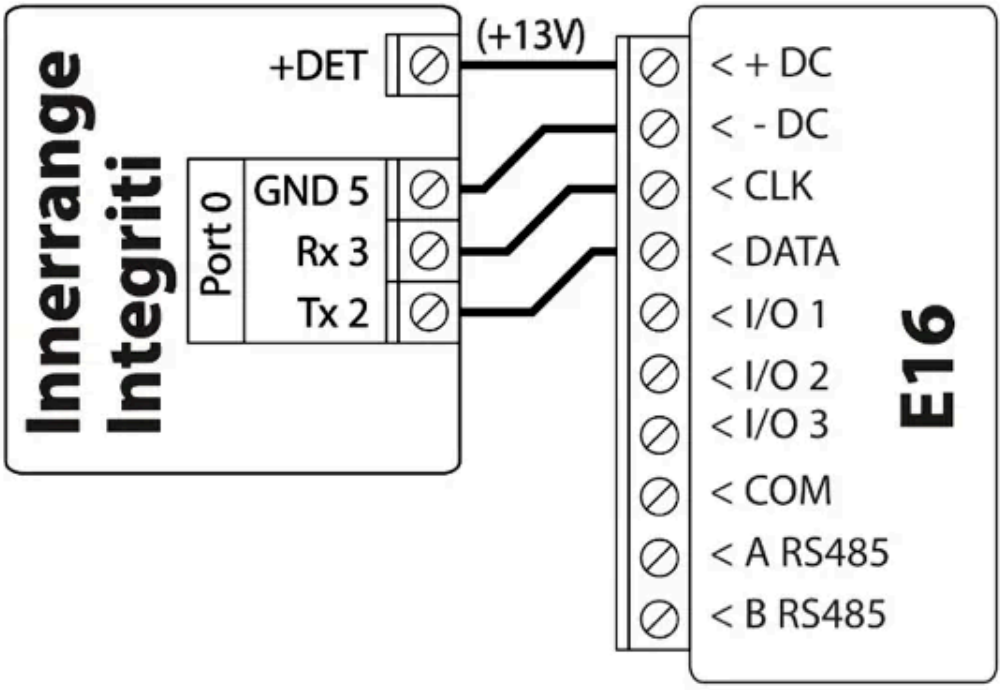


Figure 15. Raccordement à une centrale InnerRange Integriti avec le câble Inner Range référence INTG-996795 : +DET (+13 V) → +DC, Port 0 GND (5) → −DC, Rx (3) → CLK, Tx (2) → DATA.

3.4 Raccordement d'une zone à clé

Si la centrale ne fait pas partie des modèles à commande directe, ou si vous ne souhaitez pas utiliser la commande directe, l'armement et le désarmement à distance peuvent se faire par une **zone à clé** : vous configurez l'une des bornes I/O du communicateur **en sortie** (page IN/OUT, section 6.6) et la raccordez 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'E16 dispose de trois bornes I/O, jusqu'à trois partitions peuvent être gérées, chacune avec sa propre sortie.

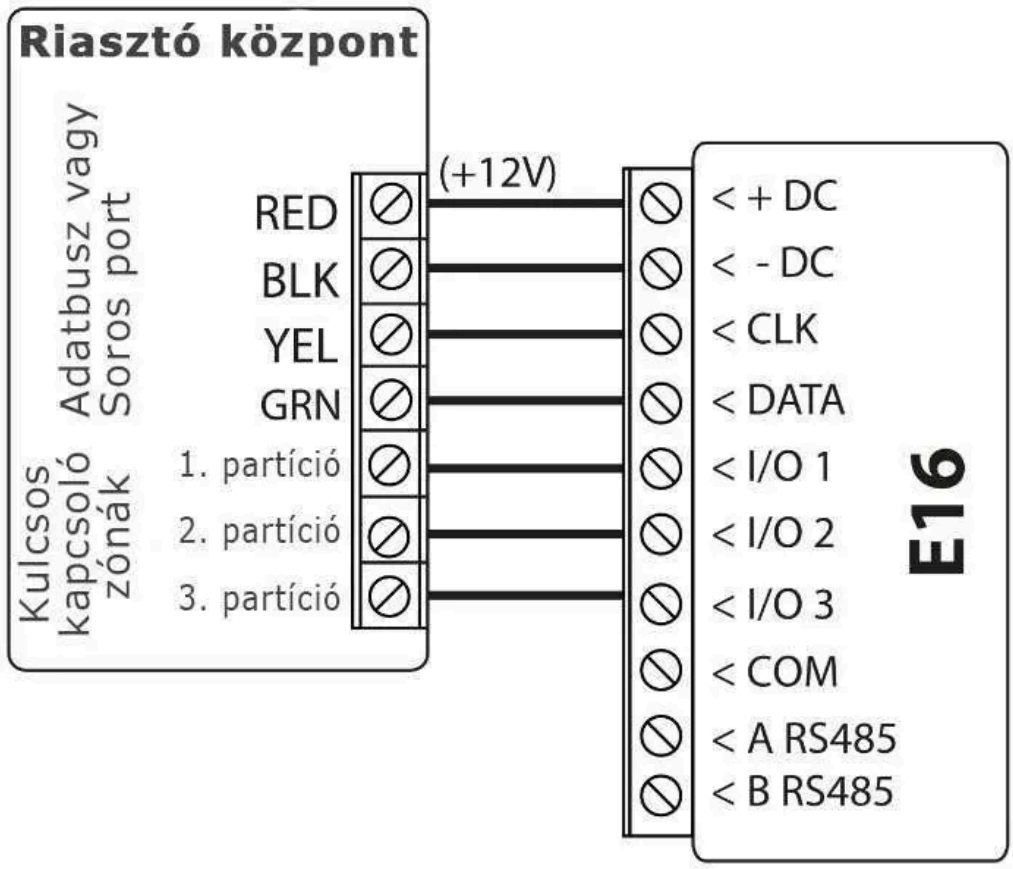


Figure 16. Armement et désarmement par zone à clé : le communicateur lit les événements sur le bus de la centrale, et les sorties I/O 1–3 commutent la zone à clé des partitions 1–3 de la centrale.

- Sur la page **System settings** de TrikdisConfig, **Remote Arm/Disarm** doit rester **décoché** – les deux ne peuvent pas être utilisés en même temps.
- La zone à clé peut être à impulsion ou bistable ; le même mode doit être réglé dans l'application Protegus 2 (section 5.3).

Un article distinct 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.

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 NO, NC, NC/EOL, NO/EOL, NO/DEOL et NC/DEOL avec résistance de fin de ligne de 2,2 kΩ ; pour les types DEOL, le circuit d'autoprotection est aussi raccordé.

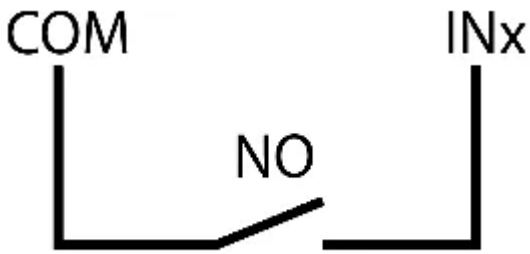


Figure 17. NO – circuit ouvert au repos : fermé – alarme, ouvert – état de repos.

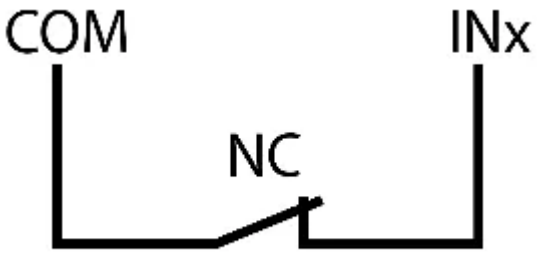


Figure 18. NC – circuit fermé au repos : ouvert – alarme, fermé – état de repos.

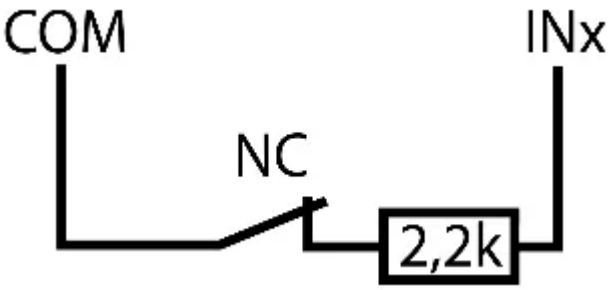


Figure 19. NC/EOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

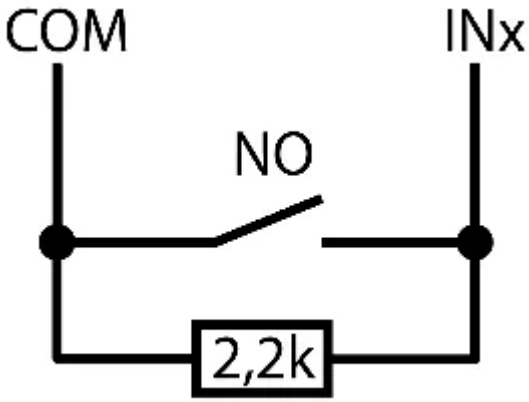


Figure 20. NO/EOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ : court-circuit ou coupure – alarme, 2,2 kΩ – état de repos.

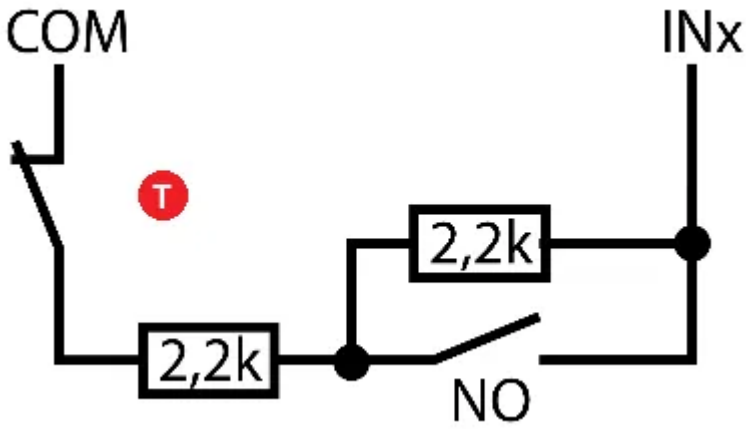


Figure 21. NO/DEOL – circuit ouvert au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – alarme, 3,3–5,5 kΩ – état de repos.

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

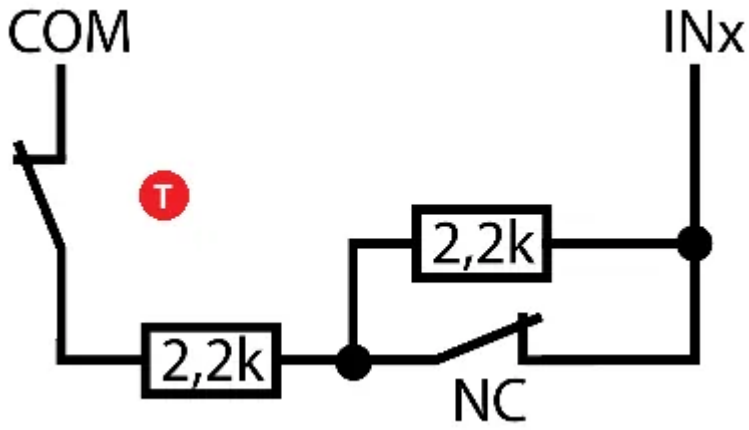


Figure 22. NC/DEOL – circuit fermé au repos avec résistance de fin de ligne de 2,2 kΩ et détection d'autoprotection : court-circuit ou coupure – autoprotection, 2,2 kΩ – état de repos, 3,3–5,5 kΩ – alarme.

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

3.6 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. Avec les contacts du relais, vous pouvez allumer et éteindre divers appareils électriques. 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. La borne I/O utilisée doit être configurée en sortie (**OUT**) sur la page **IN/OUT** de TrikdisConfig (section 6.6).

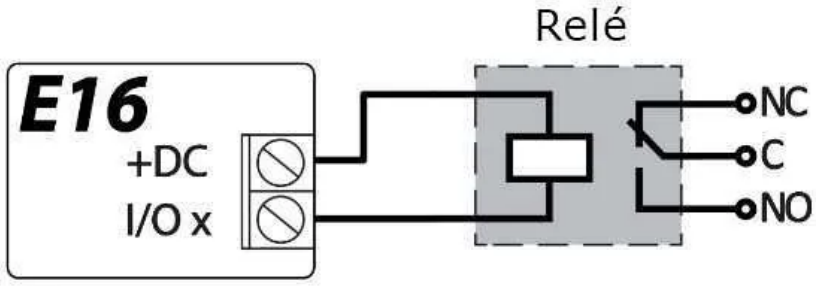


Figure 23. Raccordement d'un relais à la sortie du communicateur : la bobine se place entre +DC et la borne I/O x, les contacts (NC, C, NO) commutent le consommateur.

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

3.7 Raccordement du module d'extension iO-8

Si davantage d'entrées ou de sorties sont nécessaires, un module d'extension **iO-8** peut être raccordé au bus RS485 de l'E16 ; chacun ajoute 8 I/O à double fonction. Reliez les bornes A RS485 et B RS485 aux bornes A et B du module, et prenez l'alimentation du module sur la sortie AUX 12 V de la centrale. Le module doit être ajouté sur la page **RS485 modules** de TrikdisConfig (section 6.7) ; les événements des entrées partent vers la télésurveillance et vers Protegus 2, les sorties se commandent depuis l'application.

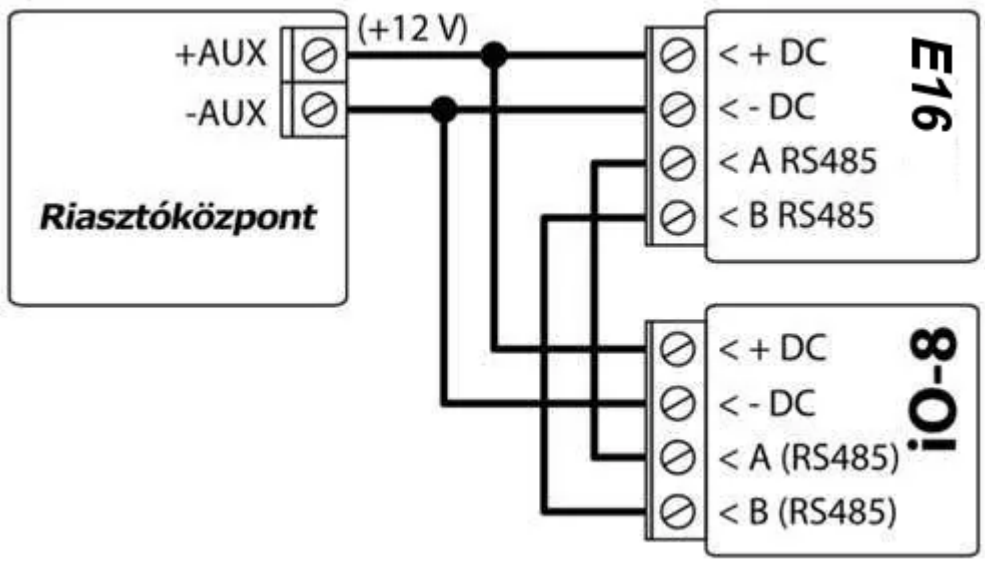


Figure 24. Raccordement du module d'extension iO-8 au bus RS485 de l'E16 (A RS485 → A, B RS485 → B) ; les deux appareils sont alimentés par la sortie AUX (+12 V) de la centrale d'alarme.

3.8 Raccordement du câble Ethernet

Branchez une extrémité du câble Ethernet dans la prise RJ45 du circuit imprimé de l'E16, 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 du boîtier. Après la mise sous tension, l'établissement de la connexion réseau est signalé par la lumière verte de la LED **NETWORK**.

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 en même temps que la centrale d'alarme est mise sous tension. Voici ce que vous devez voir sur la face avant :

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

Tout autre état des LED signale un défaut ; identifiez-en la cause à l'aide du tableau des LED de la section 1.6. Si TROUBLE clignote, le nombre de clignotements indique la cause (section 1.6) : 1 = pas de liaison physique (câble, port), 2 = pas d'adresse IP obtenue (DHCP), 3 = erreur DNS, 6 = le récepteur ou le cloud Protegus n'est

pas joignable. **7 clignotements** signalent l'absence de liaison avec la centrale : vérifiez les fils CLK et DATA, le type de centrale choisi et – si nécessaire – la programmation de la centrale (chapitre 4). Si aucune LED ne s'allume, vérifiez l'alimentation et le câblage.

4. Programmation de la centrale d'alarme

Ce chapitre décrit, par fabricant, ce qu'il faut régler dans la centrale d'alarme pour que l'E16 lise les événements et – quand c'est possible – commande la centrale à distance. Pour la plupart des centrales, rien n'est à programmer pour la lecture des événements ; pour la **commande directe**, cochez l'option **Remote Arm/Disarm** sur la page **System settings** de TrikdisConfig et, pour une centrale Paradox ou Texecom, indiquez aussi le mot de passe PC ou UDL de la centrale dans le champ **Security panel PC download password** (sections 2.2 et 6.2).

Si vous commandez la centrale non pas directement, mais par une zone à clé (section 3.4), **Remote Arm/Disarm** doit rester décoché, et ce chapitre ne concerne que les réglages nécessaires à la lecture des événements.

4.1 DSC

Les centrales **DSC PowerSeries** (liste des modèles pris en charge au point 1.2) ne nécessitent aucun réglage particulier : le communicateur raccordé au Keybus lit immédiatement les événements et, une fois **Remote Arm/Disarm** coché, l'utilisateur arme et désarme depuis l'application avec son propre code clavier. Les détails de la commande directe – états des zones, exclusion de zones, détection automatique des partitions – font l'objet d'un article séparé : Commande directe des centrales d'alarme DSC PowerSeries.

Le communicateur ne fonctionne pas avec les centrales **DSC PowerSeries NEO** : le fabricant de la centrale n'autorise aucun appareil externe sur le bus NEO. Pour une NEO, il faut un communicateur sur ligne téléphonique (TIP/RING) – voir DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions.

4.2 Paradox

Les centrales **Paradox** ne doivent être programmées que pour la commande directe ; aucun réglage n'est nécessaire pour la lecture des événements. Le firmware de la centrale doit être au moins en version **V.4**.

Sur les centrales Paradox plus récentes (par exemple les séries SP+, MG+ et EVOHD+), le port série peut être **verrouillé en usine** : le communicateur ne reçoit aucune donnée tant que le port n'est pas déverrouillé. Procédure de déverrouillage : Déverrouillage du port série verrouillé sur les centrales d'alarme Paradox.

Pour la commande, il faut régler le **mot de passe PC** (PC password) de la centrale et saisir le même dans le champ **System settings** → **Security panel PC download password** de TrikdisConfig – les deux doivent être identiques.

1. Entrez dans la programmation installateur de la centrale depuis le clavier.
2. Ouvrez la section du mot de passe PC : section **911** pour les séries **MAGELLAN et SPECTRA**, section **3012** pour la série **DIGIPLEX EVO**.
3. Saisissez un mot de passe de **4 caractères**. Le mot de passe ne peut pas être 0000 et **ne doit pas commencer par zéro**.
4. Quittez la programmation et **redémarrez la centrale** – la modification du mot de passe PC prend effet après le redémarrage. Saisissez ensuite le même mot de passe dans TrikdisConfig.

Erreurs fréquentes et solutions

- Le **code clavier attribué à la partition ne peut pas être le code maître** : donnez un autre code à l'utilisateur, et l'armement / le désarmement depuis Protegus 2 fonctionnera avec celui-ci.
- **Après toute modification d'un code clavier, redémarrez le communicateur** (coupure d'alimentation ou commande SMS `RESET`) : il lit les codes au démarrage et ne voit pas les modifications ultérieures.

4.3 Texecom

Les centrales **Texecom Premier / Premier Elite** doivent être programmées aussi bien pour la lecture des événements que pour la commande : il faut régler le mot de passe à 4 caractères de la centrale appelé **UDL passcode** et saisir le même dans le champ **System settings → Security panel PC download password** de TrikdisConfig – les deux doivent être identiques.

Avec le logiciel Wintex de Texecom : l'UDL passcode se trouve dans l'onglet **Options** de la fenêtre **Communication Options**.

Depuis le clavier :

1. Saisissez le code installateur à 4 chiffres et appuyez sur la touche **[Menu]** pour entrer dans le menu de programmation.
2. Appuyez immédiatement après sur la touche **[9]**.
3. Appuyez sur **[7][6]**, puis sur la touche **[2]**, et saisissez l'UDL passcode à 4 chiffres.
4. Appuyez sur la touche **[Yes]**, puis quittez la programmation avec la touche **[Menu]**.

4.4 UTC Interlogix (Caddx)

Le firmware de la centrale **UTC Interlogix (Caddx) NetworX** doit être au moins en version **V2**. Les réglages suivants se font sur le clavier de la centrale :

1. Appuyez sur les touches **[*][8]** et saisissez le code installateur (en usine **9713**).
2. Saisissez le **numéro d'appareil** attribué au communicateur (device address ; en usine **0**).
3. Programmez l'une après l'autre les lignes du tableau ci-dessous : saisissez l'emplacement (location), le numéro de segment, puis le réglage. La touche **[*]** permet de revenir au champ précédent. `12345678` signifie que les huit interrupteurs du segment sont activés (tous les chiffres sont visibles à l'écran).

Emplacement (location)	Segment	Réglage
23	3	12345678
37 (pas forcément nécessaire)	3	12345678
37 (pas forcément nécessaire)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678

Emplacement (location)	Segment	Réglage
108	3	12345678

4. Une fois toutes les lignes programmées, appuyez deux fois sur la touche **[Exit]** pour quitter la programmation.

4.5 Crow et Pyronix

Les centrales **Crow Runner 4/8** et **Runner 8/16** ne nécessitent aucun réglage particulier.

Les centrales **Pyronix** ne nécessitent pas non plus de programmation, mais après le réglage et le raccordement du communicateur, **mettez la centrale hors tension** (secteur et batterie) et redémarrez-la : la centrale accepte au démarrage le communicateur raccordé à son bus.

4.6 Honeywell Ademco Vista

Le firmware des centrales **Honeywell Ademco Vista-20** et **Vista-48** doit être au moins en version **V5.3**. Le réglage se fait sur le clavier de la centrale.

Accès à la programmation – de deux façons :

- saisissez le code installateur (en usine **4112**), puis les touches **[8][0][0]** ; ou
- mettez la centrale sous tension et, **dans les 50 secondes**, appuyez simultanément sur les touches **[*]** et **[#]** (cela ne fonctionne que si l'on a quitté la programmation précédente avec les touches [*][9][8]).

Réglages :

1. Activez l'envoi des événements Contact ID sur la sortie radio longue portée (LRR) : appuyez sur les touches **[*][2][9][1][#]**.
2. Pour la commande à distance, autorisez l'utilisation de la **2e adresse AUI** (2nd AUI address) : appuyez sur les touches **[*][1][8][9][1][1][#]**.

Sortie de la programmation : appuyez sur les touches **[*][9][9]**.

4.7 InnerRange Inception et Integriti

Le firmware de la centrale **InnerRange Inception** doit être au moins en version **2.3.0.3507-r0**, et la centrale a besoin d'une connexion Internet. Le réglage se fait dans l'interface web de la centrale :

1. Ouvrez dans un navigateur l'adresse `https://skytunnel.com.au/inception/NUMERODESERIE`, où NUMERODESERIE est le numéro de série figurant sur la boîte de la centrale. Connectez-vous avec le compte installateur.
2. Ouvrez la page **Configuration** → **General** → **Alarm Reporting**.
3. Dans le groupe **3rd Party Device Configuration** : - cochez l'option **Enable 3rd Party Device Reporting** ; - dans le champ **3rd Party Device Type**, choisissez la valeur **Trikdis** ; - dans le champ **Serial Port**, choisissez la valeur **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Enregistrez les réglages et quittez l'interface.

Le firmware de la centrale **InnerRange Integriti** doit être au moins en version **19.1.0.36608**, et son logiciel de programmation (Integriti Professional) au moins en version **19.1.0.15396**. Le réglage se fait dans le logiciel de programmation de la centrale :

1. Pour le port série (**TTL Port-0**) auquel le communicateur est raccordé, choisissez le protocole de communication **Trikdis**.
2. Le format de données doit être **Contact ID**.
3. Réglage du port : **19200, 8, N, 1**.
4. Enregistrez les réglages et quittez le logiciel.

Inception et Integriti transmettent les événements au communicateur ; pour l'armement et le désarmement, une zone à clé est nécessaire (sections 1.2 et 3.4).

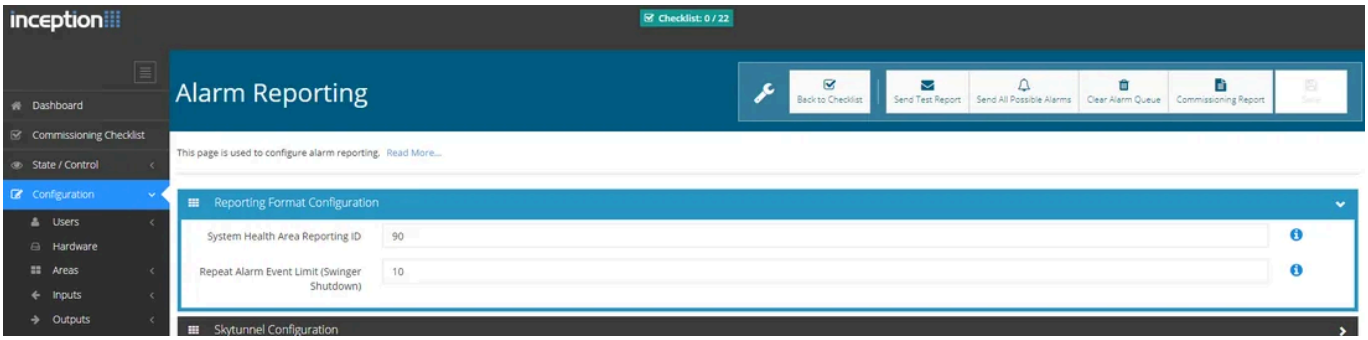


Figure 25. Interface web Inception – Configuration → General → Alarm Reporting.



Figure 26. Inception – 3rd Party Device Configuration.

- 1 **Enable 3rd Party Device Reporting** – coché.
- 2 **3rd Party Device Type** – Trikdis.
- 3 **Serial Port** – Serial Port 1 (Plugged In, In Use By 3rd Party Device).

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. Sur l'E16, l'armement peut se faire de deux façons : sur les centrales **à commande directe**, l'utilisateur utilise son propre **code clavier** ; sur les centrales raccordées par zone à clé, c'est la **sortie** du communicateur qui agit.

5.1 Ajout de l'appareil

Avant d'ajouter l'appareil, vérifiez :

1. L'E16 est connecté au réseau et accède à Internet : la LED **NETWORK** est allumée en vert, la LED **TROUBLE** ne clignote pas.
2. Sur la page **User reporting** → **PROTEGUS Cloud** de TrikdisConfig, **Enable connection** est coché 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.

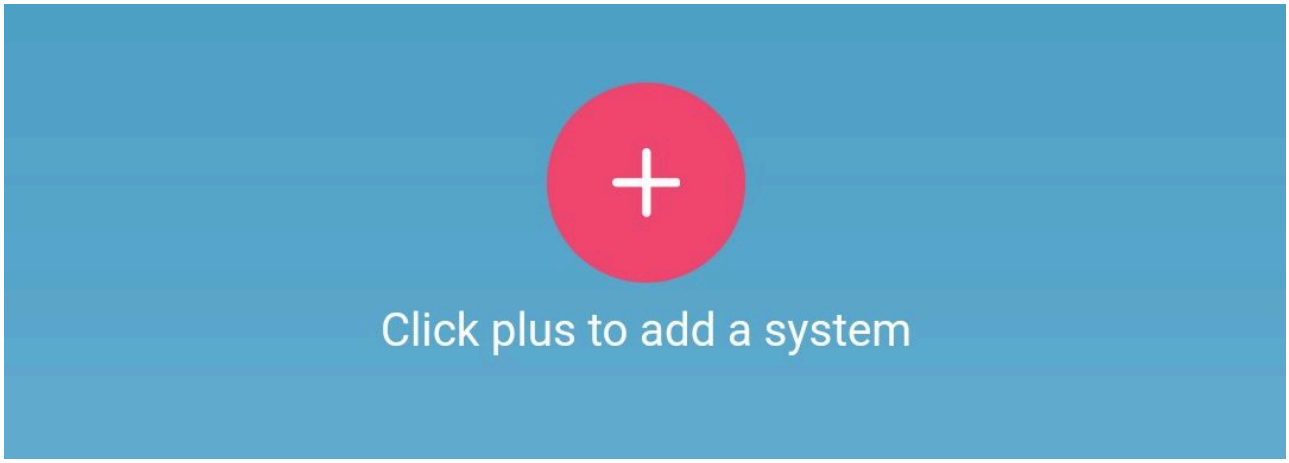
La LED DATA est le moyen le plus simple de vérifier l'accès à Internet. La LED DATA est allumée lorsque la mémoire de l'appareil contient un message en attente d'envoi. Le vert de la LED NETWORK indique seulement que la connexion réseau est établie – pour un appareil mobile, qu'il s'est enregistré sur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



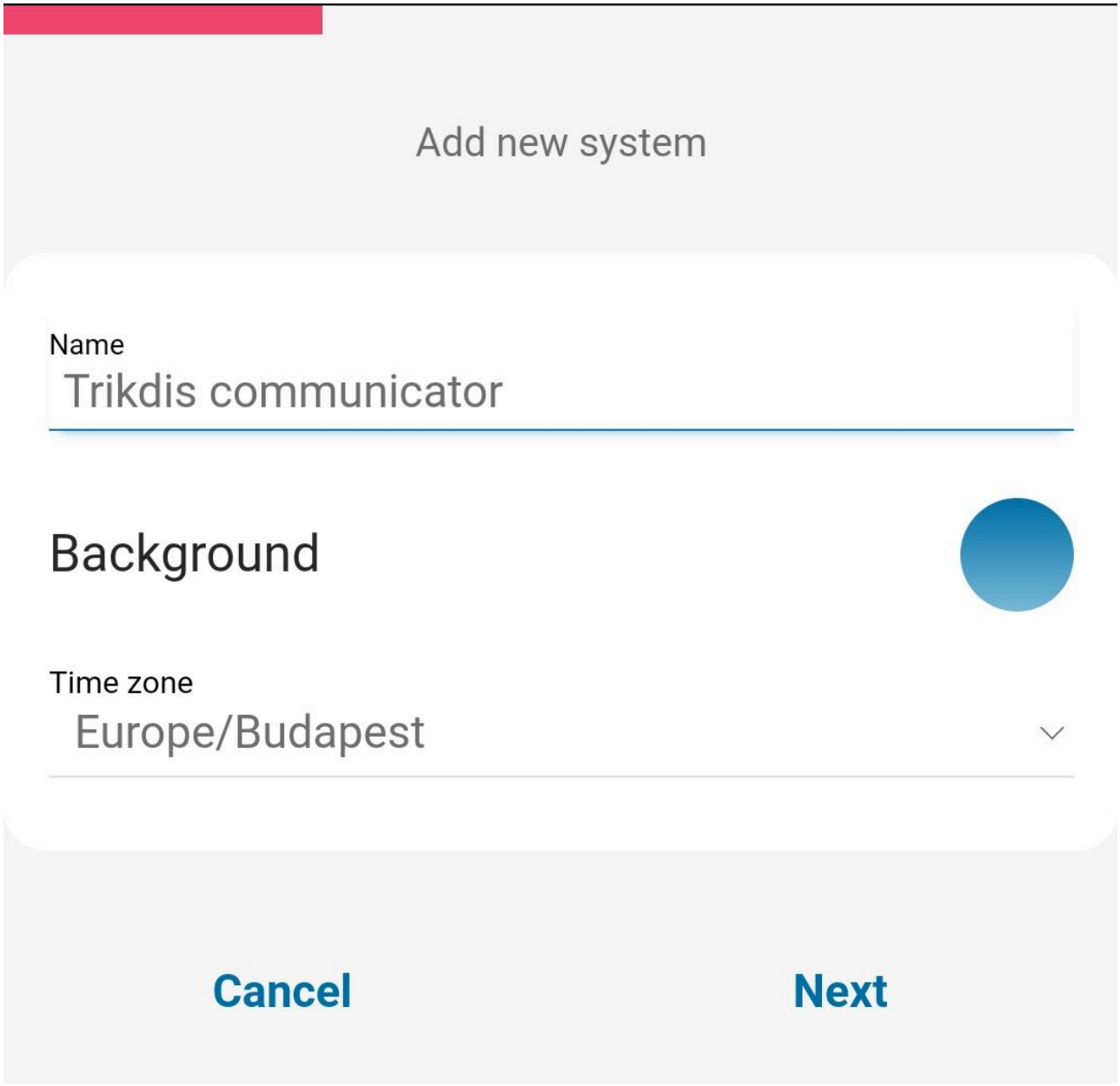
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



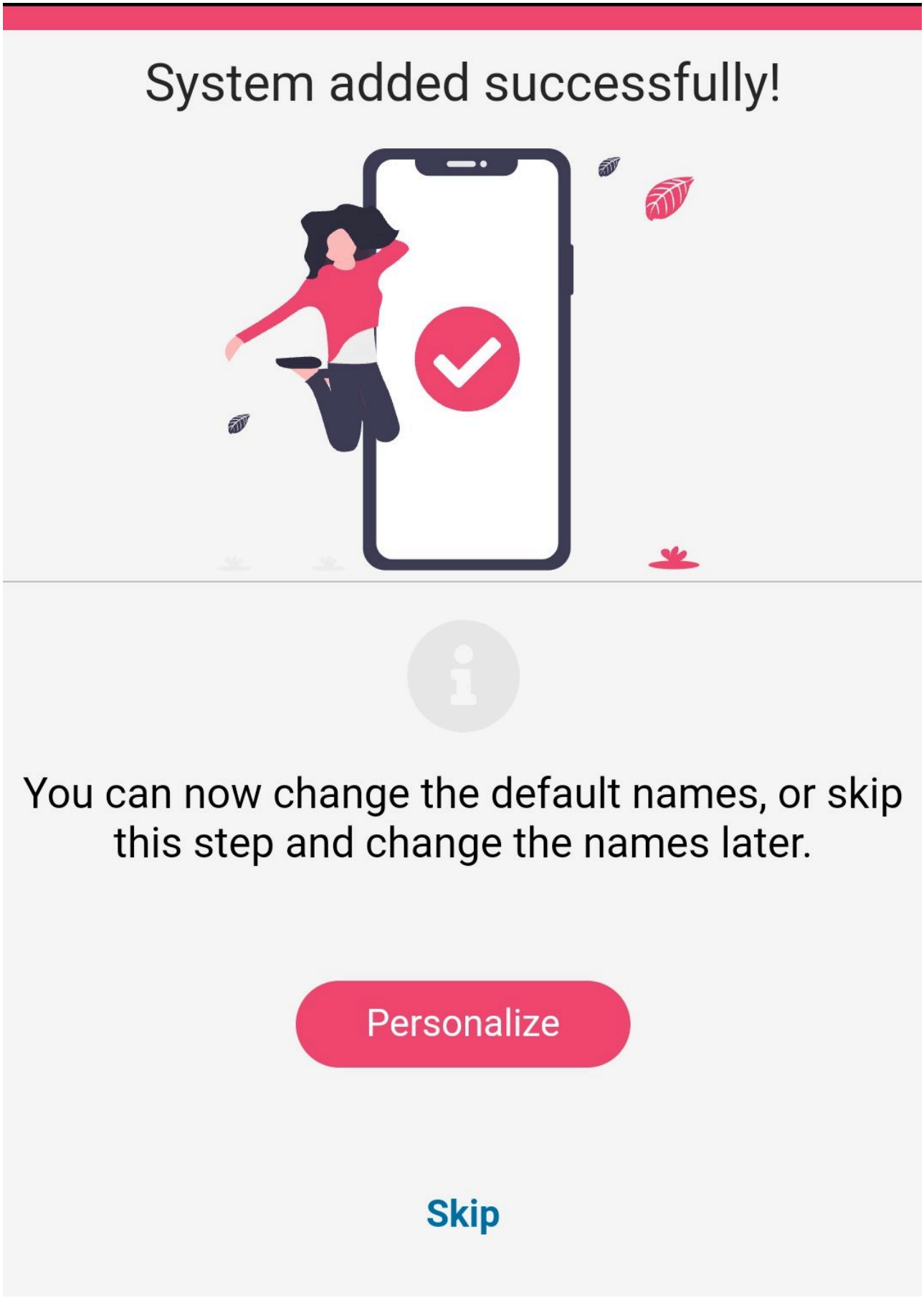
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



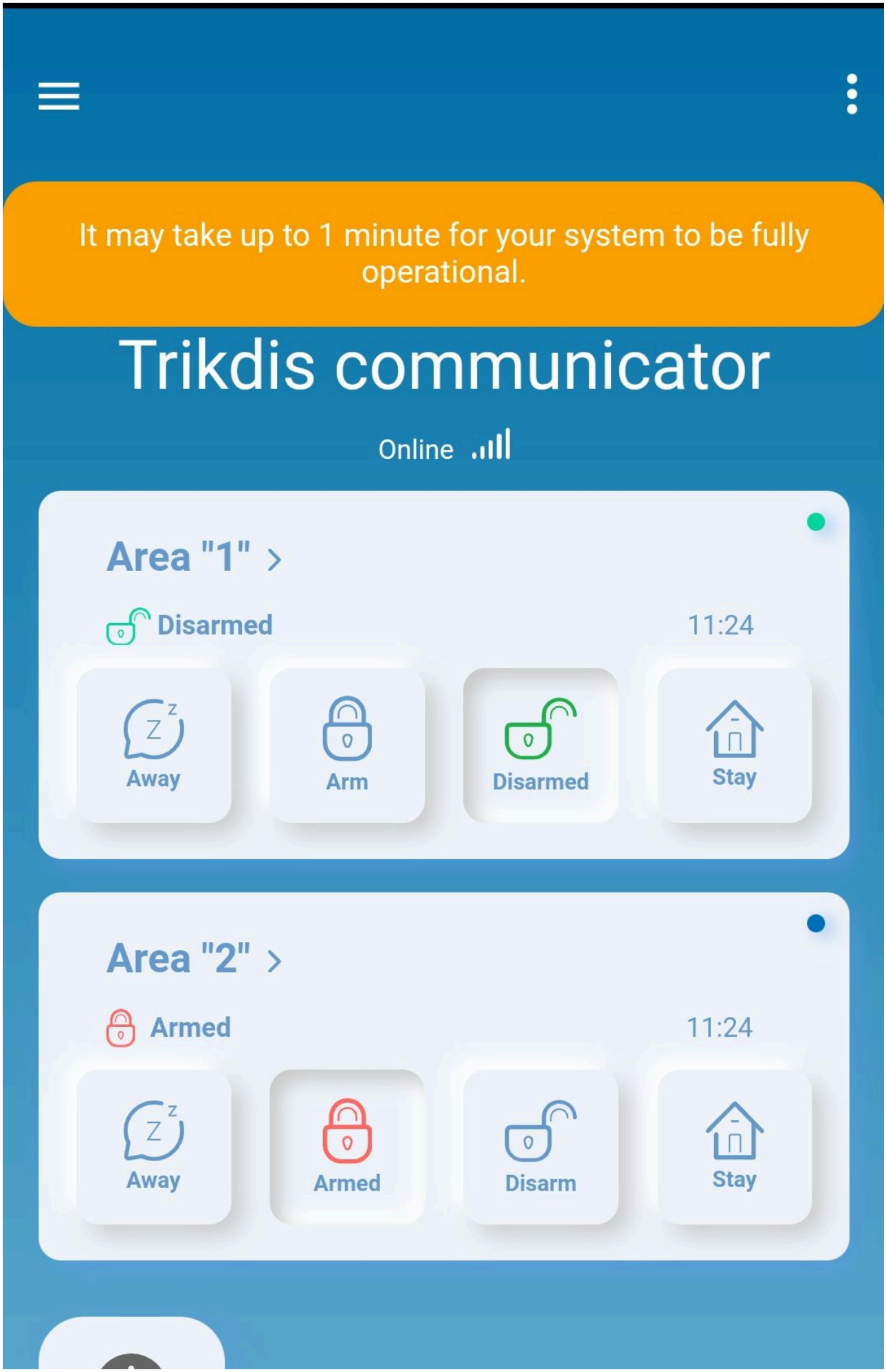
6. Add meg a rendszer nevét és válassz idozónát



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'E16, l'identifiant unique de l'appareil est l'**adresse MAC (Unique ID)** : elle figure sur la boîte et au dos de l'appareil, et la barre d'état de TrikdisConfig l'affiche aussi (section 6.1). C'est elle qu'il faut saisir comme identifiant de l'appareil lors de la création du système dans l'application.

5.2 Commande directe avec le code clavier

Si la centrale fait partie des modèles à commande directe (section 1.2) et que **Remote Arm/Disarm** est coché sur la page **System settings** de TrikdisConfig, Protegus 2 affiche les partitions de la centrale avec l'état lu sur le bus, et pour l'armement / le désarmement, l'utilisateur saisit dans l'application **le code clavier de la centrale** – le même que celui qu'il utilise sur le clavier. Ni sortie séparée ni zone à clé ne sont nécessaires.

- Selon le fabricant, un réglage est nécessaire pour cela dans la centrale (Paradox : mot de passe PC, Texecom : mot de passe UDL ; pour les centrales Caddx, Honeywell et InnerRange, l'activation du bus ou du port série, déjà nécessaire à la lecture des événements) – voir le chapitre 4.
- Le code clavier est vérifié par la centrale, et le journal d'événements de la centrale enregistre l'utilisateur, pas le communicateur.
- Sur une centrale Paradox, le code de l'utilisateur **ne peut pas être le code maître** ; après une modification de code, redémarrez le communicateur (section 4.2).
- Sur une centrale DSC PowerSeries, l'application affiche aussi l'état des zones, et l'exclusion de zones est possible – détails dans l'article sur la commande directe DSC (l'article porte sur le G16, mais il s'applique de la même façon à l'E16).

Lors de la création du système, Protegus 2 demande si l'armement est commandé par une sortie du communicateur. En commande directe, **n'attribuez pas** de sortie à la partition (**Control with Protegus2** désactivé) : la partition est gérée par la centrale, l'état arrive par le bus.

5.3 Armement par zone à clé

Si la centrale ne peut pas être commandée directement, ou si vous ne souhaitez pas l'utiliser ainsi, vous raccordez l'une des sorties du communicateur à la zone à clé de la centrale (section 3.4), **Remote Arm/Disarm** reste décoché dans TrikdisConfig, et dans Protegus 2 vous attribuez la sortie à la partition.

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.

5.4 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.

En commande directe, l'application demande le code clavier de la centrale ; en armement par zone à clé – s'il est activé – le mot de passe Protegus 2.

L'E16 n'a ni commande par SMS ni notification par SMS : l'armement, le désarmement et la commande des sorties se font depuis l'application Protegus 2, et les notifications arrivent par message push.

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'E16, 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 27. La barre d'état de TrikdisConfig avec un E16 lu : adresse MAC (Unique ID, laissée vide sur l'image), état, type (E16_1100), numéro de série, versions, mode de connexion et niveau d'accès.

Sur l'E16, l'identifiant unique de l'appareil est l'**adresse MAC** : c'est elle que demande Protegus 2 lors de la création du système, et TrikdisConfig pour l'accès à distance (Unique ID). Cette même adresse figure aussi sur la boîte et au dos de l'appareil.

6.2 System settings

La page comporte deux groupes : dans le groupe **General**, vous réglez le fonctionnement de base de l'appareil et sa liaison avec la centrale d'alarme ; dans le groupe **Access**, les niveaux d'accès.

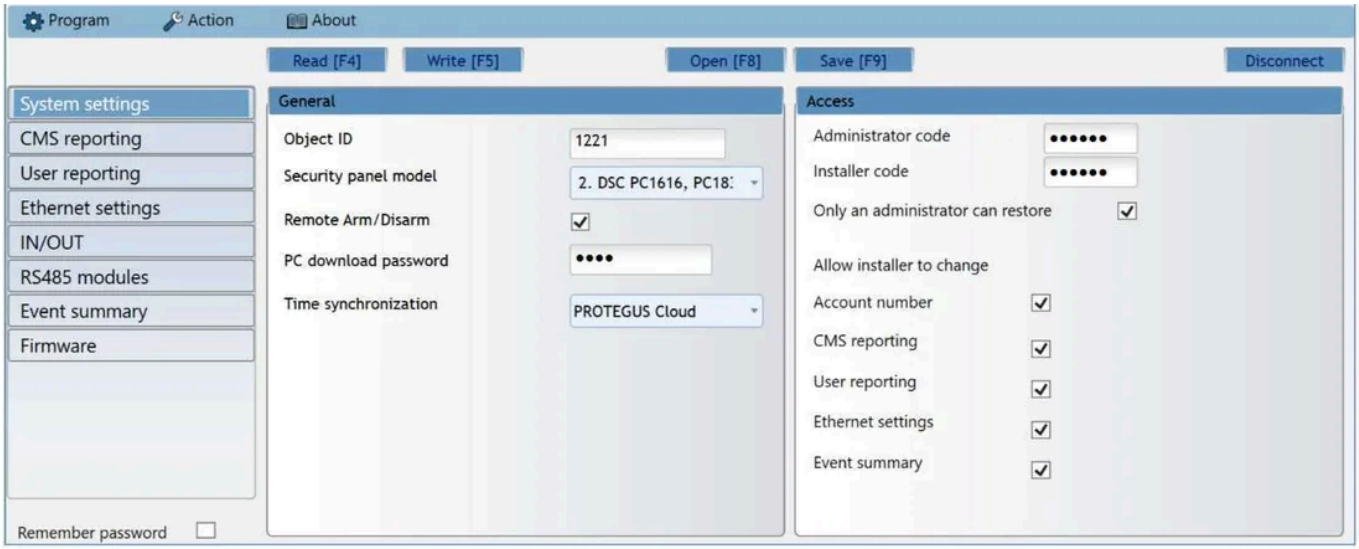


Figure 28. TrikdisConfig – page System settings : groupes General et Access.

- **Object ID** – l'identifiant d'objet fourni par le centre de télésurveillance (4 caractères hexadécimaux, 0–9, A–F). Obligatoire si l'appareil transmet aussi à un centre de télésurveillance ; `FFFE` et `FFFF` ne peuvent pas être utilisés.
- **Security panel model** – le type de la centrale d'alarme raccordée, à choisir dans la liste. C'est de lui que dépend la façon dont le communicateur lit le bus ; choisissez donc le type exact de la centrale raccordée.
- **Remote Arm/Disarm** – coché, le communicateur commande directement la centrale : l'utilisateur arme et désarme depuis Protegus 2 avec son code clavier. Il n'apparaît que pour les types de centrales à commande directe ; selon le fabricant, un réglage est nécessaire dans la centrale (chapitre 4). Pour l'armement par zone à clé, laissez-le décoché.
- **Security panel PC download password** – pour la commande directe d'une centrale Paradox ou Texecom, le mot de passe PC ou UDL de la centrale (4 caractères) ; il doit être identique à celui configuré dans la centrale (sections 4.2 et 4.3).
- **Time synchronization** – la source de l'horloge de l'appareil (par défaut **PROTEGUS Cloud**, le cloud Protegus).

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.

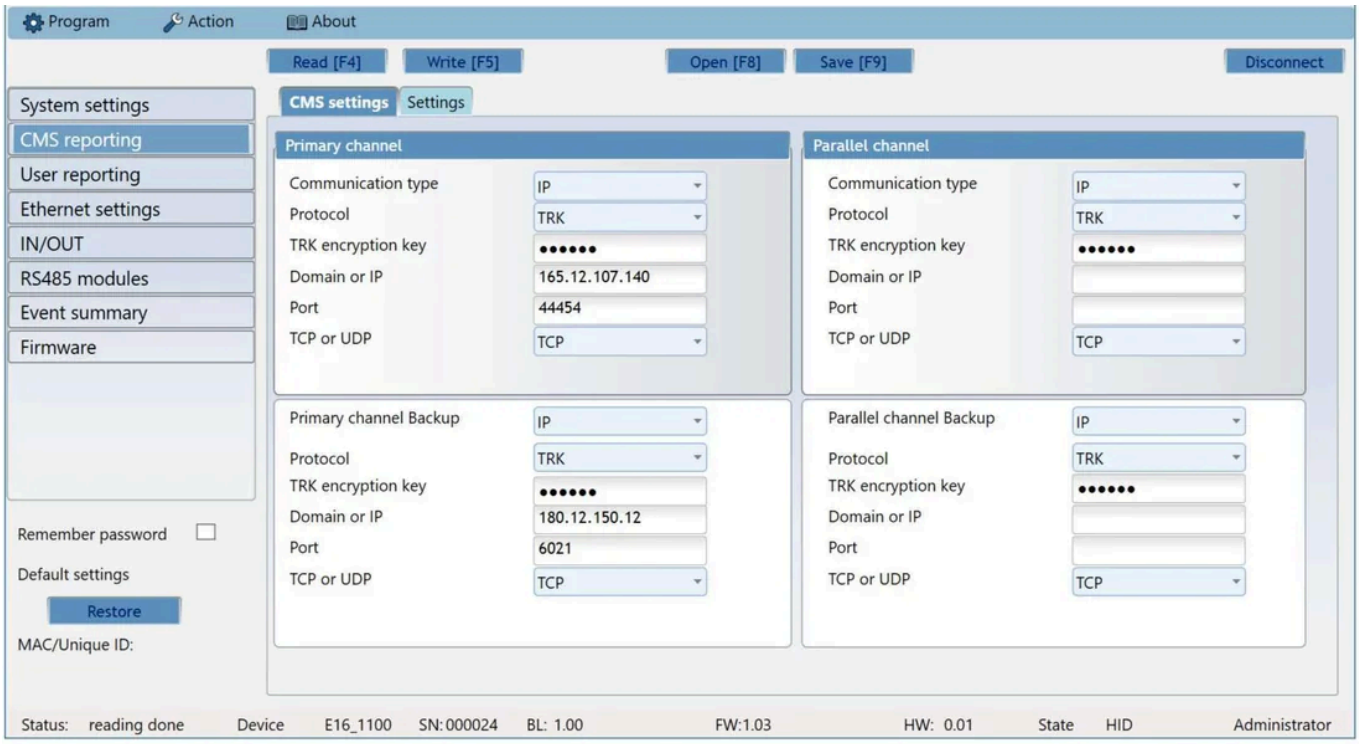


Figure 29. TrikdisConfig – CMS reporting, onglet CMS settings : canal principal et canal parallèle (en haut), les canaux de secours correspondants (en bas).

Primary channel – canal principal

- **Communication type** – **IP** ; avec la valeur **Disable**, le canal peut être désactivé (par exemple si l'appareil fonctionne uniquement avec Protegus 2, sans télésurveillance).
- **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 et le port du récepteur.
- **TCP or UDP** – le protocole de transport.

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. Comme l'E16 communique par une seule voie réseau (le réseau local), le canal de secours est une seconde adresse de récepteur sur cette même voie : il pallie une panne côté récepteur, mais pas la perte de la connexion Internet.

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.



Figure 30. TrikdisConfig – CMS reporting, onglet Settings : rapport de test, PING, temporisations du canal de secours et données DC-09.

Sur l'onglet **Settings**, vous réglez les temporisations et les données DC-09.

- **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.

Le groupe **DC-09 settings** n'est visible que si le protocole DC-09 est réglé sur l'un des canaux. Sur l'E16, les serveurs de noms (DNS) ne se saisissent pas ici, mais sur la page **Ethernet settings** (section 6.5).

6.4 User reporting

Sur l'onglet **PROTEGUS Cloud**, vous activez le service Protegus, qui permet à l'utilisateur de surveiller et de commander le communicateur à distance ; plus d'informations sur le service : www.protegus.app. L'E16 n'a ni notification ni commande par SMS ; cette page ne comporte donc que cet onglet.

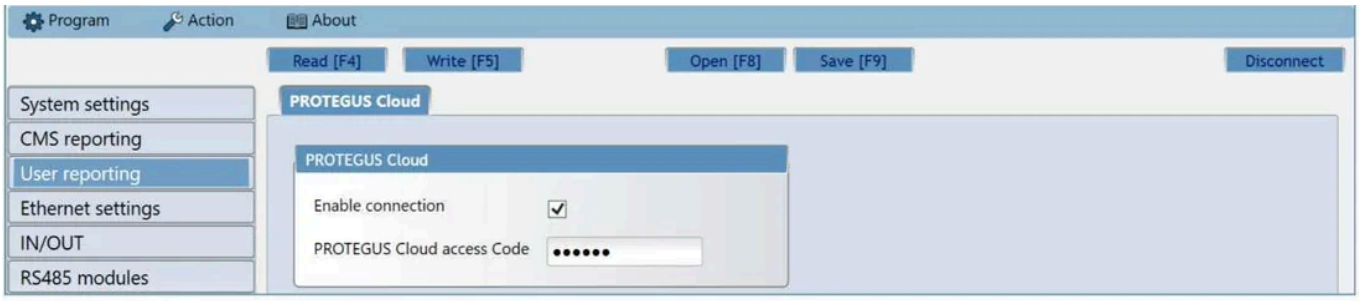


Figure 31. TrikdisConfig – User reporting, onglet PROTEGUS Cloud.

- **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). 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 réglez la façon dont l'E16 se connecte au réseau local. En usine, **Use DHCP** est coché : l'appareil obtient automatiquement du routeur l'adresse, la passerelle et les serveurs de noms, et dans la plupart des cas il n'y a rien d'autre à faire.



Figure 32. TrikdisConfig – page Ethernet settings : configuration réseau DHCP ou manuelle, serveurs de noms.

- **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.

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). Réglage d'usine : I/O 1 et I/O 2 en entrée (NO), I/O 3 en sortie.

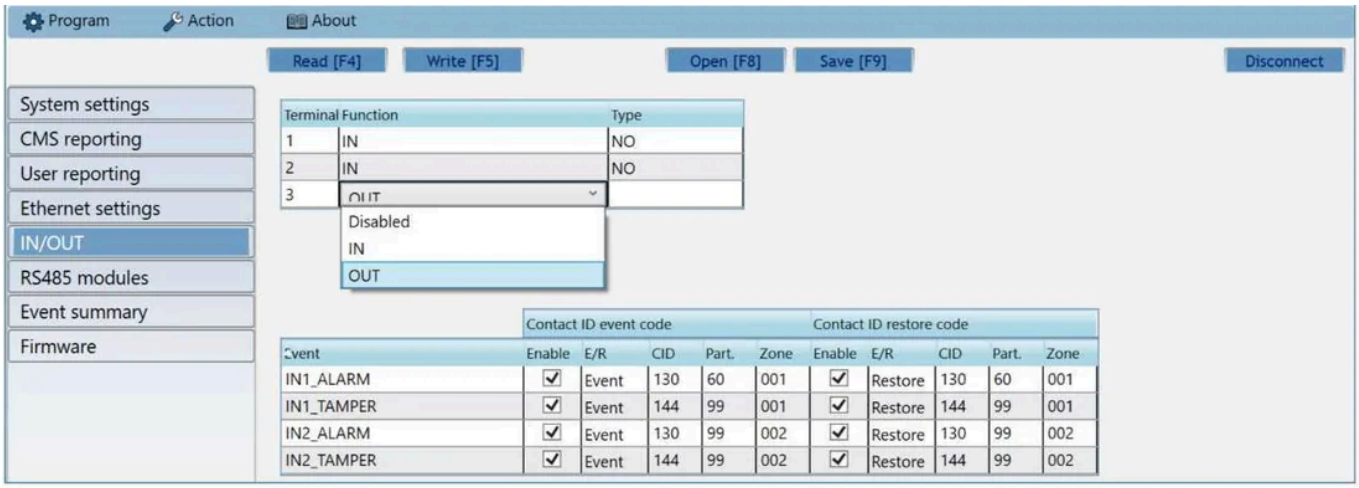


Figure 33. TrikdisConfig – page IN/OUT : fonction des bornes I/O et événements des entrées.

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 ; vous pouvez le saisir ou conserver la valeur par défaut. L'événement part avec ce code vers Protegus 2 et le centre de télésurveillance.
- **Part.** – le numéro de partition dans le message.
- **Zone** – le numéro de zone dans le message.

6.7 RS485 modules

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

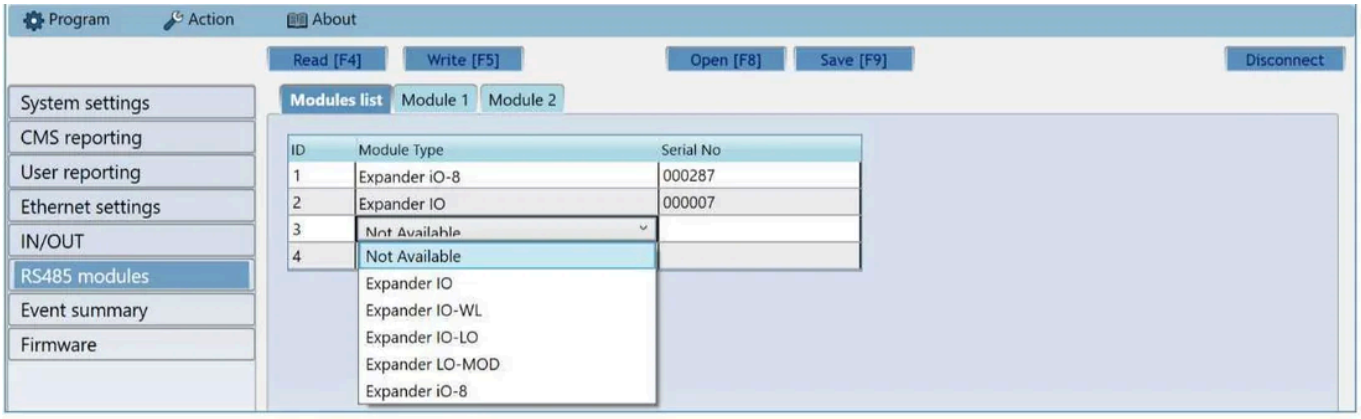


Figure 34. TrikdisConfig – RS485 modules, onglet Modules list : type du module (Expander iO-8) et numéro de série.

- **Module Type** – le type du module raccordé, à choisir dans la liste (**Expander iO-8**).
- **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.

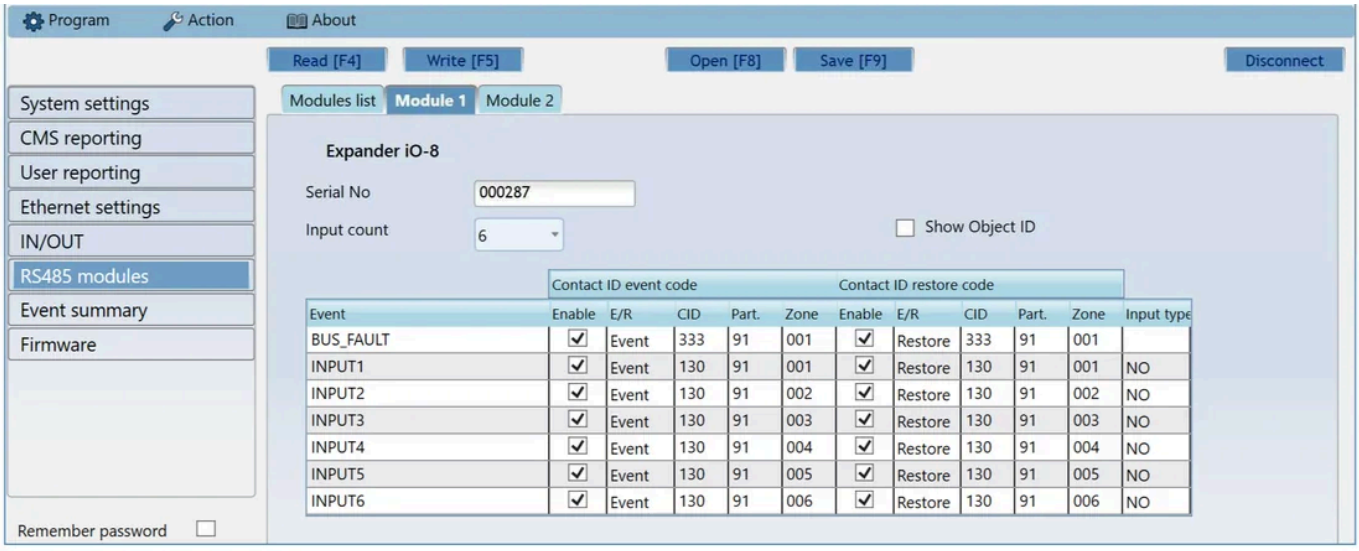


Figure 35. TrikdisConfig – RS485 modules, onglet du module iO-8 (en haut) et tableau des événements du module d'extension (en bas).

- **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 par zone à clé 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**.

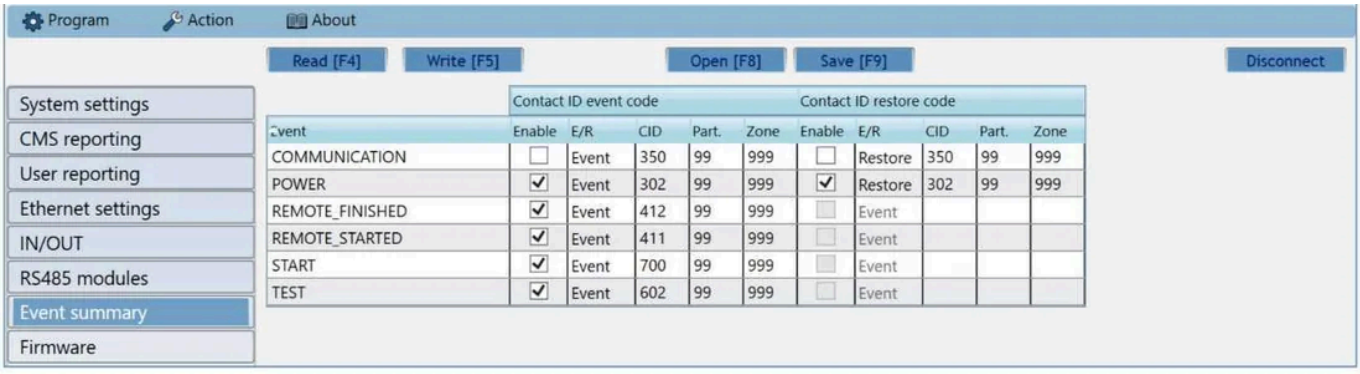


Figure 36. TrikdisConfig – page Event summary : messages internes de l'appareil (COMMUNICATION, POWER, REMOTE_FINISHED, REMOTE_STARTED, START, TEST) et les codes Contact ID correspondants.

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.

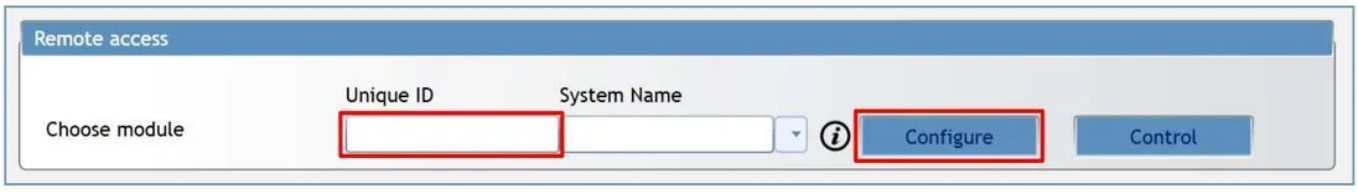


Figure 37. TrikdisConfig – Remote access : identifiant de l'appareil (Unique ID – sur l'E16, l'adresse MAC), nom du système et bouton Configure.

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.

Avec une centrale raccordée au bus, vérifiez aussi que le communicateur lit bien la centrale : armez et désarmez la centrale au clavier, et regardez si, dans la liste des événements de Protegus 2 (et au centre de télésurveillance), l'événement apparaît avec le bon numéro de partition et d'utilisateur. En commande directe, faites aussi un essai d'armement depuis l'application, avec le code clavier de l'utilisateur.

Vérifiez aussi le comportement en cas de perte du réseau : débranchez le câble Ethernet et regardez si la LED TROUBLE signale l'absence par 1 clignotement, puis, après rebranchement, si la LED NETWORK se rallume en vert et si les événements mémorisés arrivent au centre de télésurveillance et dans l'application.

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.

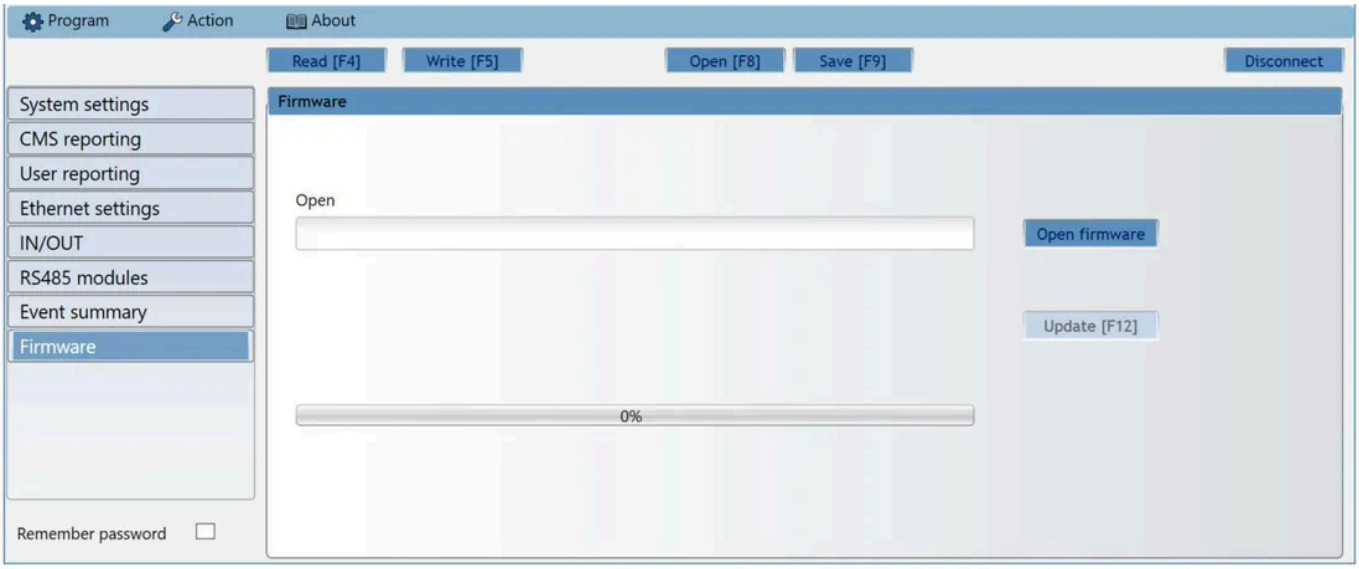


Figure 38. TrikdisConfig – page Firmware : Open firmware et Update [F12] (en haut), indicateur de progression de la mise à jour (en bas).

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, modifiez les paramètres de l'antivirus, ou 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 (câble, port), 2 = pas d'adresse IP obtenue (DHCP), 3 = impossible de résoudre le nom du récepteur ou du cloud Protegus (DNS).
2. **1 clignotement :** vérifiez le câble Ethernet à ses deux extrémités, et que le port du routeur ou du switch est actif (la LED du port est allumée) ; essayez un autre port ou un autre câble.
3. **2 clignotements :** le DHCP doit être activé sur le routeur, ou donnez à l'appareil une adresse IP fixe sur la page **Ethernet settings** (section 6.5). Sur un réseau d'entreprise, l'administrateur système peut autoriser l'appareil d'après son adresse MAC.
4. **3 clignotements :** le serveur de noms n'est pas joignable. En usine, c'est le DNS public de Google qui est configuré ; si le réseau interdit les DNS externes, saisissez le serveur de noms local sur la page **Ethernet settings**.

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. Sur un réseau filtré par un pare-feu, le trafic TCP/UDP sortant vers le port du récepteur doit être autorisé ; il n'est pas nécessaire d'ouvrir de port (entrant) sur le routeur.

La LED TROUBLE clignote sept fois – le communicateur ne voit pas la centrale

1. Vérifiez le raccordement d'après le schéma de la section 3.3 : l'erreur la plus fréquente est l'inversion des fils **CLK** et **DATA**, ou une ligne de données raccordée à la mauvaise borne de la centrale.
2. Le type exact de la centrale raccordée doit être sélectionné dans le champ **System settings** → **Security panel model** de TrikdisConfig.
3. Pour les centrales Texecom, Caddx, Honeywell et InnerRange, un réglage est aussi nécessaire dans la centrale (chapitre 4) – sans lui, la centrale ne fournit pas de données sur le bus.
4. Sur une centrale Paradox, le port série est peut-être verrouillé en usine – voici comment le déverrouiller.
5. Après le raccordement, mettez une centrale Pyronix hors tension puis redémarrez-la pour qu'elle accepte le communicateur.
6. L'E16 ne fonctionne pas avec une centrale DSC PowerSeries **NEO** (elle n'autorise pas d'appareil externe sur son bus) – il faut ici un communicateur sur ligne téléphonique (E16T).

Les événements arrivent, mais je ne peux pas armer depuis l'application

En commande directe :

1. **Remote Arm/Disarm** doit être coché sur la page **System settings**.
2. Pour une centrale Paradox ou Texecom, le **Security panel PC download password** doit correspondre au mot de passe PC ou UDL de la centrale (sections 4.2 et 4.3).
3. Sur une centrale Paradox, le firmware de la centrale doit être au moins en **V.4** ; le code de l'utilisateur ne doit pas être le code maître ; après une modification de code, redémarrez le communicateur.
4. Sur une centrale Honeywell Vista, l'adresse AUI 2 doit être activée (section 4.6).
5. Dans Protegus 2, **aucune** sortie ne doit être attribuée à la partition (Control with Protegus2 désactivé).

Avec une zone à clé :

1. **Remote Arm/Disarm** doit être décoché, et la borne I/O doit être réglée sur **OUT** sur la page **IN/OUT**.
2. La zone de la centrale doit être de type zone à clé, et dans Protegus 2 la bonne sortie doit être attribuée à la partition, dans le mode à impulsion ou bistable correspondant à la zone (section 5.3).

Protegus 2 ne voit pas l'appareil

1. **Enable connection** doit être coché sur la page **User reporting** → **PROTEGUS Cloud**.
2. Lors de la création du système, il faut saisir le **Protegus Cloud access code** défini dans l'appareil ; il ne peut plus être modifié dans l'appareil une fois le système créé.
3. Saisissez l'**adresse MAC (Unique ID)** exactement, en la recopiant depuis la boîte ou le dos de l'appareil.

4. L'appareil doit être en ligne : la LED NETWORK est verte, TROUBLE ne clignote pas, et la LED DATA s'éteint après un événement. Sur un réseau avec pare-feu, la connexion sortante vers le cloud Protegus doit être autorisée.

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

1. L'appareil doit être en ligne (LED NETWORK verte), et la connexion Protegus doit être activée.
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 ouvrir ou rediriger un port sur le routeur ?

Non. L'E16 n'établit que des connexions **sortantes** vers le récepteur et le cloud Protegus ; ni redirection de port ni adresse IP publique ne sont donc nécessaires, et la programmation à distance passe elle aussi par cette connexion sortante. Veillez seulement à ce que le pare-feu ne bloque pas le trafic sortant vers le port du récepteur et vers le cloud Protegus.

Fonctionne-t-il en Wi-Fi ou sur le réseau mobile ?

Non : l'E16 n'a qu'un connecteur Ethernet filaire. Si l'alimentation du routeur n'est pas fiable, alimentez les équipements réseau par une alimentation sans interruption (onduleur).

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

L'E16 est alimenté par la centrale d'alarme ; il continue donc de fonctionner sur la batterie de la centrale, mais le routeur et le modem s'arrêtent généralement, et Internet disparaît avec eux. Tant qu'il n'y a pas de liaison, la LED TROUBLE le signale par 1 ou 6 clignotements, l'appareil mémorise les événements (60 messages au maximum) et les envoie dans l'ordre au retour d'Internet. Si la perte d'Internet n'est pas admissible pour le système, alimentez aussi les équipements réseau par une alimentation sans interruption (onduleur).

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 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

- Moteur de recherche de compatibilité – quel communicateur convient à quelle centrale d'alarme.
- G16 – commande directe des centrales d'alarme DSC PowerSeries – armement avec le code clavier, état des zones, exclusion de zones ; s'applique de la même façon à l'E16.
- DSC Power Series NEO et communicateurs Trikdis : compatibilité et solutions – pourquoi l'E16 ne peut pas être raccordé à la NEO, et quelle est la solution.
- Déverrouillage du port série verrouillé des centrales d'alarme Paradox – déverrouillage du port série des centrales Paradox récentes.
- 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 E16 Ethernet Communicator - Module IP

Câble de connexion de port série Trikdis CRP2 pour les centrales d'alarme Paradox

Câble de connexion de port série CRP2B pour les centrales d'alarme Paradox

Câble série Trikdis CRP4 pour les panneaux de contrôle Texecom

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-e16