SYSTÈME HISEC

Contrôle d'Accès

18-006-06F

AVANT PROPOS

Cette notice a pour but de vous donner toutes les informations nécessaires à l'utilisation du Système Contrôle d'Accès HI SEC.

Dans le cadre d'une politique continuelle de recherche et de développement, les informations contenues dans ce document sont sujettes à modification sans préavis.

HI SEC International dégage toute responsabilité concernant le non-respect ou une mauvaise utilisation de cette notice ainsi que les erreurs ou omissions et leurs conséquences sur les installations.

Notice référence stock	: 18-006-05F
Créée-le	: 28/01/91
Dernière Révision	: 10/03/03

Toutes les marques et produits cités dans cette notice sont déposés:

MS-DOS® et WINDOWS® sont des marques déposées de MICROSOFT Corporation.

IBM® est une marque déposée de International Business Machines Corp.

Wiegand® est une marque déposée de Sensor Engineering Co.

TABLE DES MATIERES

1-Description Fonctionnelle

1 Description fonctionnelle

1.1 Description Générale

Le système de Contrôle d'Accès qui peut être utilisé en **Autonome**, dans une configuration **Multi-lecteurs** ou **Intégré** à un système d'intrusion HISEC. L'unité lecteur de badges HISEC sera la même dans ces différentes configurations.

La capacité totale du système dans ces configurations est la suivante:

Mono-BUS

¨ **Nombre max. de lecteurs en mode système Multilecteurs**	31
¨ **Nombre max. de Centrale Intrusion par système intégré**	1
¨ **Nombre max. de badges programmés actifs**	16000
¨ **Nombre max. de badges par système**	65500
¨ **Nombre max. d'événements dans l'historique Local**	2100 par Lecteur
¨ **Nombre max. d'alarmes dans l'historique Global**	100
¨ **Nombre max. de groupes de personnel**	250
¨ **Nombre max. de Zones d'anti-retour**	16
¨ **Nombre max. de programmes horaires hebdomadaires**	35
¨ **Nombre max. de périodes horaires par jour (par prog. Hebdo.)**	8
¨ **Nombre max. de périodes de congés**	25

Dans tous ces types de configurations, le système travaillera sans contrôleur commun, de ce fait, le lecteur individuel aura toutes les informations utiles à son fonctionnement et sa propre "intelligence".

Toutes les entrées/sorties pour les contacts de portes, bouton poussoir de sortie, gâche électrique etc. seront gérées par le bus S-ART du lecteur. Les S-ART seront connectés au lecteur par le contrôleur intégré à celui-ci. Un maximum de 15 S-ART pourra être connecté localement sur chaque lecteur.

Multi-BUS

¨ **Nombre max. de lecteurs en mode système Multilecteurs**	961
¨ **Nombre max. de Centrale Intrusion par système intégré**	31
¨ **Nombre max. de badges programmés actifs**	16000
¨ **Nombre max. de badges par système**	65500
¨ **Nombre max. d'événements dans l'historique Local**	2100 par Lecteur
¨ **Nombre max. d'alarmes dans l'historique Global**	100 par Bus
¨ **Nombre max. de groupes de personnel**	250 par Bus
¨ **Nombre max. de Zones d'anti-retour par Bus**	16
¨ **Nombre max. de Zones d'anti-retour (Totalité Site)**	465
¨ **Nombre max. de programmes horaires hebdomadaires**	35 par Bus
¨ **Nombre max. de périodes horaires par jour (par prog. hebdo.)**	8
¨ **Nombre max. de périodes de congés**	25 par BUS

Pour le raccordement en mode multi-Bus se reporter au Logiciel AIMS et documents associés.

Toute information détaillée concernant le système d'intrusion HISEC pourra être trouvée dans le "*MANUEL TECHNIQUE D'INTRUSION HISEC*".
Dans la présente notice, seules seront décrites de façon succincte les fonctions du lecteur de badges opérant avec la centrale intrusion HISEC.

1.1.2 Liste des Eléments constituant le Système

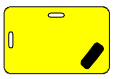
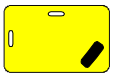
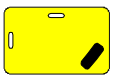
La totalité des éléments suivants (décrits dans ce manuel) est disponible aujourd'hui :

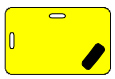
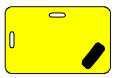
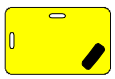
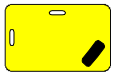
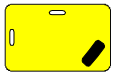
TYPE N°	DESCRIPTION
95T ACM 	Lecteur de Contrôle d'Accès & Terminal Intrusion avec lecteur magnétique incorporé, afficheur et clavier pour usage intérieur et extérieur. M
95T ACW 	Lecteur Contrôle d'Accès & Intrusion avec les mêmes fonctions que 95 T ACM mais avec tête de lecture Wiegand incorporée. W
95T ERC 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur incluant une sortie pour tête de lecture externe, fonctions identiques au 95 T ACM. M/W/P/ML/IR
95T ACP 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur avec tête de lecture proximité incorporée pour badges DEISTER. P (deister)
95T ACP-H 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur avec tête de lecture proximité incorporée pour badges HID. P (HID)
95T ACPM 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur avec tête de lecture proximité incorporée pour badges DEISTER et tête magnétique incorporée pour système double technologie. M/P (deister)
95T ACC 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur avec tête de lecture carte à puce incorporée pour badges HISEC (autre origine de badge, contacter HISEC). C
95T ACM-E 	Lecteur de Contrôle d'Accès & Terminal Intrusion avec lecteur magnétique intégré, afficheur et clavier. Pour usage intérieur uniquement Une version pour extérieur (IP 45), est disponible sur demande. M

TYPE N°	DESCRIPTION
95T ACM-L 	Lecteur **COMPACT** : Contrôleur d'accès avec tête de lecture magnétique intégrée et connexion pour un lecteur déporté. Sera aussi utilisé en fonction ERC dans le cas d'utilisation de têtes de lectures déportées ou de têtes de lectures non supportées en interne. M
95T ACP-L 	Lecteur **COMPACT** : Contrôleur d'accès avec tête de lecture proximité P
95T ACM-S 	Lecteur **STYLE** : Contrôleur d'accès avec tête de lecture magnétique intégrée et connexion pour une tête de lecture déportée. Sera aussi utilisé en fonction ERC dans le cas d'utilisation de tête de lectures déportées ou de têtes de lectures non supportées en interne. M
95T ACP-S 	Lecteur **STYLE** : Contrôleur d'accès avec tête de lecture proximité. P (deister)
95T DS 	Kit d'évolution d'un lecteur COMPACT en STYLE

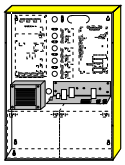
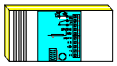
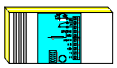
TYPE N°	DESCRIPTION
90T EMR-S 	Tête de lecture extérieure Magnétique incluant 2,5 m de câble blindé. M
90T RKP EWR 	Tête de lecture extérieure Wiegand incluant 2.5 m de câble blindé. W
95T EIRS 	Tête de lecture pour badges codes barres infrarouge incluant 2.5 m de câble blindé. IR

TYPE N°	DESCRIPTION
90T HC 	Badge Magnétique Haute Coercivité ISO piste 2
90T W 	Badge WIEGAND

TETES DE LECTURE DEISTER	
95T PRX5V 	Antenne 5 V avec interface incorporée. Lecture jusqu'à 12 cm. Se connecte directement sur un 95T ERC DEISTER
95T PRX5 	Antenne 12 V avec interface incorporée. Lecture jusqu'à 12 cm. Se connecte directement sur un 95T ERC DEISTER
95T AP5 	Coque de montage en saille pour PRX 5 et PRX 5V. DEISTER
95T PRX15 	Antenne 24V avec interface incorporée. Lecture jusqu'à 60 cm. Se connecte directement sur un 95T ERC. DEISTER
95T PRX15 EXT 	Antenne 24V avec interface incorporée pour montage en extérieur. Lecture jusqu'à 60 cm. Se connecte directement sur un 95T ERC. DEISTER
BADGES DEISTER	
95T PC 101 	Badge passif Proximité/Mains libres sans logo, non personnalisable, programmé (85x54x2,3mm) DEISTER
95T PC 110 	Badge passif Proximité/Mains libres sans logo, personnalisable par autocollant programmé(85x54x1,3mm) DEISTER
95T PC 111 	Badge passif Proximité/Mains libres avec sans logo, personnalisable par imprimante MAGICARD, programmé (85x54x1,3mm) DEISTER
95T PC 112 (FORMAT LIBRE) 	Badge double technologie passif Proximité/Mains libres format ISO avec possibilité de piste magnétique, sans logo, personnalisable par imprimante de badges, programmé (85x54x0,8mm) DEISTER
95T PC 114 (FORMAT STANDARD) 	Badge double technologie passif Proximité/Mains libres format ISO avec possibilité de piste magnétique, sans logo, personnalisable par imprimante de badges, programmé (85x54x0,8mm) DEISTER
95T PCK 105 	Badge Clé Proximité/Mains libres, sans logo, programmé DEISTER

TETES DE LECTURE HID	
99T HP 	**Antenne externe avec interface incorporée ProxPoint, lecture jusqu'à 6 cm.** Se connecte directement sur un 95T ERC P (HID)
99T HSP 	**Antenne externe avec interface incorporée MiniProx, lecture jusqu'à 9 cm.** Se connecte directement sur un 95T ERC P (HID)
99T HPP 	**Antenne externe avec interface incorporée ProxPro. Lecture jusqu'à 20 cm.** Se connecte directement sur un 95T ERC Pour usage intérieur et extérieur, 12V DC. P (HID)
99T HMP 	**Antenne externe avec interface incorporée MaxiPro, lecture jusqu'à 60 cm.** Se connecte directement sur un 95T ERC Pour usage intérieur et extérieur, 24V DC. P (HID)
BADGES HID	
99T HPC 	(ProxCard II) Badge passif Proximité haute résistance, non personnalisable. Programmé au format HISEC BFORM 04 (P)HID
95T HPC-ID 	(ProxCard II) Badge passif Proximité haute résistance, avec possibilité d'étiquette autocollante pour personnalisation. Utilisable avec étiquette 99T HDIL. Programmé au format HISEC BFORM 04 (P)HID
99T HDIL 	Etiquette autocollante pour badges HID 99T HDIL (P)HID
99T HPD 	(DuoProx) Badge double technologie passif Proximité/ format ISO avec piste magnétique. Personnalisable par imprimante de badges Portée réduite de 30% environ par rapport au 99T HPC. Programmé en format HISEC BFORM 04, piste magnétique non-encodée (P)HID
95T HPK 	Badge passif Proximité Clé. Portée réduite de 50% environ par rapport au 99T HPC. Programmé au format HISEC BFORM 04 (P)HID
99T HVIC 	Badge passif Proximité Véhicule. Programmé au format HISEC BFORM 04
95T HPC-S 	Badge Proximité de Maintenance pour Installateur
99T HPC-M 	Badge Proximité Maître

TYPE N°	DESCRIPTION
95T GPI COM 	Interface de communication RS 232 sur Bus RS 485 (pour HISEC Intrusion ou contrôle d'accès) avec les fonctions suivantes: Interface Imprimante RS 232 C Interface PC (AIMS & AICS) Interface Modem (RTC & X28) Interface Transmetteur SERIAL (SECOM)
95T GPI COM IP 	Interface de communication IP sur Bus RS 485 (pour HISEC Intrusion ou contrôle d'accès)
95T GPI BR 	Interface de connexion inter-bus RS 485 (pour HISEC Intrusion ou contrôle d'accès)
95T GPI DLC 	Interface Amplificateur de bus RS 485 (pour HISEC Intrusion ou contrôle d'accès)
95T GPI DLM/ BRM 	Interface Modem RS232 pour ligne spécialisée sur Bus RS 485 (pour HISEC Intrusion ou contrôle d'accès)
95T GPI DLM IP / BRM IP 	Interface IP pour liaison permanente sur Bus RS 485 (pour HISEC Intrusion ou contrôle d'accès)
90T GIB 	Carte opto-coupleurs utilisables sur toutes les anciennes interfaces GPI (sauf IP).

TYPE N°	DESCRIPTION
95T PS 	Alimentation 24 V 3 A (2,2 A disponibles) dans un coffret métallique avec emplacement disponible pour 2 Batteries 12 V 24 Ah, 3 S-Arts, 1 Interface GPI COM
90T S102 	S-Art pour contrôle de porte avec 2 entrées, 1 sortie relais pour : contact porte, bouton poussoir de sortie, gâche électrique.
90T S112 	S-Art pour contrôle de porte avec 2 entrées, 1 sortie relais pour : contact porte, bouton poussoir de sortie, gâche électrique.

95T CRP 	Capot métallique antivandalisme pour lecteurs 95T

1.2 Description du Système

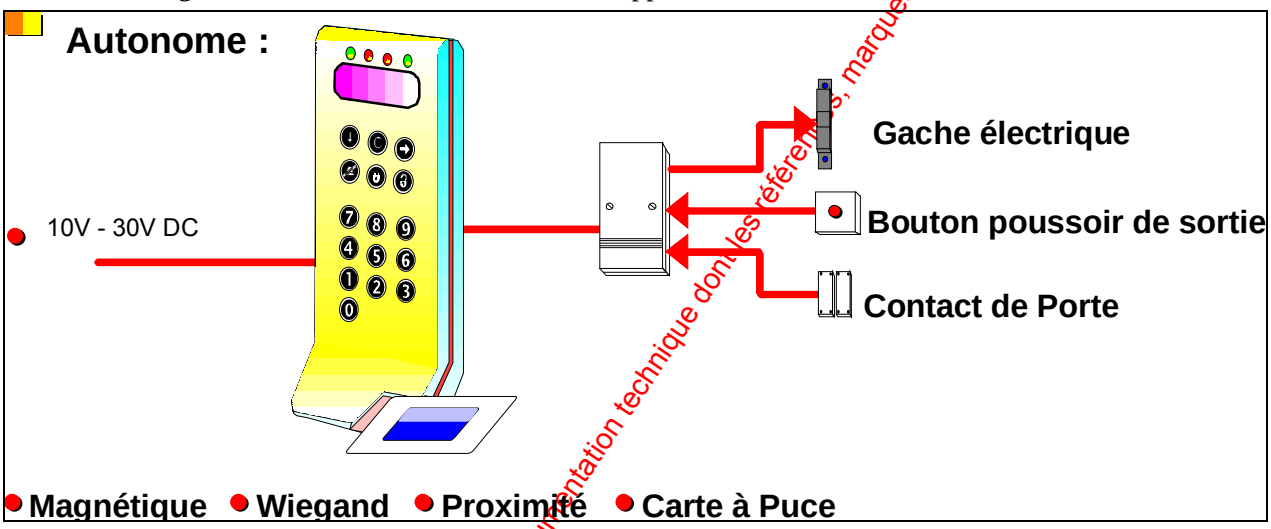
Le système de Contrôle d'Accès HISEC est construit autour d'un lecteur de badges, lequel comprend toute l'intelligence, la base de données etc. pour faire fonctionner le système. Le lecteur de badges peut être utilisé dans différentes configurations dépendantes de l'application souhaitée.

- Soit comme un lecteur **Autonome** gérant une seule porte.
- Soit comme un système **Multi-lecteurs** connectés entre eux par l'intermédiaire du bus multi-maîtres RS485.
- Soit comme une partie **Intégrée** au système d'intrusion HISEC où il est possible de réaliser à la fois des fonctions de Contrôle d'Accès et d'Intrusion.

Dans toutes ces applications, le lecteur intelligent sera la même unité.

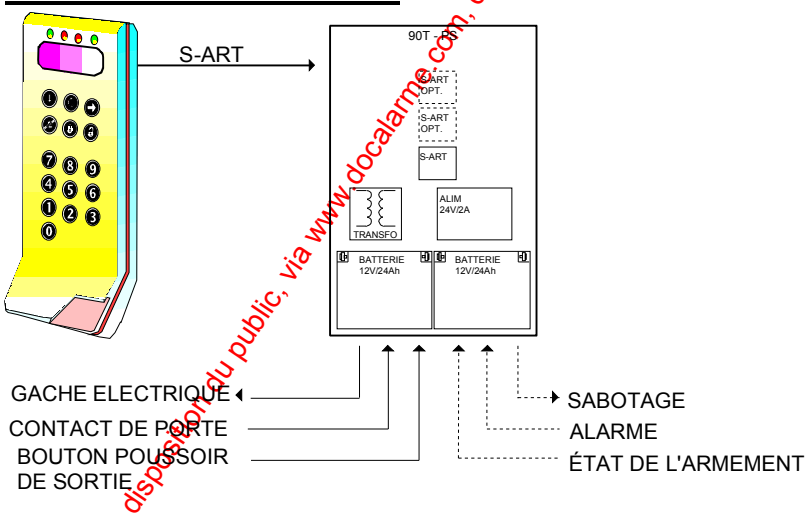
1.2.1 Système Autonome

Les deux configurations du lecteur HISEC dans des applications en mode Autonome sont les suivantes :



Nota: Ce mode ne permet pas de communiquer par le bus RS 485 et par conséquent il est impossible d'utiliser les périphériques de bus (interface imprimante, carte GPI).

Utilisation du coffret 90T-PS



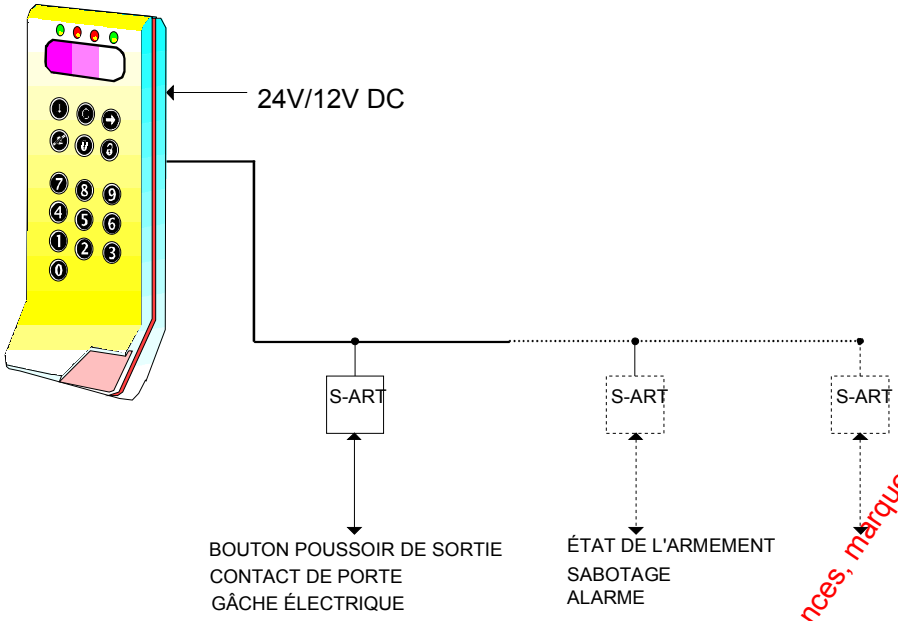
Le lecteur HISEC peut être installé en utilisant l'unité d'alimentation 95T-PS avec l'interface de porte incorporée comme représenté sur la figure ci-dessus.

L'unité 95T-PS comprend un coffret pour l'alimentation, la place pour deux batteries 24 Ah et une interface optionnelle pour imprimante et a l'avantage de pouvoir être installée à l'intérieur de la zone protégée, si nécessaire.

Un S-ART incorporé au chargeur permet de surveiller l'alimentation.

Un emplacement est prévu pour deux S-ART optionnels permettant par exemple de programmer des interfaces vers un système d'alarme "Non HISEC". Dans l'exemple, ci-dessus, le lecteur HISEC peut indiquer sur l'afficheur l'état de l'installation (armé ou désarmé) et l'indication d'alarme venant du système d'intrusion et envoyer au système d'intrusion un signal de sabotage. Cela peut être réalisé avec deux S-ART 90T-S102.

Utilisation d'une alimentation indépendante



Sur la figure ci-contre, l'interface de porte est réalisée au moyen d'un montage de S-ART externes. Ces S-ART sont connectés par l'intermédiaire du contrôleur de S-ART intégré. Une installation très simple peut être réalisée si les signaux de contrôle de la porte et le lecteur ne sont pas à la même place. Le nombre maximum de S-ART connectables directement au lecteur est de 15.

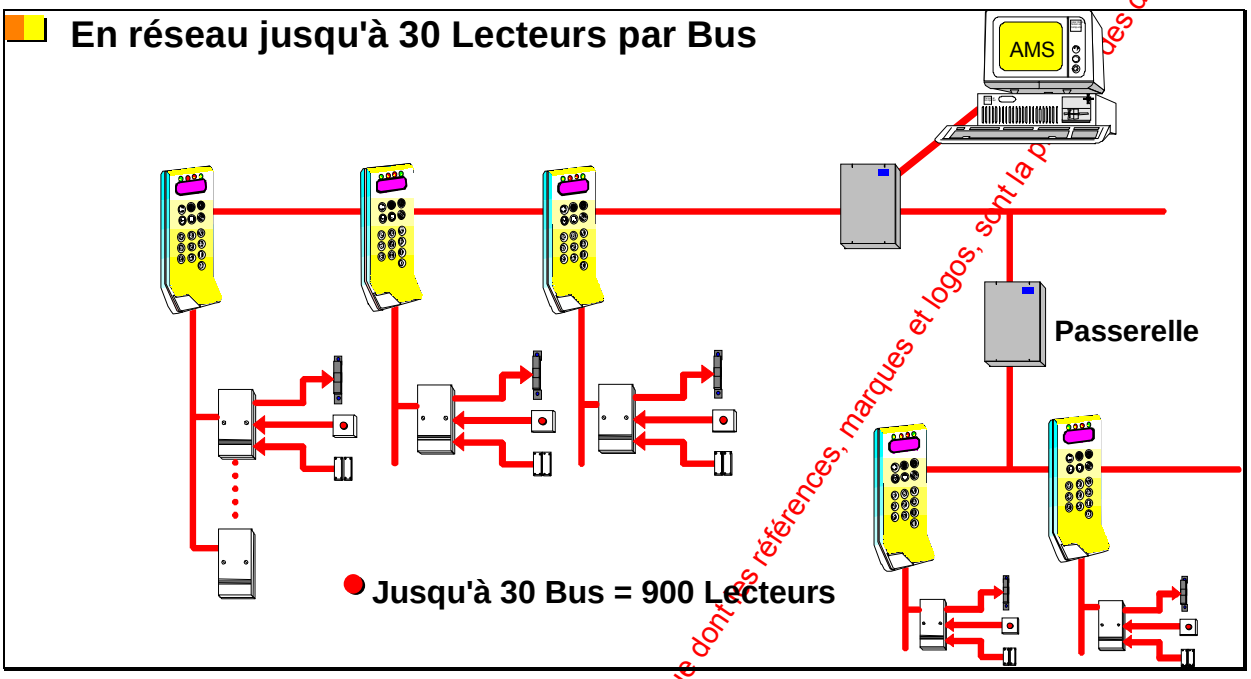
Dans cette solution les signaux armement/désarmement venant ou provenant d'un système d'intrusion "Non HISEC" pourront aussi être intégrés dans les fonctions Contrôle d'Accès.

Une source d'alimentation 12 ou 24V extérieure pourra être utilisée ou bien l'alimentation standard HISEC 90T-PS. Une interface imprimante séparée pourra aussi être directement connectée au lecteur par l'intermédiaire du bus RS 485.

Un système minimum pourra être réalisé en utilisant seulement UN S-ART 90T-S102 dont les 2 entrées seront utilisées pour le contact de porte et le bouton poussoir de sortie, le relais de sortie sera utilisé pour la commande de gâche.

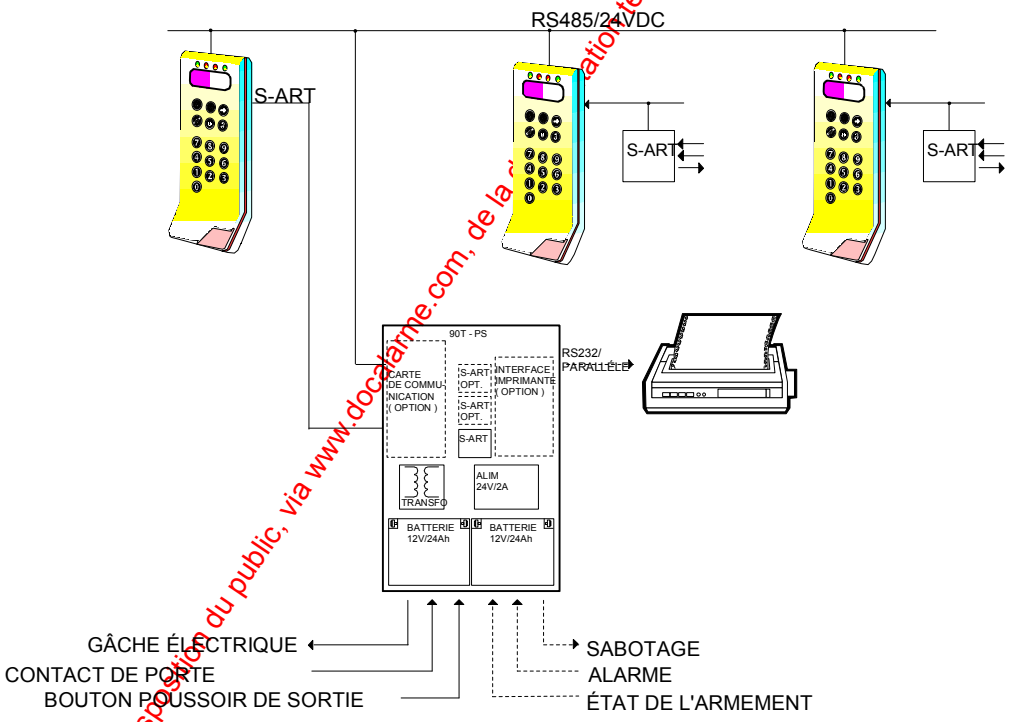
1.2.2 Système Multi lecteurs

Les lecteurs HISEC peuvent être connectés ensemble sur le bus RS485 en utilisant le même protocole multi maîtres, ceci sans contrôleur externe ni intelligence centrale. Le lecteur programmé à l'adresse N° 0 sera automatiquement considéré comme le maître du protocole multi maîtres.



Le nombre maximum de lecteurs connectables est de 31 sur 1 bus.

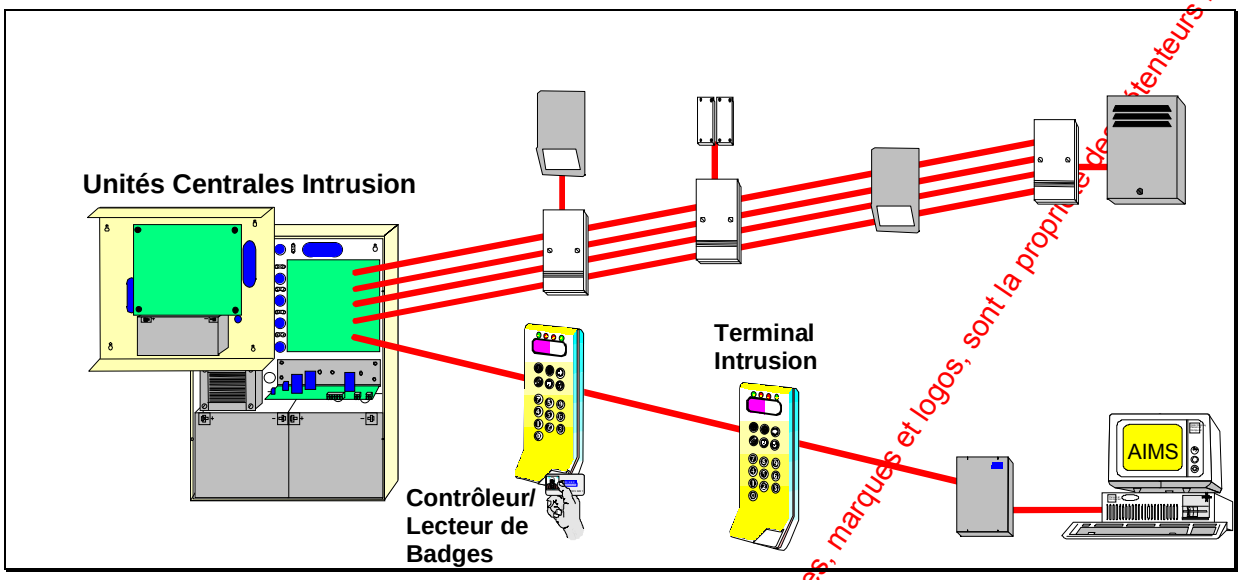
Utilisation du coffret d'alimentation 90T PS



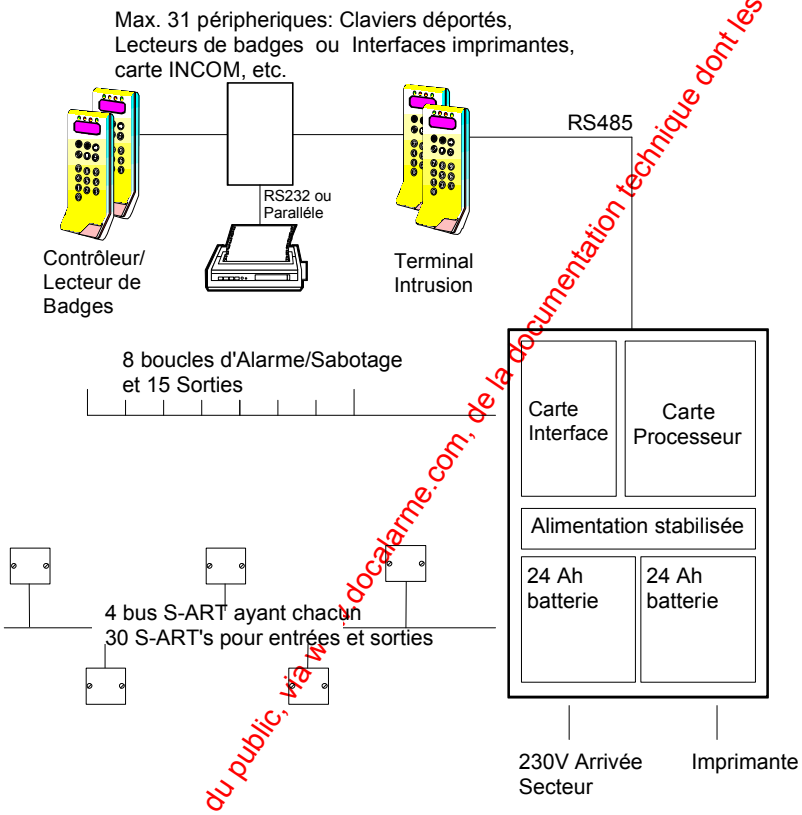
Cette configuration permet de réaliser un système multi lecteurs à un prix très compétitif pour les petites installations.

Si une imprimante est nécessaire, l'interface imprimante pourra être installée dans le coffret d'alimentation 90T-PS, ou comme une unité séparée connectée directement sur le bus RS 485.

1.2.3 Système Intégrant Contrôle d'Accès et Intrusion HISEC



Les lecteurs Contrôle d'Accès sont intégrés dans un système d'intrusion HISEC, ils sont connectés sur le bus multi-maîtres RS485 de la centrale HISEC Intrusion, les lecteurs peuvent alors servir de simples terminaux déportés pour HISEC Intrusion.



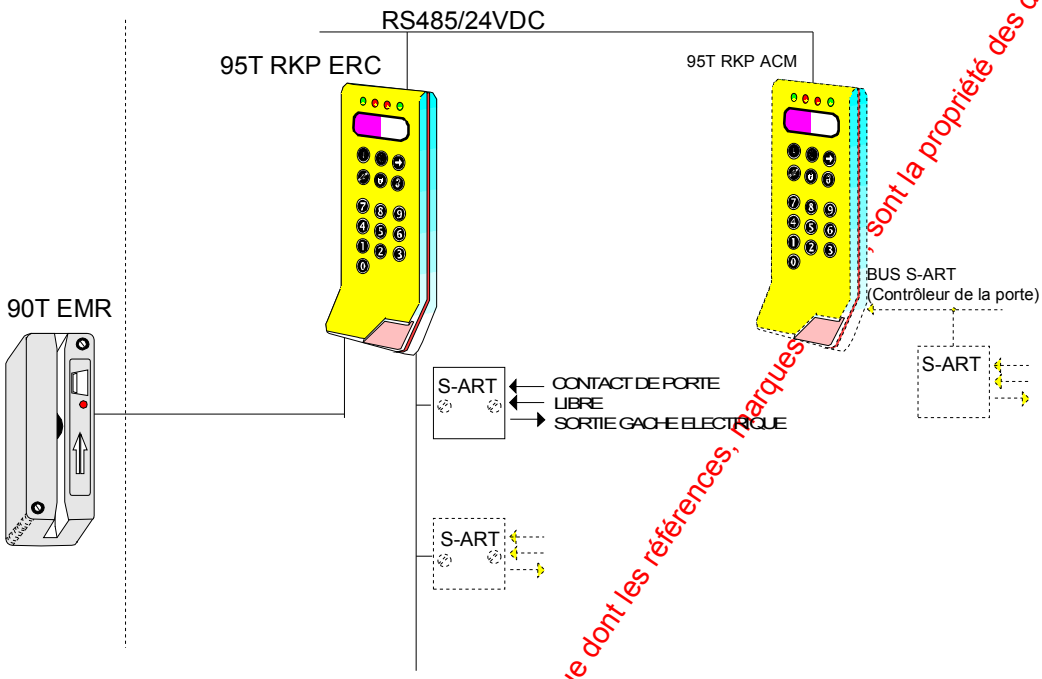
L'interface de la porte pour chaque lecteur pourra être celle représentée plus haut dans les exemples de configurations en mode Lecteur Autonome.

Suivant la configuration du système HISEC, le nombre maximum de lecteurs sur le même BUS ne pourra pas dépasser 31.

Sur un bus Multimaîtres, un ensemble de lecteurs, claviers déportés, etc. pourra être connecté et les lecteurs de Contrôle d'Accès seront partie intégrante du système d'intrusion.

1.2.4 Lecteurs à têtes externes

Les lecteurs contrôle d'accès HISEC peuvent être utilisés avec différentes têtes de lectures qui pourront être placées à une distance du terminal/contrôleur. Les têtes externes pourront être de technologie Magnétique, Wiegand, Proximité et Mains libres, codes à barres Infrarouges.



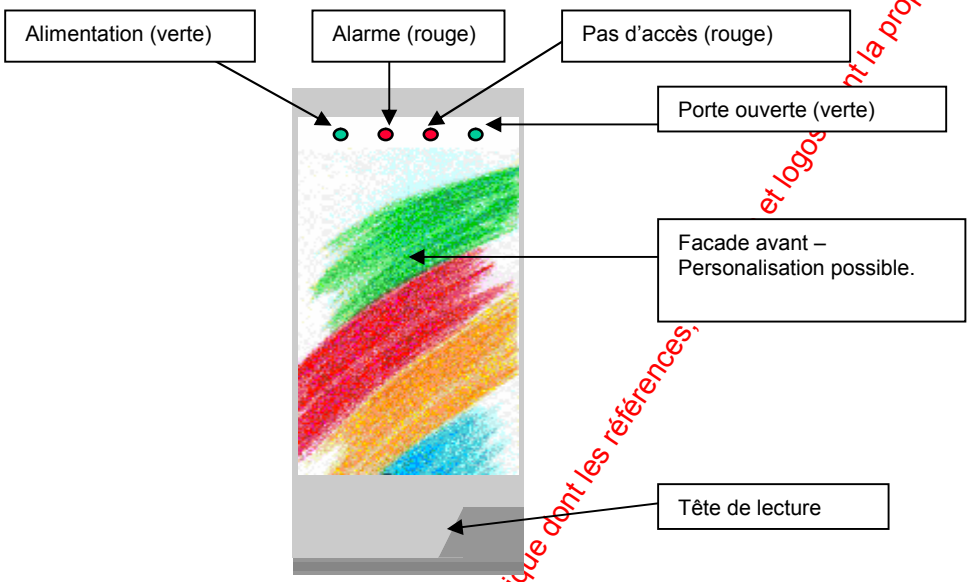
Le lecteur tête externe peut être utilisé en mode autonome, multi-lecteurs ou en système Intégré. Quand ce lecteur est utilisé avec le système intrusion HISEC, il pourra également être utilisé comme terminal standard de l'intrusion, sans utiliser de badges.

De la même façon que le lecteur classique, les entrées sorties se feront au moyen d'un bus S-arts où l'on pourra connecter jusqu'à 15 S-arts.

1.2.4 Les lecteurs Compact et Style

Ces deux lecteurs ont la particularité de ne pas posséder de clavier ni d'afficheur, et pourront être utilisés dans toutes les applications ou ces deux éléments ne sont pas nécessaires.

Ces lecteurs sont basés sur la même carte électronique que les lecteurs 95 T ACM. Tous les raccordements et concepts de câblage pourront être directement consultés dans le chapitre traitant du contrôle d'accès HISEC standard.



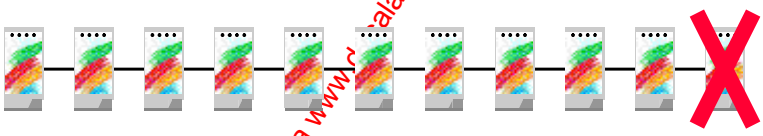
1.2.4 1 Les lecteurs Compact

Les lecteurs HISEC Compact possèdent certaines limitations de fonctionnement. Ce chapitre se propose de lister les limitations de cette gamme par rapport à un lecteur classique de type 95T AC.

1 seul S-ART

Avec HISEC Compact, il n'est possible de ne connecter qu'un seul S-ART sur le bus S-art. Ce S-art pourra être programmé avec les types logiciels désirés. Sur une installation standard, les valeurs par défaut de gestion d'une porte seront pré-programmées. S'il est nécessaire de gérer plus d'un S-art, il sera alors impératif de passer à un lecteur de HISEC Style.

Max. 10 Lecteurs



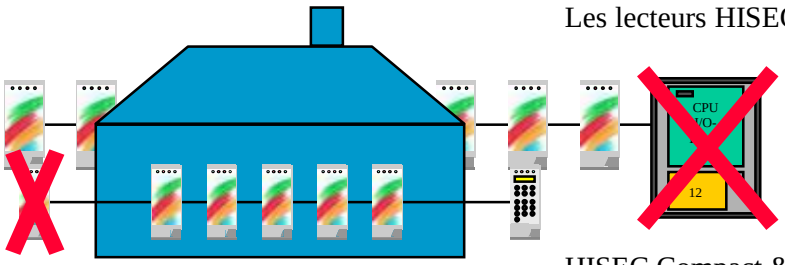
Le nombre maximum de lecteurs sur le système est de 10 lecteurs HISEC Compact.

Il est possible d'utiliser les adresses restantes (supérieures à 10) pour les périphériques tels 95T GPI COM en Modem, Imprimante et/ou Interface PC. Il n'est pas possible d'ajouter des lecteurs style à une adresse supérieure à 10 sur une installation HISEC Compact. Dans ce cas, les lecteurs Compact refuseront de démarrer.

Les lecteurs HISEC Compact refusent la présence d'une interface 95T GPI BR sur leur bus. La raison étant que les lecteurs HISEC Compact peuvent travailler uniquement sur un seul Bus (00) et de toutes façons pas sur un sous-bus.

Si vous voulez passer au-delà de cette limitation, il est nécessaire d'évoluer vers des lecteurs HISEC Style.

Utilisation en intérieur seul.



Les lecteurs HISEC Compact ne peuvent être utilisés qu'en intérieur, la raison étant que les éléments de chauffage ont été supprimés et que les têtes de lectures intégrées ne sont pas prévues pour l'extérieur.

Gamme de température des lecteurs HISEC Compact & Style : - 5^0C à + 60^0C

1.2.4 1 Les lecteurs Style

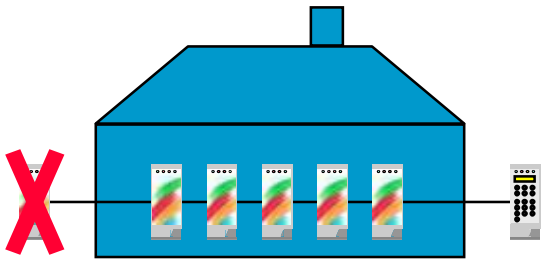
Les lecteurs HISEC Style possèdent certaines limitations de fonctionnement. Ce chapitre se propose de lister les limitations de cette nouvelle gamme par rapport à un lecteur classique de 95T AC.

Pas de limitation par logiciel

Le lecteur HISEC Style possède toutes les fonctions logicielles d'un lecteur classique, il pourra accepter jusqu'à 900 lecteurs, utiliser le mode intégré, piloter jusqu'à 15 sart's sur son propre bus, etc.

En fait, il pourra remplacer les lecteurs 95 T ACx classique partout où le clavier et l'afficheur ne sont pas nécessaires.

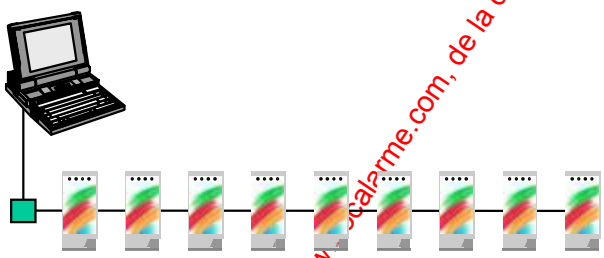
Utilisation en intérieur seul



Les lecteurs HISEC Style ne peuvent être utilisés qu'en intérieur, la raison étant que les éléments de chauffage ont été supprimés et que les têtes de lectures intégrées ne sont pas prévues pour l'extérieur.

Gamme de température des lecteurs HISEC Compact & Style : - 5^0C à + 60^0C

Programmation par PC



Les lecteurs HISEC Compact et Style seront programmés au moyen des logiciels PC AICS ou SMS.

1.2.4 Description du Lecteur de Badges HISEC Standard

Le lecteur de badges HISEC est une unité intelligente incluant une interface S-ART pour le contrôle de la porte, la base de données, l'afficheur cristaux liquides, le clavier, les voyants indicateurs. Toutes les informations concernant les badges et autres messages associés sont stockés dans sa base de données.

Si le lecteur est intégré au système d'intrusion HISEC ou dans un système Multi-lecteurs et que la communication soit coupée, le lecteur de badge continuera de prendre les décisions concernant le Contrôle d'Accès et enregistrera tous les événements.

La base de données est décrite en détail au *Chapitre 1.7.*

Les Entrées/Sorties du lecteur sont surveillées et contrôlées par une interface S-ART. Il est possible de connecter 15 S-ART comprenant chacun 2 entrées et 2 sorties sur chaque lecteur ceci pour diverses fonctions par ex : contact de porte, commande gâche électrique, bouton poussoir de sortie. La communication possède une vérification de parité ainsi que la surveillance de la ligne bus. Toutes les entrées/sorties sont librement programmables par les fonctions (types) logiciels décrites plus tard.

L'afficheur à cristaux liquides, les voyants indicateurs et le clavier sont utilisés pour les opérations quotidiennes et donnent à l'utilisateur une interface homme/machine agréable. Le clavier possède 6 touches de fonctions et 10 touches numériques. 5 voyants sont utilisés pour indiquer l'état du système.

Le lecteur de badges peut être utilisé à la fois comme clavier déporté et comme terminal de programmation du système d'intrusion HISEC.

Le lecteur de badges HISEC se présente exactement comme les claviers déportés du système intrusion HISEC avec les mêmes afficheurs, voyants, clavier. La seule différence est le montage (éventuel) d'une tête lecteur de badges sous le boîtier.

Ü Magnétique:

Le lecteur de piste magnétique est disponible suivant le standard ISO 2 et respecte les normes ISO 7810 et 7811/2 (piste 2). Les deux modes haute (3000 OE) et basse (300 OE) coercivité de badges, peuvent être lus par les têtes de lecture, mais en standard c'est le type haute coercivité qui est utilisé.

Les données contenues dans les badges sont en standard cryptées et ne peuvent pas être traduites pour calculer le numéro de badge ou de site et inversement.

Sur demande les badges peuvent être fournis au format non-crypté, pour pouvoir être utilisé par un autre système (cantine, gestion de temps de présence, etc.). Pour le détail du format Non-crypté se reporter au chapitre 1.6.7.

Ü Wiegand:

Les badges Wiegand acceptés par le lecteur sont aux (2) formats standards 25 ou 31 bits.

Ü Proximité:

Les badges proximités sont acceptés, couplés à différentes antennes qui déterminent la portée de la lecture (proximité ou mains libres), de plus deux technologies sont disponibles, **Actif** et **passif**.

Ü Code à barres infrarouges:

Les badges code à barres infrarouges sont acceptés, par contre cette configuration impose des badges fournis par le client (HISEC ne fourni pas de badges infrarouges à son catalogue). La tête de lecture HISEC accepte les principaux formats de badges existants (codabar, alpha 39, 2 parmi 5, etc.).

1.3 Le S-ART

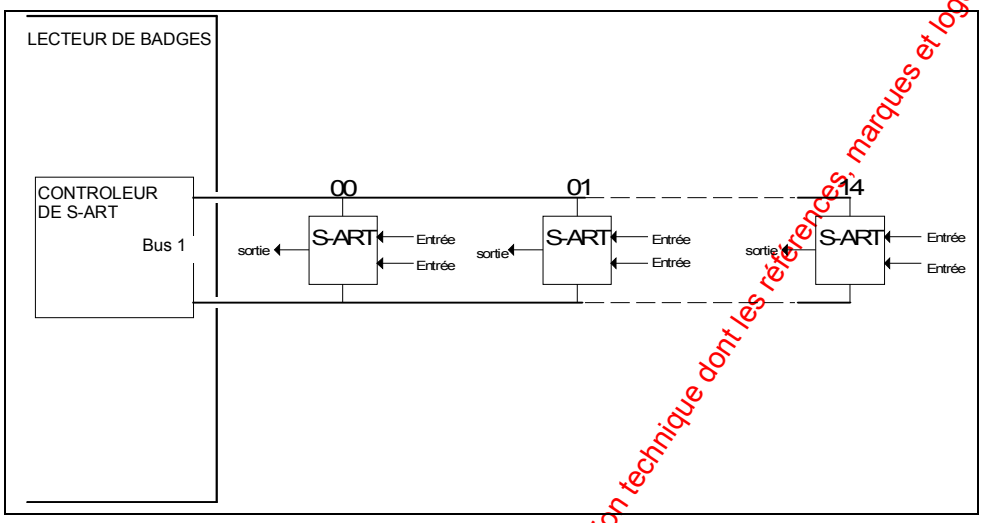
Le S-ART est un circuit intégré personnalisé, développé pour la transmission des données sur un câble à 2 fils et utilisé pour identifier individuellement chaque détecteur en alarme ou d'assurer des fonctions de Contrôle d'Accès .

Un maximum de 15 S-ART peut être connecté à un câble à 2 fils. Les 2 fils fournissent l'alimentation aux S-ART ainsi que les données - de et vers - les S-ART.

Si du 24V continu est nécessaire pour des relais, détecteurs, etc., il faudra une paire de fils supplémentaire.

1.3.1 Synoptique

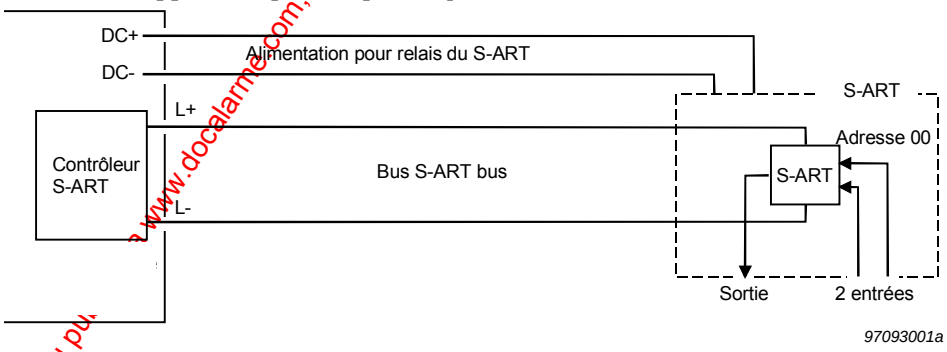
Un bus de S-ART sera connecté au contrôleur de S-ART incorporé au lecteur, celui-ci pouvant traiter un maximum de 15 S-ART.



Le contrôleur de S-ART, implanté sur la carte processeur du lecteur, scrute tous les S-ART connectés et donne les changements d'état des entrées à la carte processeur quand ils se produisent. Les sorties des S-ART sont activées ou désactivées de la même façon par des ordres issus du processeur .

Temps de scrutation : S-ART avec adresse 00,01 et 02.....: 40 à 80 ms
S-ART avec adresse 03 à 14.....: 130 à 260 ms

Si une sortie d'un S-ART doit être activée suite à un événement sur une entrée de S-ART, le système aura alors un délai de réaction appelé temps de réponse qui sera au maximum de 200 ms.

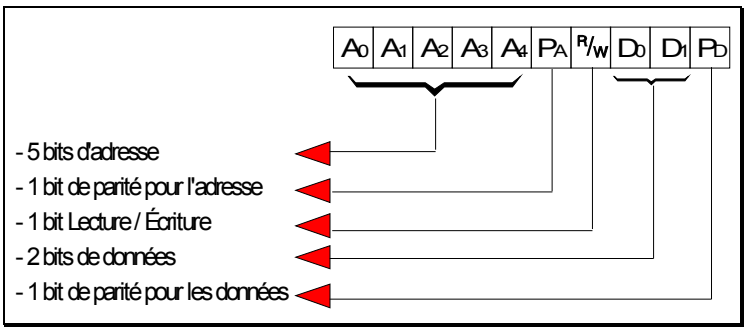


A partir de ce que nous avons vu plus haut, les adresses 00,01 et 02 ont toujours un temps de réponse plus rapide et il est fortement recommandé d'utiliser ces adresses pour les boutons poussoirs de sortie et la commande de gâche.

Les signaux de scrutation sur le bus sont expliqués en détail dans le prochain Chapitre.

1.3.2 Signaux de Bus

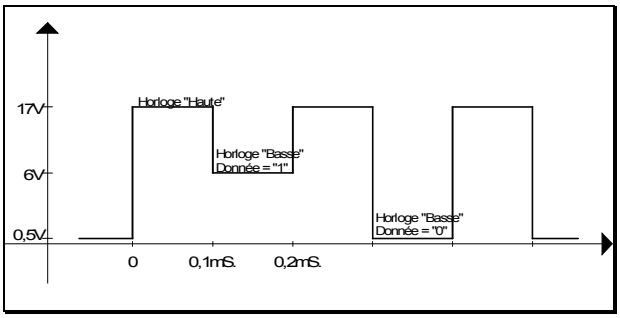
Le mot de transmission d'un S-ART comporte 10 bits:



Quand un S-ART reconnaît son adresse, il réagit en fonction du bit Lecture/Ecriture de la façon suivante:

1. Les données pour les 2 sorties - SORT0(OUT0) et SORT1(OUT1) - sont mémorisées.

2. Les données des 2 entrées - ENT0(IN0) et ENT1(IN1) - sont transférées dans le contrôleur de S-ART.



Le signal du bus est divisé en 3 niveaux afin de transmettre les **données** ainsi que l'**horloge**.

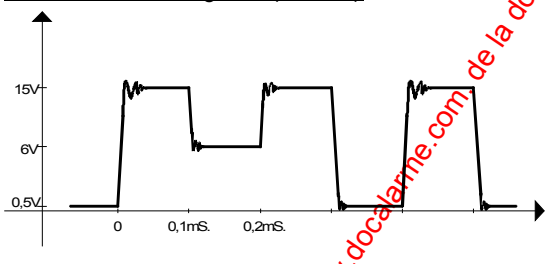
Quand l'horloge est à l'état haut (17V), tous les S-ART sont alimentés par le contrôleur de S-ART grâce à un transistor.

Quand l'horloge est à l'état bas, les données sont transmises. Le" 1 "logique est de 6,2V (fourni par le contrôleur de S-ART) et le" 0 "logique est de 0V.

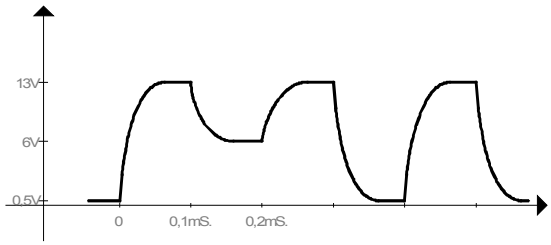
Quand le S-ART a reconnu son adresse et est prêt à transmettre une donnée d'entrée au contrôleur de S-ART, il court-circuite le bus au moyen d'une résistance de 150 ohms dans le cas d'un 0 logique, et reste en haute impédance dans le cas d'un 1 logique, maintenant ainsi le niveau 6,2V du contrôleur de S-ART.

Quand les S-ART sont connectés sur un câble, la forme du signal est déformée en fonction de la longueur de câble. Les 2 figures suivantes montrent un signal typique de S-ART sur des longueurs de câble de 200 m et de 500 à 700 m (câble 6/10 sans écran).

Câble de faible longueur (<200m)



Câble de grande longueur (>500m)



1.4 Entrées

Les fonctions d'entrées et de sorties sont spécifiées par attribution d'un type logiciel à chacune d'elles, et en plus pour les sorties par le type d'activation. Les termes de type logiciel et de type d'activation sont universels pour HISEC Intrusion et HISEC Contrôle d'Accès, par exemple un numéro de type logiciel spécifique ayant la même fonction sera identique dans les deux systèmes. (ex: N° 07 = Sabotage dans les deux systèmes).

1.4.1 Types d'Entrées

Entrées : le type logiciel indique quelle action doit être exécutée quand l'entrée change d'état y compris quel type logiciel de sortie doit être activé.

1.4.2 Description des Types Logiciels d'Entrées

Les types logiciels d'entrées sont divisés en types logiciels **standards**, **spécifiques** et **logiques**.

Types logiciels d'entrées standards:

N° Application	Description
‹ ’ **Sabotage** (commun avec l'intrusion)	Utilisé pour les contacts d'autoprotection et la déconnexion des unités dans les configurations à bus. Il peut être aussi activé par le contact autoprotection de l'unité de Contrôle d'Accès. Le type logiciel est actif quand l'entrée est active. Active le type logiciel de sortie N°02. Est transmis comme un message de sabotage HISEC et comme un message de sabotage dans l'historique.
Œ Ž **Défaut batterie** (commun avec l'intrusion)	Entrée pour test des batteries. Actif sur un défaut batterie. La condition de défaut sera remise à zéro quand l'entrée reviendra normale. Est transmis sous forme d'un message d'alarme dans l'historique.
Œ • **Défaut secteur** (commun avec l'intrusion)	Actif si le défaut secteur est présent depuis une heure. La condition de défaut sera remise à zéro quand l'entrée redeviendra normale. Est transmis sous forme d'un message d'alarme dans l'historique.

Types logiciels d'entrées spécifiques:

N° Application	Description
Ž ‹ **Contact de la porte 1**	Assure la supervision du contact de porte. Entrée permettant le contrôle de la procédure d'ouverture. Si la gâche n'est pas libérée quand cette entrée est activée, le type logiciel 70 (porte forcée) sera activé. Si la porte reste ouverte pour un temps trop long après une entrée, le type logiciel 72 (pré-alarme) sera activé suivi après délai du type logiciel 71 (porte maintenue).
Ž Œ **Contact de la porte 2**	Assure la supervision du contact de la porte 2. (avec ou sans inter-verrouillage) Entrée permettant le contrôle de la procédure d'ouverture. Si la gâche n'est pas libérée quand cette entrée est activée, le type logiciel 70 (porte forcée) sera activé. Si la porte reste ouverte pour un temps trop long après une entrée, le type logiciel 72 (pré-alarme) sera activé suivi après délai du type logiciel 71 (porte maintenue).
Ž • **Bouton poussoir de sortie**	Le bouton poussoir de sortie permet d'ouvrir la porte de l'intérieur des locaux sans provoquer une alarme porte forcée.

Le passage de l'état inactif à l'état actif commandera l'activation du type logiciel de sortie 80 (gâche électrique) et un message sera enregistré.

Ž Ž Etat de l'armement/désarmement

Etat de l'armement/désarmement venant d'un système d'intrusion où le terminal de contrôle est placé à **l'extérieur** de la zone protégée. Si le système d'intrusion est armé, l'unité Contrôle d'Accès est bloquée et une ligne de texte apparaît sur l'afficheur.

Ž • Etat de l'armement/désarmement

Etat de l'armement/désarmement venant d'un système d'intrusion où le terminal de contrôle est placé à **l'intérieur** de la zone protégée. Si le système d'intrusion est armé, l'unité de Contrôle d'Accès ne sera pas bloquée comme dans le cas du type logiciel 33. Toutefois un message apparaîtra pour attirer l'attention de l'utilisateur sur le fait que le système d'intrusion doit être désactivé après son entrée. Le message devra être confirmé en premier pour pouvoir activer la gâche.

Ž • Signal de retour d'armement/désarmement

Signal de retour d'armement/désarmement venant d'un système d'intrusion contrôlé (armement/désarmement) par une sortie de S-ART (type logiciel 75). Ce signal devra arriver dans les 10 secondes à partir de l'armement. S'il n'y a pas de retour le lecteur donnera un message défaut d'armement sur l'afficheur. Armement et désarmement seront enregistrés dans l'historique du lecteur.

Ž ‘ Entrée d'alarme

Type logiciel de suivi d'entrée. Quand ce type logiciel est actif, le texte "ALARME(S)" sera présenté sur l'afficheur avec le message "PORTE OUVERTE". Le passage de l'état passif à actif sera enregistré comme une alarme. Le badge Maintenance peut être utilisé avec le niveau de priorité le plus faible sans autorisation du Client pendant l'activation de ce type logiciel.

Ž ’ ,Ž “ Contrôle global des portes

Ces deux types logiciel seront utilisés dans les applications ou il nécessaire d'ouvrir une (ou plusieurs) porte à la fois (par ex: à partir d'une centrale incendie). Si une entrée programmée avec les types logiciel 37, 38 passe à l'état actif, un message est envoyé à chaque lecteur et chaque lecteur possédant ce type logiciel dans son équation commandera l'ouverture de porte.

Ces types logiciel d'entrées doivent être inclus dans des équations SI/ALORS par ex: 95 = 37 + 80, où le type logiciel 95 est programmé sur la sortie du S-ART contrôlant la gâche électrique. La porte pourra être ouverte dans deux cas: Lecture d'un badge (Accès normal) ou quand le type logiciel 37 est activé.

Ces deux types logiciel d'entrée rendent possible la réalisation de deux différents groupes de portes, un groupe contrôlé par le type logiciel 37 et l'autre par le type 38. Chaque type logiciel pourra contrôler un groupe de portes programmé avec les équations suivantes:

95=37+80 (1er groupe de porte)
95=38+80 (2eme groupe de porte)

La libération d'une porte par les types logiciels 37/38 créera un message PORTE FORCEE. Pour éviter cela une équation devra être réalisée avec le type logiciel 98. Le type logiciel de sortie 98 (et seulement ce type) supprime le message PORTE FORCEE. Ce type logiciel indiquera PORTE OUVERTE sur l'afficheur quand il sera activé par les types logiciel 37-38.

Ž ” Contrôle par zone des portes

L'application de ce type logiciel est très similaire au type logiciel 37 et 38. La seule différence étant que le type logiciel 39 travaille par zone. Si une entrée programmée avec un type logiciel d'entrée 39 devient active, un message est envoyé à tous les **lecteurs de la même zone** et ceux ayant ce type logiciel dans leur équation commanderont la porte.

Ce type logiciel d'entrée doit être inclus dans des équations SI/ALORS par ex: 95=39+80, ou le type logiciel 95 est programmé sur la sortie du S-ART contrôlant la gâche électrique. La porte pourra être ouverte dans deux cas: Lecture d'un badge (Accès normal) ou quand le type logiciel 39 est activé.

La libération d'une porte par le type logiciel 39 créera un message PORTE FORCEE. Pour éviter cela une l'équation devra être réalisée avec le type logiciel 98. Le type logiciel de sortie 98 (et seulement ce type) supprime le message PORTE FORCEE. Ce type logiciel indiquera PORTE OUVERTE sur l'afficheur quand il sera activé par le type logiciel 39.

- **‹ Bouton poussoir de sortie 1 Porte 2**

Le bouton poussoir de sortie permet d'ouvrir la porte 2 de l'intérieur du sas, sans provoquer une alarme porte forcée.(avec ou sans inter-verrouillage).
Le passage de l'état inactif à l'état actif commandera l'activation du type logiciel de sortie 84 (gâche électrique 2) et un message sera enregistré.

- **Œ Bouton poussoir de sortie 2 Porte 2**

Le bouton poussoir de sortie permet d'ouvrir la porte de l'intérieur des locaux sans provoquer une alarme porte forcée (avec ou sans inter-verrouillage).
Le passage de l'état inactif à l'état actif commandera l'activation du type logiciel de sortie 84 (gâche électrique 2) et un message sera enregistré.

- **• Blocage Urgence**

Cette entrée est utilisée pour bloquer les porte dans un système d'inter-verrouillage. Quand cette entrée est activée les (2) portes connectées sur le lecteur correspondant sont bloquées. Peut aussi être utilisée sans fonction d'inter-verrouillage.

‘ Œ Contact de porte Externe

L'afficheur du Lecteur indique PORTE OUVERTE quand cette entrée est activée. Normalement raccordé à la sortie correspondante d'un autre lecteur placé sur un autre Bus, programmé lui avec un type logiciel de sortie 86.

Types logiciels d'entrées logiques:

Les types logiciels d'entrées logiques seront utilisés dans les équations SI/ALORS. Ils sont activés par des événements logiques sur l'unité de Contrôle d'Accès, et ne peuvent pas être assignés à une entrée physique.

N°	Application	Description
’ ‹	**Porte forcée**	Actif après l'événement - la porte a été forcée à l'ouverture. Provoque l'activation du type logiciel de sortie 70 et est remis à zéro quand la porte est refermée. Il est transmis à l'extérieur dans l'historique des alarmes.
’ Œ	**Porte maintenue**	Actif après l'événement - porte maintenue. Provoque l'activation du type logiciel de sortie 71 et est remis à zéro quand la porte est refermée. Il est transmis à l'extérieur dans l'historique des alarmes.
’ •	**Avertissement porte maintenue**	Actif quand la porte est ouverte trop longtemps après libération. Provoque l'activation du type logiciel de sortie 72 et est remis à zéro quand la porte est refermée. N'est pas transmis à l'extérieur.
’ Ž	**Lecture de badge valide**	Actif quand un badge est lu et accepté. Provoque l'activation du type logiciel de sortie 73 et est remis à zéro quand la porte est libérée ou par fin de temporisation. Il n'est pas transmis à l'extérieur.
’ •	**Lecture de Badge invalide**	Actif quand un badge est lu avec une des conditions suivantes: Badge bloqué, Badge non valide, Erreur de Code Personnel (10 tentatives) Provoque l'activation du type logiciel de sortie 74 et est remis à zéro quand un badge valide est lu ou par fin de temporisation. Chaque événement est transmis à l'extérieur et enregistré séparément dans l'historique d'alarme.
’ ‘	**Type logiciel contrôlé par programme horaire**	Actif quand le Programme Hebdomadaire 32 est actif.
’ ’	**- Type logiciel contrôlé par programme horaire**	Actif quand le Programme Hebdomadaire 33 est actif.
’ “	**- Tous badges à l'extérieur**	La fonction ce type logiciel d'entrée/sortie est d'indiquer quand tous les badges sont à l'extérieur du système (Zone 00). Ce type logiciel d'entrée pourra être programmé dans les équations de type SI/ALORS. Cette entrée est active quand tous les badges sont enregistrés en Zone 0. Cette entrée passe au repos quand **un** seul badge n'est plus en zone 0.
’ ”	**Utilisation du code Contrainte**	Actif quand le Code Personnel hold-up a été utilisé. Provoque l'activation du type logiciel de sortie 07 et est remis à zéro sur une fin de temporisation ou l'entrée suivante d'un badge. Est transmis comme un message hold-up HISEC externe et comme un message d'alarme dans l'historique.
“ ‹	**Libération Porte 1**	Actif après acceptation de libération de la porte soit par lecture badge ou utilisation du bouton poussoir de sortie. Provoque l'activation du type logiciel de sortie 83. La remise à zéro s'effectue à l'ouverture de la porte ou sur une fin de temporisation. N'est pas transmis à l'extérieur.

“ Œ Libération Porte 2	Actif après acceptation de libération de la porte 2 soit par lecture badge ou utilisation des boutons poussoir 1 et 2 de la porte 2. Provoque l'activation du type logiciel de sortie 84. La remise à zéro s'effectue à l'ouverture de la porte ou sur une fin de temporisation. N'est pas transmis à l'extérieur.
” ‹ , ” ” Entrée SI SI/ALORS.	Utilisation libre, doit être incorporé aux équations Ce type logiciel est actif quand l'entrée est active.

1.4.3 Adresse des Entrées

Chaque S-ART possédant 2 adresses d'entrées, il est nécessaire de calculer la relation entre l'adresse du S-ART (programmé sur la carte du S-ART) et l'adresse des entrées (utilisées quand on veut programmer un type logiciel d'entrée) par l'équation suivante :

Adresse d'entrée = 2 x adresse du S-ART + N° entrée S-ART (0 ou 1)

1.5 Sorties

1.5.1 Types de Sorties

Sorties: **Le type logiciel** indique quelle action sur l'entrée doit activer la sortie.

Le type d'activation indique la polarité de la sortie et éventuellement le délai ainsi que la durée.

1.5.2 Description des Types Logiciels de Sortie

Les types logiciels de sorties sont divisés entre les types logiciels **standards** et **spécifiques**.

Les types logiciels de sorties standards :

N°	Application	Description
‹ •	**Sabotage** (commun avec l'intrusion)	Indication locale d'une alarme sabotage. Actif si un type logiciel d'entrée 67 est actif.
‹ ’	**Hold-up** (commun avec l'intrusion)	Indication locale d'une alarme Hold-up. Actif si un type logiciel d'entrée 79 est actif.
Œ •	**Défaut batterie** (commun avec l'intrusion)	Indication locale de défaut batterie. Actif si un type logiciel d'entrée 13 est actif.

Les types logiciels de sorties spécifiques:

N°	Application	Description
• ‹ , Ž •	**Zone complète**	Ce type logiciel permet d'indiquer quand une zone est "complète" c.-à-d. quand la limite max. du nombre de badges autorisés dans une zone a été atteinte, cette fonction peut être utilisé pour indiquer l'état d'une zone parking. Au moyen des logiciel AICS et AIMS il est possible de programmer le nombre max. de badges présents dans chaque zone. Quand ce nombre est atteint dans la zone, la sortie correspondante est activée. les types logiciels 20 à 35 correspondent respectivement aux zones 01 à 15. Prière de noter : La porte n'est pas bloquée quand le nombre max. de badge est atteint dans une zone, il est donc possible d'entrer d'autres badges dans la zone spécifiée. Le comptage max. n'agit que sur la sortie correspondante pour chaque zone.
• ‹ - ‘ ”	**Matrice Ascenseur**	Ces types logiciel sont utilisés pour contrôler les étages où les différents groupes de personnel ont accès. Le logiciel des lecteurs est capable de gérer 30 étages, mais du fait qu'il n'existe qu'une adresse par S-art, **seuls les 15 premiers** types logiciel pourront être utilisés. Pour chaque étage une sortie est réservée, 40 pour le 1er, 41 pour le 2éme, etc. jusqu'à 69 pour le 30eme étage. Un type logiciel de sortie pourra être directement programmé sur le lecteur ou par le logiciel AICS. La durée d'activation de la sortie sera fixée par le type d'activation choisi.
’ ‹	**Porte forcée**	Indication locale de porte forcée. Actif si un type logiciel d'entrée 70 est actif.
’ Œ	**Porte maintenue**	Indication locale de porte maintenue. Actif si un type logiciel d'entrée 71 est actif.
’ •	**Avertissement porte maintenue**	Un avertissement de porte maintenue est indiqué sur l'afficheur et par le "buzzer" interne. Cette sortie peut être utilisée pour

commander un indicateur visuel ou sonore. Actif quand un type logiciel d'entrée 72 est actif.

’ Ž Entrée d'un badge Est actif quand un badge est lu. Actif si un type logiciel d'entrée 73 est actif.

’ • Entrée d'un badge invalide Indication locale d'utilisation d'un badge invalide. Actif quand le type logiciel d'entrée 74 est actif.

’ • Contrôle d'armement/désarmement

Est utilisé pour armer/désarmer un autre système d'intrusion (Non-HISEC). Est activé par pression du bouton poussoir d'armement comme décrit dans les Procédures d'Utilisation. Il est remis à zéro par pression sur le bouton poussoir de désarmement. Les armements/désarmements sont enregistrés dans l'historique.

’ ‘ Contrôle armement/désarmement par impulsion

Est utilisé pour armer/désarmer un autre système d'intrusion (Non-HISEC). Une impulsion de 5 sec est générée par l'appui sur le bouton poussoir d'armement/désarmement comme décrit dans les Procédures d'Utilisation. Seuls les types d'activation 7 et 8 peuvent être utilisés avec ce type logiciel.
Les armements/désarmements sont enregistrés dans l'historique.

’ “ Tous badges à l'extérieur La fonction ce type logiciel est d'indiquer quand tous les badges sont à l'extérieur du système (Zone 00). Cela peut être utilisé par exemple pour activer un buzzer qui indiquera la nécessité d'armer le système intrusion.
Cette sortie est automatiquement activée si le système possède un contrôle d'entrée-sortie en périphérie et que des zones d'entrée-sorties (avec ou sans anti-retour) ont été créées. Une sortie devra être créée avec le type logiciel 78.

’ ” Shunt d'alarme Sortie utilisée pour inhiber le contact de porte connecté à un système d'intrusion externe. Est activé quand le type logiciel d'entrée 80 est activé et remise à zéro 1 sec après la nouvelle fermeture de la porte (type logiciel d'entrée 30).

“ ‹ Test batterie Est utilisé pour contrôler la commande de test de la charge des batteries. Il est actif pour 15 sec chaque heure ou quand le *Menu 93* "*Test Batterie*" est appelé. Ce type est seulement utilisable avec des coffrets chargeurs (alimentation) ayant une entrée physique de test extérieure.

“ Ž Libération porte 1 Sortie pour la gâche électrique. Est activé quand le type logiciel d'entrée 80 est actif. Obligatoirement utilisé avec les types d'activation 1 ou 2 (la durée est contrôlée par le *Menu 83 Temporisations de la Porte*).

“ • Libération porte 2 Sortie pour la gâche électrique de la porte 2. Est activé quand le type logiciel d'entrée 81 est actif. Obligatoirement utilisé avec les types d'activation 1 ou 2 (la durée est contrôlée par le *Menu 83 Temporisations de la Porte 1*).
Nota: les temporisations de porte sont les mêmes sur les portes 1 et 2.

“ ‘ Libération extérieure Est activée quand la sortie gâche électrique (Porte 1) est activée. La remise à zéro s'effectue à l'ouverture de la porte ou sur une fin de temporisation.
Normalement utilisé en connexion avec le type logiciel 61 sur le lecteur correspondant sur un autre Bus.

N°	Application	Description
” ‹ - ” •	**Sorties ALORS (pour équations SI/ALORS)**	Peuvent être utilisés pour réaliser des fonctions spéciales. Une expression est programmée pour chaque type logiciel (voir *Chapitre 1.5.3 Les Equations SI/ALORS*).
	Sortie mémorisée	Les types logiciels 90-94 sont activés quand la condition relative à l'expression SI passe de L'état "FAUX" à "VRAI". La sortie sera remise à zéro par la prochaine libération de la gâche avec un badge, ou par la fin de temporisation spécifiée par le type d'activation.
” • - ” ’	**Sorties ALORS (pour équations SI/ALORS)**	Peuvent être utilisés pour réaliser des fonctions spéciales. Une expression est programmée pour chaque type
	Sortie de suivi d'entrée	Les types logiciels 95-98 sont activés quand la condition relative à l'expression SI est "VRAI". La sortie sera remise à zéro quand la condition relative à l'expression SI deviendra "FAUSSE" ou par la fin de temporisation spécifiée par le type d'activation.
” “	**Sorties ALORS (pour équations SI/ALORS)**	Idem à 95-97, excepté quand cette équation est utilisée pour activer une gâche électrique en utilisant les types logiciel 37, 38, 39.
	Sortie de suivi d'entrée	Ce type logiciel de sortie 98 (et seulement ce type) supprime le message PORTE FORCEE. Dans le même temps ce type logiciel indiquera PORTE OUVERTE sur l'afficheur
” ”	**Sortie ALORS (pour Equation SI/ALORS à destination de l'Intrusion HISEC)**	Idem 95-98 mais transmettra aussi un message d'alarme vers le système d'Intrusion HISEC. Ce type logiciel devra être utilisé si un message d'alarme doit être transmis à la HISEC CONTROLE D'ACCES Intrusion, par exemple Porte Forcée.
	Sortie vers l'extérieur	Dans l'Intrusion HISEC il sera reçu comme l'adresse 30 + l'adresse du lecteur (sur le bus RS-485) et pourra être défini librement dans le système d'intrusion comme un type logiciel d'entrée appartenant à la liste de ceux de l'intrusion.

1.5.3 Les Equations SI/ALORS

Les équations SI/ALORS sont utilisées pour déterminer la réaction dans les différents cas de figure qui peuvent se présenter sur chaque système, par exemple: quelle alarme doit être transmise, à l'attention de quelle sortie de relais, vers un système d'alarme extérieur, et quelle alarme doit activer une sirène ou autre indicateur d'alarme.

Les équations SI/ALORS ou conditions déterminent l'interdépendance d'une ou plusieurs entrées ET/OU un nombre d'événements logiques - partie SI, et les sorties - partie ALORS.

SI(entrées) ALORS (sortie) ou (sortie) = (entrées)

La partie SI, côté droit de l'équation, est une expression des types logiciels d'entrées où les fonctions logiques "ET" ou "OU" peuvent être utilisées. "ET" est représenté par "*" et "OU" est représenté par "+".

La partie ALORS, côté gauche de l'équation, est un type logiciel de sortie qui devient actif quand les conditions des éléments du SI sont vérifiées.

Exemple : S = e1+e2+(e3*e4)

Explication : Toutes les Sorties avec le type logiciel "S" seront activées, si sont activées :

- **Une** seule entrée ou **plus** avec le type logiciel "e1"

OU

- **Une** seule entrée ou **plus** avec le type logiciel "e2"

OU

- **Une** seule combinaison d'entrée ou **plus** avec le type logiciel constitué de:
  - **Une** seule entrée ou **plus** avec le type logiciel "e3"

ET

  - **Une** seule entrée ou **plus** avec le type logiciel "e4"

Sur chaque lecteur HISEC, il est possible de définir 10 équations SI/ALORS (une équation pour chaque type logiciel de 90 à 99).

Les Equations implicites dans le Contrôle d'Accès ne pouvant être éditées, sont les suivantes :

02 = 07	70 = 70	73 = 73	79 = 80
07 = 79	71 = 71	74 = 74	83 = 80
12 = 13	72 = 72	78 = 78	

Seuls les types de 90 à 99 peuvent être utilisés comme types de sorties dans les équations SI/ALORS.

1.5.4 Les Horloges

Les horloges sont utilisés pour commander les sorties physiques et sont définis par les conditions suivantes:

Type d'activation = **Retard** / **Durée** / **Polarité**

Les types d'activation sont relatifs aux sorties physiques et non aux types logiciels, de ce fait des sorties ayant le même type logiciel pourront avoir des types d'activation différents.

Le **Reatrd** représente le délai entre l'activation d'un type logiciel et le moment où la sortie physique est activée.

La **Durée** représente la durée maximum durant laquelle la sortie sera activée.

La **Polarité** indique si la sortie est "active au niveau haut" ou "active au niveau bas".

Une sortie sera toujours remise à zéro quand le type logiciel sera remis à zéro (excepté les types logiciel de sortie Equations 90-94).

Les Horloges pré-programmées sont les suivantes : (non modifiables au clavier)

Horloges	Retard	Durée	Polarité	Description
1	0	∞	0	Arrêt au repos
2	0	∞	1	Marche au repos
3	0	∞	2	Impulsion 1 sec
4	0	3mn	0	Arrêt au repos
5	0	3mn	1	Marche au repos
6	0	3mn	2	Impulsion 1 sec
7	0	5 sec	0	Arrêt au repos
8	0	5 sec	1	Marche au repos
9	0	5 sec	2	Impulsion 1 sec
10	0	1 sec	0	Arrêt au repos
11	0	1 sec	1	Marche au repos

Nota: Les Horloges peuvent uniquement être modifiées au moyen du logiciel PC 90T AICS.

1.5.5 Les Adresses de Sorties

Etant donné que chaque S-ART possède 2 adresses de sorties (une seule est utilisable), il est nécessaire de calculer la relation entre l'adresse du S-ART (programmé sur la carte du S-ART) et l'adresse des sorties (utilisées quand on veut programmer un type logiciel de sortie) par l'équation suivante :

Adresse de sortie = 2 x adresse du S-ART + N° sortie S-ART (0 ou 1)

Avec les S-ART existants de type 90T-S102, 90T-S103 seule la sortie N° 1 peut être utilisée.

1.6 Les Badges

1.6.1 Organisation des Badges

Tous les badges ont un numéro de série imprimé sur le badge lui même. Ce numéro est en relation spécifique avec les données avec lesquelles il a été codé au moment de sa fabrication. Il possédera au minimum le numéro du badge (code utilisateur), normalement seront aussi inclus le code Client et quelques fois les codes Installateur et Distributeur.

Le code Distributeur est relatif au vendeur ou distributeur du système Contrôle d'Accès HISEC. Ce code est géré par HI SEC.

Le numéro d'Installateur est donné à chaque Installateur dépendant d'un Distributeur et il est géré par le Distributeur. Si HISEC vend directement à un Installateur, l'Installateur peut obtenir un N° de Distributeur et l'Installateur peut s'il le désire diviser son pays en régions ayant chacune un N° d'Installateur différent. Cela donne la possibilité d'avoir des badges de Maintenance différents dans chaque région.

Le code Client est relatif à chaque système installé et est décidé par l'Installateur ou le Distributeur.

Le numéro du badge identifie la personne utilisant le badge. Ce nombre peut aller de 1 à 65500, et pour cette raison le nombre maximum de badges pour un système sera de 65500. Le numéro de badge est géré par le client utilisant l'installation.

Cette méthode de gestion des numéros de code Distributeur, Installateur et Client permet de réaliser une gestion plus facile et plus sécurisante des badges distribués pour éviter d'avoir deux badges identiques et pouvoir par exemple les utiliser sur deux installations différentes.

Les badges sont fabriqués avec l'ensemble des groupes de badges suivants :

Badges Maîtres	Badges Maintenance	Badges Normaux

L'intérêt de ces groupes est de définir quelques badges (badges de Maintenance & badges maîtres), qui auront droit à des fonctions spéciales de programmation, indépendantes de la configuration du système.

Le tableau suivant présente un panorama du système de numérotation des badges :

Distributeur	Installateur	Client	N° badge	Explication
000	x	x	x	Réservé HI SEC international
001	001	000	1 à 65500	Installateur 1, badges Maintenance
001	001	001	1 à 4	Installateur 1, Client 1 et Utilisateur, badges de prog. Maître
001	001	001	5 à 65500	Installateur 1, Client 1 et Utilisateur, badges Utilisateurs normaux
001	001	002	1 à 4	Installateur 1, Client 2 et Utilisateur, badges de prog. Maître
001	001	002	5 à 65500	Installateur 1, Client 2 et Utilisateur, badges Utilisateurs normaux
001	002	000	1 à 65500	Installateur 2, badge Maintenance
001	002	001	1 à 4	Installateur 2, Client 1 et Utilisateur, badges de prog. Maître
001	002	001	5 à 65500	Installateur 2, Client 1 et Utilisateur, badges Utilisateur normaux
001	002	002	1 à 4	Installateur 2, Client 2 et Utilisateur, badges de prog. Maître
001	002	002	5 à 65500	Installateur 2, Client 2 et Utilisateur, badges utilisateur normaux

Le premier code Distributeur valide est le N°1. Le tableau précédent présente le principe de numérotation pour le Distributeur N°1. Le système de numérotation sera le même pour chaque Distributeur.

1.6.2 Badges Maîtres

Tous les badges avec les numéros allant de 0 à 4 sont des badges maîtres pour le système défini par les numéros de code - Client, Installateur et Distributeur - du badge. Le principal intérêt des badges maîtres est d'augmenter le niveau de sécurité.

Le badge Maître est confié au responsable de sécurité, au démarrage du système. Il est recommandé de placer les badges maîtres dans un endroit sûr, et les utiliser seulement conjointement à l'installation ou à la Maintenance. Un badge Maître ne peut pas être effacé une fois qu'il a été validé, aussi il est recommandé de créer le minimum absolu de badges maîtres nécessaires pour chaque système.

Le responsable de la sécurité peut décider où et quand l'utilisation des badges Maintenance est autorisée dans le système.

Le badge Maître a une valeur capitale durant la procédure de démarrage du système, et peut - sans être dépendant des programmes horaires - être utilisé comme un badge de programmation avec le plus haut niveau de priorité. Dans les systèmes intégrés à la centrale intrusion HISEC, il est nécessaire d'utiliser les badges maîtres à l'initialisation. Les autres configurations peuvent être démarrées sans badges maîtres.

1.6.3 Badges de Maintenance

Tous les badges avec le numéro de code Client N°000 sont des badges de Maintenance. Un badge de Maintenance peut donner accès à tous les systèmes ayant le même code Distributeur et N° d'Installateur, chaque Installateur peut avoir un nombre maximum de 65000 badges de Maintenance.

Les badges de Maintenance sont des badges personnels et doivent seulement être confiés au personnel de Maintenance autorisé. Chaque usage d'un badge de Maintenance est consigné dans l'historique des alarmes du lecteur. Il est toujours possible de voir quel badge de Maintenance a été utilisé et par qui.

Les badges de Maintenance peuvent être bloqués à tout moment par les badges maîtres, ceci pour augmenter le niveau de sécurité.

Le badge Maintenance est utilisé au démarrage du système pour initialiser le lecteur avec les N° de Distributeur, Installateur et N° de Client. En dehors de cela, les badges de Maintenance peuvent donner accès à certaines fonctions liées à la programmation et au test du système, dépendantes de l'autorisation du Client (voir *Chapitre 1.6.6 Badges de Programmation et Priorité des Badges*).

+ Le **Code Personnel** attribué aux badges Maintenance est **1122 (33)** et ne peut pas être changé.

L'utilisation du badge Maintenance est dépendante de l'état et de la configuration du système complet.

Autonome / Multi-lecteurs:

Le badge de Maintenance peut ouvrir la porte et avoir accès aux Menus de Maintenance avec la priorité la plus basse (voir *Chapitre 1.6.6*) en cas d'alarme venant d'un type logiciel 36.

Si le mode Maintenance est autorisé par le Client le badge de Maintenance aura accès à tous les Menus.

Intégration à HISEC INTRUSION :

Lecteur en mode Standard (tête incorporée ou lecteur intérieur)

En cas d'alarme sur la partie Intrusion HISEC, le badge Maintenance est accepté et donne un accès direct aux Menus Intrusion est entrant le code Maintenance **Intrusion** ou Intervenant. A la **fin de session** la porte sera ouverte pour permettre au technicien de Maintenance de franchir la porte.

Le technicien de Maintenance peut par la touche ➔ avoir accès aux Menus de Maintenance (Contrôle d'accès) avec la priorité la plus basse (voir *Chapitre 1.6.6*) en cas d'alarme.

Si le mode Maintenance est autorisé par le Client le badge de Maintenance aura accès à tous les menus.

Lecteur en mode tête déportée (Contrôleur à l'intérieur et tête à l'extérieur)

En cas d'alarme sur la partie Intrusion HISEC, le badge Maintenance est accepté et le lecteur ouvre la porte. Un accès direct aux Menus Intrusion est effectué par l'entrée directe sur le terminal du code Maintenance **Intrusion** ou Intervenant.

Le technicien de Maintenance peut par la touche ➔ avoir accès aux Menus de Maintenance (Contrôle d'accès) avec la priorité la plus basse (voir *Chapitre 1.6.6*) en cas d'alarme.

Si le mode Maintenance est autorisé par le Client le badge de Maintenance aura accès à tous les menus.

1.6.4 Badges Standards

Il n'existe pas de fonctions prédéfinies ou de droit de programmation pour les badges à usage normal. Les droits d'utilisation sont seulement dépendants du contenu de la base de données.

Un badge normal peut être individuellement bloqué ou complètement effacé du système. Un badge n'est pas accepté s'il est bloqué et sera seulement accepté si le blocage est supprimé. Quand vous effacez un badge, toutes les informations pour ce badge spécifique disparaissent, et celles-ci ne pourront pas être réutilisées à moins que vous ne les re-programmiez.

1.6.5 Badges Visiteurs

Un badge Visiteur est un badge normal appartenant au Groupe de Personnel N°1, auquel des conditions spéciales sont appliquées (automatiquement contrôlées par le lecteur) :

- § Un badge Visiteur est valide seulement pour une journée (le badge est automatiquement bloqué le jour même à 24:00 heures, s'il n'a pas déjà été bloqué manuellement).
- § Un badge Visiteur est toujours associé au Groupe de Personnel N°1 avec un Programme Horaire valide pour ce groupe.

Badges "carte de crédit" utilisés en badges visiteurs

Attention : cette fonction n'est utilisable que sur les lecteurs de technologie ***magnétique****.*

Toutes les "cartes de crédit" standard peuvent aussi êtres utilisées comme badges visiteurs à la place des badges HISEC. Cette possibilité ne doit pas être confondue avec l'utilisation des badges "cartes de crédit" pour ouvrir la porte des "sas bancaires" (groupe de personnel 250), voir description au Chapitre 2.2 de la présente notice.

Les badges visiteurs sont toujours pré-programmés pour utiliser les droits d'accès définis par le groupe de personnel N° 1 et ne doivent pas êtres changés. La totalité des badges visiteurs "cartes de crédit" et badges HISEC utilise le groupe de personnel N° 1.

Avant d'utiliser les "cartes de crédit" comme badges visiteurs, il est nécessaire de les avoir définies au moyen du *Menu 23*. Un badge visiteur est automatiquement bloqué après la fin de journée (24:00) mais les "cartes de crédit" peuvent être effacées avant cela par le *Menu 24*. Les badges visiteurs ne sont pas seulement bloqués à 24:00 heures mais effacés. Il est aussi possible de créer un programme hebdomadaire qui sera associé au groupe de personnel N° 1, utilisé pour bloquer les badges visiteurs.

Pour créer et effacer des badges visiteurs "carte de crédit" un niveau de priorité 1 (ou supérieur) est nécessaire.

1.6.6 Badges de Programmation et Priorité des Badges

Les badges de Programmation sont soit des badges maîtres, badges de Maintenance ou des badges Normaux avec des priorités de programmation.
Un badge de Programmation donne accès aux informations du système, à la possibilité de programmer un nouveau système, et aussi à la création, blocage et effacement des badges. Un badge de programmation est généralement donné au responsable de la sécurité, gestionnaire du système ou réceptionniste.
Les droits sont déterminés par la priorité attribuée au badge (*Menu 57*) ou par le numéro du badge (badge Maître, badge Maintenance).

Priorité des badges

Un badge normal est toujours créé avec le niveau de priorité le plus bas (0) et ne peut pas être utilisé pour la programmation, mais seulement pour des opérations courantes sur le système.
Un niveau plus élevé peut être attribué au badge en utilisant le *Menu 57* "*Edition des Badges de Programmation*".
Un badge de Maintenance a des droits prédéfinis et ne peut pas être créé. Tous les badges de Maintenance ont les mêmes droits.

Les priorités de programmation disponibles sont les suivantes :

- Aucune priorité.....(priorité 0) ..... Utilisateur normal
- Usage limité .....(priorité 1) ..... Réceptionniste
- Programmation limitée.....(priorité 2) ..... Gestionnaire de badges
- Programmation totale .....(priorité 3) ..... Responsable de la sécurité

La différence entre ces 4 priorités est la suivante :

Fonctions	Priorités 0	1	2	3	Maintenance autorisée	Maintenance non autorisée	Maintenance non autorisée & Alarme
Passage normal de la porte	J	J	J	J	J	ú	J
Edition des messages (10)	ú	J	J	J	J	ú	ú
Gestion des badges visiteurs (20-24)	ú	J	J	J	J	ú	ú
Fonction d'affichage (30-38)	ú	ú	J	J	J	ú	J
Programmation des badges (40-45)	ú	ú	J	J	J	ú	ú
Définition du système (50-57)	ú	ú	ú	J	J	ú	ú
Impression (60-64)	ú	ú	ú	J	J	ú	ú
Contrôle de la porte (70-73)	ú	ú	ú	J	J	ú	ú
Test (91-97)	ú	ú	ú	ú	J	ú	ú
Configuration système (81-86)	ú	ú	ú	ú	J	ú	ú

J = Oui **ú** = Non (50-57) = Numéro des menus Contrôle d'Accès HISEC.

Priorités des Badges de Maintenance:

Les badges de Maintenance peuvent avoir deux niveaux de priorité, dépendant du fait que le Client a autorisé ou non le mode Maintenance. Le badge Maintenance sera autorisé à entrer en session seulement en cas d'alarme, mais avec le niveau de priorité le plus bas de celui vu dans le tableau précédent. Si le Client a autorisé l'usage étendu du badge de Maintenance, il aura aussi accès aux fonctions de niveau élevé, et pourra entrer en session sur le lecteur sans condition d'alarme.

La priorité 2 sur les systèmes gérés par le logiciel PC A(I)MS:

La gestion du Contrôle d'accès par P.C. implique la redéfinition de la priorité des badges - dans le logiciel des lecteurs - . Si l'option "Mode de Programmation sur P.C." - Option 9 Menu 82- est validée, les badges avec une priorité 2 ne sont plus autorisés à éditer (programmer) ou effacer les badges directement sur les lecteurs.

Du fait de ce changement dans le "Niveau de priorité" pour le lecteur, les badges de programmation avec les priorités 1 et 2, peuvent être utilisés pour programmer les données présentes uniquement dans les lecteurs de badges, et non dans la base de données du P.C.

Avec ce nouveau niveau de priorité, le porteur du badge est habilité à:

- Bloquer / Valider les badges
- Visualiser et prendre en compte les alarmes
- Visualiser l'historique local des lecteurs de badges.
- Visualiser les badges programmés et le statut des badges
- Gérer les badges visiteurs.
- Envoyer les messages

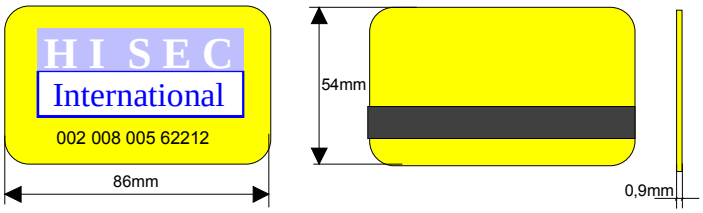
Ces fonctions sont suffisantes à l'utilisation quotidienne du système, si le "responsable de la sécurité" n'est pas disponible.

Remarque: Les fonctions des badges de Priorité 3 ne sont pas changées.

1.6.7 Description et caractéristiques des Badges

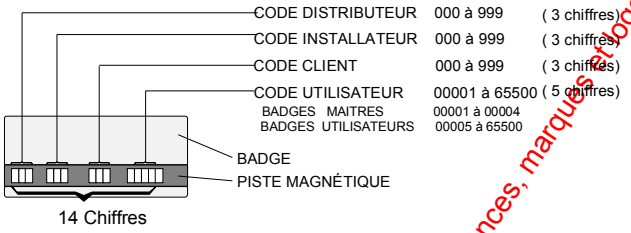
1.6.7.1 Badges magnétiques Encryptés et non-Encryptés

Dimensions



Badges encryptés au format HISEC

En standard les badges sont encryptés (pour des raisons de sécurité) avec les données suivante:



Badges Non-encryptés au format HISEC:

Le système HISEC peut utiliser des badges non encryptés, dans ce cas les badges pourront être communs à d'autres systèmes (gestion de cantine, etc.).

Il est recommandé d'utiliser des badges magnétiques à haute Coercivité (3000ø), qui donne au badge une résistance maximum aux champs magnétiques extérieurs.

En standard la piste 2 est utilisée et les données sont spécifiées avec une densité de 3 bits/mm (75 bits/inch) et suivant les spécifications ISO 7810 et 7811/2 et 4 avec le format suivant :

N° code BCD	*Spécification*
	Clock pour bit de synchro
1	Code de début: 11010
2	Code DISTRIBUTEUR (centaines)
3	Code DISTRIBUTEUR (dizaines)
4	Code DISTRIBUTEUR (unités)
5	Code INSTALLATEUR (centaines)
6	Code INSTALLATEUR (dizaines)
7	Code INSTALLATEUR (unités)
8	Code CLIENT (centaines)
9	Code CLIENT (dizaines)
10	Code CLIENT (unités)
11	N° du BADGE (dizaines de milliers)
12	N° du BADGE (milliers)
13	N° du BADGE (centaines)
14	N° du BADGE (dizaines)
15	N° du BADGE (unités)
16	Code séparateur 10110 (=)
17	N° du BADGE (dizaines de milliers)
18	N° du BADGE (milliers)
19	N° du BADGE (centaines)
20	N° du BADGE (dizaines)
21	N° du BADGE (unités)
22	Code de STOP 11111

Attention: Ce format impose d'initialiser le lecteur avec le format de badges Magnétique non-encrypté HISEC (BFORM=05).

Nota: Dans ce mode le lecteur acceptera aussi les badges normaux (encryptés).

Badges Non-encryptés Non au format HISEC:

Le système HISEC peut utiliser des badges non encryptés qui ne sont pas au format standard, dans ce cas les badges pourront être très simples et utilisables par la plupart des distributeurs de badges.

Prière de remarquer qu'il est toujours nécessaire de posséder un badge maître et un badge service standard HISEC (encryptés) pur pouvoir initialisé le lecteur et définir le code site utilisé.

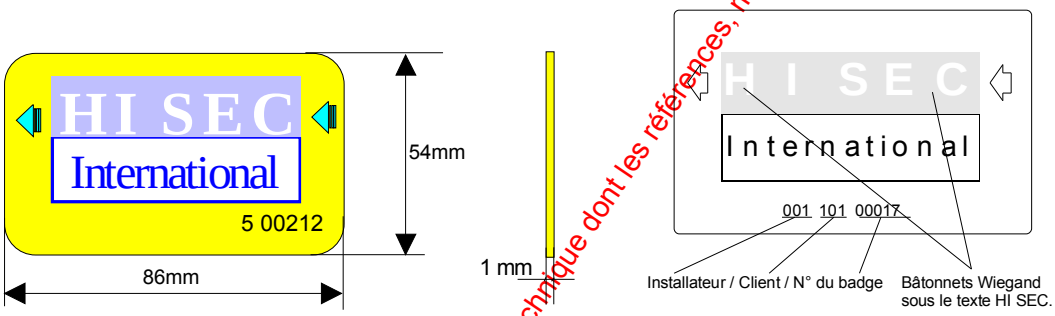
Les badges devront être encodés au format ISO avec les caractéristiques suivantes:

Caractère	Valeur	Description
1	B (hex)	Caractère de départ
2-4	1-999	Code site (client)
5-6	0	Caractères ignorés
7-11	5-65500	N° du Badge
12	D (hex)	Caractère de fin (obligatoire)

Attention: Ce format impose d'initialiser le lecteur avec le format Magnétique BCD (BFORM=13).

1.6.7.2 Badges Wiegand

Dimensions



Badges Wiegand au format HISEC

Les badges Wiegand HISEC sont au format 40 bits avec la présentation ci-dessus. Un logo différent sur le badge pourra être demandé.

Chaque badge est codé avec les informations suivantes:

- Numéro d'installateur : 3 chiffres (max.: 127)
- Numéro de Client (site) : 3 chiffres (max.: 127)
- Numéro du badge : 5 chiffres

Sur les badges au format Wiegand il est impossible d'avoir un code distributeur. Le numéro de distributeur sera le même pour tous les badges et sera un numéro spécifique à HISEC. Chaque installateur se verra donner un numéro d'installateur pouvant autoriser la possibilité de 127 installations client maximum. Si plus d'installations doivent être effectuées par le même installateur, un nouveau numéro d'installateur lui sera attribué ainsi que des nouveaux badges maintenance.

La gestion des badges maîtres et maintenance reste la même que celle des badges à piste magnétique.

Badges Wiegand non au format HISEC

Le système HISEC peut utiliser des badges Wiegand qui ne sont pas au format standard, dans ce cas les badges pourront être très simples et utilisables par la plupart des distributeurs de badges.

Prière de remarquer qu'il est toujours nécessaire de posséder un badge maître et un badge service standard HISEC pour pouvoir initialiser le lecteur et définir le code site utilisé.

Les badges devront avoir un format compris entre 25 et 31 bits (pas de code distributeur) avec la description suivante :

Caractère	Valeur	Description
1	1	Caractère de départ
2-16	1-32767	N° du Badge
17-24	0	Code site (client)
25	5-65500	Parité paire pour Code site
26	D (hex)	Caractère de fin (peut être ignoré)

Ce tableau représente le codage pour un badge 26 bits, si le format utilise plus de bits ils devront être ajoutés au n° du badge, par contre le n° du badge devra être inférieur à 32767, au contraire le badge sera traduit en enlevant 32767 de son N° réel.

Attention: Ce format impose d'initialiser le lecteur avec le format de badges Wiegand 26 bits (BFORM=15).

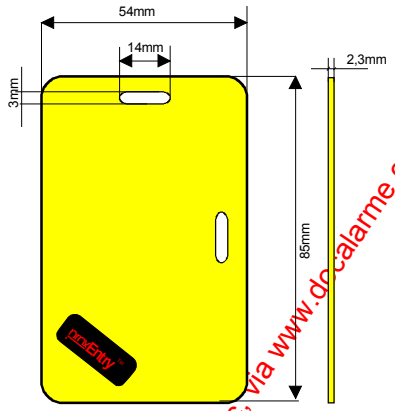
Il est également possible d'utiliser des badges avec la même description mais ayant le code client en début et le N° du badge ensuite (BFORM=16).

1.6.7.3 Badges Proximité et mains libres

L'utilisation de système "**main libre**" impose la gestion du franchissement simultané des portes par plusieurs personnes. Pour être sûr que tous les badges ont bien été pris en compte un "buffer" de 10 badges à été incorporée dans le logiciel. De ce fait un max. de 10 badges se présentant consécutivement à la même porte pourra être géré. Cette possibilité est aussi accessible aux autres technologies (magnétique, Wiegand).

Badges Passifs (DEISTER)

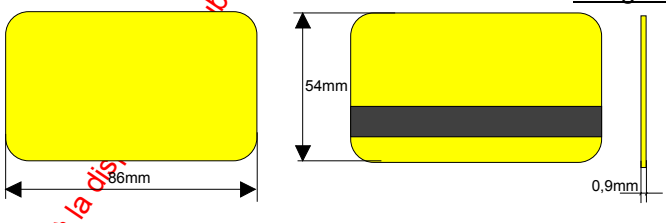
Badges Standard



Caractéristiques complémentaires
Température de fonctionnement : -25 à +60°C
Fréquence : 125 kHz

$ Pour les distances de lectures se reporter directement à la description des têtes de lectures.

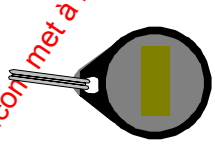
Badges ISO



Caractéristiques complémentaires
Température de fonctionnement : -25 à +60°C
Fréquence : 125 kHz

$ Pour les distances de lectures se reporter directement à la description des têtes de lectures.

Badges Clé



Caractéristiques complémentaires
Dimensions : ∅ 35mm x 6 mm
Température de fonctionnement : -25 à +60°C
Fréquence : 125 kHz

$ Pour les distances de lectures se reporter directement à la description des têtes de lectures.

1.6.7.4 Badges Codes à barres infrarouges

HISEC ne fourni pas en standard les badges Codes à barres infrarouges, par contre le système est compatible avec ces badges pour pouvoir utiliser les badges existants chez le client.

Types de codes barres infrarouges acceptés (**Max. 16 caractères**):

Code 39, 2 parmi 5, Codabar, UPC-A, UPC-E, EAN, Code 11, Code 93, Code 128, MSI.

Attention : Ces têtes de lecture ne peuvent pas lire les codes à barres contenant des caractères alphabétiques.

Il est impératif de toujours effectuer un essai sur un échantillonnage de badges du client avant de commencer toute opération dans cette technologie.

$ Pour plus amples renseignements sur cette technologie se reporter directement à la description des têtes de lectures (chapitre XX).

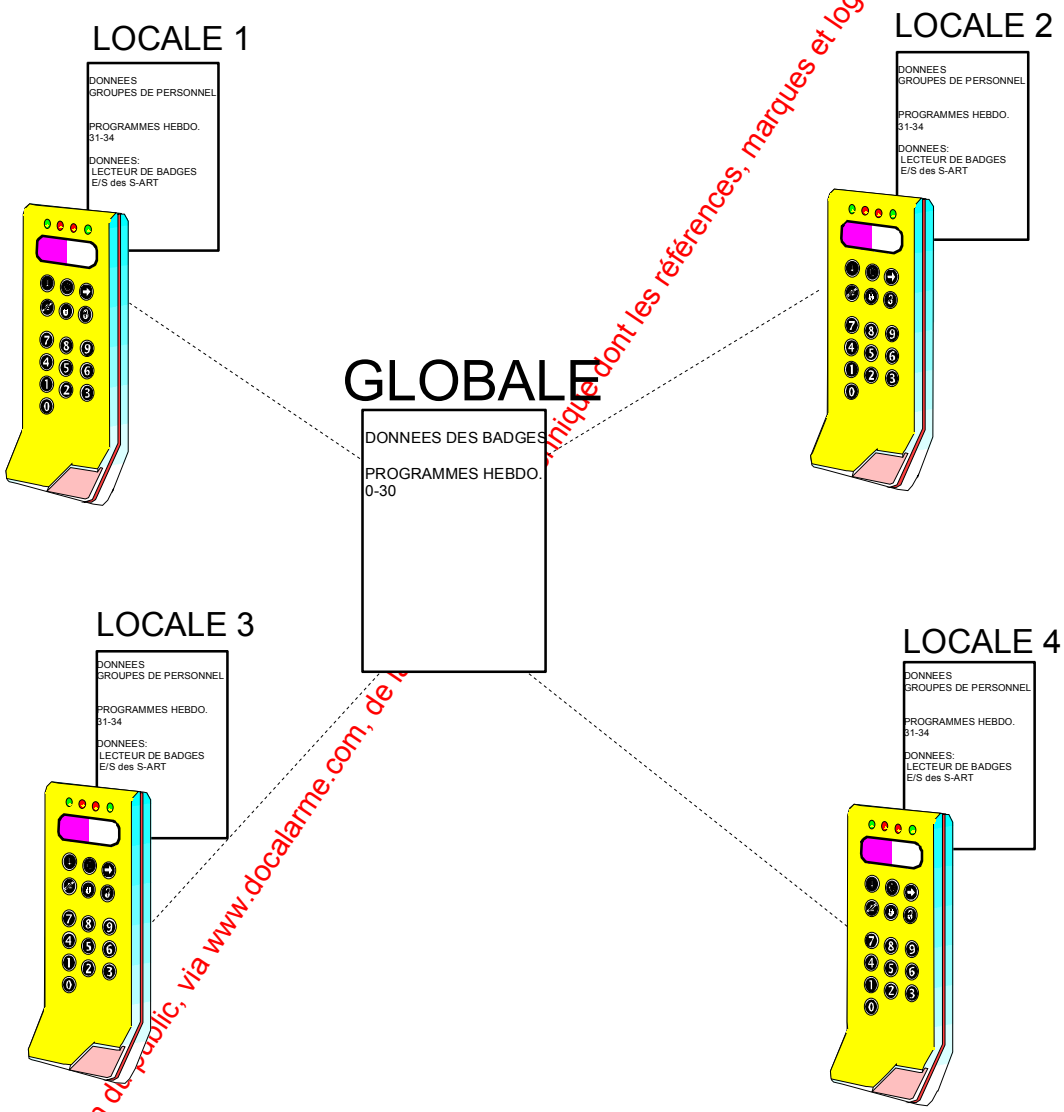
1.7 La Base de Données (Database)

Le concept du système est basé sur une intelligence distribuée. Toutes les informations et données ayant trait au Contrôle d'Accès et à la programmation sont logées dans chaque lecteur.

La base de données des lecteurs HISEC est divisée en 2 parties distinctes, une base de données commune (globale) pour tous les lecteurs et une locale qui peut être différente pour chaque lecteur. Dans la base de données locale, sont logés les informations sur les groupes de personnel, les Programmes Hebdomadaires du N° 31 à 34, les programmations d'entrées/sorties des S-ART et les données des badges du lecteur.

La base de donnée locale doit être programmée dans chaque lecteur mais il est aussi possible de faire une copie d'un lecteur vers l'autre.

Dans la base de données globale, sont logés toutes les informations sur les données des badges et les Programmes Hebdomadaires n°0 à 30.



La programmation globale de la base de données ne sera pas possible sur un système multilecteurs, si le message « PAS DE COMMUNIC » est affiché, étant donné que la base de données globale est distribuée à tous les lecteurs.

Les relations entre les différentes parties de la base de données sont représentées, ci-dessous, et des explications détaillées seront données plus avant dans cette notice.

Base de données des badges:
Numéro de badge
Code Personnel
Priorité
Etat
Zone Anti-Retour
N° de Groupe de Personnel

Base de données des Groupes de Personnel:
N° d'utilisateur HISEC Intrusion
Fonction de verrouillage ? Oui/Non
Code Contrainte ? oui / non
Enregistrement des accès normaux ? Oui/Non
N° de Programme hebdomadaire

Programme hebdomadaire (00 à 30) :
Conditions d'accès:
Lundi

Dimanche
Conditions d'accès:
Jour spécial 1
Jour spécial 2

Données du lecteur de badges : En dehors des informations relatives aux bases de données des badges, on doit aussi définir quelques variables, qui spécifient les fonctions générales du lecteur. Ces paramètres sont définis dans le menu "MODE & OPTIONS" programmé durant l'initialisation :

Lecteur :	
	Autonome
	Intégré à l'Intrusion HISEC
	Système Multilecteurs
Badges :	
	Format des Badges
Options :	
1	**Code Personnel à 4 ou 6 chiffres**
2	**Réaction locale ou globale sur alarme**
3	**Contrôleur externe de la porte**
4	**Imprimante locale/intrusion**
5	**Impression au fil de l'eau**
6	**Lecteur standard ou mode tête déportée**
7	**Badges encryptés ou non encryptés**
8	**Historique Badge + Code**
9	**Exploitation du système par PC (AMS ou AIMS)**
10	**Encryptage des communications RS 485**
11	**Contact de porte**
12	**Changement Heure d'été/hiver**
13	**Inter verrouillage**
14	**Porte forcée gérée**
15	**Imprimante sur Bus 00**
16	**Gestion des ouvrants**

Nota: Dans les *Menus* présentés sur l'afficheur du Lecteur de Badges le terme "DATABASE" a été préféré à celui de "BASE de DONNEES" pour des raisons de taille à l'affichage.

1.7.1 Base de Données des Badges

La base de données des badges comprend toutes les informations spécifiques pour les badges individuels.

Le lecteur HISEC peut contenir une quantité de badges allant jusqu'à 12000 badges en format HISEC et 4000 badges en format libre.

La base de données des badges contient par badge les informations suivantes :

Numéro du badge
Code Personnel
Etat
Priorité
Zone d'Anti-Retour
Groupe de personnel

Le champ **Numéro de badge** comprend le numéro inscrit sur le badge, et est utilisé en relation avec son emplacement dans la base de données pour les recherches.

Le champ **Code Personnel** est le code que l'utilisateur doit taper pour entrer en mode programmation, ou dans le cas où la libération de la porte a été validée avec un Code Personnel.

Le champ **Etat** comprend les 2 informations suivantes :

Bloqué/Non Bloqué
N° de message

Si le bit **Bloqué** est valide, le badge sera rejeté dans tous les cas. L'utilisation de cette fonction est utile par exemple en cas de perte d'un badge.

Le **Numéro de message** précise le N° du message standard qui doit être présenté au prochain usage du badge.

Le champ **Priorité** attribue des droits de programmation à certains badges spécifiques. Pour savoir quels Menus peuvent être utilisés et par quelle priorité, se reporter au *Chapitre 1.6.6*.

Le **Numéro de zone d'Anti-Retour** précise dans quelle zone d'anti-retour le badge est au moment donné.

Le champ **Numéro de Groupe Personnel** identifie le Groupe de Personnel auquel les utilisateurs appartiennent, et par ce moyen les droits d'accès auxquels sont liés les badges.

1.7.2 Base de Données des Groupes de Personnel

Un Groupe de Personnel est une association logique groupant des badges, lesquels ont accès à des conditions spécifiques d'accès, droits et attributions de fonctions.

Chaque unité Lecteur de badges HISEC pourra avoir un nombre maximum de 250 différents Groupes de Personnel.

Le **Groupe de personnel N°1** est prédéfini pour les badges Visiteurs avec des conditions d'accès et des droits spéciaux.

Le **Groupe de personnel N°250** est prédéfini pour la fonction utilisation des cartes bancaires en fonction "sas bancaire".

La base de données des Groupes de Personnel comprend par Groupe de Personnel les informations suivantes:

N° de Programme Hebdomadaire (00 à 30)	(PH)
Fonction de Verrouillage (entrée session HISEC) ? Oui/Non	(AS)
Code Contrainte ? Oui/Non	(HU)
N° de Code Utilisateur Intrusion HISEC	(CU)
Enregistrement des Accès Normaux ? Oui/Non	(TE)

Le champ **Numéro de Programme Hebdomadaire** définit quel programme horaire est applicable aux Groupes de Personnel (droits d'accès définis 24 heures par jour, 365 jours par an).

Le champ **Fonction de Verrouillage** (ou entrée en session HISEC) indique si le porteur d'un badge sur un lecteur donné a le droit d'armer/désarmer ou de programmer le système d'intrusion. Les droits de programmation et la définition des zones en relation avec le système d'intrusion sont programmés dans le système d'intrusion lui même, et cette information n'est pas stockée dans la base de données du lecteur.

Les fonctions de verrouillage peuvent aussi être utilisées dans des configurations sans intégration à un système d'Intrusion. Dans ce cas les deux touches "cadenas" peuvent alors servir pour verrouiller ou déverrouiller le lecteur (fonction "Premier entré / Dernier sorti"). Voir Chapitre 4.2.11

Le champ **Code Contrainte** est utilisé pour définir, si une action doit être faite en cas où l'utilisateur utilise le code Contrainte à la place de son Code Personnel normal. Généralement le code Contrainte est défini comme le Code Personnel +1. L'utilisation du code Contrainte activera une sortie spécialement dédiée et enverra un message à la centrale d'Intrusion HISEC.

Le champ **Numéro de Code Utilisateur Intrusion** HISEC indique quel code identifie les Groupes de Personnel en relation avec le système d'Intrusion HISEC, permettant ainsi la connexion avec les territoires qui peuvent être armés/désarmés par un badge appartenant à ce Groupe de Personnel.

Le champ **Enregistrement des Accès Normaux** définit si on doit - ou ne pas - enregistrer le fait qu'un utilisateur appartenant à un groupe de personnel donné a réalisé un accès et un passage normal de la porte. Si la fonction NON a été choisie, seules les exceptions seront enregistrées

1.7.3 Programmes Horaires Hebdomadaires

Les programmes horaires sont utilisés en relation avec les restrictions horaires ou autres restrictions, pour un ou plusieurs Groupes de Personnel, et sont en relation avec les conditions du lecteur lui même.

Un Programme Hebdomadaire consiste en des limitations de temps pour tous les jours de la semaine, et deux jours spéciaux. Chaque jour du Programme Hebdomadaire peut être scindé en 8 périodes horaires maximum, et une fonction pour chaque période peut être définie.

Une période horaire consiste en un "début" vers une "fin" de période exprimée en heures et minutes, et indique la période où la permission est octroyée (ou la fonction permise). Par exemple une plage de limitation de temps du lundi au vendredi de 08:00 à 16:00 H. Toute tentative en dehors de cette plage sera rejetée, le badge sera refusé et l'événement enregistré dans l'historique du lecteur HISEC.

Les plages horaires peuvent seulement être programmées par pas de 10 minutes, et il n'est pas nécessaire de définir les 8 plages horaires par jour. Par contre toute période horaire devra commencer à 00:00 H et se terminer obligatoirement à 24:00 H pour chaque jour programmé.

Les différents numéros des programmes horaires hebdomadaires sont prédéfinis pour des applications variées, et quelques définitions standards sont aussi prédéfinis.

Les explications des Programmes Hebdomadaires prédéfinis sont les suivantes :

N° Programme horaire Hebdomadaire :

0: Pas d'accès
1: Accès permanent (24h/24) **avec** Code Personnel
2: Accès permanent (24h/24) **sans** Code Personnel
3-30: Droits d'accès pour les Groupes de Personnel avec des fonctions programmables
31: Définition des Enregistrements pour le lecteur
32: Programme hebdomadaire pour les types logiciels d'entrée 76
33: Programme hebdomadaire pour les types logiciels d'entrée 77
34: Programme hebdomadaire pour la libération de la porte associée au lecteur.

Les programmes Hebdomadaires 0 à 30 (grisés) sont utilisés pour définir les droits d'accès des Groupes de Personnel, ils sont **globaux** et définissent la partie commune à tous les lecteurs.

Les programmes 31 à 34 sont **locaux** pour chaque lecteur où ils ont été programmés.

Programme horaire Hebdomadaire N° 3 - 30 :
Une des fonctions suivantes peut être allouée à la période horaire :

00 Pas d'accès
01 Accès **avec** Code Personnel
02 Accès **sans** Code Personnel
03 Fonction de bascule **avec** Code Personnel
04 Fonction de bascule **sans** Code Personnel
05 Fonction AIR **avec** Code Personnel
06 Fonction AIR **sans** Code Personnel

FONCTION 3:

Fonction bascule **avec code Personnel**. La lecture d'un badge avec cette fonction, après l'entrée du code personnel, ouvre la porte en permanence, jusqu'à ce qu'un autre badge avec la fonction bascule soit lu sur le même lecteur. La porte reviendra alors à sa position de repos (fermée). A la fin de la période "bascule", si aucun badge n'a été lu entre temps, le programme horaire remettra la porte dans son mode de fonctionnement normal (porte fermée en principe), dans le cas ou la porte serait bloquée en position ouverte une alarme porte maintenue sera générée et la porte restera ouverte.

FONCTION 4:

Fonction bascule **sans code Personnel**. La lecture d'un badge avec cette fonction "bascule" ouvre la porte en permanence, jusqu'à ce qu'un autre badge avec la fonction bascule soit lu sur le même lecteur. La porte reviendra alors à sa position de repos (fermée). A la fin de la période bascule, si aucun badge n'a été lu entre temps, le programme horaire laissera la porte dans son état (ouverte en principe).

FONCTIONS 5 & 6:

Fonctions avec activation du module de comparaison photo, voir document spécifique 92001901.

Programme horaire Hebdomadaire N° 31 (définition des enregistrements) :
Une des fonctions suivantes peut être allouée à la période horaire :

10..... Pas d'enregistrement
11..... Enregistrement des alarmes seulement. Dans ce cas l'historique local ne contiendra que les alarmes locales.
12..... Enregistrement de tous les événements excepté les passages de porte
13..... Enregistrement de tous les événements excepté les passages de porte sans utilisation du Code Personnel
14..... Enregistrement de tous les événements excepté les limitations définies dans la base de données des Groupes de Personnel
15..... Tout enregistrer

Programme horaire Hebdomadaire N° 32 et 33:
Une des fonctions suivantes peut être allouée à la période horaire :

20..... Type logiciel d'entrée 76/77 inactif
21..... Type logiciel d'entrée 76/77 actif

Programme horaire Hebdomadaire N° 34 :
Une des fonctions suivantes peut être allouée à la période horaire :

30..... Ouverture permanente (libération) de la porte pendant la période horaire spécifiée.
31..... Fermeture permanente (blocage) de la porte pendant la période horaire spécifiée.
32..... Fonctionnement normal de la porte pendant la période horaire spécifiée.
33..... Utilisation Code Personnel sans badge (voir chapitre suivant).

Les programmes horaires hebdomadaires comprennent des limitations horaires pour tous les jours de la semaine (7) et les jours spéciaux (2). Le jour de la semaine est généralement déterminé par l'horloge avec calendrier incorporée, mais si le jour est défini comme un jour spécial alors le jour de la semaine est déterminé à partir de celui spécifié dans la liste de jours de congés.

La fonction "DIGICODE"

La fonction 33 permet d'utiliser le clavier du lecteur comme un "digicode", l'entrée d'un code à **6 chiffres** ouvrant la porte pendant la période définie.

Le nombre maximum de codes différent est de **100**.

Par défaut, ce programme utilise des pseudo-badges compris en 1000 et 1099.

Les 2 premiers chiffres du code sont le numéro du badge 00 à 99 et les 4 derniers chiffres, le code personnel (4 chiffres) associé au badge.

Ne pas oublier que la validation d'un code type "digicode" répond aux mêmes procédures qu'un badge classique c'est à dire, association d'un groupe de personnel valide, puis d'une plage horaire (01 à 30) et d'un utilisateur intrusion - si système intégré.

Ex: Création d'un code personnel **322856**

- Créez le badge 1032 *(Menu 41)* avec un groupe de personnel valide, dans une plage horaire active pendant le programme de type "digicode".
- Entrez directement pendant la plage "digicode" le code **322856**.
- Le Lecteur demande Le **N**ouveau **CODE** : tapez **2856**
- Le lecteur redemande le **N**ouveau **CODE** : retapez **2856**
- Le code est enregistré, la porte s'ouvre.
- Les fois suivantes tapez **322856** directement

Le changement du code personnel (4 derniers chiffres) s'effectue de la même façon que pour un badge, par contre le changement des 2 premiers chiffres impose la création (et l'effacement éventuel) d'un badge compris entre 1000 et 1099.

La fonction "digicode" n'empêche pas l'utilisation des badges pendant sa période d'activité.

Attention : Ce programme est prioritaire sur l'entrée d'un code Intrusion, c'est pourquoi, si ce programme est utilisé sur un lecteur configuré en mode tête déportée (option 6 = 1), pendant cette période, il sera impossible de rentrer directement un code intrusion.

Nota : l'Offset qui est de 1000 par défaut est uniquement modifiable avec le logiciel A(I)MS.

1.7.4 Liste de Jours de Congés

Une liste de jours de congés est une liste de jours, par exemple vacances, avec des restrictions spécifiques. Pour chacune des dates de la liste des jours de congés, un type spécifique de jour est assigné (jour de la semaine -1 à 7- ou jour spécial -8 & 9-), avec lequel sera forcée la période d'accès à cette date spécifique.

1.7.5 Base de Données du Lecteur de Badge

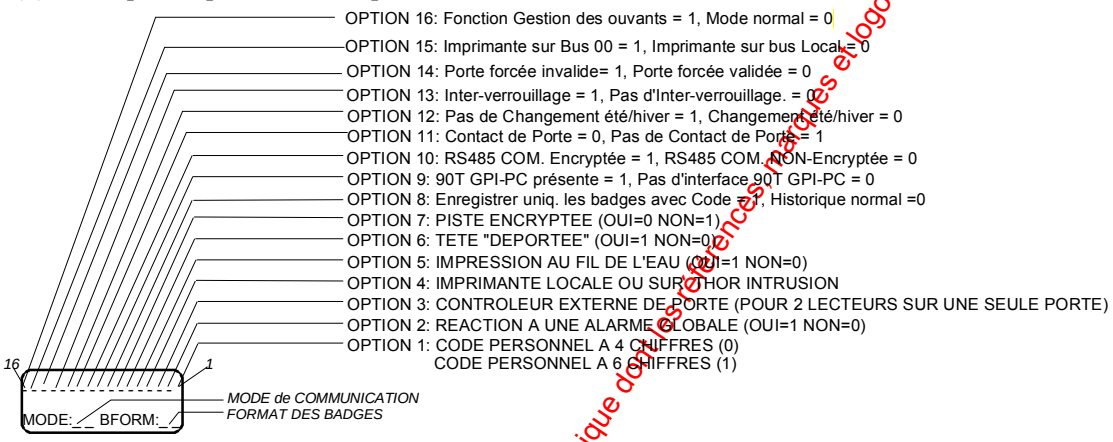
Pour chaque lecteur, il est possible de choisir différentes **Options**. Le choix de ces différentes Options est .généralement fait durant la phase d'Initialisation où les paramètres "MODE" et "OPTION" sont demandés au clavier.

Les 2 premiers chiffres sont pour le "MODE" du lecteur qui peut être :

Mode 00: Lecteur non initialisé
Mode 01: Lecteur en mode Autonome
Mode 02: Système Multi-lecteurs
Mode 03: Lecteur intégré à HISEC Intrusion

<u>Remarque</u>: Les Modes 02 et 03 peuvent cohabiter sur la même installation, cela permet de définir des lecteurs n'ayant pas le droit à l'intrusion et d'autres oui. Par ex. Pour des lecteurs placés à l'extérieur.

Chacun des 16 paramètres de la liste des OPTIONS représente une option qui peut être sélectionnée (1) ou non (0). Les options pouvant être spécifiées sont les suivantes :



- <u>Option 1:</u> **Code Personnel Contrôle d'accès (Badge + Code) à 4 ou 6 chiffres.**

  0 = 4 chiffres
  1 = 6 chiffres

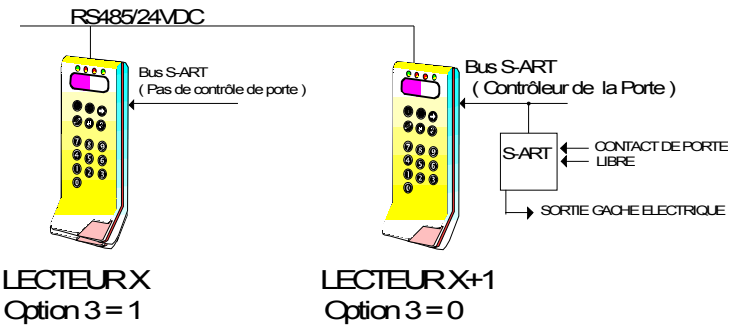
- <u>Option 2</u> : **Le type de réaction Locale ou Globale.**

  0 = Si une réaction locale a été choisie seules les alarmes du Lecteur concerné pourront être incorporées dans les équations d'alarme.

  1 = Si une réaction globale a été choisie les alarmes venant de tous les lecteurs pourront être utilisées dans les équations d'alarme SI/ALORS.

- <u>Option 3:</u> **Lecteur en Entrée/Sortie.**

  Deux lecteurs sont utilisés pour gérer la même porte et contrôler les entrées/sorties, un des lecteurs doit être sélectionné comme étant le lecteur ne gérant pas la porte. L'autre lecteur - avec une adresse supérieure d'un - contrôlera alors la porte par l'intermédiaire de son bus S-ART. Le lecteur externe commandera la porte en passant d'abord par le bus RS 485 vers le lecteur de contrôle, qui lui exécutera la commande de porte par le bus S-ART.



0 = Contrôleur local de la porte (par défaut)
1 = Contrôleur externe à la porte.

• Option 4: **Imprimante Accès ou sur le système intrusion HISEC.**

1 = Les impressions se feront sur une imprimante connectée directement sur le système d'intrusion HISEC.

0 = Les impressions se feront sur imprimante spécialement dédiée au Contrôle d'Accès.

• Option 5: **Impression à la demande ou au fil de l'eau.**

1 = L'impression aura lieu en temps réel (fil de l'eau).

0 = L'impression aura lieu à la demande (impression de l'historique du lecteur).

• Option 6: **Lecteur avec tête de lecture déportée.**

Attention ! Ce choix de mode de fonctionnement ne décide pas seulement si la tête est incorporée au contrôleur mais plutôt le type de d'exploitation en fonction du type d'installation:

0 = Mode Standard

1°) Système Autonome ou Multilecteurs : Fonctionnement normal (pas d'intrusion).

2°) Système Intégré : Le lecteur ouvre la porte uniquement si le territoire de l'opérateur est désarmé (ou part.armé). L'action de désarmement est fonction de l'option du groupe de personnel. Pour les groupes ne possédant pas cette option, ils doivent attendre le désarmement pour franchir la porte.

1 = Mode Tête déportée

1°) Système Autonome ou Multilecteurs : Le mode tête déportée permet de filtrer les signaux et de n'afficher que les messages essentiels étant donné que la tête de lecture n'est pas au même endroit que le terminal.

2°) Système Intégré : Le lecteur ouvre la porte uniquement aux groupes de personnel ayant la possibilité de désarmer (quel que soit l'état du territoire armé, désarmé ou part.armé). L'armement (et le désarmement) se fera de la même façon que sur un terminal standard intrusion (code à 6 chiffres sans badges uniquement). Les groupes ne possédant pas l'option d'armement/désarmement doivent attendre le désarmement de leur territoire pour franchir la porte.

• Option 7: **Utilisation Badges HiSec Non-encryptés.**

Le système HISEC peut utiliser des badges non encryptés (en standard les badges sont encryptés pour des raisons de sécurité) dans ce cas les badges pourront être communs à d'autres systèmes (gestion de cantine etc.).

0 = Badges Encryptés. 1 = Badges Non Encryptés.

Si le lecteur est autorisé à accepter les badges non encryptés il acceptera aussi les badges normaux (encryptés). Les badges ***Maîtres*** *et* ***Maintenance*** *sont toujours encryptés quelque soit le système choisi.*

• Option 8: **Enregistrer dans l'historique uniquement les badges nécessitant un code personnel.**

0 = Les programmes hebdomadaires et les groupes de personnel décident quels sont les badges qui sont enregistrés dans l'historique (mode de fonctionnement standard).

1 = Seules les entrées de portes ayant nécessité l'entrée du code personnel sont enregistrées dans l'historique des événements, et ceci même si le programme hebdomadaire d'enregistrement des historiques (programme hebdomadaire N° 31) est utilisé avec d'autres fonctions.

La définition de l'historique de chaque groupe de personnel ne pourra modifier les badges qui sont enregistrées dans l'historique.

• Option 9: **Exploitation du contrôle d'accès par logiciel PC A(I)MS** (*voir Chapitre 1.6.6*).

0 = Pas d'interface 90T GPI PC présente sur le bus RS 485.

1 = Interface 90T GPI PC présente sur le bus RS 485.

• Option 10: **Encryptage des communications sur le bus RS 485.**

0 = Communication non-encryptée (mode standard).

1 = Communication encryptée (attention: ce mode impose que tous les éléments du bus soit dans ce mode - U.C intrusion, interfaces PC-Imprimante).

• Option 11: **Prise en compte des entrées des badges sur les portes**.
Cette option permet de programmer à quel moment l'entrée d'un badge sera prise en compte (historique, imprimante et PC).

0 = La prise en compte de l'entrée d'un badge se fera à l'ouverture de la porte (par défaut).
1 = La prise en compte est faite après la lecture du badge même sans ouverture de porte. Cela pourra être utilisé dans les installations où il n'est pas possible d'installer de contact de porte, mais où l'enregistrement des transactions de badges est nécessaire.

Nota: Il est possible d'utiliser cette option même si le lecteur gère un contact de porte.

• Option 12 : **Changement automatique Heure d'été/hiver**
Cette option permet de valider le passage automatique d'heure d'été/hiver. Par ce paramètre il est possible de bloquer ou de valider le passage automatique de l'heure d'été/hiver en accord avec les règles européennes au printemps et à l'automne.

0 = Changement automatique
1 = Pas de changement automatique.

• Option 13: **Inter-verrouillage des portes (sas)** (voir Chapitre 3.9).
0 = La fonction inter-verrouillage n'est pas activée, par contre la fonction de contrôle de 2 portes par le lecteur est toujours possible

1 = La fonction inter-verrouillage est activée (voir description au *chapitre 3.8*).

• Option 14: **Sortie sans utilisation d'un bouton poussoir**
0 = Une alarme porte forcée sera générée si la porte est ouverte sans la lecture d'un badge valide ou l'appui sur le bouton poussoir de sortie (par défaut).

1 = Le lecteur ne provoquera pas d'alarme porte forcée. La porte peut être ouverte directement pour sortir (pas de bouton poussoir de sortie nécessaire). Si la porte est ouverte trop longtemps une alarme porte maintenue sera générée.

*Attention : Ne pas confondre cette option de sortie avec **l'Option N°11** qui indique elle la prise en compte de l'entrée d'un badge sur une porte.*

• Option 15: **Imprimante sur Bus principal 00 ou sur le Sous-Bus**
0 = le lecteur utilisera une imprimante dédiée sur son propre sous-bus (par défaut).
1 = Il est possible au lecteur d'un sous-bus d'utiliser l'imprimante présente sur le Bus maître (00) comme imprimante au fil de l'eau (événements et alarmes).

Attention : Il n'est pas possible d'imprimer la programmation, etc. sur un autre Bus. L'utilisation des menus 61 à 64 n'est possible que sur une imprimante présente sur le même bus.

Nota: Cette fonction ne pourra être utilisée sur nombre de portes important qu'avec un trafic réduit ou en utilisant des filtres dans les lecteurs (programme hebdomadaire 31) de façon à ne pas surcharger le bus RS 485 sur le Bus 00. (Le logiciel BUSSTAT peut vous indiquer l'occupation du Bus RS 485).

¤ Option 16: Validation de la fonction Contrôleur Portes blindées (gestion des ouvrants).
0 = Lecteur en mode standard.
1 = Lecteur avec des fonctions Gestion des ouvrants, le lecteur garde ses fonctions contrôle d'accès et intrusion (si existantes).

La Notice du lecteur fonctionnant en gestion de ouvrants est disponible sous forme d'un document séparé "Gestion des Ouvrants" réf. 18-006-09F.

1.8 Enregistrement dans l'Historique

Le système de Contrôle d'Accès HISEC peut enregistrer tous les événements, par exemple : franchissement d'une porte, alarmes et utilisation du système. L'enregistrement contiendra le nom de l'événement, son type, l'heure de l'événement et le numéro du badge.

2 types d'historiques sont disponibles :

- **Historique Local** contenant tous les événements y compris les alarmes. Ce mode local est valide seulement pour les événements du lecteur contenant l'historique.
- **Historique Global** des alarmes contenant tous les événements définis comme alarmes. Ce mode global est réservé aux alarmes et est commun à tous les lecteurs connectés sur le bus.

1.8.1 Historique Local - Tous les événements -

Tous les événements sont successivement numérotés et sont stockés cycliquement dans le tampon du lecteur HISEC (max. 2300 événements). En cas de dépassement, les plus anciens (premiers de la pile) seront effacés par réécriture. Cet historique est local et est propre à chaque lecteur.

Différents types de filtres pour l'historique sont disponibles dans le lecteur. Ils sont définis au moyen des Programmes Horaires et/ou des Groupes de Personnel.

Ces filtres donnent la possibilité de limiter le nombre d'événements sans intérêt enregistrés dans l'historique réduit considérablement les temps de recherches et les manipulations inutiles pour les anciens événements.

Toutes les alarmes seront également stockées dans un historique séparé -Global-.

Prière de se référer au *Chapitre 4 "Exploitation"* pour avoir la liste complète des événements pouvant être stockés dans l'historique.

1.8.2 Historique Global - Alarmes -

Toutes les alarmes sont stockées dans un historique séparé d'une capacité maximum de 100 alarmes. Cet historique est commun à tous les lecteurs. Toutes les alarmes locales pourront aussi être visualisées dans l'historique des événements.

Les événements suivants peuvent être enregistrés dans l'historique des alarmes :

Evénement	Paramètres 1	Paramètres 2
Utilisation du code Hold-Up	N° de badge	N° lecteur
Sabotage du lecteur	N° lecteur	
Sabotage de S-ART	N° de S-ART	N° lecteur
Ouverture forcée de porte	N° lecteur	
Porte maintenue	N° lecteur	
Défaut batterie	N° lecteur	
Défaut système	N° de défaut	N° lecteur
Défaut secteur d'une heure	N° lecteur	
Système d'Intrusion externe en alarme	N° de S-ART	N° lecteur
Utilisation d'un badge bloqué	N° de badge	N° lecteur
Utilisation d'un badge invalide	N° de badge	N° lecteur
Mauvais Code Personnel (10 fois)	N° de badge	N° lecteur
Base de données changée	N° lecteur	
Utilisation d'un badge Maintenance	N° de badge	N° lecteur
Coupure d'alimentation	N° lecteur	
Initialisation système	N° lecteur	

Pour chaque événement, l'heure et la date seront consignées.

Si le lecteur est intégré au système d'Intrusion HISEC, les 2 types d'alarmes transmis en priorité à la HISEC CONTROLE D'ACCES seront "Alarme Hold-Up" et "Sabotage Clavier déporté". De plus, il est possible d'avoir un ou plusieurs types d'alarmes transmis comme "Alarme Lecteur" en utilisant les équations SI/ALORS en relation avec le type logiciel 99 (voir la description des types logiciels au *chapitre 1.5.2*).

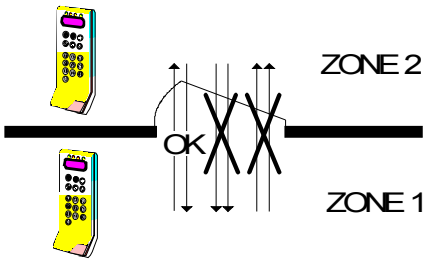
Il est aussi possible d'activer des sorties de S-ART avec une ou plusieurs des alarmes décrites au *chapitre 1.2*. Cela peut être utilisé pour une indication d'alarme locale ou pour interfacer le Contrôle d'Accès avec un système d'intrusion externe.

A l'installation, il est possible de décider quelles entrées/sorties du système réagiront sur une alarme locale seulement, ou sur n'importe quelle alarme transmise sur le bus RS485 vers l'historique des alarmes. Dans un système Multi-lecteurs, c'est par cette méthode seulement que l'on pourra interfacer UN lecteur avec un système d'alarme externe.

Si le lecteur est connecté à un système d'Intrusion HISEC, ou si un type logiciel d'entrée 36 a été défini (entrée d'alarme venant d'un système d'intrusion Non-HISEC) et que le système d'Intrusion soit en condition d'alarme, n'importe quel utilisateur du lecteur recevra un message d'alarme.

1.9 Anti-retour

Le logiciel des lecteurs possède de puissantes fonctions d'anti-retour. Le système de contrôle d'accès installé peut être divisé en un maximum de 16 zones (par BUS) avec des fonctions d'entrées/sorties par lecteur.



La définition d'un Anti-retour étant de contrôler si le porteur d'un badge est autorisé à effectuer les ouvertures successives de porte sans être ressorti au préalable. Cela permet d'interdire deux entrées (sorties) successives au même porteur du badge. L'on évite ainsi qu'un porteur de badge entré dans une zone surveillée ne prête son badge à un autre pour que celui-ci puisse entrer.

Jusqu'à 16 zones (par BUS) peuvent êtres crées, incluant la zone 000 qui représente "en dehors du système". Chaque lecteur est programmé avec la zone physique où il est placé et la zone à laquelle il donne accès.

Tous les lecteurs enregistrent dans quelles zones sont les badges au moment présent et comptent le nombre de badges présents dans chaque zone.

Installation

2 Installation

2.1 Les Lecteurs

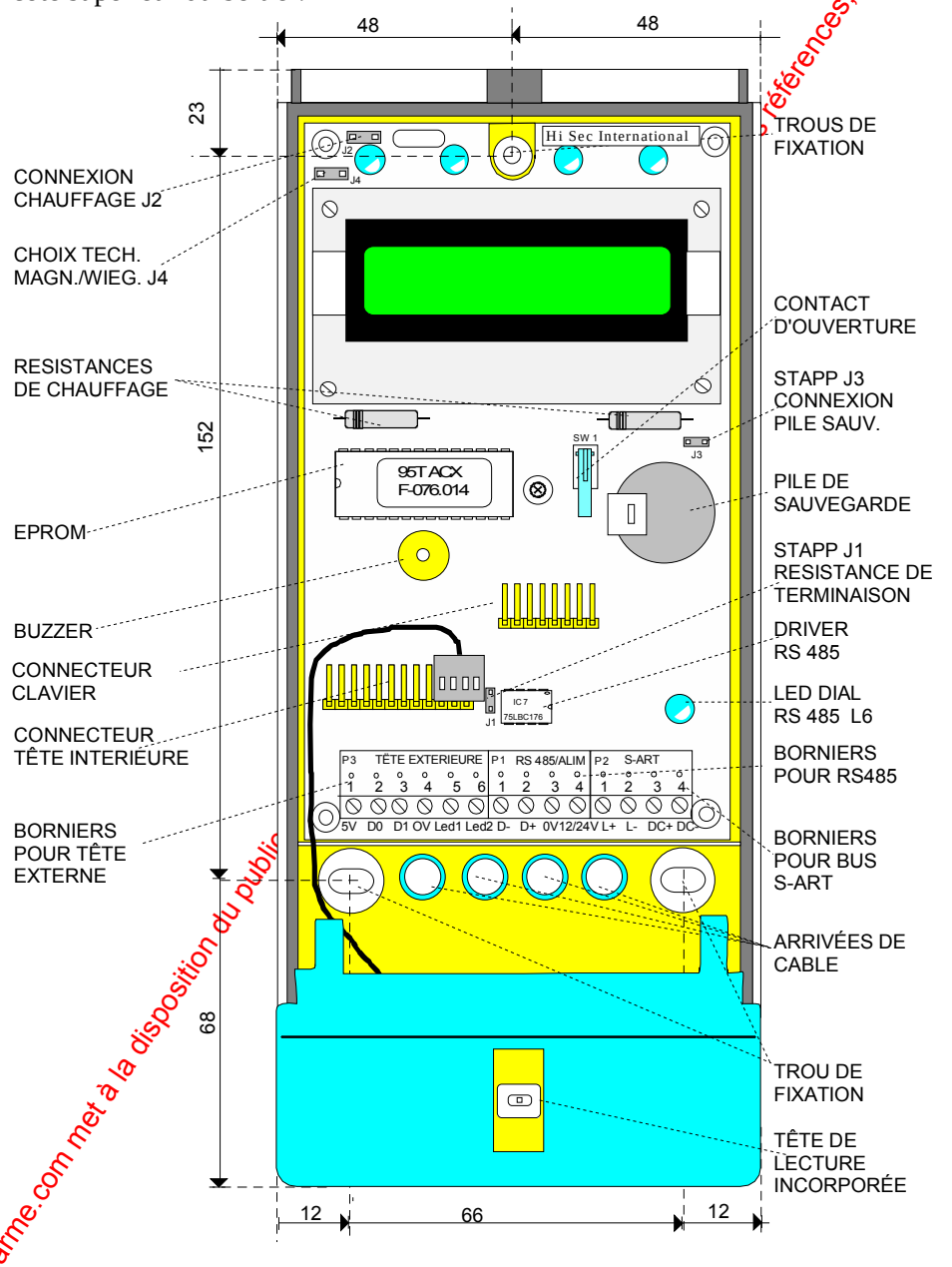
2.1.1 Dimensions Mécaniques et Disposition du lecteur Standard

L'unité Lecteur de badges s'ouvre en enlevant la vis de type I/n située au-dessus du boîtier. La vis doit être retirée sur environ 1 cm, ensuite le couvercle peut être séparé de la plaque de fond. Le câble plat reliant le clavier a la carte la carte processeur est débrochable de son support.

Après enlèvement de la partie avant du lecteur, le fond peut être fixée au mur avec 3 vis type M4 ou similaires. Les trous de fixations du clavier déporté et du lecteur de badges sont placés au même endroit.

Quand vous fixez la plaque de fond, il doit être pris en considération que le couvercle prend approximativement 3 mm d'espace en plus dans tous les sens par rapport à la surface de la plaque de fond. Pour le démontage, il est aussi nécessaire de prévoir un espace libre de 2 cm en dessous de l'unité lecteur de badges.

La hauteur de fixation recommandée pour les appareils est approximativement de 1m50 à 1m55 pour le côté supérieur du boîtier.



Caractéristiques:

Tension d'alimentation : 8,5-30 V Continu

Consommation (max.):
50 mA en 24V - 80 mA rétro-éclairage en marche
85 mA en 12V - 145 mA rétro-éclairage en marche
Avec chauffage :
Alim 28 V : 420mA
Alim 24 V : 360mA
Alim 12 V : 220mA

Longueur des câbles :
Bus RS485: max. 1200m écran, paire torsadée
Bus S-ART : max. 1000m sans écran, paire torsadée
500m écran, paire torsadée
Max: 15 Sart's (tous types sauf S-106)

Température de fonctionnement : -5°C à +60°C
Avec chauffage :
Alim 28V : -30°C à +60°C
Alim 24V : -25°C à +60°C
Alim 13,5V : -15°C à +60°C
Alim 8,5V : -10°C à +60°C

Sortie 5V Continu:
Mini 4V - Maxi 5,2V
Courant max. 200mA

Sortie S-art:
Mini 16,8V - Maxi 17,6V
Courant max. 60mA

Humidité 96% non condensée (IP 45)

Temps de sauvegarde pile (sans alim. DC): 400 jours à 50°

Température de stockage : -5°C à +60°C

Poids : 400 g

Nota : toutes les consommations sont données sans charge extérieure (S-art, tête, etc.).

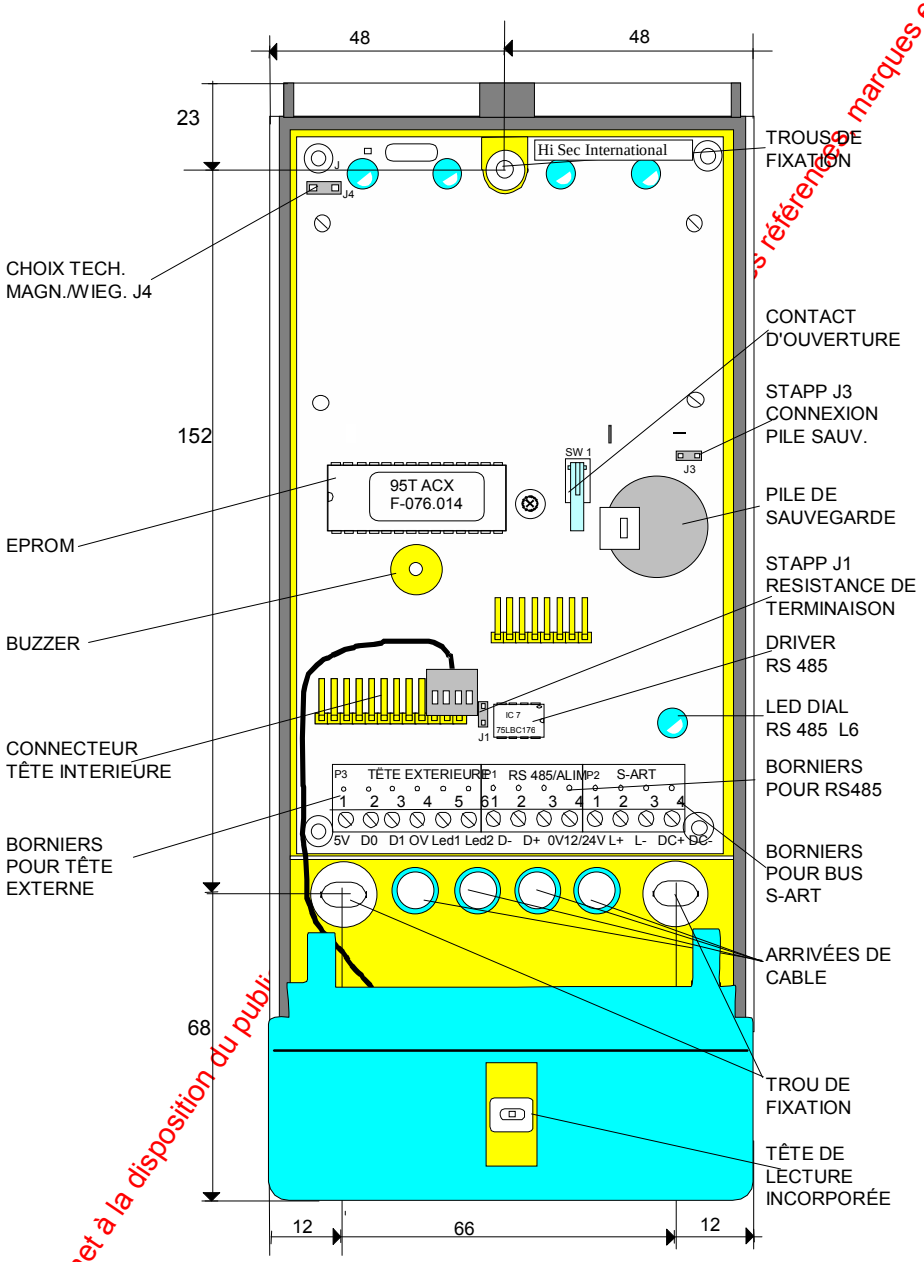
2.1.2 Dimensions Mécaniques et Disposition des lecteurs Compact et Style

L'unité Lecteur de badges s'ouvre en enlevant la vis de type I/n située au-dessus du boîtier. La vis doit être retirée sur environ 1 cm, ensuite le couvercle peut être séparé de la plaque de fond.

Après enlèvement de la partie avant du lecteur, le fond peut être fixée au mur avec 3 vis type M4 ou similaires. Les trous de fixations du clavier déporté et du lecteur de badges sont placés au même endroit.

Quand vous fixez la plaque de fond, il doit être pris en considération que le couvercle prend approximativement 3 mm d'espace en plus dans tous les sens par rapport à la surface de la plaque de fond. Pour le démontage, il est aussi nécessaire de prévoir un espace libre de 2 cm en dessous de l'unité lecteur de badges.

La hauteur de fixation recommandée pour les appareils est approximativement de 1m50 à 1m55 pour le côté supérieur du boîtier.



Caractéristiques:

Dimensions : H=234 L 95 P= 51 mm

Tension d'alimentation : 9-30 V Continu

Consommation (max.):
95T ACM S ou C
30 mA en 24V
50 mA en 12V

95T ACPS ou C
40 mA en 24V
65 mA en 12V

Longueur des câbles :
Bus RS485: max. 1200m écran, paire torsadée
Bus S-ART : max. 1000m sans écran, paire torsadée
500m écran, paire torsadée
Max: 15 Sart's (tous types sauf S-106) 1, seul pour compact

Température de fonctionnement : -5°C à +60°C

Sortie 5V Continu:
Mini 4V - Maxi 5,2V
Courant max. 200mA

Sortie S-art:
Mini 16,8V - Maxi 17,6V
Courant max. 60mA

Humidité 96% non condensée (IP 45)

Temps de sauvegarde pile (sans alim. DC): 400 jours à 50°

Température de stockage : -5°C à +60°C

Poids : 400 g

Nota : toutes les consommations sont données sans charge extérieure (S-art, tête, etc.).

2.1.3 Cavaliers de sélection sur la carte

Cavalier J1 : Terminaison bus RS 485. Voir *Chapitre 2.9 "Connexions du bus RS 485*".

Présent : résistance (220 Ω) connectée (fin de bus RS 485)

Enlevé : résistance (220 Ω) non connectée

Cavalier J2 : Connexion du circuit de chauffage (les résistances de chauffage sont incorporées au lecteur).

Attention ce strapp n'existe pas dans les lecteurs Compact et Style

Présent : résistance de chauffage connectée (appareil placé dans local non chauffé)

Enlevé : résistance de chauffage non-connectée (appareil placé en intérieur)

Le circuit de chauffage est utilisé pour protéger les appareils dans les basses températures. Son utilisation permet d'atteindre des températures allant jusqu'à -25°C.

Le rétro-éclairage de l'afficheur est automatiquement allumé quand la température descend en dessous de 10°C (+/- 10°). En même temps le circuit de chauffage est activé pour chauffer l'afficheur.

Cavalier J3 : Connexion de la pile de sauvegarde des données du lecteur.

Présent : La pile est connectée aux mémoires (les données sont sauvegardées)

Enlevé : La pile n'est pas connectée aux mémoires (les données sont perdues à la coupure de l'alimentation).

Cavalier J4 : Choix de technologie de la tête de lecture **Externe**.

Présent : La tête de lecture externe sera de type Magnétique.

Enlevé : La tête de lecture externe sera de type Wiegand (cette configuration sera aussi celle des têtes proximité, mains libres, codes barres infrarouges, etc.).

LED 6 : Indique que la communication RS 485 fonctionne et doit donner une luminosité clignotante ou presque persistante.

Attention: L'adresse du Lecteur est programmable par logiciel (voir Menu 82) dans les lecteurs standards et automatique dans les lecteurs Compact et Style.

2.1.4 Les connexions sur la carte

Borniers P1 : Raccordement BUS RS 485

N° BORNE	DESCRIPTION
1	Dialogue RS 485 (D-)
2	Dialogue RS 485 (D+)
3	Alimentation (0V)
4	Alimentation (+12/24V)

Borniers P2 : Raccordement BUS S-ART

N° BORNE	DESCRIPTION
1	Dialogue S-art (L+)
2	Dialogue S-art (L-)
3	Sortie Alimentation (+12/24V)
4	Sortie Alimentation (0V)

Borniers P3 : Raccordement Tête de lecture externe

N° BORNE	Configuration WIEGAND (voir nota)	Configuration MAGNETIQUE (voir nota)
1	Sortie Alimentation +5V (max. 200mA)	Sortie Alimentation +5V (max. 200mA)
2	Données (D0)	Données (Data)
3	Données (D1)	Horloge (Clock)
4	Sortie Alimentation 0V Référence dialogue	Sortie Alimentation 0V Référence dialogue
5	Commande Led 1 (max. 100mA)	Commande Led 1 (max. 100mA)
6	Commande Led 2 (max. 100mA)	Commande Led 2 (max. 100mA)

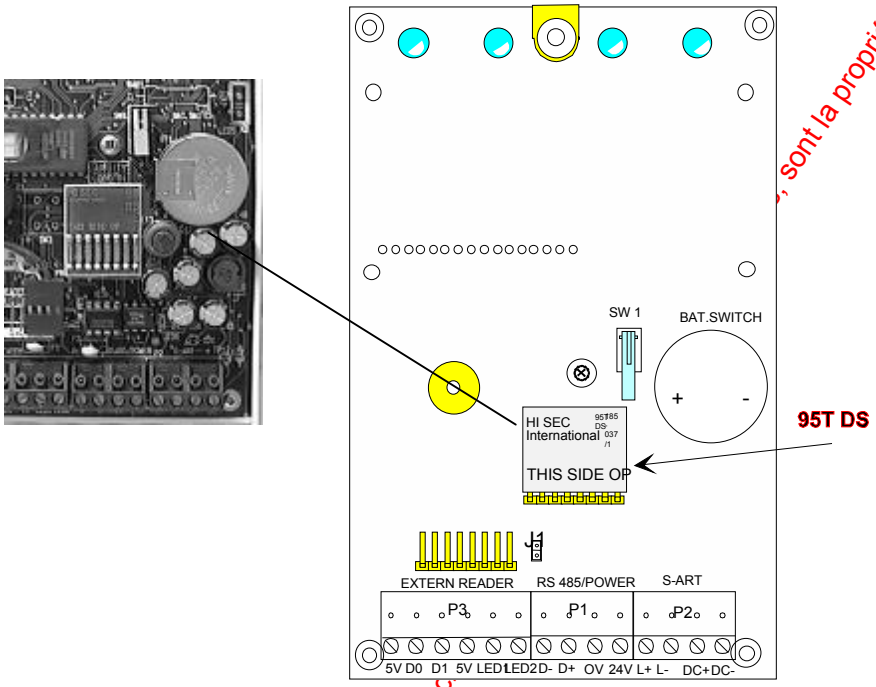
Nota : Le choix de la technologie de tête de lecture est fait au moyen du strapp J4 (voir chapitre précédent).

2.1.5 Procédure d'évolution

Les lecteurs **HISEC Compact** peuvent évoluer en **HISEC Style** en ajoutant simplement une petite carte «dongle» sur l'ancien connecteur du clavier des lecteurs classiques.

Instruction de montage du "dongle" 95T DS

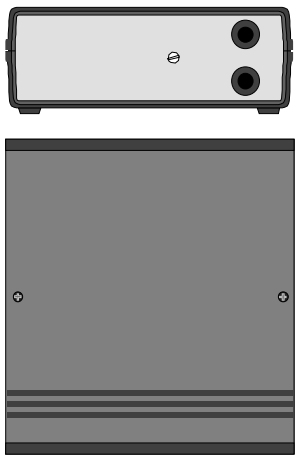
sur un lecteur Compact



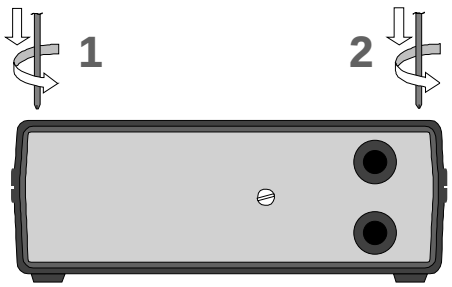
2.2 Les Interfaces GPI

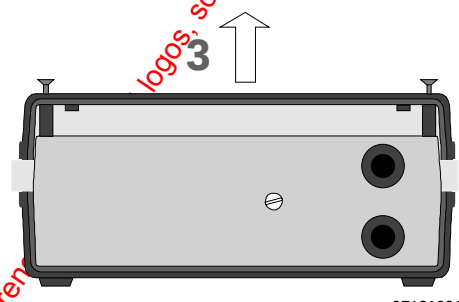
Disposition Mécanique

L'interface est en version standard, fournie en boîtier plastique auto-protégé à l'ouverture, elle assure l'interface entre le bus RS 485 et une sortie série RS232 (**Type 1**) ou entre le bus RS485 et un autre bus RS485 (**Type 2**).



97102306a

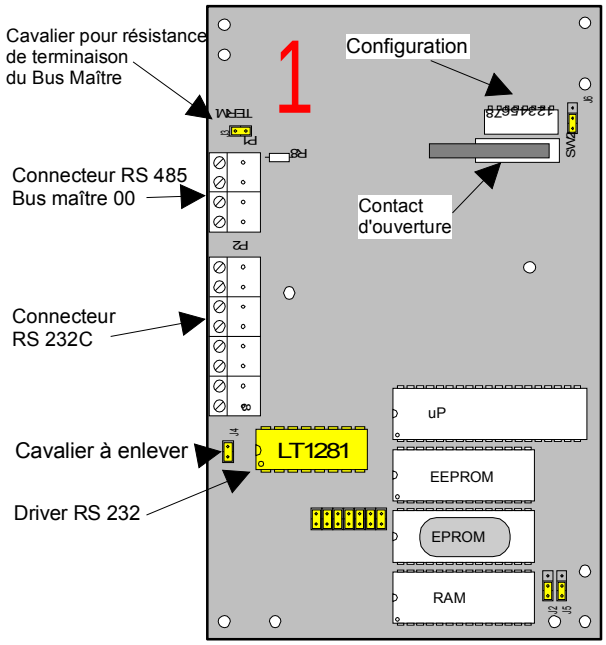




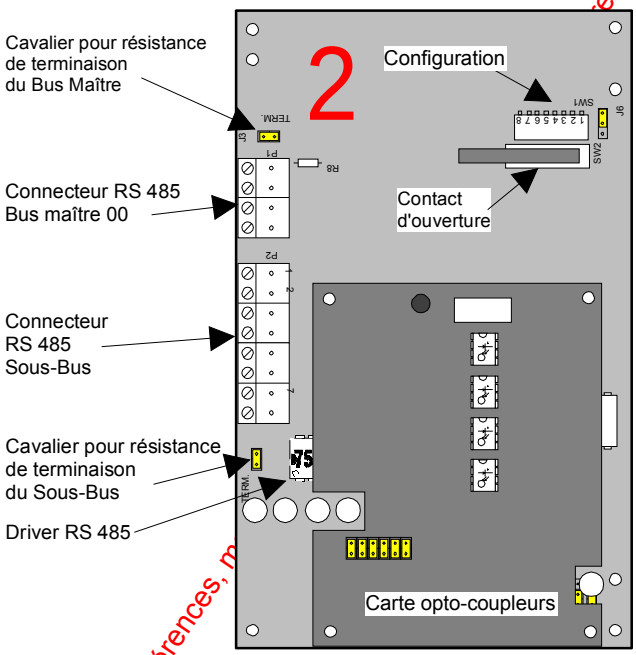
97121001a

Référence	Description	Type
95T GPI COM	**Suivant configuration assure les fonctions suivantes :**	
GPI PRI	Interface pour connexion d'une imprimante avec interface série RS232.	1
GPI PC	Interface pour connexion d'un PC, pour logiciel AIMS & AICS.	1
GPI MI	Interface pour raccordement de modems sur réseau public (RTC ou X 28).	1
GPI SECOM	Interface pour raccordement de transmetteur SECOM (SERIAL).	1
95T GPI COM IP	Interface pour connexion avec interface IP.	**3**
90T GPI BR	Interface pour l'interconnexion directe de bus RS 485 entre eux.	2
90T GPI DLC	Interface pour l'interconnexion d'un lecteur ou d'un bus RS 485 au moyen d'un câble direct (à utiliser conjointement à 90T GPI BR, sauf lecteur seul).	2
90T GPI DLM	Interface pour l'interconnexion de bus RS 485 au moyen de modem (ligne spécialisée) ou de support filaire (à utiliser conjointement à 90T GPI BRM).	1
90T GPI BRM	Interface pour l'interconnexion de bus RS 485 au moyen de modem (ligne spécialisée) ou de support filaire (à utiliser conjointement à 90T GPI DLM).	1
90T GPI DLM IP	Interface pour l'interconnexion de bus RS 485 au moyen d'un réseau IP.	3
90T GPI BRM IP	Interface pour l'interconnexion de bus RS 485 au moyen d'un réseau IP.	3

Disposition Mécanique

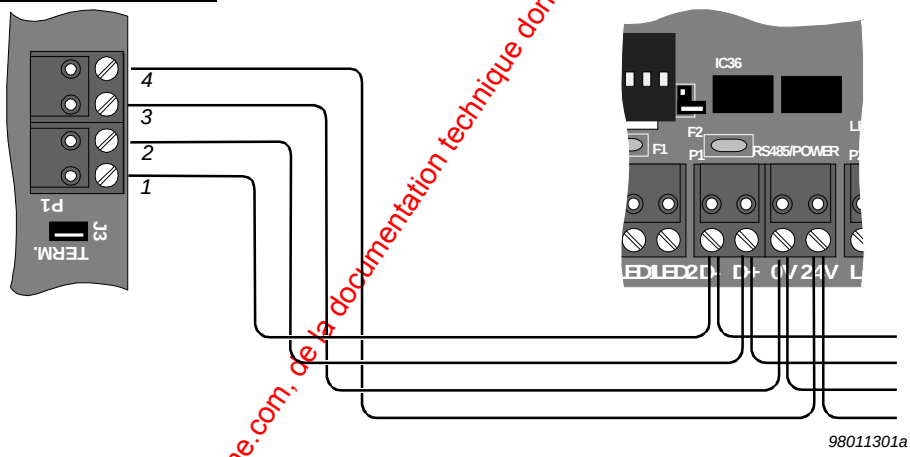


RS 485 ◄► RS 232



RS 485 ◄► RS 485

Raccordement au Bus RS 485 :



98011301a

Pour les connexions du bus RS485, se référer au *Chapitre 2.4* "*Raccordement du bus RS485*".

Montage dans un coffret d'alimentation 95T PS :

la carte peut être montée à l'intérieur du coffret d'alimentation 90T-PS en la démontant de son coffret.

Elle sera installée à l'intérieur du coffret d'alimentation au moyen de 4 vis (type M3) fournies avec le coffret. Avant de réaliser cela, il est nécessaire de fixer 2 supports dans ceux déjà existants pour donner la même hauteur aux 5 points de fixation.

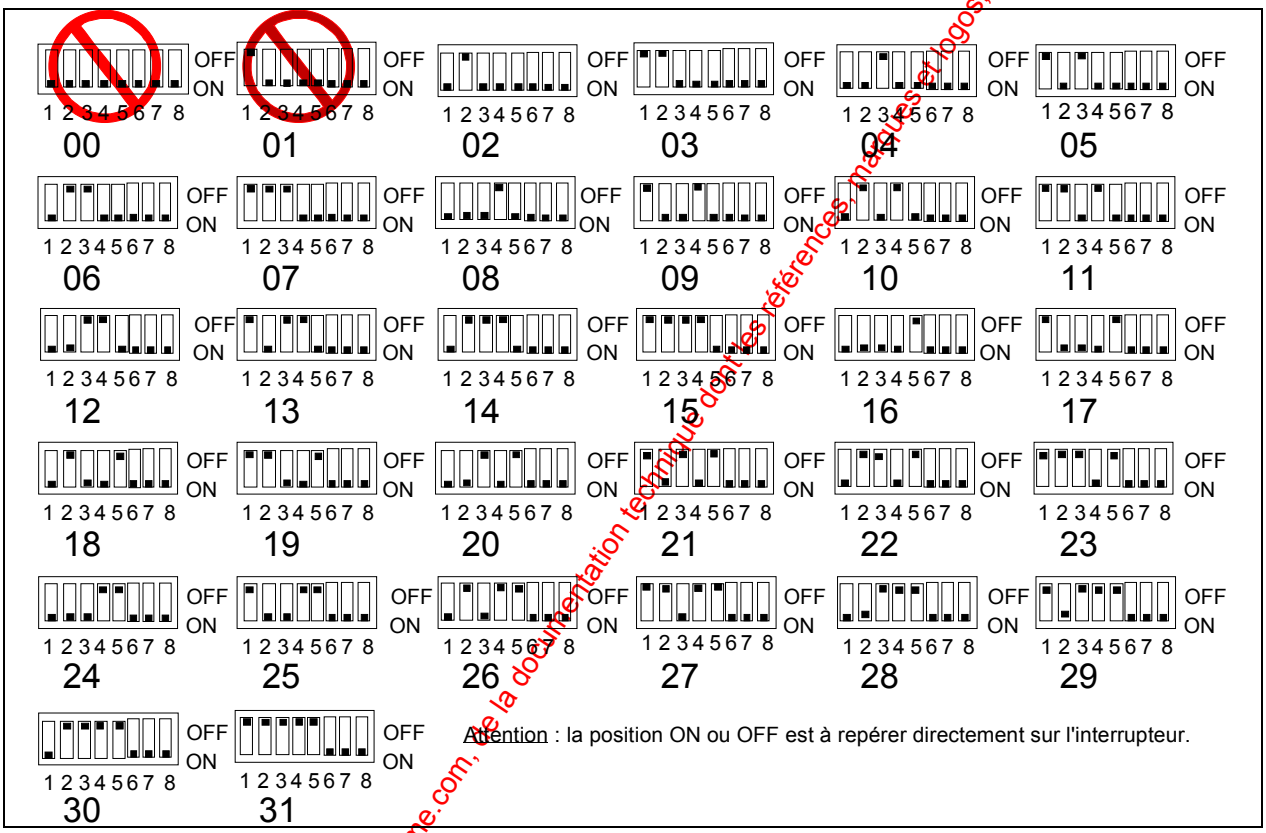
Après fixation, la carte interface peut être reliée au bus RS485 et la sortie RS 232 connectée.

Configuration des Interfaces GPI

Un dip-switch de 8 micro-interrupteurs (SW1) est utilisé pour configurer la carte (voir implantation sur les schémas précédents). Les 5 premiers micro-interrupteurs sont utilisés pour programmer l'adresse de chaque unité sur le bus.

Les interfaces GPI (comme tous les périphériques) devront être programmées à une adresse comprise entre 01 et 31 et bien sûr pas avec une adresse déjà existante (utilisée par les autres périphériques présents tels imprimantes, terminaux, lecteurs, carte INCOM, etc.).

Le maître du bus (Lecteur ou centrale intrusion) ayant toujours l'adresse 00 (et 01 pour UC Intrusion), ces adresses ne **pourront pas** être utilisées par l'interface GPI.



Les micro-interrupteurs **SW1/6** & **SW1/7** sont utilisés différemment suivant le type d'interface (voir les chapitres suivants).

SW1/8 : Encryptage des communications RS 485.

ON = Communication non-encrytée OFF = Communication encryptée

Il est possible de choisir si le système utilisera les communications encryptées (haute sécurité) ou un mode de transmission (RS 485) standard.

Attention: si le mode encrypté est choisi pour l'interface, tous les périphériques devront être dans le même mode.

Centrale intrusion : **Option 1 = 1** dans le *Menu 52* du logiciel de la centrale Intrusion.

Lecteurs Contrôle d'accès : **Option 9 = 1** dans le *Menu 82* du logiciel des lecteurs.

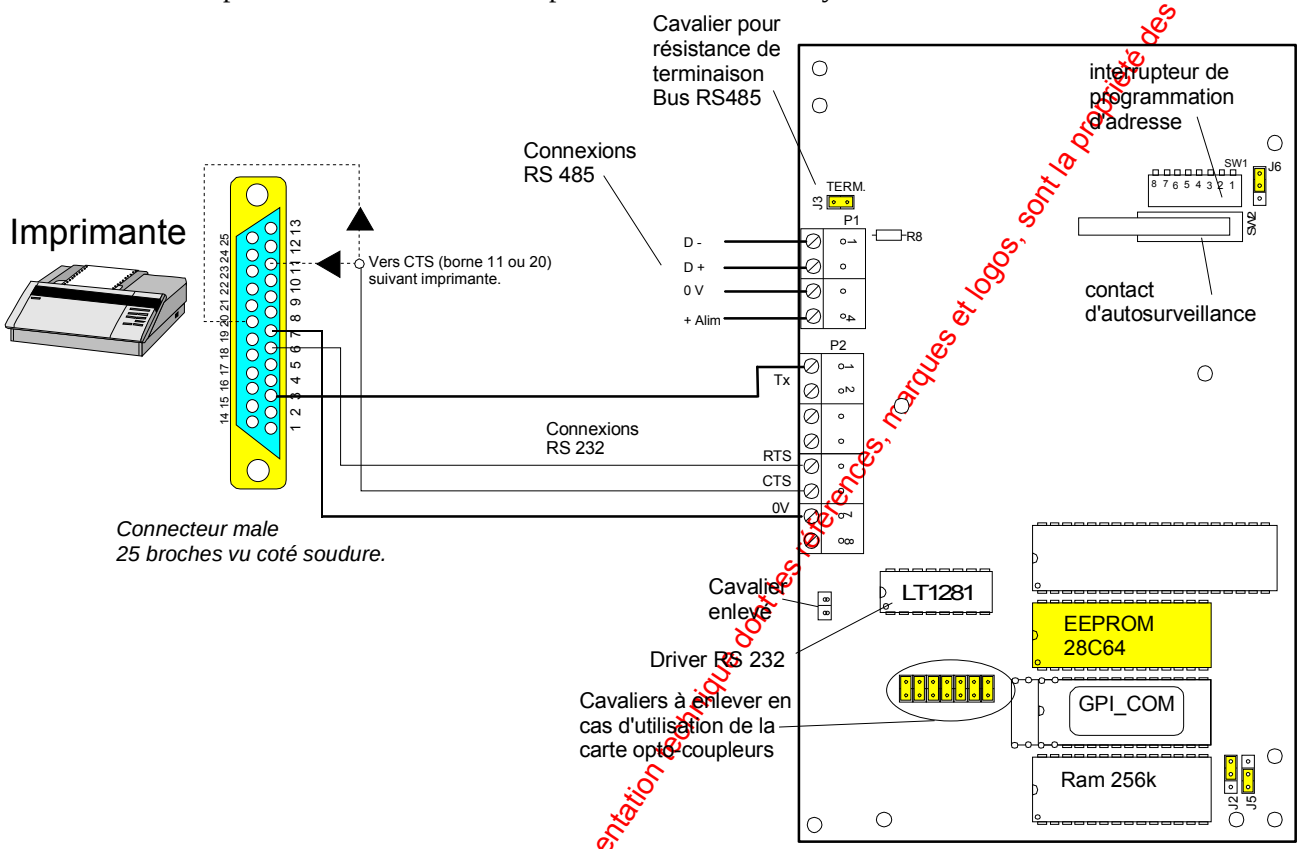
Nota: Quand l'interface est utilisée avec un seul lecteur (**Lecteur autonome**), celui ci devra avoir **l'adresse 00** et devra être initialisé par le *Menu 82* en **Mode 02**: système multi-lecteurs (et pas en mode 01: lecteur autonome).

2.2.1 L'interface 95T GPI COM

L'interface est de **Type 1** (voir schéma chapitre 2.3), l'EPROM sera de type 90T GPI COM.

2.2.1.1 Fonction GPI PRI

Cette interface permet de connecter une imprimante RS 232C au système HISEC.



Interrupteurs de configuration Interface :

Placer les interrupteurs en position suivante (**hors tension**):

SW1/6 = OFF et SW1/7 = OFF

L'imprimante peut être utilisée de deux façons : Intrusion ou Contrôle d'accès. Par défaut dans la configuration précédente l'imprimante est en fonction impression intrusion. La modification (**sous tension**) de la position l'interrupteur SW 1/6 permet de changer le mode de fonctionnement de l'interface imprimante.

SW1/6 : OFF ð ON = ACCES

SW1/6 : ON ð OFF= INTRUSION

Après ce changement il est nécessaire de déconnecter l'alimentation de l'interface et de remettre les interrupteurs dans leurs positions normales (SW1/6 & SW1/7 = OFF). A chaque nouvelle mise sous tension l'imprimante fonctionnera dans le mode (intrusion ou contrôle d'accès) que l'on a choisi au début.

Configuration de l'imprimante série:

- Vitesse de transmission	: 1200 bauds	- Nombre de bits	: 8
- Parité	: paire	- Nombre de bits d'arrêt	: 1
- Fin de ligne	: CR + LF	- Protocole	: Handshake matériel

La longueur du câble ne devra jamais dépasser 15 m.

Prière de se référer à la notice "MANUEL TECHNIQUE INTRUSION HISEC" pour les possibilités de l'interface imprimante dans les systèmes Intrusion.

2.2.1.2 Fonction GPI PC

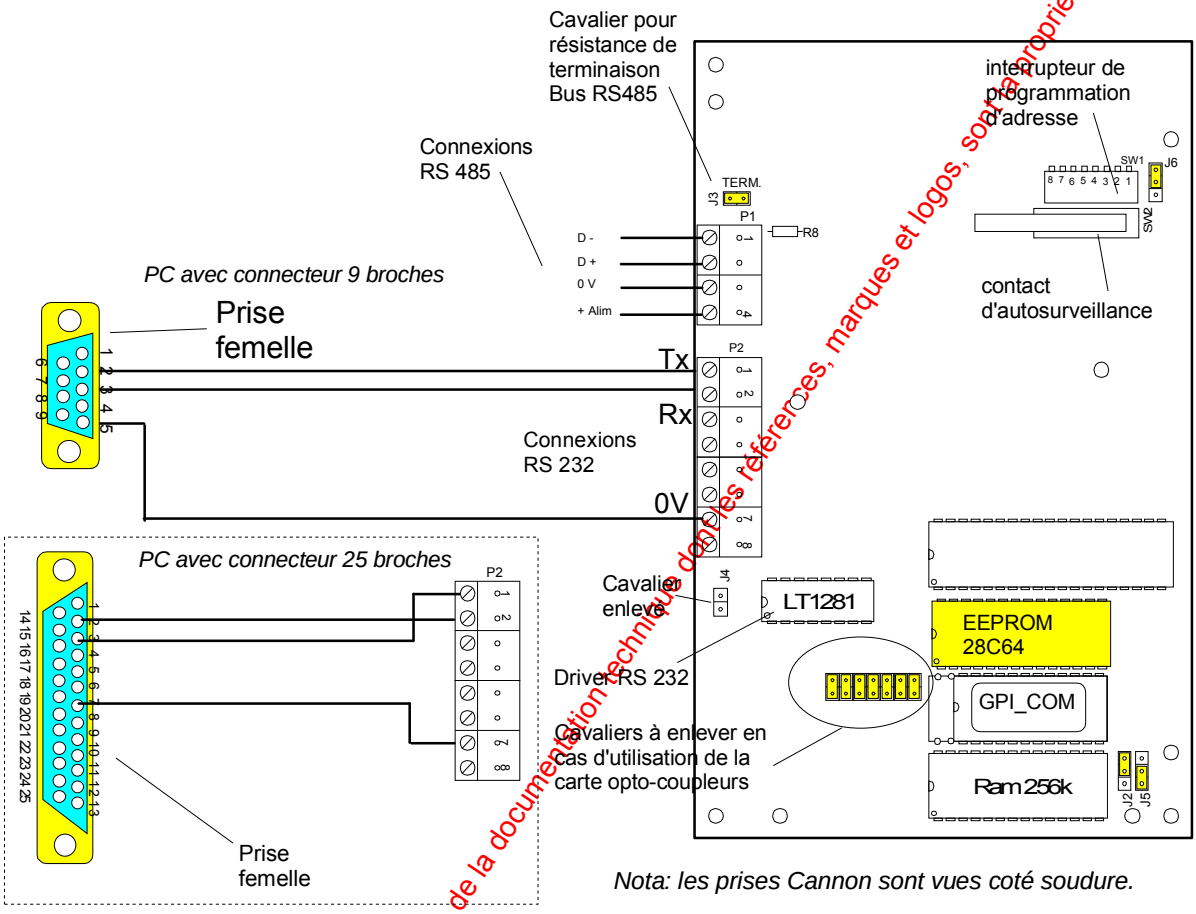
Cette interface permet de connecter le PC au système HISEC.

Interrupteurs de configuration :

Placer les interrupteurs en position suivante (**hors tension**):

SW1/6 = ON et SW1/7 = ON

La figure ci-dessous représente l'interface 95T GPI PC et les raccordements nécessaires.



Nota: les prises Cannon sont vues coté soudure.

L'interface GPI PC est toujours connectée au Bus 00 (maître).

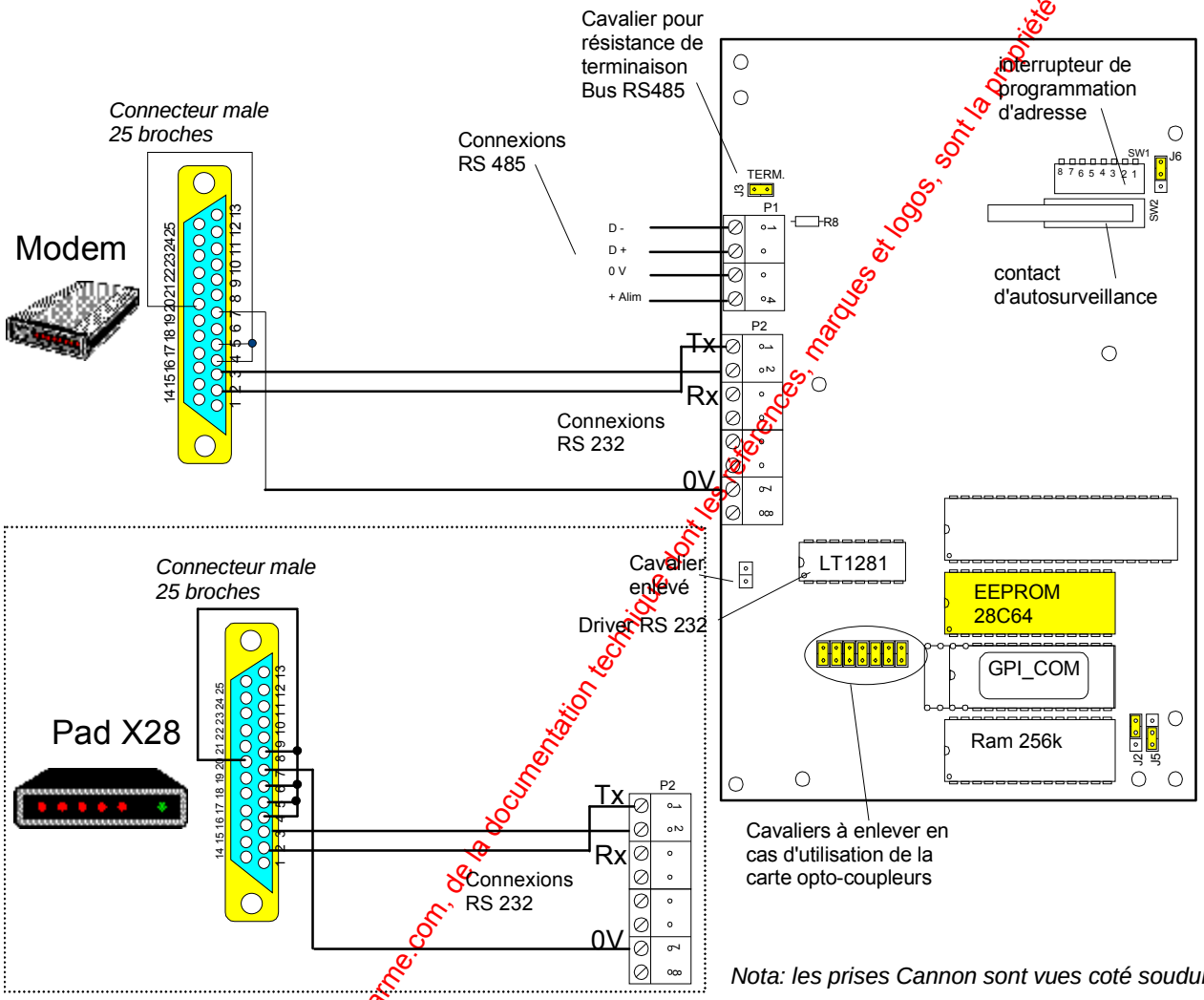
Remarque ! La majorité des PC utilisent pour les communications RS 232 une prise CANNON 9 points, au cas contraire on devra prévoir un adaptateur 9 points ⇒ 25 points ou câbler selon le schéma du bas de la figure ci-dessus.

Attention ! La longueur du câble RS 232 ne devra pas dépasser 15m.

2.2.1.3 Fonction GPI MI

La carte 95T GPI MI permet de gérer les modems (ou PAD) dans les configurations du type logiciel accès distant (AIMS M). Cette carte utilise un circuit EEPROM ou sont mémorisés les paramètres du modem (chaîne d'initialisation, N° de téléphones, etc.), ces paramètres sont programmables et changeables au moyen du logiciel AIMS M.

La figure ci-dessous représente l'interface 95T GPI MI et les raccordements nécessaires.



Nota: les prises Cannon sont vues coté soudure.

L'interface GPI MI sera toujours connectée au Bus 00 (maître), aussi bien sur le site local que sur les sites déportés.

Interrupteurs de configuration :

Placer les interrupteurs en position suivante (**hors tension**):

SW1/6 = ON et SW1/7 = OFF

L'interface peut être utilisée de deux façons : vers Modem HAYES ou PAD X 28. Par défaut dans la configuration précédente l'interface est en fonction modem HAYES. La modification (**sous tension**) de la position l'interrupteur SW 1/6 permet de changer le mode de fonctionnement de l'interface.

SW1/6 : OFF ð ON = PAD X 28 SW1/6 : ON ð OFF= Modem Hayes

Après ce changement il est nécessaire de déconnecter l'alimentation de l'interface et de remettre les interrupteurs dans leurs positons normale (SW1/6 = ON & SW1/7 = OFF) . A chaque nouvelle mise sous tension l'interface fonctionnera dans le mode (modem ou X28) que l'on a choisi au début.

2.2.1.4 Fonction GPI SECOM

La carte 95T GPI SECOM permet de piloter les transmetteurs d'alarme SERIAL de SECOM.

Placer les interrupteurs en position suivante (**hors tension**):

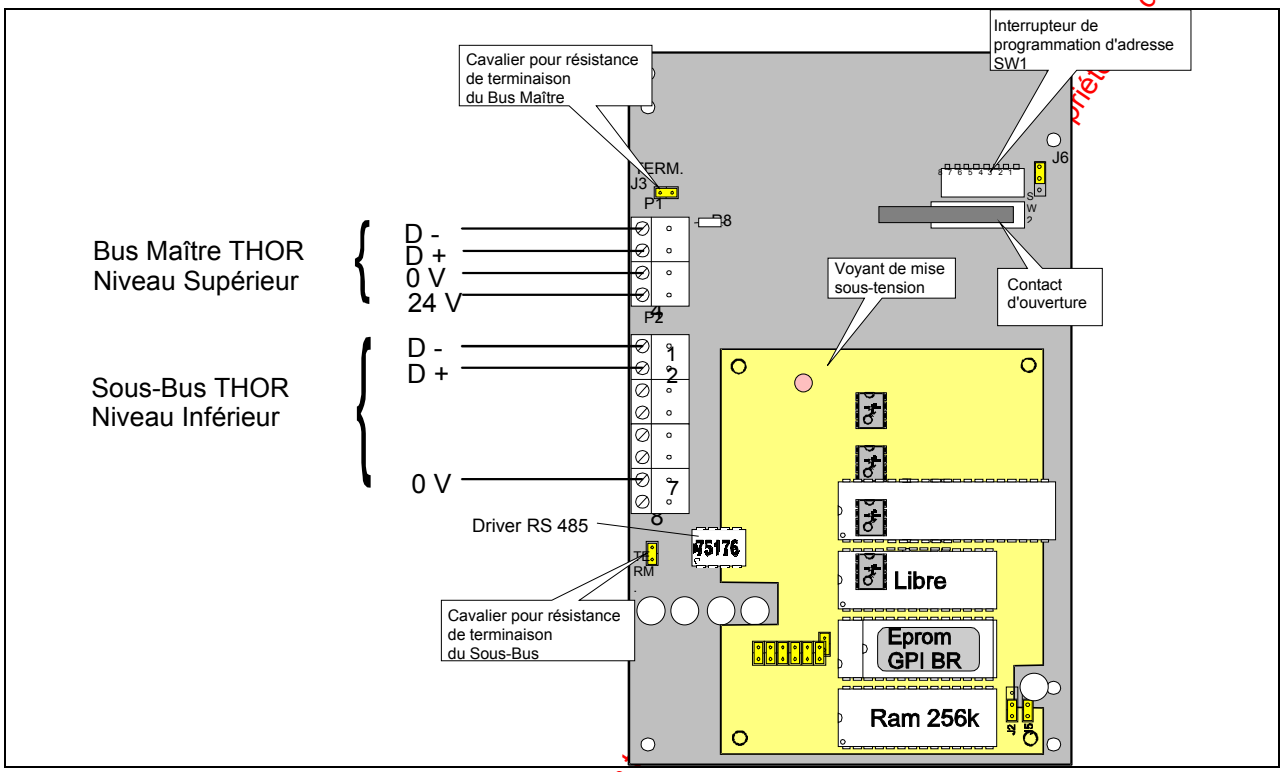
SW1/6 = OFF et SW1/7 = ON

Cette possibilité sera décrite dans un document séparé étant donné quelle n'est utilisée que par le système intrusion.

2.2.2 L'interface 90T GPI BR

L'interface est de **Type 2** (voir schéma chapitre 2.3), l'EPROM sera de type 90T GPI BR.

Cette interface est utilisée pour connecter les bus RS 485 entre eux. De ce fait, l'interface possède 2 circuits de transmission RS 485, un pour le bus maître 00 et un pour le sous-bus (N° 01 à 31).



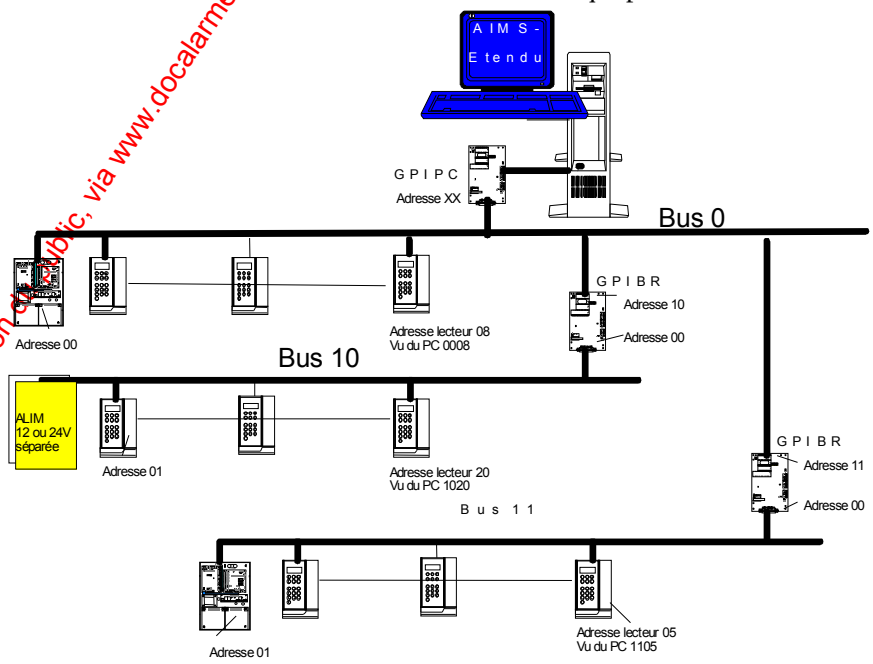
Nota: Seule l'adresse sur le bus 00 (Bus Maître) sera fixée sur l'interface BR, l'interface ayant toujours l'adresse 00 sur tous les sous-bus.

L'interface sera **toujours alimentée par le bus maître 00**; elle possède deux cavaliers pour les résistances de terminaison:

J3 : résistance de terminaison pour BUS 00

J4 : résistance de terminaison pour SOUS-BUS 01 à 31.

Les masses électriques (0V) doivent rester séparées entre BUS maître et Sous-bus ainsi qu'entre les sous-bus eux mêmes. Faire très attention aux alimentations communes qui pourraient effectuer ces liaisons.

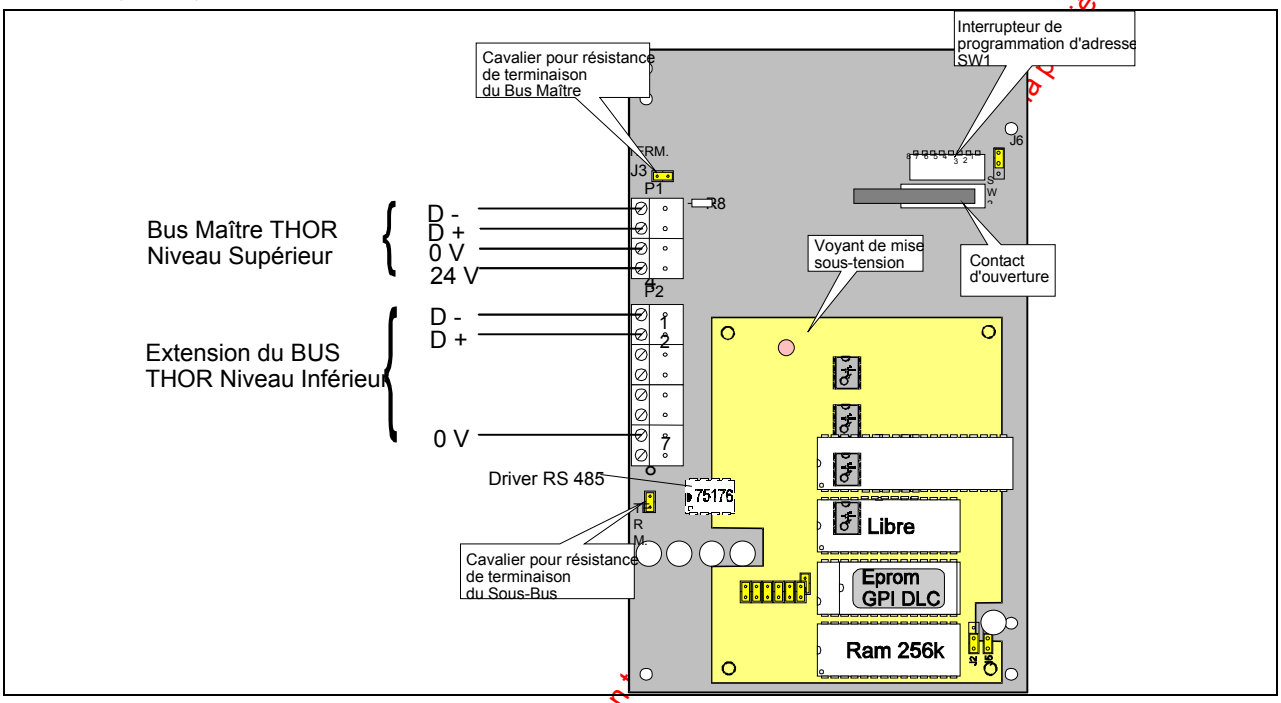


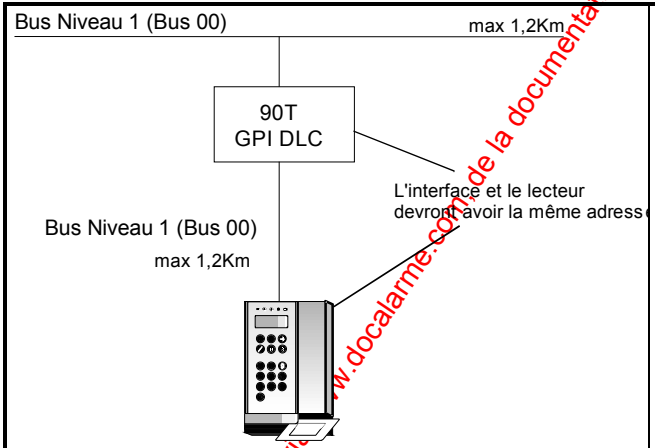
2.2.4 L'interface Amplificateur de bus RS 485 - 90T GPI DLC

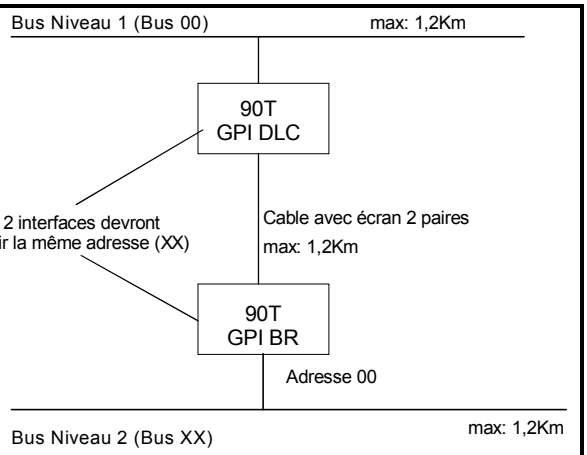
L'interface est de **Type 2** (voir schéma chapitre 2.3), l'EPROM sera de type 90T GPI DLC.

Cette interface permet de dépasser la limite de 1200m du bus RS 485 HISEC et de répondre aux installations de taille importante.

Elle permet de rajouter une section de bus de 1Km2 par élément, ou de créer un sous bus à une grande distance (2Km4).







Dans le cadre d'une connexion d'un lecteur (terminal) cette carte sera utilisée seule.

N'importe quel périphérique pourra être implanté sur la branche de fin de la ligne directe.

Elle pourra éventuellement être placée sur un sous-bus dans le cas de câblage d'un élément unique (lecteur, terminal).

Cette configuration peut être gérée comme un système monobus (logiciel standard).

Dans le cas de la création d'un sous-bus il est nécessaire de connecter une interface 90T GPI BR (voir chapitre précédent).

L'interface GPI DLC sera obligatoirement connectée au Bus 00 (maître).

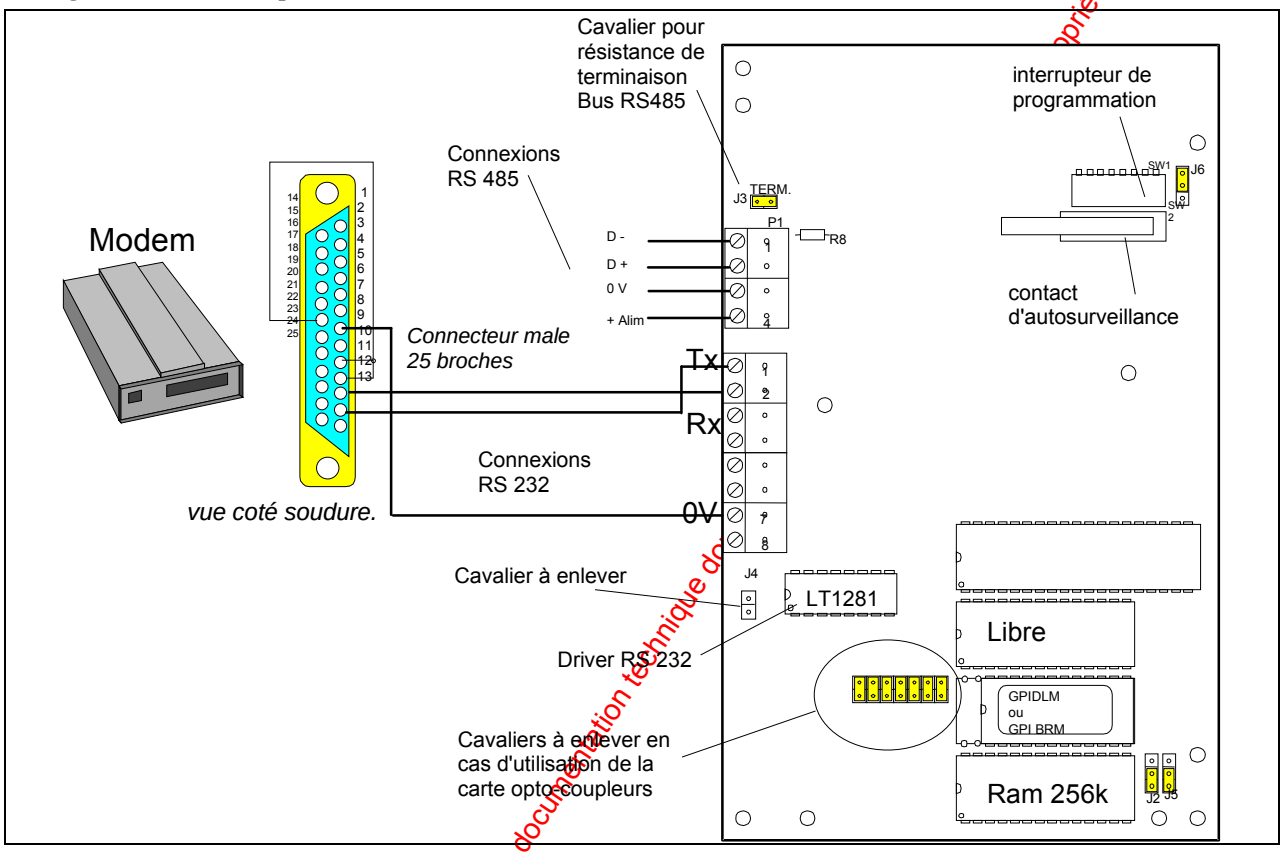
Cette configuration devra être gérée comme un système multibus (AIMS-X).

2.2.5 Les Interfaces 90T GPI DLM et BRM

L'interface est de **Type 1** (voir schéma chapitre 2.3), l'EPROM sera de type 90T GPI DLM ou BRM.

Ces interfaces permettent de dépasser la limite de 1200 m du bus RS 485 HISEC et de répondre aux installations de taille importante ainsi que les installations nécessitant de traverser la voie publique (obligation d'utiliser une ligne spécialisée).

La figure ci-dessous représente l'interface 90T GPI DLM/BRM et les raccordements nécessaires.



L'interface **GPI DLM** sera toujours connectée au **Bus 00** (maître), alors que l'interface **GPI BRM** sera toujours sur les **sous-bus**.

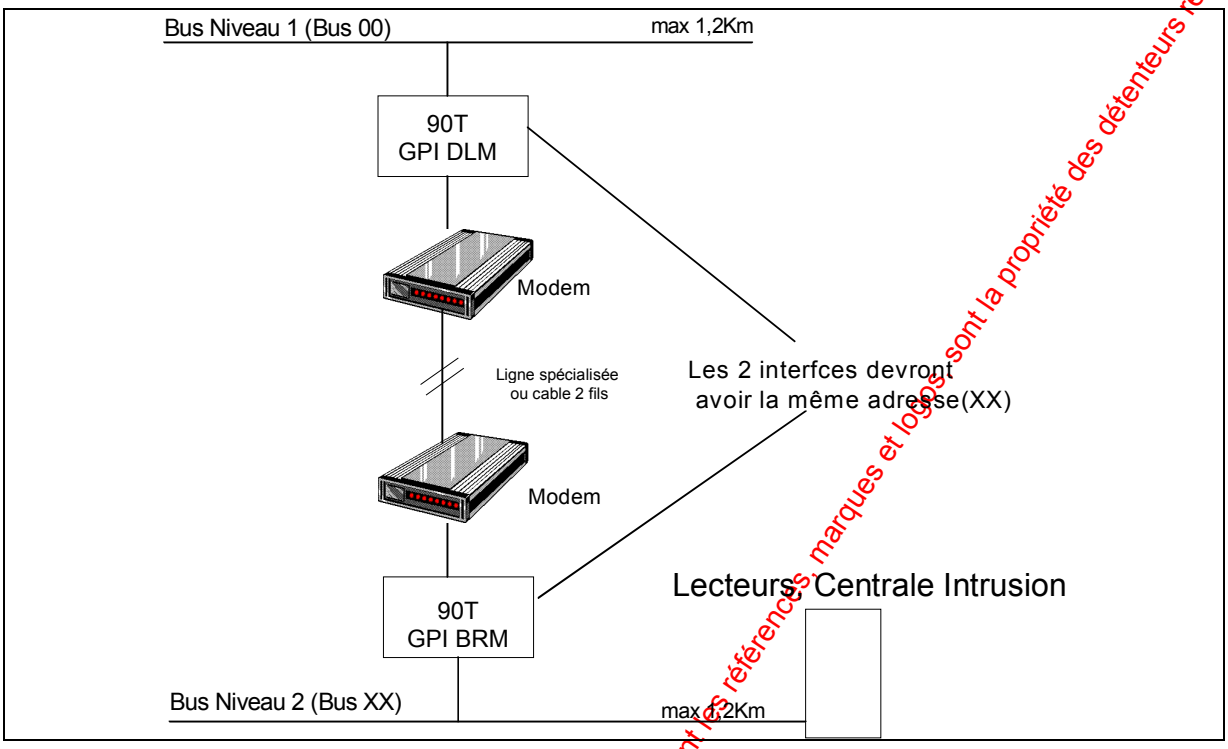
Le logiciel de ces interfaces est prévu pour piloter différents modems, ces modems doivent pouvoir fonctionner en LS 2 fils, pour la liste de compatibilité contacter HISEC International.

Les caractéristiques de ces modems sont:

Interface matérielle :	RS 232 sans handshake.
Type de transmission :	Asynchrone, 9600 bauds, 8 bits, 1 bit de stop, parité paire.
Contrôle de flux :	Aucun.
Délai de transmission :	100ms (max.) de délai entre l'émission d'un caractère sur un modem et la réception sur l'autre modem.
Délai de changement de direction : flux	100ms (max.) supplémentaires seront acceptées quand le sens du de données est changé.

Nota : si les modems ou autres coupleurs ne possèdent pas d'interface galvanique, il est toujours possible d'implanter sur les interfaces la carte opto-coupleurs 90T GIB.

L'interface ligne directe sera connectée de la façon suivante:



La liaison entre modem pourra être du type ligne spécialisée (PTT) ou liaison filaire (2 fils) permanente, pas de liaison auto commutée, ni de liaison par le réseau intérieur (les modems ne peuvent pas numéroter, et doivent être en liaison constante).

Vu du PC, l'ensemble GPI DLM, Modems, GPI BRM sera vu comme une seule interface GPI BR (passerelle).

Ne pas oublier que pour communiquer les 2 interfaces devront avoir la même adresse.

Cette programmation est sauvegardée dans les modems et n'a pas à être reprogrammée en cas de coupure d'alimentation.

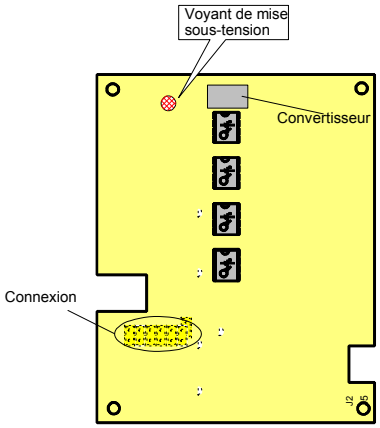
! *Ne pas oublier de placer l'interrupteur N°6 du Dip-switch SW1 des cartes GPI DLM/BRM sur la position ON.*

Remarque: Les modems pourront être remplacés par des coupleurs de fibre optique ou autre moyen de transmission.

2.2.6 L'interface opto-coupleurs 90T GIB

Cette interface est utilisée pour isoler les 2 cotés des diverses interfaces GPI-XX, elle permet de faire une isolation galvanique entre 2 x RS 485 ou entre RS 485 et RS 232. Cette carte est obligatoirement présente dans l'interface GPI-BR mais peut être installée sur n'importe quelle interface.

Elle est recommandée dans tous les cas ou l'appareil à connecter (modem, coupleur, etc.) ne possède pas d'isolation galvanique.



Nota: ne pas oublier d'enlever tous les cavaliers d'origine de la carte interface avant d'insérer cette carte.

2.2.7 L'interface 95T GPI COM 2

2.2.7.1 Généralités

Carte GPI

Une nouvelle version matérielle de carte GPI est maintenant disponible.

✖ La nouvelle disposition matérielle de la carte GPI combine l'interface 95T GPI et la carte interface d'isolation galvanique 90T GIB, de façon que toutes les interfaces à l'avenir soient fournies avec la fonction isolation galvanique intégrée.

! *La nouvelle version de carte GPI, peut utiliser indifféremment des EPROMs 256Koctets ou de 512Koctets, pour toutes les applications; excepté l'interface GPI COM où l'EPROM doit être de 512Koctets.*

Compatibilité

La nouvelle carte GPI est compatible avec la majorité des EPROMs existantes – excepté la version d'EPROM 106.0504.013 de GPI COM, et les versions précédentes, qui ne fonctionneront pas avec la nouvelle version de carte GPI.

Veuillez noter que les interfaces GPI dans leur nouvelle disposition matérielle ne sont pas compatibles avec l'interface 99T IPI. Cela signifie que la nouvelle carte GPI ne peut pas être transformée en Interfaces IP en ajoutant la carte 99T IPI.

Logiciel GPI

Deux nouveaux logiciels pour GPI sont maintenant disponibles. Ces nouveaux logiciels sont une nouvelle version du logiciel existant pour GPI BR et un nouveau logiciel pour interface 95T GPI LE.

Types de GPI disponibles

Le tableau ci-dessous présente toutes les interfaces GPI disponibles dans la nouvelle version matérielle:

Code produit	*Description*	*Référence*
95T GPI COM-3	Interface PC / Imprimante / Modem	800014
BR2 DE 95T GPI	Interface Passerelle	800015
95T GPI DLM-2	Interface Modem Ligne Directe	800016
95T GPI BRM-2	Interface Modem Passerelle	800017
95T GPI DLC-2	Interface Câble Ligne Directe	800018
95T GPI LMI-2	Interface Locale Modem	800019
95T GPI LE	Interface d'Extension de Bus	800020

✖ Veuillez noter que l'interface GPI COM n'est pas encore disponible dans cette nouvelle version matérielle. L'interface GPI COM pour la nouvelle version matérielle de GPI, sera disponible à partir de la sortie de la nouvelle version du logiciel GPI COM, version 413106.0506.00x.

Checksum EPROM

Les checksums suivants sont indiqués sur les EPROM's:

Produit	*Numéro Version*	*Type/taille EPROM*	*Checksum*	*Date:*
95T GPI BR	413073.0506.003	27C256 / 256 Kb	BCE7	20020503
	413073.0506.003	27C512 / 512 Kb	3CE7	20020503
95T GPI LE	413180.0101.001	27C256 / 256 Kb	02B7	20020530
	413180.0101.001	27C512 / 512 Kb	82B7	20020530

2.2.7.2 Implantation physique

La nouvelle plateforme matérielle GPI combine l'ancienne plateforme matérielle des GPI et l'interface galvanique 90T GIB. Le nouveau matériel est compatible au niveau logiciel avec l'ancien matériel – à une exception.

Les versions d'EPROM 106.0504.017 des 95T GPI COM (et versions antérieures) ne fonctionneront pas avec le nouveau matériel. Dans toutes les autres applications de GPI, il est possible de récupérer l'EPROM d'une ancienne GPI vers une nouvelle GPI et ensuite de configurer les cavaliers et micro interrupteurs en position souhaitée.

Veuillez noter que l'EPROM doit toujours être placée en bas du support

Cavaliers J3 - Isolement Galvanique

Cavaliers J4 à J6 pour la sélection RS232/RS485 sur le connecteur P2

LED OP1 Indication de l'alimentation électrique/CPU

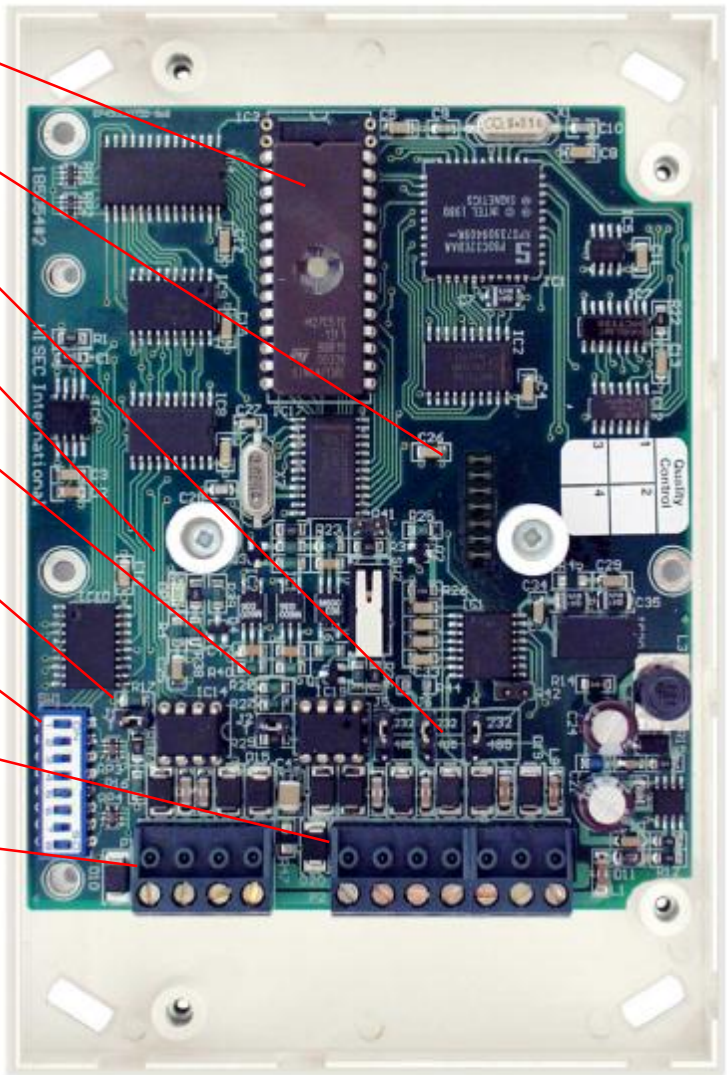
Cavalier – J2 résistance de terminaison RS 485, P2

Cavalier – J1 résistance de terminaison RS 485, P1

Micro interrupteurs SW1

Connecteur P2 – RS485/RS232

Connecteur P1 – RS485



Cette nouvelle carte dispose d'une LED (OP1) implantée sur la carte. Si l'on utilise des anciennes versions d'EPROM, la DEL indiquera la mise sous tension. En utilisant les nouvelles versions d'EPROM, la DEL indiquera également que le processeur de la GPI fonctionne en clignotant à une fréquence de 0,5 hertz.

2.2.7.3 Raccordements

La nouvelle interface GPI est équipée de deux borniers de raccordement, P1 et P2. La fonction des différents connecteurs est presque la même que pour l'ancienne version matérielle des cartes GPI – a une exception près, la borne 8 du connecteur P2 a été retirée. Cette borne n'ayant jamais été utilisée dans les applications HISEC.

✖ Ceci signifie qu'il est possible d'utiliser la documentation d'installation existante pour câbler les nouvelles interfaces GPI.

Connecteur P1

Le connecteur P1 est utilisé pour le raccordement de la GPI au bus RS485 (Bus maître pour la GPI BR). Les connexions sont décrites dans le tableau suivant:

P1	*Fonction*	
1	D –	Transmission RS485
2	D+	Transmission RS485
3	0v	Masse d'Alimentation électrique
4	12v/24v	+ Alimentation électrique

Connecteur P2

Le connecteur P2 peut être utilisé en RS485 (GPI BR / DLC / LMI / LE) ou en RS232 (GPI COM / DLM / BRM). Les fonctions présentes sur les bornes de P2 (c.-à-d. l'interface) sont déterminées par l'EPROM, la configuration des micro interrupteurs SW1 et la configuration des cavaliers.

GPI BR / DLC / LMI / LE

Les raccordements sur le bornier P2 en utilisation du mode RS485 sont décrits dans le tableau suivant:

P2	*Fonction*	
1	D –	Transmission RS485
2	D+	Transmission RS485
3	–	
4	–	
5	–	
6	–	
7	0V	Masse Signal/Alim. (du sous-bus)

✖ Veuillez noter que quand la GPI est utilisée en fonction BR, il est impératif de toujours valider l'isolation galvanique (cavaliers J3 enlevés).

Les raccordements sur le bornier P2 en utilisation du mode RS232 sont décrits dans le tableau suivant:

P2	*Fonction*	
1	TXD	Transmission RS232
2	RXD	Reception RS232
3	0v	Masse Alimentation électrique
4	12V/24v	Sortie alimentation pour périphérique basse tension (par exemple une imprimante série).
5	RTS	Request To Send
6	CTS	Clear To Send
7	GND	Masse de dialogue

- Veuillez noter qu'en utilisant l'interface GPI COM comme interface imprimante, l'isolement galvanique devra toujours être mise hors fonction (cavaliers J3 présents).

- Veuillez noter également que les bornes 3 et 4 sur P1 et P2 sont directement interconnectés (comme dans l'ancienne version de carte), et ce sans isolation galvanique – indépendamment de la configuration des cavaliers J3 (voir page suivante).

2.2.7.4 Réglage des cavaliers et micro interrupteurs

La nouvelle version matérielle de carte GPI est équipée d'un bloc de micro-interrupteurs et de sept cavaliers. Ceux-ci doivent être placés selon l'application GPI désirée, comme décrit dans les sections suivantes.

Cavaliers J1 à J6

Sept cavaliers permettent de configurer la nouvelle carte GPI, avec les fonctions suivantes:

Cavalier J1

Validation de la résistance de terminaison du BUS sur le bornier P1.

J1	*Fonction*
ON	Résistance de terminaison RS485 présente
OFF	Résistance de terminaison RS485 hors circuit

Cavalier J2

Validation de la résistance de terminaison du Sous-BUS sur le bornier P2 en mode RS485 (GPI BR / DLC / LMI / LE). Si l'interface RS232 a été sélectionnée pour P2, alors J2 n'a aucune fonction.

J2	*Fonction*
ON	Résistance de terminaison RS485 présente
OFF	Résistance de terminaison RS485 hors circuit

Cavaliers J3

La configuration de ces deux cavaliers active ou enlève l'isolement galvanique entre les borniers P1 et P2.

J3	*Fonction*
ON	L'isolement galvanique est enlevée
OFF	L'isolement galvanique entre P1 et P2 est présente (valeur par défaut)

✖ Veuillez noter que les cavaliers J3 doivent seulement être présents, si la nouvelle interface GPI est utilisée comme interface imprimante.

! *Veuillez noter que les deux cavaliers J3 doivent toujours être placés dans la même position : ON ou OFF.*

Les cavaliers J4 à J6 sont employés pour sélectionner le type de sortie : RS232 ou RS485 sur le bornier P2.

J4 à J6	*Fonction*
Haut	Fonction RS232 pour P2 (GPI COM / DLM / BRM)
Bas	Fonction RS485 pour P2 (GPI BR / DLC / LMI / LE)

✖ Veuillez noter qu'en fonction du type d'interface GPI livrée par HI SEC, les cavaliers J4 à J6 auront toujours la configuration correcte appropriée à l'EPROM.

! *Veuillez noter que tous les cavaliers de J4 à J6 doivent toujours être placés dans la même position, HAUTE ou BASSE.*

Micro interrupteurs SW1

La configuration des micro-interrupteurs 1 à 8 sur SW1 détermine l'adresse de la GPI, la fonction de la GPI (pour GPI COM seulement) et choisit le mode de transmission crypté ou non.

Micro-Interrupteurs 1 à 5

Les Micro interrupteurs 1 à 5 sont utilisés pour programmer l'adresse de l'interface GPI. Les adresses sont codées en binaires de 01 à 31. Du fait que le maître du bus à toujours l'adresse 00, cette adresse ne peut pas être employée par une interface GPI.

Adresse	*N° Interr. 5 4 3 2 1*	*Adresse*	*N° Interr 5 4 3 2 1*	*Adresse*	*N° Interr 5 4 3 2 1*
00	Non applicable	01	00001	02	00010
03	00011	04	00100	05	00101
06	00110	07	00111	08	01000
09	01001	10	01010	11	01011
12	01100	13	01101	14	01110
15	01111	16	10000	17	10001
18	10010	19	10011	20	10100
21	10101	22	10110	23	10111
24	11000	25	11001	26	11010
27	11011	28	11100	29	11101
30	11110	31	11111		

0 signifie que le commutateur est dans la position ON et 1 que le commutateur est dans la position OFF. Veuillez noter que la position ON/OFF est directement indiquée sur le commutateur.

Les micro-interrupteurs 6 et 7 sont utilisés pour programmer la fonctionnalité d'une interface de GPI COM (interface PC, imprimante ou modem).

Commutateur 6	*Commutateur 7*	*Fonction*
ON	ON	Interface PC
ON	OFF	Interface Modem
OFF	ON	Serial
OFF	OFF	Interface Imprimante série

La configuration de l'imprimante série connectée à la GPI COM en mode interface imprimante devra être:

Configuration de l'imprimante série	
Vitesse baud:	1.200 bauds
Numéro des bits de données:	8
Nombre de bits de stop:	1
Parité:	Paire
Fin de ligne:	CR + LF (retour chariot et ligne suivante)
Protocole:	matériel

✖ Veuillez vous référer au chapitres précédents pour une description complète de l'installation de GPI COM en mode interface imprimante ou en mode modem.

Micro-Interrupteur 8

Le micro interrupteur 8 est utilisé pour sélectionner le mode de communication de l'interface : "mode normal" (ON) ou mode crypté (OFF) sur le bus RS485.

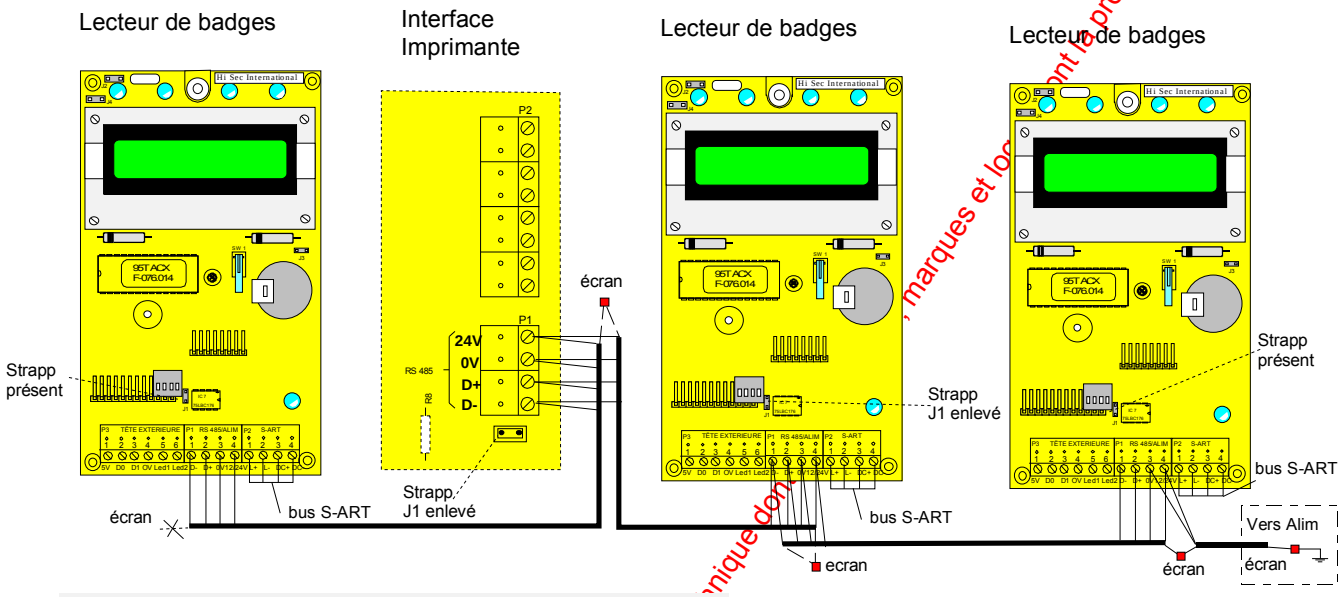
Commutateur 8	*Fonction*
ON	Transmission RS485 non cryptée
OFF	Transmission RS485 cryptée

2.3 Raccordement du Bus RS 485

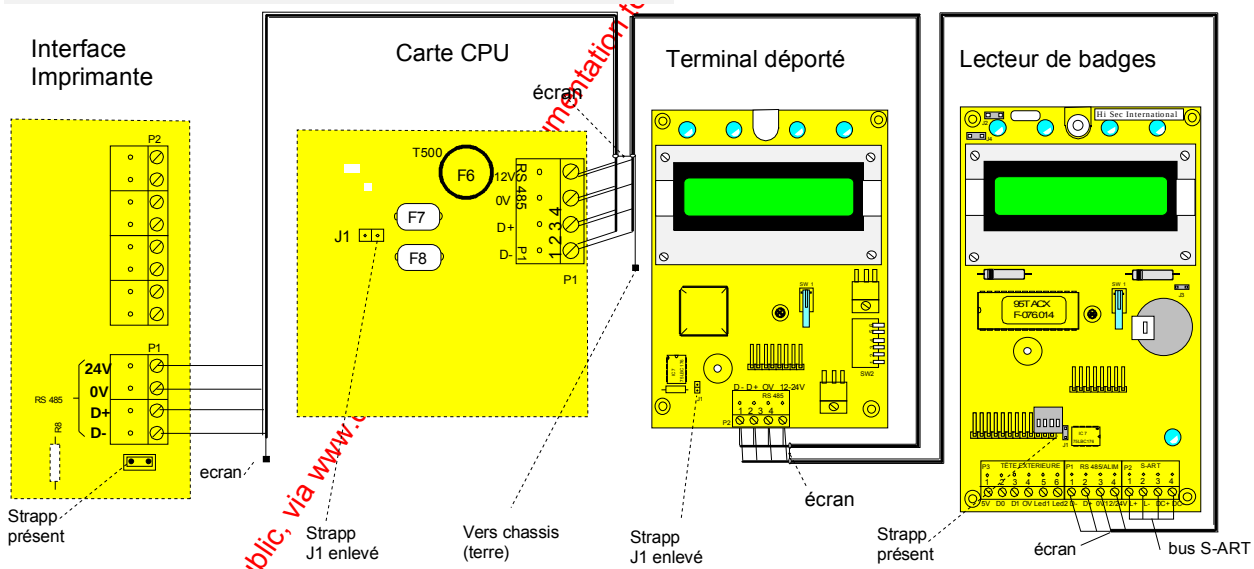
Le bus RS485 est utilisé pour faire communiquer entre eux les différents lecteurs ainsi que les divers périphériques tels imprimante déportée, synoptique etc. Toutes les unités seront connectées sur le bus comme représenté sur les schémas de raccordement ci-dessous.

Les connexions de type câblage en "étoile" ne doivent pas excéder 0m30 de longueur, par contre l'ordre dans lequel les différentes adresses sont installées sur le bus n'a aucune importance.

INSTALLATION SANS CENTRALE INTRUSION:



INSTALLATION AVEC CENTRALE INTRUSION:



Le bus doit être terminé à chaque extrémité par une résistance de 220 ohms. Ces résistances de terminaison sont implantées sur tous les appareils à la fabrication, elles doivent être enlevées des appareils connectés entre les deux extrémités du bus. Dans l'exemple représenté ci-dessus les résistances n'ont pas été enlevées sur les deux lecteurs de badges en extrémité du bus.

Sur les lecteurs de badges, il est possible d'installer un bus S-ART local séparé avec un maximum de 15 S-ART. **Ce bus ne devra pas être connecté avec d'autres bus venant des autres lecteurs ou de la centrale intrusion HISEC.** Le bus S-ART du lecteur de badges est utilisé pour raccorder les contacts de porte, gâche électrique, bouton poussoir de sortie etc. au lecteur.

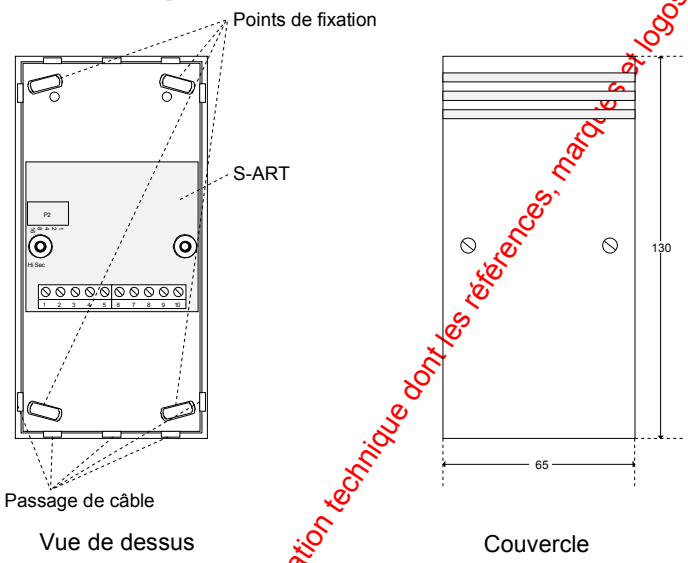
2.4 Les S-ART

Toutes les entrées/sorties venant ou provenant d'un lecteur sont réalisées par l'intermédiaire de S-ART.

Pour le Contrôle d'Accès HISEC, il est recommandé d'utiliser le S-ART type 90T-S102, mais en cas de besoin les autres types existants dans la centrale Intrusion HISEC peuvent être utilisés (excepté le S-art S 106). Le S-ART 90T S102 possède 2 entrées normalement fermées et 1 relais de sortie, qui peuvent être utilisés pour le contact de porte, le bouton poussoir de sortie et la gâche électrique.

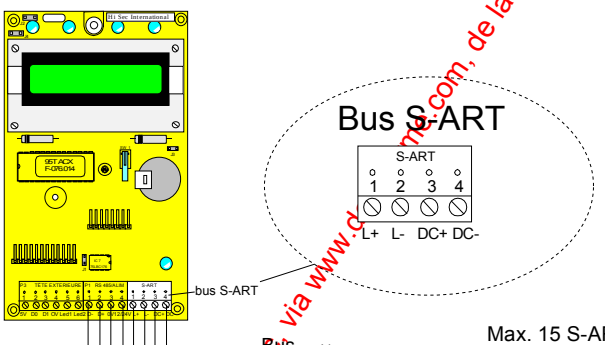
Sur le lecteur un connecteur permet de raccorder le bus S-ART (max. 15 S-ART). La totalité des 15 adresses peut être utilisée librement et être programmée avec les fonctions décrites au *Chapitre 1* "*Description Fonctionnelle*".

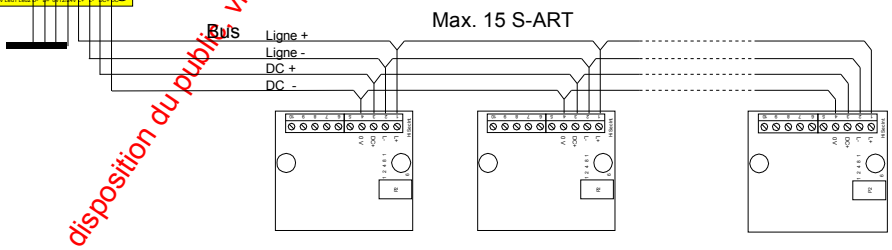
2.4.1 Dimensions mécaniques et fixation



2.4.2 Connexions des S-ART au Lecteur de Badges

Le bus est constitué de 4 fils sur lesquels sont connectés les S-ART. Deux fils sont utilisés pour la transmission des informations des S-ART, les 2 autres étant utilisés pour alimenter les S-ART.





Tous les S-ART sont installés de la même façon, comme représenté sur la figure ci- contre. Pour le raccordement du S-ART 90T S102 se reporter au chapitre suivant.

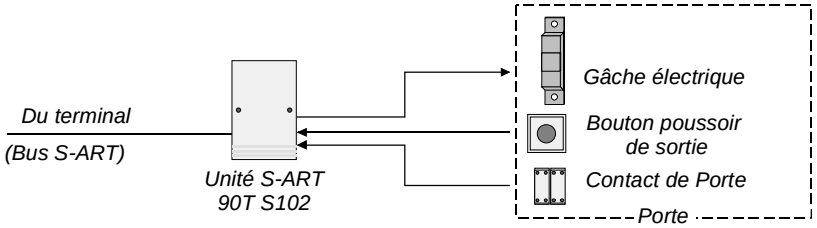
Attention à ne pas croiser les branchements des bornes 2 et 4. La communication fonctionnera sans doute, mais il est probable que vous ayez des problèmes de bruits.

Les câblages en "étoile" sont autorisés si besoin. Les câbles peuvent être tirés par le plus facile et le plus court chemin.

Consommation: ..... Bus max. 40 mA, continu: 500 mA.
Longueur des câbles:. 250m avec écran, 500m sans écran, paires torsadées 0,6/0,9 mm. Câble séparé par bus
Adresses: ..... Bus 1 :00-14
Temps de détection:... Voir description des fonctions au *Chapitre 1.3.1*

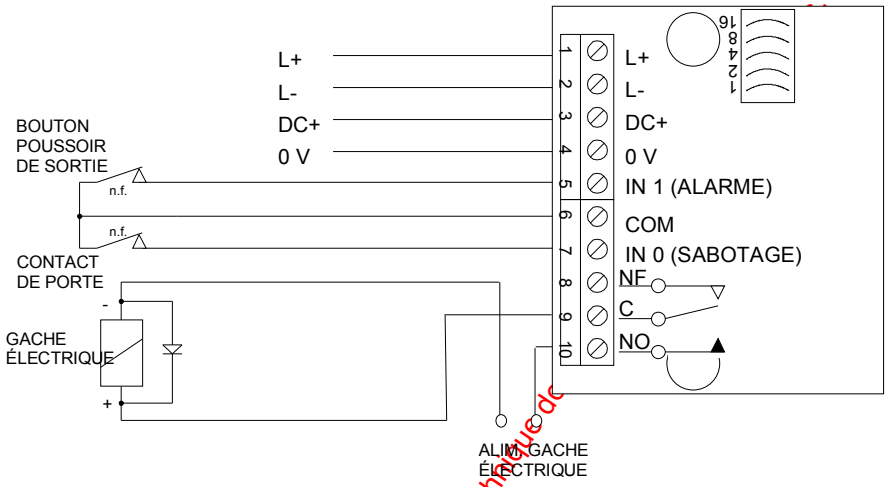
2.4.3 Connexions des Entrées/Sorties au S-ART 90T S102

Généralités :



97100801a

S-ART possédant 2 entrées et un relais de sortie.



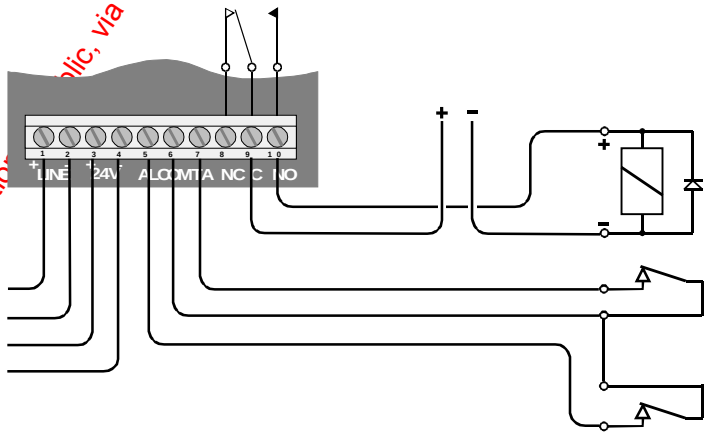
Caractéristiques.

Boucle IN 0 / IN 1 :..... Contact libre de tension, normalement fermé.
Résistance de fin de boucle :..... Pas nécessaire
Longueur maximum des câbles :..... 10 m
Consommation sous 24 V :..... Relais au repos: 0 mA
Relais actif: 6 mA
Consommation sur la ligne 17 V :..... 2 mA
Tension de commande du relais :..... Max. 125 V.
Courant de commande du relais :..... Max. 1A.
Puissance max. du relais DC/AC..... 30 W / 60 VA
Gamme de température :..... - 25 °C - + 70 °C

La consommation en courant sur la ligne 17 V est le courant pris sur le bus L+ et L-.

Le relais est toujours contrôlé par la sortie OUT1 du S-ART. (Voir *Menu 85 - Programmation des Sorties*).

Raccordement avec utilisation d'une alimentation extérieure.



97121705a

2.4.4 Codage des Adresses de S-ART

A l'installation de S-ART, le champ de codage des adresses de chaque S-ART doit être configuré avec l'adresse correcte. Ce codage est réalisé par coupure de cavaliers comme représenté dans le tableau suivant et l'exemple.

Adresse	Codage	Adresse	Codage	Adresse	Codage
00		01		02	
03		04		05	
06		07		08	
09		10		11	
12		13		14	

(Connexion enlevée) Connexion intacte

00 

ADRESSE NON -CODEE

05 

ADRESSE 05

5 cavaliers sont disponibles sur chaque carte de S-ART repérés 1,2,4,8 et 16. Chaque cavalier additionne la valeur numérotée sur l'adresse s'il est coupé, voir l'exemple ci-dessous. Un S-ART sans cavalier coupé aura l'adresse 0.

L'adresse est codée en nombre binaire, par exemple l'adresse 05 peut être écrite 00101 => 16 = 0, 8 = 0, 4 = 1, 2 = 0, 1 = 1. Si cette adresse doit être codée, les connexions 4,1 seront coupées et 2, 8, 16 laissées intactes.

Exemple de codage: (Connexion enlevée) Connexion intacte

2.4.5 Le S-ART S112

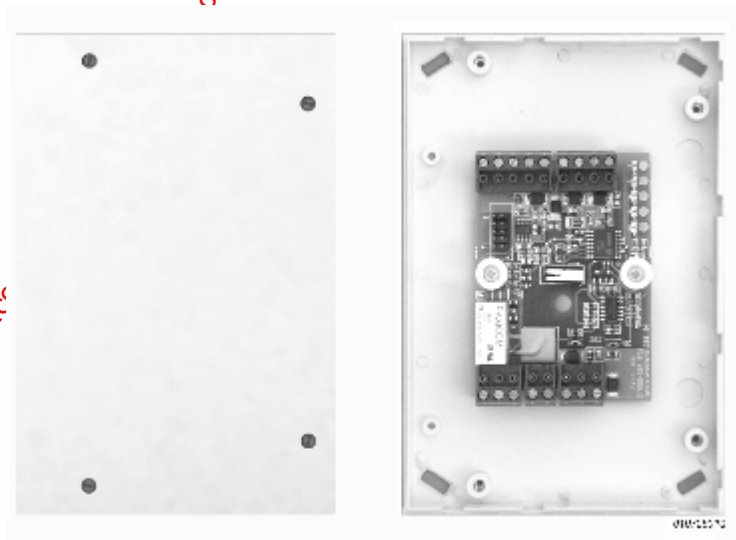
Le S-art 90T S-112 est destiné principalement aux installations de contrôle d'accès, mais peut être également utilisé dans les installation anti-intrusion où une sortie relais est nécessaire, ainsi il peut substituer aux S-art types 90T S-101 et 90T S-102. Dans des systèmes de contrôle d'accès, il est spécifiquement utilisé pour le câblage des équipements de porte.
Le 90T S-112 est livré dans un grand boîtier pour fournir l'espace supplémentaire nécessaire aux câbles. La carte est fixée par vis à la partie inférieure du boîtier. Tous les connecteurs à vis sont débrochables de la carte.

Le 90T S-112 est équipé d'un relais a contact libres de tension pouvant commuter des charge jusqu'à 2A DC. Le courant est limité par une résistance et un fusible électronique.
Pour les détecteurs ayant besoin d'une alimentation 12V DC, une sortie 12V DC 50 mA est disponible, quand le 90T S-112 est alimenté sous une tension supérieure à 17,5 V DC.
Les cavaliers permettent l'utilisation des résistances de terminaison internes (cavaliers sur OFF) ou des résistances de terminaison de 21,5KΩ externes (cavaliers sur ON) pour les boucles d'entrées.

Le contact interne de sabotage est un microcontact, mécaniquement protégé.

Le 90T S-112 est équipé d'un connecteur pour l'outil de diagnostic avec indicateurs à LED - 90T STT. Il affichera le dialogue sur le bus S-art, l'alimentation, l'état des entrées et l'état du relais de sortie.

Figure. 1 *Unité S-art 90T S-112 couvercle enlevé (échelle 1:2)*



Caractéristiques

Paramètre	*Valeur ou description*
Boucle d'Alarme/Sabotage:	Tout contact libre de tension normalement fermé.
Résistance de Terminaison	Rfl = 21,5 KΩ.
Longueur maximale de câble:	50 m (entre les éléments connectés et l'unité S-art).
État normal:	18.4kΩ < Rfl < 23.4kΩ.
Sensibilité Alarme/Sabotage:	Rfl < 17.0kΩ ou Rfl > 25,6 KΩ.

Suite…

Consommation sur bus S-art:	Maximum. 3,5 mA (L+, –L).
Tension d'alimentation	de 10 à 30 V DC (DC+, DC– ou Vdd, 0V).
Tension de sortie:	12V DC ±10% pour alimentation supérieure à 17,5V DC.
Courant de sortie:	40 mA à 30°C avec alim 24V DC. 30 mA à 70°C avec alim 28V DC.
Tension d'alimentation de relais:	De 9 à 30 V DC
Tension de commutation de relais:	Maximum 30 V (DC ou AC).
Pouvoir de coupure du relais:	DC: Maximum. 2 A. AC: Maximum. 1 A.
Puissance de commutation du relais:	DC: Maximum. 60 W. AC: Maximum. 120 VA.
Température ambiante:	-25 °C à +70 °C.
Dimensions: Hauteur: Largeur: Profondeur: Poids:	158 millimètres. 106,5 millimètres. 20,3 millimètres. 140 g.
Accessoires inclus:	Deux résistances de 21,5 k Ω

Fixation des boîtiers S-art

Boîtier 90T S-112

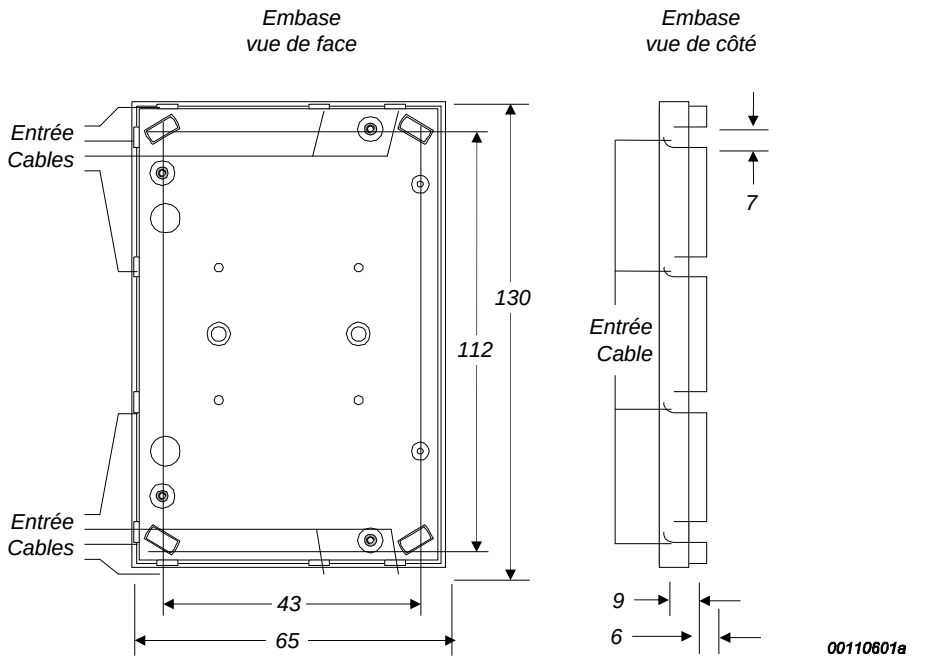
Pour monter le boîtier, desserrez les quatre vis du couvercle et retirez complètement ce dernier. Retirez la carte électronique de l'unité de S-art du boîtier.

☛ Veuillez noter que ces unités de S-art contiennent des résistances destinées a un montage dans le détecteur. Ces résistances sont contenues dans le boîtier de fixation.

Dégager les entrées de câble que vous voulez utiliser. Le boîtier possède quatre entrées de câble sur un des côtés et trois entrées de câble à chaque extrémité comme représenté en Figure. 1 ci-dessous.

Montez le boîtier à l'aide de vis appropriées (3 à 3,5mm) avec au moins deux vis placées dans les trous de fixation en diagonale.
Après montage, suivez les instructions pour la connexion, le codage de l'adresse, etc. données section suivante. Remettez alors le couvercle en place et serrer les vis.

Figure. 1 *Embase du boîtier de fixation pour des unités de S-art 90T S-106. Le schéma montre la position des trous de fixation et des entrées de câble. Toutes les mesures sont en mm*



Connexion de l'unité de S-art 90T S-112

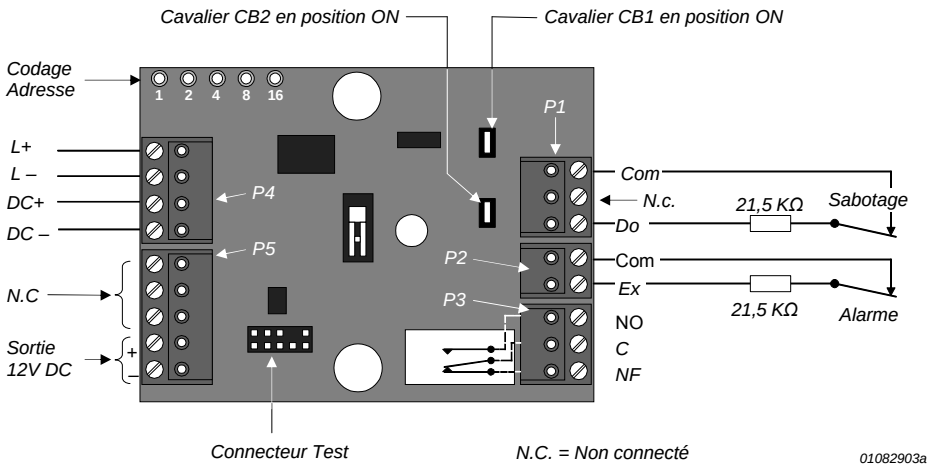
Le S-art 90T S-112 est livré avec deux résistances de 21,5kΩ placées à l'intérieur du boîtier de fixation. Leur utilisation dépend de l'application comme expliquée ci-dessous.

Connexion

Après codage de l'adresse comme expliqué à la fin de cette section et montage du boîtier, vous pouvez connecter l'unité S-art suivant l'application du produit à remplacer; 90T S-101 ou 90T S-102 avec les exemples représentés sur les figures suivantes, en association avec les tableaux de connexion.

Schéma de connexion (remplacement 90T S-101)

Figure. 1 *Exemple de connexion de 90T S-112 utilisé en remplacement du 90T S-101.*



Les cavaliers CB1 et CB2

Les deux résistances de 21,5kΩ sont utilisées comme représenté en Figure. 1. Les cavaliers "CB1" et "CB2" seront tous deux en position ON.

Tableau de connexion (remplacement du 90T S-101)

La sérigraphie des connexions est située sous les borniers débrochables de raccordement.

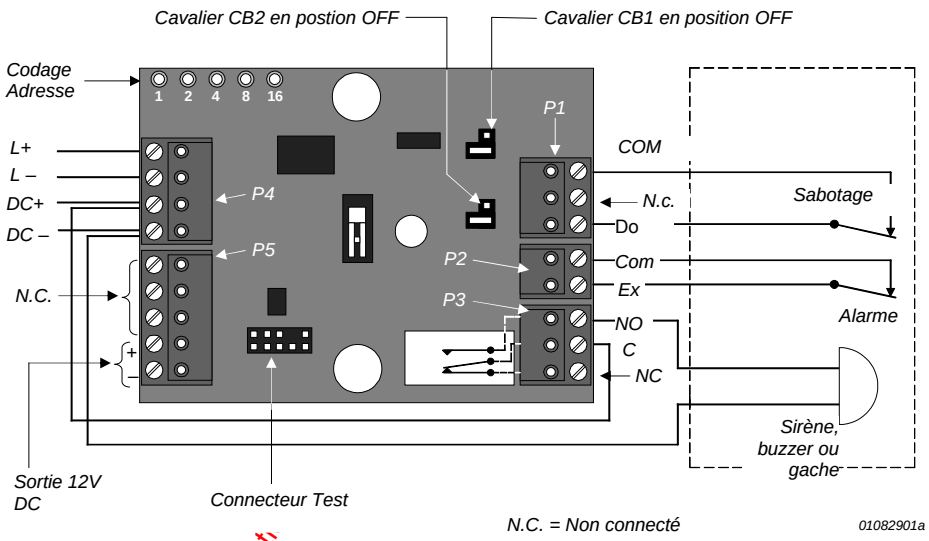
Conn.	N°	Étiquette		Description
P4	1	" L+ "		L+ bus S-art
	2	" L–"		L – bus S-art
	3	" 12V/24v "	"+"	DC+ (Vdd) bus S-art.
	4		"–"	DC– (0 V) bus S-art.
P5	1	Rien		Non connecté. Peut être utilisé pour le câblage.
	2	Rien		Non connecté. Peut être utilisé pour le câblage.
	3	Rien		Non connecté. Peut être utilisé pour le câblage.
	4	" 12V "	" + "	Sortie 12 V DC.
	5		" - "	Masse pour la sortie 12 V DC.
P1	1	"Do "		Borne pour la boucle d'entrée 0 (sabotage).
	2	" N.C"		Non connecté. Peut être utilisé pour le câblage.
	3	"COM"		Borne pour la boucle d'entrée 0 (sabotage).
P2	2	" COM "		Borne pour la boucle d'entrée 1 (alarme).

Non utilisé dans cette application

P2	**2**	" COM "	Borne pour la boucle d'entrée 1 (alarme).
	1	"Ex"	Borne pour la boucle d'entrée 1 (alarme).
P3	**3**	"NO"	Relais, contact normalement ouvert
	2	"C"	Relais, commun
	1	"NF"	Relais, contact normalement fermé

Schéma de connexion (remplacement du 90T S-102)

Figure. 1 *Exemple de connexion du 0T S-112 utilisé en remplacement du 90T S-102.*



Les cavaliers CB1 et CB2

Les deux résistances de 21,5kΩ sont utilisées comme représenté en Figure. 1. Les cavaliers "CB1" et "CB2" sont tous deux placés en position ON.

Tableau de connexion (remplacement du 90T S-102)

La sérigraphie des connexions est située sous les borniers débrochables de raccordement.

Conn.	*N°*	*Étiquette*		*Description*
P4	**1**	" L+ "		L+ bus S-art
	2	" L –"		L – bus S-art
	3	"12V/24v"	" + "	DC+ (Vdd) bus S-art.
	4		"–"	DC– (0 V) bus S-art.
P5	**1**	Libre		Non connecté. Peut être utilisé pour le câblage.
	2	Libre		Non connecté. Peut être utilisé pour le câblage.
	3	Libre		Non connecté. Peut être utilisé pour le câblage.
	4	"12V"	" + "	Sortie 12 V DC. Non utilisée dans cette application
	5		" - "	Masse pour la sortie 12V DC.
P1	**1**	"Do"		Borne pour la boucle d'entrée 0 (sabotage).
	2	"N.C"		Non connecté. Peut être utilisé pour le câblage.
	3	"COM"		Borne pour la boucle d'entrée 0 (sabotage).
P2	2	"COM"		Terminal pour la boucle 1 (alarme) de puissance d'entrée.

P2	2	"COM"	Terminal pour la boucle 1 (alarme) de puissance d'entrée.
	1	"Ex"	Terminal pour la boucle 1 (alarme) de puissance d'entrée.
P3	3	"NO"	Relais, contact normalement ouvert.
	2	"C"	Relais, commun
	1	"NC"	Relais, contact normalement fermé

Sortie Alimentation 12V DC

Cette sortie est utilisée pour alimenter n'importe quel circuit électronique, comme par exemple une sirène ou un buzzer ayant besoin d'une alimentation 12V DC dans le cas où celle-ci ne pourrait pas être prise directement sur le bus S-art +DC (Vdd) et DC– (0), au cas ou cette tension d'alimentation (par ex. 24V DC) excède la tension maximum de fonctionnement du circuit. L'utilisation de cette sortie nécessite une tension d'alimentation en entrée d'au moins 17,5V DC (DC+, DC– ou Vdd, 0V).

Codage Adresse

L'adressage du 90T S-112 est programmable par le découpage de pastilles. Les pastilles sont des trous métallisés placés près du bord de la carte et seront coupées au moyen d'une petite pince coupante. Les trous sont repérés "1", "2", "4", "8", et "16". La table ci-dessous représente la position des différents trous à couper pour obtenir l'adresse souhaitée.

	Numéro de trou						*Numéro de trou*						*Numéro de trou*				
Adresse	***1***	***2***	***4***	***8***	***16***	***Adresse***	***1***	***2***	***4***	***8***	***16***	***Adresse***	***1***	***2***	***4***	***8***	***16***
00	O	O	O	O	O	10	O	È	O	È	O	20	O	O	È	O	È
01	È	O	O	O	O	11	È	È	O	È	O	21	È	O	È	O	È
02	O	È	O	O	O	12	O	O	È	È	O	22	O	È	È	O	È
03	È	È	O	O	O	13	È	O	È	È	O	23	È	È	È	O	È
04	O	O	È	O	O	14	O	È	È	È	O	24	O	O	O	È	È
05	È	O	È	O	O	15	È	È	È	È	O	25	È	O	O	È	È
06	O	È	È	O	O	16	O	O	O	O	È	26	O	È	O	È	È
07	È	È	È	O	O	17	È	O	O	O	È	27	È	È	O	È	È
08	O	O	O	È	O	18	O	È	O	O	È	28	O	O	È	È	È
09	È	O	O	È	O	19	È	È	O	O	È	29	È	O	È	È	È

È = Coupé O = Non coupé

Dans l'exemple de droite, les cavaliers "1" et "4" ont été coupés, tandis que les cavaliers "2", "8" et "16" sont intacts et de ce fait code l'adresse à 05. Les pastilles à souder juste au-dessus des numéros peuvent être utilisées pour souder un petit morceau de fil pour rétablir une connexion si nécessaire.

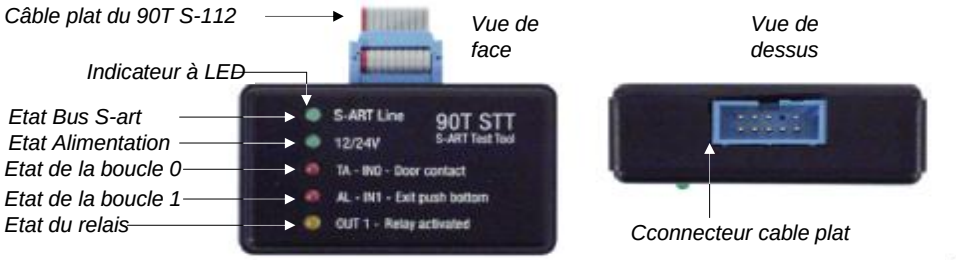
5 x 2 pastilles à souder

Connecteur pour outil de Test

Le S-art 90T S-112 est équipé d'un connecteur pour outil de test 90T STT. L'outil de test est équipé d'un câble d'un mètre facilement connectable au S-art. Avec ses indicateurs à LED, le 90T STT affiche le mode du bus S-art, l'alimentation Vdd, l'état de la boucle d'entrée 0, de la boucle d'entrée 1, et du relais.

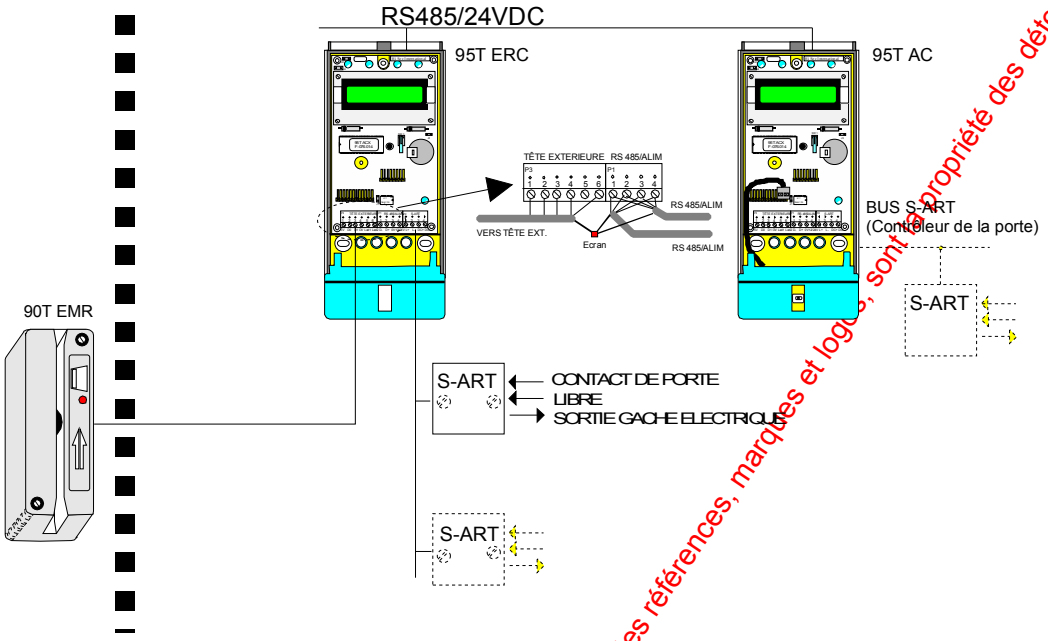
L'outil de test S-art 90T STT sera raccordé au connecteur de test sur le circuit du S-art 90T S-112 au moyen d'un câble plat terminé à ses deux extrémités par un connecteur 10-points avec détrompeur livré avec le 90T STT.

Figure. 1 *Outil de test S-art 90T STT.*



2.5 Connexion des Têtes de lectures déportées

Le terminal possède un bornier (P 3) pour raccorder directement les têtes de lectures extérieures.



Le lecteur 95T ERC ne possède pas de connecteur pour l'écran du câble de la tête de lecture, c'est pourquoi il est nécessaire de raccorder celui-ci directement sur l'écran du BUS RS 485.

2.5.1 Magnétique 95T EMR-E

La tête de lecture magnétique 95T EMR-E est présentée en boîtier métallique avec une finition satinée résistante. L'électronique est moulée dans une résine imperméable à l'eau et la tête de lecture elle-même est fabriquée dans un métal inoxydable approprié à une utilisation en extérieur.

La tête de lecture 95T EMR-E est étanche à l'eau (protection IPX7) et peut être utilisé dans une gamme de température ambiante comprise entre -20 et +70°C.

Elle est fournie avec un câble de 5 m pour la connexion directe au lecteur de contrôle d'accès HISEC. Un câble supplémentaire peut être ajouté s'il y a lieu.

L'installation de la tête de lecteur comporte les opérations suivantes :

- Montage de la tête de lecture.
- Raccordement de la tête de lecture au terminal.

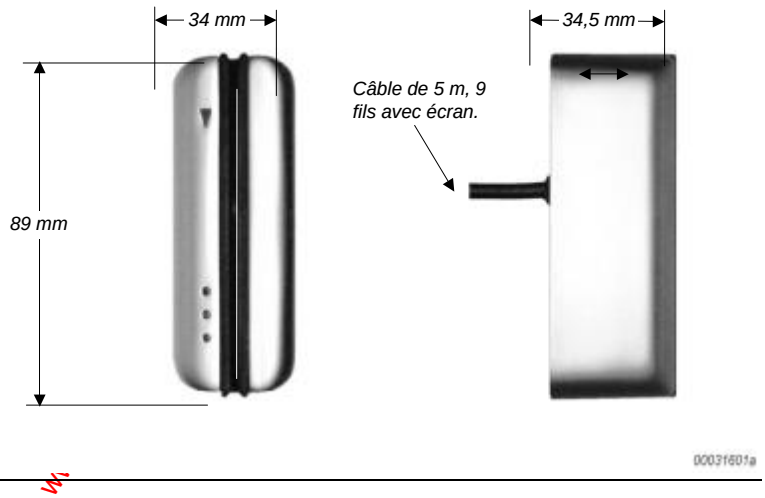
Taille et orientation de support

La tête de lecture 95T EMR-E doit être montée à une hauteur rendant facile la lecture du badge et le défilement du badge dans la tête de lecture. Une hauteur d'environ 1m35 à 1m40 pour le bas de la tête est une hauteur qui conviendra dans la plupart des cas. Il est recommandé de monter la tête de lecture 95T EMR-E avec la fente dans la position verticale.

Accessoires de montage et instructions

Les instructions pour la fixation et le gabarit de perçage sont fournis avec la tête de lecture 95T EMR-E.

Aspect et dimensions de la tête de lecture magnétique 95T EMR-E



Boucles de terre

Pour éviter tout risque de boucle de terre, l'écran du câble de la tête de lecture 95T EMR-E ne doit être connectée à aucun des écrans ou des bornes de connexions du lecteur de contrôle d'accès.

Raccordements 95T EMR _E

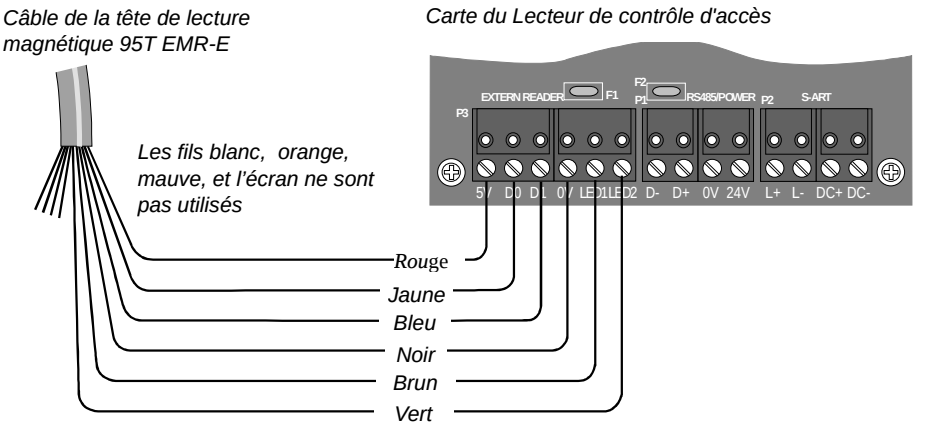


Tableau des Connexions

De la tête 95T EMR-E		*Vers Lecteur de Contrôle d'accès*	
(Câble)		*« LECTEUR EXTERNE »*	
Couleur	***Fonction***	***N° Borne***	***Description***
Rouge	5 Volt	1	"5V"
Jaune	Data	2	"D0"
Bleu	Clock	3	"D1"
Noir	0 Volt	4	"0V"
Brun	LED Rouge	5	"LED1"
Vert	LED Verte	6	"LED2"

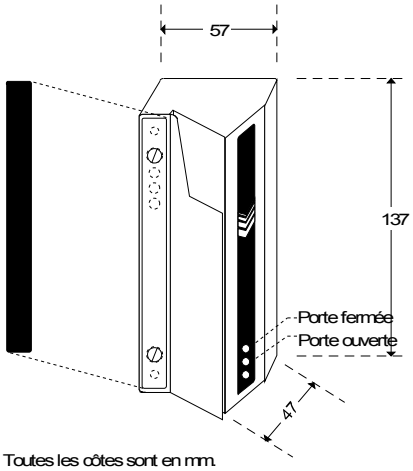
Les fils suivants ne sont **pas** utilisés: blanc, orange, mauve, et écran.

Extension de câble

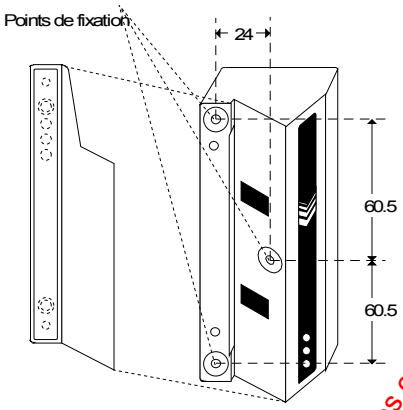
Si la distance entre la tête de lecture et le terminal de contrôle d'accès dépasse 5 m, un câble supplémentaire peut être connecté jusqu'à une longueur totale de 50 m à l'aide d'une boîte de jonction appropriée. Le câble utilisé pour l'extension devra être du même type que celui existant sur la tête de lecture. Toutefois, on n'utilise que les 5 fils + l'écran. L'écran du câble d'extension devra être connecté à l'écran du câble d'origine.

2.5.2 Wiegand

Présentation et dimensions



Toutes les côtes sont en mm.



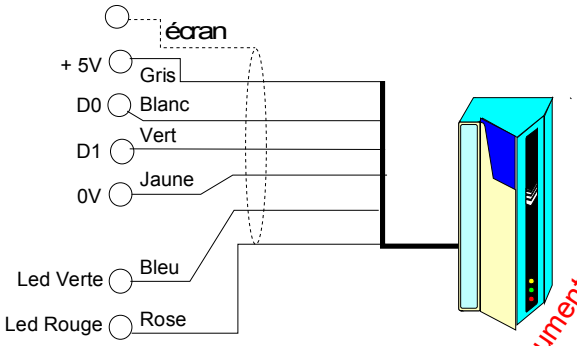
Caractéristiques :

Poids : 40 g
Température de fonctionnement : -30 à +70°C
Humidité : sans importance
Leds d'indication : rouge et verte

Avant de fixer la tête de lecture Wiegand sur le mur, la plaque de façade devra être enlevée en dévissant les 2 vis. Après cela, les 3 points de fixation seront accessibles pour la fixation sur le mur.

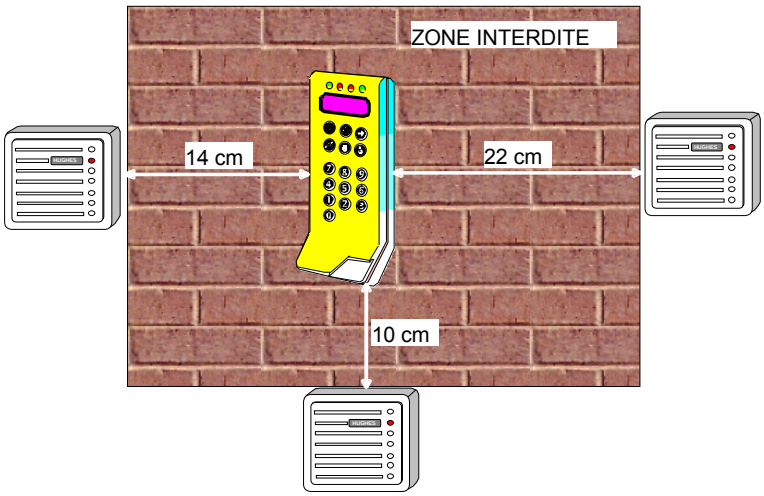
La tête de lecture est fournie avec un câble avec écran de 2,5 m de longueur. Si la distance entre la tête de lecture et le terminal est supérieure un câble avec écran (max. 50m) complémentaire peut être connecté.

Câblage



Important ?!! Les écrans des deux câbles devront être reliés ensembles.

2.5.3 Conseils d'installation des antennes

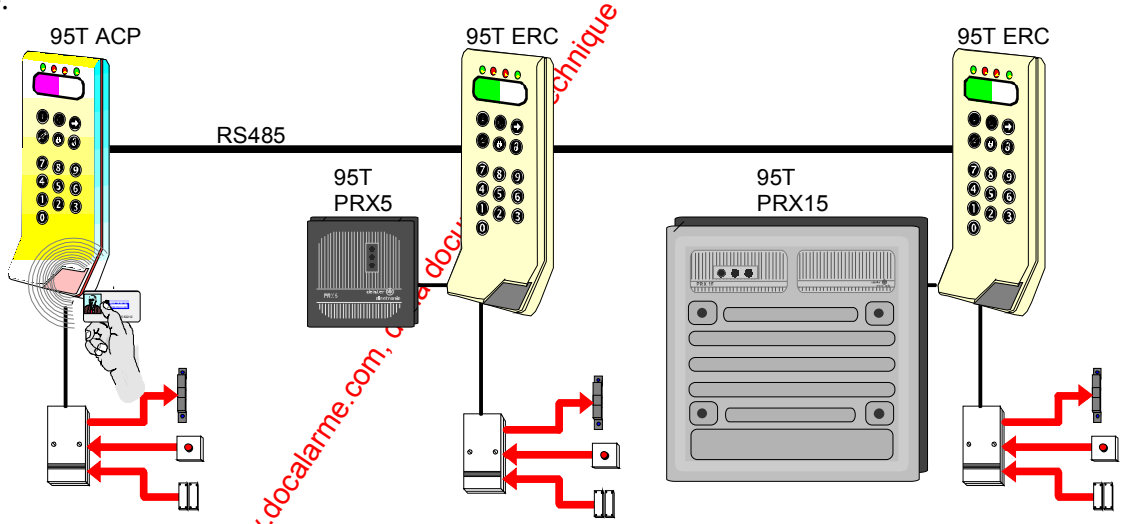


L'installation des contrôleurs ERC avec des antennes Proximité impose de respecter des distances minimum entre les appareils pour obtenir la portée maximum des antennes. Le schéma ci-contre donne les distances minimum à respecter pour les antennes. Prière de remarquer que ces distances ne sont pas les seules causes de détériorations de portée des têtes il est à s'assurer de la présence de moniteurs couleurs, ascenseurs, etc.)

2.5.4 Proximité DEISTER (PASSIF)

La gamme des antennes proximités DEISTER comprend un nombre important de références en fonction des applications et des distances de lectures. Dans cette notice seuls sont décrits les éléments 95T ACP (M)- tête incorporée, 95T PRX 5 et 95T PRX 15. Pour les autres besoins ou portées différentes prière de contacter le support technique HISEC.

La figure ci-dessous représente une configuration simple avec les différents types de lecteurs et têtes de lecture.

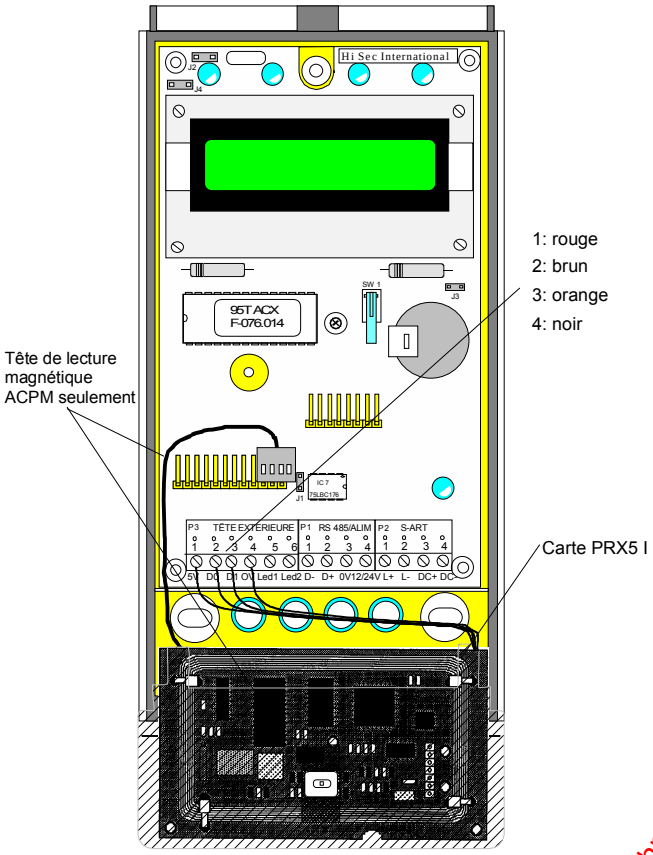


Un contrôle "**simple porte**" sera constitué des éléments suivants:

1 Terminal/Lecteur.....95T ERC
1 S-art pour le contrôle de la porte.....90T S102
1 Antenne Proximité porte max. 12,5 cm.....95T PRX5
Proximité porte max. 60 cm.....95T PRX15

Prière de noter que les lecteurs 95T ERC devront être configurés en mode interface Wiegand (J4 enlevé).

2.5.4.1 Les Lecteurs 95T ACP et 95T ACPM



Caractéristiques :

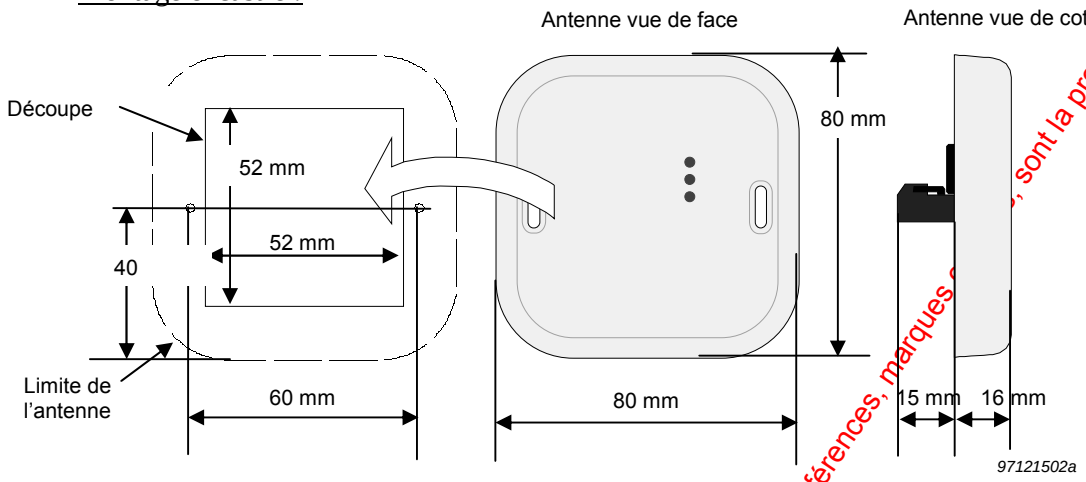
Température de fonctionnement :
sans chauffage : -5 à +60°C
avec chauffage : -15 à +60°C (12V DC)
avec chauffage : -25 à +60°C (24V DC)
Alimentation : 8-30V
Consommation: < 150mA
Portée : jusqu'à 5 cm en fonction de l'installation et du type de badge.

Pour les spécifications complémentaires (stapp, config., etc) se reporter directement au chapitre 2.1.1.

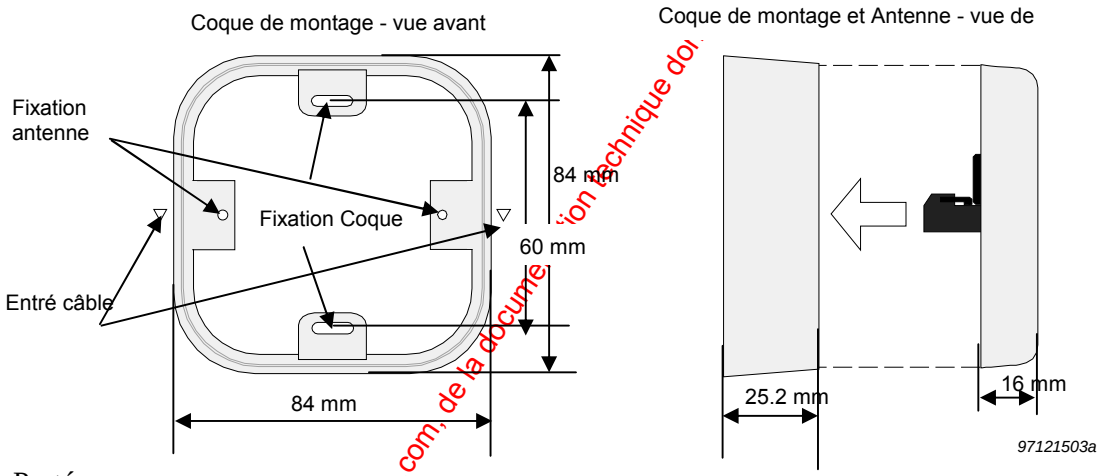
2.5.4.2 Antenne proximité PRX 5

Tête de lecture de proximité destinée à être installé a l'intérieur ou à l'extérieur des bâtiments. Son raccordement est réalisé sur bornier débrochable. Sa fixation peut se faire de façon classique en saillie, encastré, monté dans une boite électrique standard. Utilisable par tous les badges Passifs DEISTER et panachable avec les autres têtes de la gamme DEISTER

Montage encastré :



Montage en saillie :



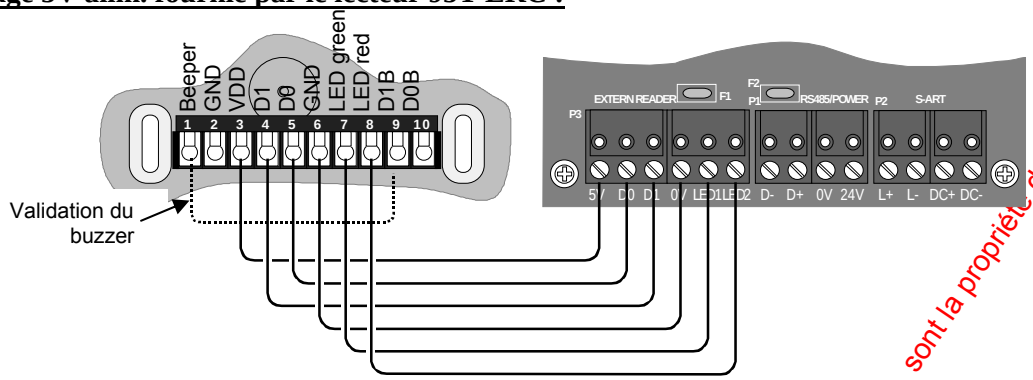
Portée :

Badges PC 101 : 12 cm max. - Badges PC 112 : 8 cm max. - Badges PC K : 8 cm max.

Caractéristiques:

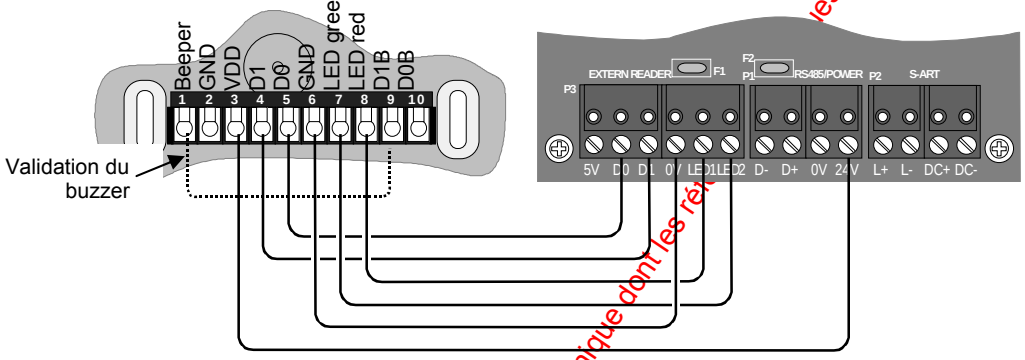
Dimensions: 80x80x16 mm
Présentation : Boîtier ABS noir, électronique moulée
Installation : Encastré
En saillie, avec coque de montage AP5 (en option), obligatoire sur support métallique.
Encastré dans une boite électrique standard
Température de fonctionnement: -25 à +70°C
Indice de protection : IP 65 suivant option de montage.
Alimentation : 8-14V DC
5V DC +/- 10% à préciser à la commande
Consommation : < 100mA
Fréquence de travail : 125 kHz
Distance max. entre antenne et lecteur 95T ERC : 2m50 câble avec écran si utilisation du 5V lecteur
50m avec alimentation externe 12V

Câblage 5V alim. fournie par le lecteur 95T ERC :



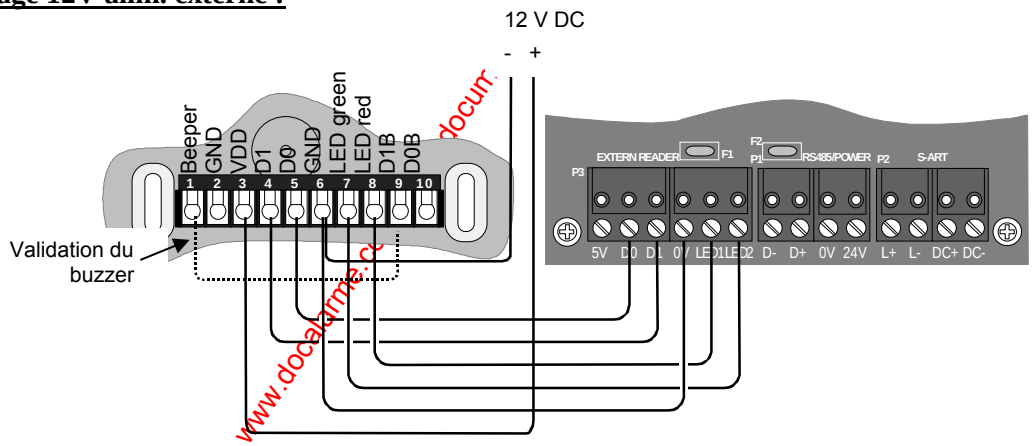
97121601a

Câblage utilisant le 12V du système :



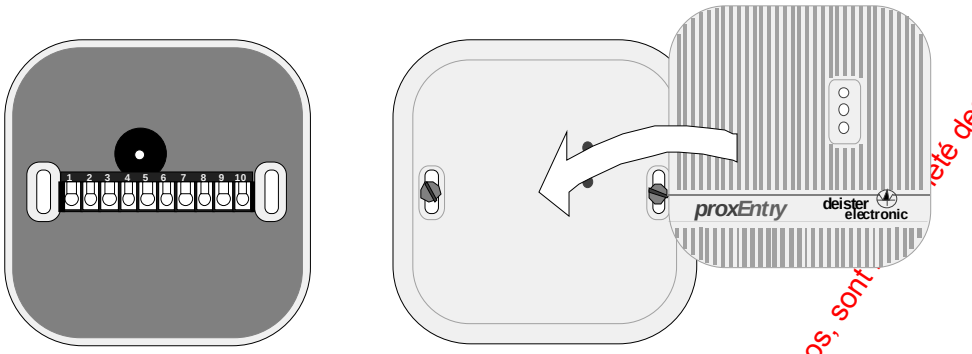
97121902a

Câblage 12V alim. externe :



97121902b

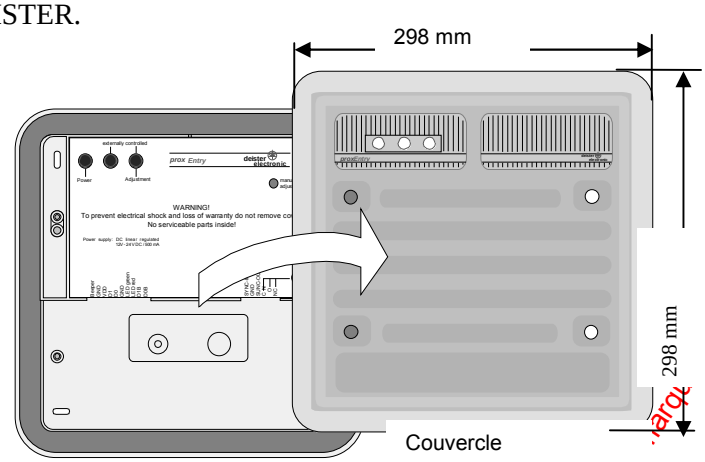
Fermeture :



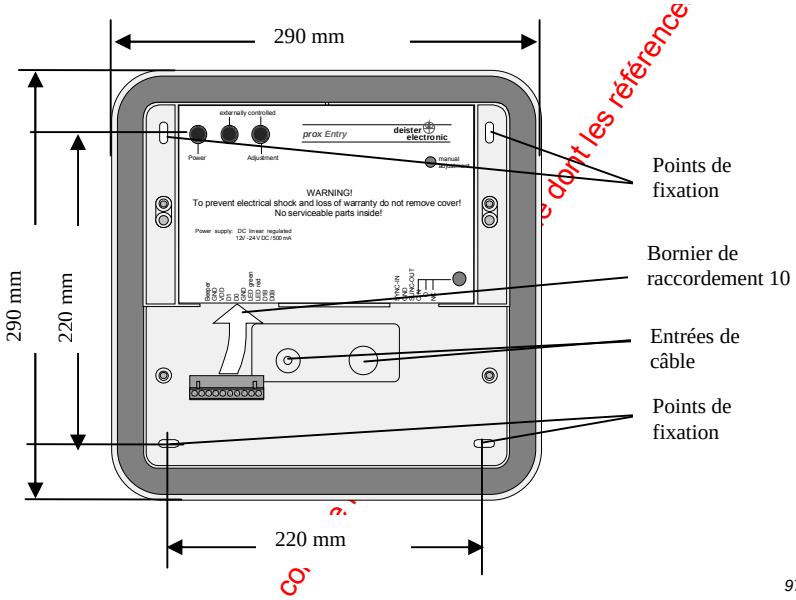
97121504a

2.5.4.3 Antenne Proximité PRX 15

Tête de lecture destinée à être installée à l'intérieur des bâtiments (95T PRX 15) et à l'extérieur (95T PRX 15-O). Son raccordement est réalisé sur bornier débrochable. Sa fixation peut se faire de façon classique en saillie ou encastré. Utilisable par tous les badges Passifs DEISTER et panachable avec les autres têtes de la gamme DEISTER.



98010801a



97122201a

Portée :

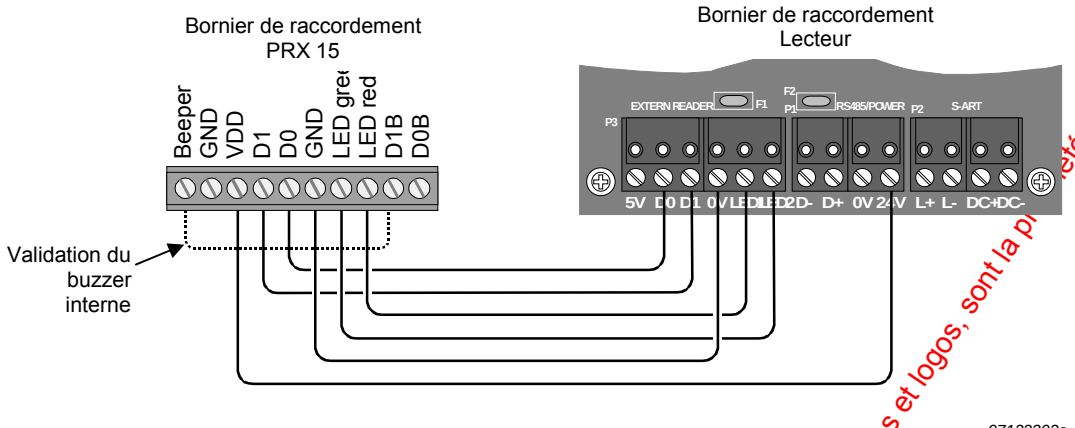
Badges PC 101 : 60 cm max. Badges PC 112 (114): 45 cm max. Badges PC K : 45 cm max.

Caractéristiques:

Dimensions: 300x300x25 mm
Présentation : Boîtier ABS noir, électronique moulée
Installation : En saillie, support non métallique.
Température de fonctionnement: en standard +5 à +60°C
Indice de protection : IP 54.
Alimentation : 24V DC +/- 25%
Consommation : < 500mA
Fréquence de travail : 125 kHz
Distance max. entre antenne et 95T ERC : 25m

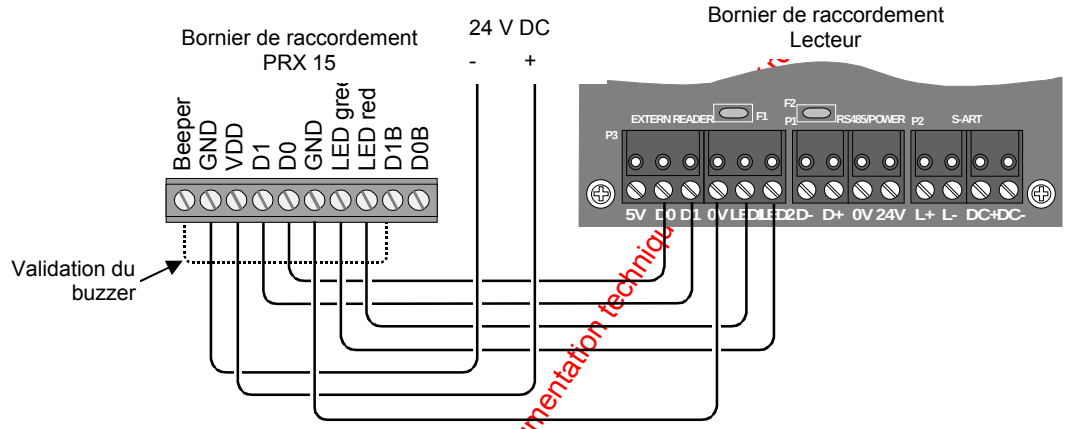
Câblage :

Utilisation de l'alimentation 12 ou 24V des lecteurs :



97122302a

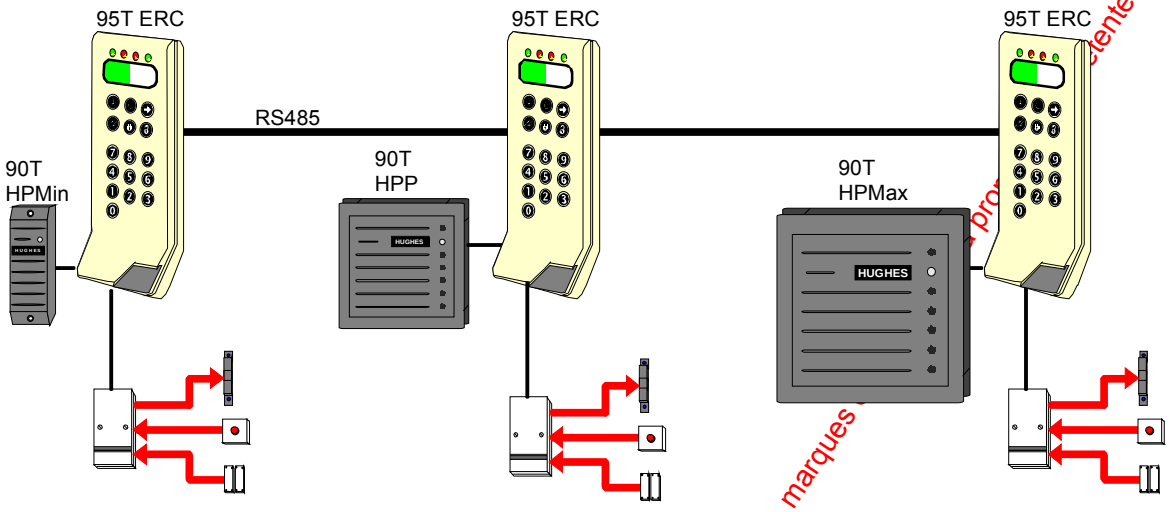
Utilisation d'une alimentation extérieure :



97122301a

2.5.5 Proximité HID Hughes (PASSIF)

La figure ci-dessous représente une configuration avec les différents types de têtes de lecture.



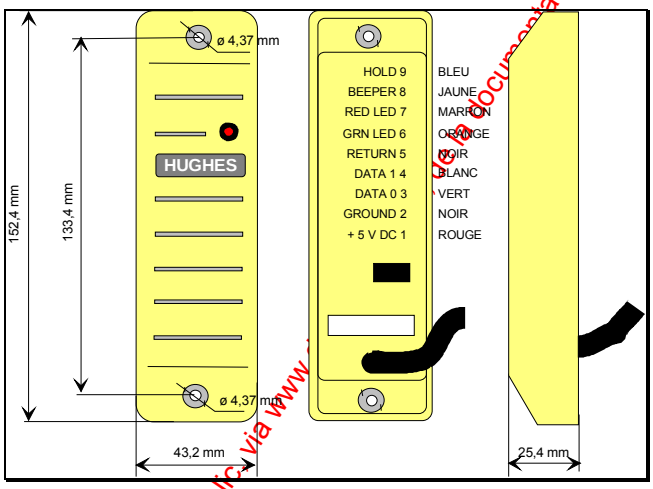
Un contrôle "**simple porte**" sera constitué des éléments suivants :

1 Terminal/Lecteur.....95T ERC
1 S-art pour le contrôle de la porte 90T S102
1 Antenne Proximité porte max. 10 cm.....90T HPMin
Proximité porte max. 20 cm.....90T HPP
Proximité portée max. 60 cm.....90T HPMax

Prière de noter que tous les terminaux lecteurs 95T ERC devront être configurés avec une interface Wiegand.

2.5.5.1 Présentation et dimensions

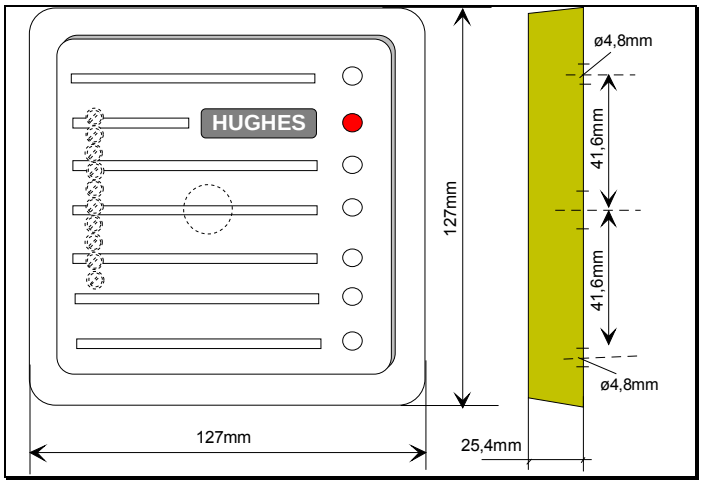
MINIPROX



Caractéristiques :

Portée : Badges Standard ..... 10-14 cm
Portée : Badges Isoprox..... 8-12 cm
Poids : 108g
Température de fonctionnement:-30 à +65°C
Humidité : 0-95% non condensée
Alimentation (fournie par le lecteur): 5V
Consommation Repos 50 mA (80 mA en activation)
Led's d'indication : Rouge et Verte

PROXPRO

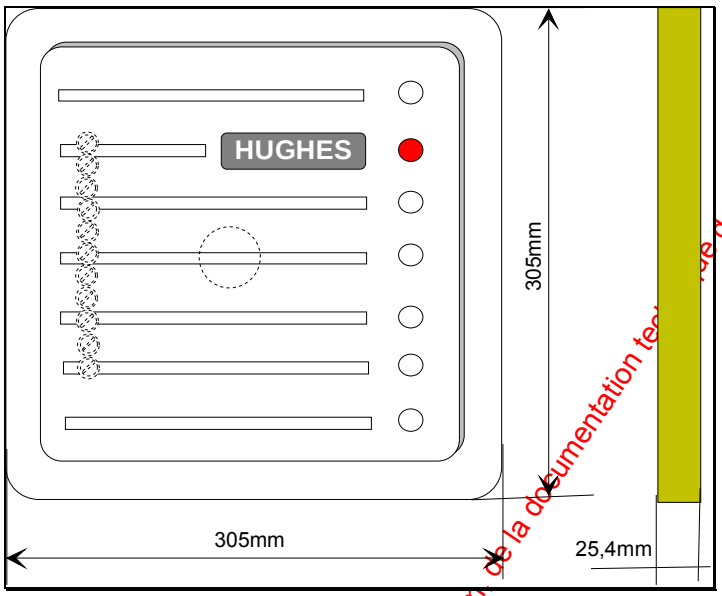


Caractéristiques :

Portée : Badges Standard..... 14-20 cm
Portée : Badges Isoprox ..... 14-18 cm
Poids : 336g
Température de fonctionnement :-30 à +65°C
Humidité : 0-95% non condensée
Alimentation : 10-28,5 V (pas d'alimentation à découpage) *voir nota
Consommation: Repos 100 mA (160 mA en activation)
Leds d'indication : Rouge et Verte

Nota: Attention les anciennes têtes de lectures ref. PR 5350 ne fonctionnaient pas au-dessus de 26V

MAXIPRO



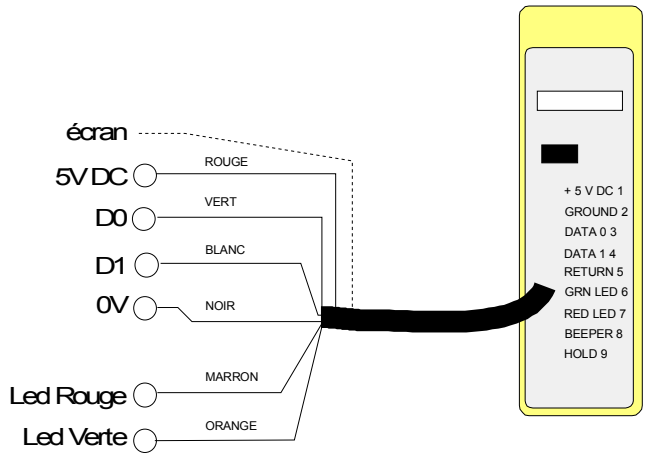
Caractéristiques :

Portée : Badges Standard .....46-61 cm
Portée : Badges Isoprox .....46-61 cm
Poids : 1,4 Kg
Température de fonctionnement : -30 à +65°C
Humidité : 0-95% non condensée
Alimentation : 14-28,5 V (pas d'alim à découpage)
Consommation : Repos 200 mA (1,5 A en activation)
Leds d'indication :Rouge et Verte

2.5.5.2 Câblage et Configuration

MINIPROX

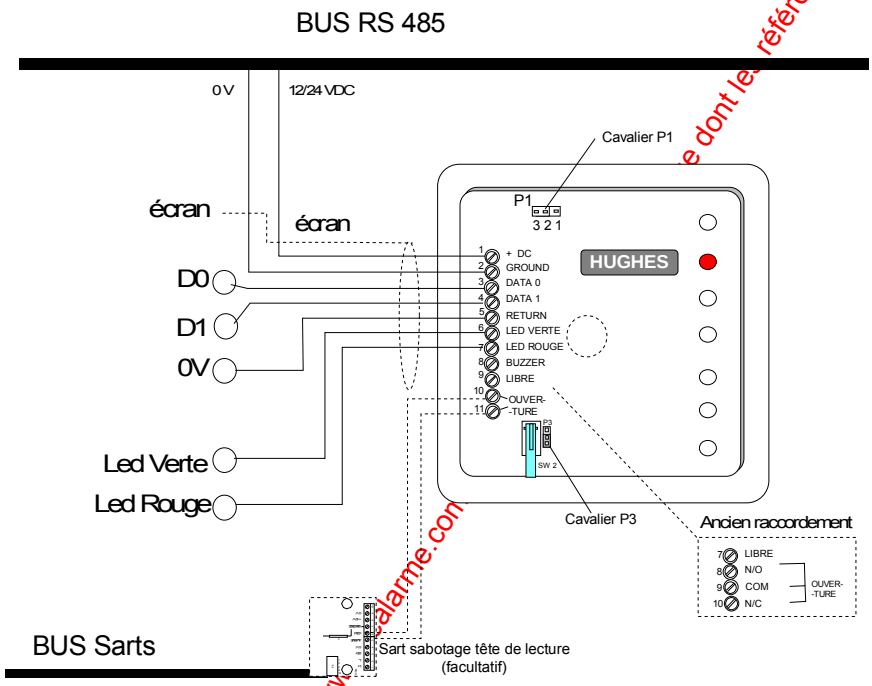
La tête de lecture est fournie avec un câble avec écran de 1 m 50 de longueur. Si la distance entre la tête de lecture et le terminal dépasse 4 m un câble complémentaire peut être connecté.



Le câble avec écran reliant les 2 unités ne devra pas dépasser 50m.

Aucune configuration n'est nécessaire.

PROXPRO



Câblage :

Le câble avec écran reliant les 2 unités ne devra pas dépasser 50m. L'utilisation d'un câble faradisé de type BELDEN 8786 (22AWG) autorise une longueur de 150m.

Cette tête de lecture possède un contact d'ouverture qui pourra être relié à un sart pour surveiller l'accès à la tête de lecture.

Il est nécessaire d'alimenter le lecteur par le bus RS485 (ou par une source auxiliaire, dans ce cas ne pas oublier d'assurer un zéro commun entre les alimentations) étant donné que dans le câble de sortie du contrôleur l'on ne dispose que de 5V.

Le cavalier P3 permet de choisir le sens du contact d'ouverture du boîtier (si utilisé), par défaut il est en position 2-3 c'est à dire NF.

Les anciennes têtes de lectures ne possèdent pas ce cavalier, les contacts Commun, NO, NF étant directement disponibles sur le bornier. Sur ces anciennes têtes le contrôle de la led rouge est impossible.

Configuration :

Switch miniature SW1: il permet de configurer la tête de lecture, cet interrupteur est configuré à la livraison pour fonctionner directement sur les lecteurs HI SEC.

Rappel de la configuration par défaut :

1	2	3	4	5	6	7	8
ON	ON	OFF	ON	OFF	ON	ON	ON

Il est possible de couper le buzzer incorporé à la tête de lecture en positionnant le Switch N°2 sur OFF.

Cavalier P1:

Ce cavalier permet de préciser sur quel type de support la tête de lecture sera fixée, métallique ou autre.

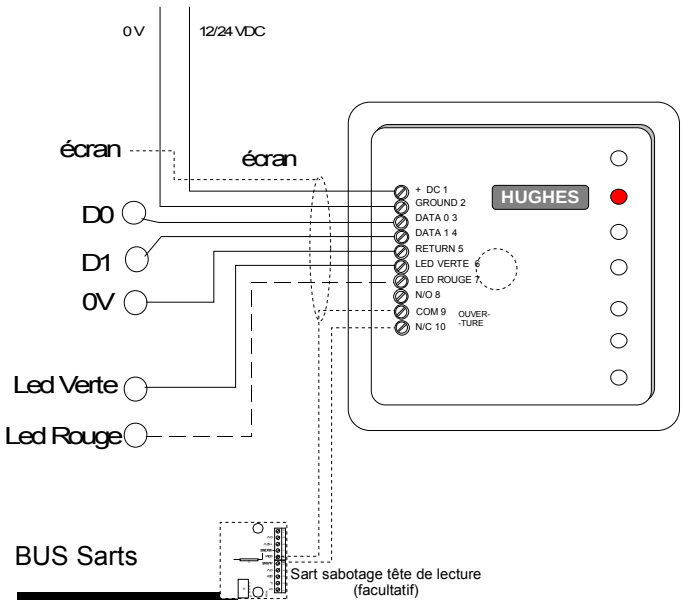
Sur un support métallique il devra être en position 1-2, sur les autres supports il devra être sur **2-3** (valeur par défaut).

Attention : Les anciennes têtes de lecture ProxPro Hughes réf. PR 5350 ne pouvaient pas être alimentées au-dessus de 26V, dans le cas d'un chargeur HISEC fournissant du 27V (non réglable), il est nécessaire d'insérer dans le + alim une série de 4 diodes 1N 4000, pour baisser la tension.

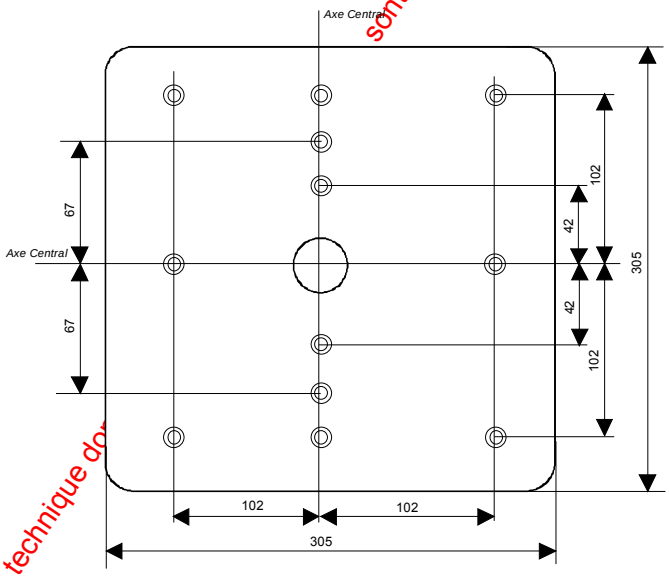
Les têtes ProxPro Hughes réf. PR 5355 n'ont plus cet inconvénient (fonctionnement jusqu'à 28,5V).

MAXIPRO

Alim 24V 1,5A



Fixation :



Câblage :

Le câble avec écran reliant les 2 unités ne devra pas dépasser 50m. L'utilisation d'un câble faradisé de type BELDEN 8786 (22AWG) autorise une longueur de 150m.

Attention : Il est nécessaire de prévoir une alimentation par tête de lecture étant donné la consommation très élevée de ce modèle.

Cette tête de lecture devra être installée à une distance minimum de 15 cm de toute surface métallique.

Configuration :

Switch miniature SW1: il permet de configurer la tête de lecture, cet interrupteur est configuré à la livraison pour fonctionner directement sur les lecteurs HI SEC.

Rappel de la configuration par défaut :

1	2	3	4	5	6	7	8
ON	ON	OFF	ON	OFF	ON	ON	ON

Il est possible de couper le buzzer incorporé à la tête de lecture en positionnant le Switch N°2 sur OFF.

Self d'optimisation :

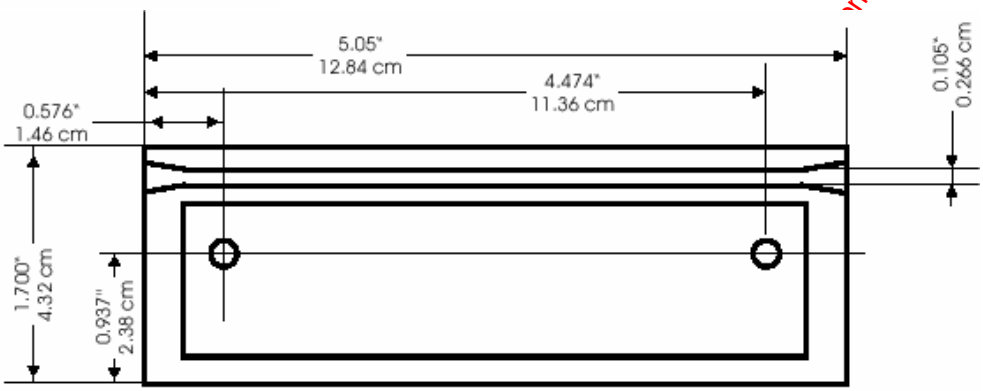
Une self (ferrite) permet d'ajuster au moyen d'une LED de contrôle la réjection des champs extérieur, en ajustant cette self (attention ce composant est fragile et le réglage fin) la LED (DS1) doit clignoter verte, le clignotement rouge indiquant la présence d'une perturbation.

Après optimisation il est nécessaire de re-vérifier la portée de la tête.

2.5.6 Codes à barres Infrarouges 95T EIRS

2.5.6.1 Présentation et dimensions

Poids : 170 g
Température de fonctionnement : -30 à +70°C
Matériau : polycarbonate noir
Leds d'indication : rouge
Consommation : 50 mA
Dimensions: 128x 43 x 39 mm



Types de codes barres infrarouges acceptés (**max. 16 caractères**); Code 39, 2 parmi 5, Codabar, UPC-A, UPC-E, EAN, Code 11, Code 93, Code 128, MSI.

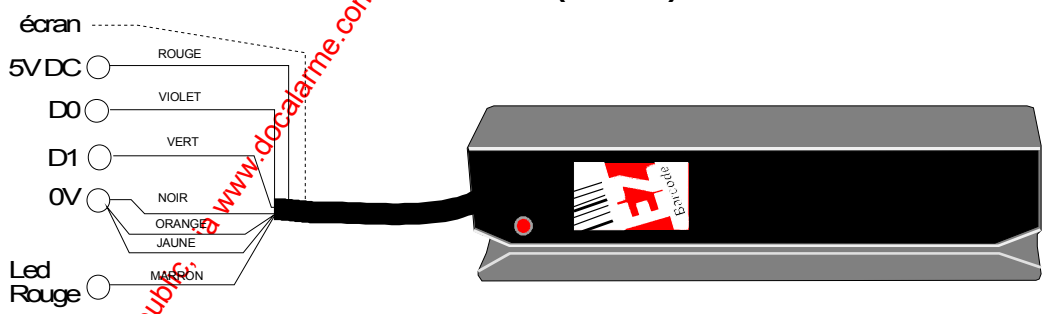
2.5.6.2 Configuration et Initialisation

Il n'existe pas de badge Maître et Maintenance au format Infrarouge, c'est pourquoi il est impératif d'initialiser le lecteur (Menu 82) au moyen d'une tête magnétique temporaire (ne pas oublier de programmer le format libre **BFORM=06**), donc il faudra posséder les badges précédemment cités avec le même code site que le logiciel (si existant).

Pour les lecteurs 95T, il est intéressant d'utiliser des modèles 95T ACM, de cette façon la tête magnétique incorporée est toujours disponible pour les opérations de maintenance.

Les Lecteurs devront être en position câblage **Wiegand**: J4 enlevé

Tête de lecture à moins de 10m du contrôleur (alim 5V)



2.6 Le coffret d'Alimentation 95T-PS 24/3.8

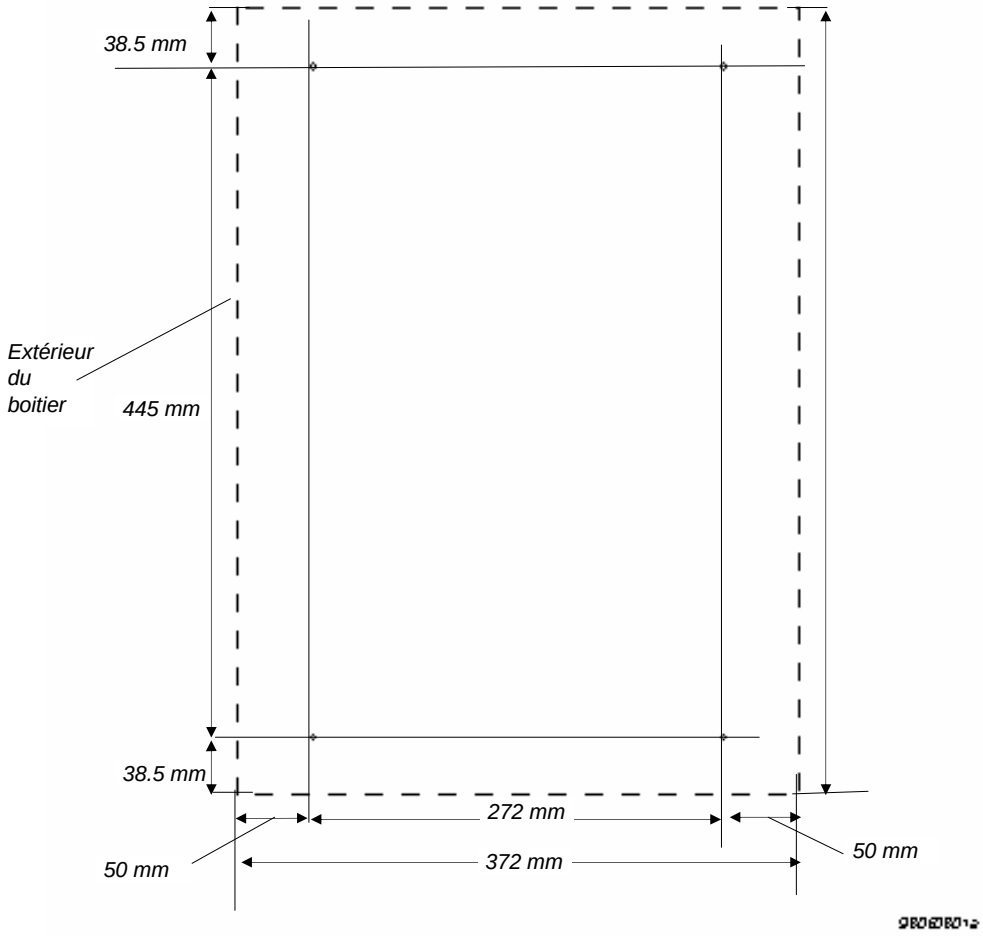
L'alimentation - Chargeur 95T PS 24/3,8 est basée sur la même carte que la centrale 95T CU-30-24V. Sur la carte interface de l'alimentation est également implanté un S-ART pour surveiller l'alimentation.

2.3.4 Montage

Le coffret sera fixé à l'aide de quatre vis ayant un diamètre approximatif de 5 millimètres. Ne pas employer de vis de plus petite taille, les vis de fixation doivent pouvoir supporter le poids des batteries de secours.

Marquer les trous à forer pour les vis de fixations. Vous pouvez marquer leur position en utilisant les trous de fixation du coffret ou en employant les côtes du plan de perçage ci-dessous.

Position des points de fixations.



Avant de fixer définitivement le coffret, insérer tous les câbles à relier dans le coffret en passant par les découpes et les canons isolants.

Le câble secteur doit être passé dans le canon isolant situé sur le côté supérieur gauche du coffret.

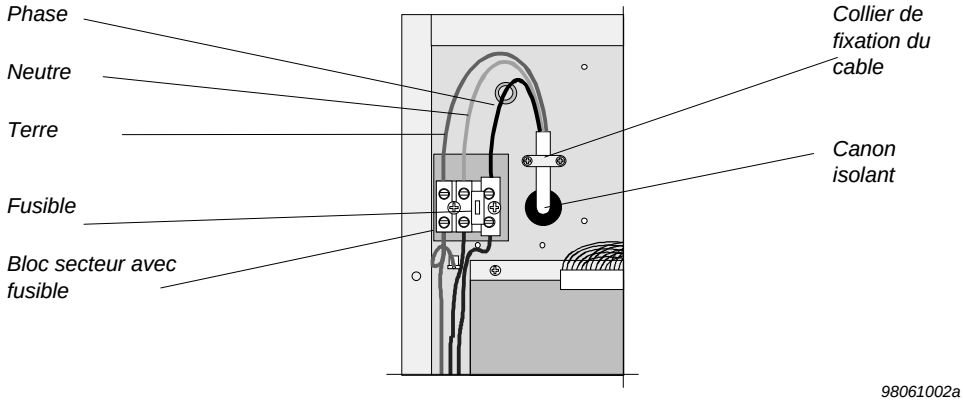
Vous êtes maintenant prêt à relier le secteur comme décrit dans la section suivante.

2.3.5 Raccordement du secteur

L'alimentation 95T PS 24/3.8 doit être raccordée au secteur (AC) comme représenté sur la figure ci-dessous. Se rappeler que les règlements locaux peuvent exiger que la centrale soit installée avec un organe de coupure secteur.

+ La directive basse tension EN 60-950 exige qu'un équipement connecté de manière permanente soit protégé avec un dispositif aisément accessible de déconnexion.

Montage et raccordement du câble secteur.



Fusible L'arrivée secteur est équipée d'un fusible (1A lent) en série avec la borne de phase.

Ne pas alimenter Ne mettre sous tension avant d'avoir réalisé le montage et le raccordement des batteries de secours comme décrit dans la section suivante.

2.3.6 Installation des batteries de secours

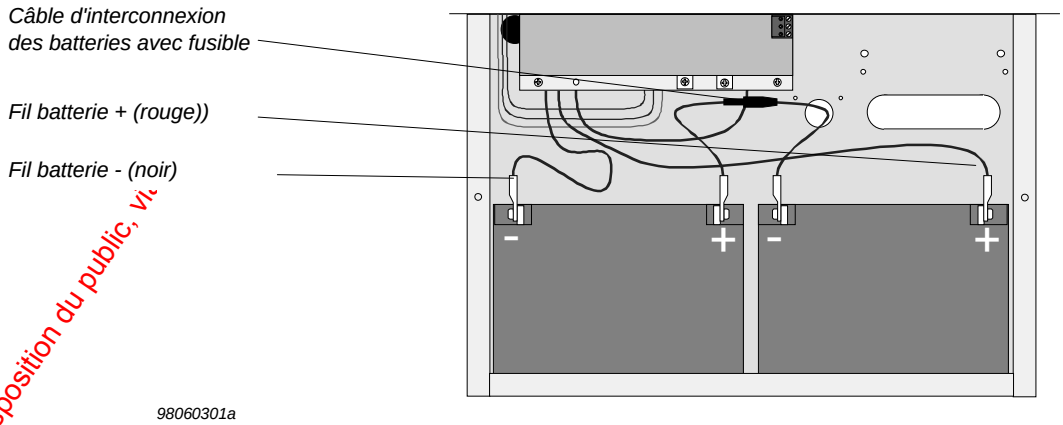
Information générale Le coffret unité centrale peut accepter deux batteries de secours de 12 V/24 Ah. Les batteries ne sont pas fournies avec la centrale.

Les batteries ne doivent pas excéder les dimensions suivantes:

Hauteur : 170 mm ; Largeur: 172 mm ;

Profondeur: 129 mm

Position et raccordement des batteries de secours.



Câble d'interconnexion Trouver le câble d'interconnexion et ouvrir le support de fusible. Enlever le fusible pour séparer le câble en deux parties

Monter la première moitié du câble d'interconnexion sur la borne positive d'une des batteries. Monter l'autre moitié du câble d'interconnexion sur la borne négative de l'autre batterie.

Batterie gauche Placer la batterie de gauche avec l'orientation montrée sur la fig. 5, de sorte qu'elle repose sur le bord

du coffret et que la borne négative soit accessible pour le raccordement

Batterie droite

Monter le fil négatif (noir) de la carte alimentation. Une fois fait, le pousser soigneusement en place.

Placer la batterie droite avec l'orientation montrée sur la fig. 5, de sorte qu'elle repose sur le bord du coffret et la borne positive soit accessible pour le raccordement

Montage fusible

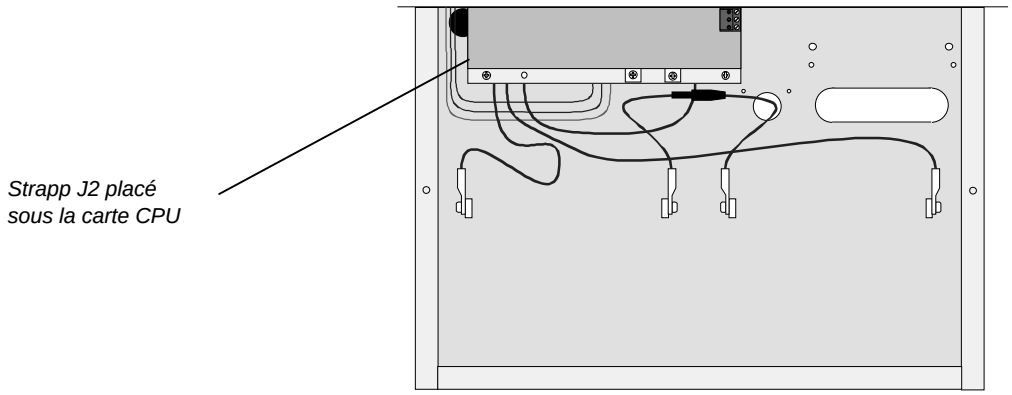
Monter le fil positif (rouge) de la carte alimentation. Une fois fait, le pousser soigneusement en place. S'assurer qu'aucun conducteur ou borne de câble n'est en contact avec le coffret avant de remettre en place le fusible.

2.6.1 Information Générale 95T PS 24/3.8.

L'alimentation peut être configurée pour 2 types de fonctionnement différents en fonction de la position du strapp J2. Le strapp J2 est accessible sur la carte alimentation elle-même (voir le schéma suivant).

☛ **Le strapp est par défaut présent (installé) et donnera le maximum de courant disponible à l'installation.**

Position du strapp J2



98060301b

Pour la position du strapp J2, se référer également au schéma du chapitre suivant.

Spécifications Techniques:

Courant de Charge (J2 installé - défaut) ***1.2A***

Courant de Charge (J2 enlevé) 1.8A

Défaut Batterie ..... 21.0V +/- 0.5V

Protection de décharge basse tension ..... 20.0V +/- 0.5V

Compensation en température de la tension de charge ..... - 36mV / ^{0}C

Courant externe pour l'installation (J2 installé - défaut) ***2.4A***

Courant externe pour l'installation (J2 enlevé)..... *1.8A*

Tension de sortie (secteur présent) ..... 28.5V +/- 0.5V

Bruit ..... max. 200 mV $_{p-p}$

Tension de sortie (secteur absent) ..... min. V_{bat} – 1V

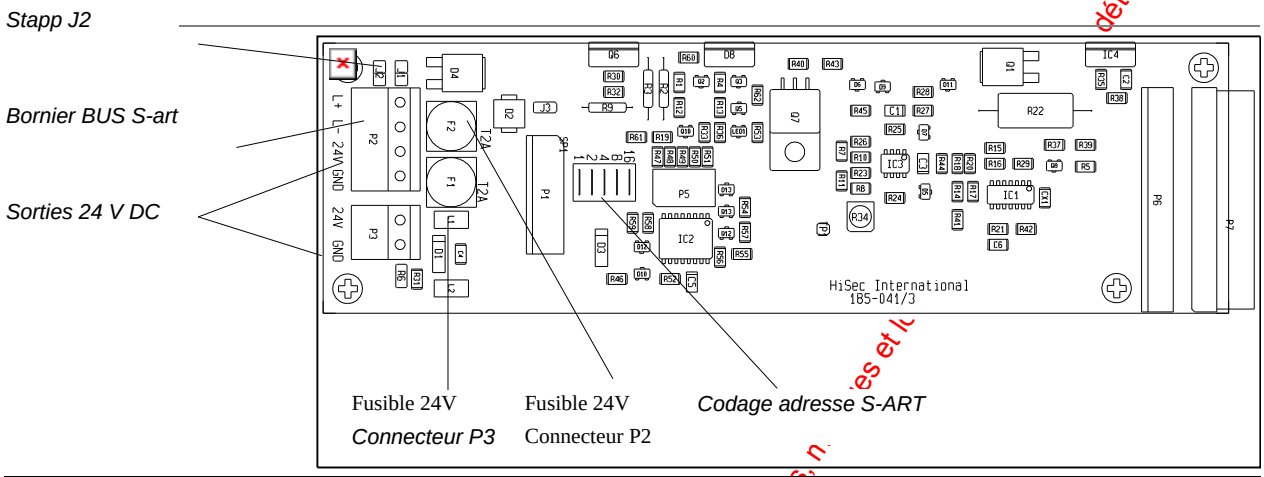
Tension d'alimentation secteur..... 176 – 264 VAC

Gamme de Température ..... -10 ^{0}C - +55 ^{0}C

2.6.2 Diagramme de raccordements 95 PS 24/3.8

La figure suivante montre la disposition de la carte interface de l'alimentation.

Disposition de la carte interface de l'alimentation.



L'alimentation 95T PS 24/3,8 peut surveiller l'état de charge des batteries reliées et la présence secteur. L'interface est faite au moyen d'un S-ART intégré.

Les connexions du bus S-ART sont décrites suivant le schéma ci-dessus. L+ et L- respectent le standard des autres produits HISEC.

Deux sorties 24V protégées par fusible sont disponibles sur les borniers P2 et P3. Ces deux sorties sont protégées par des fusibles rapides 2A.

✖ ***Prière de noter que les bornes 24V sont des sorties d'alimentation et ne doivent jamais être reliées à une autre source alimentation.***

Les entrées du S-ART sont reliées en interne comme suit:

IN0	= Surveillance batterie (défaut batterie en dessous de 20V DC)
IN1	= Surveillance secteur.
OUT1	= Test batterie. (Courant de Test : 1.5A)

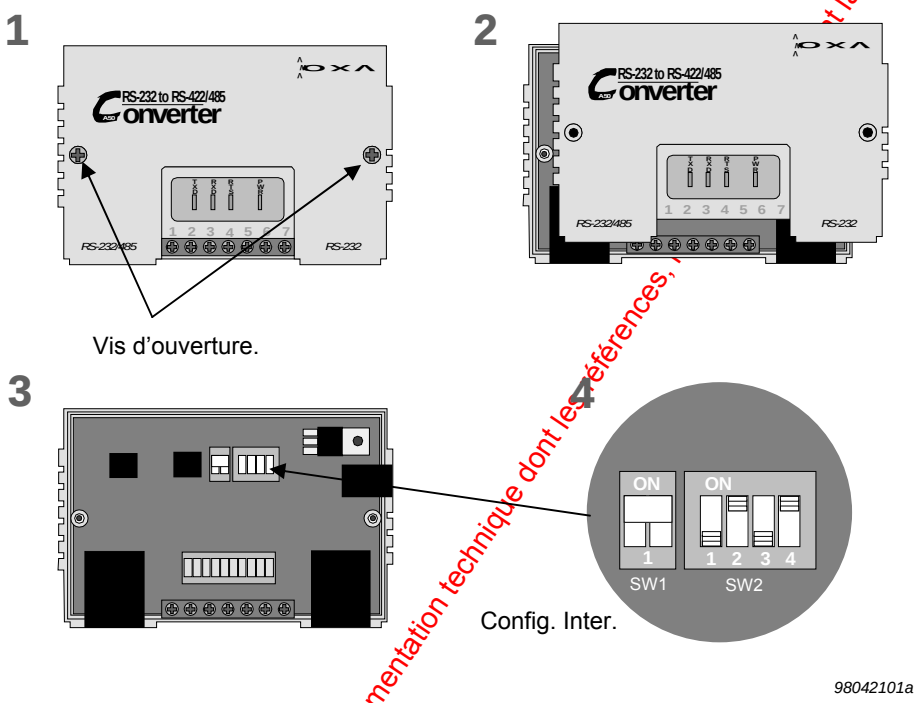
Le contact d'ouverture du coffret est placé en série avec le signal du bus S-ART et donnera un message de sabotage 4.

2.7 Interface de Programmation 95 T PCI

L'interface 95 T GPI permet de programmer le système HISEC, c'est l'interface du technicien de maintenance. Elle ne sera jamais connectée en permanence sur une installation, mais seulement utilisée le temps de programmer ou de charger une programmation.

Configuration :

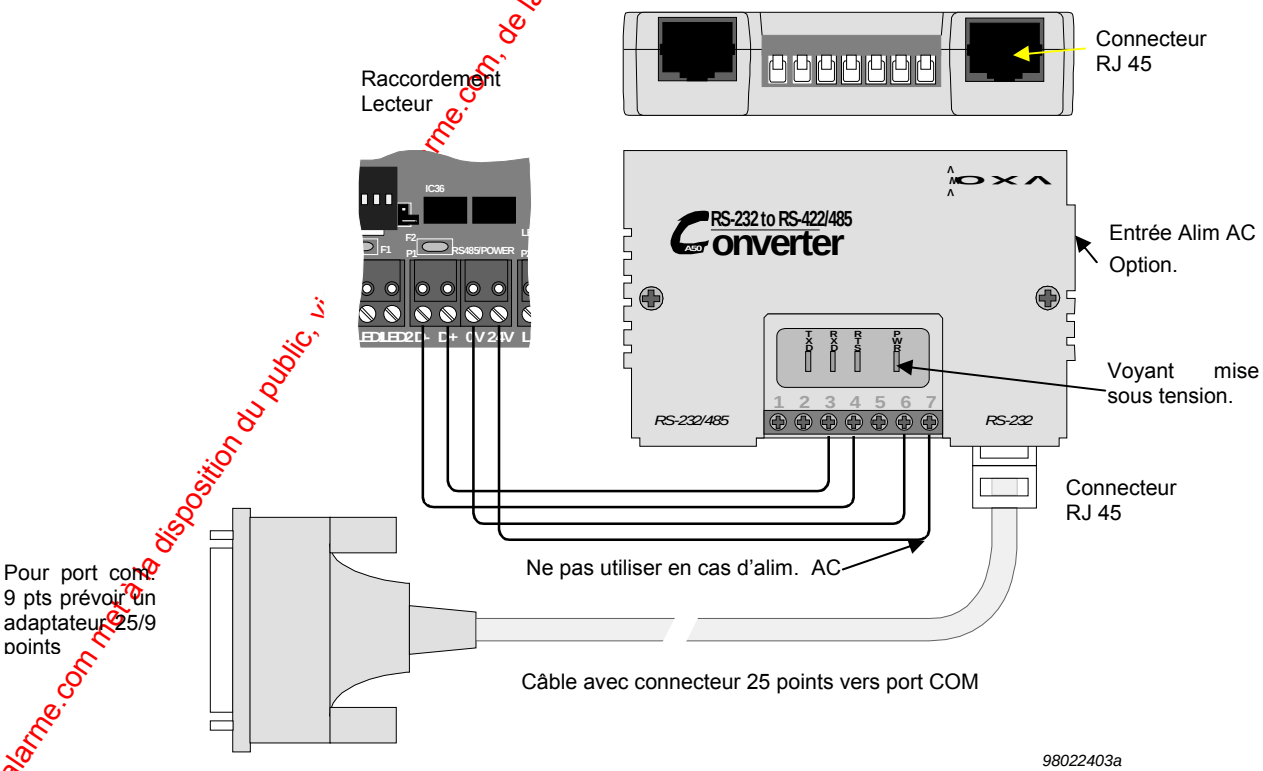
Avant la première utilisation, il est nécessaire de configurer cette interface pour fonctionner avec le système HISEC. La procédure d'ouverture et la position des micro-interrupteurs est décrite sur le schéma ci-dessous.



98042101a

Cette opération n'est à effectuer qu'à la première utilisation de l'interface 95 T PCI.

Connexion :



98022403a

2.8 Longueur de câble et dimensions

Du fait de l'installation des divers périphériques sur le système par ex.: avertisseurs acoustiques (sirènes) et optiques, claviers déportés et S-ART, les longueurs de câbles et les consommations devront être calculées pour déterminer la taille des câbles à utiliser.

Pour le bus Multi-Points RS 485, un câble avec écran et paire torsadée est recommandé. La longueur totale ne devra pas dépasser 1200m, et la tension d'alimentation à la fin de la ligne ne devra pas descendre au-dessous de 10 V. Tous les équipements de cette ligne devront être connectés en série, les "câblages en étoile" excédant 0,3m ne sont pas autorisés.

Pour les Bus de S-ART, un câble sans écran avec paire torsadée est conseillé. La longueur totale incluant les "câblages en étoile" ne devra pas dépasser 500m. La tension de ligne à l'extrémité du point le plus éloigné ne devra pas descendre en dessous de 12V (valeur normale 15V).

Les chutes de tension pour un câble 2 fils (les deux conducteurs inclus) peuvent être calculées à partir de la formule suivante :

Ua = (Rd x Idc x L) : 500, ou

Ua = chute de tension en ligne.
Rd = résistance du fil en Ohm/m.
Idc= courant consommé.
L = longueur du câble en mètres.

Résistance d'un câble de 0,6mm de diamètre (0,25 mm²) Rd= 6,15 Ohm/100m.
Résistance d'un câble de 1,0mm de diamètre (0,75 mm²) Rd= 2,32 Ohm/100m.
Résistance d'un câble de 1,4mm de diamètre (1,50 mm²) Rd= 1,16 Ohm/100m.
Résistance d'un câble de 1,8mm de diamètre (2,50 mm²) Rd= 0,69 Ohm/100m.

2.9 Consommation

Lecteur de Badges	24V/90 mA	24V/95 mA
	12V/90 mA	12V/155 mA
avec chauffage	24V/375 mA	12/230 mA
Interface imprimante	24V/200 mA	12V/100 mA
S-ART 90T-S102	24V/12mA	12V/6mA
		17V/2mA

(Ces valeurs sont données pour un S-ART, Clavier etc.).

Les valeurs données ci-dessus ne seront pas seulement utilisées pour calculer la longueur et la taille des câbles, mais aussi pour calculer la consommation totale et la capacité des batteries nécessaires

La consommation de la gâche électrique (50 à 500 mA) devra bien sur être aussi prise en considération dans ce calcul.

Pour le calcul de la capacité des batteries nécessaires, la consommation est le total des consommations sur le (12)24V et le 17 V.

Programmation

3 Programmation

3.1 Généralités

Toute la programmation peut être effectuée directement sur le lecteur HISEC. Prière de se référer au *Chapitre 4.3 "Panorama des Menus"* pour avoir une vue générale de cette programmation. Chaque menu principal possède un numéro et peut être appelé directement en composant celui-ci au clavier. Si l'utilisateur ne dispose pas de ce numéro, il est toujours possible d'aller dans le menu désiré en répondant par "OUI = ➔" ou par "NON = ⬇" aux questions sur l'afficheur.

A la mise sous tension le lecteur, s'il est initialisé en mode 2 ou 3, affiche le message "CONNECTING MMP" (MMP = Protocole Multi-Maitres) jusqu'à ce que le protocole soit accepté. Si la connexion s'avère impossible (pour cause de mauvais raccordement ou autres problèmes) le lecteur passe en mode autonome.

Si le lecteur est programmé à l'Adresse 00, il affichera ensuite l'heure et la date avec le message "DEFAUT COMM." avec la possibilité de lire le badge maintenance si besoin.

Un lecteur non-initialisé démarre toujours en affichant l'heure et la date, étant donné qu'il n'a pas besoin du Bus RS 485.

Si un lecteur appartenant à un système Multi-lecteurs est hors circuit l'afficheur donne le message suivant message "DEFAUT COMM.". De ce fait le lecteur refusera de réaliser certaines programmations étant donné qu'il n'a plus de connexion avec les bases de données des autres lecteurs.

En Appendice A, sont fournies des fiches de programmation pouvant être photocopiées et utilisées sur chaque installation. Ces fiches ont été réalisées pour vous guider à l'installation et pendant toute la programmation. Tous les menus de programmation sont expliqués au *Chapitre 4 "Instruction d'Utilisation"*.

3.2 Procédure d'Initialisation et de Démarrage

Ce chapitre décrit la procédure d'initialisation d'un lecteur n'ayant **jamais été programmé**.

A la première installation lecteur ne comporte pas de base de données et évidement pas de code Distributeur ni de code Client, ni de programmes horaires etc. Dans ces conditions, le lecteur accepte tous les badges de Maintenance HISEC avec n'importe quel code Distributeur.

La procédure d'initialisation est dépendante du mode d'exploitation du lecteur soit en mode Autonome, système Multilecteurs ou Intégration au système d'Intrusion HISEC.

La configuration minimum sera d'un Lecteur et d'un S-ART 90T-S102. Les entrées du S-ART seront connectées au contact de porte et au bouton poussoir de sortie. La sortie relais commandera l'équipement contrôlant la porte (par exemple: gâche électrique). L'adresse du S-ART de cette configuration n'a pas besoin d'être codée, elle est par défaut 00.

Après alimentation, la procédure suivante est nécessaire pour programmer un nouveau système.

N'oubliez pas de vérifier la position de l'interrupteur de la pile de sauvegarde (SW1 en 90T & J3 en 95T) placée sur le dessous de la carte. Il doit être en position ON pour avoir une sauvegarde de la mémoire RAM de programmation.

3.2.1 Intitialisation

Mode 01 lecteur Autonome.

A : Lire le badge Maintenance. Le code Distributeur du badge Maintenance est enregistré et le menu Maintenance est affiché.

B : Choisir le *Menu* 82 pour l'initialisation. L'afficheur demande le **MODE**, le format de badges **BFORM** et les **OPTIONS** du système.

Nota: A la lecture du badge maintenance le logiciel du lecteur essaie de reconnaître le format des badges et propose la valeur qu'il a reconnue.

Voir *Chapitre 4.11 " Sous - Menu 8, Menu 82 Initialisation du Lecteur "*pour les valeurs à donner aux Options, Modes, Format de badges.

C : Entrer le Mode de fonctionnement 01 pour le Mode Autonome et les Options désirées. L'afficheur demande alors le Numéro du code Client.

D : Entrer le code Client Le code Distributeur du badge de Maintenance et le numéro de code Client seront programmés dans le lecteur et la base de données du lecteur sera ré-initialisée, si la touche ➔ est appuyée.

Mode 02 Système Multi Lecteurs

Avant de commencer la programmation d'un système multilecteurs, les lecteurs devront bien sur être connectés sur le bus. On devra s'assurer qu'un lecteur est programmé avec l'adresse 00.

Dans un système Multi-lecteurs chaque lecteur devra être initialisé de la façon décrite dans la procédure suivante du point A à D.

A : Lire le badge Maintenance. Le code Distributeur du badge Maintenance est enregistré et le menu Maintenance est affiché.

B : Choisir le *Menu* 82 pour l'initialisation. L'afficheur demande le **MODE**, le format de badges **BFORM** et les **OPTIONS** du système.
Nota: A la lecture du badge maintenance le logiciel du lecteur essaie de reconnaître le format des badges et propose la valeur qu'il a reconnue.

Voir *Chapitre 4.11 " Sous - Menu 8, Menu 82 Initialisation du Lecteur "*pour les valeurs à donner aux Options, Modes, Format de badges.

C : Entrer le Mode de fonctionnement 02 pour le Mode multilecteurs et les Options désirées. L'afficheur demande alors le Numéro du Code Client.

D : Entrer le code Client. Le code Distributeur du badge de Maintenance et le numéro de code Client seront programmés dans le lecteur et la base de données du lecteur sera ré-initialisée, si la touche ➔ est appuyée.

Avant de continuer la programmation de la base de données, **chaque** lecteur connecté au bus devra être initialisé par la procédure décrite de A à D.

Il est impératif de déconnecter (puis reconnecter) le lecteur à l'adresse 00 (maître) à chaque initialisation de ce dernier par le Menu 82.

Il est très important après l'initialisation de tous les lecteurs de l'installation de s'assurer au moyen du Menu 97 que tous les lecteurs communiquent bien et qu'ils sont à une adresse correcte.

Si ce n'est pas le cas la base de données globale ne sera pas automatiquement mise à jour pendant la programmation.

Après quoi il est possible de commencer la programmation (manuelle ou par PC).

Mode 03 Système Intégré

Si un lecteur est utilisé pour initialiser la centrale d'Intrusion HISEC, on devra programmer chaque lecteur avec la procédure décrite ci-dessous de A à D avant de programmer la partie Intrusion. Quand cela sera fait, la centrale Intrusion pourra être initialisée suivant la procédure décrite dans le "MANUEL TECHNIQUE INTRUSION HISEC".

A : Lire le badge Maintenance. Le code Distributeur du badge Maintenance est enregistré et le menu Maintenance est affiché.

B : Choisir le *Menu* 82 pour l'initialisation. L'afficheur demande le **MODE**, le format de badges **BFORM** et les **OPTIONS** du système.
Nota: A la lecture du badge maintenance le logiciel du lecteur essaie de reconnaître le format des badges et propose la valeur qu'il a reconnue.

Voir *Chapitre 4.11 " Sous - Menu 8, Menu 82 Initialisation du Lecteur "*pour les valeurs à donner aux Options, Modes, Format de badges.

C : Entrer le Mode de fonctionnement 03 pour le Mode Intégré à la centrale intrusion HISEC et les Options désirées. L'afficheur demande alors de lire le badge Maître.

D : Lire le badge Maître. Le code Distributeur et le N° de badge Maintenance sont comparés et s'ils sont différents le badge sera refusé. S'ils sont identiques le code Distributeur et le code Client seront programmés dans le lecteur, et le lecteur sera ré-initialisé si la touche  est appuyée.

Avant de continuer la programmation de la base de données, **chaque** lecteur connecté au bus devra être initialisé par la procédure décrite de A à D.

Il est très important après l'initialisation de tous les lecteurs de l'installation de s'assurer au moyen du menu 97 que tous les lecteurs communiquent bien et qu'ils sont à une adresse correcte.

Si ce n'est pas le cas la base de données globale ne sera pas automatiquement mise à jour pendant la programmation.

Après quoi il est possible de commencer la programmation (manuelle ou par PC).

Les valeurs par défaut après initialisation du lecteur sont les suivantes :

S-ART adresse 00 :
- Entrée adresse 00 : Type logiciel 30 - Contact de porte
- Entrée adresse 01 : Type logiciel 32 - Bouton poussoir de sortie

- Sortie adresse 00 : Type logiciel 99 - Sortie Equation 70+71 Type d'activation 2
- Sortie adresse 01 : Type logiciel 83 - Sortie gâche électrique Type d'activation 2

Temporisations de porte

Temporisation de libération de la gâche : 10 sec.
Temporisation porte ouverte avant avertissement : 30 sec.
Temporisation d'avertissement avant alarme: 10 sec.

Groupe de Personnel :

N° 1: (badges visiteurs)
PH = 02 (Toujours sans Code Personnel)
CA = 001 (Pas d'utilisation code Intrusion HISEC)
AS = 0 (Pas de fonction verrouillage)
HU = 0 (Code Contrainte invalide)
TE = 0 (Pas d'enregistrement des accès normaux).

N° 2: PH = 01 (Toujours avec Code Personnel)
CA = 001 (Pas d'utilisation code Intrusion HISEC)
AS = 0 (Pas de fonction verrouillage)
HU = 0 (Code Contrainte invalide)
TL = 0 (Pas d'enregistrement des accès normaux).

N° 3: PH = 02 (Toujours sans Code Personnel)
CA = 002 (Pas d'utilisation code Intrusion HISEC)
AS = 0 (Pas de fonction verrouillage)
HU = 0 (Code Contrainte invalide)
TE = 0 (Pas d'enregistrement des accès normaux).

Programmes horaires hebdomadaires :

Global
N° 00: 00:00 - 24:00 H, FNC = 00 (Pas d'accès)
N° 01: 00:00 - 24:00 H, FNC = 01 (Accès permanent avec code)
N° 02: 00:00 - 24:00 H, FNC = 02 (Accès permanent sans code)

Local
N° 31: 00:00 - 24:00 H, FNC = 15 (Tout enregistrer)
N° 34: 00:00 - 24:00 H, FNC = 32 (Fonctionnement normal de la porte)

Code Personnel Maintenance : 1122(33) (Ne peut pas être changé)
Code Personnel Badge Maître : 6692(92)

Paramètres divers:

Correction d'horloge : -00
Mode : 00
Options système: Aucune

Version programme : F-006.0xxx
N° de Distributeur : 000
N° d'Installateur : 000
N° de Client : 000
Taille mémoire : 128 Kb

Anti-Retour:

Dans la Zone : 000
Vers la Zone : 000
Niveau d'anti-retour: : 03

3.2 Initialisation des lecteurs Compact et Style

Ce chapitre décrit comment initialiser et installer un lecteur HISEC Compact ou Style et comment vérifier que l'installation s'est bien déroulée.

Introduction

L'initialisation d'un lecteur HISEC Compact ou HISEC Style peut être décomposée dans les phases suivantes :

1. Identification du type de lecteur, Lecteur HISEC Compact (pas de dongle) ou Lecteur HISEC Style (avec dongle).
2. Recherche d'une adresse libre.
3. Effacement (raz) de la base de données et de l'historique.

   Puis ensuite :

4. Programmation du code site en provenance d'un badge maître.
5. Programmation des options par défaut dans le lecteur.
   (Voir notice Contrôle d'accès HISEC pour de plus amples détails).

Eléments nécessaires

Pour pouvoir réaliser une initialisation, il est nécessaire d'être en possession des éléments suivants.

1. Un badge maintenance (avec un N° d'installateur correspondant aux badges) dans la bonne technologie évidemment.
2. Un badge maître appartenant au site à installer (N° compris entre 00001 et 00004).

Les étapes de l'initialisation

Et de suivre la procédure suivante :

Etape	*Sujet*
1	Vérifier que l'installation est bien sous tension.
2	Si ce n'est pas déjà le cas, passer le lecteur en mode installation
3	Initialiser le lecteur
4	Vérifier que l'initialisation s'est bien passée.

Procédure d'initialisation

Avant de pouvoir utiliser le lecteur il est nécessaire de l'initialiser, cette initialisation ne peut être réalisée que si le lecteur est en **Mode Installation**.
Normalement le Mode Installation (voir étape 7 ci-dessous, pour vous en assurer) est automatique si vous avez suivi les étapes d'installation classique (1ére mise sous tension du lecteur).

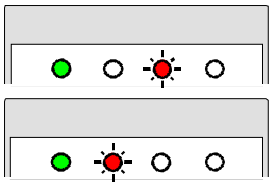
Si vous avez un doute sur l'état du mode installation se reporter directement à l'étape 7 ci-dessous

Mode Installation

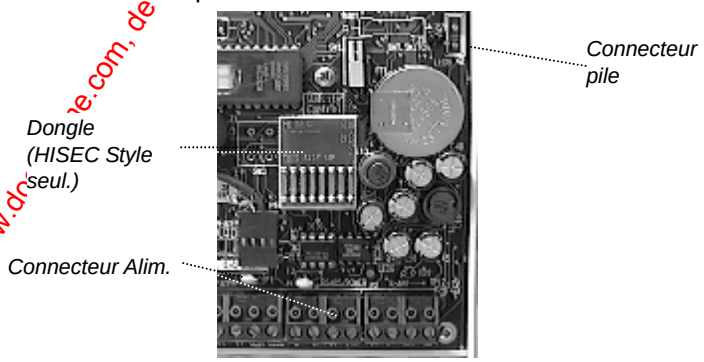
Si le mode Installation n'est pas déjà en cours, il est nécessaire de passer le lecteur en **Mode Installation** en suivant la procédure suivante :

Passage en mode installation

Etape	*Ce que vous devez faire*
1	Enlever la face avant, si ce n'est déjà fait.
2	Déconnecter l'alimentation en enlevant le bornier (RS 485) de la carte du lecteur.
3	Déconnecter la pile de sauvegarde en enlevant le strap (J3) d'alimentation la pile.
4	Patienter environ 1 minute
5	Ré-inserer le strap de la pile (J3).
6	Ré-inserer le bornier d'alimentation (RS 485).
7	Vérifier que le Mode Installation est bien atteint *HISEC Compact*: La led rouge «pas d'accès» clignote, la led verte «alimentation» est allumée. *HISEC Style*: La led rouge «alarme» clignote, la led verte «alimentation» est allumée.



Partie inférieure de la carte du lecteur représentant le connecteur batterie et le bornier d'alimentation.



Les étapes de l'initialisation d'un lecteur Compact

Avant de commencer la procédure d'initialisation, assurez-vous d'avoir en main un badge maintenance (dans la bonne technologie – magnétique ou proximité) et un badge maître (appartenant à l'installation). Après cela suivre la procédure décrite ci-dessous et vérifier au moyen des leds et du buzzer les indications correspondantes aux étapes décrites ci-dessous.

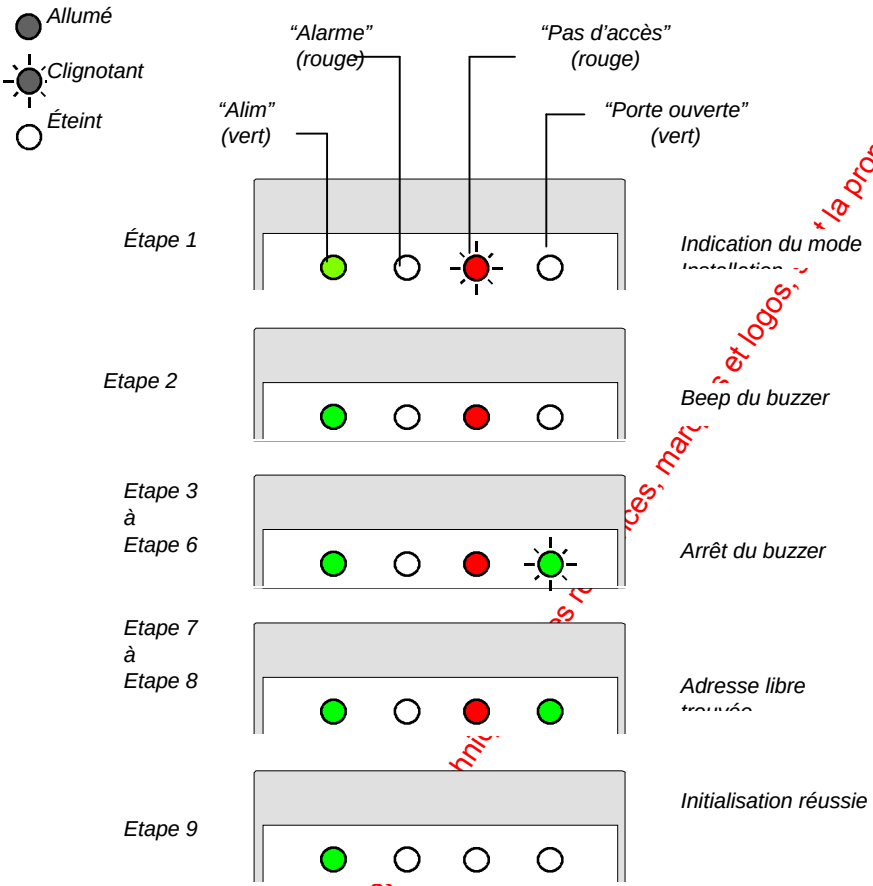
Procédure d'Initialisation

Etape	*Ce que vous devez faire …*	*Ce qui se passe …*
1	Vérifier que le lecteur est bien en mode installation.	
2	Lire le badge Maintenance sur le lecteur	La led rouge "Pas d'Accès" s'allume en fixe. Le buzzer s'active.
3	Lire le badge Maître sur le lecteur. Si vous ne lisez pas le badge maître dans un délai de 12 sec. Le lecteur annule la procédure en cours et revient en mode installation.	Le buzzer s'arrête.
4	-	Toutes les LED's s'allume un court instant pour indiquer que le lecteur effectue son reset.
5	-	La LED "Pas d'accès reste allumée.
6	-	La LED "Porte ouverte" clignote pour indiquer que le lecteur cherche une adresse libre.
7	-	Quand le lecteur a trouvé une adresse libre la LED "porte ouverte" s'allume. Cette opération peut prendre un certain temps
8	-	Toutes les LED's s'allume un court instant pour indiquer que le lecteur effectue son reset.
9	-	A la fin du reset le lecteur est initialisé et est près a être programmé. Ce état est indiqué par l'état repos correspondant à la LED verte « alimentation » allumée.

Durant la phase d'initialisation la LED verte «Alimentation» reste allumée, excepté a deux périodes (Étape 4 et Étape 8) quand le lecteur effectue son reset.

! *Le lecteur utilise une adresse temporaire (le temps d'en trouver une disponible) qui est l'adresse 31, si un élément est déjà présent a cette adresse cela n'empêche en rien le bon déroulement de l'initialisation.*

*Les indications du lecteur **HISEC Compact** pendant la phase initialisation*



Fin d'initialisation

Après une initialisation réussie, seul le voyant «alimentation» reste allumé.

La led rouge «alarme» indiquant une alarme, n'est visible qu'après chaque lecture de badge, elle doit s'éteindre à partir du moment ou il n'y a plus d'alarmes sur le lecteur (capot remis, plus de mode maintenance, etc.).

Le lecteur est maintenant prêt a être programmé en utilisant un PC de maintenance et le logiciel AICS V 6.02.

Les étapes de l'initialisation d'un lecteur Style.

Avant de commencer la procédure d'initialisation assurez-vous de tenir en main un badge maintenance (dans la bonne technologie – magnétique ou proximité) et un badge maître (appartenant à l'installation). Après cela suivre la procédure décrite ci-dessous et vérifier au moyen des leds et du buzzer les indications correspondantes aux étapes décrites ci-dessous.

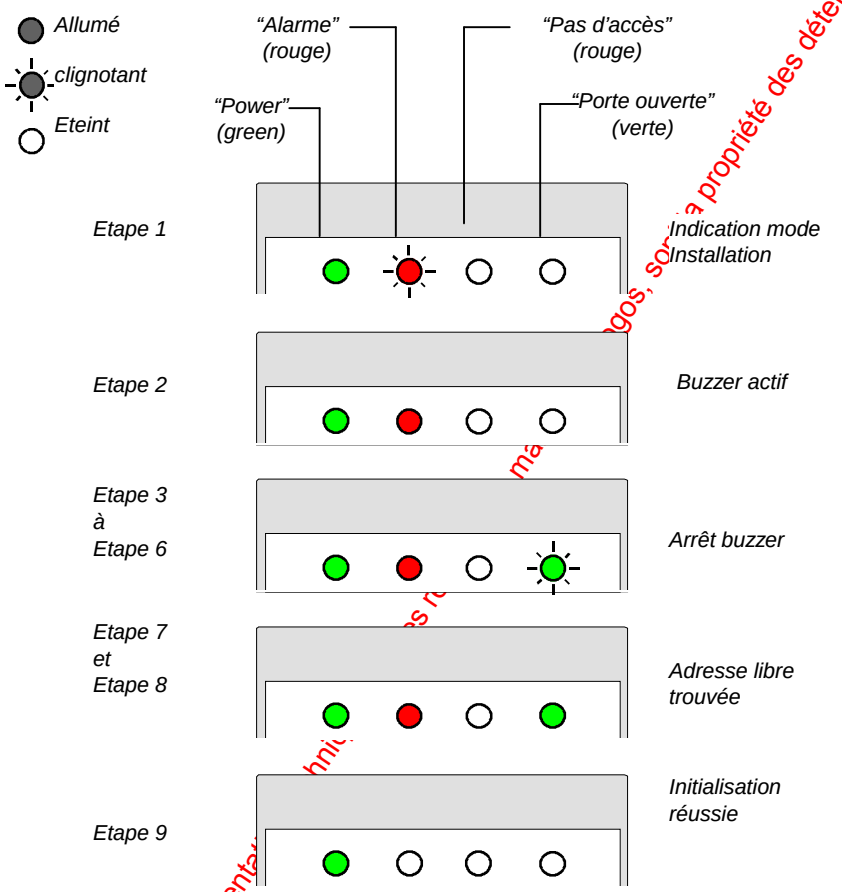
Procédure d'Initialisation

Etape	*Ce que vous devez faire …*	*Ce qui se passe …*
1	Vérifier que le lecteur est bien en **mode installation**.	
2	Lire le badge Maintenance sur le lecteur	La led rouge "Alarme" s'allume fixe. Le buzzer s'active.
3	Lire le badge Maître sur le lecteur. Si vous ne lisez pas le badge maître dans un délai de 12 sec. Le lecteur annule la procédure en cours et revient en mode installation.	Le buzzer s'arrête.
4	-	Toutes les Leds s'allume un court instant pour indiquer que le lecteur effectue son reset.
5	-	La LED rouge «Alarme» reste allumée.
6	-	La LED "Porte ouverte" clignote pour indiquer que le lecteur cherche une adresse libre.
7	-	Quand le lecteur a trouvé une adresse libre la LED "porte ouverte" s'allume. Cette opération peut prendre un certain temps
8	-	Toutes les LED's s'allume un court instant pour indiquer que le lecteur effectue son reset.
9	-	A la fin du reset le lecteur est initialisé et est près a être programmé. Ce état est indiqué par l'état repos correspondant a la LED verte «alimentation» allumée.

Durant la phase d'initialisation la LED verte « Alimentation » reste allumée, excepté a deux périodes (Etape 4 et Etape 8) quand le lecteur effectue son reset.

! *Le lecteur utilise une adresse temporaire (le temps d'en trouver une disponible) qui est l'adresse 31, si un élément est déjà présent à cette adresse cela empêche le bon déroulement de l'initialisation.*

*Les indications du lecteur **HISEC Style** pendant la phase initialisation.*



Fin d'initialisation

Après une initialisation réussie, seul le voyant «alimentation» reste allumé.

La led rouge «alarme» indiquant une alarme, n'est visible qu'après chaque lecture de badge, elle doit s'éteindre à partir du moment ou il n'y a plus d'alarmes sur le lecteur (capot remis, plus de mode maintenance, etc.) et sur le système intrusion en cas de système intégré.

Le lecteur est maintenant prêt a être programmé en utilisant un PC de maintenance et le logiciel AICS V 6.02.

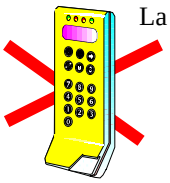
Passage en mode maintenance.

Exploitation par SMS

Le logiciel SMS possède une commande pour connaître et modifier directement l'état de maintenance (autorisation, blocage) à partir du PC. Cette fonction est accessible dans le menu : **Accès – Maintenance**.

Pas de logiciel d'exploitation

Installation sans lecteur HISEC Standard :



La seule possibilité pour passer en mode maintenance est d'effectuer une coupure d'alimentation ou de déconnecter le bornier d'alimentation (RS 485).

F Attention !! cette méthode n'effectue pas une mise en mode maintenance générale mais uniquement du (ou des) éléments dont on a coupé l'alimentation.

Installation comprenant au moins un lecteur HISEC Standard :

Il devient alors très simple de passer le système en mode maintenance au moyen du lecteur standard (Menu 56) comme par le passé. Ce passage en mode maintenance sera global et donc actif sur tous les lecteurs (Standard, Compact, Style).

3.3 Sauvegarde & Restauration sur PC

Avec le logiciel PC 95T-AICS il est possible de préparer la programmation du système contrôle d'accès HISEC sur un PC, stocker la programmation sur le disque dur et plus tard quand le système est installé de réaliser une restauration de toutes les données programmées.

Une restauration à partir du logiciel PC créera un message dans l'historique des alarmes du type Txx NOUV. DATABASE, ou xx=00 en cas de restauration de la base de données locale et xx=01 en cas de restauration de la base de données globale (ce message sera aussi crée quand l'on réalise des copies de bases de données).

Si la programmation d'un système installé a déjà été réalisée avec un lecteur classique (sans l'utilisation d'un PC), il est toujours possible de réaliser une sauvegarde de la programmation existante dans le PC et de la stocker dans le disque dur.

Le PC est connecté au contrôle d'accès HISEC par le bus RS 485 et pour faire cet office il est nécessaire de posséder une interface de conversion RS 485 **è** RS 232 . Cette interface 95T-PCI peut être directement connectée au bus RS 485 et alimentée par le 24V du bus des lecteurs.

Le coté RS 232 sera connecté sur COM1: (ou COM2:) du PC suivant disponibilité.

Le logiciel 95T-AICS travaille dans l'environnement WINDOWS et peut programmer aussi bien la centrale Intrusion HISEC que le Contrôle d'Accès HISEC.

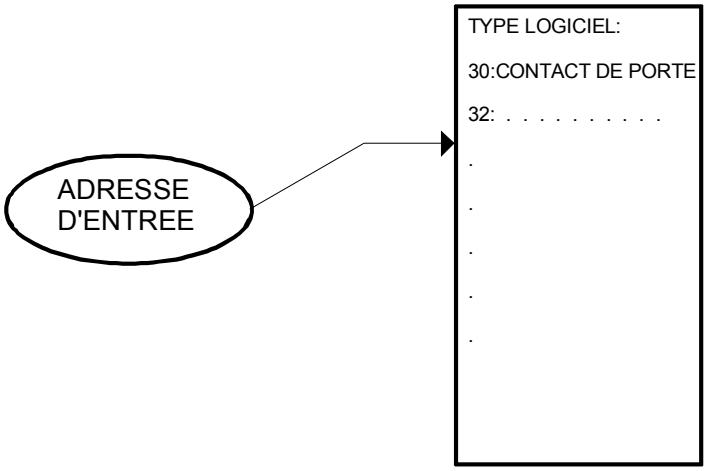
Configuration minimale du PC:

- Compatible PC
- 16 M bytes de RAM
- 1 Moniteur couleur.
- 1 Souris
- 1 Port COM:(1 ou 2) disponible.
- Environnement graphique Windows 95 (98)

Pour l'installation et l'exploitation du logiciel pour PC se reporter à la notice du "*Logiciel PC 90T-AICS*".

3.4 Programmation des Entrées

Toutes les entrées/sorties du lecteur sont réalisées au moyen de S-ART. Chaque entrée de S-ART utilisée doit être programmée avec un type logiciel d'entrée. Les entrées non programmées n'auront pas de fonction. Pour donner une fonction à une entrée, un type logiciel est "associé" à l'adresse comme illustré ci-dessous.

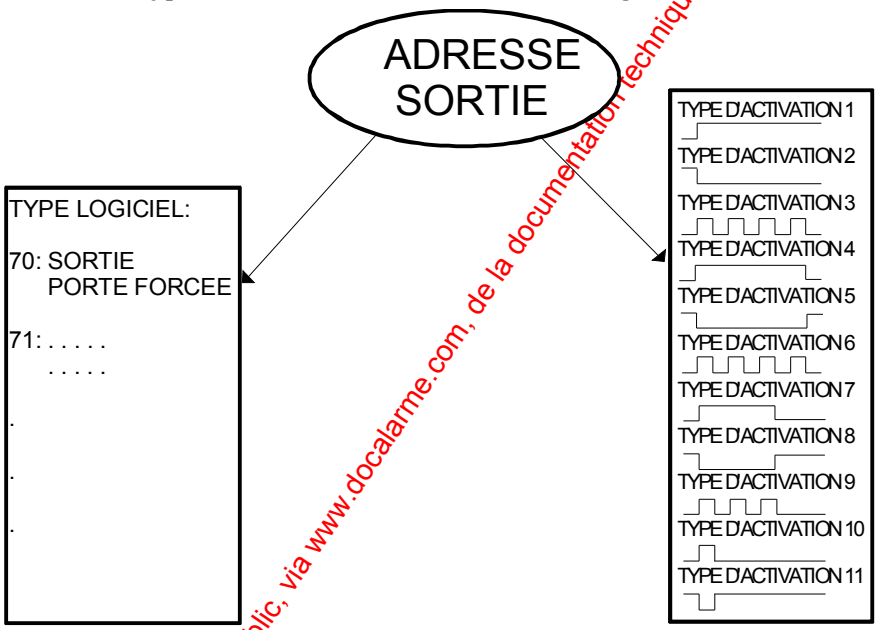


Une liste de type logiciel d'entrées prédéfinis est disponible (*voir Chapitre 1.4*).

Cette liste comprend 10 types sans fonctions prédéfinis pouvant être utilisés à des fins diverses. Ces types seront incorporés dans les fonctions utilisant les équations SI/ALORS. Les types logiciel d'entrée 30 à 36 peuvent aussi être utilisés dans les équations SI/ALORS. Prière de se référer au *Chapitre 1.4.2* "*Description des Types Logiciel d'entrées*".

3.5 Programmation des Sorties

Toutes les adresses de sorties utilisées doivent être programmées avec deux paramètres, un type logiciel de sortie et un type d'activation comme décrit dans la figure ci-dessous.



Les deux fonctions type logiciel et type d'activation sont attribuées aux adresses de sorties par programmation.

Le **Type Logiciel de sortie** défini **Quand** une sortie de S-ART doit être activée en fonction des différents événements comme la lecture d'un badge ou un événement sur un type logiciel d'entrée.

Le **Type Activation** défini **Comment** la sortie doit être activée, quand le type logiciel de sortie décide que l'adresse doit être activée.

Une liste de type d'activation prédéfinis existe et une description complète est donnée au *Chapitre 1.5.4 "Type d'Activation"*. Seul le type logiciel pour la sortie libération de gâche ne doit pas être programmé avec un type d'activation étant donné que la temporisation est définie avec le *Menu 83* "*Temporisations de Porte*".

Dans la liste des types logiciels de sortie avec des fonctions prédéfinis, sont aussi inclus 10 types n'ayant pas de fonctions prédéfinis mais pouvant être utilisés dans les équations SI/ALORS avec les types d'entrée.

Pour la programmation des équations se reporter au chapitre suivant.

3.5.1 Programmation des Equations

Trois types d'équations différentes peuvent être réalisées en fonction du N° du type logiciel de sortie.

- Type 90-94 : Ce type de sortie est un type mémorisé au moyen duquel la sortie restera active jusqu'à ce qu'un badge soit lu ou par fin de la temporisation du type d'activation.

- Type 95-98 : Ce type n'est pas un type mémorisé, de ce fait il suivra l'état de l'entrée jusqu'à la fin de la temporisation du type d'activation.

- Type 99 : Idem à 95-98 mais un message d'alarme sera en plus envoyé à la centrale Intrusion HISEC (si présente).

Prière de se référer aussi à la description des types logiciel de sortie (*Chapitre 1.5.2*).

Exemples d'applications

Equation 99 pour envoyer une information à la centrale Intrusion HISEC:

On désire transmettre l'information porte forcée pour provoquer une alarme Intrusion si la porte est forcée le système intrusion HISEC étant armé (le système intrusion étant désarmé l'information porte forcée sera locale sur le lecteur).

Les équations se programmant sur des sorties on utilisera l'adresse OUT 0 d'un S-ART existant (celui de la gâche par exemple ou seul OUT 1 est exploité) pour écrire: **Sortie 00 = 99 puis 99 = 70 + .. + ..**

Dans le système Intrusion HISEC pour être en relation avec cette information il faudra programmer l'entrée comprise entre 31 et 61 (31 correspondant au lecteur 1 et 61 au lecteur 31).

	ZZ	TT	NNN	ESCD
Ex: Lecteur 04 -> Entrée adresse 034	XX	01	XXX	XXXX

01 étant le type logiciel Intrusion.

Equation 99 pour lancer/stopper la temporisation d'entrée/sortie de la centrale intrusion HISEC:

On désire transmettre l'information porte ouverte pour provoquer un début/fin de temporisation d'entrée/sortie.

Les équations se programmant sur des sorties on utilisera l'adresse OUT 0 d'un S-ART existant (celui de la gâche par exemple ou seul OUT 1 est exploité) pour écrire: **Sortie 00 = 99 puis 99 = 30 + .. + ..**

Dans le système Intrusion HISEC pour être en relation avec cette information il faudra programmer l'entrée comprise entre 31 et 61 (31 correspondant au lecteur 1 et 61 au lecteur 31).

	ZZ	TT	NNN	ESCD
Ex: Lecteur 04 -> Entrée adresse 034	XX	01	XXX	XXXX

04 étant le type logiciel Intrusion.

Il est bien sur possible d'utiliser le type logiciel 05 "lancement de tempo" si d'autres détecteurs sont en type 04.

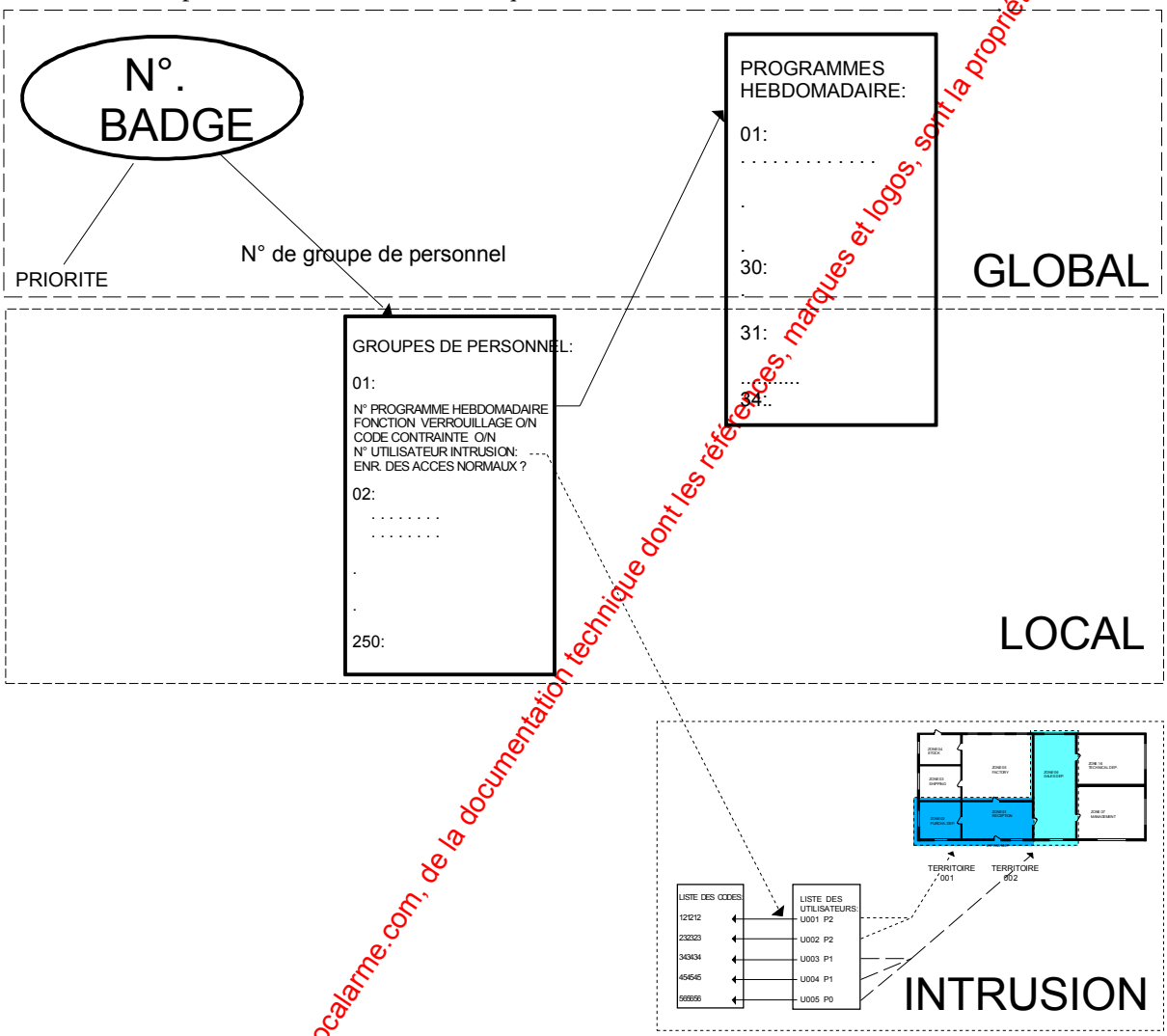
Exemple d'utilisation des types logiciel 37, 38 et 39:

Exemple 1: Ouverture de porte en cas d'alarme incendie. Connecté à une entrée de S-ART (programmé en type logiciel 37) à une sortie d'un système de centralisation d'incendie. Pour chaque commande de porte (gâche) contrôlée par la centrale incendie on devra écrire 95 = 37 + 80. L'ouverture de la porte sera alors contrôlée par le type logiciel d'entrée 37, et créera un message PORTE FORCEE. Cela pourra être évité en employant le type logiciel de sortie 98.

Exemple 2: Transmission de changement d'état d'un S-ART vers un autre en utilisant le bus RS 485. Par les types logiciel d'entrée 37 à 39 il est aussi possible de transmettre l'activation d'un S-ART d'un lecteur à une sortie se situant sur un autre lecteur. Cette application peut servir par exemple à commander un buzzer destiné à attirer l'attention quand on utilise le bouton poussoir de l'entrée principale ou pour commander l'ouverture de porte par un interrupteur.

3.6 Programmation des Badges

Comme décrit au *Chapitre 1.7*, la base de données est scindée en deux parties, une partie globale (et identique) pour tous les lecteurs et d'autre part une partie spécifique à chaque lecteur (locale). La base de données globale doit être programmée sur un lecteur seulement et sera automatiquement envoyée dans tous les lecteurs connectés au bus. La base de données locale doit être programmée sur chaque lecteur ou plus facilement copiée manuellement dans chaque lecteur.



La base de données des badges est une partie globale, mais quelques fonctions "sont liées" comme les Groupes de Personnel qui sont dans la base de données locale et peuvent être spécifiques à chaque lecteur, si nécessaire.

Pour chaque badge, on devra programmer les points suivants : **Priorité** & **Groupe de Personnel**.

La priorité définit quels Menus Contrôle d'Accès peuvent être utilisés par le propriétaire du badge.

3.6.1 Groupe de Personnel

La figure précédente, représente les paramètres à programmer pour chaque Groupe de Personnel. Chaque fonction est décrite en détail au *Chapitre 1.7.2*.

L'intégration au système Intrusion HISEC est réalisée par la programmation des Groupes de Personnel où un N° d'Utilisateur intrusion HISEC est défini. Le N° d'Utilisateur est dans un système d'Intrusion HISEC associé à un Territoire et à un Code.

Par ce moyen, un groupe de badges peut être programmé pour armer ou désarmer un territoire du système d'Intrusion HISEC.

Le Code Personnel du badge et le Code Intrusion HISEC sont indépendants pour chaque système (Intrusion et Contrôle d'accès).

Etant donné que la base de données des Groupes du Personnel est locale, il est possible d'attribuer différents territoires à un même badge, en fonction du lecteur sur lequel le badge est utilisé.

3.6.2 Programmes Hebdomadaires

Comme illustré sur la figure précédente, chaque Groupe de personnel peut être contrôlé par un Programme Hebdomadaire.

Le nombre maximum de Programmes Hebdomadaires est de 35.

Un Programme Hebdomadaire est composé de 7 jours - du lundi au dimanche - plus 2 jours spéciaux se référant à la liste des jours de congés. Par cette méthode, il est ainsi possible de programmer des demi-journées de travail, par exemple, le 24 décembre ou autre date spécifique.

Programme Hebdomadaire : 03

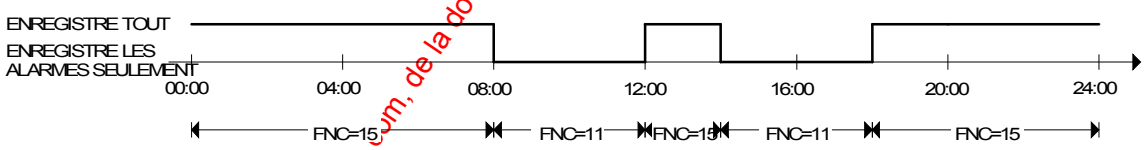
JOUR 1	LUNDI		
0 0:0 0-0 8:0 0	0 8:0 0-1 2:0 0	1 2:0 0-1 4:0 0	1 4:0 0-1 8:0 0
FNC: 0 0	FNC: 0 2	FNC: 0 1	FNC: 0 2
1 8:0 0-2 4:0 0			
FNC: 0 0	FNC:	FNC:	FNC:

La figure ci-dessous représente un exemple de Programme horaire typique pour une journée normale JOUR 1 = LUNDI.

Un jour peut avoir un maximum de 8 périodes où la première démarre à 00:00 et la dernière finit à 24:00. Dans l'exemple précédent le badge n'a pas accès avant 8:00, après cela, le badge peut être utilisé sans Code Personnel jusqu'à 12:00. A 12:00, il est demandé que les badges aient accès seulement avec le Code Personnel jusqu'à 14:00 et ainsi de suite. Chaque jour est programmé avec les périodes désirées mais les Programmes Hebdomadaires **doivent** être programmés chaque jour avec une **fin de journée à 24:00**.

Chaque période devra être programmée avec des fonctions (FNC) pour dire au système ce que l'on désire obtenir aux différentes périodes horaires.

Différentes fonctions sont disponibles en relation avec le N° du Programme Hebdomadaire programmé. Dans l'exemple détaillé ci-dessus ce sont les fonctions correspondant au Programme Horaire n° 03 à 30, lesquelles spécifient les conditions d'accès et dans l'exemple ci-dessous ce sont les fonctions spécifiant le mode d'enregistrement dans l'historique.



Des Programmes Hebdomadaires, ne se référant pas aux Groupes de Personnel, peuvent aussi être créés par exemple, programme horaire de contrôle des enregistrements des différents types d'événements ou pour contrôler les sorties des S-ART (voir la liste complète des types de Programmes Hebdomadaires au *Chapitre 1.7.3*).

3.6.3 Congés

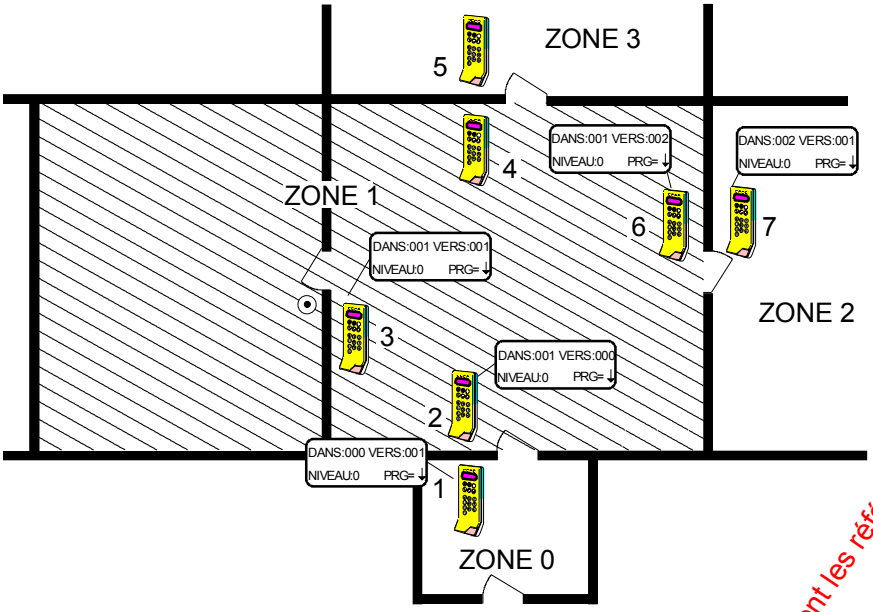
Une liste de 25 périodes de congés peut être réalisée au moyen du *Menu 53*. Pour chaque période, on devra programmer un jour N° 8 ou 9, lequel se réfère aux 2 jours spéciaux ou aux 7 jours normaux de la section des Programmes Hebdomadaire.

Normalement 2 jours spéciaux différents seront programmés. Un jour au moyen duquel on spécifie la fermeture complète pour un jour férié et un autre jour pour lequel on spécifie l'ouverture pour une demi-journée mais toute combinaison des 9 jours peut être utilisée.

Prière de se référer aux *"Instructions d'Utilisation" Menu 53* pour réaliser la programmation.

3.7 Programmation de l'anti-retour

Chaque lecteur devra être programmé avec le Numéro de zone où il est installé (DANS) et le Numéro de zone où il permet l'accès (VERS) et le Niveau de contrôle de zone (NIVEAU). Dans l'exemple d'installation représenté ci-dessous les 3 différents principes de l'anti-retour ont été programmées.



- Lecteur contrôlant l'entrée/sortie entre deux zones différentes.
- Un lecteur permettant d'entrer à partir de la zone 0 ("en dehors du système").
- Lecteur à l'intérieur d'une zone (DANS = VERS)

Le niveau de contrôle de zone (NIVEAU) peut être programmé avec 4 différentes valeurs comprises entre 0 et 3. Le niveau de contrôle permet de définir le niveau de sécurité voulu pour la fonction Anti-retour.

Les différents Niveaux peuvent êtres définis comme suit:

- 0: Pas de limites au contrôle de l'anti-retour. Le contrôle démarre à la première lecture du badge et est automatiquement lancé.
- 1: Le contrôle de l'anti-retour est effacé chaque jour à minuit (24:00) et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 2: Le contrôle de l'anti-retour est effacé chaque heure et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 3: Pas de contrôle de l'anti-retour par zone. Tous les badges pourront être utilisés en ignorant les conflits de zones possibles.

Tous les niveaux de contrôle des zones valident la fonction de comptage, même le Niveau 3.

Si un badge est utilisé dans une zone où il y a conflit avec le contrôle anti-retour, le badge se verra refusé l'accès et l'événement seront mémorisés dans l'historique des alarmes sous la forme [Bxxxxx ZONE REF.]. L'afficheur indiquera "Erreur de zone A/R".

Nota: Il n'existe pas de contrôle de Zone pour le badge Maintenance.

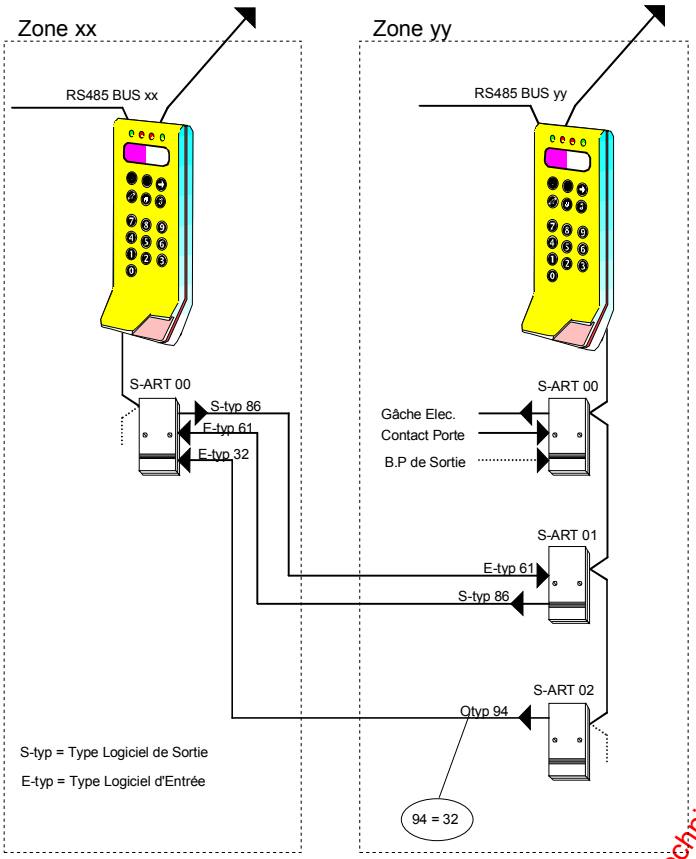
3.7.1 Système d'anti-retour Multibus

La structure du système multi-bus acceptant 900 lecteurs comme représenté sur le synoptique du *Chapitre 1.2.2*, il a été nécessaire de définir un nombre maximum de zones d'anti-retour qui est de 480. Chaque bus utilise ses zones spécifiques, bus 00 zones 00 à 15, Bus 01 zones 16 à 31, etc..

Le logiciel A(I)MS affiche automatiquement le N° de la zone correspondante au Bus sélectionné, de cette façon il n'est pas nécessaire de calculer les N° utilisés par un bus spécifique.

La **Zone 00** représentant l'"**Extérieur du site**" sera accessible sur tous les bus et tous les lecteurs.

3.7.2 Contrôle d'1 porte par 2 lecteurs sur des bus différents.



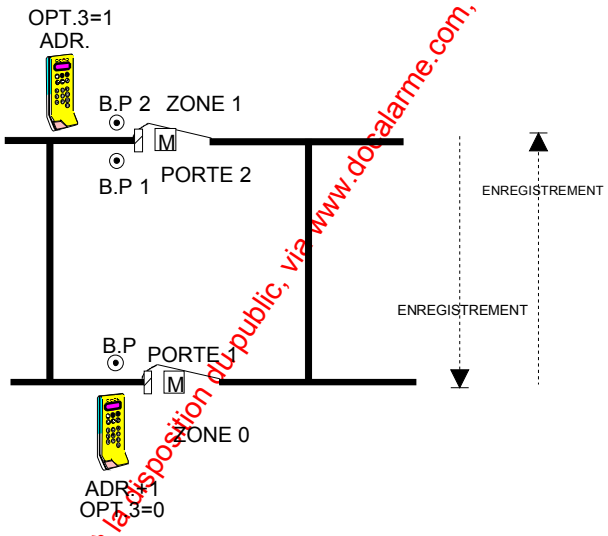
Si deux lecteurs devant contrôler la même porte sont placés sur 2 bus différents, il est nécessaire de faire l'installation suivante pour surveiller et commander la porte.

Les deux lecteurs devront obligatoirement avoir la même adresse sur chaque Bus.

Les différents types logiciels utilisés dans ce montage sont décrits en détail aux chapitres 1.4 et 1.5.

3.8 Fonction d'inter-verrouillage des portes

Comme décrit dans l'option 13 du *Menu 82*, il est possible de créer un inter-verrouillage de 2 portes, la deuxième porte ne pouvant être ouverte si la première n'est pas fermée, et inversement dans le sens de la sortie. Les 2 portes ne peuvent jamais être ouvertes simultanément. Si l'autre porte est maintenue ouverte, le lecteur indiquera PORTE BLOQUEE et vous devrez lire le badge à nouveau quand l'autre porte sera refermée pour pouvoir ouvrir la première porte.



Le schéma ci-contre représente l'installation de 2 portes avec inter-verrouillage:

Les 2 portes pourront être contrôlées par 1 Lecteur (entrée) ou par 2 lecteurs (entrée et sortie) selon le besoin, mais les S-arts contrôlant les portes seront connectés sur le même lecteur et ce lecteur sera celui ayant l'adresse la plus haute des 2 (ADRESSE +1). Sur le lecteur d'adresse basse l'option 3 devra être à 1.

Les portes forcées et portes maintenue peuvent provenir des 2 portes.

Dans le cas d'utilisation d'A(I)MS, le logiciel indiquera quelle porte est en alarme (porte 1 ou 2), les 2 portes pourront être commandées séparément dans la boite de dialogue "*Contrôle des Portes*".

Le passage de la porte n'est enregistré dans l'historique qu'une fois la seconde porte franchie, ceci est valable dans les 2 sens. Si la porte intérieure n'est pas contrôlée par un lecteur mais seulement par un bouton poussoir (entrée et sortie), l'entrée du badge sera également enregistrée dans l'historique à l'ouverture de la porte.

Le tableau ci-dessous représente les types logiciels à utiliser sur les différents S-art contrôlant la porte:

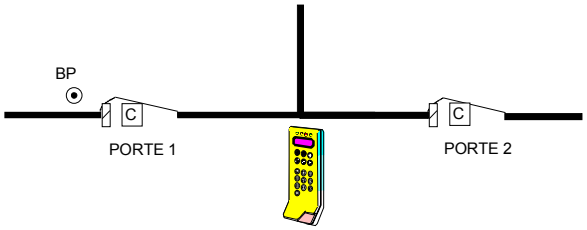
N° Porte	Contact de Porte	B.P de Sortie	Commande Gâche (Type.Log **Entrée**)	Commande Gâche (Type.Log **Sortie)**
1	30	32	80	83
2	31	40/41	81	84

Les différents types logiciels utilisés dans ce tableau sont décrits en détail aux chapitres 1.4 et 1.5.

La fonction inter-verrouilage peut être aussi utilisée dans les installations utilisant l'anti-retour. La vérification de l'anti-retour se fera à la lecture du badge avant l'ouverture de la première porte.

3.9 Contrôle de 2 Portes par 1 Lecteur

Si l'option 13 du Menu 82 est à 0 (pas d'inter-verrouillage), il est possible de gérer 2 portes de façon indépendante avec les mêmes types logiciels que dans le cas précédent. Dans l'exemple suivant le lecteur contrôle 2 portes situées de part et d'autre de celui-ci.



La programmation des groupes de personnel permet de décider si le groupe de personnel (sur ce lecteur) pourra avoir accès à la porte 1 (première porte), à la porte 2 (seconde porte) ou aux 2 portes.

Attention: Cette fonction n'est programmable qu'au moyen du logiciel A(I)MS.

Le tableau ci-dessous représente les types logiciels à utiliser sur les différents S-arts contrôlant les portes:

N° Porte	Contact de Porte	B.P de Sortie	Commande Gâche (Type.Log **Entrée**)	Commande Gâche (Type.Log **Sortie)**
1	30	32	80	83
2	31	40	81	84

Les différents types logiciels utilisés dans ce tableau sont décrits en détail aux chapitres 1.4 et 1.5.

Prière de noter les limitations de cette configuration:

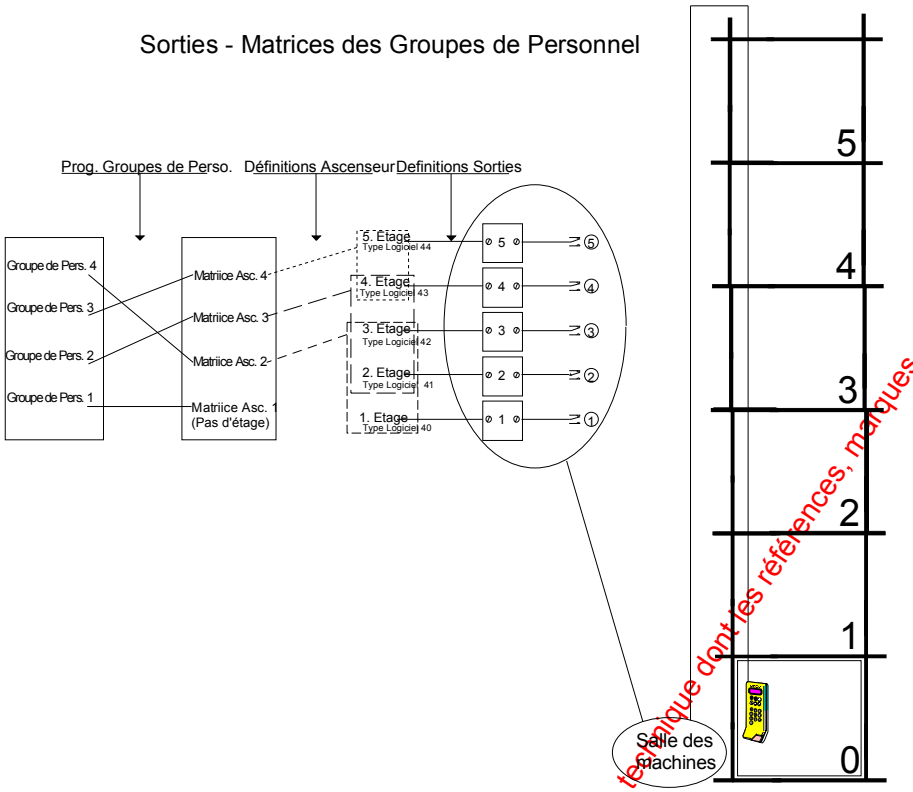
Dans cette configuration, l'historique des événements n'est pas toujours correct à 100%. Si 2 badges ayant accès aux 2 portes sont lus à la suite (avant qu'aucune porte ne soit ouverte), le lecteur est incapable de savoir qui est entré sur quelle porte. Il existe d'autre cas où l'historique peut être faux.

C'est pourquoi, il ne faut pas utiliser cette possibilité en cas de nécessité absolue d'enregistrer tous les mouvements des porteurs de badges.

Cette fonction ne devra pas être utilisée si le lecteur est un lecteur d'Entrée (ou de Sortie) d'une zone d'Anti-retour.

3.10 Programmation des définitions ascenseur

Les sorties ascenseur sont utilisées pour contrôler les étages où les différents groupes de personnel ont accès.



N.B.: Cette fonction ne peut être programmée qu'à l'aide du logiciel de configuration 90T AICS ou du logiciel de gestion contrôle d'accès 90T AMS.

Par ex: le groupe de personnel 004 = département commercial, après avoir lu son badge sur le lecteur pourra utiliser les boutons des étages 1,2 et 3.

Le logiciel des lecteurs est capable de gérer 30 étages, mais du fait qu'il n'existe qu'une adresse par S-art, **seuls 15** types logiciel pourront être utilisés.

Pour chaque groupe de personnel (250) un groupe d'ascenseur sera programmé. Les différents groupes d'étages (définitions ascenseurs) seront crées au moyen des logiciel AICS ou AMS et restaurés dans les lecteurs. De plus, la programmation dans chaque groupe de personnel des groupes d'étages ou il a accès est programmé dans le PC.

Jusqu'à 250 groupes d'étages peuvent être programmés. Pour chaque étage une sortie est réservée, 40 pour le 1er, 41 pour le 2éme, etc. jusqu'à 69 pour le 30eme étage.

Un type logiciel de sortie pourra être directement programmé sur le lecteur ou par le logiciel AICS.

La durée d'activation de la sortie sera fixée par le type d'activation choisi.

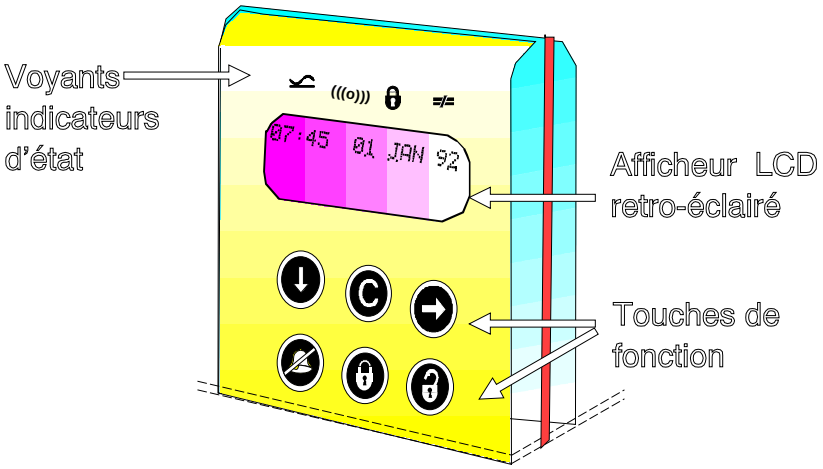
Prière de noter que si l'entrée du badge doit être enregistrée dans l'historique des événements, un contact indiquant l'utilisation d'un bouton de l'ascenseur devra être utilisée et raccordée sur une entrée de s-art avec le type logiciel 30 (contact de porte). Si cela n'est pas réalisé aucune entrée ne sera mémorisée dans l'historique des événements.

Les sorties ascenseur sont mémorisées dans la base de données locale. Une copie de base de données locale ne **copie pas** ces informations d'un lecteur à l'autre. Un lecteur peut être uniquement programmé avec des sorties ascenseur par le logiciel AICS.

Exploitation

4 Exploitation

4.1 Principe d'utilisation



Le lecteur de badges possède 4 voyants spéciaux d'état qui peuvent être contrôlés par la centrale Intrusion HISEC, quand le lecteur est un élément intégré au système d'Intrusion HISEC. La description de toutes les fonctions de ces voyants dans chaque cas est décrite dans la *NOTICE TECHNIQUE INTRUSION HISEC*.

Les voyants indicateurs peuvent aussi être contrôlés par le lecteur de badges pour indiquer les alarmes, défauts, état de l'armement etc.

Les indications des voyants sont les suivantes :

Voyant Secteur (Vert) : Allumé en permanence, il indique que le secteur est présent, le clignotement indique un défaut de l'alimentation secteur.

Voyant Alarme (Rouge) : Indiquera qu'un type logiciel d'entrée d'alarme est actif, par ex. sur un système d'Intrusion externe avec alarme connectée sur le Contrôle d'Accès HISEC. Ce voyant est actif tant que le type logiciel d'entrée est actif. Le type de message d'alarme peut être consulté dans l'historique des alarmes.

Voyant état d'armement (Jaune) : Indique l'état d'armement d'un système d'intrusion connecté au lecteur. Sera seulement actif après la lecture et l'acceptation d'un badge. Indiquera aussi l'état du lecteur quand le système est utilisé avec la fonction "Premier entré/Dernier sorti" des badges.

Voyant défaut système (Jaune) : Indique un défaut batterie ou un défaut système. Ce voyant est actif tant que le défaut est présent. Le type de défaut peut être consulté dans l'historique des alarmes.

Afficheur: Deux lignes de 16 caractères affichent l'état du système et les instructions d'utilisation. Au repos la date et l'heure sont affichées. Le rétro-éclairage est allumé à chaque fois que le clavier est utilisé ou qu'un badge est lu et est automatiquement éteint après un délai de 2 minutes (environ).

Buzzer: Utilisé pour indiquer de façon sonore un défaut ou une alarme. Aussi activé pour un temps bref pour indiquer les erreurs de manipulation ou pour attirer l'attention de l'utilisateur.

Clavier: le clavier est composé des touches numériques de 0 à 9 utilisées pour le code etc. et de 6 touches de fonctions.

Utilisée pour armer (si connexion à un système d'intrusion).

Utilisée pour désarmer (si connexion à un système d'intrusion).

Utilisée pour acquitter un(e) défaut/alarme (seulement en système Intégré à l'intrusion HISEC) ainsi que pour se déplacer à droite dans les menus de programmation.

Cette touche est utilisée pour sélectionner les fonctions des menus affichés.

Cette touche est utilisée pour revenir en arrière ou quitter une session.

Cette touche est utilisée pour avancer dans les différents menus.

4.2 Utilisation Générale

La procédure d'utilisation du HISEC est basée sur le principe de Menus, de cette façon, toutes les étapes sont affichées et l'utilisateur a juste à répondre aux questions par OUI (touche ➔) ou NON (touche ↓).

Le Menu est scindé en 9 sous-menus pour permettre l'affichage des états des badges, la programmation des badges, le test du système et les programmations diverses. Toutes ces opérations nécessitent un badge et un Code Personnel à 4 ou 6 chiffres entré au clavier. Les menus ou fonctions affichés dépendent du niveau de priorité de l'utilisateur du badge (5 niveaux).

4.2.1 Contrôle de la Porte

La fonction principale du Contrôle d'Accès HISEC est de gérer les mouvements de personnes au travers des portes, barrières etc.

L'accès est autorisé à chacun par l'usage d'un badge valide, par l'association d'un badge valide et d'un Code Personnel ou par l'entrée d'un code seul.

Les portes sont complètement supervisées, et le Contrôle d'Accès HISEC exécutera des alarmes, si les portes sont forcées, ouvertes sans autorisation ou maintenues ouvertes trop longtemps.

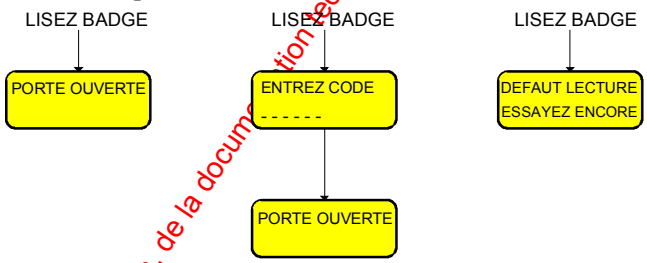
4.2.2 Franchissement Normal d'une Porte

Les opérations quotidiennes sont typiquement des entrées normales au travers des portes par l'acceptation d'un badge avec la possibilité d'associer un Code Personnel.

L'afficheur avec rétro-éclairage et la commande du "buzzer" donnent à l'utilisateur une information guidée tout au long de l'utilisation du système.

Au repos, l'afficheur indique l'heure et la date (rétro-éclairage éteint).

La figure, ci-dessous, représente les 3 différents cas d'usage normal du lecteur. Quand un badge est lu, l'afficheur s'éclaire dans le même temps.



Si le badge a été lu correctement et qu'il est sans Code Personnel, le premier affichage apparaîtra.

Si le badge a été lu correctement et qu'il est avec Code Personnel, le deuxième affichage apparaîtra.

L'utilisateur pourra de plus se voir notifier une situation de défaut avec un message à l'écran et un "beep" sonore. En cas de mauvaise lecture, le troisième affichage apparaîtra.

Un autre cas de situation de défaut est une répétition de tentatives erronées de Code Personnel. Le lecteur n'affichera pas une autre image mais le défaut sera signalé par l'émission de 4 "beep" et le badge sera bloqué après 10 tentatives infructueuses.

Un badge peut de plus être refusé par le lecteur si ce badge a été définitivement bloqué ou le lecteur lui même a été bloqué etc. L'utilisateur se verra dans ce cas présenter un nouveau message expliquant la raison du refus du badge (*Voir 4.2.1 Indications d'Alarme*).

La lecture d'un badge non créé (avec le bon code site) affichera le message BADGE N 00016 NON CREE par ex. Indiquant que le badge N°16 n'est pas programmé dans l'installation. Cela permet de retrouver un badge non programmé et éventuellement si la sérigraphie est effacée le numéro du badge, cette fonction n'est possible que sur les badges standards HISEC (pas sur les cartes de crédit, format libres, etc.).

Prise en compte du franchissement de porte

1) Porte avec contact:

La prise en compte et l'enregistrement du franchissement de porte dans l'historique se fait quand la porte est ouverte après une lecture de badge.

Cette procédure permet de s'assurer que l'événement est bien pris en compte et le badge changé de zone, ceci est valable aussi pour l'historique. Par cette méthode le badge n'est pas changé de zone si le porteur change d'avis après avoir lu son badge et ne franchit pas la porte.

Il est aussi possible de lire un autre badge avant que la porte ne soit refermée. Si le badge est lu pendant que la porte est ouverte, la position du badge sera changée. Cela donne la possibilité de résoudre les passages de flux de personnes importants sur certaines portes à des heures précises.

Prière de remarquer que cette particularité impose d'installer un contact de porte, si le contrôle des mouvements de badges est désiré.

1) Porte sans contact:

En cas d'impossibilité d'installer un contact de porte, il est possible de programmer l'option 11 (Menu 82) pour indiquer que la transaction doit être immédiatement enregistrée sans attendre l'activation d'un contact.

Dans cette configuration, l'historique des événements n'est pas toujours correct à 100%. Le lecteur est incapable de savoir qui est entré sur quelle porte. Il existe d'autre cas où l'historique peut être faux.

C'est pourquoi, il ne faut pas utiliser cette possibilité en cas de nécessité absolue d'enregistrer tous les mouvements des porteurs de badges.

Cette fonction ne devra pas être utilisée si le lecteur est un lecteur d'Entrée (ou de Sortie) d'une zone d'Anti-retour.

4.2.3 Programmation du Code Personnel

L'utilisateur sera automatiquement guidé pour entrer le Code Personnel à la première utilisation du badge.

1	Entrez le Code Personnel
2	Vérifiez le Code Personnel

Le lecteur répétera les étapes 1 et 2 jusqu'à ce que le même code soit entré deux fois.
Une fois le code accepté le lecteur est prêt à accepter le badge en état d'assurer l'ouverture normale de la porte.

4.2.4 Changement de Code Personnel

Le propriétaire d'un badge avec un Code Personnel peut changer ce Code Personnel sur le lecteur en effectuant les manipulations suivantes :

1	Entrez le Code Personnel spécial 1111 (après lecture du badge)
2	Entrez l'ancien Code Personnel
3	Entrez le nouveau Code Personnel (même nombre de chiffres)
4	Vérifiez le nouveau Code Personnel

Le lecteur répétera les opérations 3 et 4 jusqu'à ce que le même code soit entré deux fois.

Une fois le code accepté le lecteur est prêt à accepter le badge en état d'assurer l'ouverture normale de la porte.

4.2.5 Code Contrainte

Le code contrainte "Hold-Up" est défini (comme sur le système d'intrusion HISEC) comme étant le Code Personnel +1, mais cette fonction est valide seulement si elle a été autorisée pendant la programmation des Groupes Personnel. On remarquera que les Groupes de Personnel sont locaux, et donc sont individuels d'un lecteur à l'autre. L'usage du code Contrainte commandera une sortie d'alarme dédiée, et un message sera transmis au système d'intrusion HISEC.

4.2.6 Indication d'Alarme

Alarmes du Contrôle d'Accès

Les alarmes Contrôle d'Accès du genre porte forcée etc. seront seulement indiquées sur le lecteur où elles sont apparues. Toutes les alarmes seront enregistrées dans l'historique global - commun à tous les lecteurs - et pourront être visualisées ou imprimées au moyen des menus correspondants.

Les messages d'alarme seront indiqués par l'excitation du buzzer et par un message sur l'afficheur.

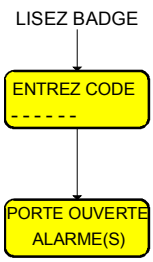
Les messages d'alarme pouvant être donnés sont les suivants :

Affichage 1ere Ligne	Affichage 2eme Ligne	Commentaires
PORTE FORCEE ATTENTION.....	FERMEZ LA PORTE	Avertissement avant alarme
PT.MAINTENUE NON ACCES.....	BADGE BLOQUE	
	HORS TEMPS.....	Badge bloqué par une plage horaire
	BADGE ILLEGAL	Badge pas au format HISEC
	PORTE BLOQUEE.....	Porte bloquée par le *Menu 71*
	BADGE NON CREE. CODE ERRONE	
	ERREUR DONN.BADGE	Le code Intrusion HISEC n'existe pas
N° DEFAUT SYSTEME :.....	1:.....	Connexion interrompue ou problèmes de communication avec le système HISEC Intrusion
Date et Heure	PAS DE COMMUNIC.	Pas de communication sur le bus dans un système multilecteurs, ou intégré
PORTE OUVERTE.....	SABOTAGE	Sabotage du lecteur ou sabotage venant d'un S-ART avec le type logiciel 07
PORTE OUVERTE.....	ALARME.....	Alarme venant d'un S-ART avec le type logiciel 36
PORTE OUVERTE.....	MAINTENANCE	Le système contrôle d'accès est en maintenance

L'indication d'alarme disparaîtra quand la porte reviendra à sa position normale et le message ne nécessitera pas d'acquittement.

Les messages ALARME et SABOTAGE activeront le voyant ((•)) du lecteur.

Message d'alarme venant d'un système d'Intrusion



Si le lecteur est connecté sur un système d'Intrusion HISEC ou si le type logiciel d'entrée 36 (entrée d'alarme venant d'un système d'intrusion non HISEC) est défini dans la programmation du lecteur et si le système d'alarme est en condition d'alarme, alors l'afficheur présentera un texte d'Alarme et donnera un court "bip" sonore à chaque fois que la porte sera ouverte par le lecteur. Le texte sera affiché jusqu'à ce que la condition d'alarme soit remise à zéro sur la centrale d'intrusion HISEC ou la condition d'alarme du type logiciel 36 soit remise à zéro.

Pendant cette condition d'alarme le badge Maintenance est autorisé avec le niveau de priorité le plus faible sans l'autorisation du Client.

Apres la lecture du badge de Maintenance la porte sera ouverte et le lecteur ira directement dans le menu Intrusion HISEC, ensuite la personne chargée de la Maintenance devra entrer son code Maintenance Intrusion HISEC ou le code Gardien.

Quand le système Intrusion HISEC est en condition d'alarme, il est possible d'utiliser les menus Contrôle d'Accès, "*Afficher les Etats Système*" et "*Test du Système*" en utilisant le code Maintenance Contrôle d'Accès.

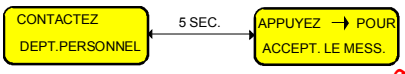
4.2.7 Messages destinés à l'Utilisateur

Le lecteur peut afficher des messages personnels destinés à l'utilisateur.

Lecteur "standard"

Le message est présenté après la lecture d'un badge, et l'attention de l'utilisateur est attirée par un court "bip" sonore.

Un exemple de message pouvant être : "APPELEZ DOMICILE" ou "CONTACTEZ DEPT. PERSONNEL".

Le message est affiché sur 2 lignes de 16 caractères:.. 

L'affichage alternera entre le message et le texte standard dans un second affichage. Quand le message a été acquitté par pression sur la touche ➔, il est possible d'afficher un autre message ou de réaliser un franchissement normal de la porte.

Après acquittement, le message est enlevé du badge. S'il n'est pas acquitté, il sera enlevé après avoir été affiché plusieurs fois, mais sera présenté la prochaine fois que le badge sera utilisé.

15 messages standards (sur 31 au total, qui peuvent être programmés au moyen du logiciel PC) sont pré-programmés dans le lecteur.

Lecteur "tête déportée"

Si un message a été associé à un badge qui est lu par le lecteur extérieur, la procédure suivante devra être utilisée:

1: La porte est ouverte normalement quand le badge est lu.

2: Le terminal 90T RKP ER attire votre attention en émettant un signal (Buzzer discontinu) pendant 1 minute ou jusqu'à la lecture du badge suivant. Le message sera en même temps présenté sur l'afficheur.

3: Le message pourra être accepté par la même méthode que celle du lecteur classique au moyen de la touche ➔, mais sans code personnel (puisque la porte s'ouvre toujours). Le message sera affiché à nouveau sur le prochain lecteur qui sera utilisé avec ce badge, si le message n'a pas été acquitté.

4: Quand le message est acquitté par l'utilisateur sur le lecteur ERC, la porte ne sera **PAS** ouverte mais l'afficheur reviendra simplement à l'heure et la date comme au repos de ce dernier.

5: Si le système intégré à l'intrusion HISEC est armé et qu'un message soit attribué au badge, la procédure de désarmement décrite précédemment ne devra pas être tentée avant acquittement du message. Cela devra être pris en compte quand on calculera la temporisation d'entrée.

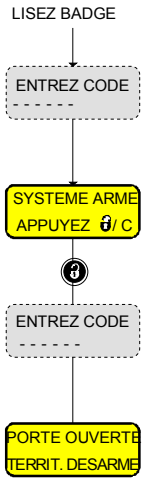
4.2.8 Armement/Désarmement Intrusion HISEC à partir du Lecteur

4.2.8.1 Lecteur en mode standard

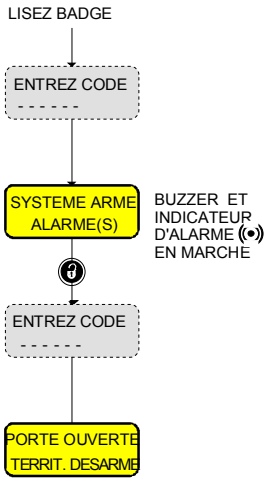
Désarmement:

Dans les systèmes intégrés HISEC, le texte d'état du système peut être "TERRITOIRE ARME" ou "SYSTEME ARME" suivant l'état courant de la totalité du système. Cela sera aussi indiqué par le lecteur.

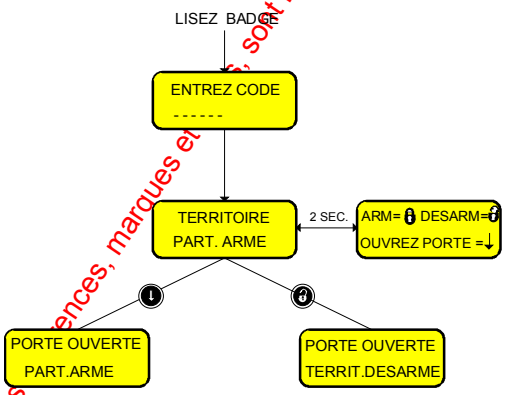
Situation normale



Situation avec alarme



Situation Territoire Partiellement Armé



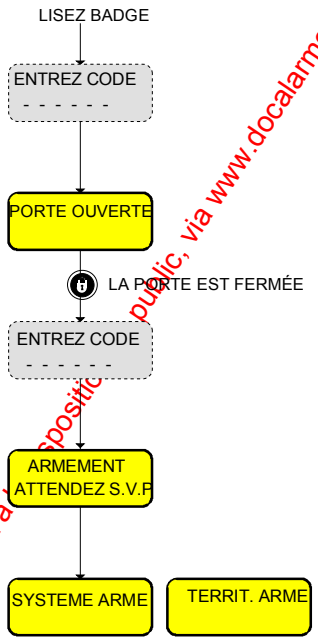
Dans les systèmes intégrés HISEC, il est aussi possible d'avoir un territoire partiellement armé. Dans ce cas, l'utilisateur peut faire le choix de désarmer le territoire complet ou d'accepter l'état du territoire et d'ouvrir la porte (voir ci-dessus).

Armement:

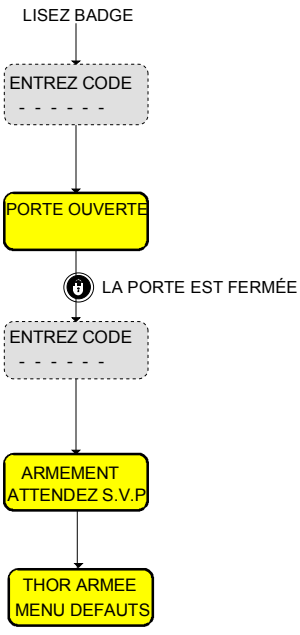
Quand une tentative d'armement est réussie sans défaut d'armement, l'affichage du lecteur sera le même pour HISEC ou non HISEC systèmes d'intrusion. Dans les systèmes d'intrusion non HISEC, c'est le type logiciel d'entrée 35 qui dit au lecteur si l'essai d'armement par le type logiciel de sortie 75 est réussi ou non.

Si le type logiciel d'entrée 35 n'a pas donné un signal d'armement dans les 10 secondes après l'armement, le lecteur HISEC affichera un défaut d'armement et il est alors nécessaire d'aller sur la centrale d'intrusion pour voir les défauts d'armements.

Procédure d'armement normale :



Procédure d'armement avec défauts :



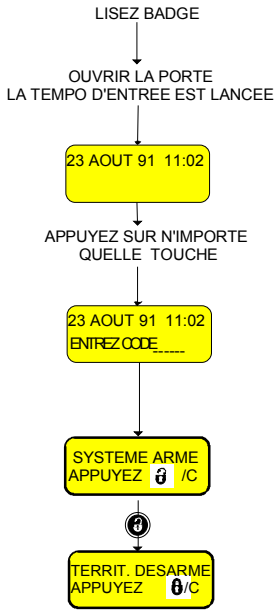
Dans un système intégré HISEC, le système d'intrusion HISEC prendra la main sur le contrôle d'accès et affichera une procédure de défaut d'armement normale sur le lecteur jusqu'à ce que la procédure d'armement soit terminée ou une fin de session réalisée par l'appui sur C.

4.2.8.2 Lecteur "tête déportée"

Etant donné que la tête de lecture est placée à l'extérieur de la porte à contrôler et que le terminal avec son clavier/afficheur incorporé de l'autre coté de la porte, un certain nombre de procédures seront différentes de celles du lecteur de badges standard RKP AC.

En général on peut dire que le lecteur se comporte comme un terminal intrusion classique, si une touche est appuyée sans lecture préalable d'un badge. La description suivante explique ces procédures qui sont un peu différentes de celle du lecteur classique ou du terminal standard.

Désarmement:



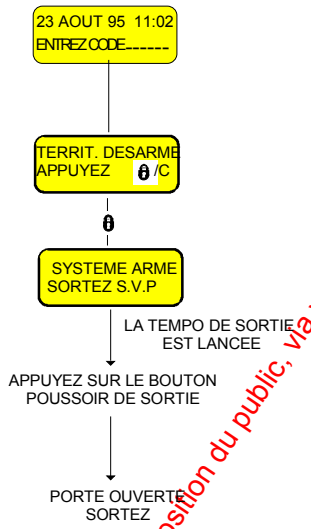
1: Lire le badge sur la tête de lecture extérieure.

2: **a**): La porte s'ouvrira si le groupe de personnel auquel appartient le badge possède la fonction de verrouillage (voir chap. 4.6) puis la temporisation d'entrée sera lancée. Le buzzer fonctionne sur le lecteur RKP ERC durant la temporisation d'entrée comme sur les terminaux classiques ou les lecteurs classiques. La temporisation d'entrée peut être lancée au moyen de l'ouverture de la porte ou par un détecteur (Infrarouge par exemple) en entrant dans la zone considérée comme route d'entrée.

b): La porte restera fermée si le possesseur du badge appartient à un groupe de personnel n'ayant pas la fonction verrouillage(AS).

3: Le terminal RKP ERC travaillera alors comme un terminal intrusion classique et acceptera directement le code intrusion (soit en entrant directement son code ou en appuyant sur n'importe quelle touche de fonction suite à quoi l'afficheur demandera d'entrer son code. Le territoire correspondant au code pourra être désarmé. Etant donné que le terminal RKP ERC est placé à l'intérieur de la zone à protéger, il n'est pas possible d'avoir accès à l'intrusion sans badge.

Armement



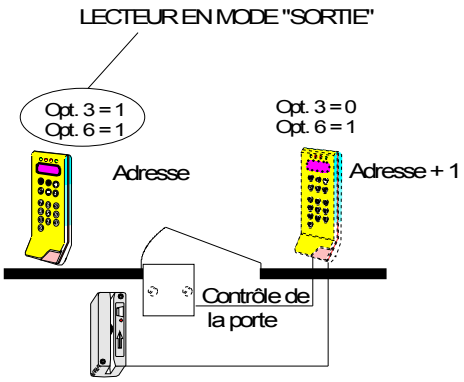
1: Composer son code Intrusion.

2: Presser la touche "cadenas fermé". La temporisation de sortie est alors lancée et le buzzer est actif pendant cette temporisation comme sur les terminaux déportés ou les lecteurs classiques.

3: Utiliser le bouton poussoir de sortie pour ouvrir la porte. L'information porte forcée peut être programmée pour donner une alarme immédiate sur le système intrusion.

4.2.9 Armement/Désarmement Intrusion à partir d'une porte avec lecteur d'entrée et sortie

Quand l'on utilise un lecteur avec tête extérieure (RKP ERC) et un lecteur standard (RKP ACC) pour contrôler la même porte, des fonctions spéciales doivent être accomplies en programmant les options 3 et 6 durant l'initialisation du lecteur comme représente sur la figure ci-dessous.



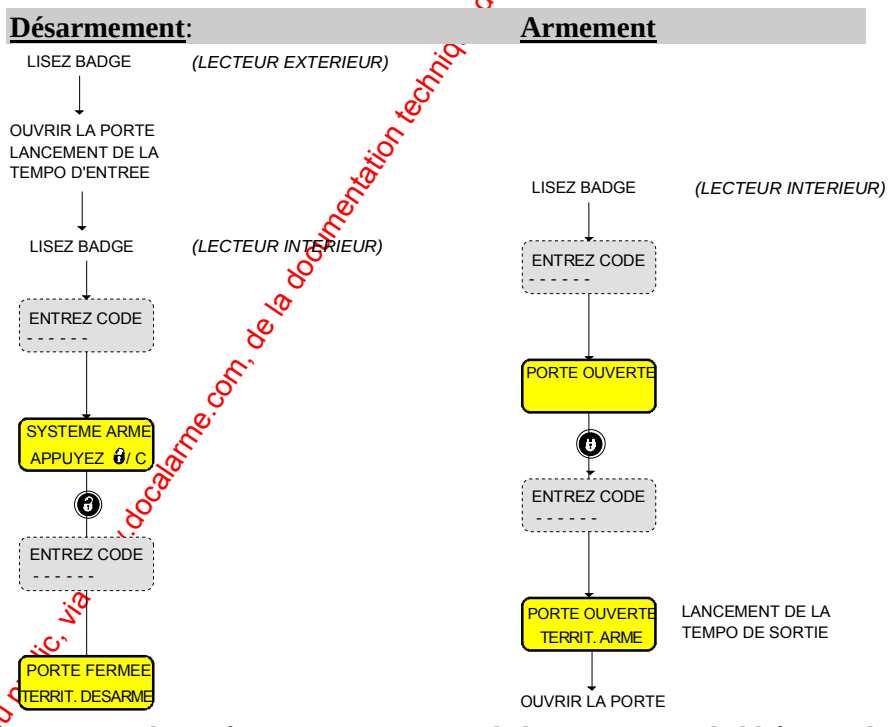
Normalement si le lecteur est de type intérieur son option 3 devra être à "1". Prière de remarquer aussi que le lecteur externe devra être celui qui contrôle la porte par un S-ART, il devra aussi avoir l'adresse supérieure de 1 sur le bus RS 485.

Le terminal du lecteur "externe" ne sera pas utilisé en fonctionnement quotidien et pour cette raison pourra être "caché". Cette configuration spéciale permet une association avec l'état d'armement/désarmement du système intrusion HISEC.

Le lecteur programmé avec les options 3 = 1 et option 6 = 1 fonctionnera dans un mode spécial de "lecteur de sortie".

Ce fonctionnement spécial "lecteur de sortie" est seulement valide pour le système intégré HISEC [Mode 03]. Dans les modes 01 et 02 le fonctionnement suit les règles classiques et habituelles.

Le lecteur contrôlant la tête extérieure (caché) fonctionne normalement excepté quand un message a été attribué à un badge, il n'attire pas l'attention avec son buzzer comme c'est le cas sur un lecteur seul sur une porte.



Après avoir armé un territoire du système intrusion HISEC, le lecteur activera la libération de la porte et le texte PORTE OUVERTE sera affiché sur le terminal (un lecteur classique RKP ACM bloquerai la porte).

Evidement si le système intrusion HISEC est armé, le lecteur activera la libération de porte pour vous éviter de rester bloquer dans le bâtiment si vous n'êtes pas autorisé à désarmer le système intrusion HISEC. Sur l'afficheur le message TERRITOIRE ARME sera indiqué.

Si un territoire du système intrusion HISEC est désarmé à partir du lecteur, le lecteur fermera la porte et indiquera TERRITOIRE DESARME, PORTE FERMEE.

4.2.10 Armement/Désarmement Intrusion non HISEC à partir du Lecteur

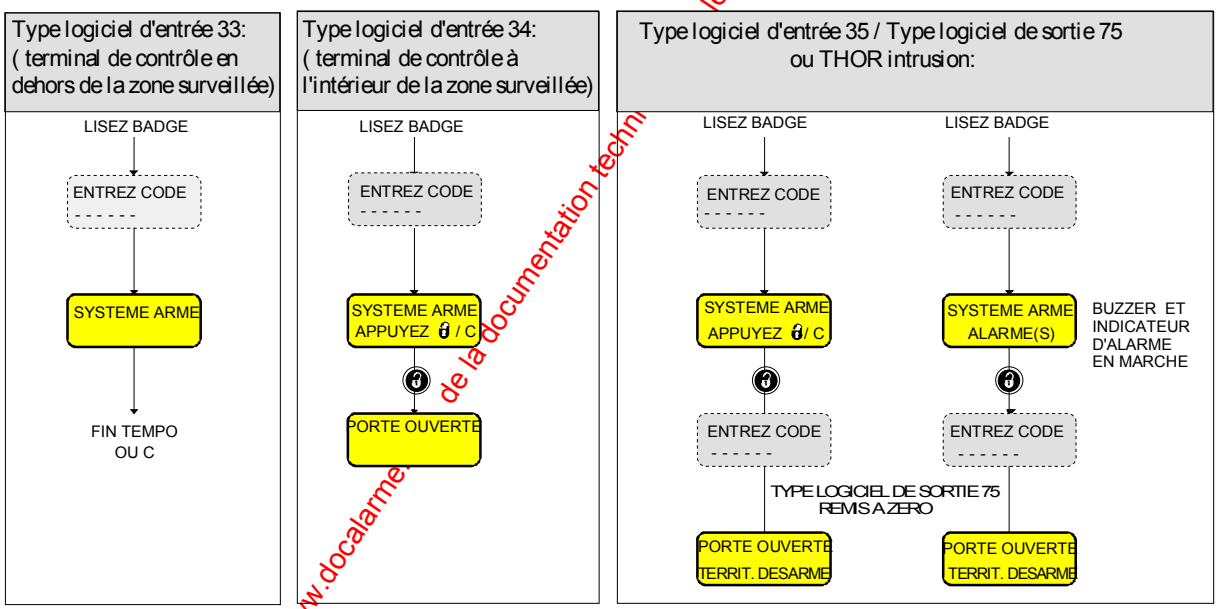
4.2.10.1 Lecteur standard

Désarmement:

Quand un système d'intrusion doit être désarmé (ou armé) le lecteur HISEC vous demandera toujours le Code Personnel appartenant au badge, même dans le cas où le système est programmé pour ne pas utiliser le Code Personnel en relation avec les procédures d'ouverture de la porte. Le code peut être entré avant ou après l'appui des touches cadenas ouvert/fermé en fonction du fait que le badge est programmé pour utiliser le Code Personnel ou non. Dans tous les cas, il est nécessaire de n'entrer qu'une seule fois le Code Personnel.

Un lecteur peut indiquer ou contrôler l'état d'armement d'un système d'intrusion non HISEC par différentes méthodes dépendantes de la définition du type logiciel d'entrée. Quand le lecteur est connecté au système d'Intrusion HISEC, il est possible de réaliser le désarmement du système d'intrusion HISEC si le Groupe de Personnel a été programmé pour pouvoir entrer en session sur le système d'intrusion (Fonction Verrouillage = Oui) avec un code correspondant au badge.

Le type logiciel d'entrée 33 est un signal d'armement/désarmement venant d'un système d'intrusion où le terminal de contrôle est placé en dehors de la zone surveillée. Si le système d'intrusion est armé, le lecteur affichera le message "SYSTEME ARME" mais n'ouvrira pas la porte comme représenté ci-dessous. Il est nécessaire d'aller sur le terminal de contrôle pour désarmer la centrale avant que l'accès ne soit donné par le lecteur HISEC.



Le type logiciel d'entrée 34 est un signal d'armement/désarmement venant d'un système d'intrusion où le terminal de contrôle est placé à l'intérieur de la zone surveillée. Si le système d'intrusion est armé, le lecteur affichera le message "SYSTEME ARME" mais ouvrira la porte - comme représenté ci-dessus - par appui sur la touche "cadenas ouvert". Il est alors nécessaire d'aller sur le terminal de contrôle et d'entrer dans la zone pour désarmer le système.

Le type logiciel d'entrée 35 est utilisé simultanément avec le type logiciel de sortie 75 où il est possible d'armer et désarmer un système d'intrusion avec un signal marche/arrêt. Le lecteur HISEC agira alors dans ce mode de la même façon qu'intégré au système d'intrusion HISEC. Quand un badge (et code) est accepté, le lecteur demandera à l'opérateur de presser la touche "cadenas ouvert" pour désarmer le système d'intrusion et après le désarmement, la porte sera ouvrable.

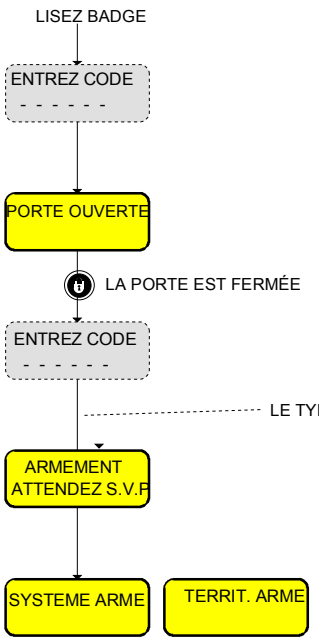
Armement:

Quand une tentative d'armement est réussie sans défaut d'armement, l'affichage du lecteur sera le même pour HISEC ou non HISEC systèmes d'intrusion. Dans les systèmes d'intrusion non HISEC, c'est le type logiciel d'entrée 35 qui dit au lecteur si l'essai d'armement par le type logiciel de sortie 75 est réussi ou non.

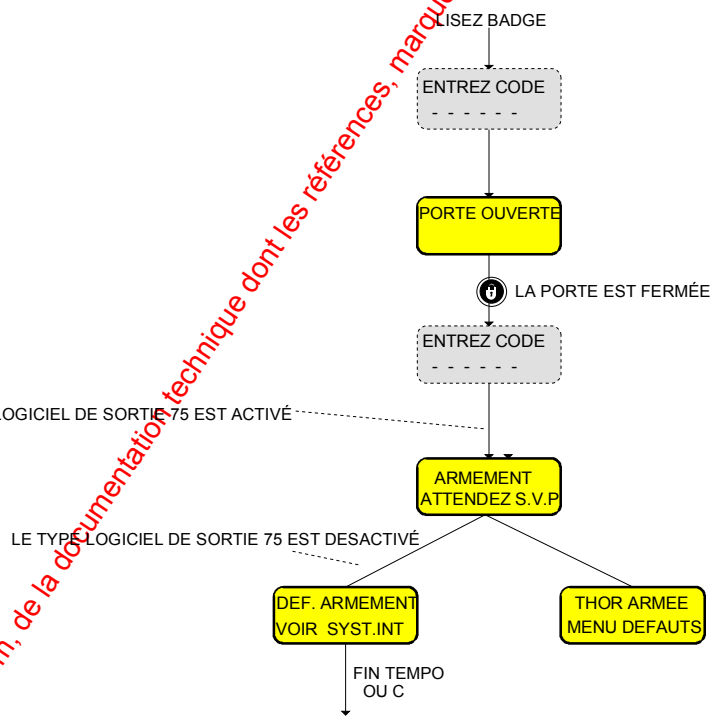
Si le type logiciel d'entrée 35 n'a pas donné un signal d'armement dans les 10 secondes après l'armement, le lecteur HISEC affichera un défaut d'armement et il est alors nécessaire d'aller sur la centrale d'intrusion pour voir les défauts d'armements.

Dans un système intégré HISEC, le système d'intrusion HISEC prendra la main sur le contrôle d'accès et affichera une procédure de défaut d'armement normale sur le lecteur jusqu'à ce que la procédure d'armement soit terminée ou une fin de session réalisée par l'appui sur "C".

Procédure d'armement normale :



Procédure d'armement avec défauts :



4.2.10.2 Lecteur "tête déportée"

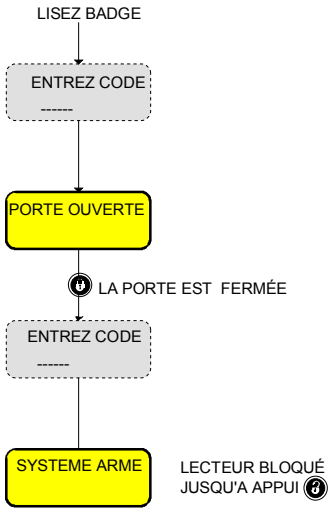
Il n'est **pas possible** de d'armer / désarmer un système d'intrusion externe (NON HISEC) avec le lecteur de contrôle d'accès à tête déportée en utilisant les types logiciel d'armement-désarmement.

4.2.11 Verrouillage/Déverrouillage du lecteur sans Intrusion

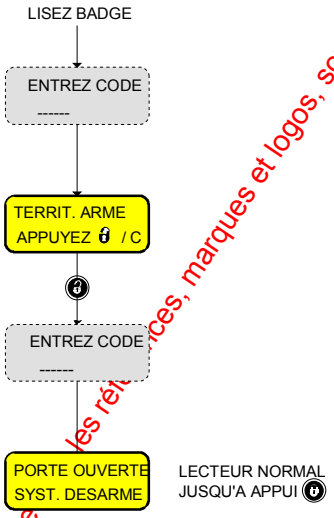
Il est possible pour des configurations sans système d'alarme de créer quelques badges avec la fonction "premier entré/dernier sorti" en donnant à ces groupes de personnel l'autorisation - fonction verrouillage = OUI -.

Par ce moyen, c'est le lecteur qui sera bloqué par l'utilisation de la touche Cadenas fermé jusqu'à ce que la touche Cadenas ouvert soit appuyée par l'utilisation d'un badge avec un groupe de personnel incluant les fonctions verrouillage.

Procédure de verrouillage



Procédure de déverrouillage



4.2.12 "Carte de crédit" pour ouverture de porte "sas bancaire"

Le groupe de personnel 250 permet d'autoriser l'utilisation des badges "cartes de crédit" pour ouvrir une porte. Cette fonction peut être utilisée dans les applications bancaires pour ouvrir la porte principale des accès aux "distributeurs de billets" par les clients de la banque. Dans le même temps le personnel de la banque peut ouvrir la porte en utilisant des badges HI SEC encryptés. Le groupe de personnel 250 peut comme les autres groupes de personnel être programmé avec des limitations et des restrictions horaires si nécessaire.

Il est très important que le programme hebdomadaire associé au groupe de personnel 250 ne soit pas programmé pour utiliser un code personnel, cela veut dire que la programmation FNC à 1 ne devra **pas** être utilisée. De plus le programme hebdomadaire 1 (pré-programmé accès permanent avec code) ne devra **pas** être utilisé. Au cas contraire le lecteur refusera les badges au format "carte de crédit".

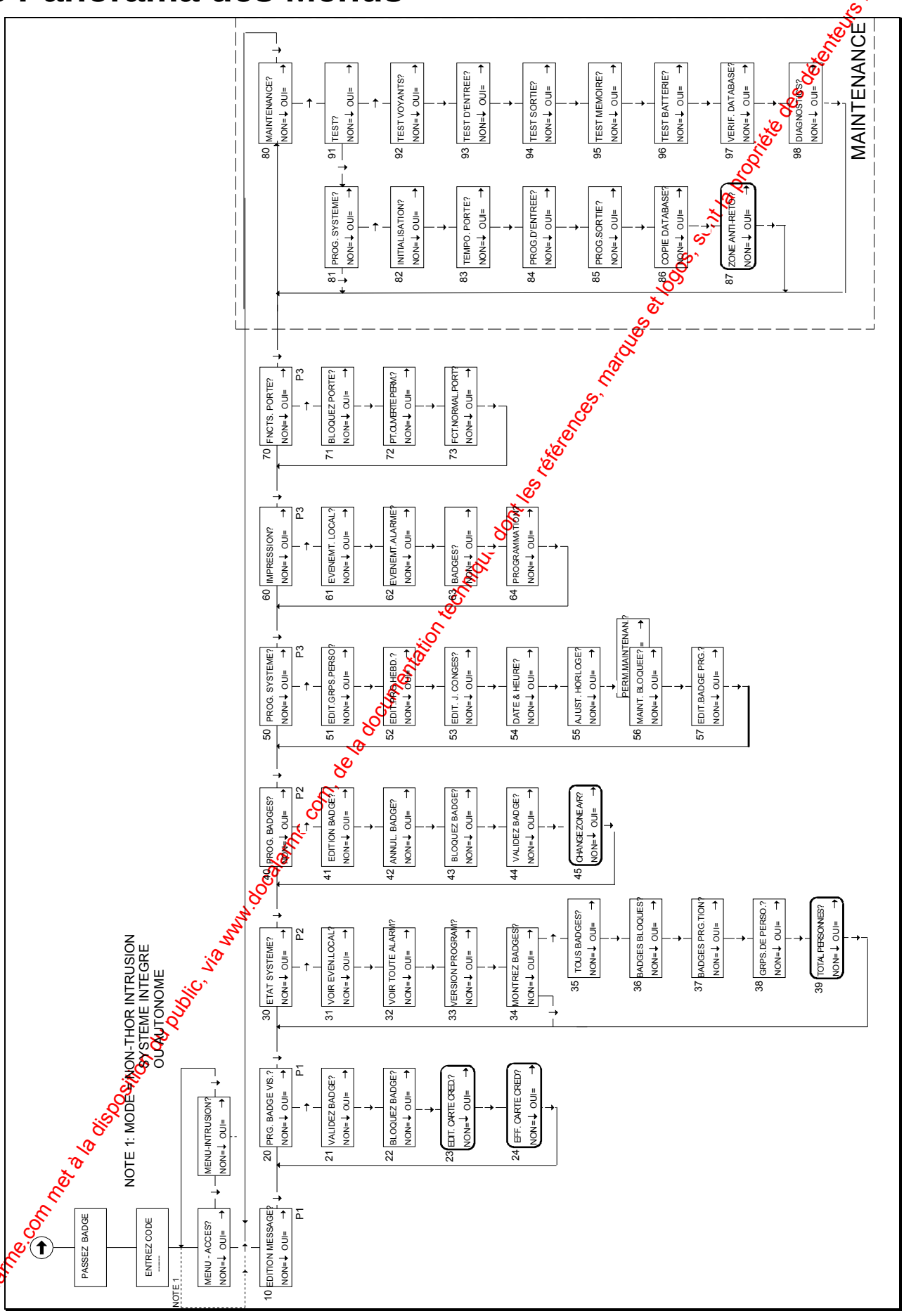
Si le groupe de personnel 250 est programmé avec pas d'accès (programme hebdomadaire 0) alors tous les badges au format "carte de crédit" seront refusés . Après initialisation du lecteur, les badges "cartes de crédit" sont bloqués et doivent êtres validés suivant la composition du groupe de personnel 250.

Le groupe de personnel 250 devra être programmé avec les paramètres suivants:

- PH = N° du programme hebdomadaire. Si le programme hebdomadaire est 02 les badges "cartes de crédit" seront acceptes 24 h sur 24.
- AS = Fonction verrouillage. Si programmée à 1 la porte s'ouvrira indépendamment de l'état d'armement désarmement du système intrusion HISEC . Si AS = 0 la porte pourra seulement être ouverte si le territoire du système d'intrusion est désarmé.
- HU = Validation du code contrainte. **Doit être programmé à 0.**
- CU = N° d'utilisateur dans le système intrusion. Doit être programmé en relation avec un numéro d'utilisateur intrusion HISEC. Le numéro d'utilisateur de l'intrusion n'aura accès à rien si la fonction AS a été programmée à 0.
- TE = Enregistre les accès normaux. Si ce paramètre est programmé à 1, tous les usages des badges "cartes de crédit" seront enregistrés. Quand un badge "carte de crédit" sera accepté une ligne sera imprimée avec les 6 derniers chiffres de la "carte de crédit" avec le texte CRED. Si cette fonction est programmée à "0" l'utilisation d'une carte de crédit ne sera pas enregistrée dans l'historique et sur l'imprimante. Cette fonction est aussi liée au programme hebdomadaire 31 "définition des enregistrements" et ceci pour tous les groupes de personnel.

Si le groupe de personnel (N° 250) des badges "cartes de crédit" est utilisé sur un lecteur intérieur de type RKP AC l'ouverture de la porte dépendra toujours de l'état d'armement/désarmement du système intrusion.

4.3 Panorama des Menus



4.4 Sous-menu 1 - Edition des Messages

Les 31 messages suivants sont pré-programmés dans le lecteur et ne peuvent pas être changés à partir du clavier du lecteur :

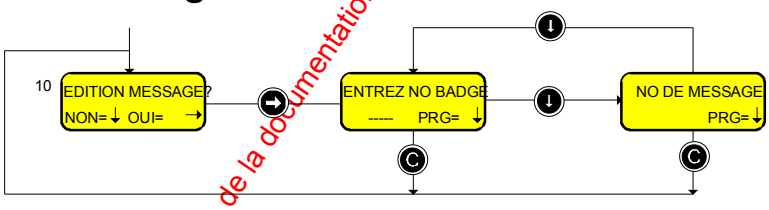
Message N°00	:	pas de message à l'utilisateur
Message N°01	:	CONTACTEZ LE DPT. PERSONNEL
Message N°02	:	CONTACTEZ VOTRE DOMICILE
Message N°03	:	CONTACTEZ LE DPT. SECURITE
Message N°04	:	CONTACTEZ LA RECEPTION
Message N°05	:	IMPORTANT MESSA. TELEPHONIQUE
Message N°06	:	CONTACTEZ VOTRE SUPERIEUR
Message N°07	:	R.D.V DEPLACEMENT ANNULE
Message N°08	:	REUNION ANNULEE
Message N°09	:	RAPPELEZ LE SIEGE
Message N°10	:	CONTACTEZ VOTRE SECRETAIRE
Message N°11	:	REVISION VEHICULE
Message N°12	:	DEPANNAGE URGENT
Message N°13	:	VISITE MEDICALE
Message N°14	:	COURRIER IMPORTANT
Message N°15	:	DOCUMENT A SIGNER

Le message programmé pour le badge sera automatiquement enlevé (message = 00) quand il sera acquitté par le porteur du badge.

Nota: Ces messages (31) peuvent uniquement être modifiés avec le logiciel PC.

Remarque: Ces messages appartiennent à la base de données **Globale** et de ce fait sont identiques pour tous les lecteurs du système.

Menu 10 : Edition Message



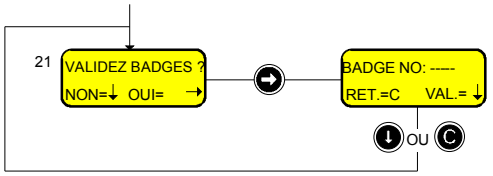
Le Menu 10 vous permet d'envoyer un message à destination de n'importe quel badge. Après appui sur la touche → le numéro du badge sera entré sur le clavier et après appui sur la touche ↓, le numéro de message associé au badge apparait. Un nouveau numéro de message choisi dans la liste du chapitre précèdent sera entré suivi par la touche ↓. Après programmation du message, l'afficheur propose le prochain badge appartenant au même Groupe de Personnel.

Pour quitter ce menu on utilisera la touche C.

4.5 Sous-menu 2 - Badges visiteurs

Les badges de programmation avec n'importe quelle priorité peuvent être utilisés pour valider ou bloquer un badge visiteur (badges appartenant toujours au Groupe de Personnel N° 1). Tous les badges visiteurs délivrés seront automatiquement bloqués à 24:00 heures le même jour, mais peuvent aussi être bloqués à la demande si nécessaire.

Menu 21 : Validation d'un Badge Visiteur



Ce Menu permet de valider (activer) un badge visiteur.

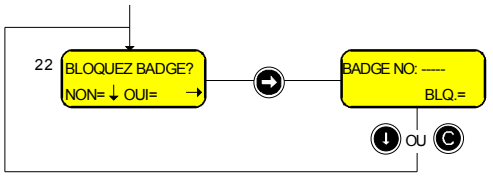
Vous devez préciser le Numéro de badge (5 chiffres) et appuyer sur la touche ⬇.

Ensuite, le badge sera valide jusqu'à 24H00 par défaut, mais pourra être bloqué manuellement au moyen du Menu 22.

þ Prière de noter que le badge devra avoir été préalablement (au démarrage du système) défini comme appartenant au groupe de personnel des visiteurs (groupe de personnel N°1).

Pour quitter ce menu on utilisera la touche C.

Menu 22 : Blocage d'un Badge Visiteur

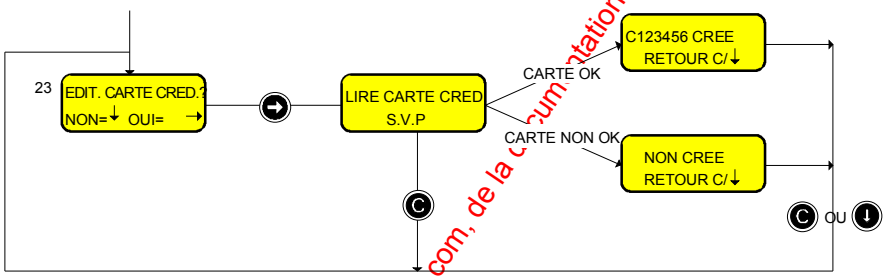


Ce Menu vous permet de bloquer de façon manuelle un badge visiteur. Vous devez préciser le Numéro de badge (5 chiffres) et appuyer sur la touche ⬇.

Après cela, le badge ne sera plus accepté sur aucun lecteur du système.

Pour quitter ce menu on utilisera la touche C.

Menu 23 : Création "Carte de crédit" Visiteur



Ce Menu vous permet de programmer les "cartes de crédit" en badges visiteurs.

Quand cette fonction est appelée le lecteur vous demande de lire la "carte de crédit" sur le lecteur.

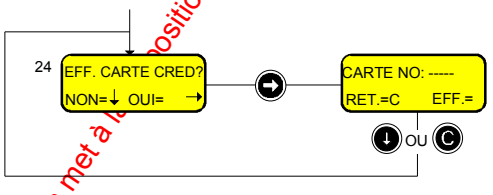
Cette opération réalisée, l'afficheur indique que la carte a été créée et donne son numéro (les 6 derniers chiffres). Le numéro peut être alors noté avec le nom du visiteur.

L'utilisation d'une "carte de crédit" sur un des lecteurs commandera l'ouverture de la porte, le numéro de la carte de crédit sera imprimé et enregistré dans l'historique avec la mention CRED.

Attention :Vous ne pouvez créer plus de **50 badges visiteurs** par système, en cas de dépassement l'afficheur indiquera NON CREE.

Pour quitter ce menu on utilisera la touche C.

Menu 24 : Effacement "Carte de crédit" Visiteur



Ce Menu vous permet de bloquer de façon manuelle un badge visiteur au format carte de crédit.

Si le visiteur quitte l'établissement avant la fin du programme hebdomadaire correspondant, il est possible d'effacer un badge visiteur "carte de crédit" par ce Menu.

Quand ce Menu est appelé le numéro de la carte doit être entré suivi par la touche ⬇. Il est aussi possible de ne pas entrer le numéro de la "carte de crédit" et de lire directement la "carte de crédit" sur le lecteur.

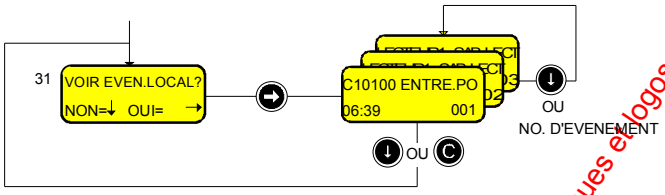
Après cela, la "carte de crédit" ne sera plus accepté sur aucun lecteur du système.

4.6 Sous-menu 3 - Affichage des Etats du Système

Avec les niveaux de priorités Utilisateur 2 & 3 et le niveau de priorité Maintenance, il est possible de visualiser la programmation des configurations système de la base de données des badges et des enregistrements d'historique.

Menu 31 : Visualiser l'historique Local

L'historique local comprend les transactions normales de porte, les lectures de badges et les alarmes du lecteur sur lequel on opère. Chaque lecteur possède un historique de 2300 événements. Quand l'historique est plein, les plus vieux événements sont écrasés.



Il est possible d'appeler un événement en tapant directement au clavier son numéro, ou obtenir l'événement suivant par appui sur la touche ↓. Le dernier (le plus récent) événement est affiché en premier (001).

Les événements, pouvant être enregistrés dans le lecteur, sont les suivants :

Texte	Explication	Paramètres	
ENTREE.P	Entrée sur porte	Numéro de Badge (B)	Lecteur N° (L)
SORTIE.P	Sortie sur porte	Numéro de Badge (B)	Lecteur N° (L)
	Changement de jour "nouvelle date"		
MAR.INSTA	Armement du système d'intrusion	Numéro de Badge (B)	Lecteur N° (L)
ARR.INST	Désarmement du système d'intrusion	Numéro de Badge (B)	Lecteur N° (L)
TEST.ENT	Test d'entrée	N° de S-ART	Etat de l'Entrée (E)
EN.SESS	Entrée en session	Numéro de Badge (B)	Lecteur N° (L)
HOR.SESS	Sortie de session	Numéro de Badge (B)	Lecteur N° (L)
EDI.BADG	Edition de badges	Numéro de Badge (B)	Lecteur N° (L)
EFF.BADG	Effacement de badge	Numéro de Badge (B)	Lecteur N° (L)
BLO.BADG	Blocage de badges	Numéro de Badge (B)	Lecteur N° (L)
VAL.BADG	Validation de badge	Numéro de Badge (B)	Lecteur N° (L)
ANC.HEUR	Ancienne heure (changement heure)	Date et Heure	
NOU.HEUR	Nouvelle heure (changement heure)	Date et Heure	
EXE.MENU	Exécution d'un Menu	Numéro de Badge (B)	Menu N° (M)
BADG.REF	Badge refusé	Lecteur N° (L)	
PORT.FER	Porte fermée (après porte maintenue)	Lecteur N° (L)	

Le N° du lecteur apparaîtra seulement sur la sortie sur imprimante de l'historique mais ne sera pas visualisé dans ce Menu, étant donné que cet historique est valable seulement pour le lecteur où l'on opère.

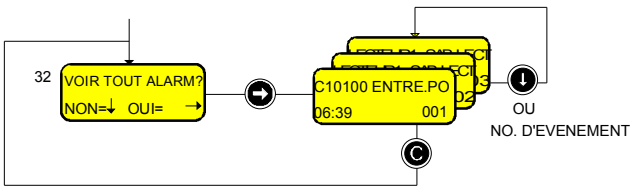
Pour chaque événement, l'heure et la date sont affichées.

Toutes les alarmes locales du lecteur seront aussi visualisées dans l'historique des événements. Voir plus avant pour une explication complète de chacun de ces événements.

Pour quitter ce menu on utilisera la touche C.

Menu 32 : Visualisation de Toutes les Alarmes

L'historique des alarmes est un historique global contenant toutes les alarmes/sabotages etc. pour le système complet. L'historique des alarmes peut contenir un maximum de 100 événements. Quand l'historique est plein, les plus vieux événements sont écrasés.



Il est possible d'appeler un événement en entrant directement son numéro au clavier ou obtenir l'événement suivant par appui sur la touche ⬇. Le dernier (le plus récent) événement est affiché en premier (001).

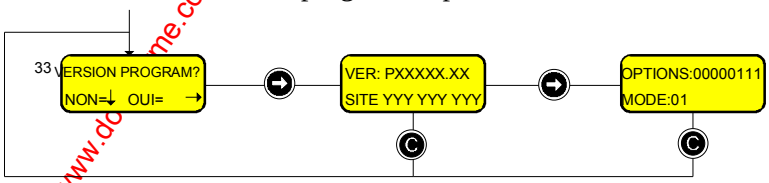
Texte	Explication	Paramètres	
HOLD-UP	Utilisation du code Contrainte	N° de Badge (B)	N° de Lecteur (L)
SAB. LECT	Sabotage du lecteur	N° de Lecteur (L)	
SAB. SART	Sabotage de S-ART	N° de Lecteur (L)	N° de S-ART
PO. FORCE	Porte forcée ouverte	N° de Lecteur (L)	
PO. MAINT	Porte maintenue	N° de Lecteur (L)	
DEF. BATT	Défaut batterie	N° de Lecteur (L)	
DEF. SYST	Défaut système	N° de Lecteur (L)	N° d'Erreur (F)
DEF. SECT	Défaut secteur d'une heure	N° de Lecteur (L)	
ALARM. EX	Système d'intrusion externe en alarme	N° de Lecteur (L)	N° de S-ART
BADG.BLO	Utilisation d'un badge bloqué	N° de Badge (B)	N° de Lecteur (L)
BADG.ILL	Utilisation d'un badge invalide	N° de Badge (B)	N° de Lecteur (L)
MAUV. COD	Mauvais Code Personnel (10 fois)	N° de Badge (B)	N° de Lecteur (L)
NOUV. B.D	Base de données changée	N° de Lecteur (L)	
MAINTENA	Utilisation d'un badge Maintenance	N° de Badge (B)	N° de Lecteur (L)
COUP. ALIM	Coupure d'alimentation	N° de Lecteur (L)	
PROG.SYS	Programmation syst avec le menu 51-57	N° de Lecteur (L)	N° de Menu (M)
P.P. OUVE	Porte ouverte en permanence	N° de Lecteur (L)	
P. NORMAL	Porte revenue à son fonction. normal	N° de Lecteur (L)	
INIT LECT	Initialisation du lecteur	N° de Lecteur (L)	

Pour chaque événement, la date et l'heure sont affichées.

Pour quitter ce menu on utilisera la touche Ⓒ.

Menu 33 : Visualisation de la Version du Programme et du code Site

Dans ce menu, il est possible de visualiser les informations sur la version du logiciel, le code site du système, les Options sélectionnées et le Mode programmé pour le lecteur.



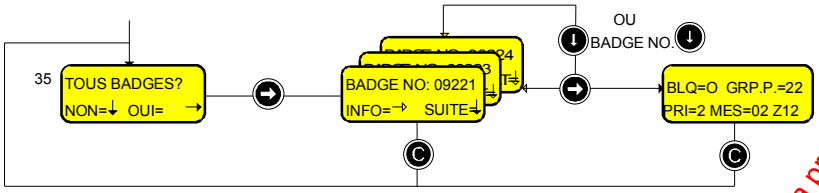
Le numéro de la version du logiciel est égal à celui indiqué sur l'EPROM à l'intérieur du lecteur et le code Site est le numéro Distributeur (3 chiffres), Installateur (3 chiffres) et le numéro de Client (3 chiffres). Par l'appui sur la touche ➡, les Options et Mode du lecteur seront affichés.

Pour quitter ce menu on utilisera la touche Ⓒ.

Menu 35 : Visualisation de Tous les Badges

Par ce menu, il est possible de visualiser toutes les informations concernant les badges programmés.

Badges en format Standard :



Quand cette fonction d'affichage est appelée, l'afficheur propose le premier badge de la base de données.

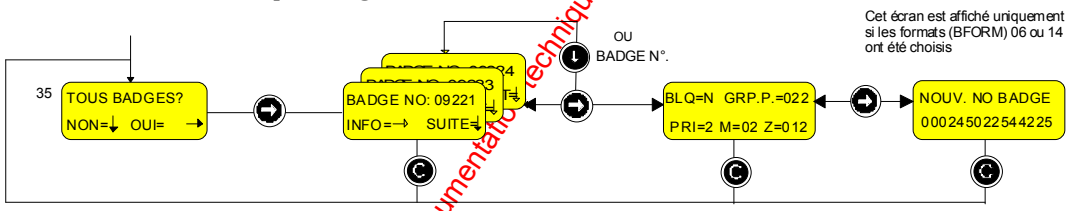
Les informations suivantes seront affichées par l'utilisation de la touche ➔ :

BLQ = Badge bloqué ou non
GRP.P = Numéro de Groupe de Personnel associé au badge
PRI = Priorité de programmation
MES = Numéro de message attribue à ce badge pour l'instant (si existant)
Z = Numéro de la zone d'anti-retour où est le badge au moment donné.

Par l'utilisation de la touche ⬇, le prochain badge programmé sera visualisé. Par entrée du numéro de badge, le premier des badges suivants sera affiché. Quand la liste est terminée, l'afficheur revient au premier badge à nouveau. Par l'intermédiaire de la touche C, la fonction d'affichage est stoppée et un retour au *Menu 35* est effectué.

Badges en format Libre (mode 06 & 14) :

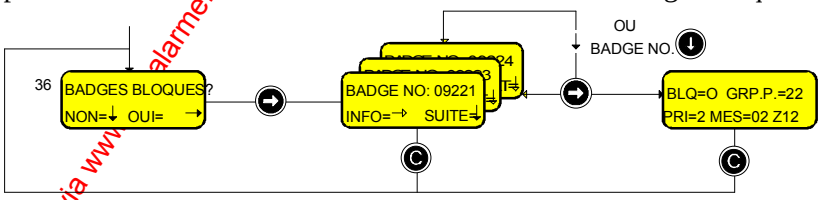
Dans tous les menus de visualisation de badges en utilisant la touche ➔ il est possible de visualiser le contenu du format libre de chaque badge.



Prière de remarquer que le menu affiche toujours 16 caractères même si l'on en utilise moins, les caractères non utilisés seront remplacés par des zéros.

Menu 36 : Visualisation des Badges Bloqués

Par ce menu, il est possible de visualiser toutes les informations sur les badges bloqués.



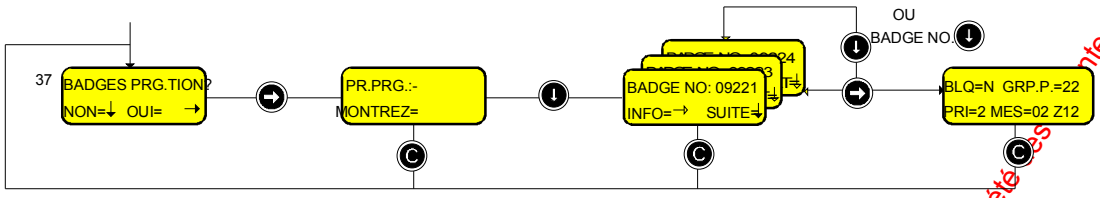
Quand cette fonction d'affichage est appelée, l'afficheur propose le premier badge bloqué.

Les informations suivantes seront affichées par l'utilisation de la touche ➔ :

BLQ = Badge bloqué ou non
GRP.P = Numéro de Groupe de Personnel associe au badge
PRI = Priorité de programmation
MES = Numéro de message attribue à ce badge pour l'instant (si existant)
Z = Numéro de la zone d'anti-retour où est le badge au moment donné.

Par l'utilisation de la touche ⬇, le prochain badge bloqué sera visualisé. Par entrée du numéro de badge, le premier des badges bloqués suivants sera affiché. Quand la liste est terminée l'afficheur revient au premier badge à nouveau. Par l'intermédiaire de la touche C, la fonction d'affichage est stoppée et un retour au *Menu 36* est effectué.

Menu 37 : Visualisation des Badges de Programmation



Quand ce menu est appelé, l'afficheur vous demande quel niveau de priorité des badges de programmation doit être visualisé. L'afficheur proposera alors le premier numéro de badge avec un niveau de programmation égal au N° entré. Le PR.PRG. indique la priorité de programmation.

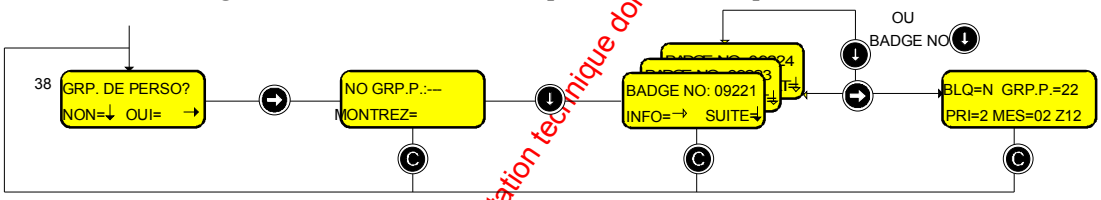
Les informations suivantes seront affichées par l'utilisation de la touche :

BLQ = Badge bloqué ou non
GRP.P = Numéro de Groupe de Personnel associé au badge
PRI = Priorité de programmation
MES = Numéro de message associé à ce badge pour l'instant (si existant)
Z = Numéro de la zone d'anti-retour où est le badge au moment donné.

Par l'utilisation de la touche ↓, le prochain badge de programmation sera visualisé. Par entrée du numéro de badge, le premier des badges de programmation suivants avec la même priorité sera affiché. Quand la liste est terminée, l'afficheur revient au premier badge à nouveau. Par l'intermédiaire de la touche C, la fonction d'affichage est stoppée et un retour au *Menu 37* est effectué.

Menu 38 : Visualisation des Groupes de Personnel

Par ce menu, tous les badges avec le numéro de Groupe de Personnel spécifié sont affichés.



Quand ce menu est appelé, l'afficheur vous demande quel numéro de groupe de personnel doit être affiché. L'afficheur présente alors le premier numéro de badge avec un numéro de groupe de personnel égal au numéro entré. Le GRP.P. indique le numéro du Groupe de Personnel.

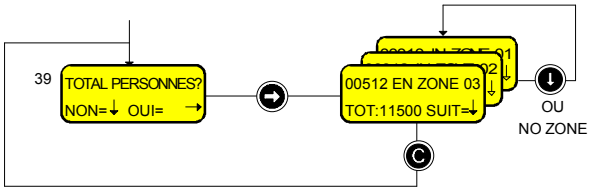
Les informations suivantes seront affichées par l'utilisation de la touche → :

BLQ = Badge bloqué ou non
GRP.P = Numéro de Groupe de Personnel associé au badge
PRI = Priorité de programmation
NO.MES = Numéro de message associé à ce badge pour l'instant (si existant)
Z = Numéro de la zone d'anti-retour où est le badge au moment donné.

Par l'utilisation de la touche ↓, le prochain numéro de badge, avec le numéro de groupe de personnel égal au numéro déjà entré, sera visualisé. Par entrée du numéro de badge, le premier des badges suivants avec ce numéro de groupe de personnel sera affichée. Quand la liste est terminée, l'afficheur revient au premier numéro à nouveau. Au moyen de la touche C, la fonction d'affichage est stoppée et un retour au *Menu 38* est effectué.

Menu 39 : Visualisation du total des personnes

Par ce menu il est possible de savoir combien de badges sont présents - à ce moment - dans chaque zone et combien de badges sont à l'intérieur du bâtiment (pas en zone 00).



Seuls les badges de priorité 2 (ou plus élevée) peuvent utiliser ce Menu.

4.7 Sous-Menu 4 - Programmation des Badges

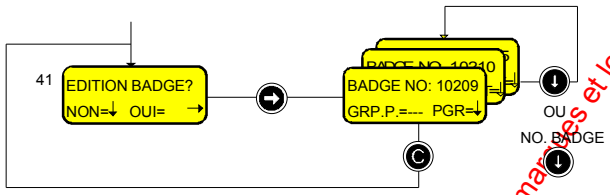
La programmation des badges consiste en l'ensemble des points suivants :

Création et effacement des badges, modifications des informations des badges, par ex : changement des Groupes de Personnel, des états des badges ayant été bloqués ou non. La programmation des badges pourra seulement être réalisée avec des badges ayant un niveau de priorité privilégié.

Menu 41 : Edition des Badges

Par ce menu, il est possible de créer un badge et en même temps de lui attribuer un numéro de Groupe de Personnel.

Badges en format Standard :



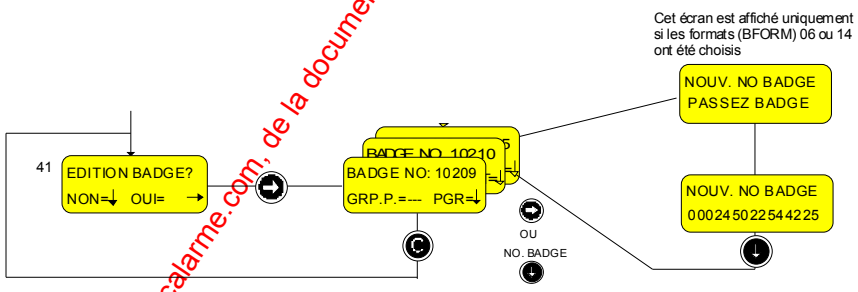
Quand cette fonction est appelée, l'afficheur vous propose le premier numéro de badge libre. A ce moment le numéro de groupe de personnel peut être entré, et la touche ⬇ valide la programmation. Si le numéro de badge n'est pas correct, un nouveau numéro de badge peut être frappé avant l'appui sur la touche ⬇.

Après la programmation du badge en utilisant la touche ⬇, le lecteur propose le prochain badge libre avec le même numéro de Groupe de Personnel. Il est alors facile de programmer un groupe de badges simplement en appuyant sur la touche ⬇ à chaque badge.

Par appui sur la touche C, l'afficheur revient au *Menu 41* sans avoir effectué de programmation.

Badges en format Libre (mode 06 & 14) :

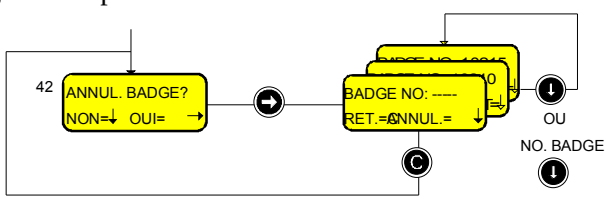
Les badges en format libre seront programmés au moyen du même menu que les badges standards. Le badge sera programmé en le lisant directement sur la tête de lecture, il est impossible de les programmer en entrant directement les données au clavier.



Prière de remarquer que le menu lit toujours 16 caractères même si l'on en utilise moins, les caractères non utilisés seront remplacés par des zéros.

Menu 42 : Effacement d'un Badge

Par ce menu, il est possible d'effacer un badge de la base de données. Toutes les données programmées précédemment dans le badge seront perdues.



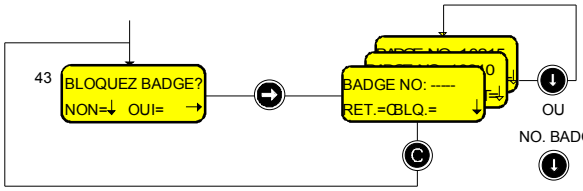
Quand cette fonction est appelée, l'afficheur demande le numéro du badge à effacer. Après que ce numéro ait été entré, l'appui sur la touche ⬇ efface le badge. Si le numéro du badge n'est pas correct, un nouveau numéro de badge peut être entré avant l'appui sur la touche ⬇.

Après que le badge ait été effacé par utilisation de la touche ⬇, le lecteur vous propose le prochain numéro de badge appartenant au même Groupe de Personnel. Il est alors facile d'effacer une série de badges, simplement en appuyant sur la touche ⬇ à chaque badge.

Par appui sur la touche C, l'afficheur revient au *Menu 42* sans avoir effectué d'effacement.

Menu 43 : Blocage d'un Badge

Par ce menu, il est possible de bloquer un badge. Toutes les données programmées précédemment dans le badge à bloquer pourront être remises dans la base de données.



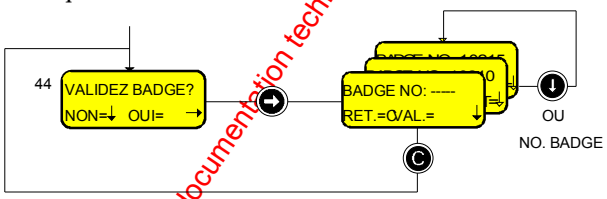
Quand cette fonction est appelée, l'afficheur demande le numéro du badge à bloquer. Après que ce numéro ait été entré, l'appui sur la touche ⬇ bloque le badge. Si le numéro du badge n'est pas correct, un nouveau numéro de badge peut être entré avant l'appui sur la touche ⬇.

Après que le badge ait été bloqué par l'utilisation de la touche ⬇, le lecteur vous propose le prochain numéro de badge appartenant au même Groupe de Personnel. Il est alors facile de bloquer un groupe de badges, simplement en pressant la touche ⬇ à chaque badge.

Par appui sur la touche C, l'afficheur revient au *Menu 43* sans avoir effectué de blocage.

Menu 44 : Validation d'un Badge

Par ce menu, il est possible de valider un badge précédemment bloqué. Les données programmées précédemment dans le badge bloqué seront remises dans la base de données.



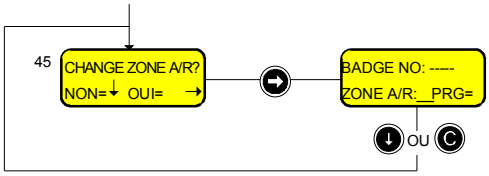
Quand cette fonction est appelée, l'afficheur propose le numéro du premier badge bloqué à valider et l'appui sur la touche ⬇ valide le badge. Si le numéro du badge n'est pas correct, un nouveau numéro de badge peut être entré avant l'appui sur la touche ⬇.

Après que le badge ait été validé par utilisation de la touche ⬇, le lecteur vous proposera le prochain numéro de badge bloqué appartenant au même Groupe de Personnel. Il est alors facile de valider une série de badges, simplement en appuyant la touche ⬇ à chaque badge.

Par appui sur la touche C, l'afficheur revient au *Menu 44* sans avoir effectué de validation.

Menu 45 : Changement de Zone d'anti-retour

Par ce menu il est possible de passer un badge d'une zone d'anti-retour à une autre.



Après l'appel de ce Menu le numéro du badge et le numéro de la zone doivent êtres entrés. Quand la touche ⬇ est appuyée pour valider la programmation, le badge peut être utilisé dans la zone choisie ou pour quitter la zone.

Seuls les badges de priorité 2 (ou plus élevée) peuvent utiliser ce Menu.

Par appui sur la touche C, l'afficheur revient au *Menu 45* sans avoir effectué de validation.

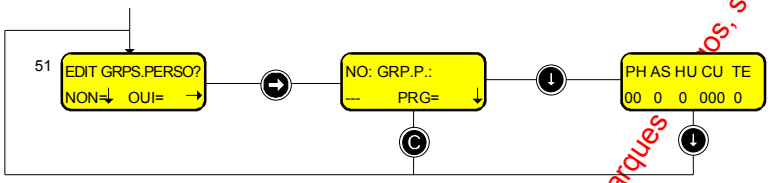
4.8 Sous-Menu 5 - Programmation Système

Par programmation système, on entend : création des groupes de personnel, périodes d'accès et jours spéciaux. La commande pour réaliser la programmation sera effectuée par un badge ayant une priorité élevée.

Menu 51 : Edition des Groupes de Personnel

Cette fonction permet à l'utilisateur de créer ou de modifier les Groupes de Personnel. Un nombre de 3 chiffres doit être entré et validé par la touche ⬇.

Après cela, les paramètres relatifs à ce groupe seront entrés. Le système est pré-programmé avec la valeur par défaut "0" pour tous les paramètres.



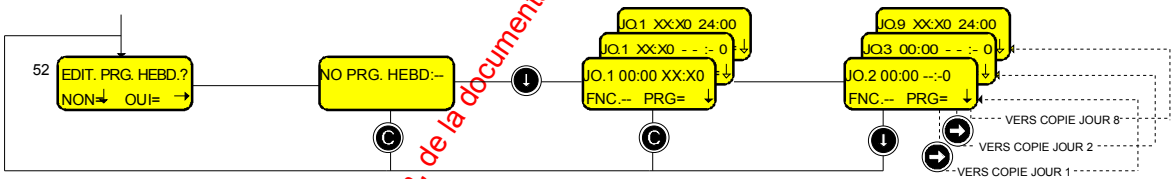
PH = N° de Programme Hebdomadaire
AS = Armement permis sur le système d'intrusion (fonction verrouillage)? (1=OUI, 0=NON)
HU = Code Hold-Up autorisé pour ce groupe ? (1=OUI, 0=NON)
CU = N° de code utilisateur du système d'intrusion (1-250)
TE = Enregistrement des transactions normales ? (1=OUI, 0=NON)

Après que ces paramètres aient été entrés, la touche ⬇ devra être utilisée pour mémoriser les données.

La base de données des Groupes de Personnel est une base de données locale, ceci est important car elle devra être programmée pour chaque lecteur ou copiée manuellement d'un lecteur à un autre.

Menu 52 : Edition des Programmes Hebdomadaires

Cette fonction est utilisée pour créer, modifier ou effacer des Programmes Hebdomadaires, un Programme Hebdomadaire possède 7 jours normaux (Lundi = 1er jour) et deux jours spéciaux (jours 8 & 9) se référant à la liste des jours de congés.



Deux chiffres sont nécessaires pour définir le numéro du Programme Hebdomadaire (max.: 35) après quoi le jour 1 est affiché avec son heure de départ 00:00. La première période sera alors de 00:00 à xx:x0 où x est le chiffre à entrer. L'heure xx:x0 sera automatiquement transférée vers l'heure de départ de la prochaine période horaire pour le JOUR 1 pour éviter à l'utilisateur de créer un programme horaires avec des "creux" ou des chevauchements de périodes. Un jour est terminé quand 24:00, est programmé comme période de fin et le jour suivant JOUR 2 est proposé sur l'afficheur. Si la touche ➡ est appuyée à cet endroit une copie du jour précédent sera effectuée pour ce jour.

Si un de ces menus est quitté par appui sur la touche Ⓒ, le programme "*Edition des Programmes Hebdomadaires*" est quitté sans mémorisation des données pour ce Programme Hebdomadaire.

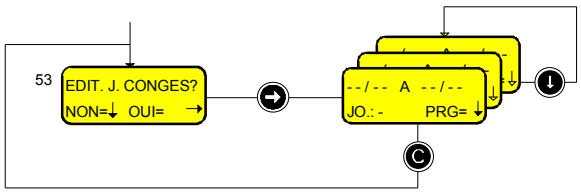
Par l'entrée de la période 00:00 à 00:00, le Programme Hebdomadaire est effacé.

Il est seulement possible de programmer les intervalles avec une résolution de 10 minutes. De ce fait, il est seulement nécessaire d'entrer 3 chiffres. Le dernier chiffre sera toujours un 0.

Le champ FNC est programmé avec les numéros des fonctions décrites au *Chapitre 1.7.3*. Cela ajoutera une fonction spécifique devant être exécutée durant les périodes décrites dans les programmes horaires.

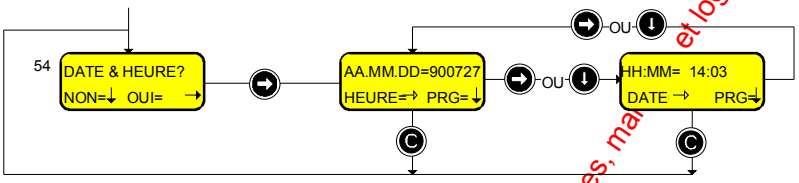
Menu 53 : Edition de la liste des périodes de Congés

Cette fonction est utilisée pour créer ou modifier une liste de jours de congés avec référence au Programme Hebdomadaire décrit ci-dessus.



La liste possède au maximum 25 périodes commençant à une date de départ et finissant à une date de fin pour chaque période. La période comprend la date de départ et la date de fin.

Menu 54 : Mise à la Date et Heure



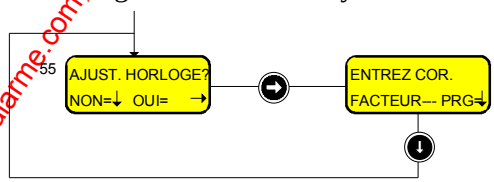
La date est changée en entrant année, mois et jour. Quand le dernier chiffre est entré suivi de la touche ⬇, l'heure apparaît automatiquement et demande un rajustement par entrée des heures et minutes. Si la date ne doit pas être changée, l'heure est affichée directement par appui sur la touche ➡, laquelle est aussi utilisée pour revenir à la date. La date et l'heure ne sont pas modifiées jusqu'à l'appui sur la touche ⬇, suite à cela, les secondes seront remises à zéro et l'affichage reviendra.

Par appui sur la touche Ⓒ, un retour au *Menu 54* est effectué.

Nota: Cette fonction n'est pas accessible dans les systèmes en mode Intégré HISEC - **Mode 03-**, dans ce cas la mise à l'heure et date se fera dans le menu Intrusion (*Menu 41*).

Menu 55 : Ajustement de l'Horloge

Dans une configuration avec intégration, la centrale Intrusion HISEC sera l'horloge maître et l'heure sera remise à jour toutes les minutes. Pour les configurations Autonomes ou Multi-lecteurs, il peut être nécessaire d'ajuster la vitesse de l'horloge avec un facteur calculé par ex. pendant une semaine. Sur un système à bus il est seulement nécessaire d'ajuster un seul lecteur. Cet ajustement sera automatiquement téléchargé dans le lecteur 0, qui est l'horloge maître dans un système Multi-lecteurs.



4 chiffres peuvent être entrés après appel de ce menu. Le premier chiffre peut seulement être 0 ou 1 et il indique si l'horloge doit être ajustée en avance (positive) ou en retard (négative).

0 : indique une correction négative (l'horloge tournera plus lentement).

1 : indique une correction positive (l'horloge tournera plus vite).

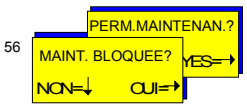
Les 3 chiffres suivants sont la quantité de secondes à incorporer à l'horloge pour l'accélérer ou la ralentir pendant **une semaine**. L'ajustement maximum sera de 999 secondes.

L'horloge sera automatiquement ajustée une fois par jour (à minuit) avec le nombre de secondes précédemment entré divisé par 7.

Nota: Cette fonction n'est pas accessible dans les systèmes en mode Intégré HISEC - **Mode 03-**, dans ce cas la mise à l'heure étant assurée par la centrale HISEC Intrusion et ne nécessite pas de correction.

Menu 56 : Blocage et Autorisation du mode Maintenance

Quand le *Menu 56* est appelé, le texte affiché déprendra des conditions du système, principalement si le mode Maintenance est autorisé ou non.

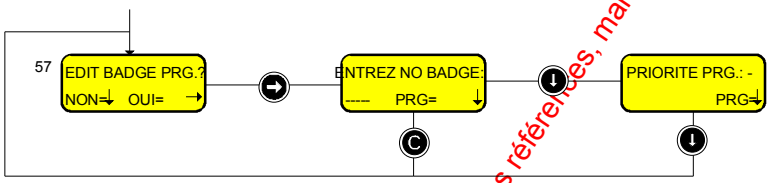


Si le mode Maintenance est autorisé, le texte "MAINT.BLOQUEE?" apparaîtra et par la réponse OUI=➊, le texte sera changé et la Maintenance ne sera pas plus autorisée.

Si le mode Maintenance n'est pas autorisé, le texte "PERM. MAINTENAN.?" apparaîtra et par la réponse OUI=➊ le texte sera changé et le mode Maintenance sera maintenant autorisé.

Menu 57 : Edition des Badges de Programmation

Cette fonction est utilisée pour attribuer ou changer la priorité affectée à un badge de programmation. Un badge de programmation ayant été **créé précédemment** par le *Menu 41* peut être affecté d'une nouvelle priorité.



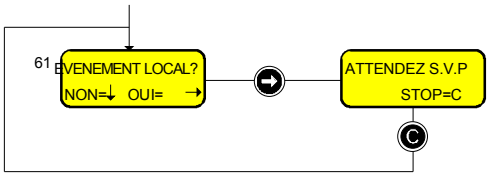
Un badge avec un niveau de priorité supérieur à 0 est appelé Badge de Programmation et peut avoir accès à certains menus. Dans le *Panorama des Menus Chapitre 4.3* est indiqué sur chaque menu la priorité (Px) minimum nécessaire pour accéder à ce menu.

4.9 Sous-Menu 6 - Impressions

Une sortie imprimante de l'historique des événements locaux, des alarmes globales, des Groupes de Personnel et de la programmation complète peut être demandée par la priorité Maintenance (quand le mode Maintenance est autorisé) et par le plus haut niveau de priorité utilisateur.

Si l'imprimante du système d'Intrusion est utilisée les lignes ayant trait au Contrôle d'Accès seront précédées de la lettre "A" pour préciser qu'il s'agit de transactions ayant trait au Contrôle d'Accès.

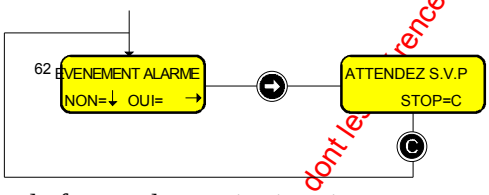
Menu 61 : Historique Local



Voir *Menu 31* pour explication sur le format des sorties imprimante.

Par appui sur la touche C, la sortie imprimante sera interrompue.

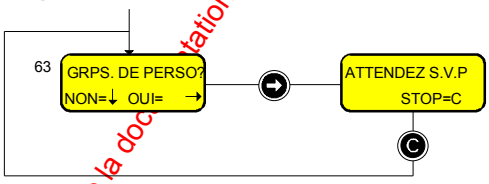
Menu 62 : Historique des Alarmes



Voir *Menu 32* pour explication sur le format des sorties imprimante.

Par appui sur la touche C, la sortie imprimante sera interrompue.

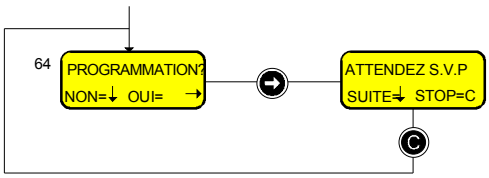
Menu 63 : Liste des Badges



Tous les badges programmés seront triés et imprimés après les N° de Groupe de Personnel. En premier tous les badges relatifs au groupe N°1 ensuite les badges relatifs au groupe N°2 etc.

Par appui sur la touche C, la sortie imprimante sera interrompue.

Menu 64 : Programmation



Si aucune action n'est faite suite à l'appel de ce Menu, il est quitté automatiquement au bout de 10s et l'impression est lancée en tâche de fond.

L'appui sur la touche ↓ permet de passer à la programmation suivante de façon à obtenir l'impression des parties utiles de la programmation seulement.

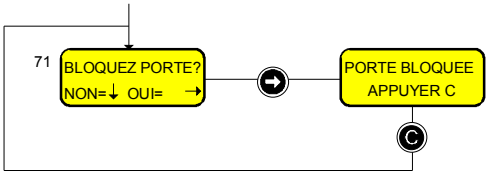
L'appui sur la touche C provoque l'interruption de l'impression.

Les touches C et ↓ peuvent être réutilisées avec les fonctions précédentes en cours d'impression en redemandant le *Menu 64* à nouveau, le fait de redemander le *Menu 64* en cours d'impression ne relance pas une impression mais permet l'accès à ces deux touches.

4.10 Sous-Menu 7 - Contrôle Manuel de Porte

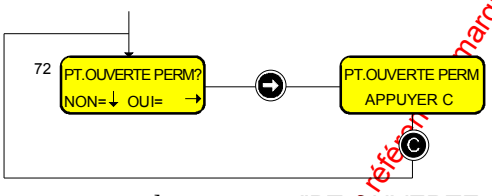
Avec un badge Maintenance (quand le mode Maintenance est autorisé) ou avec un badge de programmation ayant un niveau de priorité élevé, il est possible d'outrepasser les fonctions de contrôle automatique de la porte.

Menu 71 : Blocage de la Porte



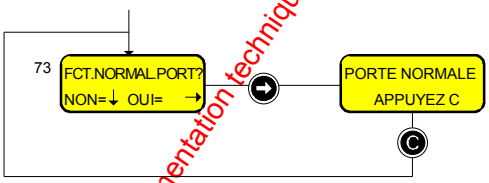
Quand la porte est bloquée en permanence, le message "PORTE BLOQUEE" sera affiché comme un message de défaut à toute personne qui essayera de réaliser un franchissement normal de la porte.

Menu 72 : Ouverture Permanente de la Porte



Quand la porte est ouverte en permanence, le message "PT.OUVERTE PERM." sera affiché comme un message de défaut à toute personne qui essayera de réaliser un passage normal de la porte.

Menu 73 : Contrôle Normal de la Porte



Après l'usage des *Menus 71* et *72*, il est nécessaire d'utiliser le *Menu 73* pour revenir au contrôle normal de la porte.

4.11 Sous-Menu 8 - Configuration du Système

Le badge de Maintenance possède des priorités spéciales de programmation, lesquelles permettent la réalisation de la configuration du système comme les temporisations de porte, la définition des entrées (type logiciel), la définition des sorties (type logiciel), et la copie de la base de données d'un lecteur vers un autre. Les menus de configurations peuvent seulement être utilisés quand le mode Maintenance est autorisé par l'Utilisateur.

Menu 82 : Initialisation du Lecteur

La procédure d'initialisation dépendra du fait que l'on fonctionne en configuration système Autonome ou intégré à l'Intrusion HISEC.

1. Choisir le menu Initialisation. Les codes Distributeur et Installateur seront enregistrés à la lecture du badge Maintenance durant l'entrée en session au Menu Contrôle d'Accès. L'afficheur demandera les Options du lecteur Le Mode de fonctionnement et le format des Badges (BFORM).
2. Entrer et les diverses **Options** désirées, le **Mode**, le **BFORM**.

   2a. Configuration en mode Autonome ou multilecteurs : L'afficheur demande alors le Code Client.

   2b. Configuration système intégré à HISEC INTRUSION : L'afficheur demandera la lecture du badge Maître.
3. Entrer le Code Client ou lire le badge Maître

   Le code Distributeur du badge Maintenance et le code Client seront programmés dans le lecteur et la base de donnée sera remise à zéro, si la touche ➔ est appuyée. Le code Distributeur et le code du badge Maintenance sont comparés et s'ils sont différents, le badge sera refusé.

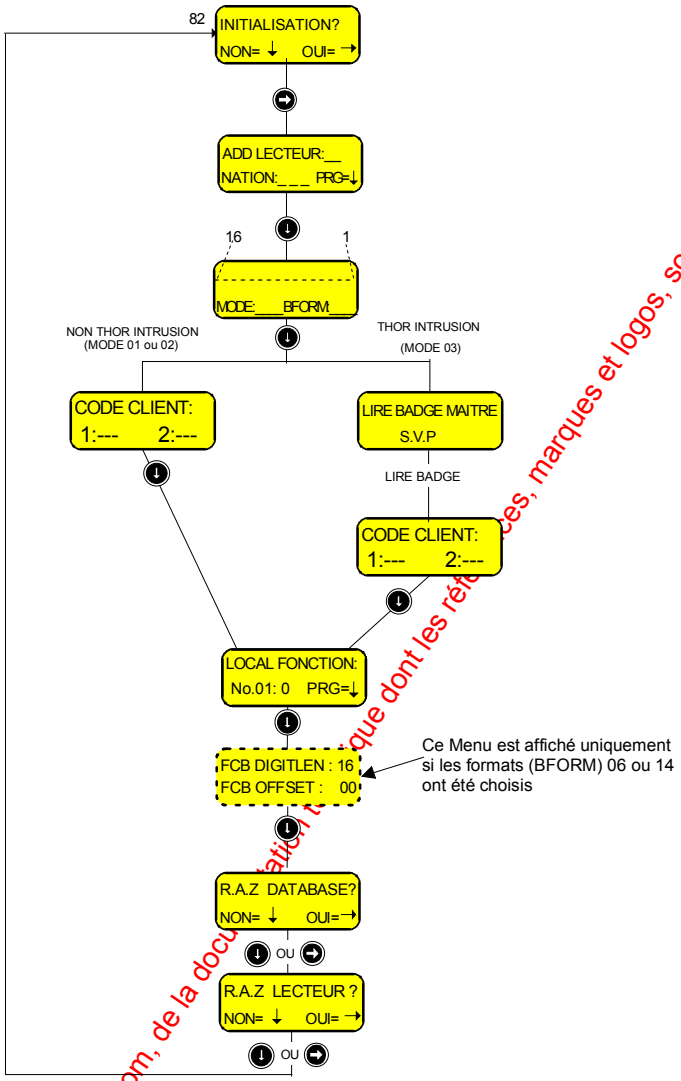
La procédure d'initialisation, décrite ci-dessus, peut être représentée par le diagramme suivant :

Ü L'adresse du lecteur

L'adresse du lecteur doit être programmée à une valeur comprise entre 00 et 31.

Ü La Langue

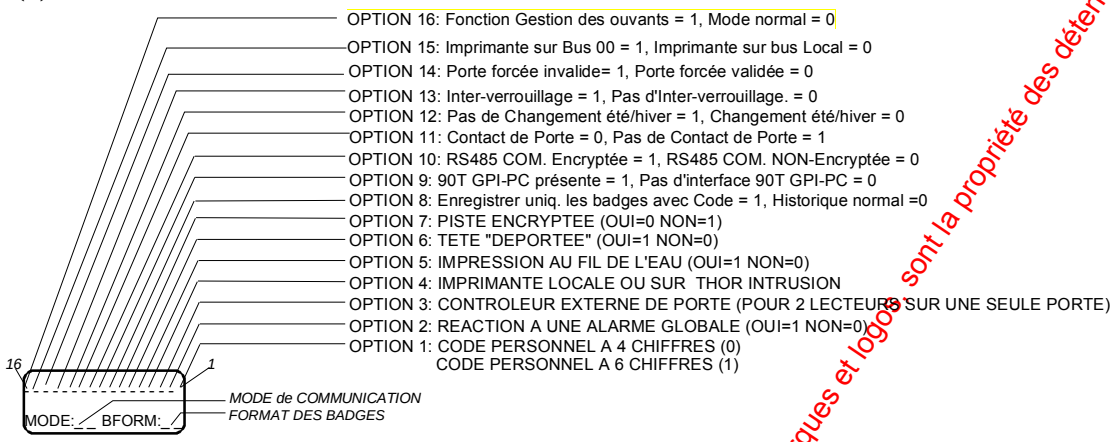
Le lecteur supporte les différentes langues du contrôle d'accès HI SEC. Le choix se fera directement en entrant l'indicatif téléphonique international.



PAYS	*Code*
Netherland	031
France	033
Spain	034
Italy	039
England	044
Denmark	045
Sweden	046
Norway	047
Poland	048
Germany	049

Ü Les Options

Les 16 paramètres de la liste des OPTIONS représentent chacun une option qui peut être sélectionnée (1) ou non (0), elles sont les suivantes :



- Option 1: Code Personnel à 4 ou 6 chiffres peut être choisi.
  - 0 = 4 chiffres
  - 1 = 6 chiffres
- Option 2: Le type de réaction Locale ou Globale peut être choisi.
  - 0 = Réaction Locale
  - 1 = Réaction Globale
- Option 3: Contrôleur externe à la porte. Deux lecteurs sont utilisés pour gérer une seule porte
  - 0 = Contrôleur local de la porte
  - 1 = Contrôleur externe à la porte.
- Option 4: Imprimante Accès ou sur le système intrusion HISEC.
  - 0 = Imprimante Accès
  - 1 = Imprimante système intrusion HISEC
- Option 5: L'imprimante peut imprimer à la demande ou en temps réel (fil de l'eau).
  - 0 = Impression à la demande
  - 1 = Impression au fil de l'eau
- Option 6: Lecteur avec tête de lecture déportée ou standard:
  - 0 = Lecteur classique (tête de lecture incorporée au lecteur)
  - 1 = Lecteur tête de lecture déportée.
- Option 7: Utilisation de badges non encryptés.
  - 0 = Badges Encryptés (HiSec).
  - 1 = Badges Non Encryptés.
- Option 8: Enregistrement Badge + Code seul.
  - 0 = Enregistrement normal.
  - 1 = Seul les badges ayant nécessité un code sont enregistrés dans l'historique..
- Option 9: Exploitation du contrôle d'accès par logiciel PC (AMS ou AIMS).
  - 0 = Pas d'interface 90T GPI PC présente sur le bus RS 485.
  - 1 = Interface 90T GPI PC présente sur le bus RS 485.
- Option 10: Encryptage des communications sur le bus RS 485.
  - 0 = Communication non-encryptée (mode standard).
  - 1 = Communication encryptée.
- Option 11: Prise en compte des transactions.
  - 0 = Enregistrement après ouverture de la porte (contact de position obligatoire).
  - 1 = Enregistrement après lecture du badge (porte avec ou sans contact de position).

¤ Option 12: Changement automatique Heure d'été/hiver.

0 = Changement automatique (mode standard).
1 = Pas de Changement automatique.

¤ Option 13: Activation du mode inter-verrouillage.

0 = Pas d'activation du mode inter-verrouillage (mode standard).
1 = Activation du mode inter-verrouillage (sas par ex.)

¤ Option 14: Gestion des portes forcées.

0 = Porte forcée valide (mode standard).
1 = Porte forcée invalide.

¤ Option 15: Emplacement de l'Imprimante fil de l'eau.

0 = Imprimante fil de l'eau sur bus local (mode standard).
1 = Imprimante fil de l'eau sur bus principal

¤ Option 16: Validation de la fonction Gestion des ouvrants.

0 = Lecteur en mode standard.
1 = Lecteur avec des fonctions Gestion des ouvrants, le lecteur garde ses fonctions contrôle d'accès et intrusion (si existantes).

La Notice du lecteur fonctionnant en gestion de ouvrants est disponible sous forme d'un document séparé "Gestion des Ouvrants" réf. 18-006-09F.

Pour de plus amples détails sur toutes les options précédentes se reporter au *Chapitre 1.7.5*.

Ü Le Mode de fonctionnement

Les 3 Modes disponibles sont les suivants :

Mode 00: Lecteur non initialisé
Mode 01: Lecteur en mode Autonome
Mode 02: Système Multi-lecteurs
Mode 03: Lecteur intégré à HISEC Intrusion

Remarque: Les Modes 02 et 03 peuvent cohabiter sur la même installation, cela permet de définir des lecteurs n'ayant pas le droit à l'intrusion et d'autres oui. Par ex. Pour des lecteurs placés à l'extérieur.

Ü Le Format des Badges

Il est nécessaire de sélectionner le format des badges (dans le cas de badges standard HISEC, le lecteur reconnaîtra automatiquement le format).

Dans le cas d'un format spécial, on devra obligatoirement entrer ce format (par défaut le lecteur sera dans le format du badge ayant servi à l'initialisation).

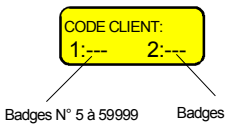
Les formats suivants sont disponibles :

00	**Lecteur non-initialisé**
01	Format magnétique encrypté HISEC
02	Format Wiegand HISEC
03	Format proximité COTAG/DEISTER -HISEC
04	Format proximité HUGES-HISEC
05	Format magnétique non-encrypté HISEC
06	Format programmable Libre ISO Code BCD 16 digits max.
07	Format magnétique BCD spécial LOREAL.
08	Format proximité DEISTER – HISEC (PC 114)
09	Format magnétique BCD spécial La CHARTE
10	Format magnétique BCD spécial ville de STRASBOURG
11	Format magnétique BCD spécial TELEMECANIQUE (ancien)
12	Format magnétique BCD spécial TELEMECANIQUE (nouveau)
13	Format magnétique BCD spécial (NCS)
14	Format programmable Libre Bit 64 bits max.
15	Format Wiegand 26 bits, N° de badge au début (NCS)
16	Format Wiegand 26 bits, N° Installateur au début (ID Solutions)
17	Format Cotag spécial
18	Format Wiegand 26 bits, avec code site + 128 (Format 15)
19	Format spécial AIRTEL
20	Format Wiegand 32 bits pour badges 1040 Westhinghouse
21	Format CardKey HID
22	Format spécial wiegand Kredit Bank
23	Format spécial magnétique Aéroport de Copenhague
24	Format magnétique encrypté HISEC avec N° de Version

Important: les formats libres 6 (format BCD) et 14 (format Bits) limitent à **4000** le nombre de badges possible sur le système (contre 16000 dans les autres formats).

Ü Le Code Site

A l'initialisation du lecteur il est possible d'entrer deux codes sites différents



Le code site N°1 est automatiquement pris dans le badge maître si le système est intégré à l'intrusion (mode 03), dans les autres cas il devra être entré à la main de la même façon que le 2° code site.

Quand on initialise le lecteur avec un badge Maître, le code site N° 1 est automatiquement pris dans le badge maître et ne peut pas être édité, seul le code site N°2 pourra être programmé.

Les badges compris entre 5 et 59999 devront avoir le code site N°1 et les badges compris entre 60000 et 65500 seront acceptés avec le Code site N°2. De cette façon, les badges compris entre 60000 et 65500 avec le code site N°1 seront refusés. Différents sites, avec différents codes sites, pourront utiliser des badges locaux (entre 5 et 60000 chacun) et avoir un 2ème code site général (badges globaux entre 60000 et 65500) pour toutes les installations, les badges seront communs à toutes les installations (si programmés bien sûr).

Prière de noter que:

- Le badge maître devra avoir le code site N°1, de la même façon le logiciel AIMS devra avoir le code site N°1.
- Les 2 codes sites devront avoir obligatoirement le même code distributeur et le même code installateur qui seront ceux du badge de maintenance (service).

Ü Le format libre (BFORM 06 & 14)

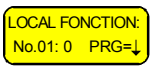
Si le format 6 ou 14 à été sélectionné un nouvel écran permet de définir le nombre de caractères (**DIGIT LENGTH**) en format magnétique (**BFORM=6**) ou le nombre de bits en format wiegand (**BFORM=14**) à lire ainsi que la position du premier caractère (bit) à lire (**OFFSET**). Les autres formats ne permettent pas d'accéder à ce menu.

DIGIT LENGTH : correspond à la ligne `DigitLen=XX` de AIMS.Ini
OFFSET : correspond à la ligne `First Format position=xx` de AIMS.INI

Prière de noter que la ligne : `Default Format=xxxxxxxxxxxxxxxx` du fichier AIMS.INI ne peut pas être paramètrée sur le lecteur.

Ü Les Fonctions Locales

Les 9 paramètres de la liste des FONCTIONS LOCALES représentent chacun une option qui peut être sélectionnée (1) ou non (0), elles sont les suivantes :



= Option suivante

La liste suivante rappelle toutes les fonctions locales existantes à partir de la version 114.0202.

- **Fonction Locale 1:** Désactivation du code personnel par défaut (1111xx).

  0: l'utilisation du code personnel par défaut 1111(11) suivi de l'entrée de son ancien code permet au porteur du badge de changer son code personnel (valeur par défaut).

  1: Le code personnel par défaut 1111(11) ne peut pas être utilisé sur ce lecteur. Le code personnel du porteur du badge pourra être changé sur un autre lecteur.

- **Fonction Locale 2:** Porte maintenue en gestion des ouvrants comme Sabotage.

  0: L'ouverture de la porte coffre sera transmise à la centrale intrusion dans l'adresse correspondante à chaque fois que la porte sera ouverte. (valeur par défaut).

  1: : Le maintien ouvert de la porte coffre après la temporisation max. d'ouverture sera transmis à la centrale intrusion dans l'adresse correspondante à la fin de la période d'ouverture comme un sabotage.

- **Fonction Locale 3:** Fonction « Simple Parking ».

  0: Les lecteurs de la zone du Parking vérifieront l'état d'Anti-retour pour chaque badge lu sur le lecteur (valeur par défaut)..

  1: Les lecteurs de la zone du Parking ne vérifieront pas l'état l'Anti-retour pour une badge lu sur ce lecteur. Cela veut dire que la zone de comptage sera augmenté ou sera diminué chaque fois qu'un badge sera lu sur le lecteur possédant cette option.

- **Fonction Locale 4:** "Badge invalide" avec fin de tempo. forcée.

  0 : Le type logiciel de sortie 74 – Badge refusé – sera remis à zéro à la lecture du prochain badge valide; ou par la fin d'activation d'une horloge. **La sortie ne sera pas réactivée avant la lecture d'un badge valide même si l'horloge à remis la sortie au repos.**

  1: Le type logiciel de sortie 74 – Badge refusé – sera remis à zéro à la lecture du prochain badge valide ; ou par la fin d'activation d'une horloge. **La sortie pourra être réactivée sans l'attente de la lecture d'un badge valide.**

- **Fonction Locale 5:** "Configuration transmission".

  0: Pas de transmission des événements du lecteur.

  1: Tous les événements du lecteur (par ex. les événements portes forcées) seront transmis à l'interface GPI modem (hors com.) ou interface « Host ».

  Cette fonction ne sera utilisable qu'à partir de la version d'EPROM 5.04 de la carte GPI COM.

- **Fonction Locale 6:** Fonction gestion des ouvrants (Obturateur de serrure)

  Voir Note de Service 006-061.

- **Fonction Locale 7:** Utilisation du frontal vidéo HISEC placé sur le bus principal (00).

  0: Le lecteur placé sur un sous bus n'enverra pas les événements au frontal de gestion de vidéo HISEC placé sur le bus principal.

  1: Le lecteur placé sur un sous bus enverra tous les événements au frontal de gestion de vidéo HISEC placé sur le bus principal.

- **Fonction Locale 8:** Temps minimum entre lecture du badge.

  0: Mode de fonctionnement normal, le badge peut ouvrir la porte autant de fois et avec la fréquence qu'il veut.

  1: Le badge est bloqué après l'ouverture de porte pour une durée programmable. Cette fonction permet de fixer un temps minimum entre deux utilisations du même badge sur la même porte.

  Cette option se valide dans chaque lecteur, la durée se programme au moyen d'AICS V 6.03 ou sup. au moyen du menu Service – Onglet Setup – Paramètre « Card Block Timer » = valeur comprise entre 0 et 250 mn, elle peut être différente sur chaque lecteur.

- **Fonction Locale 9:** Pas de lecture de badge avant re-fermeture de la porte.

  0: Mode de fonctionnement normal, pendant l'ouverture normale de la porte suite à la lecture d'un premier badge, les badges suivants entre dans la même transaction.

  1: La lecture d'un premier badge ouvre la porte et bloque la lecture de tous les badges tant que la porte n'a pas été fermée.

  Cette fonction permet de s'assurer de l'unité de passage et de gérer plus efficacement les tourniquets ou équivalents.

- **Fonction Locale 10:** Blocage du terminal en cas d'utilisation d'un code personnel erroné.

  0: Mode de fonctionnement normal, l'entrée d'un mauvais code personnel associée au badge provoque le blocage du badge au bout de 10 tentatives infructueuses par contre le lecteur continue d'avoir son mode de fonctionnement classique (clavier et afficheur actif, etc.).

  1: l'entrée d'un mauvais code personnel associée au badge provoque le blocage du badge au bout de 10 tentatives infructueuses et bloque l'utilisation du terminal pendant une durée programmable au moyen d'AICS V 6.03 ou sup. au moyen du menu Service – Onglet Options – Paramètre « Panel Block Timer » = valeur comprise entre 0 et 250 mn, elle peut être différente sur chaque lecteur.

- **Fonction Locale 11:** Code contrainte programmable librement.

  0: Le code Contrainte est le code personnel du Badges +1.

  1: Le code Contrainte peut être programmé a une valeur libre.

- **Fonction Locale 12:** Suppression du buzzer interne du lecteur.

  0: Mode de fonctionnement normal, le buzzer est activé sur n'importe quelle alarme du lecteur.

  1: Le buzzer du lecteur est bloqué pour toute alarme, par contre il est actif pour le bip des touches du clavier.

- **Fonction Locale 13:** Désactivation de l'inter-verrouillage en fonction gestion des ouvrants.

  0: Mode de fonctionnement normal, il n'est possible de commander l'ouverture d'un seul ouvrant à la fois.

  1: L'inter-verrouillage est inhibé, de cette façon il est possible de lancer l'ouverture de plusieurs ouvrants dans la même période.

- **Fonction Locale 14:** Blocage du bouton poussoir de sortie en cas de porte Bloquée.

  0: Mode de fonctionnement normal, il est possible d'utiliser le bouton poussoir de sortie en cas de porte bloquée.

  1: L'utilisation du bouton poussoir de sortie est impossible en cas de porte Bloquée.

- **Fonction Locale 15:** Validation du lecteur avec la fonction AIR (Accès Image Reconnaissance).

  0: Mode de fonctionnement normal, le lecteur ouvre la porte après vérification du badge.

  1: Le lecteur n'ouvre pas directement la porte, mais attends un ordre de l'opérateur sur AIMS pour ouvrir la porte.

  Le mode 01 active le fonctionnement de AIR pour tous les badges.

  Il est possible d'utiliser le mode 0 pour fonctionner avec AIR dans ce cas, il est nécessaire de créer des programmes Hebdomadaires avec la fonction AIR et de les attribuer directement aux groupes de personnel qui doivent fonctionner en mode Air (voir chapitre 1.7.3).

- **Fonction Locale 16:** Envoi des événements vers GPI Host sur bus principal (00).

  0: Mode de fonctionnement normal, les événements du lecteur sont envoyés à la GPI Host placée sur le bus principal (BUS 00).

  1:. les événements du lecteur ne sont pas envoyés à la GPI Host placée sur le bus principal (BUS 00).

- **Fonction Locale 17:** Envoi des événements vers GPI Host sur son propre Bus (sous Bus).

  0: Mode de fonctionnement normal, les événements du lecteur sont envoyés à la GPI Host placée sur le même bus que le lecteur.

  1:. , les événements du lecteur ne sont pas envoyés à la GPI Host placée sur le même bus que le lecteur.

- **Fonction Locale 18:** Lecture de badge avec Beep.

  0: Mode de fonctionnement normal, la lecture du badge n'active aucun indicateur sonore en cas d'acceptation de la transaction.

  1: L'acceptation du badge est indiquée par un double beep.

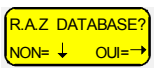
- **Fonction Locale 19:** Acceptation de tous les badges magnétiques possédant une piste ISO.

  0: Mode de fonctionnement normal, seul les badges avec le format de badges décidé a l'initialisation et par la programmation sont acceptés.

  1:. **:** Tous les badges magnétiques possédant une piste ISO peuvent ouvrir la porte.

Ü Remise à zéro (initialisation) de la base de données

Avant de quitter le Menu 82 du lecteur il est maintenant possible d'effectuer une remise à zéro de la base de données du lecteur, cela permet de vider la programmation erronée éventuelle et de recréer les valeurs par défaut (S-art à l'adresse 00, équation 99, etc.).

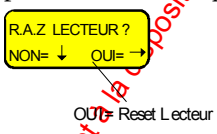


Attention ! A la première initialisation, la base de données devra obligatoirement être remise à zéro !!!

Nota: toute la programmation est perdue par cette action.

Ü Remise à zéro (initialisation) du lecteur

Avant de quitter le Menu 82 du lecteur il est maintenant possible d'effectuer un reset du lecteur, cela permet de faire repartir le lecteur (de la même façon qu'une coupure d'alimentation).



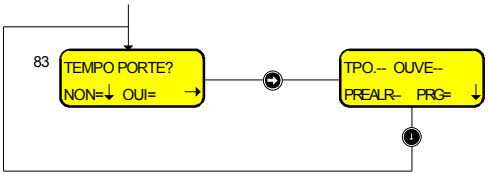
Attention: nous rappelons que cette opération est obligatoire pour le lecteur 00 pour faire fonctionner la communication du bus RS 485 (cette opération était auparavant réalisée en coupant l'alimentation).
Nota: aucune programmation n'est perdue par cette action.

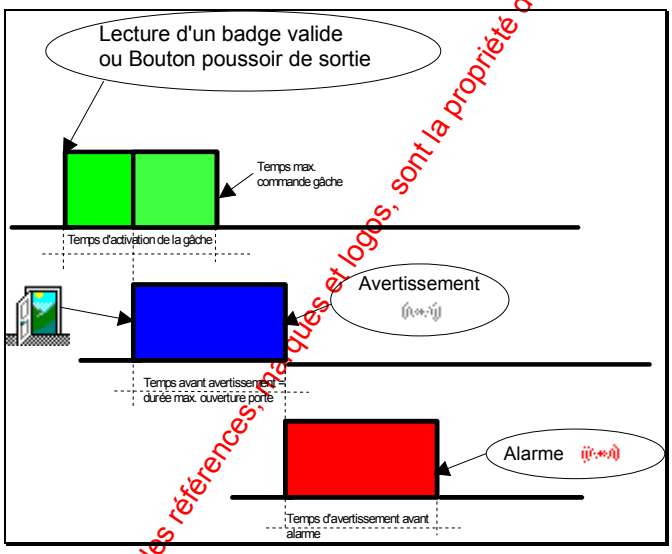
Remarque: Les **Options**, **Modes, Bform, etc.** seront à définir pour **Chaque Lecteur**.

Menu 83 : Configuration des Temporisations de porte

Les temporisations pouvant être utilisées pour le lecteur contrôlant la porte sont les suivantes :

Temporisation de libération de gâche ..... = TPO
Temporisation d'ouverture de porte avant avertissement.. = OUV.
Tempo d'avertissement avant alarme porte maintenue ..... = PREALR.





Toutes ces temporisations sont entrées en chiffre par pas de 10 secondes et chaque temporisation peut être ajustée de 0 à 990 sec. La touche ⓓ enregistrera la temporisation saisie et reviendra au *Menu 83*.

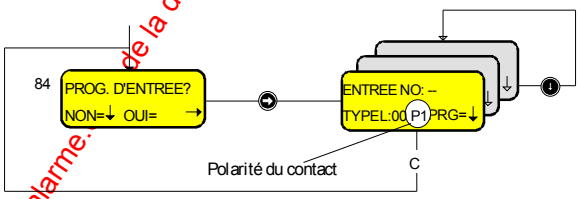
Menu 84 : Programmation des Entrées

Chaque adresse de S-ART peut être programmée avec 2 types logiciels d'entrée.

Après initialisation, toutes les entrées et toutes les sorties sont programmées avec le type logiciel 0 (pas de fonction).

Les relations entre les adresses des S-ART et les numéros d'entrées/sorties sont les suivantes :

N° d'entrée/sortie = 2x adresse du S-ART + n° entrée/sortie du S-ART (0 ou 1)



Quand ce menu est appelé, l'entrée N° 00 est affichée et un nouveau nombre peut être entré si nécessaire. Ensuite, le type logiciel d'entrée "TYPEL:" correspondant est frappé (voir la lister au *Chapitre 1.4.2*) suivi par la touche ⓓ.

Il est possible de choisir le type de contact utilisé (Px) pour chaque entrée de S-art (contact NO ou NF)

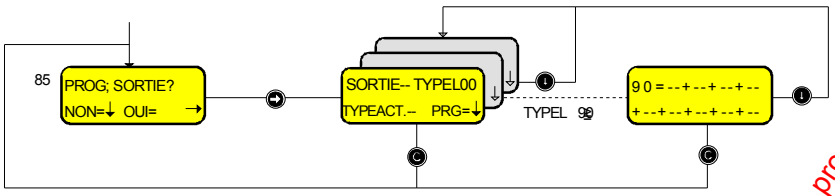
1 = Contact Normalement Fermé (NF) [valeur par défaut]

0 = Contact Normalement Ouvert (NO)

Ensuite, la prochaine adresse peut être entrée. Le menu est quitté par l'appui sur la touche ⓒ.

Menu 85 : Programmation des Sorties

Pour chaque sortie de S-ART, deux paramètres doivent êtres attribués, type logiciel de sortie et type d'activation (prière de se référer au *Chapitre 1.5.2* pour la liste des types logiciel de sortie).



Quand ce menu est appelé, la sortie N°00 est affichée et un nouveau numéro peut être entré si nécessaire. Après cela, le type logiciel de sortie correspondant et le type d'activation seront entrés et suivis de la touche ↓. Si le type logiciel de sortie est compris entre 90 et 99, un affichage supplémentaire apparaîtra où il sera possible de programmer une équation de sortie (SI/ALORS). Le numéro du type logiciel de sortie sera affiché en même temps que les champs pour 9 différents types logiciels d'entrées.

La fonction ET sera réalisée par la touche 2 et sera représentée par "*".
La fonction OU sera réalisée par la touche 0 et sera représentée par "+".

Le menu est quitté par appui sur la touche C.

Pour le calcul du numéro de sortie, se référer au *Menu 84*. Pour le S-ART type 90T-S102 seule la sortie SOR1(OUT1) est utilisable.

Programmation par défaut des équations vers l'intrusion

Le type logiciel 99 (équation vers intrusion) est pré-programmé à l'adresse 00 après l'initialisation du lecteur. L'équation SI/ALORS définie en type logiciel 99 spécifie la condition qui sera envoyée à HISEC Intrusion à l'adresse réservée pour chaque lecteur (adresse intrusion de 31 à 61).

L'équation pré-programée dans les lecteurs est donc la suivante: **99 = 70 + 71**

70 = porte forcée & 71 = Porte maintenue

L'équation donne la possibilité de définir le contact de porte du contrôle d'accès dans le système intrusion comme un détecteur en mode de surveillance 24H ou comme un détecteur classique pouvant être arme et désarmé avec la zone dans laquelle il se trouve.

L'ouverture normale de la porte au moyen d'un badge ou du bouton poussoir de sortie, n'activera pas l'entrée intrusion et seules les portes forcées et les portes maintenues activeront l'entrée intrusion.

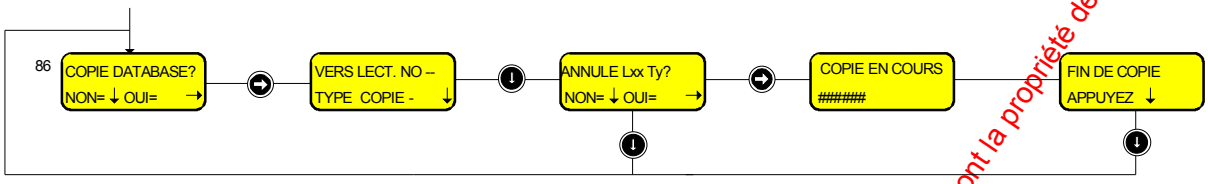
Attention : avec ce mode de fonctionnement il est impératif de ne pas utiliser l'option 14 !!! (voir chapitre précédent), au cas contraire il sera nécessaire de modifier l'équation en 99 = 30 (30= contact de porte).

La programmation par défaut de l'adresse 00 pourra de toute façon être modifiée au besoin.

Ne pas oublier que l'entrée correspondante (adresse 31 à 61) dans le système intrusion devra être programmée avec un type logiciel adéquat et une zone pour pouvoir fonctionner correctement.

Menu 86 : Copie de la Base de Données (Database)

Pour réaliser la programmation d'un système comprenant plusieurs lecteurs (Multi-lecteurs ou Intégration), il est plus facile, dans la mesure du possible, de copier la base de données locale d'un lecteur vers un autre. Il est aussi possible de copier la base de données globale à partir d'un lecteur vers un autre en cas de défaut de la base de données durant la Maintenance.



Type de copie = **0** pour la partie **Locale** de la base de données
Type de copie = **1** pour la partie **Globale** de la base de données

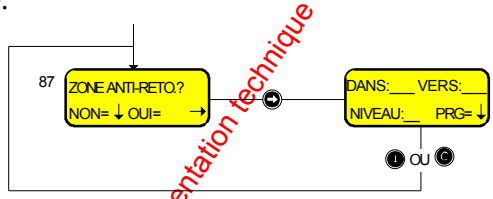
Prière de remarquer que la base de données existante dans le lecteur de destination sera effacée quand la fonction de copie sera utilisée.

Pendant le temps de copie, une ligne apparaît à l'écran indiquant l'avancement de la copie par une petite barre.

La copie de la partie globale n'est pas utile si tous lecteurs sont présents au moment de la programmation, mais est seulement utile si l'on ajoute un lecteur sur l'installation ou au remplacement d'un lecteur.

Menu 87 : Définition des zones d'anti-retour

Toutes les fonctions d'anti-retour sont programmées au moyen du *Menu 87* par le badge Maintenance. Le numéro de la zone pour DANS et VERS doivent être programmées avec 3 chiffres, le NIVEAU de contrôle ayant lui un seul chiffre.



Toutes les données programmées au moyen du *Menu 87* sont mémorisées dans la base de données locale et doivent donc être programmées dans chaque lecteur.

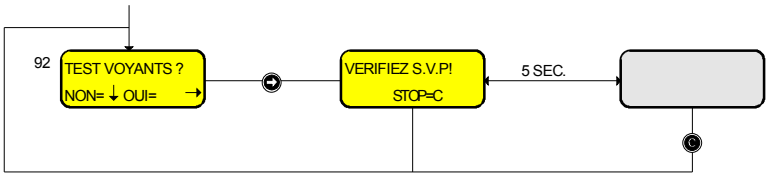
Le niveau de contrôle de zone (NIVEAU) peut être programmé avec 4 différentes valeurs comprises entre 0 et 3, qui peuvent être :

- 0: Pas de limites au contrôle de l'anti-retour. Le contrôle démarre à la première lecture du badge et est automatiquement lancé.
- 1: Le contrôle de l'anti-retour est effacé chaque jour à minuit (24:00) et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 2: Le contrôle de l'anti-retour est effacé chaque heure et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 3: Pas de contrôle de l'anti-retour par zone. Tous les badges pourront être utilisés en ignorant les conflits de zones possibles.

4.12 Sous-menu 9 - Test du Système

Le badge de Maintenance a accès aux fonctions de test par ex. test des entrées/sorties des S-ART et test des mémoires.

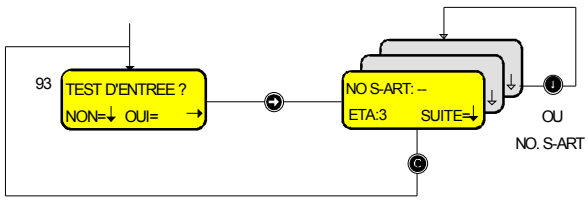
Menu 92 : Test des Voyants



Les 4 voyants indicateurs clignotent à intervalle d'une seconde et l'afficheur alterne entre deux écrans, le premier en texte pour permettre l'arrêt du test et un écran où tous les segments sont noircis ceci à intervalle de 5 secondes.

Par l'action sur la touche C, le test est stoppé et un retour au *Menu 92* est effectué.

Menu 93 : Test des Entrées de S-ART



Quand une adresse à 2 chiffres est entrée, l'entrée est transférée vers un programme de test d'état. Durant ce test, une réaction normale à une alarme est bloquée, au lieu de cela, une "condition d'alarme" est indiquée par l'excitation du "buzzer" interne pendant 1 seconde. Toutes les activations d'entrées pourront être répétées et seront enregistrées dans l'historique des événements.

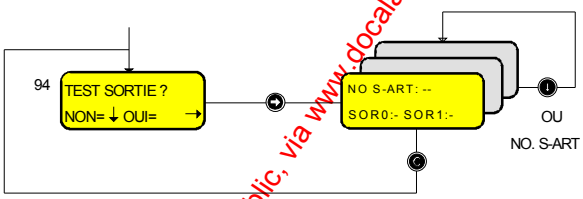
Les états des entrées des S-ART - affichés et rafraîchis toutes les 5 secondes - sont :

Ÿ ETA:0 : ENT0=0,ENT1=0 (repos)
Ÿ ETA:1 : ENT0=1,ENT1=0 (alarme 1)
Ÿ ETA:2 : ENT0=0,ENT1=1 (alarme 2)
Ÿ ETA:3 : ENT0=1,ENT1=1 (alarme 1 & 2)
Ÿ ETA:4 : pas de communication
Ÿ ETA:5 : erreur de parité

Une commande de sélection d'une autre adresse se fera en réécrivant le numéro de la nouvelle entrée ou par appui sur la touche (prochain numéro). La durée du test est illimitée, mais elle peut être stoppée par appui sur la touche C et dans ce cas, le *Menu 93* apparaît de nouveau.

Menu 94 : Test des Sorties de S-ART

Il est possible de mettre à un ou à zéro les deux sorties du S-ART par cette fonction à des fins de test. Cette commande "écriture" sera réécrite sur la condition de sortie existante.

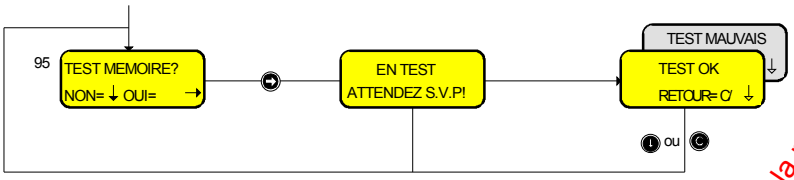


Par l'entrée du N° de S-ART et de la valeur pour les 2 sorties SOR0(OUT0) et SOR1(OUT1), les sorties seront activées selon correspondance (1 = mise à 1 et 0 = mise à 0).

La durée de test n'est pas limitée, mais elle peut être stoppée par l'appui sur la touche C, dans ce cas, le *Menu 94* apparaît à nouveau. Une commande de sélection d'un autre N° de S-ART se fera simplement en réécrivant par-dessus l'ancien la nouvelle adresse ou par l'appui sur la touche pour le prochain numéro. Après cela, les nouvelles valeurs pour SOR0(OUT0) et SOR1(OUT1) devront être entrées.

Menu 95 : Test des Mémoires

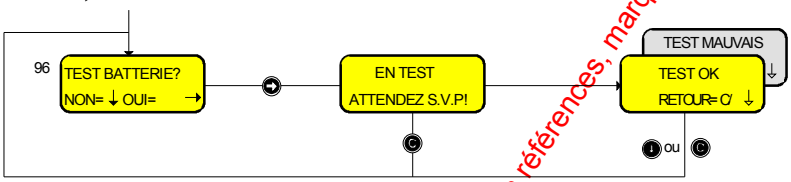
Par le *Menu 95*, il est possible de faire une vérification complète de la mémoire du logiciel pour savoir si le lecteur est "OK" ou défectueux. Ce test est valable seulement pour le lecteur d'où il est appelé (test local).



Après le test, un retour au *Menu 95* est effectué par appui sur l'une des touches ↓ ou C.

Menu 96 : Test Batterie

Par le *Menu 96*, il est possible de vérifier les batteries. Tous les S-ART définis comme type logiciel de sortie pour le test batterie seront excités pendant 15 secondes. Le test est valable seulement pour le lecteur d'où il est appelé (test local).

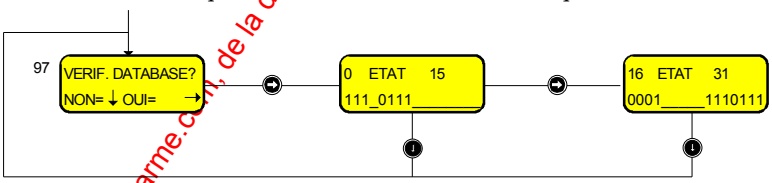


Après ce test, le résultat sera affiché et l'on reviendra au *Menu 96* par appui sur les touches ↓ ou C. Un défaut batterie activera le voyant indicateur "défaut" pendant toute la durée où le défaut existera et le type logiciel de sortie correspondant. Un nouveau test avec "BATTERIE OK" remettra à zéro la condition de défaut.

Ce menu de test peut seulement être appelé si une sortie "test batterie" existe dans la programmation du lecteur.

Menu 97 : Vérification de la Base de Données (Database)

Cette fonction est utilisée pour vérifier que les bases de données globales sont les mêmes dans tous les lecteurs. Elle permet aussi de vérifier que tous les lecteurs communiquent bien.



Ce test affiche un écran vous donnant une vue générale d'un maximum de 16 lecteurs avec le lecteur 0 à gauche et le lecteur 15 à droite.

La touche → permet d'afficher les autres lecteurs (adresses comprises entre 16 et 31).

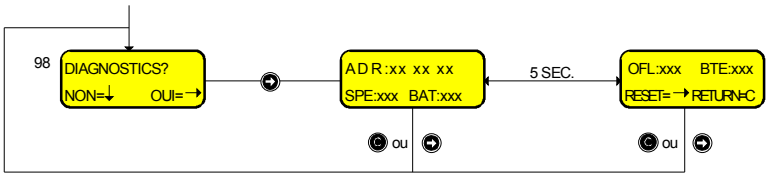
Les codes utilisés sont les suivants :

0 = Base de données différente de celle du lecteur à partir duquel le test a été lancé
1 = Base de données identique
- = Pas de réponse du lecteur

Nota: ce menu n'affiche que les lecteurs contrôle d'accès (centrale intrusion, interfaces, etc. ne sont pas visibles).

Menu 98 : Diagnostics

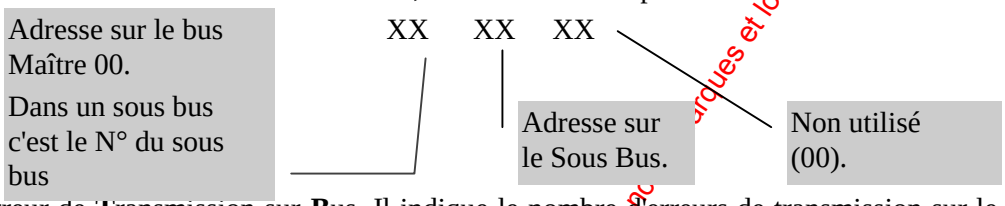
Ce menu permet de connaître directement l'adresse du lecteur (codée sur la carte du lecteur -micro-interrupteur 1- pour le lecteur 90T) et de surveiller les problèmes de communications sur les bus RS 485 et S-ART.



Deux affichages sont proposés à l'appel du menu, la commutation automatique entre ces deux affichages aura lieu toutes les 5 secondes.

Ces deux menus donnent au technicien de maintenance un certain nombre d'informations sur les divers problèmes de communications sur les bus RS 485 et S-ART.

ADR **: Adr**esse du lecteur sur le bus RS 485, codée sur la carte processeur elle même.



ETB **: E**rreur de **T**ransmission sur **B**us. Il indique le nombre d'erreurs de transmission sur le bus RS 485 depuis la dernière r.a.z des compteurs.

EPS **: E**rreur de **P**arité **S**-ART. Il indique le nombre d'erreurs de transmission qui ont eut lieu sur le bus -local- S-ART depuis la dernière r.a.z des compteurs.

ABH **: A**pplication **B**us **H**ors-temps. Il indique le nombre d'absences de réponses dans un délai donné (20 secondes) entre une unité et une autre.

DEC **: Déc**onnexion d'une unité. La fonction de ce compteur dépend si le lecteur est Maître (Adresse = 0) ou Esclave (Adresse > 0).

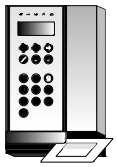
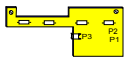
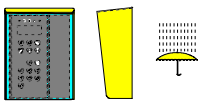
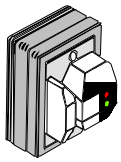
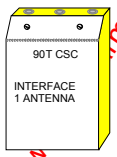
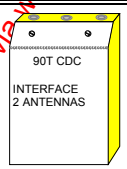
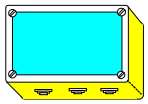
- **Maître:** Le compteur donne le nombre de fois qu'une unité (**n'importe laquelle**) a eut des problèmes de communication.
- **Esclave:** Le compteur donne le nombre de fois que **Cette** unité a eu des problèmes de communication.

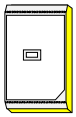
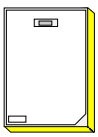
Tous les compteurs peuvent être remis à zéro en quittant le Menu par l'appui sur la touche ➔. En quittant le menu par l'appui sur la touche C, les compteurs ne sont pas remis à zéro.

Anciens Matériels

5 Anciens Matériels

LES ELEMENTS DES TABLEAUX SUIVANTS SONT DES REFERENCES SUPPRIMEES OU EN COURS DE REMPLACEMENT, POUR DE NOUVELLES ETUDES ILS NE DOIVENT PAS ETRE PROPOSES.

TYPE N°	DESCRIPTION
90T RKP ACM 	Lecteur de Contrôle d'Accès & Terminal Intrusion avec lecteur magnétique incorporé, afficheur et clavier pour usage intérieur. 005 25 200 M
90T RKP ACW 	Lecteur Contrôle d'Accès & Intrusion avec les mêmes fonctions que 90 T RKP ACM mais avec tête de lecture Wiegand incorporée. 005 25 080 W
90T RKP ERC 	Contrôleur d'Accès & Terminal d'Intrusion à installer à l'intérieur (idem en design au 90 T RKP) incluant 2,5 m de câble blindé et une boite de jonction 90 TJB , fonctions identiques au 90 T RKP ACM. 005 25 170 M/W/P/ML/IR
90T CWB 	Circuit de chauffage pour installation extérieure dans les lecteurs suivants : 90T ERC/ACW 005 25 265
90T CRP 	Capot de protection contre la pluie pour RKP ERC/ACW 005 25 270
90T EIR 	Tête de lecture pour badges codes barres infrarouge 005 25 xxx IR
90T CSC 	Interface Simple pour antenne Proximité/Mains libres. Nécessite toujours 1 x 90 (95) T ERC connecté 005 25 180 COTAG
90T CDC 	Interface Double pour deux antennes Proximité/Mains libres. Nécessite toujours deux 90 (95) T ERC connectés. 005 25 190 COTAG
90T CLC 	Ampli boucle pour des Antennes sur mesure > 70 cm < 120 cm. L'ampli boucle nécessite toujours une interface/contrôleur simple 90 T CSC et 1 x 90 T ERC. 005 25 250 COTAG

TYPE N°	DESCRIPTION
90T CPA 	Antenne Proximité. Lecture jusqu'à 20 cm. 005 25 240 COTAG
90T CHA 	Antenne Mains Libres. Lecture jusqu'à 70 cm. 005 25 245 COTAG
90T CT 	Badge actif Proximité/Mains libres avec logo HI SEC, non programmé 007 08 045 COTAG

5.1 Le Lecteur de Badges 90T

5.1.1 Dimensions Mécaniques et Disposition

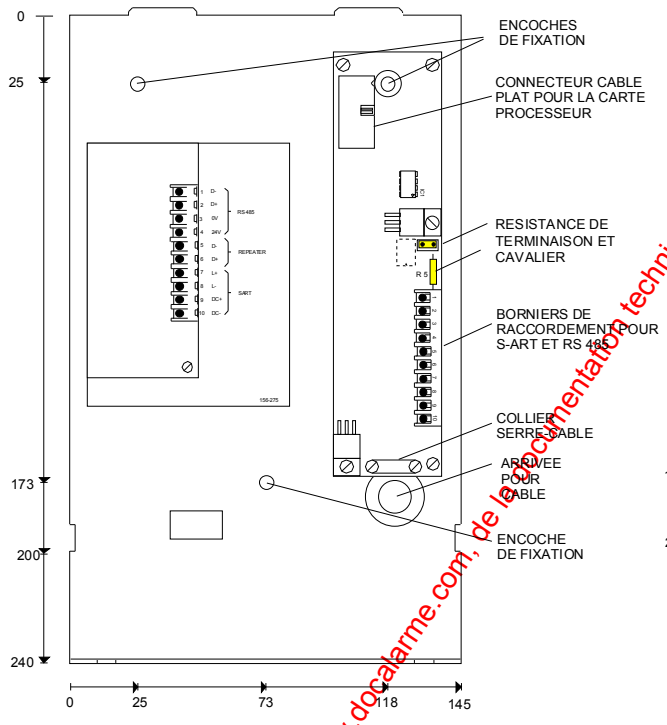
L'unité Lecteur de badges s'ouvre en enlevant les deux vis de type I/n situées au-dessous du coffret. Les vis doivent être retirées sur environ 1 cm, ensuite le couvercle peut être séparé de la plaque de fond. Le câble plat reliant la carte d'interface avec la carte Processeur est débrochable de son support.

Après enlèvement de la partie avant du lecteur, la plaque de fond peut être fixée au mur avec 3 vis type M4 ou similaires. Les trous de fixations du clavier déporté et du lecteur de badges sont placés au même endroit.

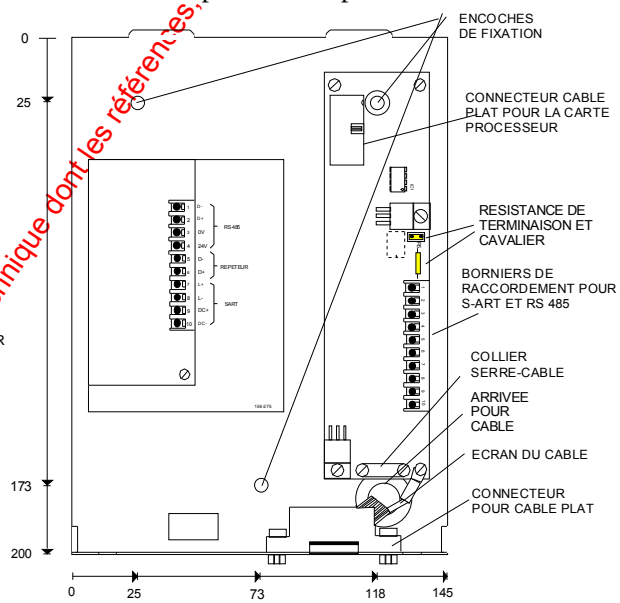
Quand vous fixez la plaque de fond, il doit être pris en considération que le couvercle prend approximativement 3 mm d'espace en plus dans tous les sens par rapport à la surface de la plaque de fond. Pour le démontage, il est aussi nécessaire de prévoir un espace libre de 2 cm en dessous de l'unité lecteur de badges.

La hauteur de fixation recommandée pour les appareils est approximativement de 1m50 à 1m55 pour le côté supérieur du boîtier.

Lecteur standard



Lecteur pour tête déportée:



Le terminal 90T RKP ERC est fourni avec un câble avec écran de 2m50 sortant par le passe fils arrière du lecteur. Le connecteur du câble plat devra être enlevé de son support avant de séparer le clavier de la plaque de fond. La disposition mécanique et la fixation sont les mêmes que celles du terminal intrusion 90T RKP.

Caractéristiques:

Tension d'alimentation : ..... 10-30 V Continu
Consommation : ..... 90 mA en 24V + 60 mA avec le rétro-éclairage en marche
Longueur des câbles :..... Bus RS485 Maximum 1000m- écran, paire torsadée
Bus S-ART Maximum 500m- sans écran, paire torsadée
250m - écran, paire torsadée

Gamme de température : 0-55°C

5.1.2 Installation en extérieur des Lecteurs 90T

L'utilisation des terminaux et lecteurs THOR en environnement extérieur impose l'emploi d'un kit de chauffage. Ce kit pour extérieur peut être installé sur les appareils suivants :

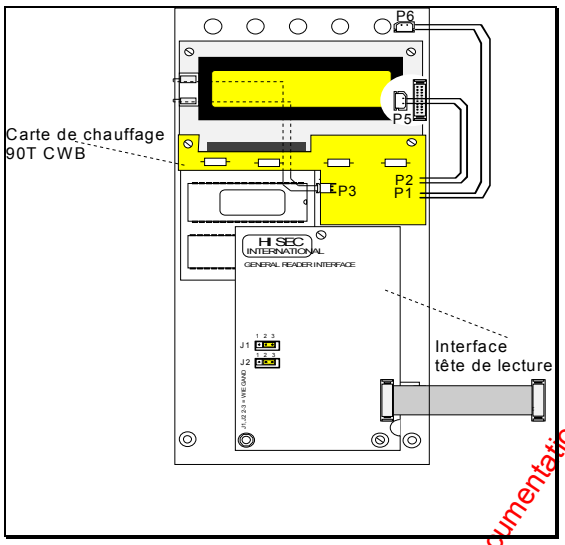
90T RKP	Terminal Intrusion standard
90T RKP ACM	Lecteur magnétique standard (Pas de protection à la pluie possible)
90T RKP ACW	Lecteur Wiegand standard
90T RKP ERC	Contrôleur pour tête extérieure

Le Kit est composé de deux éléments, un circuit de chauffage (90T CWB) et un capot de protection à la pluie (90T CRP).

Le circuit de chauffage (90T CWB) est utilisé pour protéger les appareils listés ci-dessus dans les basses températures. Son utilisation permet d'atteindre des températures allant jusqu'à -25°C.

Le rétro-éclairage de l'afficheur est automatiquement allumé quand la température descend en dessous de 10°C (+/- 10°). En même temps le circuit de chauffage est activé pour chauffer l'afficheur.

Installation du circuit 90T CWB:



1. Séparer le terminal de son fond en enlevant le câble plat.
2. Dévisser les 4 vis de maintien du circuit électronique.
3. Faire effectuer un demi-tour au circuit électronique et déconnecter le câble limande du clavier. Noter le sens de ce dernier avant de la déconnecter.
4. Séparer l'afficheur de la carte CPU en dévissant les 4 vis de maintien.
5. Insérer le connecteur venant de l'afficheur dans celui de la carte 90T CWB (repéré P3).
6. Insérer P2 de la carte 90T CWB dans P5 de la carte CPU.
7. Insérer P1 de la carte 90T CWB dans P6 de la carte CPU.
8. Remonter l'afficheur et le circuit de chauffage sur la carte CPU en s'aidant du schéma ci-dessous.

La carte 90T CWB devra être placée au-dessus du circuit de l'afficheur au moyen des vis existantes.

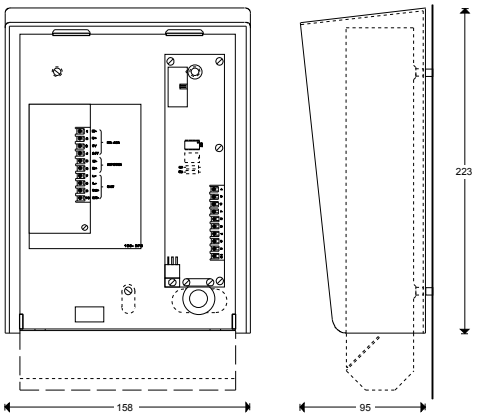
Caractéristiques techniques:

Gamme de température: ..... -25°C/24V
-15°C/12V
Consommation: ..... max. 500 mA (élément en chauffe)
sous 24V DC (inclue consom. terminal)

Protection à la pluie:

Si le terminal (Lecteur) est installé en extérieur sans protection contre la pluie il est nécessaire d'utiliser un capot de protection anti-pluie référencé 90T CRP. Ce capot de protection sera fixé par les mêmes fixations que le terminal (Lecteur).

Le schéma ci-dessous représente les dimensions du capot et le mode de montage.



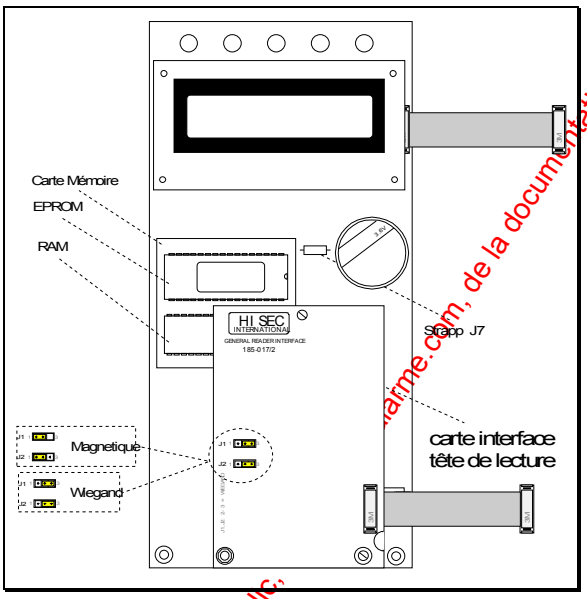
Couleur : gris (RAL 7023)

Attention : Le lecteur magnétique de type 90T RKP ACM ne peut pas être utilisé avec un capot de protection anti-pluie, étant donné que la tête de lecture n'est sont pas prévue pour un usage en extérieur et n'est pas étanche. Si des lecteurs de technologie magnétique doivent être installés à l'extérieur ont devra utiliser le terminal (contrôleur) 90T RKP ERC et une tête de lecture magnétique 90T EMR.

5.1.3 Configuration 90T RKP ERC pour le choix de tête de lecture

L'utilisation des lecteurs THOR avec différentes têtes de lecture impose de configurer les interfaces pour adapter l'interface de la tête de lecture avec le type de tête utilisé.

Deux catégories de signaux existent **Magnétique** et **Wiegand**, toutes les technologies se raccorderont sur un de ces 2 modes.



Deux cavaliers permettent de choisir la technologie adaptée à la tête de lecture:

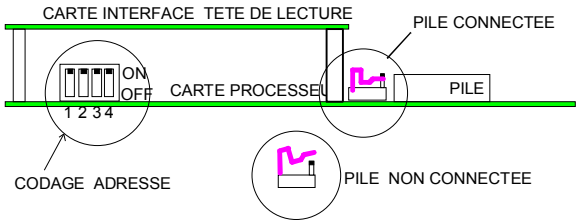
Magnétique : Magnétique (90T EMR)

Wiegand : Toutes les autres (proximité, mains libres, infrarouges)

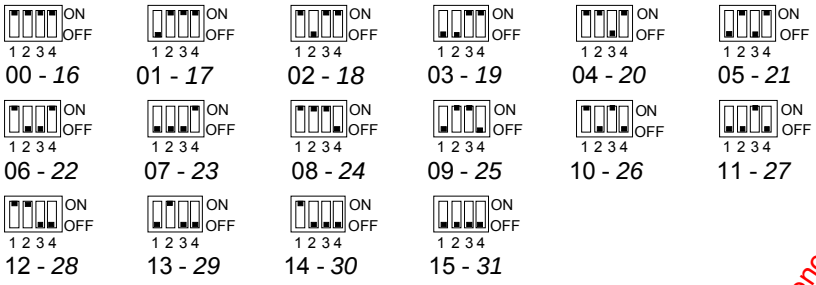
Attention : La configuration par défaut est du type Wiegand.

5.1.4 Interrupteurs du Lecteur de Badges 90 T

Quatre micro-interrupteurs sont utilisés pour programmer l'adresse de chaque unité sur le bus. Ces micro-interrupteurs sont placés sur la carte Processeur du lecteur de badges.



Le cavalier connectant la pile de sauvegarde de la carte Processeur à la mémoire RAM doit être en position ON sur le lecteur de badges. S'il est en position OFF, la programmation sera perdue en cas de disparition de l'alimentation.



0 signifie que l'interrupteur est en position "ON".

1 signifie que l'interrupteur est en position "OFF".

Les adresses sont codées en binaires, de **00 à 15** (ou de **16 à 31** avec le bit d'option 8 à 1).

L'adresse du lecteur est donnée par le micro-interrupteur et par une option de programmation du lecteur (option 8), qui permet de décider si l'adresse sera comprise entre 00 et ou entre 16 et 31.

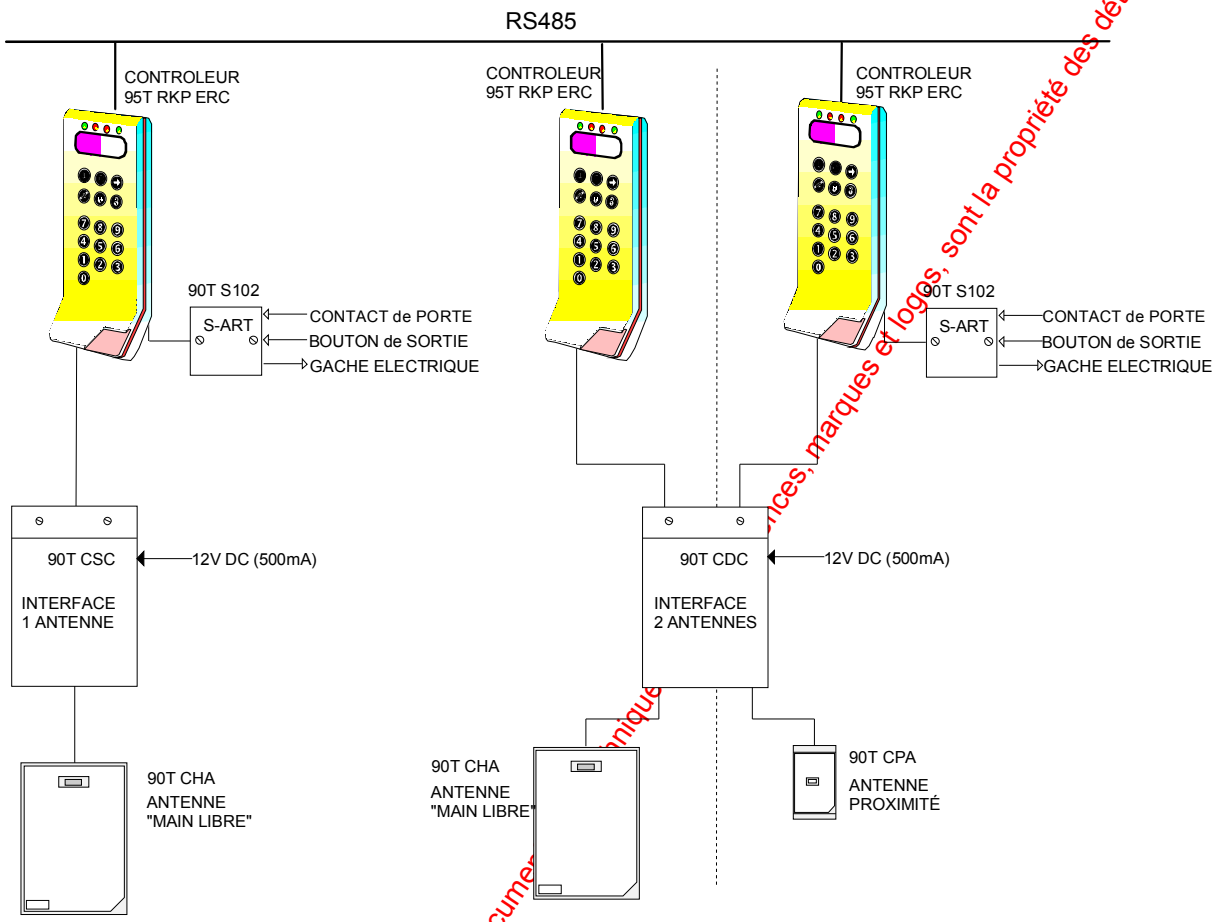
Option 8 = 0 adresse comprise entre 00 et 15.
Option 8 = 1 adresse comprise entre 16 et 31.

L'**Adresse 00** est réservée au contrôleur principal.

Dans un système avec intégration à la centrale Intrusion THOR, l'adresse 00 ne devra pas être utilisée par un lecteur de badges. Dans un système Multi-lecteurs **sans intégration**, un des lecteurs **devra** être programmé à l'adresse 00, à cette adresse il sera automatiquement considéré comme le Maître du protocole Multi-maîtres.

5.2 Proximité et Mains libres ACTIF (COTAG)

La figure ci-dessous représente une configuration simple et une configuration avec des lecteurs d'entrée et de sortie (Anti-retour possible) sur la même porte.



Un contrôle "**simple porte**" sera constitué des éléments suivants:

1 Terminal/Lecteur		..... 95T ERC
1 S-art pour le contrôle de la porte		..... 90T S102
1 Interface 1 Antenne		..... 90T CSC
1 Antenne	Proximité porte max. 20 cm	..... 90T CPA
ou	Main libre portée max. 70 cm	..... 90T CHA

Un contrôle Anti-Retour "**double sens**" sera constitué des éléments suivants:

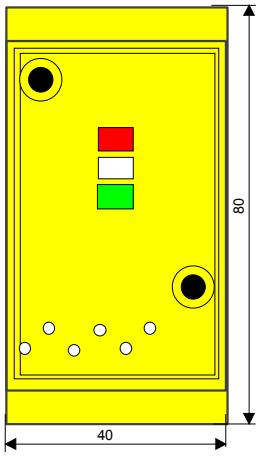
2 Terminaux/Lecteurs		..... 95T ERC
1 S-art pour le contrôle de la porte		..... 90T S102
1 Interface 2 Antennes		..... 90T CDC
2 Antenne	Proximité porte max. 20 cm	..... 90T CPA
ou	Main libre portée max. 70 cm	..... 90T CHA

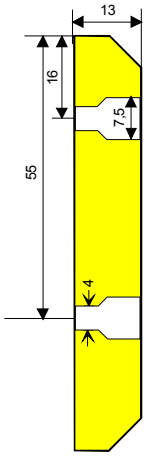
Il est recommandé d'utiliser des alimentations 12V séparées pour chaque unité contrôleur "simple/double Zone" pour s'affranchir des coupures d'alimentation sur les câbles etc.

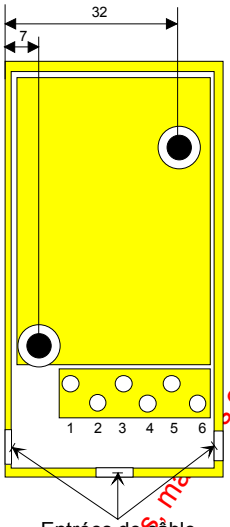
Nota :les lecteurs 95T ERC devront être configurés en interface Wiegand.

5.2.1 Dimensions mécaniques et fixation des têtes de lecture

Proximité 90T CPA







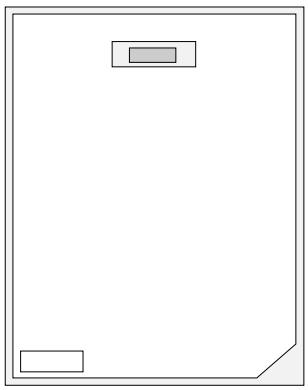
Entrées de câble

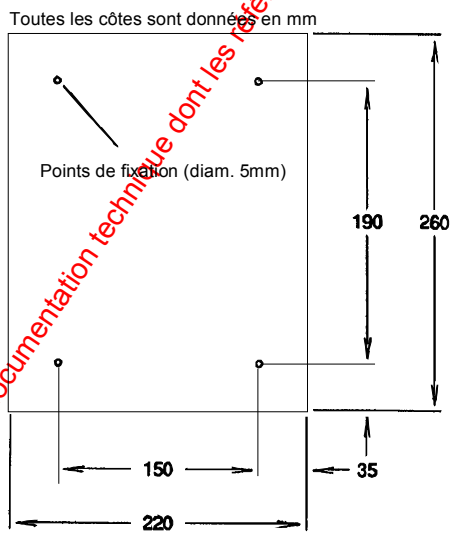
Toutes les côtes sont données en mm

Caractéristiques:

Portée : 20 cm
Taille : 80x40x13 mm
Poids : 45g
Temp. de fonct.: -40 à +70°C (IP 55)
Leds d'indication : rouge et verte

Mains libres 90 T CHA

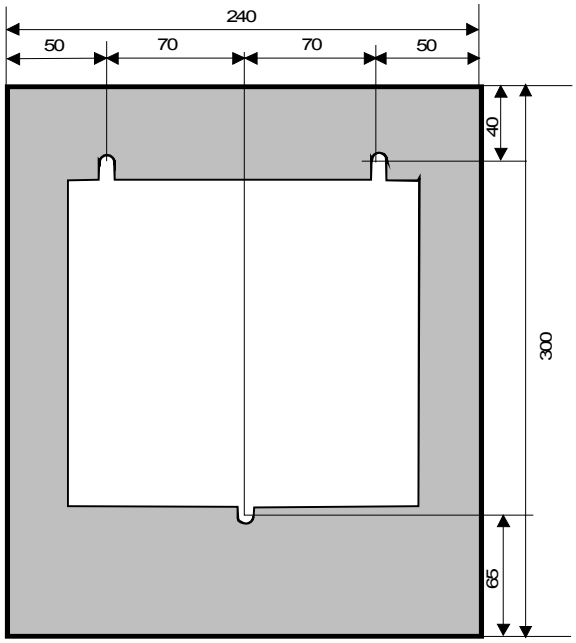




Caractéristiques:

Portée :.....70 cm
Taille :.....260x220x25 mm
Poids : 740g
Température de fonctionnement : .....-40 à +70°C (IP 54)
Leds d'indication :.....rouge et verte et jaune

5.2.2 Dimensions mécaniques et fixation des interfaces 90T CSC et 90T CDC



Toutes les côtes sont données en mm.

Caractéristiques communes:

Taille : 300x240x53
Poids: ..... 2,2 Kg
Température de fonctionnement :.. 0 à +45°C
Humidité: ..... 90 % non condensée

Alimentation : 12V DC (+25%,-10%) 500 mA, une alimentation à régulation série (pas de découpage) est conseillée.

- Distance max. Interface - tête de lecture : 300m.

  Cette longueur de câble impose du câble faradisé (type BELDEN®), de plus les câbles transmission et réception doivent être torsadés avec des écrans séparés de taille 0.5 mm² (20AWG, 16/0.2). Cela correspond à un câble Belden® 9154 ou équivalent pour un câble 1 seule paire torsadée, ou BELDEN® 9154 ou équivalent pour deux paires torsadées avec écrans séparés.

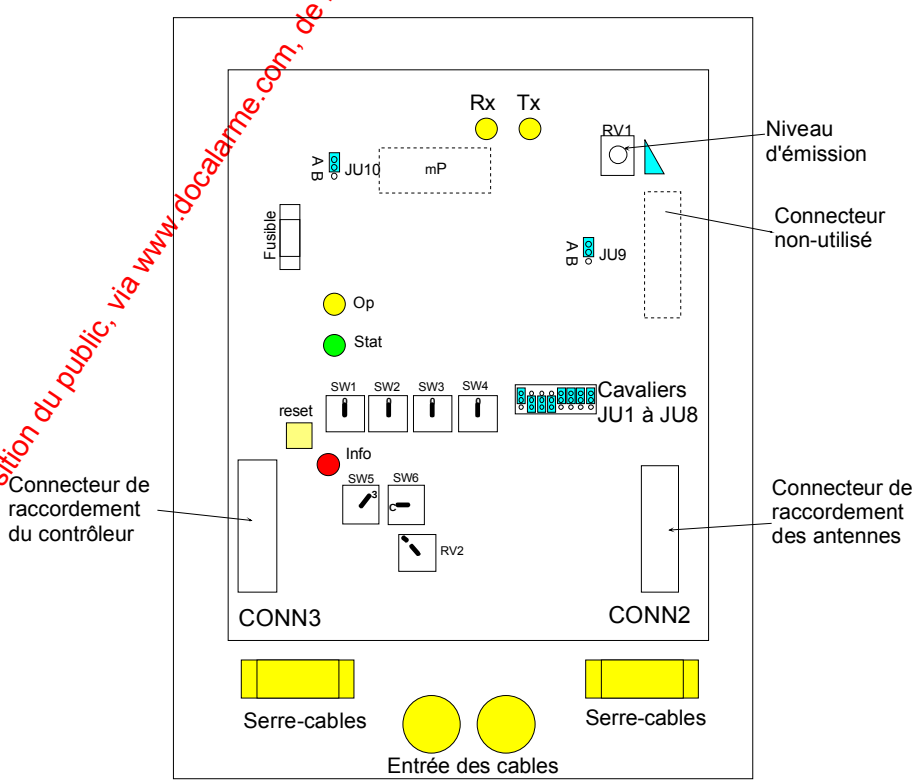
  Attention : Les écrans des câbles devront être reliés **uniquement du coté du l'interface** et surtout pas du coté de l'antenne, ou ils devront être coupés au plus court et isolés.

- Distance maximum entre Interface et terminal 95T ERC : 150m, câble standard paires torsadées (5 fils) avec écran.

  Attention : L'écran du câble devra être relié **uniquement du coté du Contrôleur 95T ERC** et surtout pas du coté de l'interface, ou il devra être coupé au plus court et isolé.

Remarque : les interfaces sont configurées en usine pour fonctionner directement sur le système HISEC, en conséquence ne pas modifier les cavaliers, interrupteurs, et autres potentiomètres.

5.1.2.1 Description et raccordements de l'interface "simple antenne" 90T CSC



Seul le potentiomètre RV1 peut être modifié pour réduire la portée de l'antenne (par défaut max.).

Nota: le pilotage des voyants sur les têtes de lecture proximités (90T CPA) impose de raccorder sur chacune de ces deux connexions une résistance de 470 Ω 1/2 W de rappel à l'alimentation de l'interface 90T CSC CONN3-1.

Fonction	Interface simple antenne 90T CSC	
Données (D0)	CONN3-3	
Données (D1)	CONN3-4	
0 Volt	CONN3-2	
	Tête Proximité CPA	Tête "mains libres" CHA
Led Verte (porte ouverte)	4 *(voir Nota)	TB1-5 D3
Led Rouge (porte fermée)	3 *(Voir Nota)	TB1-3 D1

Indicateurs à LED:

Rx et **Tx** : (jaunes) voyants indicateurs des informations transmises et reçues par l'antenne.

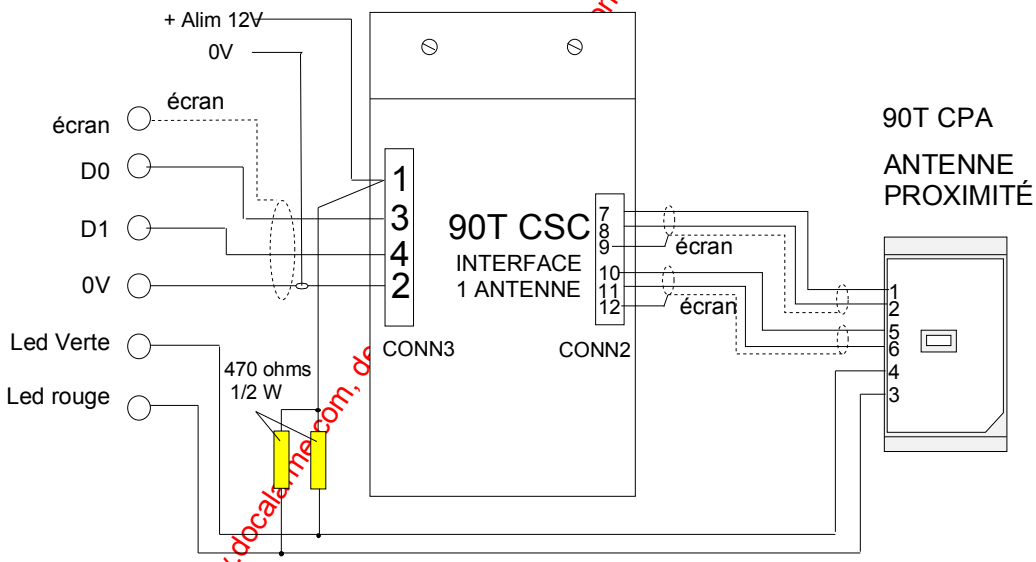
Dans des conditions de bruits normales (pas de badge présenté), la LED Rx doit s'allumer très faiblement. Elle doit s'allumer brièvement à la présentation d'un badge devant l'antenne.

Un niveau élevé de bruit provoquera un allumage plus brillant en l'absence de badge.

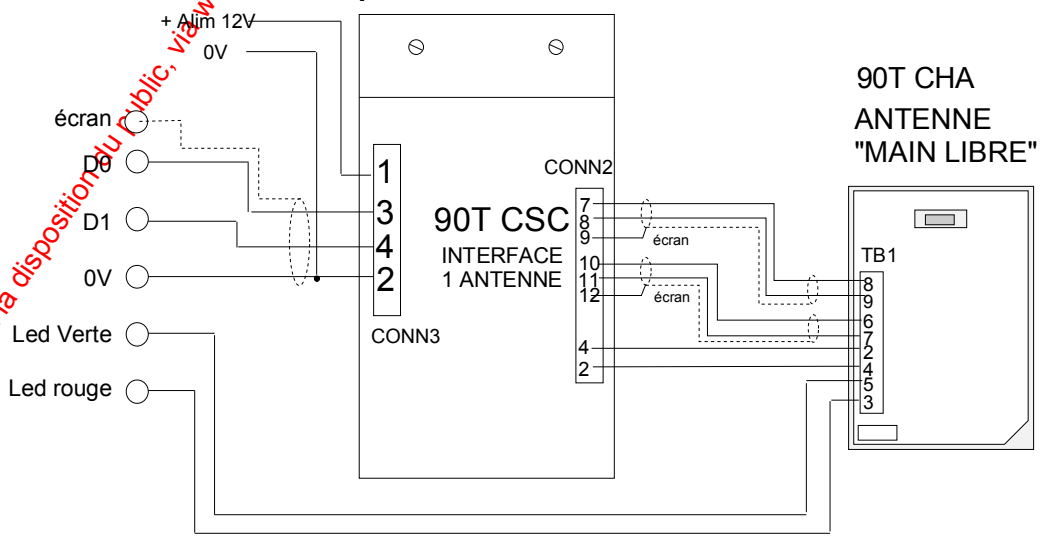
Op : (jaune) Indicateur de communication entre l'interface et le lecteur HISEC, s'allume brièvement à chaque lecture d'un badge reconnu.

Sta (verte) et **Info** (rouge): Utilisées uniquement pendant les tests en usine.

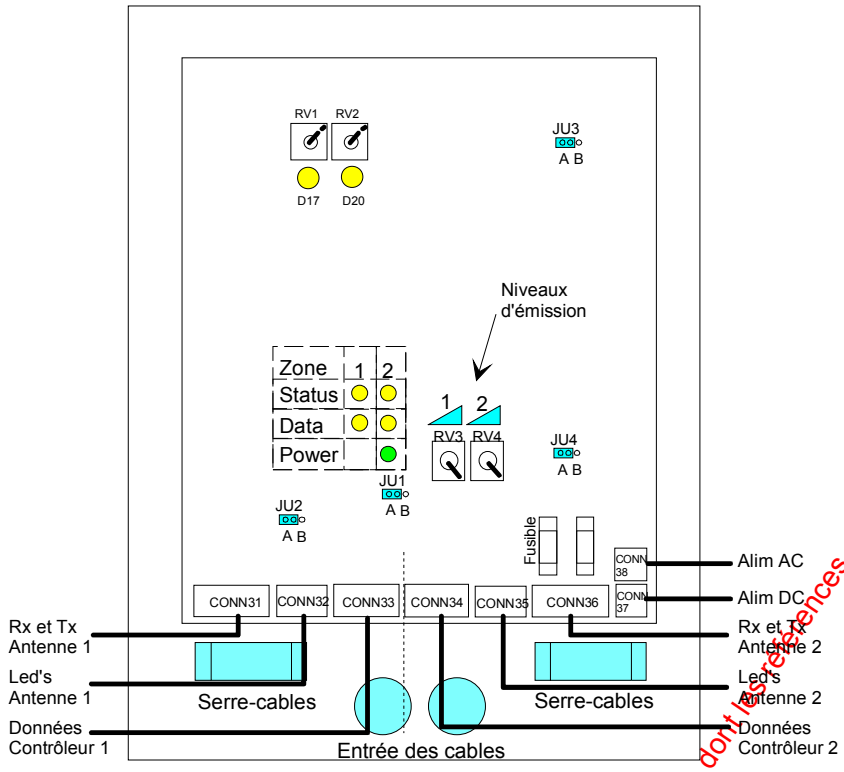
Raccordement de l'interface "simple antenne" 90T CSC sur une antenne 90T CPA



Raccordement de l'interface "simple antenne" 90T CSC sur une antenne 90T CHA



5.2.2.2 Description et Raccordement de l'interface "double antenne" 90T CDC



Seuls les potentiomètres RV3 et RV4 peuvent être modifiés pour réduire la portée de l'antenne (par défaut max.), respectivement RV3 = Antenne 1 et RV4 = Antenne 2.

Indicateurs à LED:

Rx1(D17) et **Rx2**(D18) : (jaunes) voyants indicateurs des informations transmises reçues des antennes, respectivement Rx1 = antenne 1 et Rx2 = antenne 2.

Dans des conditions de bruits normales (pas de badge présenté), ces Leds doivent s'allumer très faiblement. Elles doivent s'allumer brièvement à la présentation d'un badge devant les antennes respectives.

Un niveau élevé de bruit provoquera un allumage plus brillant en l'absence de badge.

Statuts (D23) et (D25) : (jaune) LED destinée aux tests à l'installation. En fonctionnement normal elle clignote à la même cadence que la LED Power, respectivement D23 = antenne 1 et D25 = antenne 2.

Data (D24) et (D26) : (jaune) Indicateur de communication entre l'interface et le lecteur HISEC, s'allume brièvement à chaque lecture d'un badge reconnu, respectivement D24 = antenne 1 et D26 = antenne 2.

Power (verte) : indique par son clignotement la scrutation des antennes, quand un badge est présenté sur une des antennes elle s'allume pour 1/2 seconde et clignote à nouveau. Cette séquence est répétée autant de temps que le badge est présent devant une des antennes.

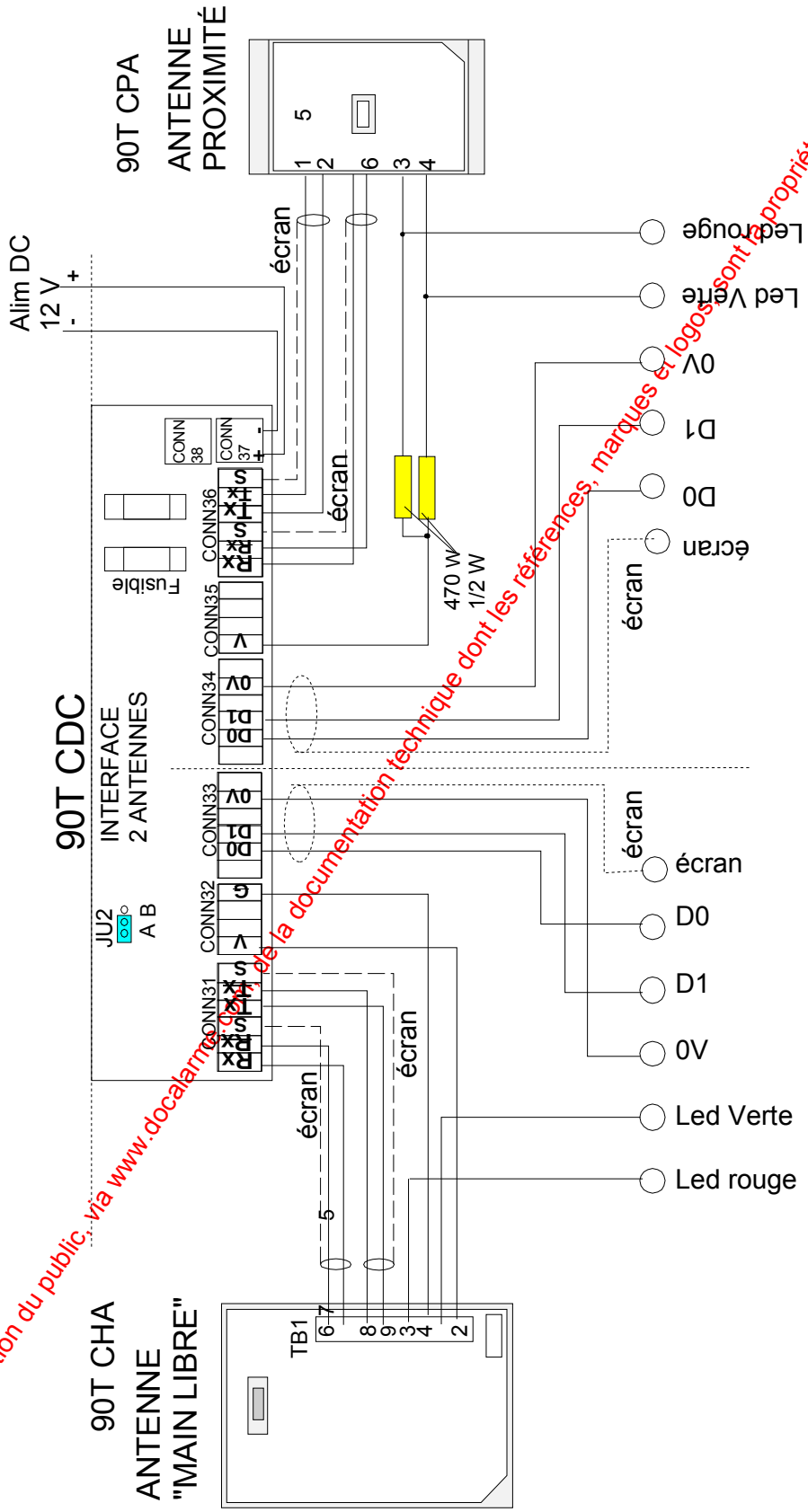
Câblage :

Le tableau suivant représente la connexion entre l'interface et les lecteurs 95T ERC.

Fonction	Antenne 1		Antenne 2	
Données (D0)	CONN34 D0		CONN33 D0	
Données (D1)	CONN34 D1		CONN33 D1	
0 Volt	CONN34 0V		CONN33	
	Tête Proximité CPA	Tête Proximité CPA	Tête mains libres CHA	Tête mains libres CHA
Led Verte (porte ouverte)	4 *(voir Nota)	4 *(voir Nota)	TB1-5 D3	TB1-5 D3
Led Rouge (porte fermée)	3 *(Voir Nota)	3 *(Voir Nota)	TB1-3 D1	TB1-3 D1

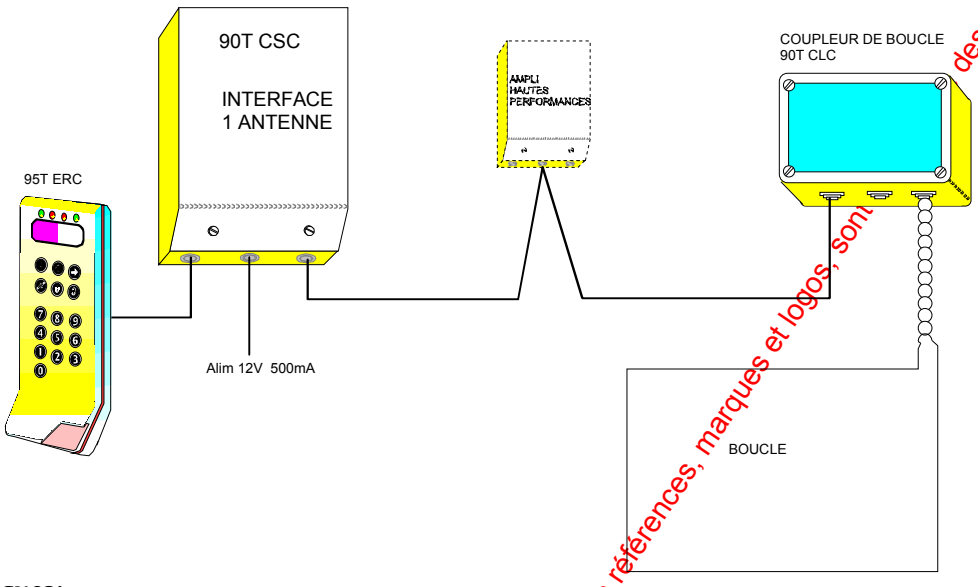
Nota: le pilotage des voyants sur les têtes de lecture proximités (90T CPA) impose de raccorder sur chacune de ces deux connexions une résistance de 470 Ω 1/2 W de rappel à l'alimentation de l'interface 90T CDC, CONN32 V pour l'antenne 1 et CONN35 V pour l'antenne 2.

Schéma de raccordement de l'interface "double antenne" 90T CDC sur une antenne 90T CPA et une antenne 90T CHA.



5.2.3.3 Le Coupleur de boucle 90T CLC

Le coupleur d'antenne sera utilisé partout où la portée des antennes standard n'est pas suffisante. Cela permet de réaliser des antennes aériennes (encadrement de portes, entrées de parkings, etc) ou des antennes encastrées sous tubes dans la cloison.

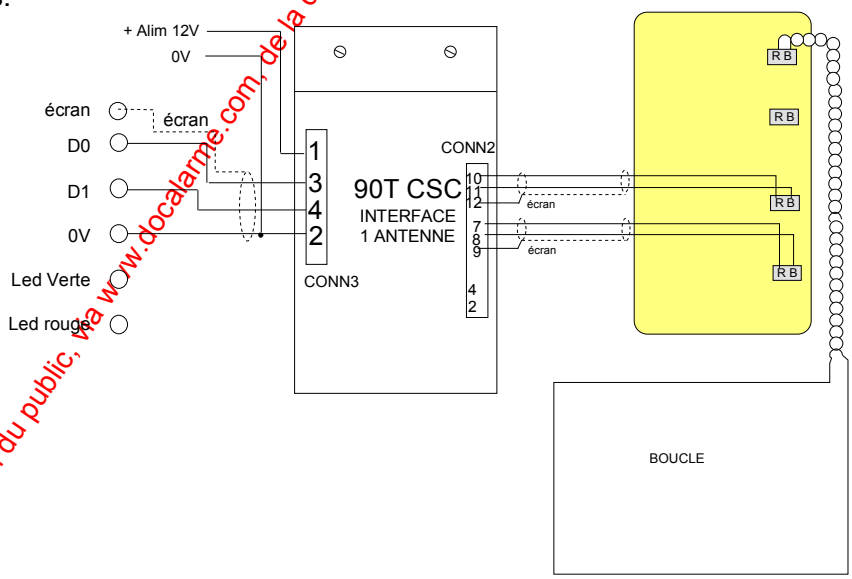


Caractéristiques:

Taille :	160x80x55 mm
Température de fonctionnement :	0 à +45°C
Humidité :	0-90% non condensée
Distance max. Entre Coupleur CLC et Boucle :	10 m (paire torsadées)
Distance max. Entre Interface CSC et coupleur CLC :	300 m (paires torsadées, écran, 0,5mm)
Alimentation :	12 V
Consommation:	max. 500mA (pas d'alim. à découpage)

Nota : l'amplificateur hautes performances est uniquement nécessaire quand la boucle est à proximité d'une surface métallique ou d'une porte métallique. Dans la plupart des installations l'interface CSC et le coupleur CLC sont suffisants.

Raccordements:



Attention : le coupleur de boucles 90T CLC ne fonctionne pas avec le contrôleur double antenne (90T CDC)

5.1.2.4 Equipements de test

Afin de faciliter l'installation des systèmes proximités et mains libres COTAG propose une série d'équipement pour l'alignement et la recherche des perturbations.

Badge Test

Ce badge est similaire a un badge classique excepté qu'il est en matière plastique transparente, ce qui permet de voir la LED de réception (rouge) qui a été inclue à l'intérieur.

Cette LED s'allume quand le badge est dans le champ de la tête de lecture, cela permet de vérifier la portée, l'interaction des têtes entre elles (entrée-sortie par exemple) etc. Il est particulièrement utile pour les antennes personnalisées.

Attention : Ne pas utiliser ce badge pour mesurer la portée espérée avec un badge classique, car la LED indique la réception du champ uniquement alors qu'un badge réel ne sera peut être pas capable d'emettre assez pour être reconnu par la tête de lecture.

Mesureur d'alignement

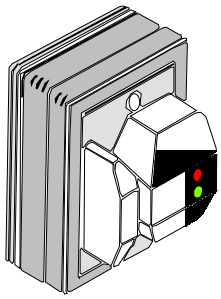
Cet appareil très complet permet d'optimiser le réglage des antennes et d'effectuer un diagnostic de l'installation, il pourra être utilisé pour mesurer le bruit, localiser les sources de bruit, détecter le métal et finaliser les réglages des antennes personnalisées. Il est fourni avec une sonde de bruit et divers accessoires de mesures.

Mesureur de champs

Cet appareil permet d'optimiser le réglage des antennes standards au moyen d'un capteur sans contact qui permet uniquement de mesurer le champ des têtes de lectures.

5.3 Codes à barres Infrarouges 90T EIR

5.3.1 Présentation et dimensions

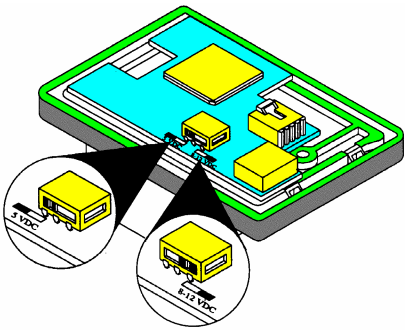


Caractéristiques complémentaires

Poids : 40 g
Température de fonctionnement : -20 à +50°C
Humidité : 0 à 80% non condensée
Leds d'indication : rouge et verte
Consommation : 150 mA
Dimensions: 51 x 80 x 89 mm

Il n'existe pas de badge Maître et Maintenance au format Infrarouge, c'est pourquoi il est impératif d'initialiser le lecteur (Menu 82) au moyen d'une tête magnétique temporaire (ne pas oublier de programmer le format libre BFORM=06), donc il faudra posséder les badges précédemment cités avec le même code site que le logiciel (si existant).

5.3.2 Configuration et Initialisation



Il est impératif de configurer la tête de lecture au moyen de l'interrupteur en fonction de la tension d'alimentation, voir les deux câblages ci-dessous suivant le schéma ci-contre.

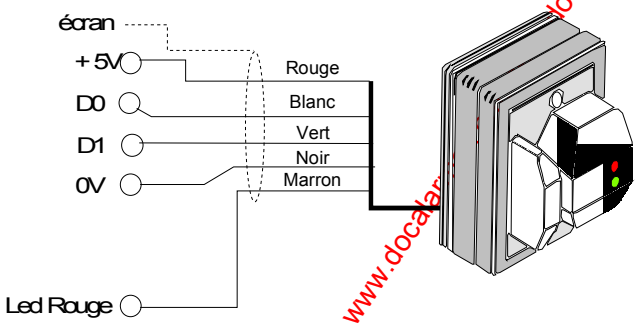
A la mise sous tension les 2 Leds clignotent alternativement pendant 3 secondes.

Ne pas oublier que pour initialiser la tête de lecture I.R il est impératif de posséder un badge d'initilisation infrarouge, 3 types différents existent, celui à utiliser sera repéré ABA-WIEGAND.

Après passage de ce badge dans la tête, les deux LED clignotent ensemble 3 secondes pour indiquer la prise en compte de l'initialisation.

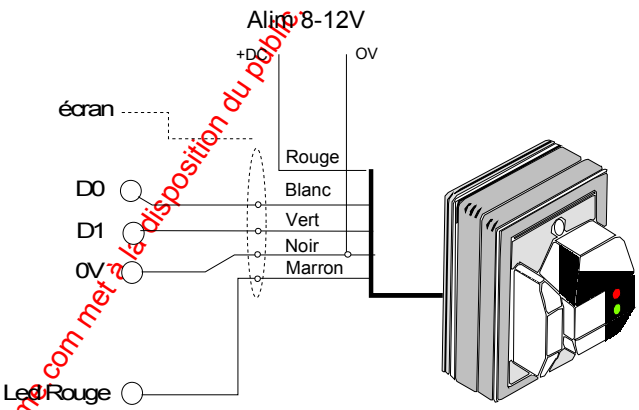
Ne pas oublier qu'a chaque coupure d'alimentation cette initialisation sera à refaire.

Tête de lecture à moins de 3m du contrôleur (alim 5V)



Dans cette configuration l'alimentation (5V) de la tête de lecture est fournie par le contrôleur 90T RKP ERC

Tête de lecture entre 3 et 30 m du contrôleur (alim 8-12V) :

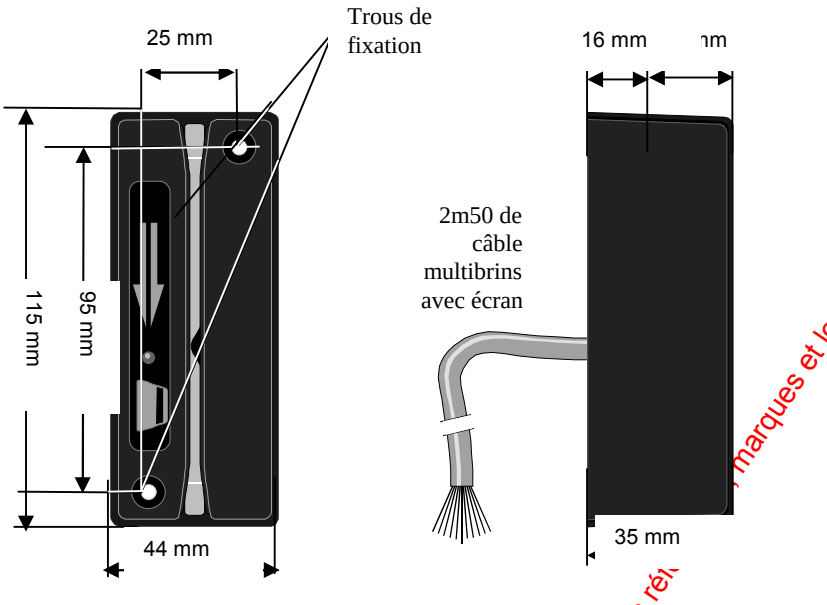


Dans cette configuration l'alimentation (12V) de la tête de lecture est fournie par une alimentation extérieure (ou par le bus RS 485, si celui-ci est en 12V).

Attention : La tête de lecture IR ne peut pas être alimentée au-dessus de 12V, dans le cas d'une alimentation/chargeur fournissant du 14 V (non réglable), il est nécessaire d'insérer dans le + alim une série de 4 diodes 1N 4000, pour baisser la tension.

5.4 Magnétique 90T EMR1

Présentation et dimensions

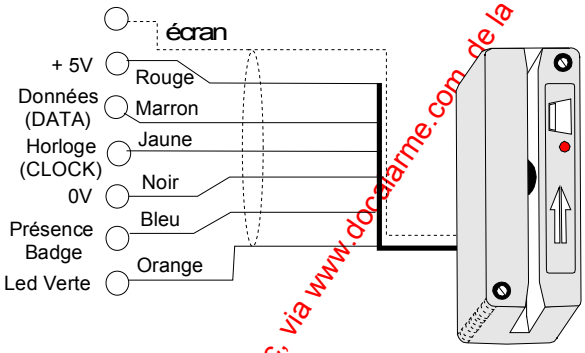


Caractéristiques :

Poids : 40 g
Température de fonctionnement : -30 à +70°C
Humidité : sans importance
Leds d'indication : rouge ou verte

Câblage

La tête de lecture est fournie avec un câble avec écran de 2,5 m de longueur. Si la distance entre la tête de lecture et le terminal est supérieure un câble avec écran (max 50m) complémentaire peut être connecté.

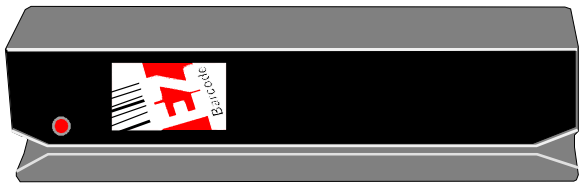


Important !!! Les écrans des deux câbles devront être reliés ensembles.

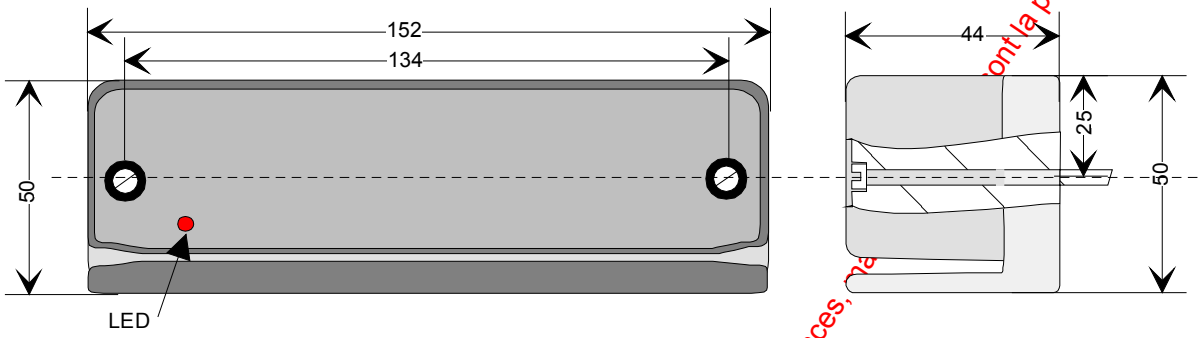
Remarque : le signal ***présence badge*** (fil bleu) n'est pas utilisé par le lecteur 95T ERC.

5.5 Codes à barres Infrarouges 95T EIR

5.3.5.1 Présentation et dimensions



Poids : 350 g
Température de fonctionnement : -30 à +70°C
Matériau : Alliage aluminium
Leds d'indication : rouge
Consommation : 100 mA
Dimensions: 152 x 50 x 44 mm



Types de codes barres infrarouges acceptés (**max. 16 caractères**) : Code 39, 2 parmi 5, Codabar, UPC-A, UPC-E, EAN, Code 11, Code 93, Code 128, MSI.

5.3.5.2 Configuration et Initialisation

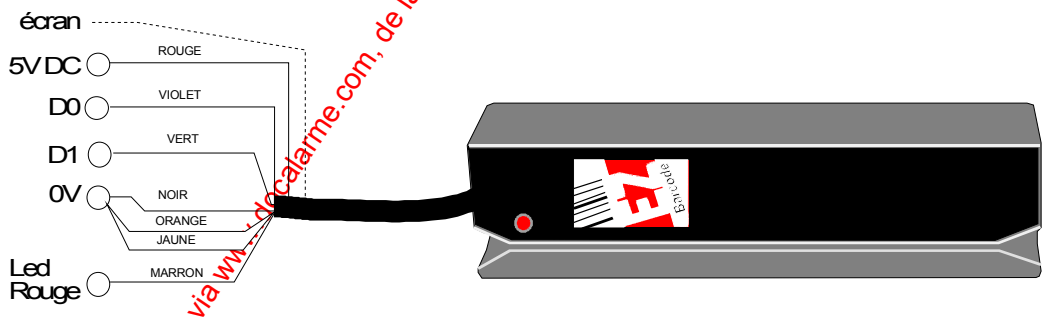
Il n'existe pas de badge Maître et Maintenance au format Infrarouge, c'est pourquoi il est impératif d'initialiser le lecteur (Menu 82) au moyen d'une tête magnétique temporaire (ne pas oublier de programmer le format libre **BFORM=06**), donc il faudra posséder les badges précédemment cités avec le même code site que le logiciel (si existant).

Pour les lecteurs 95T, il est intéressant d'utiliser des modèles 95T ACM, de cette façon la tête magnétique incorporée est toujours disponible pour les opérations de maintenance.

Les Lecteurs devront être en position câblage **Wiegand**:

90 T : J1 2-3 et J2 2-3 95 T : J4 enlevé

Tête de lecture à moins de 10m du contrôleur (alim 5V)



Fiches de Programmation

6 FICHES DE PROGRAMMATION

FICHE DE PROGRAMMATION # 1A

CONFIGURATION DU LECTEUR -Menu 82-

LECTEUR N° r r - r r

MODE: r r

01: Autonome
02: Multi-Lecteurs
03: Intégré

OPTIONS :

Option			Définition	
Option 1	(0)		0 = Code personnel. à 4 chiffres	1 = Code pers. à 6 chiffres
Option 2	(0)		0 = Réaction sur alarme locale	1 = Réac. sur alarme globale
Option 3			0 = Contrôle local de la porte	1 = Cont. externe à la porte
Option 4	(0)		0 = Imprim. contrôle d'accès	1 = Imprim. système intrusion
Option 5	(0)		0 = Impression à la demande	1 = Impression au fil de l'eau
Option 6	(0)		0 = Lecteur mode standard	1 = Lecteur mode tête déportée
Option 7	(0)		0 = Badge standard (encryptés)	1 = Badges non-encryptés
Option 8	(0)		0 = Enregistrement Histo. standard	1 = Enregistrement Badge + Code seul
Option 9	(0)		0 = Pas d'exploitation PC	1 = Exploitation par PC
Option 10	(0)		0 = Communication non-encryptée	1 = Comm. encryptée
Option 11	(0)		0 = Contact de Porte	1 = Pas de Contact de Porte
Option 12	(0)		0 = Changement Heure Eté/Hiver	1 = Pas de changement Heure Eté/Hiver
Option 13	(0)		0 = Pas d'Inter-verrouillage	1 = Inter-verrouillage (sas)
Option 14	(0)		0 = Gestion porte forcée	1 = Pas de porte forcée
Option 15	(0)		0 = Imprimante sur bus Local	1 = Imprimante sur bus principal (00)
Option 16	(0)		0 = Contrôle d'accès normal	1 = Gestion des ouvrants

FONCTION LOCALE :

Option			Définition	
Fonction 1	(0)		0 = Code personnel modifiable	1 = Code personnel non modifiable
Fonction 2	(0)		0 = Porte maintenue normale	1 = Porte maintenue en sabotage
Fonction 3	(0)		0 = Fonction normale	1 = Fonction Parking simple
Fonction 4	(0)		0 = Badge invalide normal	1 = Badge Invalide avec fin de Tempo.
Fonction 5	(0)		0 = Pas de trans. vers GPI-MI	1 = Tous les événements vers GPI-MI.
Fonction 6	(0)		0 = Gestion des ouvrants classique	1 = Obturateur de Serrure
Fonction 7	(0)		0 = Pas de trans. Vers Vidéo.	1 = Transmission vers Vidéo.
Fonction 8	(0)		0 = Pas de temps mini.	1 = Tempo. mini. entre lecture badge.
Fonction 9	(0)		0 = Lecture de badge porte ouverte.	1 = Pas de lecture de badge porte ouverte.
Fonction 10	(0)		0 = Pas de blocage terminal	1 = Blocage terminal après faux codes
Fonction 11	(0)		0 = Code contrainte = Code + 1	1 = Code Contrainte librement prog.
Fonction 12	(0)		0 = Buzzer actif	1 = Buzzer hors service
Fonction 13	(0)		0 = Inter-verrouillage en gestion des ouvrants	1 = Pas d'inter-verrouillage en gestion des ouvrants
Fonction 14	(0)		0 = Bouton poussoir de sortie toujours opérationnel.	1 = Lecteur bloqué, impossible d'utiliser le B.P de sortie
Fonction 15	(0)		0 = AIR n'est pas obligatoire	1 = AIR obligatoire pour tous les badges
Fonction 16	(0)		0 = Les événements sont transmis à GPI HOST bus principal (00)	1 = Les événements ne sont pas transmis à GPI HOST bus principal (00)
Fonction 17	(0)		0 = Les événements sont transmis à GPI HOST de son propre BUS	1 = Les événements ne sont pas transmis à GPI HOST de son propre BUS
Fonction 18	(0)		0 = Lecture de badge silencieuse	1 = Lecture de badge avec BEEP
Fonction 19	(0)		0 = Accepte les badges programmés	1 = Accepte tous les badges magnét. ISO

FICHE DE PROGRAMMATION # 1B

CONFIGURATION DU LECTEUR -Menu 82-

BFORM :

- 00: Lecteur non-initialisé
- 01: Format magnétique encrypté HISEC
- 02: Format Wiegand HISEC
- 03: Format proximité COTAG-DEISTER HISEC
- 04: Format proximité HUGES-HISEC
- 05: Format magnétique non-encrypté HISEC
- 06: Format programmable Libre ISO Code BCD 16 digits max.
- 07: Format magnétique BCD spécial LOREAL.
- 08: Format HI SEC Proximité DEISTER
- 09: Format magnétique BCD spécial La CHARTE
- 10: Format magnétique BCD spécial ville de STRASBOURG
- 11: Format magnétique BCD spécial TELEMECANIQUE (ancien)
- 12: Format magnétique BCD spécial TELEMECANIQUE (nouveau)
- 13: Format magnétique BCD spécial (NCS)
- 14: Format programmable Libre Bit 64 bits max.
- 15: Format Wiegand 26 bits, N° de badge au début (NCS)
- 16: Format Wiegand 26 bits, N° Installateur au début (ID Solutions)
- 17: Format Cotag spécial
- 18: Format Wiegand 26 bits, avec code site + 128 (Format 15).
- 19: Format spécial AIRTEL
- 20: Format Wiegand 32 bits pour badges 1040 Westhinghouse
- 21: Format cardkey HID
- 22: Format spécial kredit Bank Wiegand.
- 23: Format spécial magnétique Aéroport de Copenhague
- 24: Format magnétique encrypté HISEC avec N° de Version

Menu 83:

Temps de libération de gâche (TPO) :(10) __ __ sec.

Temps d'ouverture de porte avant avertissement (OUV) :(30) __ __ sec.

Temps d'avertissement avant alarme porte maintenue (PREAL) :(10) __ __ sec.

FICHE DE PROGRAMMATION # 2A

CONFIGURATION DES ENTREES/SORTIES du LECTEUR N° _ _-_ _

Menu 84-85:

Ad. Sart	Entrée N°	Type Logiciel	Sortie N°	Type Logiciel	Horloge	Equation (Type de sortie 90-99)
00	00	30	00			
00	01	32	01	83	2	
01	02		02			
01	03		03			
02	04		04			
02	05		05			
03	06		06			
03	07		07			
04	08		80			
04	09		09			
05	10		10			
05	11		11			
06	12		12			
06	13		13			
07	14		14			
07	15		15			
08	16		16			
08	17		17			
09	18		18			
09	19		19			
10	20		20			
10	21		21			
11	22		22			
11	23		23			
12	24		24			
12	25		25			
13	26		26			
13	27		27			
14	28		28			
14	29		29			

FICHE DE PROGRAMMATION # 2B

CONFIGURATION DE L'ANTI-RETOUR

Menu 87:

DANS	_ _ _
VERS	_ _ _

Rappel des Zones :

Zone 0 :	Extérieur du site.
Zone 1-15 :	Lecteurs de sortie connectés au bus maître au Niveau 0.
Zone 16-30 :	Lecteurs de sortie connectés au sous-bus N°1 (GPI BR adresse 1)
Zone 31-45 :	Lecteurs de sortie connectés au sous-bus N°2 (GPI BR adresse 2)
Zone 46-60 :	Lecteurs de sortie connectés au sous-bus N°3 (GPI BR adresse 3)
!	!
Zone 466-480 :	Lecteurs de sortie connectés au sous-bus N°31 (GPI BR adresse 31)

NIVEAU D'Anti-Retour: _ _

00: Anti-Retour permanent
01: Anti-Retour R.à.Z chaque jour
02: Anti-Retour R.à.Z chaque heure
03: Pas de contrôle de l'Anti-Retour

FICHE DE PROGRAMMATION # 3A

PROGRAMMES HEBDOMADAIRES N° 03 à 30

PROGRAMME HEBDOMADAIRE N° _ _ / BUS N° _ _

Menu 52:

JOUR 1				LUNDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 2				MARDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 3				MERCREDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 4				JEUDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 5				VENDREDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 6				SAMEDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 7				DIMANCHE											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

FICHE DE PROGRAMMATION # 3B

PROGRAMMES HEBDOMADAIRES N° 03 à 30

PROGRAMME HEBDOMADAIRE N° _ _ / BUS N° _ _

Menu 52:

..../....

JOUR 8				JOUR SPECIAL 1											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 9				JOUR SPECIAL 2											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

Rappel des fonctions :

00	Pas d'accès
01	Accès **avec** Code Personnel
02	Accès **sans** Code Personnel
03	Fonction de bascule avec **Code Personnel**
04	Fonction de bascule sans **Code Personnel**
05	Fonction AIR sans **Code Personnel**
06	Fonction AIR avec **Code Personnel**

FICHE DE PROGRAMMATION # 4A

PROGRAMMES HEBDOMADAIRES N° 31 à 34

PROGRAMME HEBDOMADAIRE N° 3 _ - LECTEUR N° : _ _

Menu 52:

JOUR 1				LUNDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 2				MARDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 3				MERCREDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 4				JEUDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 5				VENDREDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 6				SAMEDI											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 7				DIMANCHE											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

FICHE DE PROGRAMMATION # 4B

PROGRAMMES HEBDOMADAIRES N° 31 à 34

PROGRAMME HEBDOMADAIRE N° 3 _ - LECTEUR N° : _ _

Menu 52:

..../....

JOUR 8				JOUR SPECIAL 1											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

JOUR 9				JOUR SPECIAL 2											
00	00	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			
_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0	_ _	_ _	_ _	_ 0
FNC: _				FNC: _				FNC: _				FNC: _			

Rappel des fonctions : PH 31

10	Pas d'enregistrement
11	Enregistrement des alarmes seulement. Dans ce cas l'historique local ne contiendra que les alarmes locales.
12	Enregistrement de tous les événements excepté les passages de porte
13	Enregistrement de tous les événements excepté les passages de porte sans utilisation du Code Personnel
14	Enregistrement de tous les événements excepté les limitations définies dans la base de données des Groupes de Personnel
15	Tout enregistrer

Rappel des fonctions : PH 32-33

20	Type logiciel d'entrée 76/77 inactif
21	Type logiciel d'entrée 76/77 actif

Rappel des fonctions : PH 34

30	Ouverture permanente (libération) de la porte pendant la période horaire spécifiée.
31	Fermeture permanente (blocage) de la porte pendant la période horaire spécifiée.
32	Fonctionnement normal de la porte pendant la période horaire spécifiée.
33	Utilisation Code Personnel sans badge (DIGICODE).

FICHE DE PROGRAMMATION # 5

LISTE DES JOURS DE CONGES

Menu 53:

N°	Du				Au				N° de Jour (1 à 9)	Remarques
	J	J	M	M	J	J	M	M		
01										
02										
03										
04										
05										
06										
07										
08										
09										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										

FICHE DE PROGRAMMATION # 6A

PROGRAMMATION DES BADGES

Menu 41-57:

N° de Badge	Priorité	Groupe de Personnel	Nom
00000	3	255	Badge maître
00001	3	255	Badge maître
00002	3	255	Badge maître
00003	3	255	Badge maître
00004	3	255	Badge maître

..../....

FICHE DE PROGRAMMATION # 6B

PROGRAMMATION DES BADGES

Menu 41-57:

..../....

N° de Badge	Priorité	Groupe de Personnel	Nom

..../....

FICHE DE PROGRAMMATION # 6C

PROGRAMMATION DES BADGES

Menu 41-57:

..../....

N° de Badge	Priorité	Groupe de Personnel	Nom

FICHE DE PROGRAMMATION # 7A

PROGRAMMATION DES GROUPES DE PERSONNELS

Menu 51:

LECTEUR N° : _ _ - _ _

Groupe de Personnel	**N° de prog. Hebdo.** (PH)	**Fonction Verrou.** (AS)	**Contrainte** (HU)	**N° Util. Intrusion** (CU)	**Enregistrer les accès normaux** (TE)	**Remarques**
001	02	0	0	001	0	Visiteurs
002	01	0	0	001	0	Ne pas modifier
003	02	0	0	002	0	Ne pas modifier
004						

FICHE DE PROGRAMMATION # 7B

PROGRAMMATION DES GROUPES DE PERSONNEL

Menu 51:

LECTEUR N° : _ _ - _ _

Groupe de Personnel	**N° de prog. Hebdo.** (PH)	**Fonction Verrou.** (AS)	**Contrainte** (HU)	**N° Util. Intrusion** (CU)	**Enregistrer les accès normaux** (TE)	**Remarques**
250	**00**	**0**	**0**	**000**	**0**	**"Sas bancaire"**

FICHE DE PROGRAMMATION # 8A

PROGRAMMATION DES MESSAGES

Menu: Programmation par logiciel PC (90T AICS)

N°:	Défaut	MESSAGE														
01	CONTACTEZ LE DPT. PERSONNEL															
02	CONTACTEZ VOTRE DOMICILE															
03	CONTACTEZ DEP. SECURITE															
04	CONTACTEZ LA RECEPTION															
05	IMPORTANT MESS. TELEPHONIQUE															
06	CONTACTEZ VOTRE SUPERIEUR															
07	R.D.V DEPLACEMENT ANNULE															
08	REUNION ANNULEE															
09	RAPPELEZ LE SIEGE															
10	CONTACTEZ VOTRE SECRETAIRE															
11	REVISION VEHICULE															
12	DEPANNAGE URGENT															
13	VISITE MEDICALE															
14	COURRIER IMPORTANT															
15	DOCUMENT A SIGNER															
16	Libre															

FICHE DE PROGRAMMATION # 8B

PROGRAMMATION DES MESSAGES

Menu: Programmation par logiciel PC (90T AICS)

N°:	Défaut	MESSAGE														
17	Libre															
18	Libre															
19	Libre															
20	Libre															
21	Libre															
22	Libre															
23	Libre															
24	Libre															
25	Libre															
26	Libre															
27	Libre															
28	Libre															
29	Libre															
30	Libre															
31	Libre															

FICHE DE PROGRAMMATION # 9

PROGRAMMATION DES HORLOGES

Menu: Programmation par logiciel PC (90T AICS)

N°	DUREE		RETARD		POLARITE		Remarques
01		999		000		0	
02		999		000		1	
03		999		000		2	
04		180		000		0	
05		180		000		1	
06		180		000		2	
07		005		000		0	
08		005		000		1	
09		005		000		2	
10		001		000		0	
11		001		000		1	
12		999		000		2	
13		999		000		0	
14		999		000		0	
15		999		000		0	
16		999		000		0	

Nombre de faux codes avant alarme :(10) __ __ fois.

Délai entre lecture du badge et entrée du code :(20) __ __ sec.

Index

NOTES PERSONNELLES

Denmark	United Kingdom	France	Spain	Netherlands
HI SEC International A/S Tempovej 42, DK- 2750 Ballerup Denmark	HI SEC International Ltd. 4B Victoria Avenue, Camberley, Surrey GU15 3HX United Kingdom	HI SEC International ZAC de Nanteuil, 12, rue Jules Ferry, F-93561 Rosny sous Bois France	HI SEC International Security S.L. C/. Ávila, 48-50 3° Planta, local G-H E-08005 Barcelona España	HI SEC International B.V. Populierendreef 968B, NL-2272 HW Voorburg Netherlands
Tel.: +45 44 86 05 05 Fax: +45 44 86 05 00 E-mail: dk @ hisec.com	Tel.: +44 (0) 1276 679 950 Fax: +44 (0) 1276 679 949 E-mail: gb @ hisec.com	Tel.: +33 (0) 1 48 12 90 10 Fax: +33 (0) 1 48 12 90 20 E-mail: fr @ hisec.com	Tel.: +34 93 300.46.95 Fax: +34 93 485.60.78 E-mail:	Tel.: +31 (0) 70 386 1103 Fax: +31 (0) 70 387 4095 E-mail: nl @ hisec.com

SYSTÈME HISEC

Manuel Utilisateur

02-005/006/078-01 F

AVANT PROPOS

Ce Manuel a pour but de vous donner toutes les informations nécessaires à l'utilisation du Système HISEC.

Dans le cadre d'une politique continuelle de recherche et de développement, les informations contenues dans ce document sont sujettes à modification sans préavis.

Hi-Sec International dégage toute responsabilité concernant le non respect ou une mauvaise utilisation de ce manuel ainsi que les erreurs ou omissions et leurs conséquences sur les installations.

Manuel référence stock	:02-005/006/078-01 FR
Crée le	24 mai 1994
Révisé le	vendredi 8 octobre 1999

Toutes les marques et produits cités dans ce manuel sont déposées :

Wiegand® est une marque déposée de Sensor Engineering Co.

T A B L E D E S M A T I E R E S

INTRODUCTION GENERALE

Intrusion, Contrôle d'accès et système Intégré

Ce manuel est destiné aux utilisateurs du système Intrusion HISEC, du système Contrôle d'accès HISEC ou de la combinaison des deux (système Intégré).

Ce manuel est divisé en trois parties:

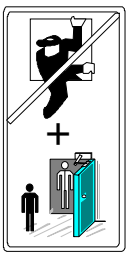
1ere partie: Intrusion

Un système Intrusion permet de détecter les intrus ou tentatives d'intrusion. Quand le système détecte une tentative d'intrusion, il passe en alarme. Cela peut se matérialiser de différentes façons: au moyen de sirènes (avertisseurs acoustiques), lampes flash (indicateurs optiques) ou au moyen d'une transmission silencieuse vers un centre de télésurveillance. La combinaison de ces différents moyens étant possible.

2eme partie: Contrôle d'accès

Un système contrôle d'accès vérifie et enregistre les mouvements de personnes entrant ou sortant d'un bâtiment. Cela est réalisé au moyen de lecteurs de badges, badges, contacts de porte, boutons poussoir de sortie. Cela permet d'exclure toutes les personnes indésirables au site et d'assurer la sécurité de votre propre personnel.

3eme partie: Système Intégré



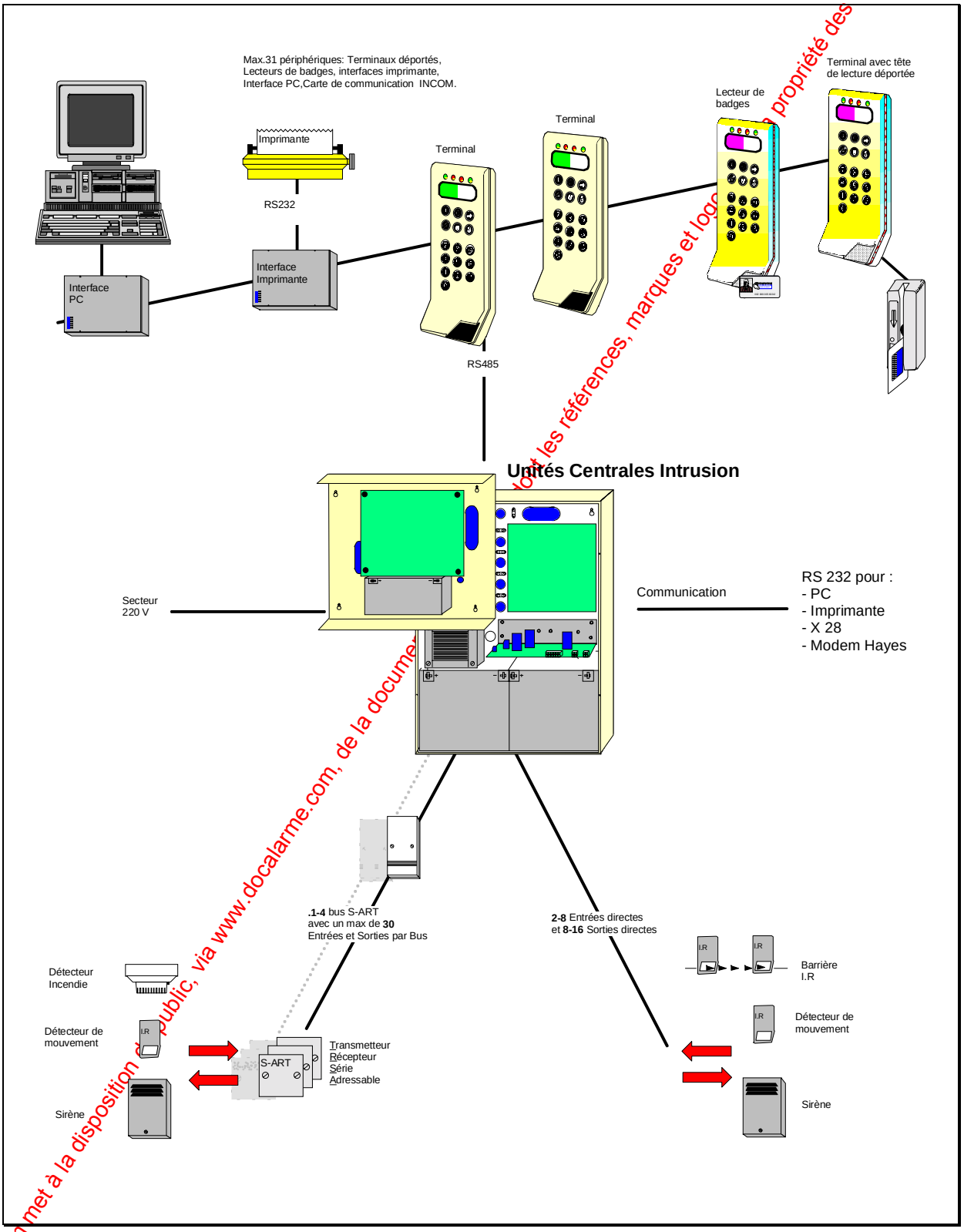
Un système intégré combine intrusion et contrôle d'accès. L'avantage de ce dernier est d'empêcher l'entrée de quiconque tant que le système est armé (sous surveillance). En dehors de cela, le système peut être exploité au moyen de terminaux et lecteurs de badges avec les possibilités des 2 systèmes précédents.

Avant toute utilisation, il est nécessaire de connaître les "règles du jeu", ceci est très important quand on utilise un système d'intrusion ou de contrôle d'accès.

Le synoptique de la page suivante vous donnera une idée de la méthode de communication des différents éléments du système. Lisez les pages suivantes avec la plus grande attention avant d'utiliser le système HISEC.

Pour l'utilisation du P.C. et de la carte de communication INCOM, prière de se référer respectivement aux notices "Manuel Utilisateur AIMS" et "Manuel Utilisateur INCOM".

Synoptique d'un système HISEC (Intégré)



AVERTISSEMENTS ET CONSEILS

Le Code Personnel

L'utilisation du code personnel est un élément très important de l'exploitation du système HISEC.

La distinction entre deux opérateurs est faite au moyen de leurs "codes personnels" respectifs.

- Pour opérer sur le système intrusion HISEC, chaque opérateur a besoin d'un code personnel à 6 chiffres.
- Pour opérer sur le système contrôle d'accès HISEC, un badge minimum est nécessaire. Le code personnel est optionnel et peut être programmé pour chaque badge; il sera de 4 ou 6 chiffres.
- Dans le cas d'un système intégré, il est possible de posséder deux codes personnels: un pour le système intrusion et un pour le système contrôle d'accès.

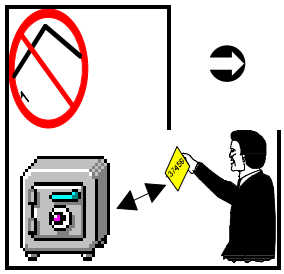
Pour éviter toute confusion, vous pouvez utiliser le petit "pense bête" suivant; quand vous opérez sur un terminal (voir le chapitre 2.1 pour sa description), utiliser votre code personnel Intrusion;. quand vous opérez sur un lecteur contrôle d'accès (voir le chapitre 7.1 pour sa description), utilisez le code personnel du contrôle d'accès.

Le code personnel est une donnée privée qui doit être uniquement connue de vous.

Si par hasard vous entrez un faux code, appuyez sur la touche C et recommencez à nouveau.

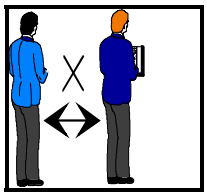
Attention! Après 3 tentatives infructueuses, le terminal du système intrusion est bloqué pendant 5 mn. Après 10 tentatives (valeur programmable) le badge utilisé pour cette opération est bloqué dans le système contrôle d'accès.

Pour éviter les mauvaises surprises avec les codes personnels, il est nécessaire de respecter les règles suivantes:

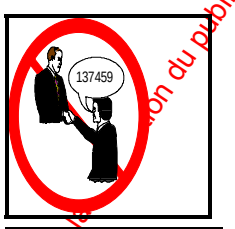


Ne pas écrire son code personnel sur un morceau de papier.

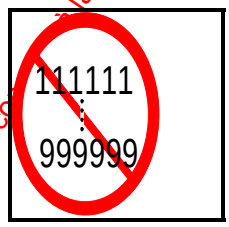
Si vous avez besoin d'un aide mémoire, placer votre code dans un endroit de sécurité et de préférence fermé à clé.



Tenir éloignées les personnes qui ne sont pas (ou plus) autorisées à exploiter le système. De même, effacer leur programmation dans le système. Voir les Chapitre 5.4 Menu 42, Chapitre 11.2 Menu 24 et Chapitre 11.4 Menu 42.

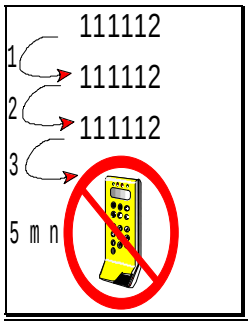


Ne jamais donner son Code Personnel à une tierce personne.

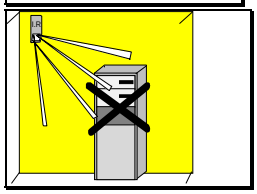


Ne pas utiliser de combinaisons simples de chiffres, quand ont choisi son code personnel. Ces dernières sont très faciles à découvrir par les personnes non habilitées.

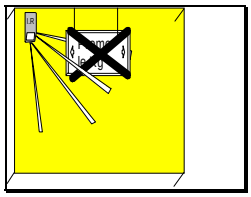
Conseils pratiques pour éviter les fausses alarmes



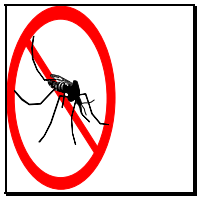
➔ Faites très attention en entrant votre code. Vous disposez seulement de **trois** tentatives! Après cela le terminal sera bloqué pendant 5 mn.



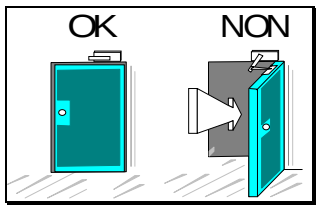
➔ Ne pas placer d'objets volumineux (meubles, cartons, etc.) dans le faisceau de détection des détecteurs.



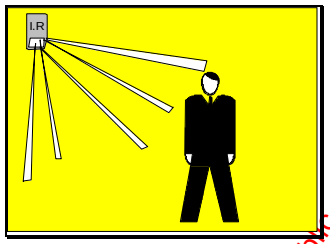
➔ Ne pas installer de panneaux mobiles ou objets oscillants dans le plan des faisceaux du détecteur.



➔ Vérifier que les détecteurs ne sont pas obturés par de la poussière ou des toiles d'araignées. Cela peut être la cause de fausses alarmes.



➔ Assurez-vous d'avoir fermé correctement toutes les portes et fenêtres, de même que les portes intérieures.
Les portes extérieures doivent être fermées correctement, un orage pouvant provoquer leur ouverture partielle et déclencher une alarme.

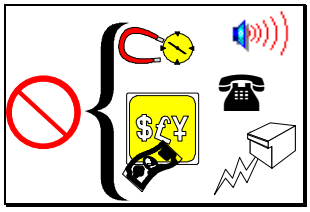


➔ Assurez-vous régulièrement de la portée des détecteurs et ci celle ci n'est pas réduite, suite à la modification de l'implantation des locaux ou autres.

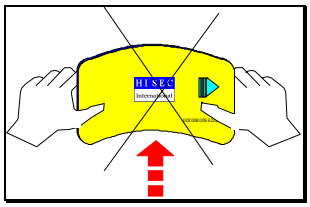
☎ Si vous avez le moindre doute sur le fonctionnement du système HISEC, ou si vous ne comprenez pas la cause d'une alarme, contactez toujours votre installateur.

☑ **Nota:** Si vous êtes raccordé à un Centre de Télésurveillance, il est nécessaire d'appeler ce dernier en cas de fausse alarme. Ceci est important, car le centre de télésurveillance intervient pour toutes les alarmes.

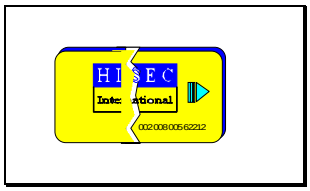
Conseils pratiques pour utiliser le système contrôle d'accès et les badges



Ne pas exposer les badges à des champs magnétiques, ne pas les poser sur les téléphones, haut parleurs, appareils électriques, terminaux de payement de boutique, etc. Les badges peuvent être endommagés et ne plus pouvoir être utilisés. Ne pas laisser les badges proximité (ou mains libres) dans le champ des têtes de lecture.

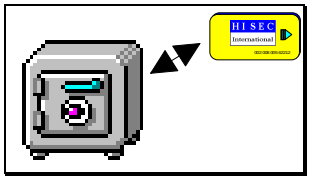


Ne jamais tordre ou plier un badge.



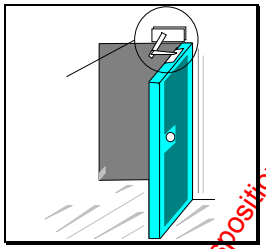
Ne jamais essayer de réparer un badge cassé avec de la bande adhésive. Un badge avec un adhésif peut endommager gravement les têtes de lectures. Pour les mêmes raisons ne jamais personnaliser un badge avec photo, étiquettes, etc. Faire appel à votre installateur ou à une société spécialisée.

Ne pas exposer les badges à des températures élevées.



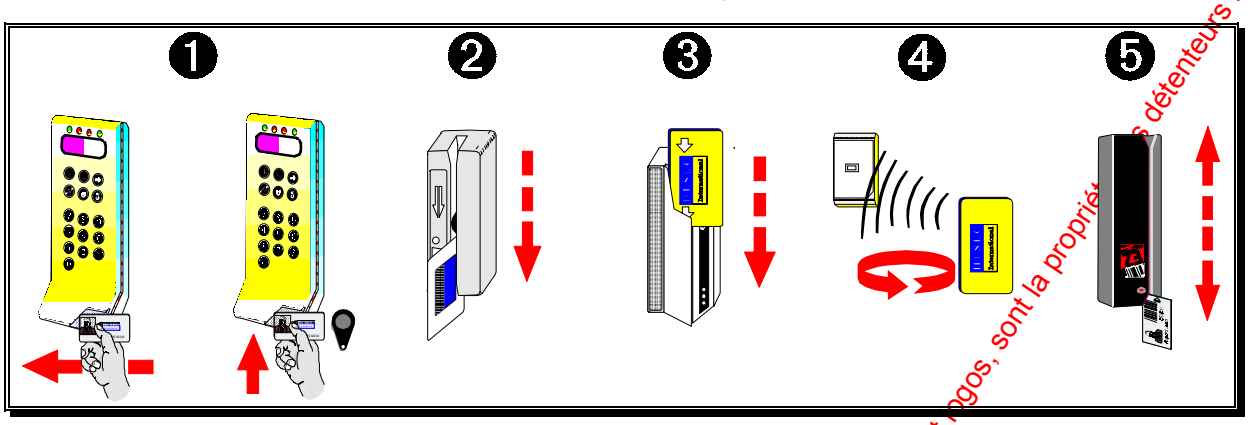
Placez les badges maîtres dans un endroit de sécurité.

Ne jamais confier son badge à une tierce personne.



Vérifiez régulièrement le bon fonctionnement des systèmes de fermeture (grooms) des portes, vérifiez que les portes se referment correctement.

Les Différents sens de lecture des badges



❶ Lecteurs avec tête incorporée: (Magnétique, Wiegand, Proximité)

M Lisez votre badge de droite à gauche; logo dessus (dans le sens de lecture) et piste magnétique dessous pour les badges magnétiques.

W Lisez votre badge de droite à gauche; logo dessus (dans le sens de lecture) et flèches de sens en haut pour les badges Wiegand.

P Lisez votre badge en le présentant dans l'axe et parallèle (le sens n'a pas d'importance) au plan de la tête de lecture, attendez la lecture avant de l'enlever.

❷ Lecteurs avec tête déportée magnétique:

Lisez votre badge de haut en bas; logo à droite (dans le sens de lecture) et piste magnétique à gauche (coté de la flèche indiqué sur la tête de lecture).

❸ Lecteurs avec tête déportée Wiegand:

Fixation Verticale:

Lisez votre badge de haut en bas; logo dessus (dans le sens de lecture indiqué par les flèches sur le badge).

Fixation horizontale:

Lisez votre badge de droite à gauche; logo dessus (dans le sens de lecture indiqué par les flèches sur le badge).

❹ Lecteurs avec tête proximité ou mains libres:

Lisez votre badge en le présentant dans l'axe et parallèle (le sens n'a pas d'importance) au plan de la tête de lecture, attendez la lecture avant de l'enlever.

N'agitez pas votre badge, la lecture est rapide si le badge est présenté lentement, en cas de tentative infructueuse, retirez le badge du champ et recommencez.

❺ Lecteurs avec tête déportée à code barres masqué :

Fixation Verticale:

Lisez votre badge de haut en bas; logo dessus (dans le sens de lecture indiqué par les flèches sur le badge).

Fixation horizontale:

Lisez votre badge de droite à gauche; logo dessus (dans le sens de lecture indiqué par les flèches sur le badge).

1. Intrusion

Chapitre 1: Zones, Territoires, Physique et Logique: Ce que vous devez savoir avant de commencer

1.1 Espaces et "Territoires" utilisateur

L'exploitation du système Intrusion HISEC nécessite de connaître les quelques principes de bases expliqués dans ce chapitre.

Une **Zone** est définie comme une surface "matérielle" de bâtiment, elle comporte en général plusieurs détecteurs. Une zone peut être constituée d'une pièce (par ex. département ventes), mais aussi d'un groupe de pièces (par ex. direction, département ventes et services techniques). Le nombre max. de zones est de 16. Pour les sites importants, cela permet de réaliser des zones comprenant de larges surfaces. La subdivision du bâtiment en Zones est à la charge de l'installateur pendant la phase d'installation du système.

Un **Territoire** est une surface "utilisateur", il est constitué d'une ou plusieurs zones. Le nombre maximum de territoires est de 250, le nombre max. d'Utilisateurs est aussi de 250, plusieurs utilisateurs peuvent partager le même territoire. De cette façon, il est possible, par ex., d'attribuer 50 utilisateurs à un même territoire.

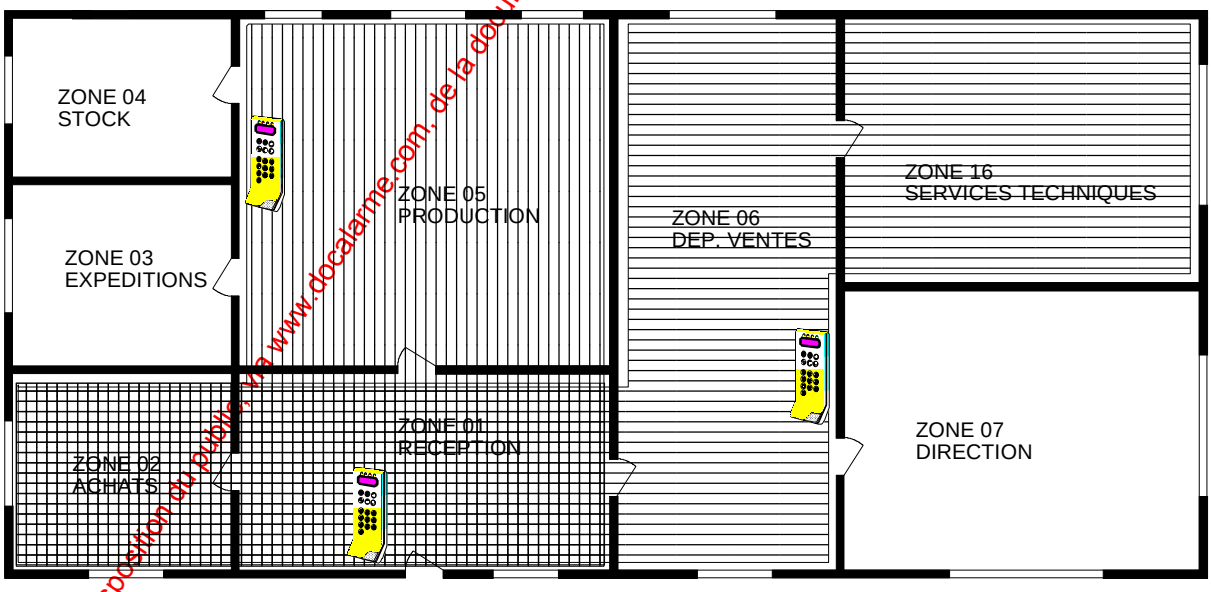
Les employés de la production ont, par exemple, le département production et la réception dans leur territoire. Ces deux parties (zones) constituent alors leur territoire. Si le directeur à accès à l'ensemble du bâtiment, alors son territoire comprendra toutes les zones du bâtiment.

Les différents territoires peuvent se chevaucher (avoir des parties - Zones - communes). Cela permet aux différents utilisateurs de partager les zones communes, par exemple la réception ou le département achats (voir le plan suivant).

Pour l'armement et le désarmement des zones communes, vous disposez d'une solution qui évite que ces zones ne soient armées avant que tout le monde n'ait quitté les locaux.

Toutefois, il existe 2 types de territoires: Physique et Logique. Ces définitions se rapportent aux procédures d'armement et de désarmement (voir le chapitre suivant).

1.2 Plan de masse



Territoire 001: Réception/Achats/Département ventes/Services techniques (Personnel entretien).

Territoire 002: Réception/Achats/Production (Personnel employé production).

Territoire physique : Si les territoires 001 et 002 sont définis comme territoires physiques dans l'exemple ci-dessus, la zone commune 01 fonctionnera de la façon suivante :

Le premier code issu du territoire 001 ou 002 va désarmer le territoire correspondant et aussi la zone commune. Dès qu'un territoire est armé, la zone commune 01 l'est aussi. Si des gens de l'autre territoire doivent partir en traversant la zone commune, cette programmation ne sera pas correcte. Il faudra alors définir ces territoires comme logiques.

Territoire logique : Si les territoires 001 et 002 sont définis comme territoires logiques dans l'exemple ci-dessus, la zone commune 01 fonctionnera de la façon suivante :

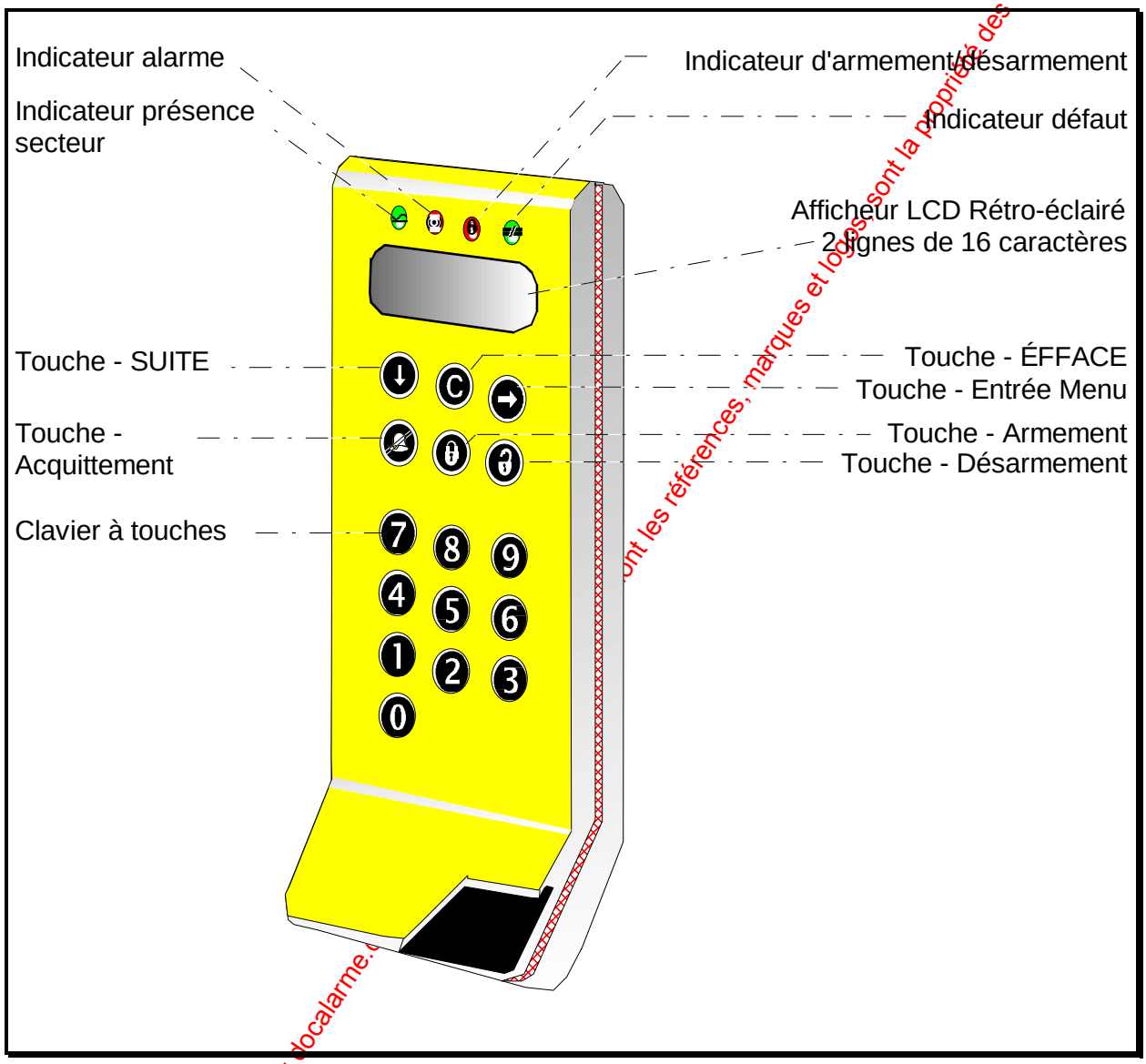
Le premier code issu du territoire 001 ou 002 va désarmer le territoire correspondant et aussi la zone commune. Dès qu'un territoire est armé, le système vérifie l'état de tous les autres territoires de façon à ce que la zone commune 01 ne soit armée que lorsque tous les territoires couvrant cette zone seront armés. Dans cette façon, les personnes peuvent armer leur territoire et quitter le bâtiment. Les personnes d'un autre territoire peuvent se déplacer dans (ou à travers) la zone commune sans déclencher d'alarme. L'armement de la zone 01 aura lieu quand la totalité des territoires sera armée.

De cette façon, il n'y a pas de danger que quelqu'un se trouve enfermé dans les locaux.

☑ Nota : Nous insistons sur la responsabilité individuelle de chaque utilisateur qui est considérable; chaque utilisateur doit toujours armer et désarmer personnellement, étant donné que le système enregistre chaque opération et la personne qui l'a effectuée.

Chapitre 2: Le Terminal Intrusion

2.1 Description du terminal



2.2 Le Terminal

Le terminal du système Intrusion HISEC est l'unité d'exploitation utilisée pour les avertissements, les opérations, et les traitements. Il est composé d'un afficheur, 4 LED, 6 touches de fonctions et 10 touches numériques.

2.2.1 L'afficheur

L'afficheur possède 2 lignes de 16 caractères chacune. Le texte contenu donne aussi bien les informations d'état du système que les instructions à l'opérateur.

Chaque fois que le terminal est utilisé, l'afficheur est éclairé. Il s'éteindra automatiquement au bout de 2 minutes après la dernière action ou en effectuant une fin de session en appuyant sur la touche C.

2.2.2 Les Led's de fonctions

Voyant Secteur (Vert) : Ce voyant allumé en permanence indique que le secteur est présent; le clignotement indiquant un défaut de l'alimentation secteur, le système fonctionne alors sur ses batteries.

Voyant Alarme (Rouge) : Allumé après une entrée en session, il indique la présence d'une alarme dans le territoire du terminal (transmission et/ou sirène a été déclenchée); laquelle apparaît sur l'afficheur. Le voyant s'éteint quand tous les messages d'alarme sont acquittés.

Voyant état d'armement (Jaune) : Allumé après une entrée en session quand toutes les zones du code utilisé sont armées (code/territoire armé), ne pas confondre cette indication avec le message "SYSTEME ARME" apparaissant sur l'afficheur, qui lui indique que toutes les zones du système sont armées.

Voyant défaut système (Jaune) : Allumé après une entrée en session, il indique la présence d'un défaut sur le territoire du terminal ; lequel apparaît sur l'afficheur. Le voyant s'éteint quand tous les messages de défaut sont acquittés.

2.2.3 Les Touches de fonction

Cette touche est utilisée pour armer.

Cette touche est utilisée pour désarmer et éjecter.

Cette touche est utilisée pour acquitter un(e) défaut/alarme et aussi pour se déplacer à droite dans les menus de programmation.

Cette touche est utilisée pour sélectionner les fonctions des menus affichés.

Cette touche est utilisée pour avancer dans les différents menus.

Cette touche est utilisée pour revenir en arrière ou quitter une session.

2.2.4 Les Touches numériques

Le clavier est composé des touches numériques de 0 à 9 utilisées pour le code etc. et des 6 touches de fonctions.

Buzzer:

Utilisé pour indiquer de façon sonore un défaut ou une alarme et les écoulements des temporisations d'entrée-sortie. Aussi activé pour un temps bref pour indiquer les erreurs de manipulation ou pour attirer l'attention de l'utilisateur.

Chapitre 3: Manipulations du système: Quelles sont vos possibilités ?

3.1 Les niveaux de priorités: Un niveau de droit pour chacun

Les possibilités et autorisations d'exploitation du système HISEC ne sont pas les mêmes pour tous les opérateurs, c'est pourquoi les opérateurs ont été divisés en 5 catégories. Ces catégories sont appelées des Niveaux de Priorité et sont numérotés de 0 à 4. Ils sont indiqués par un P(Priorité) et un chiffre. Un entretien avec votre installateur a permis, au démarrage du système, de déterminer quels opérateurs auront quels niveaux de priorité. Plus le niveau est élevé (0 à 2) et plus l'opérateur a de possibilités sur le système.

Consultez le chapitre 3.2 pour connaître les possibilités des différents niveaux d'opérateur sur le système HISEC Intrusion.

C'est l'entrée de votre code personnel à 6 chiffres qui vous donne accès aux menus qui vous sont autorisés.

3.1.1 P0: L'utilisateur standard

Code opérateur autorisant l'armement/désarmement, l'acquittement des alarmes/défauts (sauf sabotage et quelques défauts système) et le test des voyants.

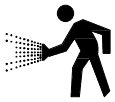
3.1.2 P1: L'utilisateur responsable système

Code directeur autorisant la plupart des possibilités d'exploitation, tests, changement de date & heure et changement de son propre code et des codes P0.

3.1.3 P2: L'utilisateur superviseur

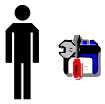
Code directeur maître autorisant toutes sortes d'exploitation - excepté le changement des codes P3-P4 et la programmation du système.

3.1.4 P3: L'Intervenant



Code intervenant ayant la plupart des possibilités d'exploitation - sauf la programmation du système et quelques fonctions de test. Le code est accepté 2 minutes après un déclenchement d'alarme/défaut, et peut être utilisé jusqu'à ce que tous les messages soit acquittés.

3.1.5 P4: Le technicien de maintenance



Code technicien autorisant toutes sortes d'exploitations - sauf le changement des codes P0-P1-P2. Le code est accepté 2 minutes après une condition d'alarme/défaut, et peut être utilisé jusqu'à l'acquittement de tous les messages. Un opérateur P1-P2 peut, en entrant dans le *Menu 50*, autoriser une seule utilisation du code technicien - jusqu'à la fin de session. Quand un code P4 utilise le *Menu 50*, le système passe en mode maintenance, autorisant un usage illimité du code technicien pour un acquittement général des alarmes/défauts, test du système etc, jusqu'à la sortie de ce mode par le *Menu 51* (tous les codes peuvent réaliser cette fonction). Le mode de maintenance est indiqué par un message de défaut (à l'affichage) et une sortie de transmission "problème" activée (automatiquement acquittée par le *Menu 51*) et empêche les déclenchements d'alarme.

Nota: Il est très important de quitter le mode maintenance après chaque usage de celui-ci, au moyen du **Menu 51 FIN MODE MAINT.?**. Si vous omettez cela, le système vous le rappelle au moyen d'un défaut système sur l'afficheur.

3.2 Liste des niveaux de priorité du système intrusion HISEC

		P0	P1	P2	P3	P4
Désarmement	Propre territoire	OUI	OUI	OUI	OUI	OUI
	Armement Auto. de territoire	NON	NON	OUI	NON	OUI
	Autre territoire	NON	NON	NON	NON	NON
Armement	Propre territoire	OUI	OUI	OUI	OUI	OUI
	Autre territoire	OUI	OUI	OUI	OUI	OUI
	Ejection de détecteurs	OUI *	OUI *	OUI	OUI	OUI
	* Pas plus d'un par zone dans son propre territoire					
Acquittement	Alarme (intrusion)	OUI	OUI	OUI	OUI	OUI
	Alarme sabotage	NON	NON	OUI	OUI	OUI
	Alarme de hold-up	NON	NON	OUI	OUI	OUI
	Alarme technique	OUI	OUI	OUI	OUI	OUI
	Alarme incendie	OUI	OUI	OUI	OUI	OUI
	Batterie/Secteur 1H	OUI	OUI	OUI	OUI	OUI
	Défauts système	NON	NON	NON	OUI	OUI
Menu 20	**Etat système**					
Menu 21	Affichage état territoire	OUI	OUI	OUI	OUI	OUI
Menu 22	Affichage état zone	OUI	OUI	OUI	OUI	OUI
Menu 23	Affichage état détecteur	OUI	OUI	OUI	OUI	OUI
Menu 25	Affichage événement	NON	OUI	OUI	OUI	OUI
Menu 26	Impression événement	NON	OUI	OUI	OUI	OUI
Menu 27	Impression d'état	NON	OUI	OUI	OUI	OUI
menu 28	Impression de programmation	NON	NON	OUI	NON	OUI
Menu 29	Affichage compteur d'alarmes	NON	NON	OUI	NON	OUI
Menu 30	**Test système**					
Menu 31	Tests voyants	OUI	OUI	OUI	OUI	OUI
Menu 32	Tests détecteurs	NON	OUI	OUI	OUI	OUI
Menu 33	Test batterie	NON	OUI	OUI	OUI	OUI
Menu 34	Test zones	NON	OUI	OUI	OUI	OUI
Menu 35	Test entrées	NON	NON	NON	NON	OUI
Menu 36	Test sorties	NON	NON	OUI	NON	OUI
Menu 37	Test imprimante	NON	OUI	OUI	OUI	OUI
Menu 38	Test sirènes	NON	OUI	OUI	OUI	OUI
Menu 40	**Programmation**					
Menu 41	Programmation date et heure	NON	OUI	OUI	OUI	OUI
Menu 42	Changement codes d'accès	NON	OUI	OUI	NON	OUI
Menu 50	**Programmation système**					
Menu 50	Autorisation code de maintenance	NON	OUI	OUI	NON	NON
	Activation mode de maintenance	NON	NON	NON	NON	OUI
	Acquit global alarmes/défauts	NON	OUI	OUI	OUI	OUI
Menu 51	Annulation mode de maintenance	OUI	OUI	OUI	OUI	OUI
Menu 55	Programmation Armement Auto	NON	NON	OUI	NON	OUI
Menu 56	Programmation Jours de Congés	NON	NON	OUI	NON	OUI

Chapitre 4: Menus: Utilisation pas à pas

4.1 Les menus

La procédure d'exploitation est basée sur des menus. Toutes les opérations sont affichées et l'opérateur répond simplement aux questions posées au moyen des touches correspondant à OUI et NON. Chaque menu est défini par un nombre (00 à 99), ces numéros ne sont pas visibles sur l'afficheur.

Le programme inclut un menu principal pour les opérations journalières et 3 sous-menus pour l'affichage ou le changement des états, le test du système et la programmation. Toute opération nécessite l'entrée d'un code à 6 chiffres, les menus accessibles dépendant de la priorité du code (5 niveaux).

☒ *Nota : Seuls les Menus présentants un intérêt pour l'utilisateur final sont décrits dans ce manuel.*

☞ La description de menus sera faite au chapitre 5 : **Description des Menus Intrusion**.

4.1.1 Les menus Principaux 00, 10, 20, 30, 40 et 50

- Le **Menu 00** est l'affichage au repos (hors session), la date et l'heure sont affichées, c'est aussi l'affichage normal après une utilisation (appui sur la touche Ⓒ ou automatiquement après 2 minutes sans manipulation). En cas de présence d'anciens messages d'alarme/défaut (l'opérateur n'ayant pas effectué d'acquittement) le Buzzer sonne pendant 15 secondes environ en fin de session.
- Le **Menu 10** est le menu général d'**Armement** et **Désarmement**. Apres avoir entré votre code personnel c'est le premier menu affiché, il permet de connaître l'état de son propre territoire et d'armer (désarmer) celui-ci.
- Le **Menu 20** est le menu général d'**Etats**. Après avoir entré votre code personnel et Menu 20, vous pouvez visualiser l'état du système. C'est à dire l'état des territoires, zones, détecteurs et sorties. De plus, il est possible de visualiser et d'imprimer l'historique (les 1000 derniers événements).
- Le **Menu 30** est le menu général de **Test**. Après avoir entré votre code personnel et Menu 30, vous pouvez tester le système. C'est à dire tester les voyants du terminal, les détecteurs, l'imprimante et les sorties de types sirènes, voyants, transmetteurs.
- Le **Menu 40** est le menu de **Programmation**. Après avoir entré votre code personnel et Menu 40, vous pouvez programmer le système. La plupart des menus existants dans cette catégorie sont réservés à votre installateur, toutefois; vous pouvez programmer l'heure et la date, ainsi que changer les codes personnels, évidemment en fonction de votre priorité.
- Le **Menu 50** est le menu de **Programmation système**. Après avoir entré votre code personnel et Menu 50, vous pouvez programmer le système. Ce menu vous permet d'autoriser (ou de bloquer) l'entrée du code technicien, ainsi que programmer les programmes d'armement automatique et les périodes de congés.

4.1.2 Les Sous Menus

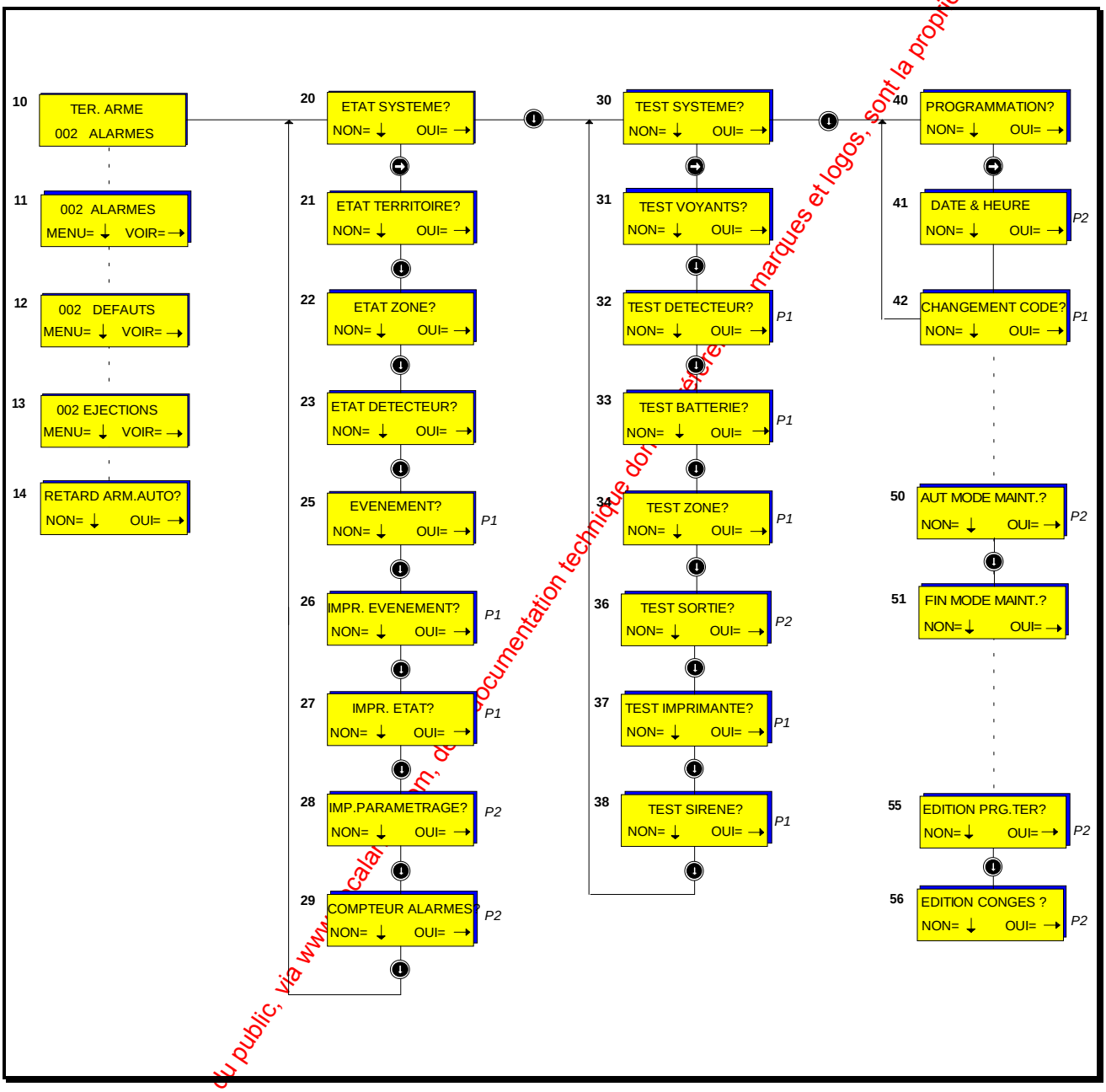
Les menus principaux ne sont en fait que des "En têtes" pour accéder aux sous-menus. Les sous menus déroulants permettent d'avoir un aperçu des possibilités offertes et les instructions opératoires.

Les sous Menus 11 à 14 sont relatifs, directement ou indirectement, au traitement d'alarme (acquittement) et à la visualisation des alarmes, défauts, détecteurs éjectés ou encore à la demande de retard à l'armement automatique. Ces menus peuvent être appelés directement par leurs numéros ou en appuyant sur la touche ⓓ ou encore de façon automatique toutes les 5 secondes, cette fonction est appelée défilement automatique (voir chapitre 6.3).

Les autres menus peuvent (en fonction du niveau de priorité) être appelés directement. De cette façon le numéro de menu sera tapé directement après avoir entré son code personnel. Les Menus déroulants vous permettent d'avoir accès aux menus simplement au moyen des réponses aux questions par OUI ou NON, le NON vous propose automatiquement le prochain menu accessible. Pour revenir au menu principal on utilisera la touche Ⓒ.

☞ Se reporter aux chapitres 3.2 "Liste des niveaux de priorité" et 4.2 pour le "Panorama des Menus Intrusion".

4.2 Panorama des Menus Intrusion

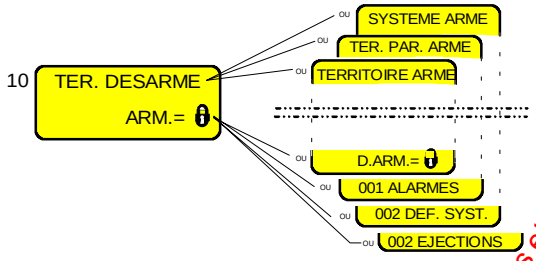


Chapitre 5: Description des Menus Intrusion

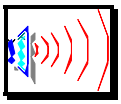
Dans ce chapitre tous les menus utilisateurs seront décrits en détail.

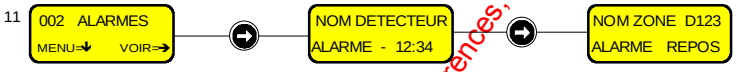
Voir les conditions d'utilisation de ces menus au chapitre 3.2 "Liste des niveaux de priorités".

5.1 Menu Principal 10



Menu 11

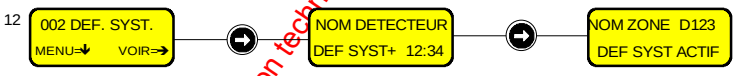




Si des alarmes ont eu lieu sur l'installation, elles seront affichées à l'entrée en session dans le Menu 11.

☒ Vous pouvez aussi appeler ce menu en tapant directement son N°.

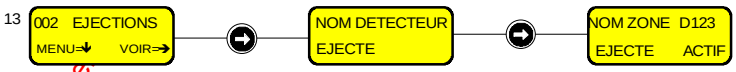
Menu 12



Si des défauts systèmes sont présents à l'entrée en session, ils seront affichés au moyen du Menu 12.

☒ Vous pouvez aussi appeler ce menu en tapant directement son N°.

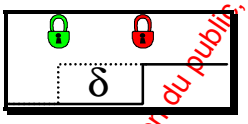
Menu 13

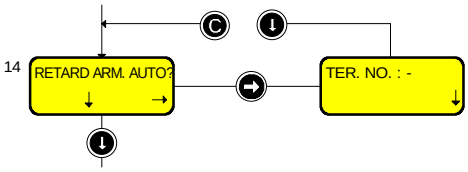


Si des éjections sont présentes à l'entrée en session, elles seront affichées au moyen du Menu 13.

☒ Vous pouvez aussi appeler ce menu en tapant directement son N°.

Menu 14



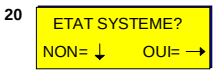


Si le système est programmé avec un armement automatique, l'heure d'armement automatique peut être repoussée - **1 seule fois** - pour une période déterminée à la programmation (Menu 55).

Vous devez préciser le N° du territoire (1 à 8) dont vous voulez retarder l'armement, suivi par la touche ⓘ.

☒ Vous pouvez aussi appeler ce menu en tapant directement son N°.

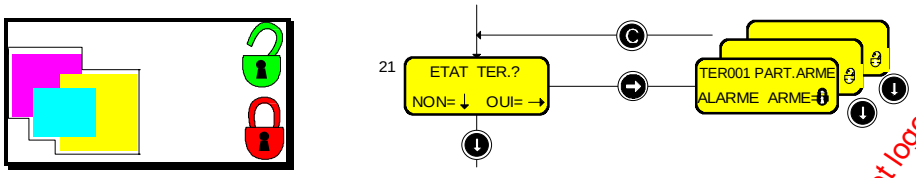
5.2 Menu Principal 20



Ce menu vous permet de visualiser l'état et d'armer (désarmer) les zones, territoires, circuits.

Il permet également de consulter l'historique et de l'imprimer, d'imprimer l'état de l'installation et la programmation et de consulter le compteur des alarmes.

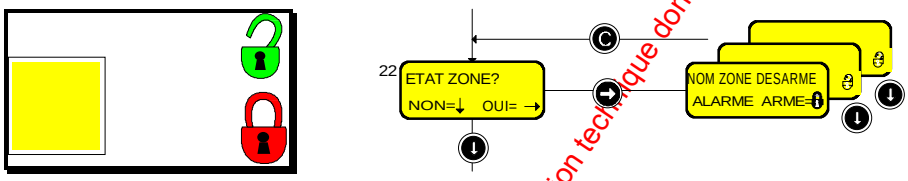
Menu 21



Le Menu 21 vous permet de connaître (visualiser) l'état de tous les territoires (armement, alarmes, etc.) du système. Ce menu vous permet également d'armer (et désarmer) son propre territoire. Tous les autres territoires pourront être armés mais non désarmés. La touche ↓ vous permet de passer du territoire affiché au suivant.

☑ Nota: En appuyant directement sur la touche →, le texte **Nouv Num.** vous permet de choisir n'importe quel territoire (toujours 3 chiffres).

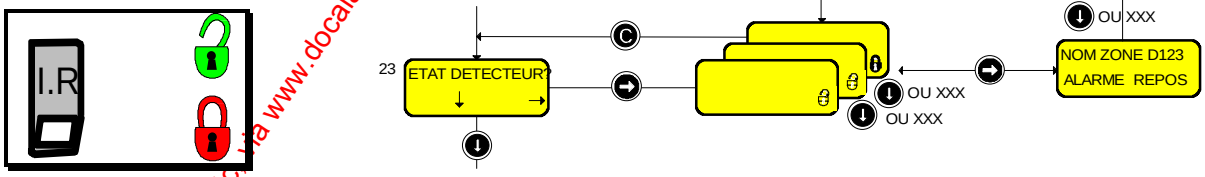
Menu 22



Le Menu 22 vous permet de connaître (visualiser) l'état de toutes les Zones (armement, alarmes, etc.) du système. Ce menu vous permet également d'armer (et désarmer) les zones appartenant à son propre territoire. Toutes les autres zones pourront être armées mais non désarmées. La touche ↓ vous permet de passer de la zone affichée à la suivante.

☑ Nota: En appuyant directement sur la touche →, le texte **Nouv Num.** vous permet de choisir n'importe quelle zone (toujours 3 chiffres).

Menu 23

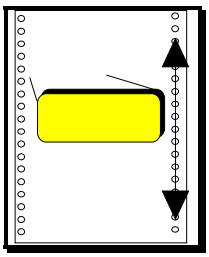


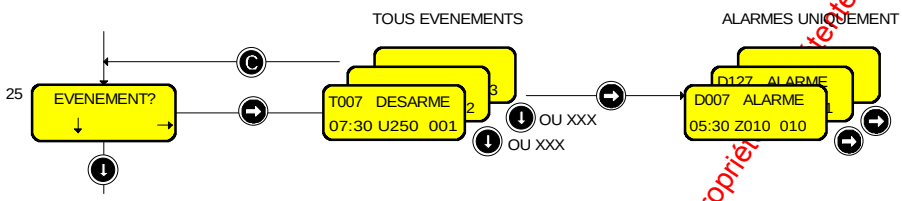
Le Menu 23 vous permet de connaître (visualiser) l'état (armement, alarmes, éjection, etc.) de tous les Circuits (Détecteurs) ou adresses du système. Ce menu vous permet également d'armer, désarmer et d'éjecter les circuits de son propre territoire. Tous les autres circuits pourront être armés (*voir remarque*) mais non désarmés. La touche ↓ vous permet de passer du circuit affiché au suivant.

☑ Nota: En appuyant directement sur la touche →, le nom de la zone et le numéro (adresse) du détecteur seront affichés. Il vous est possible d'entrer directement le numéro du détecteur désiré en tapant son adresse (toujours 3 chiffres).

Remarque: Tous les circuits ne sont pas éjectables; de plus les utilsateurs de priorité P0 et P1 ne peuvent pas éjecter plus d'un détecteur par zone.

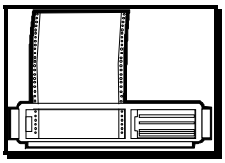
Menu 25

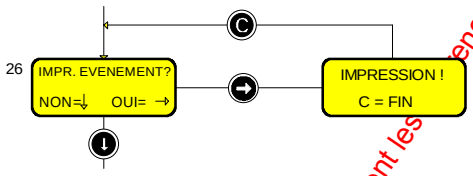




L'historique du système Intrusion a une capacité de 1000 événements. Ces événements peuvent être imprimés (Menu 26), mais également visualisés sur l'afficheur des terminaux. L'événement le plus récent est affiché en premier. La touche ⬇ permet de passer d'un événement à un autre. Si vous voulez visualiser uniquement les alarmes, appuyez sur la touche ➡, chaque nouvel appui sur cette touche passera à l'alarme suivante. Un appui sur la touche ⬇, ré-affiche de nouveau tous les événements. Il est également possible d'entrer directement le numéro d'ordre des événements (toujours avec 3 chiffres).
Pour quitter cette liste, utilisez la touche C.

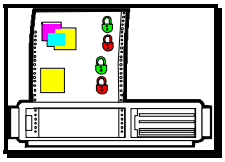
Menu 26

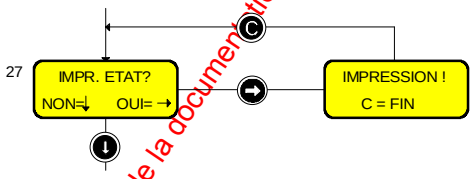




L'historique du système Intrusion (1000 événements) peut être visualisé sur les terminaux (Menu 25), mais également imprimé par le Menu 26.
Un événement est imprimé toutes les 2 secondes environ.
Pour arrêter cette impression, utilisez la touche C.

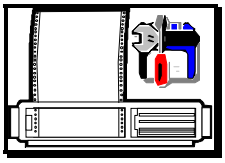
Menu 27

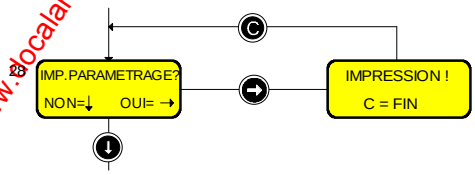




Le Menu 27 vous permet d'imprimer l'état (actuel) complet de l'installation, territoires, zones, détecteurs avec leur état d'armement, d'alarme et d'éjection.

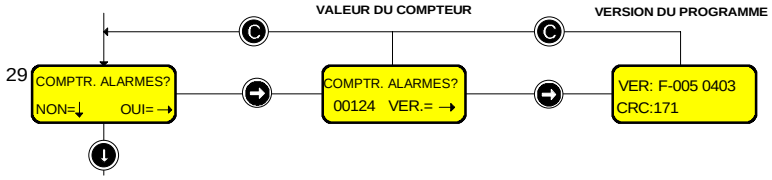
Menu 28





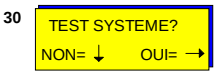
Le Menu 28 vous permet d'imprimer la totalité de la programmation de l'installation, ce menu est en principe destiné aux personnes susceptibles de l'interpréter, c'est à dire, technicien, responsable de sécurité, utilisateur superviseur.

Menu 29



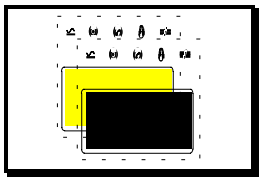
Le Menu 29 affiche le **compteur des alarmes** externes, de plus la **version** logiciel est accessible dans ce menu. Comme pour le menu 28, les informations données par ce Menu sont destinées à votre installateur ou au superviseur du système.

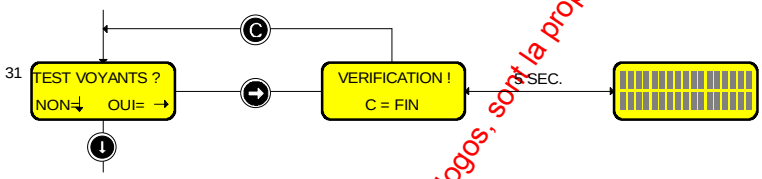
5.3 Menu Principal 30



Le test du système consiste en l'ensemble des points suivants: Test des terminaux, détecteurs, batteries, zones, sorties, imprimantes, sirènes.

Menu 31

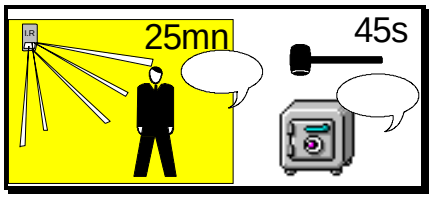


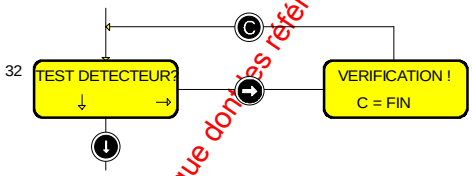


Le menu 31 vous permet de tester les Led's et l'afficheur du terminal. Pendant toute la durée du test les Led's clignoteront et l'afficheur sera noircis toutes les 5 secondes.

Pour quitter ce test, utilisez la touche Ⓒ

Menu 32





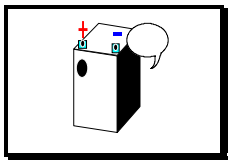
Le menu 32 vous permet de tester les détecteurs infrarouges (ou à ultrasons). Le test sera réalisé dans les zones communes au terminal. Vous disposez de 25 minutes pour effectuer ce test, l'affichage reste inchangé durant cette période.

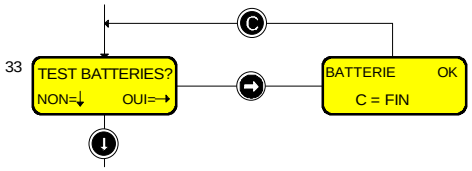
Les détecteurs sismiques équipés d'un système de test incorporé peuvent être testés au moyen de ce menu. La durée du test est de 45 secondes, pendant cette période le détecteur doit passer en alarme. Si ce n'est pas le cas, le détecteur sera affiché en défaut système.

Pour quitter ce test, utilisez la touche Ⓒ

☑ Nota: Les détecteurs que vous voulez tester devront être désarmés.

Menu 33



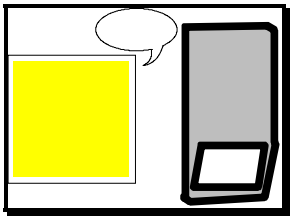


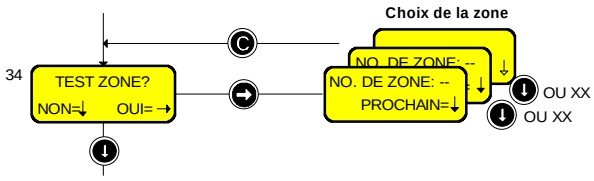
Le Menu 33 vous permet de tester les batteries de sauvegarde de l'alimentation. Quand le test démarre, le **circuit de charge de batterie** est **déconnecté** pendant 15 secondes, et l'alimentation de l'installation complète est alors fournie par les batteries. Une seconde plus tard, la condition des batteries est affichée (**OK** ou **DEFAUT**). Cette procédure est répétée toutes les 16 secondes jusqu'à l'effacement automatique (2 minutes).

Pour quitter ce test, utilisez la touche Ⓒ

☑ Nota: Un message de défaut batterie ne peut être acquitté tant que les batteries n'ont pas été réparées ou changées.

Menu 34





Le Menu 34 vous permet de tester les Zones. Après l'entrée de son **numéro** (01 à 16), la zone est passée à l'état de test. Pendant ce test, la réaction d'alarme est bloquée, une condition d'alarme est indiquée par l'activation du **Buzzer interne** pendant environ 1 seconde. Toutes les activations d'entrée (détecteurs) peuvent être répétées et sont enregistrées dans l'**historique**.

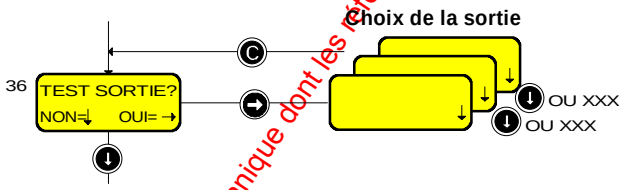
Ce test permet de déterminer la cause d'une éventuelle alarme, sans provoquer une alarme réelle.

Pour sélectionner **une autre zone**, il vous suffit de préciser son **numéro**, ou bien de presser la touche ⓓ pour afficher la zone suivante. Ce test n'est pas limité en durée.

Pour quitter ce test, utilisez la touche Ⓒ

☑ Nota: Les détecteurs de type Sabotage, Hold-up et Incendie ne peuvent pas être testés.

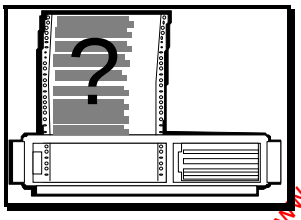
Menu 36

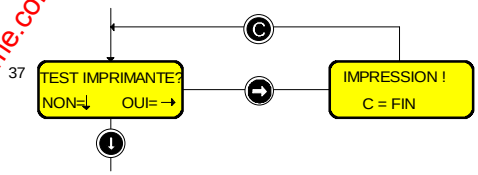


Le Menu 36 vous permet de tester les sorties (sirènes , transmetteurs, voyant d'un synoptique, etc.). Vous devez entrer un **nombre à 3 chiffres** (adresse) pour **activer** la sortie. Pour sélectionner une autre sortie il vous suffit de préciser son **numéro**, ou bien de presser la touche ⓓ pour afficher la sortie suivante. Ce test n'est pas limité en durée.

Pour quitter ce test, utilisez la touche Ⓒ

Menu 37

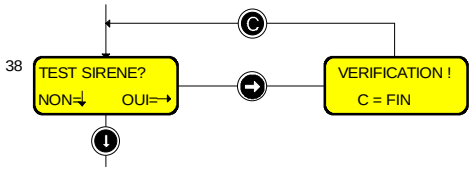




Le menu 37 vous permet de demander un test de l'imprimante.

Pour arrêter ce test utilisez la touche Ⓒ

Menu 38

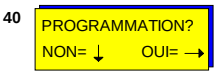


Le menu 38 vous permet de tester les sirènes et autres avertisseurs.

Seules les sorties sirènes "communes" -Z00- et les sorties sirènes d'une zone appartenant à votre code et au terminal seront activées.

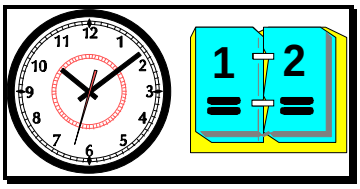
Pour arrêter ce test, utilisez la touche Ⓒ

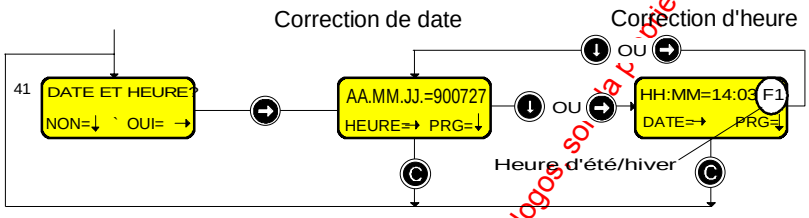
5.4 Menu Principal 40



Ce menu vous permet de changer la date et l'heure et de modifier les codes personnel.

Menu 41



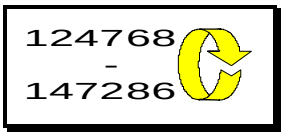


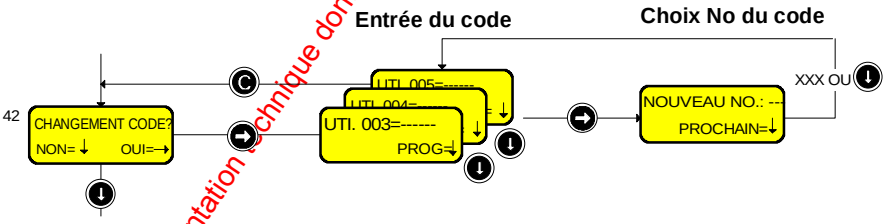
Le menu 41 vous permet de changer la date et l'heure du système intrusion. Vous devez entrer dans l'ordre l'**année** (AA), le **mois** (MM), et la **date** (JJ). L'écran suivant vous permet de modifier l'**heure** (HH) et **minutes** (MM).

Si la date ne doit pas être modifiée, il vous est possible d'accéder directement à l'écran de l'heure au moyen de la touche .

☑ Nota: Les indications **F0** et **F1** sont relatives au passage automatique Heure d'été et Heure d'Hiver; **F0** pas de changement et **F1** Changement automatique.

Menu 42





Le Menu 42 vous permet de modifier les codes personnels. Ces modifications ne sont possibles qu'en fonction de votre propre niveau de priorité.


Un utilisateur P0 ne peut pas changer de code.


Un utilisateur P1 ne peut changer que son propre code et ceux de priorité P0.


Un utilisateur P2 peut changer les codes des priorités P0, P1, P2.


Un utilisateur P3 ne peut pas changer de code.


Un utilisateur P4 peut changer les codes des priorités P3, P4.

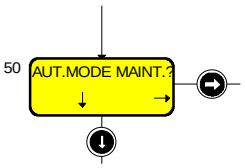
Chaque Code Personnel est identifié par un numéro d'utilisateur dans le système intrusion, ce numéro doit être entré avant de changer le code. Pour changer un code, vous devez entrer un nombre à 6 chiffres, le code sera refusé s'il est similaire à un déjà existant (4 chiffres identiques aux mêmes positions). Le nouveau code possède la même priorité que le précédent.


Le menu 42 sera utilisé pour effacer les utilisateurs indésirables au système. Cela sera réalisé en remplaçant leurs codes par **000000**.

5.5 Menu Principal 50

Ce menu vous permet d'autoriser (ou bloquer) le mode maintenance, de définir les programmes hebdomadaires d'armement automatique et les périodes de congés.

Menu 50



Le Menu 50 vous permet d'autoriser l'accès du système Intrusion au technicien de maintenance.

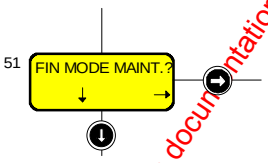
Ce Menu autorise l'entrée du Code maintenance pour **une seule** entrée en session, en utilisant la procédure suivante:

- Entrez votre Code personnel.
- Tapez **50** et tapez la touche ➡ pour répondre OUI.
- Tapez la touche C 3 fois pour effectuer une fin de session.

Après l'entrée de son code, le technicien peut, grâce à ce même menu, passer le système en mode maintenance. De cette façon, il aura accès de nouveau après chaque fin de session.

☑ Nota: Seules les priorités P1 et P2 peuvent avoir accès au Menu 50. Après une alarme, le technicien a accès directement au menu 50 sans autorisation.

Menu 51

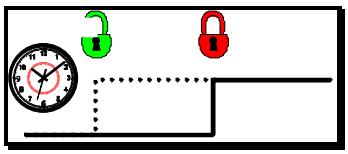


Après une utilisation du Menu 50, il est très important de quitter le mode maintenance en utilisant le Menu 51. Au cas contraire, les indicateurs d'alarmes et sirènes resteront bloqués. La procédure est la suivante:

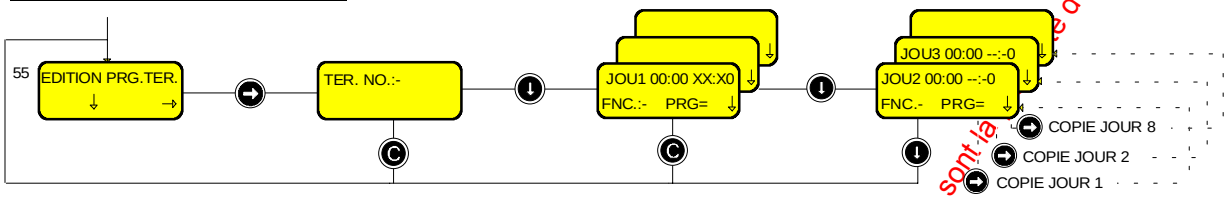
- Entrez votre Code personnel.
- Tapez **51** et tapez la touche ➡ pour répondre OUI.
- Tapez la touche C 3 fois pour effectuer une fin de session.

☑ Nota: Toutes les priorités peuvent avoir accès au Menu 51.

Menu 55



Si votre système utilise l'armement (désarmement) automatique, vous pouvez programmer les programmes hebdomadaires de contrôle au moyen du Menu 55.



Un programme hebdomadaire est composé des 7 jours normaux (Lundi = jour 1) et de 2 jours spéciaux (8 et 9) en liaison avec la liste des congés.
Un chiffre permet de choisir le numéro de territoire (1-8) que le programme hebdomadaire contrôlera. Après cela, le jour 1 est affiché avec l'heure de début 00:00. La première période sera de 00:00 à xx:x0 où x est à entrer. L'heure xx:x0 sera automatiquement transférée vers l'heure de début de la prochaine période pour le jour 1, afin de vous éviter les "trous" ou "chevauchements" de période. Un jour est terminé quand 24:00 est programmé comme heure de fin de période. Le jour 2 est alors affiché, l'utilisation de la touche → à cet instant, permet de faire une copie du jour précédent dans ce jour.

☑ *<u>Limites:</u> Les pas de programmation sont de 10 minutes uniquement, un maximum de 8 périodes est programmable par jour dans chaque programme.*

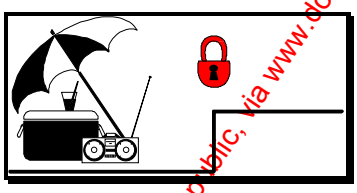
Un programme hebdomadaire d'armement automatique sera effacé en programmant une période allant de 00:00 à 00:00.

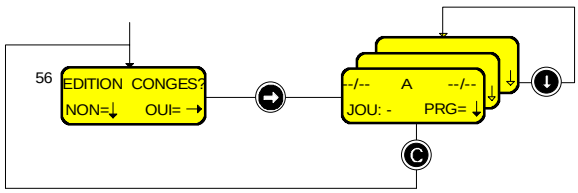
Le paramètre FNC permet d'attribuer une fonction à chaque plage. Une des fonctions suivantes peut être attribuée aux périodes horaires des programmes :

• FNC 1	Armement de territoire au début de la période ou armement à la fin de la période si un retard a été demandé sur l'un des terminaux, au moyen du Menu 14.
• FNC 2	Armement de territoire au début de la période.
• FNC 3	Armement de territoire au début de la période et possibilité de désarmement manuel à la fin de la période.
• FNC 4	Désarmement de territoire au début de la période.
• FNC 5	Pas de changement.

Nota : Si vous avez le moindre doute sur votre programmation, n'hésitez pas à consulter votre installateur, votre sécurité est en jeu, étant donné que l'armement automatique est une des pièces maîtresses du système.

Menu 56





Le Menu 56 vous permet de programmer des périodes d'exception d'armement (désarmement) automatique pendant les périodes de congés. Vous pouvez, par exemple, armer le système pour une période ininterrompue de deux semaines.

Le nombre max. de périodes est de 25, chaque période est définie par une **date de début** et une **date de fin** qui sont inclues dans la période**.**

Le paramètre **JOU:**_ permet de préciser la liaison avec les programmes hebdomadaires des jours standards 1 à 7 ou des jours spéciaux 8 et 9.

☑ Nota : Il n'est pas possible de préciser l'année, c'est pourquoi, il est très important de faire attention aux jours fériés de date variable. Ne pas oublier de les effacer après utilisation pour l'année suivante.

Chapitre 6: Utilisation quotidienne du système Intrusion

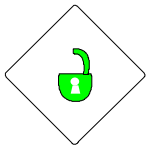
6.1 Armement :

- Entrez votre code personnel---------- ex : ☞ 1 5 2 7 9 2
- L'afficheur indique:---------- TER. DESARME ARM.= 0 *OU* TER. PAR. ARME ARM.= 0
- Appuyez sur la touche ---------- 0
- L'afficheur indique:---------- TERRITOIRE ARME SORTEZ SVP *OU* SYSTEME ARME SORTEZ SVP
- Appuyez sur la touche ---------- C
- Quittez la pièce.

Nota : La dernière personne quittant les locaux doit toujours voir le texte **SYSTEME ARME**. Si ce n'est pas le cas, le système n'est pas alors complètement armé.

☑ Vous pouvez aussi armer séparément les zones si dans l'un des écrans représentés ci-dessus, vous appuyez sur la touche →, seules les zones de **votre** territoire seront accessibles.

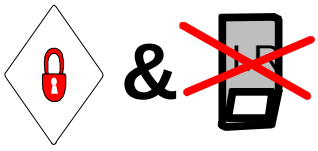
6.2 Désarmement :



- Entrez votre code personnel---------- ex : ☞ 1 5 2 7 9 2
- L'afficheur indique:---------- TERRITOIRE ARME D.ARM.= *OU* TER. PAR. ARME ARM.= 0 *OU* SYSTEME ARME D.ARM.=
- Appuyez sur la touche ---------- 0
- L'afficheur indique:---------- TER. DESARME ARM.= 0
- Appuyer sur la touche---------- C

☑ Nota : Vous pouvez aussi désarmer séparément les zones si dans l'un des écrans représentés ci-dessus vous appuyez sur la touche →, seules les zones de **votre** territoire seront accessibles.

6.3 Armement avec Ejection:



L'éjection de détecteurs est un moyen d'isoler un élément de façon temporaire. Cela peut être nécessaire pendant des modifications d'implantation ou de travaux. Les priorités P0 et P1 peuvent éjecter un seul détecteur par zone dans leur propre territoire. Les priorités P2, P3 et P4 peuvent éjecter les détecteurs sans limitation.

- Entrez votre code personnel---------- ex : ☞ ❶ ❺ ❷ ❼ ❾ ❷
- L'afficheur indique:---------- TER. DESARME ARM.= 0 *OU* TER. PAR. ARME ARM.= 0
- Appuyez sur la touche ----------

☒ **Si un détecteur de votre territoire est actif la condition sera indiquée comme suit:**

- L'afficheur indique:---------- NOM DETECTEUR DEF. ARM. → NOMZONE A123 DEF. ARM. ACTIF
- Appuyez sur la touche ---------- pour éjecter le détecteur.
- L'afficheur indique:---------- TER. DESARME 001 EJECTIONS *OU* TER. PAR. ARME 001 EJECTIONS
- Appuyez sur la touche ---------- pour armer le territoire.
- L'afficheur indique:---------- TERRITOIRE ARME 001 EJECTIONS *OU* SYSTEME ARME 001 EJECTIONS
- Appuyez sur la touche ----------
- Quittez la pièce.

Le détecteur est éjecté et votre territoire est armé.

Toutes les éjections seront automatiquement annulées au prochain désarmement du système.

Remarque: Tous les circuits ne sont pas éjectables, de plus les utilisateurs de priorité P0 et P1 ne peuvent pas éjecter plus d'un détecteur par zone.

☑ Nota : En accord avec votre installateur, vous pouvez décider quels seront les points (détecteurs) éjectables.

6.4 Acquittement d'alarme (uniquement dans votre territoire)

- Appuyez sur la touche C, pour arrêter le Buzzer du terminal.
- Entrez votre code personnel--- ---------- ex : 1 5 2 7 9 2

L'afficheur indique: -------- TERRITOIRE ARME / 001 ALARMES

- Appuyez sur la touche ---- L'afficheur indique: -------- TER. DESARME / 001 ALARMES
- Appuyez sur la touche ---- L'afficheur indique: -------- 001 ALARMES / MENU=↓ VOIR=→
- Appuyez sur la touche ---- L'afficheur indique: -------- NOM DETECTEUR / ALARME - 12:34 → NOM ZONE D123 / ALARME REPOS
- Appuyez sur la touche ---- L'afficheur indique: -------- 000 ALARMES / MENU=↓ VOIR=→
- Appuyez sur la touche C ---- L'afficheur indique: -------- TER. DESARME / ARM.= θ
- Appuyez sur la touche C

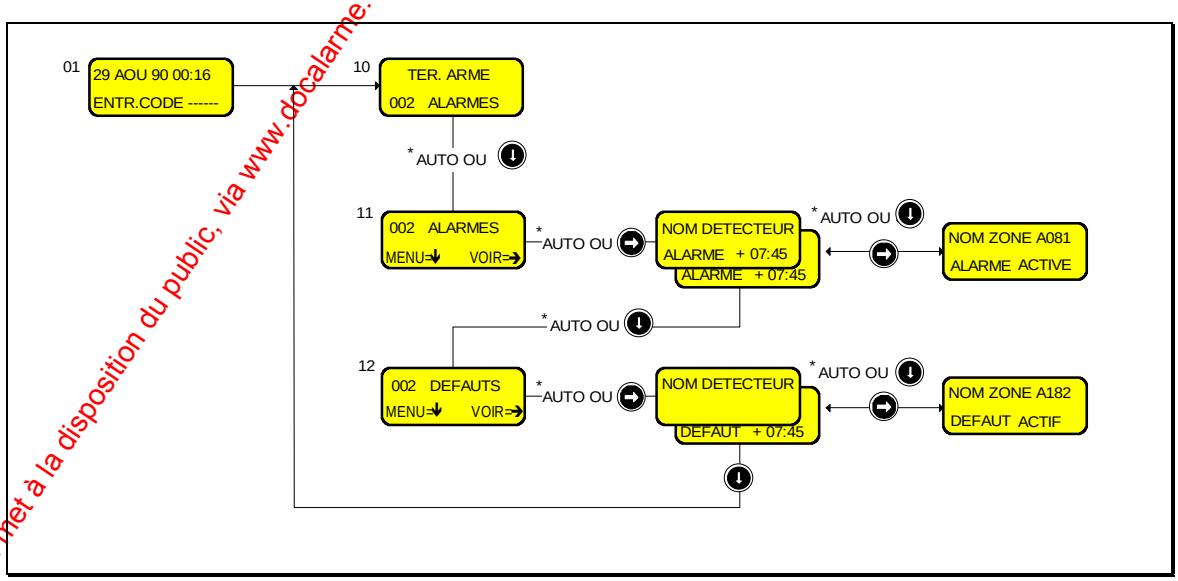
Cette procédure n'est possible que pour les alarmes ayant eu lieu dans votre propre territoire. Si ce n'est pas le cas, utilisez la touche ↓ pour accéder à la prochaine alarme.

Si vous effectuez une fin de session sans avoir acquitté toutes les alarmes, le Buzzer est activé pour environ 15 secondes, pour vous indiquer que des alarmes (appartenant à votre territoire) restent présentes.

☑ Nota : la procédure pour acquitter des défauts système est la même que celle décrite ci-dessus.

6.5 Défilement automatique

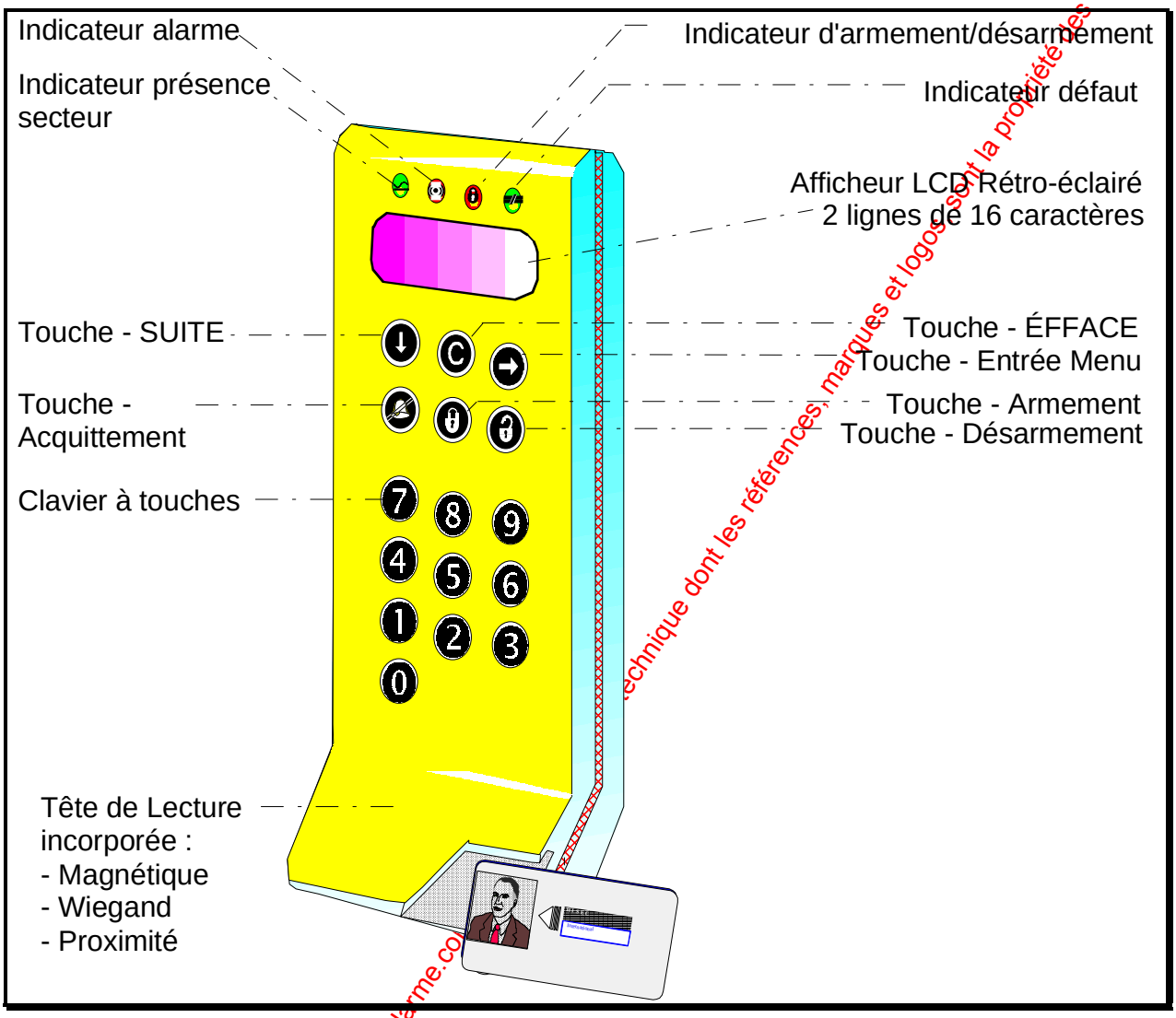
Après avoir entré votre code personnel, le Menu 10 s'affiche pour une durée de 5 secondes. Si des alarmes ou défauts système ont eu lieu, ils seront affichés automatiquement pendant 2 secondes chacun. Le défilement automatique est répété jusqu'à l'appui sur les touches C ou θ.



2. Contrôle d'Accès

Chapitre 7: Le Lecteur de Badges

7.1 Description du Lecteur de badges



7.2 Le Lecteur de badges

Le Lecteur de badges HISEC est un contrôleur/Terminal intelligent utilisé pour contrôler les portes, il possède sa propre base de données, peut transmettre des messages à l'utilisateur et à la possibilité de travailler avec le système intrusion HISEC et bien sûr de lire les badges. Il est constitué d'un afficheur, 5 LED, 6 touches de fonction et 10 touches numériques.

7.2.1 L'afficheur

L'afficheur possède 2 lignes de 16 caractères chacune. Le texte contenu donne aussi bien les informations d'état du système que les instructions à l'opérateur.

Chaque fois que le terminal est utilisé ou qu'un badge est lu, l'afficheur s'éclaire. Il s'éteindra automatiquement au bout de 2 minutes après la dernière action ou en effectuant une fin de session en appuyant sur la touche Ⓒ ou bien après le passage de la porte.

7.2.2 Les Led's de fonctions

Voyant Secteur (Vert) : Ce voyant allumé en permanence indique que le secteur est présent, le clignotement indique un défaut de l'alimentation secteur, le système fonctionne alors sur ses batteries.

Voyant Alarme (Rouge) : Allumé en cas de sabotage.

Voyant état d'armement (Jaune) : Allumé quand le lecteur a été bloqué par un utilisateur au moyen des fonctions "premier entré/dernier sorti".

Voyant défaut système (Jaune) : Allumé après une entrée en session, il indique la présence d'un défaut système. Les défauts sont visualisables au moyen du Menu Historique des alarmes (Menu 32). Le voyant s'éteint quand tous les messages de défaut ont disparus.

7.2.3 Les Touches de fonction

Cette touche est utilisée par les opérateurs possédant la fonction "premier entré/dernier sorti" pour verrouiller le lecteur.

Cette touche est utilisée par les opérateurs possédant la fonction "premier entré/dernier sorti" pour déverrouiller le lecteur.

Cette touche est utilisée pour se déplacer à droite dans les menus de programmation.

Cette touche est utilisée pour sélectionner les fonctions des menus affichés.

Cette touche est utilisée pour se déplacer dans les différents menus.

Cette touche est utilisée pour revenir en arrière ou quitter une session, ainsi que pour arrêter le Buzzer des Terminaux/Lecteurs.

7.2.4 Les Touches numériques

Le clavier est composé des touches numériques de 0 à 9 utilisées pour le code etc. et de 6 touches de fonctions.

Buzzer:

Utilisé pour indiquer de façon sonore un défaut ou une alarme. Egalement activé pour un temps bref pour indiquer les erreurs de manipulation ou pour attirer l'attention de l'utilisateur.

Chapitre 8: Programmation de la base de données

8.1 Base de données Locale et globale

Toutes les données programmées sont mémorisées dans un ou plusieurs lecteurs. Cet ensemble est appelé base de données. Le concept du système est basé sur une intelligence distribuée, toutes les données nécessaires à chaque lecteur sont présentes dans celui-ci. La base de données HISEC est divisée en 2 types, une base de données **globale** qui est identique dans tous les lecteurs (pour tous les badges) et une base de données **locale** qui peut être différente pour chaque lecteur.

L'ensemble des bases de données peut être divisé en 3 grands types:

- Base de données des Badges
- Base de données des Groupes de Personnel
- Base de données des Programmes hebdomadaires

C'est l'association "intelligente" de ces 3 catégories qui détermine complètement le fonctionnement du système HISEC.

8.1.1 La base de données des Badges

La base de données des badges appartient à la base de données **globale**, pour chaque badge les informations suivantes sont définies:

- N° du Badge
- Code personnel associé
- Etat de validité
- Priorité
- N° de groupe de Personnel

8.1.2 La base de données des Groupes de Personnel

La base de données des groupes de personnel est une partie de la base de données **locale**. Un groupe de personnel est une association logique d'un ou plusieurs badge(s) répondant aux mêmes règles, droits et fonctions. Le système peut accepter jusqu'à 250 groupes de personnel.

- Le groupe de personnel N°1 est réservé aux badges visiteurs.
- Le groupe de personnel N°250 est réservé aux badges "cartes de crédit" qui utilisent le système contrôle d'accès pour gérer un "sas de distributeur de billets".

La base de données des groupes de personnel contient les informations suivantes:

- N° Utilisateur Intrusion.....001/250
- Accès aux fonctions d'armement désarmement (verrouillage).....OUI/NON
- Code contrainte autorisé .....OUI/NON
- Enregistrer (historique) les accès normaux.....OUI/NON
- N° de Programme Hebdomadaire.....00/30

8.1.3 Les programmes hebdomadaires:

Les programmes hebdomadaires sont utilisés pour établir une liaison entre les plages horaires et les restrictions pour un (ou plusieurs) groupe(s) de personnel. En dehors de cela, ils sont utilisés pour appliquer les règles aux lecteurs de badges entiers.

Un programme hebdomadaire est constitué de périodes de temps, pour tous les jours de la semaine et 2 jours spéciaux. Chaque jour de la semaine peut être divisé en un maximum de 8 périodes, possédant chacune une fonction.

Par exemple, un accès permis les jours ouvrables de 8H à 17H, de façon à interdire l'accès au bâtiment après 17H et avant 8H. Si un utilisateur essai d'entrer dans le bâtiment en dehors de la période, son badge sera refusé et la tentative enregistrée dans l'historique du lecteur.

8.2 Programmation: une bonne préparation pour connaître les clés du système

La programmation d'un système contrôle d'accès et de ses badges est une tâche très importante, et qui peut prendre du temps si l'on ne connaît pas suffisamment le système.

Avant de commencer la programmation, il est nécessaire de répertorier ce que vous voulez changer ou entrer. Des fiches de programmation doivent vous avoir été fournies par votre installateur pour préparer votre programme. Partez toujours des anciennes fiches de programmation pour effectuer vos modifications.

8.2.1 Etape 1: Programmation du système

Pour programmer les données système vous avez besoin d'un badge de priorité 3.

Programmes hebdomadaires et Périodes de Congés:

Commencez la programmation par les programmes hebdomadaires, il existe 35 programmes hebdomadaires (01 à 34).

Généralement vous ne programmez que les 30 premiers programmes hebdomadaires qui sont destinés aux groupes de personnel, donc aux badges, les programmes hebdomadaires 31 à 34 sont réservés à votre installateur. Les données des programmes hebdomadaires 0 à 30 sont logées dans la base de données **Globale**.

Toutefois, il peut être nécessaire de programmer le Programme hebdomadaire 34 (Contrôle automatique de la porte). *Voir la partie B) de ce chapitre*. Les données des programmes hebdomadaires 31à 34 sont logées dans la base de données **Locale**.

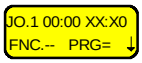
A) Programmation des programmes hebdomadaires 0 à 30:

En accédant au Menu 52 on obtient l'affichage suivant:

En vous aidant de la table suivante, choisir le N° de programme hebdomadaire désiré.

N° de Prog. Hebdomadaire	Utilisation
0	Pas d'accès (Ne doit pas être modifié)
1	Accès permanent avec code personnel (Ne doit pas être modifié)
2	Accès permanent sans code personnel (Ne doit pas être modifié)
3-30	Accès avec les règles déterminées par les fonctions programmables

Après avoir choisi le N° de programme hebdomadaire on obtient l'affichage suivant :



Un programme hebdomadaire est constitué de 7 jours standards (Lundi = Jour 1) et 2 jours spéciaux pour les congés (Jour 8 et 9). Ces derniers seront programmés de la même façon en définissant par ex. que personne n'a accès.

Vous pouvez diviser une journée en une ou plusieurs périodes, débutant toujours à 00H00 et finissant à 24H00. De façon à éviter les "trous" ou "chevauchement" de période, la période suivante est proposée avec comme heure de début l'heure de fin de la précédente. Chaque période se verra attribuer une fonction choisie dans la liste suivante, la fonction est définie par son numéro (00 à 03).

Les fonctions utilisables par les programmes hebdomadaires 0 à 30 sont les suivantes:

• FNC 00	Pas d'accès
• FNC 01	Accès avec code personnel
• FNC 02	Accès sans code personnel
• FNC 03	Fonction "bascule"

La fonction "bascule" peut être expliquée au moyen d'un petit exemple. Si le réceptionniste possède la fonction bascule, il utilise son badge quand il entre dans le bâtiment, pendant tout le temps où il sera présent la porte restera ouverte (libre). Aucun autre utilisateur voulant entrer ou sortir du batiment n'aura besoin d'utiliser son badge. Par contre, si le réceptionniste quitte le bâtiment en lisant son badge, la porte reviendra à un mode normal (contrôlé). Les porteurs de badges voulant avoir accès devront lire leur badge pour ouvrir la porte. Nota: cette fonction est obligatoirement associée à l'entrée d'un code personnel.

Quand vous avez terminé une journée par 24H00, l'afficheur passe automatiquement au jour suivant (Jour 2), si vous voulez réaliser une copie du jour précédent, appuyez sur la touche ➔.

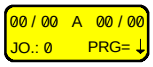
Pour effacer un programme hebdomadaire, entrez une période allant de 00H00 à 00H00, vous pouvez aussi quitter le menu au moyen de la touche Ⓒ, sans rien programmer.

B) Programmation du programme hebdomadaire 34:
La méthode de programmation est identique à celle décrite précédemment, exceptés les numéros de fonctions qui sont différents:

• FNC 30	Ouverture permanente (libération) de la porte pendant la période définie.
• FNC 31	Fermeture permanente (blocage) de la porte pendant la période définie.
• FNC 32	Fonctionnement normal de la porte pendant la période définie

C) Périodes de Congés: elles sont généralement programmées après avoir programmé les programmes hebdomadaires, au moyen du Menu 53.

L'affichage suivant est proposé:

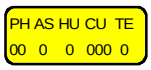


Vous devez programmer la date de début et de fin et le N° du jour de référence (Lundi= Jour 1)

Groupes de personnel:

Ensuite vous devez programmer les groupes de personnel qui constituent la partie locale de la base de données.

☒ Remarque: Cette programmation devra être effectuée sur chaque lecteur de l'installation si la modification est générale.

Après avoir appelé le Menu 51, 

l'afficheur propose la liste suivante:

PH = - N° de Programme Hebdomadaire ?	(00 à 30)
AS = - Fonction de Verrouillage (entrée session HISEC) ?	1=Oui/0=Non
HU =- Code Contrainte ?	1=Oui/0=Non
CU = - N° de Code Utilisateur Intrusion HISEC	001 à 250
TE = - Enregistrement des Accès Normaux ?	1=Oui/0=Non

PH = Numéro de Programme Hebdomadaire définit quel programme horaire est applicable au Groupe de Personnel (droits d'accès définis 24H/24, 365 jours par an).

AS = Fonction de Verrouillage (ou entrée en session HISEC) indique si le porteur d'un badge (sur ce lecteur) à le droit d'armer/désarmer ou de programmer le système d'intrusion.
Les droits de programmation et la définition des zones en relation avec le système d'intrusion sont programmés dans le système d'intrusion lui même, et cette information n'est pas stockée dans la base de données du lecteur.
La fonction de verrouillage peut être aussi utilisée en mode contrôle d'accès seul. Dans ce cas, les deux touches "cadenas" serviront pour verrouiller (ou déverrouiller) le lecteur (fonction "Premier entré/Dernier sorti").

HU = Code Contrainte est utilisé pour définir, si le système doit réagir au cas ou un opérateur ai utilisé le code Contrainte (défini comme le Code Personnel +1) à la place de son Code Personnel normal. L'utilisation du code Contrainte activera une sortie spécialement dédiée et enverra un message à la centrale d'Intrusion HISEC.

CU = Numéro de Code Utilisateur Intrusion HISEC indique quel code identifie les Groupes de Personnel en relation avec le système d'Intrusion HISEC, permettant ainsi la connexion avec le territoire qui peut être armé/désarmé par un badge appartenant à ce Groupe de Personnel.

Attention: Ce N° doit toujours être différent de 000, même dans un système contrôle d'accès seul.

TE = Enregistrement des Accès Normaux définit si on doit - ou ne pas - enregistrer le fait qu'un utilisateur appartenant à ce groupe de personnel a réalisé un accès (passage normal) de la porte. Si la fonction NON a été choisie, seules les exceptions (alarmes) seront enregistrées.

☑ **Nota**: Ne pas oublier que les groupes de personnel 1 et 250 sont réservés respectivement aux badges visiteurs et "sas bancaire".

8.2.2 Etape 2: Programmation des Badges

Pour programmer les badges, vous devez possèder un badge de priorité 1 au minimum.

Vous devez attribuer à chaque **badge** un **groupe de personnel**.

Se reporter aux données que vous avez entrées pour chaque groupe de personnel au moyen du Menu 51.

En attribuant un groupe de personnel à chaque badge au moyen du Menu 41, vous donnez automatiquement à tous ces badges des droits d'accès. Ces droits d'accès peuvent être effacés au moyen du Menu 42, bloqués au moyen du Menu 43 et re-validés au moyen du Menu 44. Il est possible (et conseillé, dans la mesure du possible) d'attribuer le même groupe de personnel à plusieurs badges.

8.2.3 Envoi d'un message

Au moyen du Menu 10, vous pouvez envoyer un message au porteur d'un badge. La liste suivante est un exemple des messages proposés, toutefois ils peuvent être modifiés, à votre demande, par votre installateur avec un maximum de 30 messages par système. Les messages sont sélectionnés par leur numéro d'ordre.

Après avoir appelé le Menu 10, vous devez entrer en premier le **numéro du badge** destinataire du message, puis le **numéro de message** choisi dans la liste.

Voir le Chapitre 11.1 "Menu 10" pour la description complète de la programmation.

Voir le Chapitre 12.2 "Messages" pour la description du traitement d'un message.

Quelques exemples:

Message N°00	:	pas de message à l'utilisateur
Message N°01	:	CONTACTEZ LE DPT. PERSONNEL
Message N°02	:	CONTACTEZ VOTRE DOMICILE
Message N°03	:	CONTACTEZ LE DPT. SECURITE
Message N°04	:	CONTACTEZ LA RECEPTION
Message N°05	:	IMPORTANT MESSA. TELEPHONIQUE
Message N°06	:	CONTACTEZ VOTRE SUPERIEUR
Message N°07	:	R.D.V DEPLACEMENT ANNULE
Message N°08	:	REUNION ANNULEE
Message N°09	:	RAPPELEZ LE SIEGE
Message N°10	:	CONTACTEZ VOTRE SECRETAIRE
Message N°11	:	REVISION VEHICULE
Message N°12	:	DEPANNAGE URGENT
Message N°13	:	VISITE MEDICALE
Message N°14	:	COURRIER IMPORTANT
Message N°15	:	DOCUMENT A SIGNER

8.3 Anti-Retour: La restriction nécessaire des déplacements du personnel

L'Anti-Retour est une forme de contrôle d'accès nécessitant une grande discipline des utilisateurs dans la pratique.

Toutefois, l'Anti-Retour peut être nécessaire dans des situations ou des données vitales à l'entreprise doivent être accessibles avec un contrôle sévère ou quand pour des raisons de sécurité il est important de savoir à tout moment où se trouve chaque personne.

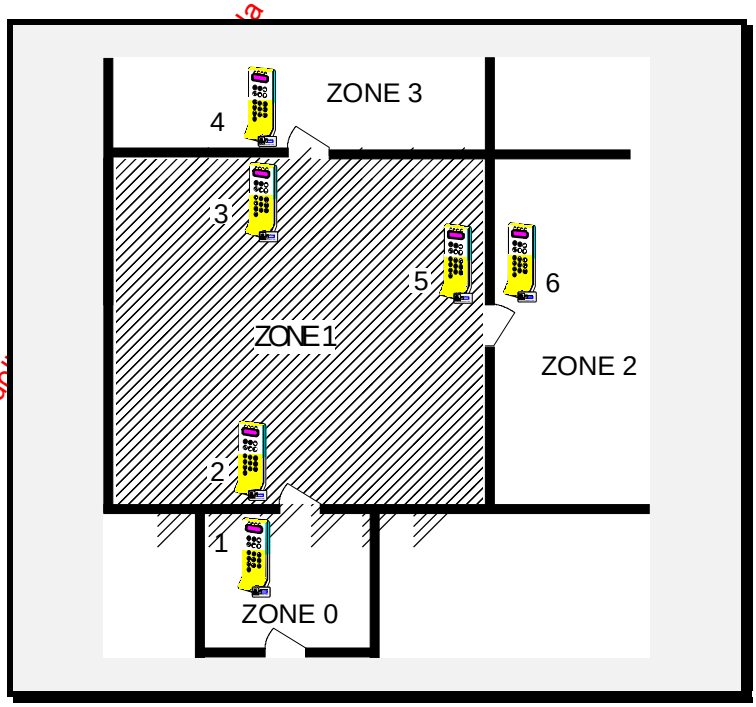
Au moyen de l'Anti-Retour, le système enregistre la situation de chaque personne en permanence. Pour réaliser cette fonction, les lecteurs de badges sont installés entre chaque passage d'une zone à l'autre. Pour entrer ou sortir d'une zone, le porteur doit utiliser son badge sur un lecteur. S'il n'exécute pas cela correctement et qu'il quitte (ou entre) dans une zone (avec la complicité d'une autre personne), il se renferme lui-même dans une zone, du fait que le système n'a pas enregistré de mouvement de la zone 1 à 3 par ex. et il bloque la porte à toute tentative de lecture du badge sur un lecteur.

La diversité des sites et des risques (sur le même site, éventuellement) a nécessité la création de catégories de niveaux d'Anti-Retour. Vous pouvez déterminer les niveaux qui vous sont nécessaires, en accord avec votre installateur (lui seul peut modifier la conception de l'installation).

- 0: Contrôle de l'Anti-Retour Permanent. Le contrôle démarre à la première lecture du badge et est appliqué en permanence.
- 1: Contrôle de l'Anti-Retour annulé chaque jour à minuit (24:00) et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 2: Contrôle de l'Anti-Retour annulé chaque heure et le contrôle de zone démarrera à nouveau à la première (prochaine) lecture du badge. Le contrôle de zone démarrera dans la zone où chaque badge sera lu.
- 3: Pas de contrôle de l'Anti-Retour par zone. Tous les badges pourront être utilisés en ignorant les conflits de zones possibles.

☒ Les différents niveaux d'anti-retour peuvent être panachés sur un même site.

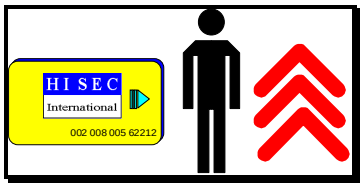
Exemple de bâtiment avec Anti-Retour



Chapitre 9: Les Badges

Chaque badge possède son propre numéro, composé des 5 derniers chiffres du N° de série du badge. Les badges ont été divisés en badges maîtres, maintenances, utilisateurs et visiteurs.

9.1 Les Badges Maîtres:



Pour chaque installation 5 badges maîtres (maximum) ont été délivrés. Ils portent les numéros de 0 à 4. Les badges maîtres sont destinés à la personne responsable de la sécurité au démarrage du système. Par la suite, le seul usage de ces badges est de programmer de nouveaux badges ayant des priorités élevées. Après cela, les badges maîtres pourront être placés dans un endroit sûr ou de sécurité.

La personne responsable des badges peut décider à quel moment les badges de maintenance seront acceptés.

9.2 Les Badges de Maintenance:

Le badge de maintenance est le badge personnel du technicien, il peut uniquement être utilisé par le personnel autorisé de votre installateur. L'utilisation des badges maintenance est toujours enregistrée dans l'historique du système. De cette façon il est toujours possible de savoir quand un badge de maintenance a été utilisé et pourquoi faire.

Le badge de maintenance est nécessaire au démarrage du système et à l'initialisation des lecteurs. Il donne également accès à certains menus de programmation et de test. Le badge de maintenance a également accès après que le système ait été en alarme depuis plus de 2 minutes.

Se reporter au chapitre 9.7 "Liste des niveaux de priorités".

Nota: le badge de maintenance peut être bloqué par un badge de priorité P3 à n'importe quel moment, pour maintenir le niveau de sécurité.

9.3 Les Badges Utilisateurs:

Les badges utilisateurs n'ont pas de droits d'accès ou de programmation définis. Ils sont entièrement dépendants de la programmation effectuée sur le système. Un badge utilisateur peut être bloqué ou complètement effacé. Un badge bloqué ne sera plus accepté sur les lecteurs, tandis qu'un badge effacé devra être programmé de nouveau s'il doit être réutilisé.

☒ Nota : Les droits d'un badge utilisateur sont uniquement définis par son niveau de priorité.

Se reporter au chapitre 9.7 "Liste des niveaux de priorités".

9.4 Les Badges Visiteurs:

Un badge visiteur est un badge normal attribué au groupe de personnel N°001, ce qui lui affecte automatiquement certaines règles.
Un badge visiteur est valide pour un jour uniquement et est bloqué à 24H00. Au moyen du Menu 22 vous pouvez bloquer un badge visiteur quand vous le voulez. Tous les badges standard programmés dans le système peuvent devenir des badges visiteurs.

9.5 Les Badges "Cartes de crédit":

Les "cartes de crédit" peuvent être utilisées comme des badges visiteurs. Dans ce cas, les mêmes règles que celles des badges visiteurs s'appliquent (voir chapitre 9.4).
50 "carte de crédit" maximum peuvent être programmées par système.

9.5.1 "Cartes de crédit" en contrôle de "sas bancaire"

En dehors de badges visisteurs, les "cartes de crédit" peuvent être utilisées pour contrôler l'ouverture des "sas des distributeurs de billets". Dans ce cas, les "cartes de crédit" sont associées au groupe de personnel 250, qui devra être programmé de la façon suivante:

PH = uniquement un numéro de programme horaire défini pour fonctionner sans code personnel.

AS = si vous programmez cette fonction à 1 (oui), la porte pourra être ouverte système intrusion armé ou non. Programmé à 0 (non) la porte pourra être ouverte uniquement si le système est désarmé.

HU = doit toujours être programmé à 0 (non).

CU = ce numéro doit être en relation avec le système intrusion et en particulier d'un territoire, son fonctionnement n'est possible que si la fonction verrouillage (AS) a été programmée à 0.

TE = programmé à 1, chaque utilisation d'une "carte de crédit" sera enregistrée. Programmé à 0 les utilisations ne seront pas mémorisées.

9.6 Priorité des badges:

Les possibilités des opérateurs sur le système contrôle d'accès HOR ne sont pas les mêmes pour chacun, c'est pourquoi les droits ont été divisés en 4 niveaux. Ces droits sont appelés "Niveaux de Priorités" et sont numérotés de 0 à 3. Ces niveaux sont indiqués par un P (pour priorité) suivi du chiffre. Plus le chiffre est élevé et plus l'opérateur aura accès aux fonctions de programmation.

Voir le chapitre 9.7 pour la "Liste des niveaux de priorités contrôle d'accès".

Les badges peuvent uniquement utiliser des codes personnels à 4 ou 6 chiffres. Ce code personnel peut être changé à volonté par l'utilisateur.

Voir le chapitre 12.4 "Changement de votre propre code Personnel".

Un badge normal est toujours créé avec le niveau de priorité le plus bas (0) et ne peut pas être utilisé pour la programmation, mais uniquement pour des opérations courantes d'ouverture de porte. Un niveau plus élevé peut être attribué au badge en utilisant le *Menu 57 "Edition des Badges de Programmation"*.

☒ Nota: Un badge de Maintenance a des droits prédéfinis et ne peut pas être créé. Tous les badges de Maintenance ont les mêmes droits.

Les priorités de programmation disponibles sont les suivantes:

- ❍ Aucune priorité ..... (priorité 0) ..... Utilisateur normal
- ❍ Usage limité ..... (priorité 1) ..... Réceptionniste
- ❍ Programmation limitée ..... (priorité 2) ..... Gestionnaire de badges
- ❍ Programmation totale ..... (priorité 3) ..... Responsable de la sécurité

9.7 Listes des niveaux de priorités Contrôle d'Accès:

Fonctions	Priorités				Maintenance autorisée	Maintenance non autorisée	Maintenance non autorisée + Alarme.
	0	1	2	3			
Passage normal de la porte	☺	☺	☺	☺	☺	▫	☺
Edition des messages(10)	▫	☺	☺	☺	☺	▫	▫
Programmation des badges visiteurs(20-24)	▫	☺	☺	☺	☺	▫	▫
Fonction d'affichage (30-38)	▫	▫	☺	☺	☺	▫	☺
Programmation des badges (40-45)	▫	▫	☺	☺	☺	▫	▫
Définition du système(50-57)	▫	▫	▫	☺	☺	▫	▫
Impression (60-64)	▫	▫	▫	☺	☺	▫	▫
Contrôle de la porte(70-73)	▫	▫	▫	☺	☺	▫	▫

☺ = Oui ▫ = Non (50-57) = Numéro des menus Contrôle d'Accès HISEC.

Nota: Les badges de Maintenance ont deux niveaux de priorité différents, liés au fait que vous ayez autorisé (ou non) le mode Maintenance. Le badge Maintenance sera autorisé à entrer en session seulement en cas d'alarme, mais avec le niveau de priorité le plus bas indiqué dans le tableau précédent. Si vous avez autorisé l'usage étendu du badge de Maintenance, il aura aussi accès aux fonctions de niveau élevé, et pourra entrer en session sur le lecteur sans condition d'alarme.

Chapitre 10: Menus: Utilisation pas à pas

10.1 Les menus

La procédure d'exploitation est basée sur des menus. Toutes les opérations sont affichées et l'utilisateur répond simplement aux questions posées au moyen des touches correspondant à OUI et NON. Chaque menu est défini par un nombre (10 à 98), ces numéros ne sont pas visibles sur l'afficheur.

Les menus accessibles dépendent du niveau de priorité de l'opérateur.

☒ *Nota : Seuls les Menus présentant un intérêt pour l'utilisateur final sont décrits dans ce manuel.*

☞ La description des menus sera faite au chapitre 11 : **Description des Menus Contrôle d'accès**.

10.1.1 Les menus Principaux 10, 20, 30, 40, 50, 60 et 70

- Le **Menu 10** est le menu d'**Edition des messages**. Au moyen de ce menu, vous pouvez transmettre des messages aux utilisateurs du contrôle d'accès. Le message apparaîtra sur l'afficheur, la prochaine fois que le badge choisi sera lu sur un lecteur. Le message devra être acquitté pour pouvoir ouvrir la porte.
- Le **Menu 20** est le menu général des **Badges visiteurs**. Au moyen de ce menu, les badges visiteurs pourront être validés, bloqués, etc. De plus, c'est le menu pour les visiteurs utilisant les "cartes de crédit".
- Le **Menu 30** est le menu général d'**Etat**. Au moyen de ce menu, vous pouvez visualiser l'état des alarmes, l'historique, visualiser les badges et la programmation.
- Le **Menu 40** est le menu général de **Programmation des badges** Au moyen de ce menu les badges pourront être créés, validés, bloqués, effacés, etc.
- Le **Menu 50** est le menu de **Programmation**. Au moyen de ce menu, la plupart des données relatives au contrôle d'accès pourront être programmées, c'est à dire, les groupes de personnel, programmes hebdomadaires, date et heure, etc. Ce menu vous permet également d'autoriser (ou de bloquer) l'entrée du badge maintenance (technicien).
- Le **Menu 60** est le menu d'**Impression**. Au moyen de ce menu, il vous est possible d'imprimer les alarmes (historique), la liste des badges, la programmation, etc.
- Le **Menu 70** est le menu de **Contrôle des Portes**. Au moyen de ce menu, il vous est possible de commander (ouvrir ou fermer) directement la porte associée au lecteur.

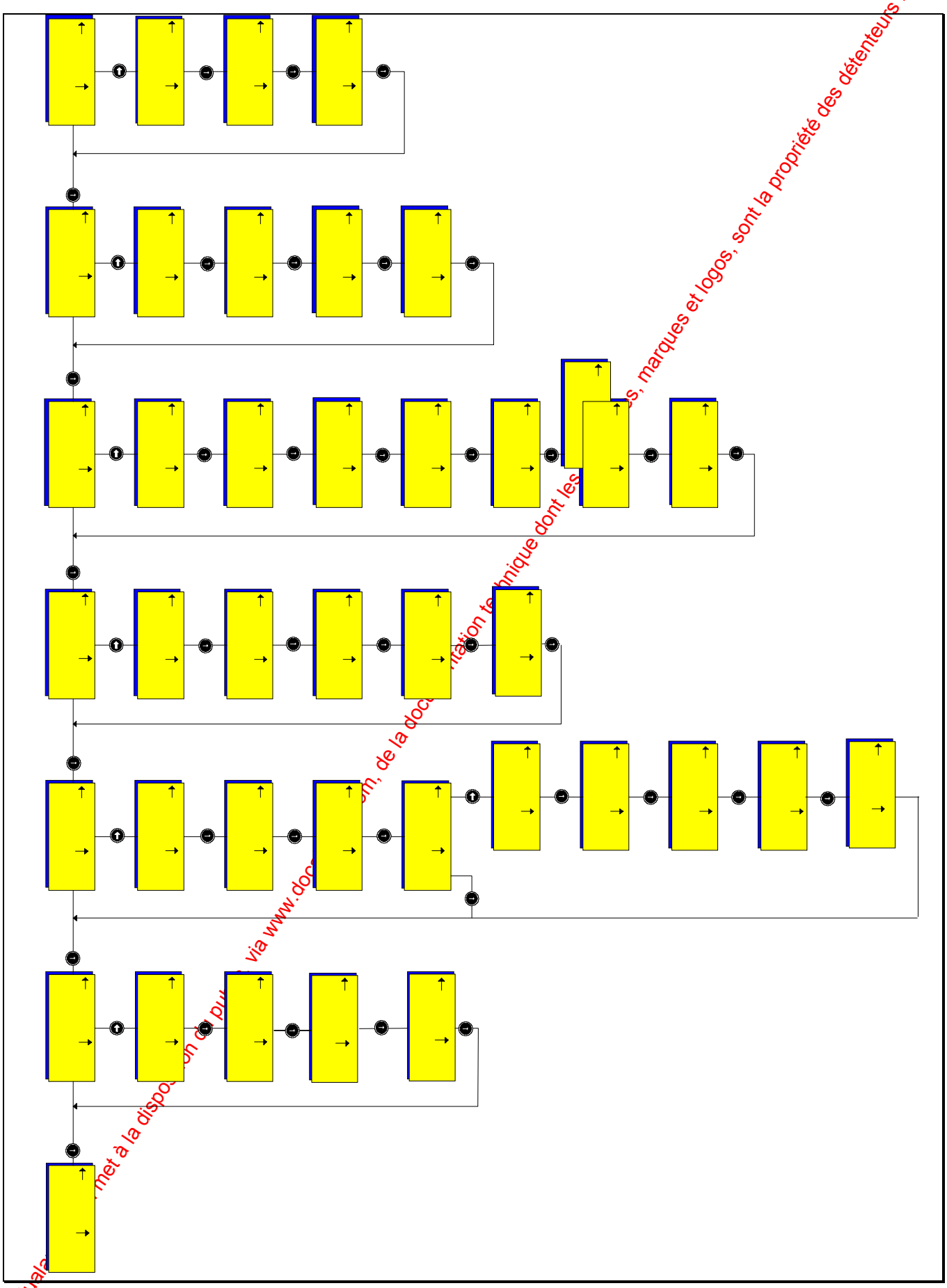
10.1.2 Les Sous Menus

Les Menus principaux ne sont en fait que des "En-têtes" pour accéder aux sous menus. Ces sous menus déroulants permettent d'avoir un aperçu des possibilités offertes et les instructions opératoires.

Les sous-menus peuvent (en fonction du niveau de priorité) être appelés directement. De cette façon, le numéro de menu sera tapé directement après avoir entré son code personnel. Les Menus déroulants vous permettent d'avoir accès aux menus uniquement au moyen des réponses aux questions OUI ou NON, le NON vous propose automatiquement le prochain menu accessible. Pour revenir au menu principal on utilisera la touche Ⓒ.

☞ Se reporter au chapitre 9.7 "Liste des niveaux de priorités" et au chapitre 10.2 pour le "Panorama des Menus contrôle d'accès".

10.2 Panorama des Menus Contrôle d'Accès

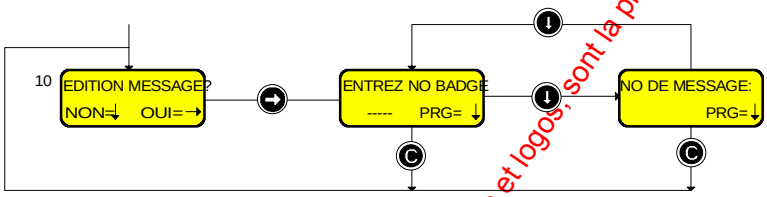


Chapitre 11 Description des Menus Contrôle d'Accès

Dans ce chapitre tous les menus utilisateurs Contrôle d'accès seront décrits en détail.

Voir aussi le Chapitre 10.2 "Panorama des Menus contrôle d'accès".

11.1 Menu Principal 10

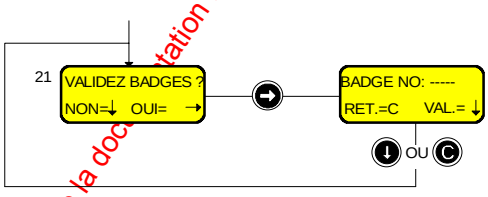


Le Menu 10 vous permet d'envoyer un message à destination de n'importe quel badge. Après appui sur la touche → le numéro du badge sera entré sur le clavier et après appui sur la touche ↓, le numéro de message associé au badge apparaît. Un nouveau numéro de message choisi dans la liste du chapitre 8.2.3 sera entré suivi par la touche ↓. Après programmation du message, l'afficheur propose le prochain badge appartenant au même Groupe de Personnel.

11.2 Menu Principal 20

Ce menu vous permet de valider (bloquer) les badges visiteurs et "cartes de crédit".

Menu 21



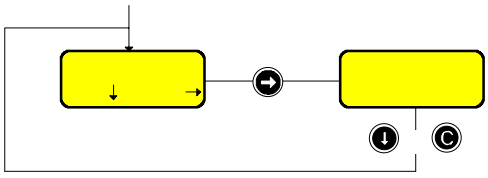
Le Menu 21 vous permet de valider (activer) un badge visiteur.

Vous devez préciser le Numéro de badge (5 chiffres) et appuyer sur la touche ↓

Ensuite, le badge sera valide jusqu'à 24H00 par défaut, mais pourra être bloqué manuellement au moyen du Menu 22.

☑ Prière de noter que le badge devra avoir été préalablement (au démarrage du système) défini comme appartenant au groupe de personnel des visiteurs (groupe de personnel N°1).

Menu 22

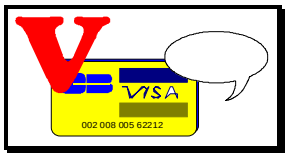


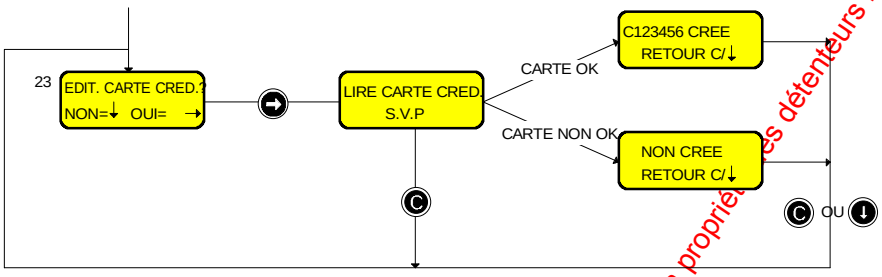
Le Menu 22 vous permet de bloquer de façon manuelle un badge visiteur.

Vous devez préciser le Numéro de badge (5 chiffres) et appuyer sur la touche ↓.

Après cela, le badge ne sera plus accepté sur aucun lecteur du système.

Menu 23





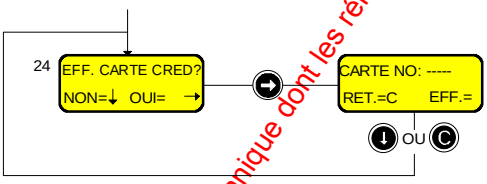
Le Menu 23 vous permet de programmer les "cartes de crédit" en badges visiteurs.

Quand cette fonction est appelée le lecteur vous demande de lire la "carte de crédit" sur le lecteur. Cette opération réalisée, l'afficheur indique que la carte a été créée et donne son numéro (les 6 derniers chiffres).

Ce numéro peut être alors noté avec le nom du visiteur.

Vous ne pouvez créer plus de **50 badges visiteurs** par système, en cas de dépassement l'afficheur indiquera NON CREE.

Menu 24

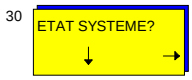


Le Menu 24 vous permet de bloquer de façon manuelle un badge visiteur "carte de crédit".

Il est nécessaire d'entrer le N° de la "carte de crédit", c'est pourquoi il est important de l'avoir noté à l'utilisation du Menu 23.

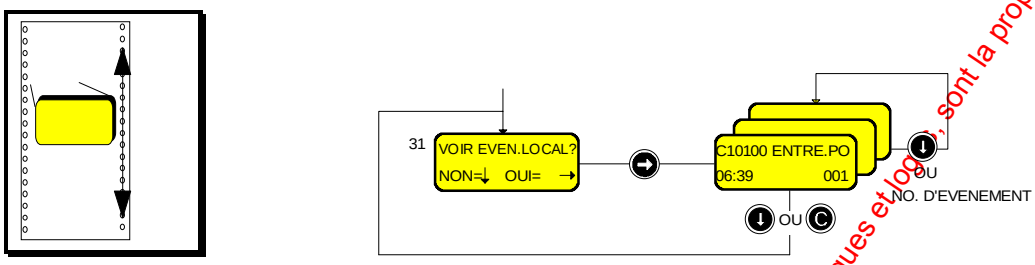
Après cela, la "carte de crédit" ne sera plus accepté sur aucun lecteur du système.

11.3 Menu Principal 30



Ce menu vous permet de visualiser la programmation et la configuration du système, de la base de données, des badges et des enregistrements du journal (historique).

Menu 31

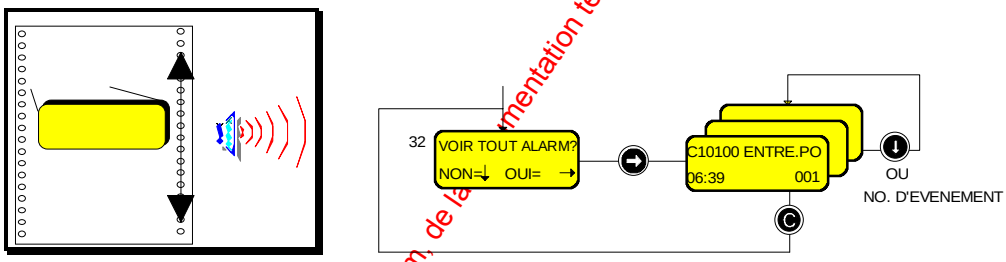


Le Menu 31 vous permet de visualiser tous les événements du journal (historique) local, il contient les transactions normales de porte, les lectures de badges et les alarmes du lecteur sur lequel on opère. Chaque lecteur possède un journal (historique) de 1000 ou 2300 événements. Le dernier (le plus récent) événement est affiché en premier (001). Quand le journal (historique) est plein, les plus vieux événements sont écrasés.

Vous pouvez appeler directement un événement en entrant son numéro (toujours 3 chiffres) sur le clavier, ou obtenir l'événement suivant par appui sur la touche ⬇. Le Numéro de l'événement est affiché en bas à droite de l'écran.

Pour quitter cet affichage, utilisez la touche Ⓒ

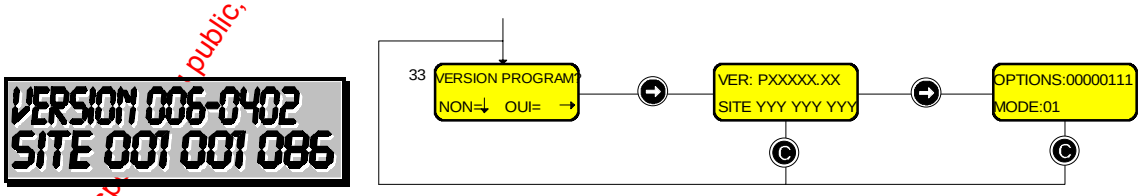
Menu 32



Le Menu 32 vous permet de visualiser toutes les alarmes du journal (historique) global du système complet (tous les lecteurs). L'historique global des alarmes a une capacité de 100 alarmes. La dernière (la plus récente) alarme est affichée en premier (001).

Vous pouvez appeler directement une alarme en entant son numéro (toujours 3 chiffres), ou obtenir l'alarme suivante par appui sur la touche ⬇. Le Numéro de l'alarme est affiché en bas à droite de l'écran. Pour quitter cet affichage, utilisez la touche Ⓒ

Menu 33



Le Menu 33 vous permet de visualiser les informations sur la **Version** du logiciel, le **Code Site** du système, les **Options** sélectionnées et le **Mode** programmé pour le lecteur.

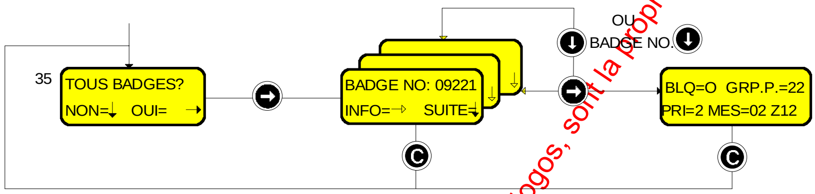
☑ Les informations contenues dans ce Menu sont destinées à votre installateur ou au superviseur du système.

Menu 34

34 

Ce menu vous permet de visualiser la programmation des badges et de compter les personnes (dans un système utilisant l'anti-retour).

Menu 35



Le Menu 35 vous permet de visualiser la totalité des informations concernant les badges existants dans le système.

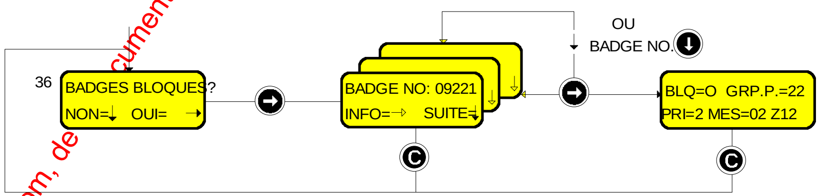
Quand cette fonction de visualisation est appelée, l'afficheur propose le premier badge de la base de données. Si vous voulez visualiser un badge précis, entrez le Numéro du badge (5 chiffres).

Les INFOrmations suivantes seront affichées après utilisation de la touche ➡:

- BLQ = Badge bloqué ou non
- GRP.P = Numéro de Groupe de Personnel associé au badge
- PRI = Priorité de programmation
- MES = Numéro de message attribué à ce badge pour l'instant (si existant)
- Z = Numéro de la zone d'Anti-retour où est le badge est présent à cet instant

Au moyen de la touche ⬇, le badge suivant (programmé) sera visualisé. Quand la liste est terminée, l'afficheur revient au premier badge. Au moyen de la touche Ⓒ, la fonction d'affichage est arrêtée et un retour au *Menu 35* est effectué.

Menu 36

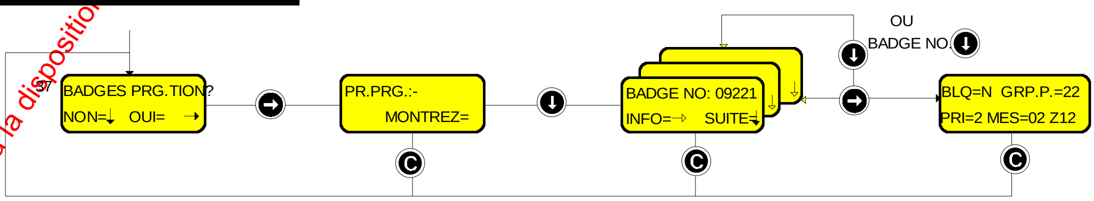


Le Menu 36 vous permet de visualiser la totalité des informations concernant les badges bloqués sur le système.

Se reporter au menu 35 pour le mode d'utilisation qui est similaire.

Menu 37

Le Menu 37 vous permet de visualiser la totalité des informations concernant les badges de programmation (c'est à dire les badges ayant une priorité supérieure à 0) du système.

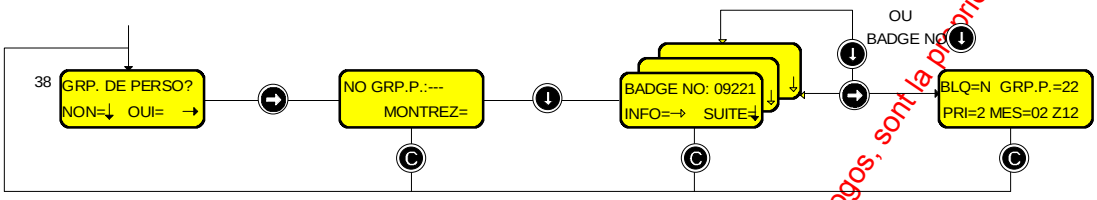


Vous devez préciser en premier la priorité (0 à 3) des badges que vous voulez visualiser.

Se reporter au *Menu 35* pour le mode d'utilisation qui est similaire.

Menu 38

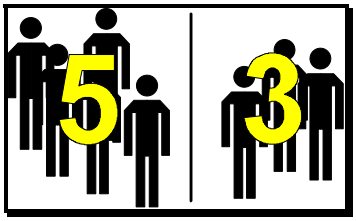
Le Menu 38 vous permet de visualiser la totalité des informations concernant les badges appartenant à un groupe de personnel choisi.

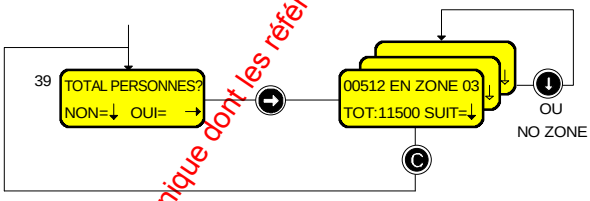


Vous devez préciser en premier le numéro du groupe de personnel (001 à 250) des badges que vous voulez visualiser.

Se reporter au *Menu 35* pour le mode d'utilisation qui est similaire.

Menu 39





Le Menu 39 vous permet de savoir combien de badges sont présents - à cet instant - dans chaque zone et combien de badges sont à l'intérieur du bâtiment.

Vous pouvez appeler directement une zone en entrant son numéro (toujours 2 chiffres) sur le clavier, ou obtenir la zone suivante par appui sur la touche ↓.

Le nombre de personnes (badges) présentes dans chaque zone est donné à gauche du N° de la zone, le compteur **TOT:** permet de connaitre le nombre de badges présents sur le site (toutes les zones intérieures).

Se reporter au chapitre 8.3 pour les concepts de l'anti-retour.

☑ Nota : la zone 00 représente l'extérieur du batiment.

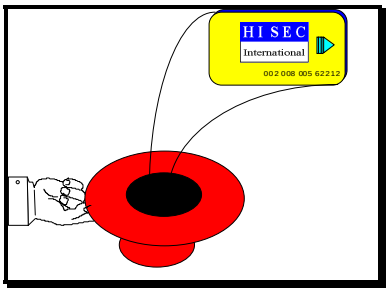
Pour quitter ce Menu on utilisera la touche C

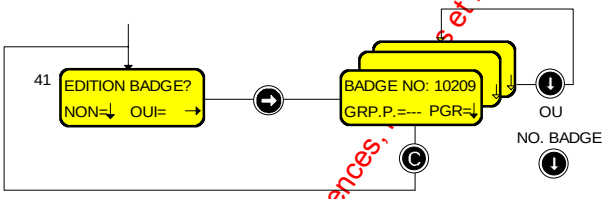
11.4 Menu Principal 40

La programmation des badges consiste en l'ensemble des points suivants: création et effacement des badges, modifications des informations des badges par ex: changement de Groupe de Personnel, modification de l'état des badges ayant été bloqués (ou non).

Se reporter également au Chapitre 8 "Programmation de la base de données".

Menu 41

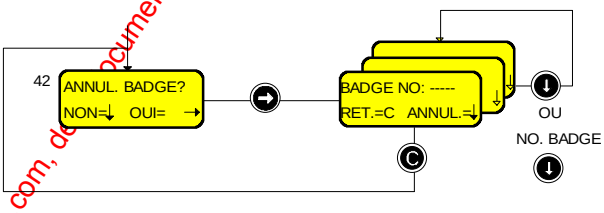




Le menu 41 vous permet de **créer** les badges. Quand ce menu est appelé, l'afficheur vous propose le premier numéro de badge libre. Ensuite, le numéro de groupe de personnel doit être entré, la touche ⬇ valide la programmation. Si le numéro de badge n'est pas celui désiré, un nouveau numéro de badge peut être entré avant l'appui sur la touche ⬇.

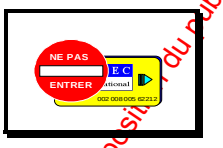
Après la programmation du badge avec la touche ⬇ le lecteur propose le prochain badge libre avec le même numéro de Groupe de Personnel. Il est alors facile de programmer un groupe de badges, simplement en appuyant sur la touche ⬇ à chaque badge.

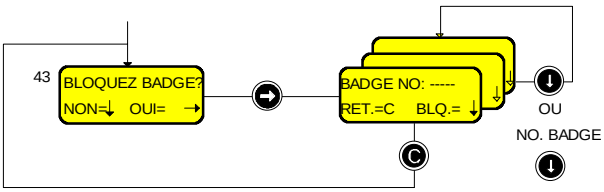
Menu 42



Le menu 42 vous permet d'**effacer** des badges. Le numéro de badge à effacer doit être entré avant l'appui sur la touche ⬇, ensuite le lecteur propose le prochain badge avec le même numéro de Groupe de Personnel. Il est alors facile d'effacer un groupe de badges simplement en appuyant sur la touche ⬇ à chaque badge.

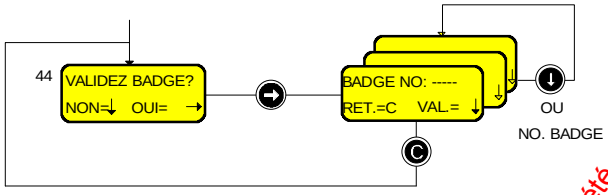
Menu 43





Le menu 43 vous permet de **bloquer** des badges. Le numéro de badge à bloquer doit être entré avant l'appui sur la touche ⬇, ensuite le lecteur propose le prochain badge avec le même numéro de Groupe de Personnel. Il est alors facile de bloquer un groupe de badges simplement en appuyant sur la touche ⬇ à chaque badge.

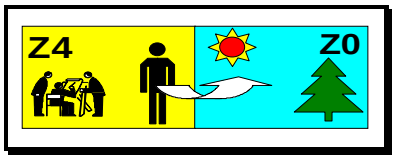
Menu 44

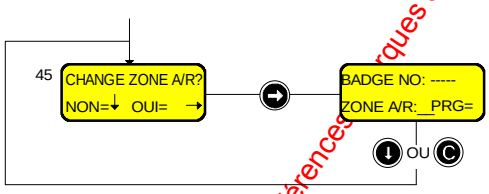


Le menu 44 vous permet de valider un badge ayant précédemment été bloqué au moyen du Menu 43 ou encore si l'opérateur a fait 10 tentatives de code erroné sur un lecteur.

Après la validation du badge au moyen de la touche ⬇, le lecteur propose le prochain badge bloqué appartenant au même numéro de Groupe de Personnel. Il est alors facile de valider un groupe de badges, simplement en appuyant sur la touche ⬇ à chaque badge.

Menu 45





Le menu 45 est nécessaire pour corriger les erreurs effectuées par les porteurs de badges dans le système Anti-Retour. Ce Menu sera utilisé pour passer le porteur d'un badge d'une zone à une autre.

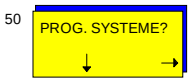
Vous devez préciser en premier le numéro du badge (5 chiffres), puis le numéro de la zone d'anti-retour (00 à 15) où vous voulez placer le badge.

L'Anti-Retour recommencera alors à fonctionner à la prochaine transaction du badge dans la zone programmée.

☒ Rappel : La Zone 00 est considérée comme l'extérieur du bâtiment.

Se reporter au chapitre 8.3 pour les concepts de l'anti-retour.

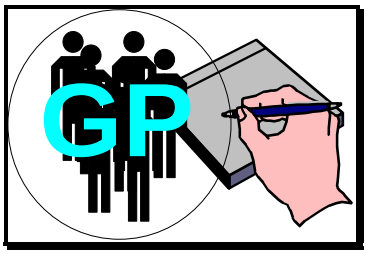
11.5 Menu Principal 50

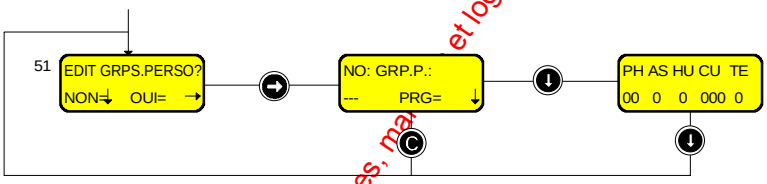


La programmation système consiste en l'ensemble des points suivants: Création des groupes de personnel, périodes d'accès et jours spéciaux (congés). Ce Menu permet également de programmer la date et l'heure et d'autoriser (bloquer) la maintenance.

Se reporter aussi au Chapitre 8 "Programmation de la base de données".

Menu 51





Le Menu 51 vous permet de créer ou de modifier les Groupes de Personnel. Un nombre de 3 chiffres doit être entré et validé par la touche ⬇.

Après cela, les paramètres relatifs à ce groupe seront entrés. Le système est pré-programmé avec la valeur par défaut "0" pour tous les paramètres.

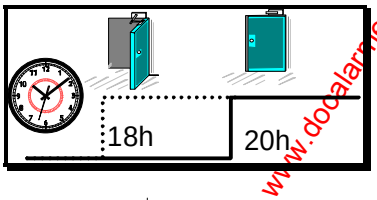
- PH = N° de Programme Hebdomadaire(00-35)
- AS = Armement permis sur le système d'intrusion (fonction verrouillage)? (1=OUI, 0=NON)
- HU = Code hold-up autorisé pour ce groupe ? (1=OUI, 0=NON)
- CU = N° de code utilisateur du système d'intrusion (1-250)
- TE = Enregistrement des transactions normales ? (1=OUI, 0=NON)

Se reporter au chapitre 8.2.1 pour une explication plus complète de tous ces paramètres.

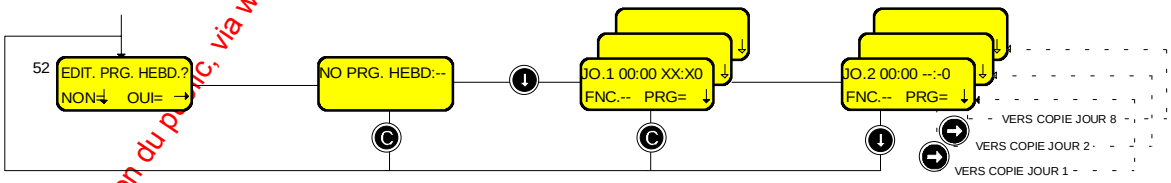
Après l'entrée de ces paramètres, la touche ⬇ sera utilisée pour enregistrer les données.

☑ La base de données des Groupes de Personnel est **Locale**, ceci est important car elle devra être programmée pour chaque lecteur.

Menu 52



Le Menu 52 vous permet de créer, modifier ou effacer les programmes hebdomadaires.



Deux chiffres sont nécessaires pour définir le numéro du Programme Hebdomadaire (max.: 35), après quoi le jour 1 (LUNDI) est affiché avec son heure de début 00:00. La première période sera alors de 00:00 à xx:x0 où x est le chiffre à entrer. L'heure xx:x0 sera automatiquement transférée vers l'heure de départ de la période horaire suivante pour le JOUR 1, pour éviter à l'utilisateur de créer un programme horaire avec des "trous" ou des "chevauchements" de périodes. Un jour est terminé quand 24:00 est programmé comme période de fin et le jour suivant JOUR 2 est proposé sur l'afficheur. Si la touche ➡ est appuyée à cet endroit une copie du jour précédent sera effectuée pour ce jour.

Se reporter au chapitre 8.2.1 pour une explication plus complète de ces éléments.

Le champ FNC est programmé avec les numéros des fonctions décrites au *Chapitre 8.2.1,* cela attribue la fonction spécifique devant être exécutée durant chaque période du programme horaire.

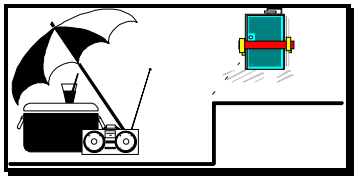
Vous pouvez quitter la programmation au moyen de la touche Ⓒ

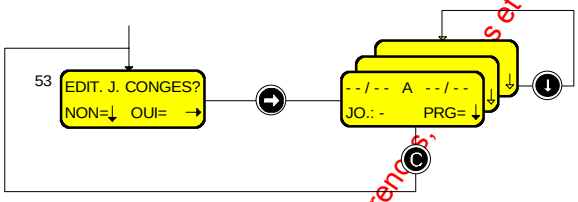
Pour effacer un programme hebdomadaire existant, entrez la période 00:00 à 00:00.

☒ *Remarque: Il est uniquement possible de programmer les intervalles avec une résolution de 10 minutes. De ce fait, il est seulement nécessaire d'entrer 3 chiffres, le dernier chiffre étant toujours un 0.*

Nota: Si vous avez le moindre doute sur votre programmation, n'hésitez pas à consulter votre installateur.

Menu 53





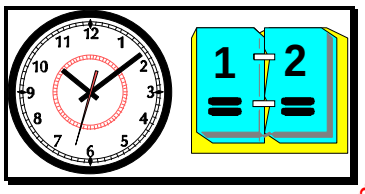
Le Menu 53 vous permet de créer (modifier) une liste de jours de congés, en liaison avec les Programmes Hebdomadaires décrits précédemment. Cela peut être utilisé, par exemple, pour bloquer les badges pendant une période ininterrompue de 2 semaines.

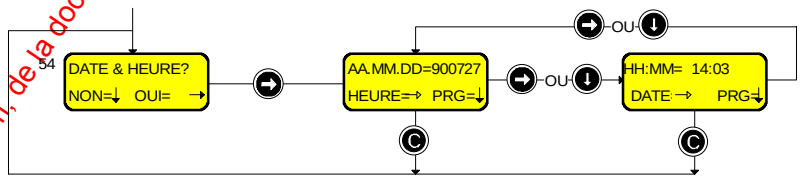
La liste comporte un maximum de 25 périodes avec une date de départ et une date de fin pour chaque période, ainsi que le jour de la semaine de référence (Lundi = Jour 1) que vous voulez qui prennent la place des jours de congés.

Se reporter au chapitre 8.2.1 pour une explication plus complète de tous ces paramètres.

☑ *Nota: La période inclut la date de départ et la date de fin.*

Menu 54





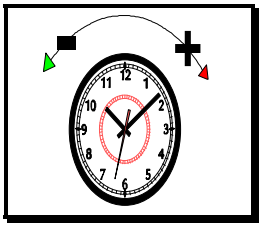
Le Menu 54 vous permet de changer l'heure et la date du système.

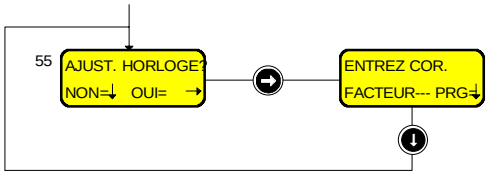
Pour modifier la date, vous devez entrer dans l'ordre l'**année** (AA), le **mois** (MM) et la **date** (DD). Quand le dernier chiffre est entré, suivi de la touche ⓓ, l'heure s'affiche et peut être modifiée par l'entrée des **heures** (HH) et **minutes** (MM).

Si la date ne doit pas être changée, l'heure sera affichée directement en appuyant sur la touche ➡, qui est aussi utilisée pour revenir à la date. La modification de l'heure et de la date sont prises en compte à l'appui sur la touche ⓓ, ensuite les secondes seront remises à zéro et l'affichage est mis à jour.

☑ Nota: Ce Menu n'est pas accessible dans un système en mode Intégré HISEC, dans ce cas la mise à l'heure et date se fera dans le menu Intrusion (*Menu 41*).

Menu 55





Le Menu 55 vous permet de corriger une éventuelle "dérive" de l'horloge du système, il est nécessaire d'ajuster la vitesse de l'horloge avec un facteur calculé sur une semaine.

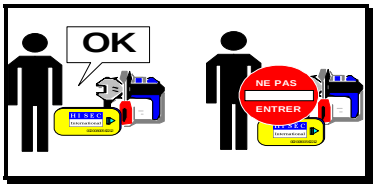
Quatre chiffres seront entrés après l'appel de ce menu, le premier chiffre peut seulement être 0 ou 1 et il indique si l'horloge doit être ajustée en avance (positive) ou en retard (négative).

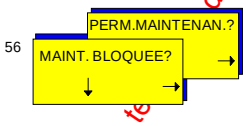
0 indique une correction négative (l'horloge tournera plus lentement).
1 indique une correction positive (l'horloge tournera plus vite).

Les 3 chiffres suivants sont la quantité de secondes à incorporer à l'horloge pour l'accélérer (ou la ralentir) par **semaine**. L'ajustement maximum est de 120 secondes.

☑ Nota: Ce Menu n'est pas accessible dans un système en mode Intégré HISEC, dans ce cas la mise à l'heure et date se fera dans le menu Intrusion (*Menu 41*).

Menu 56





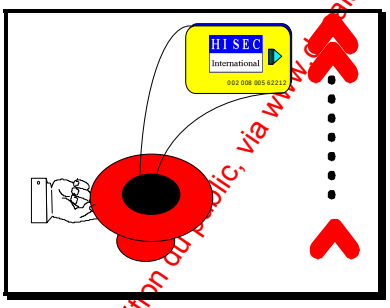
Le Menu *56* vous permet d'autoriser (ou d'empêcher) l'utilisation du badge de maintenance.

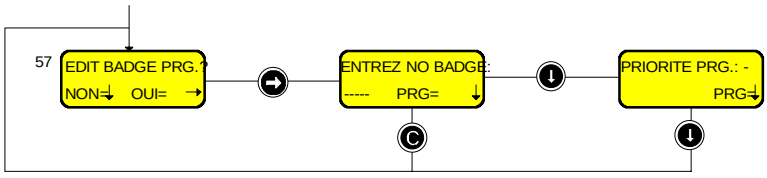
L'affichage dépend de l'état actuel du système, c'est à dire si le mode Maintenance est déjà autorisé ou non.

Si le mode Maintenance est autorisé, le texte "MAINT. BLOQUEE.?." apparaîtra et par la réponse OUI=➔, le texte sera changé et la Maintenance ne sera pas plus longtemps autorisée.

Si le mode Maintenance n'est pas autorisé, le texte "PERM. MAINT ?." apparaîtra et par la réponse OUI=➔, le texte sera changé et le mode Maintenance sera maintenant autorisé.

Menu 57





Le Menu 57 vous permet d'attribuer (ou de changer) la priorité affectée à un badge. Le badge devra avoir été **créé précédemment** par le *Menu 41* pour pouvoir être affecté d'une nouvelle priorité.

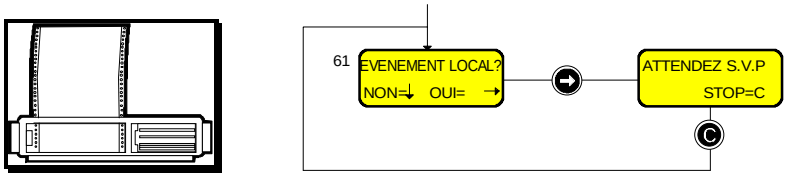
☑ Un badge avec un niveau de priorité supérieur à 0 est appelé Badge de Programmation et peut avoir accès à certains menus. Dans le *Panorama des Menus Contrôle d'accès Chapitre 10.2* est indiquée sur chaque menu la priorité (Px) nécessaire pour accéder à ces menus.

11.6 Menu Principal 60

Ce Menu vous permet d'imprimer le journal (historique) des événements locaux, les alarmes globales, les groupes de Personnel et de la programmation complète du système.

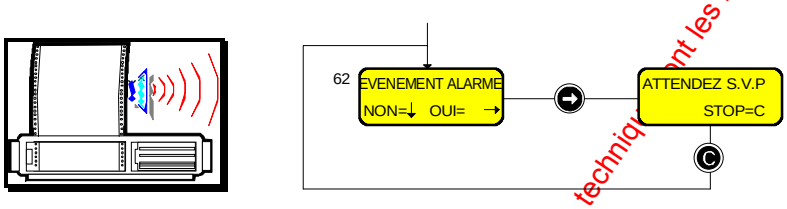
Après l'activation d'un de ces menus, au bout de 12 secondes, l'afficheur revient au menu principal et le lecteur de badges peut être utilisé normalement pendant l'impression. Si vous voulez arrêter l'impression, il suffit de revenir au menu à nouveau et appuyer sur la touche C, comme illustré dans les écrans suivants.

Menu 61



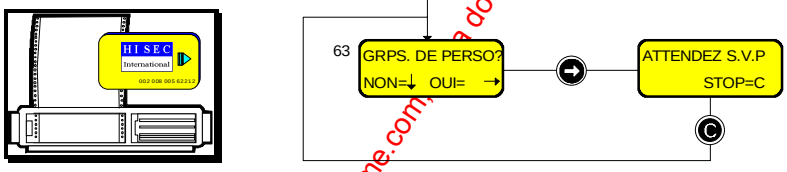
Le Menu 61 vous permet d'imprimer la totalité de l'historique des événements du lecteur ou l'opération a été demandée.

Menu 62



Le Menu 62 vous permet d'imprimer la totalité de l'historique (global) des alarmes du système complet et ceci sur n'importe lequel des lecteurs.

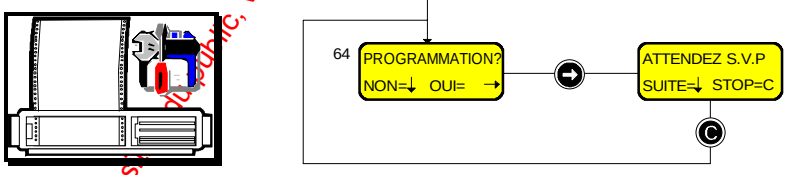
Menu 63



Le Menu 63 vous permet d'imprimer les badges et des groupes de personnel auquels ils appartiennent.

Tous les badges programmés seront triés et imprimés avec leurs N° de Groupe de Personnel. En commencant par tous les badges relatifs au groupe N°1, puis les badges relatifs au groupe N°2, etc.

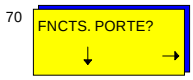
Menu 64



Le Menu 64 vous permet d'imprimer la totalité de la programmation du système HISEC contrôle d'accès, programmes hebdomadaires, groupe de personnel, etc.

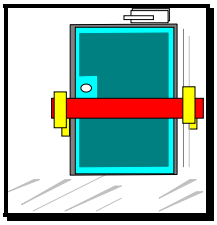
L'appui sur la touche ↓ (SUITE) permet de passer au chapitre de la programmation suivant, de façon à obtenir exactement l'impression des parties de la programmation souhaitées.

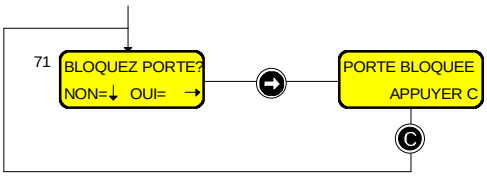
11.7 Menu Principal 70



Ce menu vous permet d'outrepasser les fonctions de contrôle automatique de la porte en bloquant, libérant en permanence ou revenant à un fonctionnement normal.

Menu 71

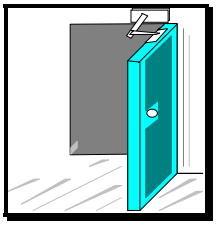


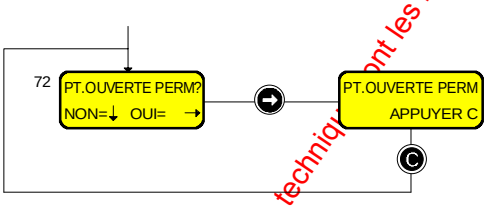


Le Menu 71 vous permet de bloquer le lecteur (plus personne ne peut entrer sur cette porte).

Quand la porte est bloquée en permanence, le message "PORTE BLOQUEE" sera affiché comme un message de défaut à toute personne qui essayera de réaliser un passage normal de la porte.

Menu 72

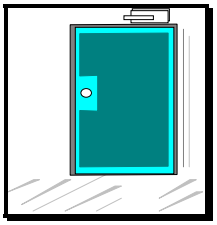


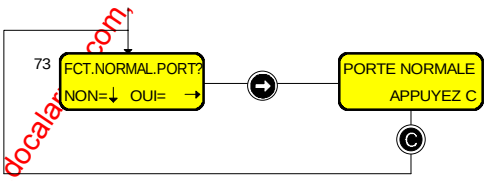


Le Menu 72 vous permet de commander la libération permanante de la porte (accès libre).

Quand la porte est ouverte en permanence, le message "PT.OUVERTE PERM." sera affiché comme un message de défaut à toute personne qui essayera de réaliser un passage normal de la porte.

Menu 73





Le Menu 73 vous permet de remettre la porte dans un mode de fonctionnement normal.

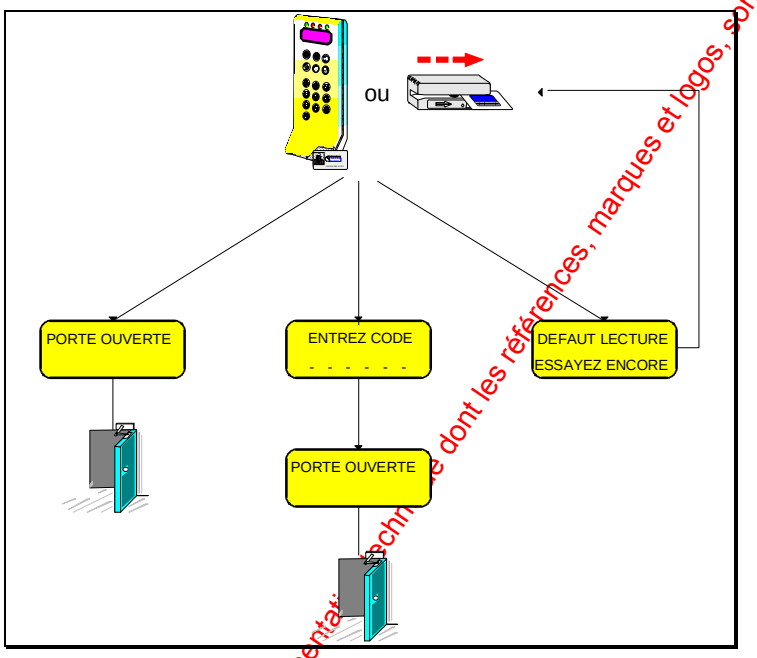
Après l'usage des *Menus 71* et *72*, il est nécessaire d'utiliser ce menu pour revenir au contrôle normal de la porte.

Chapitre 12: Utilisation quotidienne du système Contrôle d'accès

Attention ! Si vous voulez programmer ou tester le système il est impératif d'appuyer sur la touche ➔ avant de lire votre badge. Cela vous donne accès aux menus, en cas contraire vous effectuez uniquement une tentative d'ouverture de porte.

12.1 Accès normal

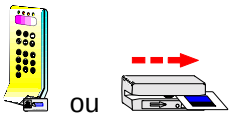
Lisez votre badge sur le lecteur ou la tête déportée :

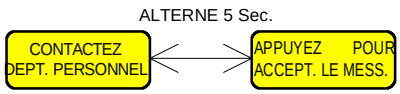


☑ Nota : Vous disposez de 10 tentatives pour entrer votre code personnel. Après cela votre badge sera bloqué et vous n'aurez plus accès. Ce nombre de 10 tentatives peut uniquement être modifié par votre installateur.

12.2 Messages

Si quelqu'un a programmé un message à votre destination, il sera affiché après la lecture de votre badge et devra être acquitté avec la procédure suivante:

- Lisez votre badge sur le lecteur ou tête déportée ---------- 

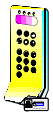
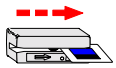
  - ♦ L'afficheur indique:---------- 

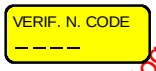
- Appuyer sur la touche ➔ pour accepter le message.

  Sans acquittement, la porte ne s'ouvrira pas et le message sera proposé à la prochaine utilisation du badge.
- La porte s'ouvre---------- 

12.3 Programmation de votre code Personnel

Si votre badge a été défini pour utiliser un code personnel, le système vous interroge à la première utilisation du badge pour que vous choisissiez un code personnel. Utilisez la procédure suivante:

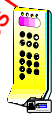
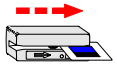
- Lisez votre badge sur le lecteur ou tête déportée ----------  ou 
  - ♦ L'afficheur indique:---------- 

- Entrez le **nouveau** code personnel---------- ex : 
  - ♦ L'afficheur indique:---------- 

- Confirmez votre **nouveau** code personnel---------- ex : 
- Le système a enregistré votre nouveau code et la porte s'ouvre 

12.4 Changement de votre propre code Personnel

Vous pouvez changer votre code personnel chaque fois que vous le désirer, en utilisant la procédure suivante:

- Lisez votre badge sur le lecteur ou tête déportée ----------  ou 
  - ♦ L'afficheur indique:---------- 

- Entrez le code personnel **spécial** ---------- 
  - ♦ L'afficheur indique:---------- 

- Entrez votre **ancien** code personnel---------- ex : 
  - ♦ L'afficheur indique:---------- 

- Entrez le **nouveau** code personnel---------- ex : 
  - ♦ L'afficheur indique:---------- 

- Confirmez votre **nouveau** code personnel---------- ex : 
- Le système a enregistré votre nouveau code et la porte s'ouvre 

☑ Nota : Le code personnel Contrôle d'accès peut avoir 4 ou 6 chiffres, en fonction du nombre de tirets apparaissant sur l'afficheur.

12.5 Messages d'alarme

Les messages d'alarmes du contrôle d'accès peuvent avoir un rapport avec votre badge (bloqué, illégal, hors-temps, etc.) ou avec l'état de la porte (bloquée, maintenue, forcée, etc.). L'afficheur indique le message à la lecture de votre badge, ou en permanence en cas d'alarme de porte.

Les alarmes contrôle d'accès ne nécessitent pas d'acquittement, le retour à l'état normal est considéré comme un acquittement.

Chaque alarme pourra être consultée au moyen du Menu 32 - Voir toutes les alarmes.

3. Système Intégré

Chapitre 13: Utilisation quotidienne du système Intégré

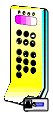
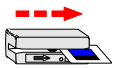
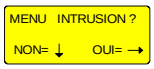
13.1 Les fonctions du terminal et du lecteur de badges dans le système intégré

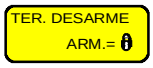
Se reporter aux chapitres 2.1 et 7.1 pour les descriptions respectives du terminal et du lecteur de badge. Le fonctionnement du terminal est identique dans un système intégré à celui décrit dans le système intrusion. Toutes les fonctions décrites dans la première partie de ce document restent valables.

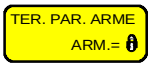
Les possibilités du lecteur de badge sont sensiblement différentes, dans un système intégré. Le lecteur de badge n'est pas uniquement utilisé pour contrôler les portes, mais aussi pour toutes les fonctions du système d'intrusion.

Si vous voulez accéder à une pièce du bâtiment, lisez votre badge comme dans un système contrôle d'accès classique (Voir le chapitre 12.1 "Accès Normal").

Si vous voulez exploiter le système intrusion, utilisez la procédure suivante:

- Appuyez sur la touche ----------
- Lisez votre badge sur le lecteur ou tête déportée -------  ou 
- Entrez votre code personnel ---------- ex : ☞ ❶ ❺ ❷ ❼ (x x)
  - ♦ L'afficheur indique: ---------- 

- Appuyer sur la touche----------
  - ♦ L'afficheur indique: ---------- 

    ou 

- Vous êtes maintenant dans le système Intrusion.

  ☞ Suivre les instructions de la 1ere partie de ce Manuel.

☞ **Nota: si vous voulez accéder aux menus contrôle d'accès, suivre la même procédure et répondre NON au MENU INTRUSION? puis Oui au MENU ACCES?, le menu 10 contrôle d'accès est alors affiché.**

☞ **Suivre les instructions de la 2eme partie de ce Manuel.**

13.2 Armement et désarmement Intrusion dans un système intégré

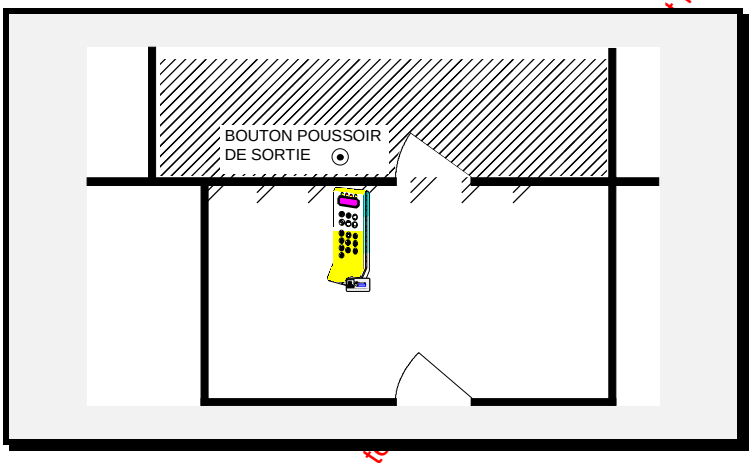
Quand un système HISEC contrôle d'accès est intégré avec un système Intrusion HISEC, il est possible à certaines personnes d'armer et désarmer le système au moyen du lecteur de badges.

Du fait que le contrôle d'accès utilise différents types de lecteurs de badges dans des configurations diverses, la procédure n'est pas identique sur tous les systèmes. Les chapitres suivants décrivent pour chaque configuration, la procédure pour armer et désarmer. Vérifiez quelle est la configuration qui correspond à votre cas particulier.

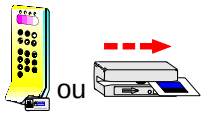
Se reporter aux chapitres 2.1 et 7.1 pour la description du Terminal et du Lecteur de badge.

Le fonctionnement du terminal est identique dans un système intégré à celui décrit dans le système intrusion. Toutes les fonctions décrites dans la première partie de ce document sont toujours valables.

13.2.1 Situation N°1 : Armement et Désarmement sur le Lecteur de badge

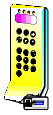
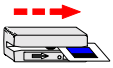


Armement:

- Lisez votre badge sur le lecteur ou tête déportée ---------  ou
- Entrez votre code personnel ---------- ENTREZ CODE ------ ex: ☞ ❶❺❷❼(xx)
- L'afficheur indique:---------- PORTE OUVERTE
- Appuyez sur la touche ---------- (porte fermée) 
- L'afficheur indique:---------- TERRITOIRE ARME PORTE FERMEE ou SYSTEME ARME PORTE FERMEE

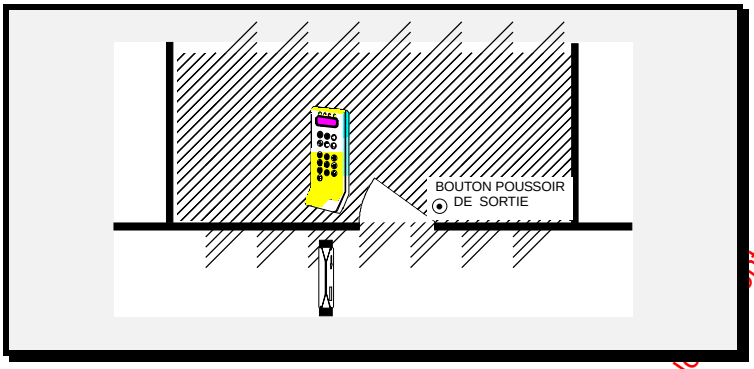
☞ **Nota : dans cette configuration, le lecteur de badges sera à l'extérieur de la zone protégée, du fait que la porte est fermée avant l'armement.**

Désarmement:

- Lisez votre badge sur le lecteur ou la tête déportée----  ou 
- Entrez votre code personnel ---------- ENTREZ CODE ------ ex: ☞ ❶❺❷❼(xx)
- L'afficheur indique:---------- TERRITOIRE ARME D.ARM.=🔒 *OU* SYSTEME ARME D.ARM.=🔒
- Appuyez sur la touche ---------- 🔒 ---------- 
- L'afficheur indique:---------- PORTE OUVERTE TER. DESARME ----- 

Il est maintenant possible d'accéder aux locaux.

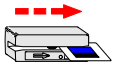
13.2.2 Situation N°2 : Armement et Désarmement sur un Terminal intérieur et tête de lecture extérieure



Armement:

- Entrez votre code personnel **Intrusion**---------- ex : ☞ ❶ ❺ ❷ ❼ ❾ ❷
- L'afficheur indique:---------- TER. DESARME ARM.= 0 *OU* TER. PAR. ARME ARM.= 0
- Appuyez sur la touche ---------- 🔒
- L'afficheur indique:---------- TERRITOIRE ARME SORTEZ SVP *OU* SYSTEME ARME SORTEZ SVP
- Appuyez sur la touche ---------- Ⓒ
- La temporisation de sortie est lancée. ----------
- Appuyez sur le bouton poussoir de sortie----------
- La porte est ouverte, quittez la pièce. ----------
- Refermez la porte----------

Désarmement:

- Lisez votre badge sur la tête déportée----------

- La porte s'ouvre ----------

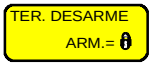
- Entrez pour lancer la temporisation d'entée ----------

- Appuyez sur n'importe quelle touche du terminal -------

- Entrez votre code personnel **Intrusion** ---------- ex :

- L'afficheur indique:----------


- Appuyez sur la touche ----------

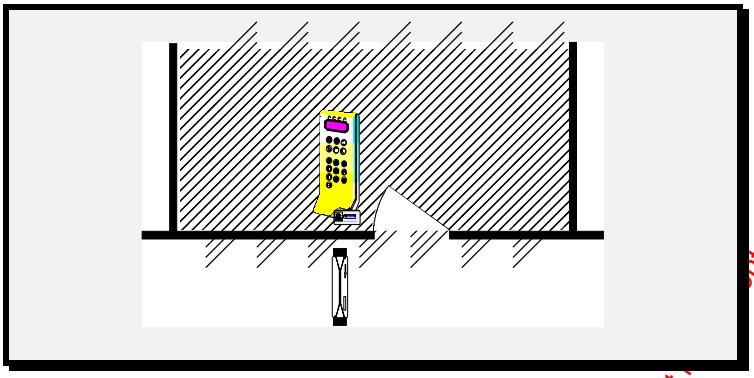
- L'afficheur indique:


- Appuyez sur la touche ----------

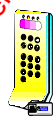

Il est maintenant possible d'accéder aux locaux.

☑ Nota : Vous disposez d'un temps pré-programmé pour désarmer le système. Si vous dépassez la temporisation d'entrée, le système génère une alarme intrusion.

13.2.3 Situation N°3 : Armement et Désarmement sur un Lecteur intérieur et tête de lecture extérieure



Armement:

- Lisez votre badge sur le lecteur ---------- 
  - ♦ Si votre badge est programmé pour utiliser un code personnel

    Entrez votre code personnel 

ex: ☞ ❶❺❷❼(xx)
- L'afficheur indique:---------- 

- Appuyez sur la touche ---------- 
  - ♦ Si cela n'a pas été fait précédemment à l'étape 2

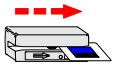
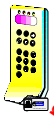
    Entrez votre code personnel---------- 

ex: ☞ ❶❺❷❼(xx)
- L'afficheur indique:---------- 

- La temporisation de sortie est lancée---------- 
- La porte est ouverte, quittez la pièce---------- 
- Refermez la porte---------- 

Vous devez avoir refermé la porte avant la fin de la temporisation de sortie.

Désarmement:

- Lisez votre badge sur la tête déportée---------- 
- La porte s'ouvre ---------- 
- Entrez pour lancer la temporisation d'entrée ---------- 
- Lisez votre badge sur le lecteur intérieur---------- 
- L'afficheur indique: TERRITOIRE ARME D.ARM.=🔒 *OU* SYSTEME ARME D.ARM.=🔒
- Appuyez sur la touche ---------- 
- Entrez votre code personnel ---------- ENTREZ CODE ------ ex: ☞ ❶❺❷❼(XX)
- L'afficheur indique: PORTE FERMEE TER. DESARME

Il est maintenant possible d'accéder aux locaux.

Glossaire

Acquittement d'alarme : L'acquittement d'alarme est l'effacement d'un message d'alarme au moyen d'un terminal ou lecteur. Cela est nécessaire pour permettre de préparer le détecteur (en alarme) à pouvoir générer une nouvelle alarme.

Afficheur : L'afficheur est l'interface entre l'utilisateur et le système. Il donne les instructions, informations et descriptions sur 2 lignes de 16 caractères alphanumériques.

Anti-Retour: L'Anti-Retour est un système qui enregistre où se trouvent les personnes en permanence. Pour réaliser cela, des lecteurs sont placés à chaque passage d'une zone à l'autre. Il empêche d'effectuer deux entrées ou sorties successives avec le même badge sur une même porte et oblige à entrer et sortir par les portes contrôlées. Pour entrer dans une zone, l'utilisateur doit impérativement lire son badge sur un lecteur. S'il ne réalise pas cela et qu'il entre (ou sorte) d'une zone en passant avec quelqu'un d'autre par exemple, il se renferme lui-même: étant donné que le système le considère dans une zone différente de celle où il est réellement et il lui bloquera la porte à la prochaine lecture de son badge.
L'Anti-Retour est une restriction qui peut être nécessaire pour augmenter le niveau de sécurité.

Base de données : Le système HISEC possède plusieurs bases de données, que ce soit dans l'unité centrale ou dans les lecteurs de badges. Ces bases de données contiennent toutes les informations programmées, par exemple, les noms des détecteurs, des zones, les N° de badges et leur programmation.

Batteries : Les batteries sont le système d'alimentation de secours en cas de disparition du secteur. Ces batteries sont rechargées par le système HISEC et sont logées dans le coffret de l'unité centrale.

Code personnel : L'utilisateur ne peut opérer sur le système sans l'entrée préalable d'un code personnel. Ce code est de 6 chiffres dans le système intrusion et 4 ou 6 dans le système contrôle d'accès. Le code personnel est une donnée strictement confidentielle et ne doit être connu que de vous.

Contrôle d'accès : Ce nom est le dénominateur commun à l'ensemble des éléments nécessaires pour contrôler et enregistrer les mouvements de personnes et les entrées sorties d'un bâtiment, au moyen de lecteurs, boutons poussoir de sortie, imprimante, contact de portes, etc.

Défaut système : Alarme défaut technique. Les défauts systèmes sont affichés sur le terminal et les lecteurs contrôle d'accès.

Défilement automatique : Procédure automatique d'affichage des alarmes, défauts et éjections permettant au personnel non coutumier du système de consulter les informations sans effectuer de manipulation autre que l'entrée de leur propre code.

Détecteurs : Les détecteurs sont les "yeux et oreilles" du système d'alarme. Ils sont directement raccordés à la carte processeur du système. Il existe différents types de détecteurs, qui ont été divisés en plusieurs catégories en fonction de leur principe. Nous pouvons distinguer :
- Détecteur de mouvement (infrarouge, hyperfréquence)
- Détecteur d'ouverture magnétique pour portes et fenêtres
- Détecteur de bris de vitres
- Détecteur sismique (détecteur de vibration)

Ejection : L'éjection de détecteur permet d'isoler ceux ci pour une durée temporaire. Cela peut être nécessaire pendant une modification des locaux ou pour la maintenance.

Entrée : Elément ayant la possibilité de connecter un détecteur.

Entrée en session: L'entrée en session vous permet d'avoir accès au système au moyen d'un code personnel (intrusion) ou d'un badge (contrôle d'accès). Cette opération est indispensable avant toute manipulation, car c'est elle qui identifie l'opérateur.

Fin de session : La fin de session est le moyen de quitter le terminal (ou lecteur) après avoir effectué les manipulations, elle est réalisée par une série d'appuis sur la touche Ⓒ. Le système effectue une fin de session forcée après 2 minutes sans manipulation sur le clavier.

Fonction armement : Les fonctions d'armement se réfèrent à la possibilité d'un opérateur d'armer ou désarmer le système intrusion sur un lecteur de badges du contrôle d'accès. Les utilisateurs avec la fonction "premier entré/dernier sorti" auront la possibilité de bloquer et débloquer le lecteur contrôle d'accès.

Groupe de personnel : Un groupe de personnel est une association de badges ayant les mêmes droits d'accès, restrictions et fonctions. Le système peut avoir un max. de 250 groupes de Personnel. Un groupe de personnel peut être constitué d'une ou plusieurs personnes.

Historique : Toutes les manipulations, défauts et messages d'alarmes sont enregistrés dans l'historique du système. Cet ensemble d'événement - historique - peut être consulté sur l'afficheur des lecteurs et terminaux ou encore sur l'imprimante du système. L'historique du système Intrusion a une capacité de 1000 événements. Le contrôle d'accès a scindé son historique en 2 parties distinctes, historique local et global.

Historique Global : Tous les défauts et messages d'alarmes sont enregistrés dans l'historique du système. Chaque lecteur possède son propre historique, mais les alarmes du système complet sont enregistrées dans l'historique global. Cet historique a une capacité de 100 alarmes.

Historique Local : Toutes les manipulations, défauts et messages d'alarmes sont enregistrés dans l'historique du système. Chaque lecteur possède un historique individuel où sont enregistrées toutes les informations qui lui son propre. En fonction du type de lecteur, cet historique peut avoir une capacité de 1000 ou 2300 événements.

Intégré : Ce terme désigne la combinaison sur un même site des systèmes HISEC Intrusion et HISEC Contrôle d'accès.

Lecteur de badges: Le lecteur contrôle d'accès est une unité intelligente permettent de surveiller et de commander l'ouverture des portes. Il possède sa base de données, peut afficher les messages et les instruction opératoires et bien sûr de lire les badges. De plus, le lecteur de badges peut être utilisé comme terminal intrusion dans les systèmes intégrés.

LED : Abréviation pour diode électroluminescente. Signal lumineux des terminaux et lecteurs pour informer sur l'état du système.

Logique : Ce terme est utilisé pour définir la façon dont ont été programmés les territoires (Voir Chapitre 1).

Menus : Les menus sont l'interface de dialogue avec l'opérateur et constituent le programme proprement dit. Dans ce programme sont contenues les données et instructions relatives aux états et manipulations du système. Les menus du système HISEC sont affichés sur l'écran des terminaux et lecteurs de badges.

Message d'alarme : Un message d'alarme peut être:

1. Un message affiché sur l'écran du terminal ou Lecteur
2. Une sirène et/ou dispositif optique (flash)
3. Un message vers une centrale de réception d'alarme (si raccordé)
4. Un Buzzer de terminal ou lecteur de badges

Niveau de priorité : Le niveau de priorité indique les possibilités données à un opérateur sur le système. Il existe 5 niveaux de priorités (P0 à P4) dans le système intrusion et 4 niveaux de priorité (P0 à P3) dans le système contrôle d'accès. Plus le chiffre est élevé et plus l'opérateur a de possibilités sur le système. Les niveaux sont indiqués par la lettre P suivi du chiffre. Votre installateur doit vous avoir donné les niveaux de priorité définis à l'installation. Voir les chapitres 3.2 "Liste des niveaux de priorités Intrusion" et 9.7 "Liste des niveaux de priorité Contrôle d'accès" pour connaître les possibilités respectives de ces différents niveaux de priorité.

Physique : Ce terme est utilisé pour définir la façon dont ont été programmés les territoires (Voir Chapitre 1).

Premier entré/Dernier sorti : Ce terme est utilisé pour définir les badges qui seront autorisés à bloquer le lecteur quand ils quittent les locaux (dernier sorti) et à débloquer le lecteur à leur arrivée (premier entré).

Programme hebdomadaire : Un programme hebdomadaire est constitué de périodes de temps pour tous les jours de la semaine et 2 jours spéciaux. Chaque jour de la semaine programmé peut être divisé en un maximum de 8 périodes ayant chacune une fonction attribuée.
Par exemple, un accès permis les jours ouvrables de 8H à 17H, de façon à interdire l'accès au bâtiment après 17H et avant 8H. Si un utilisateur essai d'entrer dans le bâtiment en dehors de la période son badge sera refusé et la tentative enregistrée dans l'historique du lecteur.

Responsable système : Le système effectue une distinction entre les différents utilisateurs. Le responsable système est la personne qui a le plus de possibilités - après le superviseur - sur le système intrusion. En général, il existe un seul superviseur et plusieurs responsables système, surtout sur les sites de grande taille.

Sorties : Les sorties donnent la possibilité de connecter les flashs, sirènes, verrouillage, transmetteurs, gâches électriques, etc. au système HISEC.

Station Centrale de télésurveillance : Pour transmettre ce que l'on appelle "les alarmes silencieuses" le système d'alarme doit être raccordé à une station centrale de télésurveillance. Cette liaison est réalisée au moyen d'un transmetteur d'alarme raccordé sur le réseau téléphonique. Tous les messages reçus sont automatiquement enregistrés et si nécessaire affichés sur l'écran de l'opérateur, qui prendra les mesures adaptées à l'information.

Superviseur : Le système effectue une distinction entre les différents utilisateurs. Dans le personnel interne (l'intervenant et technicien appartiennent au personnel externe) le superviseur est la personne qui a le plus de possibilités sur le système intrusion. Il est hautement responsable du système intrusion et est la personne à contacter en cas de dommages. Le superviseur a une priorité de niveau 2.

Système Intrusion : Ceci est le terme général pour l'ensemble des éléments nécessaires à protéger un bâtiment contre les tentatives d'intrusion. Cet ensemble peut être divisé en 3 parties:
- détection (détecteurs volumétriques, bris de vitres, boutons hold-up, etc.)
- exploitation (terminaux, lecteurs de badges, unité centrale)
- alarmes (sirènes, flashs, transmetteurs numériques)

Voir aussi le synoptique du système HISEC en Introduction.

Temporisation d'entrée : La temporisation d'entrée est la durée dont vous disposez pour mettre hors service le système intrusion à l'entrée dans le bâtiment. Cette durée est programmée par votre installateur et peut aller de quelques secondes à plusieurs minutes. Elle est démarrée à votre entrée dans le bâtiment.

Temporisation de Sortie : La temporisation de sortie est la durée dont vous disposez pour quitter le bâtiment après une mise en service du système intrusion. Cette durée est programmée par votre installateur et peut aller de quelques secondes à plusieurs minutes. Elle est démarrée après que la dernière personne quittant le bâtiment ait armé le système.

Terminal : Ensemble constitué d'un clavier et d'un afficheur. Toutes les opérations du système Intrusion peuvent être réalisées sur le terminal.

Territoire : Un territoire est une "surface" utilisateur. Cela permet de déterminer quelle partie de l'installation un opérateur est autorisé à armer ou désarmer; il est constitué d'une ou plusieurs zones. Le nombre maximum de territoires est de 250; le nombre max. d'utilisateurs est aussi de 250. Il est possible aux utilisateurs de partager le même territoire. De cette façon, il est possible par ex d'attribuer 50 utilisateurs à un même territoire.
Les employés de la production ont, par exemple, le département production et la réception dans leur territoire. Ces deux parties constituent alors leur territoire. Si le directeur a accès à toutes les parties du bâtiment, alors son territoire comprendra toutes les zones du bâtiment.

Transmetteur d'alarmes : Tous les messages d'alarmes, défauts et manipulations peuvent être transmis à une station centrale de télésurveillance. Cette transmission est réalisée au moyen d'un numéroteur automatique appelant la station centrale. Ce transmetteur travaille en général avec une ligne téléphonique. Dans le système HISEC, ce transmetteur peut être incorporé au système (Carte de communication INCOM) ou extérieur.
Le transmetteur a toujours la priorité sur la ligne et gére les appels "entrant" et "sortant".

Unité centrale : L'unité centrale est le "coeur" du système intrusion. Dans son boîtier, sont inclues la carte processeur, les batteries et l'alimentation secteur. Tous les éléments du système comme les détecteurs, terminaux, lecteurs de badges et dispositif de signalisation d'alarme (sirènes) sont connectés à l'unité centrale.

Zone : Une zone est définie comme une partie matérielle de bâtiment. Une zone comporte en général plusieurs détecteurs. Une zone peut être constituée d'une pièce (par ex. Département ventes), mais aussi d'un groupe de pièces (par ex. direction, département forces de ventes et services techniques). Le nombre max. de zones est de 16. Pour les sites importants, cela permet de réaliser des zones comprenant de larges surfaces. La subdivision du bâtiment en zones est à la charge de votre installateur pendant la phase d'installation du système.

Index

NOTES PERSONNELLES

Denmark	United Kingdom	France	Spain	Netherlands
HI SEC International A/S Tempovej 42, DK- 2750 Ballerup Denmark	HI SEC International Ltd. 4B Victoria Avenue, Camberley, Surrey GU15 3HX United Kingdom	HI SEC International ZAC de Nanteuil, 12, rue Jules Ferry, F-93561 Rosny sous Bois France	HI SEC International Security S.L. C/. Ávila, 48-50 3° Planta, local G-H E-08005 Barcelona España	HI SEC International B.V. Populierendreef 968B, NL-2272 HW Voorburg Netherlands
Tel.: +45 44 86 05 05 Fax: +45 44 86 05 00 E-mail: dk @ hisec.com	Tel.: +44 (0) 1276 679 950 Fax: +44 (0) 1276 679 949 E-mail: gb @ hisec.com	Tel.: +33 (0) 1 48 12 90 10 Fax: +33 (0) 1 48 12 90 20 E-mail: fr @ hisec.com	Tel.: +34 93 300.46.95 Fax: +34 93 485.60.78 E-mail:	Tel.: +31 (0) 70 386 1103 Fax: +31 (0) 70 387 4095 E-mail: nl @ hisec.com