

3.2.1.8.7. Matériel anti-agression

A. Guichet anti-agression

Ce matériel a pour objet d'assurer, dans des locaux accessibles au public où sont manipulés des fonds et des valeurs, la protection des personnes et des biens contre les agressions à main armée, notamment.

On distingue deux types de guichets :

A.1 guichet mobile

Il se présente sous forme d'éléments modulaires dans lesquels un panneau mobile blindé est incorporé en partie basse.

En cas de besoin, ce panneau se ferme et isole les employés des agresseurs en supprimant tout contact physique, visuel et phonique.

A.2 guichet fixe

Il se présente sous forme d'éléments modulaires constitué en partie inférieure de panneau blindé et en partie supérieure de vitrage renforcé, voire pare-balle.

Il est équipé de passe-documents, de passe-paquets, et de moyens de communication.

B. Caisse escamotable

Elle permet la protection instantanée des fonds et des valeurs en cas d'agression. Une pédale ou un bouton déclenche l'escamotage. D'un faible encombrement, elle est, en outre, rapide et discrète.

3.2.1.9. Equipement de protection contre les impulsions électro-magnétiques et les rayonnements compromettants.

Ces domaines spécifiques sont rappelés pour mémoire, le ministère de la défense, le ministère de l'intérieur, notamment, sont capables, cas par cas, d'évaluer les risques et de proposer les solutions.

3.2.2. *Contrôle d'accès*

3.2.2.1. Définitions

Le contrôle d'accès identifie et autorise à pénétrer toute personne se présentant par une entrée normale dans une enceinte protégée ou une zone contrôlée.

L'efficacité du contrôle d'accès dépend de l'étanchéité de l'enceinte, du nombre d'accès, des flux d'entrées et de sorties, de la définition précise des procédures de circulation autour du bâtiment comme à l'intérieur des locaux.

La valeur opérationnelle du contrôle d'accès est fonction de sa capacité à :

- identifier et/ou authentifier ;
- informer ;
- retarder ;
- intervenir.

Ces quatre critères doivent tenir compte :

- du nombre de personnes susceptibles de franchir chaque point de passage ;
- de la faculté de le pénétrer en force ou de déjouer les sécurités de l'accès ;
- de la permanence du contrôle : relèvements ou repos des personnels, maintenance des équipements ;
- et des conditions particulières : d'environnement (température, humidité, etc.) ou d'exploitation.

Le contrôle d'accès peut être confié à des personnels ou à des systèmes. Ces derniers seront spécifiques et indépendants des autres systèmes de gestion « GTB » – « GTC », etc., cette dernière disposition est impérative.

3.2.2.2. Contrôle par surveillance humaine

Un gardien, un surveillant ou autre préposé contrôle les personnes (personnel et visiteurs) se présentant à l'accès.

La vérification peut se fonder sur un document administratif d'identité, de préférence, muni d'une photographie.

L'autorisation délivrée au visiteur précise en outre les locaux accessibles et la durée de validité.

3.2.2.3. Contrôle par systèmes mixtes

Un gardien, un surveillant ou autre préposé associé à des systèmes de contrôle d'accès valide l'autorisation d'accès.

3.2.2.4. Contrôle automatique

L'autorisation d'accès au porteur d'un signe de reconnaissance est confié à un système.

Cette autorisation peut être générale à l'ensemble du bâtiment ou réservée à certaines zones, permanente ou limitée par tranches horaires déterminées au préalable.

3.2.2.4.1. Systèmes d'identification par cartes

Ces systèmes sont les plus fréquemment utilisés.

Les différents types de cartes appelées également badges sont notamment :

- magnétiques :
 - à piste ou couche mince ;
 - à couche épaisse ;
- à effet Wiegand ;
- de proximité (électronique passive) ;
- mains libres (électronique active) ;
- optiques ;
- à circuit microprogrammé :
 - à circuit intégré (ou à microprocesseur) dite à « puce » ;
 - à logique électronique.

Chaque technologie ayant des avantages et des inconvénients, le choix est fonction :

- de l'application souhaitée (contrôle d'accès, horaire variable, restauration...) ;
- de catégorie d'utilisateurs (bureaux, ateliers...) ;
- de l'environnement radio-électrique ;
- de l'environnement atmosphérique (corrosion...) ;
- du degré de sécurité recherché.

3.2.2.4.2. Systèmes d'identification par code

Un lecteur électronique enregistre sur place les données codées que lui fournit la personne désireuse d'entrer. Le code est le plus souvent composé sur un clavier digital, qui peut être à touches aléatoires.

On distingue la composition d'un code :

- général ;
- individuel ;
- individuel après lecture d'un badge général ;
- individuel après lecture d'un badge personnalisé.

3.2.2.4.3. Systèmes d'identification physique

Ces systèmes permettent, à partir de matériels spécifiques, de reconnaître une particularité physique de la personne.

- Élément anthropométrique :
 - empreinte digitale ;
 - forme générale de la main ;
 - image rétinienne ;
 - forme du profil ;
 - morphologie de l'oreille ;
- empreinte vocale ;
- dynamique de signature ;
- etc.

3.2.2.4.4. Systèmes à comparaison vidéo

L'image de la personne que transmet la télévision en circuit fermé est comparée à une image de référence. Cette comparaison peut être électronique ou humaine.

3.2.3. Moyens de détection

Les moyens de détection peuvent être installés à l'extérieur (à la périphérie, sur le périmètre du bâtiment) ou à l'intérieur, afin de déjouer la pénétration hors des accès autorisés.

Ce sont notamment :

- des matériels utilisant l'électronique ;
- des équipements facilitant la surveillance humaine ;
- une combinaison de ces deux moyens.

3.2.3.1. Moyens électroniques

3.2.3.1.1. Limites d'utilisation

Une analyse fine des conditions locales doit précéder le choix de tout système de détection.

Il faut, dans ces cas, tenir compte de :

- la topographie du terrain ;
- l'environnement atmosphérique (vent, pluie, brouillard, neige, orages...) ;
- l'environnement des établissements (lignes à haute tension, voie ferrée et routière, présence d'animaux...).

Toutefois, quelles que soient les technologies retenues, des déclenchements n'ayant pas de rapport avec un facteur humain peuvent survenir.