

# Centrale du système de sécurité JA-100K

La centrale est un élément du système de sécurité JABLOTRON 100. Considérée comme la plus petite centrale de la série JA-10xK, elle est conçue pour protéger des locaux de petite et moyenne dimension. Le système de sécurité propose de nombreuses options de configuration, y compris des profils du système pour aisément répondre aux exigences de sécurité de niveau 2.

La centrale est compatible avec des périphériques BUS et/ou sans fil (en cas d'équipement avec un module radio). Il est recommandé dans le système de n'utiliser que des périphériques de la gamme JABLOTRON 100. Le cas échéant, il est impossible de garantir le bon fonctionnement du système.

**Attention :** le système de sécurité JABLOTRON 100 ne peut être installé que par un technicien qualifié muni d'un certificat en vigueur émis par un distributeur agréé.

**Le manuel est destiné à des techniciens qualifiés et s'applique au micrologiciel de la centrale LJ60421 et à la configuration du logiciel F-Link 1.6.0 ou supérieure.**

## Table des matières

1	Description de base et définitions .....	3
1.1	Exigences de configuration du système de base .....	6
1.2	Codes d'accès et leur paramétrage par défaut .....	7
1.2.1	Modification des codes d'accès .....	8
1.2.2	Codes d'accès de sécurité et périphériques RFID .....	8
1.3	Contrôle régulier du système (maintenance) .....	9
2	Dimension du système .....	10
2.1	Configuration et répartition .....	10
2.2	Commande du système .....	10
3	Paramètres utilitaires de la centrale JA-100K .....	11
3.1	Description de la centrale JA-100K .....	11
3.2	Voyants LED de signalisation de la carte de la centrale .....	13
3.3	Connecteurs supplémentaires sur le circuit de la centrale .....	13
3.4	Bornes de connexion sur le circuit de la centrale .....	13
4	Avant l'installation du système .....	14
5	Installation des périphériques BUS .....	14
5.1	BUS JA-100 .....	15
5.2	Câbles du BUS .....	15
5.3	Longueur du BUS et nombre de périphériques connectés .....	15
5.4	Exemple de calcul de consommation du BUS en cas d'alimentation de secours du système .....	16
5.5	Besoins en alimentation électrique .....	16
6	Utilisation des périphériques sans fil .....	17
6.1	Installation du module radio JA-111R .....	17
6.2	Installation de périphériques sans fil - mode d'inscription .....	18
7	Activation du système .....	18
8	Configuration du système .....	18
8.1	Profils du système .....	19
8.2	Modes de fonctionnement de la centrale .....	22
8.3	Autorisation des utilisateurs .....	23
8.4	Paramètres en option du système (F-Link - onglet Paramètres) .....	24
8.4.1	Inscription et effacement des périphériques .....	24
8.4.2	Liste des réactions applicables .....	26
8.4.3	Limitation des fausses alertes .....	27
8.5	Types d'alarmes .....	27
8.5.1	Alarme d'intrusion .....	28
8.5.2	Alarme de sabotage .....	28
8.5.3	Alarme d'incendie .....	28
8.5.4	Alarme de détresse .....	29
8.5.5	Alarme 24 heures .....	29
8.6	Défaillances du système .....	29
8.7	Défaillance provoquée par la perte d'un périphérique .....	30
9	Options de commande du système .....	31
9.1	Méthode d'autorisation .....	31
9.2	Commande du système par le clavier .....	32
9.3	Commande du système par télécommande .....	34
9.4	Commande du système par un calendrier .....	34
9.5	Commande du système via le menu vocal du transmetteur supplémentaire (GSM / PSTN) .....	36

9.6	Consignes SMS .....	38
9.7	Contrôle du système via F-Link.....	40
9.8	Commande via l'application Internet MyJABLOTRON.....	40
9.9	Commande via l'application mobile MyJABLOTRON .....	41
9.10	Commande d'accès sous contrainte .....	41
9.11	Obstacles empêchant l'armement du système .....	42
9.12	Échec de l'armement .....	43
9.13	Tableau récapitulatif des groupes d'évènements signalés aux utilisateurs.....	43
9.14	indication acoustique du système .....	44
9.15	Désactivation et blocage des options.....	45
9.15.1	Désactivation.....	45
9.16	Fonctions non relatives à une alarme - Fonctions des sorties PG .....	45
10	Armement du système avec le logiciel F-Link.....	46
10.1	Démarrage du programme F-Link et configuration de la dimension du système .....	46
10.2	Onglet Sections.....	47
10.3	Onglet Périphériques .....	47
10.3.1	Configuration du clavier.....	48
Onglet Paramétrage :	.....	51
10.3.2	Paramètres de la sirène interne .....	52
10.4	Onglet Utilisateurs.....	53
10.5	Onglet Sorties PG .....	54
10.5.1	Carte d'activation des sorties PG .....	55
10.6	Onglet Rapports aux utilisateurs .....	56
10.7	Onglet Paramètres.....	58
10.8	Onglet Calendriers .....	61
10.9	Onglet Communication .....	62
10.9.1	Paramètres JA-190Y .....	63
10.9.2	Redémarrage GSM .....	64
10.9.3	Paramètres LAN.....	64
10.9.4	Paramètres PSTN .....	65
10.10	Onglet Télésurveillance (ARC) .....	66
10.10.1	Exigences pour la configuration des voies de transmission vers une télésurveillance .....	67
10.10.2	Voies de transmission.....	67
10.10.3	Codes CID et SIA JABLOTRON 100 .....	67
10.11	Onglet Diagnostic .....	70
11	Autres options F-Link.....	71
11.1	Commande du système par F-Link .....	71
11.2	Historique événementiel : .....	71
11.3	Paramétrage du système .....	72
11.4	Signal RF .....	73
11.5	Service .....	74
11.6	Rafraîchir .....	74
11.7	Mode en ligne .....	74
11.8	Internet.....	74
11.9	Informations relatives à l'installation .....	75
11.10	Mise à jour du micrologiciel .....	76
11.11	Historique des configurations .....	76
12	Réinitialisation de la centrale .....	76
13	Mises à jour du micrologiciel.....	77
13.1	Règles générales de mise à jour du micrologiciel (FW).....	77
13.2	Mises à jour du micrologiciel de la centrale et des périphériques connectés au BUS.....	77
13.3	Mises à jour du micrologiciel pour les périphériques sans fil .....	78
13.4	Contrôle après une vérification du micrologiciel.....	79
13.5	Fenêtre d'informations .....	79
14	Informations supplémentaires.....	80
14.1	Tableau récapitulatif de la consommation en courant des périphériques BUS .....	80
14.2	Dimensions des centrales.....	80
15	Prise en charge du système par l'utilisateur .....	81
16	Caractéristiques techniques .....	82

# 1 Description de base et définitions

**Architecture modulaire** - permet de configurer le système pour des installations, des dimensions et des besoins spécifiques de l'utilisateur.

**Mise à jour du micrologiciel (FW)** - procédure de mise à jour vers une nouvelle version du micrologiciel dans le système contenant de nouvelles fonctions, des améliorations et des adaptations. Nous vous recommandons de vérifier la mise à jour du micrologiciel au cours de toute installation ainsi que lors des contrôles de maintenance réguliers. En plus de la mise à jour micrologicielle de la centrale, il est nécessaire d'en faire de même avec tous les périphériques en cas de besoin (claviers, modules radio, détecteurs de mouvement avec caméra, etc...).

**Clavier de commande** - module destiné à autoriser l'utilisateur, à la commande du système et à l'indication de son état. Il se compose d'un lecteur de carte/badge RFID, d'un clavier de saisie des codes d'accès digitaux, de quatre touches fonctionnelles et d'un écran LCD. Le clavier est fourni en version BUS et sans fil.

**Indicateur du système** - voyant LED carré dans le coin supérieur gauche du clavier ; l'indication est réalisée en 3 couleurs : vert = OK, centrale sans défaillance ; rouge = alarme et mémoire d'alarme ; jaune = défaillance du système, etc.

**Indicateur de section** - voyants LED marqués avec des lettres représentant les sections A, B, C, D et la couleur (rouge, jaune et vert) indiquant le statut de toutes les sections du système.

**Touche fonctionnelle** - touche universelle programmable / de commande / d'indication sur le clavier intérieur. Il existe 4 touches fonctionnelles disponibles marquées A, B, C, D. Chaque touche fonctionnelle individuelle dispose d'une signalisation intuitive par rétroéclairage de couleur différente, tout en proposant également la commande du système (sections choisies).

**Types d'alarme** - le système peut réagir aux événements tels qu'une intrusion, une détresse, un sabotage, un incendie, une fuite de gaz et une inondation. L'utilisation de détecteurs appropriés permet également de signaler d'autres dangers (un individu se déplaçant dans le jardin, la manipulation d'un objet protégé, etc.). Des moyens visant à réduire l'occurrence des fausses alertes sont disponibles. Les détecteurs situés dans un environnement difficile d'un point de vue structurel ou opérationnel peuvent être armés de sorte que leur activation soit confirmée par un autre détecteur.

**Vérification visuelle de l'alarme** - les périphériques de vérification photo (détecteurs caméra, caméras de vérification photo) peuvent automatiquement prendre et envoyer des clichés de tout ce qui se passe dans la zone surveillée.

**Protection personnelle** - en cas de détresse, de problème de santé ou d'incendie, l'utilisateur peut demander de l'aide (en appuyant sur la touche d'un clavier, en saisissant un code de détresse, en activant une touche de détresse ou en utilisant une télécommande sans fil).

**Commande d'accès sous contrainte** - sert au déclenchement d'une alarme silencieuse par autorisation uniquement ou par commande du système (armement, désarmement, commande PG, ...) quand un utilisateur est en présence d'un individu dangereux. Une alarme de détresse est déclenchée lors de la commande du système quand un code est saisi avec le chiffre 1 ajouté à la valeur du dernier chiffre.

**Détresse temporisée** - fonction destinée à émettre une alarme de détresse avec une temporisation permettant à l'alarme d'être stoppée. La fonction est conçue pour les utilisateurs ayant peur d'ouvrir la porte d'entrée en cas de présence d'un inconnu qui pourrait les attaquer. Ainsi, l'utilisateur active le signal de détresse temporisé avant d'ouvrir la porte et, s'il est sûr d'être en sécurité, il doit annuler la fonction avant l'expiration du délai prédéfini. La temporisation de détresse peut être définie dans les paramètres internes du périphérique spécifique utilisé pour déclencher l'alarme de détresse.

**Notification d'évènement** - le rapport de tous les événements à un centre de télésurveillance peut garantir l'intervention opportune de professionnels. Les informations peuvent également être envoyées directement aux utilisateurs par un transmetteur LAN intégré ou par un transmetteur GSM ou PSTN, via des messages SMS (GSM uniquement) ou des appels vocaux. Les rapports directs conviennent surtout pour le suivi des coupures d'électricité, des départs et des arrivées des enfants comme des employés, etc.

**Commande à distance** - un numéroteur téléphonique supplémentaire permet aux utilisateurs autorisés d'appeler le système et, à l'aide d'un menu vocal, de commander ou de vérifier le statut de l'armement. Les statuts des sections individuelles peuvent être commandés à distance au moyen de commandes SMS définies (GSM uniquement). Des consignes SMS peuvent également être utilisées pour activer ou désactiver les sorties programmables (PG). Elles peuvent également être activées par simple sonnerie (sans établir d'appel) à partir de numéros de téléphone autorisés. Le logiciel F-link est destiné aux techniciens de service pour réaliser la commande à distance. Le système peut également être commandé à distance via les applications Internet ou mobiles MyJABLOTRON ou MyCOMPANY.

**Droits d'accès des utilisateurs** - l'option détermine le niveau d'autorisation d'accès de l'utilisateur. Il est possible de modifier les droits d'accès et de commande de l'utilisateur à certains lieux protégés qui lui sont

attribués au moyen de sorties programmables (PG). L'utilisateur prouve son identité en présentant une carte sans contact ou en saisissant un code à l'aide du clavier.

**Administrateur** - (Maître) un nombre requis d'administrateurs peut être déterminé dans le système, ces derniers paramétrant les droits d'accès des utilisateurs ordinaires. Les différentes sections du site peuvent avoir des administrateurs différents. Dans les paramètres par défaut, il existe un administrateur principal du système (position 1), qui est toujours autorisé à définir les droits d'accès pour tous les utilisateurs ; les codes par défaut sont 1234 ou 123456, en fonction de l'option de longueur du code (onglet Configuration initiale) ou du profil du système prédéfini.

**Technicien de service** - code de service spécial (code par défaut 1010 ou 101010 en fonction du profil sélectionné). Avec ce code, le technicien est autorisé à configurer toutes les caractéristiques du système. Il peut y avoir plusieurs techniciens de service autorisés (si nécessaire). L'accès du technicien de service peut être sujet à l'accord préalable de l'administrateur. Le technicien du centre de télésurveillance (ci-après désigné « télésurveillance/ARC » dans les textes) représente un cas particulier d'autorisation de service. Ce technicien peut utiliser son code (menu F-Link : Paramètres / Utilisateurs / Autorisation de l'utilisateur = télésurveillance) pour verrouiller l'accès aux réglages des paramètres de communication avec la télésurveillance.

**F-Link (J-Link)** - pour programmer le système, un ordinateur doté du système d'exploitation Windows est requis (WIN XP SP3 ou supérieur). La centrale peut être localement connectée à l'ordinateur en utilisant un câble USB ou à distance à partir d'un ordinateur connecté à Internet. Toutes les caractéristiques sont définies à l'aide de l'ordinateur et du programme F-Link. Ce programme est exclusivement conçu pour les techniciens qualifiés. L'accès ne peut être accordé à un administrateur ou un utilisateur final du système. Une version simplifiée de ce programme (J-Link) est conçue à cet effet, permettant aux administrateurs système d'accéder à certains réglages (gestion des utilisateurs, diagnostics, établissement des événements programmés, lecture de l'historique événementiel).

**Mode Service** - mode dans lequel il est possible de modifier la totalité de la configuration du système. Seul un technicien de service (ou un technicien de la télésurveillance) peut accéder au système en mode Service. Cela est réalisable en utilisant un clavier avec un écran LCD, une connexion locale de la centrale et un ordinateur (avec un câble USB) ou un accès à distance via Internet. En mode SERVICE, le système n'est pas opérationnel (il ne surveille rien et ne fournit aucune fonction utilisatrice, comme par ex. la commande des sorties programmables PG). Le technicien de service peut aussi modifier une partie considérable des caractéristiques au cours du fonctionnement (sans avoir besoin de passer en mode Service).

**Commande domotique** - le système dispose de sorties programmables PG permettant d'activer et de désactiver différents périphériques. Il représente la logique du système et il commande le nombre requis de modules de sortie (périphériques affectés vers le système). Une sortie peut être commandée à l'aide d'une touche fonctionnelle du clavier, par activation de détecteurs, de télécommandes, par un événement du système (par ex. armement d'une section, déclenchement d'une alarme, ...), par une action programmée, à l'aide d'une commande SMS, par la sonnerie d'un utilisateur autorisé. L'activation d'une sortie PG peut également être bloquée par le statut d'une section ou d'un détecteur ou encore toute autre sortie PG. Hormis l'indication optique, l'activation de la sortie PG peut aussi être signalée par voie acoustique (sirène).

**Commande du verrou de porte** - un verrou de porte électrique (connecté à la sortie PG) peut être ouvert par présentation d'une carte à puce ou en saisissant un code sur le clavier. Chaque utilisateur peut être assigné à la porte qu'il est autorisé à ouvrir. Une sortie peut être bloquée par une section armée de manière à ce qu'un danger d'intrusion dans la zone soit éliminé, en cas de surveillance (armement). L'ouverture d'une porte par l'autorisation d'un utilisateur peut être enregistrée dans l'historique événementiel du système.

**Planning des événements automatiques (Calendrier)** - il est possible de programmer les sorties programmables à l'aide du calendrier hebdomadaire automatique de surveillance (armement / armement partiel / désarmement) des sections et des commandes PG (activation / désactivation, blocage / déblocage). Le calendrier annuel peut être utilisé pour définir les écarts dans les horaires du calendrier hebdomadaires (par ex. les fêtes nationales, les congés). Le calendrier annuel peut être paramétré pour l'année en cours et la suivante.

**Périphériques BUS** - ils sont connectés vers le système à l'aide d'un câble BUS (4 conducteurs). Le BUS assure l'alimentation ainsi que la communication. Les périphériques BUS (détecteurs, claviers, sirènes, etc.) nécessitent pour leur fonctionnement l'inscription sur une position (adresse) dans le système. Il existe cependant également des périphériques qui sont seulement raccordés et fonctionnent sans inscription sur une position (certains modules de sortie PG, les indicateurs de statut, les séparateurs de BUS, etc.).

**Périphériques sans fil** - afin d'assurer la communication, la centrale doit être équipée d'un module radio et les périphériques sans fil (détecteurs, claviers, sirènes, etc.) doivent être inscrits sur une position (adresse) dans le système. Il peut cependant également y avoir des périphériques dans le système qui n'occupent pas de position (ils sont utilisés uniquement pour la réception et ne communiquent pas avec la centrale), par ex. les modules de sorties PG. Pour la couverture d'une zone plus importante d'un site, il est possible d'installer jusqu'à 3 modules radio dans le système (raccordés par un câble BUS). L'activité des périphériques sans fil sélectionnés est régulièrement contrôlée par la centrale (Paramètre de supervision), qui vérifie également le statut effectif des batteries. Si la communication avec un périphérique sans fil est coupée, la centrale signale

une défaillance de communication. Les modules radio vérifient les brouillage / interférence RF sur la bande de communication du système JABLOTRON 100. Si la bande est brouillée, le système déclenche une erreur.

**Détecteurs d'intrusion** - groupe de détecteurs destinés à identifier un intrus. Cela comprend des détecteurs de mouvement, d'ouverture, de bris de verre, d'inclinaison ou de choc. Si les détecteurs sont configurés pour déclencher une alarme temporisée ou immédiate avec ses variations (par exemple répétée ou confirmée), cela détermine la façon dont le détecteur réagira à son activation. Les détecteurs d'incendie, d'inondation ou de détresse n'appartiennent pas au groupe des détecteurs d'intrusion.

**Transmetteur GSM** - fournit la connexion au réseau de téléphonie mobile et à Internet. Le système peut ainsi transmettre des données au centre de télésurveillance sous forme de canal principal ou de secours. Le transmetteur fournit l'accès à distance à la centrale par l'intermédiaire du programme F-Link, signale les événements aux utilisateurs, commande à distance le système (par menu vocal, consigne SMS).

**Transmetteur LAN** - s'il est inclus avec la centrale, il fournit un accès à distance rapide par le logiciel F-Link (J-Link) et peut également transmettre des données à un centre de télésurveillance équipé d'une technologie de réception spécifique à l'IP du protocole Jablotron. Dans les réglages de la centrale, il est possible de sélectionner les types de communication primaire / de secours.

**PSTN - Transmetteur téléphonique** - il est possible de l'installer dans la centrale comme module optionnel pour les lignes téléphoniques analogiques PSTN. Il est capable de transmettre des données au centre de télésurveillance aux formats téléphoniques classiques (CID, SIA DC-05 et SIA DC-03). Il est également capable de signaler les événements aux utilisateurs (par un appel) et permet la commande à distance du système via le menu vocal. Le module téléphonique est généralement utilisé comme élément de secours pour la communication LAN. Le module peut également communiquer avec une ligne téléphonique simulée par un émetteur radio.

**Section** - le système peut être divisé en zones (sections) pouvant être armées ou désarmées indépendamment. Une section peut également être un appartement particulier dans un immeuble résidentiel, un magasin dans un centre commercial ou un département dans une entreprise ou un immeuble de bureaux. L'interdépendance de la section peut être définie de manière à rappeler qu'elle est protégée par la centrale en propre (droits d'accès, rapports, affichage des éléments sur le clavier, indication acoustique, ...).

**Section commune** - section distincte conçue pour être une sous-section pour un groupe sélectionné d'autres sections. Lorsque la section principale est armée en dernier, la section commune est alors armée automatiquement. Lorsque la section principale est désarmée, la section commune est alors également désarmée. Elle a pour objectif de sécuriser des espaces tels que des halls, des toilettes, des cuisines dans les entreprises, etc.

**Armement partiel** - paramétrable séparément pour chaque section. Si l'armement partiel est activé, le système ne réagit pas aux détecteurs d'intrusion qui ont une réaction armée « interne » (à savoir surveiller l'espace intérieur). Ainsi, par exemple, le mouvement est autorisé dans la partie résidentielle de la maison, mais le système déclenche une alarme ou une temporisation d'accès en cas d'entrée par une porte ou de mouvement dans un garage, une cave, etc. Si une section est complètement armée, elle réagit à l'activation de tous les détecteurs qui lui sont attribués.

**Dérivation** – le statut actif des périphériques ou une défaillance existante dans le système sont confirmés lors de l'armement du système. Le statut des entrées actives est ignoré après une dérivation jusqu'au passage en mode veille (désactivation). Le passage des entrées en mode veille (désactivées) est inclus avec la surveillance. En contournant les défaillances du système, l'utilisateur confirme qu'elle a été reconnue, mais ne modifie pas son statut (une défaillance est toujours présente dans le système). La fonction dépend de l'option donnée par le paramètre Méthodes d'armement.

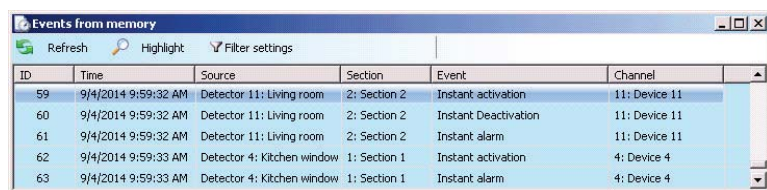
**Blocage** - blocage de l'entrée d'un périphérique actif pour activer une sortie PG ou pour réaliser toute activation de réaction. Réaliser le blocage manuellement avec le clavier, F-Link, J-Link ou l'application MyJABLOTRON. Il est ainsi possible de bloquer une entrée de périphérique à tout moment en dehors de la procédure de réglage. La fonction dépend de l'option donnée par le paramètre Méthodes d'armement.

**Dérivation automatique** - dérivation automatique de la réaction du système vers un périphérique en fonction des options. Activation d'entrée après 3 activations ou 3 alarmes (en option, par le logiciel F-Link, onglet Paramètres), défaillances après 3 activations également.

**Désactivation** - cette option sert à désactiver temporairement et manuellement des sections, des périphériques, des utilisateurs, des sorties programmables (PG) ou des actions programmées sélectionnés. La section à laquelle la centrale est attribuée (toujours la section 1) ne peut être désactivée, tout comme le code de service en position 0 et le code de l'administrateur en position 1. Pour les périphériques, nous distinguons les notions de blocage (ne concerne que l'activation de l'entrée) et de désactivation du périphérique, voir le chapitre 9.15 Désactivation et blocage des options.

**Méthodes d'armement** - sélection du niveau de procédure d'armement du système. Les options vont du niveau le plus faible, où le système ne vérifie rien (armement systématique), au niveau le plus fort, où le système ne permet pas l'armement pour tout périphérique activé (par exemple une fenêtre ouverte), voir le chapitre 9.9 Obstacles empêchant l'armement du système.

**Historique évènementiel** - Le système enregistre les évènements survenus dans sa mémoire. Le contenu de la mémoire peut être visualisé à partir du logiciel F-Link, en utilisant la touche « Historique évènementiel » ou à partir du clavier. Le début d'un évènement est généralement enregistré comme une activation (statut d'un périphérique, défaillance, sabotage, etc.) et la fin d'un évènement comme une désactivation. Les statuts des sections sont enregistrés sous la forme Armer/Désarmer, les statuts de l'alarme en tant que Alarme/Fin d'alarme, Alarme silencieuse ou Annulation de l'alarme.



ID	Time	Source	Section	Event	Channel
59	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant activation	11: Device 11
60	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant Deactivation	11: Device 11
61	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant alarm	11: Device 11
62	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant activation	4: Device 4
63	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant alarm	4: Device 4

Activation et désactivation de l'aimant  
Début et fin de l'alarme

Certains évènements peuvent avoir uniquement un enregistrement d'activation (par ex. nouvelle image, alarme de détresse, configuration modifiée).

**Carte mémoire microSD** - la centrale utilise une carte microSD en tant que support mémoriel. Après avoir connecté la centrale à un PC via un câble USB, deux lecteurs seront affichés dans le gestionnaire de fichiers. FLEXI\_CFG et FLEXI\_LOG. La capacité de la carte fournie est de 4GB (SD/SD-HC) ou supérieure. Avant d'utiliser une nouvelle carte SD, réinitialiser la centrale - pour les paramètres par défaut, se référer au chapitre 12 Réinitialisation de la centrale. Puis mettre à jour le micrologiciel, voir le chapitre 13 Mises à jour du micrologiciel. Cette procédure sauvegarde tous les fichiers requis (textes par défaut, messages vocaux, etc..) sur la carte SD.

**FLEXI\_CFG** - contient les répertoires et les fichiers masqués des paramètres du système. Ne pas modifier le contenu du disque, il existe un risque de perte de fonctionnalité du système.

**FLEXI\_LOG** - Contient le répertoire SAUVEGARDE, PHOTO et le fichier FLEXILOG.TXT, où tous les évènements du système sont enregistrés. Les données sélectionnées du fichier peuvent être visualisées dans F-Link / Historique évènementiel. Le répertoire PHOTO est utilisé pour stocker les fichiers IMGnnnn.JPG qui ont été envoyés vers la centrale depuis les périphériques dotés de caméra (par ex. à partir du détecteur de mouvement avec caméra JA-160PC). Les deux types de fichiers (txt et jpg) sont stockés sous une forme cryptée et leur contenu ne peut normalement être visualisé avec un programme gérant les aperçus texte et image. Leur contenu ne peut être visualisé que si le programme F-Link est lancé simultanément sur le PC et l'autorisation d'accès Service, Administrateur ou Télésurveillance est confirmée en saisissant le code correspondant. Les évènements sont enregistrés dans le fichier FLEXILOG.TXT jusqu'à une taille de 10 MB, puis le fichier est renommé FLEXILOG.OLD et un nouveau fichier est créé.

**Verrouillage SIM** - fonction de la centrale qui peut être activée par la télésurveillance correspondante lors de son enregistrement sur MyJABLOTRON. Si cette fonction est activée et après le remplacement de la carte SIM utilisée par une autre, le système supprimera automatiquement le paramétrage de la télésurveillance (l'enregistrement du système sur MyJABLOTRON devra être renouvelé). Cette étape sert à prévenir la transmission d'informations non désirées à la télésurveillance à partir d'une carte différente de celle qui a été enregistrée à cet effet et à partir de laquelle le paramétrage a été réalisé.

## 1.1 Exigences de configuration du système de base

Elles adhèrent aux exigences des normes en vigueur lors de la conception du système. Le manuel de base pour la conception des systèmes de sécurité, leur mise en service ainsi que leur maintenance sont décrits dans les spécifications techniques CLC/TS 50131-7. Ce document doit être appliqué aux systèmes installés et classés conformément à la norme EN 50131-1, niveau de sécurité 2.

La centrale JA-100K peut être configurée pour avoir un comportement conforme à un **profil du système** prédéfini ainsi que d'autres conditions indiquées qui sont conformes aux profils suivants :

1. **Par défaut** Profil prédéfini par défaut, tous les paramètres du système sont facultatifs.
2. **N50131-1, niveau 2** Profil prédéfinissant certains paramètres spécifiques du système (variables pour la centrale, les claviers, les sirènes, etc.) conformément aux exigences de la norme donnée en vigueur pour le niveau de sécurité 2.
3. **INCERT T031, niveau 2** Profil prédéfinissant certains paramètres spécifiques du système (variables pour la centrale, les claviers, les sirènes, etc.) conformément aux exigences de la norme donnée (directive Belgique T031) en vigueur pour le niveau de sécurité 2. Le profil est basé sur le profil EN 50131-1, niveau 2 et est très apprécié du fait de la sécurité accrue des locaux contre le sabotage et l'intrusion.

En ce qui concerne les rapports d'alarme et compte tenu du profil sélectionné en vigueur pour le niveau de sécurité 2, la centrale doit être au minimum installée conformément à une des configurations suivantes :

Méthodes de signalement	Profil du système et configuration adéquate		
	Défaut	EN 50131-1, niveau 2	INCERT T031, niveau 2
Signalement d'alarme local	<b>Recommandé :</b> JA-110A ou JA-163A Ou JA-110A pré-réglé comme sirène externe	<b>Requis :</b> JA-110A ou JA-163A Ou JA-110A pré-réglé comme sirène externe	<b>Requis :</b> JA-110A ou JA-163A ou JA-110A pré-réglé comme sirène externe
Signalement d'alarme à distance - canal principal (voie de communication principale vers la télésurveillance)	<b>Recommandé :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact	<b>Recommandé :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact	<b>Requis :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact
Signalement d'alarme à distance - canal de secours (voie de communication de secours vers la télésurveillance)	<b>Recommandé :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact	<b>Recommandé :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact	<b>Recommandé :</b> LAN ou canal GSM / GPRS avec protocole IP ou ligne PSTN avec protocole d'identification de contact

**REMARQUE 1 :** le système d'alarme JABLOTRON 100 est conçu pour se conformer aux normes mentionnées dans les profils du système individuels. Il faut au moins respecter les exigences de base relatives aux méthodes de signalement d'alarme et aux indications d'avertissement. Les méthodes de signalement données par ce tableau sont basées sur les normes EN 50131-1 + A1+A2, exigences, paragraphe 8.6.4, tableau 10. Les exigences détaillées concernant les propriétés de la voie de communication vers la télésurveillance sont mentionnées dans le chapitre sur les paramètres du transmetteur.

**REMARQUE 2 :** le terme Voie de communication concerne un moyen de transmission physique, par exemple des câbles métalliques, des fibres / câbles optiques ou une transmission radio.

**REMARQUE 3 :** une voie de communication de secours doit être réalisée en utilisant un support de transmission physique différent du support principal. Il n'est pas possible de combiner par exemple la technologie GSM et un dispositif LAN basé sur un réseau WIFI. Les deux voies sont des transmissions radio qui peuvent être brouillées simultanément (sabotage).

**\*Attention :**

- S'assurer que tous les périphériques LAN fournissant une connexion au réseau Internet ont une alimentation de secours !
- L'accès aux périphériques LAN ou à d'autres panneaux de communication ou d'échanges devrait être restreint pour les personnes non autorisées !

Lors de la conception du système, il faut tenir compte du fractionnement en sections et des temporisations d'entrée prédéfinies pour pouvoir paramétrer la définition des zones temporisées. Il peut y avoir 2 types de zones temporisées (temporisation et porte de garage), chacune d'elle ayant sa propre minuterie pour prédéfinir les temps d'entrée et de sortie.

Les itinéraires des entrée / sortie, à savoir le chemin allant de la porte d'entrée au clavier de commande, doivent être les plus courts possible. Le clavier (périphérique de commande principal du système de sécurité) devrait être placé près de la porte d'entrée, compte tenu du fait que l'utilisateur devrait pouvoir désarmer le système en 30 secondes à compter de l'entrée dans les locaux protégés. Cette exigence oblige à utiliser plusieurs claviers dans les locaux protégés et des voies d'accès multiples.

## 1.2 Codes d'accès et leur paramétrage par défaut

Une autorisation nécessaire s'obtient par l'utilisation d'un code valide ou la présentation d'une carte ou d'un badge RFID sur le module d'autorisation (clavier) pour pouvoir utiliser le système (armement, désarmement ou vérification du statut de certaines sections ou périphériques). Selon le niveau d'autorisation de l'utilisateur spécifique, le système présente toutes les informations et permet la commande du système appropriée à vos droits d'accès. Un technicien de service, accédant au système à partir du programme F-Link (J-Link), à distance avec l'application MyJABLOTRON ou par menu vocal, doit également être autorisé en saisissant un code d'accès valide.

Le code d'accès peut comporter 4 ou 6 chiffres (en fonction du profil du système sélectionné).

Codes pour JA-100K	Profil par défaut (codes à 4 chiffres)	Profil EN50131-1, (Codes à 6 chiffres)	INCERT T 0xx (Codes à 6 chiffres)
Format du code :	nnnn	nnnnnn	nnnnnn
Service (code par défaut) :	1010	101010	101010
Administrateur (code par défaut) :	1234	123456	123456

**Avertissement** : lorsque le paramétrage du profil du système est modifié, tous les codes définis par l'utilisateur sont effacés et les codes par défaut (Service, Administrateur) sont prédéfinis aux valeurs par défaut. L'ensemble des cartes / badges RFID restent définis dans le système.

Le code Service par défaut est automatiquement implémenté par le programme F-Link et n'est donc pas exigé par le programme, de la première activation jusqu'à sa modification. Toutefois, pour des raisons de sécurité et une fois l'installation terminée, il est impératif de modifier tous les codes par défaut.

### 1.2.1 Modification des codes d'accès

La création ou la modification des codes d'utilisateur ou des badges / cartes RFID peuvent être réalisées par l'administrateur du système ou un technicien de service. De nouveaux code ou badge/carte RFID peuvent être attribués à l'utilisateur avec une autorisation prédéfinie. Seul le technicien de service a le droit de créer un tel utilisateur en utilisant le logiciel F-Link.

**Les codes d'accès peuvent être ajoutés et modifiés par :**

- L'administrateur à partir d'un clavier LCD (condition : le PC doit être déconnecté de la centrale, sans connexion à distance ou locale et l'utilisateur doit être prédéfini avec l'autorisation requise).
- Un technicien de service avec le logiciel F-Link (condition : le paramètre activé Service et Télésurveillance peut commander le système).
- Un utilisateur qui n'a pas l'autorisation de modifier son propre code.

Chaque code d'utilisateur peut être réglé sur une valeur arbitraire compte tenu de la longueur de code donnée par le profil du système sélectionné, mais la centrale empêche l'utilisation d'une valeur de code qui a déjà été utilisée dans le système pour un autre utilisateur. Le ou les administrateurs Système sont uniquement et entièrement responsables de l'inscription et l'édition des codes d'utilisateur.

### 1.2.2 Codes d'accès de sécurité et périphériques RFID

La centrale autorise pour chaque utilisateur l'inscription d'un code (en fonction du profil sélectionné) et d'un badge / d'une carte RFID pour l'autorisation de l'utilisateur. Une autorisation est requise lorsque le système fonctionne avec un clavier. Le niveau de sécurité est correspondant et peut être représenté par des nombres dans le tableau suivant.

**Le calcul des combinaisons de code pour 1 utilisateur est illustré dans les exemples suivants :**

Paramètres de la centrale	Codes à 4 chiffres	Codes à 6 chiffres
Commande d'accès sous contrainte - ARRÊT Autorisation standard - ARRÊT	$= 10^4$ - (Nombre d'utilisateurs stockés dans le système - 1)	$= 10^6$ - (Nombre d'utilisateurs stockés dans le système - 1)
Commande d'accès sous contrainte - MARCHÉ Autorisation standard - MARCHÉ	$\leq 10^4$ - ((Nombre d'utilisateurs stockés dans le système - 1) * 3)	$\leq 10^6$ - ((Nombre d'utilisateurs stockés dans le système - 1) * 3)
Commande d'accès sous contrainte - ARRÊT Double autorisation - ARRÊT	$= 10^8 * (10^4$ - (Nombre d'utilisateurs stockés dans le système - 1))	$= 10^8 * (10^6$ - (Nombre d'utilisateurs stockés dans le système - 1))
Commande d'accès sous contrainte - MARCHÉ Double autorisation - MARCHÉ	$\leq 10^8 * (10^4$ - ((Nombre d'utilisateurs stockés dans le système - 1) * 3))	$\leq 10^8 * (10^6$ - ((Nombre d'utilisateurs stockés dans le système - 1) * 3))
Utilisation de la carte RFID uniquement sans code numérique	$= 10^8 = (100\ 000\ 000)$	$= 10^8 = (100\ 000\ 000)$

#### Exemple :

Profil sélectionné : Par défaut ~ Codes à 4 chiffres  
 Nombre d'utilisateurs stockés dans le système : 33 max.  
 Commande d'accès sous contrainte : Désactivée  
 Nombre de combinaisons de code :  $10^4 - 33 = 9\ 967$  combinaisons / utilisateurs (avec 33 utilisateurs)

#### Augmentation du niveau de sécurité des codes :

- Sélectionner un code à 6 chiffres (profil du système EN-50131-1, INCERT).
- Sélectionner le niveau « Double autorisation », où un code d'accès valide standard et des badge/carte RFID doivent être appliqués ensemble.

#### Protection contre une tentative de décodage :

La centrale compte les tentatives de saisie de codes erronés et à la **10<sup>e</sup> tentative**, le système déclenche l'événement de sabotage « tentative de décodage », l'alarme est déclenchée et signale cet événement à des numéros prédéfinis. Aucun blocage supplémentaire de saisie d'autres codes dans le système n'est appliqué. Après une saisie de code valide, le compteur de saisie des codes erronés est réinitialisé et l'alarme déclenchée interrompue. Ce compteur est prédéfini sur 10 tentatives et ne peut être modifié.



### 1.3 Contrôle régulier du système (maintenance)

L'ensemble du système de sécurité nécessite un test périodique de bon fonctionnement, y compris de l'ensemble de ses éléments, mais également un nettoyage, des contrôles visuels externes (poussière et impuretés, généralement réalisés par l'utilisateur du système) et internes (toiles d'araignées, insectes, état de la batterie, etc., réalisés par le technicien de service). Certaines parties spécifiques du système peuvent réaliser un test automatique et un éventuel rapport de défaillance à la centrale, le rapport de ce statut étant fonction des paramètres. Presque toutes les étapes de la maintenance doivent être réalisées par un technicien de service pendant la vérification annuelle du système.

La batterie de secours principale est testée périodiquement plusieurs fois par minute par la centrale à l'aide d'un test de charge. Les batteries des périphériques sans fil (dans les détecteurs, les claviers, les sirènes, les télécommandes) sont automatiquement testées avec chaque transmission de test de liaison. Le système signale une batterie faible à partir de chaque périphérique inscrit, de la détection jusqu'à son remplacement, par un rapport SMS prédéfini et simultanément sur le clavier LCD. Le remplacement des batteries ne peut être réalisé que par un technicien de service. Lorsqu'une batterie est enlevée, il faut attendre quelques instants (20 secondes) pour décharger les condensateurs internes avant d'insérer une nouvelle batterie.

#### Aperçu de la maintenance recommandée / commande fonctionnelle :

Type de périphérique	Description	Qui entreprend l'action ?	Fréquence de l'action
Détecteurs d'incendie	Test fonctionnel ; informer la télésurveillance avant d'y procéder !	Administrateur	Une fois par mois
	Nettoyer la poussière et les impuretés.	Administrateur	Deux fois par an
	Vérification de la batterie (BUS et périphériques sans fil)	Technicien de service	Une fois par an
Touches de détresse	Test fonctionnel ; Informer la télésurveillance avant d'y procéder !	Administrateur	Une fois par mois
	Vérification de la batterie, mesure de la tension, état physique.	Technicien de service	Une fois par an
Détecteurs	Nettoyer la poussière et les impuretés.	Administrateur	Une fois par an
	Test fonctionnel ; test de la gamme RF pour les détecteurs sans fil. Pour les détecteurs avec caméra intégrée, tester en prenant un cliché.	Technicien de service	Une fois par an
	Vérification de la batterie, mesure de la tension de chaque batterie, état physique, etc.	Technicien de service	Une fois par an
Claviers	Nettoyer la poussière et les impuretés.	Administrateur	Deux fois par an
	Tester toutes les touches, touches fonctionnelles et capteur RFID ; tester la gamme RF pour les claviers sans fil.	Technicien de service	Une fois par an
	Vérification du statut de la batterie et du statut physique, mesure de la tension de chaque batterie, etc.	Technicien de service	Une fois par an
Sirènes	Nettoyer la poussière et les impuretés, les insectes, vérifier l'absence de pénétration de l'eau dans les circuits, etc.	Technicien de service	Une fois par an
	Test fonctionnel ; tester la gamme RF pour les sirènes sans fil.	Technicien de service	Une fois par an
	Vérifier les batteries ou les batteries de secours, mesures, état physique, mesures de la tension de chaque batterie	Technicien de service	Une fois par an
Commandes à distance (RC)é	Test fonctionnel ; gamme RF, vérification d'indication de batterie faible. Nettoyage ou remplacement du boîtier en plastique.	Administrateur ou technicien de service	Une fois par an
Statut d'alarme	Test de communication vers la télésurveillance, appels vocaux et rapports SMS.	Administrateur ou technicien de service	Une fois par an
Batterie de secours dans la centrale	Test pendant la déconnexion du secteur (AC) et mesure de la tension de la batterie de secours après 5 minutes d'absence de courant.	Technicien de service	Une fois par an
Sorties programmables (PG)	Test fonctionnel ; gamme RF des modules sans fil	Technicien de service	Une fois par an

La priorité de l'ensemble des procédures recommandées par le producteur du système ne surpasse pas celle des règlements et décrets locaux.

## 2 Dimension du système

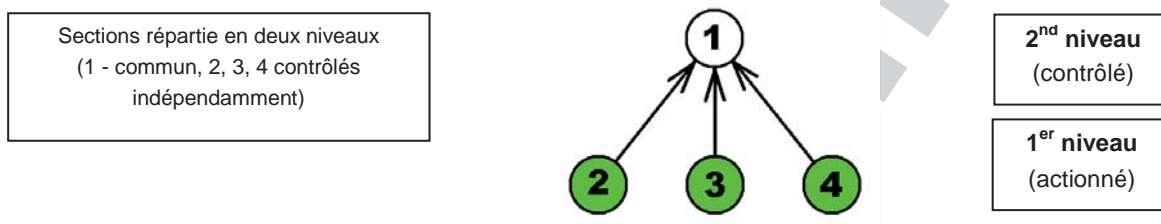
La dimension du système de sécurité peut être définie en option en fonction de la taille du site protégé et des exigences de l'utilisateur final.

La centrale peut être divisée en 4 sections (zones réglables indépendamment). Chaque périphérique possède sa propre adresse (claviers, détecteurs, sirènes) et doit être inscrit sur l'une des sections. Le nombre de périphériques, les sections, les utilisateurs et les sorties programmables sont définis à l'aide du programme F-Link sur l'onglet Configuration initiale. Cela facilite la programmation. Leur quantité peut être augmentée ou réduite (la réduction n'est possible que lorsqu'il n'y a pas encore de liens logiques prédéfinis qui la bloqueraient).

Il est ainsi possible de créer un système pour un petit appartement avec une section et quelques périphériques, comme pour un grand bâtiment qui utilise tout le potentiel de la centrale JA-100K avec des sections commandées indépendantes. Les sections peuvent être liées à d'autres sections (section commune) pour les commander, elles et leur statut.

### 2.1 Configuration et répartition

La centrale du système de sécurité JA-100K est destinée à la protection de locaux de petite et moyenne dimension, du fait de son envergure, ses dimensions et son nombre de sections. Une section est un élément du système qui se voit attribuer des périphériques liés à une zone protégée. Les petits locaux peuvent avoir une section de base (appartement, garage, etc.), tous les périphériques étant dans ce cas attribués à la même section. Les systèmes de taille moyenne peuvent disposer de plusieurs sections (par exemple, une maison familiale ou un immeuble de bureaux) ainsi que de leur propre *section commune de 2<sup>nd</sup> niveau* (salle commune, caves, garages, toilettes, etc.). Pour l'exploitation de tels systèmes, il est très important d'accorder l'autorisation de l'utilisateur au niveau de contrôle le plus bas des sections de base. Une section commune est armée automatiquement lorsque chaque section commune est armée, et désarmée automatiquement si au moins une des sections de base est désarmée.

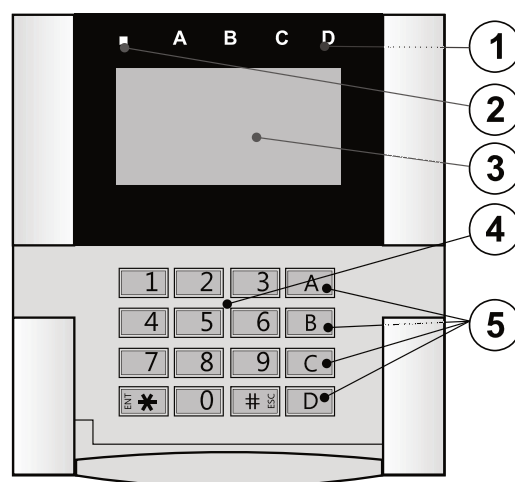


Remarque : l'utilisateur « agent d'entretien » ayant accès uniquement à la section commune peut avoir une section virtuelle attribuée (1<sup>er</sup> niveau) sans avoir à inclure de détecteurs. Le désarmement de cette section virtuelle permet également de désarmer automatiquement toutes les sections communes des locaux (2<sup>nd</sup> niveau), lui permettant ainsi de se déplacer.

### 2.2 Commande du système

Le clavier Système est destiné à la commande de base du système. Il peut y avoir plusieurs claviers utilisés dans le système et chacun d'eux peut fonctionner différemment conformément à ses propres paramètres. Toute section du système peut être commandée à partir de chaque clavier.

Chaque clavier propose 4 **touches fonctionnelles** pour la commande rapide. Chacune d'entre elle peut être configurée pour diverses fonctions telles que les armement/désarmement, la commande des appareils ou les appels d'urgence. Elles peuvent également être utilisées pour l'indication du statut de la section ou l'indication de sortie PG (indication éventuelle de statut actif par un voyant LED rouge ou vert standard - fonction « Indication PG inversée »). Les touches fonctionnelles peuvent par exemple servir d'indicateur pour un contact magnétique placé sur une porte afin de voir si la porte est ouverte ou fermée. Une option supplémentaire réside dans la « touche fonctionnelle commune » permettant, à ce titre, de commander plusieurs sections simultanément. La configuration du clavier est décrite dans le chapitre 10.3.1 Configuration du clavier.



1 - Indicateur d'état ; 2 - Indicateur Système ; 3 - Écran LCD ; 4 - Clavier et lecteur RFID ; 5 - Touches fonctionnelles

## 3 Paramètres utilitaires de la centrale JA-100K

Le composant principal du système JABLOTRON 100 est la centrale JA-100K. Ses paramètres de base sont résumés dans le tableau ci-dessous :

Tableau 1

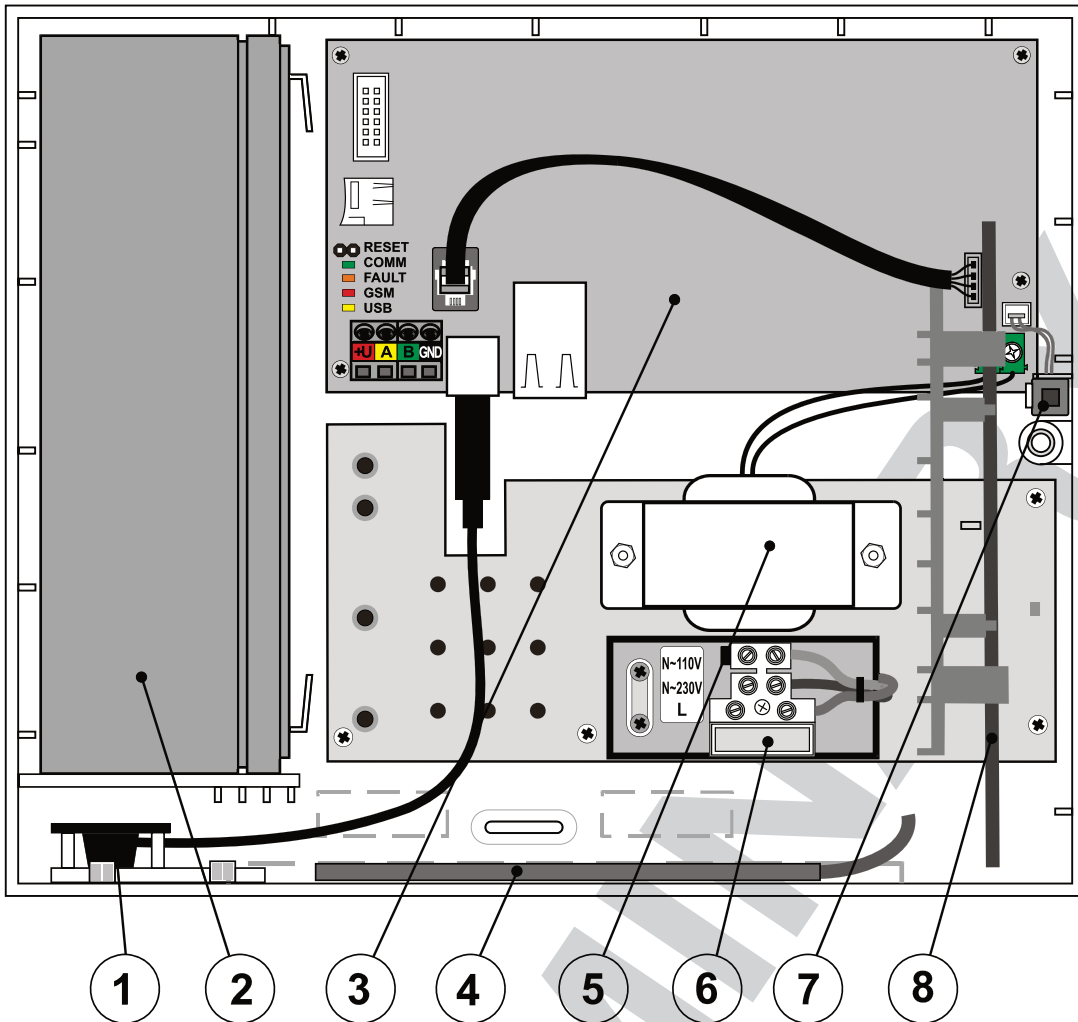
Caractéristique / type	JA-100K	Remarque
Nombre maximal de périphériques	32	Somme des composants sans fil et BUS
Nombre maximal d'utilisateurs	33	
Nombre maximal de sections indépendantes (partitions)	4	
Nombre maximal de sorties programmables	4	
Nombre maximal de modules radio	3	
Transmetteur IP LAN (Ethernet)	Oui	
Transmetteur GSM/GPRS	Non	Accessoire optionnel
Transmetteur téléphonique PSTN	Non	Accessoire optionnel
Batterie de secours 12 V recommandée	Max. 2,6 Ah	Batterie plomb-acide
Consommation maximale en courant continu disponible pour les périphériques à partir de la centrale	85 mA (avec LAN) 125 mA (sans LAN)	Pour une alimentation de secours de 12 heures à partir de la batterie recommandée, la valeur tient compte de la consommation interne de la centrale
Demande de courant maximal possible à court terme	1000 mA	5 min. max.
Bornes BUS	Connecteur 1+RJ	Le connecteur RJ ne sert qu'à la connexion directe du module radio dans la centrale
Longueur maximale du câble BUS	500 m	

### 3.1 Description de la centrale JA-100K

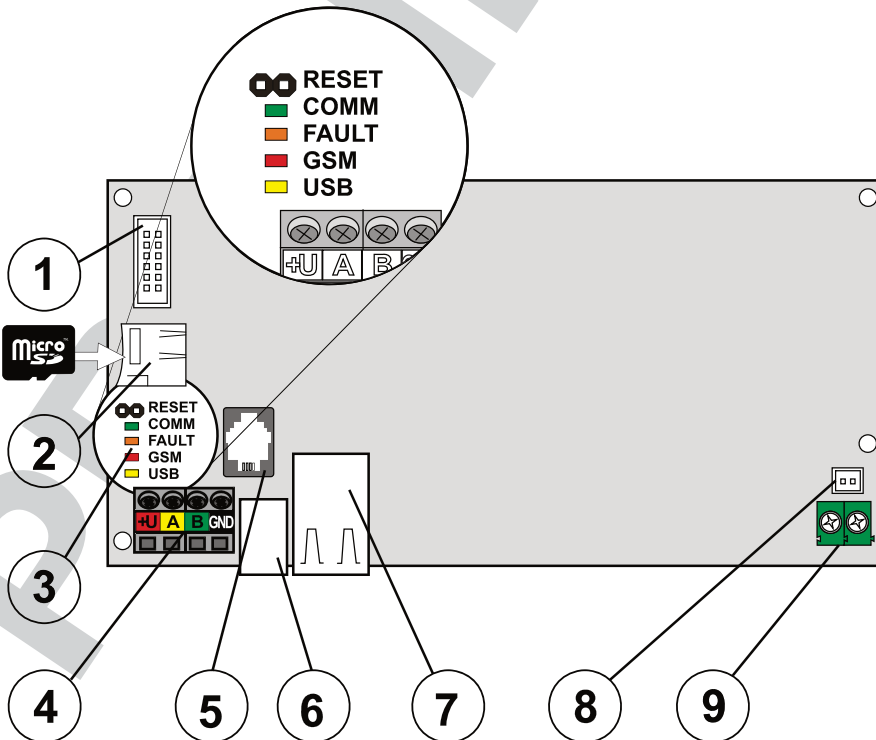
La centrale JA-100K peut également être fournie avec le module radio JA-111R installé au préalable, le kit étant alors dénommé JA-100KR.

La centrale JA-100K est conçue pour les **petits systèmes BUS** et pour les **systèmes de taille moyenne** avec communication sans fil. La centrale JA-100K est équipée d'un transmetteur LAN permettant une connexion à Internet et doté de la capacité d'envoyer des données, aux fins de sécurisation des zones de stockage de masse, vers le nuage dénommé le Cloud (clichés pris par les détecteurs PIR avec une caméra ou les caméras de vérification photographique) ou vers le serveur des agences de sécurité dotées de l'équipement technique pour la réception des données. Elle est également capable de fournir un accès à distance à l'aide du logiciel F-Link (J-Link) grâce à une connexion Internet.

La centrale peut également être équipée du dispositif JA-190Y pour une utilisation avec le réseau d'un fournisseur GSM ou du transmetteur téléphonique supplémentaire JA-190X (PSTN) devant être connecté sur une ligne analogique (par ex. PSTN) ou des lignes téléphoniques simulées. L'utilisation simultanée des deux dispositifs est impossible (il n'y a qu'un seul connecteur sur le circuit imprimé). Ces modules supplémentaires peuvent être utilisés pour le rapport des événements du système ainsi que comme transmetteur de secours si le transmetteur LAN mentionné précédemment indiquait une défaillance (voie de communication défaillante).



1 - Connecteur USB pour la connexion au PC ; 2 - Batterie de secours 2,6 Ah ; 3 - Circuit imprimé de la centrale ;  
 4 - Antenne GSM d'un numéroteur GSM supplémentaire ; 5 - Transformateur ; 6 - Bornes d'alimentation, fusible 200 mA ;  
 7 - Contact de sabotage du logement ; 8 - Module radio ;



1 - Connecteur des modules supplémentaires (transmetteur GSM ou PSTN) ; 2 - Support de carte MicroSD ; 3 - Indicateurs LED et cavalier de réinitialisation ; 4 - Bornier du BUS ; 5 - Connecteur BUS interne pour le module JA-11xR ; 6 - Connecteur de câble USB ;  
 7 - Connecteur LAN ; 8 - Connecteurs de l'interrupteur de sabotage de la centrale ; 9 - Entrée d'alimentation à partir du transformateur

### Éléments de la centrale JA-100K (parties modifiables) :

- Carte MicroSD 4 GB ou plus - aux fins de stockage pour enregistrer des événements, des images à partir de détecteurs PIR et de caméras

### Pour étendre les options de la centrale, utiliser les éléments suivants :

- Module radio JA-111R (installation par défaut dans le kit JA-100KR)
- Transmetteur PSTN JA-190X
- Transmetteur GSM JA-190Y
- Batterie de secours SA-214 / 2,6 Ah

### Les accessoires de la centrale incluent les éléments suivants :

- 1x Prolongateur de câble USB (20 cm) installé dans la centrale
- 1x Fusible T 0,2 A ; 250 V (destiné à protéger un circuit 230 V)
- 1x Fusible T 0,4 A ; 250 V (destiné à protéger un circuit 110 V)
- 3x Attaches 8 mm
- 2x Vis 40 mm
- 2x Dispositifs de serrage 100 mm
- Manuel d'installation

## 3.2 Voyants LED de signalisation de la carte de la centrale

Les voyants LED d'indication suivants se trouvent sur la carte mère :

Description	Couleur	Fonction
<b>COMM</b>	vert	Le clignotement pendant le fonctionnement de la communication BUS indique un fonctionnement approprié
<b>DÉFAILLANCE</b>	jaune	L'éclairage permanent indique une erreur générale dans le système (des informations plus complètes sont fournies par F-Link ou un clavier muni d'un écran).
<b>GSM</b>	rouge	Indication du statut d'un transmetteur supplémentaire (GSM ou PSTN)
<b>USB</b>	jaune	Indique le raccordement par câble USB à l'ordinateur.

## 3.3 Connecteurs supplémentaires sur le circuit de la centrale

Connecteurs supplémentaires sur le circuit de la centrale :

- **Cavalier de RÉINITIALISATION** sur le circuit, permettant au système de revenir aux paramètres par défaut (s'il est activé par le paramètre « Réinitialisation autorisée »). La procédure est décrite au chapitre 12 Réinitialisation de la centrale.
- **Connecteur à 10 broches** à utiliser pour connecter un transmetteur supplémentaire.
- **Connecteur RJ (RJ-44)** pour la connexion du module radio JA-111R en cas d'installation dans le boîtier de la centrale. Il est strictement interdit de connecter tout périphérique à ce connecteur hors du boîtier de la centrale.
- **Connecteur LAN** pour la connexion à Internet
- **Connecteur à 2 broches** conçu pour le contact de sabotage devant être connecté. Il indique toute tentative d'endommagement du capot avant ou d'ouverture de la centrale. Un contact de sabotage arrière n'est pas inclus avec cette version de la centrale.

## 3.4 Bornes de connexion sur le circuit de la centrale

La centrale d'un système de sécurité a l'obligation d'être connectée au secteur (230 V / 50 Hz ou 110 V / 60 Hz) en permanence. Pour de plus amples détails, voir le chapitre 16 Caractéristiques techniques

L'alimentation secteur est connectée via des bornes équipées d'un fusible remplaçable. La centrale est un périphérique de protection de niveau 2 avec isolation double. C'est pourquoi un câble à 2 conducteurs est suffisant (un conducteur alimenté et un neutre). Avec un câble à 3 pôles, laisser le câble de mise à la terre débranché et isolé.

**Attention :** ne jamais connecter le câble de mise à la terre à toute borne de la centrale !

Pour alimenter la centrale avec une basse tension et l'isolation de sécurité BUS à partir du réseau, un petit transformateur isolant de protection est utilisé. Le transformateur est connecté à la centrale par la petite borne verte.

La communication interne entre la centrale et les périphériques connectés s'effectue via le BUS à 4 conducteurs. Ceci est réalisé par un seul bornier à quatre couleurs (rouge, jaune, vert et noire).

Un connecteur USB intégré de type B est placé sur les circuits de la centrale. En utilisant une extension courte, il est possible d'établir une connexion avec un PC via le câble USB sans ouvrir la centrale.

## 4 Avant l'installation du système



Sélectionner un emplacement dissimulé pour la centrale (à l'intérieur de la zone protégée) qui dispose d'une alimentation en courant électrique.

L'alimentation de la centrale ne peut être installée que par une personne ayant la qualification électrotechnique requise.

Le fabricant ne permet pas d'alimenter la centrale à partir d'autres sources d'alimentation alternatives telles que les batteries à haute capacité chargées par l'énergie solaire, etc.

La centrale JA-100K fournit des bornes d'alimentation permettant de sélectionner 2 types de réseau de tension d'alimentation : ~230 V / 50 Hz et ~110 V / 60 Hz. Il est nécessaire d'utiliser la borne de connexion adéquate et le fusible correspondant en fonction du type de système de tension d'alimentation, conformément au chapitre 16 Caractéristiques techniques.

L'alimentation de la centrale dispose d'une double séparation de sécurité des circuits. Aucun conducteur de protection n'est raccordé.

Lors du montage et du raccordement des composants BUS de la centrale, il faut mettre hors circuit toutes ses alimentations.

**Le fabricant décline toute responsabilité relative aux dommages provoqués si le système est installé ou configuré de manière inadéquate.**

1. La disposition et la configuration du système doivent correspondre à la documentation de conception d'un système d'alarme conforme à la spécification technique CLC/TS 50131-7, à la consultation du client et aux normes techniques en vigueur pour les installations électriques.

2. Préparation de l'alimentation de la centrale - utiliser un câble approprié avec une isolation double et une section transversale de 0,75 à 1,5 mm<sup>2</sup>. Une protection contre les surtensions du réseau électrique sur la centrale est recommandée. Il est également recommandé d'utiliser un câble unique avec un disjoncteur (2A - 6A) qui fonctionne également comme interrupteur principal.

Attention : ne connecter aucun autre périphérique électrique sur ce circuit spécifique, y compris une alimentation pour les sorties PG externes, le système de chauffage ou tout autre périphérique lié aux fonctions de la centrale (commande du chauffage, etc.). Placer une étiquette adhésive marquée « Ne pas éteindre » sur le disjoncteur placé sur le tableau de distribution.

3. Il est recommandé de mettre une protection contre les surtensions dans le circuit principal pour la centrale.

4. Fixer la centrale directement au mur ou sur toute autre surface incombustible. Vérifier qu'il n'y a pas d'objets métalliques qui pourraient avoir une influence négative sur la transmission ou la réception des signaux radio (module radio et transmetteur GSM). Utiliser le gabarit fourni pour préparer les orifices pour les attaches. Placer les vis dans les orifices supérieurs du boîtier en plastique pour le maintenir à 1 cm du mur, puis accrocher le boîtier de la centrale. Mettre également une vis supplémentaire dans le ou les orifices inférieurs et visser pour stabiliser la position de la centrale. Serrer toutes les vis.

## 5 Installation des périphériques BUS

Le BUS du système JABLOTRON 100 est destiné à être utilisé avec les périphériques BUS de la série JA-1xx. Procéder comme suit :

1. Lors du raccordement de tout module BUS, il faut mettre hors circuit l'alimentation de la centrale (y compris la batterie de secours).

2. Procéder conformément aux manuels d'installation des périphériques individuels.

3. Le câble du BUS doit être installé à l'intérieur de la zone protégée par le système. À l'intérieur des murs, des tuyaux en métal, dans un plafond bas ou au travers de zones non accessibles facilement.

4. Si le câble se trouve en dehors de la zone protégée, cette partie doit être séparée par l'isolateur BUS JA-110T. Ce dispositif isolant doit être placé dans les locaux protégés et les câbles installés hors de la zone protégée ne sont pas destinés à des applications de sécurité.

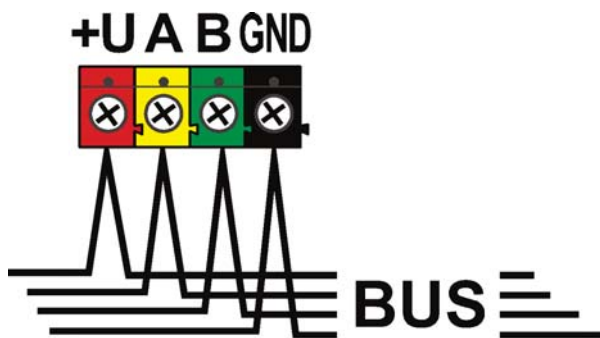
5. Pour la ramification de ligne, utiliser le répartiteur BUS JA-110Z (et/ou JA-110Z-B, JA-110Z-C).

6. Lors de la connexion des périphériques BUS, faire attention à la couleur des câbles (rouge, jaune, vert, noir).

La connexion de périphériques tiers est possible via un module approprié, tel que JA-111H, JA-116H, JA-118M, JA-114HN, etc. Le producteur ne peut garantir le fonctionnement approprié du périphérique connecté ni son niveau de sécurité.

## 5.1 BUS JA-100

Le BUS du système JABLOTRON 100 se compose de quatre câbles (4 conducteurs). Le BUS ne peut pas être partagé avec un autre système, même pour alimenter différents périphériques.



Borne	Couleurs	Remarque
+U	rouge	Borne d'alimentation positive - elle sert uniquement à l'alimentation des périphériques de la gamme JABLOTRON 100
A	jaune	Données A
B	vert	Données B
MASSE	MASSE	Borne commune (borne d'alimentation négative)

Bornier du BUS

## 5.2 Câbles du BUS

Résistance de la paire de conducteurs d'alimentation (va et vient)		
CC-01	Résistance de la paire pour 1 m	0,0754 Ω
	Résistance de la paire pour 10 m	0,754 Ω
	Résistance de la paire pour 100 m	7,54 Ω
CC-02	Résistance de la paire pour 1 m	0,1932 Ω
	Résistance de la paire pour 10 m	1,932 Ω
	Résistance de la paire pour 100 m	19,32 Ω
CC-11	Résistance de la paire pour 1 m	0,0754 Ω
	Résistance de la paire pour 10 m	0,754 Ω
	Résistance de la paire pour 100 m	7,54 Ω

Raccorder les périphériques BUS avec un câble CC-01, CC-02, CC-11 ou équivalent.

**Le câble CC-01** est conçu pour la ligne principale du BUS ou la connexion d'éléments dotés d'une consommation élevée (sirène) ou d'éléments distants. Le câble dispose de 4 conducteurs (les couleurs correspondent aux couleurs du BUS). Les conducteurs d'alimentation (noir et rouge) ont une section transversale du cœur supérieure (0,5 mm<sup>2</sup>) à celle des conducteurs de communication (0,2 mm<sup>2</sup>). Le câble est fourni sous forme conditionnée (1 paquet - 300 m).

**Le câble CC-02** est conçu pour les ramifications de la ligne principale du BUS, pour la connexion des éléments ayant une faible consommation (détecteurs) ou sur de courtes distances. Le câble dispose de 4 conducteurs (les couleurs correspondent aux couleurs du BUS). Tous les conducteurs du câble CC-02 ont une même section transversale centrale (0,2 mm<sup>2</sup>). Le câble est fourni en conditionnement unitaire de 300 m.

**Le câble CC-11** est conçu pour la ligne principale du BUS, la connexion des éléments ayant une consommation élevée (sirène) ou des éléments distants. Le câble dispose de 4 conducteurs (les couleurs correspondent aux couleurs du BUS). Les conducteurs d'alimentation (noir et rouge) ont une section transversale du cœur supérieure (0,5 mm<sup>2</sup>) à celle des conducteurs de communication (0,2 mm<sup>2</sup>). Le câble est fourni sous forme conditionnée (1 paquet - 300 m) et possède une certification incendie.

### Agencement du BUS :

Le câble du BUS **ne doit pas** être connecté de manière à créer **une boucle fermée** de n'importe quel conducteur (les extrémités des ramifications individuelles ne doivent jamais être interconnectées entre elles et le conducteur GND commun ne doit pas l'être non plus).

## 5.3 Longueur du BUS et nombre de périphériques connectés

La longueur maximale d'un BUS sans renfort (séparation) est de 500 m. La longueur est égale à la somme de la longueur de tous les câbles, sur l'ensemble des éléments connectés. Le nombre de périphériques BUS connectés est limité par la capacité de la batterie de secours de la centrale. Pour respecter la norme de sécurité de niveau 2, en cas de panne du secteur 230 V, le système doit fonctionner de façon fiable pendant au moins 12 heures avec la source de secours. Ainsi, la consommation totale de tous les éléments du BUS ne doit pas dépasser la consommation continue maximale de courant à partir de la centrale, voir le chapitre 5.4 Exemple de

calcul de consommation du BUS en cas d'alimentation de secours du système. Pour calculer la consommation totale continue des éléments connectés, additionner leur **consommation de secours** (elle est spécifiée dans le manuel ou utiliser le tableau récapitulatif, voir le point 14.1 Tableau récapitulatif de la consommation en courant des périphériques BUS.

Un autre paramètre limitant la longueur maximale d'un BUS est lié à la chute de tension le long du câble (clairement démontrée par l'option Diagnostic du système de F-Link et J-Link).

## 5.4 Exemple de calcul de consommation du BUS en cas d'alimentation de secours du système

Le tableau présente l'exemple d'un petit système comportant 5 périphériques BUS. La consommation totale au repos en mode de secours est de 78 mA. Il est ainsi possible d'utiliser la centrale JA-100K, ce qui permet un chargement permanent maximal de 125 mA et 85 mA lorsque le module LAN est activé.

Tableau 5

Périphérique	Description	Nombre de pièces	Consommation en mode de secours
JA-111R	Module de communication radio	1	25 mA
JA-110E	Clavier de commande	1	18 mA
JA-110A	Sirène intérieure	1	5 mA
JA-111A RB	Sirène extérieure de secours	1	5 mA
JA-110N	Module de sortie PG	1	25 mA
<b>TOTAL</b>			<b>78 mA</b>

Paramètre	JA-100K
Courant permanent maximal du BUS	400 mA en permanence (1000 mA pendant 5 minutes)
Courant permanent maximal pour une alimentation de secours pendant 12 heures	125 mA (avec une batterie de secours de 2,6 Ah)

Calcul du courant du BUS conformément à la configuration matérielle de la centrale :

Batterie de secours 2,6Ah	175mA - Courant max. à partir de la batterie de secours													
<b>JA-100K</b>	50	x	x	x	x	x	x	x	x	x	x	X	x	x
<b>JA-111R</b>	30		x	x	x	x							x	x
<b>LAN</b>	40			x	x	x	x	x	x					
<b>JA-190Y</b>	25				x				x		x		x	
<b>JA-190X</b>	15					x			x		X			x
Courant maximal prélevé du BUS pour une alimentation de secours pendant 12 heures (mA)		125	95	55	30	40	85	60	70	100	110	70	80	

## 5.5 Besoins en alimentation électrique

Un système de sécurité qui doit se conformer à un niveau de sécurité 2 doit être protégé par une batterie de secours pendant 12 heures (conformément à EN 50131-1) et 24 heures (conformément à INCERT T 031) pendant une panne de courant secteur ; il doit également être entièrement rechargé dans les 72 heures (conformément à EN 50131-1) et dans les 48 heures (conformément à INCERT T 031) après la restauration de l'alimentation secteur.

Pour respecter cette exigence, il est nécessaire de s'assurer que la capacité de la batterie de secours est appropriée à la durée requise, voir l'exemple suivant. La capacité nominale de la batterie doit être vérifiée par un test, voir les spécifications techniques CLC/TS 50131-7, test du système.

Calcul du courant permanent maximal prélevé à partir du système BUS conformément à la capacité de la batterie de secours :



## Centrale JA-100K

Pour une batterie de 2,6 Ah

**2,6 Ah** \* 0,8 / 12 h = 0,17 A

$I_{max} = 0,17 A - 0,05 A = \mathbf{0,12 A}$

(le calcul est valable pour 80% de la capacité de la batterie)

(conformément à la capacité - courant maximal pendant 12 heures)

(soustraire le propre courant de la centrale 0,05 A)

Le courant pris à partir de chaque borne de sortie du BUS est indiqué dans le logiciel F-Link dans l'onglet Diagnostic sur la ligne 0 où se trouve la centrale. Il est nécessaire de prendre en considération le courant affiché en particulier lorsque le module JA-111R est utilisé (centrale sans fil) et connecté au connecteur spécial RJ afin d'ajouter également le courant de ce module. Ce courant est comparé à un courant calculé et il détermine si la capacité de la batterie de secours est adéquate avec les exigences de la norme pour la durée d'alimentation de secours du système. Si le courant mesuré est supérieur à celui qui est calculé, la batterie de secours devrait avoir une capacité supérieure.

Diagnostics		Calendars	Communication	ARC
Battery stat...	Voltage/ loss	RF Signal level	Chan...	Note
13,7 V/13,6 V	13.7 V/0 mA			
	0,0 V		BUS 1	

## 6 Utilisation des périphériques sans fil

Dans le système JA-100, il est possible d'utiliser les périphériques sans fil de la gamme JA-1xx. La centrale doit être équipée d'au moins un module radio JA-111R, un maximum de 3 modules radio pouvant être utilisés dans le système.

Lors de l'installation des différents périphériques, procéder conformément aux instructions de leur manuel.

### 6.1 Installation du module radio JA-111R

1. Le kit JA-100KR dispose du module radio intégré JA-111R dans le boîtier de la centrale à côté du transformateur dans un support en plastique particulier.
2. Si la centrale est installée sur un emplacement doté d'une mauvaise réception de signal GSM, le module de communication GSM augmente sa puissance d'émission, ce qui peut avoir un impact négatif sur la portée des modules de communication radio. Dans un tel cas, il est recommandé de placer le module radio à l'extérieur de la centrale, à une distance minimale de 2 m, où il ne sera plus influencé négativement et aura une réception radio de qualité supérieure à partir de la périphérie, ce qui permettra des portées supérieures et par conséquent des distances d'installation plus grandes. Il est nécessaire d'installer JA-111R à l'extérieur du boîtier de la centrale dans le boîtier d'installation PLV-111R (il n'est pas fourni avec le kit JA-100K et doit être commandé individuellement).



**Le connecteur RJ du BUS sur la carte de la centrale est exclusivement destiné au raccordement du module radio placé à l'intérieur de l'armoire de la centrale.**

3. Un espace plus grand peut être couvert avec un signal radio en installant jusqu'à 3 modules radio JA-11xR dans leur propre boîtier en plastique, à différents endroits (par ex. à des étages différents). Le signal provenant d'un périphérique sans fil (ci-après désigné le « périphérique ») peut être reçu par plusieurs modules radio simultanément. La centrale communique de manière cyclique avec les modules radio individuels, de sorte qu'elle recevra les informations envoyées par un périphérique à partir du module radio, celui-ci ayant été le premier à recevoir un signal intact et à y réagir. Elle ne recevra ensuite plus la même information des autres modules radio, même si elle a été reçue avec un signal plus fort. Il peut ainsi arriver que les signaux du même périphérique unidirectionnel présentent des données très différentes dans les paramètres F-Link / Configuration du système / Diagnostic, lors de mesures répétées, en fonction du module à partir duquel le signal a été perçu. En ce qui concerne les périphériques bidirectionnels, la centrale « réserve » le canal déjà utilisé (communication avec le premier module radio) puis elle communique uniquement avec le périphérique particulier via ce module radio (indiqué dans la section Diagnostic, colonne Canal) jusqu'à ce que le périphérique cesse de répondre. Puis elle recherche le signal de connexion dans les autres modules radio. Si la qualité de la connexion des périphériques individuels vers les modules radio individuels doit être vérifiée, cela doit être réalisé avec le graphique du signal RF dans le logiciel F-Link (touche sur la barre d'outils supérieure). Sélectionner le module radio pour lequel la communication doit être vérifiée et activer les périphériques à vérifier. Le graphique de la communication radio indique la puissance du signal RF mesurée par le module radio particulier. Il est également possible d'avoir plusieurs fenêtres de signal RF ouvertes afin de simplement surveiller la couverture RF sur ces emplacements.
4. Monter verticalement le module radio sur le mur. Il ne doit pas se trouver à proximité d'objets qui perturberaient ou brouilleraient la communication (métaux, équipements électroniques, câbles, tuyauterie, etc.).

- Après la mise en marche du système, il faut **tout d'abord inscrire les modules radio**. Une fois fait, il est alors possible d'inscrire des périphériques sans fil.
- Recommandations : il est recommandé d'inscrire des périphériques sans fil vers le système lorsqu'ils sont définitivement positionnés. Cette procédure d'installation n'est pas la plus confortable, mais elle aide à obtenir une meilleure réception radio, plus fiable, au niveau du module radio. Le module radio comporte un algorithme qui assure un « signal minimum » à partir du périphérique, évalué en mode Service. Une réserve est alors comptée en cas d'aggravation des conditions radio en mode pleinement opérationnel (par exemple lorsqu'un bâtiment est de nouveau configuré, en cas d'interférences industrielles, etc.). Voir les informations plus détaillées dans la norme EN 50131-5-3.

## 6.2 Installation de périphériques sans fil - mode d'inscription

Les périphériques sans fil doivent être individuellement inscrits vers le système. La procédure d'inscription peut être réalisée en mode d'inscription uniquement à l'aide d'un PC avec le logiciel F-Link installé. Voir le chapitre 8.4.1 Inscription et effacement des périphériques.

# 7 Activation du système

- Vérifier le raccordement des câbles du BUS.
- Vérifier si une carte microSD est insérée dans le support de la carte de la centrale.
- Vérifier si le câble d'alimentation est correctement branché à la centrale et si le cordon d'alimentation est bien fixé.
- Insérer la batterie dans la centrale et la fixer dans l'armoire (par des blocs autocollants ou une bande)  
**Attention - la batterie de secours est livrée chargée, elle ne doit pas subir de court-circuit !**
- Raccorder les câbles d'alimentation de la batterie. Attention à la polarité (rouge +, noir -).
- Lancer l'alimentation à partir du réseau et vérifier les voyants de signalisation LED sur la centrale :
  - Le voyant LED vert clignote (fonction du BUS).
  - Le voyant LED rouge clignote - connexion au réseau GSM en cours avec le transmetteur GSM supplémentaire.
  - Le voyant GSM LED rouge s'éteint - le transmetteur GSM est connecté au réseau GSM.
  - Le voyant LED rouge reste allumé - la centrale ne s'est pas connectée au réseau GSM.
- Dès que les périphériques BUS commencent à clignoter en jaune, les inscrire vers le système ; se référer au chapitre 8.4.1 Inscription et effacement des périphériques.
- Réaliser la configuration des claviers, se référer au chapitre 10.3.1 Configuration du clavier.
- Configurer les fonctions demandées et vérifier le système, se référer au chapitre 10.7 Onglet Paramètres.

# 8 Configuration du système

Le système de sécurité (locaux protégés - bâtiment) peut être divisé en parties indépendantes - sections. Chaque section peut également être surveillée comme une section à part entière ou seulement en tant qu'élément du système. Cela correspond à un armement partiel. Les détecteurs dotés d'un paramètre activé « Interne » ne surveillent pas dans un tel mode.

La **protection périphérique** constitue la sécurité de base. Elle sécurise les portes principales, les portes de garage, les fenêtres, les portes de balcon et les entrées de service ainsi que celles du toit. Parmi les périphériques assignés à la protection périphérique, il existe des détecteurs magnétiques, des détecteurs de bris de verre, des détecteurs de vibration / d'inclinaison ainsi que des barrières infrarouges. La seule spécificité réside dans le fait que les portes principales ou les portes de garage sont généralement temporisées et le reste des zones est défini avec une réaction instantanée.

La partie suivante concerne les **détecteurs de mouvement**. Le mouvement dans les locaux protégés est surveillé à l'aide de détecteurs de mouvement (PIR) ou en combinaison avec d'autres détecteurs. Les détecteurs placés dans une entrée ont généralement une réaction de temporisation prédéfinie ou une réaction de temporisation différée. Le reste des détecteurs de mouvement est dans la plupart des cas prédéfini sur des réactions instantanées. Il est possible de sélectionner jusqu'à 2 minuteurs pour créer les voies d'entrée (par exemple, un délai plus long lors de l'entrée dans un garage).

La **protection des locaux** est utilisée pour un coffre-fort ou des objets de valeur, mais aussi la détection d'intrusion par la force brute. Les portes de garage peuvent être endommagées avec n'importe quelle ouverture. Des détecteurs de vibration et d'inclinaison sont inclus dans la protection des **locaux**, ainsi que les habituels détecteurs magnétiques pour la détection de l'ouverture des portes - généralement en tant que capteur temporisé.

La protection des composants individuels de sécurité est réalisée par des contacts de sabotage indiquant un fonctionnement non autorisé du périphérique.

La **protection de l'environnement** comprend principalement des détecteurs d'incendie, des détecteurs pour la détection de gaz combustibles et toxiques et des détecteurs d'inondation. Tous les détecteurs mentionnés ont une réaction paramétrable en permanence indépendante du statut du système, simplement dénommée Réaction 24 heures.

## 8.1 Profils du système

La sélection du profil du système vous permet de globalement prédéfinir les paramètres du système suivants (F-Link / onglet Paramètres) pour modifier le comportement du système afin de se conformer à la norme donnée et au niveau de sécurité requis. Ces options pourraient être bloquées lorsqu'un profil spécifique est sélectionné pour les modifications.

**Attention :** *le réglage des paramètres individuels par sélection d'un profil du système ne garantit pas que le système installé soit conforme au niveau 2 de sécurité. Seule une conception adéquate du système (en utilisant les périphériques appropriés), une installation appropriée aux exigences CLC/TS 50131-7 et la mise en place d'un service de télésurveillance peuvent garantir la sécurité de niveau 2. La classification de la centrale JA-100K et des périphériques individuels du système JABLOTRON 100 pour un niveau 2 de sécurité représente la base sur laquelle la qualité de sécurité des locaux protégés peut être définie.*

**Aperçu des paramètres du système en fonction du profil du système défini :**

Périphérique	Profil Paramètre	DÉFAUT		EN50131-1, niveau 2		INCERT	
		Option activée	Blocage	Option activée	Blocage	Option activée	Blocage
Centrale	Sirène lors de l'armement partiel (IW)	NON	NON	NON	NON	NON	NON
Centrale	Sirènes activées	OUI	NON	OUI	OUI	OUI	OUI
Centrale	Droits Service / Télésurveillance restreints par l'administrateur	NON	NON	OUI	OUI	OUI	OUI
Centrale	Commandes Service et télésurveillance du système	OUI	NON	NON	OUI	NON	OUI
Centrale	Commande d'accès sous contrainte	OUI	NON	OUI	NON	OUI	NON
Centrale	Confirmation de l'alarme dans une section	NON	NON	NON	NON	NON	NON
Centrale	Sirène (sortie IW) en cas d'enclenchement de sabotage	NON	NON	OUI	OUI	OUI	OUI
Centrale	Réinitialisation autorisée	OUI	NON	NON	OUI	NON	OUI
Centrale	Signal de section désarmée	NON	NON	NON	NON	NON	NON
Centrale	Échec de l'armement	NON	NON	OUI	OUI	OUI	OUI
Centrale	Indication de mémorisation de l'alarme	OUI	NON	NON	OUI	NON	OUI
Centrale	Rapport retardé à la télésurveillance	NON	NON	OUI	NON	OUI	NON
Centrale	Méthodes d'armement	Selon le profil du système	NON	Selon le profil du système	OUI	Selon le profil du système	OUI
Centrale	Type d'autorisation	Standard	NON	Standard	NON	Standard	NON
Centrale	Perte d'un périphérique BUS	Défaillance	NON	Sabotage toujours	NON	Sabotage toujours	NON
Centrale	Durée de l'alarme	240	90..1200	240	90...900	240	90...900
Centrale	Temporisation d'entrée	30	5...120 s	30	5...30 s	30	5...30 s
Centrale	Temporisation de sortie	30	5...120 s	30	5...60 s	30	5...60 s
Centrale	Temporisation d'entrée par la porte de garage	60	5...360 s	30	5...30 s	30	5...30 s
Centrale	Temporisation de sortie par la porte de garage	60	5...360 s	60	5...60 s	60	5...60 s
Module Radio	Détection de brouillage RF	Désactivé	NON	Faible	NON	Faible	NON
Clavier	Paramétrage de l'indication optique	1.(BUS) ou 4.(RF)	NON	2.(BUS) ou 4.(RF)	OUI	2.(BUS) ou 4.(RF)	OUI
Clavier	Indication du statut DÉSARMÉ	OUI	NON	NON	NON	NON	NON
Clavier	Indication du statut ARMÉ	OUI	NON	NON	NON	NON	NON
Sirène	Avertissement (indication acoustique)	NON	NON	OUI	OUI	OUI	OUI
Sirène	Perte de communication	NON	NON	OUI	OUI	OUI	OUI
Sirène	Avertissement (indication optique)	NON	NON	OUI	OUI	OUI	OUI

En définissant le profil du système « par défaut », tous les paramètres mentionnés sont prédéfinis sur les paramètres par défaut et tous les paramètres peuvent être modifiés. Le système d'alarme ne se conforme pas aux exigences de sécurité de niveau 2 et enfreint également les exigences imposées par une compagnie d'assurance ou les réglementations locales. En cas d'événement dommageable, la compagnie d'assurance n'est pas obligée de rembourser le dommage en raison d'un système mal programmé par la société d'installation.

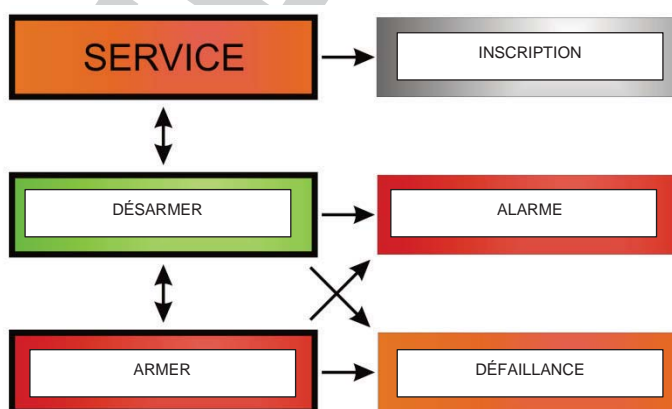
**Aperçu global des raisons empêchant le paramétrage en fonction du profil du système prédéfini :**

Évènement	Profil	Défaut		EN50131-1, niveau 2		INCERT, niveau 2	
		Franchissable	Infranchissable	Franchissable	Infranchissable	Franchissable	Infranchissable
Sabotage actif		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Entrée active (toute entrée)						<input checked="" type="checkbox"/>	
Entrée instantanée active		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Indication de la mémoire d'alarme active					<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Périphérique RF – absence de réponse pendant 20 min				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Défaillance de la sirène					<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Défaillance		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Perte d'un périphérique		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Batterie faible dans le périphérique		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Batterie faible dans la centrale		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Défaillance de la batterie dans la centrale		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Défaillance d'alimentation secteur				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Défaillance d'alimentation secteur supérieure à 30 min		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Système en configuration					<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Défaillance GSM		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Défaillance LAN		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Défaillance PSTN		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Défaillance de tous les centres de télésurveillance					<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

## 8.2 Modes de fonctionnement de la centrale

Le système de sécurité comporte plusieurs modes de fonctionnement. La commutation entre les modes dépend des niveaux d'autorisation des utilisateurs.

MODE	Description
<b>SERVICE (+ mode d'inscription)</b>	Mode dans lequel aucune alarme ne peut être déclenchée. Il est uniquement destiné à un technicien de service ou de la télésurveillance aux fins d'inscription de nouveaux périphériques et de configuration du système. Aucune commande n'est disponible dans ce mode (localement ou à distance). Les touches fonctionnelles des claviers sont éteintes et le mode est indiqué par un clignotement jaune de la touche de signalisation du système (2 clignotements toutes les 2 secondes), les signaux des télécommandes ou d'autres périphériques étant ignorés. L'entrée ou la sortie du mode Service peuvent être réalisées à partir d'un clavier LCD ou d'un PC à l'aide du logiciel F-Link. Lorsqu'un PC est connecté en ligne, il est impossible d'entrer ou de sortir du mode Service depuis le clavier.
<b>DÉSARMER</b>	Mode normal dans lequel les détecteurs d'intrusion ne surveillent pas. Il est possible de se déplacer librement dans les locaux, l'ouverture des fenêtres et des portes étant autorisée. Des détecteurs environnementaux (détecteurs de fumée / thermiques, de fuite de gaz ou d'inondation) ou des touches de détresse peuvent déclencher une alarme à tout moment. De plus, les contacts de sabotage de tous les périphériques assurent en permanence la protection et, lorsqu'ils sont activés, le système déclenche une alarme de sabotage. Le mode Désarmer est indiqué sur le clavier par un voyant vert sur l'indicateur de statut spécifique (lettres A-D) et la touche d'indication.
<b>ARMER</b> (complètement ou partiellement)	Tous les détecteurs sont actifs et assurent la surveillance (à l'exception des détecteurs internes lorsqu'ils sont partiellement armés) ; lorsqu'ils sont activés, une alarme est déclenchée (point suivant). Le mode Armer est indiqué sur le clavier par un voyant rouge (jaune en cas d'armement partiel) sur l'indicateur d'état spécifique (lettres A-D) et la touche d'indication.
<b>ALARME</b>	L'alarme est un état où, pour un temps prédéfini (durée d'alarme), les sorties IW et EW sont activées et les sirènes intérieures et extérieures sonnent. Le statut de l'alarme est indiqué sur le clavier par un clignotement rapide du voyant rouge du système. Pour une description des différences de comportement de sortie EW et IW, lire le chapitre 8.5 Types d'alarmes.
<b>DÉFAILLANCE</b>	La défaillance est un signal d'avertissement du système indiquant un certain état anormal de la centrale, des transmetteurs ou des périphériques ainsi que leurs problèmes d'alimentation (alimentation secteur ou batterie) ou de communication.



## 8.3 Autorisation des utilisateurs

Toute personne autorisée à commander un système de sécurité ou réaliser un quelconque réglage est appelée Utilisateur du système. Le premier utilisateur prédéfini muni de l'une des plus importantes autorisations d'accès et ne pouvant être effacé est le détenteur du code de service. Le deuxième code prédéfini ne pouvant être effacé est celui de l'administrateur principal. Les autres utilisateurs pouvant être ajoutés peuvent également être simplement effacés et disposent d'une autorisation paramétrable.

Code d'autorisation	Description du type
<b>Code de télésurveillance (ARC)</b>	Ce code dispose du plus haut niveau d'autorisation pour configurer le comportement du système et est exclusivement habilité à réaliser le déblocage du système suite au déclenchement d'une alarme. Il peut accéder au mode Service, à tous les onglets et options, y compris la communication avec la télésurveillance et peut refuser l'accès à un technicien de service (code de service). Tant que le paramètre « Droit d'administrateur restreint Service /Télésurveillance » reste décoché, le code de télésurveillance peut commander toutes les sections et les sorties PG utilisées dans le système. Ce code permet d'ajouter des administrateurs et des utilisateurs avec un niveau d'autorisation inférieur attribué par des codes, des badges ou des cartes RFID. Il permet également d'effacer l'alarme et la mémoire d'alarme de sabotage. Le nombre de codes de télésurveillance est uniquement limité par la capacité restante de la centrale. Le nombre de codes de télésurveillance est limité dans le système uniquement par la capacité restante de la centrale et aucun code de télésurveillance n'est prédéfini par défaut.
<b>Code de service (Service)</b>	Il peut accéder au mode Service et configurer le comportement du système. Il peut accéder à tous les onglets et options, y compris la communication avec la télésurveillance, sauf si l'accès est limité par un technicien de la télésurveillance. Tant que le paramètre « Droit d'administrateur restreint Service /Télésurveillance » reste décoché, le code de service peut commander toutes les sections et les sorties PG utilisées dans le système. Il peut créer un utilisateur doté d'une permission de type télésurveillance, d'autres techniciens de service, des administrateurs ainsi que d'autres utilisateurs avec un niveau d'autorisation inférieur et les inscrire avec des codes, des badges ou des cartes RFID. Le nombre de codes de service est uniquement limité par la capacité restante de la centrale. La position 0 est attribuée et ne peut être modifiée. Le code de service par défaut est 1010 et lorsque le profil EN est activé, 101010. Le code ne peut pas être effacé.
<b>Administrateur (Principal)</b>	Ce code donne toujours l'accès complet à toutes les sections et est autorisé à commander toutes les sorties PG. L'administrateur peut créer un autre administrateur et d'autres codes avec un niveau d'autorisation inférieur et leur attribuer un accès aux sections et aux sorties PG, des codes d'accès, des puces et des cartes RFID. Il est autorisé à effacer la mémoire d'alarme. Il ne peut y avoir qu'un seul code Administrateur principal, qui ne peut être effacé. Lorsque le paramètre « Droit d'administrateur restreint Service /Télésurveillance » est activé, le code Administrateur doit être autorisé pour confirmer l'accès. La position 1 est attribuée et ne peut être modifiée. Le code d'administrateur par défaut est 1234 et lorsque le profil EN est activé, 123456. Le code ne peut pas être effacé.
<b>Administrateur (Autres)</b>	Il permet l'accès aux sections choisies par l'Administrateur principal pour lesquelles un autre administrateur peut ajouter de nouveaux utilisateurs avec un niveau d'autorisation similaire ou inférieur pour commander les sections et les sorties PG, les attribuer avec des codes d'accès, des badges ou des cartes RFID. Il est habilité à effacer la mémoire d'alarme dans les sections attribuées. Lorsque le paramètre « Droit d'administrateur restreint Service /Télésurveillance » est activé, le code Administrateur doit être autorisé pour confirmer l'accès. Le nombre de codes d'Administrateur (autre) est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.
<b>Utilisateur</b>	Ce code donne l'accès, du fait des droits attribués par un administrateur, aux commandes de sections et PG. Les utilisateurs peuvent ajouter / supprimer leurs badges et cartes d'accès RFID et modifier leurs numéros de téléphone. Il donne l'autorisation d'effacer la mémoire d'alarme dans les sections attribuées. Les utilisateurs sélectionnés peuvent voir leur accès aux sections limité par un programme. Le nombre de codes d'utilisateur est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut. L'utilisateur n'a pas la permission de modifier son propre code d'accès ni de l'effacer.
<b>Armer</b>	Ce code est uniquement autorisé pour armer une section désignée. Les utilisateurs avec ce niveau d'autorisation ne sont pas autorisés à modifier leur code ni à effacer la mémoire d'alarme. Le nombre de codes d'armement est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.
<b>PG seulement</b>	Il permet à l'utilisateur de commander les sorties programmables par seule autorisation. Cela concerne aussi bien la mise sous tension que hors tension. Les utilisateurs avec ce niveau d'autorisation ne sont pas autorisés à modifier leur code ni à effacer la mémoire d'alarme. Le nombre de codes PG est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.
<b>Détresse</b>	Ce code est uniquement autorisé pour déclencher une alarme de détresse. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Détresse est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.
<b>Code Garde</b>	Ce code est destiné à une agence de sécurité. Ce niveau d'autorisation permet d'armer l'ensemble du système. Cependant, le code Garde peut désarmer le système uniquement lors d'une alarme ou ultérieurement, aussi longtemps que la mémoire d'alarme est toujours active. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Garde est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.
<b>Code Déblocage</b>	Ce code sert à débloquer le système après le verrouillage du système par l'alarme. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Déblocage est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défini par défaut.

Le logiciel F-Link gère la création des nouveaux utilisateurs et la gestion de leur niveau d'autorisation.

## 8.4 Paramètres en option du système (F-Link - onglet Paramètres)

**Sirène en cas d'armement partiel IW** - cette fonction permet l'activation de sirènes internes lors d'une alarme d'intrusion (elle n'est pas liée aux alarmes d'incendie ou 24hr) lorsque le système est partiellement armé.

**Sirènes activées** - active toutes les sirènes BUS et sans fil du système. Conçu pour désactiver l'alarme sonore pendant les tests du système.

**Administrateur - droits de service / télésurveillance restreints** - L'autorisation de l'administrateur (code en position 1) est nécessaire pour accéder au système pour la télésurveillance ou le technicien de service. En cas d'accès à distance vers le système via F-Link par un technicien de service, l'administrateur peut être autorisé en utilisant un clavier sur le site. En cas de connexion locale à la centrale via un câble USB par un technicien de service, l'administrateur peut être autorisé à distance en utilisant le menu vocal lorsqu'un transmetteur GSM est connecté.

**Commandes du système Service et télésurveillance** - permet aux techniciens de service et à la télésurveillance (Armer/Désarmer) de commander toutes les sections et les sorties PG (MARCHE / ARRÊT) nécessitant une autorisation.

**Commande d'accès sous contrainte** - cette fonction déclenche une alarme de détresse silencieuse par autorisation uniquement ou pendant la commande du système (armement, désarmement, PG) lorsqu'un utilisateur est contraint par un intrus. Une alarme de détresse est déclenchée lors de la commande du système en ajoutant la valeur « 1 » au dernier chiffre du code. Lorsque le dernier chiffre du code de l'utilisateur est 9, saisir 0 comme dernier chiffre pendant la commande d'accès.

**Confirmation d'alarme dans une section** - Si la réaction de confirmation par un autre détecteur est définie pour un détecteur, cette option de confirmation peut être utilisée pour uniquement limiter la confirmation à la même section (sinon, un détecteur de n'importe quelle section peut confirmer une alarme). Valable pour les détecteurs d'intrusion ainsi que pour les détecteurs d'incendie.

**Sirène (sortie IW) en cas de sabotage** - les sirènes dotées d'une réaction IW indiquent par voie acoustique une alarme de sabotage si la zone est désarmée ou partiellement armée. Les sirènes signalent toujours lorsque le système (section) est entièrement armé.

**Réinitialisation activée** - possibilité de verrouiller la réinitialisation de la centrale avec un cavalier sur la carte. Si l'option de réinitialisation est désactivée et le code de service est perdu, la centrale ne peut être déverrouillée que par le fabricant. La réinitialisation de la centrale est décrite au chapitre 12 Réinitialisation de la centrale.

**Signalement de section désarmée** - le système signale une section désarmée lorsqu'il n'y a pas de mouvement détecté depuis 16 heures.

**Échec de l'armement** - fonction lancée pendant chaque procédure d'armement. Si une zone instantanée est déclenchée au cours de la temporisation de sortie ou si une zone temporisée reste ouverte lorsque la temporisation de sortie expire, le système ne s'arme pas et déclenche l'événement « Échec de l'armement » puis l'enregistre dans l'historique. Si un transmetteur GSM supplémentaire est utilisé, le rapport est également réalisé via un SMS à un utilisateur prédéfini si l'événement « SMS relatif à l'échec de l'armement » est autorisé à être envoyé. Il est indiqué par des claviers ainsi que par une sirène extérieure. Pour annuler l'indication concernant l'échec de l'armement, il faut enclencher « Annuler l'indication d'avertissement » dans le menu du clavier LCD.

**Indication de la mémoire d'alarme** - indication d'une alarme par un voyant LED intégré dans le détecteur qui a déclenché l'alarme. Disponible pour les périphériques prenant en charge cette fonction.

**Méthodes d'armement** - Choix de la façon dont le système réussit à armer le système avec un périphérique ou une défaillance du système. Au niveau le plus bas, le système s'arme toujours indépendamment des périphériques actifs ou des défaillances jusqu'au niveau le plus élevé où il ne peut pas être armé avec un périphérique actif (zone instantanée).

**Type d'autorisation** - sélection de la manière dont le système traite l'autorisation de l'utilisateur. Par autorisation standard (code ou carte uniquement), confirmation d'une carte RFID par un code (si l'utilisateur se voit attribuer les deux) ou double autorisation, ce qui implique l'utilisation obligatoire de la carte et du code. Confirmation du code de l'utilisateur par une carte afin de réduire le risque d'accès ou de commande non autorisés par un tiers.

**Perte d'un périphérique BUS** - la centrale traite la perte d'un périphérique ou un court-circuit sur le BUS du système. Selon l'option sélectionnée, elle réagira en déclenchant une alarme de défaillance ou de sabotage avec chaque perte de périphérique ou en déclenchant une alarme de sabotage après confirmation que tout autre périphérique est également perdu.

### 8.4.1 Inscription et effacement des périphériques

Le périphérique installé (détecteur, clavier, sirène, badge, etc.) ne peut fonctionner qu'une fois inscrit sur une position (adresse) dans le système. Après l'inscription, certains périphériques occupent plusieurs positions (entrées magnétiques multiples, dispositifs d'extension d'entrée). Certains périphériques (modules de sortie PG, indicateurs d'état, séparateurs et répartiteurs BUS) ne sont inscrits sur aucune position. Les informations détaillées se trouvent dans le manuel du périphérique correspondant.



1. L'inscription du périphérique s'effectue par le programme F-Link, l'onglet Périphériques, la touche **Inscription**. **L'inscription n'est possible qu'en mode Service**.
2. Il est possible d'inscrire un périphérique de plusieurs façons :
  - a. **Enclenchement de l'interrupteur de sabotage d'un périphérique BUS = fermeture du capot** (certains périphériques peuvent être inscrits par la pression d'une touche - voir le manuel du périphérique particulier).
  - b. **Connexion de la batterie vers un périphérique sans fil** - Cependant, au moins un module radio doit être inscrit en premier. Dans le cas des télécommandes du type JA-186Jx, la connexion de la batterie peut être réalisée en enclenchant et en maintenant deux touches (formation d'une paire). Les télécommandes du type JA-154Jx sont inscrites en appuyant sur n'importe quelle touche.
  - c. **Saisie du numéro de série dans le champ du code de production SN** (situé sous le code-barres sur la carte à l'intérieur du périphérique, par ex. 1400-00-0000-0123). Le numéro peut aussi être lu par un lecteur optique de code-barres. Par la suite, le détecteur doit être activé pour vérifier son inscription.
  - d. **Chargement sélectif des périphériques BUS non-inscrits** - Si un ou plusieurs périphériques non encore inscrits sont connectés au BUS, après avoir sélectionné **Inscrire** dans **Périphérique**, la touche **Scanner / inscrire les nouveaux périphériques BUS** s'affichera, ce qui proposera l'inscription du périphérique BUS. Inscrire le périphérique en double-cliquant sur l'élément sélectionné.
  - e. **Chargement collectif des périphériques BUS non-inscrits** - si un ou plusieurs périphériques non encore inscrits sont connectés au BUS, après avoir sélectionné la touche **Scanner / inscrire les nouveaux périphériques BUS**, tous les périphériques BUS seront inscrits collectivement. Cette procédure ne permet pas de déterminer les positions séquentielles des périphériques individuels.
3. Un périphérique peut-être supprimé en supprimant son numéro de série (seul le périphérique sera supprimé), en sélectionnant la ligne correspondante dans l'onglet Périphériques et l'option Supprimer dans le menu, sur la touche droite de la souris ou en appuyant simplement sur la touche Supprimer, qui permet de supprimer la totalité de la ligne du périphérique (avec ses paramètres relatifs à la section, la réaction, la commande de sortie PG, les remarques et les autres options). Il est ainsi possible après avoir marqué plusieurs périphériques (clic+Shift ou clic+Ctrl) de les supprimer ou simplement modifier un paramètre commun.

**Attention :**

*Il est recommandé d'inscrire des périphériques sans fil dans le système conformément au point B en conditions réelles et à l'emplacement requis dans les locaux protégés. Cela permet d'éviter les problèmes liés à une portée RF insuffisante lorsque des périphériques sont inscrits autrement.*

**Remarques :**

- Les périphériques BUS non-inscrits clignotent en jaune. Si un périphérique non-inscrit ne commence pas à clignoter en jaune dans les 180 secondes suivant la mise en service de l'alimentation de la centrale (au cours de l'initialisation), vérifier si le périphérique est correctement raccordé.
- Les périphériques sans fil qui communiquent unilatéralement ne disposent pas d'une signalisation de demande d'inscription.
- Si le périphérique est inscrit vers le système de la manière décrite au préalable, la position suivante sera automatiquement proposée. Il n'est pas nécessaire de prendre d'autres mesures ; les périphériques doivent uniquement être inscrits dans l'ordre sélectionné. Le déplacement automatique vers la position suivante peut être annulé dans la fenêtre d'inscription du périphérique.
- Si un périphérique déjà inscrit est de nouveau inscrit sur autre position, il sera automatiquement déplacé.
- Si le périphérique occupe plusieurs positions, il occupera automatiquement le nombre respectif de positions consécutives grâce à une seule inscription (par ex., le module JA-116H, doté de seize entrées d'alarme, occupera seize positions). Attention, une suppression accidentelle d'un périphérique inscrit sur une autre position peut se produire !
- Si un périphérique est inscrit dans la position la plus élevée possible, le processus d'inscription progressive prend fin.
- Les positions libres sont attribuées par défaut à la section 1. L'attribution de la section peut être ultérieurement modifiée.
- Pour les périphériques à positions multiples, tels que JA-116H, JA-118M, JA-114HN, JA-150M, etc., il est possible de limiter le nombre de positions occupées en effaçant des lignes spécifiques lorsque le module est inscrit. Réaliser l'effacement en cliquant sur la ligne particulière à la position requise (pas la touche dans le type de colonne !) et appuyer sur la touche Supprimer du clavier du PC.

## 8.4.2 Liste des réactions applicables

Dans l'onglet Périphériques, il est possible de définir la réaction de l'activation du système d'un périphérique inscrit. De tels types de réactions sont proposés uniquement pour les périphériques individuels faisant sens pour le produit concret. Certains périphériques ne peuvent se voir attribuer une réaction (par ex. la sirène externe).

**Attention :** la gamme des réactions peut être limitée par le profil du système.

<b>Temporisée</b>	Alarme d'intrusion avec temporisation d'entrée / de sortie
<b>Instantanée</b>	Alarme instantanée en cas d'armement. Si une temporisation d'entrée est paramétrée, une alarme IW est enclenchée. L'alarme EW est uniquement enclenchée après l'expiration de la durée de temporisation d'entrée (pour de plus amples informations sur EW et IW, voir le chapitre 8.5 Types d'alarmes).
<b>Porte de garage</b>	Alarme d'intrusion avec temporisation d'entrée / de sortie, minuteur de porte de garage. Dans l'onglet Paramètres, il est possible de programmer cette réaction de sorte que la temporisation de sortie se prolonge par un détecteur d'état activé avec la réaction Porte de garage (par ex. pendant la durée d'ouverture de la porte de garage).
<b>Temporisée différée</b>	Alarme d'intrusion. Un détecteur propose la même temporisation de sortie que celle des détecteurs temporisés dans la même section. Ce détecteur ne propose la temporisation d'entrée que s'il est activé après le détecteur dont la réaction temporisée est programmée. S'il est le premier à être activé, l'alarme sera immédiatement activée. Ce paramètre n'a de sens que si le détecteur temporisé est activé dans la même section.
<b>Instantanée permanente</b>	Réaction instantanée de la zone. En cas d'armement et en fonction de l'activation, la réaction instantanée, y compris les avertissements d'alarme EW et IW, est également activée pendant la durée de temporisation de sortie.
<b>Instantanée/temporisée</b>	Le système réagit au déclenchement d'un détecteur (alarme, temporisation d'entrée) lorsqu'il est partiellement armé en tant que zone instantanée et lorsqu'il est complètement armé en tant que zone temporisée A.
<b>Instantanée confirmée</b>	Alarme d'intrusion instantanée - voir le chapitre <b>Réaction d'intrusion confirmée</b> ci-dessous.
<b>Temporisation confirmée</b>	Alarme d'intrusion avec une temporisation d'entrée et de sortie, minuteur A - voir le chapitre <b>Réaction d'intrusion confirmée</b> .
<b>Sabotage</b>	Alarme de sabotage permanente (il n'est pas nécessaire d'armer la section).
<b>24 heures</b>	Alarme d'intrusion immédiate (il n'est pas nécessaire d'armer la section).
<b>Détresse silencieuse</b>	Alarme de détresse silencieuse : 1) EW et IW non activés (voir le chapitre 8.5 Types d'alarmes) ; 2) Le clavier n'émet pas de bip à moins qu'il ne soit paramétré ainsi ; 3) Si le système peut distinguer qui a déclenché l'alarme de détresse (par ex. par le badge avec l'identité de l'utilisateur ou la saisie du code par l'utilisateur), il n'envoie pas de SMS de détresse à cet utilisateur.
<b>Détresse sonore</b>	Alarme sonore de détresse (le comportement est identique à une détresse silencieuse, cependant l'alarme est signalée par la sirène utilisée conformément au tableau du chapitre 8.5 Types d'alarmes).
<b>Alarme d'incendie</b>	Alarme d'incendie indépendante du statut de la section (il n'est pas nécessaire d'armer la section).
<b>Confirmation d'incendie</b>	Alarme d'incendie indépendante du statut de la section (il n'est pas nécessaire d'armer la section), voir le chapitre <b>Réaction d'incendie confirmée</b> ci-dessous.
<b>Incendie instantané</b>	Alarme d'incendie uniquement si la section respective est armée.
<b>Gaz</b>	Une alarme d'incendie déclenchée par un détecteur de fuite de gaz peut toujours être déclenchée quel que soit le statut de la section.
<b>Problèmes de santé</b>	Envoi d'un rapport relatif à un problème de santé.
<b>Inondation</b>	Envoi d'une alarme d'inondation
<b>Armé / Partiellement armé</b>	Armement (armement partiel) d'une section. Si la section est commune, toutes les sections qui lui appartiennent seront armées en même temps. Cette réaction est aussi dotée d'une fonction Désarmer.

<b>Silencieux</b>	Arrêt de la sirène interne avec rapport ultérieur de la présence d'un individu sur le site.
<b>Aucune</b>	Sans effet sur l'alarme d'intrusion, le périphérique peut cependant servir à l'activation des sorties PG. Les détections de sabotage, de supervision et des défaillances sont conservées.
<b>Aucune en l'absence de sabotage</b>	Le système réagit au déclenchement du détecteur uniquement par la commande de la sortie PG. Aucun type d'alarme n'est déclenché (même une alarme de sabotage), la détection de défaillance est maintenue.

### 8.4.3 Limitation des fausses alertes

Dans les installations présentant un risque élevé de fausses alertes, il est possible d'utiliser des types spéciaux de réaction :

**Réaction d'intrusion confirmée** - s'il y a une activation d'un détecteur dans la section armée, le système ne signale qu'une alarme non confirmée au centre de télésurveillance et attend une confirmation d'un autre détecteur. L'alarme peut être confirmée par n'importe quel détecteur d'intrusion dans la section armée. Dans l'onglet Paramètres, il est possible de déterminer si la confirmation est envoyée de n'importe quelle section armée ou de la même section. Il est aussi possible de programmer une période pendant laquelle le système attend la confirmation par un autre détecteur dans l'onglet Paramètres (jusqu'à 60 min.). Si la confirmation de l'alarme n'a pas eu lieu pendant la durée prédéfinie, l'alarme n'est pas déclenchée. En cas de paramétrage d'une réaction temporisée confirmée, l'activation du détecteur n'envoie qu'une alarme non confirmée une fois la temporisation d'entrée terminée. La réaction confirmée ne peut être utilisée que si un nombre supérieur de détecteurs d'intrusion est installé sur le site (pour activer la confirmation).

**Réaction d'incendie confirmée** - s'il y a une activation d'un détecteur d'incendie avec cette réaction, seule une alarme d'incendie non confirmée est signalée au centre de télésurveillance et le système attend la confirmation de l'incendie par un autre détecteur d'incendie. Dans l'onglet Paramètres, il est possible de déterminer si la confirmation est envoyée de n'importe quelle section armée ou de la même section. La durée d'attente de la confirmation de l'alarme d'incendie est programmée dans l'onglet Paramètres. Si la confirmation de l'incendie n'a pas eu lieu pendant la durée prédéfinie, l'alarme d'incendie ne se déclenche pas. La réaction confirmée ne peut être utilisée que si un nombre supérieur de détecteurs est installé sur le site (pour activer la confirmation).

**Avertissement** : cette fonction et son utilisation doivent être prises au sérieux conformément aux normes locales.

**Fonction Triple tentative (3x et STOP !)** - tous les détecteurs dotés d'une réaction d'alarme activée des types Intrusion et Incendie ont un nombre limité à trois activations maximales possibles de la centrale pendant une période de surveillance. Après trois activations (à la quatrième intrusion), une dérivation est activée pour l'entrée d'alarme correspondante et le capteur correspondant est exclu de toute activité ultérieure. Si ces trois activations se produisent au cours d'une alarme, trois messages SMS sont générés au total puis le détecteur est désactivé. Si ces trois activations se produisent à des intervalles de temps supérieurs à ceux de la durée de l'alarme, trois messages SMS sont générés, trois alarmes sont déclenchées puis le détecteur est désactivé.

Une dérivation peut être annulée en désarmant et en armant à nouveau la section, puis le détecteur retourne en mode de surveillance. La dérivation pour les réactions Incendie et Inondation est également automatiquement annulée le lendemain à 12h00. Le mécanisme des trois tentatives ne s'applique pas aux périphériques dotés d'une réaction de détresse.

**Rapport différé au centre de télésurveillance** - conformément à la norme EN50131-1, aux fins de réduction du nombre de fausses alarmes provoquées par l'utilisateur final par manipulation erronée du système et des interventions de l'agence de sécurité. Lorsqu'elle est activée, une alarme interne (sirènes, indication du clavier) sera déclenchée après l'expiration de la temporisation d'entrée, mais le système attendra 15 secondes pour envoyer un rapport d'alarme à la télésurveillance. Un utilisateur dispose de 15 secondes de plus pour désactiver le système sans déclencher une alarme signalée à la télésurveillance. S'il le fait à temps, rien ne sera signalé. Ce délai n'est lié qu'à une alarme déclenchée par une zone temporisée. D'autres types d'alarme (instantané, incendie, sabotage, etc.) sont signalés immédiatement sans temporisation, indépendamment de cette fonction.

## 8.5 Types d'alarmes

Le principal objet du système de sécurité est de signaler les événements à son propriétaire et ses utilisateurs ou une agence de sécurité professionnelle pour informer sur des menaces. Il pourrait s'agir d'un intrus mais aussi d'effets environnementaux tels que de la fumée, un incendie, des fuites de gaz, une inondation dans les locaux protégés. L'indication de chaque type d'alarme peut être différente conformément à sa cause. En ce qui concerne les sirènes, les alarmes sont divisées en type interne (IW) et externe (EW).

Tous les types de sirènes du système sonnent avec une tonalité intermittente (continue ou intermittente en option) et le clignotement de la sirène extérieure se fait par une lampe rouge ou bleue (clignotante). La durée d'indication est donnée par le paramètre de durée de l'alarme dans la centrale. Chaque sirène dispose de ses propres réglages, comme la limitation de la durée de l'alarme, permettant ainsi de prédéfinir une durée plus

courte d'indication d'alarme de la sirène externe par rapport à la sirène interne. Chaque alarme (à l'exception de l'alarme de détresse silencieuse) a un début et une fin (expiration ou annulation par l'utilisateur) et est enregistrée avec la cause de l'événement dans les événements avec un horodatage.

Sur tous les claviers du système, toutes les alarmes (à l'exception de l'alarme de détresse silencieuse) sont indiquées par un clignotement rouge de l'indicateur du système avec une indication acoustique continue.

**L'aperçu des sorties IW et EW en fonction du type d'alarme et du statut de la section se trouve dans le tableau suivant :**

Statut de la section	Type d'alarme					Réglage du système - paramètres		Activation	
	Intrusion	Sabotage	Détresse sonore	Incendie	24h / Inondation	Sirène IW lors de l'armement partiel	Sirène IW lors du sabotage	EW	IW
Désarmer		X				N/A	NON		
		X				N/A	OUI		X
			X			N/A	N/A	X	X
				X	X	N/A	N/A		X
Armer partiellement		X				N/A	NON		
		X				N/A	OUI		X
	X					OUI	N/A		X
	X					NON	N/A		
			X			N/A	N/A	X	X
				X	X	N/A	N/A		X
Armer	X	X	X	X	X	N/A	N/A	X	X

### 8.5.1 Alarme d'intrusion

C'est un état d'alarme de la centrale qui peut être déclenché par des détecteurs avec des réactions instantanées ou temporisées (et leurs variations), valable pour un système partiellement ou totalement armé. Il est indiqué par des sirènes internes et externes, voir le tableau ci-dessus. La durée de l'alarme est donnée par le réglage des paramètres de la centrale du système. À la fin d'une alarme, les claviers et les sirènes arrêtent de signaler. Lorsqu'un utilisateur est autorisé, il coupe l'indication acoustique de toutes les sirènes et des claviers, sans pour autant annuler le statut de l'alarme du système ni son désarmement. Cela doit être réalisé ultérieurement avec la touche fonctionnelle ou l'option de menu du clavier « Commande de section ».

### 8.5.2 Alarme de sabotage

La centrale supervise tous les périphériques inscrits vers le système indépendamment du statut du système (armé / désarmé). La plupart des périphériques ont un contact de sabotage intégré pour détecter l'ouverture de leur capot et l'arrachage du mur. Une activation déclenche une alarme de sabotage, signalée par une sirène interne (conformément au paramètre Sirène IW en cas de sabotage) dans un système désarmé, par les deux sirènes (interne et externe) dans un système armé, voir le tableau ci-dessus. Une alarme de sabotage peut également signifier la perte des périphériques BUS (par court-circuit par exemple) ou une tentative de décodage (10x) sur le clavier.

### 8.5.3 Alarme d'incendie

Une alarme d'incendie est déclenchée en actionnant les détecteurs avec une réaction d'incendie définie. Les détecteurs suivants sont tous pris comme des détecteurs d'incendie (fumée, haute température, détecteur de gaz combustibles ou détecteur de CO toxique). Une alarme d'incendie est indiquée par les sirènes internes lorsque le système est désarmé ou partiellement armé ; lorsque le système est armé, l'indication se fait par les sirènes internes et externes.

Il existe différents types d'alarmes :

1. **Incendie** - réaction de base pour tous les détecteurs d'incendie
2. **Incendie confirmé** - option pour une plus grande fiabilité. 2 détecteurs d'incendie doivent être au minimum installés dans chaque pièce avec les mêmes paramètres.
3. **Incendie instantané** - utilisé spécialement pour les locaux où il y a de la fumée en temps normal (restaurants, ateliers de soudure, etc.), la détection n'étant réalisée que lorsque le système est armé.
4. **Gaz** - réaction spéciale des détecteurs d'incendie avec l'identification de gaz combustibles et toxiques pour un rapport spécifique de cet événement à la télésurveillance.

### 8.5.4 Alarme de détresse

Une alarme de détresse est un événement spécial qui peut être déclenché de 2 manières différentes, sous forme de **détresse silencieuse** et de **détresse sonore**. Chacune d'elle a des comportements différents.

- 1) **Détresse silencieuse** - événement spécial non attribué à un groupe d'alarmes d'intrusion, qui seraient indiquées par une sirène ou un clavier. Une détresse silencieuse n'a pas de minuteur et il n'y a pas de fin à cet événement. Il ne peut donc pas être utilisé pour la commande du statut d'une sortie PG. Cela ne sert qu'à déclencher une alarme de détresse silencieuse et appeler de l'aide en cas de contrainte sans en informer l'attaquant. Une détresse silencieuse peut être déclenchée à partir d'une touche de détresse particulière (touche cachée ou portable), habituellement par une touche prédéfinie pour une détresse silencieuse, par une combinaison des touches A, B, C ou D de la télécommande, par un clavier avec une touche fonctionnelle spécialement prédéfinie pour une détresse silencieuse (dans ce cas, une alarme de détresse peut être temporisée avec un minuteur en option), en appuyant sur la touche de la sirène interne, par une entrée sur le module BUS destiné aux périphériques câblés ou en saisissant un code spécial pour le déclenchement d'une alarme de détresse silencieuse. Une détresse silencieuse peut également être déclenchée lorsque la commande d'accès sous contrainte est réalisée (voir le chapitre 9.8), le code de l'utilisateur standard étant alors modifié.
- 2) **Détresse sonore** - événement d'alarme habituel avec un début et une fin, indiqué par voie acoustique via la sirène et le clavier. Il peut être utilisé pour la commande du statut d'une sortie PG. Il est surtout utilisé pour déclencher une alarme de détresse avec une exigence d'indication optique ou pour bloquer les verrous électriques de porte, etc. Une alarme de détresse sonore peut être déclenchée à partir d'une touche de détresse particulière (touche cachée ou portable), habituellement par une touche prédéfinie pour une détresse silencieuse, par une combinaison de touches sur la télécommande, par un clavier avec une touche fonctionnelle spécialement prédéfinie pour une détresse silencieuse (dans ce cas, une alarme de détresse peut être temporisée avec un minuteur en option), en appuyant sur la touche de la sirène interne, par une entrée sur le module BUS destiné aux périphériques câblés.

**Attention** : les deux types d'alarme de détresse sont spécifiques du fait qu'ils pourraient être déclenchés à plusieurs reprises sans limitation ni blocage automatique.

### 8.5.5 Alarme 24 heures

Les détecteurs qui assurent une protection permanente (supervision de leur état) quel que soit le statut du système (armé ou désarmé) peuvent avoir une réaction prédéfinie de 24 heures ou de type Inondation. Ce type d'alarme est affecté au groupe d'alarmes d'intrusion, mais indépendamment de ce fait, il peut être déclenché lorsque le système est désarmé. Conformément au statut du système, une alarme est également indiquée par les sirènes internes et externes, voir le tableau ci-dessus. Les rapports d'alarme sont réalisés de la même manière que pour les autres alarmes.

## 8.6 Défaillances du système

Une défaillance est un signal d'avertissement du système qui indique un état anormal de la centrale, de la communication ou des périphériques. Le problème peut être lié à la radio, au module GSM supplémentaire ou au transmetteur LAN, au masquage des détecteurs (avec une fonction anti-masquage), aux problèmes d'alimentation (alimentation secteur ou batterie) ou à l'alimentation de secours. La ou les défaillances sont indiquées par voie optique sur les claviers du système par le voyant jaune du système. Le rapport de défaillance est issu de chaque source et à la 4<sup>e</sup> activation de défaillance, la source de la défaillance est dérivée, impliquant que la 4<sup>e</sup> défaillance n'est pas signalée.

L'aperçu des défaillances générales du système est donné dans le tableau suivant :

Source de la défaillance	Cause
Centrale	Alimentation secteur déconnectée pendant plus de 30 minutes
	Batterie de secours défectueuse ou faible dans la centrale
Transmetteur	Perte de connexion LAN, signal GSM perdu ou défaillance de ligne PSTN, au minimum 15 minutes
	Un ou des événements non délivrés à la télésurveillance dans un temps donné
Module radio	Brouillage de la bande radio 868 MHz
	Perte de communication BUS
Claviers	Perte de communication radio ou BUS (voir le chapitre 8.7)
Sirènes	
Modules	
Détecteurs	Masquage des détecteurs de mouvement (anti-masquage)
	Défaillance du détecteur interne (détecteur de fuite de gaz)
	Défaillance due à la réduction de l'intensité des rayons infrarouges (infra-barrière)

## 8.7 Défaillance provoquée par la perte d'un périphérique

Chaque périphérique (BUS ou sans fil) du système est supervisé par la centrale lorsque le paramètre Supervision est activé (voir l'onglet Paramètres / colonne Supervision) et si la communication avec la centrale est perdue (pas de réponse dans un délai prédéfini), alors le système déclenche l'évènement « Activation de la défaillance » et, conformément à l'évènement « Perte d'un périphérique BUS », une alarme de sabotage peut se déclencher. Le dispositif est optionnel et peut être déclenché lorsque le module radio détecte un brouillage RF ou une sorte d'interférence RF qui prend un minimum de 30 secondes à 2 niveaux de détection. Cela peut également déclencher une alarme de sabotage lorsqu'un court-circuit se produit sur le système BUS, empêchant la bonne communication des périphériques BUS. Le délai de communication est fixe et ne peut être modifié. Pour les périphériques BUS, le délai est de 8 secondes et pour les périphériques sans fil, il est de 120 minutes à compter de la dernière communication.

L'option modifiant la réaction de la centrale à la perte des périphériques BUS est appelée « **Perte d'un périphérique BUS** », voir le logiciel F-Link, onglet Paramètres. Les options suivantes sont proposées :

- **Défaillance** - la centrale traite toujours la perte d'un périphérique sur le BUS ou un court-circuit du BUS comme une défaillance.
- **Sabotage permanent** - la centrale traite la perte d'un périphérique sur le BUS ou un court-circuit du BUS comme une alarme de sabotage à chaque fois que cela se produit. Si le module radio possède une détection de brouillage RF autorisée et en cas de détection réelle, elle déclenche alors également une alarme de sabotage. Une alarme de sabotage est également suivie d'une défaillance et, lorsque la défaillance disparaît, l'alarme de sabotage disparaît.
- **Sabotage après confirmation** - la centrale traite la perte du premier périphérique comme une défaillance et si, dans un délai prédéfini donné par le paramètre « Période d'attente pour la confirmation d'alarme », une autre perte de périphérique se produit, alors le système confirme et déclenche une alarme de sabotage. Lorsque la défaillance de tous les périphériques perdus est restaurée, le système annule l'alarme de défaillance et de sabotage.

## 9 Options de commande du système

Le système de sécurité peut être commandé de différentes manières. Les options de commande de base sont locales ou à distance. D'autres options sont mentionnées dans le tableau suivant :

Type	Méthode / Mode	Périphérique	Condition	Description de la commande
Local	Clavier (autorisation et touche fonctionnelle)	JA-110E, JA-150E	Module radio JA-111R pour un clavier sans fil	L'exploitation peut être réalisée après l'autorisation de l'utilisateur, en appuyant sur une touche fonctionnelle spécifique ou via le menu du clavier.
	Lecteur RFID (autorisation uniquement)	JA-110E, JA-150E	Module radio JA-111R pour un clavier sans fil	L'exploitation peut être réalisée après l'autorisation de l'utilisateur, par l'utilisation d'un badge RFID ou la saisie d'un code
	Calendrier	10 actions de calendrier		Chaque action de calendrier dispose d'options de sélection des éléments suivants : événement, heure des performances, jour de la semaine. Il peut y avoir commande simultanée des sections et des sorties PG. Les sorties PG peuvent être bloquées.
	Logiciel F-Link ou J-Link	PC avec Windows	Câble USB	Les sections et les sorties PG peuvent être commandées après autorisation.
À distance	Menu vocal	Téléphone	Numéroteur GSM ou PSTN supplémentaire	Appel du numéro de téléphone du système et système de commande par tonalités DTMF après autorisation.
	Commande à distance	JA-16xJ	Module radio JA-111R	Armement ou désarmement en appuyant sur une touche prédéfinie d'une télécommande.
	Message SMS	Téléphone mobile	Numéroteur GSM supplémentaire	Commande autorisée pour l'armement ou le désarmement des sections ainsi que la commande des sorties PG.
	Numérotation à partir d'un numéro de téléphone autorisé	Téléphone (commande PG seulement)	Numéroteur GSM ou PSTN supplémentaire	Pour chaque numéro de téléphone autorisé, une sortie PG spécifique peut être commandée
	Logiciel F-Link ou J-Link	PC avec Windows (XP SP 3 ou supérieur)	Numéroteur GSM ou LAN supplémentaire	Les sections et les sorties PG peuvent être commandées par un clavier virtuel après autorisation.

Toutes les méthodes mentionnées peuvent être utilisées pour la commande du système (armement, armement partiel, désarmement) pour la commande de sortie PG (activer, désactiver, minuterie).

### 9.1 Méthode d'autorisation

L'autorisation est un facteur clé pour commander le système et vérifier si l'utilisateur est vraiment autorisé pour son exploitation. Conformément à la procédure d'autorisation, le système décide si l'utilisateur est autorisé à armer ou désarmer les sections, activer ou désactiver les sorties PG à l'aide des touches fonctionnelles ou s'il peut uniquement parcourir le statut du système et le journal de l'historique à l'aide du menu du clavier. Chaque utilisateur peut s'autoriser les options suivantes :

- Code d'accès (4 ou 6 chiffres en fonction du profil du système sélectionné, par défaut, EN, INCERT)
- Carte ou badge RFID
- Numéro de téléphone pour l'autorisation lors de l'accès à distance par appel téléphonique ou par SMS (lorsqu'un numéroteur GSM supplémentaire est connecté)

Pour ajuster le niveau de sécurité, le niveau d'autorisation peut être prédéfini sur les 2 niveaux suivants :

1. **Standard** - l'autorisation est réalisée en présentant des carte/badge RFID ou en saisissant un code d'accès valide

2. **Double autorisation** - Pour l'autorisation sur le clavier du système, il est toujours nécessaire de saisir un code d'accès valide et des badge/carte RFID (quel que soit l'ordre d'autorisation). Pendant l'accès à distance, le numéro de téléphone est toujours vérifié comme la saisie d'un code d'accès valide. F-Link surveille si un code et une carte sont affectés à un utilisateur dans l'onglet Utilisateurs (sinon F-Link ne permettra pas d'enregistrer la configuration).

**Attention** : la confirmation d'un code de l'utilisateur par une carte RFID réduit le risque d'exploitation non autorisée ou de prise de commande du système par un tiers.

## 9.2 Commande du système par le clavier

La meilleure façon de commander un système de sécurité et sa surveillance est d'utiliser un clavier système et, grâce à des voyants de commande principale LED de différentes couleurs indiquant le statut du système, les défaillances et les alarmes peuvent être vérifiées. Par l'utilisation d'autres touches fonctionnelles, le statut des sections et des sorties PG peut également être contrôlé, tout comme les options du système telles que l'indication de la mémoire d'alarme, le déclenchement d'une alarme de détresse ou des problèmes de santé. À l'aide d'un clavier, il est possible de naviguer dans le menu interne pour obtenir des informations relatives aux défaillances, aux événements, aux détecteurs actifs ou dérivés et ou aux détecteurs empêchant l'armement du système - l'ensemble est possible après une autorisation spécifique. Absence d'autorisation = absence d'accès au menu du clavier et conformément aux réglages individuels du clavier, les éléments du menu peuvent être rendus invisibles, protégeant ainsi le système contre tout fonctionnement non autorisé.

L'armement et le désarmement des sections est une fonction de base du clavier du système. Le système peut être armé complètement ou partiellement. La commande s'effectue de différentes manières :

1. Avec les touches fonctionnelles - l'enclenchement de la touche peut armer entièrement ou uniquement partiellement, ou bien partiellement et complètement. L'armement peut être suivi d'une autorisation (l'historique enregistre l'origine de l'armement d'une section déterminée) ou sans autorisation (aucun code n'est requis, l'historique n'enregistre donc pas l'origine de l'armement d'une section déterminée). Lors du désarmement du système par les touches fonctionnelles, l'autorisation est toujours requise ce qui permet d'enregistrer l'utilisateur à l'origine du désarmement dans la mémoire de la centrale.
2. Dans le menu du clavier - appuyer sur la touche « \* » après l'autorisation et armer partiellement, complètement ou désarmer.
3. Par autorisation uniquement - au vu des réglages, il est possible d'armer complètement (uniquement) et de désarmer par seule autorisation, par code ou par présentation des carte/badge RFID. Pour entrer dans le menu du clavier, appuyer sur la touche « \* » avant de s'autoriser soi-même.

### Procédure d'armement :

#### **1. Armement de la section complète avant de quitter les locaux protégés (locaux vides) :**

Un système entièrement armé est indiqué par une touche fonctionnelle de couleur rouge ou un numéro de section complètement surligné sur l'écran LCD du clavier pendant la commande du menu.

Pour la commande du système à partir d'un clavier placé dans des locaux protégés, il est nécessaire d'assurer un chemin de sortie et d'entrée, protégé par des détecteurs avec une réaction temporisée. Les zones de temporisation et de temporisation différée ne sont pas incluses dans la protection immédiatement après l'armement de la section, les zones ayant une réaction instantanée sont cependant incluses. L'utilisateur doit pouvoir quitter les locaux protégés après l'armement du système et avant l'expiration de la temporisation de sortie. Et lorsque la temporisation d'entrée est déclenchée par une zone temporisée, l'utilisateur doit pouvoir se rendre vers le clavier à partir duquel il doit désarmer le système. Si l'utilisateur ne désarme pas la section à temps (la temporisation d'entrée a expiré), le système déclenche une alarme dans la zone temporisée. Si l'entrée est réalisée par un chemin différent du chemin d'entrée, le système déclenche une alarme dans une zone instantanée - cela active immédiatement la sirène.

#### **2. Armement partiel, l'utilisateur reste dans les locaux :**

Un système partiellement armé est indiqué par une touche fonctionnelle de couleur jaune ou un numéro de section entièrement surligné sur l'écran LCD du clavier pendant la commande du menu.

Lorsque le système est partiellement armé, l'utilisateur reste dans les locaux protégés et seule la protection périphérique est incluse pour la surveillance (cela assure le libre mouvement à l'intérieur des locaux). Il existe 2 versions de commande :

- a) Commande à partir d'un clavier placé à l'intérieur des locaux protégés avec protection périphérique (hall d'entrée, etc.). Tous les détecteurs dans le hall d'entrée doivent être prédéfinis sur une réaction temporisée pour s'assurer que lorsque le système est armé, leur activation déclenche un délai permettant de laisser le temps d'entrer pour désarmer le système.
- b) Commande à partir d'un clavier placé à l'extérieur des locaux protégés avec une protection périphérique (hall interne, escaliers, chambre, etc.). Cette variante ne permet pas l'entrée d'une personne sans déclenchement instantané de l'alarme. Il est possible d'accéder aux locaux avec un désarmement préalable par télécommande, et en cas de module GSM supplémentaire connecté, par menu vocal ou par SMS. Dans ce cas, les détecteurs sont prédéfinis sur une réaction instantanée ou différée.



## Commande du système avec le clavier - procédure :

Le système propose plusieurs profils du système conformes aux différentes exigences de la norme, modifie également le comportement du clavier et bien sûr, la méthode de leur commande.

### Armement du système :

1. Une section désarmée est indiquée par une touche fonctionnelle qui s'allume en vert.
2. En appuyant sur la touche fonctionnelle, une demande d'armement de la section est émise. Un nombre supérieur de demandes peut être sélectionné en fonction du nombre de touches fonctionnelles utilisées.
3. Si l'autorisation est nécessaire pour l'armement de la section, la couleur rouge (armement complet) ou jaune (armement partiel) de la touche fonctionnelle indique le délai d'attente de l'autorisation par un clignotement lent (8 sec.).
4. La présentation des carte/badge RFID ou la saisie d'un code permettent l'autorisation (lorsqu'un code et une carte sont tous deux nécessaires, l'ordre est sans importance).
5. Si après une sélection, la touche fonctionnelle clignote toujours en rouge ou en jaune (8 sec.), le système détecte un obstacle empêchant l'armement (voir le chapitre 9.11 Obstacles empêchant l'armement du système).
6. Un armement ou un armement partiel réussi est confirmé par l'éclairage permanent de la touche fonctionnelle de couleur rouge ou jaune.

### Désarmement du système :

1. Une section armée est indiquée par une touche fonctionnelle qui s'allume en rouge ou en jaune. Lorsqu'une intrusion dans les locaux protégés est détectée, cela déclenche une temporisation d'entrée indiquée par un clignotement rapide de la touche fonctionnelle spécifique.
2. En appuyant sur la touche fonctionnelle désirée (ou plus de touches progressivement), une demande de désarmement de la section est opérée et la touche fonctionnelle indique une autorisation attendue par un clignotement lent.
3. La présentation des carte/badge RFID ou la saisie d'un code permettent l'autorisation (lorsqu'un code et une carte sont tous deux nécessaires, l'ordre est sans importance).
4. Un désarmement réussi est confirmé par l'éclairage permanent de la touche fonctionnelle de couleur verte.
5. Si après avoir désarmé la section, la touche fonctionnelle rouge continue à clignoter rapidement, elle indique la mémoire d'alarme dans la section. L'annulation de cette indication peut être réalisée en appuyant davantage sur cette touche avec l'autorisation d'annuler la mémoire de l'alarme ou en utilisant le menu du clavier LCD et en sélectionnant l'option « Annuler l'indication d'avertissement ».

### Indicateur du système du clavier - aperçu des statuts :

Voyants verts allumés	Fonctionnement normal. Les sections commandées par le clavier sont en ordre et sans défaillance.
Voyants jaunes allumés	Fonctionnement normal et dans certaines des sections contrôlées, une défaillance a été détectée. Dans le menu du clavier, il est possible d'obtenir des informations plus détaillées après autorisation de l'utilisateur en fonction des droits d'accès. Si la défaillance est suivie du logo rotatif Jablotron sur le clavier, cela représente une défaillance de la transmission radio entre la centrale et le clavier.
Voyants rouges allumés	Clavier en mode BOOT, lors d'une mise à niveau du micrologiciel.
Clignotement vert (2 Hz)	Autorisation réalisée, l'utilisateur peut modifier le statut du système par la touche fonctionnelle ou parcourir le menu du clavier. Le délai d'autorisation prend 8 secondes à compter de l'enclenchement de la dernière touche ou peut être annulé en appuyant sur ESC.
Clignotement jaune (8 Hz)	Indication d'avertissement de l'échec de l'armement.
Clignotement rouge (8 Hz)	Indication d'une alarme déclenchée actuellement dans une section spécifique sur le clavier. Le type d'alarme, le nom de la section où l'alarme a été déclenchée et la source de l'alarme déclenchée sont visibles sur le clavier LCD.
Clignotement alternatif rouge / jaune	Alarme déclenchée avec une défaillance active.
Clignotement alternatif vert / rouge	Autorisation avec mémoire d'alarme.
Clignotement alternatif vert / jaune	Autorisation avec une défaillance active.

Clignotement jaune (2x toutes les 2 secondes)	Mode Programmation / service. Toutes les touches fonctionnelles ne sont pas disponibles pour le menu du clavier de l'administrateur et des utilisateurs. Le menu du clavier n'est disponible que pour le technicien de service à moins qu'un PC ne soit connecté à la centrale.
Clignotement rouge (2x toutes les 2 secondes)	Indication de la mémoire d'alarme.
Clignotement jaune (1x toutes les 2 secondes)	Indication de défaillance sur le clavier en mode veille (valable uniquement pour le profil EN50131-1).
Clignotement rouge (1x toutes les 2 secondes)	Indication de la mémoire d'alarme sur le clavier en mode veille (valable uniquement pour le profil EN50131-1).
Absence d'indication	Clavier en mode veille.

#### Vue d'ensemble de l'indication optique de la touche fonctionnelle du clavier :

La touche s'allume en vert	Le statut de la section est Désarmé ou une sortie PG est désactivée.
La touche clignote en vert (4 Hz)	La temporisation d'entrée est en cours d'exécution et le système attend l'autorisation pour être désarmé.
La touche s'allume en jaune	Le statut de la section est Partiellement armé.
La touche s'allume en rouge	Le statut de la section est Armé ou Sortie PG activée.
La touche clignote en jaune (4 Hz)	Le système s'attend à une autorisation lorsqu'il est partiellement armé ou il signale une défaillance pendant l'armement partiel.
La touche clignote en jaune (8 Hz)	Indication d'avertissement de l'échec de l'armement.
La touche clignote en rouge (4 Hz)	Le système attend l'autorisation lors de l'armement ou il signale un problème lors de l'armement.
La touche clignote en rouge (8 Hz)	La mémoire d'alarme est indiquée jusqu'à ce qu'elle soit annulée.
La touche ne s'allume pas	Mode Service ou section bloquée après l'alarme.

### 9.3 Commande du système par télécommande

Si une commande du système avant l'accès aux locaux protégés est requise (arrivée en voiture dans le garage) ou un bâtiment doit être protégé uniquement par des détecteurs à réaction instantanée, cela garantit que personne ne peut désarmer le système à partir d'un clavier à l'intérieur des sites protégés (pas de chemin d'entrée), ce qui peut être réalisé à distance avant d'accéder au bâtiment. Cela nécessite que le module radio JA-111R soit inscrit vers le système pour la communication avec les périphériques sans fil. Il doit être placé au bon endroit pour assurer une communication fiable avec la télécommande en plus de la distance opérationnelle requise.

Chaque touche de commande peut commander une section choisie (la touche droite arme systématiquement et la gauche désarme systématiquement). Les télécommandes respectent les règles de la configuration du système, de sorte que tout obstacle empêchant l'armement rendra impossible l'armement du système.

L'utilisation d'une télécommande unidirectionnelle (JA-16xJ) indique par sa LED uniquement l'enclenchement de cette touche et l'envoi de la commande. Il n'y a pas de rétroaction de la centrale et l'utilisateur devrait utiliser un autre type d'indication d'état pour confirmer un changement d'état de la section, comme des stridulations de sirène, d'autres indications optiques ou des rapports SMS relatifs aux armement / désarmement.

### 9.4 Commande du système par un calendrier

La commande automatique du système peut être réalisée par le calendrier interne de la centrale. Le calendrier peut être prédéfini pour réaliser jusqu'à 10 actions (armement complet, armement partiel, désarmement des sections sélectionnées et blocage / déblocage ou activation / désactivation des sorties PG sélectionnées).

Chaque action peut permettre que les jours de la semaine (du lundi au dimanche) soient prédéfinis, seuls les jours ouvrés ou le weekend peuvent être prédéfinis. Pour chaque action, il est nécessaire de sélectionner l'heure et l'action particulière à réaliser ainsi qu'un événement (action) pour la commande de sortie PG. Ainsi, les sections peuvent être simultanément à des moments spécifiques armées ou désarmées et une sortie PG activée ou désactivée. Ce réglage sert de manière typique à l'armement automatique d'une section dans des magasins, l'armement partiel d'un immeuble pendant la nuit ou la commande des lumières la nuit. Chaque événement automatique est enregistré dans le journal de l'historique avec le nom de la source, « Calendrier ».

**Options de commande du calendrier liées à la surveillance :**

<b>Armement</b>	Le dispositif arme la ou les sections prédéfinies en commençant par une temporisation de sortie de 180 secondes (quelle que soit la durée du temps de sortie paramétrée dans la centrale) ; au cours de cette durée, toutes les zones d'alarme se comportent comme une zone temporisée. Une durée prolongée d'indication acoustique de sortie est destinée à avertir les utilisateurs qui se trouvent dans les locaux protégés du fait que le système a été armé par une minuterie automatique. Pendant cette période, l'utilisateur doit se rendre immédiatement vers le clavier du système et désarmer la section de la manière habituelle ou quitter les locaux protégés. S'il ignore cet avertissement, reste dans le bâtiment et continue de se déplacer, une alarme sera alors déclenchée. La centrale respecte pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement partiel</b>	Le dispositif arme partiellement la ou les sections prédéfinies en commençant par une temporisation de sortie de 180 secondes (quelle que soit la durée du temps de sortie paramétrée dans la centrale) ; au cours de cette durée, toutes les zones d'alarme se comportent comme une zone temporisée. Une durée prolongée d'indication acoustique de sortie est destinée à avertir les utilisateurs qui se trouvent dans les locaux protégés du fait que le système a été partiellement armé par une minuterie automatique. L'armement partiel n'est généralement pas indiqué par voie acoustique (voir l'onglet Paramètres pour l'activer). La centrale respecte pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement immédiat</b>	Le dispositif arme immédiatement la ou les sections prédéfinies sans temporisation de sortie ni indication acoustique. Le système est armé immédiatement, de sorte qu'aucun mouvement n'est possible dans les locaux protégés. Si quelqu'un continuait à se déplacer dans les locaux après un armement automatique, une alarme serait alors déclenchée dans la ou les sections définies. L'option permet un armement rapide et silencieux, sans avertissement. La centrale respecte pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement partiel immédiat</b>	Le dispositif arme partiellement et immédiatement la ou les sections prédéfinies sans temporisation de sortie ni indication acoustique. Le système est armé immédiatement au moment prédéfini. L'option permet un armement rapide et silencieux, sans avertissement. La centrale respecte pleinement toutes les méthodes de configuration et de vérification des règles d'armement des systèmes.
<b>Armement permanent</b>	Le dispositif arme la ou les sections prédéfinies en commençant par une temporisation de sortie de 180 secondes (quelle que soit la durée du temps de sortie paramétrée dans la centrale) ; au cours de cette durée, toutes les zones d'alarme se comportent comme une zone temporisée. La centrale ne respecte pas pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement partiel permanent</b>	Le dispositif arme partiellement la ou les sections prédéfinies en commençant par une temporisation de sortie de 180 secondes (quelle que soit la durée du temps de sortie paramétrée dans la centrale) ; au cours de cette durée, toutes les zones d'alarme se comportent comme une zone temporisée. La centrale ne respecte pas pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement permanent immédiat</b>	Le dispositif arme immédiatement la ou les sections prédéfinies sans temporisation de sortie ni indication acoustique. Le système est armé immédiatement, de sorte qu'aucun mouvement n'est possible dans les locaux protégés. L'option permet un armement rapide et silencieux, sans avertissement. La centrale ne respecte pas pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Armement partiel permanent et immédiat</b>	Le dispositif arme partiellement et immédiatement la ou les sections prédéfinies sans temporisation de sortie ni indication acoustique. Le système est armé immédiatement au moment prédéfini. L'option permet un armement rapide et silencieux, sans avertissement. La centrale ne respecte pas pleinement toutes les méthodes d'armement et de vérification des règles d'armement des systèmes.
<b>Désarmement</b>	Désarme la section prédéfinie à partir de n'importe quel niveau de protection (totalement ou partiellement armé).
<b>Aucun</b>	Aucune fonction de commande prédéfinie.

#### Options de commande de sortie PG à l'aide du calendrier :

<b>Activer PG</b>	Activer la ou les sorties programmables si elles ne sont pas bloquées (par exemple par des calendrier, périphérique ou section).
<b>Désactiver PG</b>	Désactiver les sorties PG programmables.
<b>Bloquer PG</b>	Bloquer les sorties PG prédéfinies. Ces sorties ne pourront absolument pas être allumées jusqu'à ce qu'elles soient débloquées par l'action de calendrier « Débloquer PG ». Entrer ou quitter le mode Service, ne pas débloquer
<b>Débloquer PG</b>	Débloquer le blocage de sortie PG prédéfini.
<b>Aucun</b>	Aucune fonction de blocage prédéfinie.

#### Action de blocage de la fonction par le calendrier :

Chaque action planifiée peut être bloquée par une sortie PG optionnelle. Sens du blocage : lorsqu'une sortie PG est activée, une action spécifique ne sera alors pas réalisée pendant un temps prédéfini. Ce blocage peut, par exemple, être une action de calendrier bloquée au profit d'un désarmement avant un départ en vacances. Le blocage peut être indiqué sur une touche fonctionnelle du clavier (prédéfini sur PG MARCHE / ARRÊT) nommée « vacances », etc.

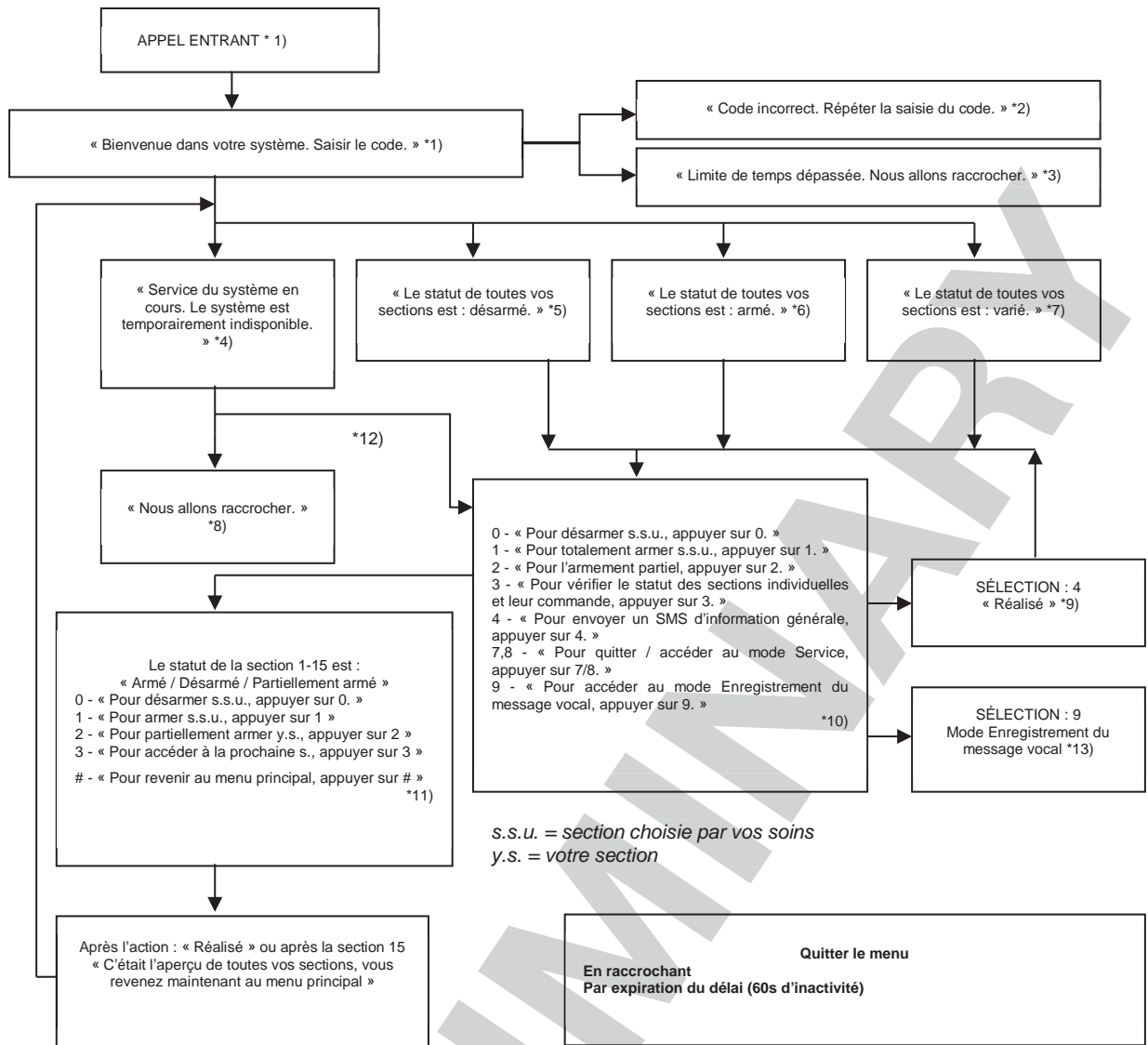
## 9.5 Commande du système via le menu vocal du transmetteur supplémentaire (GSM / PSTN)

Le système de sécurité peut être commandé à distance via un transmetteur supplémentaire (GSM ou PSTN) et des tonalités DTMF sur le téléphone portable de l'appelant. En appelant à partir d'un numéro de téléphone d'une carte SIM précédemment connu ou d'un numéro de téléphone de ligne fixe, le système reprend l'appel après un nombre prédéfini de sonneries (3 sonneries par défaut), la centrale lance un message vocal d'introduction et, conformément aux paramètres, demande éventuellement une entrée de code valide. L'appelant doit s'autoriser avec son code d'accès. Lorsque le code est validé, le système impose le statut de l'ensemble du système et, en fonction de l'autorisation de l'appelant, propose les options de commande disponibles.

Par menu vocal, il est possible de commander les sections, accéder et quitter le mode Service, enregistrer des messages vocaux avec le nom des sections individuelles et des rapports spéciaux. La commande des sorties PG est impossible via le menu vocal.

**Attention** : s'assurer que personne ne soit présent dans les locaux protégés avant l'armement du système à distance.

## Aperçu du menu vocal :



- \*1) Réponse après 3 sonneries. Le nombre de sonneries avant la réponse (1.10) est ajustable dans l'onglet Communication et l'onglet du transmetteur respectif où l'entrée dans le menu vocal sans code peut être autorisée.
- \*2) Saisie de code incorrecte. Après une troisième saisie incorrecte, l'appel sera raccroché.
- \*3) Délai de 60 sec. pour la saisie du code. Toutes les 5 sec., la demande « Saisir le code » est répétée.
- \*4) Le menu vocal ne peut pas être utilisé pendant le service.
- \*5) Toutes les sections qui peuvent être commandées sur la base d'une autorisation sont désarmées.
- \*6) Toutes les sections qui peuvent être commandées sur la base d'une autorisation sont armées.
- \*7) Les sections qui peuvent être commandées sur la base d'une autorisation sont dans des statuts variés.
- \*8) Valable pour toutes les autorisations à l'exception des télé-surveillance/service.
- \*9) Après l'envoi d'un SMS INFO au numéro de l'appelant.
- \*10) Les points du menu n'ayant pas de sens sont ignorés (par ex., si tout est armé, la sélection 1, 2, 3 est inapplicable).
- \*11) Le menu est adapté au statut effectif de la section.
- \*12) Si l'utilisateur a été autorisé par le code de service, la sélection 9 est possible - « Pour le Mode Enregistrement du message vocal, appuyer sur 9. ».
- \*13) Mode Enregistrement du message vocal **SÉLECTION 9** :
- 0 - « Pour enregistrer le nom de l'installation, appuyer sur 0 » puis « Appuyer sur l'astérisque (\*). »
- 1 - « Pour enregistrer les noms de section, appuyer sur 1 », saisir le numéro de la section à enregistrer, puis « Appuyer sur astérisque (\*). »
- 9 - « Pour supprimer tous les messages enregistrés, appuyer sur 9. »
- # - « Pour revenir au menu principal, appuyer sur #. »

### Remarques :

- 1 - « Vous n'êtes pas autorisé pour cette sélection » - systématiquement si l'utilisateur n'est pas autorisé à gérer une section ou vérifier le statut.
- 2 - « Rapport requis d'un message important, nous allons raccrocher dans 30 secondes » - les rapports / messages importants à la télésurveillance sont prioritaires sur le menu vocal en cours.
- L'entrée dans le mode Enregistrement est indiquée par un bip. Le message enregistré est rejoué pour une écoute immédiate après l'enregistrement.
- Si l'enregistrement est jugé insatisfaisant, il est possible de procéder à immédiatement un nouvel enregistrement.
- Il convient de commencer l'enregistrement immédiatement après le bip et d'appuyer sur le caractère final\* immédiatement après la fin de votre enregistrement.
- Le nom de l'installation peut durer 40 sec. au plus. Tout autre message peut durer 20 sec. au plus.

## 9.6 Consignes SMS

Le système peut être commandé avec des consignes SMS grâce à un transmetteur GSM supplémentaire. Les consignes SMS peuvent être utilisées pour commander les statuts paramétrés des différentes sections (armement, désarmement) ou tout simplement interroger les statuts des sections individuelles ou les autres statuts de l'ensemble du système. Les textes des consignes utilisés pour commander les sorties PG sont modifiables, les autres textes ne peuvent pas être modifiés. Il n'y a pas de consigne par défaut pour commander les sorties PG, il faut les définir en premier. Les autres textes sont déjà définis.

### Structure des consignes SMS

#### **Kkkk\_commande**

où : **kkkk** est le code de l'utilisateur ;  
\_ est un espace de séparation ;  
**commande** est la consigne d'exécution (voir la liste des commandes ci-dessous).

### Consignes de requête :

Une information sur le statut du système peut également être générée à l'aide des consignes suivantes :  
**DINFO, STATUT, COM et GSM** (les textes des consignes ne peuvent être modifiés).

### Consignes de commande :

La commande d'armement du **système** dans son ensemble ou simplement de ses **sections** individuelles peut être générée à l'aide des consignes suivantes :

**ARMER, DÉSARMER, ou ARMER x x x, DÉSARMER x x x, où x représente le numéro des sections** (les textes des consignes ne peuvent être modifiés).

Les consignes de commande pour la commande des sorties **PG** ne sont pas prédéfinies par le fabricant et, si nécessaire, doivent être créées.

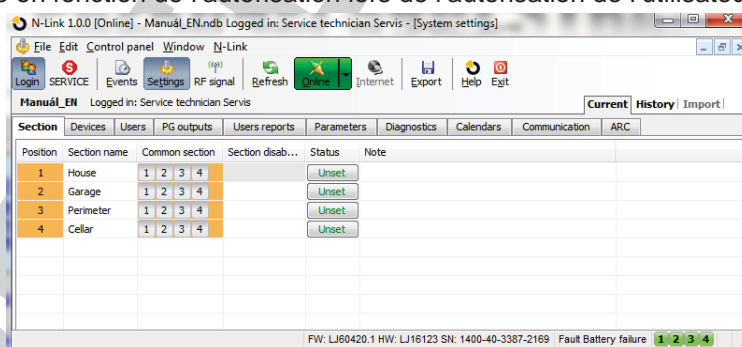
**Attention :** si les consignes de commande incluent des diacritiques spécifiques (comme pour certaines langues), le paramètre Diacritiques sur l'onglet Communication sous la touche « Paramètres JA-190Y » doit être activé pour un fonctionnement approprié et fiable. Il est également nécessaire de prendre en compte les lettres minuscules et majuscules en cas d'activation des diacritiques. Avec les caractères usuels, la taille n'importe pas.

Consigne et autorisation de commande	Réponse (exemple)	Remarque
<b>DINFO</b> (informations de base relative à l'installation)  <b>Autorisation :</b> Service, Administrateur	JABLOTRON 100: TYPE: JA-100K, SN: 14004026532523, SW: LJ60420, HW: LJ16123, RC: 79167-5FYA9-ZSQJ, GSM: 90%, GPRS: ok,  LAN: désactivé Time 17:01 22.7	Nom de l'installation conformément à l'onglet Communication Type de centrale Numéro de série Version du micrologiciel Version de l'équipement Code d'enregistrement du transmetteur GSM Qualité du signal GSM, disponibilité des données GPRS  Statut de la connexion LAN (activé ou désactivé) Heure et date de remise du SMS sur le réseau GSM
<b>STATUT</b> (statut des sections)  <b>Autorisation :</b> Service, Administrateur, Utilisateur Si l'utilisateur n'a accès qu'à certaines sections, le statut des sections qui lui sont accessibles sera transmis.	JABLOTRON 100 : Statut : Section 1 : désarmé ; Section 2 : armé ; Section 3 : désarmé ; Section 4 : armé ; erreur ;  GSM : 90% ; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Statut : Nom et statut de la section 1 Nom et statut de la section 2 Nom et statut de la section 3 Nom et statut de la section 4  Force du signal GSM Heure et date de remise du SMS sur le réseau GSM
<b>COM</b> (information relative à la communication)  <b>Autorisation :</b> Service	JABLOTRON 100: GSM: 90%, DATA: ok, CELLID: 44905, OPID: 23003, LAN: ok, MAC: hh:hh:hh:hh:hh:hh, PSTN: off, ARC: 1:ok, 2:ok, 3:off, 4:ok, 5:off, Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Qualité du signal GSM, disponibilité des données GPRS Numéro de la cellule et opérateur assurant la connexion GSM Statut de la connexion LAN et adresse MAC Statut de la connexion téléphonique (possible avec JA-190X) Statut d'activation des transmissions à chaque télésurveillance Heure et date de remise du SMS sur le réseau GSM
<b>GSM</b> (redémarrage GSM)  <b>Autorisation :</b> Service, Administrateur, Utilisateur	JABLOTRON 100: SMS processed OK: GSM; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Confirmation de remise du SMS (avant le redémarrage) Heure et date de remise du SMS sur le réseau GSM
<b>ARMER</b> (commande de l'ensemble du système)  <b>Autorisation :</b> Tout	JABLOTRON 100 : Statut : Section 1 : armé ; Section 2 : armé ; Section 3 : armé avec zone active ; Section 4 : armé ; erreur ;  GSM : 90% ; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Statut : Nom et statut de la section 1 Nom et statut de la section 2 Nom et statut de la section 3 Nom et statut de la section 4  Force du signal GSM Heure et date de remise du SMS sur le réseau GSM

<b>DÉSARMER</b> (commande de l'ensemble du système)  <b>Autorisation :</b> Tout	JABLOTRON 100 : Statut : Section 1 : désarmé ; Section 2 : désarmé ; Section 3 : désarmé ; Section 4 : désarmé, erreur ; GSM : 90% ; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Statut : Nom et statut de la section 1 Nom et statut de la section 2 Nom et statut de la section 3 Nom et statut de la section 4 Force du signal GSM Heure et date de remise du SMS sur le réseau GSM
<b>ARMER 1 3</b> (commande des sections choisies du système)  <b>Autorisation :</b> Tout	JABLOTRON 100 : Statut : Section 1 : armé ; Section 3 : armé avec zone active ; GSM : 90% ; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Statut : Nom et statut de la section 1 Nom et statut de la section 3 Force du signal GSM Heure et date de remise du SMS sur le réseau GSM
<b>DÉSARMER 2 4</b> (commande des sections choisies du système)  <b>Autorisation :</b> Tout	JABLOTRON 100 : Statut : Section 2 : désarmé ; Section 4 : désarmé ; GSM : 90% ; Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Statut : Nom et statut de la section 2 Nom et statut de la section 4 Force du signal GSM Heure et date de remise du SMS sur le réseau GSM
<b>CRÉDIT</b> (Vérification du solde créditeur sur la carte SIM prépayée)  <b>Autorisation :</b> Tout	JABLOTRON 100 : ... ... ... Time 17:01 22.7.	Nom de l'installation conformément à l'onglet Communication Texte de la réponse du fournisseur GSM Texte de la réponse du fournisseur GSM Texte de la réponse du fournisseur GSM Heure et date de remise du SMS sur le réseau GSM

## 9.7 Contrôle du système via F-Link

Le logiciel F-Link est utilisé pour la programmation locale et à distance de l'ensemble du système ou pour l'édition d'un utilisateur ; il autorise la visualisation des statuts des sections et la commande des sections. La commande est possible en cliquant sur l'onglet « Section » dans la colonne « Statut » ou en cliquant sur le numéro de la section sur la barre de menu inférieure. Le système enregistre la commande du système sur sa mémoire événementielle en fonction de l'autorisation lors de l'autorisation de l'utilisateur dans le logiciel.



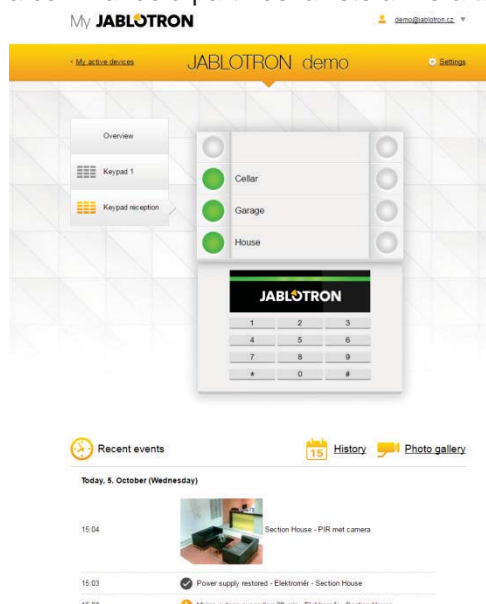
## 9.8 Commande via l'application Internet MyJABLOTRON

La commande à distance via l'application Internet MyJABLOTRON est la manière la plus conviviale de commander le système de sécurité à partir de n'importe quel navigateur Internet quelle que soit la plate-forme informatique. Une fois la connexion sécurisée, l'application vous permet de commander le système non seulement à partir du clavier virtuel de chaque clavier physique présent dans le système, mais vous permet également de commander toutes les sections et les sorties PG d'une liste globale. L'utilisateur peut également parcourir l'historique des événements détaillés, y compris des clichés pris. De nouvelles photos peuvent être prises instantanément à la demande d'un utilisateur. Au contraire du système physique, l'utilisateur peut visualiser les températures effectives à partir des thermomètres, les valeurs de différents compteurs et



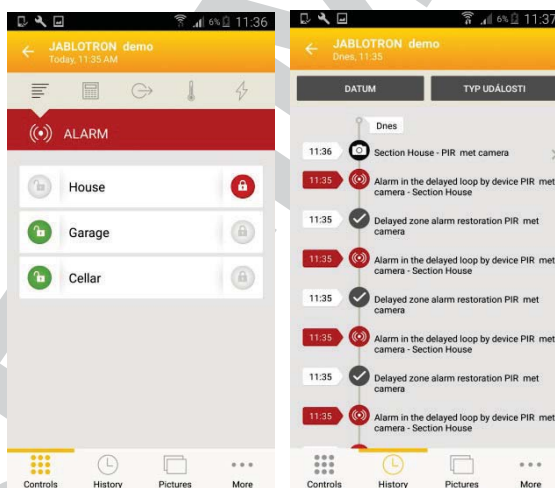
configurer les messages l'informant sur les événements du système ou des valeurs définies par l'utilisateur (telles que la température).

Il est nécessaire de saisir le code de l'utilisateur à chaque connexion pour commander le système. L'armement des sections à l'aide de touches fonctionnelles est identique à leur configuration réelle. Si les touches fonctionnelles permettent un armement partiel, il sera possible d'armer partiellement le système à distance. Dans tous les autres cas, la commande à partir de la liste armera toujours des sections entières.



## 9.9 Commande via l'application mobile MyJABLOTRON

Les utilisateurs de MyJABLOTRON peuvent télécharger une application pour les smartphones, disponible pour iOS et Android. L'application mobile est la manière la plus conviviale de commander le système de sécurité que l'utilisateur peut même avoir en poche grâce à un accès Internet presque illimité. Une fois la connexion sécurisée, l'application permet de commander le système non seulement à partir du clavier virtuel de chaque clavier physique présent dans le système, mais permet également de commander toutes les sections et les sorties PG d'une liste globale.



## 9.10 Commande d'accès sous contrainte

Cette option, désactivée avec les paramètres par défaut, permet aux utilisateurs de commander (armer ou désarmer) le système avec un code différent lorsqu'ils sont menacés par une autre personne. Ce code attirera discrètement l'attention sur une situation de ce type en déclenchant une alarme de détresse silencieuse sans indication acoustique ou visuelle. Une alarme de détresse est déclenchée en ajoutant 1 au code de l'utilisateur existant.

### Exemple :

Code utilisateur = 4444. Code de commande d'accès sous contrainte = 4445.

**Avertissement** : Si le code de l'utilisateur se termine par le chiffre 9 et en cas d'utilisation de la commande d'accès sous contrainte, le dernier numéro du code sera alors 0 (4449 - 4440).

## 9.11 Obstacles empêchant l'armement du système

Conformément aux **Méthodes d'armement** (voir l'onglet Paramètres), la centrale peut vérifier les statuts déclenchés ou défaillants des périphériques individuels ou d'une section particulière lors de l'armement de chaque section du système. Grâce à cette option, la centrale indique certains obstacles pendant l'armement (obstacles franchissables) et certains états, elle peut même empêcher le système de s'armer le cas échéant (obstacles infranchissables).

L'un des obstacles les plus courants est la défaillance du système (indiquée par un voyant du système jaune), une perte de connexion avec un détecteur sans fil ou un détecteur d'état déclenché (typiquement un capteur d'ouverture magnétique) armé avec une réaction de zone temporisée (capteurs de porte d'entrée et porte de garage), une faible batterie du système, une panne d'alimentation de longue durée ou une défaillance de communication de l'un des transmetteurs. Le dispositif est influencé par le profil du système.

Un obstacle infranchissable empêchant l'armement du système est par exemple constitué par un **détecteur d'état** déclenché (habituellement un capteur d'ouverture de porte magnétique) défini avec une réaction **Instantanée**. Les périphériques qui appartiennent à ce groupe sont des détecteurs d'ouverture de fenêtre, de balcon ou de porte de service, mais il peut également s'agir de défaillances systémiques critiques telles qu'une défaillance d'alimentation de secours ou de communication avec la télésurveillance. Les raisons qui empêchent les armements du système sont différentes en fonction du profil du système prédéfini. Une exception empêchant le système d'armer une section qui ne vérifie aucun détecteur déclenché ou défaillance est constituée par l'armement automatique par un calendrier en utilisant l'option « Armement .... permanent ». Le calendrier armera toujours chaque section sous réserve qu'il soit configuré pour réaliser une telle action.

Le déclenchement d'un détecteur d'impulsions (ex. de détecteurs : mouvement, bris de verre, inclinaison, choc et similaire) ne peut empêcher l'armement.

Le système informe quant à l'armement avec une zone active par un rapport SMS (à un groupe d'utilisateurs avec des rapports d'alarme prédéfinis) avec une description détaillée.

### Méthodes d'armement - aperçu du tableau

	Clavier du système	Via les menu vocal / SMS / télécommande / calendrier	F-Link J-Link	Application Internet et mobile
<b>Armement permanent</b>	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés
<b>Armement avec avertissement</b>	En essayant d'armer avec une défaillance ou un périphérique déclenché, le clavier clignote pendant 8 secondes, puis le système s'arme automatiquement. Il est possible d'armer le système en appuyant de nouveau sur la touche fonctionnelle ou en appuyant sur la touche Entrée.	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement conformément à « Méthodes d'armement » dans l'onglet Configuration du service
<b>Armement après confirmation</b>	En essayant d'armer avec une défaillance ou un périphérique déclenché, le clavier clignote pendant 8 secondes, puis le système s'arme automatiquement. Il est possible d'armer le système en appuyant de nouveau sur la touche fonctionnelle ou en appuyant sur la touche Entrée.	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés	Armement conformément à « Méthodes d'armement » (armement avec vérification / armement sans vérification) dans l'onglet Configuration du service

<p><b>Absence d'armement avec un élément actif</b></p>	<p>En essayant d'armer avec une défaillance ou un périphérique déclenché, le clavier clignote pendant 8 secondes, puis le système s'arme automatiquement. Il est possible d'armer le système en appuyant de nouveau sur la touche fonctionnelle ou en appuyant sur la touche Entrée.</p>	<p>Absence d'armement lorsqu'un détecteur déclenché est armé sur une réaction de zone INSTANTANÉE</p>	<p>Armement permanent en dépit des défaillances ou du statut des périphériques déclenchés</p>	<p>Absence d'armement lorsqu'un détecteur déclenché est armé sur une réaction de zone INSTANTANÉE</p>
--	--	---	---	---

## 9.12 Échec de l'armement

C'est une fonction de sécurité permettant à la centrale de vérifier si l'armement du système peut être exécuté au cours de la temporisation de sortie, la sécurité des locaux protégés n'étant pas limitée par les cas suivants. Si la fonction est activée, alors l'**échec de l'armement** peut être provoqué par les points suivants :

1. Activation instantanée du détecteur à tout moment pendant la temporisation de sortie (un individu entre dans une zone déjà protégée)
2. Activation permanente d'un détecteur avec une réaction différée après expiration de la temporisation de sortie (l'utilisateur a oublié de fermer la porte principale, le garage ou le portail, etc.)

Dans le cas où l'armement du système est empêché, un événement « Échec de l'armement » est déclenché et signalé par un clignotement rapide du voyant du système avec une couleur jaune sur les claviers, des bips ainsi que par voie acoustique par une sirène extérieure. Il est simultanément signalé à un utilisateur spécifique ou à l'administrateur du système si le rapport « Échec de l'armement » est activé, voir le logiciel F-Link, onglet Communication.

Pour annuler l'indication d'un échec de l'armement, il faut sélectionner dans le menu du clavier l'option intitulée « Annuler l'indication d'avertissement » ou si le profil du système « par défaut » a été prédéfini, en armant alors cette section.

## 9.13 Tableau récapitulatif des groupes d'évènements signalés aux utilisateurs

Lorsqu'un transmetteur GSM ou PSTN supplémentaire est connecté, les événements du système peuvent être envoyés non seulement à la télésurveillance mais aussi à 8 utilisateurs max. (alarmes, appels vocaux et rapports SMS). Les événements qui peuvent être signalés aux utilisateurs sont divisés en 5 groupes. Chaque groupe peut être assigné aux utilisateurs arbitrairement. Les utilisateurs auxquels un groupe sera assigné recevront des rapports de ce groupe. Lorsque les paramètres de base des groupes sont insuffisants, 2 groupes spéciaux existants et définis par l'utilisateur peuvent être utilisés. Les événements sélectionnés peuvent être ajoutés à ces groupes et donc uniquement signalés aux utilisateurs spécifiques.

**Tableau de synthèse :**

Commande	Évènement	Groupe
1	Armement	SMS relatif aux armement / désarmement (3)
2	Désarmement	SMS relatif aux armement / désarmement (3)
3	Armement partiel	SMS relatif aux armement / désarmement (3)
4	Défaillance de l'alimentation 30 min.	Alertes SMS (1) / Appel d'alarme (2)
5	Restauration du courant après 30 min.	Alertes SMS (1) / Appel d'alarme (2)
6	Alarme instantanée	Alertes SMS (1) / Appel d'alarme (2)
7	Alarme instantanée annulée	Alertes SMS (1) / Appel d'alarme (2)
8	Temporisation d'alarme	Alertes SMS (1) / Appel d'alarme (2)
9	Temporisation d'alarme annulée	Alertes SMS (1) / Appel d'alarme (2)
10	Alarme de sabotage	Alertes SMS (1) / Appel d'alarme (2)
11	Alarme de sabotage annulée	Alertes SMS (1) / Appel d'alarme (2)
12	Alarme d'incendie	Alertes SMS (1) / Appel d'alarme (2)
13	Alarme d'incendie annulée	Alertes SMS (1) / Appel d'alarme (2)
14	Alarme de détresse	Alertes SMS (1) / Appel d'alarme (2)

15	Alarme de détresse annulée	Alertes SMS (1) / Appel d'alarme (2)
16	Problèmes de santé	Alertes SMS (1) / Appel d'alarme (2)
17	Inondation	Alertes SMS (1) / Appel d'alarme (2)
18	Tentative de décodage	Alertes SMS (1) / Appel d'alarme (2)
19	Armé avec une zone active (en cas de confirmation activée)	Alertes SMS (1) / Appel d'alarme (2)
20	Section sans mouvement	Alertes SMS (1) / Appel d'alarme (2)
21	Activation du mode Surchauffe	Alertes SMS (1) / Appel d'alarme (2)
22	Désactivation du mode Surchauffe	Alertes SMS (1) / Appel d'alarme (2)
23	Activation du mode Gel	Alertes SMS (1) / Appel d'alarme (2)
24	Désactivation du mode Gel	Alertes SMS (1) / Appel d'alarme (2)
25	Démarrage du système (en mode Service)	SMS de défaillance et de service (5)
26	Batterie faible du périphérique	SMS de défaillance et de service (5)
27	Batterie du périphérique OK	SMS de défaillance et de service (5)
28	Défaillance (périphérique, transmetteur)	SMS de défaillance et de service (5)
29	Fin de la défaillance	SMS de défaillance et de service (5)
30	Accès au mode Service	SMS de défaillance et de service (5)
31	Sortie du mode Service	SMS de défaillance et de service (5)
32	BATTERIE faible	SMS de défaillance et de service (5)
33	BATTERIE OK	SMS de défaillance et de service (5)
34	Défaillance de communication à la télésurveillance	SMS de défaillance et de service (5)
35	Communication à la télésurveillance restaurée	SMS de défaillance et de service (5)
36	Brouillage RF	SMS de défaillance et de service (5)
37	Fin de brouillage RF	SMS de défaillance et de service (5)
38	Crédit faible	SMS de défaillance et de service (5)
39	Photo d'alarme	Photo (5)

L'inscription des événements en groupes, définis par le système, est indiquée dans le tableau. En cas d'apparition d'un événement, le système génère un SMS au format suivant :

**Nom de l'installation** (voir l'onglet Configuration)

**Temps** (de survenue d'un événement), **Évènement** (voir le tableau).

**Source de l'évènement** (voir l'onglet Périphériques / Nom ou Utilisateur / Nom), **Section** (où l'évènement s'est produit) ;

**Temps** (heure et date d'envoi)

Exemple de SMS envoyé :

**JABLOTRON 100**

(nom de l'installation)

**17:01:10, Alarme temporisée**

(heure de l'évènement, évènement)

**Aimant de porte, Rez-de-chaussée**

(nom du détecteur, nom de la section)

**17:01:25, Alarme instantanée**

(heure de l'évènement, évènement)

**Mouvement dans l'escalier, Étage**

(nom du détecteur, nom de la section)

**Temps 17:01 22.7.**

(heure d'envoi)

## 9.14 indication acoustique du système

L'indication acoustique du système peut indiquer non seulement le statut de l'alarme, mais aussi d'autres états ou des modifications d'état. Pour un aperçu relatif à l'indication acoustique, voir les tableaux suivants :

**Indication acoustique par les clavier / lecteur :**

Son	Description de l'action
Un bip court	Touche de confirmation
Un bip long	Activation de la touche fonctionnelle, armement d'une section ou activation d'une PG
Deux bips longs	Désactivation de la touche fonctionnelle, désarmement d'une section ou désactivation d'une PG

Deux bips longs répétés	Échec de l'armement
Trois bips longs	Section désarmée avec indication de mémoire d'alarme
Bip permanent	Temporisation de sortie
Bip continu	Temporisation d'entrée
	Alarme

**Indication acoustique par des sirènes intérieures / extérieures :**

Son	Description de l'action
Un bip court	Armement de la section
	Activation de la sortie PG
Deux bips courts	Désarmement de la section
	Désactivation de la sortie PG
Trois bips courts	Section désarmée avec indication de mémoire d'alarme
	Échec de l'armement
	Armement avec une zone active (jusqu'au micrologiciel 13 uniquement)
Bip rapide permanent	Indication de statut PG - bip rapide
Bip lent permanent	Temporisation de sortie
	Indication de statut PG - bip lent
Bip continu	Temporisation d'entrée
	Indication de statut PG - stridulation permanente
Sifflement	Alarme dans une section

**Indication acoustique des détecteurs d'incendie (fumée, thermique, gaz) :**

Son	Description de l'action
Bip rapide permanent	Alarme d'incendie
Hurllement permanent	

## 9.15 Désactivation et blocage des options

### 9.15.1 Désactivation

Avant d'armer le système, il se peut qu'un périphérique doive être intentionnellement éliminé de la surveillance par dérivation (par exemple, un garage en raison d'une activité de construction ou la présence d'un chien dans une pièce habituellement protégée). Cette option est intitulée **Désactivation du périphérique** et est disponible dans le menu du clavier ou avec le logiciel F-Link pour le technicien de service ; elle peut être mise en œuvre à deux niveaux conformément à l'autorisation de l'utilisateur :

1. **Blocage de l'entrée (BLK)** - la fonction consiste à bloquer une entrée de détecteur (elle bloque son activation). Le système ignore toute activation du détecteur = une alarme n'est pas déclenchée, il n'y a aucun rapport d'activation PG. Les alarmes de sabotage, les défaillances ou les rapports de batterie faible sont surveillés en permanence. Dans le logiciel F-Link, cela est indiqué par un point jaune. L'administrateur et le technicien de service peuvent autoriser et réaliser le blocage.
2. **Désactivation du périphérique (DIS)** - cette fonction permet de désactiver (DIS) un détecteur. Le système ignore toutes les fonctions du périphérique = il ne déclenche aucune alarme ni alarme de sabotage, rapport ou défaillance. Dans le logiciel F-Link, cela est indiqué par un point rouge. L'autorisation de désactivation est uniquement réalisée par le technicien de service.

Un périphérique tout comme une section peuvent également être **désactivés**, mais seul un des deux sans la centrale. Ceci s'applique également aux utilisateurs, sauf ceux correspondant aux positions 0 (technicien de service) et 1 (Administrateur), aux sorties PG ou aux actions du calendrier. La désactivation est permanente jusqu'à ce qu'elle soit annulée par la même procédure que l'activation.

**Attention** : il est impossible de bloquer ou désactiver la centrale ou un périphérique avec la réaction Détresse !

## 9.16 Fonctions non relatives à une alarme - Fonctions des sorties PG

Le système de sécurité permet aux utilisateurs autorisés (conformément aux paramètres) de commander les fonctions du système - les fonctions liées à la protection des sections ainsi que la commande des sorties PG programmables (marche / arrêt). En utilisant des modules relais ou un module doté de sorties semi-conductrices spéciales, des périphériques peuvent être enclenchés, tels que des indicateurs acoustiques ou d'autres appareils liés au système de sécurité, comme des lumières, des systèmes de commande d'accès, le

blocage du chauffage lorsqu'une fenêtre est ouverte ou lorsqu'une section est armée, l'arrosage du jardin, etc., autrement dit ce qui concerne la domotique.

Fonction de sortie PG	Description	Exemple
Marche / arrêt	L'état de sortie stable dédié peut être modifié par une commande arbitraire ou un périphérique.	Mise en marche manuelle des appareils à l'aide d'une touche fonctionnelle, d'un SMS ou par certains périphériques avec une option de coupure manuelle sans limitation. En règle générale, la commande du chauffage, la climatisation, les lumières
Impulsion	Statut de sortie stable et simple avec temps prédéfini	Commutation par impulsion d'autres circuits de commande supplémentaires tels que la commande du portail, des stores, des jalousies, de l'arrosage du jardin, des verrous de porte, etc.
Copier	Statut de sortie avec la logique OR. La sortie sera active si au minimum un périphérique est également actif, mais la désactivation se produit lorsque tous les périphériques de commande sont inactifs.	Utile pour l'indication de certains états individuels ou collectifs (généralement des fenêtres ouvertes, des portes de garage, etc.) sur la touche fonctionnelle du clavier. De même, les statuts de toutes les sections, les alarmes, les mémoires d'alarme, les défaillances et bien d'autres événements peuvent également être indiqués lorsque le début et la fin sont indiqués.

Le système propose également des fonctions utilisatrices telles que la mesure de la température, qui peut être affichée sur le clavier LCD et dans l'application MyJABLOTRON.

## 10 Armement du système avec le logiciel F-Link

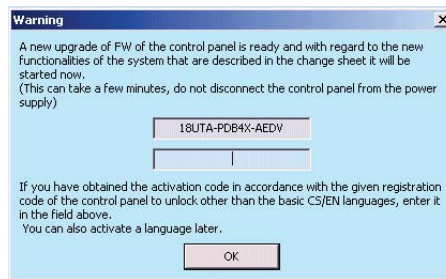
Le système JABLOTRON 100 est exclusivement configuré à l'aide d'un ordinateur via le programme F-Link. La version actuelle du logiciel F-Link peut être obtenue auprès du distributeur ou fournisseur ou être téléchargée après autorisation sur [www.myjablotron.com](http://www.myjablotron.com).

Immédiatement après l'ouverture de la fenêtre initiale de sélection de la connexion, le programme F-Link peut être commuté sur l'environnement linguistique souhaité en cliquant sur l'icône de la langue (drapeau). La langue peut être ultérieurement modifiée à tout moment dans le menu F-Link. La fenêtre initiale propose les options suivantes :

- Connexion locale** - pour la connexion de l'ordinateur à la centrale. Un câble USB est nécessaire (avec les connecteurs A-B).
- Connexion à distance** - option permettant une connexion à distance à partir d'une base de données de fichiers enregistrés préalablement. Pour établir une communication à distance avec la centrale, l'ordinateur doit avoir accès à Internet et la centrale doit voir le transmetteur LAN connecté à Internet ou avoir un transmetteur GSM supplémentaire doté d'une carte SIM de données. Pour une connexion sans problème, d'autres conditions doivent être remplies comme par ex. l'autorisation de configuration à distance dans la centrale, un code d'enregistrement approprié, un code de service, et si le transmetteur LAN n'est pas utilisé, alors un signal GSM suffisant au niveau de l'emplacement de la centrale.
- Paramètres hors connexion** - ils permettent d'accéder aux données de configuration de la centrale. Il est ici possible par ex. d'obtenir la liste des périphériques ou des enregistrements du dernier remplacement de la batterie, etc.

### 10.1 Démarrage du programme F-Link et configuration de la dimension du système

- Connecter l'ordinateur à la centrale avec un câble USB - l'ordinateur initialisera le nouveau dispositif USB (lors de la première connexion de la centrale, cela peut prendre un certain temps).
- Après la connexion, l'ordinateur affichera deux lecteurs nouvellement trouvés : FLEXI\_CFG et FLEXI\_LOG. En cas d'affichage dans une nouvelle fenêtre, il est possible de la fermer.
- Démarrer le programme F-Link. Si la centrale est paramétrée par défaut, la fenêtre Configuration s'ouvrira et le système passera automatiquement en mode Service. Si la centrale a déjà été paramétrée (son code de service a été modifié), le programme demandera la saisie du code - il doit être saisi au format **nnnn** (le code Service par défaut est 1010). Il est possible d'utiliser l'option **Garder en mémoire** pour que le programme enregistre le code jusqu'à la fermeture de la base de données. Utiliser l'option **Affichage du code** pour vérifier le code saisi, par ex. en cas d'utilisation d'un clavier alphanumérique où une erreur peut être commise.
- Après une autorisation valide, ce message peut être affiché :



Dans un tel cas, il est recommandé de réaliser une mise à jour. En cliquant sur la touche OK, le nouveau micrologiciel est téléchargé, ce qui peut prendre quelques minutes. Lorsque le processus de mise à jour est terminé, l'assistant fait apparaître l'onglet de configuration initiale.

Remarque : Après avoir établi la connexion avec le câble USB, la possibilité de modifications de programmation des paramètres du clavier LCD sera désactivée (l'élément du menu Paramètres est désactivé). Après déconnexion du câble, l'élément s'affiche de nouveau dans le menu en quelques secondes.

## 10.2 Onglet Sections

Il est utilisé pour configurer les paramètres des sections surveillées et commandées indépendamment (zones). Pour apporter des modifications dans cet onglet, il n'est pas nécessaire d'être en mode Service.

Position	Section name	Common section	Section disabled	Status	Note
1	House	1 2 3 4		Service mode	
2	Garage	1 2 3 4		Service mode	
3	Garden	1 2 3 4		Service mode	
4	Shop	1 2 3 4		Service mode	

**Nom de la section** - désignation des sections utilisées aux fins d'élaboration de rapports événementiels textuels (SMS), d'affichage sur un clavier et de lecture de la mémoire, pour faciliter la reconnaissance en cas de rapport (par ex. rez-de-chaussée, magasin, etc.).

**Section commune** - permet de programmer l'armement automatique de la section si toutes les sections pour lesquelles elle est commune sont armées (adapté pour les couloirs, les escaliers et les autres parties communes). Avertissement relatif à la limitation de l'utilisation éventuelle de la touche fonctionnelle du clavier pour la fonction de la section commune : si l'une des sections a été désarmée séparément, la touche fonctionnelle de la section commune **ne peut pas être** utilisée pour désarmer les sections restantes. Ces sections doivent être désarmées séparément.

**Section désactivée** - désactivation de l'option d'armement de la section (le blocage d'une section entraîne la désactivation collective de tous les périphériques assignés à la section), indiquée par un point rouge. La section sur laquelle la centrale est attribuée ne peut pas être bloquée. Une section peut uniquement être bloquée par un technicien de service (via F-Link).

*Avertissement : lorsque la section où le module radio a été inscrit est bloquée, ce module radio arrête alors de recevoir les signaux de toutes les autres sections. C'est pourquoi il est recommandé de l'inscrire sur la section 1 où la centrale est également inscrite. Le blocage de la section faisant partie de la touche fonctionnelle commune indiqué par la couleur jaune (il est impossible d'indiquer si toutes ses sections sont entièrement armées ou désarmées).*

**Statut** - touche indiquant le statut réel de la section (désarmé, armé, sortie temporisée, entrée temporisée, armé partiellement, alarme, mémoire de l'alarme, désactivé, mode Service). En appuyant sur la touche, le système peut être commandé conformément à l'autorisation donnée par l'identifiant de connexion (il modifie l'état de la section - partiellement armé / armé / désarmé ...).

**Remarque** - il est possible de décrire les détails relatifs à une section pour faciliter l'orientation lors des inspections annuelles, etc.

## 10.3 Onglet Périphériques

Cet onglet est utilisé pour l'inscription des périphériques installés dans le système et leur paramétrage. La centrale est automatiquement inscrite en position 0 dans la section 1 et il est impossible de la supprimer ou de l'effacer. Pour apporter des modifications dans cet onglet, il faut être en mode Service.

Position	Name	Type	Section	Reaction	Internal	Internal settings	Disable	Status	Note
0	Control panel	JA-100K	1: House			Enter		Error	
1	Device 1	JA-111R	1: House			Enter		OK	
2	Device 2	JA-110E	1: House	None	<input type="checkbox"/>	Enter		??	
3	Device 3	JA-110A	1: House	None	<input type="checkbox"/>	Enter		??	
4	Device 4	Enroll	1: House	-	<input type="checkbox"/>				
5	Device 5	Enroll	1: House	-	<input type="checkbox"/>				
6	Device 6	Enroll	1: House	-	<input type="checkbox"/>				
7	Device 7	Enroll	1: House	-	<input type="checkbox"/>				
8	Device 8	Enroll	1: House	-	<input type="checkbox"/>				
9	Device 9	Enroll	1: House	-	<input type="checkbox"/>				
10	Device 10	Enroll	1: House	-	<input type="checkbox"/>				
11	Device 11	Enroll	1: House	-	<input type="checkbox"/>				
12	Device 12	Enroll	1: House	-	<input type="checkbox"/>				
13	Device 13	Enroll	1: House	-	<input type="checkbox"/>				
14	Device 14	Enroll	1: House	-	<input type="checkbox"/>				
15	Device 15	Enroll	1: House	-	<input type="checkbox"/>				
16	Device 16	Enroll	1: House	-	<input type="checkbox"/>				

**Nom** - utilisé dans les rapports d'évènements sous forme textuelle et dans le relevé de la mémoire (par ex., Porte principale).

**Type** - affiche le type de périphérique attribué. Une position vide permet d'inscrire un nouveau périphérique.

**Inscription des périphériques**, voir le chapitre 8.4.1 Inscription et effacement des périphériques.

**Section** - détermine dans quelle section sous surveillance le périphérique signalera des évènements (alarme, sabotage, défaillance, etc.). Remarque : division d'un bâtiment en sections - voir le chapitre 10.2 Onglet Sections.

**Réaction** - détermine la réaction relative à l'activation par un périphérique donné. Si un périphérique n'a aucune entrée d'alarme (par ex. un module d'accès BUS), il est impossible de lui attribuer une réaction. La liste complète des réactions pour les périphériques est affichée si l'option Paramètres avancés est activée. La description de toutes les réactions se trouve dans le chapitre 8.4.2 Liste des réactions applicables.

**Interne** - ce paramètre n'est disponible que pour les détecteurs d'intrusion. Les signaux provenant des périphériques comportant cette mention ne sont pas évalués comme des signaux d'alarme si une section est partiellement armée. Armement partiel d'une section - voir le chapitre 10.2 Onglet Sections.

**Paramétrage interne** - accès aux réglages des paramètres internes des périphériques connectées au BUS ou disposant d'une communication sans fil bidirectionnelle. Les différents périphériques ont des paramètres internes différents (certains n'en ont aucun). Le paramétrage interne du clavier est décrit au chapitre 10.3.1 Configuration du clavier. Pour les autres périphériques, se référer à leur manuel.

**Désactiver** - réalisable sur 2 niveaux, en fonction de l'autorisation de l'utilisateur :

- 1. Blocage de l'entrée** (point jaune), sert au blocage permanent de l'entrée du détecteur (BLK). Le système ignore toute activation du périphérique = l'alarme ne se déclenche pas et PG n'est pas commandée, mais les alarmes de sabotage et les défaillances sont normalement enregistrées.
- 2. Désactivation du périphérique** (point rouge), sert à complètement désactiver le périphérique (Désactivé). Le système ignore toutes les fonctions du périphérique connecté = absence d'alarme, de sabotage, d'activation PG, de défaillance, de rapport, ...).

Il est impossible de désactiver la centrale ou un périphérique si la réaction détresse est activée.

**Statut** - indique le statut effectif du périphérique. OK = tout est en ordre ; TMP = sabotage ; ACT = entrée d'alarme activée ; BLK = bloqué ; Désactivé = désactivé ; ERR = erreur ; ?? = le périphérique ne répond pas ; Alimentation du réseau = défaillance de l'alimentation ; Batterie = batterie déchargée ou déconnectée dans la centrale ; Chargement = chargement de la batterie de secours dans le périphérique ou la centrale ; BOOT = état relatif à la mise à jour en cours du périphérique ou l'échec de la mise à jour (réitérer la mise à jour). En pointant la souris sur l'élément STATUT du périphérique, les données détaillées s'affichent.

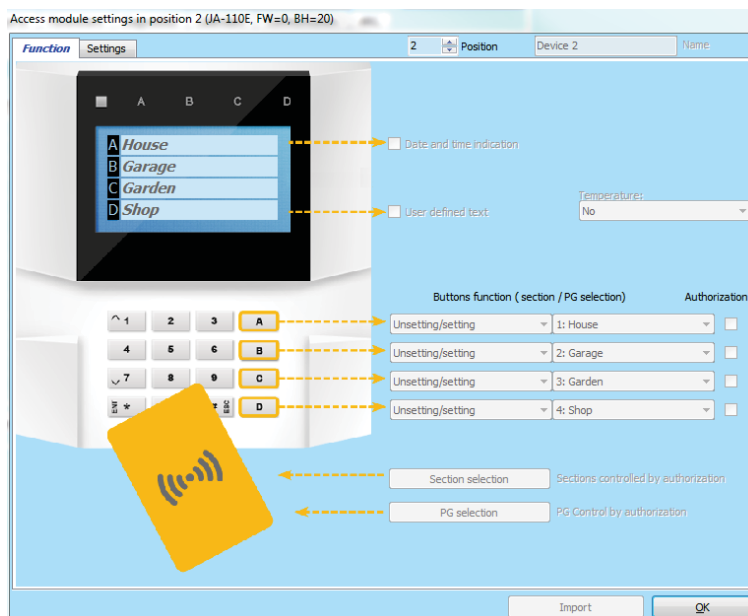
**Remarque** - permet de décrire les détails du périphérique, par ex. l'emplacement, la date du dernier remplacement de la batterie, l'intensité moyenne du signal RF au cours du dernier test, etc.

### 10.3.1 Configuration du clavier

En entrant dans les paramètres internes du clavier (onglet Périphériques), la fenêtre suivante s'ouvrira (l'exemple se réfère au clavier JA-110E).



## Onglet Fonction :



**Date et heure** - permet d'afficher l'heure système effective dans le coin supérieur droit du clavier

**Texte Utilisateur** - permet d'afficher du texte arbitraire sur le clavier LCD (numéro de téléphone de l'installateur, etc.). L'activation d'une telle option désactive la touche fonctionnelle « D ».

**Température** - Permet d'afficher la température mesurée d'un détecteur sélectionné dans le coin du clavier inférieur

**Touches fonctionnelles** - sur le côté gauche, sélectionner les touches fonctionnelles et sur le côté droit, la section ou la sortie PG à laquelle est attribuée la fonction. Les éléments suivants peuvent être inscrits sur les touches fonctionnelles : Aucun, Désarmer / armer, Désarmer / armer partiellement, Désarmer / armer partiellement / armer, Indication de section, Détresse silencieuse, Incendie, détresse sonore, Problèmes de santé, PG MARCHÉ / ARRÊT, PG EN MARCHÉ, PG À L'ARRÊT, indication PG, PG inversée, touche fonctionnelle commune.

**Autorisation** - l'autorisation de l'utilisateur est nécessaire pour l'armement et le désarmement. Lorsque ce paramètre est désactivé, toutes les touches fonctionnelles peuvent être commandées sans autorisation à l'exception de la fonction Section désarmée pour laquelle l'autorisation est toujours requise. En ce qui concerne l'activation et la désactivation des sorties PG, le paramétrage de la fonction Autorisation / Sans autorisation est valable pour les deux commandes.

**Importer** - permet de copier les paramètres actuels du clavier vers d'autres claviers de même type, par exemple dans le cas où un bâtiment protégé dispose de plusieurs entrées supplémentaires et chaque entrée nécessite d'avoir un clavier avec les mêmes fonctions. Une copie est possible pour le même type de clavier. Ou la fonction peut être utilisée lorsqu'un clavier est remplacé par un nouveau. La touche Importer propose l'historique des derniers paramètres connus du clavier à cette position donnée.

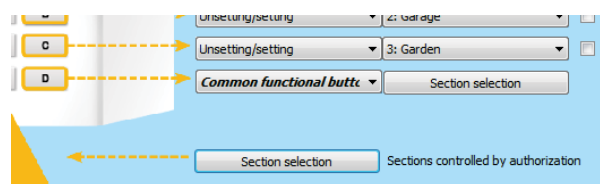
**Sélection de la section** - sections prédéfinies devant être commandées uniquement par autorisation (carte/badge RFID ou code).

**Commande PG** - sélectionner les sorties PG pour une commande uniquement par autorisation (carte/badge RFID ou code)

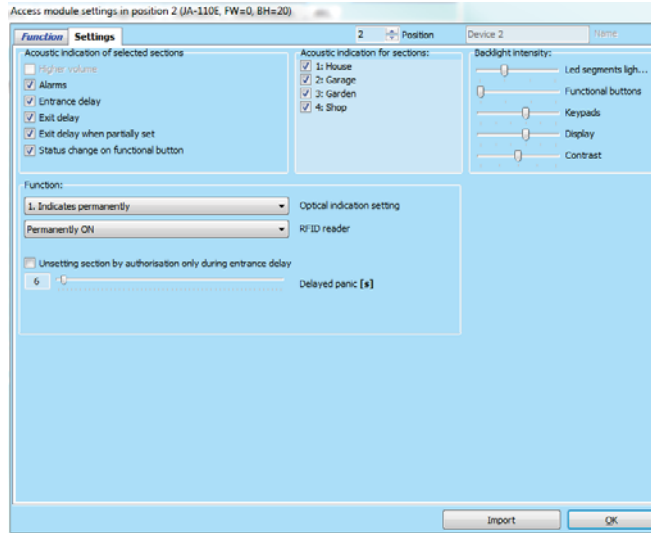
<b>Aucune</b>	La touche fonctionnelle n'a pas de fonction ; désactivée
<b>Désarmer / Armer</b>	Commande de la section Indication de la touche fonctionnelle : section désarmée = vert, armée = rouge.
<b>Désarmer / Armer partiellement</b>	Permet d'activer le mode d'armement partiel de la section (en cas d'activation dans l'onglet Sections). Indication de la touche fonctionnelle : section désarmée = vert, partiellement armée = jaune.
<b>Désarmer / Armer partiellement / Armer</b>	Permet de sélectionner le niveau d'armement. L'enclenchement de la touche fonctionnelle (Armer) permet de proposer l'armement partiel, un appui répété permet un armement complet du système. Lorsque le système est entièrement armé, un appui sur la touche fonctionnelle le désarme complètement. Indication de la touche : section désarmée = vert, partiellement armée = jaune, totalement armée = rouge.

<b>Indication de la section</b>	La touche fonctionnelle n'affiche que le statut de la section et ne permet pas sa commande (convient par ex. à la signalisation du statut des sections communes, de l'escalier, etc.). En cas de déclenchement d'alarme, elle permet son annulation en enclenchant la touche verte de la touche fonctionnelle suivie de l'autorisation valide de l'utilisateur.
<b>Détresse (silencieuse)</b>	La touche fonctionnelle déclenche une alarme de détresse silencieuse. Après l'enclenchement de la touche, un rapport de détresse silencieuse est envoyé à partir de la section à laquelle la touche fonctionnelle est attribuée, sans indication acoustique. L'alarme de détresse peut également être différée avec une durée ajustable et la possibilité d'annulation avant l'expiration de la durée prédéfinie (voir le point Détresse temporisée). Si la section est armée, elle ne sera pas désarmée.
<b>Incendie</b>	La touche fonctionnelle permet de déclencher une alarme d'incendie. Ensuite, l'alarme d'incendie est déclenchée à partir de la section à laquelle la touche fonctionnelle est attribuée.
<b>Détresse sonore</b>	La touche fonctionnelle active une alarme de détresse sonore. Après l'enclenchement, l'alarme de détresse sonore est déclenchée à partir de la section à laquelle la touche fonctionnelle est attribuée. L'alarme de détresse sonore peut également être différée avec une durée ajustable et la possibilité d'annulation avant l'expiration de la durée paramétrée (voir le point Détresse temporisée). Si la section est armée, elle ne sera pas désarmée.
<b>Problèmes de santé</b>	La touche fonctionnelle permet d'envoyer un rapport relatif à un problème de santé (sans activer une sirène) de la section à laquelle la touche fonctionnelle est attribuée.
<b>Désactiver PG / activer PG</b>	La touche fonctionnelle permet de commander la sortie PG. Indication : PG inactive = vert, PG active / enclenchée = rouge.
<b>Activer PG</b>	La touche fonctionnelle permet uniquement d'activer la sortie PG (par ex., allumer l'éclairage pour une période prédéfinie).
<b>Désactiver PG</b>	La touche fonctionnelle permet uniquement de désactiver la sortie PG (par ex., la fonction de la touche ARRÊT d'urgence).
<b>Indiquer PG</b>	La touche fonctionnelle indique uniquement le statut de la sortie PG sans possibilité de commande (la couleur rouge indique le statut actif).
<b>Indiquer PG en mode de logique inversée</b>	La touche fonctionnelle indique uniquement le statut de la sortie PG avec une logique inversée (la couleur verte indique le statut actif) sans possibilité de commande.
<b>Touche fonctionnelle commune</b>	<p>Permet la commande simultanée de plusieurs sections à l'aide de la touche fonctionnelle du clavier. Après avoir enclenché la touche fonctionnelle commune, la commande Désarmer / Armer est réalisée collectivement pour les touches de la section choisie. Si certaines sections commandées par la touche commune sont armées et les autres désarmées, après avoir utilisé la touche fonctionnelle commune, les touches restantes seront désarmées par un court enclenchement / armées complètement par un enclenchement prolongé. Si un armement partiel est activé pour une des touches fonctionnelles choisies (pour les détails, voir le point 9.2 Commande du système par le clavier), la touche commune se comportera de la manière suivante : 1<sup>er</sup> enclenchement de l'armement = armement partiel, 2<sup>e</sup> enclenchement de l'armement = armement complet. Il n'est pas approprié de combiner la touche fonctionnelle commune avec les fonctions Section / Section commune.</p> <p>Indication de la touche commune : toutes les sections désarmées = vert, toutes les sections entièrement armées = rouge, toute section armée (partiellement armée) = jaune.</p> <p>Les sections sont attribuées à la touche fonctionnelle commune dans une autre fenêtre lorsque l'option est sélectionnée.</p>

#### Touche fonctionnelle commune :



## Onglet Paramétrage :



### Indication acoustique des sections choisies :

Volume supérieur	Réglage du volume de l'indication sauf pour l'alarme
Alarmes	Sortie acoustique en cas d'alarme (sirène sonore)
Temporisation d'entrée	Tonalité de sifflement acoustique continue au cours de l'entrée temporisée
Temporisation de sortie	Bips intermittents lents (1/s)
Sortie temporisée en cas d'armement partiel	Bips intermittents lents (désactivé par défaut)
Changement d'état de la touche fonctionnelle	Indication acoustique avec un bip lors d'une modification

### Fonctions :

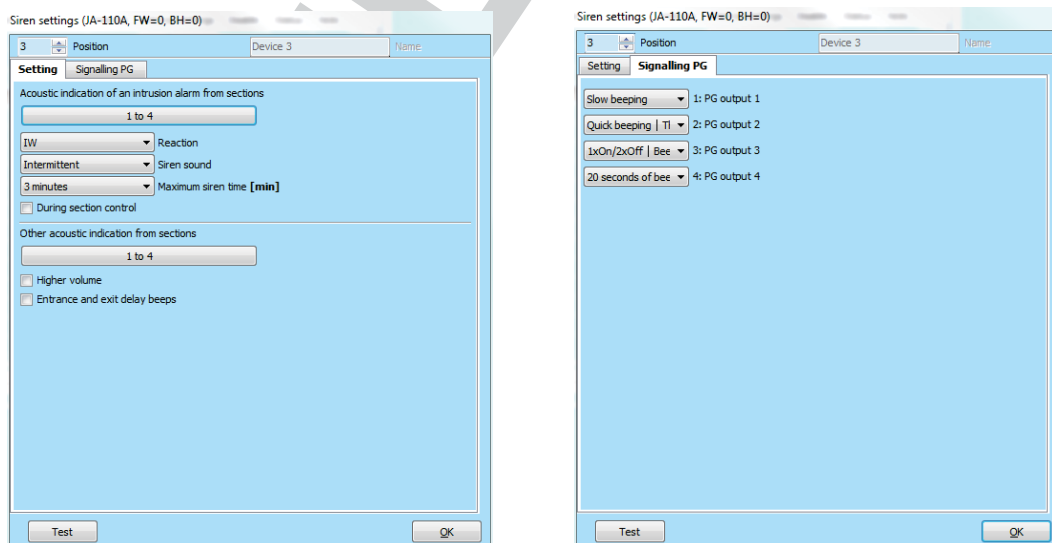
Lecteur RFID		Pour économiser l'énergie, l'activité du lecteur peut être limitée à 3s à partir de l'enclenchement au niveau du capot. Le lecteur RFID peut également être complètement désactivé. Ce paramètre s'applique aux claviers sans fil qui sont alimentés en permanence à partir d'une source externe, sinon leur lecteur RFID est toujours automatiquement éteint.
	Activé en permanence	Le lecteur RFID est activé en permanence. Dans le cas d'un clavier BUS, il ne respecte pas le paramétrage de sortie de veille.
	Activé par enclenchement	Sortie de veille du lecteur RFID 3s après l'activation sur le clavier.
	Arrêt	Le lecteur RFID est désactivé en permanence.
Paramétrage de l'indication optique :	En appuyant ou en exigeant l'autorisation	Sortie de veille du lecteur RFID après la demande d'activation ou d'autorisation d'un clavier.
	1. Signalisation permanente	Le clavier BUS signale en permanence. Le clavier sans fil ne signalera en permanence qu'avec une alimentation externe. Sans alimentation externe, il se comporte comme dans l'option 2.
	2. Après un changement de statut de la section sur le clavier	Le clavier indique un changement de statut d'une section / PG. Un changement de statut est indiqué uniquement sur la touche fonctionnelle concernée. L'entrée temporisée et l'alarme sont indiquées par l'ensemble du clavier.
	3. Après un changement de statut de la section - voyant	Un changement de statut d'une section / PG est indiqué uniquement sur la touche fonctionnelle concernée.
	4. Modification du voyant d'état sur le clavier	Les temporisations d'entrée et les alarmes ne sont signalées que par voie acoustique. Un changement de statut est indiqué uniquement sur la touche fonctionnelle concernée. Cette option constitue le réglage par défaut.

	5. Après une entrée et l'alarme	Le clavier indique l'entrée temporisée et l'alarme sur la touche fonctionnelle concernée. Une modification du statut de sortie PG et du statut de la section n'est absolument pas indiquée.
	6. Sortie de veille par enclenchement	Le clavier ne donne des indications optiques et acoustiques qu'après l'ouverture du capot avant, l'appui sur une touche, une touche fonctionnelle ou le capot avant.
Désarmement de la section par autorisation uniquement pendant la temporisation d'entrée	En cas d'activation, la section, lorsque la temporisation d'entrée a commencé, est alors désarmée par les carte / badge RFID valide de l'utilisateur ou un code d'autorisation uniquement. Avec les claviers sans fil, l'autorisation peut être réalisée après l'activation de la temporisation d'entrée. ATTENTION : il est recommandé de désactiver cette fonction lorsque la temporisation d'entrée couvre généralement une section commune, sinon toutes les sections affectées à la section commune seront désarmées pour une autorisation donnée.	
Sortie de veille du clavier par présentation d'une carte RFID	Lorsqu'une carte RFID est présentée, le clavier se réveille. Il n'est pas recommandé d'activer cette fonction s'il existe de nombreux obstacles tels que des objets métalliques et des câblages électriques aux abords du clavier. Si l'activation est cependant décidée, s'assurer que le clavier ne sorte pas de veille de manière concomitante pour prévenir une durée de vie réduite de la batterie.	
Détresse temporisée	La fonction permet de retarder le déclenchement d'une détresse silencieuse ou sonore avec un temps prédéfini. Il est possible de déterminer l'intervalle de temps en cas d'annulation de l'activation en appuyant plusieurs fois sur la même touche fonctionnelle avec une fonction de détresse silencieuse ou sonore prédéfinie. Lorsque l'autorisation est activée, elle est alors nécessaire pour l'activation comme la désactivation. La temporisation est réglable dans une plage de 1 à 255 secondes.	

#### Intensité du rétroéclairage :

Voyants	Réglage de l'éclairage des voyants
Touches fonctionnelles	Réglage des touches fonctionnelles
Clavier	Réglage du rétroéclairage du clavier
Affichage	Réglage du rétroéclairage de l'écran LCD
Contraste	Réglage du contraste de l'écran LCD

### 10.3.2 Paramètres de la sirène interne



**Indication acoustique d'une alarme d'intrusion à partir des sections** - utilisé pour sélectionner les sections pour lesquelles l'alarme sera signalée par voie acoustique par les sirènes.

**Réaction** - sélection des options de signalisation de l'alarme EW (indication d'avertissement externe) ou IW (indication d'avertissement interne). La différence est décrite dans le tableau 8.5 Types d'alarmes.

**Son de la sirène** - choix du type de son de la sirène : intermittent (50/50) / continu.

**Temps de sirène maximal** - limitation du temps de sifflement maximal de 1 à 5 minutes (en supposant que l'alarme de la centrale dure plus, sinon il s'arrête en même temps que l'alarme de la centrale).

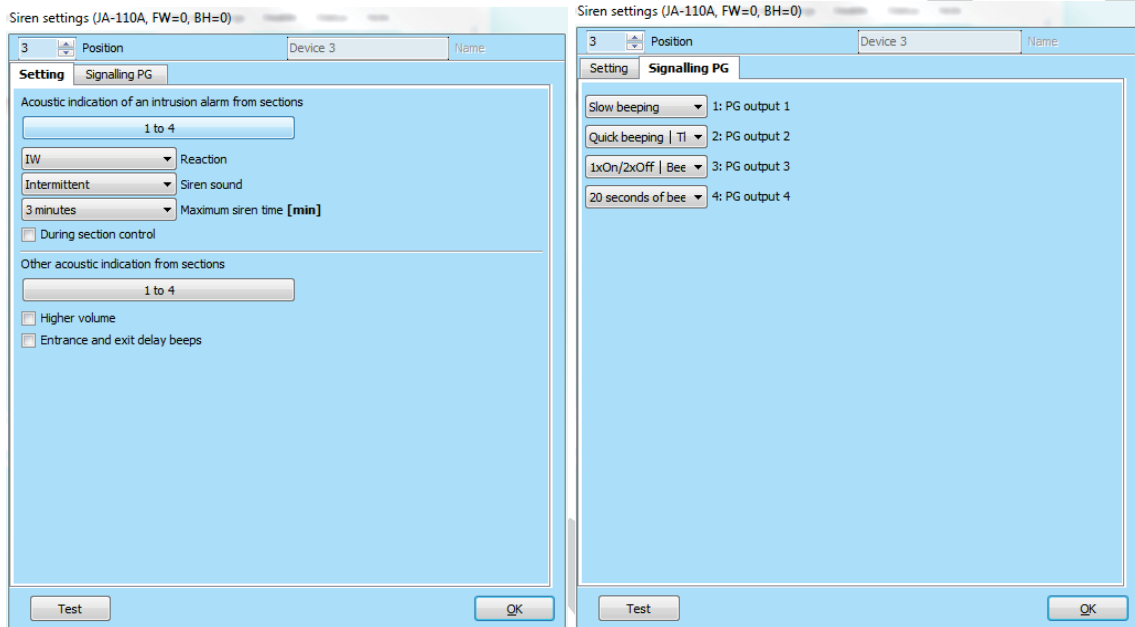
**Pendant la commande de la section** - confirmation acoustique des changements de statut de la section (bips 1x - armé / 2x désarmé)

**Autres indications acoustiques à partir des sections** - sélection des sections pour d'autres indications acoustiques (temporisation des entrée / sortie)

**Volume supérieur** - possibilité de fixer un volume d'intensité acoustique supérieur et inférieur pour la signalisation de temporisation d'entrée et de sortie et la signalisation de commande de sortie PG. Il n'y a pas d'impact sur le sifflement de l'alarme, qui est toujours réglé sur le volume le plus fort.

**Bips de temporisation d'entrée et de sortie** - indication acoustique d'une temporisation des entrée / sortie

**Test** - touche de test de 3 secondes relatif à la signalisation acoustique et optique de l'alarme.



## 10.4 Onglet Utilisateurs

Il est utilisé pour définir de nouveaux utilisateurs du système et paramétrer leurs droits. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.

Position	Name	Telephone number	Code	Card	Authorization	Section	PG	Dialling in activates PG	User blocking	Note
0	Service		****	No	Service	1 2 3 4	1 2 3 4			
1	Master		****	No	Administrator	1 2 3 4	1 2 3 4			
2	User 2			No		1 2 3 4	1 2 3 4			
3	User 3			No		1 2 3 4	1 2 3 4			
4	User 4			No		1 2 3 4	1 2 3 4			
5	User 5			No		1 2 3 4	1 2 3 4			
6	User 6			No		1 2 3 4	1 2 3 4			
7	User 7			No		1 2 3 4	1 2 3 4			
8	User 8			No		1 2 3 4	1 2 3 4			
9	User 9			No		1 2 3 4	1 2 3 4			
10	User 10			No		1 2 3 4	1 2 3 4			
11	User 11			No		1 2 3 4	1 2 3 4			
12	User 12			No		1 2 3 4	1 2 3 4			
13	User 13			No		1 2 3 4	1 2 3 4			
14	User 14			No		1 2 3 4	1 2 3 4			
15	User 15			No		1 2 3 4	1 2 3 4			
16	User 16			No		1 2 3 4	1 2 3 4			

**Nom** - les noms des utilisateurs sont utilisés dans les rapports d'évènements textuels dans la mémoire de l'historique des évènements, dans les onglets pour les rapports, les paramètres d'autorisation ou l'autorisation sur un clavier, ou encore dans les rapports SMS envoyés par le transmetteur GSM supplémentaire.

**Numéro de téléphone** - utilisé pour le rapport évènementiel lorsque les transmetteurs supplémentaires sont connectés, l'identification des utilisateurs pour la commande du système par téléphone à l'aide du menu vocal comme pour l'activation des sorties PG par un appel / SMS. Le numéro de téléphone doit être toujours indiqué au format international (par ex. +420710123456).

**Code** - le code d'accès de l'utilisateur est saisi au format **nnnn** (4 ou 6 chiffres en fonction du profil du système). Les codes sur les positions 0 et 1 ne peuvent pas être effacés (service et administrateur principal).

**Carte** - sert à l'inscription des cartes d'accès RFID (à puce). Chaque utilisateur peut avoir une carte RFID. Des carte/badge sont attribués de la manière suivante :

- en saisissant le numéro de série (il peut être lu avec un lecteur de code-barres à partir des carte/badge RFID)
- en utilisant le lecteur USB JA-190T pour un PC et **en présentant** les carte/badge RFID
- en utilisant n'importe quel clavier et en présentant des carte/badge RFID

**Autorisation** - détermine les droits de l'utilisateur. Les autorisations des positions 0 et 1 ne peuvent être modifiées.

Détails - voir le chapitre 8.3 Autorisation des utilisateurs.

**Section** - détermine les sections que l'utilisateur peut commander. L'administrateur peut aussi paramétrer les codes et les cartes des utilisateurs dans les sections attribuées. Une section ne peut pas être attribuée à un utilisateur qui n'a d'autorisation que pour la commande des sorties PG.

**PG** - détermine les sorties PG que l'utilisateur a le droit de commander (si l'autorisation est requise pour la commande de sortie).

**Désactiver** - possibilité de bloquer un utilisateur. Il est impossible de bloquer les utilisateurs en positions 0 (technicien de service) et 1 (administrateur principal). La désactivation d'un utilisateur est signalée par un point rouge. L'administrateur (à l'aide du clavier) et le technicien de service (via F-Link) sont autorisés à désactiver les utilisateurs.

**Remarque** - permet de décrire les détails d'un utilisateur, par ex. l'autorisation de l'accès en dehors du temps de travail, etc.

## 10.5 Onglet Sorties PG

Il paramètre les fonctions et les liens des sorties programmables. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.

Position	Name	Function	Time	Activation	Blocking of PG outputs	Reports	PG disabled	Current status	Test PG output	Note
1	PG output 1	Impulse	01:30:14	Activation	Sections	Enter			Test PG output	
2	PG output 2	Impulse	00:00:05	Activation	None	Enter			Test PG output	
3	PG output 3	ON/OFF		Activation	None	Enter			Test PG output	
4	PG output 4	ON/OFF		Activation	None	Enter			Test PG output	

**Nom** - désignation de la sortie (par ex. Climatisation, Porte du dépôt,...).

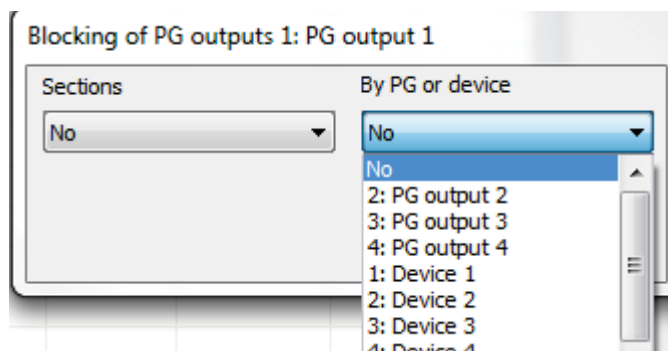
**Fonction** - détermine le comportement de la sortie après l'activation.

<b>Impulsion</b>	Activation avec une limitation temporaire (la durée est paramétrée avec la touche Temps).
<b>MARCHE/ARRÊT</b>	La commande d'enclenchement provoque l'activation, la commande de neutralisation la désactivation alors que le statut de la source ou la durée ne sont pas contrôlés, la dernière commande est toujours exécutée.
<b>Copier</b>	Copie l'activation du détecteur ou du statut interne ; en cas de requête issue de deux périphériques, la logique OR s'applique.

**Heure** - réglage du temps pour la fonction Impulsion. Le temps est paramétré au format *hh:mm:ss* dans l'envergure 00:00:01 - 23:59:59.

**Activation** - ouverture de la Carte des activations de la sortie PG - se référer au chapitre 10.5.1 Carte d'activation des sorties PG.

**Blocage d'une PG** - pour bloquer une sortie par un statut de section ou un détecteur ou une autre sortie PG. Le blocage empêche l'activation de la PG donnée ; si elle est déjà activée, il la désactive. Cela convient par ex. pour le blocage du verrou de la porte si la section correspondante est armée. Dans le cas d'un blocage par le statut d'une section, il est possible de choisir si le blocage est effectif lorsque la section est armée ou désarmée et, dans le cas d'un blocage par un périphérique, si cela est déterminé par son activation ou sa désactivation. Les deux options de blocage (par une section et un périphérique ou par une section et une sortie PG) peuvent être utilisées en même temps.



**Désactiver** - possibilité de bloquer une sortie PG. La désactivation (blocage) d'une sortie est signalée par un point rouge. Le technicien de service (en utilisant F-Link) est autorisé à désactiver une sortie.

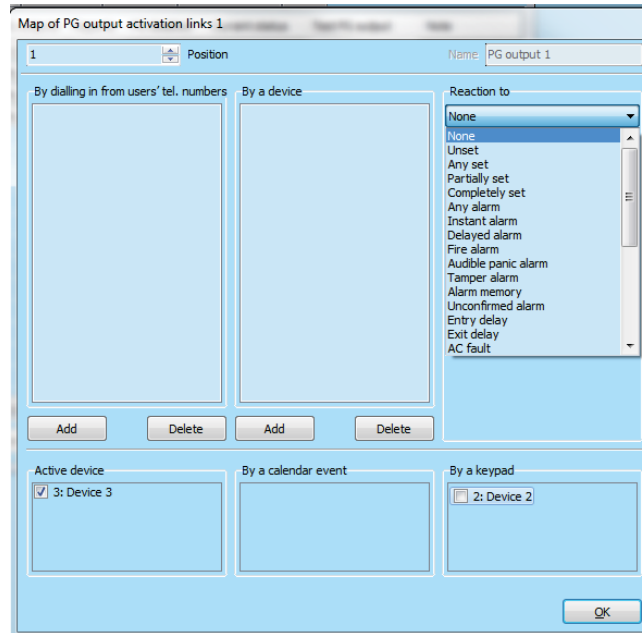
**Statut réel** - information codée en couleur relative au statut réel d'une sortie PG. La signalisation verte correspond au voyant vert de la touche fonctionnelle, la signalisation rouge correspond au voyant rouge de la touche.

**Test** - possibilité de commander manuellement une sortie depuis l'ordinateur en utilisant le logiciel F-Link. Selon la fonction sélectionnée, l'activation (ou la désactivation) de la PG concernée sera réalisée.

**Remarque** - permet de décrire les détails d'une sortie PG, son utilisation, un comportement particulier, la notification de l'activation avec d'autres sorties, etc.

### 10.5.1 Carte d'activation des sorties PG

La sélection Activation dans l'onglet Sorties PG permet d'accéder aux liens de la carte d'activation. La carte détermine les actions auxquelles la sortie réagit.



**Par numérotation à partir des numéros de téléphone de l'utilisateur** - utilisateurs définis ayant le droit d'activer une sortie PG par numérotation à partir de leur téléphone lorsqu'un transmetteur GSM ou PSTN supplémentaire est connecté. Les numéros de téléphone utilisés pour l'activation par sonnerie ne doivent pas être cachés (le service CLIP ne doit pas être désactivé en ce qui les concerne). Le terme « sonnerie » implique qu'après avoir composé le numéro de téléphone, l'appelant attende au moins une sonnerie et raccroche avant que la centrale ne réponde à l'appel (voir le nombre de sonneries des appels entrants dans les paramètres du transmetteur). La sortie PG s'allume lorsque l'appelant raccroche. Si l'appel est pris en communication par la centrale, la sortie ne sera pas activée.

**Par un périphérique** - permet d'activer la sortie PG par un périphérique (activation du détecteur, enclenchement du badge, etc.). La configuration est liée à l'onglet Utilisateurs. Un périphérique donné ne peut activer qu'une sortie PG.

**Réaction** - permet l'activation d'une sortie par un événement sélectionné dans le système (par ex., un armement, une alarme, une panne d'alimentation, une erreur, etc.). Pour un statut interne (29 statuts internes au total, voir le tableau suivant), il est possible de définir le groupe de sections pour lequel le signal sera accepté (logique OR). La sortie PG concernée peut être armée pour copier le statut d'une autre sortie PG ou de plusieurs autres sorties lorsqu'une logique réciproque peut être sélectionnée (OR ou AND). Le dernier élément du menu vous permet de définir l'activation d'une sortie et sa désactivation en réponse à un événement complètement différent (par ex., l'activation dans le cas d'une alarme, mais la désactivation par désarmement seulement).

**Activation par un périphérique** - une liste de périphériques qui activent la sortie PG concernée avec leur activation, par exemple une photo d'un détecteur de mouvement doté d'une caméra (la fonction peut être réglée dans les paramètres internes du périphérique) ou l'indication acoustique par les sirènes, etc.

**Par un événement programmé** - liste des événements programmés qui activent, désactivent ou bloquent la sortie PG concernée (fenêtre d'information).

**Par un clavier (touche fonctionnelle)** - affiche la liste des claviers et des télécommandes dans le système avec la capacité de commander la sortie PG spécifique.

**Par des consignes SMS** - en cas de transmetteur GSM supplémentaire connecté, permet de programmer les consignes textuelles pour l'activation et la désactivation par téléphone d'une sortie PG. Pour la commande des sorties, utiliser un SMS au format **code commande**, par ex. **2345\_allumer\_lumière** (remarque : le caractère \_ correspond à un espace). Le code préalable à la commande n'est pas obligatoire si, dans l'onglet **Communication**, l'option « Menu vocal et consigne SMS sans code » est activée et le numéro de téléphone de l'utilisateur autorisé à commander la sortie PG correspondante est identifié.

**Avertissement :** les sorties PG ne sont pas fonctionnelles si le système est en mode Service. En appuyant sur la touche Test, toutes les sorties PG peuvent être testées (par le logiciel F-Link). Lors de l'activation du mode Service, toutes les sorties PG sont désactivées. Après la sortie du mode Service de F-Link, leur réactivation est proposée.

### Statuts internes pour la commande des sorties PG :

1. Désarmement	11. Mémoire d'alarme	21. Détecteur déclenché
2. Quelconque armé	12. Alarme non confirmée	22. Périphérique à faible batterie
3. Armement partiel	13. Temporisation d'entrée	23. Périphérique avec sabotage activé
4. Totalement armé	14. Temporisation de sortie	24. Aucun mouvement dans la section
5. Alarme quelconque	15. Défaillance d'alimentation secteur	25. Notification de vérification annuelle
6. Alarme instantanée	16. Défaillance d'alimentation secteur supérieure à 30 min	26. Défaillance GSM
7. Alarme temporisée	17. Défaillance de la batterie de secours	27. Défaillance LAN
8. Alarme d'incendie	18. Avertissement interne (IW)	28. Défaillance PSTN
9. Alarme de détresse sonore	19. Avertissement externe (EW)	29. Évènement dans le système
10. Alarme de sabotage	20. Défaillance	

## 10.6 Onglet Rapports aux utilisateurs

Cet onglet est disponible lorsqu'un transmetteur GSM ou PSTN supplémentaire est connecté et utilisé pour définir les utilisateurs auxquels le système fera un rapport sur des groupes d'événements sélectionnés sous la forme de SMS ou d'appels vocaux sur leurs téléphones. Les groupes et le format SMS sont décrits dans le tableau ci-joint. La structure de base du menu vocal est décrite dans le tableau ci-joint 9.5. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.

Position	User	SMS alerts	Alarm Call	SMS about setting/unsetting	Photo	Fault and Service SMS	User defined SMS 1	User defined SMS 2	Section reporting	PG output reports	Test SMS
1	0: Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
2	1: Master	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
3	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
4	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
5	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
6	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
7	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test
8	No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 2 3 4	1 2 3 4	Test

**Utilisateur** - permet de sélectionner un utilisateur à partir de la liste des utilisateurs.

**Alertes SMS** - groupe de rapports d'alarme pouvant être sélectionné pour lesquels un rapport textuel est envoyé sur un événement d'alarme dans la section choisie, puis sur une défaillance ou une restauration de l'alimentation supérieure à 30 minutes, l'armement d'une zone ouverte ou un rapport éventuel sur une section désarmée sans mouvement (voir l'onglet Paramètres).

**Appel d'alarme** - un groupe de rapports pour lequel (après l'envoi de rapports SMS) le système transmet un message vocal d'alarme à l'utilisateur. En cas d'absence de réponse à l'appel en 30 sec., le système appelle l'utilisateur suivant dans l'ordre donné. En cas de réponse à l'appel, le message vocal est joué à plusieurs reprises. La structure du message est la suivante : Vos rapports d'alarme - Type d'alarme - N° de section. Après que l'utilisateur a raccroché, mais au plus tard après 50 sec., l'appel est raccroché et l'utilisateur suivant Centrale du système de sécurité JA-100K



est appelé. L'utilisateur peut confirmer la réception de l'appel en appuyant sur la **touche #** du téléphone et après le message vocal, l'utilisateur doit saisir un code valide. Quand un code valide a été saisi, **l'alarme est stoppée et l'utilisateur suivant n'est plus appelé**. Pour le rapport vocal, un message vocal universel est prédéfini dans le système. Les messages vocaux peuvent être enregistrés à nouveau en remplaçant les noms de ceux qui sont requis dans le menu vocal.

**Attention** : le rapport d'un événement vocal est limité à un maximum de 5 utilisateurs.

**SMS relatif aux armement/désarmement** - groupe de rapports pour lequel un message textuel relatif à l'armement et au désarmement est envoyé. Le rapport d'armement est envoyé avec un **décalage de 60 secondes** après l'armement. L'armement et le désarmement ne sont pas signalés à l'utilisateur qui les a réalisés. L'armement d'une section commune représente une exception (la centrale s'en charge, en aucun cas l'utilisateur).

**Photo** - envoi à l'utilisateur d'un SMS annonçant qu'un cliché d'alarme a été pris si des périphériques de vérification photographiques sont installés. Pour de plus amples détails - voir les manuels des détecteurs respectifs.

**SMS de défaillance et de service** - envoi de rapports textuels relatifs à des erreurs (batteries déchargées, accès au mode Service).

**Utilisateur défini 1** - 1<sup>er</sup> groupe spécial où le technicien d'installation peut transférer certains événements à déclarer (en général, rapports de défaillances et de restauration de l'alimentation ou, éventuellement, armement avec un périphérique actif) uniquement aux utilisateurs sélectionnés (administrateur, etc.).

**Utilisateur défini 2** - 2<sup>nd</sup> groupe spécial où le technicien d'installation peut transférer certains événements à déclarer (généralement, faible niveau de charge des batteries des périphériques ou faible niveau de charge de la batterie de secours) uniquement aux utilisateurs sélectionnés (généralement le technicien de montage, etc.).

**Rapport de section** - détermine les sections pour lesquelles les groupes d'événements sélectionnés seront signalés.

Si les SMS de défaillance et de service sont vérifiés et aucune section n'est sélectionnée, les défaillances du système et le service sont uniquement signalés (ils sont toujours attribués à la section n°1). Il n'y a pas de lien entre l'autorisation et la capacité de commande de la section.

**Rapport de sortie PG\*** - possibilité de signaler à l'utilisateur l'activation ou non des sorties PG. Les messages sont envoyés avec une temporisation fixe de 60 secondes. Les textes des messages SMS sont définis dans l'onglet Sorties PG, voir le chapitre 10.5 Onglet Sorties PG.

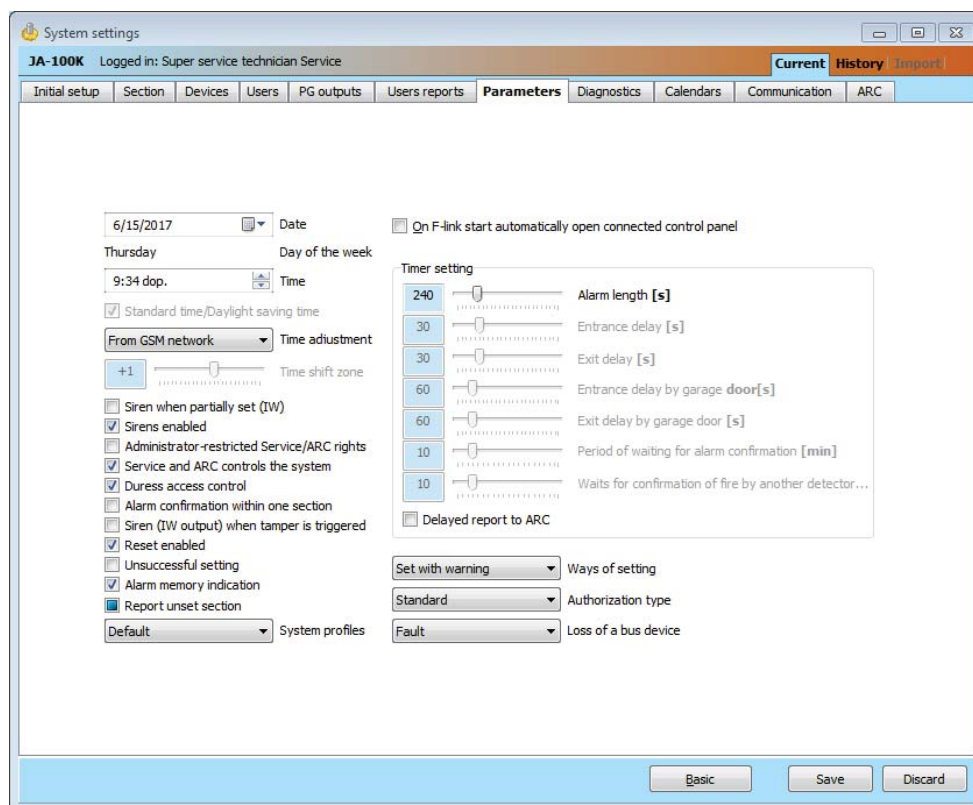
**Test** - en enclenchant la touche, un rapport SMS de test est envoyé à l'utilisateur : « Rapport de test, Centrale, Section 1 ».

**Tableau des événements et des groupes prédéfinis :**

Event	Alarm	Setting/Unsetting	Failures and service	User defined SMS 1	User defined SMS 2
AC fault 30 minutes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC fault after 30 min restored	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Instant alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Instant alarm cancelled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delayed alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delayed alarm cancelled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tamper alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tamper alarm cancelled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fire alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fire alarm cancelled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gas leak alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Panic alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Panic alarm cancelled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Health troubles	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Flooding	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Code breaking attempt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Set with active device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No movement in the section	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overheating activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overheating deactivation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freezing activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freezing deactivation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Set	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unset	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Partially set	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System BOOT	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device low battery	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device low battery restored	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fault	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fault restored	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enter service mode	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Leave service mode	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup battery LOW	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup battery restored	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ARC communication fault	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ARC communication fault restored	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RF jamming	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RF jamming ended	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Low credit balance	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 10.7 Onglet Paramètres

Il est utilisé pour programmer les paramètres et les fonctions optionnelles de la centrale. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.



<b>Date</b>	Paramétrage du calendrier interne.	
<b>Jour de la semaine</b>	Affichage du jour de la semaine.	
<b>Heure</b>	Paramétrage de l'horloge interne.	
<b>Heure d'hiver/d'été*</b>	Le passage automatique à l'heure d'hiver et d'été peut uniquement être sélectionné pour le paramétrage manuel de l'heure. Le changement se produit le dernier dimanche de mars ou d'octobre, respectivement à 01h00 UTC (à savoir par ex. 02h00 CET ou 03h00 CEST).	
<b>Réglage de l'heure*</b>	Méthode d'ajustement de l'heure et de la date interne :	
	Manuellement	Réglage manuel de l'heure et de la date en utilisant F-Link
	À partir du réseau GSM	L'heure et la date sont fournies par le fournisseur GSM à chaque connexion au réseau GSM
	Du serveur Jablotron (LAN / GSM)	L'heure et la date sont ajustées automatiquement en fonction du serveur de communication. L'option ne fait rien lorsque le type de communication est réglé sur « Sans programmation à distance » (réglage par défaut)
<b>Sirène IW lors de l'armement partiel</b>	Possibilité de régler l'alarme sonore avec le système IW si la section est partiellement armée. Les réactions d'incendie et 24 heures n'activent jamais une sirène dans le cas d'une alarme, peu importe comment ce paramètre est réglé.	
<b>Sirènes activées*</b>	Activation de toutes les sirènes BUS et sans fil du système (conçu pour désactiver l'alarme sonore pendant les tests du système).	
<b>Restrictions de l'administrateur pour le service et la télésurveillance</b>	Blocage de l'accès indépendant vers le système pour les techniciens de service et le centre de télésurveillance. Remarque : en cas d'accès à distance par un technicien vers le système via F-Link, l'administrateur peut être autorisé en utilisant un clavier sur le site. En cas de connexion locale d'un technicien à la centrale à l'aide d'un câble	

	USB et d'un transmetteur supplémentaire GSM / PSTN, l'administrateur peut être autorisé à distance en utilisant le menu vocal.	
<b>Système de commande du service et de la télésurveillance*</b>	Ce paramètre permet aux techniciens de service et de la télésurveillance de commander le système pour toutes les sections. Si ce paramètre est désactivé, le technicien n'est pas autorisé à commander les sections et ne sera qu'en mesure d'accéder au mode Service après le désarmement de toutes les sections par l'administrateur ou un utilisateur.	
<b>Commande d'accès sous contrainte</b>	Sert au déclenchement d'une alarme silencieuse par autorisation uniquement ou par commande du système (armement, désarmement, commande PG, ...) quand un utilisateur est en présence d'un malfaiteur. Une alarme de détresse est déclenchée lors de la commande du système quand un code est saisi avec le chiffre 1 ajouté à la valeur du dernier chiffre. Exemple : code de l'utilisateur 4444, pour la commande d'accès sous contrainte, saisir 4445. Attention : lorsque le dernier chiffre du code de l'utilisateur est 9, utiliser pour la commande d'accès sous contrainte 0 en dernière position. Exemple : pour un code d'utilisateur sans préfixe = 4449, saisir pour la commande d'accès sous contrainte 4440 (saisir uniquement 0 à la fin). Attention : l'activation de cette fonction effacera tous les codes prédéfinis dans le système !!!	
<b>Confirmation de l'alarme dans une section*</b>	Si le détecteur est programmé pour la confirmation de la réaction par un autre détecteur, cette option de confirmation permet de limiter la confirmation uniquement pour la <b>même</b> section (sinon, la confirmation d'alarme est réalisée par un détecteur de n'importe quelle section). Autant valable pour les détecteurs d'intrusion que les détecteurs d'incendie.	
<b>Sirène (sortie IW) en cas de sabotage*</b>	Une sirène avec une réponse acoustique IW indique une alarme de sabotage dans une zone en statut désarmé ou partiellement armé.	
<b>Réinitialisation activée*</b>	Possibilité de bloquer la réinitialisation de la centrale par un cavalier sur la carte. Si la réinitialisation est interdite et le code de service est perdu, la centrale ne peut être déverrouillée que par le fabricant. La remise à zéro de la centrale est décrite au chapitre 12 Réinitialisation de la centrale.	
<b>Échec de l'armement</b>	La fonction est traitée pendant chaque procédure d'armement. Si une zone instantanée est déclenchée au cours de la temporisation de sortie ou si une zone temporisée reste ouverte lorsque la temporisation de sortie expire, le système ne s'arme pas et déclenche l'événement « Échec de l'armement » puis l'enregistre dans l'historique. Il est enregistré dans l'historique du système et également signalé par un module GSM ou PSTN supplémentaire, en cas de connexion, par SMS à un utilisateur prédéfini et si l'événement « SMS relatif à l'échec de l'armement » est activé pour l'envoi. Il est indiqué par des claviers ainsi que par une sirène extérieure. Pour annuler l'indication concernant l'échec de l'armement, il faut appuyer sur « Annuler l'indication d'avertissement » dans le menu du clavier.	
<b>Indication de mémoire d'alarme</b>	L'option permet l'indication de la mémoire d'alarme par un voyant LED intégré dans le détecteur qui a déclenché l'alarme. Disponible uniquement pour les périphériques pris en charge.	
<b>Profils du système</b>	Sélection des profils du système prédéfinis conformément aux exigences.	
	Défaillance	Paramètres par défaut avec option de modification conformément aux besoins
	EN50131-1, niveau 2	Certains paramètres sont prédéfinis automatiquement pour se conformer à EN50131-1, niveau 2 sans option de modification
	INCERT, niveau 2	Certains paramètres sont prédéfinis automatiquement pour se conformer à INCERT, niveau 2 sans option de modification
<b>Méthodes d'armement</b>	Sélection de la méthode par laquelle le système gère le processus d'armement. Du niveau le plus bas où le système s'arme toujours indépendamment des périphériques actifs ou des défaillances dans le système au niveau le plus élevé où ce dernier ne peut pas être armé avec des périphériques actifs (zone instantanée). Ce paramètre est également lié au profil du système.	

	Armement permanent	Arme systématiquement quel que soit le statut du système (défaillances, détecteurs actifs, etc.).
	Armement avec avertissement	Indique par voie optique (touche fonctionnelle et affichage) le statut du système (défaillances, éléments actifs, batterie ou batterie de secours faibles) pendant 8 secondes et arme automatiquement à l'expiration de cette période. L'armement est également possible en enclenchant plusieurs fois la touche fonctionnelle (ou en appuyant sur la touche ENTRÉE).
	Armement après confirmation	Indique par voie optique (touche fonctionnelle et affichage) le statut du système (défaillances, éléments actifs, batterie ou batterie de secours faibles) pendant 8 secondes. Peut être armé UNIQUEMENT en enclenchant plusieurs fois la touche fonctionnelle (ou en appuyant sur la touche ENTRÉE).
	Ne pas armer avec un élément actif	Indique par voie optique (touche fonctionnelle et affichage) le statut du système (défaillances, périphérique actif, batterie ou batterie de secours faibles) pendant 8 secondes. Le système peut être armé en appuyant plusieurs fois sur la touche fonctionnelle (ou en appuyant sur la touche ENTRÉE), mais seulement si le détecteur actif a une réaction du type TEMPORISÉE ou TEMPORISÉE DIFFÉRÉE. Un élément actif avec toute autre réaction d'alarme NE PEUT PAS être armé de cette façon. ATTENTION !!! Cela vaut également pour la commande à distance (menu vocal, SMS, Internet ou application mobile, action via le calendrier).
Type d'autorisation	Sélection de la manière dont le système traite l'autorisation de l'utilisateur. Également lié à la commande d'une sortie PG avec autorisation.	
	Standard	La saisie d'un code de l'utilisateur, l'utilisation d'une carte ou d'un badge RFID valideront l'autorisation. Seule une de ces options est requise pour commander le système.
	Double autorisation	La saisie d'un code de l'utilisateur, l'utilisation d'une carte ou d'un badge RFID permettront une autorisation valide. F-Link surveille si un code et une carte sont attribués à un utilisateur dans l'onglet Utilisateurs (sinon F-Link ne permettra pas d'enregistrer la configuration). L'accès téléphonique à distance est activé uniquement pour les numéros autorisés.
Perte d'un périphérique BUS	La centrale traite la perte d'un périphérique ou un court-circuit sur le BUS du système. Selon l'option sélectionnée, le système réagira à la situation suivante :	
	Défaillance	La centrale traite toujours la perte d'un périphérique sur le BUS ou un court-circuit du BUS comme une défaillance.
	Sabotage permanent	La centrale traite la perte d'un périphérique sur le BUS ou un court-circuit du BUS comme une alarme de sabotage permanent en cas de survenue. Si le module radio possède une détection de brouillage RF autorisée et qu'un brouillage est détecté, il déclenche également une alarme de sabotage. Une alarme de sabotage est également suivie d'une défaillance et, lorsque la défaillance disparaît, l'alarme de sabotage disparaît également.

	Sabotage après confirmation	La centrale traite la perte d'un premier périphérique comme une défaillance et si, dans un délai prédéfini donné par le paramètre « Période d'attente pour la confirmation d'alarme », une autre perte de périphérique se produit, alors le système les confirme et déclenche une alarme de sabotage. Lorsque tous les périphériques perdus sont restaurés, le système annule l'alarme de défaillance et de sabotage.
<b>Paramétrage du minuteur</b>	Dans chaque section, les temporisations d'entrée et de sortie sont mesurées séparément. Si des sorties temporisées différentes sont programmées pour les détecteurs d'une même section, la temporisation la plus longue est prise en compte. En cas de temporisations d'entrée différentes, celle qui appartient au détecteur activé est mesurée. En cas d'activation de plusieurs détecteurs, l'entrée temporisée définie la plus courte est prise en compte.	
<b>Durée de l'alarme</b>	Durée de l'alarme - s'applique à toutes les sections. Amplitude 5s - 20min.	
<b>Temporisation d'entrée</b>	Minuteur. Amplitude 5s - 2 min.	
<b>Temporisation de sortie</b>	Minuteur. Amplitude 5s - 2 min.	
<b>Temporisation d'entrée de la porte du garage</b>	Minuteur. Amplitude 5s - 6 min.	
<b>Temporisation de sortie de la porte du garage</b>	Minuteur. Amplitude 5s - 6 min.	
<b>Attente de la confirmation d'intrusion par un autre détecteur</b>	Durée d'attente de la confirmation de l'alarme par un autre détecteur de la section armée. Valable pour tous les détecteurs ayant une réaction Confirmée immédiate / Confirmée temporisée (1 - 60 min).	
<b>Attente de la confirmation d'incendie par un autre détecteur</b>	Durée d'attente de la confirmation de l'alarme d'incendie par un autre détecteur. Valable pour tous les détecteurs ayant une réaction Incendie confirmée (1 - 60 min.).	
<b>Rapport de section désarmée</b>	Une section qui est restée désarmée sans détection de mouvement pendant plus de 16 heures signalera une « section désarmée ».	
<b>Rapport différé à la télésurveillance</b>	En cas d'activation, une alarme interne sera déclenchée après l'expiration de la temporisation d'entrée, mais le système attendra 15 secondes pour envoyer un rapport d'alarme à la télésurveillance. Un utilisateur dispose ainsi de 15 secondes supplémentaires pour désarmer le système sans déclencher une alarme signalée à la télésurveillance.	

## 10.8 Onglet Calendriers

Il est ici possible de définir le calendrier des événements que le système réalisera automatiquement et régulièrement. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.

Event	Days of the week	Time	Guarding	Section	PG Control	PG number	Block...	Note
1	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	No	1 2 3 4	No	1 2 3 4	No	
2	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Set	1 2 3 4	No	1 2 3 4	No	
3	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Set partially	1 2 3 4	No	1 2 3 4	No	
4	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Unset	1 2 3 4	No	1 2 3 4	No	
5	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Set immediately	1 2 3 4	No	1 2 3 4	No	
6	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Set partially now	1 2 3 4	No	1 2 3 4	No	
7	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Set always	1 2 3 4	No	1 2 3 4	No	
8	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Always set partially	1 2 3 4	No	1 2 3 4	No	
9	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Always set immediately	1 2 3 4	No	1 2 3 4	No	
10	Mon, Tue, Wed, Thu, Fri, Sat, Sun	00:00	Always set partially and immediately	1 2 3 4	No	1 2 3 4	No	

**Jours de la semaine** - définit les jours où l'action est exécutée (par ex. tous les lundis).

**Temps** - détermine à quel moment l'action sera exécutée le jour fixé.

**Surveillance** - permet d'exécuter les actions « Armement », « Armement partiel » avec la version « Instantané » (pas de temporisation de sortie ou d'indication acoustique) et la version « Permanent » (règles d'armement définies toujours ignorées), « Désarmement ».

**Sections** - précise dans quelle(s) section(s) l'action du type d'armement sera exécutée.

**Commandes PG\*** - permet de paramétrer l'activation ou la désactivation PG, le blocage ou le déblocage des sorties PG. Le blocage des sorties PG ne peut être commandé à partir de la touche fonctionnelle ou par SMS.

**Nombre PG\*** - précise la ou les sorties qui seront activées ou désactivées.

**Blocage** - les sorties PG y sont proposées, leur activation permet de bloquer une action programmée.

**Désactiver** - permet de bloquer l'action respectives. La désactivation est signalée par un point rouge. Le technicien de service (via F-Link) est autorisé à désactiver le calendrier.

**Remarque** - fournit la possibilité d'une description personnalisée des événements programmés.

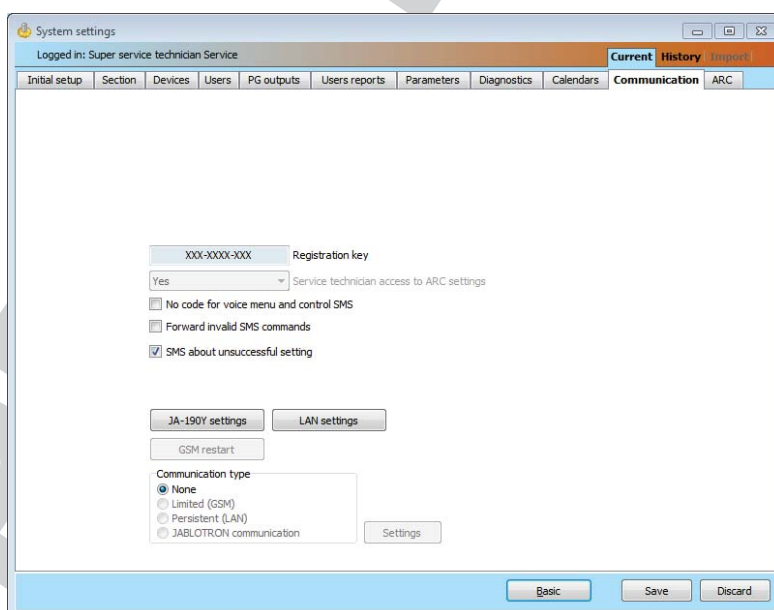
**Calendrier annuel** - permet de modifier l'attribut du jour sur « Dimanche » pour les différents jours de l'année en cours et celle qui suit. Il est possible de le modifier en cliquant (de manière répétée) sur la touche de la souris sur le jour correspondant. Exemple d'application : pour un jour férié (jour non ouvrable) tombant un mercredi, il est possible de modifier l'attribut de la journée du mercredi par celui du dimanche. Les événements qui sont automatiquement planifiés conformément aux paramètres de base du calendrier et valides pour les jours ouvrables ne sont pas réalisés ce jour-là. Toutefois, le programme valable pour le dimanche sera conservé. De cette façon, il est possible d'ajuster la commande des sections ou la commande PG par ex. pour les périodes de fermeture de l'entreprise, etc. La valeur « arrêt » implique la désactivation - les jours indiqués de cette manière, aucun événement programmé n'est exécuté.

#### Remarques :

- Un événement du calendrier peut commander (activer ou désactiver) l'armement et les sorties PG en même temps.
- Le lancement et l'arrêt d'une application pour une certaine période est possible de 2 façons. Il est possible de paramétrer l'action pour l'activation et l'action pour la désactivation de la sortie PG ou uniquement l'action pour l'activation et l'armement d'une impulsion de la durée requise pour la sortie PG.
- Si la sélection Armement (armement partiel) est choisie pour une section spécifiée, une temporisation de sortie à l'heure spécifiée avec un temps fixe de 3 min. est d'abord activée. Tous les capteurs dans les sections spécifiées avec une réaction instantanée sont réajustés avec une réaction temporisée au cours de cette période de 3 minutes. Si la sélection Armement immédiat est choisie, aucune temporisation de sortie n'est fournie et tous les détecteurs sont actifs immédiatement (y compris les détecteurs temporisés).

## 10.9 Onglet Communication

L'onglet est utilisé pour définir le comportement des transmetteurs et la voie de communication. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.



**Clé d'enregistrement** - code d'enregistrement unique de la centrale.

**Menu vocal et commande SMS sans code** - en cas d'utilisation d'un téléphone autorisé à commander une fonction par un appel, l'utilisateur n'a pas à saisir son code (il est autorisé en appelant de son téléphone). Pour cette fonction, l'identification de l'appelant (CLIP) doit être activée.

**Transfert de commandes SMS invalides** - choix de la transmission vers le numéro de téléphone de l'administrateur en position 1 des messages SMS incompréhensibles vers la centrale (informations de facturation de l'opérateur, etc.).

**SMS relatif à un échec de l'armement** - en cas d'activation, la centrale envoie un SMS relatif à l'échec de l'armement. Lorsque la commande est réalisée par un utilisateur autorisé, la centrale envoie alors un SMS sur le téléphone attribué à cet utilisateur autorisé. Lors de la commande sans autorisation, la centrale envoie alors un SMS vers le numéro de téléphone de l'administrateur en position 1.

**Type de communication** - le système propose plusieurs méthodes de communication / configuration à distance.

- **Sans configuration à distance** - aucune communication de données n'est utilisée. La configuration à distance par F-Link n'est pas possible.
- **Restreint (GSM)** - la centrale peut établir une connexion de données avec le serveur et permet une connexion à distance via F-Link. La connexion n'a pas la même période de consommation que la communication permanente (LAN). Lorsque le système est équipé d'un transmetteur GSM, l'option peut être activée.
- **Permanent (LAN)** - la centrale communique en permanence avec le serveur et permet la connexion à distance via F-Link. Lorsque le système n'inclut pas de numéroteur GSM, cette option peut être activée.
- **Communication Jablotron** - l'enregistrement sur le Cloud JABLOTRON autorise toutes les options proposées par le système, telles que la connexion à distance via F-Link et les applications MyJABLOTRON et MyCOMPANY.

**Réglages** - Sélection du type de centrale avec une communication externe avec le serveur JABLOTRON. Permet la commande à distance via le logiciel F-Link, l'enregistrement du système sur le CLOUD et l'utilisation des applications MyJABLOTRON et MyCOMPANY.

### 10.9.1 Paramètres JA-190Y

Utilisé pour définir les paramètres et le comportement du transmetteur GSM supplémentaire JA-190Y.

**Transmetteur GSM** - possibilité d'éteindre le transmetteur.

**Signal GSM** - donnée concernant la puissance du signal en pourcentage (la mesure s'effectue chaque minute). Pour un fonctionnement adéquat, le signal doit avoir un niveau de puissance d'au moins 50%. En cas de difficultés avec la qualité du signal GSM, il est recommandé d'essayer une carte SIM d'un autre opérateur. Pour le transmetteur, il n'est pas recommandé d'utiliser une antenne GSM directionnelle ou un amplificateur (elle ramène la connexion du module à 1 seule cellule du réseau = communication instable). Il est également possible d'obtenir des informations sur la qualité du signal en utilisant la consigne SMS STATUT (voir le point 9.6 Consignes SMS).

**PIN** - il est recommandé d'utiliser une carte SIM avec un code PIN désactivé.

**APN\*** - paramétrage de la communication de données GPRS. La communication de données permet l'accès aux services tels que l'accès à distance du technicien de service et de l'utilisateur, la communication avec le CLOUD JABLOTRON, la télésurveillance etc. Hormis le paramétrage APN, la carte SIM utilisée doit autoriser les transmissions de données.

**Utilisateur APN\*** - nom (si le réseau ne l'utilise pas, ne rien saisir).

**Mot de passe APN\*** - mot de passe (si le réseau ne l'utilise pas, ne rien saisir).

**Sensibilité de la détection DTMF à partir de la télésurveillance** - paramétrage de la sensibilité de réception des signaux générés par la télésurveillance. La sensibilité est réglable par pas de 10, la valeur optimale par défaut est 6.

**Niveau de DTMF généré vers la télésurveillance** - paramétrage de l'intensité du signal transmis de tonalité DTMF généré par la centrale. L'intensité est réglable par pas de 10, la valeur optimale par défaut est 4.

**Nombre de sonneries pour les appels entrants** - nombre de sonnerie jusqu'à une réponse automatique par le transmetteur. Il est possible de définir une réponse après 1 à 10 sonneries (correspondant à 5 - 50 secondes). La valeur par défaut est 3 (15 secondes).

**Autorisation des symboles alphanumériques étendus** - si les symboles alphanumériques étendus (ICC) sont autorisés, les messages du système peuvent être envoyés en plusieurs SMS. Les symboles alphanumériques étendus doivent être activés s'ils sont utilisés dans les messages, par ex. avec l'alphabet russe, etc.

**Commande à distance par téléphone** - paramètre la possibilité de commander le système à distance à l'aide du menu vocal. En cas de sélection des utilisateurs, il n'est possible d'entrer dans le menu qu'à partir des téléphones des utilisateurs définis (dans l'onglet Communication, il est également possible d'autoriser aux utilisateurs l'accès au menu vocal sans saisie de leur code d'utilisateur - sélection Commande sans code dans le menu vocal). Si « aucun utilisateur » n'est sélectionné, il est possible d'entrer dans le menu vocal à partir de n'importe quel téléphone. Cependant, lors de l'accès au menu, la saisie du code d'accès de l'utilisateur sera toujours requise.

**Commande à distance par envoi de SMS** - paramètre la possibilité de commander le système à distance à l'aide de consignes SMS. Si elle est paramétrée pour l'utilisateur, le système n'accepte les consignes SMS que des téléphones des utilisateurs définis (dans l'onglet Communication, il est également possible d'autoriser aux utilisateurs l'accès aux consignes SMS sans saisie d'un code - sélection Commande sans code dans le menu vocal). Si « aucun utilisateur » n'est défini, la consigne SMS peut être envoyée de n'importe quel téléphone ; elle est cependant conditionnée par la saisie d'un code d'accès.

**Information relative au solde** - en appuyant sur cette touche, il est immédiatement possible d'obtenir des informations sur le solde créditeur de l'opérateur (si cette fonction est prise en charge).

**Solde - limite** - possibilité de saisir une limite inférieure pour la vérification automatique du solde sur une carte SIM prépayée. Si le solde constaté est inférieur à cette limite, le système envoie un SMS d'information à la personne sélectionnée pour la réception d'un **SMS d'erreur et de service**. Attention : **il n'est pas recommandé d'utiliser une carte prépayée dans le système - cela augmente le risque de défaillance de communication**.

**Séquence du solde SIM** - commande pour la vérification automatique du solde d'une carte SIM prépayée (en cas de prise en charge par l'opérateur). La commande peut être obtenue auprès de votre opérateur.

**Solde - position dans le texte** - position (numéro séquentiel du caractère) dans le rapport du solde de l'opérateur à partir de laquelle l'information numérique relative au solde commence (le transmetteur ne recherche que les valeurs numériques figurant dans le rapport et ignore les autres caractères).

**Solde - période de vérification** - paramètre relatif à la fréquence à laquelle le système vérifie le solde (il est possible de saisir 0 à 99 jours, où 0 correspond à une désactivation).

**Numéro de téléphone de la carte SIM** - le numéro de téléphone de la carte SIM insérée est affiché ici, le système l'obtient du serveur.

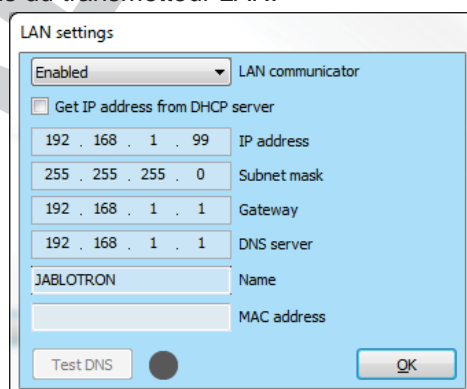
**Obtenir le numéro de téléphone du transmetteur** - la touche sert à obtenir manuellement le numéro de téléphone du serveur.

## 10.9.2 Redémarrage GSM

Touche pour la déconnexion et la reconnexion du transmetteur GSM au réseau. La reconnexion GSM au réseau peut durer plusieurs dizaines de secondes (fonction de l'état dans lequel se trouve le système). Le système GSM peut aussi être relancé en utilisant la consigne SMS GSM (voir le chapitre 9.6 Consignes SMS).

## 10.9.3 Paramètres LAN

Utilisé pour paramétrer les fonctions du transmetteur LAN.



**Transmetteur LAN** - possibilité d'activer ou désactiver la communication LAN.

**Obtenir l'adresse IP du serveur DHCP** - configuration automatique des paramètres du réseau. Si le réseau ne prend pas en charge pas cette fonction, il faut saisir manuellement les paramètres correspondants. La saisie manuelle n'est possible que si l'option est désactivée.



**Adresse IP** - paramétrage manuel de l'inscription d'une adresse IP qui n'est disponible que si l'inscription automatique à partir du serveur DHCP n'est pas activée. Le paramétrage par défaut est 192.168.1.99.

**Masque de sous-réseau** - paramétrage manuel pour l'inscription du masque de sous-réseau IP qui n'est disponible que si l'inscription automatique à partir du serveur DHCP n'est pas activée. Le paramétrage par défaut est 255.255.255.0.

**Passerelle** - paramétrage manuel pour l'inscription par défaut de la passerelle IP qui n'est disponible que si l'inscription automatique à partir du serveur DHCP n'est pas activée. Le paramétrage par défaut est 192.168.1.1.

**Serveur DNS** - paramétrage manuel de l'inscription de l'adresse IP du serveur DNS qui n'est disponible que si l'inscription automatique à partir du serveur DHCP n'est pas activée. Le paramétrage par défaut est 192.168.1.1.

**Nom** - nom du périphérique facilitant l'identification sur le réseau local.

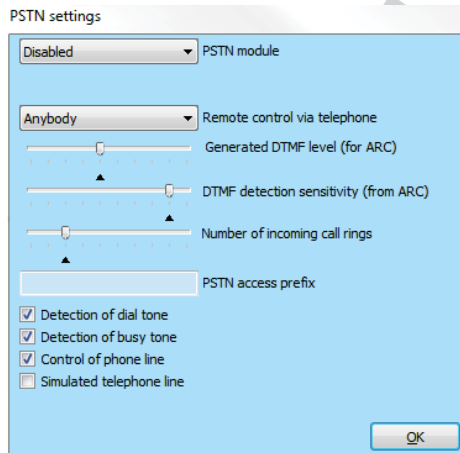
**Adresse MAC** - adresse unique de chaque périphérique LAN (identification de la source des données).

Périphérique LAN pour l'identification de la source d'information

**Test DNS** - lorsque le transmetteur LAN est connecté à Internet, les paramètres peuvent être testés quant à leur exactitude. Si un point vert apparaît après avoir enclenché la touche, la connexion au serveur a été établie, mais si un point rouge s'affiche au bout de quelques secondes, le temps d'établissement de la connexion a expiré, ce qui indique un mauvais paramétrage ou une erreur dans la connexion du transmetteur LAN.

### 10.9.4 Paramètres PSTN

Il est utilisé pour paramétrer le transmetteur téléphonique (si la centrale en est dotée).



**Module PSTN** - possibilité d'activer ou désactiver la communication par téléphone.

**Commande à distance par téléphone** - paramètre la possibilité de commander le système à distance à l'aide du menu vocal. En cas de sélection des utilisateurs, il n'est possible d'entrer dans le menu qu'à partir des téléphones des utilisateurs définis (dans l'onglet Communication, il est également possible d'autoriser aux utilisateurs l'accès au menu vocal sans saisie de leur code d'utilisateur - sélection Commande sans code dans le menu vocal). Si aucun utilisateur spécifique n'est sélectionné, il est possible d'entrer dans le menu vocal à partir de n'importe quel téléphone. Cependant, lors de l'accès au menu, la saisie du code d'accès de l'utilisateur sera toujours requise.

**Niveau DTMF généré (pour la télésurveillance)** - paramétrage de l'intensité du signal transmis relatif à la tonalité DTMF généré par la centrale. L'intensité est réglable par pas de 10, la valeur optimale par défaut est 4.

**Sensibilité de détection DTMF (à partir de la télésurveillance)** - paramétrage de la sensibilité de réception du signal généré par la télésurveillance. La sensibilité est réglable par pas de 10, la valeur optimale par défaut est 8.

**Nombre de sonneries pour les appels entrants** - nombre de sonnerie jusqu'à ce que l'appel soit pris par le transmetteur. Il est possible de définir une réponse après 1 à 10 sonneries (correspondant à 5 - 50 secondes). La valeur par défaut est 3 (15 secondes).

**Préfixe d'accès PSTN** - code de numérotation relatif aux centraux téléphoniques.

**Tonalité** - si ce paramètre est désactivé, le transmetteur va commencer à composer le numéro de téléphone défini quels que soient le type ou la présence de tonalité. S'il est activé, le transmetteur ne commence à fonctionner que lorsqu'il détecte la tonalité (par ex. la temporisation d'inscription de tonalité dans certains centraux téléphoniques).

**Détection de la tonalité d'occupation** - si le transmetteur détecte une tonalité d'occupation, par ex. sur une ligne parallèle, il raccroche et informe le système. Il n'est pas recommandé d'activer ce paramètre si le transmetteur ne détecte pas le fait de raccrocher.

**Contrôle de ligne téléphonique** - le transmetteur désactive complètement la détection de la tension dans la ligne de téléphone. Cela signifie qu'il ne signalera pas l'erreur relative à une ligne téléphonique arrachée. Le

cas échéant, une erreur sera indiquée après 30 min. à compter de la détection de la perte de la ligne téléphonique. Le transmetteur indique l'erreur par un voyant jaune.

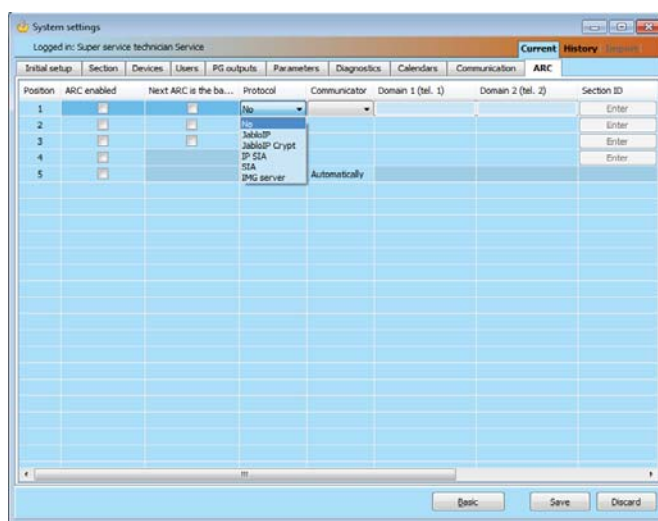
**Ligne téléphonique simulée** - si elle est activée, le transmetteur ne vérifie pas la présence de la ligne téléphonique ou de la tonalité. Ainsi, il ne détecte pas une erreur de ligne téléphonique pour une tension inférieure à 15 V. Cela sert aux modems radio.

Une description détaillée des paramètres se trouve dans le manuel du module du transmetteur téléphonique JA190X.

## 10.10 Onglet Télésurveillance (ARC)

Cet onglet est utilisé pour paramétrer la communication jusqu'à 4 voies de transmissions d'alarme ou par 4 protocoles de communication. Chaque voie de transmission peut être utilisée pour 4 centres de télésurveillance différents ou généralement pour 4 récepteurs de rapports d'alarme différents.

Si l'accès du technicien de service est limité dans l'onglet Communication, il n'est possible de réaliser le paramétrage que par une personne dotée du niveau d'accès du technicien de télésurveillance. L'option est également indisponible en cas de sélection de la Communication Jablotron, ce qui simplifie grandement le paramétrage de la configuration de la partie liée à la communication du système. Pour apporter des modifications dans cet onglet, il n'est pas requis d'être en mode Service.



**Télésurveillance activée** - possibilité de désactiver la communication paramétrée.

**Centre de télésurveillance suivant de secours** - en cas d'activation, la position suivante ne sera utilisée que si les données ne peuvent être transmises à partir de cette position.

**Protocole** - paramétrage du protocole de transmission.

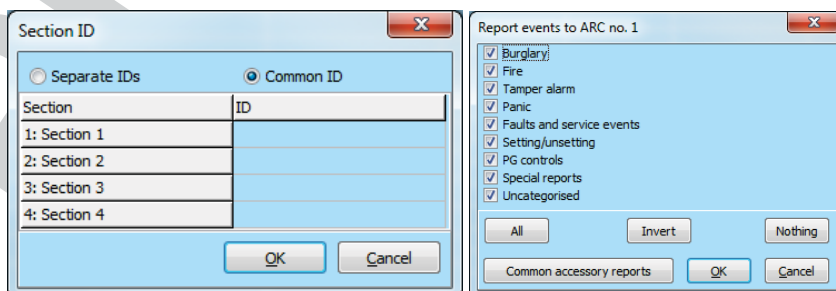
**Transmetteur** - si le protocole sélectionné peut être transmis de plusieurs façons, le type de transmetteur est sélectionné.

**Domaine 1 (tél. 1)** - paramétrage du domaine principal (utilisation de l'URL ou l'adresse IP), éventuellement du numéro de téléphone principal en fonction du protocole utilisé. Si la communication IP est utilisée, il faut saisir le port de communication après l'adresse IP, séparé par une colonne. Les données relatives au port de communication et à l'adresse IP sont obtenues auprès de la télésurveillance vers laquelle est acheminée la communication. Si aucun port de communication n'est complété, l'évènement ne sera pas transmis.

**Domaine 2 (tél. 2)** - paramétrage du domaine de secours (utilisation de l'URL ou l'adresse IP), éventuellement du numéro de téléphone de secours en fonction du protocole utilisé.

**ID des sections** - paramètre l'identification du site (commune à tout le site ou séparée pour les sections).

**Avertissement** : le paramétrage par défaut est zéro, pour lequel le transmetteur n'enverra aucun rapport !



**Évènements signalés** - sélection des types d'évènements signalés et possibilité de paramétrer les codes des rapports supplémentaires (sorties PG).

**Minuteur** - réglage des limites temporelles pour les transmissions et réglage de la période de vérification de la connexion.

**Test de télésurveillance** - son enclenchement déclenche un test de vérification de la connexion avec le protocole correspondant.

**Note** - détails relatifs aux paramètres de la télésurveillance, date de démarrage du service, etc.

### 10.10.1 Exigences pour la configuration des voies de transmission vers une télésurveillance

La centrale JA-100K peut établir des voies de transmission vers les télésurveillances conformément aux normes européennes EN 50136-1 et EN 50136-2. Le tableau suivant détermine les paramètres individuels conformes à la classe ATS spécifique. La prise en charge totale des classes ATS par la télésurveillance est nécessaire.

Classe ATS	Interfaces utilisables (Protocoles d'alarme)	Vérification de la connexion au moment fixé	Temps de vérification de la connexion	Défaillance lors du dépassement de la temporisation de rapport d'événement	Nombre de répétitions	Période d'attente après une tentative infructueuse	Cryptage Temps du système Temps de l'événement
SP2	PSTN / GSM / LAN (JABLO IP, SIA IP, SIA CID)	Optionnel	1x par 24 heures	120 s	2	30 s	Optionnel Requis Requis
SP3	GSM / LAN (JABLO IP, SIA IP, SIA CID)	Interdit	1x 30 min	60 s	2	30 s	Optionnel Requis Requis
SP4	GSM / LAN (JABLO IP, SIA IP)	Interdit	1x 3 min	60 s	3	20 s	Requis Requis Requis
SP5	GSM / LAN (JABLO IP, SIA IP)	Interdit	1x 1 min	30 s	6	5 s	Requis Requis Requis
DP2	LAN + PSTN (JABLO IP, SIA IP)	Interdit	1x 30 min	60 s	2	30 s	Optionnel Requis Requis
DP3	LAN + GSM (JABLO IP, SIA IP)	Interdit	1x 3 min	60 s	3	20 s	Requis Requis Requis

### 10.10.2 Voies de transmission

Pour la communication GSM (GPRS) et LAN utilisant des protocoles IP :

- 1) Protocole ANSI SIA DC-09, SIA IP (DC9), méthodes DCS ou ADM\_CID (message de données)
  - cryptage conformément à la norme AES avec des clés de 128, 192 ou 256 bits
  - message unique horodaté
  - synchronisation du temps très précise entre le système d'alarme et la télésurveillance
- 2) Protocole JABLO\_IP (message de données)
  - Protocole Jablotron propriétaire
  - Cryptage 256 bits
  - message unique horodaté
  - synchronisation du temps précise entre le système d'alarme et la télésurveillance
- 3) JABLO\_SMS (messages SMS de données)
  - basé sur le protocole JABLO\_IP avec un cryptage de données flottantes

### 10.10.3 Codes CID et SIA JABLOTRON 100

CID	SIA	Évènement EN	Catégorie de rapport
1101	QA	Problème de santé	Cambriolage
1110	FA	Alarme d'incendie	Incendie
1118	FG	Alarme d'incendie non confirmée	Incendie
1120	PA	Alarme de détresse	Détresse
1130	BA	Alarme instantanée	Cambriolage
1133	BA	Alarme 24H	Cambriolage

1134	BA	Alarme temporisée	Cambriolage
1138	BG	Alarme non confirmée	Cambriolage
1144	TA	Sabotage d'un périphérique	Sabotage
1151	GA	Fuite de gaz	Incendie
1154	WA	Alarme d'inondation	Sabotage
1170	UA	Réaction spéciale A	Rapports spéciaux
1171	UA	Réaction spéciale B	Rapports spéciaux
1172	UA	Réaction spéciale C	Rapports spéciaux
1173	UA	Réaction spéciale D	Rapports spéciaux
1174	UA	Non utilisé	Rapports spéciaux
1175	UA	Non utilisé	Rapports spéciaux
1176	UA	Non utilisé	Rapports spéciaux
1177	UA	Armoire à clés	Rapports spéciaux
1300	ET	Défaillance	Évènements de défaillance et de service
1301	AT	Perte de l'alimentation	Cambriolage
6301	AT	Perte de l'alimentation supérieure à 30 min (à compter de la version 10 et supérieure du micrologiciel)	Cambriolage
1302	YT	Batterie faible dans la centrale	Évènements de défaillance et de service
1305	RR	Démarrage du système	Évènements de défaillance et de service
1306	LB	Entrée en mode Service	Évènements de défaillance et de service
1308	RE	Arrêt du système	Évènements de défaillance et de service
1313	YX	Blocage après alarme - Redémarrage	Non catégorisé
1314	YG	Paramètres de la télésurveillance effacés	Non catégorisé
1344	XQ	Brouillage RF / interférence RF	Évènements de défaillance et de service
1350	YC	Évènement non envoyé à télésurveillance	Non catégorisé
1354	YS	Évènement non envoyé à télésurveillance dans la période programmée	Évènements de défaillance et de service
1384	XT	Batterie faible dans le périphérique	Évènements de défaillance et de service
1401	OP	Désarmement	Armement / Désarmement
1402	OG	Désarmement partiel	Armement / Désarmement
1406	BC	Alarme annulée par l'utilisateur	Cambriolage
1407	OQ	Désarmement à distance	Armement / Désarmement
1412	LF	Accès à distance	Non catégorisé
1416	LS	Configuration sauvegardée	Non catégorisé
1454	CI	Section sans mouvement	Évènements de défaillance et de service
1455	CI	Échec de l'armement	Non catégorisé
1461	JA	Nombre de tentatives de décodage dépassé	Sabotage
1521	BL	Sirène muette	Non catégorisé
1570	EB	Dérivation du périphérique (désactivé)	Non catégorisé
1572	TB	Dérivation de sabotage	Évènements de défaillance et de service
1573	BB	Dérivation de l'activation	Évènements de défaillance et de service
1574	UB	Dérivation du périphérique (désactivé)	Non catégorisé
1578	UO	Dérivation de la défaillance	Évènements de défaillance et de service
1601	RX	Test manuel	Évènements de défaillance et de service
1602	RP	Test périodique / test du lien	Non catégorisé
1625	JT	Réinitialisation de l'heure	Non catégorisé
1661	RC	PG1 activée	Commandes PG
1662	RC	PG2 activée	Commandes PG
1663	RC	PG3 activée	Commandes PG
1664	RC	PG4 activée	Commandes PG
3101	QR	Problèmes de santé (désactivation)	Cambriolage
3110	FR	Alarme d'incendie (désactivation)	Incendie
3118	FG	Alarme d'incendie non confirmée (désactivation)	Incendie
3120	PR	Détresse (désactivation)	Détresse
3130	BR	Alarme instantanée (désactivation)	Cambriolage
3133	BR	Alarme 24h (désactivation)	Cambriolage
3134	BR	Alarme temporisée (désactivation)	Cambriolage
3138	BG	Alarme non confirmée (désactivation)	Cambriolage
3144	TR	Sabotage (désactivation)	Sabotage
3151	GR	Fuite de gaz (désactivation)	Incendie
3154	WR	Alarme d'inondation (désactivation)	Sabotage

3170	UR	Réaction spéciale A (désactivation)	Rapports spéciaux
3171	UR	Réaction spéciale B (désactivation)	Rapports spéciaux
3172	UR	Réaction spéciale C (désactivation)	Rapports spéciaux
3173	UR	Réaction spéciale D (désactivation)	Rapports spéciaux
3174	UR	Non utilisé	Rapports spéciaux
3175	UR	Non utilisé	Rapports spéciaux
3176	UR	Non utilisé	Rapports spéciaux
3177	UR	Armoire à clés (désactivation)	Rapports spéciaux
3300	ER	Défaillance (désactivation)	Évènements de défaillance et de service
3301	AR	Retour de l'alimentation réseau	Non catégorisé
3302	YR	Batterie de la centrale OK	Rapports spéciaux
3306	LX	Sortie du mode Service	Rapports spéciaux
3313	YZ	Déblocage après alarme	Non catégorisé
3344	YH	Interférence RF / brouillage RF (désactivation)	Évènements de défaillance et de service
3350	YK	Restauration de la communication vers la télésurveillance	Non catégorisé
3354	YL	Évènement non envoyé à télésurveillance dans la période programmée (désactivation)	Évènements de défaillance et de service
3384	XR	Batterie du périphérique OK	Évènements de défaillance et de service
3401	CL	Armer	Armement / Désarmement
3402	CG	Armement partiel	Armement / Désarmement
3407	CQ	Armer à distance	Armement / Désarmement
3412	LE	Accès à distance terminé	Non catégorisé
3417	CU	Armé partiellement à distance	Armement / Désarmement
3570	EU	Fin de la dérivation du périphérique (désactivation)	Non catégorisé
3572	TU	Fin de la dérivation de sabotage	Sabotage
3573	BU	Fin de la dérivation d'activation	Non catégorisé
3574	UU	Fin de la dérivation de la section (désactivation)	Non catégorisé
3578	UP	Dérivation de la défaillance (désactivation)	Évènements de défaillance et de service
3661	RO	PG1 désactivée	Commandes PG
3662	RO	PG2 désactivée	Commandes PG
3663	RO	PG3 désactivée	Commandes PG
3664	RO	PG4 désactivée	Commandes PG

Code source	Description
001 - 120	Périphériques
501 - 800	Codes utilisateurs
500	Code de service
901	Centrale
921	Télésurveillance1
922	Télésurveillance2
923	Télésurveillance3
924	Télésurveillance4
912	Transmetteur LAN
913	Transmetteur PSTN
914	Transmetteur GSM supplémentaire

## 10.11 Onglet Diagnostic

Il est utilisé pour commander et vérifier le statut des périphériques et leurs propriétés.

P	Name	Type	Section	Activation...	Status	Battery status/voltage	Voltage/ loss	RF Signal level	Channel	Note
0	Control panel	JA-101K	1: Ground floor		OK	13.7 V/13.7 V	13.7 V/163 mA	100 % GSM		
1	Radio module	JA-110R	1: Ground floor		OK		-0,1 V		RJ	
2	LCD keypad	JA-114E	1: Ground floor		OK		-0,4 V		RJ	
3	Main door	JA-110M	1: Ground floor		ACT		0,0 V		Bus 1	
4	Kitchen window	JA-110M	1: Ground floor		OK		0,0 V		Bus 1	
5	Garage door	JA-111M	3: Garage		ACT		0,0 V		Bus 1	
6	Hall	JA-110P	1: Ground floor		OK		-0,1 V		Bus 1	
7	Garage PIR	JA-120PW	3: Garage	ACT	OK		-0,2 V		RJ	
8	Indoor siren	JA-110A	1: Ground floor		OK		0,0 V		Bus 1	
(?) 9	Balcony door	JA-150M	2: First floor		ACT	100 %		100 %		
(?) 10	Balcony window	JA-150M	2: First floor		OK	100 %		100 %		
(?) 11	Living room	JA-151P	2: First floor		ACT	100 %		80 %		
12	Interface	JA-121T	1: Ground floor		OK		-0,3 V		RJ	
(?) 13	Remote control	JA-182J	4: Fully set							

**Mémoire d'activation** - enregistre les activations du périphérique qui se sont produites depuis le dernier effacement de cette colonne. La mémoire des activations de tous les périphériques peut être effacée avec la touche Effacer la mémoire (menu du bas). La mémoire du périphérique sélectionné peut être effacée avec la touche droite de la souris. L'activation du capteur de sabotage (TMP) a la plus haute priorité lors de l'enregistrement des événements dans la mémoire.

**Statut** - indique le statut effectif du périphérique. OK = tout est en ordre ; TMP = sabotage ; ACT = entrée d'alarme activée, ERR = erreur ; ?? = le périphérique ne répond pas ; Alimentation du réseau = panne de l'alimentation (ou batterie complètement déchargée) ; En cours de rechargement = rechargement de la batterie de secours dans le périphérique ou la centrale ; Batterie = batterie déchargée ou déconnectée dans la centrale ; BOOT - mise à jour du périphérique en cours ou échec de la mise à jour (réitérer la mise à jour). En pointant le curseur de la souris sur l'option STATUT du périphérique correspondant, les données détaillées s'affichent.

**Statut / tension de la batterie\*** - si le périphérique contient une batterie, son état s'affiche. Pour la centrale (position 0), la tension de la batterie de secours s'affiche. Si le périphérique sans fil ne contient pas de données sur la tension, la communication du périphérique n'a pas encore eu lieu - activer sa transmission (par ex. au moyen du capteur de sabotage ou dans F-Link, cliquer sur la touche Rafraîchir) ou attendre que la transmission automatique se produise. Si les claviers sans fil sont alimentés par une source d'alimentation externe, la mention « Alimenté par une source externe » est indiquée. Code couleur du statut de la batterie : 10% rouge, 20% jaune, 30% et plus vert.

**Tension / perte\*** - affichage sur la position (0) de la centrale de la tension aux bornes de la centrale et du courant alimentant les périphériques du BUS à partir de la centrale. Pour les périphériques du BUS, la chute de tension de la ligne par rapport à la centrale est affichée. La perte ne doit pas être supérieure à 2 V ; sinon, le problème doit être résolu (par ex. en ajoutant un amplificateur de BUS).

**Niveau du signal RF\*** - indique la qualité du signal par lequel la centrale communique en mode GSM en cas de connexion d'un transmetteur GSM supplémentaire ou d'un périphérique sans fil RF. La valeur doit être d'au moins 50%. Si l'indication est absente, le périphérique n'a pas encore communiqué - activer sa transmission (par ex. au moyen du capteur de sabotage) ou attendre que la transmission automatique se produise. La valeur sur la ligne de la centrale correspond à la force du signal du réseau GSM (pour l'interférence entre les modules radio et le module GSM, voir aussi le chapitre 6.1 Installation du module radio JA-111R).

Code couleur du signal GSM : 0-30% rouge, 40-50% jaune et 50% et plus, vert.

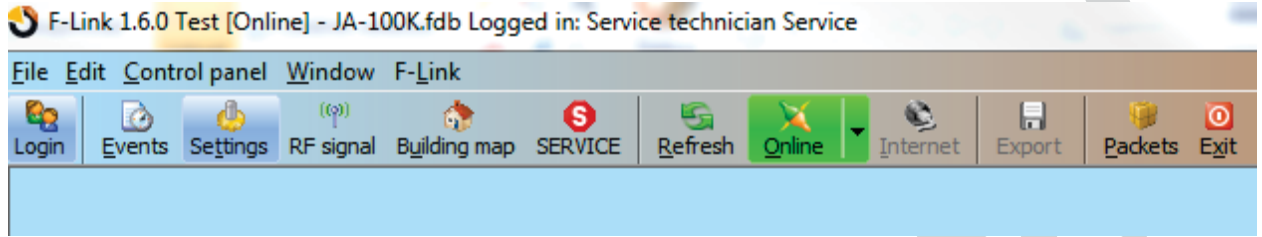
Code couleur du signal RF : 10% rouge, 20% jaune, 30% et plus vert.

**Canal\*** - informe sur le BUS utilisé par le périphérique pour communiquer. Deux voies sont distinguées : Sortie BUS et connecteur RJ conçu pour le module radio JA-11xR. Il existe une colonne spéciale intitulée Canal qui affiche la communication en cours des périphériques bidirectionnels.

# 11 Autres options F-Link

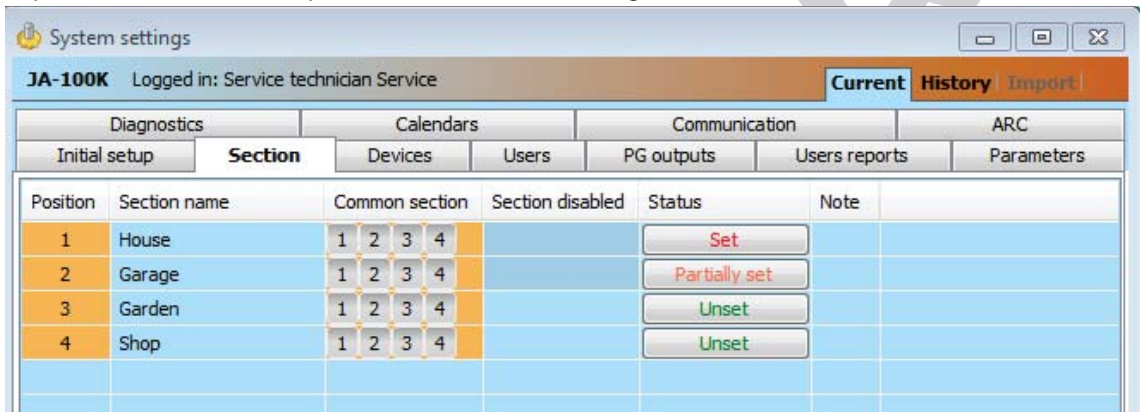
La version F-Link est toujours indiquée dans la barre supérieure derrière le nom.

La barre d'outils propose un accès rapide aux éléments souvent utilisés tels que la touche pour les changements de mode, les événements du système, les paramètres, le signal RF des modules radio, les paramètres d'exportation ou l'accès local et distant à la centrale.

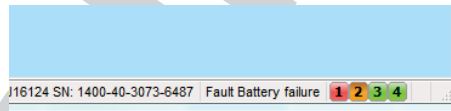


## 11.1 Commande du système par F-Link

Des sections individuelles dans le logiciel F-Link peuvent être commandées localement ou à distance de deux façons. La première consiste à cliquer sur la touche dans l'onglet Section, colonne Statut.



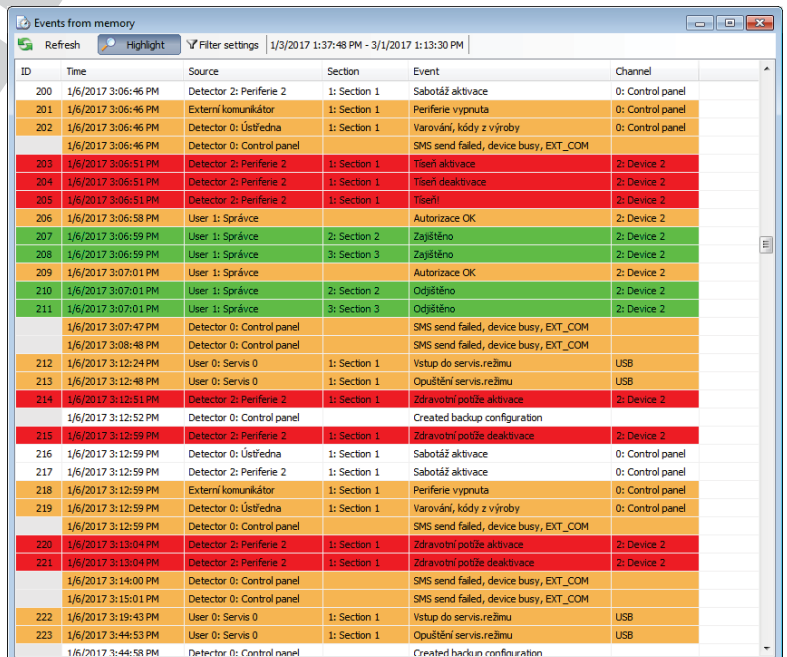
La deuxième consiste à cliquer sur les icônes représentant le statut du système sur la barre d'outils inférieure ; l'autorisation de l'utilisateur est enregistrée dans l'historique du système en fonction du code actuel utilisé pour se connecter au logiciel F-Link.



## 11.2 Historique événementiel :

Les événements de l'historique sont accessibles dans F-Link en appuyant sur la touche Événements et en sélectionnant « Historique événementiel ». Dans la mémoire de la centrale (carte microSD), jusqu'à plusieurs millions d'enregistrements peuvent être stockés avec un numéro d'ordre, la date et l'heure exactes et la source de l'évènement.

**Évènements à partir de la mémoire de la centrale** (également disponible après avoir appuyé sur F8) - des événements d'une taille d'env. 100 kB (à partir de la carte microSD) sont chargés. Si la plage de chargement est insuffisante, il est possible de sélectionner à plusieurs reprises les options Charger / Suivant 100(500)KB ou Tout. Avertissement : si la sélection Charger / Tout est choisie dans une centrale avec un temps plus long d'exploitation, le chargement peut prendre quelques minutes. L'historique n'enregistre Centrale du système de sécurité JA-100K



pas les événements qui se produisent lors de la configuration de service (seules l'ouverture et la fermeture du mode Service sont enregistrées). Les événements chargés peuvent être enregistrés dans un fichier dans le menu Fichier en utilisant l'option Export (Maj+Ctrl+S), sous plusieurs formats (FDE, PDF, TXT, CSV, XML, HTML ou HTM). Le suffixe FDE permet à F-Link de télécharger les événements à nouveau.

**Évènements en ligne** (disponible également après avoir appuyé sur F7) - tous les événements dans l'historique des événements qui se produisent après l'activation de cette option, y compris les événements au cours du paramétrage de service, sont enregistrés dans un tableau temporaire.

**Signaux en ligne** (également disponible après avoir appuyé sur F6) - tous les signaux enregistrés par le BUS (par ex. l'activation et la désactivation des capteurs) sont enregistrés dans un tableau temporaire.

**Évènements à partir d'un fichier** - les événements de l'historique événementiel enregistrés dans le format de fichier de la base de données FDE peuvent être ouverts (voir Évènements à partir de la mémoire de la centrale).

**Rafraîchir** - permet de charger un plus grand nombre d'évènements plus importants de l'historique, de 100, 500 kB (100 kB pour environ 1200 événements) ou l'ensemble.


**Surbrillance** - la couleur de la surbrillance permet de distinguer les types d'évènements (alarme - rouge, commande - vert, erreur - orange, sabotage - bleu, neutre - bleu clair, automatisation ou transmissions - gris, etc.).

**Paramètres du filtre** - le filtre permet d'obtenir uniquement les informations souhaitées en fonction du temps, par type d'évènement, sections, utilisateurs, périphériques ou sorties PG d'une manière très détaillée. Les filtres peuvent être combinés pour augmenter l'efficacité de recherche dans l'historique.

## 11.3 Paramétrage du système

Cette fenêtre permet de définir le comportement du système, de tous les périphériques, des sections, des utilisateurs, des sorties PG, des transmetteurs et des transmissions à la télésurveillance ; elle est disponible en appuyant sur la touche Paramètres dans le menu supérieur de base.

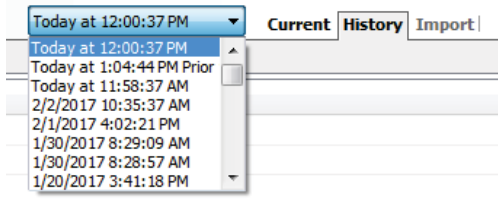
	Name	Type	Section	Reaction	Internal	PG activation	Intern...	Supervision	Alar...	Disable	Status
0	Control panel	JA-101K	1: Groud floor				Enter				TMP
1	Radio module	JA-110R	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
2	LCD keypad	JA-114E	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
3	Main door	JA-110M	1: Groud floor	Delayed zone A alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
4	Kitchen window	JA-110M	1: Groud floor	Instant zone alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
5	Garage door	JA-111M	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		ACT
6	Hall	JA-110P	1: Groud floor	Next delay zone alarm	<input checked="" type="checkbox"/>	2: Light hall	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
7	Garage PIR	JA-120PW	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	3: Light garage	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
8	Indoor siren	JA-110A	1: Groud floor	Siren mute			Enter	<input checked="" type="checkbox"/>			OK
9	Balcony door	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			ACT
10	Balcony window	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			OK
11	Living room	JA-151P	2: First floor	Instant zone alarm	<input checked="" type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>			TMP
12	Interface	JA-121T	1: Groud floor				Enter	<input type="checkbox"/>			OK
13	Remote control	JA-182J	4: Fully set	Set		No	Enter	<input type="checkbox"/>			
14	Device 14	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
15	Device 15	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
16	Device 16	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		

1. La fenêtre Paramétrage du système s'ouvre et se ferme avec la touche **Paramétrage**  en haut dans la barre d'outils.
2. Il est possible de basculer dans la fenêtre entre les **onglets** suivants : **Sections, Périphériques, Utilisateurs, Sorties PG, Paramètres, ...**
3. La fenêtre affiche le **paramétrage actuel de la centrale** chargé à l'ouverture du logiciel F-Link (désigné SW). La touche **Rafraîchir** dans la barre d'outils supérieure peut être utilisée pour charger le contenu actuel de la centrale à tout moment.
4. Pour consulter les **paramétrages précédents de la centrale**, utiliser l'**onglet Historique** en haut à droite. L'historique ne peut pas être modifié, mais il est possible de le sauvegarder dans la centrale (au



cas où il est nécessaire de revenir à un paramétrage précédent). Les 100 paramètres précédents sont écrasés dans l'historique (réorganisés par date et heure) ainsi que toutes les modifications de réglage.


- Il est possible **d'importer les paramètres** d'une autre installation vers le système, par ex. après avoir remplacé une centrale dépassée par une nouvelle ou en utilisant un modèle par défaut. Si la centrale est remplacée par une nouvelle, après la connexion, une toute nouvelle base de données sera créée dans l'ordinateur. Pour importer les paramètres d'une autre base, dans le menu supérieur du menu principal, sélectionner **Fichier / Importer** et sélectionner le fichier à partir duquel il faut importer les paramètres. Après cette sélection, la touche **Importer** dans l'onglet **Paramètres du système** apparaîtra.

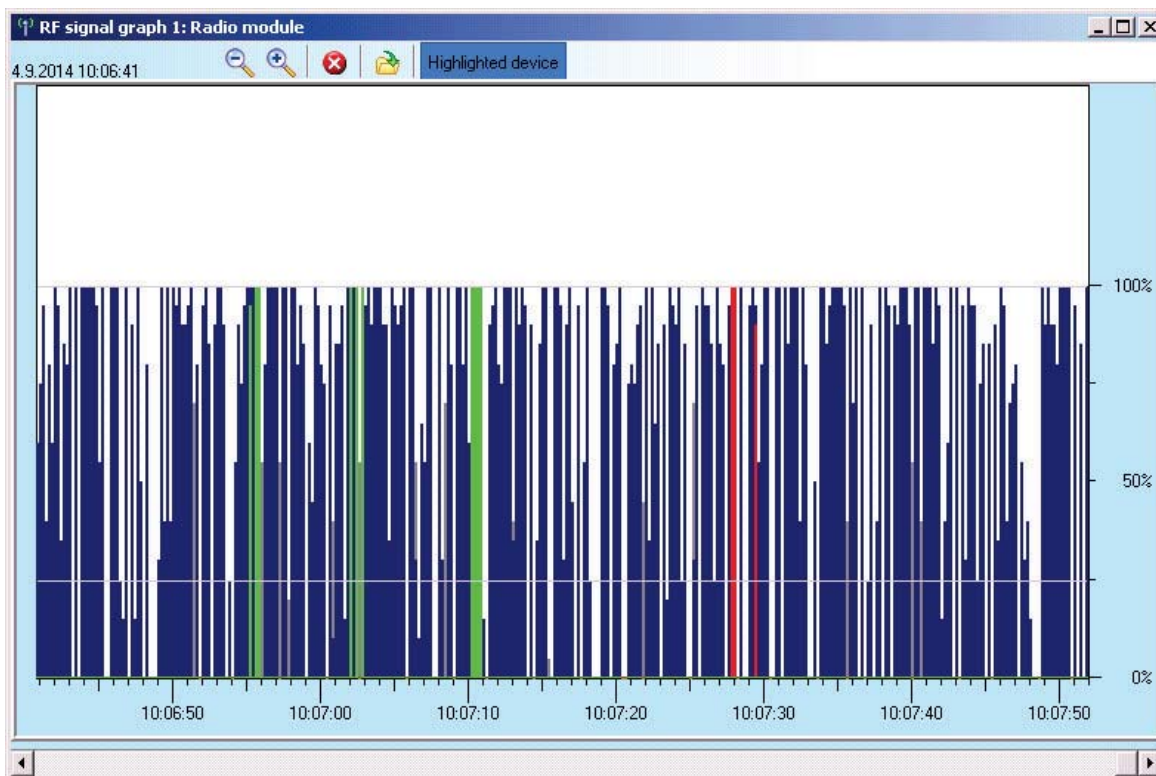


- Si un paramètre est modifié, il sera indiqué avec un texte en bleu** (le nom de l'onglet prendra de la même manière la couleur bleue). L'indication bleue disparaîtra dès que les modifications seront enregistrées.
- Il est possible de **sauvegarder les paramètres** en utilisant la touche **Sauvegarder** (en bas à droite). Si les paramètres sont enregistrés dans la centrale pour la première fois, le logiciel demandera à **saisir le nom du fichier**. Dans l'ordinateur, un fichier avec l'extension \*FDB sera créé là où l'historique des paramètres est progressivement sauvegardé (chaque fois que les paramètres sont enregistrés dans la centrale). Si les modifications ne doivent pas être enregistrées, cliquer sur la touche **Annuler** et au moment de la confirmation, sélectionner **Ignorer**. Les paramètres peuvent être modifiés dans plusieurs onglets, il est ensuite possible d'enregistrer toutes les modifications.
- La touche **Inscrire l'élément non inscrit** (barre de menu inférieure dans l'onglet Périphériques) ouvrira une boîte de dialogue pour l'inscription collective (sans possibilité de sélectionner les positions) des périphériques qui sont connectés au BUS et n'ont pas été connectés vers le système d'une autre façon. Voir le chapitre 8.4.1 Inscription et effacement des périphériques.
- La touche **Envoyer le signal d'inscription** (onglet périphériques et sorties PG) permettra l'envoi du code d'inscription de la centrale pour les périphériques sans fil, par ex., les modules de sortie sans fil.
- Le réglage de tous les paramètres n'est possible qu'en mode Service** (le système n'est pas en mode de paramétrage actif.) Le mode Service est activé et désactivé avec la touche **Service** dans la barre d'outils supérieure.
- Certains paramètres peuvent être modifiés pendant le fonctionnement.** Par conséquent, l'onglet Paramétrage peut être ouvert sans entrer en mode Service. Toutefois, seules les options disponibles peuvent être paramétrées.
- Le logiciel contient des info-bulles** - après avoir placé le curseur de la souris sur un élément, la description textuelle s'affiche. Les info-bulles peuvent être désactivées dans le menu déroulant de F-Link.

## 11.4 Signal RF

Fenêtre de représentation graphique de l'intensité d'interférence de la bande radio avec possibilité de sélectionner des modules radio utilisés. La présence de signaux dans la bande est indiquée en bleu. La couleur rouge identifie les signaux de communication de l'ensemble du système (périphériques inscrits) et le vert est utilisé pour afficher le périphérique sélectionné dans la liste de l'élément **Périphérique en surbrillance** (voir la figure). Le registre relatif aux interférences de surveillance (lorsque la fenêtre de signal RF est ouverte) peut

être exporté à partir du menu principal vers un fichier doté de l'extension FDR et la touche  peut être utilisée pour l'importer de nouveau aux fins de visualisation.



## 11.5 Service



Modification du mode de la centrale entre le statut Désarmé (en cas de changement de paramétrage pouvant être réalisé dans tous les onglets sauf l'onglet Paramétrage) et le mode Service (les modifications peuvent être réalisées dans l'onglet Périphériques, y compris l'inscription, les modifications de paramétrage interne et la suppression des périphériques).

## 11.6 Rafraîchir



Mettre à jour les paramètres internes des périphériques après une modification matérielle.

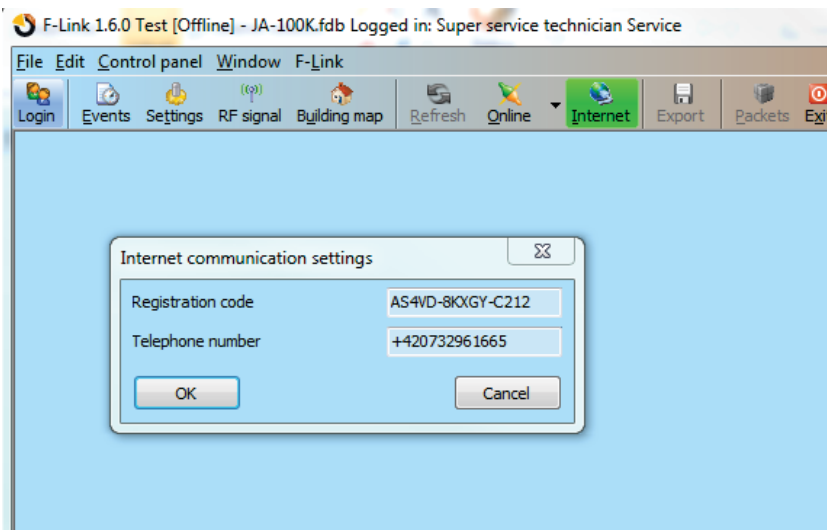
## 11.7 Mode en ligne



Connexion ou déconnexion de F-Link à partir de la centrale à l'aide d'un câble USB. Après la connexion, le programme trouvera automatiquement le port de la centrale utilisé pour la communication.

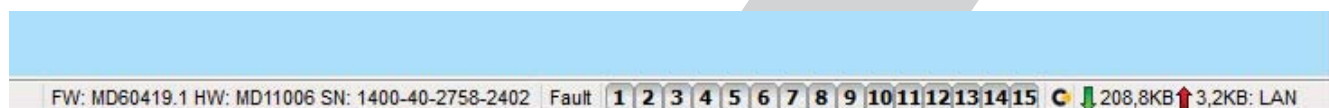
## 11.8 Internet

Connexion ou déconnexion à distance de F-Link à partir de la centrale via Internet. La condition préalable à l'établissement de la connexion est un code d'enregistrement correctement saisi (il est automatiquement pré-saisi de la base de données qui a été utilisée pour programmer la centrale), le numéro de téléphone de la carte SIM dans la centrale le cas échéant (également pré-saisi à partir des informations relatives à l'installation) et un ordinateur connecté à Internet. L'accès à distance peut être désactivé dans l'onglet Communication / Type de communication = Sans communication à distance.



Après avoir cliqué sur la touche Internet, une boîte de dialogue avec des données pré-saisies s'affiche. Si la connexion s'effectue à partir d'une nouvelle base de données « vide », le code d'enregistrement et le numéro de téléphone devront être ajoutés. Lorsqu'un transmetteur LAN est utilisé et que la communication Jablotron est activée, le numéro de téléphone ne peut pas être complété (le champ doit rester vide). L'établissement de la connexion ne prend que quelques secondes, mais le téléchargement de la configuration dépend de la taille du système et il peut souvent prendre de 1 à 2 minutes.

**Remarque :** les informations relatives à la façon d'établir la connexion GPRS / LAN et la quantité envoyée et reçue de données sont affichées dans le coin en bas à droite.

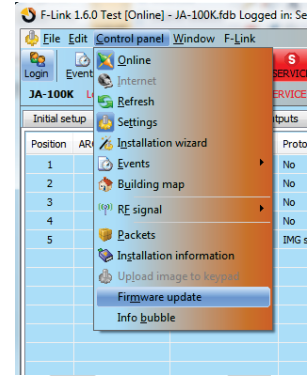


## 11.9 Informations relatives à l'installation

La fenêtre contient des éléments pour la société d'installation permettant d'enregistrer les informations de contact importantes sur le propriétaire du système, l'ensemble du système et, éventuellement, un document externe lié au site (offre, enregistrement d'acceptation, facture, etc.). Sur un chantier, le technicien d'installation peut saisir dans les remarques les renseignements obtenus lors du montage pouvant être utiles, par ex. en cas d'extension du système.

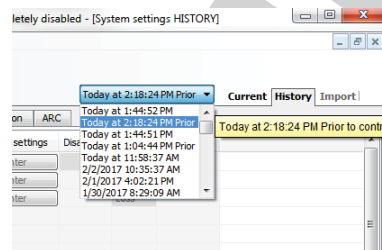
## 11.10 Mise à jour du micrologiciel

La mise à jour du micrologiciel permet de modifier le comportement des périphériques pouvant être mis à jour (centrale, modules radio, claviers, détecteurs, etc.) avec le micrologiciel que le fabricant publie officiellement sur le serveur Jablotron. Les téléchargements F-Link depuis le serveur Jablotron se font automatiquement (après une requête) si, dans le menu F-Link, l'élément Mises à jour automatiques est activé (réglage par défaut). Si l'élément n'est pas activé, F-Link pourra trouver manuellement le chemin des fichiers PFE dans l'ordinateur avant la mise à jour. De plus amples informations dans le chapitre 13 Mise à jour du micrologiciel.



## 11.11 Historique des configurations

La centrale enregistre les paramètres de tous les périphériques avec des modifications de leur programmation sur la carte SD. Elle enregistre également l'événement « Sauvegarde de configuration créée » dans l'historique avec les informations sur le nom du fichier. Cela comprend la configuration avant l'exécution de la modification pour permettre la récupération de la configuration précédente, pour la visualisation et la vérification de la date de cette modification. Pour visualiser les modifications de configuration enregistrées, ouvrir l'élément Événements à partir de la mémoire de la centrale et rechercher les événements de modification de configuration en fonction de la date et de l'heure ; aux fins de comparaison avec la programmation du système actuelle, charger l'élément et regarder dans l'onglet « Historique » disponible à gauche dans le coin supérieur de la fenêtre « Paramètres du système ». Les modifications de configuration sont mises en évidence avec un lettrage en italique bleu. Il est possible à partir du fichier de sauvegarde d'accepter les modifications, et en cliquant sur la touche « Enregistrer », de les sauvegarder dans la centrale ou, après avoir visualisé les modifications, de revenir aux paramètres actuels en cliquant sur l'onglet « Actuel ». Toutes les modifications de configuration sont enregistrées dans le dossier appelé SAUVEGARDE dans le fichier CFGxxxxx.bak, comprenant un nombre conforme à l'ordre des modifications réalisées.



Le logiciel F-Link enregistre (3 à 10 dans la fenêtre Information d'installation) l'historique des paramètres dans sa propre base de données par ordre décroissant. Cet historique des configurations est utilisé par le programme dans les mises à jour du micrologiciel de la centrale puisqu'une modification provoque toujours une perte du paramétrage précédent, cet historique pouvant être utilisé pour le restaurer. La même option peut être utilisée en cas de réinitialisation de la centrale avec les paramètres par défaut, de remplacement de la carte SD, de changement de langue lorsque les textes sont supprimés, ce qui peut être restauré de cette façon ou tout simplement en cas de modification accidentelle d'un paramètre.

## 12 Réinitialisation de la centrale

Il n'est possible de restaurer les paramètres par défaut de la centrale que de la manière suivante si l'élément « Réinitialisation autorisée » est coché dans l'onglet Paramètres dans le logiciel F-Link. Si la réinitialisation n'est pas autorisée et le code de service est inconnu, Il n'est pas possible de réinitialiser la centrale et la carte de la centrale doit être envoyée au distributeur.

Procédure :

1. Mettre la centrale en mode Service (non obligatoire).
2. Ouvrir le capot de la centrale : La réinitialisation exige que le contact de sabotage soit actif. Si la centrale n'est pas en mode Service, une alarme d'incendie est déclenchée.
3. Débrancher le câble USB de la centrale.
4. Couper l'alimentation électrique (le plus facilement en libérant le fusible de l'alimentation) et débrancher la batterie.
5. Connecter les broches sur la carte de la centrale marquée RESET (en utilisant le cavalier inclus dans la livraison).

6. Connecter d'abord la batterie puis l'alimentation de la centrale et attendre. Les voyants de signalisation vert, jaune et rouge au niveau du cavalier s'allument (si seul le voyant de signalisation rouge reste allumé, l'option Paramètres / Réinitialisation autorisée n'est pas activée).
7. Attendre environ 5 sec. puis débrancher le cavalier.
8. Après 5 sec., tous les voyants de signalisation clignotent indiquant la confirmation de l'achèvement de la remise à zéro de la centrale. Un redémarrage de la tension de la centrale et des périphériques BUS sera ensuite réalisé.
9. La centrale a été de cette façon réinitialisée avec ses paramètres par défaut, y compris le choix de la langue. Toutefois, la réinitialisation de la centrale ne provoque pas la suppression de l'historique des événements enregistrés sur la carte mémoire SD. Si la réinitialisation n'a pas été exécutée correctement, la centrale gardera les paramètres d'origine sans modification.

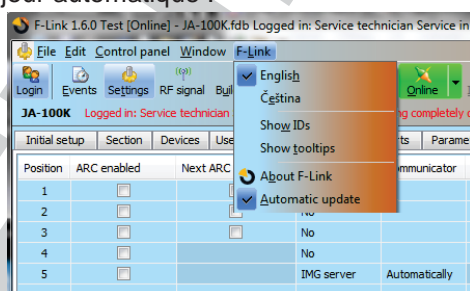
## 13 Mises à jour du micrologiciel

Les centrales et d'autres périphériques du système JABLOTRON 100 permettent la modification du micrologiciel. Le micrologiciel est généralement modifié pour améliorer les paramètres utiles de l'équipement et prendre en charge les nouveaux produits lancés.

### 13.1 Règles générales de mise à jour du micrologiciel (FW)

1. Une mise à jour du micrologiciel ne peut être réalisée qu'avec un ordinateur muni du logiciel **F-Link**, soit avec un accès local via un câble USB, soit à distance lorsque la possibilité de modifier le micrologiciel est limitée aux périphériques du BUS ainsi qu'aux périphériques sans fil bidirectionnels.
2. Le micrologiciel (FW) peut être modifié par un utilisateur avec l'autorisation de service.
3. La dernière version de F-Link est accessible pour les techniciens agréés après la connexion à MyCOMPANY (le logiciel F-Link contient aussi le micrologiciel). Si F-Link est déjà installé et que l'ordinateur a accès à Internet, F-Link vérifie alors automatiquement les mises à jour disponibles après le démarrage et en cas de version plus récente, il proposera son téléchargement avec la dernière version du micrologiciel.
4. Connecter un ordinateur à la centrale à l'aide d'un câble USB.
5. Démarrer le programme **F-Link** avec la centrale connectée.
6. Passer la centrale en mode **Service**.
7. Démarrer la **Mise à jour de la centrale / du micrologiciel**. Si l'élément **Mise à jour automatique** est autorisé dans le menu **F-Link** (paramétrage par défaut), la liste des périphériques pouvant être mis à jour s'affiche. Le fichier se trouve dans le répertoire **F-Link x.x.x / Micrologiciel** et son statut relatif à la mise à jour est uniquement garanti au moment du téléchargement de F-Link.

Emplacement du paramètre Mise à jour automatique :



### 13.2 Mises à jour du micrologiciel de la centrale et des périphériques connectés au BUS

1. Dans la fenêtre de sélection de la mise à jour du micrologiciel, les périphériques sans fil bidirectionnels et du BUS de la centrale pouvant être mis à jour sont affichés. F-Link sélectionne automatiquement les périphériques pour lesquels une mise à jour est nécessaire (ils ont un micrologiciel antérieur à celui présent dans le kit).
2. F-Link affiche également des périphériques sans fil qui peuvent être mis à jour sans fil (voir 13.3 Mises à jour du micrologiciel pour les périphériques sans fil) ou individuellement par un câble USB supplémentaire connecté à l'ordinateur.
3. Des informations plus détaillées sur les versions existante et nouvelle des périphériques individuels sont affichées dans l'info-bulle après avoir placé le curseur de la souris sur chacun des périphériques proposés.

4. Dans les cases de sélection, les périphériques pour lesquels le micrologiciel ne sera jamais disponible sont vérifiés, il est recommandé de les laisser cochées. Certains éléments peuvent être obligatoires et indisponibles (grisés) pour l'annulation de la mise à jour.
5. Si la mise à jour de la centrale est cochée, la possibilité de conserver le menu vocal modifié de l'utilisateur est affichée (en cas de désactivation, l'enregistrement par défaut du menu vocal sera restauré).
6. Cliquer sur OK pour lancer la mise à jour du micrologiciel de tous les périphériques sélectionnés. Toutes les modifications seront exécutées en quelques minutes (en fonction du nombre de périphériques). Enfin, la centrale redémarrera le système.
7. Après un changement de micrologiciel, une partie du code d'enregistrement peut être modifiée. Son changement n'aura aucun impact sur la possibilité d'accès à distance (utilisation de F-Link) ou la communication éventuelle de la centrale avec le service JABLOTRON Cloud et le serveur [img.jablotron.com](http://img.jablotron.com).
8. Si au cours de la mise à jour de la centrale, F-Link trouve des fichiers endommagés dans la carte SD, il la formatera et après l'achèvement de la mise à jour, il proposera de réimporter les paramètres d'origine.
9. Effectuer une vérification conformément à la description dans le chapitre 13.4 Contrôle après une vérification du micrologiciel.

### 13.3 Mises à jour du micrologiciel pour les périphériques sans fil

La façon la plus pratique de mettre à jour le micrologiciel pour les périphériques sans fil sélectionnés se trouve sur le réseau radio du système sans nécessité d'une connexion câblée. Si une mise à jour sans fil de n'importe quel périphérique est impossible (par exemple en raison des conditions radio locales réelles), elle peut être réalisée avec un câble USB.

#### Mise à jour sans fil à l'aide du module radio :

1. Démarrer le programme F-Link avec la centrale connectée.
2. Ouvrir le menu dans le **logiciel F-Link : Centrale** → **Mise à jour du micrologiciel**
3. Le logiciel propose un tableau avec des périphériques inscrits pouvant être mis à jour, vérifier si tous les périphériques sans fil requis sont sélectionnés (une mise à jour des périphériques grisés peut être obligatoire et sélectionnée automatiquement pour des raisons de compatibilité).
4. Des informations plus détaillées sur les versions existante et nouvelle des périphériques individuels sont affichées dans l'info-bulle après avoir placé le curseur de la souris sur chacun des périphériques proposés.
5. En appuyant sur la touche OK, tous les périphériques sélectionnés seront mis à jour.
6. Une fois la mise à jour réalisée, réaliser la vérification conformément à la description dans le chapitre 13.4 Contrôle après une vérification du micrologiciel.

#### Mettre à jour à l'aide d'un câble USB :

1. Ouvrir le périphérique sans fil pouvant être mis à jour (non lié à AC-160xx).
2. Si des piles sont incluses, les retirer et si le périphérique est alimenté par un adaptateur externe, le débrancher de la même façon (AC-160xx uniquement).
3. Lancer F-Link, ouvrir la base de données et connecter un câble USB à l'ordinateur (miniUSB ou microUSB conformément au périphérique utilisé).  
**Avertissement** : les câbles USB ne sont pas inclus avec les périphériques individuels. Nous recommandons d'utiliser une connexion USB directe à l'ordinateur, une connexion avec un répartiteur USB pouvant réduire la fiabilité.
4. Les mises à jour du micrologiciel des périphériques sans fil doivent être réalisées progressivement et ne peuvent être faites en même temps avec plusieurs câbles USB.
5. Dans le périphérique sans fil devant être mis à jour, ouvrir le mode relatif au chargement d'un nouveau micrologiciel. Suivre les instructions des manuels respectifs.
6. Puis continuer de manière similaire à la mise à jour du système avec le **logiciel F-Link : Centrale** → **Mise à jour du micrologiciel**.
7. Dans le tableau de sélection des périphériques, sélectionner l'élément USB (généralement en première position).
8. Des informations plus détaillées sur les versions existante et nouvelle des périphériques individuels sont affichées dans l'info-bulle après avoir placé le curseur de la souris sur chacun des périphériques proposés.
9. En appuyant sur la touche OK, tous les périphériques seront mis à jour.
10. Une fois la mise à jour terminée, débrancher le câble USB, insérer les batteries ou brancher l'alimentation électrique et remonter le module.

11. Réaliser un contrôle conformément à la description du chapitre 13.4 Contrôle après une vérification du micrologiciel.
12. Passer à la mise à jour du périphérique sans fil suivant.

## 13.4 Contrôle après une vérification du micrologiciel

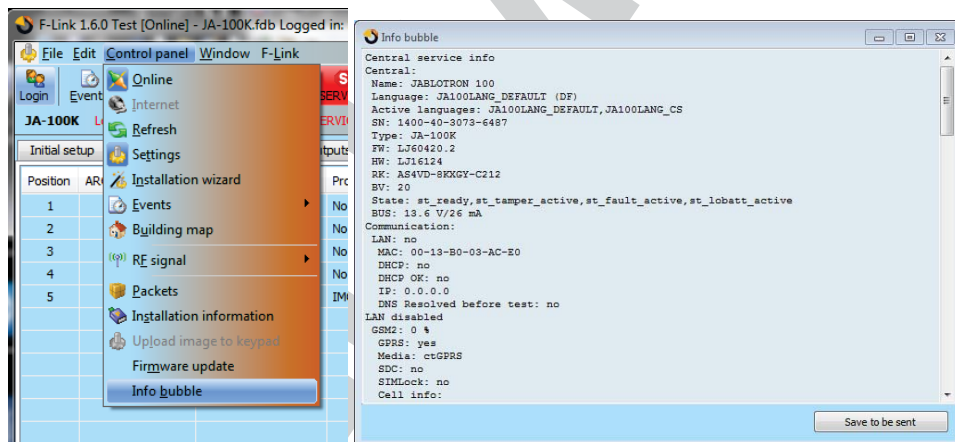
1. Vérifier les paramètres de tous les périphériques modifiés et de la centrale dans **F-Link, Périphériques / Paramètres internes**. En fonction de l'envergure des modifications mises en œuvre au cours de la mise à jour, la configuration précédente peut être maintenue ou réinitialisée avec les valeurs de production par défaut. Si la réinitialisation avec les valeurs par défaut a été réalisée, il est possible d'utiliser la touche Importer dans les paramètres internes des périphériques individuels pour sélectionner les configurations précédentes.
2. Si de nouveaux éléments ont été ajoutés au cours de la mise à jour, ils seront dotés des paramètres par défaut. Les vérifier et les adapter aux réglages nécessaires à l'installation.
3. Vérifier les paramètres et tester l'activité des périphériques mis à jour.

## 13.5 Fenêtre d'informations

Elle s'ouvre à partir du menu principal **Centrale / Fenêtre d'informations**. Lors de l'ouverture de la fenêtre d'informations, la centrale interroge tous les périphériques connectés et les périphériques sans fil quant à leur statut effectif.

La fenêtre d'informations propose une vue d'ensemble des données techniques de l'ensemble du système, y compris la centrale (numéro de série, code d'enregistrement, versions du micrologiciel et matérielle, tension et courant du BUS, plage de paramétrage des : périphériques, sections, sorties PG), les transmetteurs utilisés (GSM : numéro de téléphone, signal du numéro BTS ou PSTN : statut de la ligne téléphonique), LAN : statut , MAC, IP, ainsi que tous les périphériques BUS et sans fil (uni et bidirectionnels) : type de périphérique, identification des versions du micrologiciel et matérielle des périphériques individuels et leur statut. Elle est disponible dans tous les statuts du système (armé / désarmé / service).

Ces données sont par ex. nécessaires pour la communication avec le conseiller technique à qui est destinée la touche « Enregistrer pour envoi » située dans le coin en bas à droite. Le fichier est un fichier compressé ZIP et contient les données numériques de l'installation, y compris une partie de l'historique évènementiel (100 kB), mais il ne contient pas de données sensibles comme les numéros de téléphone des utilisateurs ou leurs codes d'accès ou d'autres données confidentielles.

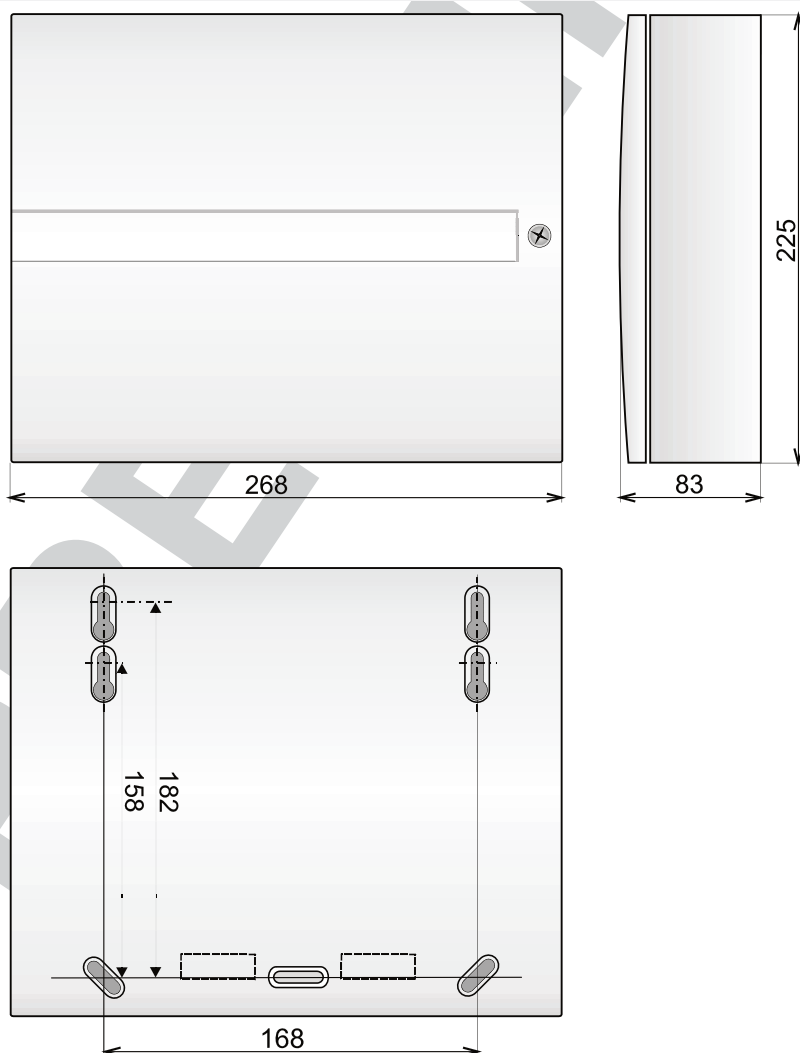


## 14 Informations supplémentaires

### 14.1 Tableau récapitulatif de la consommation en courant des périphériques BUS

Périphérique	Consommation en mode secours (mA)	Consommation pour la sélection du câble	Remarque
JA-110E - Clavier LCD avec lecteur RFID	15	110	
JA-11xR - Module radio de connexion sans fil	25	25	
JA-110A - Sirène intérieure	5	30	30 mA pendant l'alarme
JA-111A - Sirène extérieure	5	50	Lors d'une coupure AC sans chargement de la batterie, sinon 550 mA en fonction de la charge de la batterie
JA-190X - Module du transmetteur téléphonique	15	30	
JA-190Y - Transmetteur GSM	25	220	Courant maximal de communication avec le fournisseur

### 14.2 Dimensions des centrales





## 15 Prise en charge du système par l'utilisateur

Lorsque l'installation du système de sécurité est terminée, il est généralement recommandé de créer la documentation (rapport sur la remise du système, LOG du système de sécurité, etc.) comprenant toutes les informations sur le nombre et l'emplacement des périphériques tels que les détecteurs, les sirènes, les claviers, leurs touches fonctionnelles et la manière dont ils ont été configurés. Les utilisateurs du système devraient être formés à l'utilisation du système conformément aux points suivants :

1. Commande à partir du clavier du système. Armement et désarmement des sections (à l'aide des touches fonctionnelles ou du menu du clavier).
2. S'assurer que la temporisation de sortie / entrée est suffisante et valable également pour les portes de garage ou d'autres voies d'accès.
3. Expliquer ce qu'est une autorisation, à quoi elle sert et les options comme les codes, les badges RFID, etc.
4. Armement partiel au domicile. Différence dans la signalisation entre les armements partiels et complets.
5. Commande domotique en utilisant des touches fonctionnelles et d'autres fonctions (détresse, incendie, problèmes de santé).
6. Déclencher une alarme lorsque le système est armé, y compris les sirènes, l'appel de test d'alarme.
7. Expliquer la différence entre l'annulation d'alarme par autorisation et le désarmement d'une section.
8. Commande de section (à distance via le menu vocal à l'aide du clavier du téléphone portable).
9. Commande de section et domotique (sorties PG) par SMS.
10. Commande par l'utilisation de l'application Internet ou mobile à partir de tablettes, de smartphones ou d'un site Internet.

Ne pas oublier de proposer une vérification annuelle du système au client. Il est très utile de vérifier périodiquement les fonctions du système, non seulement de la centrale, mais aussi de tous les périphériques installés. Le technicien crée un rapport sur la réalisation de la vérification annuelle qui peut servir pour la compagnie d'assurance.



## 16 Caractéristiques techniques

Paramètre	JA-100K
Type d'installation	Installation fixe
Tension nominale de la centrale / fréquence / fusible	~ 230 V / 50 Hz, fusible T200 mA 250 V 5 x 20 mm ~ 115 V / 60 Hz, fusible T400 mA 250 V 5 x 20 mm
Plage de tension AC d'exploitation	~ 195 V ÷ 250 V ~ 110 V ÷ 120 V
Alimentation / courant électrique	Max. 23 VA / 0,1 A
Classe de protection	II.
Batterie de secours	12 V ; 2,6 Ah max. (plomb-acide)
Faible tension de la batterie (indication de défaillance)	≤ 11 V
Durée maximale de recharge de la batterie	48 ÷ 72 h
Tension du BUS / Ondulation de tension max. (rouge-noir)	12.0 ÷ 13.8 V <sub>DC</sub> / ± 100 mV
Consommation continue max. à partir de la centrale BUS +RJ	400 mA en permanence (1000 mA pendant 5 minutes)
@ 12 heures de secours (2,6 Ah)	LAN désactivé : 125 mA - consommation des modules JA-190X (Y) LAN activé : 85 mA - consommation des modules JA-190X (Y)
Nombre max. de sections	4
Nombre max. de périphériques	32
Nombre max. d'utilisateurs	33
Nombre max. de sorties PG	4
Connexion d'alarme	BUS Jablotron - connexion filaire dédiée Connexion sans fil (avec JA-111R) - connexion sans fil non spécifiée, protocole sans fil Jablotron
Classification du système d'alarme	Niveau de sécurité 2 / Classe environnementale II
@ Conformément aux normes	EN 50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN50131-10, EN 50136-1, EN 50136-2
@ Environnement	Intérieur, général
@ Température / humidité de service	-10°C à +40°C, humidité relative 75% sans condensation
@ Alimentation	Type A - alimentation primaire avec batterie de secours chargée
@ Historique évènementiel	Environ 7 millions d'évènements antérieurs, y compris la date et l'heure
@ Réaction du système à la perte de communication	Défaillance ou sabotage - conformément au profil prédéfini @ BUS - jusqu'à 10 sec. @ Communication sans fil - en 2 heures (rapport) @ Communication sans fil - 20 minutes, dans un système de blocage à configurer
@ Réaction à la saisie d'un code invalide	Après 10 saisies de code incorrectes, une alarme de sabotage est déclenchée et, conformément au profil sélectionné, il y a blocage de tous les périphériques de commande pendant 10 min.
@ Classification ATS	Classe ATS prises en charge : SP2 - SP 5, DP2 - DP3 SPT : Type Z Type d'opération : Transit LAN intégré : SP2 - SP5 (avec protocole IP) JA-190Y SP2 - SP5 (avec protocole IP) JA-190X SP2 (avec protocole d'identification de contact)

	LAN + JA-190Y DP2 - DP3 (avec protocole IP) LAN + JA-190X DP2 (avec protocole IP / CID)
@ Protocoles de transfert ATS	JABLO IP, SIA IP, ID de contact, JABLO SMS
@ Protection ATC contre la substitution et la protection des données	Protocole Jablotron : Cryptage AES propriétaire avec une clé minimale de 128 bits Protocole ANSI SIA DC-09.2012 avec cryptage AES 128 bits
Transmetteur LAN	Interface Ethernet CAT 5 (RJ-45)
Dimensions (mm)	268 x 225 x 83
Poids	1450 g
Paramètres de base du module JA-111R	868,1 MHz, <25 mW, GFSK <80 kHz
Émissions radio	ETSI EN 300 220-2 (module R)
EMC	EN 50130-4, EN 55022, ETSI EN 301 489-7, ETSI EN 301 489-3
Sécurité électrique	EN 60950-1
Conditions d'exploitation	ERC REC 70-03, ERC DEC (98) 20
Organisme de certification	TREZOR TEST



JABLOTRON ALARMS a.s. déclare par la présente que les centrales JA-100K sont conformes aux exigences de base et aux autres dispositions afférentes des directives n° 2014/53/UE, 2014/35/UE, 2014/30/UE et 2011/65/UE. L'original de la déclaration de conformité est disponible sur [www.jablotron.com](http://www.jablotron.com).



Remarque : Le produit, même s'il ne comprend aucune matière nocive, ne doit pas être jeté dans les ordures ménagères mais remis dans un lieu de récupération des déchets électroniques. Pour de plus amples informations, se rendre sur [www.jablotron.com](http://www.jablotron.com), section Support technique.