REPUBLIQUE DU CAMEROUN
Paix - Travail - Patrie

AUTORITE AERONAUTIQUE

REPUBLIC OF CAMEROON
Peace - Work - Fatherland

CAMEROON CIVIL AVIATION AUTHORITY

Instruction n° 00078 /CCAA/DG/DSF du 07 AVR. 2006
fixant les dispositions matérielles de sûreté aérienne

1- Généralités

1.1 Les dispositions matérielles ne sont qu'un aspect de la protection en matière de sûreté et elles doivent être appuyées par un personnel convenablement formé, une planification conjoncturelle rationnelle et complète et des plans et ordres de sûreté concis et bien écrits.

1.2 Pour que les risques soient bien gérés dans le domaine de la sûreté, il faut trouver les façons les plus efficaces (et les plus économiques) de contrer la menace par une combinaison de mesures dans chacun de ces domaines. Cependant, une bonne protection matérielle, de préférence incorporée dès le début dans tout aéroport ou bâtiment, est d'une importance fondamentale pour la riposte aux actes d'intervention illicite.

2- Dispositions de sûreté au périmètre extérieur

3. Le périmètre d'une zone de sûreté à accès réglementé peut être défini par une limite naturelle, par des clôtures ou des murs indépendants, par les murs extérieurs d'un bâtiment ou par des séparations à l'intérieur d'un bâtiment. Il a pour fonction d'exercer sur les intrus un certain degré de dissuasion d'ordre physique, psychologique ou légal. Son efficacité comme mesure de sûreté peut être rehaussée par un système périphérique de détection d'intrusion, la télévision en circuit fermé, un éclairage de sûreté et des patrouilles par des gardes.

2.1 Clôtures

2.1.1 Le niveau de protection procuré par une clôture dépend de sa hauteur, de sa construction, des matériaux utilisés et de toutes caractéristiques additionnelles de sûreté servant à rehausser son efficacité, par exemple barbelés au sommet, détecteurs d'intrusion, éclairage, télévision. Le type de clôture à employer sur le périmètre d'un site doit correspondre aux types de menaces à attendre, et pour l'évaluation des risques de sûreté et la riposte les clôtures sont classifiées selon le niveau de protection qu'elles procurent, la classe A étant celle du plus haut degré et la classe D celle du degré le plus bas.

- *Classe A.* Barrière de haute sûreté conçue pour procurer le maximum de dissuasion et de retardement dans le cas d'un intrus habile et déterminé, bien équipé et doté de bonnes ressources. Elle est conçue et construite pour bien résister à une attaque par franchissement ou par brèche. Ce type de clôture est normalement complété par d'autres systèmes de sûreté périphérique.

- *Classe B.* Barrière de sûreté intermédiaire, conçue pour dissuader et retarder un attaquant ingénieux qui a accès à un jeu limité d'outils à main. La conception et la construction procurent une résistance aux tentatives de franchissement et de brèche.

- *Classe C.* Clôture anti-intrusion offrant un certain degré de résistance aux tentatives de franchissement et de brèche par un intrus opportuniste n'ayant pas d'habileté particulière et utilisant un matériau et des moyens aisément accessibles.

- *Classe D.* Clôture conçue sans exigence particulière de sûreté. Ce genre de clôture ne sert qu'à marquer une limite et ne procure qu'un minimum de dissuasion ou de résistance, sans effet sur un intrus déterminé ou même du bétail. Tous types de matériaux de construction ou de haies peuvent être considérés comme constituant une clôture de classe D.

2.1.2 Une clôture ne procure à elle seule qu'un degré limité de sûreté. Toute clôture peut être franchie ou trouée en quelques minutes ou même quelques secondes par un intrus habile et déterminé. Pour rehausser son efficacité comme barrière ou dissuasif d'intrusion, la clôture doit être surveillée et dotée d'une certaine forme de système de détection d'intrusion. De plus, elle doit être inspectée fréquemment afin qu'il soit vérifié qu'elle est en bon état et ne porte pas de signes d'immixtion.

2.1.3 L'efficacité d'un périmètre de sûreté dépend en grande partie du niveau de sûreté aux points d'entrée. Les portes doivent être construites selon la même norme de sûreté que la clôture et une certaine forme de contrôle d'entrée doit être en place, sinon la sûreté de la clôture n'est pas garantie. Les clôtures et tous points d'entrée doivent aussi être dotés d'un éclairage de sûreté adéquat. Les caractéristiques ci-après sont souhaitables :

- la hauteur et la construction de la clôture de sûreté doivent être en rapport avec le degré de dissuasion physique requis;
- l'accès ne doit pas être possible au-dessous de la clôture ou par des conduits, caniveaux, etc. Le bas du matériau de clôture doit être bien enterré ou sécurisé d'une autre façon (idéalement dans un seuil en béton) pour empêcher d'y creuser;
- si possible, la clôture doit être en ligne droite pour faciliter la construction et la surveillance. Les points où la clôture change de direction sont habituellement plus faciles à franchir et doivent donc être aussi peu nombreux que possible;
- la totalité de la zone de la clôture doit, si possible, être observable par des gardes en poste fixe ou en patrouille. Il peut être nécessaire de raccourcir le périmètre pour qu'il n'y ait pas de zone clôturée qu'il soit impossible d'apercevoir. Cela s'applique non seulement aux murs et aux clôtures en matériaux opaques, mais aussi aux clôtures transparentes, car celles-ci deviennent ordinairement opaques sous certains angles. On peut aussi avoir recours à la télévision en circuit fermé;
- si possible, la superficie des deux côtés de la clôture doit être dégagée sur une distance raisonnable, afin de ne pas permettre à un intrus de se cacher, et il ne doit pas y avoir d'obstacles empêchant de voir (poteaux d'éclairage, panneaux de signalisation, équipements, véhicules, arbres) ou facilitant le franchissement de la clôture. À cet effet, il peut être nécessaire de placer la clôture en retrait de la limite réelle du site, afin de laisser une superficie dégagée à l'extérieur de la clôture;
- des moyens de dissuasion de franchissement, par exemple des fils barbelés ou des enroulements de barbelés, doivent être placés au sommet de la clôture. Des fils barbelés ou des enroulements de barbelés au bas de la clôture, sur le côté intérieur, peuvent dissuader de creuser. Il peut y avoir des incidences judiciaires si ces moyens sont utilisés dans des zones auxquelles le public a accès, aussi est-il bon d'obtenir un avis juridique sur cette question;
- les portes doivent être construites selon des normes comparables à celles de la clôture;
- le type de clôture retenu doit être compatible avec le terrain et avec le besoin de systèmes de détection d'intrusion et/ou de télévision en circuit fermé.

2.1.4 Des clôtures transparentes sont habituellement préférées à des clôtures opaques, car elles permettent aux gardes de voir à l'extérieur de la zone protégée. Elles peuvent être construites en treillis métallique, en tôles ajourées, en grilles d'acier ou en maillage soudé.

8. Si une clôture opaque est nécessaire, il faut tenir compte de ce qui suit :

- les clôtures en acier profilé sont habituellement faites de tôles d'acier galvanisé boulonnées sur un cadre de clôture en acier;
- des murs ne sont pas ordinairement recommandés à des fins de sûreté, même si leur pénétration est relativement difficile, parce que leur construction est coûteuse;
- les clôtures en bois de tous genres sont interdites à des fins de sûreté.

2.2 Systèmes périphériques de détection d'intrusion

2.2.1 Des systèmes périphériques de détection d'intrusion peuvent être utilisés sur le périmètre afin de rehausser le niveau de sûreté de la clôture. Ce sont des dispositifs électroniques qui permettent de détecter l'entrée ou une tentative d'entrée par un intrus sur le périmètre extérieur d'une installation, et qui déclenchent une alarme. S'ils sont bien déployés, ils peuvent rehausser l'efficacité d'autres moyens périphériques (par exemple clôtures et gardes) mais ils sont sujets à de fausses alarmes et par conséquent ne doivent être utilisés qu'avec un système de vérification d'alarmes, par exemple télévision en circuit fermé ou gardes. De plus, s'ils sont mal situés leur taux probable de détection peut être faible. Ces systèmes peuvent être installés comme moyens furtifs (mais cela est habituellement pour des raisons d'esthétique) ou comme moyens visibles et dissuasifs.

2.2.2 Avant de décider d'installer un système de détection d'intrusion, il importe de déterminer si cela est vraiment nécessaire et de procéder à une étude sur le terrain pour déterminer la faisabilité. L'étude sur le terrain doit être effectuée par un géomètre qualifié qui doit prendre en compte :

- le type de clôture ou de mur à surveiller;
- la longueur de chaque périmètre à surveiller;
- la présence ou l'absence d'une superficie suffisante pour établir des zones stériles de détection sur le côté exposé de chaque périmètre;
- la nature du terrain et de la surface du sol;
- les conditions météorologiques dominantes et la faune locale;
- les ressources disponibles pour la vérification des alarmes, par exemple télévision en circuit fermé et gardes.

3- Eclairage de sûreté

3.1 Généralités

3.1.1 Un éclairage de sûreté peut être un excellent moyen de dissuader des intrus potentiels, en plus d'illuminer pour une surveillance efficace, soit directement par des gardes soit indirectement par télévision en circuit fermé. Un éclairage de sûreté peut beaucoup contribuer à la sûreté matérielle, mais s'il est mal appliqué il risque d'être plus utile aux intrus qu'aux gardes. Un bon éclairage de sûreté devrait :

- permettre aux gardes d'apercevoir les intrus avant qu'ils atteignent leurs objectifs;
- ne pas permettre aux intrus d'apercevoir les gardes;
- dissuader les intrus ou les gêner dans leur action.

3.1.2 Un éclairage de sûreté est un dissuasif particulièrement utile et économique. Même un faible degré d'éclairage dissuade la plupart des intrus et vandales potentiels. Si la télévision en circuit fermé est installée, le niveau et l'uniformité de l'éclairage doivent permettre de présenter aux gardes une image claire sur les moniteurs.

3.1.3 Il est nécessaire d'inspecter fréquemment et d'entretenir les lampes de sûreté, car la lumière qu'elles projettent diminue notablement après un usage prolongé. Les lampes qui nécessitent une longue période d'activation ne conviennent pas pour certaines applications d'éclairage de sûreté. Des commutateurs programmables, des détecteurs de mouvement ou des détecteurs photoélectriques peuvent être utiles pour commander l'éclairage de sûreté, mais les derniers nommés sont vulnérables aux immixtions.

3.2 Types d'éclairage de sûreté

3.2.1 Il y a différents types d'éclairage de sûreté pour certaines applications :

- *L'éclairage périphérique* est conçu pour projeter une forte lumière sur le périmètre. Il peut être réalisé par des lampes en position élevée ou par des lampes en position basse qui éblouissent et dissuadent les intrus. Dans le cas de ces dernières, il faut veiller à ce qu'elles ne créent pas une nuisance ou un danger pour les aéronefs.
- *L'éclairage de superficie* est destiné à éclairer des zones à l'intérieur du périmètre, que des intrus doivent traverser pour atteindre leurs objectifs. Il améliore l'aptitude des gardes à détecter les intrus et constitue un puissant dissuasif. Idéalement, l'éclairage doit être uniforme et sans ombres. Chaque partie de la superficie à couvrir doit être éclairée par deux lampes au minimum, pour prémunir contre les lampes brûlées.
- *L'éclairage local* doit éclairer les zones mal couvertes par l'éclairage de superficie, où un intrus peut se dissimuler. De petites lampes encastrées, solides et résistantes aux immixtions, doivent être utilisées. Des lampes fluorescentes ou des lampes au tungstène ou à halogène peuvent être utilisées dans de petits projecteurs. Tous les points sombres doivent être éliminés. Les toits, issues d'incendie et sorties de secours doivent être dotés d'un éclairage local.
- *L'éclairage d'illumination* doit être utilisé pour illuminer des surfaces (par exemple bâtiments et clôtures) devant lesquelles des intrus doivent passer pour atteindre leurs objectifs. Aux faibles niveaux d'illumination typiques de l'éclairage de sûreté, l'oeil compte surtout sur l'aptitude à distinguer des silhouettes. Une silhouette mouvante ressort clairement devant un mur illuminé (de préférence peint en blanc ou d'une couleur claire).

3.2.2 La protection physique procurée par les installations d'éclairage doit être en rapport avec la menace. Des fixations solides, des fils blindés et des commutateurs protégés sont normalement nécessaires. L'alimentation électrique doit être distincte de l'alimentation normale. Les aires particulièrement importantes, par exemple les postes de stationnement isolé d'aéronefs, peuvent nécessiter un double câblage et des générateurs de secours pour garantir la continuité en cas d'immixtion. Les circuits d'éclairage peuvent être reliés aux systèmes de détection afin que toute immixtion déclenche une alarme.

4- Télévision en circuit fermé

4.1 Généralités

4.1.1 L'utilisation de la télévision en circuit fermé pour la surveillance permet d'économiser de la main-d'oeuvre et de couvrir de vastes superficies ou de longs périmètres, particulièrement si elle est en conjonction avec des systèmes de détection d'intrusion et de contrôle automatique d'accès, et elle peut compléter, étendre et améliorer un système de sûreté existant. Elle rehausse aussi l'efficacité de la sûreté périphérique, particulièrement si elle sert à vérifier les alarmes d'un système de détection d'intrusion. Elle peut aussi améliorer les conditions de travail des gardes, qui n'ont pas à s'exposer au danger, aux intempéries ou à d'autres inconvénients de patrouilles de routine et de tâches connexes. Toutefois, l'efficacité du système dépend de la sélection d'un équipement adéquat et de sa bonne installation.

4.1.2 La gamme des systèmes de télévision en circuit fermé va de simples systèmes intérieurs ou extérieurs jusqu'à des systèmes complexes à plusieurs caméras pour les bas niveaux d'éclairage. Dans le système le plus simple, une caméra est reliée par fil à son propre moniteur qui est normalement situé dans un centre de surveillance. Une caméra fixée sur un bâtiment ou une autre construction extérieure procure un champ de vision qui permet à un garde de contrôler, par exemple, le système d'accès à un bâtiment ou une zone sécurisée. Des systèmes plus complexes, tels que des caméras à zoom et à mouvement latéral et vertical (souvent appelées caméras mobiles), ainsi qu'un éclairage artificiel (en lumière visible ou en infrarouge), permettent une surveillance 24 heures sur 24. Les applications possibles sont notamment les suivantes :

- surveillance de superficies, par exemple parcs de stationnement;
- surveillance d'alarmes périphériques;
- surveillance ponctuelle, par exemple surveillance d'un équipement ou de points d'entrée qui ne sont pas visibles autrement;
- complément de systèmes de détection d'intrusion, par exemple vérification d'alarmes;
- surveillance de sites ou locaux ATS éloignés;
- surveillance d'équipements.

5- Considérations relatives au système

5.1 Spécifications opérationnelles

18. Il importe que les utilisateurs potentiels définissent clairement ce qu'ils attendent d'un système de télévision en circuit fermé et qu'ils connaissent ses limitations. Il convient de spécifier ce qui suit :

- superficies à surveiller et but de la surveillance de chaque superficie, par exemple contrôle d'accès ou évaluation d'alarmes;
- qualité d'image nécessaire dans chaque superficie surveillée, par exemple aptitude à identifier des personnes et des permis d'identification pour le contrôle d'accès (beaucoup moins de détail peut être acceptable à d'autres fins);
- nécessité ou non d'une relation avec un système de détection d'intrusion;
- surveillance requise;
- toutes autres conditions de performance, par exemple fonctionnement dans des conditions de faible éclairage ou mesures anti-immixtion.

5.2 Étude sur le terrain

19. Une étude sur le terrain doit être effectuée de jour et de nuit (si la surveillance de nuit est souhaitée) et porter sur les points suivants :

- terrain : une même caméra produit des résultats très différents sur des surfaces différentes, par exemple asphalte, gazon, bâtiments en brique rouge;
- climat et environnement : la performance des caméras peut être dégradée par la chaleur, la glace, la forte pluie, la condensation, la poussière, etc.; les caméras peuvent être masquées par la neige, le brouillard, la forte pluie ou la fumée; des accessoires spéciaux, par exemple pare-soleil, essuie-glaces, moyens de chauffage, peuvent être nécessaires;
- sources lumineuses existantes : il faut identifier les sources lumineuses existantes; celles qui peuvent dégrader la performance des caméras doivent être masquées, ou bien les caméras doivent être placées afin de les éviter; il peut s'agir de lampadaires, de projecteurs de sûreté, de lever ou coucher du soleil, de réflexion du soleil sur l'eau, sur des fenêtres, etc.

5.3 Enregistrement vidéo

L'enregistrement vidéo en accéléré sur magnétoscope permet d'avoir sur une seule cassette des durées allant jusqu'à 300 heures. L'aptitude d'enregistrement et de lecture est utile pour l'enregistrement et l'investigation d'alarmes.

5.4 Systèmes vidéo de détection de mouvement

5.4.1 Les équipements vidéo de détection de mouvement contrôlent le signal vidéo pour déceler les mouvements ou les changements d'intensité lumineuse dans l'image et ils alertent l'unité de riposte (normalement, un signal audible pour alerter le garde, couplé à une indication visuelle sur le moniteur). La sensibilité de l'équipement au mouvement ou aux changements d'intensité lumineuse doit être ajustée en fonction des conditions sur le site.

5.4.2 La gamme des systèmes va d'un seul processeur de caméra et d'un seul moniteur jusqu'à des groupes de caméras dont les signaux vidéo sont constamment analysés par un processeur. Il existe des dispositifs qui peuvent s'accommoder de conditions très variables à l'extérieur, alors que beaucoup d'autres sont techniquement limités et utilisables seulement à l'intérieur.

5.4.3 Il faut souligner que les détecteurs vidéo de mouvement ont de grandes limitations dans la pratique. Les caméras de détecteurs vidéo de mouvement donnent des images assez bonnes de scènes extérieures mais sont parfois inutilisables dans des conditions météorologiques défavorables, et elles sont inefficaces s'il y a de multiples mouvements légitimes. Il est toutefois possible, dans certains systèmes, de masquer les secteurs où se situent les mouvements.

5.5 Méthodologie de mise en service et de test de systèmes de télévision en circuit fermé

5.5.1 Tous les systèmes de télévision en circuit fermé doivent toujours être mis en service, puis régulièrement audités, selon une méthodologie appropriée. Une méthodologie de test acceptable doit tester, mesurer et enregistrer, au minimum, les critères suivants :

- angles d'ouverture;
- visibilité de la cible;
- hauteur de l'image de cible;
- temps de réaction du système.

5.5.2 Ces critères doivent avoir été agréés dans la déclaration originale des spécifications opérationnelles. La cible utilisée doit être en relation avec la menace perçue.

6- Définitions et normes minimales

6.1 Angles d'ouverture

Il est bon de vérifier que la zone est couverte avec un minimum de chevauchement. Le degré de chevauchement est défini en pourcentage de la largeur d'image dans le cas de secteurs horizontalement adjacents, ou de la hauteur d'image dans le cas de secteurs verticalement adjacents. Le minimum de chevauchement recommandé est respectivement de 5 et 10 %.

6.2 Visibilité de la cible

La visibilité de la cible exprime la facilité avec laquelle on peut voir une cible sur le moniteur dans les pires conditions d'éclairage. La visibilité de la cible se mesure à l'aide d'une cible camouflée*, de la façon suivante :

Placer la cible camouflée dans les endroits les plus mal éclairés, le moniteur étant obscurci. Laisser l'opérateur regarder le moniteur et noter les réponses comme suit :	
DEGRE 3	Cible facilement visible ; la cible serait immédiatement évidente, sans possibilité d'erreur.
DEGRE 2	Assez aisément visible ; il faut chercher pour trouver la cible mais on ne peut manquer de la trouver dans le temps admissible de réaction du système.
DEGRE 1	Difficile à voir ; la cible n'est trouvée qu'après une recherche longue et attentive, dépassant le temps admissible de réaction du système.
DEGRE 0	La cible n'est pas aperçue du tout.
Seuls les degrés 3 et 2 sont des résultats acceptables.	

6.3 Hauteur de l'image de cible

Il s'agit ici de la hauteur de l'image sur le moniteur, en pourcentage de la dimension verticale de l'écran. Les hauteurs minimales acceptables d'image en pourcentage de la dimension verticale du moniteur sont les suivantes :

Détection de 10 % à 30 %
Reconnaissance de 50 % à 100 %
Identification de 100 % à 250 %

* Quelques exemples de cibles camouflées :

Cible camouflée
Être humain : Une silhouette d'homme habillée d'une veste de camouflage
Porte-documents : Porte-documents sali ou couvert de boue
Plaques d'immatriculation : Plaques d'immatriculation salies avec de la boue

6.4 Temps de réaction du système

6.4.1 Lorsque la télévision en circuit fermé est utilisée en conjonction avec un système de détection périphérique, le temps de réaction est compté à partir du début d'un signal d'alarme jusqu'au moment où l'opérateur a déterminé quel moniteur regarder et a identifié la cible sous une forme visuellement utile. La cible camouflée est placée quelque part dans le champ de vision et une alarme est activée.

6.4.2 Si un système de surveillance par télévision est utilisé sans aucune indication d'alarme, le temps de réaction du système peut être défini sur la base de balayages de surveillance par un opérateur et de la durée du cycle de balayage. L'opérateur a pour rôle de réagir à l'activation d'une alarme et d'initier une riposte avant l'expiration du temps de réaction stipulé.

7- Systèmes automatiques de contrôle d'accès

7.1 Définition

Un système automatique de contrôle d'accès est un système électromécanique relié à un module de commande qui, après vérification des pièces d'identité des utilisateurs, permet automatiquement l'entrée en déverrouillant le point d'entrée. À noter que malgré l'emploi du terme automatique, il faut encore un certain degré de supervision humaine.

7.2 Avantages d'un système automatique de contrôle d'accès

Certains des avantages de l'utilisation d'un tel système sont les suivants :

- le système est permanent et continue de contrôler l'entrée en l'absence temporaire des gardes;
- un système automatique ne se laisse pas distraire, suborner, persuader ou menacer;
- la dépense initiale (à l'exclusion des coûts de maintenance régulière) est un investissement ponctuel, contrairement aux coûts répétitifs de gardes;
- le système peut être programmé pour détecter les tentatives d'utilisation de permis signalés comme perdus ou volés, ou l'emploi par un utilisateur autorisé mais sous contrainte;
- le système procure une barrière matérielle contre l'entrée forcée et protège les gardes qui surveillent le système;
- le système peut être programmé pour enregistrer les mouvements de personnel (par exemple appel nominal, travailleurs en retard).

7.3 Inconvénients d'un système automatique de contrôle d'accès

Certains des inconvénients d'un système automatique de contrôle d'accès sont les suivants :

- il nécessite une supervision humaine à l'égard des visiteurs, livraisons, pannes du système et situations d'urgence;
- il ne peut empêcher l'entrée d'une personne non autorisée en collusion avec une personne autorisée;
- il est uniquement un moyen de contrôler les entrées.

7.4 Types de systèmes automatiques de contrôle d'accès

Un système automatique de contrôle d'accès est basé sur le principe de l'identification des personnes autorisées et du contrôle des barrières d'entrée de façon que seule la personne identifiée soit admise dans la zone contrôlée. Certains des systèmes d'identification largement utilisés dans des applications commerciales sont les suivants :

- système à carte codée, avec ou sans numéro d'identification personnel (NIP);
- système « mains libres », ou par carte ou jeton de proximité (parfois appelé système par radio), avec ou sans NIP;
- système biométrique de contrôle d'accès.

7.5 Système à carte codée

7.5.1 La carte codée est habituellement du format des cartes de crédit et faite de plastique, mais d'autres formes et dimensions de cartes ou jetons sont aussi utilisées. La carte peut porter une image ou un logo et une photographie peut y être fixée afin de permettre l'utilisation comme permis officiel. Lorsque des cartes codées sont utilisées dans un système de permis d'identification de sûreté d'aéroport, les conditions de réalisation et de renouvellement des permis d'identification doivent être respectées.

7.5.2 Chaque carte codée contient un code ou numéro lisible à la machine, qui peut servir à identifier l'entrée du site ou le point de contrôle auquel elle donne accès, et elle peut être répertoriée au nom du titulaire. Il existe plusieurs technologies de codage de cartes, notamment :

- holographie;
- fil de Wiegand;
- bande magnétique en filigrane;
- code-barres en infrarouge;
- bande magnétique à induction;
- ferrite de baryum;
- carte perforée Hollerith;
- répondeur de signal radio.

7.6 Carte codée et NIP

La sûreté du système automatique de contrôle d'accès est nettement rehaussée si la carte est utilisée avec un NIP. Les systèmes où la carte est utilisée sans NIP reconnaissent la carte mais pas la personne qui l'utilise. Le NIP doit être un numéro à quatre chiffres au moins, choisi au hasard et attribué par le gestionnaire du système, et non pas choisi par le postulant.

7.7 Installation d'un système automatique de contrôle d'accès

7.7.1 Deux types de systèmes automatiques sont communément utilisés :

- le système en ligne (relié à un certain nombre de points d'entrée contrôlés qui sont centralement programmés et gérés à partir d'un module ou ordinateur central);
- le système hors ligne (autonome, fonctionnant indépendamment d'autres points d'entrée grâce à son propre module de contrôle local).

7.7.2 Un système à carte codée avec NIP comprend :

- un lecteur de carte avec pavé numérique à chaque point d'entrée;
- un module de contrôle local;
- un module ou ordinateur de contrôle central;
- un module de verrouillage et une barrière.

7.8 Lecteurs

Il existe différents types de lecteurs de cartes, adaptés à la technologie de carte qui est utilisée et à l'environnement dans lequel ils doivent fonctionner. Normalement, deux lecteurs sont utilisés à chaque porte, l'un avec un pavé numérique pour l'entrée dans la zone contrôlée, l'autre sans pavé numérique pour la sortie. De cette façon, le système permet de surveiller et répertorier toutes les entrées et sorties, d'empêcher le transfert d'un permis d'identification de la main à la main et de tenir un registre pour l'appel nominal de tous les occupants de la zone contrôlée.

7.9 Modules de contrôle

Tous les lecteurs de cartes sont reliés à un module de contrôle local. L'utilisateur insère sa carte dans le lecteur et compose son NIP. Le module de contrôle local vérifie ces données en les comparant à celles qui se trouvent dans sa base de données, et il permet l'entrée en dégageant le loquet électrique de la barrière d'entrée. Dans un système en ligne, le module de contrôle local envoie les informations d'entrée au module de contrôle central, où elles sont enregistrées et transmises à tous les autres modules de contrôle local compris dans le système. Par cette diffusion d'informations, toutes les décisions d'accès sont prises au niveau du module de contrôle local et le module de contrôle central agit comme gestionnaire du système et moyen d'archivage.

7.10 Barrières

Une barrière peut être une porte, un tourniquet ou une guérite, et elle est une partie intégrante de tout système automatique de contrôle d'accès. Dans une application de zone de sûreté à accès réglementé, les barrières doivent être hautes et installées de façon qu'il n'y ait pas d'interstices entre elles et le plafond ou les murs et cloisons contigus. Elles doivent être conçues pour ne laisser entrer qu'une personne à la fois. Des précautions additionnelles, par exemple, détecteurs de métaux ou détecteurs de masse, peuvent être incorporées dans une barrière de contrôle d'accès. Aux entrées principales, les barrières les plus efficaces pour le passage de grands nombres d'usagers sont les tourniquets, faits de barres métalliques ou de plaques de polycarbonate.

7.11 Portes

Un système de contrôle d'accès peut être utilisé en conjonction avec une porte ordinaire (par exemple pour contrôler l'accès à une salle à l'intérieur d'un bâtiment), mais cela peut poser des problèmes de sûreté. Le niveau de sûreté obtenu dépend de la sûreté de la porte. Une porte peut être contournée plus facilement qu'une barrière bien conçue, particulièrement si quelqu'un suit de très près une autre personne, aussi est-il conseillé d'installer un fermoir mécanique ajustable.

7.12 Critères de sûreté

Un système installé pour contrôler l'accès à des zones de sûreté à accès réglementé doit être conforme aux critères suivants :

- être raccordé à un générateur de secours;

- se bloquer en position fermée lorsqu'il y a une panne de courant ou une autre situation d'urgence, de sorte que la zone contrôlée par le système demeure sécurisée;
- être doté d'un moyen mécanique de commande manuelle sur le côté sécurisé de la barrière, pour permettre la sortie en situation d'urgence (lorsque le système s'est verrouillé; voir plus haut);
- être doté de serrures de sûreté à utiliser hors des heures de service, à moins d'être situé à l'intérieur du périmètre du site;
- être à l'épreuve des manipulations et immixtions (c'est-à-dire que le câblage peut nécessiter une protection spéciale);
- être doté d'un moyen d'alarme pour signaler les défaillances ou utilisations impropres du système;
- être conçu pour détecter les tentatives d'utilisation de permis d'identification signalés comme perdus ou volés, et empêcher l'entrée;
- être conçu pour refuser l'accès après plusieurs tentatives infructueuses d'entrée (le nombre maximal de tentatives infructueuses ne doit pas normalement être supérieur à trois).

7.13 Système de contrôle d'accès «mains libres»

7.13.1 Dans le système de contrôle d'accès «mains libres» ou par radio, une carte en plastique ou un jeton répond au module d'interrogation de la porte en transmettant un signal codé spécifique. Ce signal est reçu par le module de la porte et vérifié par le système de contrôle d'accès. Si le signal est accepté, la porte est déverrouillée.

7.13.2 Ce type de système présente l'avantage de laisser les mains libres mais il a plusieurs inconvénients du point de vue de la sûreté. Le signal codé peut être enregistré et le jeton peut être copié, ou bien un signal parasite pourrait activer le système de déverrouillage. C'est pourquoi les systèmes «mains libres» doivent toujours être utilisés avec un NIP dans les applications de zone de sûreté à accès réglementé.

7.13.3 Les systèmes «mains libres» peuvent fonctionner sur des distances longues ou courtes. La carte ou le jeton à courte portée doit être placé à moins d'un mètre environ du module de la porte avant de pouvoir agir sur le système de contrôle d'accès. Le système à longue portée, qui agit sur plusieurs mètres, comporte une pile de longue durée à l'intérieur de la carte et s'appelle système de carte active. Les utilisateurs doivent savoir que, vu l'aptitude à transmettre indépendamment du système de contrôle d'accès, un système «mains libres» activé peut présenter un risque de sûreté en servant de microphone d'émission radio.

7.14 Systèmes biométriques

7.14.1 Les systèmes biométriques vérifient l'identité de l'utilisateur en comparant une caractéristique physiologique présentée au point d'entrée avec la même caractéristique stockée dans la mémoire d'un ordinateur. Les systèmes qui existent actuellement sont basés notamment sur les caractéristiques physiologiques suivantes : empreintes digitales, géométrie de la main, rétine de l'oeil, veines sur la main, signature et tonalité de la voix.

7.14.2 Le principal avantage d'un système biométrique est qu'il vérifie l'identité de la personne qui demande l'accès alors que les autres systèmes vérifient seulement la carte (qui a pu être perdue, volée ou contrefaite) et le NIP (qui a pu être mal gardé ou divulgué par le titulaire). L'utilisation frauduleuse d'une caractéristique physiologique est pratiquement impossible sans la coopération active de l'utilisateur légitime.

7.14.3 Les systèmes biométriques ont tendance à être coûteux, leur utilisation demande plus de temps et ils peuvent être considérés comme indiscrets. Il faut les régler à un niveau de sensibilité assez élevé pour empêcher l'accès non autorisé. Cela peut amener à refuser l'accès à un pourcentage excessif d'utilisateurs autorisés.

8- Gestion d'un système automatique de contrôle d'accès

8.1 Planification du système

8.1.1 Un système automatique de contrôle d'accès peut être une méthode efficace, économique et fiable de contrôle d'accès à une zone de sûreté à accès réglementé. Certains systèmes peuvent toutefois être très coûteux et nécessiter une supervision attentive pour le maintien de la sûreté, ainsi qu'une gestion spécialisée et un personnel de soutien.

8.1.2 Un gestionnaire du système doit être désigné pour être responsable du contrôle global et de la supervision du système. Les responsabilités du gestionnaire comprennent le contrôle de la délivrance des cartes et NIP, la validation et l'annulation des autorisations d'accès, l'examen des registres du système et l'investigation des alarmes et défauts de fonctionnement. Seuls le gestionnaire du système et son adjoint doivent avoir accès aux moyens de programmation du système.

8.2 Maintenance et formation

Tous les défauts de fonctionnement doivent être signalés et réparés promptement, et les tentatives de contourner le système doivent être minutieusement investiguées. Il importe de former le personnel de mise en oeuvre et de maintenance avant que le système soit officiellement accepté et remis à l'utilisateur.

8.3 Sûreté du système

Une fois qu'un système a été installé, sa fiabilité et sa sûreté ne peuvent être maintenues que par une bonne gestion, une supervision suffisante et un entretien régulier. Pour cela, il faut veiller à ce que seul le personnel autorisé ait accès à l'ordinateur et à son logiciel. Toutes les cartes perdues, volées ou ayant cessé d'être nécessaires doivent être extraites du système dès que possible. Il peut être approprié de prévoir des arrangements spéciaux, par exemple retrait de cartes ou leur extraction du système, dans le cas de titulaires qui pendant une période prolongée n'ont pas besoin d'accéder à la zone de sûreté à accès réglementé, pour des raisons de congé, maladie ou mutation.

9- Systèmes de détection d'intrusion

9.1 Généralités

9.1.1 Les systèmes de détection d'intrusion (SDI) sont conçus pour détecter l'entrée ou une tentative d'entrée d'un intrus dans une zone protégée, d'identifier le lieu de l'intrusion et d'envoyer une alarme à une unité de riposte.

9.1.2 Aux fins de l'évaluation des risques de sûreté et de la riposte, les SDI sont classés selon le niveau de sûreté qu'ils procurent. Un système de classe 4 procure la sûreté la plus élevée et un système de classe 1 la plus basse; les classes sont les suivantes :

- *Classe 4.* Système d'alarme destiné à des applications où la sûreté est prioritaire par rapport à tous les autres facteurs. Il est destiné à protéger contre les intrus qui sont censés planifier l'intrusion en détail et être en possession d'un jeu complet d'équipements permettant de neutraliser des éléments cruciaux du système. Un système de classe 4 doit être complété par tout un ensemble de dispositions matérielles de sûreté et de procédures de sûreté.
- *Classe 3.* Système d'alarme utilisé dans les locaux où se trouvent des avoirs de grande valeur. Pareil système est aussi complété par des dispositions matérielles de sûreté. Il doit protéger contre des intrus qui connaissent bien les systèmes de détection d'intrusion et ont en leur possession un jeu complet d'outils et d'appareils électroniques portables.
- *Classe 2.* Système d'alarme normalement utilisé dans des locaux où le risque d'attaque sophistiquée n'est pas trop élevé. Les intrus potentiels sont censés avoir une connaissance limitée des systèmes d'alarme et n'avoir en leur possession que des outils et instruments portables simples.
- *Classe 1.* Système d'alarme destiné à des locaux à faible risque, où les intrus potentiels ne connaissent pas bien les systèmes d'alarme et n'ont en leur possession qu'un jeu limité d'outils ordinaires. Pareil système n'est probablement pas complété par une unité de riposte désignée mais compte sur la réaction du public à une alarme sonore locale ou des feux à éclats.

9.1.3 Un SDI assure une surveillance continue sur la zone protégée et permet éventuellement de réduire les effectifs de gardes. Dans certaines circonstances, il peut remplacer les gardes ou encore, s'il est utilisé en conjonction avec des gardes, il peut étendre la couverture à des zones qui ne sont pas normalement accessibles à des patrouilles, par exemple toitures ou salles verrouillées. Il permet de compléter d'autres mesures de sûreté dans l'application du principe de sûreté en profondeur. Un SDI doit toujours être utilisé en conjonction avec des dispositions matérielles de sûreté, par exemple salles fermées à clé et périmètre sécurisé.

9.2 Installation

Il faut procéder avec soin dans la sélection, l'application et l'installation d'un SDI, pour empêcher qu'il soit contourné ou que son utilité soit compromise par un grand nombre de problèmes techniques ou de fausses alarmes. Il importe que les utilisateurs potentiels définissent clairement ce qu'ils attendent d'un SDI et qu'ils connaissent ses limitations. L'étude d'une éventuelle installation de SDI doit clairement établir :

- la superficie ou les équipements à protéger;
- le niveau ou degré de menace;
- si une liaison est nécessaire avec d'autres systèmes électroniques, par exemple télévision en circuit fermé, système automatique de contrôle d'accès;
- si la zone à protéger a des gardes sur le site ou un signal transmis à une unité de riposte;
- le type d'unité de riposte ou d'arrangements de surveillance nécessaires.

9.3 Composants du système

Une installation de SDI comprend une partie ou la totalité des composants ci-après :

- détecteurs;
- tableau de commande avec éventuellement enregistreur et imprimante;
- visualisation d'alarmes;
- câblage d'installation;

- raccordement de signalisation d'alarme entre le tableau de commande et la visualisation d'alarmes;
- unité de riposte;
- alimentation électrique indépendante ou d'appoint, selon le cas.

9.4 Détecteurs

Les détecteurs sont conçus pour déceler une intrusion dans la zone qu'ils couvrent et pour transmettre au tableau de commande une indication de l'état d'alarme. Il existe différents types de détecteurs et le choix dépend de la nature de l'emplacement à protéger. Plusieurs types de détecteurs peuvent être utilisés en combinaison afin de couvrir des secteurs techniques vulnérables, de réduire l'incidence de fausses alarmes et de suppléer aux pannes. L'installation la plus appropriée concentre les détecteurs de SDI aux points d'entrée, c'est-à-dire portes et fenêtres.

9.5 Types de détecteurs

Il existe différents types de moyens de détection, qui se rangent dans les catégories suivantes :

- *Détecteurs par contact,* par exemple microcommutateurs, commutateurs à lamelle magnétique, détecteurs sensibles à la pression ou aux vibrations. Les commutateurs peuvent être utilisés dans le mode ouvert ou fermé, mais il faut veiller soigneusement à ce qu'une panne de courant accidentelle ou délibérée déclenche un signal d'alarme. Dans les installations de haute sûreté, les commutateurs à lamelle magnétique doivent être du type à double lamelle avec protection contre les immixtions.
- *Détecteurs spatiaux ou volumétriques,* conçus pour déceler les mouvements dans leur champ de vision directe et utilisés pour couvrir des salles, des couloirs, des toitures, d'autres zones ouvertes ou des trajets d'entrée. Les détecteurs à ultrasons font appel à des ondes sonores de haute fréquence et à l'effet Doppler de transmissions rayonnées et réfléchies. Ils sont fiables et difficiles à contourner, mais il peut y avoir des fausses alarmes dues à la turbulence atmosphérique ou à des bruits extérieurs comme des sonneries de téléphone. Les détecteurs passifs à infrarouges surveillent le profil de chaleur en infrarouges dans une zone et détectent les changements causés par des intrusions humaines. Les détecteurs à micro-ondes font appel à des transmissions radio en haute fréquence et à leurs réflexions pour déceler les mouvements. En raison des propriétés de pénétration des micro-ondes, il faut étudier attentivement l'implantation et le travail d'installation pour éviter des fausses alarmes qui sont causées par des mouvements hors de la zone protégée.
- *Dispositifs à interruption de faisceau,* habituellement du type actif à infrarouges faisant appel à un émetteur et un récepteur et parfois à des moyens réfléchissants pour projeter un faisceau par le travers d'une ouverture comme une porte ou une fenêtre. L'interruption du faisceau par l'ouverture de la porte ou de la fenêtre ou par le passage d'une personne déclenche l'alarme.
- *Détecteurs de vibrations,* de différents types ou technologies. Le *commutateur à inertie* réagit aux vibrations ou à un impact au moyen d'une bille qui est délogée de ses contacts, ce qui produit une alarme; le *géophone* détecte le mouvement au moyen d'un aimant suspendu se déplaçant à l'intérieur d'une bobine de détection; le *cristal piézoélectrique* a des propriétés qui produisent un courant électrique à partir de pressions structurales et il est utilisé pour détecter les vibrations et déclencher une alarme.
- *Détecteurs à technologie double,* où deux technologies de détection (par exemple infrarouges et micro-ondes) dans un même boîtier se combinent pour déclencher une alarme. De cette façon, la probabilité de fausses alarmes est nettement réduite. Les détecteurs à technologie double doivent toutefois être utilisés avec précaution et seulement là où les circonstances locales ne se prêtent pas à un autre système. Il y a aussi le risque que la

sensibilité globale du système soit réduite s'il est nécessaire que deux dispositifs soient activés à la fois pour qu'une alarme soit déclenchée.

9.6 Tableau de commande

Le tableau de commande a pour fonctions principales de :

- contrôler l'état des détecteurs;
- détecter toute immixtion;
- mettre en marche et arrêter le système;
- signaler un état d'alarme.

9.7 Registre

Les tableaux de commande les plus sophistiqués comportant un microprocesseur incluent généralement un registre électronique qui peut être relié à une imprimante. Ce registre est destiné à répertorier toutes les alarmes et instructions de fonctionnement, par exemple « mise en marche » ou « arrêt » du système, et est utile pour contrôler la sûreté du système et fournir une piste d'audit. Si le tableau de commande n'est pas situé en un point où des gardes sont postés en permanence, il doit être placé au coeur de l'installation de SDI, où il est protégé le mieux possible par le système lui-même et par d'autres dispositions matérielles de sûreté.

9.8 Visualisation d'alarmes

9.8.1 Toute alarme doit être transmise à un poste de contrôle doté d'un personnel permanent, où peuvent être prises des mesures de riposte appropriées. Les alarmes sont normalement données à la fois par des moyens sonores et des moyens visuels et doivent indiquer la nature de l'alarme (c'est-à-dire détection, immixtion, panne de courant) ainsi que son emplacement (c'est-à-dire quel détecteur a provoqué l'alarme). Dans les grands systèmes sophistiqués, des graphiques informatisés et des modules d'affichage visuel peuvent être utilisés pour indiquer le circuit à l'origine de l'alarme, la ou les zones dans lesquelles l'alarme s'est produite, ainsi que ce que le garde doit faire.

9.8.2 Dans les sites à faible risque dotés d'un équipement d'alarme commercial ou domestique contre les cambriolages, la signalisation de l'alarme peut consister en une sonnerie extérieure et un feu à éclats. Ce genre de système repose habituellement sur une réaction du public à l'alarme, car il n'y a pas normalement une unité de riposte désignée. L'emploi de signaux d'alarme publiquement audibles et/ou visibles dans des installations de haute sûreté n'est pas recommandé. Dans ces systèmes, l'alarme indique à l'attaquant où les détecteurs sont installés et quelles réactions l'alarme produit. Les vulnérabilités du système peuvent alors être identifiées et exploitées.

9.10 Transmission d'alarmes

Une certaine forme de communication à distance pour signaler les alarmes à un poste de surveillance est nécessaire si le site protégé est éloigné et s'il ne s'y trouve pas du personnel constamment en poste. La transmission de l'alarme peut se faire par les moyens suivants :

- *lignes exclusives,* c'est-à-dire lignes téléphoniques directes employées exclusivement pour la transmission des alarmes et la surveillance. Ce système protège contre la mise hors circuit ou le sectionnement de lignes, qui causent immédiatement une alarme. Les lignes exclusives risquent d'être coûteuses;
- *autocomposition,* faisant appel à une ligne et un équipement de standard téléphonique; lorsqu'une alarme est déclenchée, le système compose automatiquement un numéro d'appel

d'urgence et transmet un message préenregistré. Dans ce système, la ligne doit être hors annuaire ou servir exclusivement à transmettre des appels mais pas à en recevoir. Cela permet d'assurer que la ligne ne peut pas être occupée par des appels qui empêcheraient la transmission de l'alarme. Ces systèmes ne permettent pas la surveillance continue de la ligne et ne peuvent pas identifier immédiatement les défectuosités ou le sectionnement de la ligne. Ils ne sont donc pas recommandés pour les installations de haute sûreté;

- *liaisons radio,* dans un système de communications multitrajets pouvant inclure différentes caractéristiques comme appels automatiques à des pagers, codage de données et protocoles bilatéraux d'interrogation et de réponse. Le choix du système et ses caractéristiques doivent être étudiés attentivement pour que le niveau approprié de sûreté soit réalisé.

9.11 Câblage

Le câblage d'un système de haute sûreté doit être automatiquement contrôlé en permanence, c'est-à-dire qu'il doit y avoir une analyse électronique continue des connexions des circuits pour vérifier leur bon état de fonctionnement et détecter les immixtions. Il doit y avoir une alarme immédiate en cas de détection d'une défaillance ou d'une immixtion sur la ligne. Dans le cas des installations comportant un niveau de sûreté moins élevé, la surveillance des lignes n'est normalement valable qu'à l'intérieur de la zone protégée. Les câblages qui sont hors de la zone protégée ne peuvent pas être considérés comme sécurisés s'il n'y a pas une protection matérielle additionnelle, par exemple conduits protégés ou câbles blindés.

9.12 Unité de riposte

La mise en place d'une unité de riposte est un élément crucial de tout système de détection d'intrusion. Le délai maximum prescrit d'arrivée d'une unité de riposte sur le site est habituellement de 15 minutes. Si ce délai ne peut pas être respecté, l'efficacité de la riposte est nécessairement douteuse.

Note : Ce délai est un délai maximal et autant que possible l'unité de riposte doit chercher à réaliser un délai de riposte plus court, particulièrement dans des installations de haute sûreté.

9.13 Mise en marche et arrêt

Dans le cas des sites sans personnel permanent, une procédure de mise en marche est nécessaire afin que le SDI puisse être mis en marche et arrêté par du personnel autorisé sans qu'une alarme soit déclenchée. Il y a différents types de procédures de mise en marche, notamment :

- *mécanisme de mise en marche automatique,* par lequel le système est mis en marche et arrêté à une heure prédéterminée;
- *mécanisme de retardement,* par lequel le système laisse s'écouler un délai prédéterminé afin de permettre à l'utilisateur de sortir du site protégé ou d'y entrer après l'exécution de la procédure de mise en marche ou avant la procédure d'arrêt, sans déclencher l'alarme;
- *système de dernière sortie,* par lequel la fermeture de la dernière porte de sortie d'un bâtiment ou d'un site active le SDI grâce à un contacteur monté dans le chambranle de la porte ou dans la serrure;
- *pavé de composition de NIP,* hors de la zone protégée, nécessitant l'entrée d'un numéro codé pour mettre en marche le système ou activer le compte à rebours du mécanisme de retardement.

9.14 Gestion du système

Pour être efficace, un SDI doit être convenablement géré. Une fois installé, on ne peut pas le laisser fonctionner tout seul. Des lignes directrices sur la gestion des SDI sont exposées dans les paragraphes qui suivent.

9.15 Installation et maintenance

9.15.1 La sûreté d'un SDI dépend d'une bonne installation et d'une bonne maintenance. Les schémas de circuits, manuels et pièces de rechange des installations de SDI doivent toujours être tenus sous bonne garde. De plus, s'il y a lieu, tous les travaux d'installation et de maintenance doivent être exécutés par du personnel autorisé, et supervisés par du personnel de sûreté. Toute modification du système doit être notées dans les dossiers, en compagnie des spécifications ou schémas initiaux.

9.15.2 Une source d'alimentation électrique de secours doit toujours permettre au SDI de continuer à fonctionner en cas de panne ou de débranchement de l'alimentation principale. Des piles constamment rechargées sont normalement utilisées à cette fin. Elles doivent avoir une capacité suffisante pour toutes les éventualités. L'état des piles doit être vérifié régulièrement par du personnel autorisé.

9.16 Accès au tableau de commande

Le SDI ne doit être mis en marche ou arrêté que par du personnel autorisé. Le tableau de commande doit par conséquent être positionné et protégé de façon à ce que seul y ait accès le personnel désigné. Si le tableau de commande est doté d'une clé, la clé ne doit jamais être laissée sur le panneau et doit être traitée comme une clé de sûreté. Les codes de fonctionnement doivent être protégés de la même façon que les numéros de serrures à combinaison ou les mots de passe du système. Si le tableau de commande est situé dans une zone qui n'est pas supervisée en permanence, il peut être nécessaire d'empêcher l'accès non autorisé en le sécurisant au moyen d'un placard ou boîtier d'un niveau de sûreté approuvé. Ce dernier doit être fermé à clé et protégé par le SDI.

9.17 Accès aux détecteurs

Il importe de veiller à ce que des personnes non autorisées ne puissent avoir accès aux détecteurs de SDI. Les alarmes d'immixtion doivent être surveillées 24 heures sur 24 et le bon fonctionnement de tous les détecteurs doit être vérifié à des intervalles réguliers.

9.18 Voyants de bon fonctionnement

Des voyants de bon fonctionnement, habituellement des diodes électroluminescentes rouges montées à l'avant du détecteur, sont destinés à indiquer que le dispositif fonctionne bien. Cette indication risque toutefois d'être erronée et ne doit pas être considérée comme un test du système. La seule façon efficace de tester une installation de SDI consiste à activer un détecteur et de vérifier qu'une alarme a été déclenchée. Un voyant peut aussi révéler à un attaquant l'angle de couverture et la portée du détecteur. Il est donc fortement conseillé de masquer ou déconnecter les voyants dans toutes les installations de haute sûreté.

9.19 Tests

Les SDI installés dans les sites de haute sûreté doivent être testés au moins une fois par jour. Si cela n'est pas possible, ils doivent être testés régulièrement à des intervalles prescrits dans la réglementation locale de sûreté. Les tests doivent inclure une vérification du fonctionnement et de la sensibilité de chaque détecteur et de la bonne réception du signal d'alarme au tableau de commande. Tout défaut de fonctionnement doit être signalé immédiatement pour que le service de gestion de la sûreté y remédie.

9.20 Registre automatique

Si le système est doté d'un système de registre automatique d'événements, celui-ci doit être examiné régulièrement par le service de gestion de la sûreté et comparé aux comptes rendus donnés par les gardes. Il importe que le personnel soit bien entraîné à reconnaître le déroulement d'une suite suspecte d'événements, et qu'il ait l'autorité nécessaire pour investiguer les incidents, par exemple coupure d'alimentation électrique. S'il y a une imprimante sur papier, les feuilles imprimées doivent être conservées pendant au moins trois ans, afin de permettre l'analyse rétrospective et l'investigation.

9.21 Alarmes

Lorsqu'il y a une alarme dont la cause n'est pas immédiatement apparente, il peut être tentant de la négliger sans investigation, comme ayant probablement été causée par un facteur environnemental ou une défaillance technique dans le système. On risque alors de ne pas avoir connaissance d'une attaque délibérée sur le système. En cas d'attaque sur un SDI, il est possible que le seul avertissement soit donné par un détecteur avant qu'il soit contourné. Par conséquent, chaque alarme doit être minutieusement investiguée par le personnel de sûreté, au besoin avec le concours d'un technicien de SDI, et il faut faire tout ce qui est possible pour déterminer la cause. Il convient aussi d'envisager la possibilité qu'une séquence d'alarmes non expliquées sur une assez longue période de temps soit une indication d'interventions préparatoires à une attaque ou de tentatives, par un attaquant, de saper la crédibilité du système.

9.22 Rénovation de bâtiments

Il peut arriver que des bâtiments ou des groupes de bureaux soient rénovés après l'installation d'un SDI. Le réaménagement de cloisons et le déplacement d'équipements protégés risquent de réduire le niveau de protection initialement procuré par le SDI. Il convient donc, si c'est nécessaire, d'effectuer une nouvelle étude et d'adapter l'installation du SDI aux nouveaux aménagements. S'il y a des travaux de reconstruction, il faut veiller à empêcher les travailleurs du bâtiment d'avoir accès sans surveillance à des composants du SDI, et une vérification minutieuse du système doit être effectuée aussitôt après l'achèvement des travaux. S'il s'agit de grandes modifications, il peut être nécessaire de mettre le SDI hors service jusqu'à ce que les travaux soient achevés.

10- Sûreté matérielle des bâtiments

Les indications ci-après portent sur les aspects à prendre en compte à des fins de planification générale.

10.1 Mesures de protection

10.1.1 Tout bâtiment faisant partie intégrante du périmètre du côté piste ou d'une zone de sûreté à accès réglementé doit avoir aussi peu de points de sortie et d'entrée que le permettent les fonctions du bâtiment et les considérations de sécurité.

10.1.2 Il doit être procédé à une analyse du bâtiment en vue de sécuriser le maximum de points d'accès, notamment : toutes les portes et autres entrées (y compris portes d'intercommunication avec d'autres parties du bâtiment ayant d'autres occupants), fenêtres au rez-de-chaussée, autres fenêtres accessibles, zones extérieures en contrebas, goulottes à combustible, couvercles de trous d'homme, quais de chargement, installations électriques, conduits d'écoulement et toitures.

10.1.3 Différentes dispositions matérielles de sûreté, par exemple barres de fenêtres, grilles, volets, portes renforcées, peuvent servir à protéger les ouvertures accessibles dans l'enveloppe d'un bâtiment. Leur efficacité peut être rehaussée par un système de détection d'intrusion, la télévision en circuit fermé ou une surveillance par des gardes. Dans le choix entre les nombreuses options possibles, les aspects ci-après doivent être pris en compte :

- les barrières protectrices ont pour objet principal de dissuader les intrus. Elles doivent aussi mettre en difficulté et retarder les intrus qui ne sont pas dissuadés, en les obligeant à utiliser des outils et à faire du bruit. En fin de compte, aucune barrière n'est jamais impénétrable pour ceux qui sont très motivés et ont des outils appropriés;
- s'il n'y a pas de problème de ventilation, une barrière en matériau massif est préférable à une barrière à claire voie. Autrement dit, une porte en matériau massif procure une meilleure sûreté qu'une porte en grille;
- une barrière fixe est préférable à une barrière mobile (coulissante ou articulée);
- une barrière placée à l'intérieur d'un couloir ou en retrait d'une embrasure de porte est moins facile à forcer avec des outils tels que béliers, masses ou leviers.

10.2 Portes extérieures

10.2.1 Les portes extérieures doivent être en bois massif, à âme en sandwich ou en contreplaqué très solide, et avoir une épaisseur d'au moins 44 mm. Idéalement, ces portes doivent s'ouvrir vers l'extérieur, de sorte qu'il soit plus difficile de les forcer. Une attention spéciale doit être donnée aux charnières, qui doivent normalement être complétées par des protecteurs de charnières. Les portes doivent être bien ajustées et munies de serrures adéquates. Des barres fixées en travers du côté intérieur de la porte donnent un degré supplémentaire de protection. Si c'est nécessaire, les impostes vitrées doivent être munies de barres ou de grilles et les ouvertures pour le courrier doivent être fermées hermétiquement ou protégées d'une autre façon.

10.2.2 Les portes extérieures qui ne sont jamais utilisées et qui ne sont pas des issues de secours doivent être obturées en maçonnerie ou sécurisées en permanence par une tôle d'acier vissée sur l'intérieur du chambranle.

10.2.3 Les trous de serrure des portes extérieures rarement utilisées doivent être obturés sur le côté extérieur. De forts verrous cadenassés ou de fortes barres assujetties sur l'intérieur peuvent rehausser la protection.

10.2.4 Les portes à panneaux peuvent être renforcées par des tôles d'acier, de préférence repliées et fixées sur la tranche des portes.

10.2.5 Les portes vitrées ou semi-vitrées peuvent être renforcées jusqu'à un certain point par un treillis métallique. Ou encore, des grilles repliables ou des volets à enrouleur peuvent être installés derrière les portes.

10.2.6 Les portes à deux battants doivent être sécurisées au moyen de verrous (en haut et en bas) sur le battant qui se ferme en premier et par une serrure à pêne dormant, de préférence complétée par un loquet à enclenchement sur l'autre battant. Les portes à deux battants qui ne donnent pas sur l'extérieur peuvent aussi être renforcées par des barres en travers sur l'intérieur et le battant qui se ferme en deuxième lieu peut être sécurisé par des loquets.

10.3 Portes entre secteurs communicants

Les portes qui donnent accès à d'autres parties du bâtiment ayant d'autres occupants doivent en général procurer un degré de sûreté similaire à celui des portes extérieures. Il est en général conseillé de protéger ces portes au moyen d'alarmes d'intrusion et de systèmes de contrôle d'accès.

10.4 Portes intérieures

91. Il peut être nécessaire de fermer à clé les portes donnant accès au sous-sol ou au rez-de-chaussée. Les clés des serrures de ces portes doivent être tenues sous bonne garde mais les personnes autorisées doivent y avoir aisément accès.

10.5 Portes d'issues de secours

Lorsqu'il s'agit de sécuriser les issues de secours, il y a souvent opposition entre les exigences de la sûreté et celles de la sécurité. La plupart des moyens de fermeture d'issues de secours, y compris celles qui s'ouvrent si l'on pousse une barre, ne procurent pas une sûreté suffisante et les issues de secours doivent normalement être dotées de dispositifs de détection d'intrusion.

10.6 Chambranles de portes

La sûreté d'une porte dépend en partie de la solidité de son chambranle et de sa fixation dans l'embrasure. Dans certains cas, il peut aussi être nécessaire de renforcer le seuil en remplaçant le bois par du béton. Si le chambranle n'est fixé dans la maçonnerie que par des clous, on peut rehausser la sûreté par des fixations en acier sur ses deux côtés, solidement jointes à la maçonnerie; ou encore des vis ou boulons de fixation par écartement peuvent être utilisés, à condition qu'ils aillent assez profondément dans la maçonnerie.

10.7 Verrous de portes

Des verrous doivent normalement être utilisés sur les portes, en conjonction avec des serrures de sûreté, et par paires en haut et en bas de la porte. Dans l'installation des verrous, il convient de veiller à ce qu'ils ne puissent pas être ouverts de l'extérieur de la porte et que la fixation et la tige mobile soient adéquates. Si la tige du verrou s'insère dans le sol ou le plancher, elle doit s'engager assez profondément et il faut veiller à ce que le trou ne soit pas obturé. Pour sécuriser les portes de façon plus permanente, les verrous doivent être munis de cadenas de sûreté.

10.8 Charnières et protecteurs de charnières

Les axes de charnières ne doivent pas pouvoir être enlevés de l'extérieur de la porte, et les vis de fixation de charnières ne doivent pas être accessibles, ni d'un côté ni de l'autre, lorsque la porte est fermée. Les charnières peuvent être renforcées par l'installation de protecteurs à enclenchement

près de chaque charnière. La moitie mâle de chaque protecteur de charnière doit être fixée sur la tranche de la porte et la moitié femelle sur le chambranle. Les deux moitiés s'enclenchent lorsque la porte est fermée, ce qui empêche de séparer la porte du chambranle par l'action d'un levier sur le côté où sont les charnières, même si ces dernières sont enlevées.

10.9 Grilles et volets

10.9.1 Des grilles repliables, des grilles à enrouleur ou des volets à enrouleur peuvent être utilisés dans des embrasures de portes, des passages ou d'autres ouvertures. Ils peuvent aussi servir de deuxième ligne de défense à l'arrière de portes extérieures, particulièrement s'il y a une menace d'attaque par la force. Les grilles sont toutefois vulnérables dans la mesure où elles permettent d'accéder aux deux côtés de la serrure, et cette faiblesse potentielle doit être prise en compte.

10.9.2 Les encadrements de grilles ou volets doivent être solidement fixés à la structure du bâtiment, et de préférence être inaccessibles de l'extérieur du bâtiment.

10.10 Judas à optique de grand-angle

98. S'il est nécessaire que des gardes puissent identifier des visiteurs sans ouvrir la porte, ou regarder à l'intérieur d'une salle sans y entrer, des judas à optique de grand-angle doivent être installés, au lieu d'ouvertures avec vitrage de sûreté. L'installation d'un miroir convexe en conjonction avec un judas permet d'apercevoir des endroits qui autrement seraient cachés. Il doit y avoir un éclairage suffisant pour illuminer la zone située de l'autre côté de la porte, et le garde doit avoir accès au commutateur.

10.11 Fenêtres

10.11.1 Toutes les fenêtres accessibles mais non essentielles doivent être obturées par de la maçonnerie ou sécurisées d'une autre façon. Toutes les fenêtres de sous-sol, de rez-de-chaussée et autres qui sont aisément accessibles doivent être solidement protégées. Les lucarnes sont parfois facilement accessibles depuis la toiture. Les loquets de fenêtres doivent être examinés et ceux qui sont défectueux doivent être remplacés. Une protection par alarme d'intrusion doit être envisagée. La responsabilité de sécuriser les fenêtres à la fin de la journée de travail doit être clairement établie dans les instructions de sûreté de l'établissement.

10.11.2 Certaines fenêtres, par exemple celles qui donnent sur la zone de sûreté à accès réglementé, ont besoin d'une protection plus positive au moyen de serrures. Les fenêtres les plus vulnérables sont habituellement celles du sous-sol ou du rez-de-chaussée, celles qui sont à proximité d'issues d'incendie ou de vérandas, ou celles qui sont immédiatement au-dessous de la toiture.

10.11.3 Lorsqu'il est nécessaire de sécuriser une fenêtre plus efficacement que par une serrure ou un loquet, l'utilisation de barres, de grilles ou de volets doit être envisagée. L'installation de détecteurs d'intrusion doit aussi être envisagée.

10.12 Vitrages

On trouve dans le commerce de nombreux types de vitrages ayant des appellations trompeuses, par exemple «vitres blindées», donnant à penser qu'ils peuvent être utilisés indépendamment comme barrières de sûreté. Il y en a très peu qui soient effectivement utilisables comme vitrages de sûreté et, si la sûreté est une considération primordiale, des avis spécialisés doivent être demandés aux services de sûreté de l'État.

10.13 Doubles vitrages

10.13.1 Les doubles vitrages peuvent procurer une excellente protection contre des attaques inopinées et un certain degré de protection contre des attaques par la force. Ils ne gênent pas la vue, attirent moins d'attention sur un secteur sensible et sont esthétiquement plus acceptables que des barres ou des grilles. Les doubles vitrages peuvent être dotés d'alarmes et présentent l'avantage supplémentaire d'une bonne isolation thermique et acoustique.

10.11.2. Dans le cas de tous les vitrages, il y a lieu de veiller à ce que le mastic ou la matière utilisée pour assujettir la vitre sur l'encadrement de la fenêtre ne soit pas accessible de l'extérieur, ce qui rendrait la fenêtre vulnérable à une attaque inopinée.

10.14 Toitures

Il y a lieu d'examiner les toitures pour déterminer s'il est possible d'y accéder à partir de bâtiments contigus, de bâtiments voisins, d'arbres, d'issues d'incendie, d'équipements de nettoyage de fenêtres, etc. Si c'est le cas, il peut être nécessaire d'ériger des barrières. Si l'accès est nécessaire, par exemple dans le cas d'un trajet d'évacuation en cas d'incendie, des alarmes d'intrusion peuvent être nécessaires. L'accès à un bâtiment est parfois possible via une mansarde ou une cavité de toiture. Des mesures de protection de ces moyens d'accès doivent être incorporées. L'accès à un bâtiment à partir d'une toiture peut dans certains cas être possible via une cheminée. Si c'est le cas, des mesures adéquates doivent être prises pour bloquer l'accès, par exemple grâce à l'installation d'une grille.

10.15 Trappes de toiture

Si le toit est accessible à partir de bâtiments voisins ou à partir du sol, les trappes d'accès installées sur le toit doivent être sécurisées de la même façon que les portes extérieures. Si les trappes sont sur un trajet d'évacuation en cas d'urgence à l'usage des occupants d'un bâtiment voisin, des dispositifs de sortie adéquats et des dispositifs d'alarme d'intrusion doivent être installés sur ces trappes.

10.16 Fenêtres de toit, lucarnes et oeils-de-boeuf

Il est possible de sécuriser les fenêtres de toit, lucarnes et oeils-de-boeuf au moyen de serrures ou de verrous. Si une meilleure protection est nécessaire, une des mesures suivantes peut être retenue :

- remplacer le vitrage par un vitrage de sûreté;
- installer des barres ou des grilles;
- visser les encadrements en place et couvrir le vitrage d'un treillis en acier fixé solidement sur l'intérieur de l'encadrement;
- installer des dispositifs de détection d'intrusion.

10.17 Descentes de gouttières

L'accès aux étages supérieurs d'un bâtiment, à partir du sol ou du toit, est parfois possible par les descentes de gouttières. On peut rendre l'accès plus difficile en encastrant les conduits de descente ou en les traitant au moyen d'une peinture antiescalade (qui conserve en permanence la consistance d'une graisse peu épaisse). La peinture doit être appliquée seulement à une hauteur supérieure à 2,5 m (8 ft) environ pour éviter le contact accidentel par des passants. La peinture antiescalade peut entraîner des incidences judiciaires dans les zones auxquelles le public a accès, et un avis juridique devrait toujours être obtenu.

10.18 Zones en contrebas

Beaucoup de bâtiments ont des zones extérieures en contrebas, au niveau du sous-sol, qui sont accessibles à partir de la rue. Elles peuvent permettre à des personnes de se frayer un accès par les fenêtres de sous-sol et elles sont un endroit commode pour déposer des engins explosifs ou incendiaires. Il peut être nécessaire de les protéger au moyen de grilles ou de treillis métalliques fixés par en dessous, pourvu qu'ils ne facilitent pas l'accès au bâtiment. Les orifices dans les zones en contrebas ou au niveau de la rue sont aussi vulnérables et il peut être nécessaire d'y installer des grilles métalliques du côté de l'intérieur. L'accès par des tunnels de service ou des goulottes à combustible doit être obstrué au moyen de cadenas ou de barres transversales cadenassées installées du côté de l'intérieur. Il peut aussi être nécessaire d'installer des détecteurs d'intrusion.

10.19 Places de stationnement/quais de chargement

Il peut être difficile et coûteux de protéger des places de stationnement ou des quais de chargement sous un bâtiment. Hors des heures de service, ils doivent être fermés par des volets à coulisse ou à enrouleur, installés du côté de l'intérieur. Durant les heures de services, les quais doivent être surveillés par un gardien ou, si la menace est élevée, fermés au moyen de volets commandés électroniquement et ne s'ouvrant que lorsqu'un véhicule qui se présente a été identifié et, au besoin, fouillé.

10.20 Installations d'adduction

10.20.1 Les installations d'adduction de gaz, d'électricité et d'eau dans des bâtiments peuvent être des points d'accès vulnérables. Autant que possible, les câbles et conduits doivent pénétrer dans le bâtiment au-dessous de la surface du sol. Les compteurs doivent si possible être placés de façon à être accessibles sans qu'il soit nécessaire d'entrer dans des zones de sûreté à accès réglementé.

10.20.2 Si la climatisation est indispensable pour le fonctionnement d'équipements (par exemple ordinateurs), l'alimentation des climatiseurs en électricité et en eau doit être bien protégée. S'il y a une menace de sabotage, des mesures additionnelles de sûreté peuvent être nécessaires et des avis doivent être demandés aux services de sûreté compétents de l'État.

10.21 Vitrages d'aérogare

Un engin explosif mis à feu à l'intérieur ou au voisinage d'une aérogare produit d'importants dommages, particulièrement sur les vitrages, et entraîne ainsi des blessures. Dans certaines aérogares il y a assez peu de vitrages sur l'extérieur du bâtiment, mais dans la plupart des cas des baies vitrées sont largement utilisées, de sorte qu'il importe de comprendre les mécanismes de rupture des différents types de verre. Il n'est guère pratique, dans la plupart des cas, d'entreprendre la réfection des vitrages existants, mais il y a différentes mesures qui peuvent servir à réduire les risques de blessures par projections de verre, par exemple l'application sur le verre d'une pellicule antiéclats en polyester transparent et/ou l'installation de rideaux ou filets protecteurs.

10.22 Mécanismes de rupture de types de verre

10.22.1 Les mécanismes de rupture de types de verre sont les suivants :

- le verre *flotté* ou *recuit ordinaire* est cassant et se rompt facilement à de faibles pressions de souffle, s'éparpillant en fragments coupants et dangereux qui, projetés par le souffle de l'explosion, peuvent causer de graves blessures;

- le verre *trempé* est plus résistant et donne un niveau de protection à peu près double de celui du verre ordinaire. Des points de tension y sont incorporés, de sorte que lorsqu'il se brise il explose en de nombreux petits fragments cuboïdes qui sont moins dangereux que les fragments coupants du verre ordinaire;
- le verre *feuilleté* est constitué (en général) de deux feuilles de verre entre lesquelles il y a une couche adhésive de polyvinylbutyle (pvb). Le verre cède à une pression analogue à celle du verre ordinaire, mais la couche intermédiaire de pvb forme une membrane qui peut résister à des pressions beaucoup plus grandes, à condition que le verre feuilleté soit bien fixé dans le cadre. Le niveau de protection procuré par du verre feuilleté de 7,5 mm d'épaisseur est de l'ordre de trois fois celui du verre recuit ordinaire.

10.22.2 Si l'on compare le verre trempé et le verre feuilleté, les incidences des mécanismes de rupture sont les suivantes :

a) le verre trempé résiste nettement mieux aux chocs accidentels localisés et aux impacts de chariots, etc., sans se fendre;
b) pour une charge explosive donnée, le verre feuilleté se fend et doit être remplacé sur une surface beaucoup plus grande;
c) en cas d'explosion assez lointaine pour que le verre trempé ne soit pas endommagé, le verre feuilleté se fend mais ne se brise pas;
d) aux distances intermédiaires, le verre trempé se désintègre, laissant passer le souffle qui emporte des morceaux de verre cuboïdes, alors que le verre feuilleté fléchi sans se briser et procure une protection complète;
e) la rigidité de l'encadrement des vitres est cruciale pour ce qui est du point de rupture du verre trempé;
f) la résistance ultime (même en cas de déflexion) de l'encadrement et la résistance et la profondeur de la rainure sont cruciales pour ce qui est du point de rupture du verre feuilleté. Cela est plus critique dans le cas d'une forte charge qui peut projeter une vitre toute entière si cette vitre peut être délogée de sa rainure avant la rupture de la feuille intermédiaire de pvb.

10.22.3 En fin de compte, les différences se ramènent à ceci :

a) pour toute «menace de charge» donnée, il y a toujours une plage de distances d'explosion auxquelles le verre feuilleté offre plus de sécurité que le verre trempé;
b) il s'agit de déterminer si cette plage de distances offre des avantages théoriques de sécurité qui l'emportent sur d'autres considérations.

10.22.4 Dans cette détermination, il faut prendre en compte ce qui suit :

a) la grandeur précise de la plage est difficile à déterminer à cause de l'incertitude au sujet de l'efficacité de l'encadrement et de la rainure, ainsi qu'au sujet des extrapolations des essais de verres;
b) il peut y avoir des incertitudes sur l'ampleur réelle de la menace et son emplacement;
c) à proximité et au-dessous de l'extrémité rapprochée de la plage :
    1) les fragments de verre trempé approchent des vitesses meurtrières;
    2) on court le risque que des vitres feuilletées soient projetées «en masse» par des charges plus fortes.

10.22.5 Les verres de tous types cèdent si une bombe contenant 5 kg d'explosif brisant explose à une distance allant jusqu'à 4 m environ. Des blessures mortelles peuvent évidemment être dues aux effets directs d'une explosion à cette distance.

10.22.6 À une distance allant jusqu'à 12 m environ, une vitre intérieure de verre flotté peut rebondir dans le hall, infligeant des blessures de lacération à des personnes qui auraient autrement échappé à des blessures directes autres que la rupture du tympan. Les personnes présentes de l'autre côté du verre flotté subiraient des blessures analogues. Le verre flotté doit donc être évité dans l'une et l'autre de ces situations.

10.22.7 Une bombe de 5 kg placée dans une valise ne provoque pas la rupture :

a) d'un vitrage double en verre feuilleté à une distance d'environ 5 m,
b) d'un vitrage double en verre trempé à une distance d'environ 8,5 m, (en supposant dans les deux cas un encadrement rigide).

10.22.8 Le verre trempé feuilleté combine les avantages du verre trempé et ceux du verre recuit feuilleté. On ne dispose pas de résultats d'essais de résistance aux explosions, mais on peut déduire les propriétés suivantes :

a) il se fend à peu près aux mêmes pressions que le verre trempé de la même épaisseur totale, c'est-à-dire à des pressions plus fortes que le verre recuit ordinaire ou le verre recuit feuilleté;
b) entre la première fente et la rupture finale, il se comporte probablement de la même façon que le verre recuit feuilleté.

10.22.9 Comme dans le cas du verre trempé, le rayon des dommages (à partir d'une charge) du verre trempé feuilleté est inférieur à celui du verre recuit feuilleté, mais aux distances auxquelles le verre trempé se désintègre, il résiste à la rupture totale aussi bien que le verre recuit feuilleté. Il est possible que le verre trempé feuilleté présente deux autres avantages :

a) comme dans le cas de tout matériau en sandwich, il est théoriquement moins résistant qu'une feuille simple de verre trempé de la même épaisseur totale, mais il est probablement plus flexible. Il peut ainsi résister à des pressions plus élevées (c'est-à-dire des distances plus faibles) jusqu'à la fente initiale, particulièrement dans les cas où la défaillance est régie par la flexion de l'encadrement;
b) sous la forme de vitrage double, sa résistance jusqu'à la fente initiale peut lui permettre de réfléchir les premières pressions de l'explosion, ce qui augmente la résistance de la vitre intérieure, tant dans le cas de la fente initiale que dans le cas de la rupture finale. L'avantage est proportionnellement moindre avec de plus fortes charges, et aussi dans les cas où la défaillance est régie par la résistance de l'encadrement et le point où la vitre est délogée par le souffle.

10.22.10 Il est indispensable de tenir compte des limitations structurales de l'encadrement. Il faut calculer le risque de rupture des meneaux ainsi que la limite de défaillance en flexion des traverses et des meneaux. La résistance du vitrage choisi dépend aussi de la résistance de l'encadrement et de la profondeur des rainures.

10.23 Protection contre les éclats de verre

Il y a deux moyens principaux de traiter les vitrages pour réduire le risque de blessures causées par des éclats de verre :

- appliquer sur le verre une pellicule transparente de polyester antiéclats;
- installer des rideaux ou filets de protection.

10.24 Pellicule transparente de polyester antiéclats

10.24.1 Une pellicule en polyester de qualité appropriée, d'une épaisseur d'au moins 100 µ (0,004"), avec une surface adhésive par simple pression, s'applique sur l'intérieur des baies vitrées. Dans le cas d'une explosion, le verre reste collé à la pellicule et il n'y a pas de projections d'éclats dangereux. Pour les baies de plus de 3 m², ou si le verre a une épaisseur de plus de 6 mm, il convient d'utiliser une pellicule de 175 µ. Cette dernière qualité de pellicule doit aussi être utilisée si l'on n'a pas installé de rideaux ou filets de protection contre le souffle d'explosions. L'utilisation d'une pellicule de 300 µ doit être envisagée pour les baies de plus de 10 m² et pour les fenêtres de plus de 3 m² au rez-de-chaussée, s'il n'y a pas de rideaux ou filets de protection contre le souffle d'explosions.

10.24.2 Sur les fenêtres neuves ou sur les surfaces à revitrer, les nouvelles vitres doivent de préférence être traitées avant d'être fixées dans le cadre, la pellicule recouvrant alors complètement le verre jusqu'à sa bordure extérieure. La décision d'appliquer une pellicule avant l'installation doit être appréciée dans le contexte du contrat et du site si d'autres travaux, rénovations, poussière, etc., risquent de produire des éraflures inacceptables.

10.24.3 Sur les fenêtres existantes, la pellicule doit être appliquée aussi près que possible du mastic, avec un intervalle de moins de 3 mm. Toutefois, il est parfois nécessaire d'admettre des intervalles allant jusqu'à 5 mm le long des bordures de mastic particulièrement irrégulières ou vieillies.

10.24.4 La pellicule ne doit être appliquée que sur des surfaces propres et exemptes de poussière. On ne peut l'appliquer sur le côté de la surface en relief du verre dépoli, orné ou rainuré; on peut cependant envisager d'intervertir les deux faces de la vitre.

10.24.5 Si la pellicule n'est pas assez large pour recouvrir la vitre en une seule pièce, on peut coller deux pellicules en juxtaposition.

10.24.6 La bonne application de la pellicule antiéclats aux fenêtres à double vitrage dépend du genre de fenêtre dont il s'agit.

10.24.7 Si la fenêtre comprend deux châssis distincts et si, en utilisation normale, le châssis intérieur peut s'ouvrir indépendamment de l'autre, une pellicule doit être appliquée aux deux vitres, sur le côté intérieur du verre. Si le châssis intérieur ne s'ouvre pas indépendamment, ou s'il s'agit d'un double vitrage en unité scellée, il suffit normalement de traiter la vitre intérieure. À noter que la vitre intérieure de certains systèmes de double vitrage n'est pas toujours solidement fixée. Dans ce cas, il convient de la fixer plus solidement.

10.24.8 Il existe un test de résistance au décollement pour contrôler sur place la qualité de l'installation de la pellicule, et pour vérifier périodiquement s'il y a une dégradation de l'adhésif.

10.25 Rideaux de protection contre le souffle d'explosions

10.25.1 Les rideaux de protection contre le souffle doivent être composés d'un tissu de térylène polyester de 90 à 100 deniers, ayant deux fois la largeur et une fois et demie la longueur de la fenêtre. L'ourlet du bas doit comprendre des poids souples, à raison de 400 g par mètre. La longueur excédentaire doit servir à former des plis en accordéon dans une auge à la partie inférieure de la fenêtre. À la suite d'une explosion extérieure qui brise la fenêtre, le tissu des rideaux forme un écran en forme de « spinnaker » et arrête les projections de verre qui, à cause de la pellicule antiéclats, sont formées de morceaux plus grands se déplaçant à une vitesse plus faible que dans le

cas d'un verre non traité. Dans des conditions un peu plus extrêmes, les rideaux se détachent des fixations du haut et en même temps s'incurvent sur les côtés et à la partie inférieure, ce qui enveloppe le verre et le fait tomber au sol près de la fenêtre. Dans des conditions de souffle encore plus extrêmes, en plus d'arrêter les fragments de verre qui sont projetés, les rideaux s'enveloppent encore autour des morceaux de verre petits et moyens, ce qui les fait tomber plus près de la fenêtre et avec moins de danger qu'avec le même verre et la même pellicule mais sans rideaux.

10.25.2 Les rideaux doivent normalement être installés à une distance de 5 à 10 cm du verre; s'ils sont plus éloignés, des éclats de verre peuvent tournoyer et couper les rideaux, et le souffle de l'explosion peut faire voler les rideaux de sorte que le verre ne sera pas bien capté. Néanmoins, comme le verre recouvert d'une pellicule perd sa vitesse assez rapidement après les premières dizaines de centimètres, on peut fixer les rideaux à une plus grande distance si les circonstances l'exigent.

10.25.3 Les rideaux ne doivent pas être utilisés sans pellicule antiéclats sur les vitres. Leur installation est particulièrement importante lorsqu'il s'agit de protéger des fenêtres à croisillons et à petites vitres.

REPUBLIQUE DU CAMEROUN
REPUBLIC OF CAMEROON
Paix-Travail-Patrie
Peace-Work-Fatherland
Le Directeur Général
CAMEROON CIVIL AVIATION AUTHORITY
AUTORITE AERONAUTIQUE

Le Directeur Général,

SAMA JUMA Ignatius