

## SYSTÈME D'ACCÈS PAR CARTES TX3-CX



## Manuel d'Installation et d'Utilisation



Copyright novembre 2018 Mircom Inc. Tous droits réservés.

Manuel d'Installation et d'Unitilsation de la série TX3 de marque Mircom, v.5

Microsoft, MS-DOS, Windows, et Windows 2000/NT/XP/Vista/7/8/10 sont des marques de commerce déposées ou des marques de commerce de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Mircom 25 Interchange Way Vaughan, Ontario L4K 5W3 905.660.4655 Fax:905.660.4113

http://www.mircom.com



## Contents

- 1.1 Introduction au système d'accès par carte TX3-CX 6
- 1.2 Applications 6
- 1.3 Fonctions configurables **7**
- 1.4 Responsabilités de l'installateur 8
- 1.5 Configuration du réseau 8
- 1.6 À propos de ce manuel **10**
- 1.7 Contactez-nous 12

#### 2 Fonctions configurables 13

- 2.1 Entrées 13
- 2.2 Corrélations 14
- 2.3 Critères d'accès 16
- 2.4 Temporisations 23
- 2.5 Horaires 25
- 2.6 Jours fériés 26
- 2.7 État du système 26

#### 3 Installation et configuration 27

- 3.1 Mise à la terre du système d'accès par carte 27
- 3.2 Installation du contrôleur et des composants 28
- 3.3 Composantes de la carte contrôleur 32
- 3.4 Raccordement des entrées 37
- 3.5 Raccordement des sorties **41**
- 3.6 Raccordement du lecteur de carte 44
- 3.7 Réglages des commutateurs DIP SW2 46
- 3.8Réglages des cavaliers48
- 3.9 Alimenter contrôleur 48
- 3.10 Mise à jour du micrologiciel 48
- 3.11 Commencer à configurer 49

#### 4 Réglages du commutateur DIP d'adressage 51

#### Bloc d'alimentation TX3-CX-2 et calculs de batterie 54

- 5.1 Nombre de fois que la porte est ouverte par heure 54
- 5.2 Courant total de verrouillage de porte 55
- 5.3 Exigences de capacité de batterie 55
- 5.4 Sélection de batterie 55

#### Information sur la garantie et mise en garde 56

#### Avis spéciaux 61

5



## List de Figures

- Figure 1. Système d'accès par cartes de base 8
- Figure 2. Réseau de système d'accès par cartes 9
- Figure 3. Système d'accès par cartes utilisant un réseau Ethernet TCP/IP. Les contrôles connectés à un réseau Ethernet sont des nœuds principaux 9
- Figure 4. Système d'accès par cartes utilisant un réseau Ethernet et des réseaux RS-485 10
- Figure 5. Dimensions du capotage arrière du contrôleur et l'emplacement de composant facultatif 28
- Figure 6. Emplacement de la carte modem **30**
- Figure 7. Emplacement de la carte de module IP 31
- Figure 8. Module MD-993 31
- Figure 9. Emplacement des connexions de la carte contrôleur 34
- Figure 10. Alimentation électrique 35
- Figure 11. Câblage de la batterie de la carte contrôleur 36
- Figure 12. RS-485 37
- Figure 13. Bornes d'entrée de la carte contrôleur **38**
- Figure 14. Exemple de connexions des bornes d'entrée 38
- Figure 15. Entrée Mode de contrôle Ouvert 40
- Figure 16. Entrée Mode de contrôle fermé 40
- Figure 17. Entrée-surveillance des états fermés ouverts 41
- Figure 18. Exemple de raccordement aux bornes de sortie du contrôleur 43
- Figure 19. Exemple de raccordement aux sorties 7 et 8 44
- Figure 20. Les connecteurs de lecteur de carte de la carte contrôleur 45
- Figure 21. Emplacement des cavaliers JW1 JW5 et des commutateurs SW1 et SW2 47



# Bienvenue

Ce manuel fournit des informations sur l'installation et l'utilisation du système d'accès par carte TX3-CX ; Il doit être lu intégralement avant d'entamer l'installation.

L'installation doit être effectuée par un technicien qualifié conformément aux normes et aux avis spéciaux fixés par les instances de régulation locales.

#### Remarque: Mircom met à jour, périodiquement, le logiciel et le micrologiciel du panneau, afin d'ajouter des fonctions ou de corriger des incohérences mineures. Visitez le site web de Mircom, au www.mircom.com, pour se renseigner sur les tous nouveaux micrologiciels et logiciels.

Pour tout renseignement sur la garantie et les avis spéciaux, se référer au chapitre Garantie et avis spéciaux, à la page 56.

#### Avertissement: Le système d'accès par carte doit être mis à la terre par un technicien qualifié. Un système mis à terre incorrectement peut entraîner la défaillance de l'équipement et une électrocution.

#### Ce chapitre décrit:

- Introduction au système d'accès par carte TX3-CX
- Applications
- Fonctions configurables
- Responsabilités de l'installateur
- Configuration du réseau
- À propos de ce manuel
- Contactez-nous

Mircom<sup>®</sup>

## 1.1

# Introduction au système d'accès par carte TX3-CX

Le système d'accès par carte TX3-CX compte parmi la gamme de produits de Mircom qui fournit des solutions spécifiques aux bâtiments - des solutions de surveillance, de contrôle et de sécurité intégrées; des solutions applicables dans les tours d'habitation et les grands ensembles résidentiels.

Le système d'accès par carte répond aux exigences du marché de grands ensembles résidentiels; une nécessité de trouver des utilitaires de configuration et des systèmes d'accès faciles à utiliser.

Ce manuel fournit au technicien des informations sur l'utilisation et la configuration du système d'accès par carte; il explique comment configurer divers composants d'un système nouvellement installé ou comment modifier ceux d'un système déjà existant.

## 1.2 Applications

Le système d'accès par carte de Mircom comprend un contrôleur, deux lecteurs de carte et un logiciel configurateur. Le contrôleur accepte, à la fois, différents types de lecteurs de cartes pour contrôler deux portes ou deux points d'accès. Le système d'accès par carte peut contrôler l'utilisation de l'ascenseur, si les commandes d'ascenseur sont utilisées.

De différents lecteurs de cartes sont supportés - tel que le récepteur sans fil Wiegand TX3-CX-REC - tous configurables, par biais du logiciel configurateur.

Le système d'accès par carte peut être utilisé en mode autonome ou en réseau de point à point par le biais d'une connexion RS-485 (en série).

Ce réseau peut comporter seulement le contrôleur d'accès par carte ou une combinaison d'Écrans Tactiles et de modules de contrôle pour le hall, de restriction de l'utilisation de l'ascenseur et d'accès par carte, jusqu'à un maximum de 63 modules. Une adresse réseau valide varie entre une valeur de 1 à 63. Un des modules du réseau, qui est doté d'une horloge en temps réel - tels que l'Écran Tactile, le contrôle du hall ou l'accès par carte - doit avoir comme adresse la valeur 1.

#### 1.2.1 Interface Wiegand

L'interface Wiegand utilise un câblage standard pour les lecteurs de carte d'accès pour établir des connexions entre le lecteur de carte d'accès et le système d'accès par carte. Cette interface est une interface série, nécessitant 7 à 10 conducteurs pour établir une communication entre le lecteur et le contrôleur. Elle fournit, au lecteur, une tension de 12V.



La carte d'accès compatible Wiegand est dotée de 26 bits d'information. Le lecteur de carte d'accès lit et enregistre les informations programmées sur la carte et les renvoie au contrôleur en train de bits.

#### 1.2.2 Système d'accès par carte

Le système d'accès par carte de Mircom supporte la technologie d'encodage propriétaire 37 bits et le format SIA 26 bits ; il comprend un maximum de 63 contrôleurs d'accès par carte reliés en réseau. Chaque contrôleur d'accès par carte peut avoir deux lecteurs de cartes d'accès. Le système d'accès par carte offre, en option, une batterie de secours et une horloge en temps réel.

Le système d'accès par carte s'intègre avec le système d'accès par téléphone TX3; il suffit de connecter les deux systèmes à un réseau commun.

Un PC sert à configurer et à suivre, en ligne, l'état des systèmes d'accès par carte et d'intercom. Une fois ces systèmes configurés, le PC n'est plus nécessaire.

## 1.3 Fonctions configurables

Le système est configuré en raccordant les entrées et les sorties aux dispositifs de point d'accès et en utilisant le logiciel configurateur afin d'établir des corrélations entre les entrées et les sorties.

Une configuration physique supplémentaire est requise par le biais de commutateurs DIP et de cavaliers sur le contrôleur. Les commutateurs DIP établissent l'adresse réseau du contrôleur d'accès par carte. Les réglages du cavalier configurent le contrôleur pour les mises à jour du micrologiciel.

#### 1.3.1 Logiciel configurateur pour PC

Le logiciel configurateur TX3-MSW configure un système alliant un système d'accès par téléphone et un système d'accès par carte et utilise une base de données commune. Une fois le contrôleur est installé, le système applique les paramètres par défaut. Utilisez le logiciel configurateur afin de configurer intégralement le système. Référez-vous à la documentation suivante:

- LT-995FR TX3 Manuel de Configuration et d'Administration
- LT-973FR Systèmes d'accès par Téléphone Démarrage rapide du Configurateur



## 1.4 Responsabilités de l'installateur

L'installation et la mise en service doivent être effectuées par un technicien qualifié. Le technicien doit installer tous les composants du système, raccorder le câblage des entrées et des sorties aux portiers et s'assurer, en utilisant le logiciel configurateur, que le câblage répond aux exigences du système pour un bon fonctionnement.

## 1.5 Configuration du réseau

Le système de cartes d'accès peut comprendre des contrôles de cartes d'accès autonomes ou en réseau. Les contrôles de cartes d'accès en réseau peuvent communiquer sur un réseau RS-485, un réseau Ethernet TCP/IP ou une combinaison de réseau Ethernet avec des sous-réseaux RS-485. Tous les contrôles de cartes d'accès peuvent communiquer sur un réseau RS-485. Pour communiquer sur un réseau Ethernet, vous avez besoin d'au moins un contrôle de cartes d'accès avec capacité IP.

Le logiciel de configuration TX3 peut se brancher à n'importe laquelle de ces configurations de réseau. La façon d'établir la connexion à un réseau (c'est-àdire, par TCP/IP, USB, modem ou port de communication) détermine quels dispositifs pourront être configurés sur le réseau à l'aide de l'outil de configuration TX3. Les différentes configurations de réseau sont expliquées dans les prochaines parties de la présente section.

La figure 1 illustre un système d'accès par carte de base : un contrôleur d'accès par carte et deux lecteurs de carte. La distance maximale entre le contrôleur d'accès et le lecteur est de 152 m (500 ft).



#### Figure 1. Système d'accès par cartes de base

La figure 2 illustre deux contrôleurs d'accès par cartes, chacun avec deux lecteurs de carte d'accès, sur un réseau RS-485. Le système d'accès par cartes peut comprendre, au maximum, 63 contrôleurs d'accès reliés en réseau. Si vous

## Millin Mircom

vous branchez à un dispositif sur le réseau RS-485 (par USB, modem ou port de communication), vous pouvez également vous brancher à tout autre dispositif sur le réseau RS-485 et le configurer avec l'outil de configuration TX3.





La figure 3 montre une configuration avec les dispositifs TX3 connectés à un réseau Ethernet TCP/IP. Cette configuration élimine la limite de 63 dispositifs que vous avez sur un réseau RS-485. Les dispositifs connectés à un réseau Ethernet TCP/IP s'appellent des nœuds principaux. Lorsque vous établissez une connexion à un réseau TCP/IP avec l'outil de configuration TX3, vous pouvez vous connecter à tout nœud principal sur le réseau Ethernet TCP/IP et le configurer. Si vous vous connectez directement à un des nœuds principaux par USB, modem ou port de communication, vous serez en mesure de configurer ce dispositif, mais aucun autre.





Remarque: Afin qu'un panneau devienne un nœud principal, il doit répondre aux conditions suivantes :

- Il doit posséder une capacité IP. Les panneaux ayant une capacité IP comportent habituellement un « A », « B » ou « C » à la fin de leur nom de modèle.
- S'il ne s'agit pas d'un écran tactile, un module IP TX3-IP doit être installé.



La figure 4 montre un système d'accès par carte utilisant un réseau Ethernet TCP/ IP avec des sous-réseaux RS-485. Les contrôles de cartes d'accès connectés au sous-réseau RS-485 d'un nœud principal sont des nœuds esclaves au nœud principal. Chaque sous-réseau RS-485 peut accueillir jusqu'à 63 contrôleurs; vous pouvez toujours avoir plus de 63 nœuds principaux reliés au réseau Ethernet.



#### Figure 4. Système d'accès par cartes utilisant un réseau Ethernet et des réseaux RS-485

Si vous vous connectez au réseau Ethernet TCP/IP avec l'outil de configuration TX3, vous pouvez configurer n'importe lequel des nœuds dans le système. Si vous vous connectez directement à un contrôle par USB, modem ou port de communication, vous serez seulement en mesure de configurer les dispositifs qui se trouvent sur le même sous-réseau RS-485 que le dispositif.

Remarque: Il peut seulement y avoir un nœud principal sur un sous-réseau RS-485. C'est-à-dire que vous ne pouvez pas connecter un sousréseau RS-485 à un autre sous-réseau RS-485.

## 1.6 À propos de ce manuel

Ce manuel fournit des informations détaillées sur l'installation et la configuration du système d'accès par carte qu'effectuera le technicien. Les tâches sont décrites dans l'ordre probable d'installation.



Le chapitre 2 décrit l'installation du contrôleur.

Le chapitre 3 décrit les modes de fonctionnement configurables.

Ce manuel concerne les deux modèles suivants:

- Kit système d'accès par carte deux portes TX3-CX-2K
- Contrôleur d'accès par carte deux portes TX3-CX
- TX3-CX-2K-A IP Ensemble de contrôle de cartes d'accès à deux portes avec capacité IP
- TX3-CX-2-A Contrôle de cartes d'accès à deux portes avec capacité IP

#### 1.6.1 Documentation supplémentaire

Les documents suivants de Mircom vous serviront de documentation supplémentaire:

- LT-6618 TX3-CX-1 Installation Manual
- LT-969 TX3 Telephone/Card Access System Installation and Operation Manual
- LT-968FR Guide de l'utilisateur Configuration du clavier
- LT-971 TX3 MDM Modem Module Installation
- TX3 Two Door Card Access System Kit Catalogue Number 6531
- TX3 Series Elevator Restriction Accessories Catalogue Number 6532
- LT-995FR TX3 Manuel de Configuration et d'Administration
- LT-973FR Systèmes d'accès par Téléphone Démarrage rapide du Configurateur
- LT-6027 TX3-USB-AD Kit Installation Instructions
- LT-1161 TX3-IP IP Module Installation Instructions
- LT-1160 TX3-CX-A8 Aperio<sup>™</sup> Door Controller System Installation and Operation Manual

#### 1.6.2 Termes clés

Les termes spécifiques suivants apparaissent dans ce manuel:

CAU. « Card Access Unit » (module de contrôle d'accès par carte)

**ERU.** « Elevator Restriction Unit » (module de restriction de l'utilisation de l'ascenseur)

LCU. « Lobby Control Unit » (module de contrôle pour le hall)



## 1.7 Contactez-nous

#### 1.7.1 Information Générale

Ligne sans frais: 1-888-660-4655

Appels locaux: 905-660-4655

**Télécopie locale:** 905-660-4113

#### 1.7.2 Site Web

http://www.mircom.com



# **2** Fonctions configurables

Ce chapitre décrit toutes les fonctions configurables et leurs modes de fonctionnement; il décrit en détails comment configurer le système par le biais du logiciel configurateur.

#### Ce chapitre décrit les :

- Entrées
- Corrélations
- Critères d'accès
- Temporisations
- Horaires
- Jours fériés
- État du système

### 2.1 Entrées

Chaque contrôleur d'accès par carte comprend huit entrées pour supporter les fonctions spéciales suivantes :

- Demande de sortie pour le lecteur A ou B
- Capteur de porte pour le lecteur A ou B
- Usage général

#### 2.1.1 Demande de sortie au lecteur A ou B

Lorsqu'une entrée est active, la porte se déverrouille et la temporisation commence. À l'expiration de celle-ci, ou lorsqu'un capteur porte lié à ce lecteur de carte devient active, la porte se verrouille.

L'entrée est associée à la fonction de demande de sortie.



#### 2.1.2 Capteur de porte pour lecteur A ou B

- Lorsque la porte est ouverte, cette entrée est active et lorsqu'elle est fermée, l'entrée est inactive. Cette entrée :
- Détecte si la porte s'est ouverte après avoir été déverrouillée en raison d'un accès qui a été accordé. Si la porte ne s'est pas ouverte même si elle s'est déverrouillée pendant la période programmée, l'état est signalé au configurateur, si cela a été configuré.
- Détecte une entrée forcée. Si la porte est verrouillée et que l'entrée du contact de porte devient active, l'alarme d'entrée forcée s'active. Pour modifier cette fonction, choisir Désactiver l'alarme d'entrée forcée.
- Détecte si la porte est maintenue ouverte. Cela arrive lorsque la porte est déverrouillée et que le contact de porte devient actif, mais ne se désactive pas avant la fin de la minuterie de la période de déverrouillage ou de la minuterie de la période prolongée de déverrouillage. Dans ces cas-là, la minuterie d'avertissement de porte maintenue ouverte s'actionne. Si la porte demeure ouverte à la fin de la période de cette minuterie, un avertissement de porte maintenue ouverte est signalé au configurateur.

À la fin de la période de la minuterie d'avertissement de porte maintenue ouverte, la minuterie d'alarme de porte maintenue ouverte s'actionne. Lorsque la minuterie d'alarme de porte maintenue ouverte prend fin, une alarme de porte maintenue ouverte est signalée au configurateur.

Si la porte se ferme pendant que la minuterie d'avertissement de porte maintenue ouverte ou la minuterie d'alarme de porte maintenue ouverte sont actionnées, l'alarme ou l'avertissement est annulé et l'événement d'avertissement de porte ouverte réinitialisé ou d'alarme de porte ouverte réinitialisée est signalé au configurateur.

## 2.2 Corrélations

Les corrélations vous permettent d'établir des liens précis entre les entrées du panneau (évènements) et les sorties (actions), par exemple, allumer la lumière lorsqu'une porte s'ouvre. Les corrélations vous permettent aussi de spécifier un horaire à ces liens, par exemple, accorder un accès seulement durant certains heures ou jours de la semaine. Un maximum de 32 corrélations est permis.

#### 2.2.1 Assigner des évènements aux points d'accès

L'assignation d'événements aux points d'accès associe le point d'accès à un évènement. Le configurateur vous permet d'assigner des évènements d'entrée par l'étiquetage des points d'accès suivants :

- Lecteur A
- Lecteur B
- Entrée 1 à 8



#### 2.2.2 Évènements

Les évènements sont définis par les suivants entrées et états du lecteur :

- Accès accordé (du lecteur A ou B)
- Accès refusé (du lecteur A ou B)
- Alarme ouverture forcée (du lecteur A ou B)
- Alarme porte retenue (du lecteur A ou B)
- Porte non ouverte (du lecteur A ou B)
- Entrée est active (du lecteur A ou B)
- Mode Déverrouillage est activé (du lecteur A ou B)
- Mode Déverrouillage est désactivé (du lecteur A ou B)
- Haute sécurité est activée (du lecteur A ou B)
- Haute sécurité est désactivée (du lecteur A ou B)

#### 2.2.3 Actions

Une action est définie par le type d'action que déclenche une entrée spécifique; elle consiste à :

- Activer une sortie « ON » (marche)
- Désactiver une sortie « OFF » (arrêt)
- Activer Haute sécurité « ON » (marche)
- Désactiver Haute sécurité « OFF » (arrêt)

#### 2.2.4 Panneaux

Les corrélations peuvent être appliquées à un des panneaux, à tous les panneaux ou à un groupe personnalisé de panneaux sur votre système (pour les réseaux TCP/IP seulement), à l'échelle de tous les panneaux sur le réseau et pouvant survenir sur le panneau local, des panneaux répartis ou différents types de panneaux (accès par cartes ou téléphoniques) sur le réseau.

**Remarque:** Les signaux de corrélation ne peuvent pas être transmis par les nœuds principaux d'écran tactile. Si vous prévoyez régler des corrélations pour tous les panneaux de votre réseau ou un groupe personnalisé de panneaux, vous ne devriez pas avoir de nœuds principaux d'écran tactile sur votre réseau.



#### 2.2.5 Sortie

Les actions sont appliquées à une sortie sur le(s) panneau(x) choisi(s). Cette option précise quelle sortie.

#### 2.2.6 Durée

La durée de l'action est exprimée en minutes et secondes; l'action peut durer indéfiniment.

#### 2.2.7 Horaire

L'horaire vous permet de spécifier quand des évènements corrélés doivent se produire.

## 2.3 Critères d'accès

Le configurateur, s'il est connecté au PC, surveille l'état de fonctionnement des périphériques et des entrées de tous les panneaux et détecte, automatiquement, l'état des composants connectés (marche/arrêt). Les sorties sont programmées pour une fonctionnalité spécifique (par exemple, un délai spécifique, l'horaire de mise en marche/ arrêt).

L'accord d'accès est déterminé selon différents critères, tels que des mesures de sécurité et des privilèges d'accès accordés au détenteur de carte. Afin d'empêcher tout accès non autorisé, le contrôleur est doté de plusieurs fonctions configurables pour définir le type et les conditions d'accès.

Les exigences relatives à l'accord d'accès sont fonctions de l'horaire, des jours fériés, des mesures de sécurité et des privilèges d'accès. Ces paramètres sont configurables et permettent un fonctionnement précis du système. Par exemple, certains privilèges d'accès peuvent avoir des dépendances et, ainsi, il serait plus approprié de les gérer en tant que tâches programmées.

Le logiciel configurateur vous permet de définir et de configurer divers modes de fonctionnement afin de gérer l'accès, de définir les entrées et d'attribuer des sorties. Pour utiliser efficacement le configurateur, vous devez comprendre les fonctions configurables suivantes :

- Verrouiller/déverrouiller
- Haute sécurité
- Décision requise du PC
- Code de l'installation
- Carte + NIP
- Anti-retour



- Carte d'accès temporaire
- Interverrouillage
- Niveau d'accès
- Options du contrôleur
- Options des points d'accès
- Options des cartes d'accès

#### 2.3.1 Verrouillage et déverrouillage

Un point d'accès peut présenter un des suivants modes d'état d'une serrure :

**Mode verrouillage :** en mode verrouillage, la porte est, normalement, verrouillée. Toute carte valide déverrouillera la porte pour la durée d'une temporisation réglable :

- temporisation d'ouverture
- temporisation d'ouverture retardée

Durant ce mode, la DEL rouge, associé avec ce point d'accès, s'active et passe au vert pendant toute la durée de la temporisation d'ouverture.

**Mode déverrouillage :** en mode déverrouillage, la porte est déverrouillée. La DEL verte reste allumée, sur le lecteur associé à ce point d'accès. Durant ce mode, le capteur de porte n'est l'objet d'aucun suivi des états suivants :

- la porte ne s'est pas ouverte
- avertissement de porte retenue
- alarme ouverture forcée

#### 2.3.1.1 Changer les modes verrouillage et déverrouillage

Les modes verrouillage et déverrouillage peuvent-être changés d'une de ces trois façons :

- un administrateur, par le biais du configurateur, peut envoyer une commande de changement de modes, entre verrouillage et déverrouillage.
- Si une carte d'accès, avec des privilèges verrouillage/déverrouillage, est glissée deux fois de suite, il y a bascule entre les modes verrouillage et déverrouillage.
- un horaire lié au mode verrouillage/ déverrouillage : lorsque l'horaire lié à ces modes est actif, le mode passe au déverrouillage; une fois l'horaire est inactif, le mode repasse au verrouillage.



Chaque fois que le mode d'état passe de verrouillage à déverrouillage, et vice versa, le bipeur du lecteur associé à ce point d'accès émet un signal sonore distinct indiquant le changement de mode.

#### 2.3.2 Haute sécurité

Le mode haute sécurité accorde l'accès aux cartes avec des privilèges Haute sécurité. Ce monde peut-être changé comme suit.

- Si le point d'accès est défini comme Haute sécurité, le mode Haute sécurité lui est attribué par défaut; sauf si ce mode est changé par le biais du PC ou d'une carte ayant des privilèges Haute sécurité
- Si une carte d'accès avec des privilèges Haute sécurité est glissée quatre fois de suite, le mode bascule entre « Haute sécurité activée » et « Haute sécurité désactivée »
- Le logiciel configurateur peut faire passer le mode « Haute sécurité activée » au mode « Haute sécurité désactivée » et vice-versa.
- Un évènement corrélé à une action d'activer ou de désactiver le mode « Haute sécurité »

Le mode « Haute sécurité » verrouille toutes les portes sous mode « Déverrouillage »

Chaque fois que le mode « Haute sécurité » change, le bipeur du lecteur, associé à ce point d'accès, émet un signal sonore distinct.

#### 2.3.3 Décision requise du PC

Durant ce mode, la décision d'accorder un accès est transféré à un gardien. Par le biais du PC, le gardien peut accorder un accès ou le refuser. Seules les cartes valides, programmées avec la fonction/option « décision requise du PC », sont capables de faire une telle demande.

#### 2.3.4 Mode « code de l'installation »

Les cartes d'accès comportent deux codes : le code de l'installation et le code de la carte. Le code de l'installation est conçu pour les nouvelles installations auxquelles les cartes accès ne sont pas programmées dans la base de données. Lorsque le mode « code de l'installation » est actif, les cartes avec le code de l'installation auront l'accès accordé.

Le code de l'installation peut prendre n'importe quelle valeur. Celle-ci sera définie à zéro, par défaut, comme paramètre fictif, si aucune valeur n'est fixée.

En ce mode, la porte est déverrouillée pour la même période de temps que celle d'une porte standard. Ce mode est configuré pour chaque point d'accès.



#### 2.3.5 Carte + NIP

Ce mode fournit un autre mécanisme de sécurité à certaines heures de la journée. Durant ce mode, une carte valide n'est pas suffisante pour obtenir un accès, il faut aussi un code NIP. Celui-ci peut comporter jusqu'à quatre chiffres et est programmé sur chaque carte. Le chiffre zéro ne constitue pas un code NIP valide.

À ce mode correspond un horaire. Si cet horaire est activé, le mode est activé aussi; s'il est désactivé, le mode l'est aussi.

Cette fonction exige un lecteur de carte muni d'un clavier.

#### 2.3.6 Anti-retour

Ce mode empêche les utilisateurs non autorisés d'obtenir un accès. Durant la temporisation d'anti-retour, une carte valide présentée à un point d'accès ne peut y être représentée avant l'expiration de la temporisation prédéfinie. Après l'expiration, l'utilisateur peut obtenir un accès, à nouveau.

#### 2.3.7 Carte d'accès temporaire

Ce genre de carte peut être créé en imposant une limite à l'utilisation de la carte; chaque fois qu'une carte est utilisée, le lecteur de carte déduit une unité du nombre limite d'utilisation. Une fois, ce dernier est à zéro, l'accès est refusé. Ceci n'est pas un mode proprement dit. Cependant, en configurant les paramètres précédents, on peut créer une « carte temporaire ».

Un nombre d'utilisation fixé à 255 fois indique un usage illimité de la carte.

#### 2.3.8 Interverrouillage

Le mode interverrouillage est généralement utilisé dans le cas de porte double pour interdire l'accès non autorisé. Dans ce mode, l'utilisateur présente la carte à chaque porte. La seconde porte s'ouvre après avoir présenté la carte et, seulement, si la première porte est fermée et verrouillée.

Ce mode activé, la porte B se déverrouille, une fois, et seulement si la porte A est verrouillée et fermée ; la porte A se déverrouille, une fois, et seulement si la porte B est verrouillée et fermée.

#### 2.3.9 Niveau d'accès

La création d'un niveau d'accès vous permet de définir quand et où utiliser une carte et d'établir l'utilisation de l'ascenseur si les commandes de ce dernier sont utilisées.

Un maximum de 128 niveaux d'accès est défini pour chaque commande. Un horaire est lié à chaque niveau d'accès pour tous les points d'accès sur la commande, tel qu'indiqué dans l'exemple suivant :

## Millin Mircom

L'ID du niveau d'accès = 1

- Horaire du lecteur A = Toujours
- Horaire du lecteur B = Jamais

L'ID du niveau d'accès = 2

- Horaire du lecteur A = Heures d'ouverture
- Horaire du lecteur B = Toujours

Si une carte possède un niveau d'accès 1, le lecteur A accordera, en tout temps, l'accès à l'utilisateur, mais le lecteur B ne lui accordera jamais un accès.

Si une carte possède un niveau d'accès 2, le lecteur A accordera, durant les heures d'ouverture, l'accès à l'utilisateur, et le lecteur B le lui accordera en tout temps.

Chaque niveau d'accès comporte l'option « contrôleur ascenseur ». Si cette option est activée, avec un niveau d'accès spécifique, le passage d'une carte valide, avec le même niveau d'accès, active les relais d'étage appropriés. Les relais à activer sont déterminés individuellement pour chaque niveau d'accès. Un maximum de 16 relais peut être activé pour chaque niveau. Si plus de 16 relais sont attribués à un niveau d'accès spécifique, 16, seulement, seront activés.

#### 2.3.10 Options du contrôleur

Les options, suivantes, du contrôleur sont configurables :

Format de la carte : les formats suivants sont reconnus :

- 26-bit Wiegand SIA
- 37-bit Mircom
- 35-bit Indala
- 50-bit RBH
- 32-bit CSN
- 37-bit HID 10304
- 35-bit HID corporate 1000
- 36-bit HID Simplex
- 36-bit Keyscan C15001
- 37-bit Cansec
- 39-bit Kantech

Faire état d'évènements temps réel au PC : une fois activée, seuls les registres en temps réel sont envoyés au PC.



**Interverouillage :** une fois activée, la porte B se déverrouille, une fois, et seulement si la porte A est verrouillée et fermée ; la porte A se déverrouille, une fois, et seulement si la porte B est verrouillée et fermée

**Code de l'installation :** le code peut prendre n'importe quelle valeur. La valeur par défaut est définie à zéro.

#### 2.3.11 Options des points d'accès

Les options, suivantes, des points d'accès sont configurables :

**Reverrouillage automatique :** cette option, une fois activée, verrouille la porte avant l'expiration des temporisations d'ouverture et d'ouverture retardée. Une fois désactivée, cette option ne verrouille la porte qu'après l'expiration des temporisations d'ouverture et d'ouverture retardée.

**Déduire le nombre d'utilisation :** Pour les cartes désignées comme « temporaires » (c'est-à-dire l'option du compteur d'utilisation est activée et réglée à une valeur inférieure à 255), cette option réduit le compte d'utilisation de un chaque fois que la carte est utilisée à un point d'accès. Lorsque le compteur d'utilisation atteint zéro, la carte se désactive.

**Désactiver l'alarme d'entrée forcée :** Si cette option est activée, l'alarme d'entrée forcée ne s'actionne pas, même si la porte est ouverte sans permission. L'accès est plutôt accordé. Cela est habituellement utilisé aux points d'accès qui ne sont pas équipés d'un dispositif de demande de sortie.

**Remarque:** Si cette option est sélectionnée, choisir aussi **Signaler une demande de sortie** de sorte que chaque fois qu'un accès est accordé, il est signalé dans les événements en ligne.

**Ignorer le code de l'installation de la carte :** cette option est activée par défaut. Le cas échéant, le numéro de la carte est le seul paramètre à traiter pour accorder un accès. Une fois cette option désactivée, le numéro de la carte et le code de l'installation seront traités pour accorder un accès.

**Décision requise du PC :** Une fois cette option est activée, la décision d'accorder l'accès est transférée du contrôleur au PC. Pour que cette option soit valide, le PC doit-être connecté en tout temps. Utilisez cette option, si le bâtiment a un concierge ou un bureau de la sécurité.

**Première personne arrivée :** la configuration du point d'accès selon un horaire de verrouillage/déverrouillage garde la porte verrouillée au début des heures de déverrouillage, jusqu'à ce qu'une personne présente au lecteur une carte valide ayant le privilège Première personne arrivée. La porte restera déverrouillée durant le reste des heures de déverrouillage.



**Contournement de la demande de sortie :** Activer cette option si la porte est équipée d'un dispositif mécanique de sortie. Dans ce cas-là, la porte est déverrouillée manuellement et le système TX3 ne déverrouille pas la porte. Si la porte est ouverte, le système met à jour le statut de la porte et la DEL sur le lecteur passe au vert. Le contact de porte est contourné et il n'y a pas d'alarme d'entrée forcée.

Haute sécurité : cette option, une fois activée, accorde l'accès aux détenteurs de carte ayant cet attribut.

**Signaler une demande de sortie :** cette option enregistre et suit les évènements de l'état du système. Une fois activée, elle enregistre et signale chaque demande de sortie au configurateur. Puisque la personne qui sort est inconnue, seules l'heure et la date sont enregistrées et signalées.

Signaler : porte ne s'ouvre pas : une fois activée, cette option enregistre et signale des évènements pour lesquels un accès est accordé mais la porte ne s'est jamais ouverte.

**Signaler un format inconnu :** une fois activée, cette option enregistre et signale des tentatives d'accès avec une carte dont le format est inconnu.

**Mode code de l'installation :** l'activation de ce mode accorde l'accès selon le code de l'installation uniquement ; ce qui permet aux cartes non-programmées d'accorder un accès total au bâtiment. À n'utiliser qu'en cas d'absolue nécessité.

**Interdire ID :** une fois activée, cette option n'envoie pas le code de la carte au PC. Cette fonction est utilisée à des fins d'enregistrement et de rédaction.

Anti-retour contre la montre : une fois activée, cette option n'accorde pas l'accès à un détenteur de carte, au même point d'accès, au cours de la temporisation réglable d'anti-retour.

#### 2.3.12 Options des cartes

Les cartes d'accès sont configurables pour les fonctions suivantes :

**Compteur d'utilisation :** Seul le nombre d'utilisations d'une carte temporaire est compté. Le nombre d'utilisation est fixé, à priori, entre 1 à 255 fois. Le nombre 255 indique qu'aucune restriction n'est imposée à l'usage de la carte. Toute autre valeur inférieure à 255 indique le nombre de fois que l'on peut utiliser la carte.

État : l'état de la carte d'accès est indiqué comme suit :

- Actif
- Inactive
- Perdue



En cas de perte ou d'inactivité, l'accès est refusé. L'accès est accordé aux cartes actives, pourvu que toutes les autres conditions soient satisfaites (par exemple, horaire et privilèges).

Niveau d'accès : le niveau d'accès est configurable en fonction des privilèges.

**Code NIP :** le code est programmé à n'importe quelle valeur numérique de quatre chiffres ; et utilisé durant l'horaire Carte + NIP. Le chiffre zéro ne constitue pas un code NIP valide.

**Ignorer anti-retour :** une fois cette option est activée, la carte ne fonctionne pas sous le mode « anti-retour contre la montre ».

**Privilège verrouillage-déverrouillage :** cette option, une fois activée, permet au détenteur de carte de déverrouiller la porte en la présentant deux fois de suite au lecteur de carte.

Accès aux zones de haute sécurité) : cette option accorde l'accès seulement aux détenteurs de carte ayant cet attribut.

**Temps de déverrouillage prolongé :** cette option, une fois activée, ouvre la porte pour un temps prolongé prédéterminé. Cette option est généralement utilisée pour accommoder les personnes âgées et handicapées.

**Handicap**: lorsque cette option est activée, la sortie désignée comme accessible est activée avec la porte principale.

**Première personne arrivée :** cette option fonctionne en liaison, seulement, avec l'horaire prévu des modes de verrouillage et déverrouillage. Si cette option est activée, seul le détenteur de carte avec ce privilège, Première personne arrivée, peut déclencher le mode déverrouillage.

## 2.4 Temporisations

Les temporisations suivantes sont liées à l'opération du système d'accès par carte :

- Temps de déverrouillage
- Temps de déverrouillage prolongé
- Anti-retour
- Avertissement de porte retenue
- Alarme de porte retenue



#### 2.4.1 Horaires

L'horaire des évènements est établi par l'administrateur; l'évènement peut être activé ou désactivé en permanence. Des modes suivent un horaire, par exemple :

Horaire de déverrouillage automatique : une fois activée, la porte reste déverrouillée selon cet horaire.

**Horaire affecté à un NIP :** selon cet horaire, l'accès par carte exige la saisie d'un NIP.

#### 2.4.2 Temps de déverrouillage

La temporisation commence au déverrouillage de la porte. À son expiration, la porte se verrouille. Pour la porte principale, la temporisation est réglable de 0 à 300 secondes, 10 secondes par défaut.

#### 2.4.3 Temps de déverrouillage prolongé

Ce mode est utilisé avec les cartes dont l'option « Temps de déverrouillage prolongé » est activée. La temporisation commence au déverrouillage de la porte. À son expiration, la porte se verrouille. La temporisation est réinitialisée quand le capteur de porte de la porte principale est inactif. La temporisation de déverrouillage retardée est réglable de 10 à 300 secondes, 15 par défaut.

#### 2.4.4 Anti-retour

La temporisation d'anti-retour commence à l'accord d'accès. En ce mode, l'utilisateur ne pourra repasser par la même porte avant l'expiration de la temporisation d'anti-retour. À son expiration, l'utilisateur pourra y repasser. La temporisation d'anti-retour est réglable de 0 à 900 secondes, 300 secondes par défaut.

#### 2.4.5 Avertissement de porte retenue

Cette temporisation commence à l'accord d'accès. Lorsque la temporisation de déverrouillage expire, si la porte ne s'est pas refermée durant ce délai, un avertissement d'une porte retenue est envoyé au PC ; aussi, l'état Problèmes courants devient actif. Si la porte se referme durant la temporisation au déclenchement de l'avertissement, celle-ci est réinitialisée et aucun rapport d'avertissement n'est envoyé au PC.

La temporisation au déclenchement d'un avertissement d'une porte retenue est réglable de 10 à 900 seconds, 30 secondes par défaut.



#### 2.4.6 Alarme de porte retenue

Cette temporisation commence à l'expiration de la temporisation au déclenchement d'un avertissement alors que la porte est toujours ouverte. À l'expiration de la temporisation au déclenchement de l'alarme, si la porte est toujours ouverte, une alarme porte retenue est envoyée au PC ; aussi, l'état Alarme courante devient actif. La temporisation au déclenchement d'une alarme porte retenue est réglable de 10 à 900 secondes, 60 secondes par défaut.

## 2.5 Horaires

Les horaires vous permettent d'établir un calendrier pour l'exécution de certaines actions, par exemple, accorder l'accès. Ces horaires sont désignés et classés par dénomination dans le logiciel configurateur ; ils sont sélectionnables pour accorder l'autorisation d'accès au besoin.

Un nombre maximal de 64 horaires est programmé dans le système. Chaque horaire consiste en huit périodes, chacune comportant :

- le début et la fin de la période, format d'affichage : 00:00
- sélection des jours de la semaine, du week-end et des jours fériés

Chaque horaire a une ID et une étiquette avec lesquels un horaire, à utiliser, est identifié dans le logiciel configurateur.

Si l'heure actuelle et les données correspondent à l'une des quatre périodes dans un horaire, celui-ci est considéré comme actif, sinon, il est inactif.

Par défaut, les deux horaires suivants ne peuvent être modifiés :

- Toujours
- Jamais

Les horaires sont liés aux options / modes suivants :

- Temporisation
- Corrélations
- Déverrouillage automatique
- NIP requis
- Niveaux d'accès



## 2.6 Jours fériés

Les jours fériés font parties de l'horaire; il existe un maximum de 128 jours féries. Chaque jour férié a une :

- heure / date de début
- heure / date de fin

Si un jour férié tombe à la même date chaque année, il peut être programmé comme un évènement annuel.

Chaque jour férié a une ID et une étiquette avec lesquels un jour férié, à utiliser, est identifié dans le logiciel configurateur.

Par défaut, seul le nouvel an est programmé dans le système.

## 2.7 État du système

Le contrôleur surveille les entrées quant aux conditions de problèmes et d'alarmes.

#### 2.7.1 Problème courant

L'indicateur d'un problème courant s'active chaque fois qu'une condition de problèmes se présente à une des entrées suivantes :

- Toute entrée surveillée
- Alimentation (CA et batterie)
- Avertissement d'une porte retenue

L'état normal est rétabli seulement si toutes les entrées susmentionnées reviennent à leur état normal. Quand un état « problème courant » est actif, la DEL Problème courant , clignote lentement.

#### 2.7.2 Alarme courante

L'état « alarme courante » s'active, lorsqu'une condition d'alarme se présente à une des entrées suivantes :

- alarme ouverture forcée
- alarme porte retenue

L'état normal est rétabli seulement si toutes les entrées susmentionnées reviennent à leur état normal. Quand un état « alarme courante » est actif, la DEL, liée à cet état, clignote rapidement.



# **3** Installation et configuration

Ce chapitre décrit l'installation et la configuration du contrôleur et du lecteur de carte d'accès.

#### Ce chapitre décrit:

- Mise à la terre du système d'accès par carte
- Installation du contrôleur et des composants
- Composantes de la carte contrôleur
- Raccordement des entrées
- Raccordement des sorties
- Raccordement du lecteur de carte
- Réglages des commutateurs DIP SW2
- Réglages des cavaliers
- Alimenter contrôleur
- Mise à jour du micrologiciel
- Commencer à configurer

## 3.1 Mise à la terre du système d'accès par carte

La mise à terre réduit le risque de choc électrique en fournissant un circuit de fuite au courant électrique. Le système d'accès par carte est équipé d'un fil électrique de calibre 16 fixé à la borne de terre du châssis du panneau.

Remarque: Ne pas déconnecter ce fil.

Raccordez le bout du fil fourni à un fil de mise à la terre convenable de calibre 16 ou plus, puis raccordez l'autre bout à une conduite d'eau.



## 3.2 Installation du contrôleur et des composants

Le contrôleur d'accès par carte est monté en surface, à l'aide de quatre vis, comme le montre la figure 5. Le capotage arrière mesure 15 pouces de large sur 14 pouces de long. Les deux trous de montage du haut sont séparés de 10 pouces.



Figure 5. Dimensions du capotage arrière du contrôleur et l'emplacement de composant facultatif

#### 3.2.1 Composants facultatifs

Installer les composantes facultatives suivantes au besoin:

- Interrupteur d'autoprotection
- Module- TX3-MDM Modem
- Module IP TX3-IP (seulement pour les modèles TX3-CX-2-A ou TX3-CX-2K-A)
- Module-MD-993 RS-485 à USB
- Accumulateurs



#### 3.2.2 Installation du contrôleur d'accès par carte

Le boîtier du contrôleur d'accès se fixe sur une solive murale en utilisant les trous de montage, comme le montre la figure 5.

#### Monter le lecteur de carte

- 1. Trouver un emplacement approprié près d'une solive murale
- 2. Utiliser le capotage arrière du contrôleur comme gabarit et marquer les deux trous de montage du haut séparés de 10 pouces comme le montre la figure 5.
- 3. Insérez les vis à mi-distance aux endroits marqués à l'aide d'un tournevis adapte.
- 4. Accrocher le boîtier sur les deux vis.
- 5. Visser les deux autres vis au bas du panneau.
- 6. Serrer les quatre vis.

#### 3.2.3 Installation de l'interrupteur d'autoprotection

L'interrupteur d'autoprotection se situe au coin supérieur droit du capotage arrière, montré sur la figure 5. Raccordez le fil de l'interrupteur d'autoprotection à l'entrée d'usage général et corréler l'ouverture du couvercle à une sortie spécifique (action). Pour une description complète des corrélations, référez-vous au chapitre 2: Fonctions configurables.

#### 3.2.4 Installation du modem

**Remarque:** Le module de modem TX3-MDM est conçu pour fonctionner seulement avec les lignes téléphoniques de base.

Installez le module facultatif TX3-MDM Modem dans l'emplacement représenté sur la figure 6 en utilisant les quatre vis fournies.



Le TX3 MDM Modem Module Installation Instructions LT-971 vous servira de documentation supplémentaire.



Figure 6. Emplacement de la carte modem

#### 3.2.5 Installer le module IP

La trousse de module IP TX3-IP optionnelle comprend le module IP MD-921, qui permet à un contrôle de cartes d'accès de se connecter à un réseau Ethernet/IP en tant que nœud principal. Installez le module MD-921 à l'endroit indiqué à la figure 7. Fixez en place le module IP à l'endroit approprié en utilisant les quatre vis fournies.

Pour en savoir davantage, consultez le manuel d'installation du module IP MD-921 LT-1161.

**Remarque:** Le module IP MD-921 peut seulement être installé sur les modèles TX3-CX-2-A ou TX3-CX-2K-A.





Figure 7. Emplacement de la carte de module IP

#### 3.2.6 Installation de l'ensemble TX3-USB-AD

L'ensemble TX3-USB-AD transforme les signaux RS-485 au format USB. Installez le module MD-993 dans l'emplacement représenté sur la figure 6, en utilisant les quatre vis fournies. Le câble-ruban du module MD-993 se connecte au connecteur P3 sur la carte contrôleur.

Le module comporte un connecteur RS-485, tel que représenté sur la figure 8.



Figure 8. Module MD-993



Mode	JW1	JW2
Aucune terminaison	Ouvert	Ouvert
Terminaison CA 120R + 1nF	Court- circuit	Ouvert
Aucune terminaison	Ouvert	Court- circuit
Terminaison CC 120R (par défaut)	Court- circuit	Court- circuit

#### Table 1: Réglages – Cavalier MD-993

**Remarque:** Pour ce qui est de la principale application du MD-993, JW1 and JW2 doivent rester selon la position de fonctionnement (« Marche »).

Vous trouverez une description de la procédure d'installation du module MD-993 dans le manuel TX3-USB-AD Kit Installation Instructions LT-6027.

### 3.3 Composantes de la carte contrôleur

Le système d'accès par carte contrôle les points d'accès en fonction de la définition des entrées et des sorties et de la corrélation entre elles. Les entrées et les sorties sont définies par la façon dont les points d'accès et de contrôle sont branchées au contrôleur.

Avant de commencer, vous devez établir les actions des sorties en fonction des entrées. Vous trouverez une description détaillée des corrélations et des modes de fonctionnement au chapitre 2: Fonctions configurables.

Gardez les informations sur le câblage à des fins de configuration.

#### 3.3.1 DELs du panneau Contrôleur

Le panneau du lecteur de carte a trois DELs signalant un état:

DEL Alimentation CA: la DEL verte s'allume lorsqu'une alimentation AC est présente.

DEL Problèmes: la DEL orange clignote lentement lorsque qu'une condition de problème courant se présente. Le problème pourrait être:

• N'importe quelle entrée surveillée



- Alimentation CA/batterie faible
- Alarme porte retenue

**DEL Alarme:** la DEL rouge clignote rapidement au cas d'une ouverture forcée ou à l'expiration de la temporisation au déclenchement d'alarme porte retenue.

#### 3.3.2 Composants de la carte contrôleur

Le contrôleur d'accès par carte est constitué des terminaux suivants:

- 8 entrées
- 8 sorties (6 sorties à relais contact et 2 sorties fournissant un courant 12V c.c.)
- Connexions pour deux lecteurs de cartes (indiqué comme Lecteur A lecteur B)
- Alimentation électrique
- Connecteur RS-485
- Connecteurs d'USB, module IP, et de modem

## Mircom<sup>®</sup>



#### Figure 9. Emplacement des connexions de la carte contrôleur

**Remarque:** Se référer à la section 3.6.2 à la page 45 pour la connexion des bornes des deux lecteurs de carte.



#### 3.3.3 Alimentation électrique

La connexion au réseau électrique se situe en bas à droite de la carte contrôleur principale et reçoit une alimentation de 16 VCA, 40 VA. Utilisez un fil de calibre 18 AWG. Un transformateur enfichable externe PS-4 ou PS-4P se branche sur les bornes d'alimentation. Se référer à la figure 10.







#### 3.3.4 Interrupteur marche/arrêt et accumulateurs de secours

Un accumulateur de secours est fourni d'une capacité de 12V 6.5AH et s'installe en bas de l'unité. Connectez l'accumulateur aux bornes situées à gauche de l'interrupteur marche/arrêt SW1, tel qu'indiqué sur la figure 11.



Remarque: L'accumulateur de secours est proposée en option.



#### 3.3.5 RS-485

Câble blindé ou non blindé de catégorie 5

Longueur maximale du câble RS-485 : 1219,2 m (4000 pi)

Un connecteur RS-485 vous permet de facilement connecter, en réseau, plusieurs contrôleurs d'accès par carte et par téléphone. Le connecteur RS-485se situe en bas, au milieu de la carte contrôleur principale et est constitué de deux bornes distinctes, une pour une sortie, l'autre pour une entrée.

Connectez l'entrée RS-485 à la sortie RS-485 d'un autre contrôleur.



Sur les panneaux de modèle MD-10xx, il est possible de court-circuiter le JW5 sur le premier et le dernier panneau, au lieu d'utiliser des résistances de fin de ligne  $120 \Omega$ .



Figure 12. RS-485

#### 3.3.6 Port USB

Le port USB permet de se connecter à un PC, de configurer un système d'accès par carte et de télécharger n'importe quel nouveau micrologiciel.

## 3.4 Raccordement des entrées

Chaque contrôleur d'accès par carte possède huit entrées pour accueillir les différents types de fonctions configurables, liées aux entrées. Pour obtenir des détails supplémentaires et une description complète des différents types de fonctions configurables, référez-vous au chapitre 2: Fonctions configurables.

À la fin de l'installation et de la mise en marche, l'état de fonctionnement de toutes les entrées et les modes de contrôle du circuit doivent être configurés avec le logiciel configurateur. Durant la configuration, vous établirez les corrélations entre les entrées et les sorties.

En fonction du dispositif, chaque entrée est configurée selon:



- type de fonction de l'entrée
- état actif
- contrôle requis
- temporisation de l'alarme





#### 3.4.1 Entrées 1 à 8

Les entrées 1 à 8 sont des entrées programmables. Configurez chaque entrée pour une des actions suivantes. figure 14 montre un exemple de connexion.

- Demande de sortie (lecteur A)
- Demande de sortie (lecteur B)
- Capteur porte (lecteur A)
- Capteur porte (lecteur B)
- Entrée d'usage général



8 bornes d'entrée

Figure 14. Exemple de connexions des bornes d'entrée

#### 3.4.2 Demande de sortie

L'activation de cette entrée déverrouille la porte et démarre la temporisation de déverrouillage de porte.



#### 3.4.3 Capteur porte

Lorsque la porte est ouverte, cette entrée est active; lorsque la porte est fermée, l'entrée est inactive.

#### 3.4.4 Entrée d'usage général

L'entrée d'usage général sert principalement à établir une corrélation avec une sortie spécifique. L'activation d'une entrée d'usage général est considérée comme un évènement qui entraîne l'activation ou la désactivation d'une sortie d'usage général ou l'activation ou la désactivation du mode haute sécurité. Parmi les autres évènements corrélés se trouvent différentes fonctions tels que l'ouverture forcée, le ré-déverrouillage automatique et l'interverrouillage.

#### 3.4.5 État actif

Un état actif survient lorsque le circuit d'entrée est considéré comme actif et est configuré comme un des deux:

- ouvert
- fermé (par défaut)

La configuration de l'état actif est soumise à certaines restrictions, en fonction du mode de contrôle requis.

Si l'entrée n'est pas contrôlée, l'entrée est soit « ouverte » ou « fermée ». Si le mode de contrôle de l'entrée est « ouvert », l'état actif ne peut être « ouvert ».

Si le mode de contrôle est "ouvert" et "fermé", l'état actif ne peut être « ouvert ».

#### 3.4.6 Contrôle requis

Chaque entrée est configurée pour un mode de contrôle spécifique, en fonction de vos conditions d'installations particulières:

- pas de contrôle
- mode de contrôle « ouvert »
- mode de contrôle « fermé »
- mode de contrôle « ouvert » et « fermé »

#### 3.4.6.1 Pas de contrôle

Lorsque les entrées sont configurées avec un mode de contrôle « pas de contrôle», l'état actif est soit « ouvert » ou « fermé », selon la programmation.



#### 3.4.6.2 Mode de contrôle « ouvert »

Lorsque les entrées sont configurées avec un mode de contrôle « ouvert», l'état actif est « fermé » (court-circuit). Le mode de contrôle « ouvert » se sert d'une seule résistance 47K ohms.



Figure 15. Entrée – Mode de contrôle Ouvert

Remarque: L'état actif peut être un état ouvert.

#### 3.4.6.3 Mode de contrôle « fermé »

Lorsque les entrées sont configurées avec un mode de contrôle « fermé », l'état actif est « ouvert ». Une seule résistance 47K ohms est nécessaire pour un mode de contrôle « fermé ».



Figure 16. Entrée – Mode de contrôle fermé

Remarque: L'état actif ne peut être un état court-circuit.



#### 3.4.6.4 Mode de contrôle « ouvert » et « fermé »

Lorsque les entrées sont configurées avec un mode de contrôle « ouvert » et « fermé », l'état actif ne peut être « ouvert » ; aussi, l'état actif est « fermé ». Deux résistances 47K ohms sont nécessaires pour ce mode de contrôle.



Figure 17. Entrée-surveillance des états fermés ouverts

**Remarque:** L'état actif ne peut être un état ouvert.

#### 3.4.7 Temporisation d'alarme

La temporisation d'alarme est un paramètre défini par le configurateur; celui-là détermine la durée de la temporisation jusqu'à ce que l'entrée indique une condition d'alarme. Pour plus d'informations, voir chapitre 2: Fonctions configurables.

## **3.5** Raccordement des sorties

Au coin supérieur droit de la carte contrôleur se trouvent 8 sorties, tel qu'indiqué sur la figure 9.

Chaque sortie est câblée pour effectuer une fonction spécifique ou pour un état actif. Déterminez les exigences fonctionnelles du dispositif et, par conséquent, raccordez les sorties. Pour obtenir des détails supplémentaires et une description complète des différents types de fonctions configurables, référez-vous au chapitre 2: Fonctions configurables.

À la fin de l'installation et de la mise en marche, l'état de fonctionnement de toutes les sorties doit être configurés avec le logiciel configurateur.

#### 3.5.1 Fonctions spécifiques

Chaque sortie est câblée pour une fonction spécifique:

• Verrouillage, lecteur A ou B



- Verrouillage accès handicapés, lecteur A ou B
- Sortie d'usage général

Lock for reader A or B (verrouillage lecteur A ou B): cette sortie affecte la porte principale soit au lecteur A soit au lecteur B. Une fois l'accès est accordé au lecteur désigné, cette sortie déverrouille la porte.

Handicap lock for reader A or B (verrouillage accès handicapés lecteur A ou B): cette sortie contrôle l'accès handicapés. L'accès est accordé aux détenteurs de carte ayant ce privilège.

**General purpose output (sortie d'usage général):** la sortie d'usage général sert à toute autre action: allumer la lumière, par exemple.

#### 3.5.2 État actif

Les sorties requièrent des états actifs. Chaque sortie est configurée dans l'état actif indiquant une des deux:

- sous tension
- hors tension

#### 3.5.3 Sorties 1 à 6

Les sorties 1 à 6 sont des contacts de relais programmables avec les caractéristiques suivantes:

- normalement ouvert (NO)
- normalement fermé (NC) disponible
- 125 VCA / 2 A
- 30 VCC / 1 A





La figure 18 illustre un exemple de connexion.





#### 3.5.4 Sorties 7 et 8

Les sorties 7 et 8 sont programmables et fournissent un courant combiné de 1A. Chaque sortie fournit:

- 12 VCC
- 500mA (700 mA maximum)

**Remarque:** Les sorties 7 et 8 fournissent, chacune, un courant maximum de 700 mA et un courant combiné de 1 A. Par exemple, si la sortie 7 fournit 700 mA, alors sortie 8 fournit 300 mA.





La figure 19 illustre une gâche électrique activée et alimentée par la sortie 8.

### **3.6** Raccordement du lecteur de carte

Les lecteurs de carte sont fabriqués par AWID et font partie du système d'accès par carte de Mircom. Les cartes sont fabriquées par Mircom. Le contrôleur supporte deux lecteurs de carte.

#### 3.6.1 Conditions requises du lecteur de carte

Mircom fournit le lecteur de proximité multiprotocole SR-2400MI-GR-MP.

Les lecteurs de carte d'un tiers doivent remplir les conditions requises, énumérées ci-dessous, pour qu'ils soient compatibles avec le système d'accès par carte de Mircom:

- supporter le protocole SIA 26 bits standard
- l'interface standard Wiegand
- indicateur d'état à DEL
- vibreur d'alerte ou d'alarme



- branchement 12 V
- utilisez un fil de calibre 20 AWG pour une distance maximale de 500 pieds (152,4 m) entre le lecteur de carte et le contrôleur ; pour une distance de 250 pieds (76,2 m), utilisez un fil de calibre 22 AWG

#### 3.6.2 Raccordement du lecteur de carte



Figure 20. Les connecteurs de lecteur de carte de la carte contrôleur

Brancher les lecteurs aux bornes illustrées à la figure 20.

Table 2: Connexions pour les lecteurs TX3-P300-HA et TX3-P500-HA

Couleur	Borne
Bleu	TÉLÉAVERTISSEUR
Orange	DEL ROUGE
Brun	DEL VERTE
Rouge	PWR+
Vert	DATA0
Blanc	DATA1
Noir	COM(-)

Les lecteurs de cartes fournis par Mircom requièrent un câble toronné à conducteur multiple d'au moins 22 AWG blindé avec une feuille de métal. Par exemple, utiliser un câble Belden 9535 ou un câble semblable.



Le fil noir peut être connecté à l'un des connecteurs COM (-) sur la plaque à bornes.

Pour les autres marques de lecteurs de cartes, suivre les instructions dans le manuel du lecteur de cartes.

**Remarque:** Certains lecteurs de cartes abordent les connexions des DEL verte et rouge différemment. Il pourrait être nécessaire d'inverser les connexions des DEL verte et rouge pour assurer un fonctionnement approprié. Cette note s'applique aux lecteurs à DEL à ligne simple et à ligne double.

#### 3.6.3 DELs indicateurs d'état du lecteur de carte

Le lecteur de carte a trois DELs signalant un état :

DEL verte: s'allume en vert continu lorsqu'une porte est déverrouillée

DEL rouge: s'allume en rouge continu lorsqu'une porte est verrouillée

**DEL orange:** s'allume en orange continu jusqu'à ce qu'une carte soit utilisée pour la première fois. La DEL reprend un éclairage normal lors des utilisations ultérieures. (Uniquement pour certains modèles)

#### 3.6.4 Vibreur du lecteur de carte

Le vibreur signale des évènements spécifiques par le biais de signaux sonores cadencés:

Carte présentée: un bip bref

Accès accordé: deux bips brefs

Accès refusé: un bip bref et un long bip

**Mode de fonctionnement changé:** trois bips brefs indiquent un changement de l'état du mode Haute sécurité (arrêt ou marche) ou du mode Verrouillage.

Alarme: une série de bip à cadence rapprochée

## 3.7 Réglages des commutateurs DIP SW2

Les commutateurs DIP établissent l'adresse du contrôleur d'accès par carte. Une adresse valide est un nombre quelconque de 1 à 63. Les commutateurs DIP 1 à 6 sont pour l'adressage binaire, le commutateur DIP 1 étant le bit le moins significatif. Le commutateur DIP SW2 se trouve sur la partie centrale supérieure de la carte du contrôleur d'accès par carte. Voir figure 9.



Consultez la section 4 à la page 51 pour obtenir de l'information.

**Remarque:** Les commutateurs 7 et 8 ne sont pas utilisés et doivent gardés les valeurs de réglage d'usine.

**Remarque:** Le commutateur DIP 8 détermine la façon dont l'adresse IP est assignée au module IP pour les contrôles de cartes d'accès avec capacité IP.

- Commutateur DIP 8 FERMÉ : l'adresse IP est assignée à l'aide d'un serveur DHCP. Il s'agit du réglage à l'usine par défaut.
  - Commutateur DIP 8 OUVERT : l'adresse IP est assignée à l'aide du logiciel de configuration.



Figure 21. Emplacement des cavaliers JW1 - JW5 et des commutateurs SW1 et SW2



## 3.8 Réglages des cavaliers

Sur la carte contrôleur se trouvent six cavaliers prédéfinis, comme suit (voir figure 21):

JW1 : sert à mettre à jour le micrologiciel et est toujours ouvert par défaut.

JW2 : sert à mettre à jour le micrologiciel et est ouvert par défaut.Se réferer à la section 3.10 à la page 48.

JW3, JW4 and JW5 : JW3 et JW4 ne sont pas utilisés et s'ouvrent par défaut. Sur les panneaux de modèle MD-10xx, il est possible de court-circuiter le JW5 sur le premier et le dernier panneau, au lieu d'utiliser des résistances de fin de ligne 120  $\Omega$  pour le RS-485.

JW6 : n'est pas utilisé et est ouvert par défaut.

## 3.9 Alimenter contrôleur

Avant d'alimenter le contrôleur, il faut s'assurer que les raccordements sont conformes au bon fonctionnement des appareils. Par exemple, la serrure magnétique exige une alimentation avec la configuration par défaut.

Une fois le contrôleur alimenté, vous devez commencer à configurer. Pour obtenir des informations détaillées sur la façon de configurer le contrôleur, référez-vous au Manuel de configuration et d'administration LT-995.

#### 3.9.1 Valeurs par défaut de la configuration

Une fois le contrôleur alimenté, il fonctionne selon les valeurs prédéterminées par défaut. Quand vous utilisez le logiciel configurateur pour la première fois, celui-ci utilise les valeurs par défaut comme réglages par défaut.

Les valeurs prédéterminées par défaut sont utilisées, seulement, dans les cas suivants:

- le système est alimenté pour la première fois
- corruption de la mémoire
- mise à jour du programme

## 3.10 Mise à jour du micrologiciel

Vous pouvez mettre à niveau le micrologiciel sur votre panneau avec le logiciel de configuration TX3 en utilisant l'une des méthodes suivantes :



- Assistant intelligent de mise à niveau du micrologiciel
- Mise à niveau du micrologiciel de réseau

L'assistant de mise à niveau du micrologiciel peut être utilisé pour mettre à niveau un panneau à la fois. Il fonctionnera sur tous les panneaux.

La procédure de mise à niveau du micrologiciel de réseau peut mettre à niveau plus d'un panneau à la fois. Pour être en mesure d'utiliser la mise à niveau du micrologiciel de réseau, tous les panneaux doivent déjà avoir un micrologiciel qui supporte cette fonction installée.

Consultez le manuel de configuration TX3 et de l'administrateur LT-995 pour connaître les instructions relatives aux méthodes de mise à niveau du micrologiciel. Le manuel LT-995 se trouve sur le CD d'installation du logiciel de configuration TX3, sur la clé USB ou le site Web de Mircom.

#### 3.10.1 Contrôle de version du micrologiciel

Le numéro de version est accessible depuis le logiciel configurateur et change chaque fois qu'une mise à jour, majeure, mineure ou une révision est apportée.

La convention suivante indique des modifications majeures, mineures ou des révisions:

Version initiale. Version 1.00.0

Version majeure. Version 2.00.0

Version mineure. Version 2.01.0

Révisions. Version 2.01.1

## 3.11 Commencer à configurer

Le contrôleur d'accès par carte est, maintenant, configurable soit par une:

- connexion USB
- connexion Ethernet
- connexion port COM
- connexion modem

Pour une description détaillée de la configuration et de la façon d'établir une connexion au contrôleur d'accès par carte par le biais d'une connexion USB, port COM ou modem, se référer aux manuels:

• LT-995FR TX3 Manuel de Configuration et d'Administration

# Mircom<sup>®</sup>

• LT-973FR Systèmes d'accès par Téléphone Démarrage rapide du Configurateur

#### S'assurer:

- que le contrôleur et tous les dispositifs et composantes raccordés sont entièrement opérationnels.
- que les commutateurs DIP du contrôleur (SW2) ont une adresse réseau unique.
- que le logiciel configurateur est établi avec la bonne adresse réseau du contrôleur.
- que votre PC et le Configurateur sont établis avec la date et l'heure exactes.

#### Commencer à configurer

- 1. Connectez le PC au contrôleur par le biais d'un port USB.
- 2. Lancez le Configurateur et cliquez sur « Connect » (connecter). Une fois connecté, l'icône « connexion » s'affiche dans la barre d'outils du Configurateur.
- 3. Configurez le système d'accès par carte, en suivant les instructions indiquées au Configurator Software Program TX3-MSW ou au LT-995 Configuration and Administration Guide.



# **4** Réglages du commutateur DIP d'adressage

ADRESSE	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
1	ON	OFF	OFF	OFF	OFF	OFF
2	OFF	ON	OFF	OFF	OFF	OFF
3	ON	ON	OFF	OFF	OFF	OFF
4	OFF	OFF	ON	OFF	OFF	OFF
5	ON	OFF	ON	OFF	OFF	OFF
6	OFF	ON	ON	OFF	OFF	OFF
7	ON	ON	ON	OFF	OFF	OFF
8	OFF	OFF	OFF	ON	OFF	OFF
9	ON	OFF	OFF	ON	OFF	OFF
10	OFF	ON	OFF	ON	OFF	OFF
11	ON	ON	OFF	ON	OFF	OFF
12	OFF	OFF	ON	ON	OFF	OFF
13	ON	OFF	ON	ON	OFF	OFF
14	OFF	ON	ON	ON	OFF	OFF
15	ON	ON	ON	ON	OFF	OFF
16	OFF	OFF	OFF	OFF	ON	OFF
17	ON	OFF	OFF	OFF	ON	OFF
18	OFF	ON	OFF	OFF	ON	OFF
19	ON	ON	OFF	OFF	ON	OFF
20	OFF	OFF	ON	OFF	ON	OFF
21	ON	OFF	ON	OFF	ON	OFF
22	OFF	ON	ON	OFF	ON	OFF
23	ON	ON	ON	OFF	ON	OFF
24	OFF	OFF	OFF	ON	ON	OFF
25	ON	OFF	OFF	ON	ON	OFF
26	OFF	ON	OFF	ON	ON	OFF
27	ON	ON	OFF	ON	ON	OFF

#### Table 3: Réglages du commutateur DIP d'adressage SW2



ADRESSE	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
28	OFF	OFF	ON	ON	ON	OFF
29	ON	OFF	ON	ON	ON	OFF
30	OFF	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON	OFF
32	OFF	OFF	OFF	OFF	OFF	ON
33	ON	OFF	OFF	OFF	OFF	ON
34	OFF	ON	OFF	OFF	OFF	ON
35	ON	ON	OFF	OFF	OFF	ON
36	OFF	OFF	ON	OFF	OFF	ON
37	ON	OFF	ON	OFF	OFF	ON
38	OFF	ON	ON	OFF	OFF	ON
39	ON	ON	ON	OFF	OFF	ON
40	OFF	OFF	OFF	ON	OFF	ON
41	ON	OFF	OFF	ON	OFF	ON
42	OFF	ON	OFF	ON	OFF	ON
43	ON	ON	OFF	ON	OFF	ON
44	OFF	OFF	ON	ON	OFF	ON
45	ON	OFF	ON	ON	OFF	ON
46	OFF	ON	ON	ON	OFF	ON
47	ON	ON	ON	ON	OFF	ON
48	OFF	OFF	OFF	OFF	ON	ON
49	ON	OFF	OFF	OFF	ON	ON
50	OFF	ON	OFF	OFF	ON	ON
51	ON	ON	OFF	OFF	ON	ON
52	OFF	OFF	ON	OFF	ON	ON
53	ON	OFF	ON	OFF	ON	ON
54	OFF	ON	ON	OFF	ON	ON
55	ON	ON	ON	OFF	ON	ON
56	OFF	OFF	OFF	ON	ON	ON
57	ON	OFF	OFF	ON	ON	ON
58	OFF	ON	OFF	ON	ON	ON
59	ON	ON	OFF	ON	ON	ON

#### Table 3: Réglages du commutateur DIP d'adressage SW2



ADRESSE	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
60	OFF	OFF	ON	ON	ON	ON
61	ON	OFF	ON	ON	ON	ON
62	OFF	ON	ON	ON	ON	ON
63	ON	ON	ON	ON	ON	ON

#### Table 3: Réglages du commutateur DIP d'adressage SW2



# 5 Bloc d'alimentation TX3-CX-2 et calculs de batterie

Utiliser les renseignements ci-dessous pour déterminer la source d'alimentation secondaire requise (batteries).

Entrer les valeurs dans les zones ombragées.

 Tableau 4:
 Courant de réserve

Modèle	Numéro		En réserve	Total en réserve (ampères)
ТХЗ-СХ-2	1	Х	0,5	= 0,5
Sortie 7	*	Х	(A) **	=
Sortie 8	*	Х	(B) **	=
Total du courant de r	= (C)			

\* Entrer 1 si une serrure magnétique est utilisée, sinon, entrer 0.

\*\* Entrer les courants tirés pour les sorties 7 et 8. Consulter les spécifications du fabricant du dispositif pour obtenir cette information.

Le courant total des sorties 7 et 8 ne doit pas dépasser 1 A.

## 5.1 Nombre de fois que la porte est ouverte par heure

Entrer les valeurs dans les zones ombragées.

#### Tableau 5: Nombre de fois que la porte est ouverte par heure

Minuterie de porte ouverte (secondes)		Nombre approximatif de fois que la porte est déverrouillée par heure		Nombre de fois que la porte est ouverte par heure (heures)
	Х		/3600	= (D)



## 5.2 Courant total de verrouillage de porte

Entrer les valeurs dans les zones ombragées.

Tableau 6:	Courant total de verrouillage de porte
------------	--

Nombre de fois que la porte est ouverte par heure (tiré du tableau 5)		Nombre d'heures que le panneau doit être alimenté avec les batteries		Courant de réserve pour les sorties 7 et 8 (tiré du tableau 4)	Courant total de verrouillage de porte (Ah)
(D)	Х		Х	(A + B)	= (E)

## 5.3 Exigences de capacité de batterie

Entrer les valeurs dans les zones ombragées.

Total du courant de réserve (tiré du tableau 4)		Nombre d'heures que le panneau doit être alimenté par les batteries (cette valeur doit être identique à celle du tableau 6)		Total de courant pour le verrouillage de porte (tiré du tableau 6)	Exigences de capacité de batterie (Ah)
(C)	Х		+	(E)	= (F)

## 5.4 Sélection de batterie

Entrer les valeurs dans les zones ombragées.

#### Tableau 8: Sélection de batterie

Exigences de capacité de batterie (tirées du tableau 7)			La valeur nominale en Ah requise pour la batterie
(F)	Х	1,2	=Ah



## Information sur la garantie et mise en garde

## **MISE EN GARDE!**

Veuillez lire le présent document ATTENTIVEMENT, car il contient des mises en garde ainsi que des renseignements utiles sur la sécurité des personnes concernant les produits fabriqués par Mircom Group of Companies, y compris les produits de marque Mircom et Secutron qui comprennent, sans s'y limiter, les produits d'alarme incendie, d'appel infirmier, d'immotique, de contrôle d'accès et de cartes d'accès (ci-après appelés individuellement ou collectivement, selon le cas, «système de Mircom»).

## NOTE À TOUS LES LECTEURS :

- 1. **Nature des mises en garde.** Les mises en garde décrites dans le présent document sont communiquées au lecteur par mesure de précaution et ne constituent aucune obligation légale, d'une quelconque nature, pour Mircom Group of Companies. Sans restreindre le caractère général de ce qui précède, le présent document NE doit PAS être interprété d'aucune manière comme étant une modification des droits et des obligations des parties, régis par les documents légaux qui s'appliquent selon les circonstances.
- 2. **Application.** Les mises en garde contenues dans le présent document s'appliquent à l'ensemble du système de Mircom et doivent être lues en parallèle avec :
  - a. le manuel du produit pour le système de Mircom spécifique qui s'applique selon les circonstances;
  - les documents légaux qui s'appliquent à l'achat et à la vente d'un système de Mircom, qui peuvent inclure les modalités ainsi que les énoncés de garantie de la société;
  - c. l'information supplémentaire concernant le système de Mircom ou les droits ou les obligations des parties, selon le cas et les circonstances.
- 4. **Sécurité et assurance.** Peu importe ses capacités, aucun système de Mircom ne constitue un substitut d'assurance des biens ou d'assurancevie. De plus, aucun système de Mircom ne constitue un substitut au comportement sécuritaire des propriétaires, des locataires ou des autres occupants pour prévenir ou minimiser les effets dangereux d'une situation d'urgence. Les systèmes d'immotique produits par Mircom Group of Companies ne doivent pas être utilisés comme systèmes de sécurité incendie, d'alarme incendie ou de sécurité des personnes



## **NOTE AUX INSTALLATEURS :**

Tous les systèmes de Mircom ont été soigneusement conçus pour être aussi efficaces que possible. Cependant, il existe certaines circonstances où ils ne pourraient pas offrir une protection. Voici certaines raisons pouvant être à l'origine d'une défaillance du système. Puisque vous êtes la seule personne en contact avec les utilisateurs du système, veuillez porter chaque élément de cet avertissement à l'attention des utilisateurs du présent système de Mircom. À défaut de bien informer les utilisateurs du système des circonstances en vertu desquelles une défaillance du système pourrait survenir, les utilisateurs pourraient avoir une confiance exagérée envers le système. Par conséquent, il est essentiel d'informer correctement chaque client pour qui vous effectuez une installation de système des différentes formes de défaillance :

- 5. **Installation inadéquate.** Tous les systèmes de Mircom doivent être installés conformément à tous les codes et à toutes les normes applicables afin de fournir une protection adéquate. Les normes nationales exigent une inspection et une approbation par l'autorité compétente après l'installation initiale du système et après tous les changements apportés au système. De telles inspections confirment l'installation appropriée du système.
- 6. Mise à l'essai inadéquate. La plupart des problèmes pouvant empêcher le fonctionnement approprié d'un système de Mircom peuvent être constatés en effectuant une mise à l'essai et un entretien réguliers. L'ensemble du système devrait être mis à l'essai par l'autorité compétente immédiatement après un incendie, une tempête, un tremblement de terre, un accicent ou toute autre activité de construction à l'intérieur ou à l'extérieur des lieux. La mise à l'essai devrait comprendre tous les dispositifs de détection, les claviers, les dispositifs d'affichage d'alarme ainsi que tous les autres dispositifs opérationnels, de même que toutes les consoles, qui font partie du système.

## NOTE AUX UTILISATEURS :

Tous les systèmes de Mircom ont été soigneusement conçus pour être aussi efficaces que possible. Cependant, il existe certaines circonstances où ils ne pourraient pas offrir une protection. Voici certaines raisons pouvant être à l'origine d'une défaillance du système. L'utilisateur peut minimiser l'occurrence des événements suivants grâce à une formation appropriée, à la mise à l'essai et à l'entretien des systèmes de Mircom :

7. **Mise à l'essai et entretien inadéquats.** Il est essentiel d'effectuer une mise à l'essai et un entretien périodiques des systèmes. Les pratiques exemplaires et l'autorité compétente déterminent la fréquence et le type d'essai qui sont requis au minimum. Le système de Mircom peut ne pas fonctionner correctement et l'occurrence des autres défaillances de



système cernées ci-dessous pourrait ne pas être minimisée si la mise à l'essai et l'entretien périodiques du système de Mircom ne sont pas effectués avec diligence et selon les exigences établies.

- 8. **Fonctionnement inapproprié.** Il est important que les utilisateurs du système soient correctement formés sur le fonctionnement du système d'alarme et qu'ils sachent comment réagir lorsque le système affiche une alarme. Un système de Mircom pourrait ne pas fonctionner comme prévu pendant une situation d'urgence où l'utilisateur est incapable de faire fonctionner un interrupteur d'alarme ou un commutateur d'urgence en raison d'une invalidité permanente ou temporaire, d'une incapacité à atteindre le dispositif à temps, d'un manque de familiarité avec le fonctionnement approprié ou de circonstances connexes.
- 9. **Réaction en temps opportun.** Des circonstances peuvent exister où un système de Mircom fonctionne comme prévu, mais où les occupants ne sont pas protégés contre une situation d'urgence en raison de leur incapacité à réagir aux avertissements en temps opportun. Si le système est surveillé, la réponse peut ne pas survenir suffisamment à temps pour protéger les occupants ou leurs biens.
- 10. **Insouciance ou risques pour la sécurité.** De plus, les détecteurs de fumée pourraient ne pas fournir d'avertissements en temps opportun dans le cas des incendies causés par insouciance ou de risques pour la sécurité, notamment fumer dans le lit, les explosions violentes, la libération de gaz, le rangement inapproprié des matériaux inflammables, la surcharge des circuits électriques ou les enfants qui s'amusent avec des allumettes, ou encore, les incendies criminels.
- 11. **Panne d'électricité.** Certains composants des systèmes de Mircom requièrent une alimentation électrique appropriée pour fonctionner. Par exemple, les détecteurs de fumée, les balises, le CVCA et les contrôleurs d'éclairage. Si un dispositif fonctionne seulement avec une alimentation CA, toute interruption, aussi brève soit-elle, rendra le dispositif non fonctionnel pendant que l'alimentation est coupée. Les pannes de courant, peu importe leur durée, sont souvent accompagnées de fluctuations de tension qui peuvent endommager les systèmes de Mircom ou d'autres équipements électroniques. Après une panne d'électricité, effectuez une mise à l'essai complète du système sur-le-champ pour vous assurer qu'il fonctionne comme prévu.
- 12. **Défaillance de la batterie.** Si le système de Mircom ou tout dispositif connecté au système fonctionne à batterie, il est possible que celle-ci fasse défaut. Même si les batteries n'ont pas fait défaut, elles doivent être pleinement chargées, en bon état et installées correctement. Certains systèmes de Mircom utilisent des batteries remplaçables, qui ont des durées de vie limitées. La durée de vie prévue d'une batterie est variable et dépend, en partie, de l'environnement du dispositif, de l'usage et du type. Les conditions ambiantes, comme l'humidité, les températures élevées ou basses ou les fluctuations importantes de la température, peuvent réduire la durée de vie prévue de la batterie. De plus, certains systèmes de Mircom



ne sont pas dotés d'un dispositif de surveillance de la batterie pour alerter l'utilisateur dans l'éventualité où la batterie s'approcherait de la fin de son cycle de vie. La mise à l'essai régulière et les remplacements sont essentiels pour s'assurer que les batteries fonctionnent comme prévu, qu'elles soient ou non dotées d'un dispositif de surveillance de batterie faible.

- 13. **Obstacles physiques.** Les détecteurs de mouvements qui font partie du système de Mircom doivent être dégagés, exempts d'obstacles qui pourraient nuire à la capacité des détecteurs de détecter les mouvements. Les signaux communiqués par un système de Mircom pourraient ne pas atteindre le récepteur si un article (en métal, en béton ou de l'eau) est placé sur ou à proximité de la trajectoire radio. Le brouillage intentionnel ou toute autre interférence radio accidentelle peut aussi nuire au fonctionnement du système.
- 14. **Proximité de l'emplacement des dispositifs sans fil.** De plus, tous les dispositifs sans fil doivent respecter les distances minimales et maximales des larges objets en métal, tels que les réfrigérateurs. Vous devez consulter le manuel spécifique au système de Mircom et le guide d'application pour connaître les distances maximales requises entre les dispositifs et l'emplacement suggéré des dispositifs sans fil pour un fonctionnement optimal.
- 15. **Non-déclenchement des détecteurs.** De plus, les systèmes de Mircom peuvent ne pas fonctionner comme prévu si les détecteurs de mouvements, de chaleur ou de fumée ne sont pas déclenchés.
  - a. Les détecteurs d'un système d'alarme incendie peuvent ne pas se déclencher si l'incendie se trouve dans une cheminée, dans les murs, sur le toit ou de l'autre côté des portes fermées. Les détecteurs de fumée et de chaleur peuvent ne pas détecter de fumée ou de chaleur si l'incendie se trouve sur un autre étage de la résidence ou du bâtiment. Dans ce cas, le panneau de contrôle pourrait ne pas alerter les occupants de la présence d'un feu.
  - b. Les détecteurs d'un système d'appel infirmier pourraient ne pas se déclencher si les mouvements surviennent à l'extérieur de la plage de détection. Par exemple, si les mouvements surviennent de l'autre côté des portes fermées ou sur un autre étage de la résidence ou du bâtiment, le détecteur de mouvements pourrait ne pas se déclencher. Dans ce cas, le contrôleur central pourrait ne pas enregistrer un signal d'alarme.
- 3. **Interférence avec les appareils de notification sonores.** Les autres sources de bruits, notamment les chaînes stéréo, les radios, les téléviseurs, les climatiseurs, les appareils ou la circulation avoisinante, peuvent nuire aux appareils de notification sonores. Cependant, peu importe le réglage du volume, les personnes malentendantes pourraient ne pas entendre les appareils de notification sonores.

# 

- 4. **Autres obstacles.** Les appareils de notification d'alarme, comme les sirènes, les cloches, les klaxons ou les stroboscopes, pourraient ne pas avertir ou réveiller un occupant qui dort si un mur ou une porte nuit au passage de l'alarme. Il est moins probable qu'un occupant soit alerté ou réveillé lorsque les appareils de notification sont situés sur un étage différent de la résidence ou des lieux.
- 5. **Défectuosité du logiciel.** La plupart des systèmes de Mircom sont dotés d'un logiciel. Aucune garantie n'est fournie concernant les composants du logiciel des produits ou les produits logiciels autonomes des systèmes de Mircom. Pour consulter les énoncés de garanties ainsi que les exclusions et les limitations de responsabilités, référez-vous aux modalités et aux garanties de la société.
- 6. **Défectuosité des lignes téléphoniques.** Le service téléphonique peut entraîner une défaillance lorsque le système est fondé sur les lignes téléphoniques. Les alarmes et l'information provenant d'un système de Mircom pourraient ne pas être transmises si une ligne téléphonique est hors de service ou occupée pendant une certaine période. Les alarmes et l'information pourraient ne pas être transmises lorsque les lignes téléphoniques ont été compromises par l'entremise d'activités de sabotage criminel, de la construction locale, des tempêtes ou des tremblements de terre.
- 7. **Défaillance des composants.** Même si tous les efforts ont été déployés pour assurer la fiabilité maximale du présent système de Mircom, le système peut ne pas fonctionner comme prévu en raison de la défaillance d'un composant.
- 8. **Produits intégrés.** Le système de Mircom pourrait ne pas fonctionner comme prévu s'il est connecté à un produit qui ne provient pas de Mircom ou à un produit de Mircom qui est jugé incompatible avec un système de Mircom particulier. Vous pouvez demander et obtenir une liste des produits compatibles.

## Garantie

Tous les achats des produits de Mircom sont régis par :

https://www.mircom.com/product-warranty

https://www.mircom.com/purchase-terms-and-conditions

https://www.mircom.com/software-license-terms-and-conditions



## Avis spéciaux

## Numéro du modèle: TX3

## Conforme aux:

#### Federal Communications Commission (FCC):

- CFR 47, Partie 15, Sous partie B, Classe B
- Rayonnements non intentionnels

#### Industrie Canada (IC):

- ICES-003, 4e édition, CLASSE B
- Vérification autorisation appareil numérique

## Numéros d'homologation

FCC (É.U.): 1M8TE00BTX3

IC (Canada): 1156A-TX3