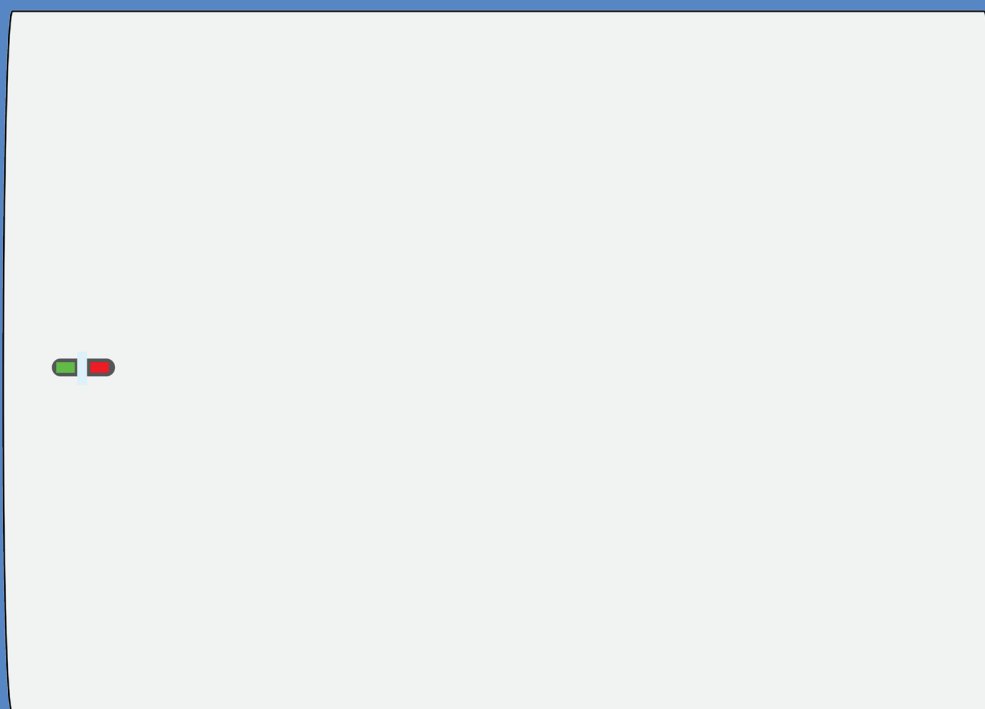




CENTRALE D'ALARME **W ET WIP**

DOC. - REF. 130-WIP210
DATE DE MODIF. : AVRIL 2015
VERSION LOGICIELLE : XLP.05.21.00.XXX ET SUIVANTES





Description

Avec les caméras Motion Viewer™ et la gamme de produits Videofied®, RSI VIDEO TECHNOLOGIES fournit depuis 2002 la seule levée de doute vidéo sans-fil du marché.

Après 2 ans de développement, RSI VIDEO TECHNOLOGIES est fier de vous présenter la centrale W.

La centrale W est un système de sécurité sans fil, fonctionnant sur alimentation secteur avec une batterie de secours rechargeable (fournie). C'est la première centrale d'alarme entièrement connectée conçue par RSI VIDEO TECHNOLOGIES.

Elle est destinée principalement aux marchés du résidentiel et des petits commerces.

Comme nos autres centrales d'alarme, la centrale W est compatible avec tous les périphériques conçus par RSI VIDEO TECHNOLOGIES.

Technologie

La centrale d'alarme W comme tous les produits Videofied®, utilise la technologie brevetée S2View®.

Cette technologie interactive et sans fil permet d'assurer une véritable intégrité du signal. Sa fiabilité est garantie par une liaison radio bidirectionnelle.

Un cryptage AES protège les communications entre la centrale et les périphériques. La sécurité des transmissions est optimale.

La fonction de détection du brouillage radio identifie le brouillage intentionnel du système par des tiers.

La fonctionnalité supervision permet à la centrale W de communiquer avec chaque périphérique du système. Les détecteurs transmettent toutes les 8 minutes un signal de présence à la centrale.

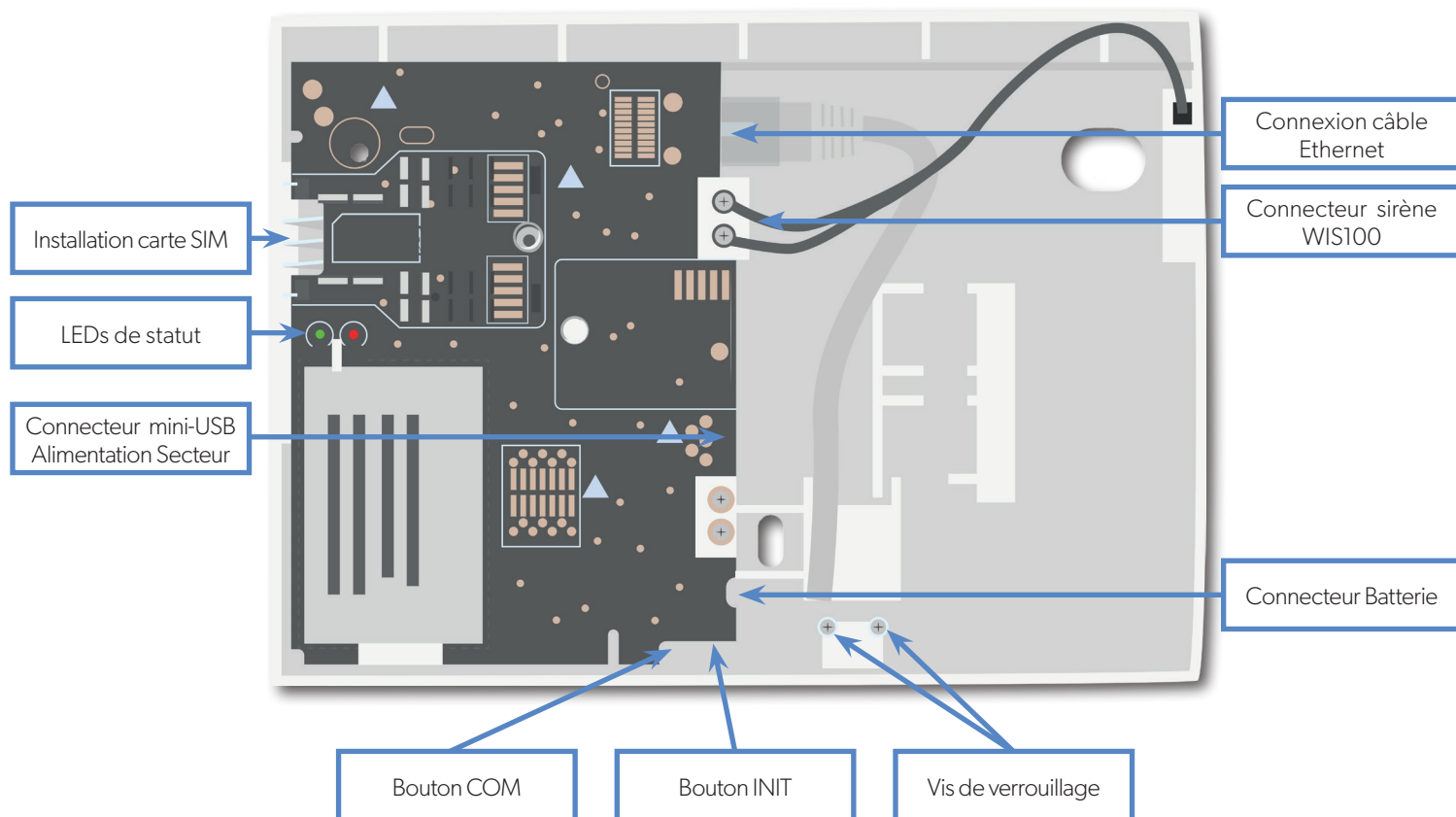
L'ensemble de l'équipe RSI VIDEO TECHNOLOGIES vous souhaite une bonne installation.



Introduction.....	2
Table des matières.....	3
1. Installation et configuration de la Centrale W.....	4
1.1 Présentation de la centrale.....	4
1.2 Fixation de la centrale W.....	4
1.3 Connexion du câble Ethernet.....	5
1.4 Installation de la carte SIM.....	5
1.5 Alimentation et initialisation.....	5
1.6 Signification des voyants lumineux.....	6
1.7 Enregistrer le clavier.....	6
2. Programmation de la W.....	7
Configuration des paramètres ETHERNET.....	11
3. Guide des fonctions de la W.....	15
3.1 Accéder au niveau 4.....	15
3.2 Armer/Désarmer le système.....	15
3.3 Programmer les modes d'armement spéciaux et les modes sirènes.....	16
3.4 Gérer les badges/codes d'accès.....	17
3.5 Supprimer un périphérique.....	19
3.6 Lire le journal des évènements.....	20
3.7 Les règles d'or.....	20
4. Paramètres Ethernet.....	21
5. Codes alarme.....	22
6. Codes erreur 2G3G.....	23
7. Certifications et notes de sécurité.....	24
8. Caractéristiques techniques.....	26



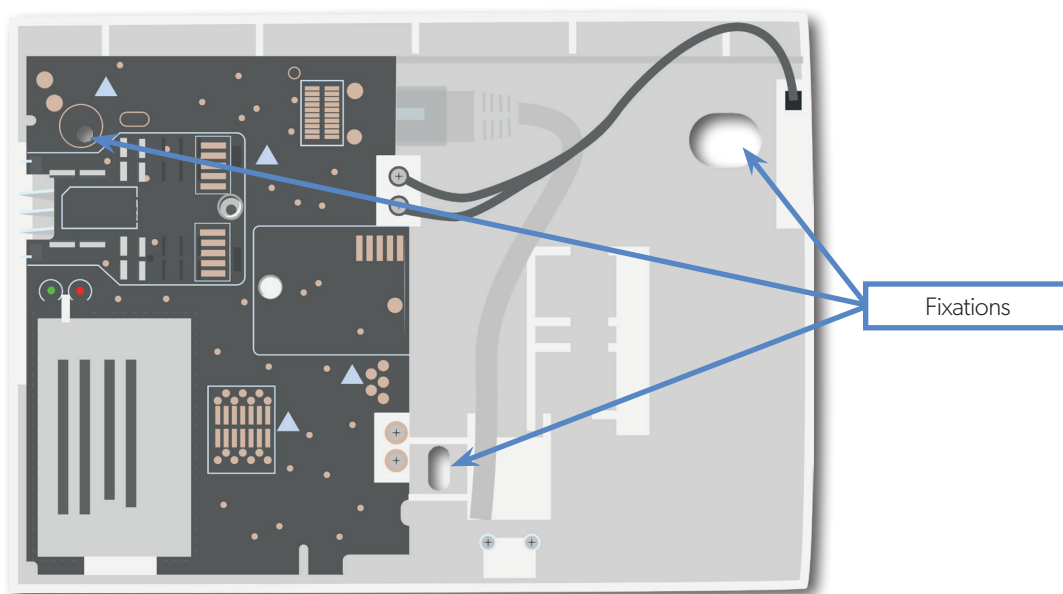
1.1 Présentation de la centrale



1.2 Fixation de la centrale W

Fixer la centrale au mur en utilisant les trois trous de fixation (diamètre 4mm) détaillés ci-contre.

La fixation de la centrale n'est pas obligatoire pour la programmation.





1.3 Connexion du câble Ethernet

**Uniquement pour les WIP 210/220/230, WIP 620/630 et WIP 720/730*

Une fois la centrale fixée à son emplacement définitif, connecter un câble RJ45 entre le réseau internet filaire du site (box, réseau d'entreprise) et le port Ethernet de la centrale d'alarme.

Lorsque la centrale tentera de transmettre en Ethernet, les indicateurs lumineux clignoteront. Cela permettra à l'installateur de savoir si la centrale est connectée à un réseau viable.

Ne pas manipuler le câble RJ45 lorsque la centrale est alimentée.

IMPORTANT :

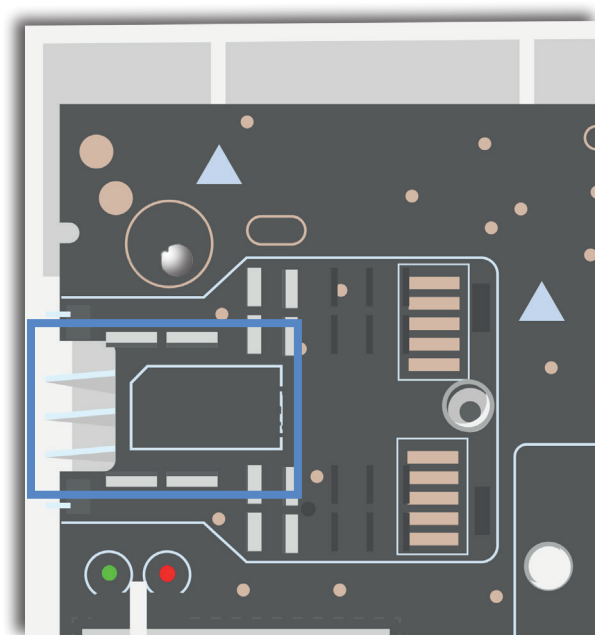
Ne branchez que des réseaux TBTS de type 10Base-T

1.4 Installation de la carte SIM

Insérer une carte SIM (de type Mini-SIM 2FF) dans l'emplacement prévu à cet effet (veiller à respecter le sens d'introduction). Se référer au marquage positionné à côté du connecteur de la SIM.

Utiliser une carte 2G3G de type M2M (machine-to-machine). Si la centrale est utilisée avec une application smartphone, la carte SIM doit pouvoir recevoir des SMS.

Ne pas manipuler la carte SIM lorsque la centrale est alimentée.



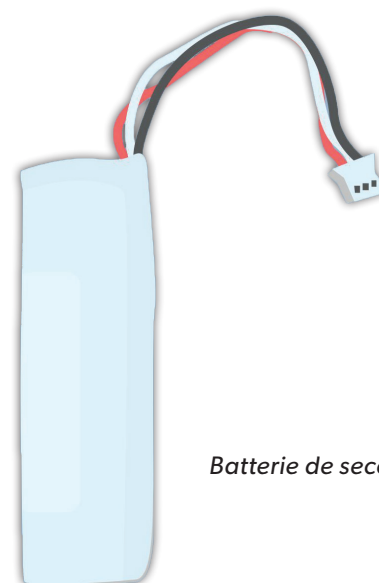
1.5 Alimentation et initialisation

Alimentation

- Connectez la batterie de secours.
- Installer l'alimentation secteur à l'intérieur ou à l'extérieur du boîtier selon la longueur de câble souhaitée
- Connecter l'alimentation secteur sur le connecteur mini-USB de la centrale
- Brancher l'alimentation secteur à une prise secteur. Si la batterie n'est pas connectée, la LED rouge clignote rapidement.
- Ne jamais connecter l'entrée 12V (scellée par une étiquette), spécifiquement lorsque la centrale est alimentée.

Initialisation







- **Laisser le capot de la centrale ouvert.** La LED de statut verte est allumée. Appuyez 6-7 secondes sur le bouton INIT jusqu'à ce que la LED de statut rouge s'allume pendant 1 seconde.
- La LED rouge clignote plusieurs fois puis s'éteint. Cette manipulation vide la mémoire de la centrale.
- La centrale est maintenant initialisée. Un clavier Videofied® doit être enregistré pour pouvoir configurer la centrale.



Batterie de secours



1.6 Signification des voyants lumineux

	LED rouge allumée 	LED rouge clignotante 	LED rouge clignotante (3 sec) 	LED rouge éteinte 
LED verte allumée (secteur présent) 	N/A	Batterie hors service ou absente.	Batterie tension basse.	Etat normal.
LED verte éteinte (secteur absent) 	Batterie tension basse.	N/A	Fonctionnement sur batterie. Batterie OK.	Produit hors service ou non alimenté.

1.7 Enregistrer le clavier (Se référer aux fiches d'installation des claviers Videofied®)

- Appuyez brièvement sur le BOUTON INIT de la centrale pour qu'elle passe en mode d'enregistrement de clavier.
- Insérez 3 ou 4 **piles Lithium LS14500** dans le clavier.
- Ne montez pas le clavier. Celui-ci affiche l'un des écrans suivants:

RSI (c) 2014
 videofied.com

ou

<=====XX=====>

- Appuyer simultanément** sur les touches **CLR** et **ESC NO** du clavier jusqu'à ce que le voyant du clavier clignote, puis relâchez et attendez la confirmation de l'enregistrement du clavier.
- Si le clavier ne parvient pas à s'enregistrer** alors qu'il affichait XX, c'est que ce dernier est toujours enregistré sur un autre système d'alarme. Le clavier doit donc être réinitialisé. Retirez les piles du clavier et appuyez de façon répétée sur son bouton d'autoprotection. Une fois cette procédure terminée, répétez la procédure ci-dessus.

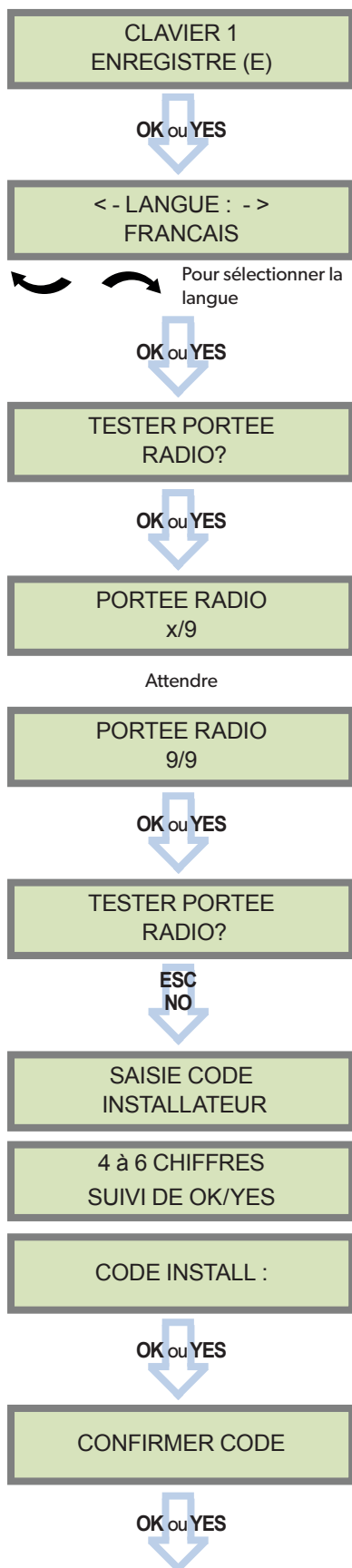


2. PROGRAMMATION DE LA CENTRALE W

Se référer aux instructions du clavier pour programmer la centrale

Affichage du clavier

Commentaires



Le système pourra également être configuré en : anglais, italien, allemand, néerlandais, espagnol, suédois, portugais, danois, tchèque, turc et polonais.

La langue pourra être modifiée une fois la centrale configurée dans le menu MAINTENANCE.

Le test de portée radio doit être réalisé lors de l'enregistrement du clavier de sorte à favoriser le bon fonctionnement du système et faciliter ainsi la configuration de ce dernier.

Ce test est important, il évalue la qualité de la portée radio entre la centrale et le clavier. Lors du test, le clavier vous informe en temps réel de l'évolution du niveau de portée radio sur une échelle de 9. De sorte à optimiser au maximum la qualité de ce test, celui ci doit durer au minimum 30 secondes.

Le niveau de portée radio doit être au minimum de 8/9.

Utiliser le clavier alphanumérique pour entrer le code installateur de votre choix.

Ce code est très important, vous en aurez besoin pour l'ensemble de la configuration et des maintenances futures.

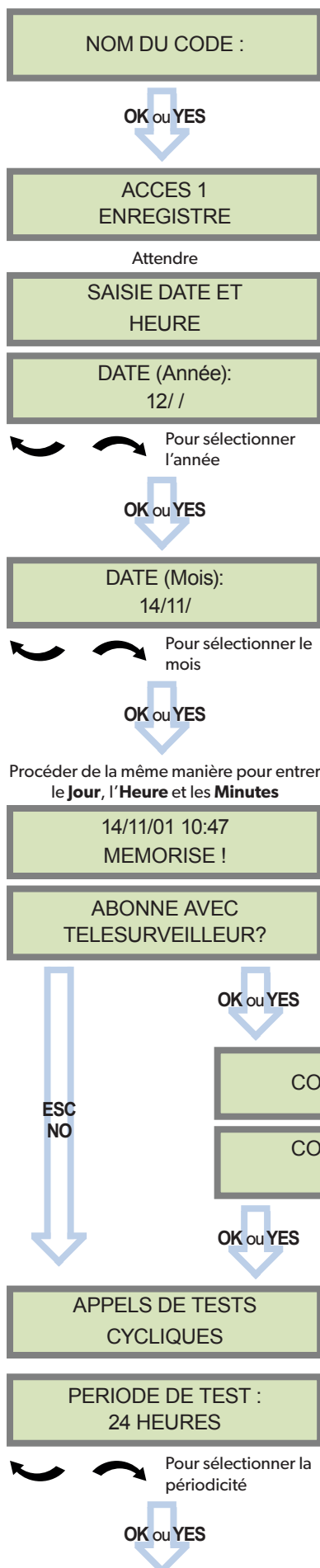
Il n'y a aucun moyen de paramétrer le système sans le code installateur.

Mémoirisez-le bien.

Certains codes sont interdits et ne peuvent être utilisés. Veuillez-vous reporter au chapitre 3.4.



2. PROGRAMMATION DE LA CENTRALE W



Donner un nom significatif à votre code installateur à l'aide du clavier alphanumérique.

Si vous possédez un paramétrage automatique (appelé liste installateur), entrez le nom associé à la liste installateur.

Attention : Si vous ne donnez pas le bon nom de code pour la liste installateur, vous ne pourrez pas paramétrer automatiquement votre centrale plus tard, le système devra être réinitialisé.

Si vous laissez le champ vide en appuyant sur **ESC NO**, le nom du code par défaut sera 'ACCES 1'.

A l'aide du clavier alphanumérique, entrer le code abonné (compris entre 4 et 8 chiffres) fourni par votre centre de télésurveillance.

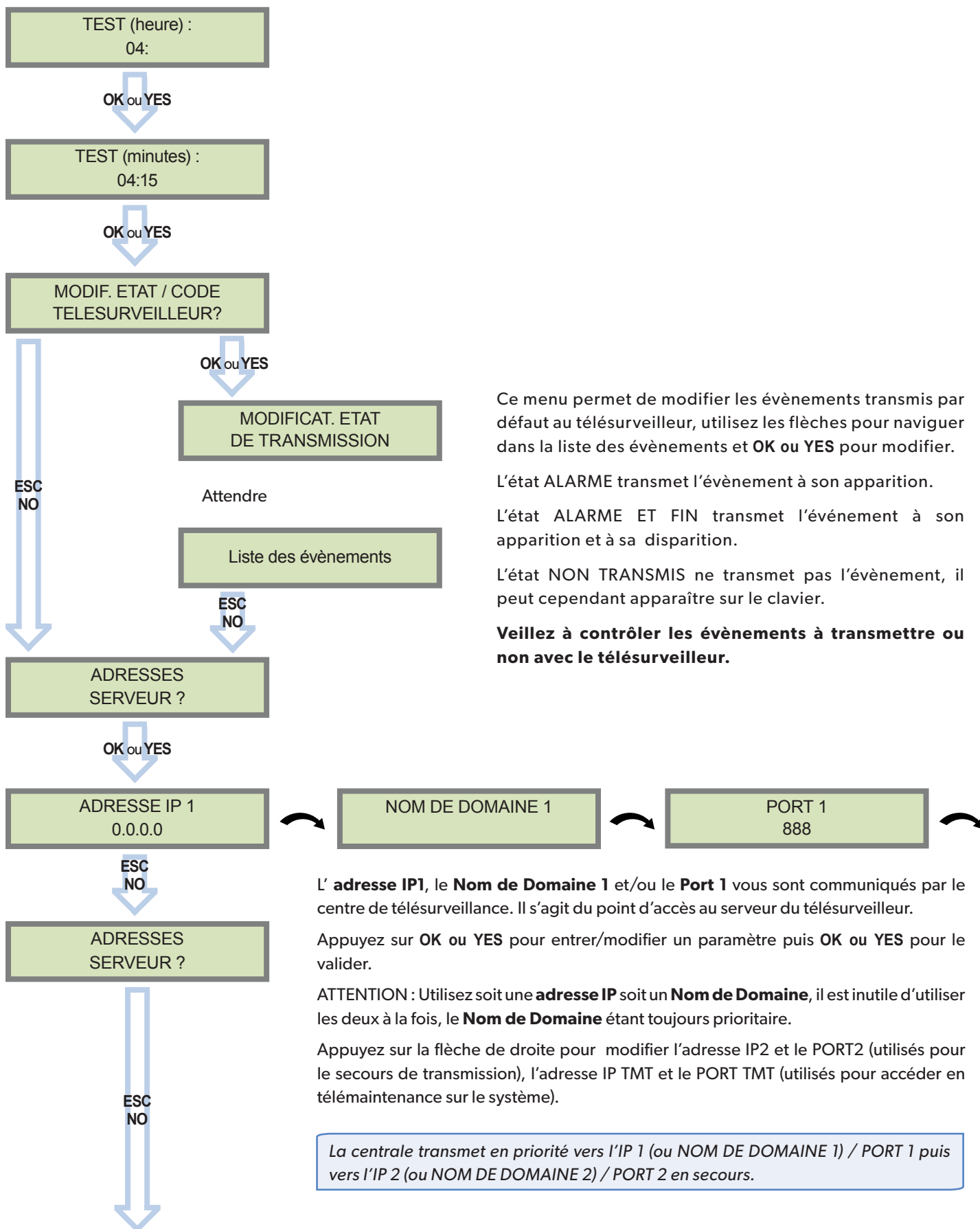
Ce code identifie le système installé chez le télésurveilleur.

Périodicité du test : 1 heure, 12 heures, 24 heures, 48 heures, 7 jours ou pas de test.

Nous recommandons un test périodique toutes les 24 heures.

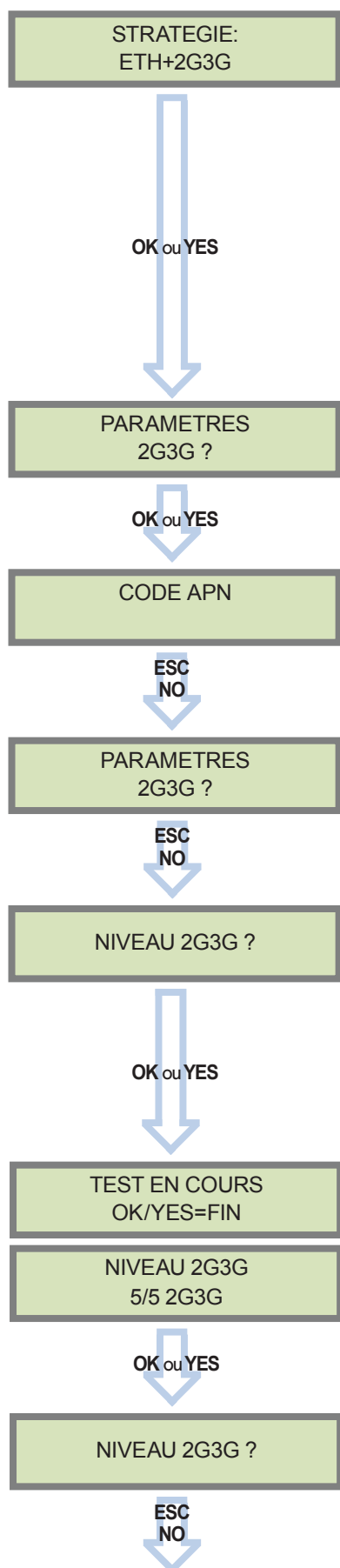


2. PROGRAMMATION DE LA CENTRALE W





2. PROGRAMMATION DE LA CENTRALE W



Modes de transmission des alarmes et vidéos au centre de télésurveillance :

2G3G : Communication carte SIM seule
 ETH : Communication Ethernet* seule (non recommandé***)
 WLAN : Communication Wi-Fi** seule (non recommandé***)
 ETH+2G3G : Communication Ethernet* avec carte SIM de secours
 2G3G+WLAN : Communication Wi-Fi** avec carte SIM de secours
 ETH+WLAN : Communication Ethernet* avec secours Wi-Fi** (non recommandé***)
 ETH+2G3G+WLAN : Communication Ethernet* avec secours Wi-Fi** puis 2G3G

* Uniquement pour les WIP 210/220/230, WIP 620/630 et WIP 720/730

**Uniquement disponible lorsque l'option WWB100 est installée.

***En cas de perte de connexion internet ou défaut secteur, les événements ne seront pas transmis si le Wi-Fi et/ou l'Ethernet sont les seuls modes de transmission.



Le **Code APN** (Access Point Name), le **Nom Utilisateur** et/ou le **Mot de Passe** vous sont communiqués par le fournisseur de la carte SIM. Ces paramètres sont utilisés par la carte SIM pour se connecter au réseau 2G3G.

Appuyez sur **OK** ou **YES** pour entrer/modifier un paramètre puis **OK** ou **YES** pour le valider.

Remarque:

Les paramètres 2G3G sont sensibles à la différence minuscules/majuscules !

Utilisez la touche **M/m** du clavier (clavier CMA) ou maintenez une touche numérique (**XMA**, **XMB**) pour basculer entre les lettres minuscules/majuscules.

Une fois le test de niveau 2G3G complété, le système affichera l'une des réponses suivantes :

- Un niveau entre 0/5 et 5/5.
- Un code erreur (veuillez vous référer au Chapitre 6 : Codes Erreur 2G3G).

En cas de mise en veille de l'écran, de sorte à le rallumer appuyer sur n'importe quelle touche du clavier sauf **OK** ou **YES**, **ESC NO** ou **CLR**.

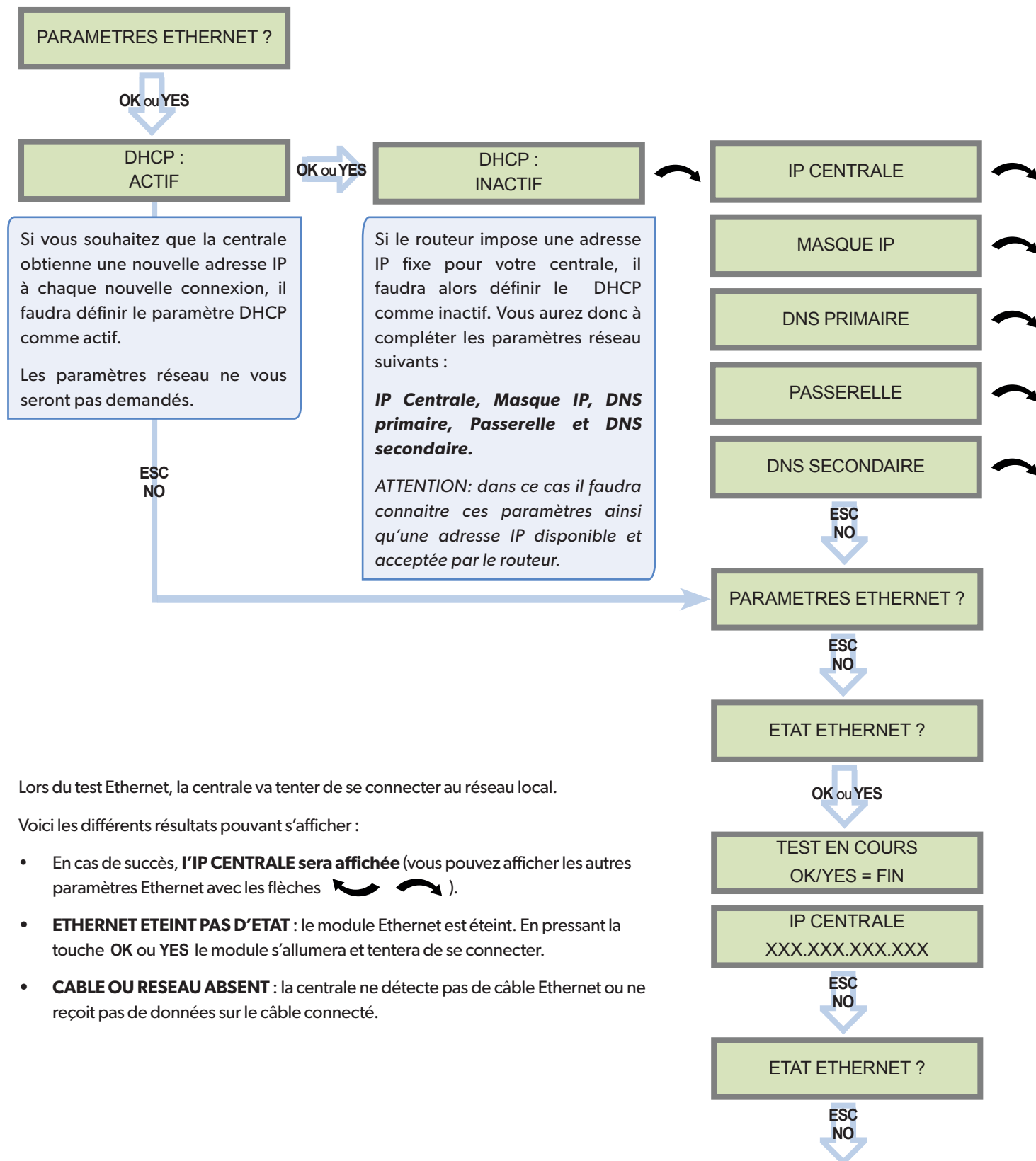
Le test de niveau 2G3G peut prendre plusieurs minutes. **Ne pas l'interrompre ou retirer la carte SIM pendant ce test.**

Il est impératif d'avoir au minimum un niveau 2G3G de 3/5 de sorte à transmettre correctement.



Configuration des paramètres ETHERNET

Uniquement pour les WIP 210/220/230, WIP 620/630 et WIP 720/730



Lors du test Ethernet, la centrale va tenter de se connecter au réseau local.

Voici les différents résultats pouvant s'afficher :

- En cas de succès, **l'IP CENTRALE sera affichée** (vous pouvez afficher les autres paramètres Ethernet avec les flèches ↩ ↪).
- **ETHERNET ETEINT PAS D'ETAT** : le module Ethernet est éteint. En pressant la touche **OK** ou **YES** le module s'allumera et tentera de se connecter.
- **CABLE OU RESEAU ABSENT** : la centrale ne détecte pas de câble Ethernet ou ne reçoit pas de données sur le câble connecté.



2. PROGRAMMATION DE LA CENTRALE W

Si vous souhaitez utiliser le mode de fonctionnement de la norme EN50131, valider par **OK** ou **YES**. Sinon appuyer sur **ESC NO**.

Cette option est indispensable à un fonctionnement conforme aux certifications EN50131 et NF&A2P.

Entrez le nom de la zone 1 et validez avec **OK** ou **YES**.

Recommencez l'opération pour les zones 2, 3 et 4.

Reportez-vous au chapitre 3.3 pour plus d'informations.

Les valeurs de temporisation de sortie possibles sont : 45 secondes, 1 minute et 2 minutes.

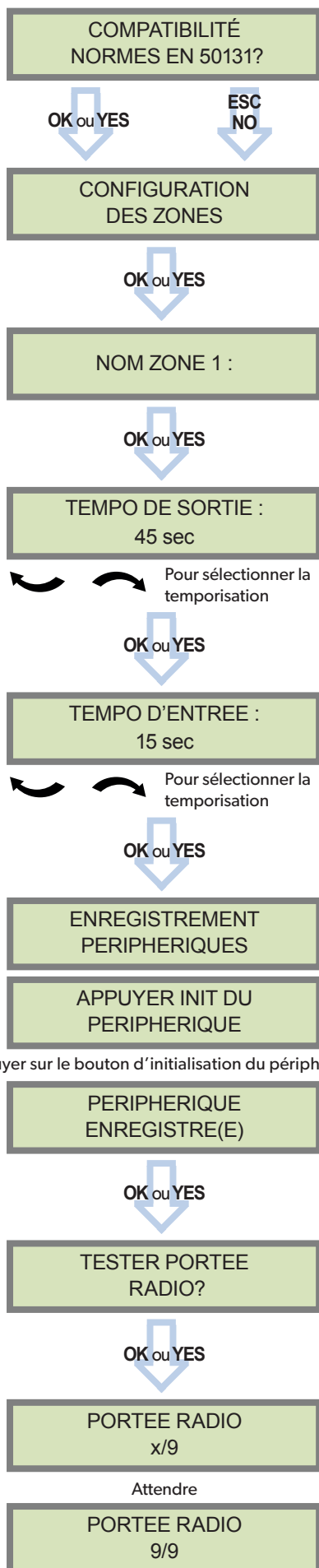
Les valeurs de temporisation d'entrée possibles sont : 15 secondes, 30 secondes, 45 secondes, 1 minute et 2 minutes.

Enregistrez vos périphériques les uns à la suite des autres, chaque périphérique a un bouton d'initialisation unique ou une manipulation spécifique permettant de l'associer à la centrale d'alarme (se référer aux fiches d'installation de chaque périphérique).

Vérifier que le niveau radio de chaque périphérique est suffisant lorsqu'il est installé à son emplacement définitif.

Le niveau radio minimum doit être de 8/9.

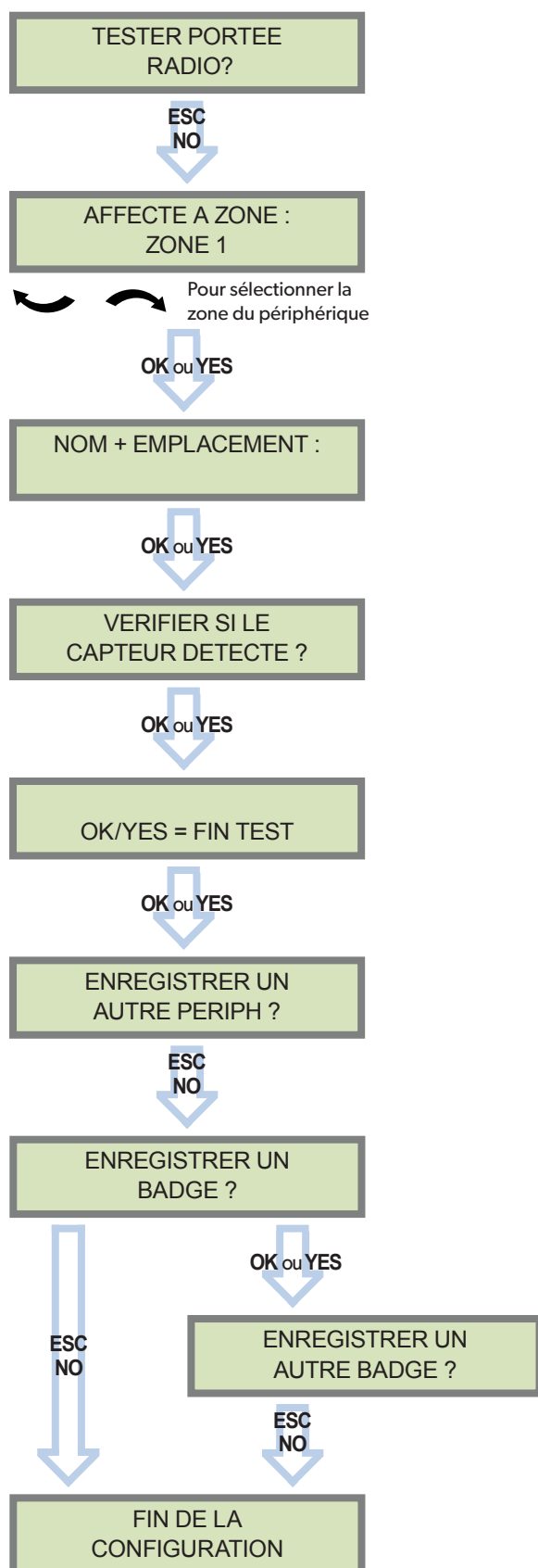
Pour plus d'informations sur la portée radio, se référer à la page 6.



Appuyer sur le bouton d'initialisation du périphérique



2. PROGRAMMATION DE LA CENTRALE W



Chaque périphérique est enregistré dans une zone. Il est possible de paramétrer la temporisation de chaque zone. Le paramétrage des armements partiels utilise aussi les zones.

Pour plus d'informations sur les armements partiels, se référer au chapitre 3.3.

Par défaut (zone paramétrée comme Automatique), la zone 1 est temporisée et les zones 2, 3 et 4 sont immédiates. L'enregistrement d'un clavier ou d'un lecteur de badge dans une zone temporise cette zone.

Nommez le périphérique de façon appropriée afin de donner le maximum d'informations en cas d'alarme.

Pendant le test de détection, le périphérique allumera un indicateur rouge s'il détecte une intrusion.

Appuyez sur **OK** ou **YES** pour enregistrer un autre périphérique ou **ESC NO** pour terminer.

Chaque système peut inclure un maximum de 25 périphériques, **clavier déporté inclus**.

Appuyez sur **OK** ou **YES** si vous utilisez un ou plusieurs badges. **ESC NO** dans le cas contraire.

Ces badges serviront de premier accès utilisateur (Niveau 3) et seront nécessaires pour passer en niveau 4 (installateur).

Si vous souhaitez un code utilisateur, ignorez cette étape et enregistrez le dans le menu **BADGES/CODES D'ACCES** (voir chapitre 3.4 pour plus d'informations).

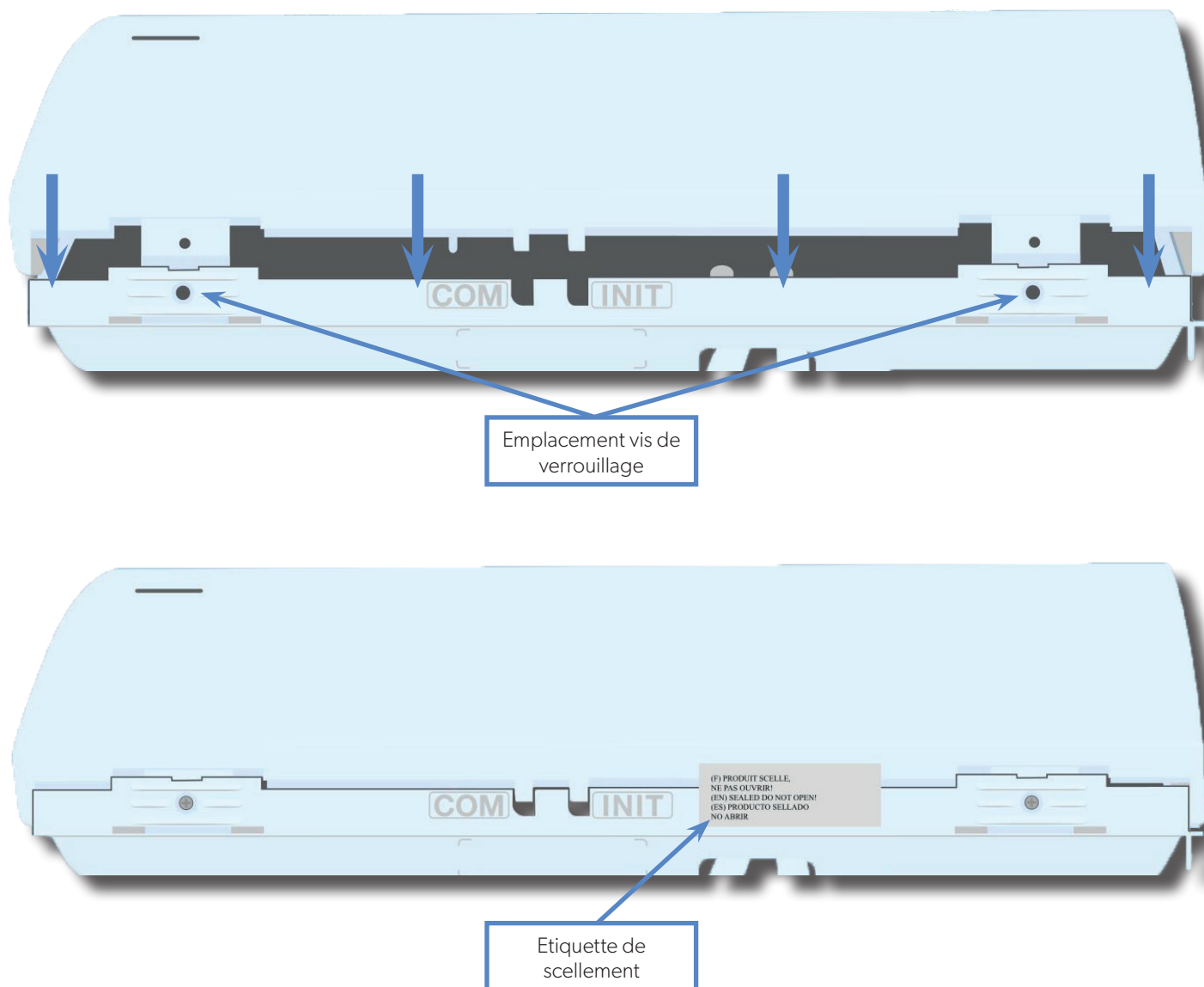
Le nombre de codes ou badges enregistrés dans le système est limité à 49 accès utilisateur et 1 code installateur.



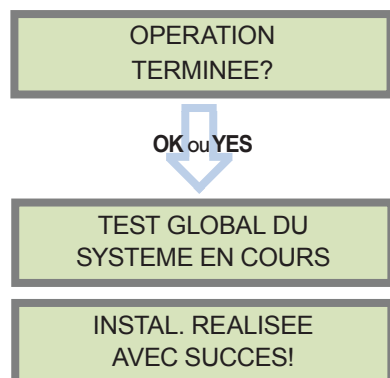
2. PROGRAMMATION DE LA CENTRALE W

Une fois cette configuration terminée, fermer la centrale en rabattant le capot comme indiqué ci-dessous. Verrouiller le boîtier avec les vis de verrouillage fournies dans le boîtier (voir chapitre 1.1 page 4) puis sceller avec l'étiquette de scellement fournie.

Le verrouillage et scellement du boîtier est obligatoire pour la conformité aux normes NF&A2P et EN50131.



L'affichage indique :



Avant de terminer la programmation vérifier qu'aucun périphérique ne soit en autoprotection. Pour cela l'indicateur lumineux de chaque élément doit être éteint.

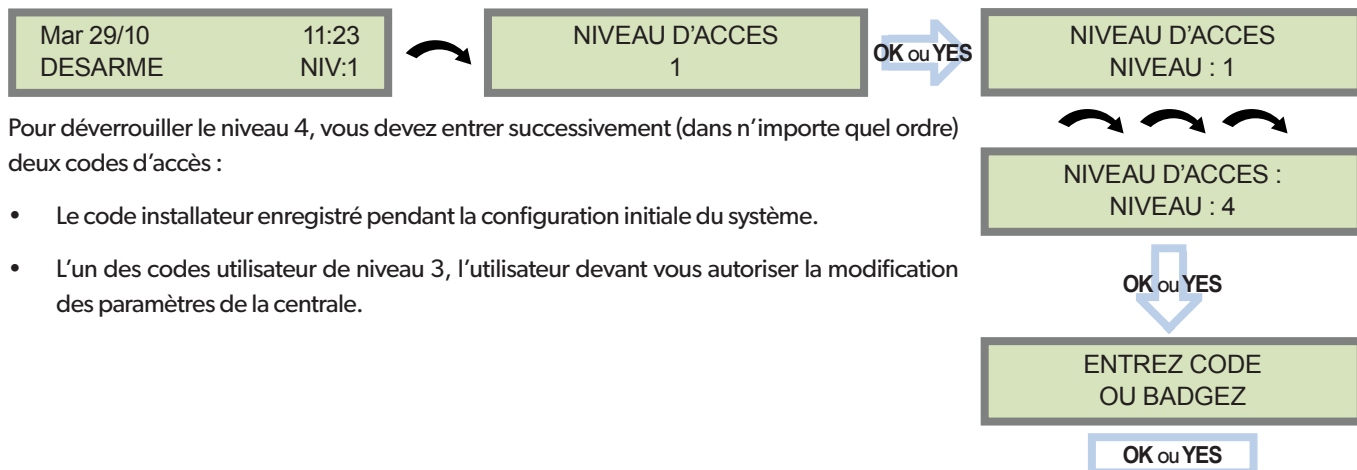
Il ne reste plus qu'à programmer les codes utilisateurs et les modes d'armement partiels.

Une fois votre installation terminée, se référer à la structure des menus (synoptique) de la W afin d'identifier toutes les fonctionnalités de la centrale d'alarme.



3. GUIDE DES FONCTIONS DE LA CENTRALE W

3.1 Accéder au niveau 4







Pour déverrouiller le niveau 4, vous devez entrer successivement (dans n'importe quel ordre) deux codes d'accès :

- Le code installateur enregistré pendant la configuration initiale du système.
- L'un des codes utilisateur de niveau 3, l'utilisateur devant vous autoriser la modification des paramètres de la centrale.

3.2 Armer/Désarmer le système

En mode veille, le système peut être armé par un clavier déporté et/ou un lecteur de badge déporté.

	Armement total avec code utilisateur	Armement total avec badge	Armement partiel 1	Armement partiel 2
Avec un clavier déporté	Entrez votre code utilisateur et appuyez sur OK / YES	Présentez votre badge sur le clavier (uniquement sur le XMB)	Appuyez sur  entrez votre code utilisateur et appuyez sur OK / YES	Appuyez sur  entrez votre code utilisateur et appuyez sur OK / YES
Avec un lecteur de badge déporté BR250	non applicable	Présentez votre badge sur le lecteur de badge	non applicable	non applicable
Avec une télécommande	Appuyer sur ON	Appuyer sur ON	Appuyez sur 	Appuyez sur 




3.3 Programmer les modes d'armement spéciaux et les modes sirènes



- Avec les flèches de directions   allez au menu :

CONFIGURATION (NIV 4) -> MODE ALARMES PROGRAMMABLES -> MODE NORMAL

- Puis utilisez les flèches de direction pour sélectionner le mode d'armement concerné et la touche **OK** ou **YES** pour le modifier.

- **Il y a trois modes d'armement possibles :**

Le MODE NORMAL correspond au mode d'armement général, lancé à l'aide d'un badge ou avec un code utilisateur puis la touche **OK** /  sur le clavier.

Le MODE SPECIAL 1 correspond à un mode partiel activé par la saisie d'un code utilisateur et la touche  sur un clavier ou la touche  sur une télécommande.

Le MODE SPECIAL 2 est disponible sur un clavier par la touche  et sur une télécommande par la touche .

Pour chaque mode d'armement, il est possible de déterminer comment chacune des 4 zones est armée et comment le système réagit pendant une alarme.

Zones : 1 2 3 4

Etat : A A A A

À chaque pression sur un chiffre correspondant à une zone, le système modifie l'état d'armement de la zone concernée.

Appuyez sur la touche **OK / YES** après cette étape de la configuration. Le système affiche alors le mode sirène activé pour ce mode spécial. Choisissez le mode sirène à l'aide des flèches de direction puis appuyez sur **OK / YES**.

A	Armé
D	Désarmé
P	Périmètre (arme tous les périphériques identifiés comme périmétriques*)
E	Externe (arme tous les périphériques identifiés comme extérieurs*)

Sirène	Déclenchement immédiat de toutes les sirènes
Pré-alarme	Bips de temporisation, puis déclenchement des sirènes
Silencieuse	Sans sirène, sans bips
Sans sirène	Bips sur le clavier uniquement

* Un périphérique peut être identifié comme extérieur, périmétrique, ou extérieur+périmétrique dans le menu :

CONFIGURATION (NIV 4) > ZONES ET PERIPHERIQUES > PERIPHERIQUES > CONFIGURATION PERIPHERIQUE > TYPE PERIPH.



3.4 Gérer les badges/codes d'accès

Niveau d'accès

Niveaux d'accès sur la centrale W	Définition et droits
NIV 1	Niveau attente
NIV 2	Niveau UTILISATEUR restreint , permettant uniquement d'armer/désarmer le système.
NIV 3	Niveau UTILISATEUR , permettant d'armer/désarmer le système, de consulter le journal des événements et de tester les périphériques. Il n'est pas possible de modifier les réglages à ce niveau. L'utilisateur Niveau 3 peut créer des codes d'accès Niveau 2 et Niveau 3 .
NIV 4	Niveau INSTALLATEUR , permettant de modifier les paramètres du système. Pour accéder au Niveau 4 , il est nécessaire de saisir un code de Niveau 3 ou de Niveau 2 , l'utilisateur devant vous autoriser la modification des paramètres de la centrale. Un code de Niveau 4 peut créer le premier code Niveau 3 .

Les codes et les badges se voient attribuer des droits d'accès correspondant à l'un des 4 niveaux d'accès disponibles.

Notez que la centrale W ne dispose pas d'un accès fabricant (niveau 4 de la norme EN50131).

Comment retourner au NIV 1 ?

- Si le clavier n'est pas utilisé et qu'il n'y a pas de test en cours, le système retourne au NIV 1 avec un affichage en veille au bout de 1 min.
- Une pression de 5s sur la touche **ESC NO** fait retourner au NIV 1.

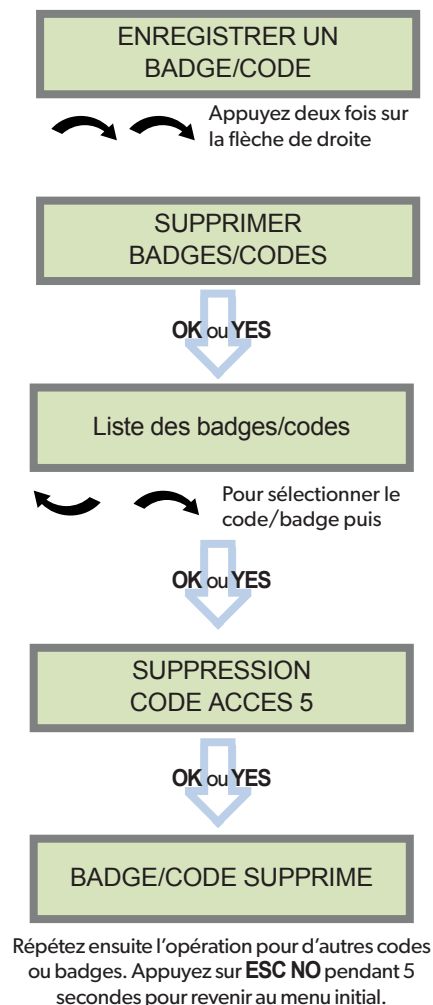


3. GUIDE DES FONCTIONS DE LA CENTRALE W

Enregistrer un nouveau badge ou code



Supprimer un code ou un badge



Codes réservés

Il est possible de créer jusqu'à 49 codes (ou badges) différents en plus du code installateur. Chaque code utilise 4 à 6 chiffres (de 0 à 9).

Les codes ci-contre sont **réservés** et ne peuvent pas être utilisés. Ils sont utilisés pour la maintenance du système ou comme codes panique/codes sous contrainte.

186 codes au total sont interdits.

Codes réservés
000000
De 9998 à 9999
De 99998 à 99999
De 999898 à 999999
De 314157 à 314159
Tous les codes utilisateur +1
Tous les codes utilisateur +2
Tous les codes utilisateur -1
Tous les codes utilisateur -2

La création d'un code (par exemple 1000) entraîne la réservation des 2 codes suivants et précédents (0998, 0999, 1001 et 1002).

Le code +1 (1001) est utilisé pour un désarmement sous contrainte.

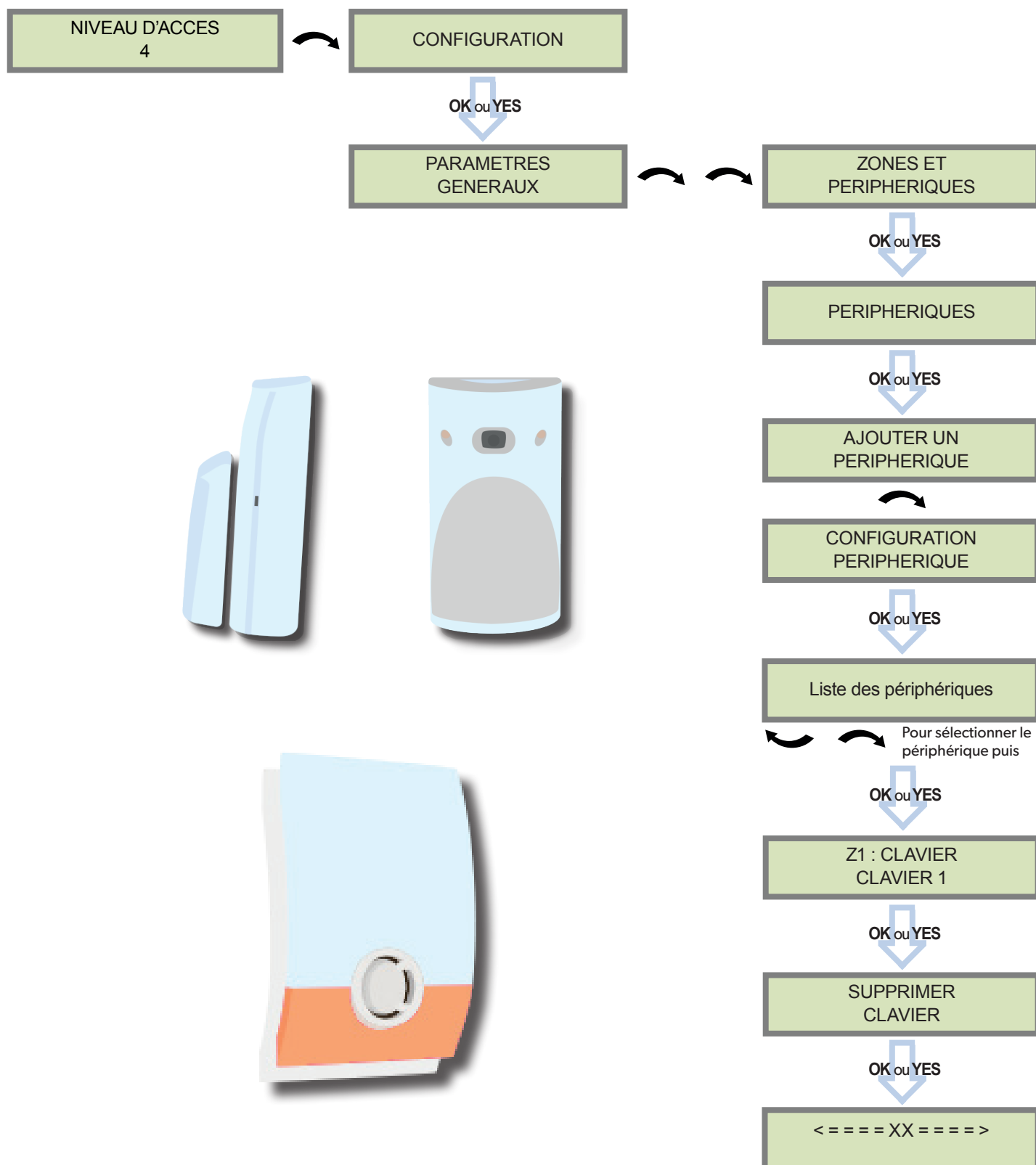
Le code +2 (1002) est utilisé pour un déclenchement panique.

Les codes -1 et -2 (0998 et 0999) sont réservés pour éviter les conflits lorsque vous créez un nouveau code utilisateur.



3. GUIDE DES FONCTIONS DE LA CENTRALE W

3.5 Supprimer un périphérique



Vous pouvez enlever les piles du périphérique.



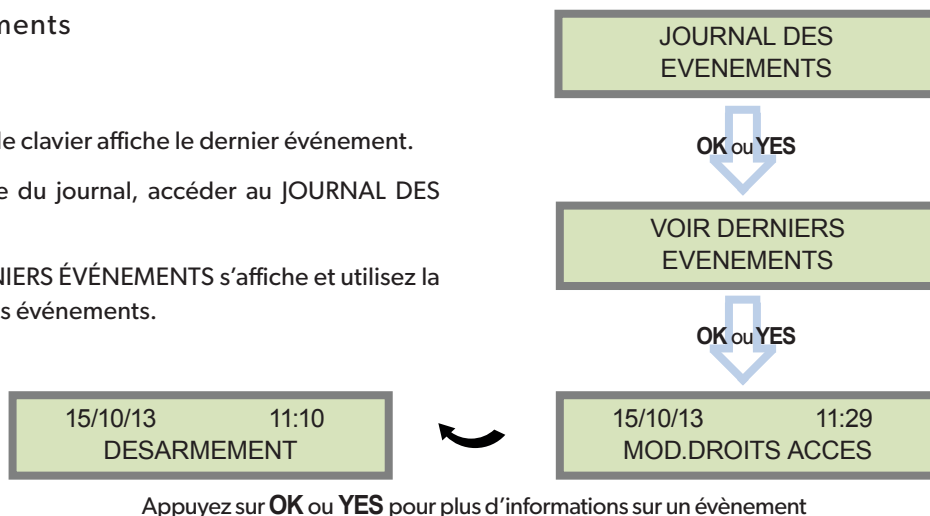
3. GUIDE DES FONCTIONS DE LA CENTRALE W

3.6 Lire le journal des évènements

Quand un utilisateur désarme le système, le clavier affiche le dernier événement.

Si l'utilisateur a besoin de lire l'ensemble du journal, accéder au JOURNAL DES ÉVÉNEMENTS.

Appuyez sur **OK** ou **YES** quand VOIR DERNIERS ÉVÉNEMENTS s'affiche et utilisez la flèche de gauche pour parcourir la liste des événements.



3.7 Les règles d'or

1. Les périphériques dans la **Zone 1** sont **temporisés** par défaut (paramètre Mode Zone : Auto). Ajouter un clavier ou un lecteur de badge dans une zone (paramétrée en Auto) temporisera automatiquement cette même zone.
2. **N'installez pas** la centrale W sur ou près d'un **tableau électrique haute tension**, à cause des interférences possibles qui nuiraient aux performances du modem radio et 2G3G.
3. Utilisez la touche **CLR** pour effacer le caractère précédent lorsque vous entrez un paramètre.
4. Ne jamais enregistrer 2 fois le même périphérique sans l'avoir, au préalable, supprimé de la programmation de la centrale.
5. Le système permet l'enregistrement d'un **maximum de 25 périphériques**, tous types confondus (clavier et télécommandes inclus).
6. Respecter les hauteurs et consignes d'installation des caméras MotionViewer. Ces périphériques doivent être installés en tenant compte du champ de vision infrarouge, de façon à protéger un bien plutôt qu'une zone.
7. Installez le clavier déporté en dernier, car il est utile d'avoir un clavier mobile pendant la procédure d'installation.
8. **Toujours essayer** l'objectif des caméras une fois posées (utilisez un chiffon propre et sec en prenant soin de ne pas exercer de pression sur l'objectif).
9. Faire preuve de prudence lors de l'ouverture et la fermeture du capot de la centrale, car les composants internes sont fragiles.
10. Le clavier se met en veille après 30 secondes d'inactivité. Appuyer sur **une flèche ou une touche numérique** pour faire revenir l'affichage.
11. Les détecteurs infrarouges ne doivent jamais être placés dans un escalier, ou à proximité d'un escalier (risque de fausses alarmes).
12. L'affichage de deux points [:] signifie que le paramètre peut être modifié. Appuyer sur **OK/YES** pour afficher les deux points.



4. PARAMÈTRES ETHERNET

Pour configurer ou modifier les paramètres Ethernet*, à l'aide des flèches de direction aller dans le menu :



Dans le menu Ethernet il est possible de paramétrer:

- Paramètres IP :

Lorsque vous souhaitez utiliser le mode de transmission Ethernet, deux options s'offrent à vous:

1. DHCP ACTIF : A chaque fois que la centrale se connectera à votre réseau, elle obtiendra une nouvelle adresse IP (adresse IP dynamique). Cette option est configurée par défaut dans la centrale.
2. DHCP INACTIF : Soit vous décidez de fixer l'adresse IP de la centrale. A chaque connexion de votre centrale au réseau (pour transmettre une alarme), la centrale W aura les mêmes paramètres de connexion. Il faudra alors se connecter au routeur (box) pour connaître les paramètres du réseau local ainsi que les adresses IP disponibles. Les paramètres IP CENTRALE, MASQUE IP, PASSERELLE, DNS PRIMAIRE, DNS SECONDAIRE sont à renseigner dans le menu PARAMETRES IP.

- Ethernet Permanent :

Trois options sont disponibles :

1. Mode « Auto ». Nous recommandons ce mode de fonctionnement. Lorsque la centrale sera alimentée par le secteur, la centrale sera connectée en permanence au réseau Ethernet. Lors d'une intrusion, la centrale n'aura pas de période de connexion au réseau et donc l'alarme arrivera en quelques secondes au PC de télésurveillance. Lors d'une coupure secteur, le module Ethernet va rester allumé pendant un certain temps DELAI AVANT OFF compris entre 5 et 30 minutes. Ce délai est configurable dans le menu :

CONFIGURATION (NIV 4) -> PARAMETRES GENERAUX -> ETHERNET -> ETH. PERMANENT -> DELAI AVANT OFF.

2. Mode « ON ». La centrale sera connectée en permanence au réseau Ethernet même en cas de coupure secteur (ce qui risque de réduire fortement l'autonomie de la batterie de secours).
3. Mode « OFF ». A chaque transmission, la centrale devra d'abord se connecter au réseau Ethernet.

- Réponse PING, Time Out Server, Taille Segment

- Réponse PING : Permet de rendre actif la réponse au PING envoyés à la centrale
- Time Out Server : En cas de déconnexion au réseau local la centrale aura un délai (time out server) avant de tenter une reconnexion au réseau.
- Taille Segment : Taille des paquets envoyés.

**Uniquement pour les WIP 210/220/230, WIP 620/630 et WIP 720/730*



5. CODES ALARME

La centrale W peut être configurée pour activer ou désactiver la transmission de certains événements comme les alarmes ou les défaillances.

L'installateur peut modifier les réglages par défaut pour ces événements, mais toute modification mettra fin à la conformité à la norme EN50131.

Par défaut sont transmis les événements :	Par défaut ne sont pas transmis :
DETECTEUR (intrusions) ALERTE (bouton panique) PILES CENTRALE AUTOPROTECTION (sabotage) PILE DETECTEUR TEST CYCLIQUE CODE CONTRAINTE INCENDIE ASSIST. MEDICALE CABLE ETHERNET SECTEUR CENTR. (alimentation secteur)	RESET CENTRALE DEFAUT LIGNE (ligne téléphonique défectueuse) BROUILLAGE RADIO (brouillage radio) SUPERVISION (filaire et radio) CODES FAUX (saisie de 5 codes/badges erronés) MEMO ALARME (reconnaissance de l'alarme au clavier) ARMEMENT/DESARMEMENT (marche/arrêt) EJECTION PERIPH. (activation/désactivation de la fonction bypass) SWINGER SHUTDOWN (activation/désactivation de la fonction déclenchements intempestifs)

Il existe 3 états de transmission :
ALARME , l'événement est transmis quand il se produit.
ALARME ET FIN , l'événement est transmis quand il se produit et au retour à la normale.
NON TRANSMIS

Exemple :

Si le système est configuré au centre de télésurveillance pour la surveillance des armements et désarmements, le paramètre **ARMEMENT/DESARMEMENT** doit être changé de **NON TRANSMIS** à **ALARME /FIN**.

Comment modifier l'état de transmission des événements

Deux Méthodes :

- Lors de la programmation initiale, juste après APPELS DE TESTS CYCLIQUES, le clavier demande :

MODIF. ETAT/CODE
TELESURVEILLEUR

Appuyez sur la touche OK ou YES pour accéder au menu **MODIF. ETAT DE TRANSMISSION**

- Après l'installation initiale, en utilisant un clavier déporté :

Utilisez les flèches de direction   pour accéder au menu :



CONFIGURATION (niveau 4) >

PARAM. CONNEXION FRONTEL >

PARAMETRES TELESURVEILLANCE >

MODIF. ETAT DE TRANSMISSION

Puis :

Utilisez les flèches   pour trouver le type d'événement à modifier. Appuyez sur OK ou YES pour éditer l'élément puis sur les flèches de direction pour choisir l'option de transmission.

Appuyez sur la touche OK ou YES pour enregistrer l'option.



6. CODES ERREUR 2G3G

Les fonctions de sécurité des cartes SIM utilisées avec les centrales de commande Videofied doivent être désactivées.
 Le code PIN de la SIM doit être désactivé ou paramétré comme 0000.

Vous trouverez ci-dessous la liste des codes d'erreur pouvant s'afficher pendant le test de niveau 2G3G.

NIVEAU 2G3G :
 ERREUR XXX

En cas d'erreur 2G3G pendant la programmation initiale, nous vous conseillons de poursuivre l'installation avec l'enregistrement des détecteurs et périphériques, puis de revenir au test du niveau 2G3G une fois la configuration initiale terminée.

Codes	Erreurs
03 ou 04	Pas de couverture réseau ou pas de carte SIM insérée
003	Carte SIM non détectée/non insérée
010	SIM non insérée
011	Code PIN -> <i>Le code PIN doit être désactivé</i>
012	Code PUK nécessaire, Carte SIM bloquée
013	Carte SIM défectueuse
014	Carte SIM occupée
015	Erreur sur SIM
030, 043, 057, 102, 132, ...	<ul style="list-style-type: none"> Pas de couverture réseau ou pas de carte SIM active/provisionnée Erreur typographique dans le code APN, le nom d'utilisateur ou le mot de passe, ou service 2G3G non activé Carte SIM non activée

Nous vous fournissons cette liste d'erreurs 2G3G à titre indicatif. **Cette liste n'est pas exhaustive.** Les événements ou les codes peuvent être soumis à modification.

Cependant la grande majorité des erreurs 2G3G ont les causes suivantes :

- Délai d'activation Carte SIM:**
 Certains opérateurs ont un délai pouvant aller jusqu'à 48 heures pour activer la transmission des données sur une carte SIM.
 Veuillez à contrôler la bonne activation de la carte avec votre fournisseur avant l'installation.
- Code APN, nom d'utilisateur ou mot de passe erronés :**
 Chaque fournisseur a des identifiants 2G3G spécifiques à leur carte SIM.
 Veuillez à entrer des identifiants corrects dans le système. *Attention, les majuscules/minuscules doivent être respectées pour chaque paramètre.*
- Réseau 2G3G insuffisant :**
 La centrale ne parvient pas à trouver un réseau, retestez le niveau 2G3G en déplaçant la centrale à un autre emplacement du site d'installation.
 Vous pouvez également consulter votre fournisseur de carte SIM pour des informations sur l'état du réseau 2G3G sur le site d'installation.



7. CERTIFICATIONS ET NOTES DE SÉCURITÉ

Certifications

868MHz (WIP 210/220/230 et W 210)



Conforme à l'annexe IV de la Directive R&TTE 1999/5/CE

NF&A2P - 2 boucliers – suivant le référentiel NF324-H58



**Matériels de sécurité électroniques, détection d'intrusion
CENTRALE D'ALARME + TRANSMETTEUR**

Marque commerciale :	Référence Produits :	N° de Certification :
Videofied	Centrale WIP210	
Videofied	Centrale WIP220	
Videofied	Centrale WIP230	
Videofied	Centrale W210	

Normes :

NF EN50131-1: 2007 - Grade 2 – Classe II

NF EN50131-3: 2009 - Grade 2

& **RTC 50131-3:** 2009

NF EN50131-5-3: 2005 - Grade 2

NF EN50131-6: 2008 Grade 2 – Type B

& **RTC 50131-6:** 2008

NF C 48-212: 2004

NF EN50130-4: 1995; A1:1998; A2:2003

NF EN50130-5: 1998 Classe II

Organisme certificateur :

CNPP Cert.

Route de La Chapelle Réanville CS22265

F—27950 SAINT MARCEL

Tel : +33(0)2.32.53.63.63

Fax: +33(0)2.32.53.64.46

Sites Internet : <http://www.cnpp.com>

Email : certification@cnpp.com

Organisme certificateur :

AFNOR Certification

11, rue François de Pressensé

93571 Saint Denis La Plaine Cedex

Tel : +33(0)1.41.62.80.00

Fax: +33(0)1.49.17.90.00

Sites Internet : <http://www.afnor.org>

et <http://www.marque-nf.com>

Email : certification@afnor.org

915MHz (WIP 620 /630)



UL 1610

USA FCC (Part 15C, 22H, 24E and 27)

Canada IC (RSS-210 Issue 8, RSS-132, RSS-133 and RSS-139)

920MHz (WIP 720/730)



Australia A-Tick

(AS/NZS4268, AS/CHS42 and AS/NZS 60950)



Ce symbole, apposé sur le produit ou sur son emballage, indique que ce produit ne doit pas être traité avec les déchets ménagers. Il doit être remis à un point de collecte approprié pour le recyclage des équipements électriques et électroniques. En s'assurant que ce produit est bien mis au rebut de manière appropriée, vous aiderez à prévenir les conséquences négatives potentielles pour l'environnement et la santé humaine. Le recyclage des matériaux aidera à préserver les ressources naturelles. Pour toute information supplémentaire au sujet du recyclage de ce produit, vous pouvez contacter votre municipalité, votre déchetterie ou la société qui a installé le produit.



Notes de sécurité / (EN) Security notes / (DE) Hinweise zur Sicherheit

Français

- Retirez la batterie avant toute opération de maintenance !
- Attention ! Il y a un risque d'explosion si la batterie utilisée est remplacée par un mauvais modèle !
- Respectez la polarité lors de la mise en place de la batterie !
- Ne jetez pas la batterie usagée ! Ramenez-la à votre installateur ou à un point de collecte spécialisé.

English

- Remove the battery before any maintenance !
- WARNING, there is a risk of explosion if a battery is replaced by an improper model !
- Observe polarity when setting up the battery!
- Do not throw the battery when it is used! Dispose of it properly according to Lithium Metal requirements

Deutsch

- Batterien vor jeglichen Wartungsarbeiten entfernen!
- Vorsicht, es besteht Explosionsgefahr, wenn eine Batterie durch eine Batterie falschen Modells ersetzt wird!
- Achten Sie beim Einsetzen der Batterie auf die Polung!
- Entsorgen Sie Batterie nicht im normalen Haushaltsmüll! Bringen Sie Ihre verbrauchten Batterie zu den öffentlichen Sammelstellen.

FCC Regulatory Information for USA and CANADA

FCC Part 15.21 Changes or modifications made to this equipment not expressly approved by RSI Video Technologies may void the FCC authorization to operate this equipment.

FCC Part 15.105 Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- > Reorient or relocate the receiving antenna.
- > Increase the separation between the equipment and receiver.
- > Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- > Consult the dealer or an experienced radio/TV technician for help.

Radio frequency radiation exposure information according 2.1091 / 2.1093 / OET bulletin 65

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions:

- 1 This device may not cause harmful interference, and
- 2 This device must accept any interference received, including interference that may cause undesired operation.

Cet appareil est conforme à la Partie 15 des réglementations de la FCC et avec la norme RSS-210 de l'Industrie Canadienne.

Son fonctionnement est soumis aux deux conditions suivantes :

- 1 Cet appareil ne doit pas causer d'interférences nuisibles et
- 2 Cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant entraîner un fonctionnement indésirable.



8. CARACTÉRISTIQUES TECHNIQUES

PROPRIÉTÉS ÉLECTRIQUES

Alimentation	
W210 / WIP 210 / WIP 220 / WIP 230	
	Connecteur Mini-USB 5V _{DC} /1A
Adaptateur AC/DC (110/230V _{AC} /50-60 Hz) disponible (WPS100)	
WIP 620 / WIP 630 / WIP 720	
	Connexion filaire 12V _{DC} /1A

Alimentation de secours	
Technologie batterie	Lithium-ion 3.7V rechargeable
Tension batterie (100% de charge)	4.1 V
Seuil de batterie basse	3.95 V
Autonomie garantie après seuil de batterie basse atteint	36h
Consommation moyenne en veille	600 µA
Consommation maximale	1 A

Technologie RF S2View®	
Type radio	RF Bidirectionnelle
Fréquence de fonctionnement	868MHz - WIP210/220/230 - W210 (Europe, Afrique du Sud, Asie) 915MHz - FHSS - WIP620/630 (USA, Canada, Amérique du Sud) 920MHz - FHSS - WIP720/730 (Australie, Amérique du Sud)
Sécurité des transmissions	Cryptage par algorithme AES
Détection du brouillage radio	Oui
Supervision	Oui
Antenne radio	intégrée

Détection vandalisme et sabotage	
Autoprotection	Arrachement et ouverture

BOITIER

Caractéristiques physiques et environnementales	
Température de fonctionnement	-10°/+55°C
Humidité relative maximale	75%, sans condensation
Indice de protection	IP31 / IK06
Matériau	ABS—ULV0

Dimensions	
Centrale	143 mm x 200 mm x 44mm

Installation / Montage	
Centrale / Base	Deux vis pour la fermeture du couvercle Trois vis fixent la base de la centrale au mur

TRANSMISSION

Transmetteur	
Type de transmetteur	2G & LAN Ethernet (WIP210) 2G (W210) LAN Ethernet (WIP220 / WIP 620 / WIP 720) 3G & LAN Ethernet (WIP230 / WIP 630 / WIP 730)
Protocole Sécurité	Frontel
Pile IP	TCP/IP
Transmission vidéo	Par protocole Frontel au centre de télésurveillance ou aux serveurs App
Antenne 2G3G	Intégrée

Modules optionnels	
Transmission Wi-Fi	WWB100 (WLAN 802.11 b/g/n)
Entrée/Sorties filaires	WIO100 (hors certification NF&A2P)
Sirène filaire	WIS100

Vidéo	
Format vidéo	WMV ou MPEG
Images par seconde	5
Taille de l'image	320x240 ou 640x480 pixels
Durée vidéo	4 à 12 secondes

Divers	
Programmation	Clavier alphanumérique
Périphériques par système	24 maximum
Badges/Codes d'accès	50 maximum
Modes d'armement	4
Nombre de zones	4
Journal des événements	4000 événements stockés sur mémoire flash

EMEA SALES

23, avenue du Général Leclerc
92340 BOURG-LA-REINE
FRANCE
E-Mail : emeasales@rsivideotech.com

North American Headquarters

1375 Willow Lake Blvd, Suite 103
Vadnais Heights, MN 55110
USA
E-Mail : usasales@rsivideotech.com

