

WiComm Pro



Modèle : RW332M

FR

Guide d'installation rapide

Rendez-vous sur notre site Internet : www.riscogroup.com

Pour plus d'informations sur les bureaux, les distributeurs et la gamme complète de produits RISCO Group, rendez-vous sur le site riscogroup.com.



Table des matières

1. INTRODUCTION	3
2. INSTALLATION DU SYSTEME	3
2.1 REMARQUES PREALABLES A L'INSTALLATION DE L'UNITE CENTRALE	3
2.2 INSTALLATION DE LA CENTRALE	3
3. ADRESSAGE DES PERIPHERIQUES SANS FIL	7
3.1 ADRESSAGE DU CLAVIER ET SELECTION DE LA LANGUE	7
3.2 OPTIONS D'ADRESSAGE DES PERIPHERIQUES SANS FIL.....	8
Adressage rapide des périphériques sur la centrale	8
Table d'Adressage des Périphériques	9
4. PROGRAMMATION DU SYSTEME	10
4.1 PROGRAMMATION AVEC LE CLAVIER LCD/PANDA	10
4.2 ACCES AU MENU DE PROGRAMMATION	10
4.3 CONFIGURATION MANUELLE DE LA DATE ET DE L'HEURE	10
4.4 MESURE DU BRUIT ET CALIBRAGE DU RECEPTEUR.....	11
4.5 TEST DE COMMUNICATION.....	12
4.6 PROGRAMMATION DES DETECTEURS ET DES ACCESSOIRES.....	13
4.7 PROGRAMMATION ET TEST DES ZONES (DETECTEURS).....	14
4.8 PROGRAMMATION ET TEST DES TELECOMMANDES	15
Paramètres de la télécommande monodirectionnelle à 4 boutons	15
Paramètres de la télécommande bidirectionnelle à 8 boutons.....	16
4.9 PROGRAMMATION DES CLAVIERS	17
4.10 PROGRAMMATION ET TEST DES SIRENES.....	18
4.11 DEFINITION DES CANAUX DE COMMUNICATION	19
Connexion via GSM/GPRS	19
Connexion via IP	19
4.12 DEFINITION DE LA COMMUNICATION AVEC LA TELESURVEILLANCE.....	20
4.13 DEFINITION DES DESTINATIONS SUIVEZ-MOI	20
4.14 DEFINITION DES PARAMETRES SYSTEME	21
4.15 DEFINITION DES UTILISATEURS DU SYSTEME (CODES D'UTILISATEUR)	22
4.16 CONNEXION AU CLOUD	23
Étape 1 : activation de la communication Cloud.....	23
Étape 2 : définition de la communication GPRS ou IP.....	23
Étape 3 : définition des paramètres Cloud pour IP ou GSM	23
4.17 CONFIGURATION DU PIR CAM SANS FIL	24
5. TEST DU SYSTEME	25
6. CONSEILS AU CLIENT	26
7. CARACTERISTIQUES TECHNIQUES	27
Déclaration de conformité	28



1. Introduction

Ce guide d'installation rapide décrit les principales étapes d'installation et de programmation du système WiComm Pro à l'aide du clavier sans fil Panda (LCD + lecteur de proximité).

Le système WiComm Pro permet l'utilisation d'applications Web et Smartphone basées sur le cloud, ainsi que des fonctions de sécurité sans fil avancées. Le système WiComm Pro prend en charge les modules de communication multsockets IP et 2G/3G, qui fournissent plusieurs canaux de communication simultanés pour la communication directe et la communication via le Cloud.

Pour connaître les procédures d'installation des détecteurs et des accessoires, reportez-vous aux instructions livrées avec les appareils correspondants.

2. Installation du système

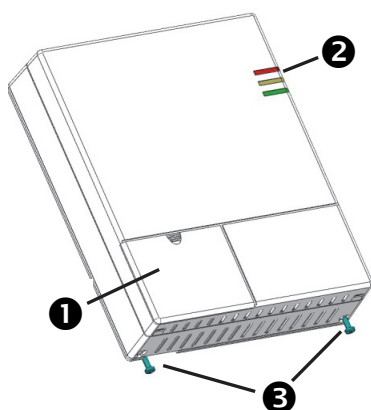
2.1 Remarques préalables à l'installation de l'unité centrale

Pour assurer un fonctionnement optimal du système, respectez les points suivants :

- Installez l'unité centrale au centre des appareils sans fil.
- Installez l'unité centrale dans un endroit avec une bonne réception GSM.
- Placez-la dans un endroit non visible depuis l'extérieur des locaux protégés et inaccessible aux personnes ne devant pas l'utiliser (par exemple, les jeunes enfants).
- Placez-la à proximité d'une prise électrique 230 V CA.
- Veillez à ce qu'elle ait accès à une connexion réseau en cas d'utilisation de la communication IP.
- Installez-la dans un endroit où l'alarme est audible lorsque le système est armé.
- Placez-la à l'écart des sources de chaleur directe, des interférences électriques et des objets métalliques volumineux susceptibles de perturber la réception.

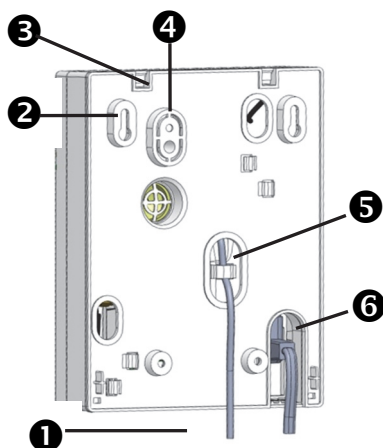
2.2 Installation de la centrale

1. Retirez le support de montage (couvercle arrière de la centrale) ; pour cela, retirez les deux vis de blocage à la base de l'unité, puis soulevez l'unité de façon à la décrocher du support de montage :

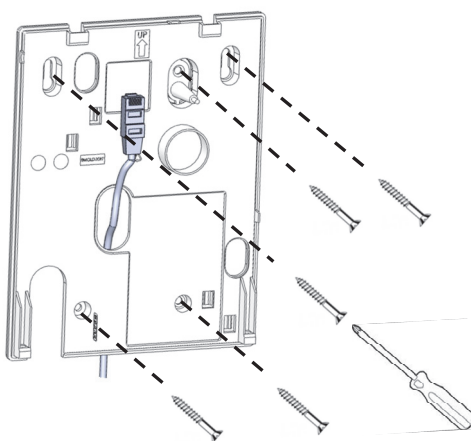


1	Couvercle d'accès avant
2	Voyants
3	Vis de blocage (2)

2. Utilisez le support de montage comme gabarit pour marquer les cinq trous sur le mur (quatre trous pour le montage et un trou pour l'autoprotection arrière), puis percez les trous et installez les chevilles. Reportez-vous à la page 4.



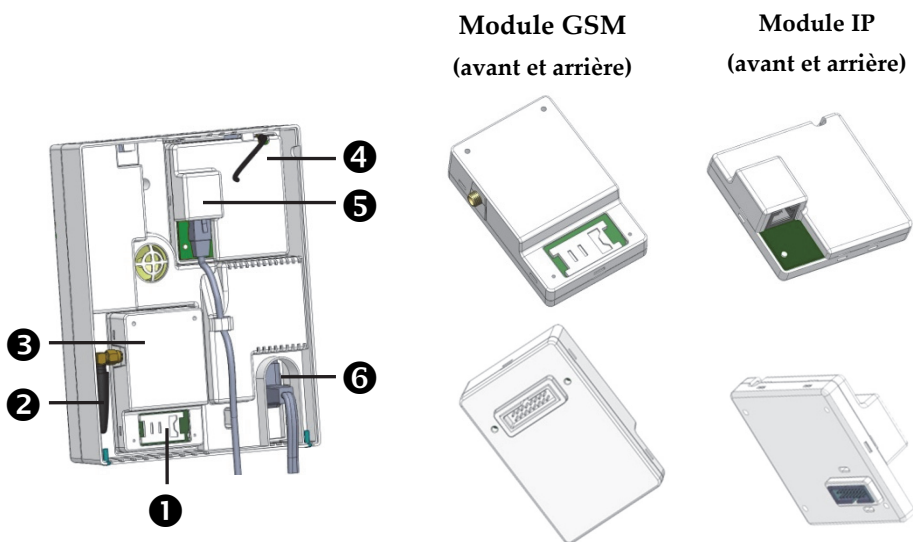
Support de montage – face
arrière



Support de montage – face avant



❶	Emplacements des vis de montage inférieures (2)
❷	Emplacements des vis de montage supérieures (2)
❸	Rainures pour fixation de l'unité principale (2)
❹	Emplacement de la vis d'autoprotection arrière
❺	Passer-fils pour le câble réseau (câble acheminé via le crochet illustré)
❻	Ouverture pour insérer le câble d'alimentation CA. (le câble est installé à l'arrière de la centrale uniquement après avoir correctement fixé le support de montage au mur)



❶	Support de carte SIM sur le module GSM
❷	Antenne pour module GSM (antenne interne installée illustrée)
❸	Module GSM
❹	Module IP
❺	Connecteur du câble réseau sur le module IP (câble connecté illustré)
❻	Câble d'alimentation CA. (câble installé depuis l'arrière de la centrale illustré)



3. Installez le module de communication IP dans son emplacement en veillant à insérer correctement son connecteur dans la prise correspondante.
4. Vérifiez que le câble réseau est inséré dans le passe-fils sur le support de montage (et qu'il est accroché au crochet de fixation). Branchez ensuite le câble réseau au connecteur correspondant sur le module (reportez-vous à l'illustration page 5).
5. Insérez la carte SIM dans son support.
6. Vissez l'antenne dans son connecteur sur le module GSM.
7. Installez le module GSM dans son emplacement en veillant à insérer correctement son connecteur dans la prise correspondante.

NOTE : ne mettez pas sous tension la centrale pour l'instant.

8. Faites passer le câble d'alimentation dans l'ouverture du boîtier (couvercle arrière), puis insérez la fiche dans la prise (reportez-vous à l'illustration page 5).

NOTE : la batterie de secours met 24 heures à se charger.

9. Fixez la centrale au support de montage en insérant les deux onglets en plastique (situés sur le dessus de la centrale) dans les rainures respectives (situées sur le dessus du support de montage), puis appuyez pour fermer le boîtier.
10. Installez les deux vis de blocage dans la partie inférieure de la centrale.
11. Branchez la centrale à l'alimentation secteur.



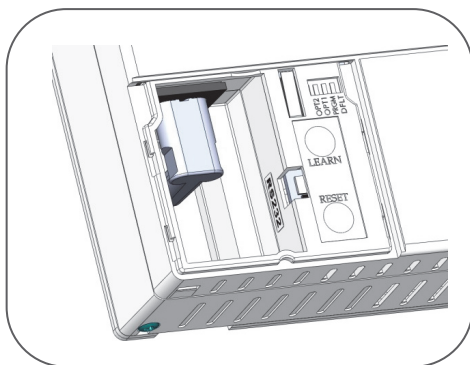
3. Adressage des Périphériques sans fil

3.1 Adressage du Clavier et Sélection de la Langue

Sur les systèmes nouvellement installés, vous devez commencer par adresser le clavier LCD sans fil bidirectionnel au système (c'est-à-dire l'enregistrer sur le système), puis définir une langue par défaut.

➤ **Pour adresser rapidement un clavier et définir la langue du système :**

1. Une fois la centrale sous tension, appuyez sur la touche **LEARN** de la centrale pendant environ 5 secondes ; les trois LEDs s'allument l'une après l'autre, indiquant que la centrale est en mode Adressage.



2. Appuyez simultanément sur  et  pendant au moins 2 secondes ; le clavier émet un signal sonore s'il est adressé.
3. Dans le menu de sélection de la langue qui s'affiche, sélectionnez la langue du système (les paramètres par défaut seront aussi définis selon la langue), puis appuyez sur  pour valider.

NOTE : si le clavier passe en mode veille avant que vous n'ayez terminé la sélection de la langue, reprenez la sélection de la langue du système sur le clavier en appuyant simultanément sur les touches * et 9 (ou  et 9).



3.2 Options d'Adressage des Périphériques sans fil

Tous les périphériques sans fil (détecteurs et accessoires) doivent être adressés au système. Vous pouvez pour cela utiliser :

- **La centrale** : effectuez l'adressage rapide de tous les accessoires par l'envoi d'un signal RF de chaque accessoire sur la centrale (voir procédure ci-dessous).
- **Le clavier LCD** : utilisez l'une des méthodes suivantes.

Adressage automatique des périphériques (séquentiellement) : vous pouvez effectuer cette méthode par "Apprentissage RF", ou en entrant le code de 11 chiffres unique de chaque accessoire (numéro de série) dans le système. Reportez-vous au manuel d'installation complet.

Sélection manuelle d'un numéro de périphérique spécifique pour l'adressage de l'accessoire : utilisez la méthode « Allocation Zone ». Reportez-vous au manuel d'installation complet.

- **Le logiciel de configuration** : reportez-vous à la documentation du logiciel de configuration pour plus d'informations.

NOTE : pour supprimer des adressages de périphériques (pour les périphériques qui ne sont plus utilisés sur le système), reportez-vous au manuel d'installation complet.

Adressage rapide des périphériques sur la centrale

Vous pouvez adresser rapidement tous les périphériques système sur la centrale.

NOTE : pour un adressage rapide via la centrale, l'option système "Apprentissage Rapide" doit être activée.

➤ **Pour adresser rapidement tous les périphériques sans fil sur la centrale :**

1. Vérifiez que chaque périphérique est doté de piles.
2. Appuyez sur la touche **LEARN** de la centrale pendant 5 secondes ; les trois LEDs s'allument l'une après l'autre, indiquant que la centrale est en mode Adressage.
3. Envoyez une transmission d'adressage à la centrale depuis chaque périphérique en suivant les instructions de la *Table d'Adressage des Périphériques*, page 9. Si un périphérique ne figure pas dans le tableau, reportez-vous aux instructions livrées avec le périphérique.

NOTE : il est recommandé de noter la description, le numéro de zone et l'emplacement d'installation de chaque périphérique adressé pour utilisation ultérieure.



Table d'Adressage des Périphériques

Périphérique sans fil	Procédure d'Adressage
Clavier LCD bidirectionnel	Appuyez simultanément sur  et  pendant au moins 2 secondes.
Clavier Panda bidirectionnel	Appuyez simultanément sur  et  pendant au moins 2 secondes.
Clavier Slim bidirectionnel	Appuyez simultanément sur  et  pendant au moins 2 secondes.
Détecteurs IRP • IRP / IRP-Pet • PIR Cam / PIR Cam-Pet	Appuyez sur l'interrupteur d'autoprotection pendant 3 secondes.
Détecteur rideau	Après avoir inséré la pile, fermez le support et attendez 3 secondes.
Contact magnétique monodirectionnel	Appuyez sur l'interrupteur d'autoprotection pendant 3 secondes.
Contact magnétique bidirectionnel	Appuyez sur l'interrupteur d'autoprotection pendant 3 secondes. NOTE: Après programmation des paramètres de cet accessoire et à la sortie de programmation, appuyez sur l'AP pendant 3 secondes, puis attendre 1 minute pour que la centrale télécharge les paramètres du détecteur
Télécommande bidirectionnelle	Appuyez simultanément sur  et  pendant au moins 2 secondes.
Télécommande monodirectionnelle	Cliquez sur  pendant au moins 2 secondes.
Détecteur de fumée & chaleur bidirectionnel	Appuyez sur l'interrupteur d'autoprotection pendant 3 sec.
Sirène intérieure	Appuyez sur l'interrupteur d'autoprotection pendant 3 sec.
Sirène extérieure	Appuyez sur le bouton de réinitialisation de la sirène (RESET). Dès que la sirène retentit, vous avez 10 secondes pour appuyer pendant 3 secondes au moins sur le contact d'AP.
Télécommande panique 2 boutons	Appuyez sur les deux touches pendant au moins 7 secondes.
Bracelet panique	Appuyez sur la touche pendant au moins 7 secondes.

- Une fois tous les périphériques associés, appuyez brièvement sur la touche LEARN pour quitter le mode Adressage ; les LEDs cessent de clignoter.



4. Programmation du système

4.1 Programmation avec le clavier LCD/Panda

Cette section vous explique comment programmer le système à l'aide du clavier LCD sans fil bidirectionnel. Vous pouvez également programmer le système WiComm Pro via le logiciel de configuration (reportez-vous à la documentation du logiciel et au manuel d'installation complet).

Les touches suivantes sont couramment utilisées lors de la programmation (les touches illustrées sont celles du clavier LCD Panda bidirectionnel sans fil avec proximité) :

Touche	Description
	Pour réveiller le clavier, revenir au niveau précédent, quitter les menus, ignorer les modifications (similaire à la touche Echap.)
	Pour sélectionner, valider (comme une touche "Entrer")
	Pour défiler dans une liste ou déplacer le curseur à gauche/droite
	Pour changer la sélection (ex: O/N)
	Pour quitter le mode programmation (suivie par  pour confirmer)

4.2 Accès au menu de programmation

Sur le clavier adressé, appuyez sur , puis entrez le code installateur (par défaut, 0132).

4.3 Configuration manuelle de la date et de l'heure

L'horloge système est automatiquement définie après la configuration de la centrale avec la communication IP ou GSM. Vous pouvez également la configurer manuellement.

➤ Pour configurer manuellement la date et l'heure :

1. Dans le **menu Installateur**, accédez à la section **5) Horloge**, puis appuyez sur  ; le menu **Heure & Date** s'affiche.
2. Appuyez sur , saisissez la date et l'heure, puis appuyez sur .



4.4 Mesure du Bruit et Calibrage du Récepteur

Vous pouvez mesurer ("calibrer") le bruit de fond que la centrale détecte, et définir également ("Voir/Editer") la valeur de seuil acceptable, selon les exigences du client.

Le bruit de fond (Interférence RF) est généralement généré par d'autres dispositifs étrangers au système se situant à proximité du système, une grande quantité de bruit de fond peut interférer avec le système, causant un "brouillage". La communication entre les appareils sans fil de votre système et la centrale doit être plus forte que le bruit de fond détecté ; effectuez par conséquent un test de communication (voir ci-dessous) pour chaque périphérique sans fil afin de vérifier la puissance du signal.

La mesure du niveau de bruit fournit l'indication que la centrale est montée à un bon emplacement, et la définition de la valeur de seuil permet de déterminer la quantité de bruit que votre système peut tolérer avant de générer des événements de brouillage. Plus vous définissez la valeur du seuil basse, "plus sensible" le système sera (il signalera des événements de brouillage plus fréquemment), et plus vous définissez la valeur du seuil haute, "plus tolérant" le système sera (il signalera des événements de brouillage moins fréquemment).

➤ Pour mesurer le bruit de fond détecté par le système :

1. Dans le **menu Installateur**, sélectionnez : **2)Tests Système > 1)Centrale > 1)Niveau Bruit > 2)Calibrer > ** ; le niveau de bruit de fond détecté s'affiche.
NOTE : une valeur faible signifie que peu de bruit de fond est détecté.
2. Une fois la mesure effectuée, si la valeur résultante est trop éloignée du seuil que vous avez défini ou si la valeur est trop élevée (reportez-vous à la rubrique *4.5 Test de Communication* ci-dessous pour une explication des résultats acceptables) et que vous pensez que la source de bruit de fond peut être due à l'emplacement de la centrale, changez la centrale de place.

➤ Pour définir le seuil du niveau de bruit de fond acceptable par le système :

1. Dans le **menu Installateur**, sélectionnez : **2)Tests Système > 1)Centrale > 1)Niveau de bruit > 1)Voir/Modifier > ** .



2. Entrez la valeur du seuil de niveau de bruit souhaitée entre **00 –99**, puis appuyez sur .

NOTE : plus la valeur définie est faible, plus le système est sensible (c'est-à-dire qu'il signale les événements de brouillage plus fréquemment) ; à l'inverse, plus la valeur est élevée, plus le système est tolérant aux interférences. Reportez-vous à la rubrique *4.5 Test de Communication* ci-dessous pour une explication des résultats acceptables.

4.5 Test de Communication

Le test de communication affiche le résultat de la force du signal mesurée après la dernière transmission reçue (détection ou message de supervision). Assurez-vous d'activer le détecteur avant le test.

➤ Pour réaliser un Test de Communication :

1. Activez le périphérique sans fil.
2. Dans le menu Installateur, sélectionnez : **2)Tests Système > 2)Zone [ou 3)Télécommande, 4)Clavier ou 5)Sirène] > 1)Test Comm.** > .
3. Recherchez la zone sur laquelle effectuer le test à l'aide des touches    .
Le résultat apparaît en pourcentage ; il représente la puissance du signal envoyé du périphérique vers la centrale. Les valeurs correctes sont les suivantes :
 - La puissance du signal doit être d'au moins 30 % (une valeur de 30 ou supérieure doit s'afficher).
 - Par ailleurs, le résultat du test de communication doit être supérieur d'au moins 10% au résultat obtenu lors de la mesure du bruit (calibrage du récepteur) réalisée par la centrale. Par exemple, si la mesure du niveau de bruit est de 25%, le résultat du test de Comm. doit être de 35% ou plus.



4.6 Programmation des détecteurs et des accessoires

Programmez le système à l'aide du clavier ou du *logiciel de configuration* (reportez-vous à la documentation du logiciel).

Pour programmer les paramètres de l'ensemble des zones et des périphériques dans le système (détecteurs et accessoires), reportez-vous aux instructions livrées avec chaque périphérique.

NOTE : une fois les paramètres du périphérique programmés, il est recommandé d'effectuer un test de communication pour chaque périphérique sans fil (reportez-vous à la rubrique 4.5 *Test de Communication*, page 12).



4.7 Programmation et test des zones (détecteurs)

Les paramètres disponibles pour chaque zone (détecteur) peuvent varier en fonction du type de zone. Reportez-vous aux instructions fournies avec chaque détecteur.

➤ **Pour programmer les paramètres du détecteur/de la zone :**

1. Dans le **menu Installateur**, sélectionnez : **1)Programmation > 2)Périph. Radio > 2)Modification > 1)Zones > 2)Paramètres**.
2. Sélectionnez la zone souhaitée à l'aide des touches   , puis appuyez sur .
3. Configurez le paramètre de base pour chaque zone en procédant comme suit :
 - 1) Nom :** Donnez un nom significatif pour la zone. Utilisez les touches  et  pour basculer entre tous les caractères disponibles pour chaque touche. Reportez-vous pour cela au tableau suivant.

Touche	Caractères disponibles
1	1 . , ' ? ! " - () @ / : _ + & * #
2	2 a b c A B C
3	3 d e f D E F
4	4 g h i G H I
5	5 j k l J K L
6	6 m n o M N O
7	7 p q r s P Q R S
8	8 t u v T U V
9	9 w x y z W X Y Z
0	0

2) Partition : utilisez la touche 1, 2 ou 3 pour définir l'attribution de partitions (par défaut, 1).

3) Type : utilisez les touches   pour sélectionner le type de zone souhaité dans la liste, puis validez par .

4) Son : utilisez   pour sélectionner le son souhaité.



5) Avancé : En fonction du type de détecteur, inclut le Carillon, la Supervision, l'activation de l'Armement Forcé, et des paramètres supplémentaires pour les détecteurs bidirectionnels.

4. Réalisez un test de communication (reportez-vous à la rubrique 4.5 *Test de Communication*, page 12).

4.8 Programmation et test des télécommandes

Chaque télécommande peut être paramétrée pour effectuer différentes opérations sur le système et contrôler différentes sorties programmables. Jusqu'à 8 télécommandes peuvent être adressées dans le système. Les options de programmation du menu paramètres varient selon le type de télécommande : Monodirectionnelle ou Bidirectionnelle. Après la programmation des paramètres, vous pouvez effectuer un test de communication.

➤ Pour programmer les paramètres de la télécommande au clavier :

1. Dans le menu Installateur, sélectionnez : **1)Programmation > 2)Périp. Radio > 2)Modification > 2)Télécommandes > 1)Paramètres.**
2. Sélectionnez une télécommande, puis appuyez sur  pour la paramétrer.
3. Utilisez les touches    pour parcourir les options suivantes, puis appuyez sur  pour les sélectionner :

Paramètres de la télécommande monodirectionnelle à 4 boutons

- 1) Nom :** Nom significatif de la télécommande (voir tableau pour plus de détails).
- 2) N° de série :** Code unique à 11 chiffres du périphérique.
- 3) Partition :** Attribution partition (dans la plupart des cas 1).
- 4) Touche 1 :** (cadenas fermé) : Armement Total.
- 5) Touche 2 :** (cadenas ouvert) : Désarmement.
- 6) Touche 3 :** (définie par l'utilisateur).
- 7) Touche 4 :** (définie par l'utilisateur).



Paramètres de la télécommande bidirectionnelle à 8 boutons

1) **Nom** : Nom significatif de la télécommande (voir tableau pour plus de détails).

2) **Numéro de série** : Code unique à 11 chiffres du périphérique.

3) **Partition** : Utilisez  pour sélectionner O/N pour les 3 partitions disponibles (utilisez    pour parcourir les partitions 1–3).

4) **Code PIN** : Si nécessaire, définissez un code PIN à 4 chiffres.

5) **Fct. Panique** : Utilisez  pour sélectionner O/N pour définir s'il est possible d'envoyer une alarme panique depuis la télécommande (par défaut: NON).

6), 7), 8) : touches 1 à 3 attribuées à l'installateur (pour les commandes de sorties programmables).

4. Appuyez sur   pour revenir au menu **Télécommandes**, puis sélectionnez **2) Contrôle**.

5. Utilisez  pour sélectionner O/N (puis utilisez    pour parcourir les 3 options disponibles), comme suit :

1) **Arm. Immédiat** : Armement Total temporisé ou non (O: immédiat).

2) **Partiel Immédiat** : Armement Partiel temporisé ou non (O: immédiat).

3) **Désarm. + Code** : Désarmement par télécommande validé ou non par code (N: code inutile).

6. Effectuez un test de communication (reportez-vous à la rubrique 4.5 *Test de communication*, page 12).



4.9 Programmation des claviers

Vous pouvez associer jusqu'à trois claviers au système. Une fois les paramètres d'un clavier programmés, vous pouvez effectuer un test de communication.

➤ **Pour programmer les paramètres du clavier (LCD ou Panda) :**

1. Dans le menu Installateur, sélectionnez : **1)Programmation > 2)Périph. Radio > 2)Modification > 3)Claviers > 1)Paramètres.**

2. Sélectionnez un clavier, puis appuyez sur  pour configurer ses paramètres de base. Utilisez    pour parcourir les options suivantes et  pour les sélectionner :

1) Nom : Nom significatif du clavier (voir tableau pour plus de détails).

2) N° de série : Code unique à 11 chiffres du périphérique.

3) Touche d'Urgence : Permet d'activer (O) ou de désactiver (N) les touches d'urgence.

4) Touches Fonction : Définit la fonction des touches   sur **Alarme panique** ou sur **Désactivé**.

8) Supervision : Utilisez  pour sélectionner O/N.

3. Appuyez sur   pour revenir au menu **Claviers**, puis sélectionnez **2)Contrôle** et accédez à :

- **Réveil RF :** Utilisez  pour sélectionner O/N et indiquer si l'écran LCD du clavier doit s'allumer automatiquement pendant le délai de temporisation d'entrée.

4. Effectuez un test de communication (reportez-vous à la rubrique 4.5 *Test de Communication*, page 12).



4.10 Programmation et test des sirènes

Vous pouvez associer jusqu'à trois sirènes intérieures ou extérieures au système. Une fois les paramètres programmés, vous pouvez effectuer un test de communication.

➤ Pour programmer les paramètres de la sirène :

1. Dans le menu Installateur, sélectionnez **1)Programmation > 2)Périphériques radio > 2)Modification > 4)Sirènes**

2. Sélectionnez une sirène, puis appuyez sur  pour configurer ses paramètres de base. Utilisez    pour parcourir les options suivantes et  pour les sélectionner :

1) Nom : Nom significatif de la sirène (voir tableau pour plus de détails).

2) Supervision : Définit si la sirène est supervisée ou non.

3) Volume : Définit le volume de la sirène lors d'une Alarme, d'une Confirmation d'Arm/Désarm ou d'une Tempo d'Entrée/Sortie.

4) Flash : Définit le fonctionnement du Flash pour les sirènes extérieures.

3. Effectuez un test de communication (reportez-vous à la rubrique 4.5 *Test de Communication*, page 12).



4.11 Définition des canaux de communication

Les menus n'affichent que les modules de communication installés dans la centrale.

➤ Pour définir les canaux de communication :

1. Dans le **menu Installateur**, sélectionnez : **1)Programmation > 4)Communication > 1)Méthode**.
2. Sélectionnez la méthode (IP et/ou GSM) et définissez les paramètres, comme suit :

Connexion via GSM/GPRS

➤ Pour se connecter avec le module GSM :

- a. Dans le **menu Programmation**, sélectionnez : **4)Communication >**

1)Méthode > 2)GSM > utilisez    pour accéder à **2)GPRS >** .

- b. Utilisez    pour sélectionner **1)Code APN, 2)Nom d'utilisateur APN ou 3) Mot de passe APN**.

Par défaut, l'APN est automatiquement configuré selon la carte SIM. Si la carte SIM n'est pas prise en charge, définissez le **code APN** et le **nom d'utilisateur et le mot de passe**, respectivement, conformément aux informations du fournisseur de la carte SIM.

Connexion via IP

- a. Dans le **menu Programmation**, sélectionnez : **4)Communication > 1)Méthode > 3)IP > 1)Config. IP**
- b. Indiquez si l'adresse IP du système est statique ou dynamique. Si elle est dynamique, sélectionnez **O** (le système utilise l'adresse IP fournie par DHCP). Si elle est statique, sélectionnez **N** et définissez tous les autres paramètres dans le menu.



4.12 Définition de la communication avec la télésurveillance

Il est possible d'envoyer des rapports directement au centre de télésurveillance, soit de la centrale vers la baie de réception en direct, soit via le RISCO Cloud. Pour une communication directe entre la centrale et la télésurveillance, vous pouvez définir jusqu'à 3 comptes TLS et plusieurs paramètres associés qui définissent la nature de la communication, les rapports d'événements et la confirmation entre l'utilisateur du système et la télésurveillance.

➤ Pour définir la communication avec le centre de télésurveillance :

1. Utilisez  pour revenir à **1)Système > 2)Paramètres > 3)Communication > Activer TLS** > utilisez  pour sélectionner **O/N** (sélectionnez **O** pour activer cette option) >  .
2. Utilisez  pour accéder à **1)Programmation > 4)Communication > 2)TLS** > sélectionnez et définissez les options correspondantes au centre de télésurveillance sélectionné (1 – 3).

4.13 Définition des destinations Suivez-moi

Le système WiComm Pro peut informer les utilisateurs finaux de différents événements système. Ces rapports peuvent être envoyés par WiComm Pro directement à l'utilisateur par SMS (jusqu'à 16). Il est également possible d'envoyer des rapports par e-mail ou notification Push à partir de l'unité centrale ou via le RISCO Cloud. Si vous utilisez le Cloud, le nombre de rapports est illimité.

➤ Pour définir le rapport Suivez-moi :

- Utilisez  pour accéder à **4) Communication > 4)Suivez-moi > 1)Définir SM > Numéro d'index de la destination SM** (par exemple, Suivez-moi 01) >  > puis sélectionnez et configurez les options suivantes :
- 1) **Type Rapport** : sélectionnez le canal, à savoir **SMS ou E-mail**. (Les événements de rapport par e-mail peuvent être établis directement depuis la centrale ou via le RISCO Cloud).



2) **Événements** : sélectionnez les notifications d'événements qui seront

envoyées. Utilisez  pour sélectionner O/N pour chaque option, puis appuyez sur  pour valider :

- **Alarmes** > Alarme intrusion, Alarme incendie, Alarme urgence, Alarme panique, Alarme autoprotection, Alarme contrainte, Inactivité
- **Arm./Désarm.** > Armement, Désarmement, Contrôle Parental
- **Défauts** > Faux code, batterie centrale faible, batterie SF faible, Brouillage, Perte SF, Coupure secteur, Défaut RTC, Réseau IP
- **GSM** > Défaut GSM, Défaut SIM, Expiration SIM, Crédit SIM
- **Environnement** > Alerte gaz, Alerte inondation, Alerte CO, Température élevée, Température faible, Technique
- **Divers** > Exclusion de zone, Test cyclique, Programmation à distance, Infos de communication

3) **Rétabl. Eve** : sélectionnez les rétablissements d'événements qui seront envoyés (pour les mêmes types d'événements répertoriés ci-dessus, à savoir Alarmes, Défaut, GSM et Environnement).

4) **Ctrl. Distant** : définissez l'opération utilisateur à distance (sur O ou N) exécutée sur le système WiComm Pro :

- Écoute à distance
- Programmation à distance

NOTE : Les destinations Suivez-Moi (n° de téléphone et adresses email) sont définies en dehors du menu de programmation (**Menu Install.** : > 4) **Suivez-Moi**), ou depuis le menu Utilisateur par le Responsable Général.

NOTE : il est possible d'attribuer d'autres destinations e-mail Suivez-moi dans le RISCO Cloud.

4.14 Définition des paramètres système

Il existe un large éventail de paramètres système qui définissent comment le système fonctionne. Ils sont paramétrables dans le menu Système. Tous ces paramètres sont définis avec des valeurs par défaut qui s'appliquent à la plupart des installations. Si vous souhaitez apporter des modifications, naviguer dans le menu pour programmer les paramètres systèmes en conséquence.



4.15 Définition des utilisateurs du système (codes d'utilisateur)

En tant qu'installateur, vous devez programmer les utilisateurs du système. Le propriétaire (Responsable Général) sera par la suite autorisé à reprogrammer tous les codes utilisateur pour personnalisation et confidentialité.

Les codes utilisateurs peuvent être définis depuis l'appli. utilisateur Web ou sur le clavier LCD..

➤ Pour définir les utilisateurs du système via le clavier :

- Utilisez   pour accéder à **1) Programmation > 3) Codes**, puis sélectionnez les options suivantes :

1) Utilisateur : pour chaque utilisateur, sélectionnez un **numéro d'index à 2 chiffres** différent, puis définissez les paramètres suivants :

- Nom** : Entrez une description unique pour identifier l'utilisateur.
- Partition** : Assignez la ou les partitions (1—3) que chaque utilisateur peut utiliser (sauf le responsable général, qui peut utiliser toutes les

partitions). Utilisez    pour parcourir les partitions, puis appuyez sur  pour les activer (O) ou les désactiver.

- Autorité** : Sélectionnez un niveau d'autorité (Utilisateur, Temporaire, Armement seulement, Contrainte, Exclusion)

2) Resp. Général : définissez le code du responsable général (par défaut 4 chiffres)

3) Installateur : définissez le code installateur (par défaut 4 chiffres)



4.16 Connexion au Cloud

Il est possible de configurer le système pour qu'il soit en permanence connecté au RISCO Cloud, un serveur d'application qui gère toutes les communications entre le système, les fournisseurs de services et les utilisateurs des applications Web/Smartphone. RISCO Cloud permet de surveiller et de contrôler le système à distance, d'envoyer des notifications d'événements et d'afficher des clips vidéo en temps réel via des caméras IP VUpoint (pour les centres de télésurveillance et les utilisateurs du système).

Étape 1 : activation de la communication Cloud

Depuis le menu *Installateur*, sélectionnez : **1)Programmation > 1)Système > 2)Paramètres > 3)Communication > Activer Cloud** > sélectionnez **O** à l'aide de



, puis appuyez sur



pour valider.

Étape 2 : définition de la communication GPRS ou IP

Reportez-vous à la rubrique 4.11 *Définition des canaux de communication*, page 19.

Étape 3 : définition des paramètres Cloud pour IP ou GSM

Dans le **menu Programmation**, sélectionnez : **4)Communication > 5)Cloud**, puis définissez les paramètres suivants :

1)Adresse IP : adresse IP du serveur (**www.riscocloud.com**)

2)Port IP : le port du serveur est défini sur **33000**.

3)Mot de passe : mot de passe d'accès au serveur envoyé par votre fournisseur (le cas échéant). Ce mot de passe doit être identique au mot de passe CP défini sur le serveur dans la page de définition de la centrale.

4)Canal : sélectionnez le canal de communication au RISCO Cloud (basé sur la communication IP ou GSM) en fonction des options disponibles.

NOTE : avant la connexion au Cloud, vérifiez que la carte SIM est installée.

5)Contrôles : le système prend en charge l'envoi de rapports via des canaux de communication parallèles (IP, GSM, SMS) en télésurveillance et aux utilisateurs Suivez-moi. Utilisez ce paramètre pour indiquer si la centrale envoie les événements en TLS ou en Suivez-moi parallèlement aux rapports transmis à RISCO Cloud (s'il existe un canal de communication supplémentaire - IP, GSM ou SMS), ou uniquement en secours si la communication Cloud ne fonctionne pas.



4.17 Configuration du PIR Cam sans fil

Les détecteurs IRP avec appareils photos (PIR Cam) apportent un stade de détection avancé en ajoutant les capacités de capture d'images. Vous pouvez adresser jusqu'à huit PIR Cam dans le système WiComm Pro. Pour l'installation physique de chaque PIR Cam, reportez-vous aux instructions du produit.

➤ Pour configurer les PIR Cam :

1. Adressez le PIR Cam comme n'importe quel autre détecteur (reportez-vous aux procédures d'adressage précédentes).
2. Définissez les paramètres du PIR Cam dans l'ordre dans lequel ils apparaissent dans la section **Paramètres de zone avancés**.
3. Définissez la communication entre le système WiComm Pro et le serveur RISCO Cloud (reportez-vous à la rubrique *4.16 Connexion au Cloud*, page 23).
4. Connectez-vous à l'application utilisateur Web (**www.riscocloud.com**), puis accédez à l'écran principal et sélectionnez l'option **Vérif. Visuelle**.
5. Ajustez la vue du PIR Cam en procédant comme suit :
 - a) Sélectionnez le PIR Cam.
 - b) Effectuez une capture d'image depuis le serveur.
 - c) Accédez à l'onglet **Événements**.
 - d) Cliquez sur l'image requise.

Si nécessaire, réglez le PIR Cam et répétez les étapes b à d.



5. Test du système

Avant de quitter le site, il est important de tester l'intégralité du système.

- **[Pour les périphériques adressés]** : dans le **menu Installateur**, sélectionnez **2)Tests Système**, puis effectuez un test de communication et un test de batterie.
- **[Pour la centrale]** : dans le **menu Installateur**, sélectionnez **2)Tests Système > 1)Centrale** pour tester le niveau de bruit, la sirène, le haut-parleur et la batterie, et confirmer la version firmware et le numéro de série de la centrale.
- **[Pour les zones]** : dans le **menu Installateur**, sélectionnez **2)Tests Système > 2)Zone** pour effectuer des tests de communication et de batterie, mais aussi un test de marche durant lequel vous armez le système, puis accédez à la zone protégée en vue de déclencher une alarme sur chaque détecteur.
- **[Pour le signal GSM]** : vous pouvez également tester la puissance du signal GSM (sur une échelle de 0 à 5) dans le **menu Installateur > 2)Tests Système > 6)GSM > 1)Signal**.
- **[Pour le Suivez-Moi]** : vous pouvez effectuer un test pour vérifier que le Suivez-Moi fonctionne.



6. Conseils au Client

Le client a généralement besoin d'aide et de conseils de l'installateur dans les domaines suivants.

- ✓ Recommandez au client de définir un code Responsable Général confidentiel une fois l'installation terminée.
- ✓ Expliquez à l'utilisateur comment définir des codes utilisateur et des destinations Suivez-moi.
- ✓ Dans le cadre de la communication avec le RISCO Cloud, demandez aux clients possédant des smartphones de télécharger l'application iRISCO depuis l'App Store d'Apple ou le Play Store Android afin de vérifier que la connexion entre l'application et le système est établie.
- ✓ Lorsque vous adressez les périphériques système, veillez à noter toutes les informations des zones (type de périphérique, numéro de zone, emplacement) afin de les transmettre au client.
- ✓ Expliquez à l'utilisateur les opérations suivantes exécutées sur les claviers et/ou les télécommandes :
 - Armement total, armement partiel et désarmement
 - Envoi d'une alarme contrainte silencieuse (« Désarmement sous contrainte ») au centre de télésurveillance dans le cas où l'utilisateur doit utiliser le système sous contrainte
 - Activation d'une alarme panique
 - Utilisation des SMS pour les commandes à distance



7. Caractéristiques Techniques

Configuration	
Modes (modules) de communication	GPRS/GSM (2G), GSM (3G), IP
Zones sans fil	32
Fréquences sans fil	868 MHz, 433 MHz
Utilisateurs du système (codes utilisateur)	32 (dont 1 code Installateur, 1 code sous-installateur et 1 code Responsable Général)
Destinations Suivez-moi	16
Options de programmation de la centrale	• Clavier (localement) • Logiciel de configuration (localement, à distance)
Partitions	3
Comptes de centre de télésurveillance	3
Journal d'événements	1 000 entrées
PIR Cam	8
Sirènes (intérieures/extérieures)	3
Claviers	3
Télécommandes	8
SMS pour les commandes à distance	Oui
Centrale (RW332M)	
Alimentation électrique	230 V CA, 50/60 Hz 0.6 A max.
Câble d'alimentation CA	• 14 mm de diamètre, conduit de 16 mm • Conforme à la norme de sécurité IEC 60227
Consommation (centrale)	166 mA en veille
Batterie de secours (dans la centrale)	• Batterie rechargeable au lithium polymère de 2 350 mAh. • Durée de recharge max. à 80 % : 34 heures • Signal de faible tension à 7.2 V CC
Plage d'humidité	Humidité relative moyenne de 75 %
Température de fonctionnement	-10 °C – 55 °C
Dimensions (H × L × P)	197.5 mm × 152.5 mm × 52 mm
Poids	0.77 kg
Puissance de sortie	• Sécurité 868.65 MHz, 10 mW • Caméra 869.525 MHz, 100 mW
Modules GSM 2G et GSM 3G (RP512G2, RP512G3)	
Consommation électrique	Moyenne : 30 mA Pic : 130 mA
Module IP (RP512IP)	
Consommation électrique	Moyenne : 60 mA Pic : 115 mA



Claviers LCD sans fil : (RW332KP)

Consommation électrique

Moyenne : 9µA
Pic : 400 mA

Déclaration de conformité

Par la présente, RISCO Group déclare que les unités centrales et les accessoires de la série WiComm Pro respectent les normes suivantes :

- EN50131-1
- EN 50131-3 Grade 2 - Classe d'environnement II
- EN50131-6 Type A
- EN50136-1
- EN50136-2
- EN50131-10 Transmetteurs des locaux surveillés Type Z
- EN50131-5-3
- Compatibilité avec l'interface série avec AS
- Compatibilité avec le protocole GPRS
- Compatibilité avec le protocole TCP/IP
- Méthode de fonctionnement de la centrale : intercommunication
- Sécurité des signaux : sécurité de substitution S2
- Sécurité des informations I3

Classification et catégories des systèmes de transmission d'alarme :

- GSM 2G/3G (SP5)
- IP (SP6)
- GSM principal et IP secondaire (DP4),
- IP principal et GSM secondaire (DP4)

Conformité avec la norme EN50136 :

- RISCO déclare que les modules de communication GSM et IP WiComm Pro sont conformes aux exigences en matière de sécurité des informations et de sécurité des substitutions selon la norme EN50136.



Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates ("**Risco**") guarantee Risco's hardware products to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by Risco, for a period of (i) 24 months from the date of connection to the Risco Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the "**Product Warranty Period**" respectively).

Contact with customers only. This Product Warranty is solely for the benefit of the customer who purchased the product directly from Risco, or from any authorized distributor of Risco. Nothing in this Warranty obligates Risco to accept product returns directly from end users that purchased the products for their own use from Risco's customer or from any installer of Risco, or otherwise provide warranty or other services to any such end user. Risco customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. Risco's customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that Risco has any warranty or service obligation to, or any contractual privity with, any recipient of a product.

Return Material Authorization. In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, Risco shall, at its option, and at customer's expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization ("**RMA**") number from Risco prior to returning any Product to Risco. The returned product must be accompanied with a detailed description of the defect discovered ("**Defect Description**") and must otherwise follow Risco's then-current RMA procedure in connection with any such return. If Risco determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty ("**Non-Defective Products**"), Risco will notify the customer of such determination and will return the applicable Product to customer at customer's expense. In addition, Risco may propose and assess customer a charge for testing and examination of Non-Defective Products.

Entire Liability. The repair or replacement of products in accordance with this warranty shall be Risco's entire liability and customer's sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. Risco's obligation and the Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the product functionality.

Limitations. The Product Warranty is the only warranty made by Risco with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, the Product Warranty does not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the product and a proven weekly testing and examination of the product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow Risco's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without Risco's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond Risco's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any delay or other failure in performance of the product attributable to any means of communications, provided by any third party service provider (including, but not limited to) GSM interruptions, lack of or internet outage and/or telephony failure.



BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY.

Risco makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:

DISCLAIMER. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND LOSS OF DATA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT BY CUSTOMER OR END USER SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

Risco does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.

Risco does not guarantee that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof. Consequently Risco shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.

No employee or representative of Risco is authorized to change this warranty in any way or grant any other warranty.



Rapport de Conformité de RED

Par la présente, RISCO Group, déclare cet équipement est en conformité aux conditions essentielles et à d'autres dispositions appropriées de la directive 2014/53/EU. Vous pouvez trouver la copie complète de la déclaration de conformité à la directive 2014/53/EU sur notre site web, à l'adresse suivante : www.riscogroup.com:

Contacter RISCO Group

RISCO Group s'engage à fournir à ses clients un service et un support sur ses produits. Vous pouvez nous contacter via notre site Web **www.riscogroup.com** ou de la manière suivante :

Belgique (Benelux)

Tél. : +32-2522-7622

support-be@riscogroup.com

Chine (Shanghai)

Tél. : +86-21-52-39-0066

support-cn@riscogroup.com

France

Tél. : +33-164-73-28-50

support-fr@riscogroup.com

Israël

Tél. : +972-3-963-7777

support@riscogroup.com

Italie

Tél. : +39-02-66590054

support-it@riscogroup.com

Espagne

Tél. : +34-91-490-2133

support-es@riscogroup.com

Royaume-Uni

Tél. : +44-(0)-161-655-5500

support-uk@riscogroup.com

États-Unis

Tél. : +1-631-719-4400

support-usa@riscogroup.com

Ce produit RISCO a été acheté chez :



Aucune partie de ce document ne peut être reproduite, sous quelque forme que ce soit, sans l'autorisation écrite préalable de l'éditeur.

© RISCO Group 04/2018. Tous droits réservés

5IN2779