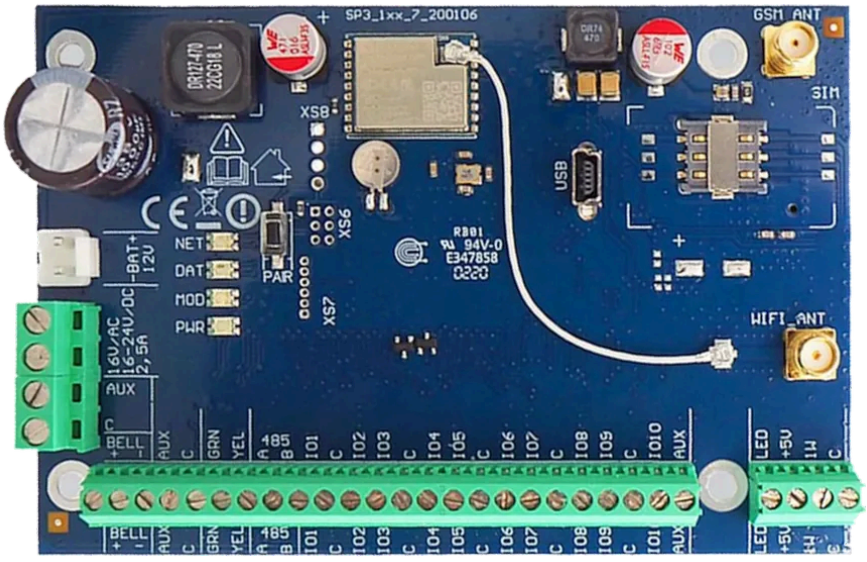
Centrale d'alarme « FLEXi » SP3 – manuel d'installation et de programmation

Manuel d'installation et de programmation de la centrale d'alarme Trikdis « FLEXi » SP3 : alimentation, raccordement des zones et des sorties PGM, claviers et extensions, programmation dans TrikdisConfig, transmission vers le centre de télésurveillance, application Protegus 2.



Édition: 2026-11-17
Version web toujours à jour: https://trikdis.fr/manuel-flexi-sp3

Sommaire

1. Présentation

1.1 À quoi elle sert, comment elle fonctionne
1.2 Versions et codes de type
1.3 Caractéristiques techniques
1.4 Modules et claviers compatibles
1.5 Éléments de la carte et borniers
1.6 Signalisation des LED
1.7 Versions du firmware

2. Alimentation et mise en service rapide

2.1 Alimentation secteur
2.2 Batterie
2.3 Contenu de l'emballage, coffrets : K01 et K02
2.4 Les étapes de la mise en service en bref

3. Installation et raccordement

3.1 Ordre recommandé de l'installation
3.1.1 Montage de la carte dans le coffret
3.1.2 Ordre de raccordement des appareils
3.2 Raccordement des détecteurs
3.2.1 Schémas de raccordement
3.3 Raccordement des détecteurs de fumée
3.4 Raccordement de la sirène
3.5 Raccordement des claviers et des lecteurs RFID
3.6 Raccordement des lecteurs de clés TM17 et CZ-Dallas
3.7 Raccordement des sondes de température
3.8 Raccordement d'un relais et d'un voyant LED
3.9 Mise sous tension de la centrale

4. Raccordement des extensions et des modules radio

4.1 Module Ethernet E485
4.2 Récepteur radio RF-SH (Crow)
4.3 Récepteur radio RTX3 (Paradox)
4.4 Récepteur radio RF-HW (Honeywell)
4.5 Récepteur radio RF-S8
4.6 Récepteur radio RF-LORA
4.7 Extensions LORA
4.8 Extensions de la série iO
4.9 Émetteur radio T16
4.10 Module Sigfox SF485
4.11 Mesure de tension continue

5. Protegus 2 et commande à distance

5.1 Association au compte Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armement et désarmement dans l'application
5.3 Configuration et commande par SMS
5.4 Commande par appel téléphonique

6. TrikdisConfig – les réglages en détail

- 6.1 La barre d'état
- 6.2 System Options
  - 6.2.1 Onglet System general
  - 6.2.2 Onglet Partitions
  - 6.2.3 Onglet Scheduler
  - 6.2.4 Onglet Holidays
  - 6.2.5 Onglet System troubles
  - 6.2.6 Onglet Access
- 6.3 Reporting to CMS
  - 6.3.1 Onglet Reporting
  - 6.3.2 Onglet Settings
- 6.4 Users & Reporting
  - 6.4.1 Cartes et badges RFID
  - 6.4.2 Clés iButton
  - 6.4.3 Onglet Protegus
  - 6.4.4 Onglet SMS answer texts
- 6.5 Modules
- 6.6 Wireless sensors
  - 6.6.1 Enregistrement du RF-LORA
  - 6.6.2 Appairage des détecteurs à distance
  - 6.6.3 Appairage avec le bouton LEARN
  - 6.6.4 RF-SH et appareils Crow
- 6.7 Zones
- 6.8 PGM
- 6.9 Sensors
- 6.10 System events
- 6.11 Events log
- 6.12 Restauration des réglages d'usine

7. Programmation à distance

8. Vérification du fonctionnement du système

9. Mise à jour du firmware

10. Dépannage et questions fréquentes

11. Garantie et consignes de sécurité

- 11.1 Garantie et limitation de responsabilité
- 11.2 Consignes de sécurité

Voir aussi

1. Présentation

La « FLEXi » SP3 est la **centrale d'alarme intrusion et incendie** de Trikdis, avec communicateur intégré : par connexion Wi-Fi et/ou Ethernet, ou par modem 2G / 4G (sur le réseau mobile, si une carte SIM est insérée), elle transmet directement chaque événement déclenché au centre de télésurveillance et à l'application Protegus 2 (cloud Protegus). Elle possède dix bornes IO à fonction configurable (zone ou sortie PGM), gère huit partitions et peut être étendue à 32 ou 64 zones – selon la version du firmware – avec des claviers, des extensions iO et des récepteurs sans fil. Vous effectuez les réglages avec le logiciel TrikdisConfig, par câble USB ou à distance ; l'utilisateur commande le système depuis un clavier filaire ou sans fil, avec une clé iButton, une carte RFID, depuis l'application Protegus 2 et, sur les versions avec modem, également par SMS et par appel téléphonique – il peut aussi changer à distance le mode de protection des différentes zones du bâtiment (partitions). La centrale est certifiée EN 50131 Grade 3.

1.1 À quoi elle sert, comment elle fonctionne

Utilisations principales

- **Système d'alarme de petits et moyens bâtiments**, de préférence complété par la télésurveillance : elle accepte aussi bien des détecteurs filaires que sans fil, transmet les événements au centre de télésurveillance et à l'utilisateur, et tous deux peuvent la commander à distance.
- **Remplacement d'une centrale d'alarme existante** : la valeur des résistances de fin de ligne présentes dans les détecteurs se règle dans la centrale sur celle de la centrale remplacée ; il n'est donc pas nécessaire de modifier les détecteurs un par un.
- **Automatisation** en plus de la protection : porte de garage et portail, arrosage, éclairage, chauffage, ventilation, climatisation et tout ce qui peut être allumé et éteint – depuis les sorties PGM, avec une logique de fonctionnement, une programmation horaire ou en mode thermostat.

Fonctionnement

- **Transmission au centre de télésurveillance** via la connexion Wi-Fi, Ethernet ou mobile intégrée ; avec un module supplémentaire, également par canal Ethernet (E485), radio VHF/UHF (T16) ou Sigfox (SF485), avec une priorité au choix. Tout centre de télésurveillance disposant d'un récepteur IP logiciel ou matériel Trikdis, ou d'un récepteur IP compatible avec le protocole SIA DC-09, peut la recevoir. Elle peut transmettre en parallèle aux récepteurs de deux sociétés de sécurité différentes, chacune avec un récepteur principal et un récepteur de secours.
- **Notification de l'utilisateur** dans l'application Protegus 2 par notification push avec un signal sonore distinct ; les versions avec modem envoient aussi des SMS à 8 numéros de téléphone au maximum. Seule l'ancienne version SP3_12xx, avec un firmware 1.13 au maximum, peut prévenir par appel avec message vocal préenregistré (8 numéros de téléphone au maximum). Il est possible de régler que l'événement soit d'abord envoyé au centre de télésurveillance, et seulement ensuite à l'utilisateur.
- **Commande à distance** : armement, désarmement, mode partiel (Stay) et mode nuit (Sleep), commande des appareils raccordés aux sorties PGM et surveillance de la température depuis l'application ; sur les versions avec modem, également par SMS et par appel téléphonique.
- **Entrées et sorties** : 10 bornes IO, chacune utilisable comme entrée (types NC, NO, EOL, ATZ, avec une valeur de résistance réglable dans les circuits EOL et ATZ) ou comme sortie à collecteur ouvert ; le nombre d'entrées peut être porté à 64 avec des claviers et des extensions iO, iO-8, iO8-LORA, iO-LORA et iO-WL, celui des sorties à 16 avec ces mêmes extensions ; deux sorties dédiées (BELL pour la sirène, LED pour le voyant) ; sept modes de fonctionnement des sorties, et à chaque sortie on peut attribuer

une logique de fonctionnement, une programmation horaire prédéfinie ou par exemple le mode thermostat ; sur le bus 1-Wire, jusqu'à 8 sondes de température, 1 sonde de température et d'humidité ou un lecteur iButton ; sur le bus clavier GRN / YEL, 8 claviers du même type et le récepteur radio Paradox RTX3 (4.3) ; sur le bus RS485, des extensions iO, des récepteurs radio (RF-LORA, RF-SH, RF-S8, RF-HW), les modules E485, T16 et SF485.

- **Utilisation** : 40 codes utilisateur (1 code maître et 39 codes normaux, à 4 ou 6 chiffres), utilisables aussi comme codes sous contrainte – le code désarme l'alarme, mais le centre de télésurveillance reçoit un signal distinct indiquant que le désarmement a eu lieu sous la contrainte. Claviers Trikdis, Paradox et Crow, lecteurs iButton CZ-Dallas et TM17 (plus fabriqué), lecteurs RFID Wiegand 26/34.
- **Installation et configuration** : kits en coffret métallique avec alimentation intégrée, en plusieurs tailles, avec transformateur abaisseur ou alimentation à découpage ; les réglages d'usine conviennent sans modification à la plupart des petits et moyens sites (sept sur dix) ; l'ancienne centrale peut être remplacée sans changer les résistances des détecteurs ; les réglages peuvent être enregistrés dans un fichier ; deux niveaux d'accès (installateur et administrateur) ; à distance, TrikdisConfig ne fait pas que configurer, il montre aussi le fonctionnement de la centrale.

1.2 Versions et codes de type

La centrale est un circuit imprimé unique, disponible en six versions selon les modules de communication intégrés. La version est indiquée par le premier chiffre (**y**) du code **SP3_yxxz** dans le nom du fichier firmware ; vous voyez la même chose dans la barre d'état de TrikdisConfig, et lors d'une mise à jour, seul un firmware portant le même chiffre peut être chargé (section 1.7).

Version	Connexion	Code (y)	Logement SIM
SP3 WiFi	Wi-Fi	2	–
SP3 Ethernet	réseau filaire (Ethernet, RJ45)	3	–
SP3 WiFi + 2G	Wi-Fi + modem 2G (GSM/GPRS)	5	1 × nano-SIM
SP3 WiFi + 4G	Wi-Fi + modem 4G (LTE)	1	1 × nano-SIM
SP3 Ethernet + 4G	Ethernet + modem 4G (LTE)	6	1 × nano-SIM
SP3 Ethernet + 2 SIM 4G	Ethernet + modem 4G (LTE), avec deux logements SIM	à vérifier dans la barre d'état de l'appareil	2 × nano-SIM

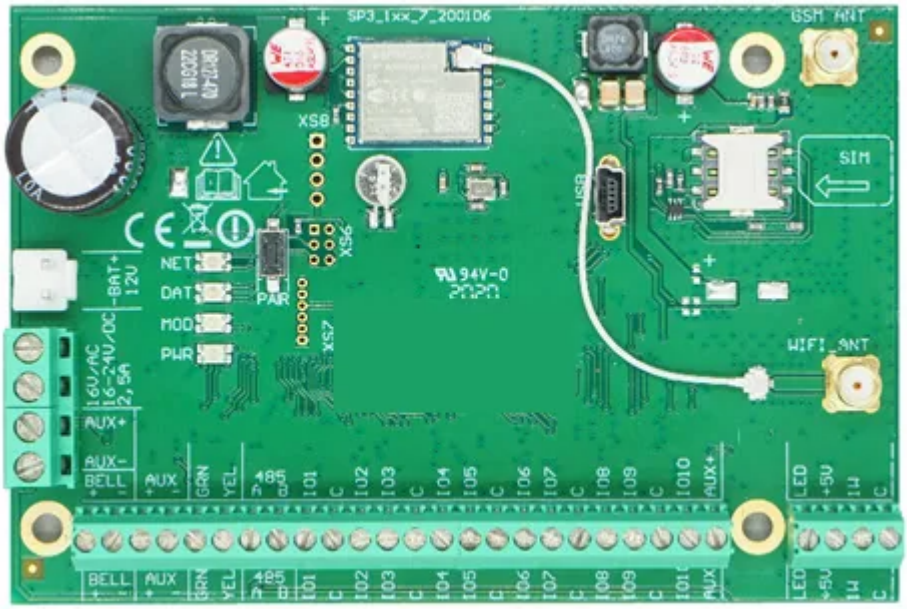


Figure 1. Le circuit imprimé de la « FLEXi » SP3 version WiFi + 2G : connecteurs SMA des antennes Wi-Fi et réseau mobile, logement nano-SIM et borniers.

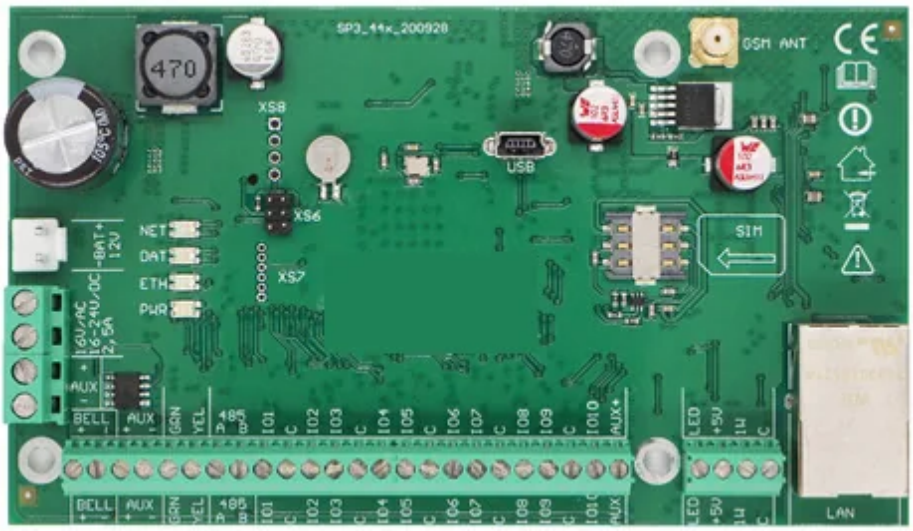


Figure 2. La « FLEXi » SP3 version Ethernet + 4G : la prise Ethernet RJ45 à la place du connecteur de l'antenne Wi-Fi.

Un ou deux canaux de communication. Les versions WiFi et Ethernet communiquent sur un seul canal, les versions avec modem sur deux (dual path) : en plus de la connexion filaire, aussi sur le réseau mobile.

WiFiun canal
Ethernetun canal
WiFi + 2Gdeux canaux · 1 SIM
WiFi + 4Gdeux canaux · 1 SIM
Ethernet + 4Gdeux canaux · 1 SIM
Ethernet + 2 SIM 4Gdeux canaux · 2 SIM

- En Wi-Fi et en Ethernet, l'accès depuis le téléphone est rapide et il n'y a pas de frais de données mobiles.
- Si l'Internet filaire est coupé, ou si le routeur s'éteint lors d'une coupure de courant, la centrale avec modem bascule automatiquement sur le réseau mobile.
- Grâce aux deux canaux qui se secourent mutuellement (dual path), le signal arrive à destination même si l'une des voies tombe en panne.

- Sur une connexion Wi-Fi, Ethernet et 4G rapide, la programmation à distance et la mise à jour du firmware sont confortables.

Le modem **2G** des versions avec modem fonctionne sur les bandes 850 / 900 / 1800 / 1900 MHz, le modem **4G (LTE)** sur les bandes B1 / B3 / B7 / B8 / B20 / B28 utilisées en Europe (EMEA) ; pour d'autres régions (Amérique latine, Australie, Amérique du Nord), il existe aussi des versions avec un modem aux bandes différentes (les bandes figurent dans le tableau de la section 1.3). Le Wi-Fi est en 2,4 GHz, 802.11 b/g/n, avec chiffrement WPA / WPA2.

1.3 Caractéristiques techniques

Caractéristique	Valeur
Tension d'alimentation [AC / DC]	16 V AC ou 16–24 V DC, 2,5 A
Consommation	50 mA au maximum en veille ; 200 mA au maximum brièvement, pendant l'envoi
Alimentation de secours [BAT]	batterie au plomb 12 V, 4 Ah ou 7 Ah
Courant de charge de la batterie	500 mA au maximum
Alimentation des appareils externes [AUX]	12 V DC, 1 A au maximum
Sortie sirène [BELL]	1 A
Sortie LED [LED]	0,1 A
Sortie PGM (borne IO utilisée comme sortie)	à collecteur ouvert, 0,1 A au maximum
Module Wi-Fi	intégré sur les versions Wi-Fi ; 2,4 GHz, 802.11 b/g/n, WPA / WPA2 / WPA mixte
Configuration réseau	DHCP ou manuelle
Carte SIM	1 nano-SIM sur les versions avec modem (2 sur la version à 2 SIM)
Bandes du modem 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Bandes du modem 4G (LTE) – « FLEXi » SP3_14E / SP3_24E, EMEA et Thaïlande	B1 / B3 / B7 / B8 / B20 / B28
Bandes du modem 4G (LTE) – « FLEXi » SP3_24S, Amérique latine / Australie / Nouvelle-Zélande	B1 / B3 / B4 / B5 / B7 / B8 / B28
Bandes du modem 4G (LTE) – « FLEXi » SP3_24A, Amérique du Nord	B2 / B4 / B12
Destinations de l'envoi des événements	récepteur principal et de secours de 2 sociétés de sécurité ; cloud Protegus, application Protegus 2 iOS / Android ; SMS à 8 numéros de téléphone ; appel à 8 numéros de téléphone – si l'utilisateur décroche, la centrale annonce par message vocal ce qui s'est passé (uniquement la version SP3_12xx, avec un firmware 1.13 au maximum)
Canaux d'envoi des événements	GPRS ou 4G, Wi-Fi, Ethernet (intégré ou avec le module E485), SMS ; appel vocal à 8 numéros de téléphone au maximum (uniquement la version SP3_12xx, avec un firmware 1.13 au maximum) ; radio VHF/UHF (avec le communicateur T16) ; Sigfox (avec le module SF485)

Caractéristique	Valeur
Liaison avec le centre de télésurveillance	TCP/IP ou UDP/IP, ou SMS
Codage des événements	Contact ID
Chiffrement	TRK AES-128, SIA IP AES-128
Horloge interne	oui
Mémoire tampon des messages	60 événements
Journal des événements	1000 événements au maximum ; lorsqu'il est plein, le plus ancien est effacé
Codes utilisateur	40 (à 4 ou 6 chiffres)
Code sous contrainte	deux modes de saisie au choix lors de la programmation
Bornes à double fonction [IO]	10 ; fonction IN ou OUT lors de la programmation. En entrée : NC, NO, EOL, EOL_T, 3EOL, ATZ, ATZ_T. En sortie : à collecteur ouvert (OC), 100 mA au maximum
Partitions	8
Zones	10 (20 avec le doublement de zones ATZ) ; jusqu'à 64 avec des extensions (section 1.7)
Sorties PGM	2 (12 si les bornes IO sont réglées en sortie ; 16 avec des extensions)
Claviers	8 au maximum (les types sont énumérés à la section 1.4)
Lecteurs RFID (Wiegand 26/34)	2 au maximum
Longueur du bus 1-Wire [1 WIRE]	30 m au maximum
Sondes de température	Maxim / Dallas DS18S20, DS18B20 ; série AM2301
Nombre de sondes de température sur le bus 1-Wire	8 (Dallas) ou 1 (AM2301)
Clés électroniques (iButton) [1 WIRE]	Maxim / Dallas DS1990A, 40 clés au maximum
Longueur du bus RS485	100 m au maximum
Appareils sur le bus RS485	8 au maximum
Environnement de fonctionnement	−10 °C … +50 °C, humidité relative de 80 % au maximum à +20 °C, sans condensation
Dimensions de la carte	117 × 79 × 25 mm ; 137 × 79 × 25 mm pour les versions Ethernet + 4G
Poids	0,1 kg

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

1.4 Modules et claviers compatibles

La sortie AUX de la centrale fournit 1 A au maximum aux appareils externes ; pour dimensionner la batterie de secours (section 2.1), il faut additionner la consommation de tous les modules raccordés. La liste d'origine :

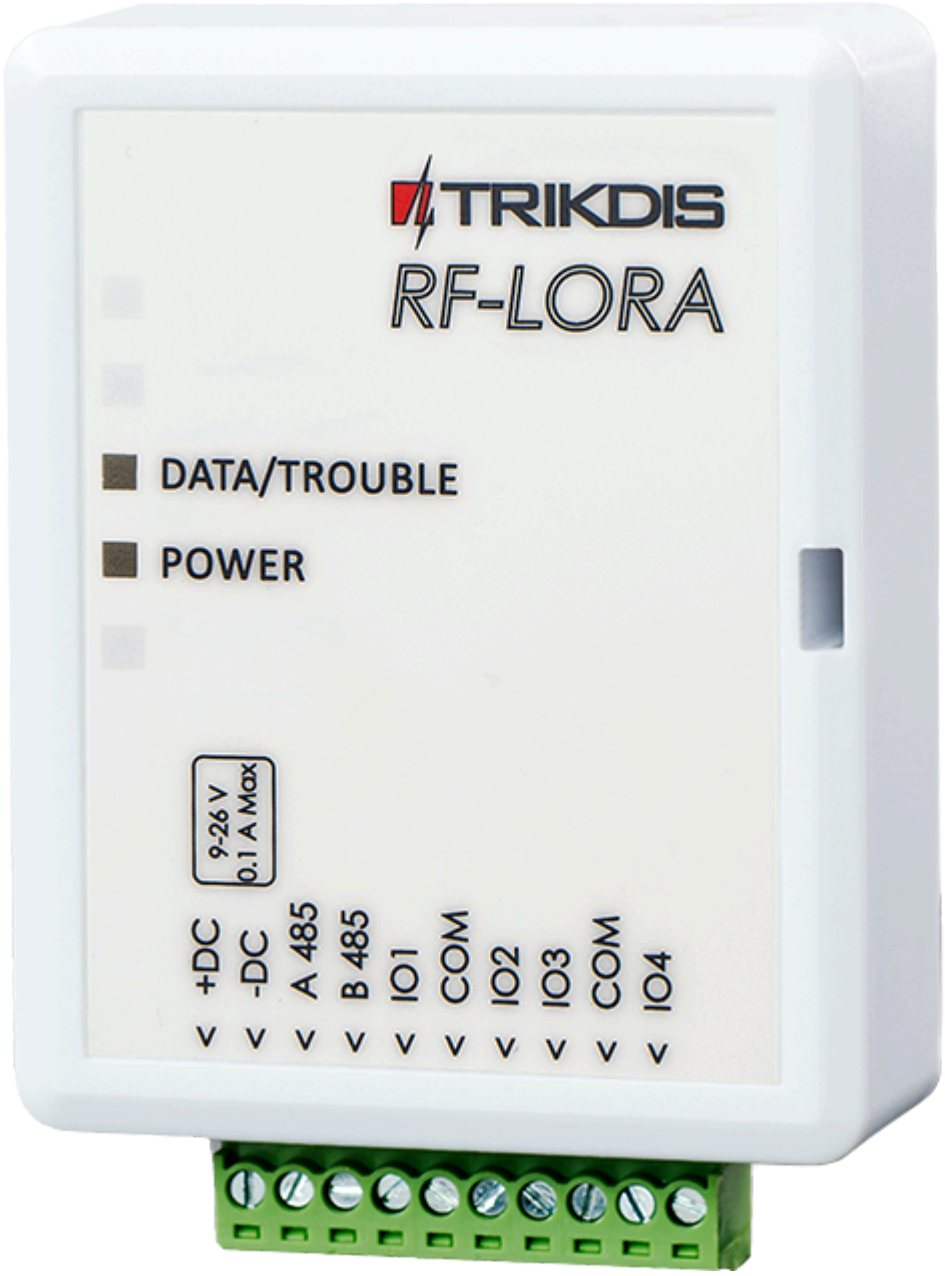
Module	Consommation
Clavier SK-LED TouchPad (Protegus SK232 LED W)	60–150 mA
Clavier SK-LCD TouchPad (FLEXi SK232LCD – dans la boutique : clavier FLEXi LCD)	25–60 mA
Clavier SK LCD Button	70 mA au maximum
Clavier SK LED Button	70 mA au maximum
Clavier Paradox K636	40–70 mA
Clavier Paradox K10H(V)	44–72 mA
Clavier Paradox K32 LED, K32+ LED	49–148 mA
Clavier Paradox K32LCD+	70–150 mA
Clavier Paradox K35	30–70 mA
Clavier Paradox TM50	100–230 mA
Clavier Paradox TM70	200–330 mA
Clavier Crow CR16, CR-LCD	40–75 mA
Extension iO-8	20 mA au maximum
Extension iO	50 mA au maximum
iO-MOD – émetteur-récepteur radio iO-WL	50–150 mA
Extension sans fil iO-WL	200 mA au maximum
Récepteur radio RF-SH (pour détecteurs Crow)	100 mA au maximum
Émetteur-récepteur radio Paradox RTX3	200 mA au maximum
Émetteur-récepteur radio RF-HW (pour détecteurs Honeywell)	100 mA au maximum
Émetteur-récepteur radio RF-S8 (pour détecteurs S8)	100 mA au maximum
Émetteur-récepteur radio RF-LORA (pour détecteurs et modules LORA)	50–150 mA
Extension iO-LORA, iO8-LORA	50 mA au maximum
Bouton panique PB-LORA	pile propre, 3 V CR123A
Module relais REL-LORA	45 mA au maximum
Module Ethernet E485	50–150 mA
Lecteur iButton TM17	50 mA au maximum
Lecteur iButton CZ-Dallas	25 mA au maximum
Communicateur radio VHF / UHF T16	100 mA – 1,2 A
Lecteur RFID (Wiegand 26/34)	100 mA au maximum

Claviers. Jusqu'à 8 claviers du même type peuvent être raccordés au bus GRN / YEL :

Trikdis PROTEGUS SK232LED, FLEXI LCD, FLEXI LED, SK-LCD Button, SK-LED Button
Paradox K32LCD+, K32+, K32LED, K32+ LED, K35, K10H, K10V, K636, TM50*****, TM70*****
Crow CR16, CR-LCD
A LED-es kezelők csak az első 2 partíció állapotát képesek megjeleníteni, de kezelhetik mind a 8 partíciót.
*Ez a kezelő csak az első 2 partíciót kapcsolhatja ki/be.

Appareils sans fil. Le type de récepteur radio dépend de la version du firmware de la centrale (section 1.7) : une centrale fonctionne avec un seul type de récepteur à la fois.

Vezeték nélküli érzékelők és eszközök hozzáadása a FLEXi SP3 riasztórendszerhez





A **TRIKDIS RF-LORA** vagy **Paradox RTX3** vezeték nélküli bővítő modullal a „klasszikus" vezetékes riasztó hibrid vagy teljesen vezeték nélküli módon is működhet. Hasznos, ha nincs lehetőség vezeték kiépítésére és vezeték nélküli érzékelőkre vagy egyéb vezeték nélküli eszközökre van szükség.

A RIKDIS RF-LORA-hoz a Trikdis vezeték nélküli bővítőket, érzékelőket és eszközöket lehet párosítani.

A Paradox RTX3-mal a Paradox vezeték nélküli érzékelőket, eszközöket és billentyűzeteket lehet használni.

1.5 Éléments de la carte et borniers

Le dessin montre les principaux éléments de la carte ; le tableau sous le dessin énumère la fonction des bornes.

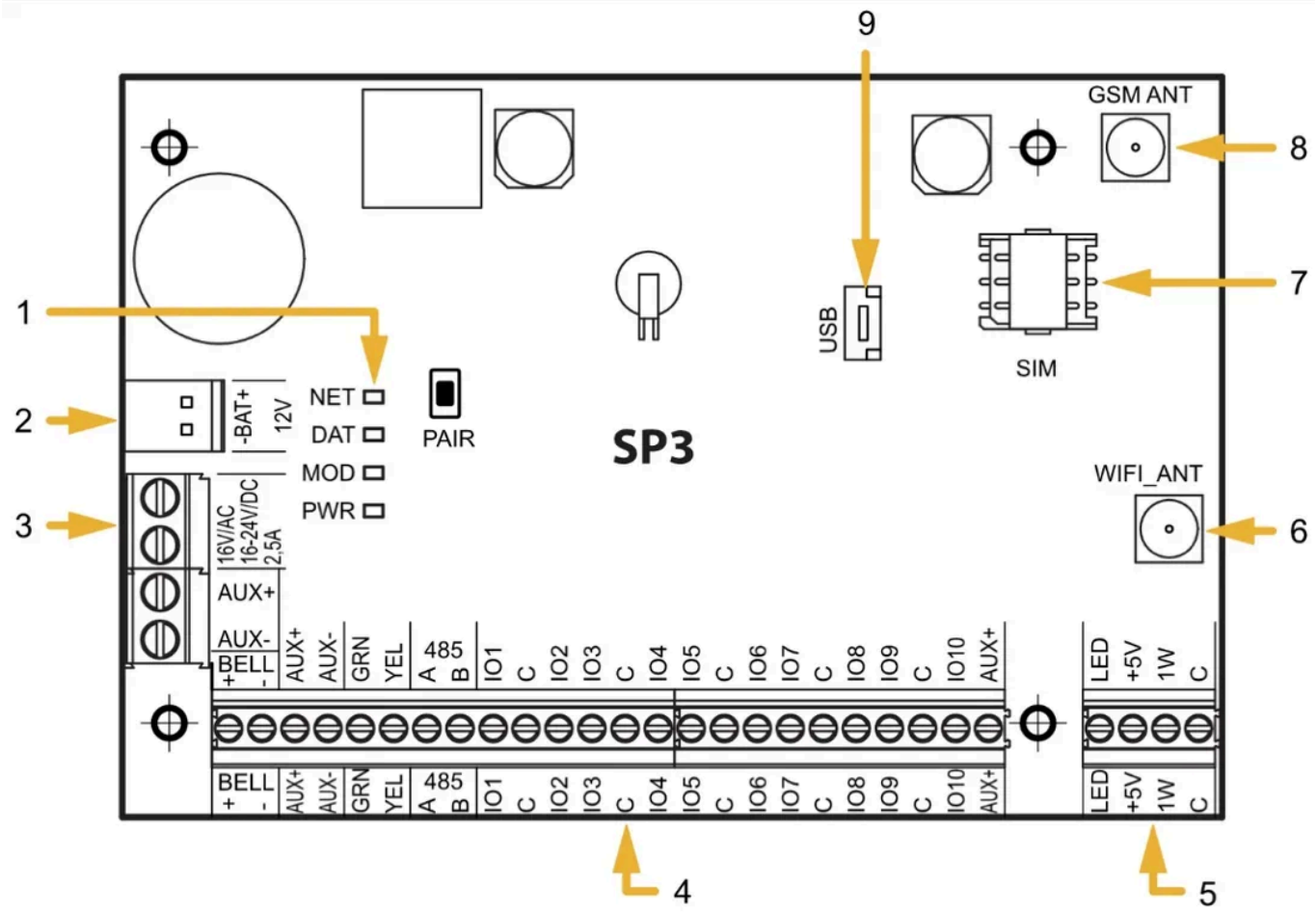


Figure 3. Le circuit imprimé de la « FLEXi » SP3 (version Wi-Fi + mobile). Sur la version Ethernet, une prise Ethernet RJ45 se trouve à la place du n° 6.

- 1 Voyants LED de connexion et de fonctionnement (section 1.6)
- 2 Bornier de l'alimentation de secours (batterie)
- 3 Bornier de l'alimentation principale
- 4 Bornier des appareils externes
- 5 Bornier du bus de données 1-WIRE
- 6 Connecteur SMA pour l'antenne Wi-Fi
- 7 Logement nano-SIM
- 8 Connecteur SMA pour l'antenne réseau mobile
- 9 Prise USB Mini-B pour la programmation

Borne	Fonction
AC/DC (2 bornes)	Alimentation principale : 16 V AC, ou pôles positif et négatif de 16–24 V DC
BAT+	Pôle positif de l'alimentation de secours (batterie 12 V)
BAT−	Pôle négatif de l'alimentation de secours
AUX+	+12 V pour les appareils externes (1 A au maximum)
AUX−	Négatif commun
BELL+	Sortie sirène : +12 V pour la sirène
BELL−	Sortie sirène : pôle négatif commuté de la sirène (1 A au maximum)
GRN	Bus clavier (données)
YEL	Bus clavier (données)
A 485	Fil A du bus RS485

Borne	Fonction
B 485	Fil B du bus RS485
IO1 – IO9	Entrées/sorties (réglage d'usine : entrée)
IO10	Entrée/sortie (réglage d'usine : sortie PGM, réinitialisation des détecteurs incendie)
C	Négatif commun
LED	Sortie PGM (réglage d'usine : indication de l'état du système)
+5 V	Alimentation +5 V des appareils 1-Wire
1 WIRE	Bus de données 1-Wire
C	Négatif commun

Les borniers sont débrochables : vous pouvez donc raccorder les fils sans la carte, et la carte peut être retirée lors d'une intervention.

1.6 Signalisation des LED

LED	Signal	Signification
NET	clignote en vert	la carte SIM s'enregistre sur le réseau mobile
	allumée en vert	la carte SIM est enregistrée sur le réseau mobile
	clignote en jaune	niveau du signal mobile, de 0 à 5 clignotements ; 3 suffisent
DAT	éteinte	aucun événement non envoyé
	allumée en vert	envoi de message en cours
	allumée en jaune	des événements non envoyés attendent dans la mémoire tampon
MOD (version Wi-Fi)	clignote en vert	connexion au réseau Wi-Fi en cours
	allumée en vert	connectée au réseau Wi-Fi
ETH (version Ethernet)	clignote en vert	pas de câble LAN, ou erreur DHCP
	allumée en vert	connectée au réseau filaire
PWR	clignote en vert	aucun défaut de fonctionnement
	1 clignotement rouge	pas de carte SIM
	2 clignotements rouges	code PIN de la carte SIM erroné
	3 clignotements rouges	impossible de se connecter au réseau mobile
	4 clignotements rouges	le récepteur de télésurveillance n'est pas joignable sur le canal 1
	5 clignotements rouges	le récepteur de télésurveillance n'est pas joignable sur le canal 2
	6 clignotements rouges	l'horloge interne n'est pas réglée
	7 clignotements rouges	tension de l'alimentation de secours (batterie) faible
	8 clignotements rouges	pas d'alimentation secteur (AC)
	9 clignotements rouges	impossible de se connecter au réseau Wi-Fi

Le dépannage est traité au chapitre 10.

1.7 Versions du firmware

Le nom du fichier firmware de la centrale a la forme **SP3_yxxz_NNNN.fw**. **y** est la version matérielle (section 1.2) – elle ne peut pas être modifiée lors d'une mise à jour. **z** indique le type de récepteur sans fil et donc le nombre de zones gérées ; c'est vous qui le choisissez lors de la mise à jour, en fonction du récepteur radio utilisé. **NNNN** est le numéro de version du firmware ; en général, il vaut mieux utiliser la version la plus élevée.

Firmware (z)	Récepteur sans fil	Détecteurs sans fil	Zones	Claviers	Modules
SP3_xxx0	RF-SH (fin de série), RF-LORA	Crow	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-SH
SP3_xxx1	Paradox RTX3, RF-LORA	Paradox	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA
SP3_xxx2	RF-HW, RF-LORA	Honeywell (345 MHz, non utilisé en Europe)	64	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-HW
SP3_xxx4	RF-LORA, RF-S8	MAXIMUM (M4), S8 (Heyi)	64	Trikdis (FLEXi), Paradox	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-S8

Le firmware **SP3_xxx4** n'est nécessaire que pour les détecteurs sans fil : il fait fonctionner les appareils sans fil MAXIMUM (RF-LORA) et S8 (RF-S8), avec 64 zones. Il faut au moins la version 1.21, et la 1.22 pour les appareils S8. Les extensions LORA raccordées via le RF-LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) fonctionnent avec les quatre versions. L'extension Paradox RTX3 nécessite le **SP3_xxx1**, avec 32 zones. Chargez toujours la version la plus récente : en novembre 2026, c'est la 1.27, avec une communication améliorée, et l'envoi d'un trop grand nombre de SMS y a été corrigé. Le codage et les règles de choix sont décrits dans un article à part : Firmware FLEXi SP3 : comment choisir le bon ?. Les étapes de la mise à jour se trouvent au chapitre 9.

2. Alimentation et mise en service rapide

La centrale, et avec elle tout le système d'alarme, est alimentée par une alimentation secteur ; le secours est assuré par une batterie 12 V. Dans ce chapitre, vous trouverez les règles de l'alimentation, les kits d'origine et un bref ordre des étapes de la mise en service ; le détail du raccordement se trouve aux chapitres 3 et 4, celui des réglages aux chapitres 5 et 6.

2.1 Alimentation secteur

La centrale fonctionne sous **16 V AC** ou **16–24 V DC**, à partir d'une source pouvant fournir au moins **2,5 A**. En courant alternatif, elle est alimentée depuis le secteur par un transformateur abaisseur Class II ; en courant continu, par une alimentation à découpage de 16–24 V (dans les coffrets K01 et K02 disponibles chez nous : Mean Well APV-35-24). Vous raccordez l'alimentation principale aux deux bornes **AC/DC** de la carte ; en

courant continu, le pôle positif et le pôle négatif dans l'ordre indiqué sur les bornes. Dans les deux cas – alimentation en courant alternatif comme en courant continu – le raccordement de l'alimentation de secours, une batterie 12 V, est obligatoire, afin que l'alimentation reste continue sans interruption (section 2.2).

Disjoncteur et mise à la terre

Un disjoncteur automatique bipolaire, dont les contacts ouverts sont distants d'au moins 3 mm, doit être intégré au circuit d'alimentation ; l'interrupteur doit se trouver à un endroit connu et accessible du technicien qui assure la maintenance de la centrale. Dans le cas d'un coffret métallique, mettez le coffret à la terre. Le coffret, l'alimentation, la batterie et l'appareil de programmation doivent être conformes à la norme EN 60950.

Calcul de la consommation. Selon la norme EN 50131, l'alimentation de secours doit faire fonctionner le système pendant **12 heures** (Grade 2) ou **60 heures** (Grade 3) après la coupure de l'alimentation secteur. Pour cela, additionnez le courant de veille de la centrale (50 mA) et la consommation des claviers, modules, détecteurs et signalisations raccordés – les données des appareils Trikdis et des appareils tiers pris en charge figurent dans le tableau de la section 1.4 –, et choisissez la capacité de la batterie en conséquence. La borne **AUX+** peut fournir au total 1 A au maximum aux appareils externes ; s'il faut davantage, utilisez une alimentation séparée, avec un négatif commun.

2.2 Batterie

L'alimentation de secours est une **batterie au plomb 12 V, 4 Ah ou 7 Ah** (au moins 7 Ah pour le Grade 3), raccordée aux bornes **BAT+ / BAT–** de la carte avec le câble de liaison fourni dans la boîte. La centrale la charge avec 500 mA au maximum.

- En cas de coupure de l'alimentation secteur, la centrale envoie l'événement **AC Fault** (défaut secteur) et passe sur la batterie.
- À 11,5 V, l'événement **Low Battery** (batterie faible) est généré ; en dessous de 9,5 V, la centrale **déconnecte** la batterie pour la protéger de la décharge profonde.
- Au retour de l'alimentation secteur, elle envoie l'événement **AC Restore** et commence la charge ; à 12,6 V, elle envoie l'événement **Battery Restore** (batterie rétablie).

La batterie doit être rechargée en 72 heures pour satisfaire l'exigence Class II, et en 24 heures pour l'exigence Class III – cela résulte de la capacité de la batterie combinée au courant de charge de 500 mA.

2.3 Contenu de l'emballage, coffrets : K01 et K02

La centrale est disponible seule (carte) ou avec un coffret métallique préparé. L'emballage d'origine de la carte contient : la carte « FLEXi » SP3, un câble de liaison pour la batterie, 20 résistances de 2,2 kΩ et 10 de 4,7 kΩ, 4 entretoises en plastique pour la fixation, ainsi que, pour les versions avec modem, une antenne ME301M à embase magnétique avec 2,5 m de câble (2 pièces selon la liste de colisage d'origine). Le **câble USB Mini-B** nécessaire à la programmation et la batterie ne font pas partie de l'emballage.

Dans les versions en coffret, la centrale est montée dans un coffret métallique équipé d'un contact d'autoprotection, avec une alimentation préparée : alimentation à découpage Mean Well APV-35-24, point de raccordement au réseau 230 V avec fusible de 3,15 A, tout est déjà câblé. Il existe deux tailles de coffret :

Coffret	Dimensions	Remarque
K01 – coffret métallique de taille normale	285 × 280 × 80 mm	pour toutes les versions SP3
K02 – petit coffret métallique	200 × 210 × 80 mm	la version Ethernet + 4G n'y rentre pas

Boîte métallique de taille normale avec PSU pour panneau de commande Flexi SP3

Boîte en métal de petite taille avec PSU pour panneau de commande Flexi SP3

Les deux coffrets (K01 et K02) contiennent une alimentation à découpage Mean Well avec un bornier à fusible de 3,15 A ; les anciens coffrets K01 contenaient encore un transformateur 230 V / 16 V, 40 VA. Les kits d'origine (SP3 KIT, SP3 KITi) comprennent, outre la carte montée dans le coffret métallique, 2 antennes ME301M (avec 2,5 m de câble), un câble de liaison pour la batterie, 20 résistances de 2,2 kΩ et 10 de 4,7 kΩ, ainsi qu'un détecteur d'autoprotection.

2.4 Les étapes de la mise en service en bref

Ce dont vous aurez besoin

Câble USB Mini-B · tournevis plat pour les borniers · les résistances de 2,2 kΩ et 4,7 kΩ fournies dans la boîte · batterie 12 V 7 Ah · pour la version avec modem, une nano-SIM active avec service de données mobiles (désactivez au préalable la demande de code PIN dans un téléphone) · pour la version Wi-Fi, le nom et le mot de passe du réseau · le logiciel TrikdisConfig sur un ordinateur Windows.

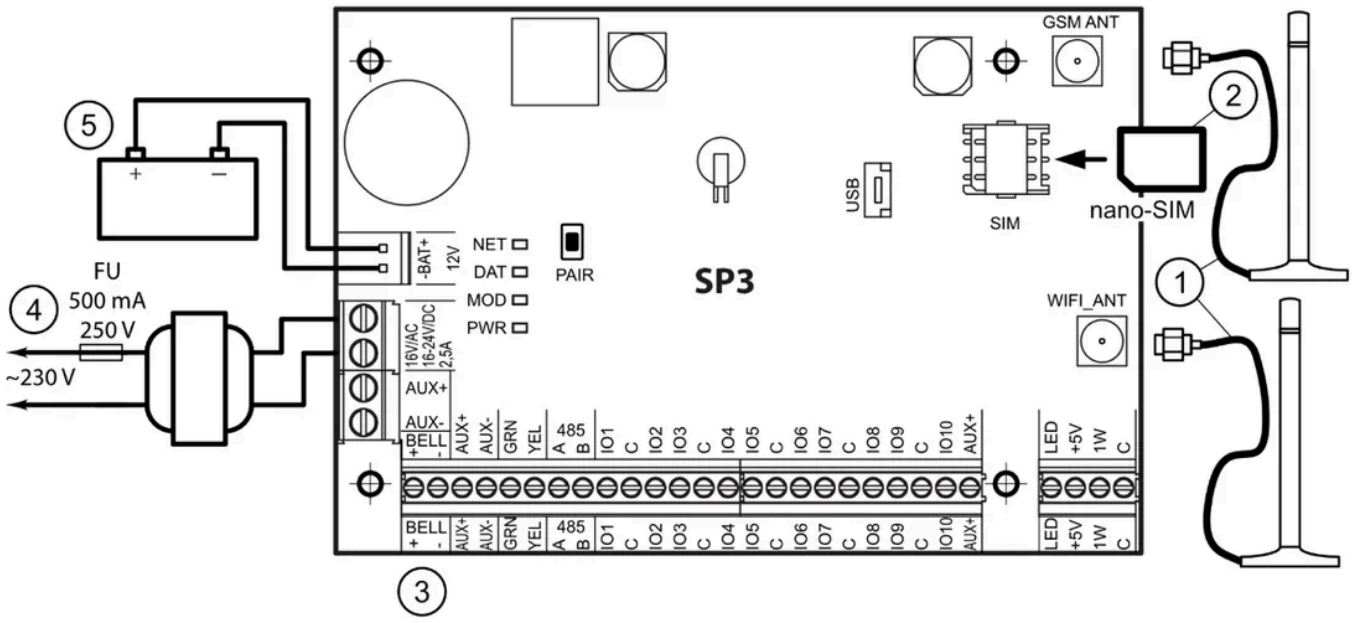


Figure 4. Raccordement de l'alimentation et ordre de la mise en service. Alimentation secteur : transformateur (« Transformer »), ~230 V / 16 V, 40 VA, 50 Hz, avec un fusible de 500 mA / 250 V (FU) sur la branche 230 V, ou alimentation en courant continu 16–24 V, 2,5 A (« or DC power supply source 16-24 V, 2,5 A ») ; alimentation de secours : batterie (« Battery »), 12 V, 7 Ah.

- 1 Visser les antennes mobile et Wi-Fi sur les connecteurs d'antenne
- 2 Insérer la carte nano-SIM dans le logement SIM
- 3 Raccorder les appareils aux borniers
- 4 Raccorder l'alimentation secteur aux bornes AC/DC
- 5 Raccorder la batterie aux bornes BAT+ / BAT−

1. **Concevez le système.** Déterminez l'emplacement du coffret, des claviers, des signalisations sonores et lumineuses et des appareils commandés ; en fonction de la zone à protéger et des caractéristiques des détecteurs, décidez du nombre, du type et de l'emplacement des détecteurs.
2. **Montez la carte dans le coffret** avec les entretoises en plastique, et mettez le coffret métallique à la terre (section 3.1).
3. **Vissez les antennes** (mobile et Wi-Fi) et insérez la carte nano-SIM activée (version avec modem).

4. **Raccordez les appareils** selon les schémas de raccordement : détecteurs d'ouverture, détecteurs de mouvement, d'incendie et autres (3.2–3.3), sirène (3.4), claviers et lecteurs (3.5–3.6), sonde de température (3.7), relais et voyant (3.8), contact d'autoprotection du coffret ; extensions et récepteurs radio selon le chapitre 4.
5. **Mettez l'alimentation secteur** sur les bornes AC/DC. À la mise sous tension, la centrale reconnaît les claviers, extensions et lecteurs correctement raccordés aux bus 1-WIRE et GRN / YEL (section 3.9).
6. **Raccordez la batterie** aux bornes BAT+ / BAT−.
7. **Configurez la centrale avec TrikdisConfig** par câble USB (chapitre 6). Les réglages d'usine conviennent à la plupart des petits et moyens sites ; ce qu'il faut généralement vérifier : les partitions et les données de base du système (**System Options**, 6.2), le type et le comportement des zones (**Zones**, 6.7), les utilisateurs, leurs codes et numéros de téléphone (**Users & Reporting**, 6.4), l'heure exacte (6.2), les données de la carte SIM (6.2), les récepteurs de télésurveillance – désactivés en usine (**Reporting to CMS**, 6.3) –, le cloud Protegus – activé en usine – et les notifications SMS (6.4, 6.10), le fonctionnement des sorties PGM (6.8). Les recommandations en détail :
    - **Système.** Si vous voulez armer les groupes de zones séparément, divisez le système en partitions et définissez les propriétés des partitions (6.2.2). Réglez chaque zone selon les caractéristiques du détecteur et le comportement d'alarme souhaité pour l'événement de la zone (6.7) ; dans un système divisé en partitions, vous attribuez chaque zone à la partition souhaitée. Pour l'utilisation depuis le clavier, avec une clé iButton ou par téléphone (par SMS), il faut créer des utilisateurs et leur donner des droits (6.4).
    - **Envoi des messages.** L'heure exacte doit être réglée pour que les messages reçoivent un horodatage correct (6.2.1). Le rapport d'événements est autorisé en usine pour tous les événements : lorsqu'un événement se produit, son rapport est envoyé aux destinataires configurés sur les canaux configurés ; vous pouvez interdire le rapport de certains événements dans la fenêtre **System events** (6.10). Si la centrale transmet par le réseau mobile, saisissez les données de la carte SIM (6.2.1). La transmission vers la télésurveillance est désactivée en usine (6.3). Le cloud Protegus est activé en usine, la notification par SMS et l'appel sont désactivés en usine ; le réglage de l'envoi vers le téléphone de l'utilisateur se trouve à la section 6.10.
    - **Commande à distance.** Par appel et par SMS, peut commander le système toute personne dont le numéro de téléphone figure dans la liste des utilisateurs (6.4). Par appel, on peut non seulement armer et désarmer tout ou partie du système, mais aussi allumer et éteindre les équipements raccordés aux sorties PGM – ce qu'il faut régler pour cela sur la sortie est décrit à la section 5.4. Par SMS, on peut aussi modifier certains paramètres de fonctionnement de la centrale, armer et désarmer tout ou partie du système et commander les équipements raccordés aux sorties PGM – la liste des commandes se trouve à la section 5.3.
8. **Remplacez les codes d'usine** par des valeurs connues de vous seul : le code maître dans la fenêtre **Users & Reporting**, le mot de passe SMS dans le champ **SMS Password** du groupe **System Options** → **Access**, les codes d'accès de TrikdisConfig dans ce même groupe **Access**.
9. **Associez le système à l'application Protegus 2** (section 5.1).
10. **Vérifiez le fonctionnement** selon le chapitre 8 : événement depuis le clavier, réception par la télésurveillance et dans Protegus 2, sorties, armement à distance.

3. Installation et raccordement

Figyelem!

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

Ce chapitre décrit le montage de la carte, l'ordre du raccordement, puis le raccordement des détecteurs, des détecteurs de fumée, des sirènes, des claviers et lecteurs, des sondes de température ainsi que des relais. La signification des bornes figure dans le tableau de la section 1.5 ; le raccordement des extensions et des modules radio se trouve au chapitre 4. Sur les dessins, les noms des bornes de la SP3 figurent à gauche, ceux de l'appareil raccordé à droite.

3.1 Ordre recommandé de l'installation

Conception du système :

- Esquissez le plan des locaux et indiquez-y l'emplacement du coffret de la centrale, du ou des claviers, des signalisations sonores et lumineuses, ainsi que des équipements commandés automatiquement ou à distance par la centrale.
- En fonction du site, du besoin de protection et des caractéristiques des détecteurs envisagés, décidez du nombre, du type et de l'emplacement des détecteurs.

3.1.1 Montage de la carte dans le coffret

La carte est destinée à un coffret qui contient déjà le transformateur abaisseur (avec un fusible de 500 mA) et l'emplacement de la batterie de secours. Fixez la carte dans le coffret plastique ou métallique choisi à l'aide d'**entretoises en plastique** ; **un coffret métallique doit être mis à la terre**. Le coffret doit satisfaire aux exigences des normes EN 60950 et EN 50131.

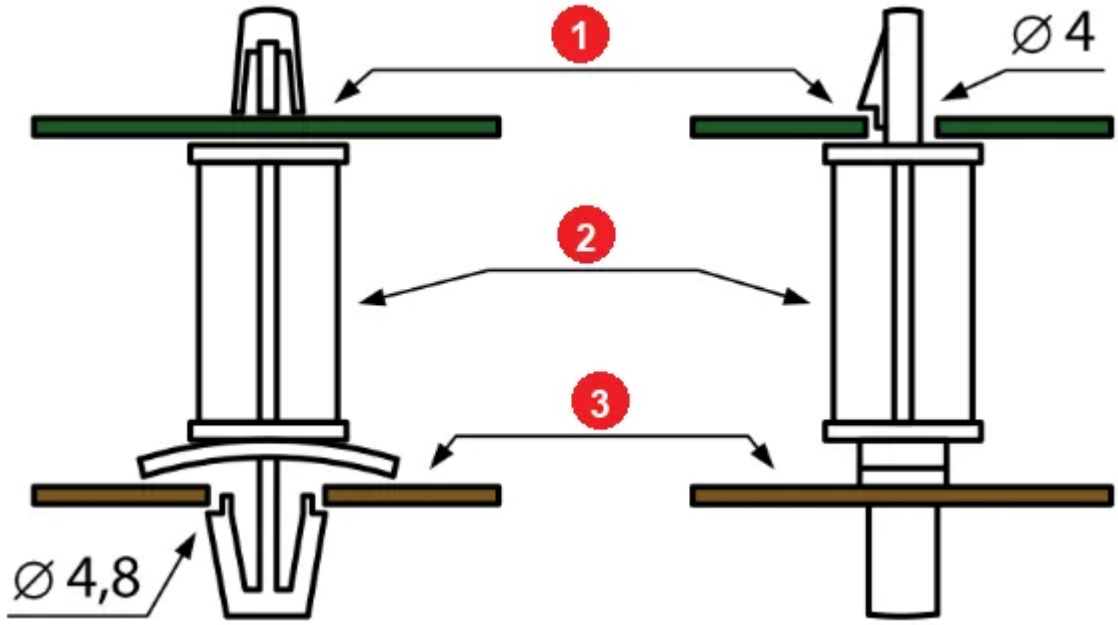


Figure 5. Fixation de la carte avec une entretoise en plastique (à gauche vue de face – « Front view », à droite vue de côté – « Side view »). Le trou de la carte fait Ø4 mm, celui du coffret Ø4,8 mm.

- 1 le circuit imprimé de la SP3 (« SP3 circuit board »)
- 2 entretoise (« Spacer »)
- 3 le coffret (« Box housing »)

Les dimensions de la carte sont de 116,5 × 78,5 mm. Les centres des quatre trous de fixation de Ø4 mm sont distants de 93 mm horizontalement et de 61 mm verticalement ; les trous de gauche sont à 5 mm du bord gauche, ceux du bas à 10 mm du bord inférieur.

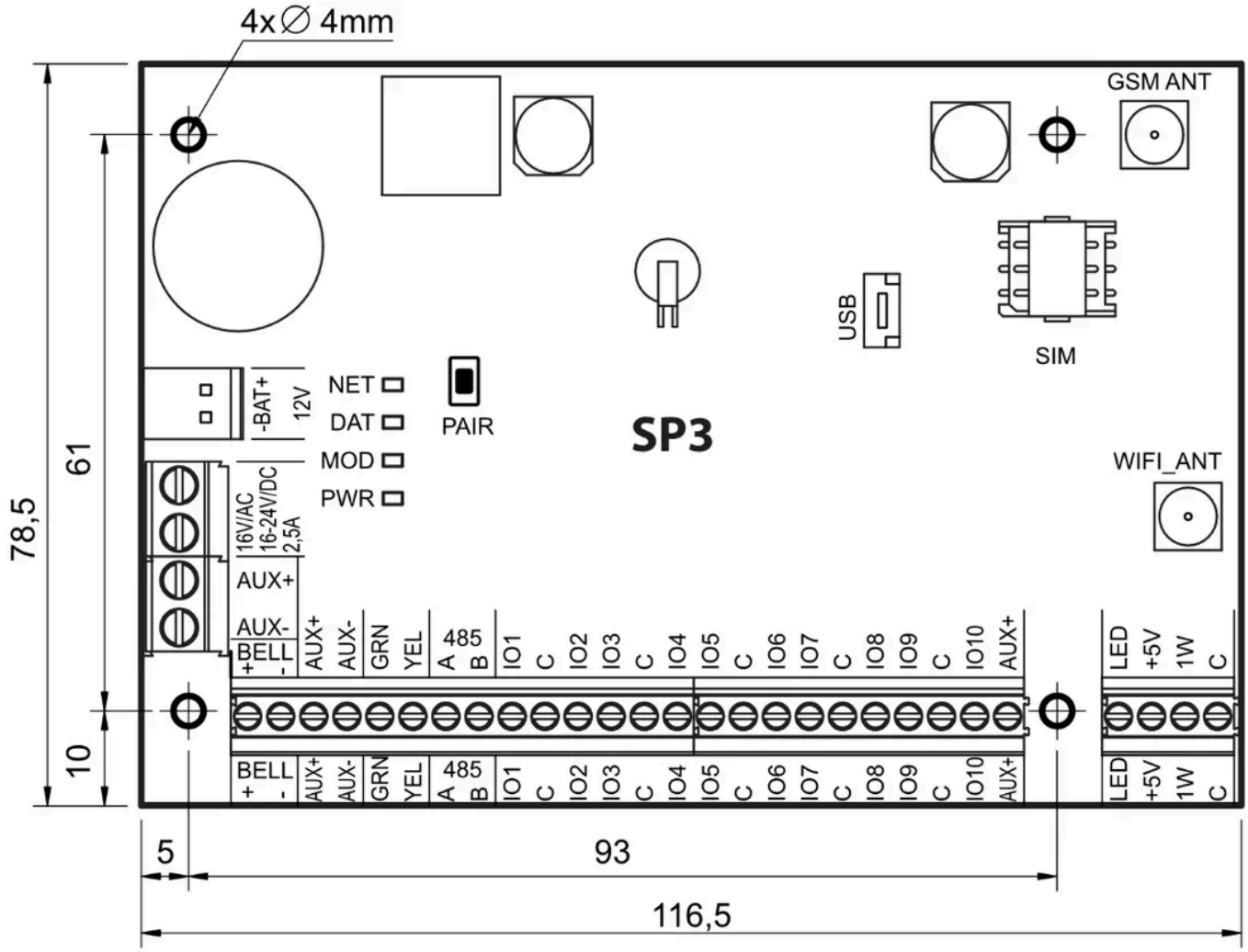


Figure 6. Dimensions de la carte et des trous de fixation en millimètres.

3.1.2 Ordre de raccordement des appareils

Raccordez les appareils dans l'ordre ci-dessous ; l'alimentation et la batterie toujours en dernier.

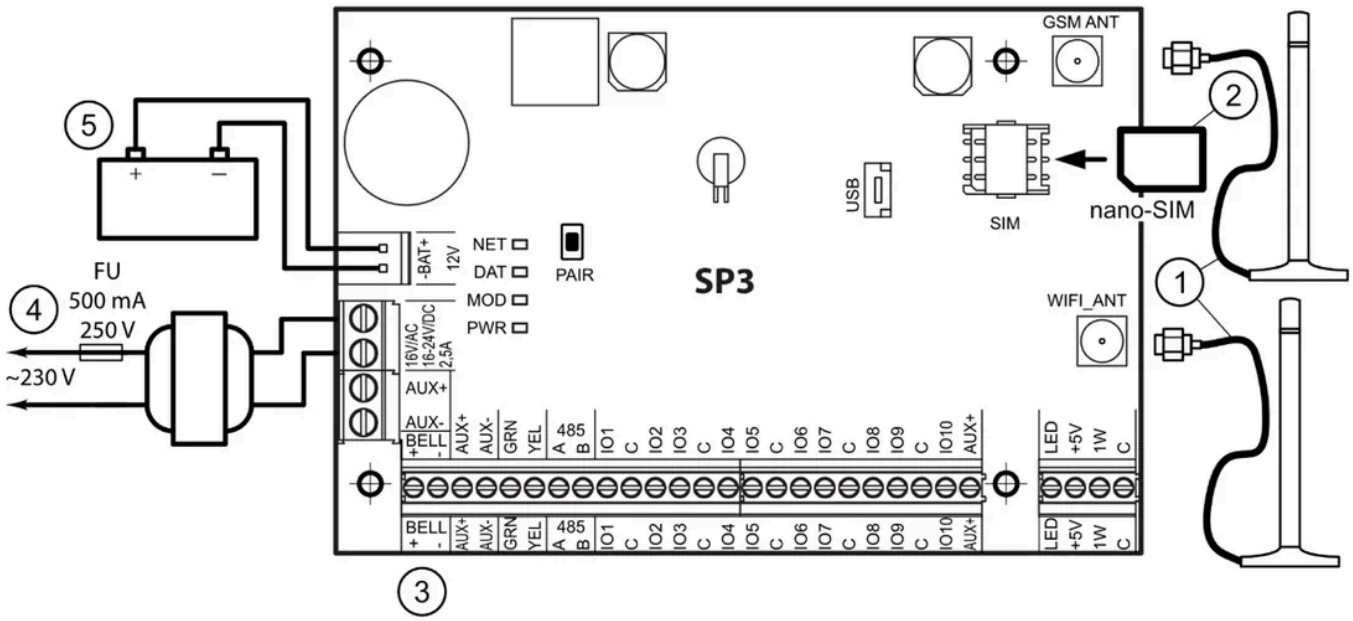


Figure 7. Vue d'ensemble de l'alimentation et des raccordements. Alimentation secteur : transformateur ~230 V / 16 V, 40 VA, 50 Hz (« Transformer » ; avec un fusible de 500 mA, 250 V côté 230 V) ou alimentation en tension continue 16–24 V, 2,5 A (« or DC power supply source 16-24 V, 2,5 A ») ; batterie de secours (« Battery »), 12 V, 7 Ah.

- 1 antennes GSM et Wi-Fi sur les connecteurs d'antenne
- 2 carte nano-SIM dans le logement SIM
- 3 les appareils sur le bornier externe
- 4 alimentation secteur sur les bornes AC/DC
- 5 batterie sur les bornes BAT+ / BAT−

1. Vissez l'**antenne GSM** et l'**antenne Wi-Fi** sur les connecteurs d'antenne (l'une ou les deux selon la version, section 1.2).
2. Sur une version avec modem, insérez la **carte nano-SIM activée** dans le logement. Il est conseillé de désactiver au préalable la demande de code PIN dans un téléphone.
3. Sur une version Ethernet (SP3_3E, SP3_44E), branchez le **câble LAN** dans le connecteur RJ45.
4. En vous basant sur les schémas de raccordement donnés ici, sur les schémas propres aux appareils raccordés et sur le plan, raccordez les détecteurs d'ouverture de portes et fenêtres, les détecteurs de mouvement, d'incendie et autres, les signalisations sonores et lumineuses, les claviers et les appareils commandés. Raccordez également aux bornes de la carte le **contact d'autoprotection** d'ouverture de la porte du coffret et d'arrachement mural.
5. Raccordez les fils de l'alimentation secteur aux bornes **AC/DC** de la carte, et mettez sous tension. La centrale reconnaît les claviers, extensions et interfaces correctement raccordés aux bus 1-WIRE et YEL/GRN.
6. Placez la batterie dans le coffret et raccordez ses cosses aux bornes **BAT+ / BAT−**.

La batterie doit être rechargée en 72 heures pour que le système satisfasse au niveau de sécurité 2 (Grade 2), et en 24 heures pour le niveau 3 (Grade 3).

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

L'ordre recommandé des réglages (partitions, zones, utilisateurs, heure, transmission, commande à distance, changement des codes) est résumé à la section 2.4, le détail au chapitre 6.

3.2 Raccordement des détecteurs

Sur la carte, **10 bornes IO** (IO1–IO10) reçoivent les circuits des détecteurs. En usine, IO1–IO9 sont des entrées, IO10 une sortie PGM (réinitialisation des détecteurs incendie, voir 3.3). Le nombre d'entrées peut être porté à 64 au maximum avec des extensions (iO, iO-8, iO-WL, RF-SH, iO-LORA, iO8-LORA). Chaque borne peut être réglée en entrée (zone), et la page **Zones** (6.7) permet de définir les propriétés de la zone : le type de circuit (**NO, NC, EOL, EOL_T, 3EOL, ATZ, ATZ_T**), la sensibilité aux événements de circuit de courte durée, ainsi que la fonction de la zone (temporisée, instantanée, instantanée stay, suiveuse, suiveuse stay, incendie, interrupteur à clé, 24 heures, silencieuse, silencieuse 24 heures). Les extensions iO-8 et iO8-LORA prennent en charge tous les types de circuit de la centrale.

Résistances de fin de ligne. Pour les circuits EOL, EOL_T, 3EOL, ATZ et ATZ_T, vous pouvez choisir parmi sept jeux de résistances dans TrikdisConfig (**System Options → System general → EOL Type**, 6.2.1) ; lors du remplacement d'une ancienne centrale, les résistances existantes peuvent donc rester dans les détecteurs. RT est la résistance du circuit d'autoprotection, R1 celle du premier détecteur, R2 celle du second (pour le 3EOL, celle du circuit de masquage). À côté de chaque jeu figurent les centrales d'alarme dont les valeurs de résistance d'usine lui correspondent :

Jeu	RT	R1	R2
1 – Trikdis par défaut : Bosch AMAX, Risco LightSYS Plus, Satel INTEGRA (EOL)	**2,2 kΩ**	**2,2 kΩ**	**4,7 kΩ**
2 – Paradox, Honeywell Galaxy Flex, Hikvision AX Hybrid PRO (3EOL)	1 kΩ	1 kΩ	2,2 kΩ
3 – DSC PowerSeries, Eldes ESIM364	5,6 kΩ	5,6 kΩ	3,3 kΩ
4 – Eldes ESIM364 (mode 6 zones, avec autoprotection)	5,6 kΩ	3,3 kΩ	5,6 kΩ
5	3,3 kΩ	6,8 kΩ	3,3 kΩ
6 – Crow Runner, Texecom Premier Elite, Pyronix Enforcer	2,2 kΩ	4,7 kΩ	8,2 kΩ
7	4,7 kΩ	4,7 kΩ	2,2 kΩ

Pour les noms de marques indiqués, les résistances d'autoprotection et de détecteur (RT, R1) correspondent ; pour la Satel INTEGRA, c'est le raccordement à une seule résistance (EOL). Pour le doublement de zones (ATZ) et le raccordement 3EOL, R2 doit aussi correspondre : c'est le cas pour Paradox et Hikvision AX Hybrid PRO avec le jeu 2, pour Eldes ESIM364 avec le jeu 3, et pour Crow Runner avec le jeu 6. Là où la valeur de résistance était réglable dans l'ancienne centrale (par exemple Crow, Risco, Honeywell Galaxy, Pyronix, Texecom), c'est la résistance présente dans les détecteurs qui décide. Les raccordements Honeywell VISTA (2 kΩ) et Satel à deux résistances (2EOL, 2 × 1,1 kΩ) ne correspondent à aucun jeu.

3.2.1 Schémas de raccordement

Sur les figures, **IOx** est la borne IO choisie, **C** la borne négative commune ; NC est un contact normalement fermé, NO un contact normalement ouvert.

Repères sur les dessins. R1, R2, RT – résistance ; RT est la résistance du circuit d'autoprotection. Le **T** rouge désigne le contact d'autoprotection, le chiffre bleu le numéro du détecteur ; la signification de chaque repère figure aussi sous le dessin concerné.

NO – normalement ouvert, sans résistance de fin de ligne. Lorsqu'il se déclenche, le détecteur ferme le circuit entre IOx et C.

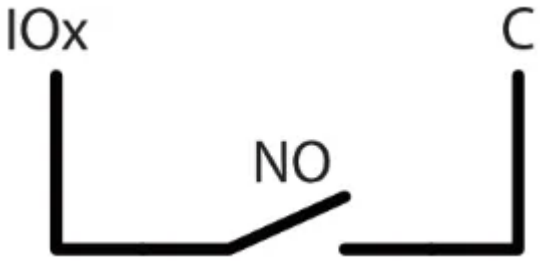


Figure 8. Zone NO : le contact normalement ouvert entre les bornes IOx et C.

NC – normalement fermé, sans résistance de fin de ligne. Lorsqu'il se déclenche, le détecteur ouvre le circuit entre IOx et C.

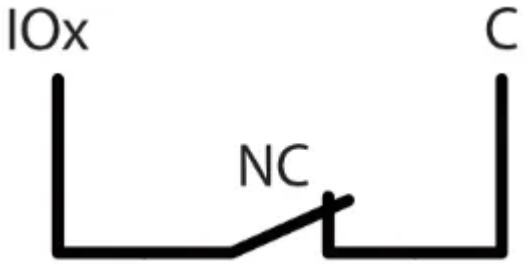


Figure 9. Zone NC : le contact normalement fermé entre les bornes IOx et C.

EOL – avec résistance de fin de ligne. Pour un détecteur NO, R1 est en parallèle avec le contact, pour un détecteur NC en série avec lui, entre IOx et C ; la centrale détecte ainsi aussi la coupure et le court-circuit du câble.

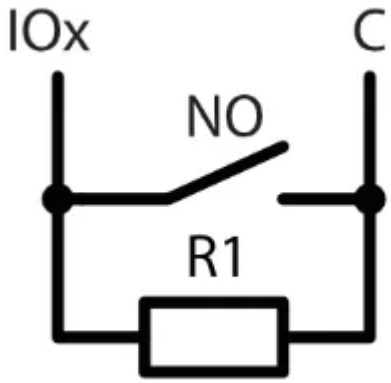


Figure 10. Zone NO avec résistance de fin de ligne (EOL) : R1 en parallèle avec le contact ouvert, entre IOx et C.

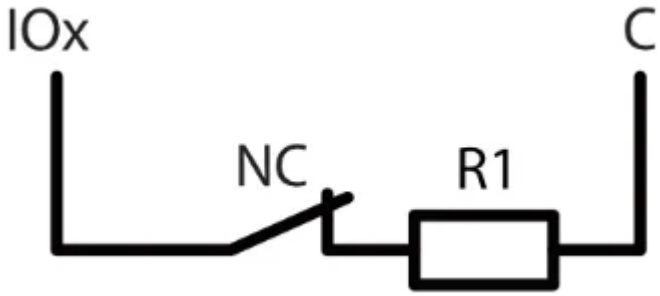


Figure 11. Zone NC avec résistance de fin de ligne (EOL) : R1 en série avec le contact fermé, entre IOx et C.

EOL_T – avec résistance de fin de ligne, détection de l'autoprotection et des défauts de câble. En partant de IOx, le contact d'autoprotection NC et RT en série, puis le contact d'alarme NC en parallèle avec R1 entre RT et C.

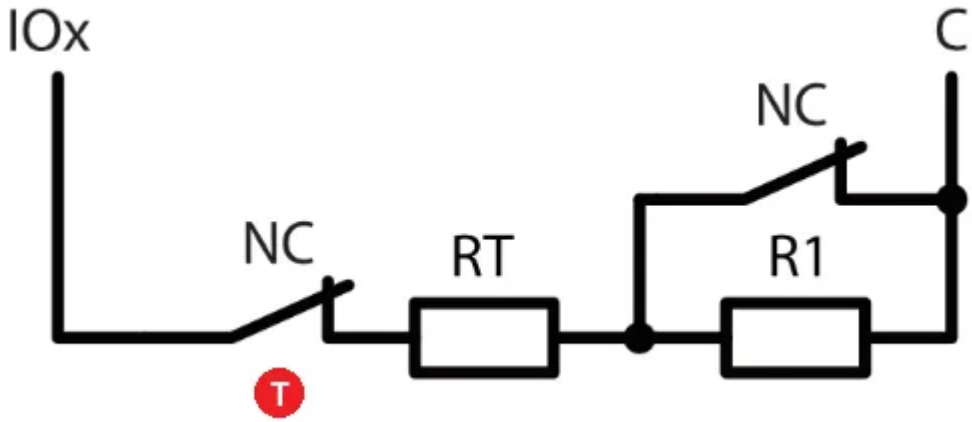


Figure 12. Zone EOL_T : IOx → contact d'autoprotection NC → RT → (contact d'alarme NC en parallèle avec R1) → C.

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

ATZ – doublement de zones. Deux détecteurs sur une borne : entre IOx et C, deux circuits en série, dans le premier un contact NC en parallèle avec R1, dans le second un contact NC en parallèle avec R2. On peut ainsi gérer 20 zones sur les 10 bornes.

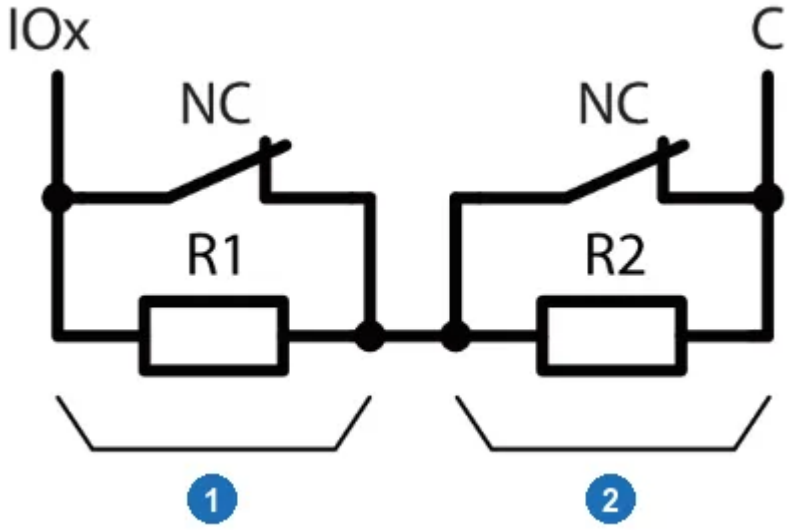


Figure 13. Zone ATZ : le contact NC du détecteur 1 en parallèle avec R1, en série avec le contact NC du détecteur 2 en parallèle avec R2, entre IOx et C.

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

ATZ_T – doublement de zones avec détection de l'autoprotection et des défauts de câble. Comme ATZ, mais le contact d'autoprotection NC est aussi en série dans le circuit de chacun des deux détecteurs, dans le premier circuit avec la résistance RT.

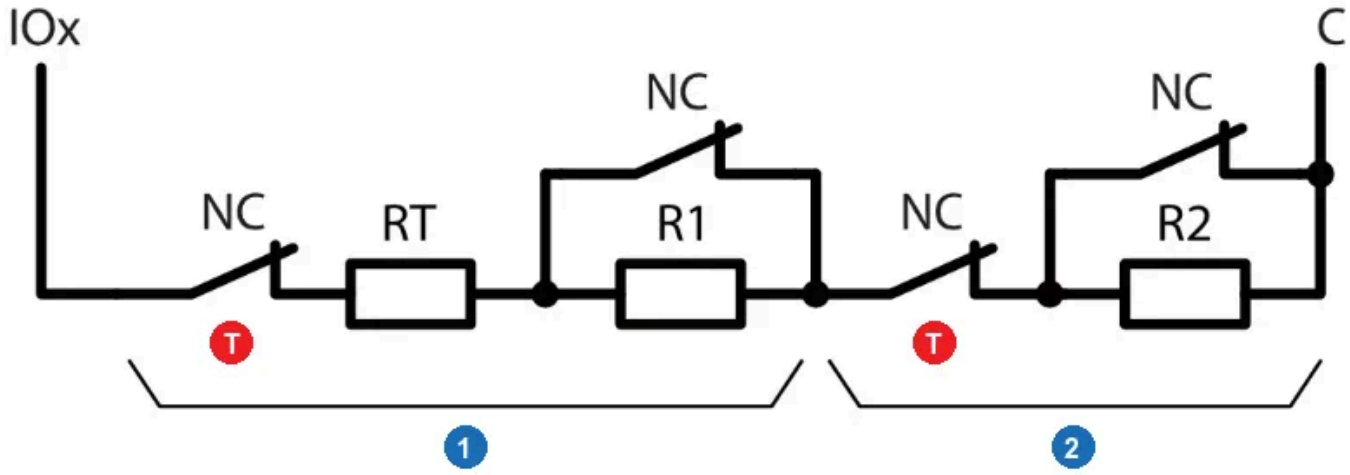


Figure 14. Zone ATZ_T : détecteur 1 – contact d'autoprotection NC et RT en série, puis contact NC en parallèle avec R1 ; détecteur 2 – contact d'autoprotection NC en série, puis contact NC en parallèle avec R2 ; les deux circuits en série entre IOx et C.

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

3EOL – trois résistances de fin de ligne : alarme, autoprotection et masquage. Dans un même détecteur, les circuits d'autoprotection, d'alarme et d'anti-masquage (anti-masking) sont détectés séparément.

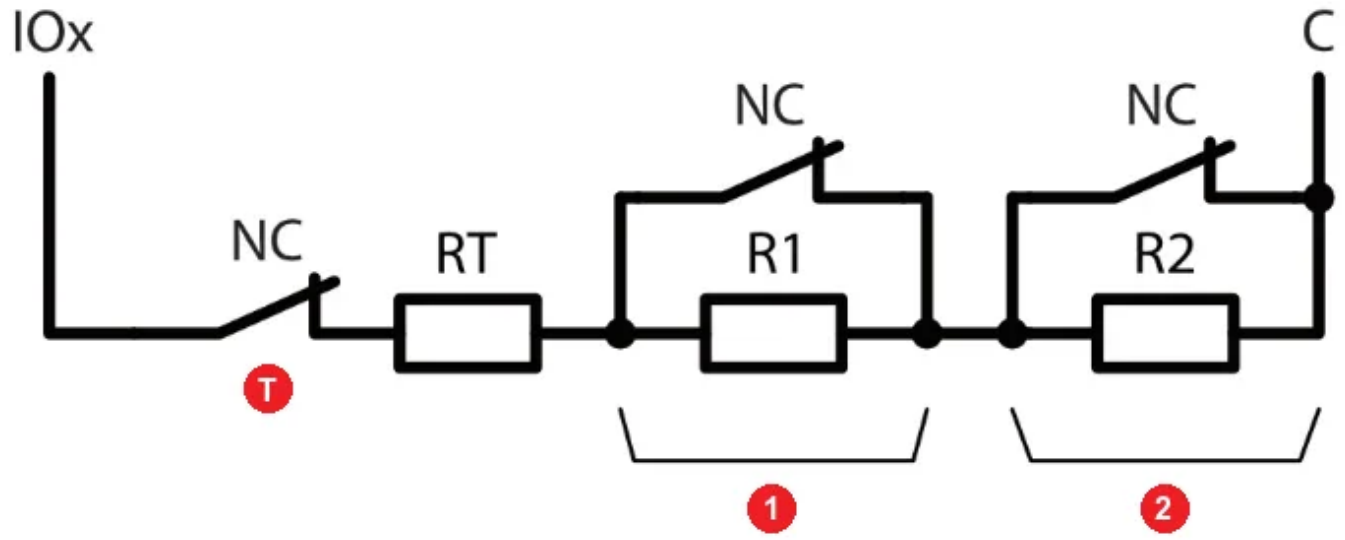


Figure 15. Zone 3EOL : IOx → contact d'autoprotection NC et RT en série → circuit d'alarme (contact NC en parallèle avec R1) → circuit de masquage (contact NC en parallèle avec R2) → C.

- T contact d'autoprotection (« Tamper »), signale l'ouverture du boîtier du détecteur
- 1 circuit d'alarme (« Alarm »)
- 2 circuit anti-masquage (« Anti-masking »), signale le masquage du détecteur

3.3 Raccordement des détecteurs de fumée

Détecteurs de fumée deux fils sur la sortie LED. Si vous raccordez les détecteurs incendie de cette façon, cochez la case **LED out as 2Wire fire** sur la page **System Options** (6.2).

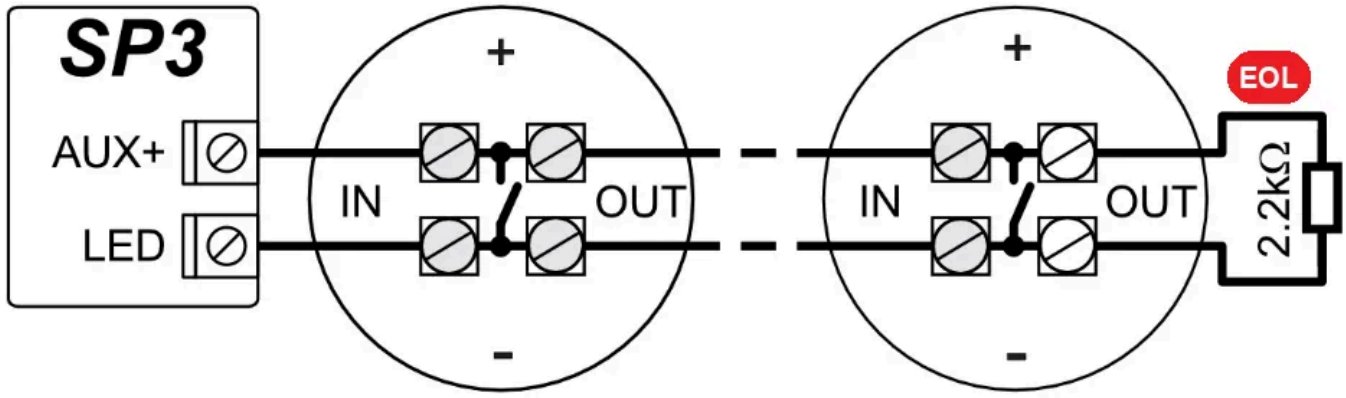


Figure 16. Détecteurs de fumée deux fils sur la sortie LED : AUX+ → borne + IN du premier détecteur, LED → − IN ; les bornes + OUT et − OUT de chaque détecteur vers la même borne IN du détecteur suivant ; après le dernier détecteur, une résistance de fin de ligne de 2,2 kΩ entre le fil + et le fil −.

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

Détecteurs de fumée quatre fils. Attribuez la fonction de zone **incendie** à l'entrée (IOx) du circuit des détecteurs de fumée (6.7). L'alimentation des détecteurs quatre fils est commutée par la sortie PGM IO10, à laquelle est associée la fonction **Fire Sensor Reset** (réinitialisation des détecteurs incendie) (6.8) – c'est le réglage d'usine de IO10. Le relais K1 signale la coupure du câble et le retrait du détecteur.

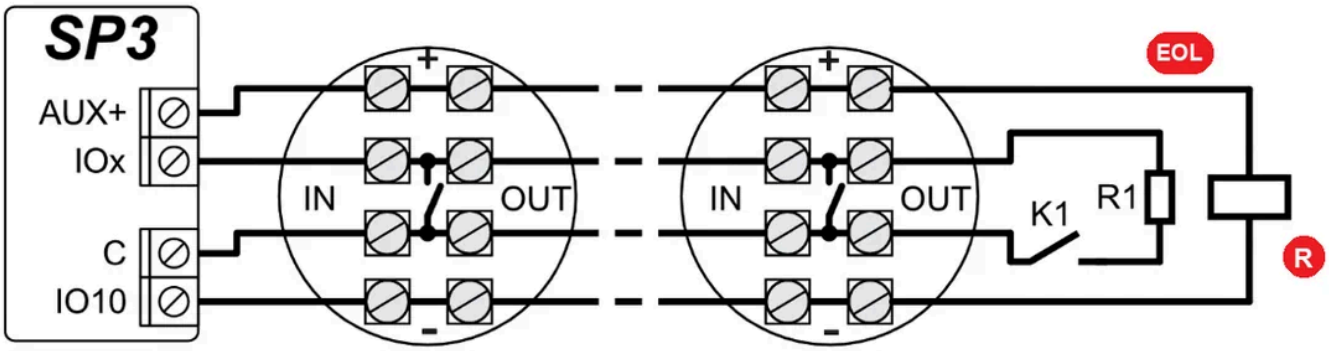


Figure 17. Détecteurs de fumée quatre fils avec relais K1. De haut en bas : AUX+ → borne + du premier détecteur, IOx → contact supérieur, C → contact inférieur, IO10 → − IN ; les quatre bornes OUT vers la même borne IN du détecteur suivant ; après le dernier détecteur, le contact de K1 et la résistance de fin de ligne R1 en série entre les fils IOx et C ; la bobine de K1 entre les fils AUX+ et IO10.

- R relais **K1** (« Relay »)
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

Détecteurs de fumée deux fils avec l'interface SM1. Avec l'interface SM1, les détecteurs deux fils peuvent être raccordés à une entrée IO ; ici aussi, le relais K1 signale la coupure du câble et le retrait du détecteur. Le circuit de surveillance peut être réalisé de deux façons :

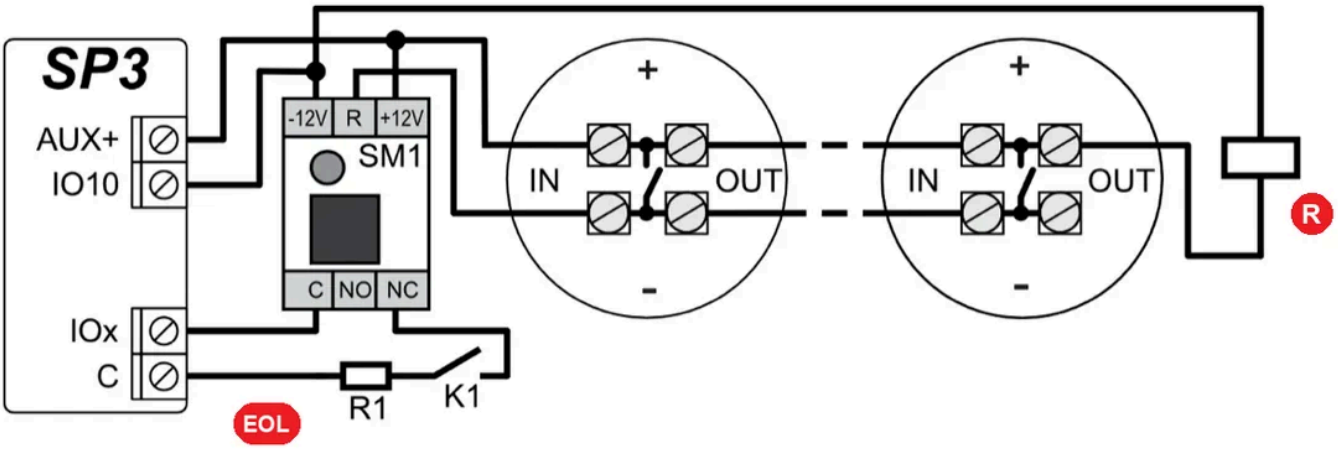


Figure 18. Détecteurs de fumée deux fils avec l'interface SM1 : AUX+ → SM1 +12V et + IN du premier détecteur ; IO10 → SM1 −12V et bobine de K1 ; SM1 R → − IN du détecteur ; les bornes IN/OUT des détecteurs en chaîne, le dernier + OUT vers K1. Circuit de surveillance : IOx → SM1 C ; borne C de la SP3 → résistance de fin de ligne R1 → contact de K1 → SM1 NC.

- R relais **K1** (« Relay »)
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

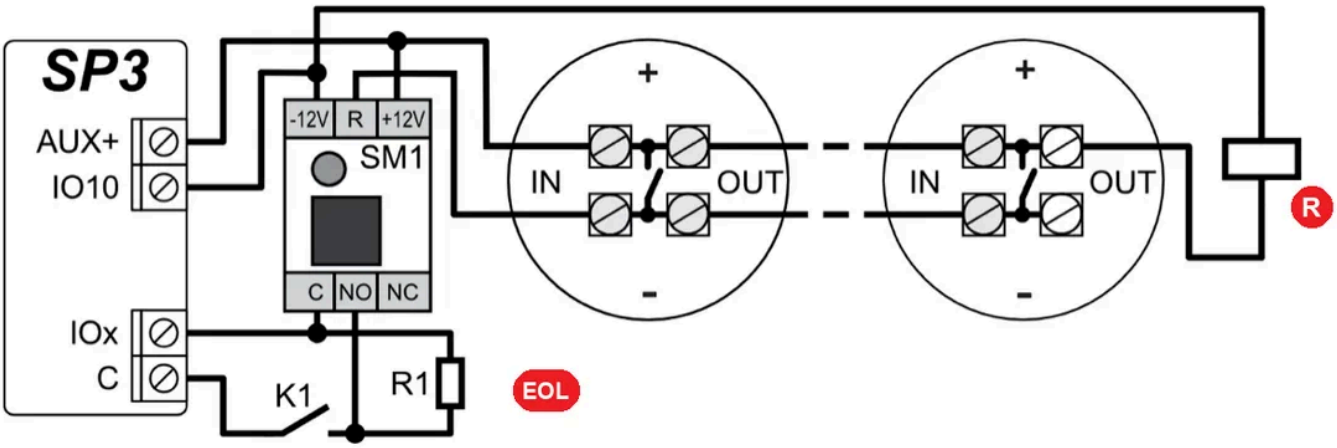


Figure 19. Le même avec l'autre circuit de surveillance : R1 entre les bornes C et NO de la SM1 ; la borne C de la SP3 vers la borne NO de la SM1 via le contact de K1.

- R relais **K1** (« Relay »)
- EOL la résistance de fin de ligne **R1** (« End of line resistor »)

3.4 Raccordement de la sirène

Raccordez la sirène à la sortie **BELL+ / BELL−** (la sortie BELL supporte 1 A, voir les caractéristiques techniques à la section 1.3).

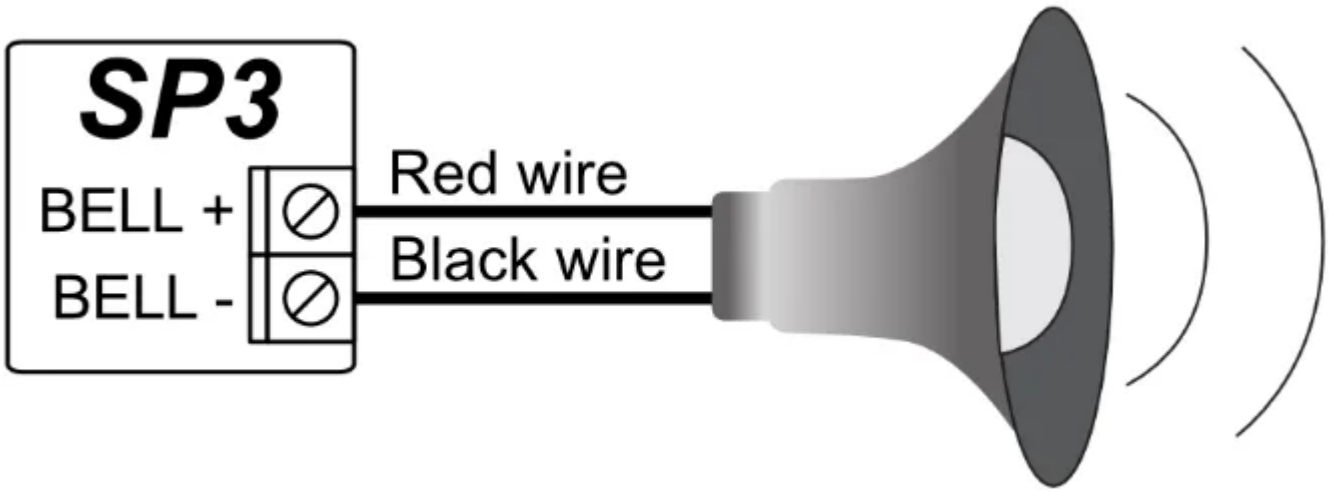


Figure 20. Sirène sur la sortie BELL : BELL+ → fil rouge, BELL− → fil noir.

Pour la sirène extérieure MR100, le circuit d'autoprotection (SAB) est aussi surveillé par la centrale : en usine avec une EOL de 2,2 kΩ, sur l'entrée **IO9**. IO9 est en usine une zone 24 heures, mais elle peut être librement modifiée. Si vous surveillez le circuit d'autoprotection de la sirène dans la centrale avec un autre mode EOL, fermez les contacts JPS1 et placez en série dans le circuit d'autoprotection une résistance de valeur appropriée.

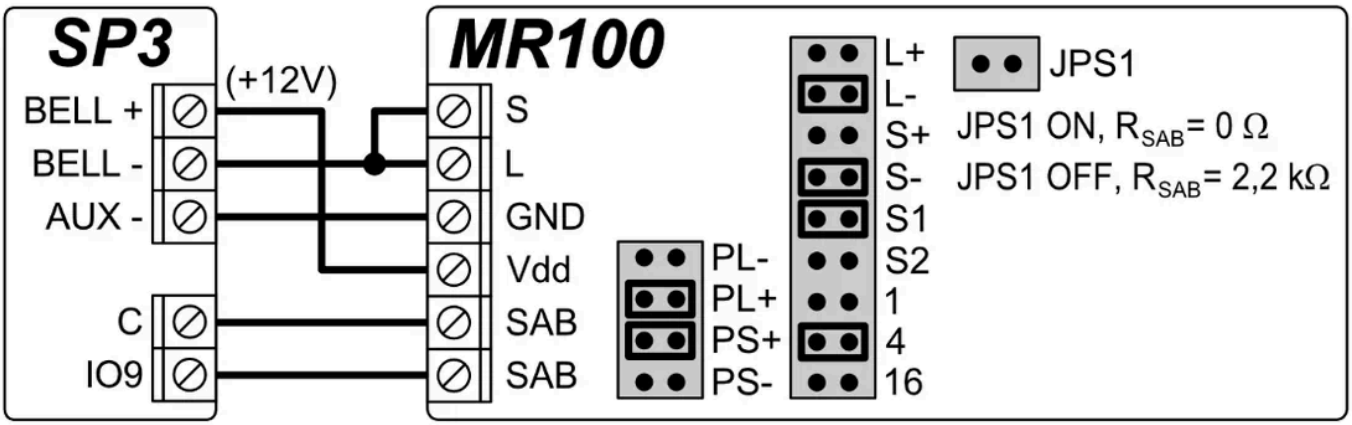


Figure 21. Sirène extérieure MR100 (« Outdoor siren ») : BELL+ (+12 V) → Vdd, BELL− → S et L, AUX− → GND, C et IO9 → les deux bornes SAB (autoprotection). Points court-circuités sur le dessin : PL+, PS+, L−, S−, S1 et 4. JPS1 fermé (« ON ») : R_SAB = 0 Ω, JPS1 ouvert (« OFF ») : R_SAB = 2,2 kΩ.

3.5 Raccordement des claviers et des lecteurs RFID

Cette section concerne les claviers sur bus clavier et les lecteurs RFID au protocole Wiegand 26/34. Jusqu'à **8 claviers du même type** peuvent être raccordés au bus clavier (**GRN**, **YEL**). Indiquez le type de clavier sur la page **Modules** (6.5) ; la centrale reconnaît et attribue automatiquement les appareils raccordés. Le clavier possède aussi sa propre entrée de zone (ZONE) : l'autre extrémité du détecteur qui y est raccordé va à la borne AUX−. L'utilisation du système depuis les claviers (codes utilisateur, exclusion de zones, iButton et RFID, appel, SMS, sorties PGM) est décrite dans le manuel utilisateur SP3 distinct, réalisé pour les claviers Protegus et Paradox.

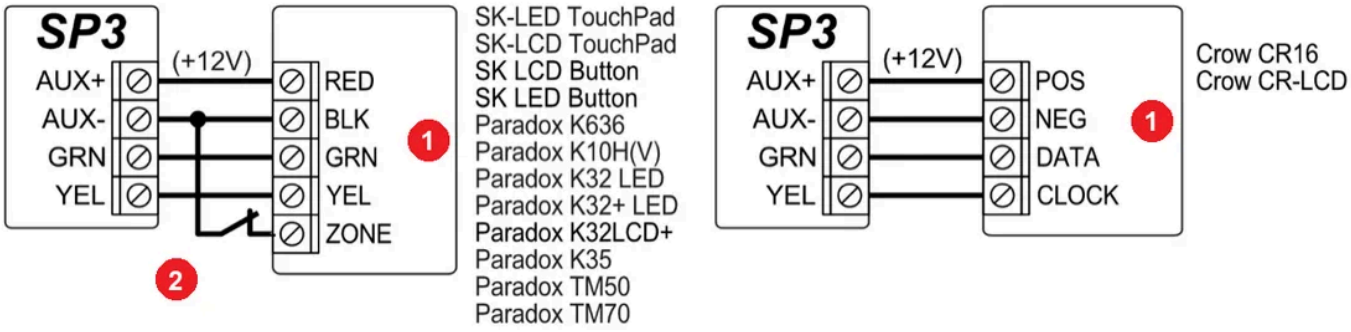


Figure 22. Raccordement des claviers. SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, ainsi que Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50, TM70 : AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL ; la borne ZONE du clavier vers la borne AUX− via le contact du détecteur. Crow CR16 et CR-LCD : AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK.

- 1 clavier (« Keypad »)
- 2 zone du clavier (« Keypad zone »)

Lecteur RFID (Wiegand 26/34). 2 lecteurs au maximum peuvent être raccordés à la centrale. Les fils de données du lecteur (D0, D1) vont soit sur le bus clavier (GRN, YEL), soit sur les bornes **IO1** et **IO2**, selon les figures. S'il y a deux lecteurs (côté entrée et côté sortie), aucun clavier ne peut plus être raccordé à la centrale.

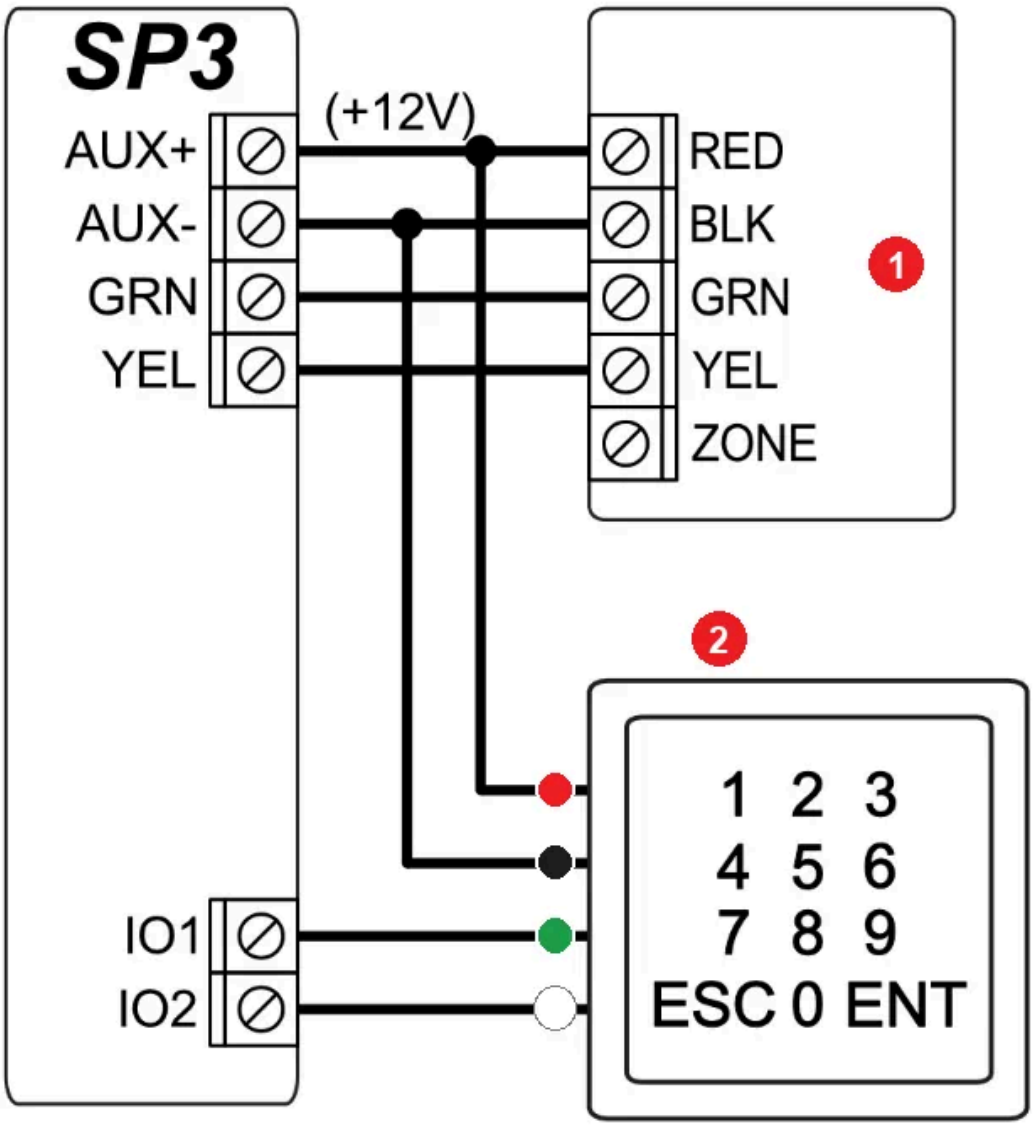


Figure 23. Clavier et lecteur d'entrée ensemble. Le clavier (SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50 ou TM70) sur le bus selon la figure précédente : AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL ; fil rouge du lecteur (+U) → AUX+, noir (GND) → AUX−, vert (D0) → IO1, blanc (D1) → IO2.

- 1 clavier (« Keypad »)
- 2 lecteur d'entrée : lecteur RFID à clavier, Wiegand 26/34 (« Entry reader », « RFID reader with keypad (Wiegand 26/34) »)
- fil rouge, +U (« R - red wire (+U) »)
- fil noir, GND (« B - black wire (GND) »)
- fil vert, D0 (« G - green wire (D0) »)
- fil blanc, D1 (« W - white wire (D1) »)

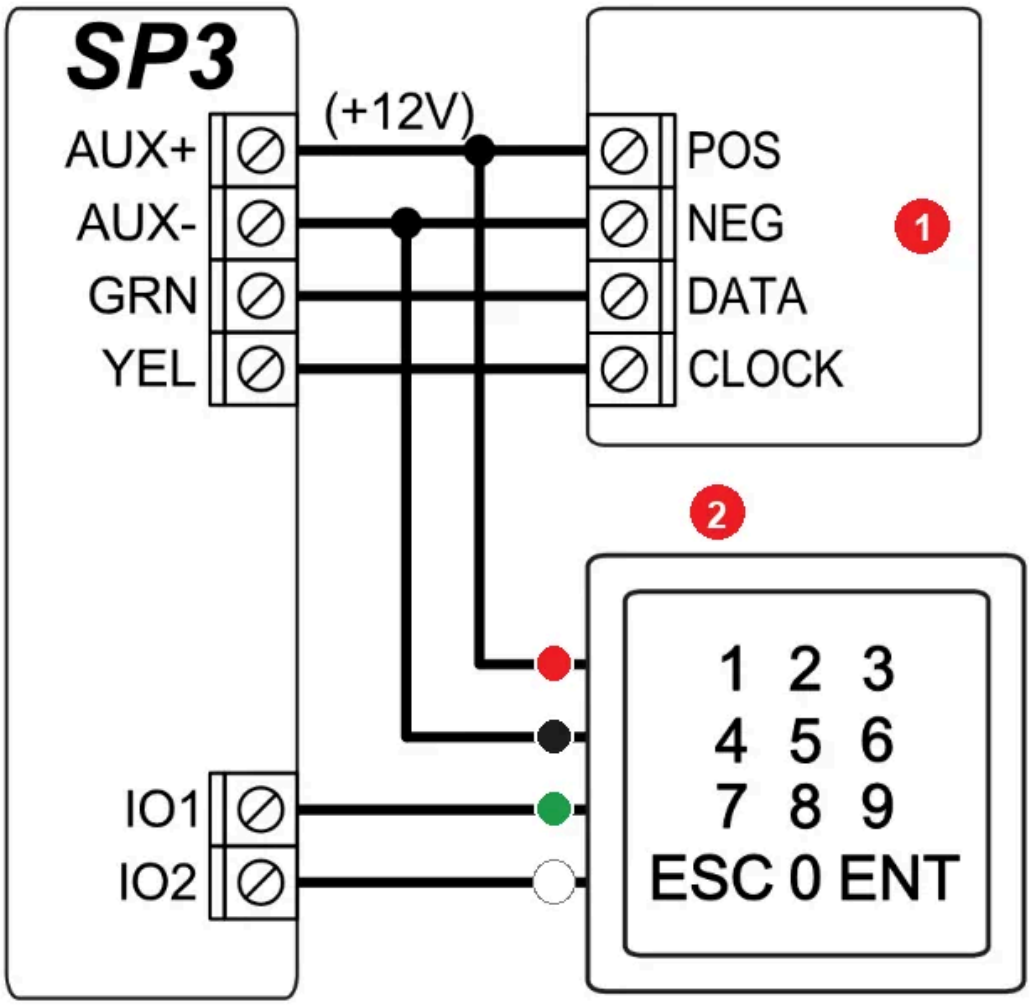


Figure 24. Clavier Crow CR16 ou Crow CR-LCD et lecteur d'entrée ensemble. Le clavier sur le bus : AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK ; fil rouge du lecteur (+U) → AUX+, noir (GND) → AUX−, vert (D0) → IO1, blanc (D1) → IO2.

- 1 clavier (« Keypad »)
- 2 lecteur d'entrée : lecteur RFID à clavier, Wiegand 26/34 (« Entry reader », « RFID reader with keypad (Wiegand 26/34) »)
- fil rouge, +U (« R - red wire (+U) »)
- fil noir, GND (« B - black wire (GND) »)
- fil vert, D0 (« G - green wire (D0) »)
- fil blanc, D1 (« W - white wire (D1) »)

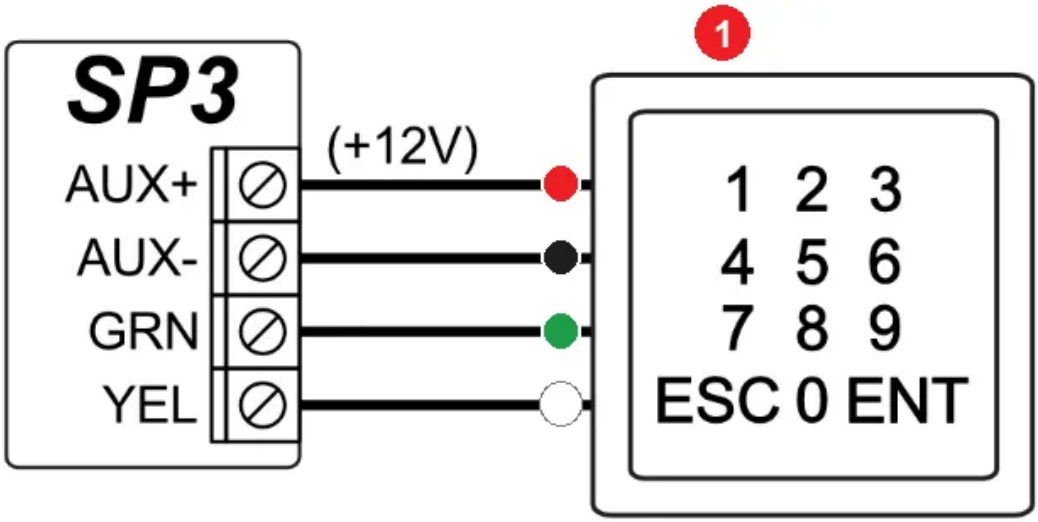


Figure 25. Un seul lecteur sur le bus clavier, sans clavier : fil rouge du lecteur (+U) → AUX+, noir (GND) → AUX−, vert (D0) → GRN, blanc (D1) → YEL.

- 1 lecteur d'entrée : lecteur RFID à clavier, Wiegand 26/34 (« Entry reader », « RFID reader with keypad (Wiegand 26/34) »)
- fil rouge, +U (« R - red wire (+U) »)
- fil noir, GND (« B - black wire (GND) »)
- fil vert, D0 (« G - green wire (D0) »)
- fil blanc, D1 (« W - white wire (D1) »)

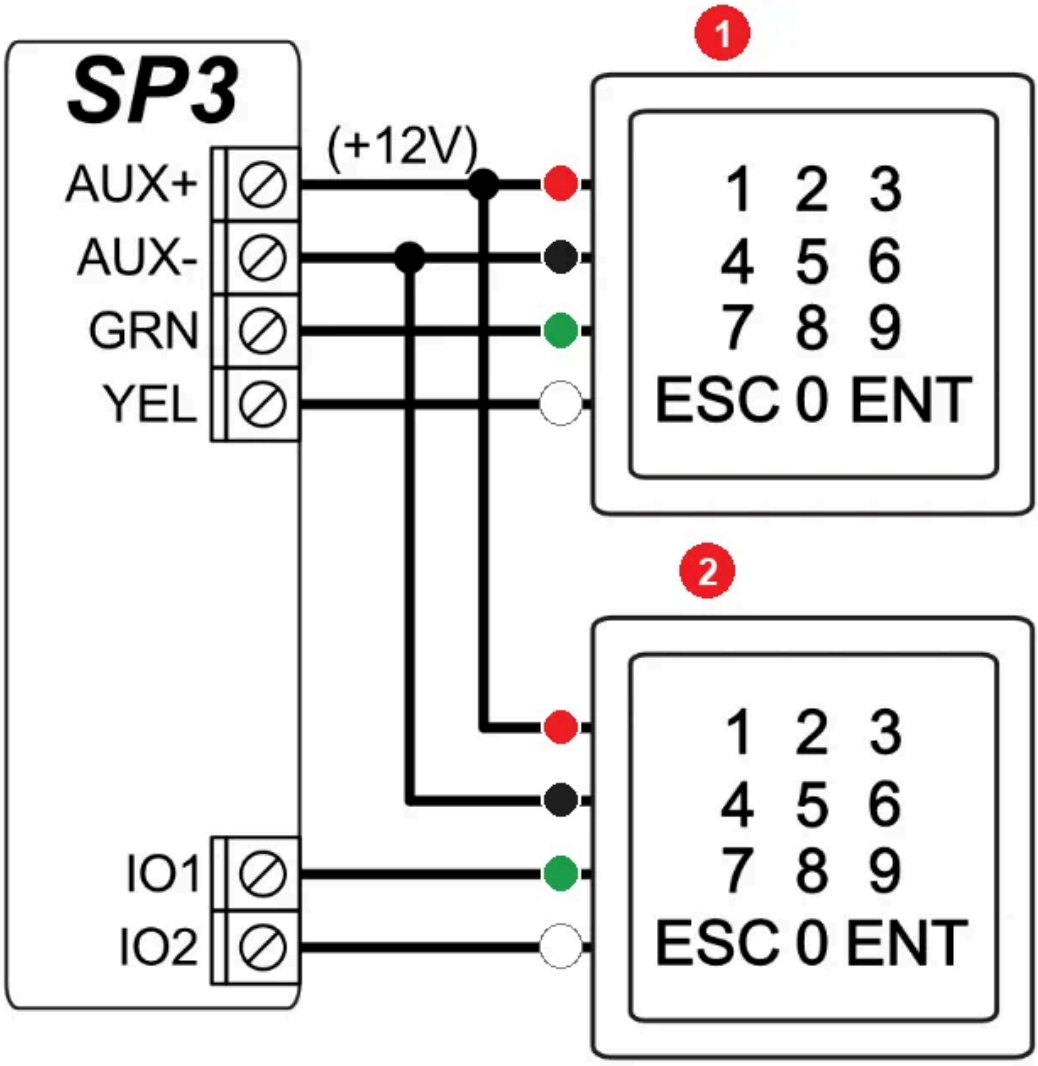


Figure 26. Deux lecteurs, tous deux des lecteurs RFID à clavier, Wiegand 26/34 (« RFID reader with keypad (Wiegand 26/34) »). Lecteur d'entrée : fil rouge (+U) → AUX+, noir (GND) → AUX−, vert (D0) → GRN, blanc (D1) → YEL. Lecteur de sortie : rouge (+U) → AUX+, noir (GND) → AUX−, vert (D0) → IO1, blanc (D1) → IO2.

- 1 lecteur d'entrée (« Entry reader »)
- 2 lecteur de sortie (« Exit reader »)
- fil rouge, +U (« R - red wire (+U) »)
- fil noir, GND (« B - black wire (GND) »)
- fil vert, D0 (« G - green wire (D0) »)
- fil blanc, D1 (« W - white wire (D1) »)

3.6 Raccordement des lecteurs de clés TM17 et CZ-Dallas

Accessoire plus fabriqué

Le lecteur de clés iButton **TM17** est un accessoire qui n'est plus fabriqué et n'est plus disponible. Sa description est conservée pour les systèmes existants.

Le lecteur de clés iButton **CZ-Dallas** se raccorde au bus **1 WIRE**, avec un câble de 30 m au maximum. Le lecteur **TM17** se raccorde au bus **RS485**, avec un câble de 100 m au maximum.

Les valeurs « 30 m au maximum » et « 100 m au maximum » sont des maximums théoriques, dans des conditions idéales – voir la remarque de la section 1.3.

Pour la signalisation lumineuse du CZ-Dallas, réglez le type de la sortie **LED** sur **System state** (état du système) (6.8) : système armé, l'anneau du lecteur est rouge ; désarmé, il est jaune.

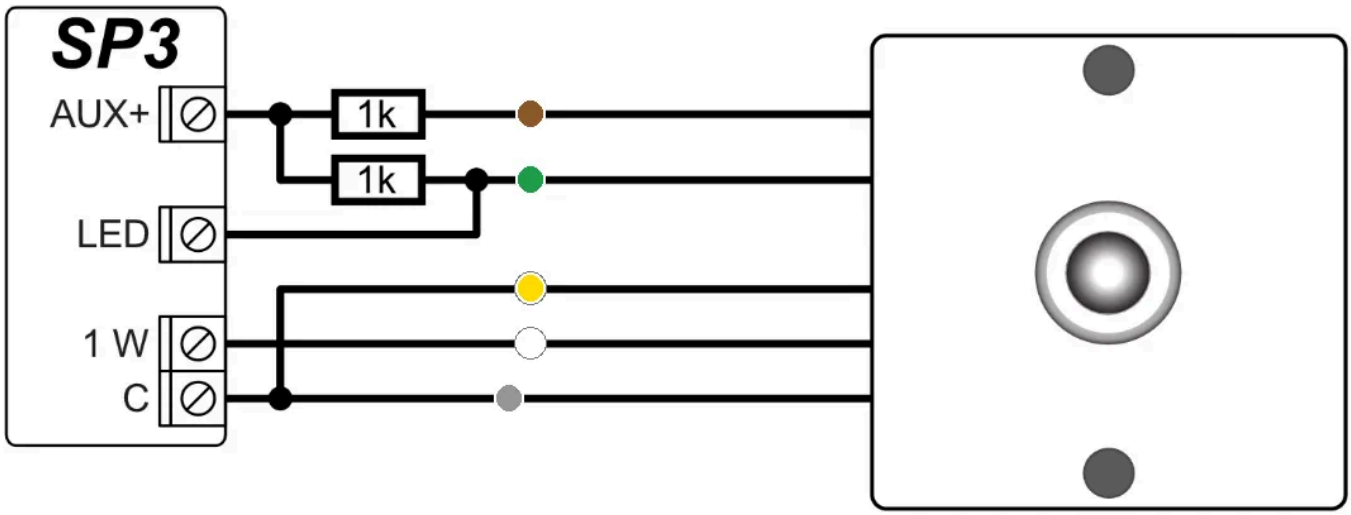


Figure 27. Lecteur CZ-Dallas (« CZ-Dallas reader ») : AUX+ → via une résistance de 1 kΩ chacun, vers le fil marron (RED LED+) et le fil vert (GREEN LED+) ; la sortie LED vers le fil vert, après la résistance ; 1 W → fil blanc ; C → fils jaune (LED−) et gris. La sortie LED doit être réglée sur le type **System state** (état du système) (« The output LED must be set to the »System state« type. ») – alarme armée, le voyant du lecteur iButton est rouge (« Security alarm system is arm - the iButton reader light is red. »), désarmée, il est jaune (« Security alarm system is disarm - the iButton reader light is yellow. »).

- fil marron, RED LED+ (« Brown wire », « RED LED+ ») – le voyant rouge
- fil vert, GREEN LED+ (« Green wire », « GREEN LED+ ») – le voyant vert
- fil jaune, LED− (« Yellow wire », « LED- »)
- fil blanc (« White wire »)
- fil gris (« Gray wire »)

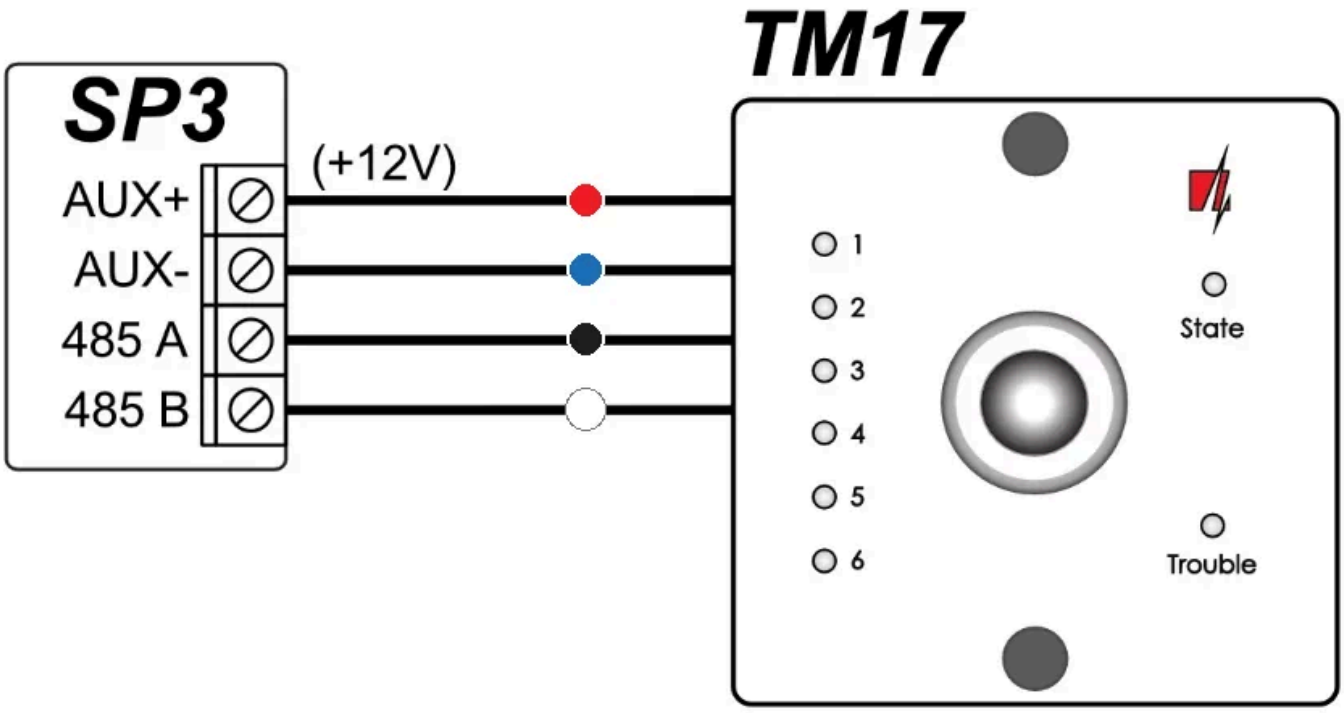


Figure 28. Lecteur TM17 : AUX+ (+12 V) → fil rouge, AUX− → bleu, 485 A → noir, 485 B → blanc.

- fil rouge (« Red wire »)
- fil bleu (« Blue wire »)
- fil noir (« Black wire »)
- fil blanc (« White wire »)

3.7 Raccordement des sondes de température

Au bus 1 WIRE peuvent être raccordées **8 sondes de température Maxim / Dallas DS18S20 ou DS18B20** au maximum, ou **1 sonde de température et d'humidité AM2301** ; la centrale les reconnaît et les attribue automatiquement, les valeurs apparaissent sur la page **Sensors** (6.9). Pour un câble de plus d'un demi-mètre, utilisez un câble à paires torsadées (UTP 4×2×0,5 ou STP 4×2×0,5). La borne **+5V** de la carte alimente les appareils raccordés au bus 1 WIRE : 5 V DC, 0,2 A au maximum, protégée contre les surcharges – en cas de dépassement du courant admissible, la sortie se coupe automatiquement.

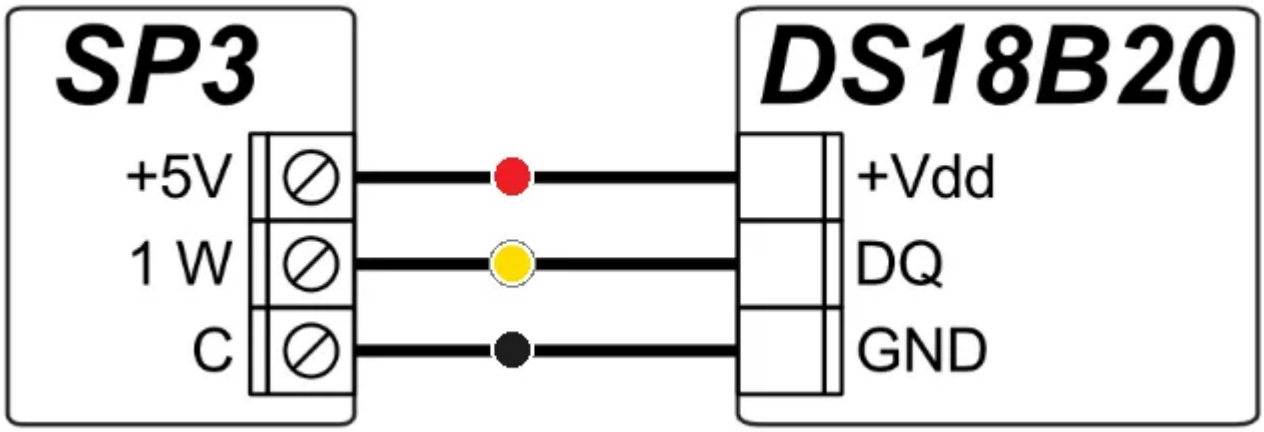


Figure 29. Sonde de température DS18B20 (« Temperature sensor ») : +5V → +Vdd (rouge), 1 W → DQ (jaune), C → GND (noir).

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

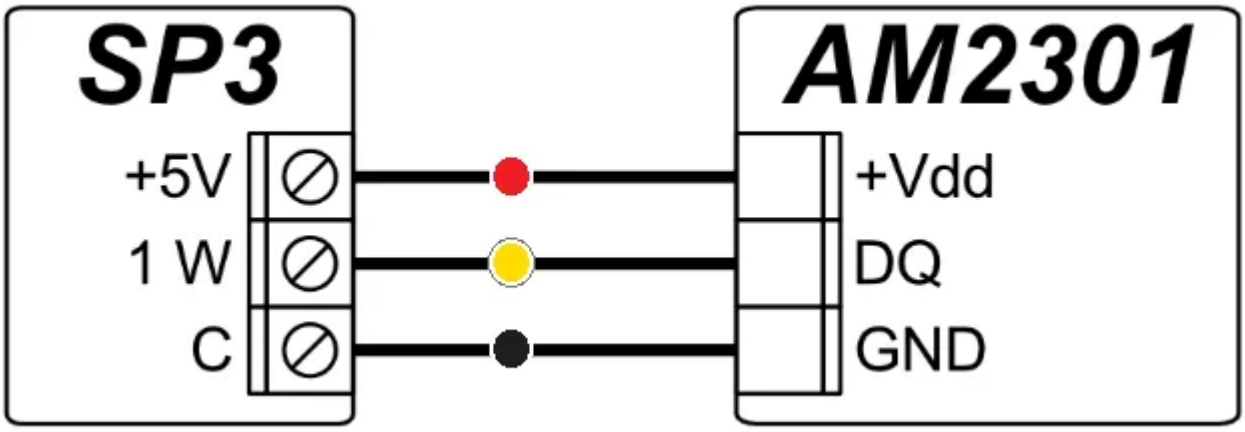


Figure 30. Sonde de température et d'humidité AM2301 (« Temperature and humidity sensor ») : +5V → +Vdd (rouge), 1 W → DQ (jaune), C → GND (noir).

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

3.8 Raccordement d'un relais et d'un voyant LED

Avec les contacts d'un relais, divers équipements électriques peuvent être commandés à distance. La borne IO choisie doit être réglée en sortie (OUT), avec la fonction **Remote control** (télécommande) (6.8). La sortie IO est à collecteur ouvert et supporte 100 mA au maximum ; commutez donc toujours une charge plus importante via un relais.

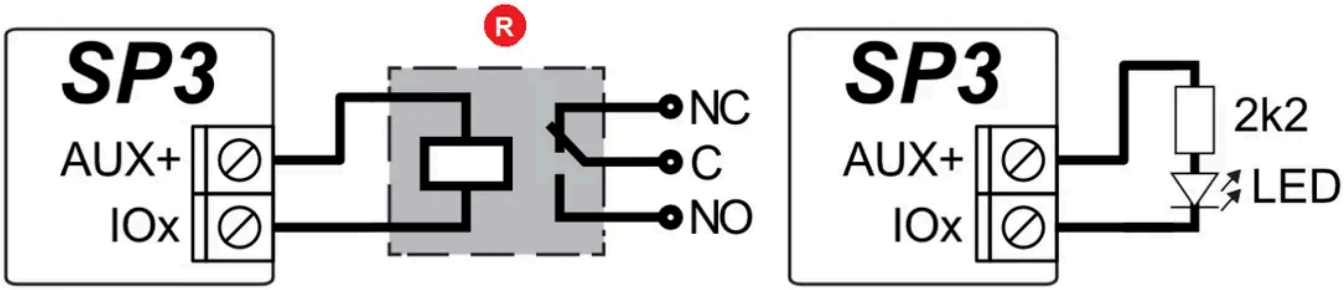


Figure 31. À gauche, relais : la bobine entre AUX+ et IOx, les contacts du relais NC, C, NO. À droite, voyant LED : AUX+ → résistance de 2,2 kΩ → LED → IOx.

- R relais (« Relay »)

3.9 Mise sous tension de la centrale

Mettez l'alimentation secteur sous tension. Les LED de la carte indiquent ce qui suit (le tableau complet se trouve à la section 1.6) :

- la LED **PWR** clignote en vert – la tension d'alimentation est correcte ;
- sur une version avec modem, la LED **NET** est allumée en vert et clignote de temps en temps au moins trois fois en jaune – le vert indique que la carte SIM s'est connectée au réseau mobile, le nombre de clignotements jaunes (0–5) indique le niveau du signal ;
- sur une version Wi-Fi, la LED **MOD** clignote en vert tant que la centrale se connecte au réseau Wi-Fi, et reste allumée en vert en continu lorsque la connexion est établie.

Le niveau de signal mobile suffisant est **3** (trois clignotements jaunes de la LED NET). S'il y a moins de clignotements, le signal du réseau mobile est insuffisant : choisissez un autre emplacement pour la centrale ou l'antenne, ou utilisez une antenne plus sensible. Si les LED indiquent autre chose, la cause ressort du tableau de la section 1.6. Si aucune LED de la centrale ne s'allume, vérifiez l'alimentation et les raccordements.

4. Raccordement des extensions et des modules radio

La plupart des extensions et des modules de communication se raccordent au bus de données **RS485**. L'alimentation du module est fournie par les bornes **AUX+** (+12 V) et **AUX–**, les fils de données vont aux bornes **485 A** et **485 B**, toujours A → A, B → B. **8 appareils** au maximum peuvent être raccordés au bus, la longueur du câble du bus est de **100 m** au maximum. Exception : le récepteur Paradox RTX3, qui se raccorde au bus clavier (GRN, YEL) (4.3). Vous réglez les modules sur la page **Modules** (6.5), et vous ajoutez les appareils radio sur la page **Wireless** (6.6).

La valeur « 100 m au maximum » est un maximum théorique, dans des conditions idéales – voir la remarque de la section 1.3.

Parmi les récepteurs radio, chaque version du firmware ne prend en charge que le sien ; le tableau complet des versions et des modules pris en charge se trouve à la section 1.7.

Module	Système radio	Firmware nécessaire (1.7)
RF-SH	Crow	SP3_xxx0, version 1.01 ou plus récente (SP3_xxx0_0101)
RTX3	Paradox	SP3_xxx1, version 1.12 ou plus récente (SP3_xxx1_0112)
RF-HW	Honeywell	SP3_xxx2, version 1.14 ou plus récente (SP3_xxx2_0114)
RF-S8	S8	SP3_xxx4, version 1.22 ou plus récente (SP3_xxx4_0122)
RF-LORA	appareils LoRa « Maximum »	pour les appareils sans fil MAXIMUM, SP3_xxx4, version 1.21 ou plus récente (SP3_xxx4_0121) ; pour les extensions LORA, n'importe quelle version
E485, T16, SF485, iO, iO-8, iO-WL, iO-MOD, extensions LORA	–	n'importe quelle version

4.1 Module Ethernet E485

Avec le module E485, la centrale envoie et reçoit les rapports d'événements et les commandes par Internet filaire. Si un E485 est raccordé à la centrale, les rapports vers la télésurveillance et vers Protegus 2 passent par Internet filaire, l'Internet mobile n'est pas utilisé ; si la connexion filaire est coupée, la centrale bascule sur l'Internet mobile, et revient automatiquement sur la connexion filaire lorsque celle-ci est rétablie. Vous réglez la priorité des canaux (SIM, Wi-Fi, LAN – E485) sur la page **Reporting to CMS** (6.3), les réglages de l'E485 sur la page **Modules** (6.5). Avec l'E485, la centrale n'a pas besoin de carte SIM.

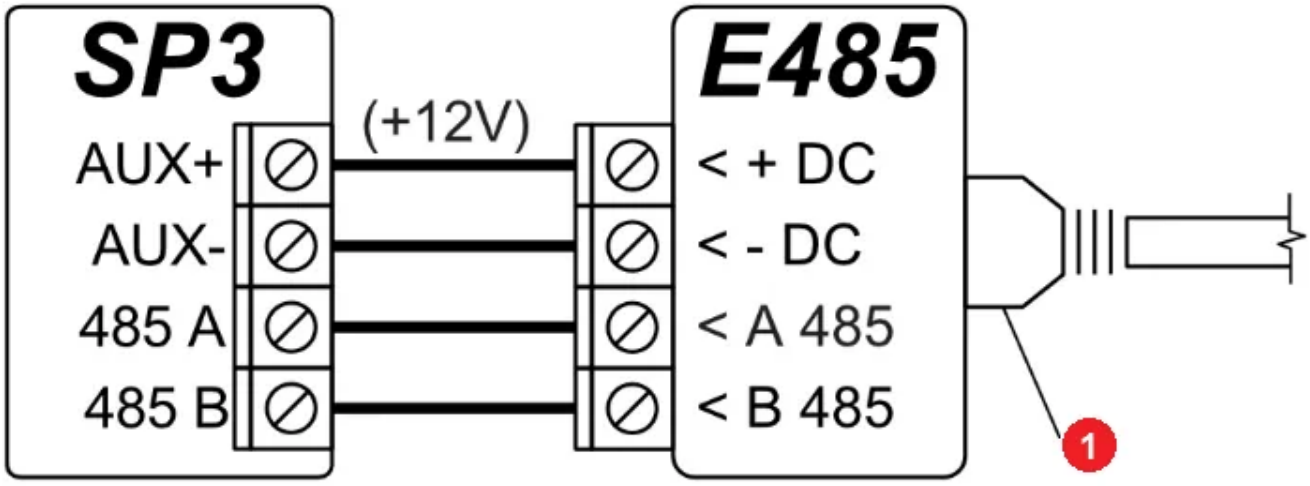


Figure 32. Module Ethernet E485 : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485 ; le câble LAN dans le connecteur RJ45 de l'E485. Liaison RS485 (« RS485 connection »), 100 m au maximum (« up to 100 m »).

- 1 câble LAN (« LAN cable »)

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

4.2 Récepteur radio RF-SH (Crow)

Avec le récepteur RF-SH, la centrale gère les appareils sans fil Crow : 32 détecteurs, 16 sirènes, 42 télécommandes et 8 claviers radio au maximum. Firmware nécessaire : SP3_xxx0_0101 ou plus récent (1.7).

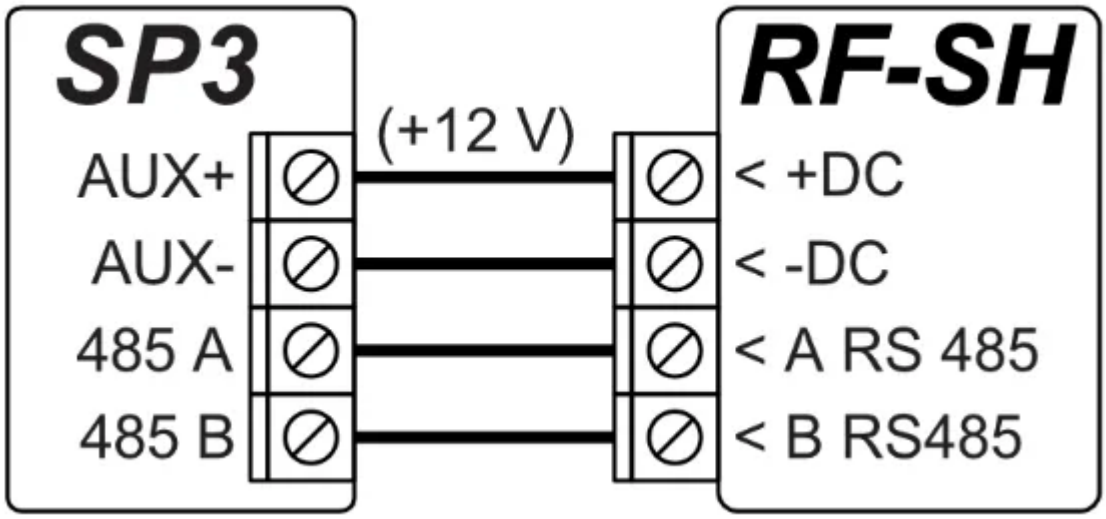


Figure 33. RF-SH : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

4.3 Récepteur radio RTX3 (Paradox)

Le récepteur RTX3 ne se raccorde pas au bus RS485, mais au **bus clavier**. Avec lui, la centrale gère les appareils sans fil Paradox : détecteurs d'ouverture, détecteurs de mouvement, détecteur de bris de vitre G550, détecteur de fumée SD360, télécommandes REM2 et REM25, sirènes SR230 et SR250, clavier K37, extension

PGM et de zones 2WPGM, répéteur RPT1. Firmware nécessaire : SP3_xxx1_0112 ou plus récent (1.7). Un article à part traite du firmware du RTX3, de son raccordement ainsi que de l'ajout et de la suppression des appareils Paradox : FLEXi SP3 et le module d'extension sans fil Paradox RTX3.

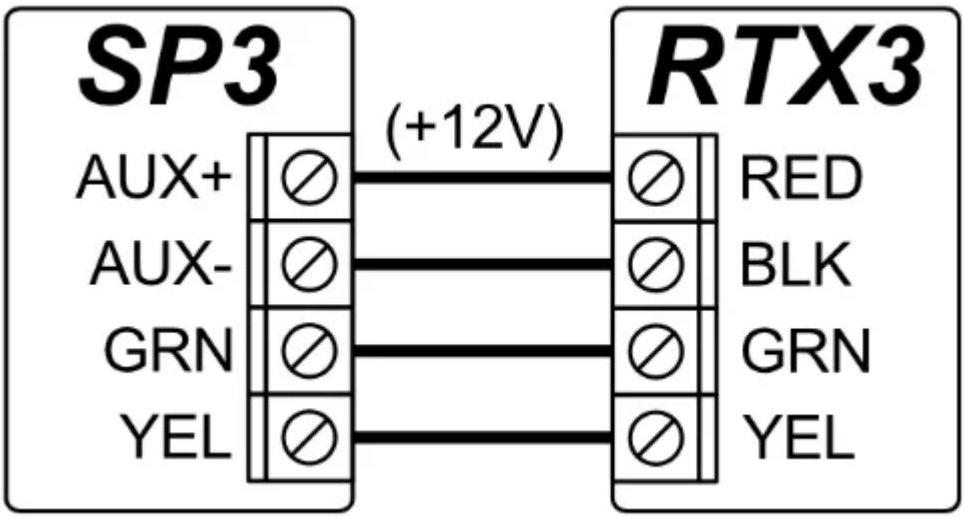


Figure 34. RTX3 sur le bus clavier : AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL.

4.4 Récepteur radio RF-HW (Honeywell)

Avec le récepteur RF-HW, la centrale gère les détecteurs, sirènes, claviers et télécommandes sans fil Honeywell. Firmware nécessaire : SP3_xxx2_0114 ou plus récent (1.7).

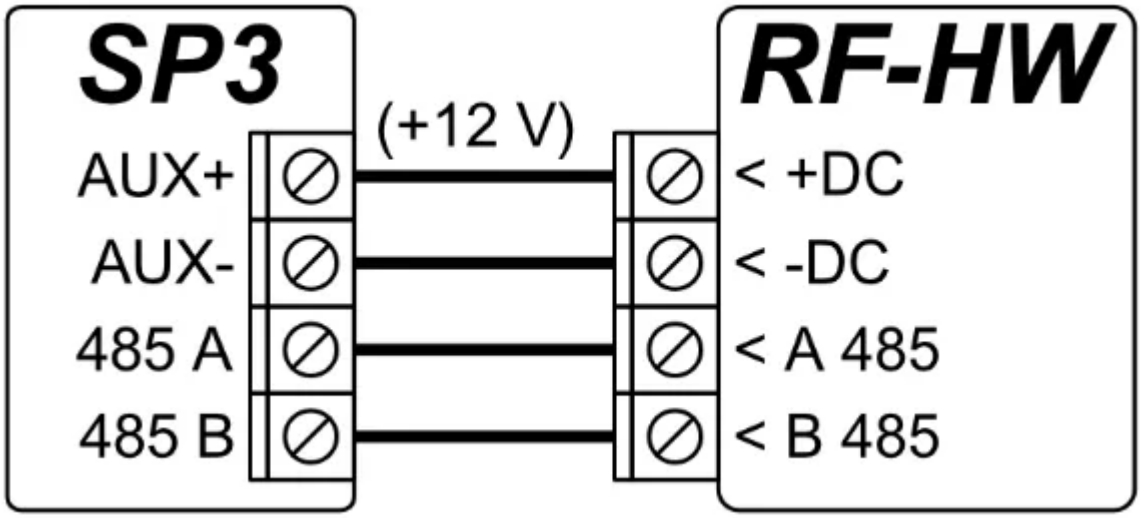


Figure 35. RF-HW : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.5 Récepteur radio RF-S8

Avec le récepteur RF-S8, la centrale gère les détecteurs, sirènes et télécommandes sans fil S8. Firmware nécessaire : SP3_xxx4_0122 ou plus récent (1.7). L'enregistrement du RF-S8, le changement de firmware et l'appairage des appareils S8 sont décrits dans un manuel à part : Manuel de l'émetteur-récepteur RF-S8 et des détecteurs S8.

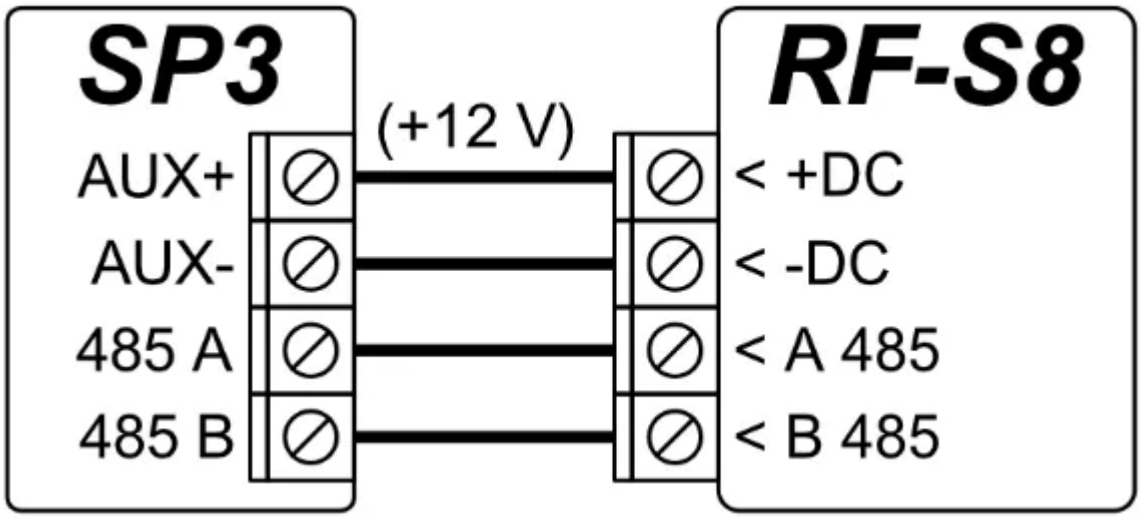


Figure 36. RF-S8 : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.6 Récepteur radio RF-LORA

Avec le récepteur RF-LORA, la centrale gère les appareils radio LoRa « Maximum » : 32 détecteurs, 16 sirènes et 32 télécommandes au maximum, ainsi que les extensions LORA (4.7). Les détecteurs, sirènes et télécommandes MAXIMUM nécessitent le firmware SP3_xxx4, version 1.21 ou plus récente ; les extensions LORA fonctionnent avec n'importe quelle version du firmware (1.7). Le récepteur se règle sur la page **Modules** (6.5), les appareils s'ajoutent sur la page **Wireless** (6.6).

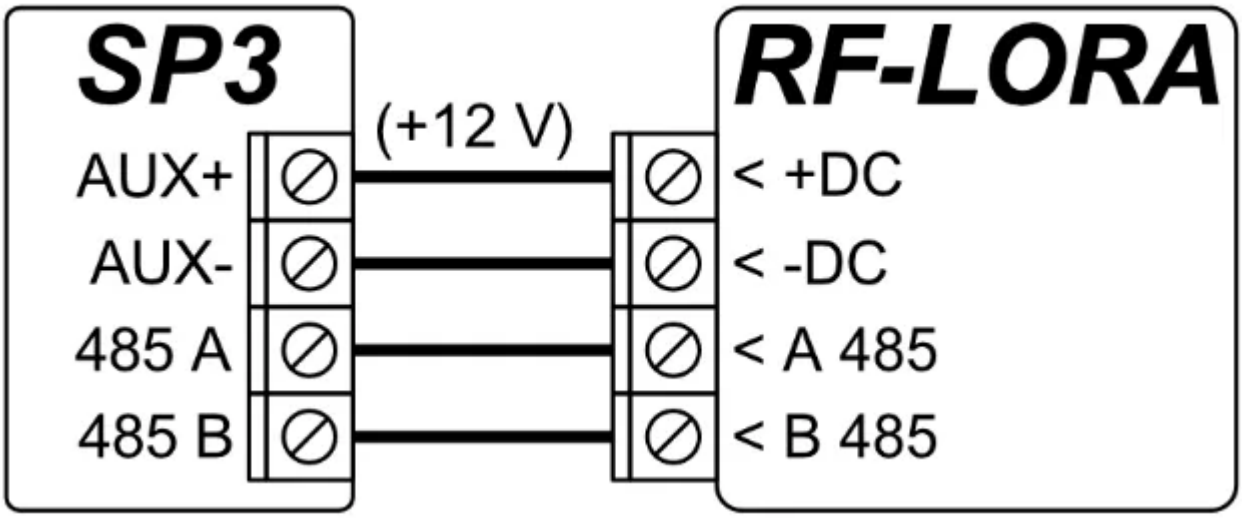


Figure 37. RF-LORA : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.7 Extensions LORA

Les extensions LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) se connectent à la centrale par radio, via le récepteur RF-LORA, jusqu'à 5000 m. **iO-LORA** : extension d'entrées et de sorties avec raccordement d'un lecteur iButton CZ-Dallas, alimentée en 12 V DC ; le lecteur Wiegand qui y est raccordé ne fonctionne pas avec la SP3. **iO8-LORA** : extension à huit entrées/sorties, alimentée en 12–26 V, avec tous les types de circuit de la centrale (3.2). **PB-LORA** : bouton panique. **REL-LORA** : module relais, alimenté en 100–230 V AC.

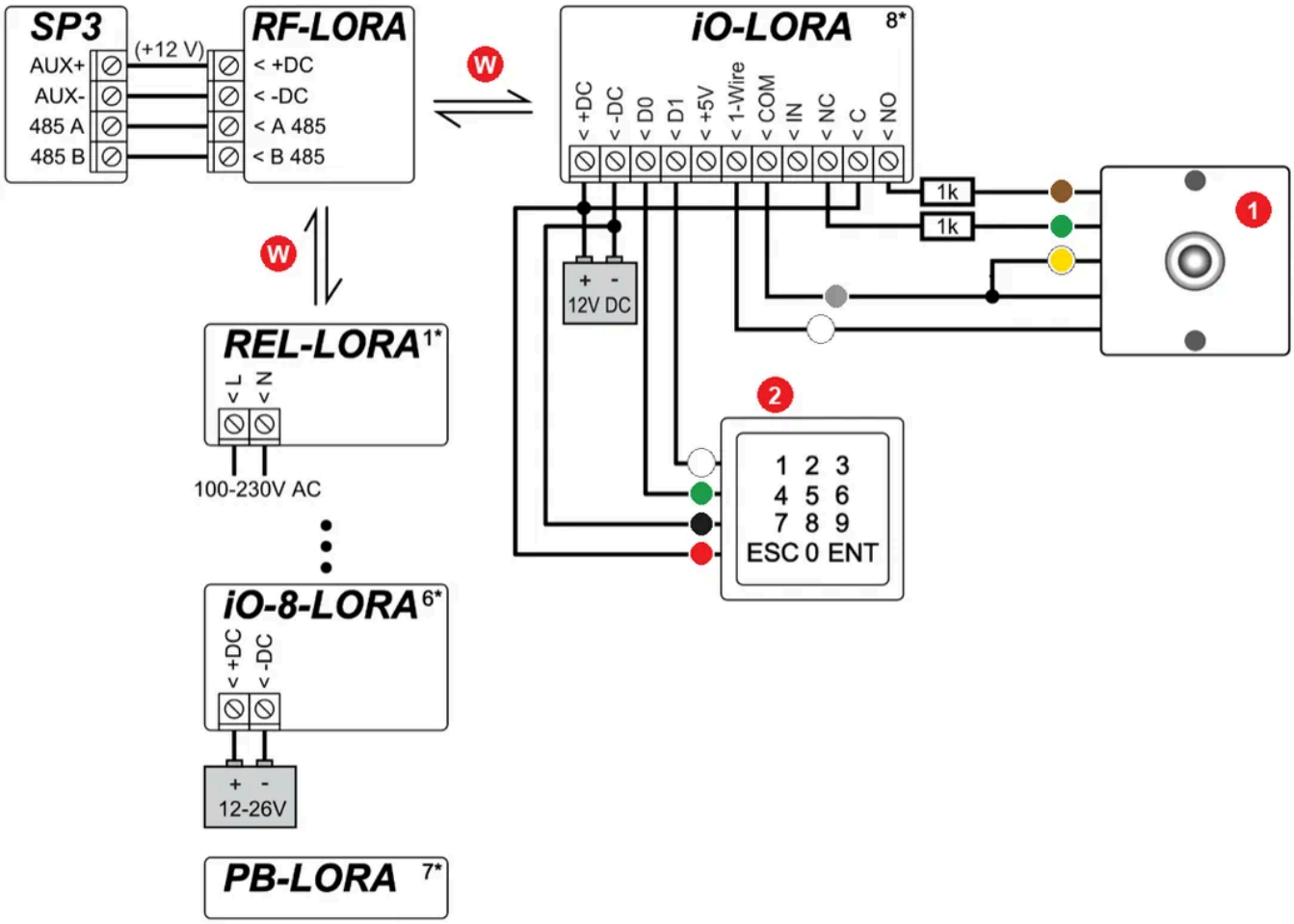


Figure 38. Extensions LORA via le récepteur RF-LORA. SP3 → RF-LORA : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485 ; le RF-LORA atteint par radio, jusqu'à 5000 m, les unités iO-LORA, iO8-LORA, PB-LORA et REL-LORA. REL-LORA : L, N → 100–230 V AC. iO8-LORA : +DC, −DC → 12–26 V. iO-LORA : +DC, −DC → 12 V DC ; fil rouge du lecteur d'entrée (+U) → +DC, noir (GND) → −DC, vert (D0) → D0, blanc (D1) → D1 ; la liaison 1-Wire du lecteur CZ-Dallas fait 30 m au maximum (« 1-Wire connection up to 30 m ») : 1-Wire → blanc, COM → gris et jaune (LED−), C → +DC, NO → 1 kΩ → marron (RED LED+), NC → 1 kΩ → vert (Green LED+). La sortie xOUT doit être réglée sur le type **System State** (état du système) (« The output xOUT must be set to the »System State« type. ») – alarme armée, le voyant du lecteur iButton est rouge (« Security alarm is on - the iButton reader light is red. »), désarmée, il est vert (« The security alarm is off - the iButton reader light is green. »).

- 1 lecteur iButton CZ-Dallas (« CZ-Dallas reader »)
- 2 lecteur d'entrée : lecteur RFID à clavier, Wiegand 26/34 (« Entry reader », « RFID reader with keypad (Wiegand 26/34) ») – ne fonctionne pas ainsi avec la FLEXi SP3
- W liaison sans fil (« Wireless connection »), 5000 m au maximum (« up to 5000 m »)
- fil marron, RED LED+ (« Brown wire », « RED LED+ ») – le voyant rouge
- fil vert : sur le lecteur CZ-Dallas Green LED+, le voyant vert (« Green wire », « Green LED+ ») ; sur le lecteur d'entrée D0 (« G - green wire (D0) »)
- fil jaune, LED− (« Yellow wire », « LED- »)
- fil gris (« Gray wire »)
- fil blanc (« White wire ») ; sur le lecteur d'entrée D1 (« W - white wire (D1) »)
- fil rouge, +U (« R - red wire (+U) »)
- fil noir, GND (« B - black wire (GND) »)

Sur le dessin, le lecteur d'entrée (2) raccordé à l'iO-LORA ne fonctionne pas avec la FLEXi SP3. Raccordez le lecteur RFID directement à la centrale (3.5).

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

distances, vérifiez la liaison lors de la mise en service.

4.8 Extensions de la série iO

Si la centrale a besoin de davantage d'entrées (IN) ou de sorties (OUT), raccordez-lui une extension Trikdis filaire ou sans fil de la série iO (iO, iO-8, iO-WL, iO-MOD). **iO** : extension d'entrées/sorties avec raccordement 1-Wire. **iO-8** : extension à huit entrées/sorties, avec tous les types de circuit de la centrale (3.2). **iO-WL** : extension sans fil qui se connecte à la centrale via l'émetteur-récepteur **iO-MOD**, jusqu'à 300 m ; elle peut aussi être raccordée par câble au bus RS485. Le système peut comporter 8 modules d'extension et 4 iO-MOD au maximum. Les extensions se règlent sur la page **Modules** (6.5).

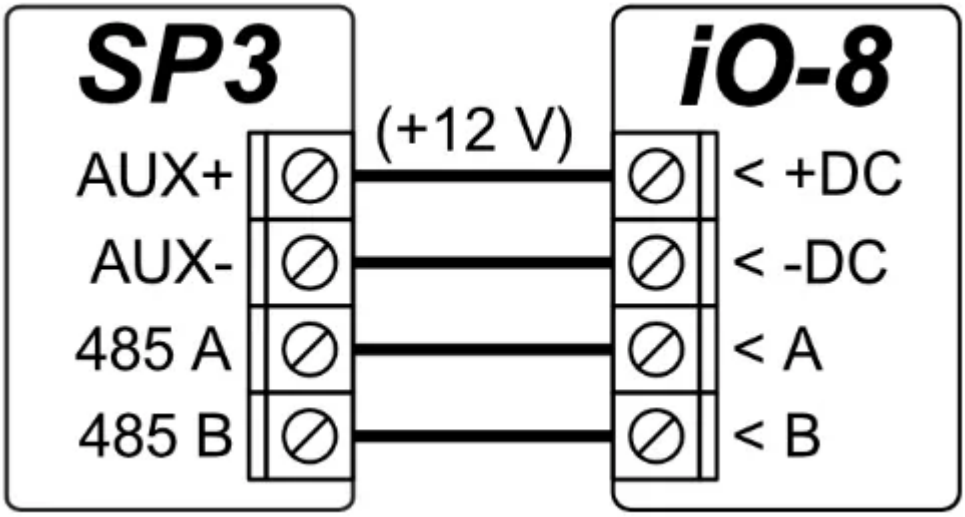


Figure 39. iO-8 : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A, 485 B → B.

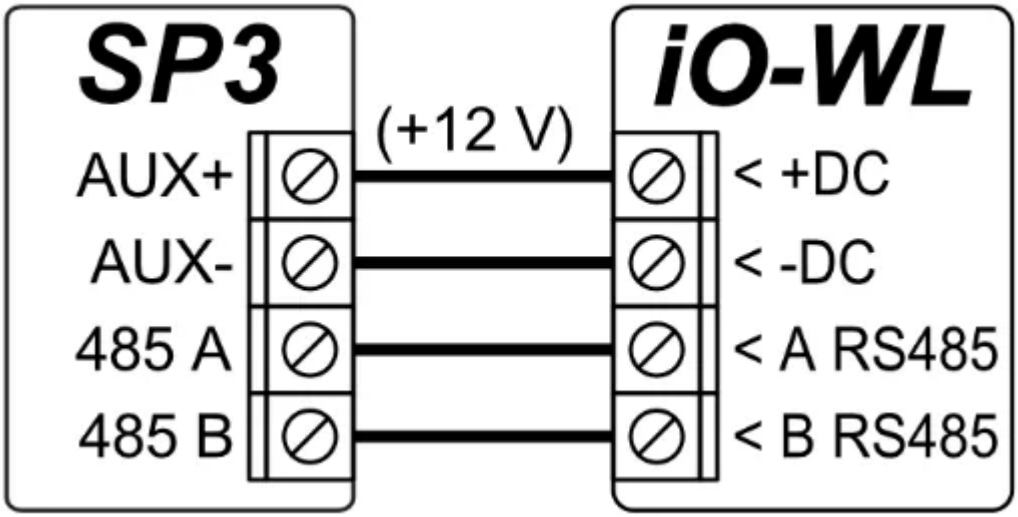


Figure 40. iO-WL par câble : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

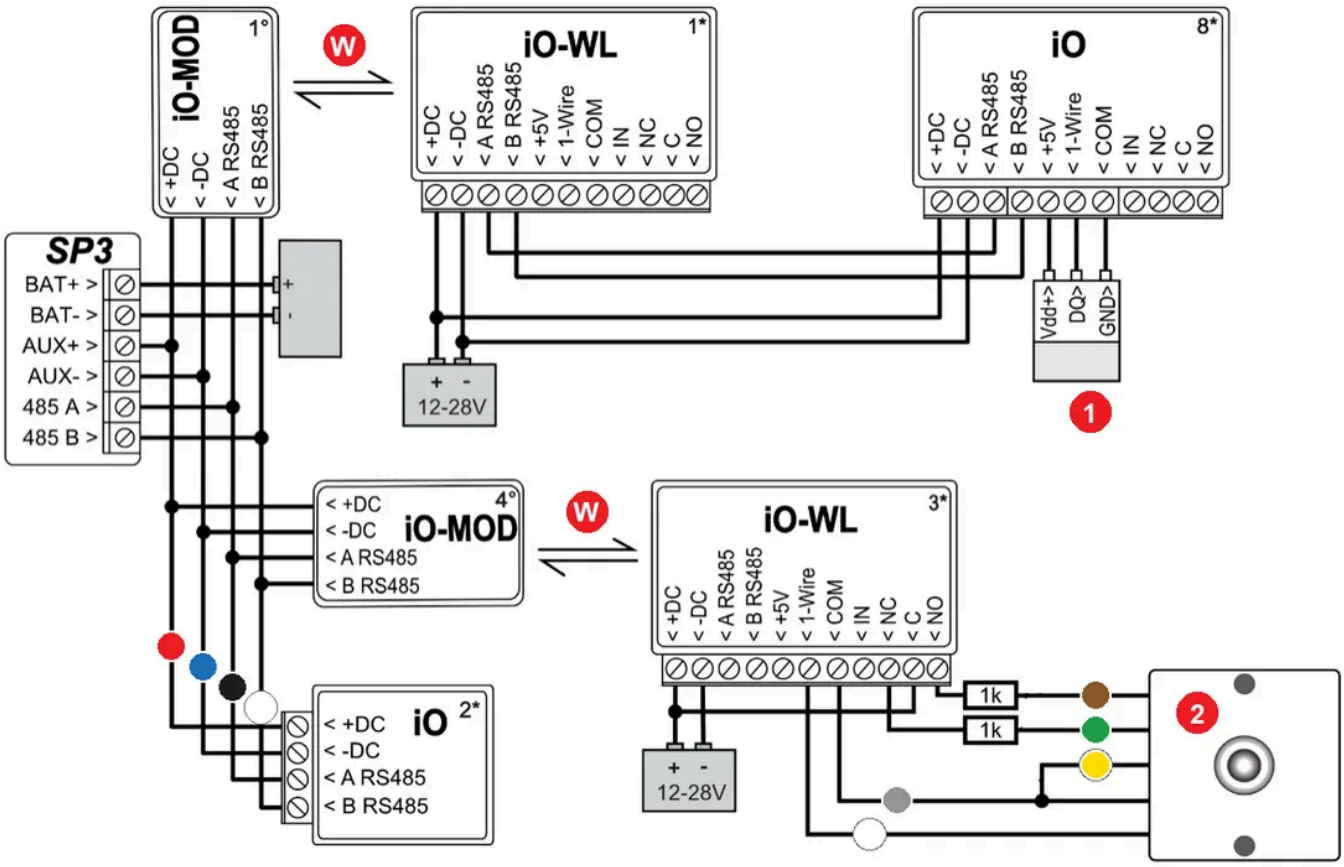


Figure 41. Vue d'ensemble du système iO. SP3 : BAT+ / BAT− → batterie 12 V (« Battery 12V ») ; AUX+ (rouge) et AUX− (bleu) → +DC et −DC sur l'iO-MOD et l'iO ; 485 A (noir) et 485 B (blanc) → A RS485 et B RS485. Les deux iO-MOD atteignent chacun par radio, jusqu'à 300 m, une unité iO-WL. L'iO-WL et l'iO du haut fonctionnent sur une alimentation commune de 12–28 V, avec entre eux une liaison RS485 (« RS485 connection ») de 300 m au maximum (« up to 300 m ») ; les bornes +5V, 1-Wire et COM de l'iO → Vdd+, DQ et GND d'une sonde de température DS18B20 / DS18S20. L'iO-WL du bas (12–28 V) gère un lecteur CZ-Dallas, la liaison 1-Wire fait 30 m au maximum (« 1-Wire connection up to 30 m ») : 1-Wire → blanc, COM → gris et jaune (LED−), C → +DC, NO → 1 kΩ → marron (RED LED+), NC → 1 kΩ → vert (Green LED+). La sortie xOUT doit être réglée sur le type **System State** (état du système) (« The output xOUT must be set to the »System State« type. ») – alarme armée, le voyant du lecteur iButton est rouge (« Security alarm is on - the iButton reader light is red. »), désarmée, il est vert (« The security alarm is off - the iButton reader light is green. »). Parmi les unités marquées d'un astérisque, il peut y avoir 8 modules d'extension du système au maximum (« * up to 8 system expansion modules »), parmi celles marquées d'un °, 4 modules iO-MOD au maximum (« ° up to 4 iO-MOD modules »).

- 1 sonde de température, DS18B20 ou DS18S20 (« Temperature sensor: DS18B20 or DS18S20 »)
- 2 lecteur iButton CZ-Dallas (« CZ-Dallas reader »)
- W liaison sans fil (« Wireless connection »), 300 m au maximum (« up to 300 m »)
- fil rouge (« Red wire »)
- fil bleu (« Blue wire »)
- fil noir (« Black wire »)
- fil blanc (« White wire »)
- fil marron, RED LED+ (« Brown wire », « RED LED+ ») – le voyant rouge
- fil vert, Green LED+ (« Green wire », « Green LED+ ») – le voyant vert
- fil jaune, LED− (« Yellow wire », « LED- »)
- fil gris (« Gray wire »)

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

4.9 Émetteur radio T16

L'émetteur radio VHF/UHF T16 transmet les événements de la centrale au centre de télésurveillance via le réseau radio Trikdis : il envoie ses propres événements et ceux reçus de la centrale, et le centre de télésurveillance peut les transmettre à l'utilisateur.

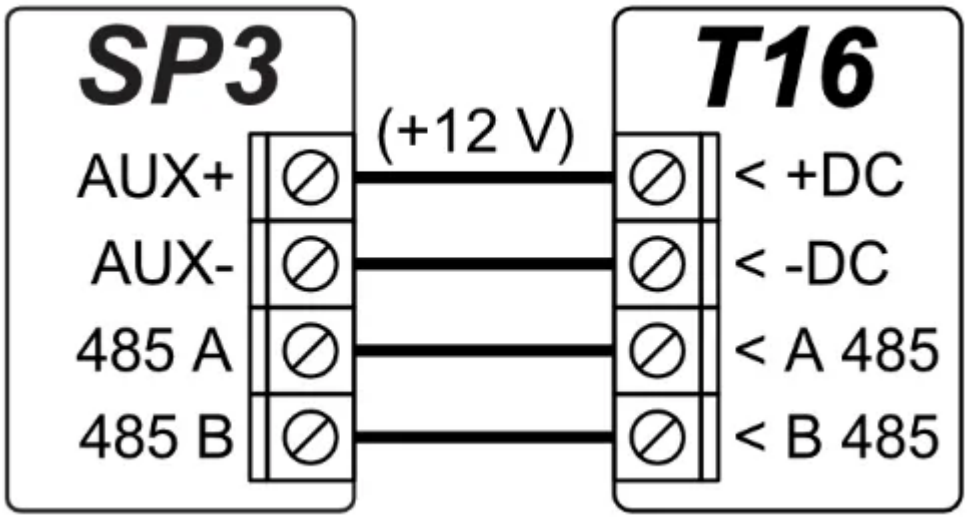


Figure 42. T16 : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.10 Module Sigfox SF485

Le SF485 est un canal de secours : si le canal principal tombe en panne, il envoie les événements de la centrale par le réseau Sigfox au centre de télésurveillance ou à l'application Protegus 2, au format Contact ID.

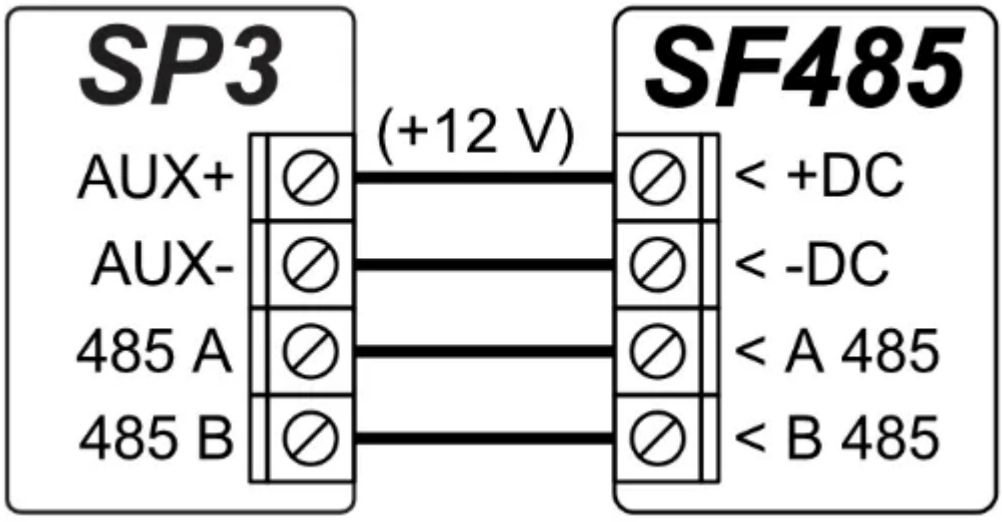


Figure 43. SF485 : AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.11 Mesure de tension continue

La centrale peut mesurer une tension continue de 0–30 V ; **au-dessus de 30 V, la carte est endommagée**. Le pôle positif de la tension mesurée va sur IO1 (IN1 sur le dessin d'origine), le négatif sur la borne C.

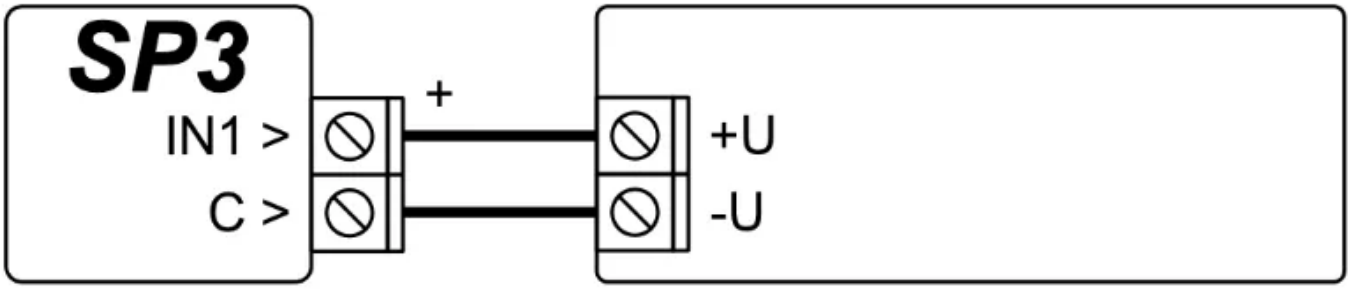


Figure 44. Mesure de tension : l'équipement mesuré (« Equipment whose voltage is measured ») +U → IO1 (IN1 sur le dessin), −U → C.

Raccordez la centrale à l'ordinateur avec un câble USB et lancez TrikdisConfig (chapitre 6) ; le programme reconnaît automatiquement la centrale raccordée et ouvre sa fenêtre de configuration. Sur la page **Sensors**, ajoutez le capteur **In1 Voltage** et les valeurs limites :

- **Max** – au-dessus de cette tension, un événement est généré si la case **High** est cochée ;
- **Min** – en dessous de cette tension, un événement est généré si la case **Low** est cochée.

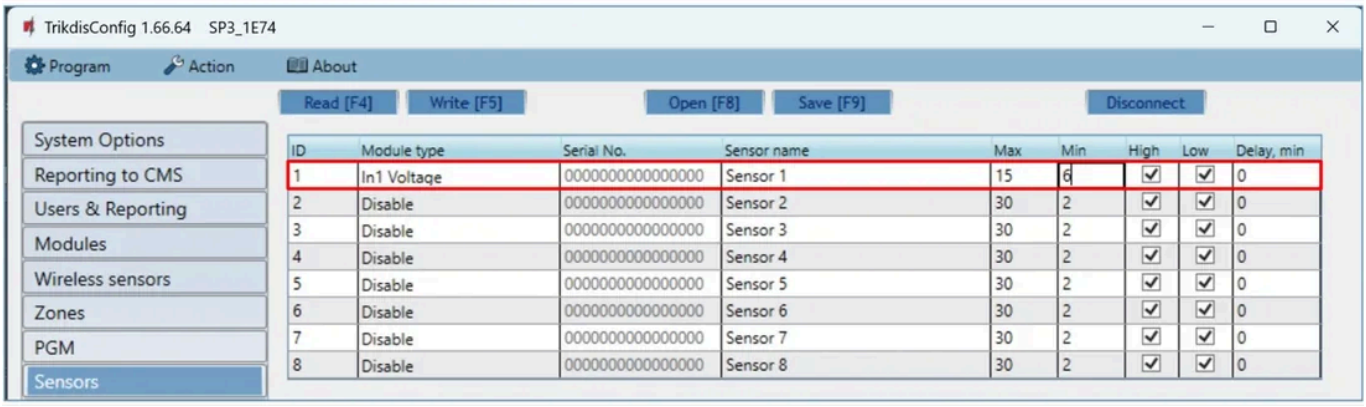


Figure 45. La page Sensors : le capteur In1 Voltage d'identifiant 1, Max 15, Min 6, High et Low cochés, Delay 0 minute.

La tension mesurée peut aussi commander une sortie PGM. Dans l'onglet **Outputs** de la page **PGM**, mettez la sortie en mode **Remote Control**, puis indiquez la condition dans l'onglet **Set Action** :

- **Enable** – activation de la PGM ;
- **PGM No.** – la sortie PGM commandée ;
- **Action** – le fonctionnement de la sortie : **PGM OFF** (désactive), **PGM ON** (active), **Pulse OFF** (sur commande, se désactive pendant la durée de l'impulsion, puis se réactive), **Pulse ON** (s'active pendant la durée de l'impulsion, puis se désactive) ;
- **Pulse time, s** – la durée de l'impulsion, 0–9999 s ;
- **Factor** – la source de la condition : **Sensor** ;
- **Factor No.** – l'entrée de mesure de tension (S1) ;
- **Start when** – la condition : **Higher than set** (au-dessus de la valeur réglée) ou **Lower than set** (en dessous) ;
- **Set value** – la tension surveillée (V).

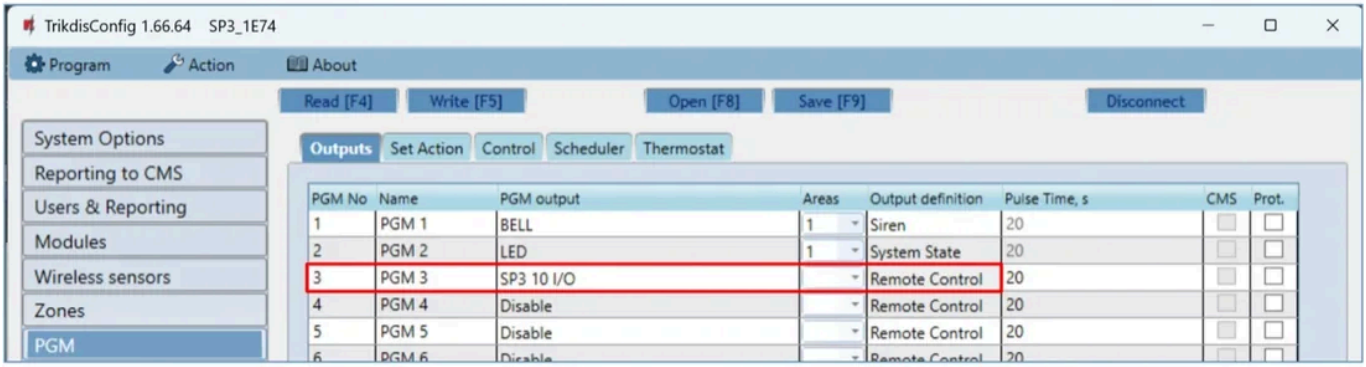


Figure 46. L'onglet Outputs de la page PGM : la PGM 3 sur la borne I/O 10 de la SP3, de type Remote Control, avec une durée d'impulsion de 20 s.

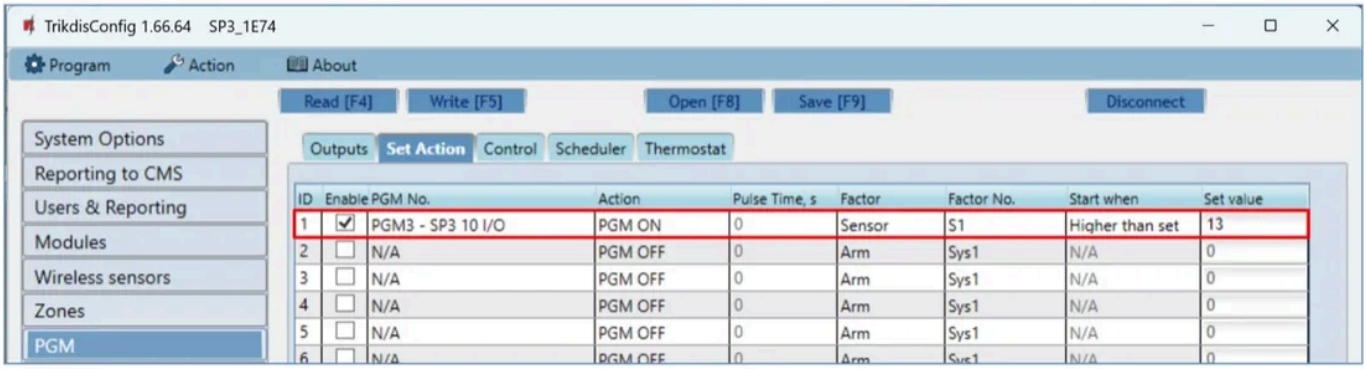


Figure 47. L'onglet Set Action : Enable coché, PGM No. PGM3, Action PGM ON, Pulse Time 0, Factor Sensor, Factor No. S1, Start when Higher than set, Set value 13 V.

5. Protegus 2 et commande à distance

Vous pouvez commander la « FLEXi » SP3 à distance de trois façons : depuis l'application Protegus 2, par SMS et par appel téléphonique. L'application fonctionne sur toutes les versions qui ont accès à Internet (WiFi, Ethernet ou réseau mobile). Les commandes SMS et la commande par appel ne sont disponibles que sur les versions avec modem mobile (par exemple SP3_24E, SP3_44E, SP3_12E) et uniquement avec une carte SIM fonctionnelle. La version SP3_3E (WiFi + Ethernet) n'a pas de modem.

5.1 Association au compte Protegus 2

Dans Protegus 2, l'utilisateur arme et désarme le système, voit l'état des zones et des partitions, et reçoit des notifications sur les événements. Avant d'ajouter la centrale au compte, vérifiez les points suivants :

- **Tension d'alimentation** – la LED **POWER** est allumée en vert en continu.
- **Réseau** – la LED **NET** est verte en continu (réseau mobile) et/ou la LED **MOD** est verte en continu (module WiFi ou Ethernet). La signification des LED est décrite à la section 1.6.
- **Carte SIM** – sur une version avec modem, la SIM est active, et vous avez saisi le code PIN dans TrikdisConfig (**System Options** → **SIM** → **PIN**), ou vous avez désactivé la demande de code PIN sur la carte.
- **Service cloud** – dans l'onglet **Users & Reporting** → **Protegus** de TrikdisConfig, **Enable cloud service** est coché (6.4). La valeur d'usine du **Cloud access code** est 123456 ; si vous la modifiez, l'application demandera le nouveau code lors de l'ajout du système.
- **Identifiant unique** – le numéro **IMEI/Unique ID** de la centrale figure sur l'autocollant de l'emballage et de la carte, et apparaît aussi en bas à gauche de TrikdisConfig une fois la centrale lue.

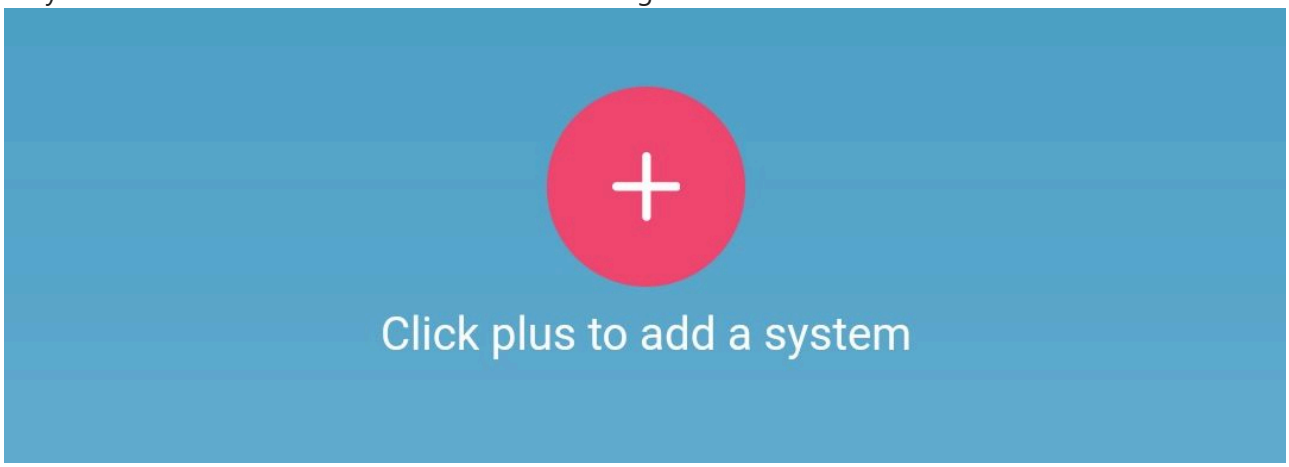
Si vous n'avez pas encore de compte Protegus, créez-le sur le site www.protegus.app avec le lien **Sign up**, et activez-le en cliquant sur le lien reçu par e-mail ; installez ensuite l'application Protegus 2 sur votre téléphone, et connectez-vous avec votre nom d'utilisateur et votre mot de passe.

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

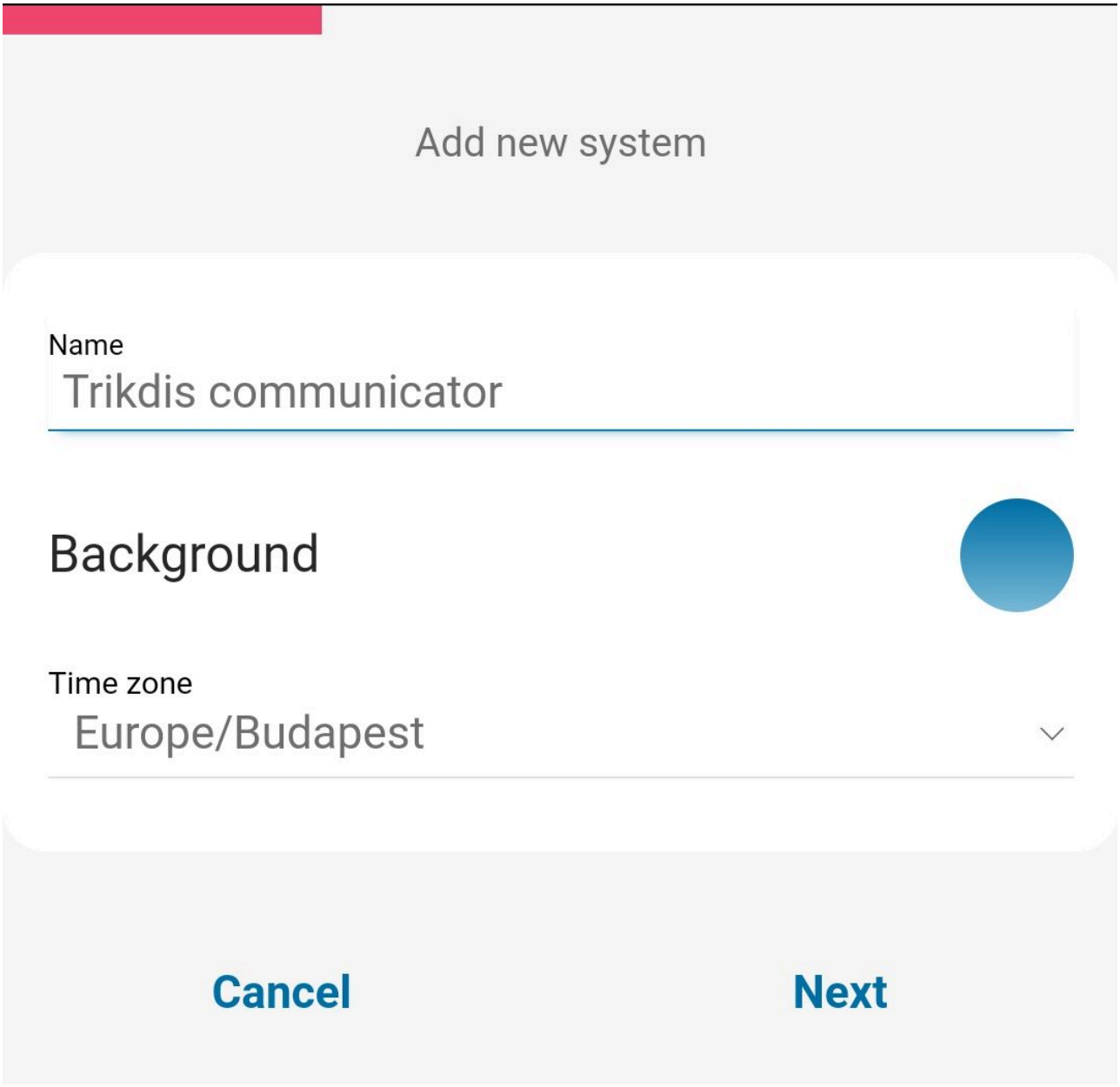


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

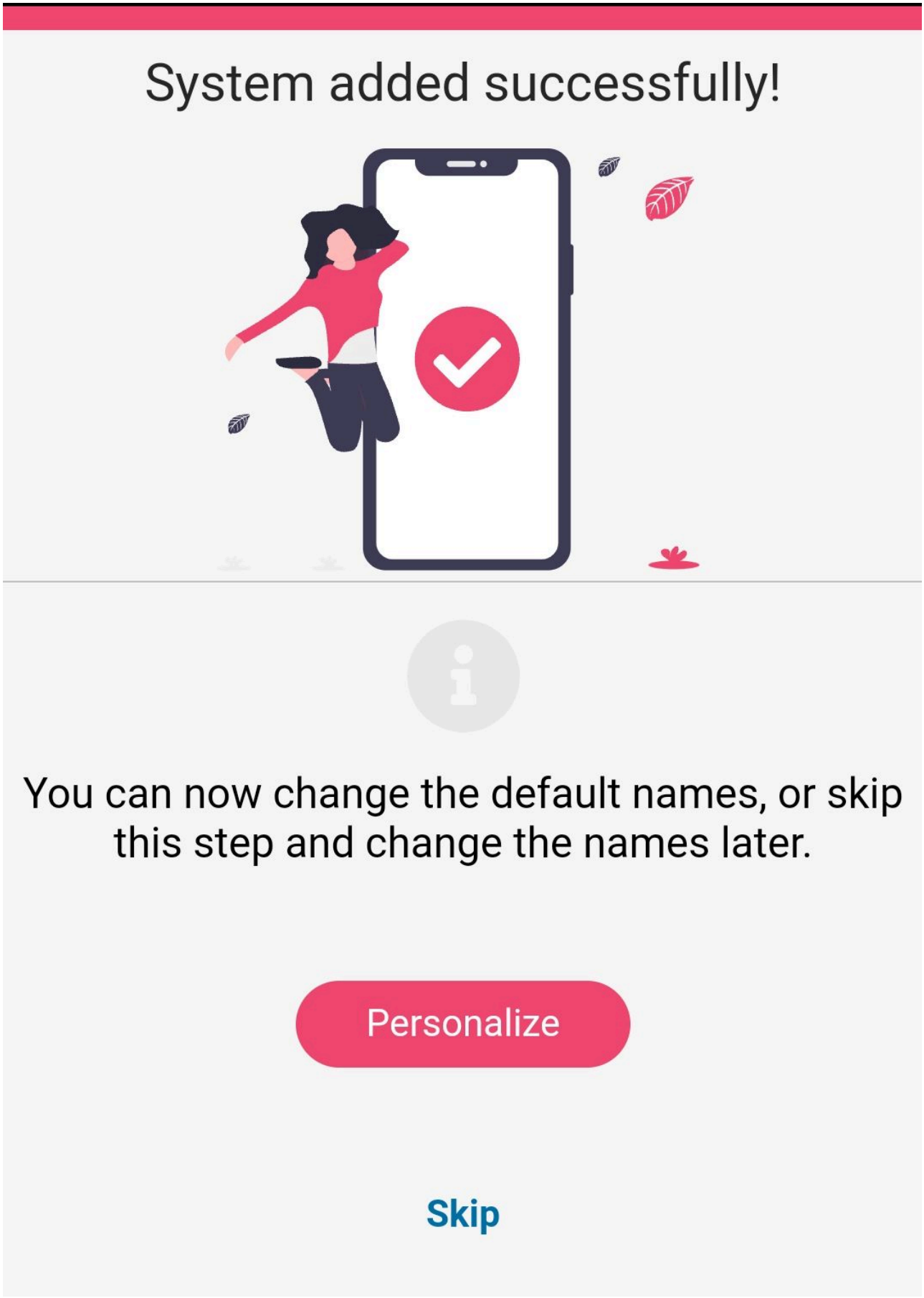
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



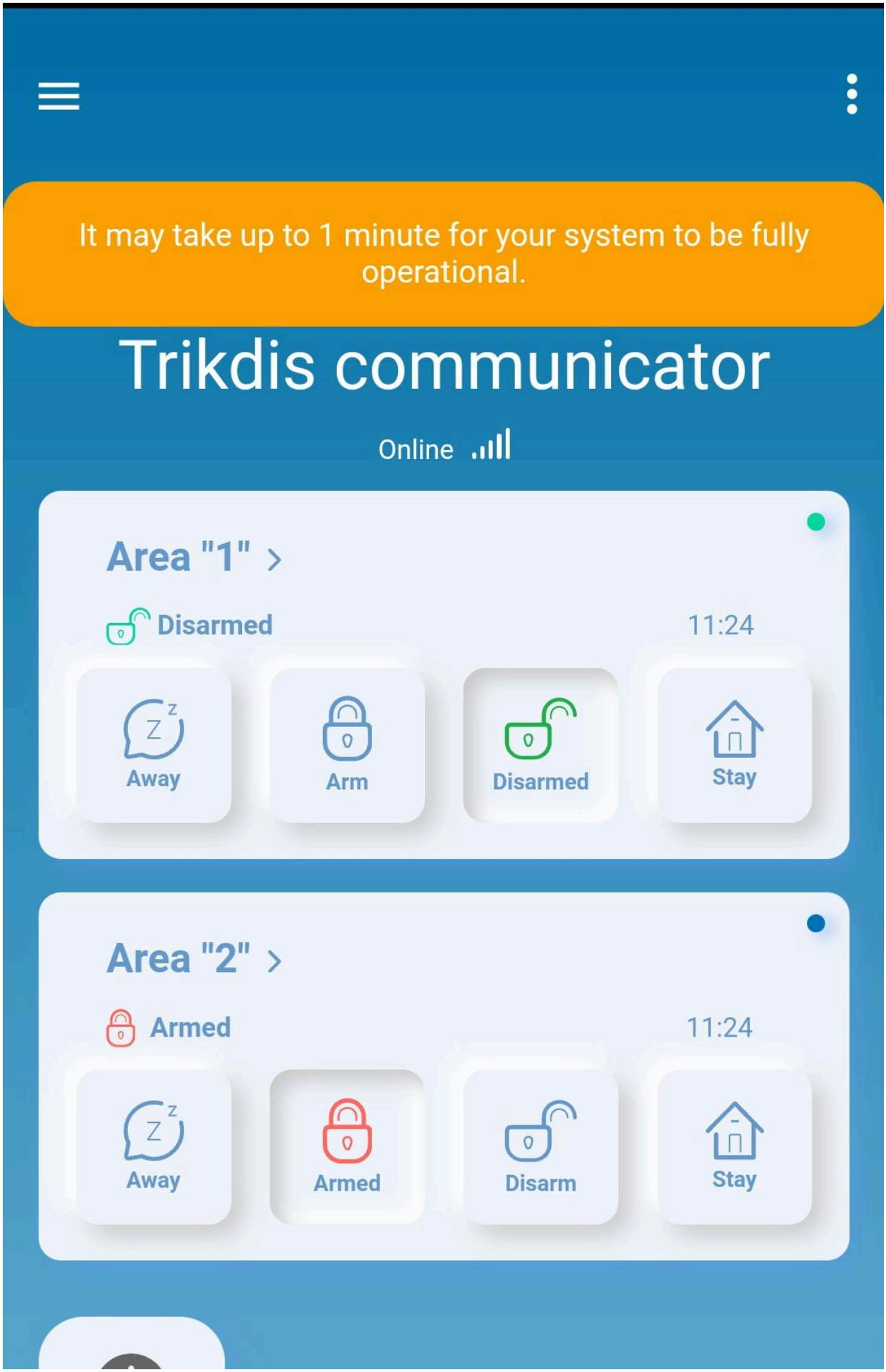
6. Add meg a rendszer nevét és válassz idozónát



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

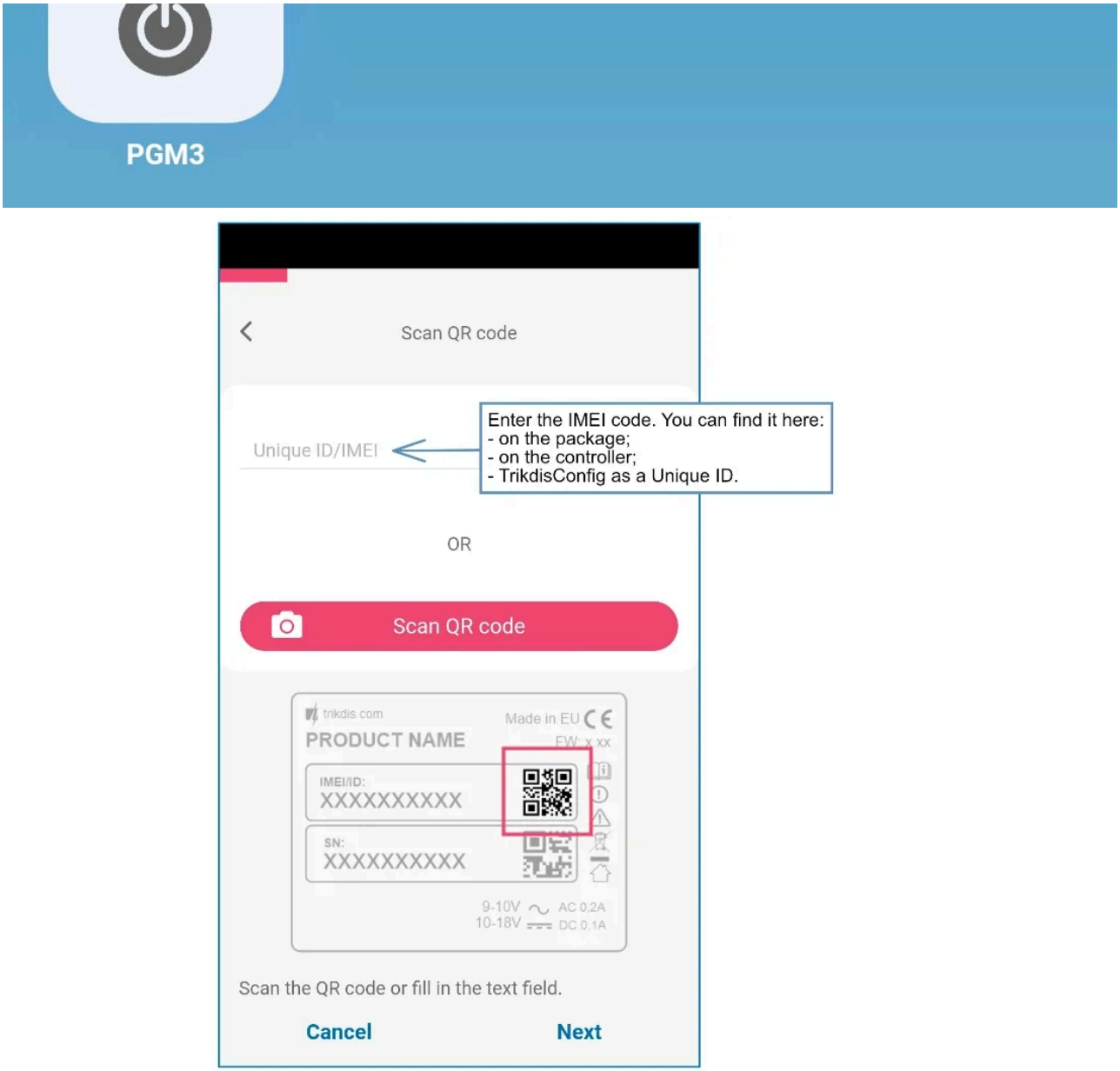


Figure 48. Ajout du système dans Protegus 2 : vous saisissez le numéro **IMEI/Unique ID**, ou vous scannez le code QR de l'autocollant avec l'appareil photo.

Utilisateurs supplémentaires

Le propriétaire peut inviter d'autres utilisateurs dans Protegus 2. Le système envoie également une invitation aux adresses saisies dans la colonne **Email** de l'onglet **Users & Reporting** → **Users** de TrikdisConfig ; l'utilisateur voit ainsi le système depuis son propre compte (6.4).

5.2 Armement et désarmement dans 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.

Sur la SP3, après avoir touché le cadenas, vous devez saisir le **code utilisateur** de la centrale. Il s'agit du code figurant dans la colonne **Code** de l'onglet **Users & Reporting** → **Users** de TrikdisConfig, et non du mot de passe du compte Protegus 2. Chaque partition apparaît sur une carte distincte, et vous ne voyez que les partitions pour lesquelles l'utilisateur a des droits dans la colonne **Areas**. Outre l'armement total, vous lancez aussi les modes partiels depuis l'application : **Stay** (vous restez à la maison, les zones intérieures ne sont pas armées) et **Sleep** (mode nuit). Le mode dans lequel une zone surveille est déterminé par le champ **Definition** de la zone (6.7).

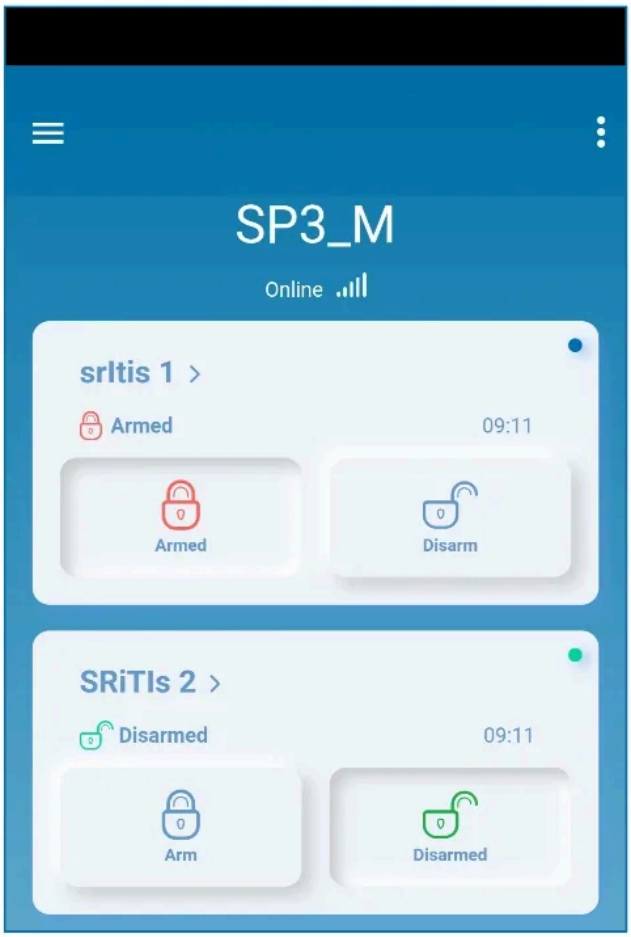


Figure 49. Deux partitions dans Protegus 2 : la 1 armée (cadenas rouge, fermé), la 2 désarmée (cadenas vert, ouvert).

Si l'application ne suit pas la centrale

Si rien ne se passe après les commandes, ou si l'application affiche tout autre chose que l'état réel de la centrale, ouvrez dans Protegus 2 le menu **Settings** → **System configuration**, et appuyez sur le bouton **Sync** à la ligne **System out of sync?**. L'application relit les réglages de la centrale.

5.3 Configuration et commande par SMS

Uniquement sur les versions avec modem. Vous envoyez le SMS au numéro de la carte SIM de la centrale. Tous les messages ont la même structure :

Commande espace **Mot de passe** espace **Données**

Le mot de passe est le **SMS password** à six chiffres (**System Options** → **Access**, 6.2). Sa valeur d'usine est **123456**. Pour des raisons de sécurité, lors de la mise en service, remplacez-le par un mot de passe connu de vous seul dans TrikdisConfig ou avec la commande `PSW` – et ne l'oubliez pas –, et ne communiquez pas inutilement le numéro de la carte SIM de la centrale. Le champ de données dépend de la commande ; pour plusieurs commandes, il est vide.

Qui peut envoyer des commandes ?

L'administrateur peut commander la centrale par SMS et par appel. Si vous voulez autoriser un autre utilisateur, ajoutez son numéro de téléphone dans l'onglet **Users & Reporting** → **Users** de TrikdisConfig (6.4) ou avec la commande `SETN`. La centrale envoie ses réponses avec les textes définis dans l'onglet **SMS answer texts**.

Commande	Donnée	Fonction	Exemple
INFO	–	Interrogation de l'état : nom du site, état des partitions, IMEI, niveau de signal, version du firmware, numéro de série.	`INFO 123456`
RESET	–	Redémarrage de la centrale.	`RESET 123456`
OUTPUTx	ON	Activation de la sortie x.	`OUTPUT1 123456 ON`
	OFF	Désactivation de la sortie x.	`OUTPUT1 123456 OFF`
	PULSE=ttt	Activation de la sortie x pendant ttt secondes (trois chiffres).	`OUTPUT1 123456 PULSE=002`
PSW	nouveau mot de passe	Changement du mot de passe SMS.	`PSW 123456 654123`
TIME	AAAA/MM/JJ,hh:mm:ss	Réglage de la date et de l'heure.	`TIME 123456 2026/10/30,10:02:00`
TXTA	nom du site	Réglage du nom du site (il figure dans les rapports).	`TXTA 123456 Maison`
RDR	numéro de téléphone#texte	La centrale transfère par SMS le texte situé après le # au numéro indiqué. Le numéro commence par le signe + et l'indicatif du pays.	`RDR 123456 +33612345678#texte transmis`
ASKI	–	État des entrées (IN) par SMS.	`ASKI 123456`
ASKO	–	État des sorties (OUT) par SMS.	`ASKO 123456`
ASKA	–	État des partitions par SMS.	`ASKA 123456`

Commande	Donnée	Fonction	Exemple
ASKT	–	Valeurs de tous les capteurs de température par SMS.	`ASKT 123456`
ARM	SYS:x	Armement de la partition x (1–8).	`ARM 123456 SYS:1`
DISARM	SYS:x	Désarmement de la partition x (1–8).	`DISARM 123456 SYS:1`
STAY	SYS:x	Armement de la partition x en mode Stay (1–8).	`STAY 123456 SYS:1`
SLEEP	SYS:x	Armement de la partition x en mode Sleep (1–8).	`SLEEP 123456 SYS:1`
FRS	–	Réinitialisation de l'alimentation des détecteurs incendie, si la définition d'une sortie est **Fire Sensor Reset**.	`FRS 123456`
SETN	PhoneX=numéro#nom#e-mail	Ajout d'un utilisateur à la ligne x avec numéro de téléphone, nom et adresse e-mail ; le numéro de téléphone et le nom sont séparés par le signe #. Le numéro commence par le signe + et l'indicatif du pays.	`SETN 123456 PHONE5=+33612345678#JEAN#jean@exemple.fr`
	PhoneX=DEL	Suppression du numéro de téléphone et du nom de la ligne x.	`SETN 123456 PHONE5=DEL`
UUSD	*code#	Envoi d'un code USSD à l'opérateur mobile (par exemple, consultation du crédit). Dans la centrale, le nom de la commande figure ainsi, sous la forme UUSD.	`UUSD 123456 *245#`
CONNECT	Protegus=ON	Connexion au cloud Protegus.	`CONNECT 123456 PROTEGUS=ON`
	Protegus=OFF	Déconnexion de Protegus.	`CONNECT 123456 PROTEGUS=OFF`
	Code=123456	Code d'accès au cloud Protegus (**Cloud access code**).	`CONNECT 123456 CODE=123456`
	IP=adresse:port	Adresse IP et port du canal principal de télésurveillance.	`CONNECT 123456 IP=0.0.0.0:8000`

Commande	Donnée	Fonction	Exemple
	IP=0	Désactivation du canal principal.	`CONNECT 123456 IP=0`
	ENC=123456	Clé de chiffrement TRK.	`CONNECT 123456 ENC=123456`
	APN=nom	Nom d'APN de la carte SIM.	`CONNECT 123456 APN=INTERNET`
	USER=nom	Nom d'utilisateur APN.	`CONNECT 123456 USER=User`
	PSW=motdepasse	Mot de passe APN.	`CONNECT 123456 PSW=Password`

Première vérification

La commande `INFO` est le moyen le plus rapide de voir sur place que la SIM fonctionne, que la centrale accepte les commandes, et quel est le niveau du signal. La réponse arrive en quelques secondes.

5.4 Commande par appel téléphonique

Pas sur toutes les versions

La commande par appel ne fonctionne pas sur les centrales **SP3_xx7x**. Le type **SP3_12xx** avec un firmware 1.14 ou plus récent ne diffuse pas de message vocal, mais les commandes par touches fonctionnent quand même.

Conditions :

1. Le numéro de téléphone de l'appelant figure dans l'onglet **Users & Reporting** → **Users**, et la colonne **PGM** (commande des sorties par téléphone) est cochée pour l'utilisateur, ou le système est divisé en au moins une partition, et l'utilisateur a des droits sur celle-ci.
2. Le champ **Output definition** de la sortie à commander est **Remote control** (6.8). Pour une commande par impulsion, **Pulse time** est aussi renseigné.

Appelez le numéro de la carte SIM de la centrale. La centrale décroche, puis composez la commande sur le clavier du téléphone :

Touches	Fonction	Exemple
[1][partition][#]	Armement de la partition indiquée.	`12#` – armement de la partition 2
[2][partition][#]	Désarmement de la partition indiquée.	`22#` – désarmement de la partition 2
[3][sortie][#][état]	Commande de la sortie indiquée. État : 0 – désactive, 1 – active, 2 – désactive pendant la durée d'impulsion, 3 – active pendant la durée d'impulsion.	`31#1` – activation de la sortie 1 ; `32#3` – activation de la sortie 2 pendant la durée d'impulsion

Uniquement sur les anciennes centrales SP3_12xx (firmware 1.13 au maximum), pour les messages vocaux :

Touches	Fonction	Exemple
[4][#][numéro de l'enregistrement][#]	Démarrer l'enregistrement d'un message vocal (1–5).	`4#1#`
[5]	Réécouter le message qui vient d'être enregistré.	`5`

Touches	Fonction	Exemple
[6]	Enregistrer le message.	`6`

Enregistrement des messages vocaux

Le début et la fin de l'enregistrement sont signalés par un bip. Un message dure 15 secondes au maximum. La fin de la réécoute est aussi signalée par un bip, et ne lancez l'opération suivante qu'après le bip. La centrale diffuse le message enregistré à l'utilisateur appelé en cas d'alarme : quel message correspond à quelle zone, c'est le champ **Sound** de la zone qui l'indique (6.7). L'appel vocal n'existe que sur la version SP3_12xx, avec un firmware 1.13 au maximum.

6. TrikdisConfig – les réglages en détail

TrikdisConfig est le logiciel de configuration gratuit de Trikdis, fonctionnant sous Windows. Il vous permet de lire et d'écrire tous les réglages de la centrale : sur place par USB, ou à distance via le cloud Protegus. Vous téléchargez le programme sur le site trikdis.com (saisissez dans le champ de recherche : 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!

Connexion par USB

1. Installez et lancez TrikdisConfig.
2. Reliez la centrale à l'ordinateur avec un câble USB Mini-B. Le programme reconnaît la centrale et ouvre la fenêtre de configuration de la SP3.
3. Appuyez sur le bouton **Read [F4]**. Si le programme demande un code, saisissez le code administrateur ou installateur (6.2.6). Avec le code administrateur d'usine, il ne le demande pas.
4. Réglez ce qui est nécessaire, puis appuyez sur le bouton **Write [F5]**. Ce n'est qu'ainsi que le réglage est enregistré dans la centrale.

Mode programmation

Si vous branchez le câble USB sur une centrale sous tension et en fonctionnement, la centrale passe en mode programmation et n'assure plus de fonction d'alarme jusqu'au débranchement du câble. Sur un système en service, prévenez l'utilisateur, et débranchez le câble à la fin.

Les boutons de la ligne supérieure : **Read [F4]** – lecture depuis la centrale ; **Write [F5]** – écriture dans la centrale ; **Open [F8]** – ouverture d'un réglage enregistré auparavant dans un fichier ; **Save [F9]** – enregistrement du réglage actuel dans un fichier ; **Disconnect** – coupure de la connexion. Les fenêtres du menu de gauche : **System Options**, **Reporting to CMS**, **Users & Reporting**, **Modules**, **Wireless sensors**, **Zones**, **PGM**, **Sensors**, **System events**, **Events Log** et **Firmware** (mise à jour du firmware, chapitre 9). En bas à gauche apparaissent les cases **Remember password** et **Show passwords**, le bouton **Default settings → Restore** (6.12) et le numéro **IMEI/Unique ID** de la centrale.

Enregistrez dans un fichier

Le fichier enregistré avec le bouton **Save [F9]** constitue la documentation du système. Après un remplacement de carte ou une réinitialisation d'usine, vous rechargez le tout en quelques minutes avec le bouton **Open [F8]**, puis **Write [F5]**.

Vous pouvez aussi configurer la centrale à distance : sur l'écran d'accueil de TrikdisConfig, saisissez le numéro **IMEI/Unique ID** de la centrale dans le champ **Remote access**, et appuyez sur le bouton **Configure** (figure à la section 6.6.2, procédure complète au chapitre 7). Cela suppose que le service cloud soit activé (6.4.3) et que la connexion réseau fonctionne.

6.1 La barre d'état

Lorsqu'une centrale est raccordée, la ligne inférieure du programme et le champ en bas à gauche affichent les données de l'appareil.

Champ	Signification
IMEI/Unique ID	L'identifiant unique de la centrale. Sur les versions avec modem, l'IMEI ; sur les versions WiFi/Ethernet, un identifiant matériel. C'est ce que demandent Protegus 2 et **Remote access**.
Status	L'état de l'opération (par exemple « reading done »).
Device	Le type de la centrale, sous la forme SP3_xxxx.
SN	Le numéro de série de la centrale.
BL	La version du chargeur d'amorçage (bootloader).
FW	La version du firmware.
HW	La version du matériel.
State	Le mode de connexion : **USB** ou à distance.
Role	Le niveau d'accès après saisie du code : **Administrator** ou **Installer**.



Figure 50. La barre d'état de TrikdisConfig. Les valeurs **IMEI/Unique ID** et **SN** ont été masquées sur la figure.

Le bouton **Read [F4]** lit et affiche les réglages enregistrés dans la centrale. Nous passons ensuite en revue les champs fenêtre par fenêtre.

6.2 System Options

Elle se compose de six onglets : **System general**, **Partitions**, **Scheduler**, **Holidays**, **System troubles** et **Access**.

6.2.1 Onglet System general

Groupe **General** :

- **Object ID** – identifiant du site, nombre hexadécimal à quatre chiffres (0–9, A–F). Il est attribué par le centre de télésurveillance (CMS) ; il n'est nécessaire que si la centrale transmet à un centre de télésurveillance. FFFE et FFFF ne peuvent pas être utilisés.
- **Object name** – le nom du site, 20 lettres et chiffres au maximum. Il figure dans les rapports SMS.

- **Test period** – si la case est cochée, la centrale envoie un rapport de test à cet intervalle, sauf si **Start test at** est aussi coché et qu'une heure a été indiquée.
- **Start test at** – l'heure quotidienne du rapport de test.
- **Areas in test SMS** – le SMS de test contient aussi l'état des partitions indiquées.
- **Clear Events after reset** – au redémarrage, les événements non encore envoyés sont effacés de la mémoire tampon.
- **Text language** – les SMS utilisent les caractères propres à la langue choisie.
- **Suspend event reporting when … same events per … s** – suspension de la transmission si le même événement se répète plus que le nombre indiqué pendant la durée indiquée (par exemple un détecteur défectueux). **Restore event reporting after** – après ce nombre de minutes (0–999), la centrale signale de nouveau l'événement.
- **Call** – lors d'un événement, la centrale appelle l'utilisateur ce nombre de fois. Si l'appel est pris ou rejeté, elle ne rappelle plus. Un appel dure 20 secondes.
- **EOL Type** – la valeur des résistances de fin de ligne raccordées aux zones : RT est la résistance d'autoprotection, R1 celle du 1er détecteur, R2 celle du 2e. Le raccordement est présenté au chapitre 3.
- **Communication path test** – à cet intervalle, la centrale envoie aussi un message d'essai au centre de télésurveillance sur les canaux de secours, puis revient sur le canal principal.
- **LED out as 2Wire fire** – cochez si vous raccordez des détecteurs incendie deux fils à la sortie LED.

Groupe **SIM** :

- **PIN** – le code PIN de la carte SIM. Si la carte n'a pas de demande de PIN, laissez la valeur d'usine.
- **APN** – le nom du point d'accès Internet de l'opérateur mobile. Obligatoire si la centrale transmet au cloud Protegus ou au centre de télésurveillance par l'Internet mobile.
- **Login**, **Password** – nom d'utilisateur et mot de passe APN, uniquement si l'opérateur les demande.
- **Locked ICCID** – le numéro ICCID de la carte SIM. Si vous le renseignez, la centrale ne fonctionne qu'avec cette carte.
- **Preferred operator** – code opérateur (MCC + MNC). Si vous le renseignez, la centrale ne s'enregistre que sur le réseau de cet opérateur.

Codes opérateurs – exemples

France : Orange 20801, SFR 20810, Bouygues Telecom 20820, Free Mobile 20815. Hongrie : Yettel 21601, Telekom 21630, One (anciennement Vodafone) 21670. Le code de votre opérateur se compose de la même façon du MCC du pays et du MNC de l'opérateur. Si le champ est laissé vide, la centrale choisit automatiquement le réseau ; n'indiquez le code que si elle doit rester sur un réseau donné.

Groupe **Time settings** :

- **Set PC time** – écrit l'heure de l'ordinateur dans la centrale. Si le champ **Time synchronization** indique **Disabled**, cette heure est conservée ; s'il indique **modem** ou **server**, la centrale se synchronise à partir de cette source après la mise sous tension.
- **Time zone (Hours)** – le fuseau horaire ; par exemple +1 en Europe centrale (France, Belgique, Suisse, Luxembourg).
- **Time set** – le serveur de temps avec lequel la centrale se synchronise à la mise sous tension.
- **Daylight saving time** – passage automatique à l'heure d'été et à l'heure d'hiver.
- **AC failure delay** – la centrale signale la coupure de la tension secteur avec ce retard, et le retour également avec retard.

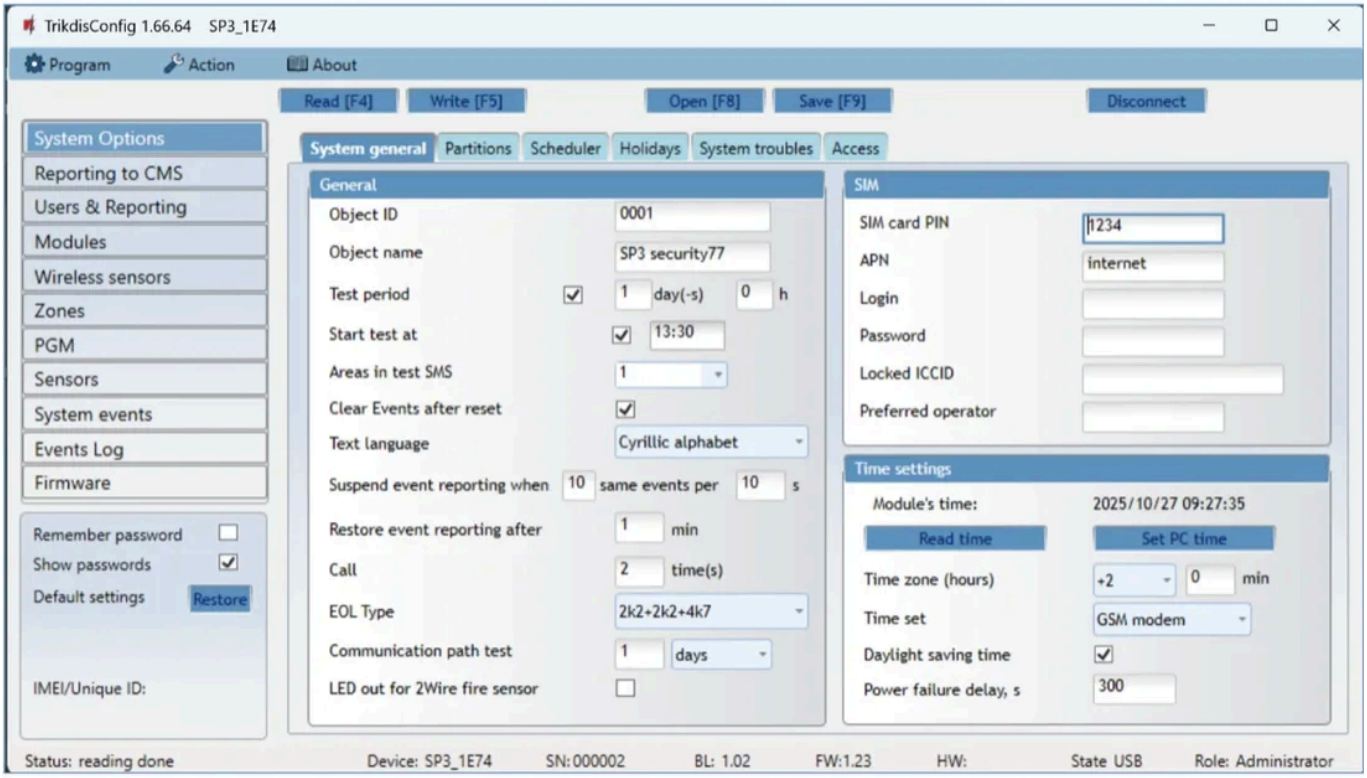


Figure 51. System Options → System general : les groupes General, SIM et Time settings.

6.2.2 Onglet Partitions

- **Partitions enabled** – en combien de parties indépendantes (partitions) vous divisez le système.
- **Partition name** – le nom de la partition.
- **Entry** – temporisation d'entrée, 0–999 s. C'est le temps dont vous disposez pour aller jusqu'au clavier en passant par la zone Delay et désarmer le système.
- **Exit** – temporisation de sortie, 0–999 s. Après l'armement – à compter du code d'armement saisi sur le clavier – c'est le temps dont vous disposez pour quitter les locaux en passant par la zone Delay. Lors d'un armement à distance (par exemple depuis Protegus 2), le système s'arme immédiatement, sans temps de sortie.
- **Bell** – durée de fonctionnement de la sirène en cas d'alarme, 0–999 s.
- **Squawk** – la sirène émet un bip à l'armement, deux au désarmement.
- **Re-ARM** – réarmement automatique si le système a été désarmé à distance, mais que personne n'a violé la zone Delay pendant le temps d'entrée.
- **Force-ARM** – armement forcé. Le système peut être armé même si des zones Stay sont ouvertes, tant que la zone d'entrée est fermée.
- **Keyswitch** – la zone interrupteur à clé arme et désarme par impulsion (**Pulse**) ou par niveau (**Level**).
- **Tamper** – le traitement de l'événement d'autoprotection lorsque la centrale détecte une autoprotection de détecteur : **Silent** (seul le rapport est envoyé aux destinataires, la sirène ne sonne pas), **Audible when armed** (le rapport est envoyé, la sirène ne sonne que si l'autoprotection se produit avec le système armé), **Always Audible** (le rapport est envoyé, et la sirène sonne aussi avec le système désarmé).

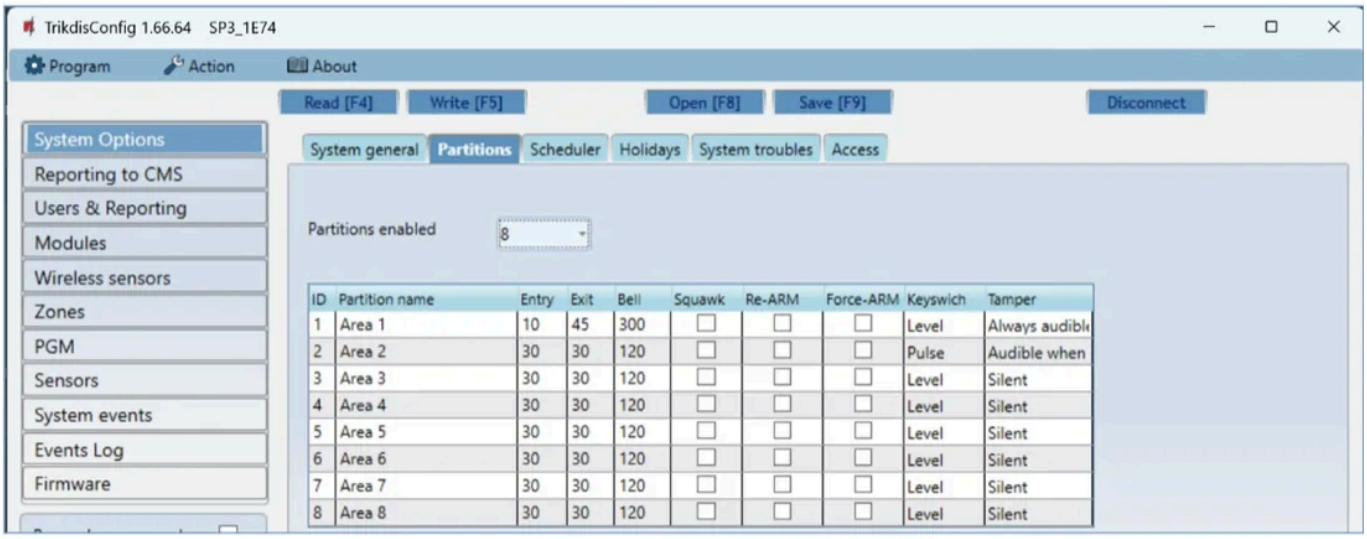


Figure 52. System Options → Partitions : pour chaque partition, les temps d'entrée, de sortie et de sirène, ainsi que le comportement.

6.2.3 Onglet Scheduler

Armement et désarmement automatiques selon les jours de la semaine, avec les jours fériés.

- **Enable** – activation de la programmation.
- **Partition** – la partition concernée.
- **Time** – l'heure de l'opération.
- **Not Armed** – l'opération n'est exécutée que si la centrale n'est pas armée en mode total (Away).
- **Action** – le mode à appliquer : **Disarm**, **Arm**, **Sleep** ou **Stay**.
- **Monday … Sunday** – les jours où elle s'applique.
- **Holiday** – comportement un jour férié : **Disabled** (pas de jour férié), **Ignore on holidays** (ne s'exécute pas les jours fériés), **Additional when holidays** (s'exécute aussi les jours fériés), **Only holidays** (ne s'exécute que les jours fériés).
- **Holiday group** – quel groupe de jours fériés (**Any**, 1–4) considérer comme férié. Avec **Any**, tout jour férié actif compte.

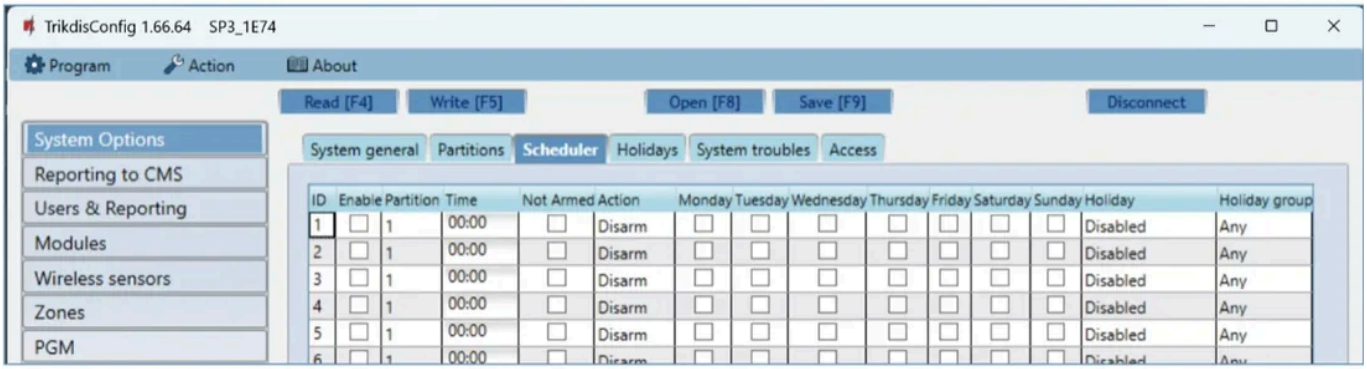


Figure 53. System Options → Scheduler : programme hebdomadaire d'armement et de désarmement.

6.2.4 Onglet Holidays

- **Enable** – activation du jour férié.
- **Start date**, **Stop date** – le premier et le dernier jour de la période fériée. Pour un jour férié d'une seule journée, les deux sont identiques.
- **Group 1 … Group 4** – vous classez les jours fériés en groupes, auxquels le programmateur fait référence.

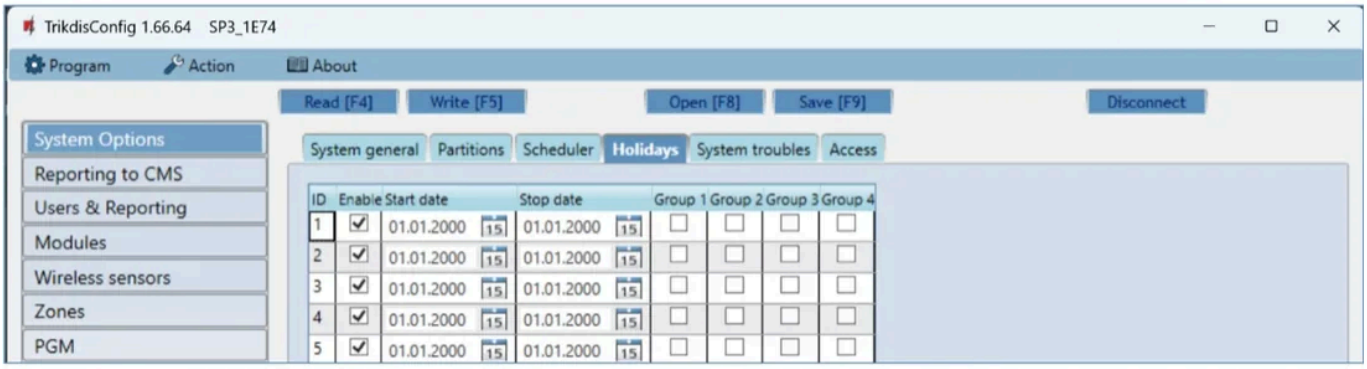


Figure 54. System Options → Holidays : jours fériés en quatre groupes.

6.2.5 Onglet System troubles

Si vous cochez ici un défaut interne, le système ne peut pas être armé tant que ce défaut persiste. Vous pouvez ainsi empêcher l'armement, par exemple avec une batterie déchargée ou sans alimentation secteur.

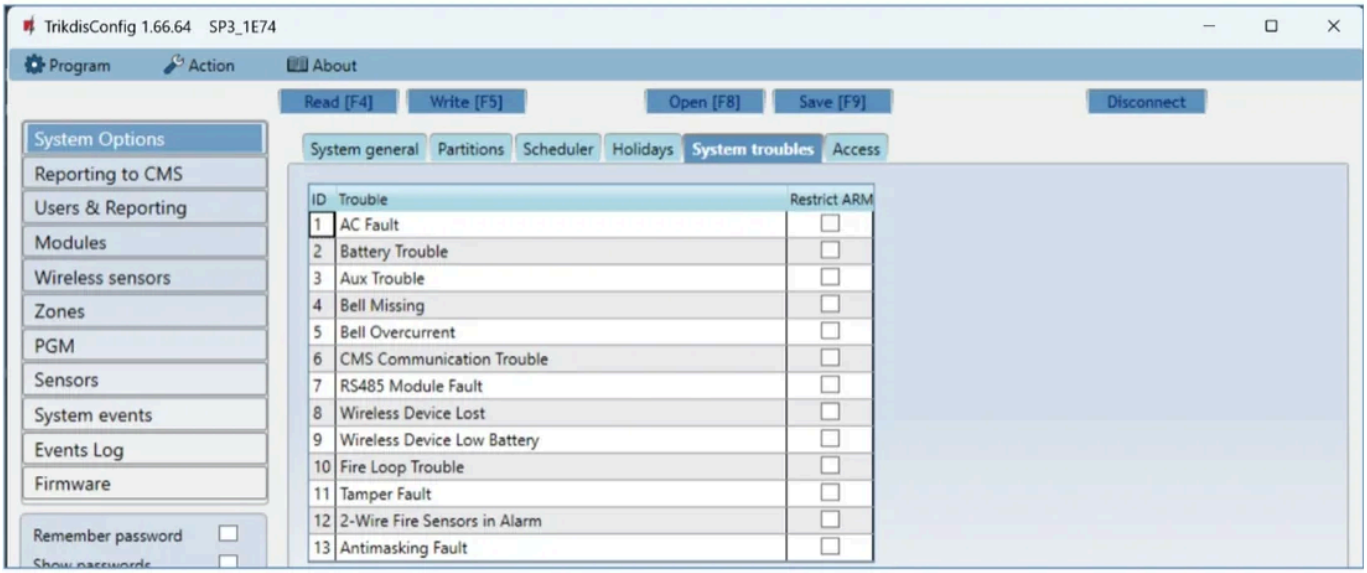


Figure 55. System Options → System troubles : les défauts qui interdisent l'armement.

6.2.6 Onglet Access

Groupe **Access codes** :

- **Administrator Code** – valeur d'usine 123456. Accès complet aux réglages. Six caractères, lettres latines et/ou chiffres.
- **SMS password** – valeur d'usine 123456. Le mot de passe des commandes SMS (5.3), qui permet de commander le système en toute sécurité par SMS ; pour des raisons de sécurité, remplacez-le par un mot de passe à six chiffres connu de vous seul.
- **Installer Code** – valeur d'usine 654321. L'accès de l'installateur aux réglages ; pour des raisons de sécurité, remplacez-le par un code à six chiffres connu de vous seul.

Groupe **Installer permissions** – vous y indiquez ce que peut régler la personne qui se connecte avec le code installateur.

Code administrateur d'usine

Tant que le code administrateur est le code d'usine 123456, le programme affiche les réglages après **Read [F4]** sans demander de code.

Avant la remise

Avant la remise, changez les trois codes. Le code administrateur appartient au propriétaire ; le propriétaire peut aussi modifier ultérieurement le code installateur et ses droits.

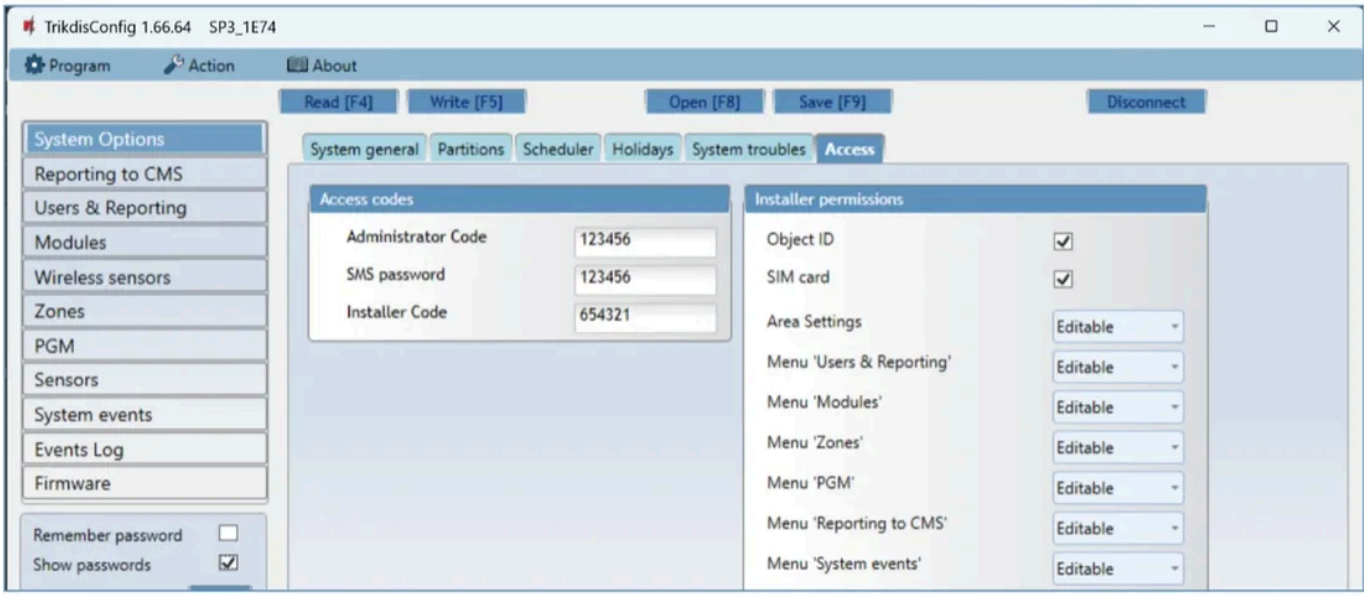


Figure 56. System Options → Access : les trois codes et les droits de l'installateur.

6.3 Reporting to CMS

La centrale envoie les événements au centre de télésurveillance (CMS) par l'Internet mobile (IP) ou par SMS. Vous pouvez définir plusieurs canaux : le canal principal (**Primary**) et le canal parallèle (**Parallel**) fonctionnent simultanément, de sorte que deux récepteurs peuvent recevoir les événements ; à chacun d'eux peut être associé un canal de secours (**Backup**), qui prend le relais si la connexion du canal principal ou parallèle est interrompue. La connexion est chiffrée et protégée par mot de passe ; la réception nécessite un récepteur Trikdis : en IP, le récepteur logiciel IPcom, le récepteur matériel RL14 ou RM14 ; pour les SMS, le RL14, le RM14 ou le GM14. Le SMS convient comme canal de secours, car il fonctionne sans Internet mobile ; il n'est pas recommandé comme canal principal.

6.3.1 Onglet Reporting

Groupes **Primary channel**, **Backup channel**, **Parallel channel** et **Parallel backup channel** :

- **Communication type** – le protocole utilisé avec le récepteur : **TCP/IP**, **UDP/IP**, **SMS** ou **Disabled**.
- **Domain or IP** – le nom de domaine ou l'adresse IP du récepteur.
- **Port** – le port du récepteur.
- **Protocol** – **TRK** pour un récepteur Trikdis, **SIA DC-09** pour un récepteur IP qui accepte le format SIA DC-09.
- **Phone number** – uniquement pour les SMS : le numéro de téléphone du récepteur SMS Trikdis, avec l'indicatif international du pays (par exemple 33… pour la France).
- **Encryption key** – clé de chiffrement à six chiffres, identique à la clé du récepteur.

Si vous renseignez aussi le canal parallèle, les événements partent simultanément sur les deux canaux, de sorte que deux récepteurs (par exemple un centre de télésurveillance local et un centre principal) les reçoivent en même temps. Les deux canaux ne peuvent pas pointer vers le même récepteur.

Backup channel 2 et **Parallel backup channel 2** – secours SMS : le champ **Phone number** reçoit le numéro du récepteur SMS du centre de télésurveillance (avec l'indicatif du pays). La centrale envoie ici si l'envoi échoue sur le canal principal, le canal parallèle et le canal de secours ; c'est particulièrement utile, car cela fonctionne même lorsqu'il n'y a pas de connexion IP dans le réseau de l'opérateur mobile. Cela ne fonctionne que si le premier canal et son secours sont en IP. Un SMS est envoyé à la première mise sous tension, et lorsque la connexion IP est interrompue sur le premier canal et sur son secours.

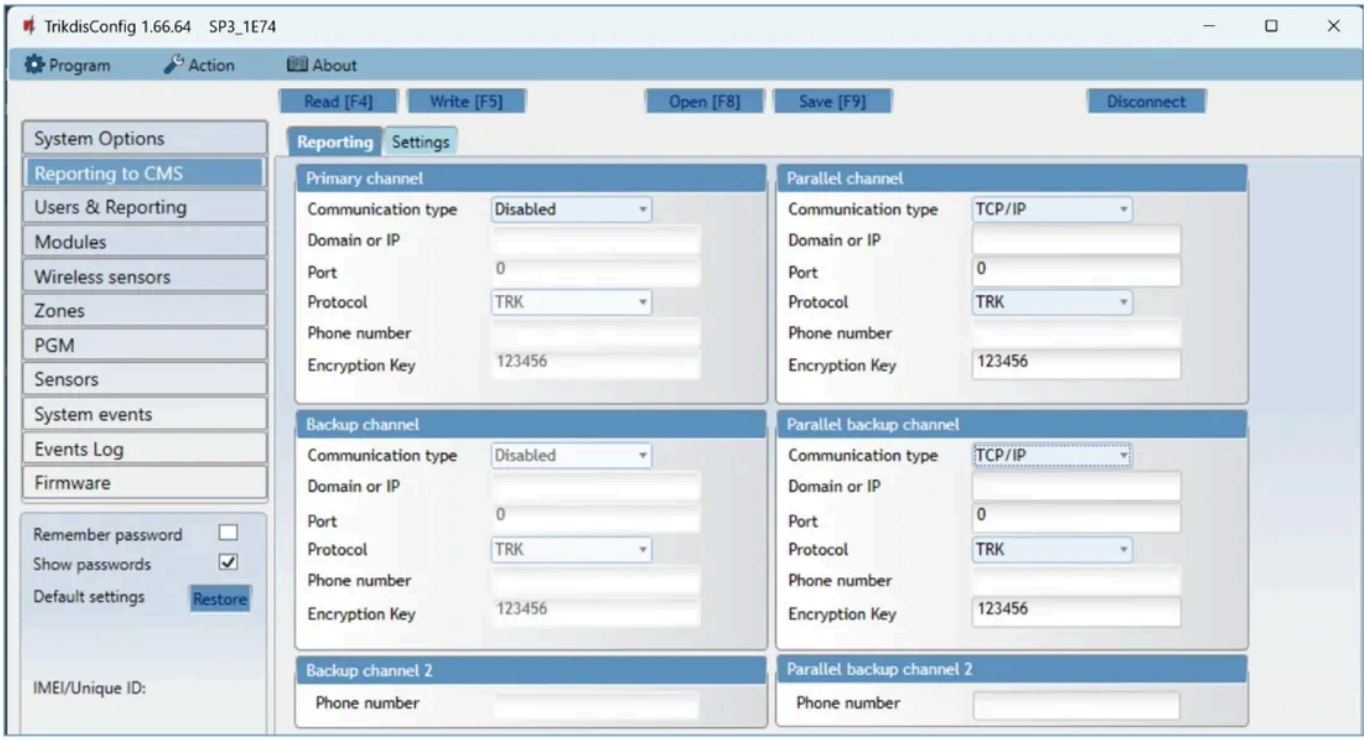


Figure 57. Reporting to CMS → Reporting : canaux principal, de secours et parallèle.

6.3.2 Onglet Settings

Groupe **Settings** :

- **Return to primary after** – après ce nombre de minutes, la centrale tente de revenir sur le canal principal.
- **IP Ping period** – l'intervalle des signaux de contrôle de la connexion IP, en secondes ; activé par la case à cocher.
- **SMS Ping period** – l'intervalle des signaux de contrôle du canal SMS, en minutes ; activé par la case à cocher.
- **Backup reporting after** – après ce nombre d'envois échoués, la centrale passe sur le canal de secours.
- **DNS1**, **DNS2** – adresses des serveurs DNS. Quel que soit le réglage IP, indiquez une adresse DNS prise en charge par le fournisseur.
- **Object ID in SIA DC-09**, **SIA DC-09 receiver No.**, **Line No.** – numéro de site, numéro de récepteur et numéro de ligne pour le protocole SIA DC-09.
- **Local time in SIA** – les messages envoyés au centre de télésurveillance contiennent l'heure propre de la centrale.

Groupe **Reporting mode** – par quelle voie la centrale communique avec le centre de télésurveillance et avec Protegus 2. L'ordre des types compte : si la connexion **Main type** ne s'établit pas, la centrale passe sur la voie **Backup type**, puis **Backup type 2**.

- **Main type**, **Backup type**, **Backup type 2** – **SIM**, **WiFi** ou **LAN(E485)**, séparément dans la colonne CMS et dans la colonne Protegus.
- **Radio T16 (SF485)** – cochez si un émetteur radio T16 transmet aussi. Le T16 fonctionne comme canal de secours si au moins une des connexions SIM, WiFi ou LAN est utilisée ; s'il n'y a pas d'autre connexion, le T16 est le canal principal. Le T16 n'envoie de rapports qu'au centre de télésurveillance.
- **Return to main (both channel)** – après ce nombre de minutes, la centrale tente de revenir sur la voie principale si elle transmettait sur la voie de secours.

Groupe **Communicator network settings** (version WiFi) :

- **DHCP mode** – si la case est cochée, la centrale reçoit automatiquement une adresse IP, un masque de sous-réseau et une passerelle.
- **Static IP**, **Subnet mask**, **Default gateway** – pour le réglage manuel.
- **WiFi SSID name**, **WiFi SSID password** – le nom et le mot de passe du réseau WiFi.

Groupe **SIM parameters** :

- **Disable indication of the absence of a SIM card** – la centrale ne signale pas l'absence de carte SIM.
- **Use dial and SMS when working over internet module** – si la case est cochée, l'appel et le SMS fonctionnent même lorsque la centrale transmet en WiFi ou en LAN. Sans la case cochée, s'il y a du WiFi, la centrale n'utilise ni SMS ni appel ; si, sans la case cochée, il n'y a pas de WiFi, la centrale reste commandable par appel et par SMS, et envoie des SMS à l'utilisateur.
- **Disable the use of SIM card mobile data** – la centrale n'utilise pas les données mobiles de la SIM, elle transmet uniquement en WiFi. Si le WiFi est temporairement indisponible, elle stocke les événements et les envoie plus tard.

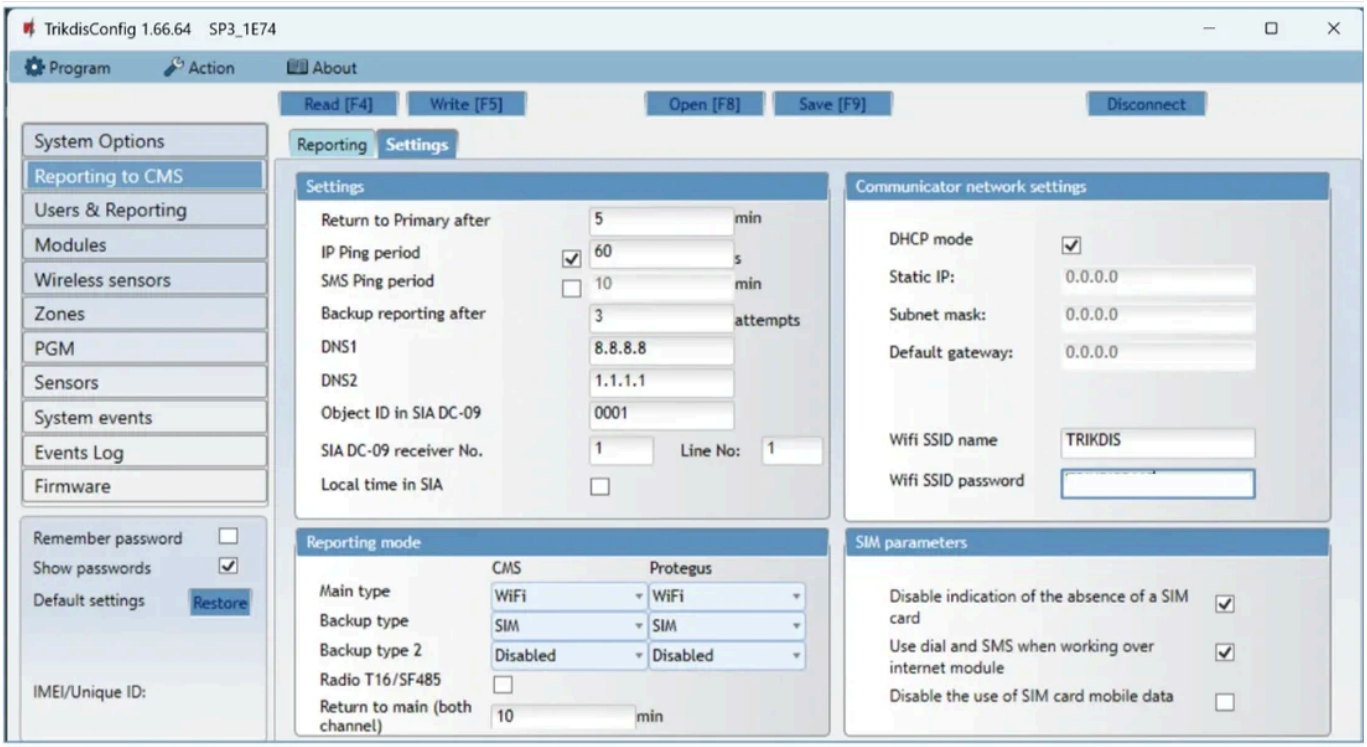


Figure 58. Reporting to CMS → Settings : signaux de contrôle, ordre des connexions, paramètres WiFi et SIM.

6.4 Users & Reporting

Dans les lignes de l'onglet **Users** (groupe **Users & Reporting to User**), vous ajoutez les utilisateurs :

- **Name** – le nom de l'utilisateur, il figure dans les SMS d'événement.
- **Tel number** – numéro de téléphone avec l'indicatif international du pays. Depuis ce numéro, l'utilisateur peut commander le système, et il y reçoit les SMS. Les huit premiers numéros reçoivent les rapports par SMS et par appel.
- **Email** – adresse e-mail ; l'utilisateur reçoit une invitation à Protegus 2.
- **Code** – le code d'armement et de désarmement de l'utilisateur.
- **Tag code** – le numéro d'identification d'une carte RFID, d'un badge porte-clés ou d'une clé iButton.
- **Areas** – les partitions qu'il peut gérer.
- **A**, **D** – il peut armer, ou désarmer.
- **PGM** – il peut commander les sorties par appel téléphonique, avec des signaux DTMF (5.4).
- **ACK** – la centrale confirme par SMS l'exécution des commandes reçues.
- **FWD** – la centrale transfère à cet utilisateur les SMS provenant de non-utilisateurs (information de solde, publicité).

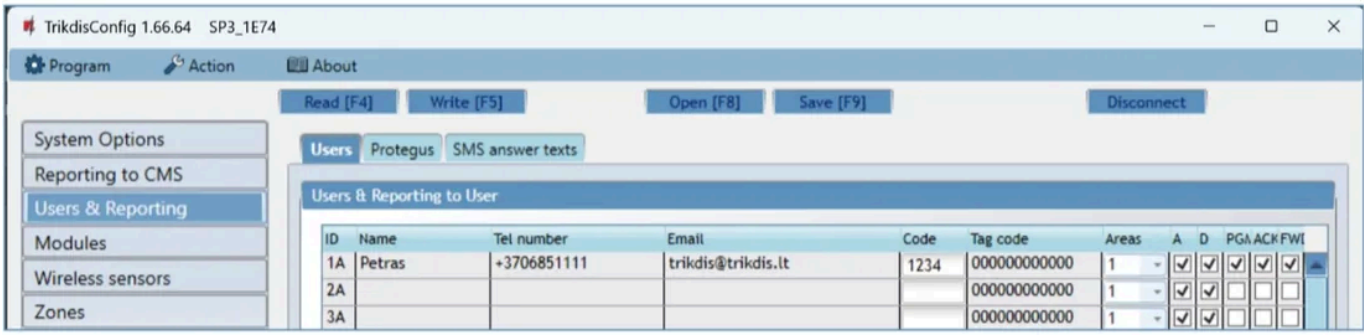


Figure 59. Users & Reporting → Users : utilisateurs, codes, identifiants et droits.

6.4.1 Cartes et badges RFID

Vous n'enregistrez pas la carte ou le badge RFID en le présentant au lecteur : vous saisissez manuellement le numéro d'identification de la carte, sous forme de nombre décimal, dans le champ **Tag code**, puis **Write [F5]**. Le numéro est imprimé sur la plupart des cartes.



Figure 60. Numéros imprimés d'une carte RFID : le premier groupe de chiffres encadré est le **Tag code**.

Un lecteur Wiegand sans clavier, pour l'ouverture de porte

1. Vous raccordez les fils de données du lecteur aux bornes **GRN** et **YEL** de la carte.
2. Dans l'onglet **Modules** → **Keypads**, groupe **Keypad parameters**, le **Keypad type** doit être **Wiegand reader**, même s'il n'y a pas de clavier.

3. Dans la fenêtre **PGM**, le champ **Output definition** de la sortie commandée est **Remote control**, **Pulse time, s** par exemple 5.
4. Dans l'onglet **PGM → Control**, à la ligne du lecteur, cochez le champ **En**, saisissez le numéro de la sortie dans le champ **PGM**, et réglez **PGM mode** sur **Pulse**.

6.4.2 Clés iButton

Enregistrement avec le lecteur **TM17** :

1. Si la liste **Tag code** est vide, la première clé enregistrée est placée sur la première ligne de la liste et devient la clé maître (Master).
2. Pour activer le mode d'enregistrement, maintenez la clé maître contre l'« œil » du lecteur pendant au moins 10 secondes. En mode d'enregistrement, la LED **State** du TM17 clignote en vert.
3. Présentez les clés utilisateur une par une au lecteur. Trois bips indiquent que la clé a été ajoutée au système.
4. À la fin, présentez de nouveau la clé maître au lecteur ; la LED **State** cesse de clignoter.
5. Pour effacer toutes les clés (y compris la clé maître), maintenez la clé maître contre le lecteur pendant au moins 20 secondes.

Avec le lecteur **CZ-Dallas**, de la même façon, mais sans signalisation LED : clé maître pendant 10 secondes, clés utilisateur une par une, à la fin de nouveau la clé maître ; effacement en 20 secondes.

Le rôle de la clé maître

La clé maître sert à enregistrer les autres clés. Si vous l'utilisez aussi pour armer et désarmer, la commande est exécutée avec un retard.

6.4.3 Onglet Protegus

Groupe **Cloud application** :

- **Enable cloud service** – activation du cloud Protegus. C'est par lui que la centrale communique avec Protegus 2, et par lui qu'elle peut être configurée à distance avec TrikdisConfig.
- **Parallel reporting** – les événements partent simultanément sur le canal principal vers le centre de télésurveillance et vers Protegus 2.
- **Cloud access code** – code à six chiffres pour la connexion Protegus 2, valeur d'usine 123456.

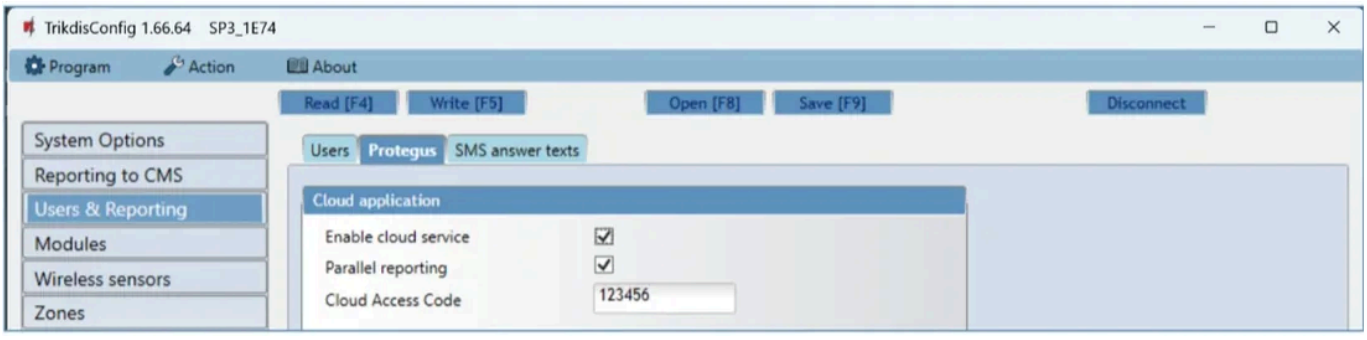


Figure 61. Users & Reporting → Protegus : l'interrupteur du service cloud et le code d'accès.

6.4.4 Onglet SMS answer texts

Vous pouvez modifier le texte des réponses aux commandes SMS dans la colonne **SMS text**, par exemple pour le mettre en français.

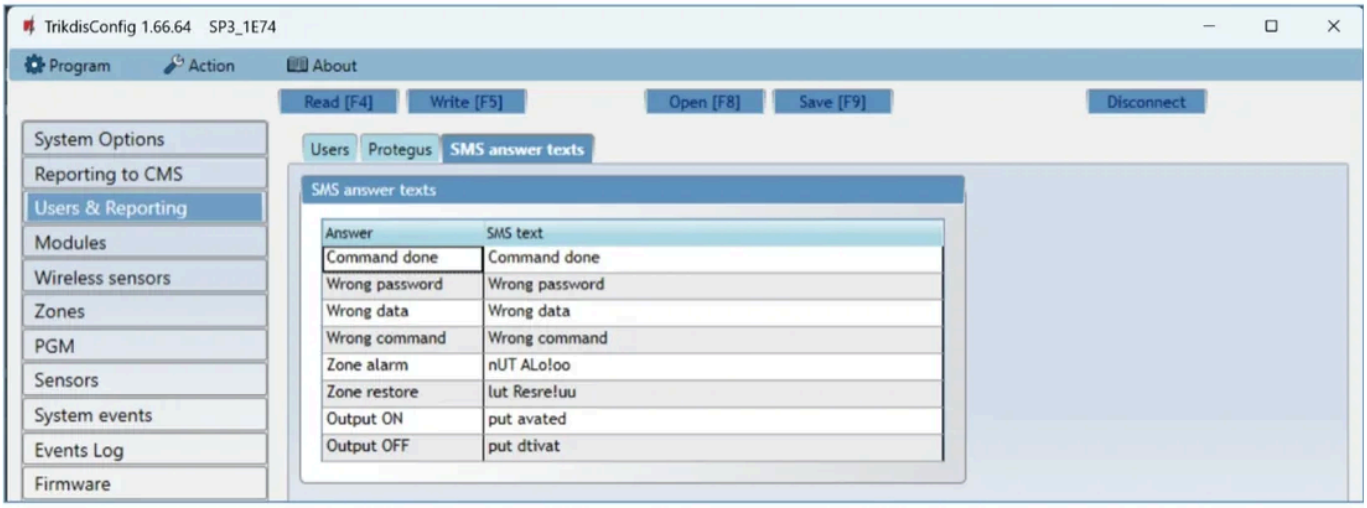


Figure 62. Users & Reporting → SMS answer texts : le texte des SMS de réponse.

6.5 Modules

Onglet **Keypads** :

- **Serial** – le numéro de série du clavier, reconnu automatiquement par la centrale. Pour le supprimer, saisissez des zéros, ou appuyez sur le bouton **Remove**.
- **Keypad type** – le type du clavier, reconnu automatiquement.
- **Areas** – les partitions que le clavier peut gérer (uniquement pour les claviers FLEXi SK LCD, FLEXi SK LED, SK LCD Button et SK LED Button).
- **Remove** – suppression du clavier de la liste.

Groupe **Keypad parameters** :

- **Keypad type** – le type du clavier raccordé aux bornes **GRN** et **YEL** : **Crow CR16**, **Paradox LED** ou **Wiegand reader**.
- **Additional Wiegand on 1IO/2IO** – cochez si vous raccordez un second lecteur RFID aux bornes **IO1** et **IO2**. Celles-ci ne peuvent alors plus être utilisées comme entrées ou sorties.
- **6 digits user code** – code utilisateur à six chiffres sur le clavier. Pour un code existant à quatre chiffres, le programme ajoute les deux premiers chiffres (1234 devient 123412) ; tous les codes utilisateur à quatre chiffres sont ainsi convertis.
- **Duress code type** – le type de code sous contrainte. Sous la contrainte, vous armez ou désarmez avec ce code : le système exécute la commande et envoie silencieusement une alarme au centre de télésurveillance.
- **Quick ARM** – les touches **ARM**, **STAY** et **SLEEP** du clavier arment sans code.
- **Incorrect codes until lockout** – après ce nombre de codes erronés, le clavier se verrouille.
- **Lockout timer** – la durée du verrouillage en minutes.
- **Panic alarm type**, **Medical alarm type**, **Fire alarm type** – l'effet des touches de fonction panique, médicale et incendie du clavier lorsqu'on les presse : **Audible** (la sirène sonne, le clavier émet une alarme sonore, et le rapport est envoyé à Protegus 2 et au centre de télésurveillance), **Silent** (seul le rapport est envoyé à Protegus 2 et au centre de télésurveillance, la centrale désactive l'alarme sonore), **Disabled** (aucun rapport n'est envoyé, ni à Protegus 2, ni au centre de télésurveillance).
- **Low voltage reader (1IO/2IO)** – si le lecteur RFID raccordé ne fonctionne pas, vous changez avec ceci le protocole entre la centrale et le lecteur.
- **Use fingerprint** – pour un lecteur d'empreintes digitales au protocole Wiegand 26/34.

- **Do not change charset** – sur le clavier SK-LCD TouchPad, le codage des caractères des noms de zones et de partitions est conservé.
- **Custom entry beep** – le son de la temporisation d'entrée sur le clavier est intermittent.

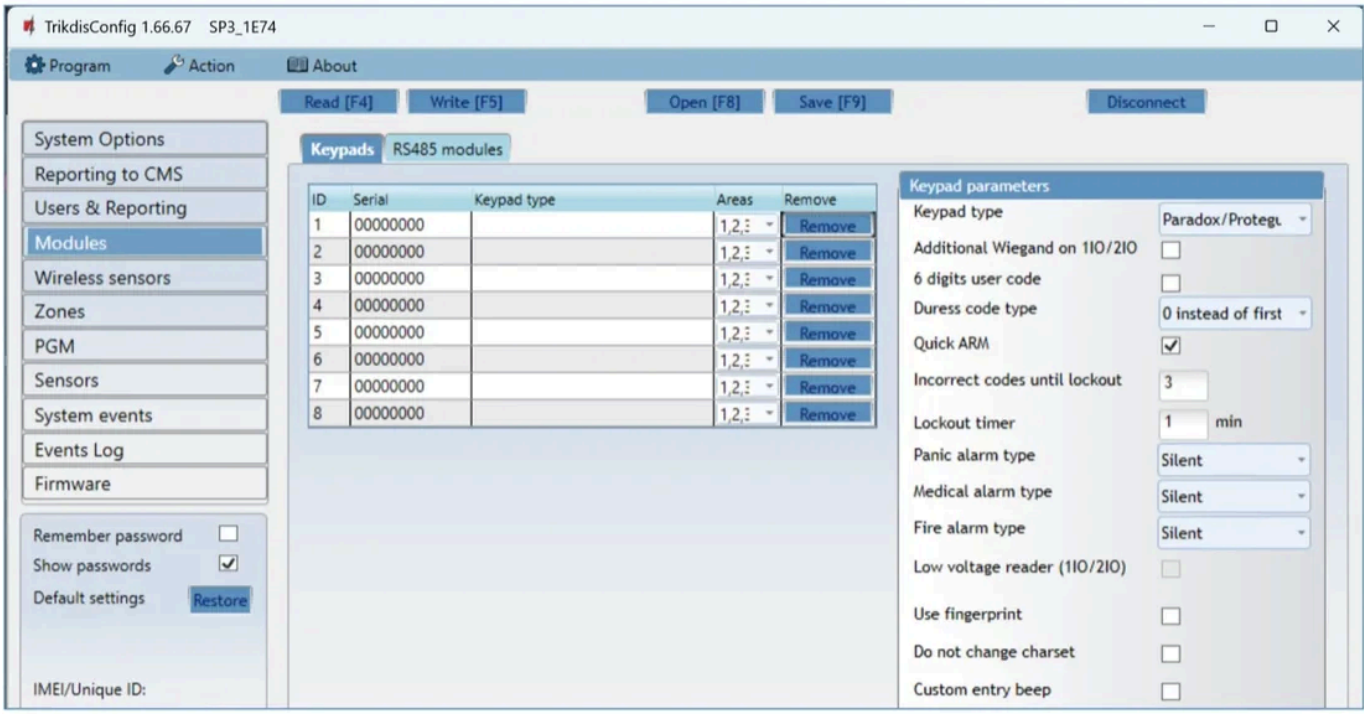


Figure 63. Modules → Keypads : les claviers reconnus et les paramètres des claviers.

Onglet **RS485 modules** :

- **ID** – le numéro d'ordre du module.
- **Module** – le type d'extension dans la liste : iO, iO-WL, TM17, iO-8, RF-SH, E485, T16, SF485, iO-MO, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-LORA, RF-HW, RF-S8.
- **Serial No.** – obligatoire, numéro à six chiffres figurant sur l'autocollant du boîtier et de l'emballage du module.
- **Area** – la partition du module. Le TM17 affiche l'état et les zones de cette partition.
- **Name** – le nom du module.
- **Firmware version** – dès que la centrale trouve le module, sa version de firmware apparaît ici. C'est le signe que le module est actif.

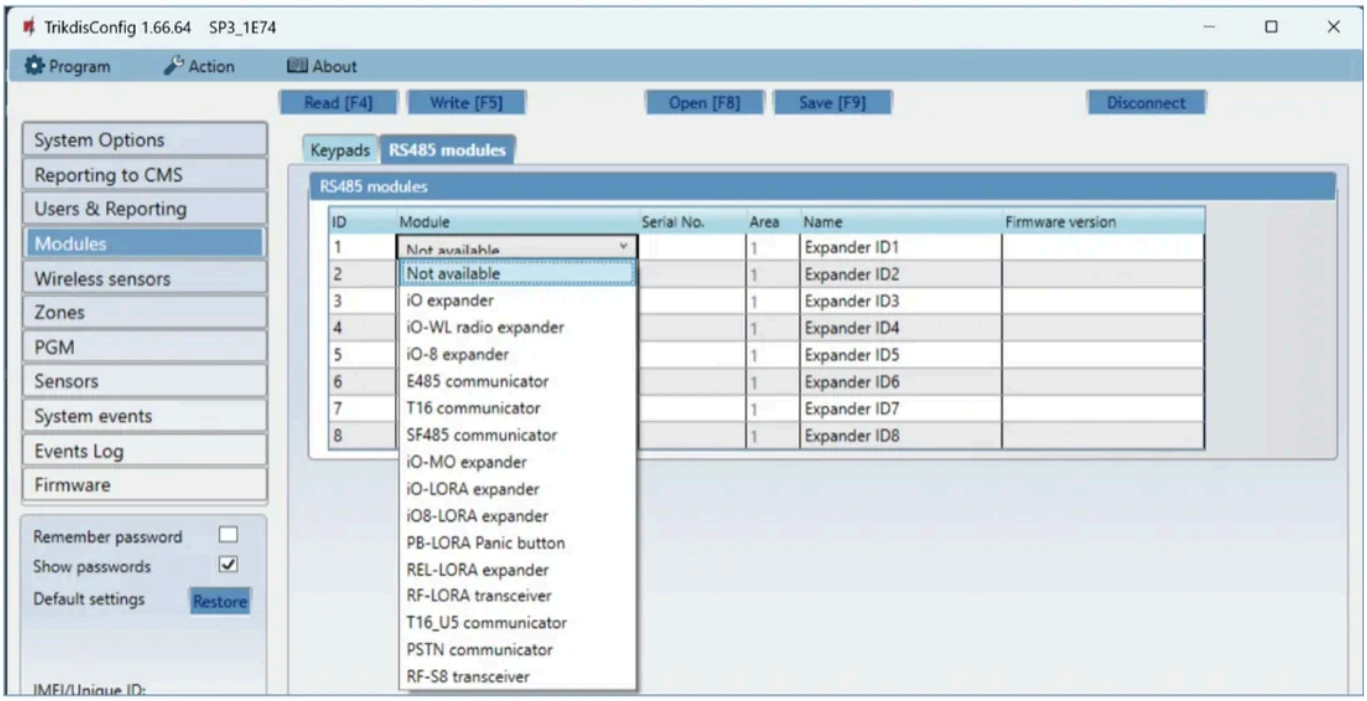


Figure 64. Modules → RS485 modules : la liste des extensions avec la liste déroulante **Module**.

Onglet **E485 settings** – les réglages réseau du communicateur LAN E485 : **DHCP mode** (adresse automatique : si la case est cochée, la centrale lit automatiquement les réglages réseau – masque de sous-réseau, passerelle – et reçoit automatiquement une adresse IP), ou pour le réglage manuel **Static IP**, **Subnet mask**, **Default gateway**.



Figure 65. Modules → E485 settings : l'adressage du module LAN E485.

6.6 Wireless sensors

Avec le module RF-LORA, la « FLEXi » SP3 utilise les détecteurs, sirènes et télécommandes sans fil du fabricant Maximum. Cela nécessite sur la centrale un firmware au code récepteur 4, au moins en version 1.21 (SP3_xxx4_0121 ou plus récent ; le 4e chiffre du nom du firmware est le type de récepteur, voir 1.7). Vous raccordez l'émetteur-récepteur RF-LORA au bus RS485 de la centrale (4.6). Vous enregistrez d'abord le module RF-LORA auprès de la centrale (6.6.1), puis vous enregistrez les détecteurs : à distance depuis TrikdisConfig (6.6.2) ou avec le bouton LEARN du module (6.6.3). L'appairage des détecteurs S8 fonctionnant avec le récepteur RF-S8 est décrit au chapitre 4 du Manuel de l'émetteur-récepteur RF-S8 et des détecteurs S8.



Figure 66. La fenêtre **Wireless sensors** : la liste des appareils enregistrés, avec au-dessus les boutons **Learn sensors** et **Update**.

6.6.1 Enregistrement du RF-LORA

1. Mettez la centrale sous tension, et attendez 1 minute.
2. Lancez TrikdisConfig, et reliez la centrale à l'ordinateur avec un câble USB Mini-B.
3. Appuyez sur le bouton **Read [F4]**, et ouvrez l'onglet **Modules → RS485 modules**. Si **RF-LORA transceiver** figure dans la liste avec son numéro de série et sa version de firmware, c'est terminé, les autres étapes sont inutiles.
4. S'il n'y figure pas, sélectionnez **RF-LORA transceiver** dans le champ **Module** d'une ligne vide.
5. Dans le champ **Serial No.**, saisissez le numéro de série du module figurant sur l'autocollant de son boîtier ou de son emballage.
6. **Write [F5]**, puis débranchez le câble USB.
7. Attendez 1 minute que la centrale et le RF-LORA se connectent.
8. Rebranchez le câble USB, et appuyez sur le bouton **Read [F4]**. La version de firmware du RF-LORA apparaît dans la fenêtre **Modules** : le module est enregistré.
9. Débranchez le câble USB, appuyez sur le bouton **Disconnect**, et attendez 1 minute.

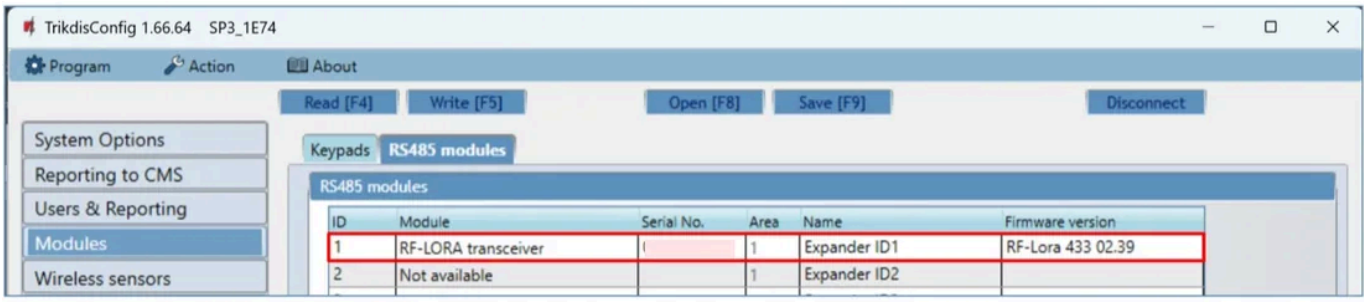


Figure 67. La ligne du RF-LORA enregistré dans l'onglet **RS485 modules** : type, **Area**, nom et **Firmware version**. Le numéro de série a été masqué sur la figure.

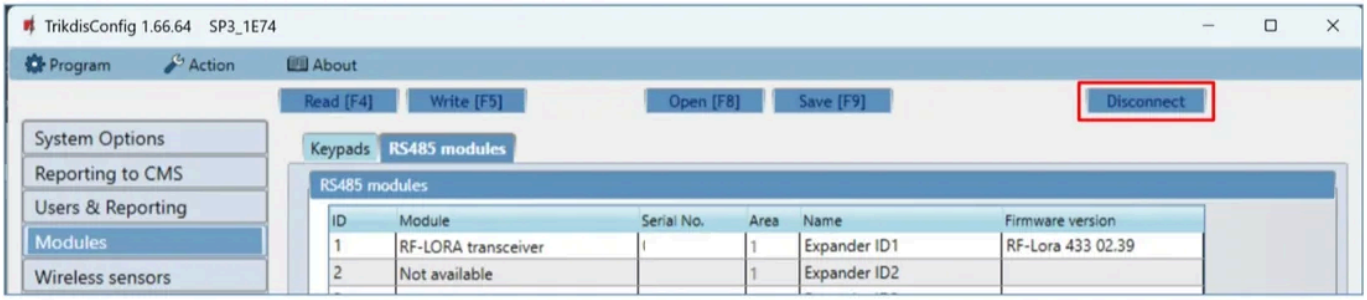


Figure 68. Après la lecture, la version de firmware du RF-LORA apparaît, ensuite **Disconnect**.

6.6.2 Appairage des détecteurs à distance

Conditions de la configuration à distance : une carte SIM activée avec PIN saisi ou désactivé et Internet mobile (ou une connexion WiFi), le service cloud activé (6.4.3), l'alimentation et la connexion réseau (la LED **NET** est verte en continu).

1. Sur l'écran d'accueil de TrikdisConfig, saisissez dans le champ **Unique ID** du groupe **Remote access** le numéro **IMEI/Unique ID** de la centrale (figurant sur l'autocollant de la carte et de l'emballage), et appuyez sur le bouton **Configure**.
2. Dans la fenêtre qui s'ouvre, **Read [F4]** ; si nécessaire, saisissez le code administrateur ou installateur.
3. Ouvrez la fenêtre **Wireless sensors**, et appuyez sur le bouton **Learn sensors**. Le RF-LORA passe en mode d'apprentissage, sa LED **DATA/TROUBLE** se met à clignoter en vert et rouge, TrikdisConfig ouvre la fenêtre d'apprentissage.
4. Insérez les piles dans les détecteurs (détecteur de mouvement, d'ouverture, d'eau, de fumée, sirène). Vous pouvez enregistrer plusieurs détecteurs à la fois. Le RF-LORA doit se trouver à au moins 1 m des détecteurs.
5. Appuyez sur le bouton **TAMPER** (autoprotection) du détecteur. La LED **DATA/TROUBLE** du RF-LORA clignote brièvement en vert (le détecteur a été ajouté), puis, après quelques secondes, de nouveau en vert et rouge.
6. TrikdisConfig ouvre une nouvelle fenêtre : indiquez les valeurs **Zone number** et **Zone definition** du détecteur, puis **Save**. Le détecteur est ajouté à la liste.
7. Pour le détecteur suivant, de nouveau le bouton **TAMPER**, et ainsi de suite. À la fin, appuyez sur le bouton **Stop learning**.
8. À la question, **Yes** : les détecteurs sont écrits dans la centrale (**No** si vous voulez encore les modifier avant). Attendez quelques minutes, puis **Read [F4]** : la fenêtre **Wireless sensors** affiche les détecteurs enregistrés, et la colonne **Serial No.** leur numéro de série.
9. Vérifiez dans la fenêtre **Zones** que les détecteurs ont été affectés à la bonne zone et à la bonne partition. Si le champ **Type** de la zone est **EOL_T**, la surveillance de l'autoprotection du détecteur est aussi active. Après modification, **Write [F5]**.

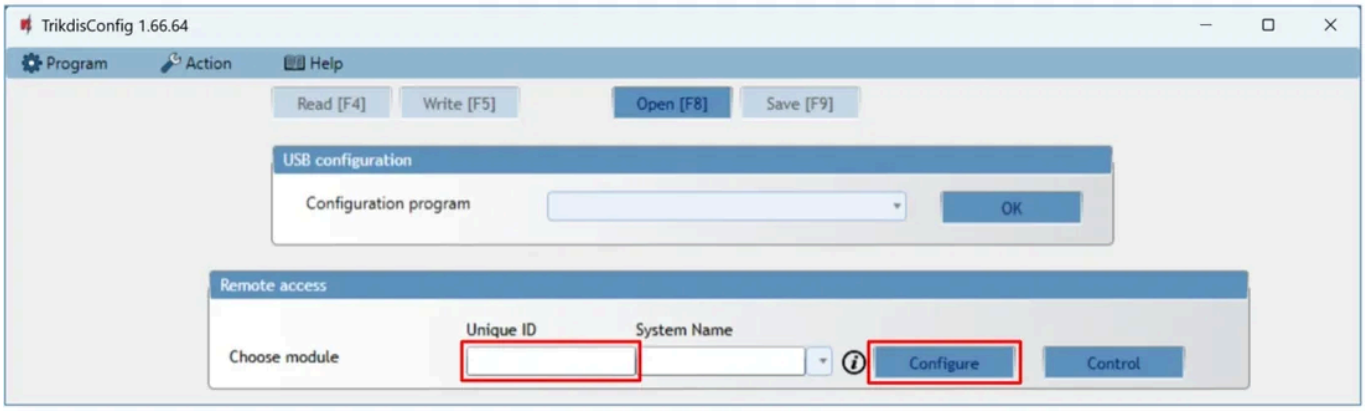


Figure 69. Le groupe **Remote access** de l'écran d'accueil : **Unique ID**, **System Name**, **Configure**.

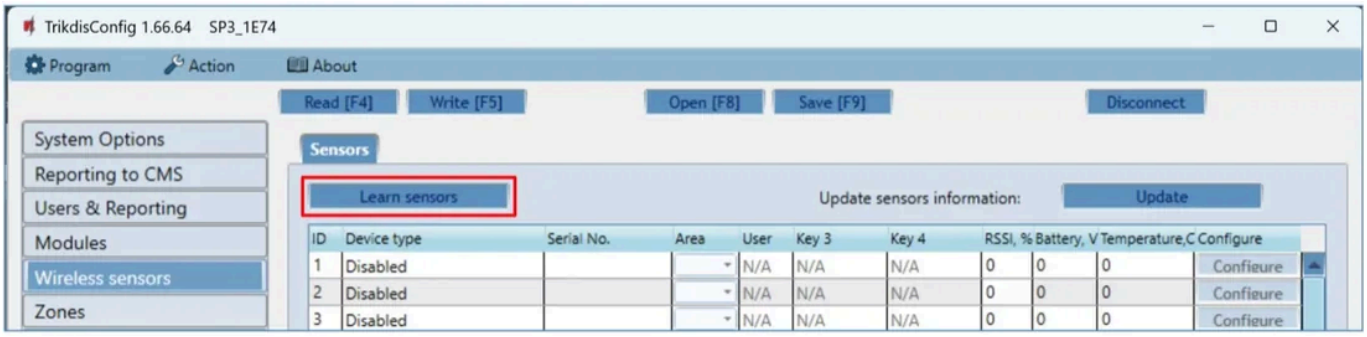


Figure 70. Le bouton **Learn sensors** de la fenêtre **Wireless sensors** lance le mode d'apprentissage.

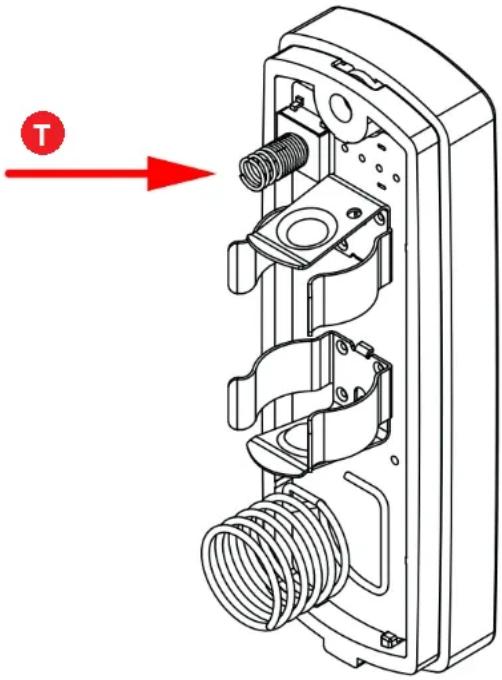


Figure 71. L'appui sur le bouton **TAMPER** situé sous le capot arrière du détecteur enregistre le détecteur.

- T bouton d'autoprotection (« Tamper »)

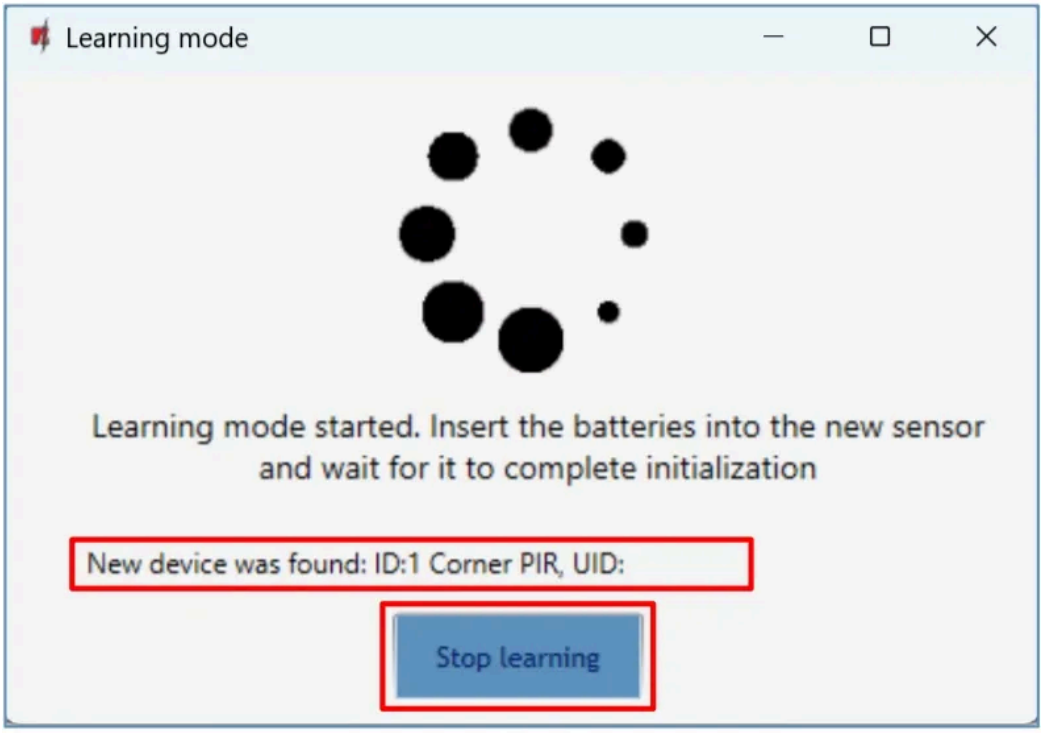


Figure 72. La fenêtre d'apprentissage : type et identifiant du détecteur trouvé, en dessous le bouton **Stop learning**. L'identifiant a été masqué sur la figure.

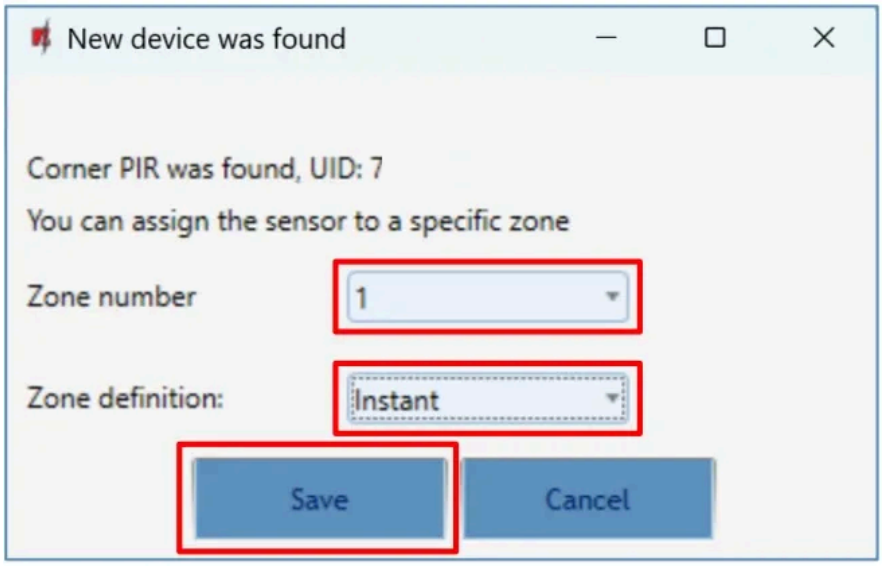


Figure 73. La fenêtre du nouvel appareil : **Zone number**, **Zone definition**, **Save**.

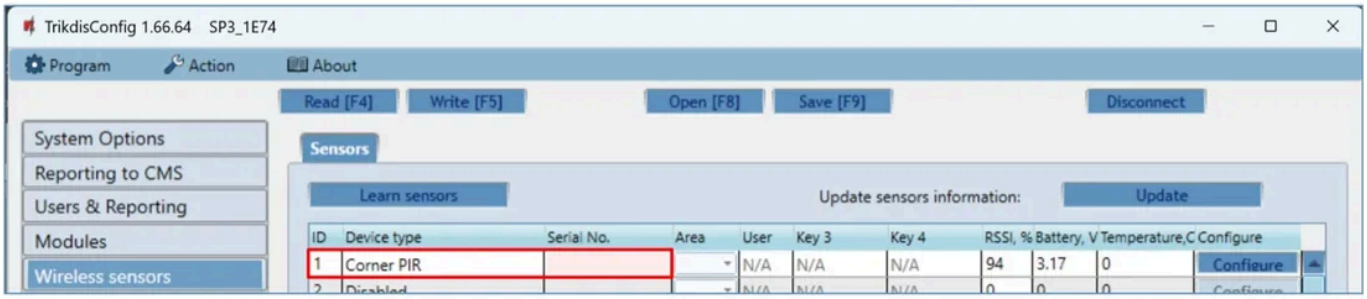


Figure 74. Le détecteur enregistré dans la liste, avec la puissance du signal (**RSSI**), la tension de la pile et la température. Le numéro de série a été masqué sur la figure.

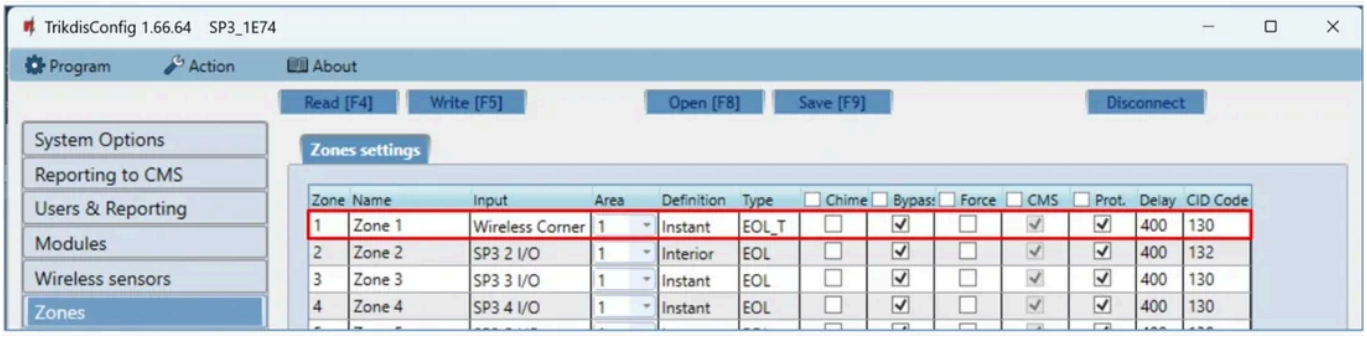


Figure 75. Dans la fenêtre **Zones**, la zone du détecteur sans fil de type **EOL_T** : le signal d'autoprotection est aussi surveillé.

Suppression d'un détecteur sans fil

Connectez-vous à la centrale par USB ou à distance, **Read [F4]**, puis dans la colonne **Device type** de la fenêtre **Wireless sensors**, sélectionnez **Disabled** pour le détecteur à supprimer, et **Write [F5]**.

6.6.3 Appairage avec le bouton LEARN

1. Le RF-LORA doit être enregistré auprès de la centrale (6.6.1), la centrale doit être sous tension.
2. Retirez le couvercle du RF-LORA. Maintenez le bouton **LEARN** enfoncé jusqu'à ce que la LED **DATA/TROUBLE** se mette à clignoter en vert et rouge, puis relâchez-le. Le clignotement indique le mode d'apprentissage.
3. Insérez les piles dans les détecteurs, et appuyez sur le bouton **TAMPER** du détecteur. Un bref clignotement vert de la LED **DATA/TROUBLE** indique la réussite ; après quelques secondes, elle clignote de nouveau en vert et rouge. Pour le détecteur suivant, de nouveau le bouton **TAMPER**.
4. À la fin, maintenez le bouton **LEARN** enfoncé jusqu'à ce que le clignotement vert et rouge cesse, puis relâchez-le. Le RF-LORA a quitté le mode d'apprentissage.
5. Reliez la centrale à l'ordinateur par USB, lancez TrikdisConfig, **Read [F4]**. Dans la fenêtre **Wireless sensors**, les appareils enregistrés apparaissent avec leur numéro de série à sept chiffres.
6. Dans la fenêtre **Zones**, vérifiez les zones et les partitions ; après modification, **Write [F5]**.

6.6.4 RF-SH et appareils Crow

Les anciens systèmes avec module RF-SH utilisent les appareils sans fil des séries Crow FW2 et Shepherd (SH). Le RF-SH n'est plus disponible ; la description est conservée ici brièvement pour la maintenance des systèmes existants ; le raccordement du module est présenté à la section 4.2.

- **Enregistrement du RF-SH** – comme pour le RF-LORA (6.6.1) : dans l'onglet **Modules → RS485 modules**, **RF-SH**, **Serial No.**, **Write [F5]**, débrancher l'USB, attendre 1 minute, rebrancher l'USB, **Read [F4]** ; l'apparition de la version de firmware est le signe de la réussite.
- **Détecteurs FW2** – appuyez sur le bouton **LEARN** du module jusqu'à ce que la LED **LEARN** clignote en vert. Insérez la pile du détecteur, et attendez que ses LED s'éteignent. Quittez avec le bouton **LEARN**, USB, **Read [F4]** : le numéro de série à sept chiffres doit correspondre à celui figurant sur le boîtier. Indiquez la zone et la partition, **Write [F5]**. Suppression : **Device type → Disabled**.
- **Télécommande FW2** – maintenez ensemble les boutons 3 et 4 jusqu'à ce que la LED clignote en jaune, puis en vert. Dans la liste, indiquez sa partition et son utilisateur ; la fonction des boutons 3 et 4 (armement, désarmement, panique silencieuse ou sonore) se choisit dans le tableau. Réinitialisation de la télécommande : boutons 2 et 3 ensemble, jusqu'à voir un clignotement vert et rouge.
- **Sirène FW2** – mettez la sirène sous tension ; le flash clignote lentement pendant 30 secondes. Pendant ce temps, maintenez le bouton **LEARN** sur la carte de la sirène jusqu'à ce que le flash clignote rapidement, et relâchez-le. Réinitialisation : en maintenant le bouton **LEARN** enfoncé, mettez sous

tension, jusqu'à trois clignotements.

- **Détecteurs et clavier SH** – insérez la pile ; l'allumage de la LED verte pendant 3 secondes indique la réussite de l'enregistrement. En cas d'échec, retirez la pile pendant 10 secondes, et réessayez.

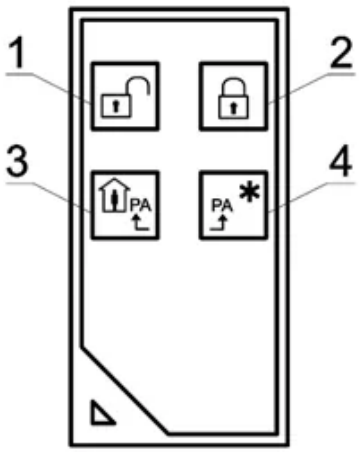


Figure 76. Télécommande Crow FW2 : pour l'enregistrement, vous maintenez ensemble les boutons 3 et 4.

6.7 Zones

Onglet **Zones settings** :

- **Zone No** – le numéro de la zone.
- **Name** – le nom de la zone.
- **Input** – l'entrée **IN** de la centrale ou de l'extension associée à la zone.
- **Area** – la partition de la zone.
- **Definition** – le fonctionnement de la zone :
  - **Delay** – zone temporisée, pour le détecteur magnétique d'ouverture de la porte d'entrée. Pour ce type de zone, vous pouvez régler un temps d'entrée et un temps de sortie. Après l'armement, pendant le temps de sortie, la zone Delay peut être violée librement (la porte peut être ouverte) ; si elle est encore violée à l'expiration du temps de sortie, les sorties **Siren** et **Flash** s'activent, et le rapport d'alarme est envoyé. Système armé, la violation de la zone Delay lance le temps d'entrée, pendant lequel le système doit être désarmé ; si vous ne le désarmez pas avant l'expiration du temps d'entrée, les sorties **Siren** et **Flash** s'activent, et le rapport d'alarme est envoyé.
  - **Interior** – zone suiveuse, pour le détecteur de mouvement situé près de la porte d'entrée. Système armé, sa violation active les sorties **Siren** et **Flash**, et le rapport d'alarme est envoyé. Si, système armé, la zone Delay est violée en premier, la zone Interior peut être violée librement pendant le temps d'entrée réglé ; si vous ne désarmez pas le système pendant le temps d'entrée, les sorties **Siren** et **Flash** s'activent, et le rapport d'alarme est envoyé.
  - **Interior Stay** – zone suiveuse, pour le détecteur de mouvement situé près de la porte d'entrée ; elle fonctionne comme la zone Interior : système armé, sa violation active les sorties **Siren** et **Flash**, et le rapport d'alarme est envoyé, mais si la zone Delay a été violée en premier, elle peut être violée librement pendant le temps d'entrée. Système armé en mode STAY, les zones Interior Stay ne sont pas protégées (la centrale ne les surveille pas).

    - **Instant** – zone instantanée, pour les détecteurs de mouvement. Si, système armé, la zone Instant est violée, les sorties **Siren** et **Flash** s'activent immédiatement, sans temps d'entrée, et le rapport d'alarme est envoyé.
    - **Instant Stay** – zone instantanée, pour les détecteurs de mouvement. Si, système armé, la zone Instant Stay est violée, les sorties **Siren** et **Flash** s'activent immédiatement, et le rapport d'alarme est envoyé. Système armé en mode STAY, les zones Instant Stay ne sont pas protégées.
    - **Fire** – pour les détecteurs incendie. Lors de sa violation, les sorties **Siren** et **Flash** démarrent immédiatement, et le rapport est envoyé.
    - **Keyswitch** – pour un interrupteur à clé ou un autre interrupteur : la zone arme et désarme. L'armement a lieu après l'expiration du temps de sortie.
    - **24_hour** – pour les détecteurs de bris de vitre et d'autoprotection. Toujours surveillée, elle déclenche immédiatement l'alarme lors de sa violation : les sorties **Siren** et **Flash** s'activent, et le rapport d'événement est envoyé.
    - **Silent** – système armé, le rapport est envoyé immédiatement lors de sa violation, mais les sorties **Siren** et **Flash** ne démarrent pas.
    - **Silent 24h** – pour un bouton panique. Quel que soit l'état du système, le rapport d'événement est envoyé immédiatement, sans sirène : les sorties **Siren** et **Flash** ne démarrent pas.
- **Type** – le type de boucle raccordée à l'entrée, dans une liste : **NC** (normalement fermée), **NO** (normalement ouverte), **EOL** (avec résistance de fin de ligne), **EOL_T** (avec résistance de fin de ligne et surveillance de l'autoprotection), **ATZ** (deux zones sur une entrée : deux circuits de zone normalement fermés avec résistances de fin de ligne, sans surveillance de l'autoprotection – pour ce type, sélectionnez aussi la seconde zone ATZ dans la liste **Input**), **ATZ_T** (deux zones avec surveillance de l'autoprotection : deux circuits de zone normalement fermés avec résistances de fin de ligne et surveillance de l'autoprotection – pour ce type aussi, sélectionnez la seconde zone ATZ dans la liste **Input**), **3EOL** (avec résistance de fin de ligne et surveillance de l'autoprotection, pour les détecteurs de mouvement avec fonction anti-masquage – anti-masking). Vous indiquez les valeurs des résistances dans le champ **System Options** → **EOL Type** (6.2.1).
- **Chime** – carillon : le clavier émet un bip à l'ouverture de la zone.
- **Bypass** – la zone peut être exclue.
- **Force** – armement forcé : le système peut être armé même avec une zone ouverte ; la zone ouverte lors de l'armement est temporairement ignorée, elle est de nouveau surveillée après sa fermeture (son rétablissement), et sa violation déclenche ensuite l'alarme.
- **CMS** – les événements de la zone sont envoyés au centre de télésurveillance.
- **Prot.** – les événements de la zone sont envoyés au cloud Protegus.
- **Delay** – le temps de réaction de l'entrée en millisecondes.
- **CID code** – le code Contact ID de l'événement, renseigné automatiquement lors du choix de la définition.
- **Sound** – le numéro du message vocal que la centrale diffuse en cas d'alarme à l'utilisateur appelé (uniquement SP3_12xx, firmware 1.13 au maximum).

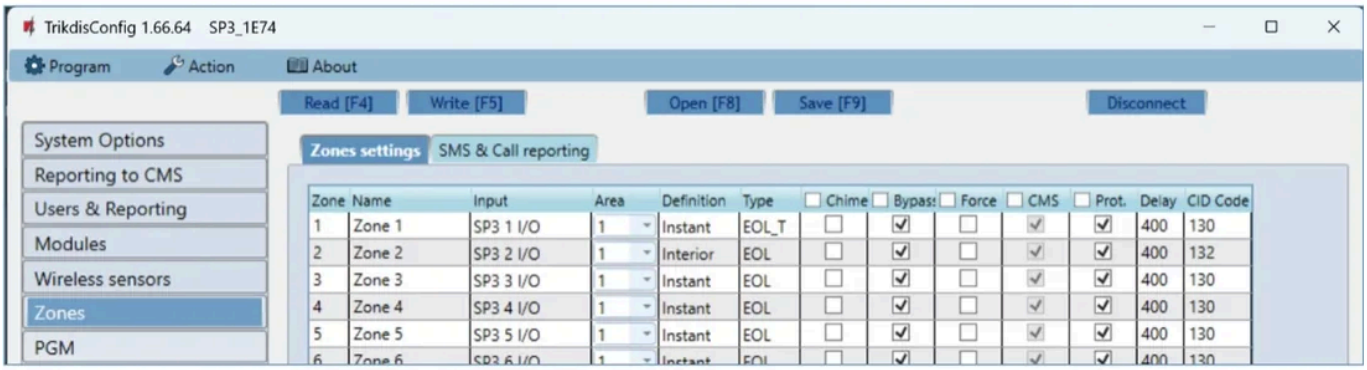


Figure 77. Zones → Zones settings : la définition, le type de boucle et les options des zones.

Onglet **SMS & Call reporting** – il n'apparaît que si la fenêtre **Users & Reporting** contient au moins un numéro de téléphone.

- **Zn** – le numéro de la zone et le type d'événement : **Event** (alarme) ou **Restore** (rétablissement).
- **User / SMS and Call** – pour chaque utilisateur, vous cochez s'il reçoit un SMS et/ou un appel pour l'événement de la zone.

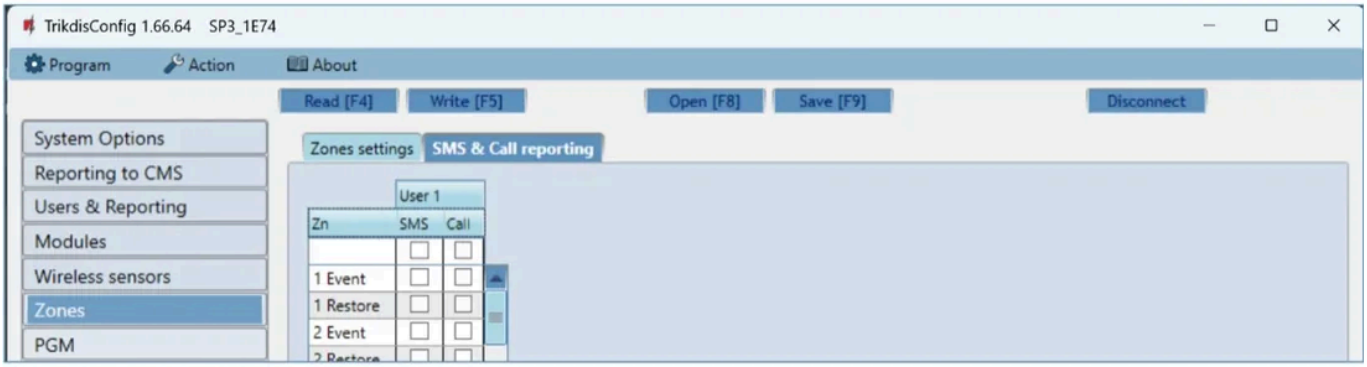


Figure 78. Zones → SMS & Call reporting : qui reçoit un SMS ou un appel pour les événements de chaque zone.

6.8 PGM

Onglet **Outputs** :

- **PGM No** – le numéro de la sortie PGM.
- **Name** – le nom de la sortie.
- **PGM output** – la sortie **OUT** de la centrale ou d'une extension associée à la PGM.
- **Area** – la partition de la sortie.
- **Output definition** – le fonctionnement de la sortie :
  - **Siren** – pour une sirène.
  - **Remote control** – pour commander un appareil externe (depuis l'application, par SMS, par appel, avec un lecteur).
  - **Fire Sensor Reset** – pour réinitialiser les détecteurs incendie après une alarme.
  - **System State** – pour un indicateur d'état, par exemple une LED indiquant si le système est armé.
  - **Flash** – pour un flash : signal continu système armé, signal impulsionnel en cas d'alarme, s'arrête au désarmement.
  - **Thermostat** – mode thermostat. Une sonde de température doit être raccordée à la centrale ; vous indiquez la température à maintenir dans l'onglet **Thermostat**.
  - **Buzzer** – répète les signaux sonores du clavier.
- **Pulse time, s** – la durée d'activation en fonctionnement impulsionnel, 0–9999 s.

- **CMS**, **Prot.** – l'activation et la désactivation de la sortie sont signalées au centre de télésurveillance, ou au cloud Protegus.

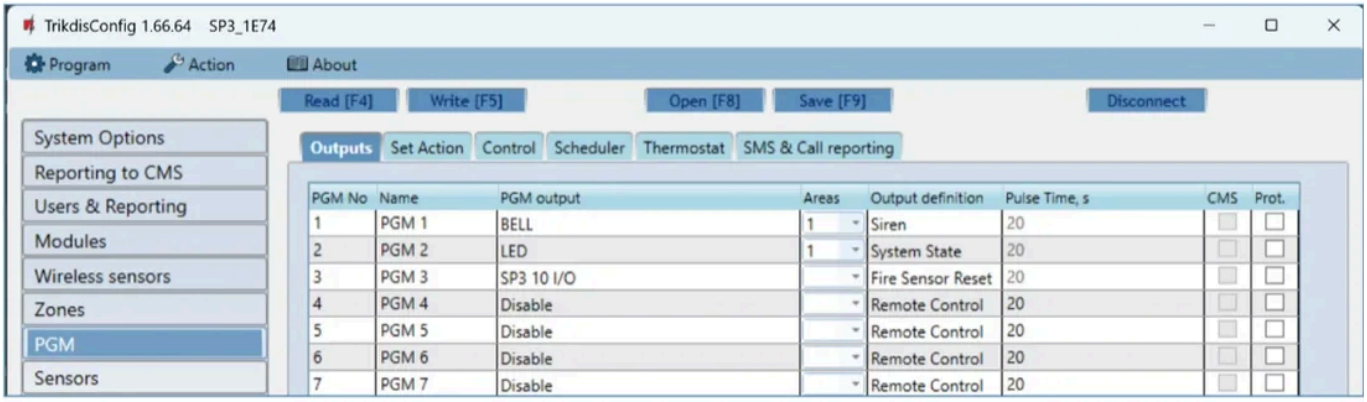


Figure 79. PGM → Outputs : la définition et la durée d'impulsion des sorties.

Onglet **Set Action** – ce qui commande la sortie :

- **ID** – le numéro de la ligne.
- **Enable** – activation de la règle.
- **PGM No.** – la sortie commandée, actionnée par l'événement décrit dans les colonnes **Factor**, **Factor No.**, **Start when** et **Set value**.
- **Action** – **PGM OFF** (désactive), **PGM ON** (active), **Pulse OFF** (activée au repos, désactivée pendant la durée **Pulse time**), **Pulse ON** (désactivée au repos, activée pendant la durée **Pulse time**).
- **Pulse time, s** – 0–9999 s.
- **Factor**, **Factor No.** – l'événement déclencheur et son numéro : **Zone**, **Sensor**, **Jamming**, **Sensor lost**, **iButton**, **Arm**, **Disarm**, **SMS received**, **Zone(follow)**, **Stay**, **Sleep**, **AC lost**, **Low battery**, **Zone tamper**. Une programmation horaire peut aussi être attribuée à la sortie – elle indique quand la sortie doit être activée ; l'onglet **Scheduler** permet d'en créer dix différentes au maximum.
- **Start when** – condition supplémentaire pour l'événement déclencheur.
- **Set value** – la valeur dépendant de la condition : texte du SMS reçu, tension ou température. Si la centrale reconnaît cette valeur, elle exécute l'opération choisie dans la colonne **Action**. Pour les SMS, vous séparez le mot-clé qui commande la sortie du reste du message reçu par des signes `%` : `%texte%` – le message contient le texte (par exemple `%hoUSe%` : le message contient « hoUSe », comme le message `VacationhoUSe25864`) ; `texte%` – le message commence par ce texte (par exemple `hoUSe%` : le message commence par « hoUSe », comme `hoUSeddss`) ; `%texte` – le message se termine par ce texte (par exemple `%hoUSe` : le message se termine par « hoUSe », comme `1144hoUSe`). Le texte est sensible à la casse.

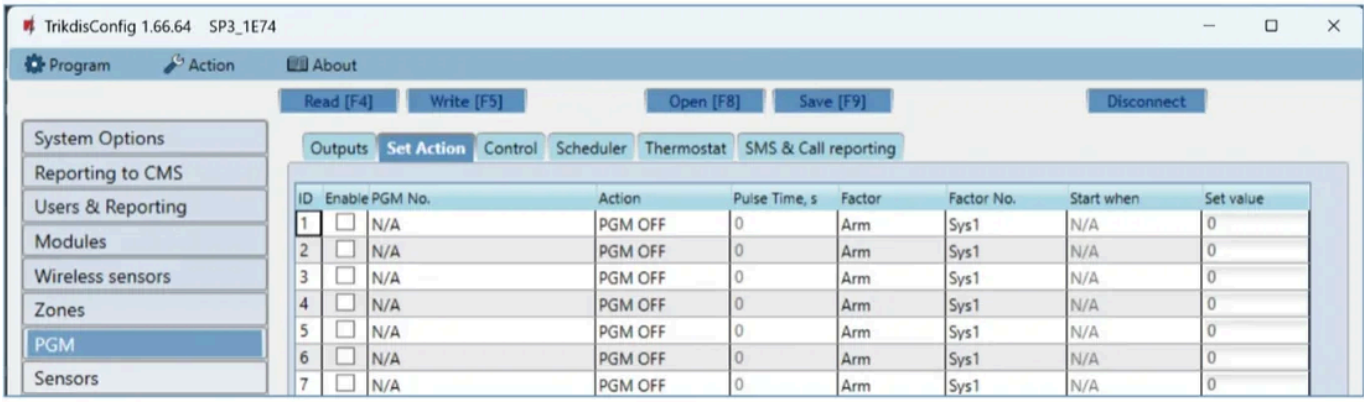


Figure 80. PGM → Set Action : sorties commandées par un événement, un SMS ou une valeur.

Onglet **Control** :

- Groupe **Entry/Exit control** : **Reader** – les lecteurs raccordables (iButton, Wiegand 1 sur la borne **G/Y**, Wiegand 2 sur la borne **IO**) ; **En** – le lecteur peut commander une sortie ; **Code** – l'opération peut aussi être exécutée avec un code utilisateur (commande de la sortie PGM ou de la centrale) ; **PGM** – la sortie commandée (doit être en mode **Remote control**) ; **PGM mode** – **Pulse** ou **Level** ; **Area action** – ce qui doit arriver à l'état d'armement du système lorsqu'une clé ou une carte est présentée au lecteur.
- Groupe **Paradox keypad control** : **Utility key** – en maintenant la touche auxiliaire du clavier pendant 3 secondes, la sortie commute : pendant la durée de l'impulsion (**Pulse**) ou en basculant (**Level**).

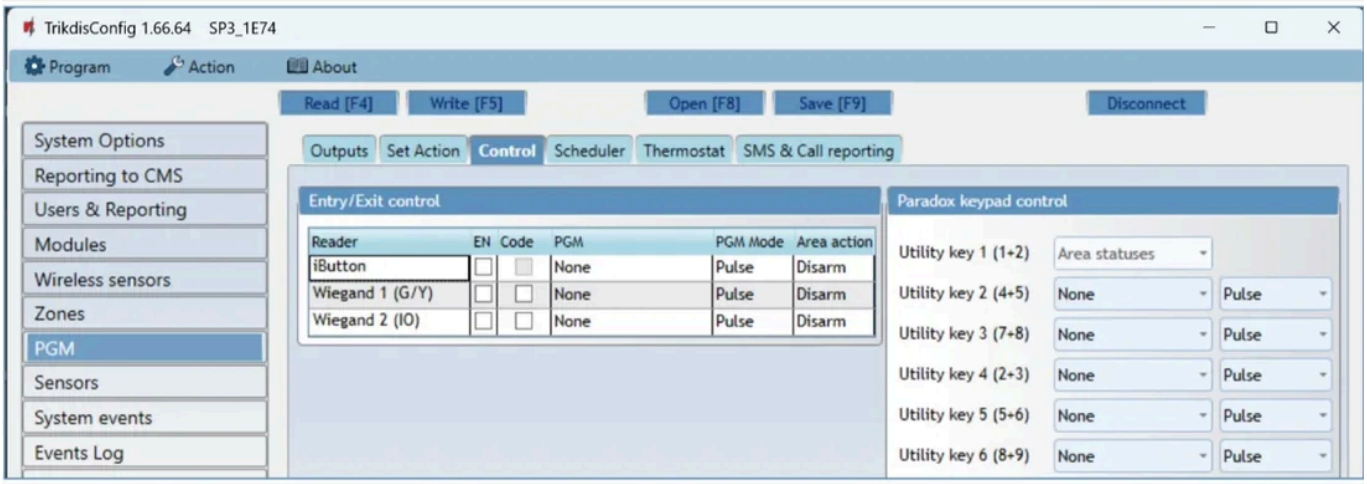


Figure 81. PGM → Control : commande des sorties par les lecteurs et les touches des claviers Paradox.

Onglet **Scheduler** – **ID**, **Enable**, **Start time** (activation), **Stop time** (désactivation), **Mon – Sun** (jours).

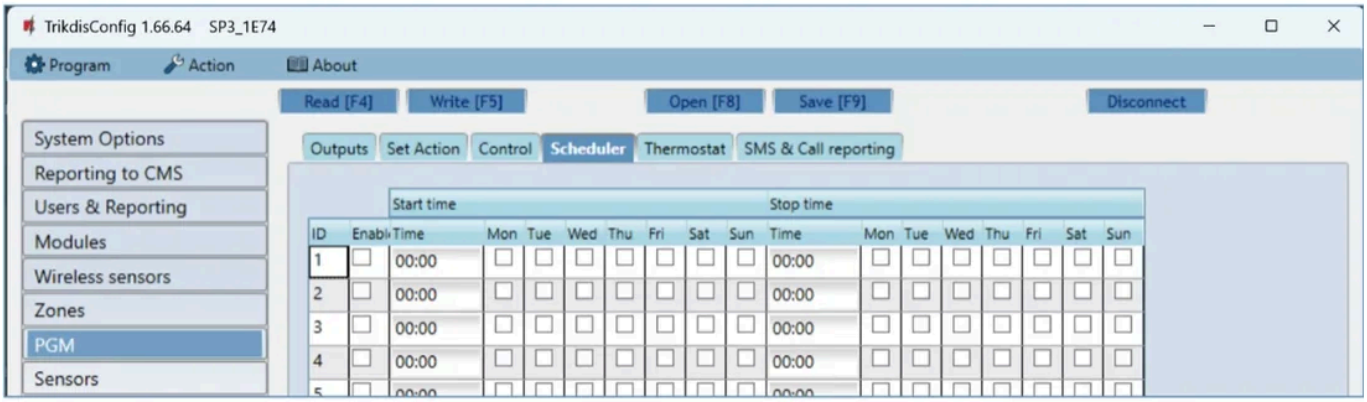


Figure 82. PGM → Scheduler : la programmation horaire des sorties, dix programmes au maximum.

Onglet **Thermostat** – **ID** ; **PGM No.** (la sortie commandée) ; **Action** (chauffage ou refroidissement) ; **Active** (le thermostat fonctionne avec la sonde sélectionnée) ; **Sensor No** (la sonde de température) ; **Temperature** (la température à maintenir).

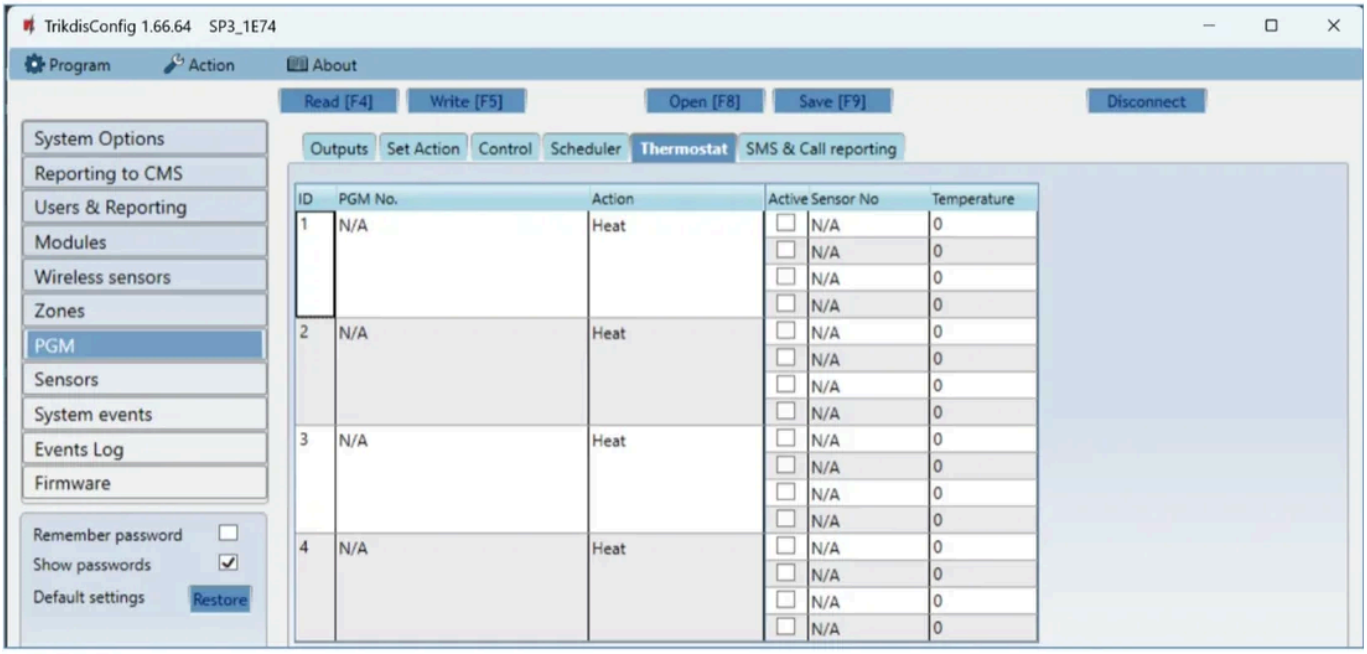


Figure 83. PGM → Thermostat : sortie pour la régulation de température.

Onglet **SMS & Call reporting** – il n'apparaît que s'il existe un numéro de téléphone utilisateur, et ne peut être réglé que pour les huit premiers utilisateurs. **PGM** – le numéro de la sortie et le type d'événement (**Event** – activation, **Restore** – désactivation) ; **User / SMS and Call** – qui reçoit un SMS et/ou un appel.

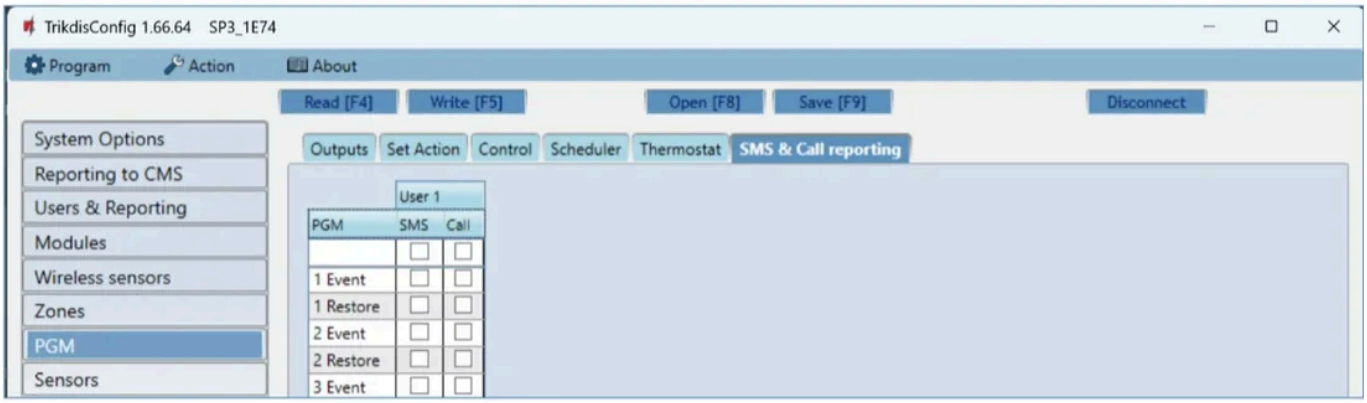


Figure 84. PGM → SMS & Call reporting : notification de la commutation des sorties.

6.9 Sensors

- **ID** – le numéro de la sonde de température.
- **Module type** – la sonde associée à l'identifiant.
- **Serial No.** – le numéro de série de la sonde raccordée à la centrale.
- **Sensor name** – le nom de la sonde.
- **Max** – au-dessus de cette température, un événement est généré si **High** est coché.
- **Min** – en dessous de cette température, un événement est généré si **Low** est coché.
- **Delay, min** – l'événement n'est envoyé que si le dépassement de la valeur limite persiste pendant ce nombre de minutes.
- **Sensor type** – **Dallas 1-Wire** : huit sondes au maximum, reconnues automatiquement ; **Humidity & Temperature (AM23xx series)** : une sonde d'humidité et de température AM2301, à sélectionner manuellement dans la colonne **Module type**.

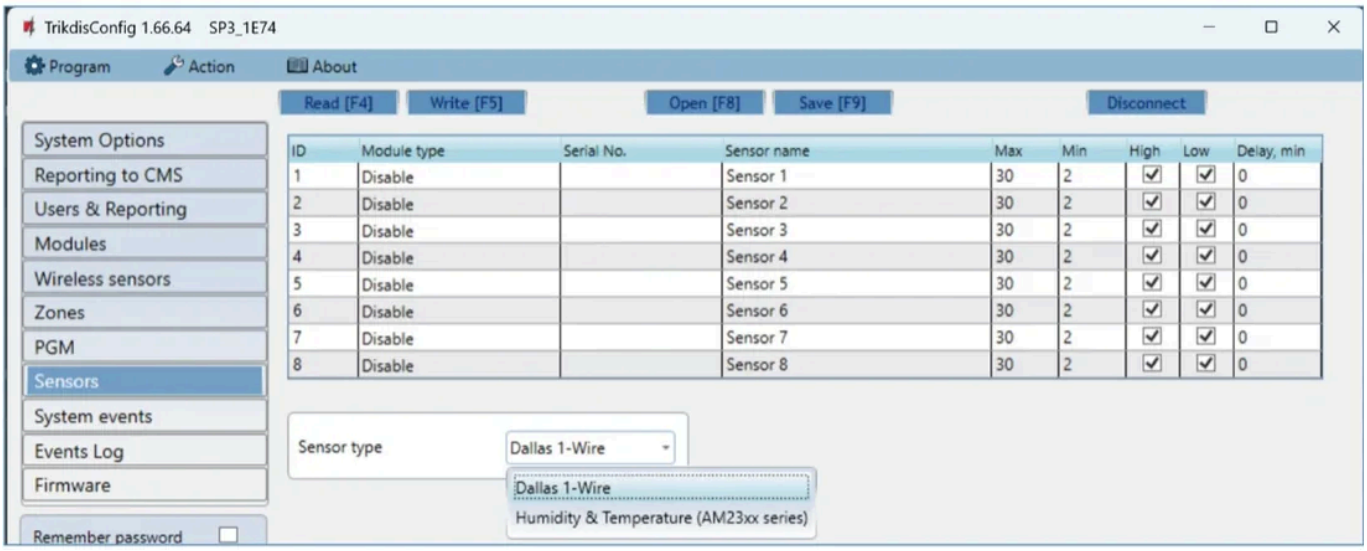


Figure 85. La fenêtre **Sensors** : valeurs limites des sondes de température. La colonne des numéros de série a été laissée vide sur la figure.

6.10 System events

Onglet **Events** :

- **ID** – le numéro de l'événement.
- **Event name** – le nom de l'événement.
- **Enable** – surveillance et rapport de l'événement.
- **CMS**, **Prot.** – rapport au centre de télésurveillance, ou au cloud Protegus.
- **CID Code** – le code Contact ID de l'événement.
- **SMS event text**, **SMS restore text** – le texte SMS de l'événement et du rétablissement.

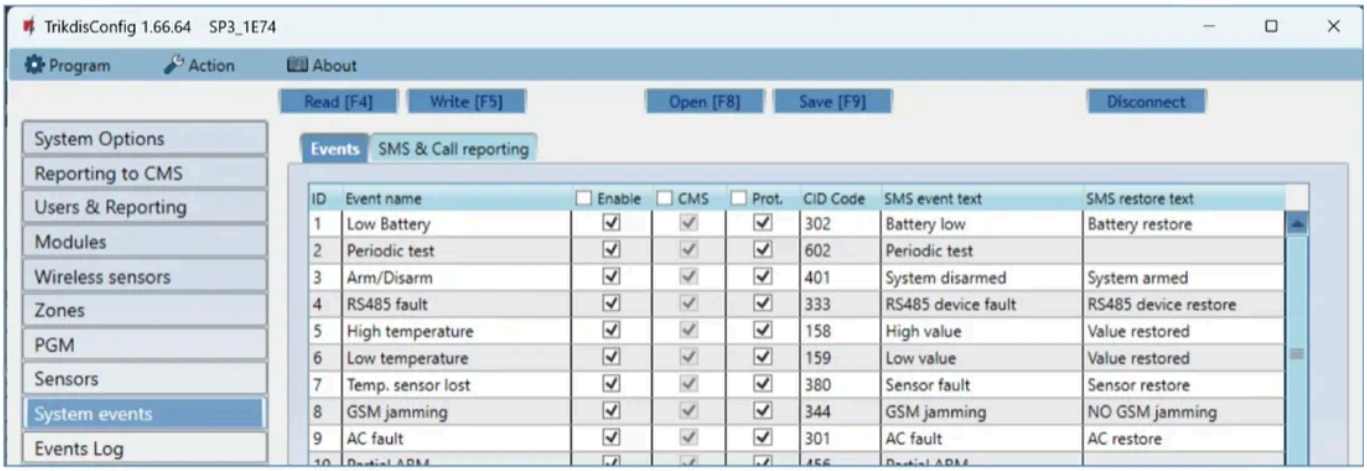


Figure 86. System events → **Events** : code, destination et texte SMS des événements système.

Onglet **SMS & Call reporting** – il n'apparaît qu'avec un numéro de téléphone utilisateur. **ID** – le numéro et le type de l'événement (**Event**, **Restore**) ; **Event SMS text** – le texte du SMS ; **User / SMS and Call** – qui reçoit un SMS et/ou un appel.

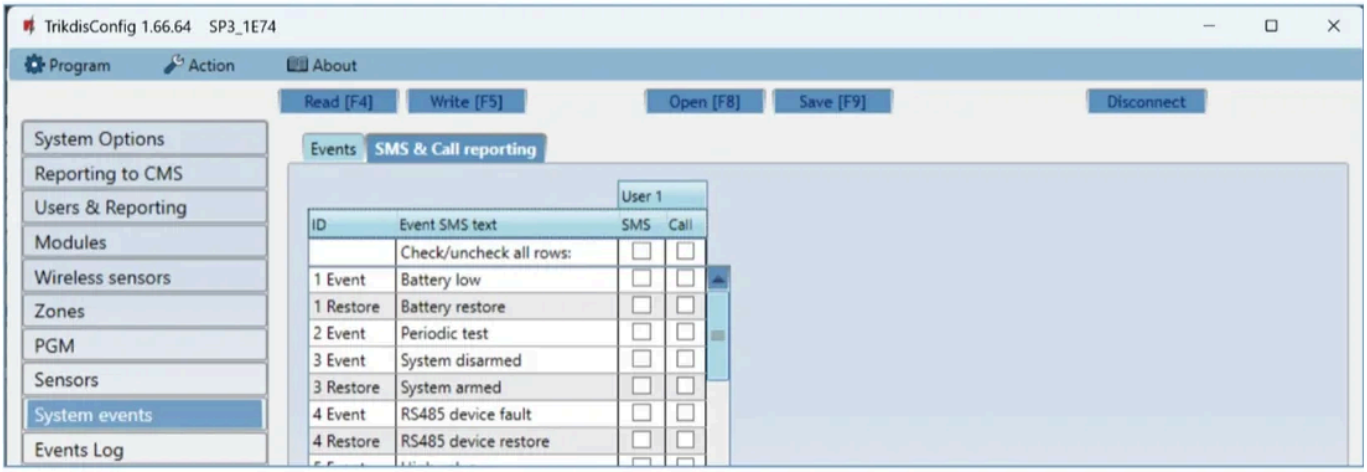


Figure 87. System events → SMS & Call reporting : notification des événements système.

6.11 Events log

- **Read Log** – lecture du journal des événements depuis la mémoire de la centrale.
- **Clear Log** – effacement du journal.
- Les colonnes du tableau : **Event No.**, **Time**, code **CID**, **Event definition**. Le journal affiche 1000 événements au maximum.

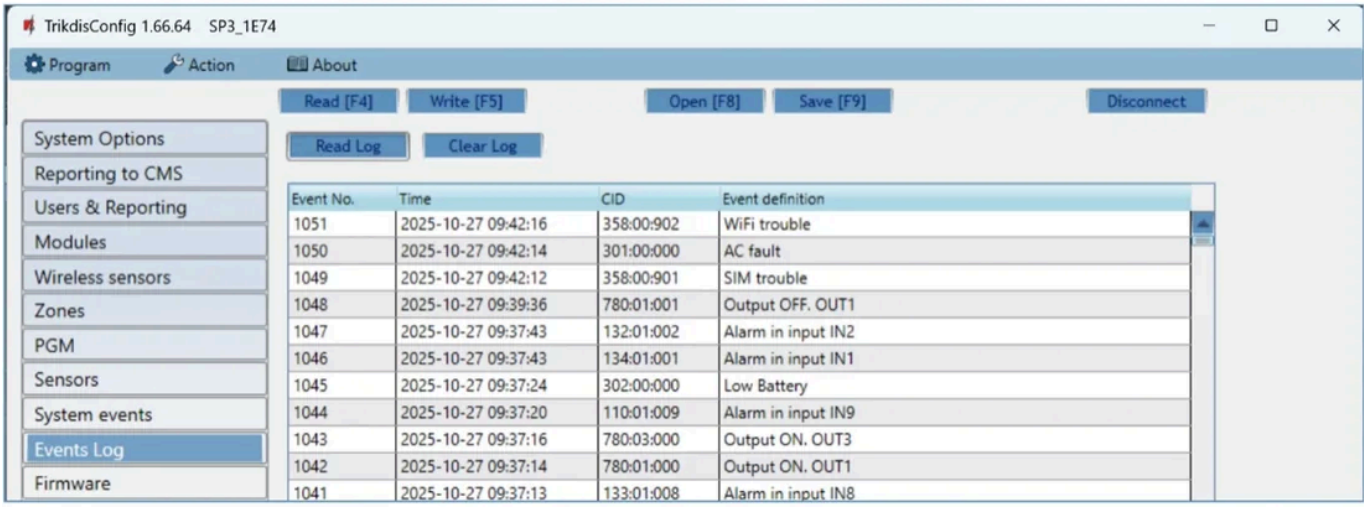


Figure 88. La fenêtre **Events log** : les 1000 derniers événements de la centrale.

Dépannage à partir du journal

En cas d'alarme contestée, lisez d'abord le journal : on y voit quelle zone a signalé, quand et avec quel code, et si le rapport a été envoyé.

6.12 Restauration des réglages d'usine

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

Avec le code installateur, ce n'est possible que si l'administrateur ne l'a pas interdit dans l'onglet **System Options → Access** (6.2.6).

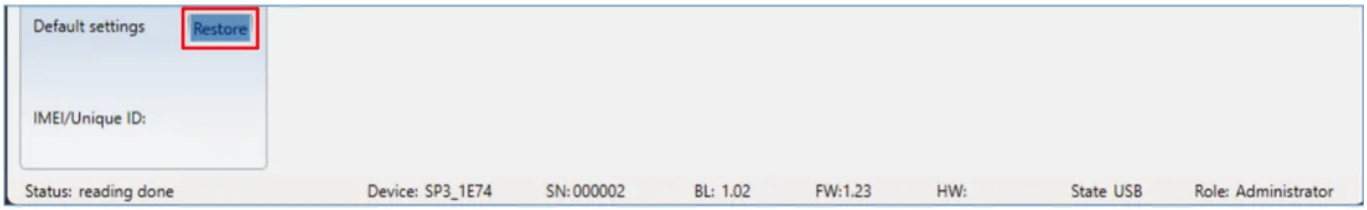


Figure 89. Le bouton **Restore** du groupe **Default settings**, en bas à gauche, restaure les réglages d'usine.

Après la restauration

Les codes reprennent leur valeur d'usine (6.2.6), le PIN de la SIM, l'APN, les données WiFi, les utilisateurs et les zones sont effacés. Si vous avez enregistré auparavant le réglage dans un fichier (**Save [F9]**), vous pouvez le recharger avec les boutons **Open [F8]** et **Write [F5]**.

7. Programmation à distance

TrikdisConfig accède à la « FLEXi » SP3 non seulement par câble USB, mais aussi **à distance, via le cloud Protegus** : vous pouvez modifier les réglages d'une centrale déjà installée, lire le journal des événements, et même mettre à jour le firmware sans vous rendre sur place.

Conditions de l'accès à distance :

1. La centrale doit être sous tension et disposer d'une connexion réseau : la LED **PWR** clignote en vert ; sur le réseau mobile, la LED **NET** est allumée en vert ; en Wi-Fi, la LED **MOD**, en Ethernet, la LED **ETH** est allumée en vert (section 1.6). Sur une version avec modem, la carte SIM est active, et la demande de code PIN est désactivée ou le PIN est saisi.
2. Le **cloud Protegus** doit être activé – réglez-le dans la fenêtre **Users & Reporting** lors de la première mise en service par USB (section 6.4).
3. Vous devez connaître l'**identifiant unique** de la centrale (**IMEI / Unique ID** – lisible sur l'étiquette de la carte et du coffret, ainsi que dans la barre d'état de TrikdisConfig) et le code administrateur ou installateur.

Étapes :

1. Lancez le logiciel TrikdisConfig.
2. Dans la partie **Remote access**, saisissez l'identifiant unique de la centrale dans le champ **Unique ID**.
3. Si vous le souhaitez, donnez un nom au système dans le champ **System name** – le programme 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]**, et saisissez le code administrateur ou installateur. Avec la case **Remember password**, le programme le mémorise.
6. Effectuez les modifications, puis envoyez-les à la centrale avec le bouton **Write [F5]**.

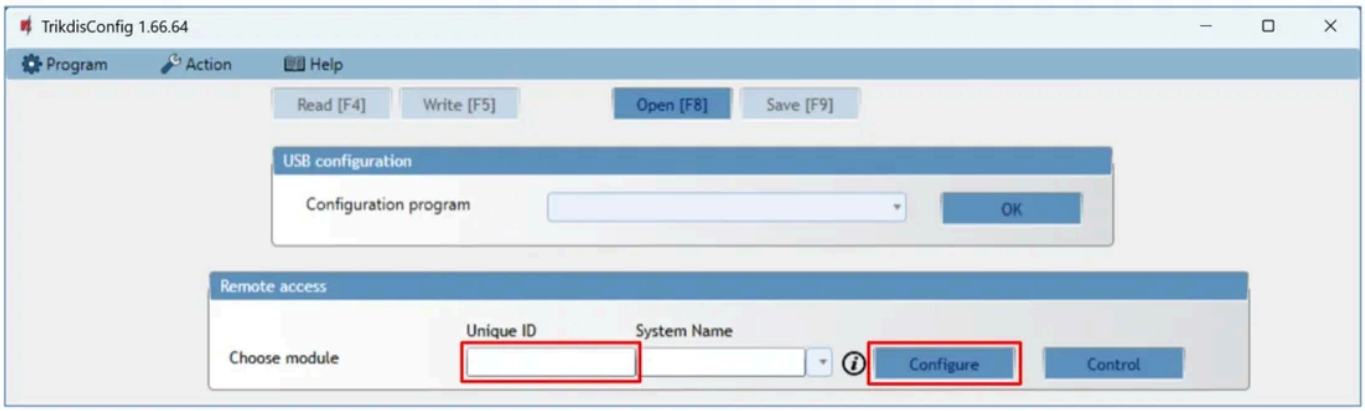


Figure 90. TrikdisConfig – Remote access : le champ Unique ID, System name et le bouton Configure.

La programmation à distance peut aussi être lancée depuis l'application Protegus 2 avec le mot de passe installateur ; pour les réglages détaillés, TrikdisConfig est toutefois nécessaire. Sur le réseau mobile, la connexion à distance consomme des données – lors d'une mise à jour du firmware, même plusieurs mégaoctets.

8. Vérification du fonctionnement du système

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

1. **Regardez les LED.** La LED **PWR** doit clignoter en vert sans clignotements rouges, la LED réseau (**NET**, **MOD** ou **ETH**) doit être allumée en vert, la LED **DAT** doit s'éteindre une fois les événements envoyés (section 1.6). Si la PWR clignote en rouge, recherchez le défaut selon le chapitre 10.
2. **Déclenchez un événement.** Armez, puis désarmez le système sur le clavier, ou violez une zone système armé, afin de générer une alarme.
3. **Vérifiez la réception.** L'événement doit apparaître dans le logiciel de télésurveillance et/ou dans la liste des événements de l'application Protegus 2 – avec le bon numéro de partition, de zone et d'utilisateur. Dans le journal propre de la centrale (**Events log**, section 6.11), vous pouvez aussi voir si l'événement a été généré et s'il a été envoyé.
4. **Zones une par une.** Violez successivement toutes les zones (ouverture, mouvement, bouton de test du détecteur de fumée, autoprotection), et vérifiez que c'est la bonne zone qui signale sur le clavier et dans Protegus 2.
5. **Sorties.** Commandez les sorties PGM à distance depuis Protegus 2, et vérifiez que l'appareil raccordé (sirène, voyant, relais) se met effectivement en marche.
6. **Armement à distance.** Si le système est aussi commandé à distance, armez-le et désarmez-le aussi depuis l'application Protegus 2, et observez si l'état du clavier suit.
7. **Coupure d'alimentation.** Débranchez l'alimentation secteur : la centrale doit continuer à fonctionner sur la batterie, et l'événement **AC Fault**, puis, après le rétablissement, l'événement **AC Restore** doivent arriver (section 2.2).

En usine, la centrale ne transmet pas au centre de télésurveillance (section 6.3), mais le cloud Protegus est activé en usine. Si le centre de télésurveillance ne reçoit pas d'événement, vérifiez d'abord les réglages **Reporting to CMS** et les 4 ou 5 clignotements de la LED PWR.

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!

Quel fichier choisir ?

Le nom du fichier firmware est **SP3_yxxz_NNNN.fw** (section 1.7). Le chiffre **y** est la version matérielle : seul le fichier correspondant à la version propre de la centrale peut être chargé ; avec une autre version, le programme signale une erreur. Le chiffre **z** est le type de détecteurs sans fil – **4** pour les détecteurs MAXIMUM (RF-LORA) et S8 (RF-S8), **1** pour le Paradox RTX3 –, choisissez-le en fonction de l'installation ; le nombre de zones gérées en dépend aussi (32 ou 64). Les règles de choix sont décrites dans l'article Firmware FLEXi SP3 : comment choisir le bon ?.

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.

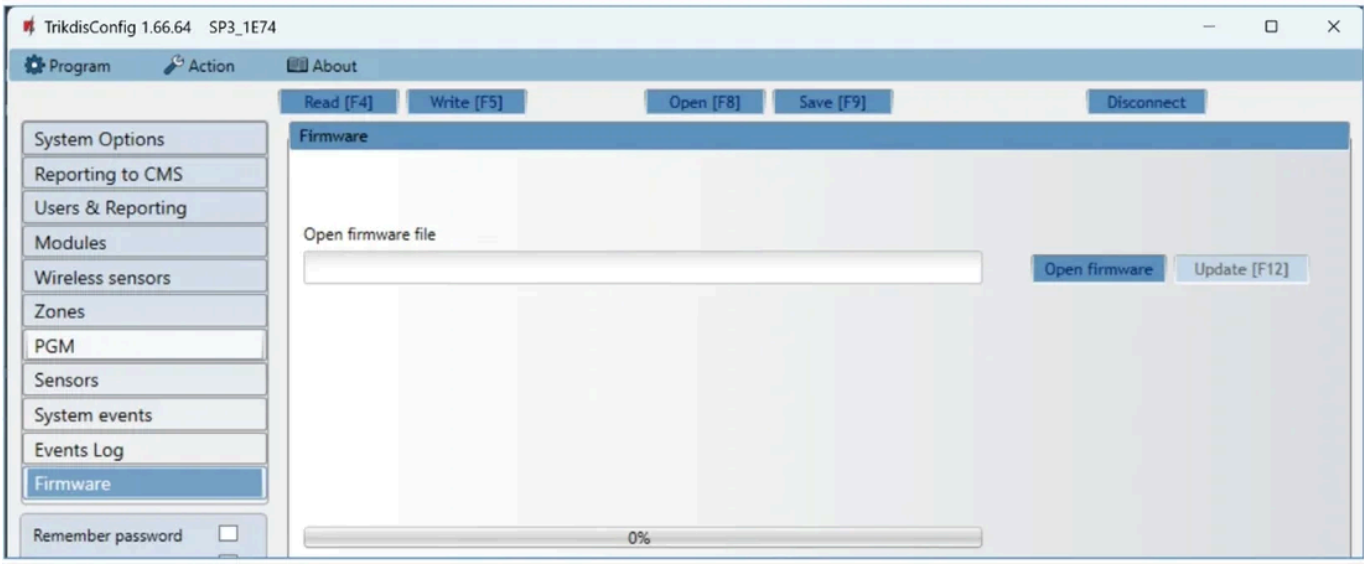


Figure 91. TrikdisConfig – page Firmware : Open firmware et Update [F12].

Après la connexion, TrikdisConfig propose automatiquement la mise à jour du firmware s'il en existe une plus récente ; cela nécessite une connexion Internet. Un antivirus ou un pare-feu peut empêcher le téléchargement automatique du firmware ; dans ce cas, autorisez TrikdisConfig, ou téléchargez le fichier manuellement (après

inscription, sur le site de Trikdis), et ouvrez-le sur la page Firmware. À la fin de la mise à jour, cliquez sur le bouton **Write [F5]**, et ne débranchez le câble USB qu'ensuite.

10. Dépannage et questions fréquentes

Les questions et défauts les plus fréquents, en partant des LED de la carte (la signification des LED se trouve à la section 1.6). Si la réponse renvoie à un chapitre détaillé, vous y trouverez l'emplacement exact du réglage.

La LED PWR clignote en rouge – que signifie le nombre de clignotements ?

En fonctionnement normal, la LED **PWR** clignote en vert. En cas de défaut, elle clignote en rouge, et le nombre de clignotements indique le problème :

Clignotements	Défaut	Où chercher
1	pas de carte SIM	nano-SIM dans le logement, contact (2.4, 6.2)
2	code PIN de la carte SIM erroné	le PIN sur la page **System Options**, ou désactivez la demande de PIN dans un téléphone (6.2)
3	impossible de se connecter au réseau mobile	antenne, niveau du signal (clignotements jaunes de la LED **NET** : 0–5, 3 suffisent), la SIM est-elle active
4	pas de connexion avec le récepteur de télésurveillance sur le canal 1	**Reporting to CMS** : adresse, port, TCP/UDP, clé de chiffrement, identifiant du site (6.3)
5	pas de connexion avec le récepteur de télésurveillance sur le canal 2	la même chose pour le récepteur de secours (6.3)
6	l'horloge interne n'est pas réglée	réglage de l'heure sur la page **System Options** (6.2)
7	tension de l'alimentation de secours insuffisante	batterie et cosses, âge de la batterie, courant de charge (2.2)
8	pas d'alimentation secteur (AC)	alimentation, disjoncteur, bornier de l'alimentation principale (2.1)
9	impossible de se connecter au réseau Wi-Fi	nom du réseau et mot de passe, réseau 2,4 GHz (voir la question suivante)

La centrale ne trouve pas le réseau Wi-Fi

1. Le module Wi-Fi de la « FLEXi » SP3 ne se connecte **qu'aux réseaux 2,4 GHz** (802.11 b/g/n, WPA / WPA2). Il ne voit pas le réseau 5 GHz ; si le routeur utilise un nom commun pour les deux bandes, la bande 2,4 GHz doit être activée.
2. Vérifiez le nom et le mot de passe du réseau sur la page **System Options** (6.2), et que le routeur ne filtre pas les appareils par adresse MAC.
3. La LED **MOD** clignote en vert pendant la connexion, et reste allumée en vert en continu lorsque la connexion est établie.
4. Dans un coffret métallique, le signal Wi-Fi peut être faible : la centrale fonctionne de façon fiable avec une antenne placée à l'extérieur du coffret, un routeur proche du coffret ou un signal plus fort.

Il y a du réseau, mais aucun événement n'arrive dans Protegus 2

1. La LED **DAT** est allumée en jaune s'il y a des messages non envoyés en mémoire : dans ce cas, c'est la connexion qui est en défaut, pas le réglage. Regardez la LED **NET** / **MOD** et les clignotements de la PWR.
2. La connexion vers le cloud Protegus est autorisée en usine ; si elle a été désactivée, réactivez-la avec la case **Enable cloud service** de l'onglet **Users & Reporting** → **Protegus** (6.4.3). L'onglet **Reporting to CMS** → **Settings** permet seulement de régler par quelle voie (SIM, Wi-Fi, LAN) passe le trafic Protegus.
3. Sur la page **System events**, l'envoi de l'événement concerné doit être autorisé (6.10) – ce qui y est interdit, la centrale ne l'envoie par aucun canal.
4. L'appareil est-il associé au compte Protegus 2 (5.1) ? L'ajout d'un nouveau système nécessite l'identifiant unique de l'appareil.

Le centre de télésurveillance ne reçoit pas d'événement

1. La transmission vers la télésurveillance est **désactivée en usine** ; il faut l'activer sur la page **Reporting to CMS** et saisir les données du récepteur (6.3).
2. 4 ou 5 clignotements rouges de la LED PWR indiquent qu'il n'y a pas de connexion avec le récepteur sur le canal 1 ou 2 : adresse, port, protocole (TCP/UDP), clé de chiffrement, identifiant du site.
3. Si la télésurveillance et Protegus 2 sont tous deux configurés, l'événement est d'abord envoyé au récepteur, puis à l'utilisateur – un événement apparaissant dans Protegus 2 ne signifie donc pas que le récepteur l'a aussi reçu.

Quel firmware charger ? Que signifient les chiffres du nom de fichier ?

Le nom du fichier firmware est `SP3_yxxz_NNNN.fw`. Le **premier** chiffre (y) est la version matérielle – 1 : Wi-Fi + 4G, 2 : Wi-Fi, 3 : LAN / LAN + Wi-Fi, 5 : Wi-Fi + 2G, 6 : LAN + 4G – ; il ne peut pas être modifié lors d'une mise à jour, et TrikdisConfig signale si vous avez choisi un fichier qui ne correspond pas au matériel. Le **dernier** chiffre (z) indique le type de récepteur sans fil et donc le nombre de zones : 0 RF-SH (32 zones), 1 Paradox RTX3 (32), 2 Honeywell (64, non utilisé en Europe), 4 détecteurs MAXIMUM (RF-LORA) ou S8 (RF-S8) (64 ; pas nécessaire pour les extensions LORA). Celui-ci peut être changé : un autre récepteur nécessite un firmware avec un autre chiffre z (section 1.7 et chapitre 9). Le nombre à quatre chiffres à la fin est la version ; en règle générale, utilisez la plus élevée.

Combien de zones puis-je avoir, et de quoi cela dépend-il ?

La carte possède **10** bornes IO, chacune pouvant être une zone (entrée) ou une sortie PGM. Avec le doublement de zones (ATZ), deux détecteurs peuvent être raccordés sur une borne, soit **20** zones. Avec des claviers, des extensions de la série iO et LORA, ainsi qu'un récepteur sans fil, le nombre de zones peut être porté à **32 ou 64** – c'est le dernier chiffre du firmware qui en décide (question précédente). Le nombre de partitions est de 8.

Je remplace une ancienne centrale – dois-je changer les résistances des détecteurs ?

Non. Dans la « FLEXi » SP3, la valeur des résistances de fin de ligne est réglable ; les détecteurs existants peuvent donc garder les résistances utilisées avec l'ancienne centrale. Vous réglez le type de zone (NC, NO, EOL, 3EOL, ATZ) et les valeurs de résistance sur la page **Zones** (3.2 et 6.7).

Je voudrais raccorder une charge plus importante (sirène, serrure, portail) à une sortie

En sortie, la borne IO est à collecteur ouvert et supporte **100 mA au maximum** – on ne peut y raccorder directement qu'un voyant ou la bobine d'un petit relais. Pour une charge plus importante, utilisez un relais selon la section 3.8. La sortie **BELL** supporte 1 A, la sortie **AUX** fournit 1 A au maximum sous 12 V DC aux

appareils externes – additionnez la consommation des claviers, extensions et détecteurs à partir du tableau 1.4, et ne la dépassez pas.

Quel clavier puis-je utiliser, et combien ?

La centrale prend en charge les claviers Trikdis FLEXi / SK et les claviers Paradox et Crow énumérés (la liste et les consommations se trouvent à la section 1.4). Sur un bus, **8 claviers au maximum**, et ils doivent être **du même type**. Les claviers LED ne gèrent que les deux premières partitions ; pour davantage de partitions, il faut un clavier LCD. Le clavier FLEXi LCD stocke quatre langues à la fois ; si la langue dont vous avez besoin n'en fait pas partie, il faut mettre à jour le firmware du clavier : https://trikdis.fr/processus-de-mise-a-jour-du-micrologiciel-du-clavier-lcd-flexi .

Je voudrais utiliser un récepteur Paradox RTX3

Pour le RTX3, le dernier chiffre du firmware doit être **1** (`SP3_xxx1_NNNN.fw`) ; vous trouverez le fichier dans le sous-dossier `Firmwares\SP3\RTX3` du dossier d'installation de TrikdisConfig, la procédure de mise à jour au chapitre 9. Après le changement, la page **Wireless** signale si aucun RTX3 n'est encore enregistré. La fréquence du RTX3 et celle des appareils sans fil doivent correspondre (433 ou 868 MHz) – vérifiez-le avant l'achat. Détails : https://trikdis.fr/flexi-sp3-module-d-extension-sans-fil-paradox-rtx3 .

La centrale ne répond pas aux commandes SMS

1. Seules les versions **avec modem** (2G / 4G) peuvent être commandées par SMS et par appel téléphonique ; une centrale uniquement Wi-Fi ou uniquement Ethernet ne le peut pas.
2. La structure du message et la liste des commandes se trouvent à la section 5.3 ; le mot de passe SMS d'usine est `123456`, qu'il est conseillé de changer immédiatement dans le groupe **System Options** → **Access** (6.2).
3. Seul l'utilisateur dont le numéro de téléphone figure dans la liste des utilisateurs de la page **Users & Reporting** peut commander par appel et par SMS (6.4).

Que dois-je absolument régler lors de la première mise en service ?

Avec les réglages d'usine, la plupart des petits et moyens systèmes fonctionnent, mais ne négligez pas ces points : le changement du **code maître** et des codes d'accès installateur / administrateur (6.2, 6.4), le réglage de l'**heure** (6.2), le type et les résistances des zones (6.7), les utilisateurs et leurs numéros de téléphone (6.4), les données du récepteur de télésurveillance, s'il y en a un (6.3), et l'association du système au compte Protegus 2 (5.1). À la fin, effectuez la vérification du chapitre 8.

11. Garantie et 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.

11.1 Garantie et limitation de responsabilité

La centrale d'alarme bénéficie d'une garantie de **24 mois** à compter de l'achat ; pendant cette période, les défauts imputables au fabricant sont réparés gratuitement. La garantie suppose que la centrale soit installée par une personne qualifiée conformément au présent manuel et aux prescriptions relatives aux équipements électriques, et que son exploitation s'y conforme également. Pour une réparation, la centrale doit être envoyée dans l'emballage d'origine, avec une description du défaut constaté ; après l'expiration de la garantie, la maintenance et la réparation peuvent être demandées contre paiement.

La garantie prend fin prématurément si

- la centrale a été réparée ou si une personne non autorisée a tenté de la réparer ;
- elle a été utilisée à une autre fin que celle prévue ;
- elle a été stockée ou installée dans un endroit inadapté (conditions climatiques inadaptées, environnement chimique agressif) ;
- elle a été endommagée mécaniquement ou détériorée intentionnellement ;
- elle a été endommagée par un cas de force majeure (par exemple la foudre).

Le fabricant n'est pas responsable

- du dysfonctionnement de la centrale si elle n'a pas été installée ou utilisée conformément au manuel ;
- du dysfonctionnement de la centrale si sa cause est un défaut ou une interruption de la connexion au réseau mobile ou à Internet, ou un défaut du réseau de l'opérateur ;
- de la limitation, de la suppression ou de l'interruption du service de réseau mobile ou d'Internet, ou de la fourniture d'électricité, ni des dommages matériels ou immatériels qui en résultent ;
- des dommages matériels ou immatériels subis par l'acheteur ou l'utilisateur du fait d'un vol à main armée, d'un cambriolage, d'un vol, d'un incendie ou d'un autre sinistre.

11.2 Consignes de sécurité

- Avant d'utiliser la centrale, lisez le présent manuel. La « FLEXi » SP3 est un équipement électrique : seule une personne qualifiée peut l'installer et en assurer la maintenance, dans le respect du manuel et des prescriptions relatives à l'installation des équipements électriques.
- **Pendant l'installation, la centrale doit être hors tension** ; avant tout raccordement et toute intervention, débranchez-la de l'alimentation : du secteur avec le disjoncteur, de la batterie en retirant les cosses.
- Montez la centrale dans un endroit inaccessible aux personnes non autorisées, à une distance sûre des équipements électroniques sensibles. La carte ne résiste pas aux vibrations, aux chocs mécaniques, à l'humidité ni à un environnement chimique agressif ; elle correspond à la classe d'environnement Class II de la norme EN 50131.
- Le coffret, le transformateur, la batterie et l'appareil de programmation doivent satisfaire aux exigences de sécurité de la norme EN 60950.
- La centrale fonctionne sur le réseau 230 V, 50 Hz via un transformateur abaisseur Class II (16–18 V AC) ou sur une alimentation 16–24 V DC ; l'alimentation de secours nécessite une batterie 12 V d'au moins 7 Ah. La consommation dépend des appareils externes raccordés (section 2.1).
- Un disjoncteur automatique bipolaire, dont les contacts ouverts sont distants d'au moins 3 mm, doit être intégré au circuit d'alimentation ; l'interrupteur doit se trouver à un endroit connu et accessible du technicien qui assure la maintenance de la centrale.
- Les défauts résultant d'une installation ou d'une utilisation inadaptée, ainsi que les modifications et réparations non autorisées par le fabricant, annulent la garantie.

- Respectez les règles locales de traitement des déchets : ne jetez pas l'appareil défectueux, la batterie ni les composants avec les ordures ménagères.

Voir aussi

- Firmware FLEXi SP3 : comment choisir le bon ? – la signification des codes matériel et récepteur, quel firmware pour quel système.
- FLEXi SP3 + module d'extension sans fil Paradox RTX3 – détecteurs sans fil Paradox avec la SP3.
- Émetteur-récepteur RF-S8 et détecteurs S8 – manuel d'installation et d'appairage – les appareils sans fil S8 avec la SP3 : raccordement, firmware, appairage.
- Contrôle d'accès sans fil flexible avec le système GATOR RF-LoRa – les modules RF-LORA et iO-LORA en système.
- La Trikdis FLEXi SP3 a obtenu la certification GRADE 3 – ce que signifie la certification.
- Trikdis FLEXi SP3 – présentation de la centrale d'alarme intelligente – présentation de la centrale, remplacement d'une ancienne centrale.
- Procédure de mise à jour du firmware du clavier FLEXi LCD – les langues du clavier et sa mise à jour.
- Clavier Trikdis FLEXi Keypad SK-LED button – guide utilisateur succinct et clavier SK-LCD button – guide utilisateur succinct – pour l'utilisateur.
- Armement à distance avec un interrupteur à clé depuis l'application Protegus 2 – si la sortie PGM de la SP3 arme une autre centrale.
- Ajout d'une caméra IP à Protegus 2 – image en direct sur l'écran d'accueil de Protegus 2.
- Documentation : docs.trikdis.com – Security control panel “FLEXi” SP3.

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

Produits associés

Panneau d'alarme intelligent Ethernet Trikdis FLEXi SP3

Panneau d'alarme intelligent WiFi Trikdis FLEXi SP3

Panneau d'alarme intelligent WiFi + 4G Trikdis FLEXi SP3

Panneau d'alarme intelligent WiFi + 2G Trikdis FLEXi SP3

Panneau d'alarme intelligent Ethernet + 4G Trikdis FLEXi SP3

Panneau d'alarme intelligent Ethernet + 2 SIM 4G Trikdis FLEXi SP3

Boîte métallique de taille normale avec PSU pour panneau de commande Flexi SP3

Boîte en métal de petite taille avec PSU pour panneau de commande Flexi SP3

Clavier LCD Trikdis Flexi **Clavier LED Trikdis Flexi**

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-flexi-sp3