SPÉCIFICATIONS DU SYSTÈME INTÉGRÉ D'ALARME ANTI-EFFRACTION et DE CONTRÔLE DE L'ACCÈS

Agriculture et Agroalimentaire Canada

107 Science Place
Saskatoon (Sask.)
S7N 0X2

Contenu

1 Aperçu fonctionnel

1.1 Le système doit intégrer des fonctions complètes de contrôle d'accès et d'alarme anti-intrusion, et doit permettre de configurer plusieurs sites à partir d'un ou de plusieurs des sites connectés.

1.2 Le système doit permettre de contrôler l'accès par des portes désignées munies d'un contrôle électrique de l'état de la porte et de lecteurs de contrôle d'accès à jeton ou biométriques. Le système vérifie la validité des droits d'accès associés à un jeton d'accès ou à un identificateur biométrique présenté selon le jeton, l'identificateur, la zone d'accès, le temps d'accès et toute autre fonction de gestion de l'accès décrite dans les présentes, tels que stockés dans des contrôleurs intelligents sur le terrain, qui accordent ou refusent l'accès en fonction des droits d'accès établis. Ces droits d'accès doivent pouvoir être configurés de plusieurs façons, afin de permettre la souplesse décrite ailleurs dans les présentes.

1.3 Le système doit prévoir le contrôle d'accès dans les ascenseurs, afin de permettre l'accès à n'importe quel ensemble d'étages pendant des périodes définies. La communication avec les systèmes d'ascenseur doit se faire par une interface de bas niveau (relais), ou de haut niveau (données).

1.4 Le système doit surveiller l'état des entrées. Il doit pouvoir être programmé de façon à appliquer diverses conditions à la surveillance de ces entrées et indiquer l'état de ces entrées conformément à la programmation faite.

1.5 Le système doit intégrer un système d'alarme anti-intrusion pleinement fonctionnel, y compris des délais d'entrée et de sortie si des capteurs de détection d'intrusion sont utilisés. Le système doit intégrer entièrement ses fonctions d'alarme d'intrusion à ses fonctions de contrôle d'accès. Il doit être possible d'activer (sécuriser) ou de désactiver (ne pas sécuriser) des zones à partir de n'importe quel lecteur de contrôle d'accès connexe à une zone, d'un lecteur de contrôle d'accès muni d'un clavier, d'un module d'activation à distance ou, au besoin, de postes de contrôle centraux établis.

1.6 Le système doit intégrer un logiciel de conception et de production de cartes d'identité avec photo.

1.7 Le système doit prendre en charge les communications OPC (alertes, événements et accès aux données) à l'aide des interfaces COM et DCOM de Microsoft, afin d'intégrer les données d'événements à d'autres systèmes tiers d'automatisation et de gestion prenant en charge OPC.

1.8 Le système doit permettre l'échange de données en format XML avec d'autres applications, aux fins de changement d'horaire et de changement aux données des cartes.

1.9 Toute communication entre les éléments du système doit se faire par réseau local ou étendu, existant ou nouvellement installé. Les soumissionnaires doivent se familiariser avec les exigences précises du projet.

1.10 Les contrôleurs intelligents sur place (CIP) doivent se brancher au système par câbles prenant en charge les protocoles Ethernet et TCP/IP, et la prise réseau doit se trouver sur le CIP. Les adaptateurs d'interface (entre Ethernet et RS-485 ou RS-232, par exemple) ne sont pas acceptables.

1.11 Pour connecter à distance les CIP n'étant pas connectés en permanence au réseau, on peut utiliser un service RTPC à l'aide de protocoles TCP/IP.

(a) Il faut connecter au serveur les CIP distants par accès commuté à un fournisseur d'accès Internet (FAI) par protocole TCP/IP chiffré et pare-feu approuvé pour la connexion à l'environnement informatique existant, ou par accès commuté directement au serveur, par connexion d'accès à distance.

1.12 Toute mise à jour logicielle des CIP doit pouvoir se faire par le réseau.

1.13 Toutes les communications réseau entre les divers CIP et entre le serveur et les CIP doivent être chiffrées par clés de session symétriques et un algorithme de chiffrement standard de l'industrie (au minimum, AES 128 bits). Il faut réinitialiser régulièrement les clés de session, et au moins toutes les 24 heures.

1.14 Il faut authentifier les communications à l'aide de clés RSA de 1024 bits.

1.15 Le système doit, selon sa configuration, signaler tous les événements aux opérateurs, et doit tenir un fichier journal de tous les événements, alertes et mesures prises par les opérateurs.

1.16 Le système doit permettre à l'opérateur d'extraire des données du journal des événements sur la configuration du système, et de présenter ces données sous forme de rapports imprimés, d'affichages ou de les sauvegarder dans des fichiers ASCII.

1.17 Le système doit présenter une interface Windows : plans de site et icônes interactives qui indiquent l'emplacement du matériel de contrôle d'accès et de surveillance des alarmes et son état en temps réel.

1.18 Le système doit fournir des rapports d'évacuation d'urgence.

1.19 Le système doit être conçu et fabriqué par une entreprise réputée certifiée ISO 9001:2000 (procédures d'assurance qualité).

1.20 Tout l'équipement fourni doit respecter les normes suivantes :

(a) FCC, Partie 15

(b) CE BS EN 50130-4, compatibilité électronique des systèmes d'alarme (immunité)

(c) CE BS EN 55022 (émissions radioélectriques)

(d) UL 294, contrôle d'accès

(e) UL 1076, systèmes anti-effraction

(f) CSA C22.2 no 205

(g) ULC-ORD-C1076

1.21 Les appareils de chiffrement et de lecture doivent également respecter les normes suivantes :

(a) CE ETS 300 683 Appareils de courte portée

(b) C-Tick AS/NZS 4251 Norme générale sur les émissions

(c) C-Tick RFS29

1.22 Le logiciel système doit être programmé dans un langage en vente libre entièrement structuré et validé, qui intègre un environnement de développement strictement contrôlé.

1.23 L'interface de gestion opérationnelle de la sécurité du site doit avoir été développée à l'aide des outils de développement Microsoft .NET et Windows Presentation Foundation (WPF).

1.24 Le logiciel système doit intégrer des fonctions complètes de sauvegarde et d'archivage.

1.25 Le système intégrer un système de cloisonnement approprié aux bâtiments à locataires multiples. Les opérateurs ne doivent pouvoir accéder qu'aux parties du système qui relèvent de leurs droits d'accès de division et d'opérateur.

1.26 Les CIP doivent prendre en charge les communications entre pairs pour les communications d'entrée/sortie entre CIP. Les systèmes qui ont besoin d'un serveur principal pour les communications entre panneaux sont inacceptables.

2 Serveurs du système et matériel des postes de travail

2.1 Les serveurs et l'équipement des postes de travail seront fournis par le Ministère, selon les exigences suivantes.

2.2 Le matériel du serveur doit prendre en charge un système d'exploitation 64 bits.

2.3 Le système d'exploitation utilisé par le serveur du système doit être l'un des suivants :

(a) Microsoft Windows 2008 Server;

(b) Microsoft Windows 2008 Server R2 (64 bits exclusivement);

(c) Microsoft Windows 7 Professional ou Ultimate;

2.4 Les postes de travail doivent exécuter Microsoft Windows 7 Professional ou Ultimate.

2.5 La base de données du système doit être mise en place sur un serveur Microsoft SQL Server, c'est-à-dire l'un des systèmes suivants :

(a) Microsoft SQL 2005, 2008, 2008R2 ou 2012 Server;

(b) Microsoft SQL 2005, 2008 ou 2012 Express Edition.

2.6 Les postes de travail doivent prendre en charge plusieurs moniteurs, ce qui permet à l'opérateur de configurer un ou plusieurs moniteurs sur chaque poste de travail.

2.7 Si un poste de travail est configuré pour une résolution inférieure, glisser une vue vers un moniteur à résolution supérieure la redimensionne afin de profiter de la résolution supérieure.

2.8 Le système doit prendre en charge le déploiement manuel à l'aide de supports d'installation.

2.9 Un opérateur doit pouvoir utiliser le système sur un poste de travail uniquement à partir de fichiers stockés sur une clé USB, sans qu'il soit nécessaire d'installer un logiciel sur l'ordinateur.

3 Exigences visant le système

3.1 Le système doit être en exploitation commerciale, dans une configuration semblable ou mieux identique à celle décrite ici, et on doit pouvoir faire une visite sur place. Le soumissionnaire doit joindre à sa soumission une liste des systèmes configurés de façon semblable et les coordonnées des personnes-ressources connexes.

3.2 Le système décrit dans les présentes prendre en charge au minimum :

(a)	Plans graphiques de sites	illimité
(b)	Lecteurs d'accès	illimité
(c)	Ascenseurs	100, jusqu'à 75 étages chacun
(d)	entrées d'alarme entièrement supervisées à 4 états	illimité
(e)	Relais de sortie	illimité
(f)	Zones de contrôle d'accès	illimité
(g)	Horaires par jour	100
(h)	Catégories d'horaires	50
(i)	Jours fériés	30
(j)	Opérateurs	illimité
(k)	Sessions d'opérateurs simultanées	illimité
(l)	Titulaires de carte	illimité
(m)	Catégories (niveaux d'accès) des cartes	15
(n)	Champs de données (personnel) des cartes	64

3.3 Le système doit être d'architecture multiniveaux composé de :

(a) une ou plusieurs installations du logiciel contrôleur, sur des serveurs et des postes de travail;

(b) des contrôleurs intelligents sur place (CIP) qui gèrent le système selon un modèle d'intelligence répartie;

(c) des sous-unités semi-intelligentes (sorties, entrées, lecteurs et autres) qui dépendent des CIP pour fonctionner.

4 Système central de contrôle et de gestion

4.1 Le système doit utiliser le système d'exploitation Microsoft Windows © tel qu'indiqué ci-dessus, et la version utilisée doit bénéficier du soutien technique de Microsoft.

4.2 La base de données du système doit être une version de Microsoft SQL Server figurant à la liste donnée auparavant; elle doit être adaptée à l'envergure du système prévu, et elle doit bénéficier du soutien technique de Microsoft.

4.3 Le système doit respecter la norme OPC en vigueur, afin de prendre en charge les communications OPC (alertes, événements et accès aux données)

4.4 Le système de contrôle central doit être mis en œuvre sur un ordinateur personnel ou un serveur de haute qualité qui intègre les composants et la conception de la présente génération. Il doit être d'un modèle approuvé par Microsoft, et prenant en charge les versions actuelles de Windows. Les caractéristiques techniques de ce serveur, y compris la cadence du processeur et la taille de la mémoire vive et du disque dur, seront choisies par le fournisseur; elles doivent cependant être suffisantes pour satisfaire ou dépasser les exigences du système indiquées.

4.5 Le système doit pouvoir prendre en charge au moins 20 postes de travail simultanément. Les postes de travail exécutant un logiciel d'émulation de terminal ne sont pas recevables.

4.6 Le système doit enregistrer et horodater automatiquement tous les événements du système, notamment les alarmes d'intrusion, les événements de contrôle d'accès, et les actions et activités de l'opérateur.

4.7 Le logiciel de commande doit être facile à utiliser, il doit présenter ses fonctions à l'aide de menus et de fenêtres, et il ne doit exiger qu'une formation minimale pour qu'un opérateur puisse l'utiliser efficacement. Les systèmes devant être configurés par ligne de commande ou scripts saisis au clavier ne sont pas recevables.

4.8 Le système de contrôle central doit pouvoir recevoir simultanément des signaux d'alarme provenant de nombreux emplacements éloignés, sans les ignorer ni les afficher à l'opérateur en retard. Tout opérateur autorisé doit pouvoir accuser réception, visualiser ou traiter une alarme à partir de n'importe quel écran.

4.9 Le système de contrôle central doit être muni d'une horloge en temps réel, qui doit continuer à donner l'heure pendant toute la durée d'une panne d'électricité. Les IFC connectés à Ethernet doivent se synchroniser automatiquement avec le serveur central, sans intervention humaine.

4.10 L'opérateur doit choisir les tâches à traiter par menus. Les opérateurs autorisés doivent pouvoir traiter les alarmes, produire des rapports et modifier les dossiers de la base de données sans que se dégradent les performances du système.

4.11 Voici les exigences opérationnelles minimales requises; le système doit permettre de :

(a) Spécifier les paramètres de contrôle d'accès d'un ou de plusieurs lecteurs de cartes, sans affecter les autres lecteurs de carte.

(b) Spécifier les droits d'accès d'un titulaire de carte ou d'un groupe de titulaires.

(c) Stocker sur chaque titulaire de carte au moins 64 champs de données ne touchant pas le contrôle d'accès. Les noms de ces champs de « données personnelles » peuvent être définis par l'utilisateur.

(d) Autoriser ou interdire un titulaire de carte répertorié, et répercuter ce changement dans tous les lecteurs du système.

(e) Activer un « suivi de carte » sur des titulaires de carte précis, pour déclencher une alarme chaque fois qu'un des titulaires visés utilise sa carte d'accès ou son jeton.

(f) Préprogrammer les congés pour y appliquer des critères d'accès différents de ceux des jours ouvrés. Le système doit prendre en charge au moins 30 jours de congé.

(g) Prendre en charge les variantes régionales visant les congés.

(h) Définir autant de zones d'accès qu'il y a de lecteurs de cartes.

(i) Autoriser ou interdire en temps réel l'accès d'un titulaire de carte à un lecteur ou à un groupe de lecteurs de cartes.

(j) Enregistrer sur le disque dur en temps réel toutes les activités du système et les activités de l'opérateur.

(k) Entrer dans le système les directives de réponse à une alarme afin qu'elles soient présentées à l'opérateur au traitement d'un événement d'alarme.

(l) Permettre à un opérateur d'entrer des messages sur les événements d'alarme.

(m) Outrepasser temporairement les droits d'accès préprogrammés d'un titulaire de carte ou d'un groupe de titulaires de carte.

4.12 Le système de contrôle central doit afficher en une ligne un message d'événement clair et simple pour chaque événement d'activité (alarme ou autre) détecté. Toutes les activités enregistrées doivent être horodatées à la seconde près (hh:mm:ss). Si l'opérateur a les droits d'accès voulus, il doit pouvoir consulter les propriétés de chaque élément de l'événement pour obtenir des détails ultérieurs. Le message d'événement doit indiquer :

i. l'heure de l'événement

ii. l'action

iii. si cette action a réussi ou échoué

iv. en cas d'échec, le motif du refus

(a) Cela comprend sans s'y limiter les éléments suivants :

i. Toutes les lectures de cartes

ii. Toutes les ouvertures et fermetures de porte

iii. Toutes les activités de l'opérateur, y compris la connexion, la déconnexion, les messages de réponse d'alarme et toute modification des fichiers de données du système

iv. Toutes les activations d'alarmes

v. Toutes les pannes des voies de communication.

4.13 Les horaires des divers « types de jours » doivent être configurables.

4.14 Les jours fériés régionaux doivent être configurables afin de tenir compte des variations régionales.

4.15 Le système doit intégrer un fichier d'aide détaillé à l'intention des opérateurs; il doit leur expliquer l'utilisation du système et proposer des tutoriels textuels, audio et vidéo.

4.16 Le système doit permettre la recherche d'éléments répertoriés par le système, selon les critères suivants :

(a) Caractéristiques de l'élément

(b) Éléments connexes

(c) l'heure des événements, y compris l'élément voulu

5 Connectivité multiserveurs

5.1 Le système doit prendre en charge de multiples serveurs installés à plusieurs endroits.

5.2 Le système doit pouvoir afficher les alarmes et les événements détectés par tous les serveurs sur toute combinaison des postes de travail, y compris tous.

5.3 La base de données des titulaires de cartes doit être distribuée automatiquement sur tous les serveurs en tant qu'entité « globale ».

5.4 Les changements aux attributs des cartes des titulaires doivent être distribués au fur et à mesure qu'ils sont apportés (aucun traitement par lots).

5.5 La communication entre les serveurs être en mode pair-à-pair.

5.6 L'environnement multiserveurs doit pouvoir produire à partir d'un serveur des rapports d'évacuation visant chaque site du système, pour un ou plusieurs serveurs distants.

5.7 Les vues et les droits d'accès des opérateurs doivent appliquer les mêmes règles, que ce soit sur plusieurs serveurs ou un seul.

5.8 Les éléments du système de sécurité configurés sur des serveurs déjà en place doivent être reconnus automatiquement par tous les serveurs ajoutés au groupe de serveurs. De même, les éléments système configurés sur tout serveur ajouté doivent être reconnus automatiquement par le groupe de serveurs en place.

5.9 Le recours à des modules d'interface logiciels écrits sur mesure pour connecter les serveurs en configuration multiserveurs n'est pas acceptable.

5.10 La saisie manuelle ou par script des données des serveurs existants dans tout nouveau serveur ajouté au groupe multiserveurs n'est pas acceptable.

5.11 Les serveurs doivent synchroniser leurs données automatiquement en temps réel, sans intervention ou initialisation humaine.

5.12 En cas de perte de communication entre deux ou plusieurs serveurs, les divers serveurs doivent continuent à fonctionner indépendamment les uns des autres, puis à la reconnexion resynchroniser automatiquement toute modification apportée hors ligne.

5.13 Si un conflit découle de la création d'éléments identiques dans plus d'un serveur hors ligne, il faut à la reconnexion signaler ce conflit par une alarme.

5.14 Si un enregistrement existant est modifié dans plus d'un serveur hors ligne, les modifications apportées doivent ensuite être répercutées dans l'ordre chronologique où elles ont été faites.

6 Interface graphique

6.1 Interface graphique de configuration :

6.1.1 Le système doit se présenter par une interface graphique.

6.1.2 Toutes les fonctionnalités doivent pouvoir être gérées par l'interface graphique.

6.1.3 On doit pouvoir choisir toutes les fonctions de configuration par menus déroulants.

6.1.4 Un menu de propriétés doit être associé à tous les éléments matériels et logiciels du système, pour pouvoir les configurer.

6.1.5 La configuration par scripts ou toute autre forme de programmation textuelle n'est pas acceptable.

6.2 Interface pour opérateur

6.2.1 Outre l'interface décrite au point 9.1, ci-dessus, l'interface pour opérateur doit prévoir les fonctions suivantes :

(a) Affichages plein écran configurables par l'utilisateur, conçus spécifiquement pour les tâches et les besoins en information des opérateurs.

(b) Des affichages par défaut doivent couvrir les fonctions principales de gestion du site :

i. Gestion des alarmes

ii. Gestion des titulaires de carte

iii. Surveillance du site

(c) Le système doit permettre de créer des affichages personnalisés.

(d) L'interface opérateur doit être entièrement configurable par tout utilisateur autorisé à configurer les affichages.

6.2.2 Chaque affichage se compose d'un volet de navigation et d'un volet de données, tel que décrit ci-dessous.

(a) Le volet de navigation doit donner la liste des informations système associées à l'affichage utilisé.

i. L'utilisateur doit pouvoir choisir et trier les colonnes de données des affichages d'alarmes et de titulaires de carte.

ii. Le système doit permettre la recherche incrémentale en fonction des colonnes de données choisies dans les affichages des titulaires de carte.

iii. Choisir un poste dans l'espace de navigation remplit automatiquement les sections de données pertinentes.

iv. Les en-têtes de l'affichage des alarmes doivent indiquer le nombre d'alarmes non traitées pour chacune.

(b) Le système doit présenter un ou plusieurs pavés de données pour afficher les données détaillées associées à l'élément choisi dans le volet de navigation.

i. Les pavés peuvent être créés à partir d'une série de pavés par défaut prévus à cet effet.

ii. Il faut pouvoir configurer chaque pavé pour y afficher les données voulues, selon la fonction du pavé.

iii. Un clic doit pouvoir maximiser les pavés.

iv. Si un pavé est maximisé, les autres pavés doivent rester visibles dans une bande, et un clic sur un des pavés doit le maximiser.

v. Le cas échéant, l'affichage des données dans les pavés en bande doit être dynamique.

7 Plans de site et icônes connexes

7.1 L'interface graphique doit permettre de gérer et de surveiller les alarmes, les dérogations, l'état général des éléments du site et l'ouverture des portes, par des plans et des icônes dynamiques interactives en temps réel.

7.2 Les écrans d'affichage des plans de site doivent être tactiles.

7.3 Toute modification d'un plan de site sur l'un des postes de travail réseau doit être répercutée automatiquement sur le plan correspondant stocké sur le serveur.

7.4 Le système doit pouvoir importer des graphiques à partir d'un logiciel de dessin externe.

7.4.1 Le système doit pouvoir importer au moins les formats graphiques suivants :

(a) BMP

(b) WMF, EMF

(c) JPG

(d) GIF

7.5 L'utilisateur doit pouvoir attribuer des icônes aux fonctions du système et les placer à n'importe quel endroit sur un plan de site.

7.6 Le système doit permettre de tracer des lignes et des surfaces pour former des « objets », puis de les associer à des éléments du système pour en indiquer l'état.

7.7 Le système doit permettre de placer du texte n'importe où sur un plan de site.

7.8 Les plans d'implantation doivent être « imbriqués », pour qu'une seule action (un clic sur l'icône d'un plan de site affiché) fasse passer l'affichage d'un plan à l'autre.

7.9 Les fonctions suivantes au minimum doivent pouvoir être exécutées par un clic sur l'une des icônes du plan de site :

(a) afficher l'état actuel d'une porte, d'une entrée ou d'une sortie;

(b) surveiller et accuser réception d'une alarme;

(c) ouvrir une porte à accès contrôlé;

(d) passer d'un plan à un autre;

(e) activer un interphone sur un lecteur de carte;

(f) outrepasser une alarme, un accès ou l'état d'une zone de clôture périmétrique;

(g) afficher les propriétés de l'élément cliqué.

7.10 Par défaut, les icônes doivent être nommées selon le nom de l'élément, mais un nom plus court peut être choisi s'il est disponible.

7.11 Il faut pouvoir redimensionner les icônes.

7.12 Le système doit comprendre un ensemble d'icônes préétablies qui comprennent les fonctions de base du contrôle d'accès.

7.13 Il doit être possible de concevoir et de charger des icônes à partir d'un logiciel externe pour les utiliser dans le système.

7.14 Le système doit permettre de concevoir des macro-commandes, qui peuvent outrepasser simultanément n'importe quel élément du site, et de les associer à un bouton placé sur un plan de site qui sert à les activer.

7.15 Le système doit permettre de sélectionner plusieurs éléments d'un plan de site, soit individuellement ou en groupe par glisser-déplacer, pour régler leur état en une seule action.

7.16 Le système doit permettre de parcourir les plans de site disponibles, de les chercher et les choisir site dans une fenêtre (pavé) unique, et d'afficher et parcourir la liste des plans de site récemment ouverts.

8 Matériel sur place

8.1 Les CIP agissent comme contrôleurs sur place. L'application réseau principale doit communiquer directement avec tous les CIP du système.

8.2 Chaque CIP doit être intelligent : en d'autres termes, il doit en cas de panne de l'alimentation du système de contrôle central ou des communications avec celui-ci, quel qu'en soit le motif, continuer à autoriser ou à refuser l'accès selon tous les critères de sécurité applicables.

8.3 Les CIP doivent enregistrer tous les paramètres de sécurité et d'accès, afin de fonctionner indépendamment du serveur de contrôle central. Les systèmes qui communiquent avec le système de contrôle central pour accorder ou refuser l'accès ne sont pas recevables.

8.4 Les CIP doivent transmettre immédiatement les données d'activité au serveur de contrôle central, en utilisant aussi peu la capacité réseau que possible.

8.5 Si les communications avec le serveur de contrôle central sont impossibles, chaque CIP doit pouvoir enregistrer jusqu'à 80 000 événements.

8.6 Les CIP doivent horodater tous les événements au moment où ils surviennent.

8.7 Au rétablissement des communications, les CIP doivent transférer automatiquement les événements mis en mémoire tampon au serveur de contrôle central.

8.8 Les CIP doivent pouvoir enregistrer jusqu'à 500 000 dossiers de cartes et les critères d'accès connexes.

8.9 Chaque CIP doit permettre de configurer le rapport entre le nombre d'événements et le nombre de dossiers de carte enregistrés, afin de l'adapter aux besoins de chaque site selon le nombre de titulaires de cartes ou d'événements.

8.10 Le système doit surveiller les circuits d'entrée et indiquer pour chacun l'un de quatre états distincts : Normal, Alarme, Circuit ouvert altéré ou Court-circuit altéré.

8.11 Le système doit permettre de configurer la plage des valeurs des résistances en fin de ligne acceptables, afin de prendre en charge au besoin les circuits d'entrée préexistants.

8.12 L'utilisation de tout circuit utilisant d'autres résistances de fin de ligne que les résistances doubles de 4700 ohms doit être approuvée par l'expert-conseil.

8.13 Les CIP doivent être protégés contre les manipulations à l'avant et à l'arrière du panneau. Le panneau avant doit être protégé contre l'ouverture de la porte, et l'arrière du panneau pour détecter s'il a été retiré du mur. Ces systèmes doivent utiliser des détecteurs d'altération optiques; les dispositifs mécaniques ne sont pas acceptables.

8.14 Les CIP doivent intégrer un processeur ARM 9, et disposer de mémoire Flash EEPROM non volatile d'au moins 256 mégaoctets. Le microcode de démarrage doit être stocké dans un

secteur protégé de la mémoire flash. Toutes les mises à niveau logicielles doivent être faites à partir du serveur réseau central.

8.15 Les CIP doivent prendre en charge la mise à niveau locale à l'aide d'une clé USB.

8.15.1 Le processus de mise à niveau ne doit accepter par le port USB que les données de mise à niveau authentifiées.

8.16 Les CIP doivent être alimentés indépendamment par une tension de 13,6 V c. c. à partir d'un système d'alimentation sans coupure (batteries).

8.17 En cas de panne de courant, les CIP doivent pouvoir fonctionner pendant au moins 24 heures.

8.18 Les CIP doivent pouvoir détecter et signaler automatiquement une panne de courant, une batterie presque déchargée et une batterie débranchée.

8.19 Après une panne de courant, les CIP doivent redémarrer et reprendre le traitement automatiquement.

8.20 Les CIP doivent être équipés d'un matériel et d'un logiciel « de garde » pour détecter automatiquement les plantages du processeur et déclencher un redémarrage.

8.21 Les CIP doivent intégrer une horloge en temps réel, qui doit se synchroniser avec celle du système de contrôle central au moins une fois l'heure. Cette horloge doit être assez précise pour que le décalage de temps entre les CIP ne dépasse jamais 0,5 seconde.

8.22 On doit pouvoir configurer le fuseau horaire des CIP en fonction de l'emplacement de leur mise en œuvre.

8.23 Les CIP doivent intégrer connexion Ethernet (TCP/IP) 10BaseT et 100BaseT et un pilote pour communiquer avec le système de contrôle central.

8.24 Si ces débits sont spécifiés, les CIP doivent prendre en charge 100BaseT et 1000BaseT.

8.25 Les CIP doivent si cela est spécifié intégrer deux ports Ethernet, afin de prendre en charge une autre voie de communication.

8.26 L'adresse IP des CIP doit pouvoir être préconfigurée pour qu'on puisse en effectuer la configuration initiale en mode autonome par un navigateur Web.

8.27 Les CIP doivent prendre en charge le service DNS (Domain Name Server) pour obtenir une adresse IP.

8.27.1 Si le serveur DNS primaire n'est pas disponible, le CIP doit pouvoir communiquer avec un serveur DNS secondaire ou tertiaire.

8.28 L'achalandage excessif du réseau, par attaque ping ou toute autre attaque semblable, doit déclencher une alarme.

8.29 Toutes les communications TCP/IP entre les CIP et le système de contrôle central doivent être chiffrées par le protocole AES 256 bits. Les communications doivent être en ligne et seront surveillées en cas d'interruption.

8.30 Les CIP doivent intégrer un port RS-232 multicommunications.

8.31 Les CIP doivent intégrer un port USB2.0.

8.32 Les CIP doivent prendre en charge l'accès à distance par ligne commutée.

8.33 Les communications à distance entre les CIP et les dispositifs distants doivent se faire par le réseau téléphonique commuté.

8.33.1 Les connexions entrantes doivent se faire par le service d'un FAI.

8.33.2 Les connexions sortantes par des modems connectés au réseau local du client ne sont pas acceptées, mais les connexions directes à partir du serveur ne sont acceptables que si le modem reste en mode « aucune réponse ».

8.34 Aux fins de mise en service et de diagnostic, les CIP doivent pouvoir afficher leur état ou leur configuration sans le recours au serveur central ou à un logiciel propriétaire; on peut par exemple utiliser un navigateur Web. Pour les applications à sécurité élevée, les CIP doivent permettre de désactiver cette fonction.

8.35 Les CIP doivent prendre en charge les fonctions logiques à l'aide de blocs logiques configurables.

8.35.1 Ces fonctions doivent pouvoir être exécutées que le système de contrôle central soit en ligne ou non.

8.35.2 Les blocs logiques doivent prendre en charge les éléments d'entrée suivants :

(a) états d'entrée physique;

(b) états de sortie (physiques et logiques);

(c) l'état des portes;

(d) autres états de blocs logiques.

8.35.3 Pour commander une sortie, les CIP doivent prendre en charge la configuration de jusqu'à 10 éléments d'entrée de blocs logiques qui combinent des portes logiques ET ou OU. Chaque élément doit pouvoir intégrer 10 portes ET ou OU.

8.35.4 Les sorties des blocs logiques doivent pouvoir être configurées comme sorties internes (virtuelles).

8.35.5 Les sorties des blocs logiques doivent pouvoir être attribuées à des sorties externes.

8.35.6 Les sorties des blocs logiques doivent pouvoir servir d'entrées pour un ou plusieurs autres blocs logiques.

8.35.7 On doit pouvoir régler la temporisation de sortie des blocs logiques selon les paramètres suivants au minimum :

(a) délai activé;

(b) délai désactivé;

(c) verrouillé;

(d) durée d'impulsion;

(e) durée d'activation maximale;

(f) explicite.

8.35.8 Les sorties des blocs logiques des CIP doivent pouvoir déclencher des actions sur d'autres CIP, que le système de contrôle central soit en ligne ou non.

8.36 Les situations d'alerte suivantes au minimum doivent déclencher l'envoi d'un message d'alarme distinct au système de contrôle central. Les messages connexes affichés doivent être clairs.

(a) Altération

(b) Retour à la normale après altération

(c) Unité inactive

(d) Erreur de carte

(e) Avertissement de maintenance

(f) Changement d'état du secteur d'alarme

(g) Activation d'un compte d'utilisateur

(h) Désactivation d'un compte d'utilisateur

(i) Suivi de la carte

(j) NIP erroné

(k) Accès refusé

(l) Sous contrainte

(m) Nombre maximum de zones

(n) Nombre minimum de zones

(o) Porte ouverte trop longtemps

(p) Porte forcée

(q) Porte non verrouillée

(r) Panne de courant

(s) Redémarrage

(t) Interphone

8.37 Les CIP doivent pouvoir commander les équipements suivants :

(a) lecteurs d'accès à jeton ou biométriques;

(b) lecteurs d'accès par carte avec pavé numérique;

(c) équipement d'accès aux ascenseurs;

(d) panneaux et équipement d'entrée/sortie pour la surveillance des alarmes;

(e) équipement de réponse d'alarme.

8.38 Toute panne d'un lecteur de jeton ou d'un lecteur biométrique, et toute panne des communications entre ces appareils et un CIP doit être signalée immédiatement comme une alarme à priorité élevée; cela ne doit pas empêcher le CIP ou ni tout autre matériel connexe de fonctionner correctement.

8.39 Les CIP doivent communiquer avec les dispositifs à distance (lecteurs biométriques et à jeton, équipement d'alarme, lecteurs d'ascenseur) par un protocole de communication chiffré de bout en bout. Les données ASCII non chiffrées et toute transmission de données semblable ne sont pas acceptables.

8.40 Toutes les communications entre les CIP et les dispositifs à distance doivent être codées à l'aide de chiffres de contrôle afin de protéger les données contre toute altération pendant la transmission.

8.41 Toutes les voies de communication entre les CIP et les dispositifs à distance doivent être surveillées, pour que toute altération ou modification des données transmises déclenche une alarme sur le système de contrôle central.

8.42 La communication entre les CIP et les lecteurs et autres dispositifs en aval doit prendre en charge le protocole de connexion Wiegand générique, prenant en charge jusqu'à 9999 bits :

8.42.1 Les formats Wiegand doivent être configurables, pour prendre en charge les éléments suivants :

(a) nombre de bits;

(b) bits ou code de l'installation ou du site;

(c) bits du numéro de la carte;

(d) configuration des bits de parité.

8.43 Les CIP et les dispositifs en aval doivent communiquer à grande vitesse, c'est-à-dire au moins 1 Mbit/s.

8.43.1 Toute session de communication de données entre les CIP et ces dispositifs doit s'établir par échange de certificats utilisant des clés de chiffrement elliptique d'au moins 256 bits.

8.43.2 Toute communication de données entre les CIP et ces appareils doit utiliser un chiffrement AES d'au moins 128 bits.

8.44 Chaque circuit de communication à grande vitesse mis en place doit prendre en charge au moins 20 dispositifs distincts.

8.45 Chaque dispositif connecté au circuit doit communiquer son numéro de série au CIP pour l'identifier et lui attribuer sa fonction.

8.46 Chaque CIP doit pouvoir prendre en charge 10 circuits de communication à grande vitesse matériels.

9 Contrôle d'accès, alarmes de sécurité et programmation des E/S

9.1 Le système doit être configurable à volonté, et pouvoir configurer toute combinaison de paramètres de contrôle d'accès, d'alarmes de sécurité et d'entrées/sorties, en fonction des limites de rendement et de mémoire des CIP.

9.2 Pour simplifier la configuration, on doit pouvoir regrouper les titulaires de carte en groupes d'accès qui partagent les mêmes droits.

9.3 On doit pouvoir prolonger le délai de déverrouillage des portes pour certains titulaires de carte, en cas d'handicap, par exemple.

9.4 Le système doit permettre d'attribuer temporairement un titulaire de carte à un groupe d'accès, et régler à l'avance le début et la fin de cette attribution.

9.4.1 Pendant cette période temporaire, le titulaire de la carte doit disposer tant des droits du groupe auquel il a été attribué que des droits d'accès permanents dont il peut disposer.

9.4.2 La page des propriétés du groupe d'accès doit afficher tous les membres, permanents et temporaires, et indiquer ainsi l'état des membres temporaires :

(a) En attente (indiquer les dates de début et de fin)

(b) Actif

(c) Échu

9.5 Les cartes ou groupes d'accès doivent pouvoir être programmés pour donner accès à toute combinaison de portes contrôlées, et chaque période d'accès de chaque porte doit pouvoir être paramétrée à la minute près.

9.6 Les CIP doivent vérifier l'accès en fonction de TOUS les critères suivants :

(a) Code d'installation

(b) Autorisation de la carte dans la base de données

(c) Numéro d'émission correct

(d) Accès autorisé à la porte ou zone

(e) Heure de la journée autorisée

(f) Validité des compétences du titulaire (voir la section 13)

(g) NIP correct (si sa saisie est exigée)

(h) Accès double (modes antiretour, anti-talonnage ou d'escorte).

9.7 Le mode antiretour doit comprendre les options de configuration suivantes :

(a) Refuser un deuxième accès à une zone si une sortie valide n'a pas été déjà enregistrée, et déclencher une alarme (antiretour strict).

(b) Permettre un deuxième accès à une zone si une sortie valide n'a pas été enregistrée auparavant, et déclencher une alarme (antiretour discret).

(c) Le système doit pouvoir exempter des groupes d'accès précis des règles d'antiretour décrites aux points (a) et (b) ci-dessus.

(d) Les règles antiretour doivent pouvoir être réinitialisées selon les critères suivants :

i. automatiquement, après un délai préétabli suivant une entrée valide;

ii. automatiquement, à une heure précise de la journée;

iii. automatiquement, à la sortie du site;

iv. manuellement, pour les outrepasser.

(e) Le système doit prendre en charge l'antiretour global, c'est-à-dire relier plusieurs zones d'accès aux fins d'antiretour par plusieurs CIP, à l'aide de communications pair-à-pair chiffrées.

(f) Les CIP ne doivent pas dépendre du serveur pour la fonction antiretour, et l'antiretour global doit pouvoir fonctionner sur plusieurs CIP, même si le serveur est hors ligne.

9.8 Le mode anti-talonnage doit comprendre les options de configuration suivantes :

(a) Interdire la sortie d'une zone si un accès valide n'a pas déjà été enregistré, et déclencher une alarme (anti-talonnage strict).

(b) Autoriser la sortie d'une zone si un accès valide n'a pas déjà été enregistré, mais déclencher une alarme (anti-talonnage discret).

(c) Le système doit pouvoir exempter des groupes d'accès précis des règles établies aux points 12.8 (a) et (b).

(d) Les règles anti-talonnage doivent pouvoir être réinitialisées selon les critères suivants :

i. Automatiquement, après un délai préétabli suivant une entrée valide;

ii. Automatiquement, à une heure précise chaque jour;

iii. Manuellement, pour les outrepasser.

(e) Les CIP ne doivent pas dépendre du serveur pour la fonction anti-talonnage, et l'anti-talonnage global doit pouvoir fonctionner sur plusieurs CIP, même si le serveur est hors ligne.

9.9 Toute saisie de NIP erronée doit déclencher une alarme au serveur de contrôle central.

9.10 Le système doit pouvoir modifier automatiquement et en tout temps le mode d'accès de toute porte, selon les commandes reçues du serveur de contrôle central. Le système doit comprendre les modes d'accès suivants :

(a) Accès libre — La porte est déverrouillée; aucune lecture de carte n'est nécessaire.

(b) Accès sécurisé — La porte est verrouillée; une carte valide est nécessaire pour entrer, et la porte se verrouille après l'accès.

(c) Accès sécurisé avec NIP — La porte est verrouillée; une carte *et* un NIP valides sont nécessaires pour entrer, et la porte se verrouille après l'accès.

(d) Dérogation au lecteur — Les membres de certains groupes d'accès doivent pouvoir modifier le mode d'accès et le NIP de la porte pendant des périodes préétablies.

(e) Autorisation double — L'accès est accordé si deux cartes différentes et valides sont présentées dans un délai préétabli.

(f) Escorte — L'accès est accordé après lecture d'une deuxième carte d'un titulaire faisant partie du Groupe d'accès d'escorte.

(g) NIP partagé — L'opérateur du système choisit le NIP de 4 chiffres et configure le système en conséquence. L'accès à la porte est accordé si on entre ce NIP au pavé numérique, suivi de la touche « Enter ».

9.11 L'accès du titulaire de la carte à la centrale et l'enregistrement dans la piste d'audit doivent pouvoir être configurés selon deux modes :

(a) Uniquement lorsque la présentation d'une carte d'accès ou d'un jeton valide a été effectuée avec succès ET que le capteur d'ouverture de porte a détecté que la porte a effectivement été ouverte.

(b) Chaque fois qu'une carte d'accès valide a été présentée avec succès, indépendamment du fait que la porte a été ouverte ou non.

9.12 Les lecteurs munis d'un pavé pour NIP et les lecteurs d'empreintes digitales doivent fournir une fonction d'entrée sous contrainte.

9.12.1 Cette condition doit être signalée par le titulaire de la carte par l'ajout de soit un numéro unique à son NIP, soit 1 au dernier chiffre de son NIP. Sur les lecteurs d'empreintes digitales, cette condition doit être indiquée par la lecture de son « doigt de contrainte » choisi à l'avance.

9.12.2 Les lecteurs ne doivent présenter AUCUNE indication de lecture sous contrainte.

9.12.3 Le poste de contrôle central doit alors signaler une « alarme sous contrainte » à priorité élevée.

9.12.4 On peut pouvoir configurer le système pour qu'il affiche au-dessus des autres fenêtres les alarmes de contrainte et toute autre alarme critique choisie, afin d'attirer immédiatement l'attention de l'opérateur. Les autres alarmes doivent être affichées, mais sans interrompre la tâche en cours.

9.13 Le système doit compter en temps réel les titulaires de cartes de chaque zone d'accès (comptage par zone).

9.13.1 La présence de moins qu'un seuil minimum de titulaires ou de plus qu'un maximum préétablis doit déclencher un événement ou une alarme.

9.13.2 Les nombres minimum et maximum de titulaires de carte dans une zone avant qu'un événement soit déclenché doivent être configurables.

9.13.3 Le système doit prévoir une temporisation, en secondes, pour permettre au nombre de titulaires d'une zone de dépasser temporairement le minimum (dans la fourchette d'utilisateurs) ou le maximum sans déclencher d'événement.

9.13.4 Le système doit permettre de configurer un message propre à chacune des conditions suivantes : nombre de titulaires inférieur au minimum, nombre dans la fourchette prévue ou nombre supérieur au maximum.

9.13.5 Le système doit prévoir le refus d'accès d'une zone à un titulaire de carte à moins de :

(a) présenter deux cartes valides différentes s'il n'y a personne dans la zone d'accès;

(b) présenter une carte pour accéder à la zone si deux personnes (cartes) ou plus y sont répertoriées;

(c) présenter une carte pour sortir d'une zone si trois personnes ou plus y sont répertoriées;

(d) présenter deux cartes valides différentes pour sortir d'une zone si deux personnes y sont répertoriées;

(e) et interdire la sortie d'une zone et déclencher une alarme si une personne y est répertoriée.

9.13.6 Le système doit prévoir l'augmentation ou la diminution du nombre de personnes d'une zone en fonction d'entrées logiques non liées à des événements d'accès.

10 Analyses de l'identité — compétences

10.1 Les compétences sont des attributs attribuables aux titulaires de carte, afin d'établir l'accès d'un titulaire à une zone précise selon des facteurs pertinents au titulaire, comme l'autorité, le degré de compétence ou tout autre facteur.

10.2 Le système doit permettre l'attribution de plusieurs compétences à un ou plusieurs dossiers de titulaire de carte.

10.3 le système doit permettre d'attribuer à chaque compétence l'un de 4 états distincts :

(a) Active — La compétence est valide pour le titulaire.

(b) Date d'expiration — La compétence est valide pour le titulaire, mais elle arrivera à échéance à la date indiquée.

i. Un message configurable doit être affiché pour informer le titulaire de la carte que sa compétence arrive à échéance.

(c) Échue — La compétence attribuée au titulaire est échue.

(d) Désactivée — La compétence est désactivée (ou remplacée) temporairement pour le titulaire.

i. Un champ doit être prévu pour justifier cette désactivation.

10.4 Ces états de compétences doivent être configurables : soit « Discret » (l'accès est accordé, mais cela déclenche une alarme), soit « Strict » (l'accès est refusé si une compétence est invalide ou désactivée).

10.5 Chaque compétence doit être établie indépendamment pour chaque titulaire de carte.

10.6 Un champ doit être prévu pour justifier la désactivation d'une compétence.

10.7 Les compétences doivent être configurées au besoin selon chaque zone d'accès.

10.8 Le système doit permettre d'exempter des groupes d'accès précis de l'obligation de satisfaire à des compétences précises.

10.9 Si le système refuse l'accès à cause d'une compétence invalide ou absente, il doit en afficher la raison sur le lecteur de porte utilisé.

10.10 L'autorisation d'accès selon les critères de compétence doit être établie par le CIP, que le serveur soit en ligne ou non.

10.11 Le motif d'un refus d'accès par compétence non valide doit être affiché sur le lecteur de porte ou le pavé numérique utilisé.

10.12 Si une compétence arrive bientôt à échéance, le système doit en informer à l'avance le titulaire de carte touché et toute autre personne désignée.

10.13 Le système doit envoyer un avis d'expiration d'une compétence d'un titulaire de carte à la personne visée et à toute autre personne désignée.

10.14 Le système doit envoyer par courriel au gestionnaire associé un rapport regroupé qui fait état des avis d'échéance de compétence envoyés.

11 Macros de configuration préprogrammées

11.1 Afin d'apporter au besoin des modifications à la configuration du système, il doit permettre l'attribution des modifications voulues à une macro-commande.

11.2 Un opérateur doit pouvoir lancer ces macros (pour apporter les modifications prévues) par une commande de menu ou une icône sur le plan de site.

11.3 Le système doit prévoir la création de ces macros par interface graphique, comme listes déroulantes ou glisser-déposer par la souris. Le recours à un langage de script n'est pas acceptable.

11.4 Le système doit prévoir l'exécution des macros à une période préétablie.

11.5 Les macros doivent pouvoir exécuter des actions par lignes de commande.

11.6 Les lignes de commande doivent prendre en charge jusqu'à 300 variables nommées.

11.7 Chaque macro doit prendre en charge de nombreuses lignes de commande.

11.8 Les droits de configuration et d'exécution des macros par ligne de commande doivent être protégés par nom d'utilisateur et mot de passe. Ces justificatifs doivent être masqués à l'entrée puis transmis et stockés en format chiffré sur le serveur du système de contrôle central.

12 Contrôle en ligne des portes

12.1 Le contrôle d'accès d'une porte doit au besoin prendre en charge les fonctions suivantes :

(a) lecteur d'accès;

(b) entrée d'un interrupteur de déverrouillage d'urgence;

(c) entrée d'un interrupteur de contrôle de réception.

12.2 La commande de sortie d'une porte doit le cas échéant prendre en charge les fonctions suivantes :

(a) lecteur de sortie;

(b) demande de sortie par bouton-poussoir;

(c) sortie d'urgence par bris de vitre.

12.3 La demande de sortie par bouton-poussoir mentionnée au point 15.2 (b) doit déclencher l'enregistrement de la sortie dans la base de données des événements.

12.4 Si un justificatif d'entrée ou de sortie valide est présenté, la porte doit se déverrouiller pendant un délai préétabli, puis se verrouiller à nouveau.

12.4.1 Si l'accès ou la sortie s'effectue avant l'échéance du délai, la porte se verrouille dès la fermeture de la porte.

12.4.2 Le système doit prolonger ce délai si le titulaire visé fait partie d'un groupe d'accès pour lequel une prolongation du délai est prévue; voir le point 12.3, ci-dessus.

12.5 Les méthodes d'entrée et de sortie visées aux points 15.1 b), 15.1 c) et 15.2 c) doivent déclencher l'enregistrement de l'événement pertinent dans la base de données des événements.

12.6 La surveillance des portes, c'est-à-dire tant l'ouverture et la fermeture que le verrouillage et le déverrouillage, doit se faire par capteurs dissimulés adaptés à l'installation de chaque porte.

12.7 Si la porte est double, la porte inactive doit être surveillée comme la porte principale (ouverture, fermeture, verrouillage et déverrouillage). On peut brancher les capteurs de surveillance de la porte inactive comme éléments de surveillance de la porte principale.

12.8 Le système doit pouvoir être configuré afin de déclencher une alarme de porte forcée si une porte est déverrouillée ou ouverte sans lecture de justificatifs ou saisie de NIP.

12.9 Toute porte laissée déverrouillée ou ouverte après une période préétablie doit déclencher une alarme pour signaler la situation.

12.10 L'ouverture et le déverrouillage d'une porte doivent déclencher un avertissement sonore.

12.11 Il doit être possible de désactiver cet avertissement sonore.

12.12 L'avertissement sonore doit pouvoir être déclenché par un relais branché ailleurs dans le système.

12.13 Si un justificatif d'accès valide est présenté à une porte, mais que la porte n'est pas ouverte (aucun accès), il doit être possible d'ignorer cette demande (de ne pas l'enregistrer comme événement d'entrée) et de verrouiller automatiquement la porte après un délai préétabli.

12.14 Si un justificatif d'accès valide est fait à une porte, elle doit se verrouiller immédiatement à sa fermeture.

12.15 Le système doit permettre de « confiner » une zone d'accès par l'attribution d'une condition d'entrée, après quoi toutes les portes de la zone d'accès doivent passer en mode sécurisé.

12.15.1 Le système doit permettre d'attribuer à certains titulaires de carte le droit d'accéder à une zone verrouillée, et refuser l'accès à tous les autres titulaires.

12.16 Le système doit permettre d'établir des liens d'interverrouillage entre les portes d'un groupe. Ces groupes d'interverrouillage doivent pouvoir compter jusqu'à 20 portes.

12.16.1 On doit pouvoir configurer ces groupes d'interverrouillage par les fonctions « glisser-déposer » de l'interface graphique, sans devoir créer un script.

12.17 Le système doit prendre en charge un mode d'intervention ou de vérification vidéo, comme indiqué ci-dessous :

12.17.1 À la lecture d'une carte, une fenêtre d'intervention doit afficher la photo du titulaire tirée de la base de données des titulaires.

12.17.2 En parallèle, le système doit aussi afficher une image vidéo provenant d'une ou de plusieurs caméras de surveillance.

12.17.3 Le mode d'intervention doit permettre d'afficher le plan du site, et montrer l'emplacement et l'état du point d'entrée contrôlé et des éléments adjacents.

12.17.4 En mode d'intervention, l'opérateur doit pouvoir consulter les cartes de site et les compétences du titulaire visé afin de l'informer sur-le-champ si certaines compétences arrivent à échéance.

12.17.5 Le système doit aussi permettre à l'opérateur de consulter les données personnelles du titulaire, comme son nom complet ou sa division.

12.17.6 Le choix et l'agencement à l'écran de la photo du titulaire, des données personnelles, de l'état de la carte et des compétences, des plans de site et des images vidéo associés à une entrée en mode d'intervention doivent être configurables par simple glisser-déposer ou par cliquer-déposer (redimensionner et placer ces données).

12.17.7 Le mode d'intervention doit être configurable de l'une de deux façons :

(a) Si la carte est valide, accès accordé automatiquement. Dans ce cas, le système doit afficher à l'écran de l'opérateur la décision en temps réel (accès accordé ou refusé).

(b) Si la carte est valide, accès accordé par intervention de l'opérateur.

12.17.8 Si une deuxième demande d'accès exigeant l'intervention de l'opérateur survient s'il reste une demande d'intervention sans réponse, la deuxième demande et toutes les demandes subséquentes doivent être mises en attente automatiquement.

12.17.9 L'opérateur doit pouvoir consulter les demandes d'intervention en attente, et les choisir puis les traiter dans l'ordre de son choix.

12.17.10 Le système doit permettre de gérer les demandes d'intervention à partir d'un seul affichage plein écran par opérateur ou plusieurs affichages filtrés, selon les directives du client.

13 Contrôle autonome des portes

13.1 Si cela est précisé, les portes doivent être gérées à l'aide d'un système de verrouillage des portes autonome (hors ligne).

13.2 Une seule interface doit permettre l'administration de ces systèmes et la création de rapports sur les systèmes de verrouillage en ligne et autonomes.

13.3 Il faut intégrer complètement les portes autonomes au système de contrôle d'accès et d'alarme contre les intrusions, tel que décrit ci-dessous :

13.3.1 Le système doit utiliser des cartes Mifare 4k sans contact standard, comme toutes les portes en ligne.

13.3.2 On doit pouvoir configurer chaque carte une seule fois pour les lecteurs de porte en ligne et autonomes.

13.3.3 Les données opérationnelles doivent être transférées automatiquement entre le système de sécurité intégré et les portes autonomes, sans intervention de l'opérateur. Données nécessaires :

(a) alerte de charge basse d'une batterie (plusieurs niveaux);

(b) activités d'accès pour toutes les portes;

(c) données sur les cartes désactivées;

(d) toute modification aux droits d'accès des titulaires de carte.

13.3.4 Une seule interface doit permettre d'attribuer les droits d'accès aux portes en ligne et autonomes.

13.3.5 Le système doit prévoir des droits d'accès fondés sur l'heure (heures de travail ou après ces heures) ou le jour (semaine ou fins de semaine), sans restriction sur les intervalles horaires ou les jours de présence de tout utilisateur.

13.3.6 Le système doit pouvoir être configuré pour mettre à jour les données d'accès des portes autonomes à intervalles réguliers (au moins de 1 à 7 jours).

13.3.7 Il ne faut pas stocker les droits d'accès dans les plaques de poignée de porte; ainsi, nul besoin de mettre à jour chaque plaque à l'ajout ou au retrait d'une carte.

13.3.8 On doit aussi pouvoir prolonger le délai de déverrouillage des portes autonomes pour certains titulaires, en cas de handicap, par exemple.

13.3.9 Les portes hors ligne doivent prendre en charge le cloisonnement; ainsi, les administrateurs peuvent contrôler l'accès et attribuer les droits d'accès pour leur propre environnement ou installation.

13.4 Le matériel prévu doit comprendre une option de verrouillage interne qui à son activation bloque l'accès à tous sauf aux utilisateurs privilégiés.

13.5 Le matériel ne doit pas utiliser de batteries spéciales; elles doivent être de type courant.

13.6 Les batteries doivent prendre en charge au moins 35 000 opérations avant leur remplacement.

13.7 Le matériel de la plaque de poignée doit être compatible avec le matériel de verrouillage spécifié pour ce projet.

13.8 Le matériel électronique des serrures doit être facile à installer sur les serrures existantes des portes.

13.8.1 La plaque de poignée de porte doit être compatible avec le mécanisme de verrouillage, et doit tenir compte de :

(a) la taille de la poignée;

(b) l'angle de rotation de la poignée.

13.9 Le personnel du client doit pouvoir effectuer la maintenance de base du matériel (remplacement des piles, changement de la configuration de base) après avoir reçu des directives minimales.

13.10 Les plaques de poignée autonomes doivent garder en mémoire au moins les 1 000 derniers événements (piste de vérification).

13.11 Les plaques de poignée autonomes doivent fonctionner selon plusieurs modes, c'est-à-dire notamment, mais sans s'y limiter : accès libre (déverrouillé), accès sécurisé (verrouillé) selon un horaire, ou encore sous le contrôle d'un utilisateur disposant des droits d'accès voulus pour modifier le mode de fonctionnement des plaques.

13.12 Une carte autorisée et configurée en conséquence doit pouvoir commuter le mode de fonctionnement d'une porte entre l'accès libre et l'accès sécurisé.

13.13 Le système doit permettre de préciser, pour chaque utilisateur, les modes dans lesquels il peut placer la serrure (par exemple, libre ou sécurisé) et les dérogations auxquelles il a droit (p. ex., entrée autorisée en cas de verrouillage).

13.14 Le système doit prévoir un dispositif utilitaire portatif pour :

(a) diagnostiquer les problèmes;

(b) déverrouiller d'urgence une plaque de poignée hors ligne;

(c) mettre à jour le logiciel;

(d) alimenter la plaque de la poignée pour résoudre un problème si la batterie ne l'alimente plus;

(e) configurer toute porte installée plus tard.

13.15 Le système doit prévoir plusieurs degrés d'avertissements pour le niveau de charge des batteries, y compris avertissements sonores, visuels et physiques : un signal visuel initial, puis un signal sonore et visuel auxquels s'ajoute plus tard un délai avant l'ouverture de la porte afin d'inciter les titulaires à signaler la situation aux responsables.

13.16 L'installation de la porte doit comprendre des mesures de protection contre les intempéries.

13.16.1 La cote des plaques de poignée doit être d'au moins IP46.

13.16.2 La cote des verrous doit être d'au moins IP66.

13.17 Les portes autonomes doivent pouvoir être configurées en mode sans fil; elles communiqueraient alors par une passerelle sans fil.

14 Contrôle sans fil des portes

14.1 Le cas échéant, on doit pouvoir gérer les portes par un système de verrouillage sans fil fondé sur les plaques de poignée.

14.2 Une seule interface utilisateur intégrée aux autres éléments, sur le système de contrôle central, doit permettre d'assurer l'intégrité des décisions sur l'accès du système de contrôle d'accès principal.

14.3 Les données des cartes RFID doivent être transmises instantanément au lecteur de cartes sans fil et au mécanisme de verrouillage (plaque de poignée ou verrou), qui doit transmettre à son tour les données d'identification de la carte au concentrateur et au système de contrôle central.

14.4 Le système de contrôle et d'alerte d'intrusion central doit immédiatement accorder ou refuser l'accès en fonction des règles décrites ailleurs dans les présentes.

14.5 Une seule interface doit permettre d'attribuer les droits d'accès aux portes connectées et sans fil.

14.6 On doit pouvoir configurer chaque carte une seule fois pour les lecteurs de porte connectés et sans fil.

14.7 Les concentrateurs sans fil RS-485 fournis doivent pouvoir prendre en charge 8 entrées ou mécanismes de verrouillage sans fil, et avoir une portée de 15 mètres (communications fiables).

14.7.1 Les concentrateurs sans fil doivent pouvoir être branchés en série par câble compatible avec la norme RS-485.

14.7.2 Les concentrateurs sans fil doivent être conformes aux normes de radiocommunications applicables à la région où ils sont installés et à la norme IEEE 802.15.4 (2400-2483,5 MHz).

14.7.3 Les communications entre concentrateur et lecteurs sans fil doivent être chiffrées (AES 128 bits).

14.7.4 Les concentrateurs doivent être munis de 16 canaux, pour permettre à l'installateur de choisir les ports voulus pour assurer des communications fiables avec chaque plaque de poignée ou mécanisme de verrouillage.

14.7.5 Le matériel doit utiliser des batteries non propriétaires facilement disponibles, et effectuer au moins 40000 opérations avant de devoir remplacer les batteries.

14.8 Les portes sans fil doivent être entièrement intégrées au système de contrôle d'accès et d'alertes anti-intrusion central, comme décrit ci-dessous :

14.8.1 Le système doit utiliser des cartes Mifare sans contact standard, comme toutes les portes en ligne.

14.8.2 Les données opérationnelles doivent être transférées automatiquement entre le système de sécurité intégré et les portes sans fil, sans intervention de l'opérateur. Données nécessaires :

(a) alerte de charge basse d'une batterie (plusieurs niveaux);

(b) activités d'accès pour toutes les portes;

(c) données sur les cartes désactivées;

(d) toute modification aux droits d'accès des titulaires de carte.

14.8.3 La plaque de poignée de porte doit être compatible avec le mécanisme de verrouillage, et doit tenir compte de :

(a) la taille de la poignée;

(b) l'angle de rotation de la poignée.

14.9 Le personnel du client doit pouvoir effectuer la maintenance de base du matériel (remplacement des piles, changement de la configuration de base) après avoir reçu des directives minimales.

14.10 L'outil de maintenance de l'installateur doit communiquer avec chaque concentrateur sans fil et lui permettre de configurer, de gérer et de commander chaque porte indépendamment du système de contrôle d'accès.

15 Intégration du système

15.1 Le système doit prendre en charge le protocole OPC (*OLE for Process Control*) afin de présenter une interface ouverte pour l'intégration avec les systèmes de gestion des bâtiments et installations et les systèmes d'information de gestion.

15.2 L'interface OPC (alarmes et événements) doit permettre aux clients OPC tiers de s'inscrire pour recevoir les alarmes et événements du système de sécurité.

15.2.1 Lorsqu'une alarme est traitée, le client d'alarmes et d'événements doit envoyer un message d'événement traité au système de sécurité pour qu'il traite aussi l'alarme.

15.3 Le système doit prendre en charge le protocole OPC afin de présenter une interface ouverte pour signaler l'état des composants du système à un client OPC externe (accès aux données).

15.4 L'interface OPC doit permettre aux clients OPC tiers de générer des dérogations visant les composants du système, y compris mais sans s'y limiter des dérogations aux zones d'alarme et d'accès.

15.5 Le système doit permettre l'importation, l'exportation et la synchronisation continuelles, par échange de données XML, des données provenant d'autres applications directement dans la base de données des titulaires de carte, soit en ligne, en temps réel, soit par lots. Une trousse de développement doit être librement accessible pour permettre de mettre cela en œuvre facilement.

15.6 Le système doit permettre la mise à jour, par échange de données XML, des horaires et échéanciers à partir d'applications tierces directement dans la base de données des titulaires de carte, soit en ligne, en temps réel, soit par lots. Une trousse de développement doit être librement accessible pour permettre de mettre cela en œuvre facilement.

15.7 Le système doit présenter une interface applicative (API) pour y intégrer des systèmes tiers.

15.7.1 Cette interface applicative doit être présente dans les CIP, pour que des signaux de systèmes tiers agissent comme entrées du système, et que les CIP puissent déclencher des actions directement dans les systèmes tiers.

15.8 L'accès par protocoles OPC ou XML doit être géré et enregistré à titre d'« événement d'opérateur ».

15.9 Le système doit prévoir un mécanisme d'exportation en temps réel des données d'alarme ou d'événement vers des systèmes tiers par chaînes de caractères adaptables, afin de commander les applications tierces.

15.10 Le système doit prendre en charge les événements provenant d'une ou de plusieurs applications tierces et les afficher ainsi que leur état dans les fenêtres d'événement ou d'alarme.

15.11 Le système doit gérer indifféremment les événements de systèmes tiers et les entrées connectées directement aux CIP.

16 Lecteurs de contrôle d'accès

Les technologies des lecteurs de contrôle d'accès sera précisée plus loi. Ces lecteurs doivent le cas échéant répondre aux spécifications suivantes :

16.1 Les spécifications suivantes visent les technologies 125 kHz et Mifare :

16.1.1 Le lecteur de cartes doit intégrer un signal sonore et des voyants à DEL rouge et vert, afin de fournir une rétroaction aux utilisateurs.

16.1.2 Le signal sonore sera différent selon que :

(a) l'accès est accordé;

(b) l'accès est refusé;

(c) l'accès exige la lecture d'une 2^{e} carte, si l'accès par deux cartes ou le mode d'escorte a été activé.

16.1.3 Un voyant rouge allumé indique que la porte est verrouillée.

16.1.4 Un voyant rouge clignotant indique que l'accès est refusé.

16.1.5 Un voyant vert allumé indique que l'accès à la porte est libre.

16.1.6 Un voyant vert clignotant indique que l'accès est accordé.

16.1.7 Les lecteurs doivent disposer d'une cote de protection contre les intempéries d'au moins IP68.

16.1.8 Les lecteurs doivent disposer d'une cote de résistance aux chocs d'au moins IK07.

16.1.9 Il faut installer dans les situations suivantes un boîtier résistant au vandalisme ayant une cote de résistance aux chocs d'au moins IK08.

(a) Il faut fixer au mur les couvercles anti-vandalisme par des vis inviolables.

(b) Les couvercles anti-vandalisme doivent avoir des rebords biseautés, pour empêcher quiconque de s'en servir pour escalader les murs.

(c) Toutes les surfaces extérieures doivent être biseautées et être exemptes de parties saillantes afin de répondre aux exigences anti-pendaison.

16.1.10 Les lecteurs doivent produire un signal de bon fonctionnement, pour que les CIP relèvent toute perte de communication et déclenchent alors une alarme.

16.1.11 Les lecteurs doivent accepter les accusés-réception des données provenant du CIP puis cesser d'envoyer ces données.

16.1.12 Chaque lecteur doit s'identifier auprès du système de contrôle central à l'aide d'un descripteur unique, clair et simple. Ce descripteur doit compter au moins 60 caractères.

16.1.13 Tout pavé numérique spécifié doit :

(a) être entièrement intégré au lecteur;

(b) être rétroéclairé;

(c) intégrer un écran à DEL rétroéclairé indiquant :

i. une carte est requise;

ii. il faut entrer un NIP;

iii. l'accès est refusé;

iv. l'alarme anti-intrusion est activée;

v. l'alarme anti-intrusion est désactivée;

vi. l'accès est libre;

vii. une 2^{e} carte est requise.

16.1.14 Le pavé numérique doit comprendre :

(a) des touches numériques standard, de 0 à 9;

(b) une touche CE (réinitialiser la saisie);

(c) une touche IN (entrée);

(d) trois touches de fonction (F1, F2 et F3).

16.2 Spécifications des technologies Mifare :

16.2.1 Il ne faut identifier les cartes d'accès par leurs numéros de série (CSN) qu'avec l'approbation de l'expert-conseil.

16.2.2 Le lecteur doit lire l'identificateur des cartes de tout secteur, de 1 à 15, tel que configuré, et identifier le secteur précis du lecteur par l'adresse MAD.

16.2.3 Les lecteurs doivent prendre en charge le chiffrement robuste décrit plus loin dans les présentes.

19. Les lecteurs livrés doivent prendre en charge plusieurs technologies, notamment Wiegand 125 kHz, Mifare, Bluetooth et les communications en champ proche (NFC).

17 Autodécouverte des lecteurs d’accès et communications

17.1 Les lecteurs doivent disposer d’un numéro de série unique.

17.2 À leur connexion à un CIP, les lecteurs doivent communiquer leur numéro de série au système de contrôle central.

17.3 Toute tentative de remplacer sans autorisation un lecteur sur le terrain auquel un CIP a attribué une fonction doit déclencher une alarme.

17.4 Les CIP et les lecteurs doivent communiquer à un débit d’au moins 1 Mbit/s.

17.5 Toute session de communication de données entre les CIP et les lecteurs doit s’établir par échange de certificats utilisant des clés de chiffrement elliptique d’au moins 256 bits.

17.6 Toute communication de données entre les CIP et les lecteurs doit utiliser un chiffrement AES d’au moins 128 bits.

18 Lecteurs de contrôle d'accès longue portée

18.1 Les exigences visant les lecteurs de contrôle d'accès longue portée seront précisées dans des documents joints. Le cas échéant, ces lecteurs doivent répondre aux spécifications suivantes.

18.2 Le lecteur doit être installé dans un boîtier résistant au vandalisme dont la cote de protection est d'au moins IP65.

18.3 Le lecteur doit avoir une portée de 10 m (33 pi).

18.4 Le lecteur doit pouvoir lire une étiquette ou un amplificateur passant dans le champ de lecture à une vitesse pouvant atteindre 200 km/h (125 MPH).

18.5 Ces lecteurs doivent prendre en charge des canaux multiples, afin de permettre à au moins 32 lecteurs de fonctionner à proximité les uns des autres.

18.6 Le lecteur doit lire les cartes d'accès et les jetons, tels que définis à la section 0 ci-dessous, à l'aide d'une étiquette ou d'un amplificateur associé.

18.7 Il faut associer temporairement la carte d'accès ou le jeton à l'étiquette ou à l'amplificateur pour transmettre les données de la carte ou du jeton au lecteur longue portée.

18.8 Le transfert des données de la carte d'accès ou du jeton, par l'étiquette ou l'amplificateur, puis au lecteur et au système, doit être transparent pour l'utilisateur.

18.9 Chaque étiquette ou amplificateur doit transmettre au lecteur un code d'identification unique.

18.10 La décision d'accorder ou de refuser l'accès doit pouvoir être fondée sur la combinaison d'une carte d'accès valide associée à une étiquette ou un amplificateur valide. On doit par exemple ne pouvoir accorder l'accès qu'à un conducteur (code d'identification de titulaire) dans un véhicule approuvé (code d'identification de l'amplificateur).

19 Cartes d'accès et jetons

19.1 Les jetons d'accès (cartes et autres dispositifs) choisis pour ce projet doivent utiliser des technologies compatibles avec celles des lecteurs, spécifiés séparément, mais en association avec la présente spécification.

19.2 La taille des cartes d'accès doit être celle des cartes de crédit (pas plus grandes que la taille CR-80), et on doit pouvoir les imprimer par sublimation à la teinture ou y coller une étiquette adhésive imprimée par ce procédé.

19.3 Toutes les cartes doivent être conformes aux normes ISO.

19.4 Outre les cartes en format CR-80, des jetons de véhicule et des transpondeurs sur porte-clés doivent aussi être proposés le cas échéant.

19.4.1 Les jetons d'accès doivent :

(a) prendre en charge des numéros de carte jusqu'à 2008 bits;

(b) si un format de numéro de carte propriétaire est proposé, il doit inclure :

i. un code de site unique qui n'est utilisé dans aucun autre système au monde;

ii. un numéro d'identification unique d'au moins 7 chiffres;

iii. un numéro d'émission pour chaque numéro de carte; ainsi, on peut remplacer les cartes perdues sans réduire les données emmagasinées sur les cartes. Le système doit prendre en charge jusqu'à 15 numéros d'émission.

19.4.2 Le jeton de contrôle d'accès doit identifier le titulaire de manière unique auprès du système de contrôle d'accès.

19.4.3 Le jeton d'accès doit emmagasiner les données de contrôle d'accès dans un format sécurisé, comme le décrivent ci-dessous les sections 22, 23 et 24.

19.4.4 La transmission des données entre le jeton d'accès et le lecteur de proximité doit se faire dans un format sécurisé, comme le décrivent ci-dessous les sections 22, 23 et 24.

19.4.5 La carte d'accès ou le jeton ne doivent pas afficher les données de chiffrement du contrôle d'accès.

19.4.6 Des mécanismes de blocage doivent empêcher le déchiffrement des données de contrôle d'accès stockées sur la carte par tout dispositif facilement accessible.

19.4.7 Des mécanismes de blocage doivent aussi empêcher la copie des données de contrôle d'accès stockées sur la carte par tout dispositif facilement accessible. Le soumissionnaire doit décrire les mécanismes utilisés.

19.4.8 Les cartes et jetons d'accès doivent pouvoir être chiffrés par le fournisseur selon les spécifications du client communiquées avec la commande. La livraison de cartes ou de jetons dont les numéros de carte sont établis par le fabricant n'est pas acceptable.

19.4.9 Les cartes et jetons doivent pouvoir être configurés pour que le titulaire puisse leur attribuer un numéro d'identification personnel (NIP) de son choix; cette exigence doit être compatible avec l'exigence indiquée au point 21.4.8 visant une carte ou un jeton tirés du stock, tel que défini ci-dessus.

19.4.10 Le soumissionnaire doit prévoir la livraison du matériel et des logiciels de chiffrement voulus pour que le client puisse chiffrer sur place ses propres cartes ou jetons.

19.5 Le système doit permettre de chiffrer des cartes ou des jetons par lots de quantité arbitraire.

20 Technologie Mifare Plus

20.1 Les cartes doivent intégrer la technologie Mifare Plus.

20.2 Le numéro de carte doit être attribué spécifiquement à la carte. Ce ne doit pas être le numéro de série de la carte (CSN).

20.3 Les données chiffrées de la carte doivent être authentifiées par secteur sécurisé afin d'empêcher le clonage de la carte. Il faut utiliser un chiffrement AES à 128 bits.

20.4 Il faut livrer la variante Mifare Plus « S ».

20.5 Les données chiffrées de la carte doivent comprendre les données suivantes :

(a) le numéro de carte tel qu'attribué;

(b) un code propre au site composé de 32 caractères hexadécimaux;

(c) ce code hexadécimal de 32 caractères peut provenir d'une clé de sécurité spécifiée par le client.

20.6 Le chiffrement des cartes doit faire partie intégrante de leur production. Consultez la section 28, ci-dessous.

20.7 Le système doit permettre de préciser dans quel secteur de la carte est enregistré le numéro de la carte.

20.8 L'utilisateur doit pouvoir établir la clé de déverrouillage de secteur et la clé de déverrouillage Mifare MAD.

20.9 Là où l'on déploie plusieurs technologies de lecture, telles que définies dans les sections sur les autres technologies, on utilisera un chiffrement des cartes à passage unique.

21 Gestion des titulaires

21.1 Dans la structure de la base de données des titulaires de carte, le champ du nom doit être le champ principal de chaque enregistrement. Un code unique peut être utilisé comme clé d'appoint pour chaque enregistrement, mais l'opérateur ne doit pas devoir l'exiger pour identifier le titulaire. Le numéro de carte n'est pas acceptable comme clé.

21.2 Chaque CIP prendra en compte le nombre de titulaires établi aux points 11.8 et 11.9, ci-dessus.

21.3 Le système doit prendre en charge au moins 15 numéros d'émission par carte ou jeton, correspondant à ceux précisés ci-dessus au point 21.4.1 (b) (iii). Toute lecture d'une carte ou d'un jeton dont le numéro d'émission est erroné doit déclencher une alarme affichée au poste de l'opérateur.

21.4 Le système doit permettre de délivrer plus d'un jeton d'accès dont la description et le numéro diffèrent (comme carte d'accès, identification biométrique et jeton de véhicule) en n'utilisant dans la base de données qu'un seul dossier de titulaire.

21.5 Si l'identification biométrique est requise, les données dactyloscopiques doivent faire partie du dossier du titulaire.

21.6 Le dossier de titulaire doit aussi comprendre des champs pour le chiffrement et l'impression des cartes.

21.6.1 Les options de chiffrement et d'impression sont les suivantes :

(a) impression de la carte;

(b) impression du chiffrement;

(c) impression et chiffrement de la carte.

21.7 Il faut pouvoir associer les groupes d'accès aux titulaires par l'attribution tant des groupes d'accès aux titulaires que des titulaires aux groupes d'accès.

21.8 Le système doit prévoir au moins 64 champs de données « à caractère personnel » définissables par l'utilisateur; ces champs peuvent faire l'objet de rapports.

21.8.1 Ces champs de données personnelles doivent pouvoir être configurés selon l'un des types suivants :

(a) Texte — saisie de données sur le titulaire;

(b) Liste — choix à partir d'une liste d'étiquettes préétablie;

(c) Chiffre — données numériques;

(d) Date — saisie selon le format des dates du poste de travail;

(e) Valeur par défaut — une valeur par défaut est affectée au champ.

(f) Image — le champ ne peut contenir qu'une image.

(g) Courriel/mobile — adresse courriel ou numéro de téléphone (notifications).

21.8.2 On doit aussi pouvoir configurer ces champs comme :

(a) Champ obligatoire — il faut saisir des données dans ce champ;

(b) Valeur unique — les données saisies doivent être différentes de toutes les autres données de la carte;

(c) Aucune valeur par défaut — valeur par défaut désactivée.

21.8.3 Les champs de données personnels doivent prendre en charge l'application de règles d'exactitude des données; vérification d'adresses courriel ou du format d'un code d'employé, par exemple.

21.9 Le système doit prévoir un champ destiné à la saisie de notes ou de commentaires sur les cartes.

21.9.1 Ce champ doit prendre en charge les fonctions de retour à la ligne, d'ajout et de suppression de texte, ainsi que les fonctions Couper, Copier et Coller.

21.10 Le système doit permettre de regrouper ou de filtrer les comptes des titulaires, pour en modifier l'accès, créer des rapports et attribuer les droits d'opérateur.

21.11 La fenêtre de modification des comptes des titulaires doit pouvoir afficher (de façon facultative) les champs suivants :

(a) date de création du compte de titulaire;

(b) date de la dernière modification.

21.11.2 Afin de simplifier l'attribution des droits d'accès, le système doit permettre de regrouper les comptes en groupes d'accès qui partagent les mêmes droits d'accès et les mêmes champs de données par défaut.

21.11.3 Le système doit prévoir la saisie d'une date et d'une heure d'échéance automatique des cartes.

21.11.4 Le système doit prévoir un délai d'échéance automatique des cartes après une période d'inactivité pouvant atteindre 999 jours.

21.11.5 Le système doit permettre le réglage des dates et heures d'entrée en vigueur et d'échéance des droits d'accès d'un groupe donné à une zone précise.

21.12 On doit pouvoir régler l'entrée en vigueur et l'échéance des droits d'accès à une minute près.

21.13 Le système doit prendre en charge l'importation des données sur des titulaires choisis à partir d'autres systèmes et leur exportation vers d'autres bases de données, avec ou sans modification automatique.

21.14 Le système doit prendre en charge la modification globale des dossiers de cartes, plus précisément, les modifications suivantes :

(a) suppression de dossiers choisis;

(b) modification des champs de données personnelles;

(c) modification des caractéristiques des cartes;

(d) modification des droits d'accès;

(e) modification de la division du système à laquelle les enregistrements sont attribués.

21.15 Le système doit permettre l'enregistrement des modifications globales afin de les exécuter ultérieurement.

21.16 Le système doit prévoir une fenêtre qui dresse la liste des modifications globales (créations, sauvegardes et modifications; réussies, en attente ou échouées).

21.17 Les dossiers des cartes doivent prévoir un champ pour un code d'utilisateur personnel de 4 ou 6 chiffres, afin de permettre l'activation et la désactivation des alarmes.

21.18 Les dossiers des cartes doivent prévoir l'attribution des droits d'accès de gestion des opérateurs du système.

21.19 Un historique des modifications doit être associé à chaque dossier de titulaire : il doit énumérer toutes les modifications apportées et qui a fait chacune.

21.20 Le système doit prendre en charge l'historique des événements associés à chaque titulaire, c'est-à-dire utilisations récentes de la carte et modifications au dossier, et permettre de régler le nombre d'événements à afficher ou la période antérieure à couvrir. Il doit permettre de configurer une période ou un nombre différent d'événements pour différents opérateurs.

21.21 Le système doit permettre à l'opérateur de l'interroger selon n'importe quelle partie du prénom ou du nom du titulaire, dans n'importe quel ordre et séparés par un espace s'il saisit le prénom et le nom. Il doit présenter des résultats dès la saisie de trois caractères, et filtrer ces résultats dynamiquement selon les données saisies.

21.22 Le système doit permettre de configurer les champs de recherche du titulaire et les résultats des interrogations. Pour simplifier la gestion des titulaires, il doit permettre à des opérateurs différents d'utiliser des champs d'interrogation et d'afficher des résultats différents.

21.23 Le système doit permettre de configurer pour chaque opérateur les données affichées sur les titulaires selon toute sous-section de l'ensemble des données du dossier du titulaire (données personnelles, cartes, groupes d'accès, compétences, informations biométriques…). Il doit

permettre à des opérateurs différents de consulter des sous-sections différentes des données de titulaire.

21.24 Pour simplifier la gestion des titulaires, le système doit prendre en charge des agencements de données différents à l'écran, selon l'opérateur.

21.25 Le système doit permettre d'afficher et de modifier les informations sur les titulaires à partir d'un seul écran.

21.26 Selon leurs droits d'accès, les opérateurs doivent être en mesure de concevoir des affichages de gestion des titulaires de cartes selon la résolution de l'écran de chaque opérateur ou des opérateurs qui utilisent ces affichages, afin d'assurer une utilisation optimale des écrans.

21.27 Le système doit permettre de maximiser au besoin des données précises sur les titulaires. Un seul clic doit déclencher l'agrandissement d'une zone et le retour à l'affichage normal.

21.28 Le système doit permettre de gérer à partir du clavier seulement toutes les fonctions de gestion des titulaires.

22 Gestion des visiteurs

22.1 Le système doit prendre en charge les fonctions de gestion des visiteurs décrites dans la présente section.

22.2 Le système doit permettre de saisir à l'avance les coordonnées des visiteurs.

22.3 Le système doit permettre de saisir à l'avance les coordonnées de plusieurs visiteurs associés à une même visite.

22.4 Il doit permettre d'attribuer une escorte à chaque visiteur.

22.4.1 La fonction d'escorte est décrite aux sections 12.10 (f) et 30.7.1 (e) des présentes.

22.5 Les attributs associés aux visiteurs doivent être configurables, et définis comme obligatoires ou facultatifs; ils doivent comprendre :

(a) l'emplacement où les visiteurs sont attendus;

(b) la catégorie de visiteurs;

(c) la personne qu'ils doivent rencontrer;

(d) l'heure d'arrivée;

(e) l'heure de départ;

(f) les droits d'accès à leur accorder;

(g) une photo d'identité.

22.6 On doit pouvoir imprime les laissez-passer des visiteurs sur une imprimante d'étiquettes à la réception.

22.7 Le système doit permettre d'enregistrer les données nécessaires sur les visiteurs en prévision de visites ultérieures.

22.8 Le système doit enregistrer ces visites dans la base de données des événements système.

22.9 Le système doit déclencher une alarme si un visiteur ne sort pas à l'heure prévue.

22.10 Le système doit prendre en charge plus d'un poste de travail pour la gestion et l'accueil des visiteurs.

22.11 L'écran de gestion des visiteurs doit présenter un « instantané » des données sur les visiteurs :

(a) heure d'arrivée prévue;

(b) emplacement : sur place, départ prochain ou temporairement ailleurs;

(c) les laissez-passer des visiteurs toujours présents après leur départ prévu doivent être désactivés automatiquement après un délai préétabli.

22.12 Le système doit permettre de choisir les groupes de visiteurs en tant que groupes et de modifier globalement les données les touchant.

22.13 Les postes de travail de gestion et d'accueil des visiteurs doivent prendre en charge des macros système préconfigurées.

22.14 Les exigences visant les rapports sur les visiteurs sont décrites au point 39.13 des présentes.

23 Gestion des cartes d'identité avec photo

23.1 Le système doit intégrer les fonctions suivantes :

(a) saisir les photos de façon électronique;

(b) stocker les images dans la base de données du serveur,

(c) intégrer ces images à une carte d'identité préconçue à partir du système;

(d) produire une carte d'identité intégrée et complète dans les délais impartis.

23.2 Par « image », on entend au moins un des éléments suivants :

(a) photographie du titulaire de la carte;

(b) signature du titulaire, de la personne autorisée, ou des deux;

(c) empreinte dactylographique du titulaire.

23.3 Le logiciel système doit intégrer un moyen de concevoir les cartes sans devoir importer des fichiers d'arrière-plan à partir d'autres logiciels, mais cette possibilité doit également être disponible, notamment logos numérisés et autres images, au besoin.

23.4 Le système proposé doit saisir des photos couleur 24 bits et d'une résolution d'au moins 640 x 480 pixels à l'aide d'un matériel vidéo standard (norme TWAIN ou Direct Draw), ou encore d'un appareil photo numérique USB.

23.5 Le système doit permettre de rogner les images pour en optimiser la taille dans la zone souhaitée. La zone de recadrage doit être mobile et l'utilisateur doit pouvoir en régler la taille.

23.5.1 Les commandes du logiciel doivent être faciles à utiliser et on doit pouvoir, après réglage, appliquer ces mêmes réglages aux photos d'autres titulaires saisies ultérieurement.

23.6 Le système doit prévoir la saisie et le stockage de jusqu'à trois images par titulaire. On définit les images selon le point 26.2, ci-dessus.

23.7 Le système doit stocker les images en format JPEG compressé. L'opérateur doit pouvoir choisir facilement l'un de trois niveaux de compression réglables.

23.8 Le système proposé doit pouvoir importer des images, pour la conception des cartes ou des photos de titulaires, à partir des formats suivants au moins :

(a) JPEG;

(b) Windows BMP;

(c) Compression LEAD.

23.9 Le logiciel de conception des cartes doit permettre d'incorporer, de stocker, d'imprimer et d'afficher les données de codes à barres; il doit prendre en charge les formats de codes à barres suivants :

(a) EAN 13 et 128;

(b) CUP A et E;

(c) Code 39 et 128;

(d) 2 de 5 entrelacés;

(e) Codabar;

(f) Telepen.

23.10 Le système doit intégrer un logiciel de conception des cartes. Les systèmes proposant un logiciel de conception distinct où il faut ensuite importer les images créées ne sont pas acceptables, mais le système proposé doit aussi prendre en charge l'importation d'images, conformément au point 28.8.

23.11 Le volet de conception des cartes doit prendre en charge jusqu'à 16,7 millions de couleurs, et intégrer une palette de couleurs personnalisable.

23.12 La conception des cartes doit prendre en charge la fonction « glisser-déposer » à l'aide d'une souris.

23.13 Le système doit pouvoir utiliser toutes les polices courantes de traitement de texte, et doit permettre de manipuler le texte : taille; justification à gauche, à droite et au centre; et texte gras, souligné et italique.

23.14 La taille des diverses photos des titulaires à intégrer aux cartes doit être réglable (pleine taille : 30 x 40 mm). Leurs dimensions doivent être entièrement configurables par l'utilisateur, c'est-à-dire au minimum du quart (25 %) au double (200 %) de la pleine taille; le système doit intégrer l'ajustement automatique du rapport largeur-hauteur dans toute la gamme de dimensions.

23.15 Le système doit pouvoir imprimer les images et les données sur n'importe quelle imprimante standard prise en charge par Windows.

23.16 Le système doit produire en une seule étape des cartes d'identité avec photo à l'aide d'une imprimante sur carte rigide compatible avec Windows. Les systèmes proposant une production en plusieurs étapes, le laminage à chaud ou la production à chaud et sous pression ne sont pas acceptables.

23.17 Le système doit pouvoir imprimer directement sur les cartes à piste magnétique Hi-Co, les cartes à effet Wiegand et les cartes de proximité sans endommager les technologies intégrées aux cartes.

23.18 Le système doit pouvoir imprimer les cartes en format paysage ou portrait; de même, les codes à barres doivent pouvoir être orientés verticalement ou horizontalement sur les cartes imprimées.

24 Gestion des opérateurs du système

24.1 Les opérateurs doivent être membres de groupes d'opérateurs.

24.2 Seuls les opérateurs principaux désignés doivent pouvoir nommer les opérateurs et tenir à jour les groupes d'opérateurs.

24.3 Les fonctions d'attribution des droits d'accès des opérateurs et d'ajout d'opérateurs aux groupes doivent être d'utilisation facile.

24.4 Le système doit limiter l'accès des opérateurs par justificatifs : nom d'utilisateur et mot de passe.

24.5 La gestion des mots de passe doit se faire par changement imposé ou non restrictif. En cas de changement imposé, les options doivent inclure :

(a) une longueur d'au moins 9 caractères;

(b) majuscules ou minuscules;

(c) caractères alphabétiques ou numériques;

(d) changement imposé après une période réglable allant jusqu'à 365 jours;

(e) l'enregistrement d'au moins 8 mots de passe utilisés auparavant afin d'en empêcher la réutilisation.

24.6 Le système doit également prendre en charge la connexion par carte Mifare.

24.7 Chaque opérateur doit pouvoir modifier son propre mot de passe, mais pas celui des autres.

24.8 Le système doit déconnecter automatiquement tout opérateur après une période d'inactivité réglable allant jusqu'à 60 minutes.

24.9 Il doit être possible de configurer le système de manière à n'autoriser qu'une seule connexion par opérateur.

24.10 Le système doit permettre de régler l'accès des opérateurs aux fonctions du menu système, y compris l'affichage des champs de données personnelles des titulaires, des notes personnelles et des images.

24.11 Le système doit permettre de restreindre l'accès des opérateurs aux titulaires de carte en fonction des divisions du système.

24.12 Le système doit permettre de régler les droits d'accès des opérateurs en fonction des divisions auxquelles ils ont accès. Par exemple, « utilisateur avancé » dans la division 1; « affichage seulement » dans la division 2 et « aucun accès » dans la division 3.

24.13 Les options de menu auxquelles un opérateur n'a pas accès doivent être grisées ou invisibles.

25 Contrôle et gestion des ascenseurs

25.1 Le système doit intégrer la commande des ascenseurs. L'équipement de commande des ascenseurs doit communiquer avec le même système de contrôle central que les lecteurs de cartes.

25.2 Le système de commande des ascenseurs doit intégrer des lecteurs de cartes dans chaque cabine d'ascenseur qui communiquent avec l'équipement de commande d'ascenseur monté dans ou à proximité de la salle des machines de l'ascenseur. Le type de lecteur doit être conforme à celui spécifié pour les portes de contrôle d'accès.

25.3 Le système de commande des ascenseurs doit être capable de commander l'accès simultanément et indépendamment dans plusieurs cages d'ascenseur.

25.4 Le système de commande des ascenseurs doit incorporer des renseignements spécialisés et une base de données locale des détenteurs de cartes autorisés.

25.5 Chaque lecteur d'ascenseur doit s'identifier auprès du système de contrôle central à l'aide d'un descripteur unique, clair et simple. Ce descripteur doit compter au moins 60 caractères.

25.6 Toute interruption des communications d'un lecteur avec la commande d'ascenseur et le retrait de tout lecteur d'un ascenseur doit déclencher une alarme.

25.7 La commande d'ascenseur doit vérifier l'accès en fonction de TOUS les critères suivants :

(a) Code d'installation

(b) Autorisation de la carte dans la base de données

(c) Numéro d'émission correct

(d) Accès autorisé à l'étage

(e) Heure de la journée autorisée

(f) NIP correct (si sa saisie est exigée)

25.7.2 Le système doit pouvoir modifier automatiquement et en tout temps le mode d'accès de tout ascenseur, selon les commandes reçues du serveur de contrôle central. Le système doit comprendre les modes d'accès suivants :

(a)	Accès libre	Le bouton de l'étage visé est déverrouillé; aucune lecture de carte n'est nécessaire.
(b)	Accès sécurisé	L'étage est verrouillé; une carte valide est nécessaire pour entrer, et l'accès à l'étage se verrouille après l'accès.

(c)	Accès sécurisé avec NIP	L'étage est verrouillé; une carte *et* un NIP valides sont nécessaires pour entrer, et l'accès à l'étage se verrouille après l'accès.
(d)	Autorisation double	L'accès est accordé si deux cartes différentes et valides sont présentées dans un délai préétabli.
(e)	Escorte	L'accès est accordé après lecture d'une carte d'un titulaire désigné.
(f)	NIP partagé	L'opérateur du système choisit le NIP de 4 chiffres et configure le système en conséquence. L'accès à l'étage est accordé si on entre ce NIP au pavé numérique, suivi de la touche « Enter ».

25.7.3 Le système de commande des ascenseurs doit pouvoir régler individuellement le mode d'accès de chaque étage, tel que décrit ci-dessus.

25.7.4 Le système de contrôle central doit pouvoir sécuriser chaque étage indépendamment, par des commandes transmises au système de commande des ascenseurs.

25.7.5 Le système de contrôle central doit permettre à un opérateur d'outrepasser temporairement les règles d'accès visant un étage précis.

25.7.6 L'interruption des communications avec le système de contrôle central ne doit en rien dégrader le rendement du système de commande des ascenseurs.

25.8 Si on spécifie une interface de bas niveau :

25.8.1 L'interface entre l'équipement de commande des ascenseurs du système d'accès et l'équipement de commande des ascenseurs proprement dit doit être assurée par des relais secs.

25.8.2 La tension d'alimentation de ces relais ne doit pas dépasser 24 volts c.a. ou c. c.

25.8.3 Le système de commande des ascenseurs doit prévoir un relais pour chaque étage desservi par chaque ascenseur. Ce relais doit servir d'interface avec l'équipement de commande des ascenseurs.

25.8.4 Une entrée doit être prévue pour chaque étage et chaque ascenseur afin d'indiquer l'étage choisi. À l'activation de toute entrée, tous les relais doivent revenir à l'état sécurisé.

25.9 Si on spécifie une interface plus générale :

25.9.1 L'interface entre l'équipement de commande des ascenseurs du système d'accès et l'équipement de commande des ascenseurs proprement dit doit être assurée par une connexion RS-232.

25.9.2 L’équipement de commande des ascenseurs doit signaler au système l’étage choisi par tout titulaire de carte.

26 Système d'alarme anti-intrusion

26.1 Le système doit comprendre un système d'alarme anti-intrusion pleinement fonctionnel.

26.2 Toutes les entrées du système doivent pouvoir servir d'entrées d'alarme d'intrusion afin de permettre d'y brancher des capteurs de détection d'intrusion.

26.3 Toutes les sorties, où qu'elles soient le système, doivent pouvoir servir d'alarme anti-intrusion, pour déclencher des sirènes à distance, par exemple.

26.4 L'armement et le désarmement du système de détection d'intrusion doivent par lecteurs de cartes, modules d'activation à distance ou interrupteurs à clé.

26.5 La zone d'alarme anti-intrusion et la zone d'accès d'une aire précise doivent être traitées de façon distincte.

26.6 Le système d'alarme anti-intrusion doit intégrer une fonction de dépendance : une zone d'alarme ne peut pas être armée tant que les zones d'alarme « dépendantes » ne sont pas toutes armées.

26.6.1 Si une zone d'alarme est armée et que la porte d'accès connexe est sécurisée :

(a) Pour obtenir l'accès à la zone, un titulaire doit disposer des droits de désarmement de la zone d'alarme anti-intrusion *et* des droits d'accès à cette zone.

(b) L'accès est refusé si la carte n'est pas autorisée à désactiver la zone d'alarme *ou* si elle n'est pas autorisée à accéder à cette zone.

26.6.2 Si la zone d'alarme est désarmée et que la porte d'accès connexe est sécurisée :

(a) L'accès est accordé si un titulaire ne dispose que du droit d'accès à cette zone.

(b) L'accès est refusé si la carte n'est pas autorisée à accéder à cette zone.

26.6.3 En fonctionnement normal, après la présentation d'un jeton autorisé et l'autorisation d'accès, la zone d'alarme doit rester désarmée après le déverrouillage de la porte.

26.6.4 Le système doit permettre d'armer automatiquement la zone après une période réglable préétablie.

26.7 Si elle est exigée, la surveillance des alarmes doit se faire par connexion avec les stations centrales de surveillance des alarmes par des communicateurs numériques de format « Contact ID » connectés directement aux panneaux des CIP.

26.7.1 Un CIP doit pouvoir gérer les alarmes d'un autre CIP muni d'un communicateur numérique (communications pair-à-pair).

26.7.2 Les communicateurs numériques doivent être en mesure de signaler des alarmes provenant de tout le système, indépendamment du serveur de contrôle central.

26.7.3 Le système doit signaler et enregistrer toute l'activité du communicateur numérique et la raison de toute interruption des communications.

26.7.4 Le système doit prendre en charge jusqu'à deux composeurs d'appoint, sur des contrôleurs différents, pour assurer une relève automatique si le communicateur numérique désigné ne fonctionne pas comme prévu si une alarme est déclenchée.

26.8 Le système doit permettre d'attribuer les titulaires à des groupes on peut attribuer toute combinaison des droits suivants touchant l'utilisation du système d'alarme d'intrusion :

(a) désarmer les zones d'alarme d'intrusion;

(b) armer les zones d'alarmes d'intrusion;

(c) consulter l'état des alarmes et des entrées sur un module d'activation à distance;

(d) accuser réception des alarmes;

(e) dériver des entrées;

(f) forcer l'armement des zones d'alarme;

(g) isoler automatiquement les zones d'alarme.

27 Tours de garde

27.1 Le système doit prendre en charge plusieurs tours de garde.

27.2 Les points de contrôle doivent être des lecteurs de cartes aux portes, des entrées et sorties, des blocs logiques ou des systèmes externes.

28 Fonctions des circuits d'entrée/sortie

28.1 Il faut connecter les circuits d'entrée aux CIP conformément à la section « Matériel sur place ».

28.2 Les entrées provenant de dispositifs de détection couvrant la même région à des fins de contrôle doivent être regroupées en zones d'alarme. Les zones d'alarme doivent être dans l'un de quatre états et doivent traiter les alarmes différemment selon cet état. Les deux premiers états doivent être Armé et Désarmé. Le système doit permettre de nommer à d'autres fins les deux autres états sur le serveur de contrôle central, pour les essais de maintenance, par exemple.

28.3 Le système doit permettre d'attribuer les priorités d'alarme à n'importe quel des quatre états d'entrée.

28.4 Le système doit prévoir des délais aux entrées et aux sorties pour l'armement et le désarmement des alarmes.

28.5 Le délai d'entrée doit être réglable de 0 à 5 minutes par incréments d'une seconde.

28.6 Un avertissement sonore facultatif doit pouvoir être activé pendant le délai d'entrée (entre le déclenchement de l'alarme et la modification de l'état de la zone). Il doit être possible de désigner des lecteurs de cartes et des modules d'activation à distance précis qui émettent les signaux sonores d'avertissement de délai d'entrée. Des relais de sortie choisis doivent aussi pouvoir fonctionner pendant le délai d'entrée, ce qui permet de raccorder des mécanismes d'avertissement sonore appropriés là où il le faut.

28.7 Un délai de sortie doit être prévu pour les groupes d'entrées de sorte qu'un changement d'état d'une zone retardée de sortie soit retardé de 5 secondes à 5 minutes par pas d'une seconde par le délai de sortie réglable.

28.8 Un avertissement sonore facultatif doit pouvoir être activé pendant le délai d'entrée sortie (entre le déclenchement de l'alarme et la modification de l'état de la zone). Il doit être possible de désigner des lecteurs de cartes et des modules d'activation à distance précis qui émettent les signaux sonores d'avertissement de délai de sortie. Des relais de sortie choisis doivent aussi pouvoir fonctionner pendant le délai d'entrée, ce qui permet de raccorder des mécanismes d'avertissement sonore appropriés là où il le faut. Cela doit s'appliquer tant à la modification manuelle de l'état d'une zone qu'à la modification automatique; dans ce dernier cas, le délai de sortie et l'avertissement sonore donnent aux personnes travaillant après les heures de travail normales le temps de désarmer les alarmes ou de quitter le bâtiment.

28.9 Le système doit inclure un événement d'escalade d'alarme. Le nouvel événement doit correspondre à l'alarme d'origine, mais avoir une priorité différente (généralement plus élevée) et peut exiger des relais d'alarme différents pour fonctionner.

28.10 Les alarmes visées par l'escalade doivent pouvoir être affichées dans une fenêtre spécialement prévue à cet effet.

28.11 Les alarmes doivent pouvoir être déclenchées dans les cas suivants :

(a) escalade s'il n'y a pas d'accusé réception de l'alarme après (X) secondes;

(b) escalade si l'état reste inactif pendant (X) secondes;

(c) escalade si (X) alarmes sont déclenchées dans une zone;

(d) escalade si deux événements sont déclenchés à partir du même point en moins de (X) secondes;

(e) escalade si deux événements sont déclenchés à partir de points différents de la même zone en moins de (X) secondes.

28.12 Il doit être possible d'armer et de désarmer automatiquement les alarmes en fonction de l'heure.

28.13 Le système doit permettre de modifier l'état d'une zone en fonction d'événements comme la lecture d'une carte ou l'actionnement d'un interrupteur à clé connecté à une entrée.

28.14 Le système doit permettre aux titulaires autorisés d'armer et de désarmer les zones d'alarme en :

(a) présentant leur carte et entrer un NIP sur un panneau d'alarme.

(b) présentant une carte valide à un lecteur associé à la zone d'alarme deux fois au cours d'une période déterminée (lecture double).

28.15 Un module d'activation à distance doit pouvoir armer et désarmer plusieurs zones d'alarme.

28.16 Toutes les alarmes doivent être transmises au système de contrôle central au plus tard 4 secondes après leur signalement à l'appareil distant sur le terrain.

28.17 Tous les événements d'alarme doivent être affichés dans une liste d'alarmes.

28.18 Les icônes interactives du plan de site doivent permettre d'afficher tous les événements d'alarme; leur état visuel et sonore doit pouvoir indiquer le déclenchement d'alarmes.

28.19 Tous les événements d'alarme signalés au système de contrôle central doivent être horodatés deux fois : l'heure de leur déclenchement et l'heure de leur enregistrement par le système de contrôle central.

28.20 Un niveau d'alarme réglable par l'utilisateur doit pouvoir être attribué à chaque événement d'alarme. Le système doit ainsi prévoir au moins 8 niveaux de priorité d'alarme plus un niveau pour les événements non pertinents et pouvant être ignorés.

28.21 Le système doit permettre d'attribuer un avertissement sonore différent à chaque niveau de priorité d'alarme.

28.22 Les alarmes entrantes doivent être présentées dans la liste d'alarmes en fonction de leur priorité attribuée, priorité la plus élevée en haut. Les alarmes de priorité identique doivent être présentées en ordre chronologique.

28.23 La priorité des alarmes dans la liste doit pouvoir être indiquée par une couleur définie par l'utilisateur.

28.24 Les alarmes identiques déclenchées pendant une période prédéfinie doivent être signalées par une seule alarme qui indique le nombre d'alarmes identiques.

28.25 Le système de contrôle central doit pouvoir réattribuer à tout moment la priorité de toute alarme déclenchée. Cela permet d'attribuer à une même alarme une priorité basse pendant les heures de travail et une priorité élevée à l'extérieur de ces heures.

28.26 Le système doit permettre de désigner une entrée, notamment détecteur de fumée, d'incendie ou de gaz, comme « entrée d'évacuation » qui met automatiquement certaines portes du site en mode d'accès libre.

28.27 Les opérateurs doivent traiter les alarmes en deux étapes, comme suit :

28.27.1 Accuser la réception de l'alarme.

(a) Une alarme ainsi reçue doit rester dans la liste d'alarmes, et être facilement identifiable comme reçue, mais non encore traitée.

(b) Le serveur de contrôle central doit enregistrer l'accusé réception de l'alarme dans son journal des activités. Une alarme est reçue par l'opérateur quand il clique le bouton « Accuser réception » de la fenêtre d'affichage des alarmes.

(c) Le système doit identifier comme nouvelle alarme une deuxième alarme provenant de la même source que l'alarme reçue.

28.27.2 Traiter l'alarme.

(a) Une alarme traitée doit être supprimée de la liste d'alarmes.

(b) Le serveur de contrôle central doit enregistrer le traitement de l'alarme dans son journal des activités. Une alarme est traitée par l'opérateur quand il clique le bouton « Traiter » de la fenêtre d'affichage des alarmes.

28.28 Le système doit permettre à un opérateur de choisir dans la liste plusieurs alarmes contiguës ou non contiguës afin d'ajouter une note, d'accuser réception de ces alarmes ou de les traiter d'un coup.

28.29 La liste des alarmes doit comprendre les champs obligatoires suivants : l'heure, la priorité et l'état de l'alarme.

28.30 Le système doit permettre à un opérateur disposant des droits d'accès appropriés de configurer l'affichage dans la liste d'alarmes de n'importe lequel des champs supplémentaires suivants ainsi que son ordre de tri :

(a) message d'alarme complet;

(b) nom du titulaire de carte connexe;

(c) nom de l'opérateur ayant accusé réception de l'alarme;

(d) zone de l'alarme;

(e) source de l'alarme;

(f) zone d'accès connexe;

(g) type d'événement;

(h) groupe d'événement;

(i) division de la source de l'alarme;

(j) nombre d'alarmes.

28.31 L'opérateur doit pouvoir trier la liste d'alarmes par n'importe lequel des champs affichés.

28.32 Le système doit afficher en tout temps un résumé des alarmes, triées par priorité, visible par l'opérateur de surveillance et mis à jour dynamiquement au fur et à mesure que de nouvelles alarmes apparaissent ou que des alarmes existantes sont déclenchées.

28.33 Le résumé des alarmes doit indiquer si des alarmes d'une priorité donnée n'ont pas fait l'objet d'un accusé réception.

28.34 Le système doit permettre de configurer des listes d'alarmes filtrées. On doit pouvoir filtrer les listes d'alarmes selon toute combinaison de divisions choisies, de l'état d'escalade ou de la priorité de l'alarme.

28.35 Le système doit permettre de configurer et d'afficher des informations différentes à l'opérateur de surveillance selon le type d'alarme.

28.36 Les alarmes de porte ouverte trop longtemps doivent être affichées avec des informations choisies et configurables, notamment photo et coordonnées de la personne qui a laissé la porte ouverte (dernier accès réussi).

28.37 Les alarmes visant les titulaires doivent afficher automatiquement les événements récents et des données choisies (nom, photo, détails, etc.) de la personne ayant déclenché l'alarme.

28.38 Le système doit empêcher de traiter et de supprime de la fenêtre des alarmes tant que la cause de l'alarme n'a pas été réglée et que l'alarme n'est pas revenue à l'état normal.

28.39 Le système doit intégrer des instructions préprogrammées à l'intention des opérateurs pour qu'ils sachent comment accuser réception et traiter chaque alarme.

28.39.1 Ces instructions doivent respecter les critères suivants :

(a) Le système doit permettre de préprogrammer les instructions par défaut et de les appliquer automatiquement à tous les événements courants, comme toutes les saisies de NIP erronées sur tous les lecteurs.

(b) Le système doit permettre de programmer et d'appliquer des instructions à des alarmes individuelles.

(c) Pendant la création des instructions programmées, un tableau des noms des personnes-ressources, numéros de téléphone et autres renseignements temporaires, mais souvent utilisés doit être affiché, et les données affichées doivent pouvoir être intégrées aux instructions d'alarme à partir d'une liste de choix.

(d) Toute mise à jour des éléments de cette liste doit aussi mettre automatiquement à jour les instructions d'alarme connexes.

28.39.2 Le système doit prévoir la mise en forme du libellé de l'instruction d'alarme à l'aide de fonctions courantes de mise en forme, y compris, mais sans s'y limiter :

(a) gras, italique et souligné;

(b) couleur du texte;

(c) justification à gauche, au centre et à droite;

(d) puces;

(e) types et tailles de polices Windows standard.

28.39.3 Il doit être possible de copier et de coller les instructions d'alarme d'un événement à l'autre.

28.40 La fenêtre des alarmes doit permettre à l'opérateur de saisir un commentaire. Ce commentaire doit être horodaté par le système et enregistré en relation avec cet événement dans la piste de vérification.

28.40.1 Une liste prédéfinie de réponses d'alarme doit au besoin être mise à la disposition des opérateurs pour qu'ils y choisissent la réponse appropriée à une alarme. Les réponses aux alarmes doivent être configurables par l'utilisateur selon les besoins du site.

28.40.2 Le système doit attribuer aux touches de fonction du clavier (F1 à F8) les 8 premiers messages de réponse d'alarme, afin de saisir au besoin le message connexe automatiquement.

28.41 Le système doit intégrer des relais de sortie activés en réponse au déclenchement d'alarmes. Voici les fonctions requises :

(a) Activation et verrouillage d'un relais en réponse à une alarme. Le relais reste verrouillé jusqu'à ce que l'alarme soit traitée.

(b) Activation d’un relais pendant une période réglable, après quoi le relais est désactivé.

(c) Activation d’un relais en parallèle avec celle d’une entrée d’alarme.

28.42 Le système doit intégrer des relais activés ou désactivés selon un échéancier, pour contrôler l’éclairage ou le chauffage, ou encore verrouiller ou déverrouiller automatiquement des portes non surveillées.

29 Modules d'activation à distance

29.1 Le système doit intégrer des modules d'activation à distance (MAD) qui rendent possibles les fonctions de pavé numérique décrites ci-dessous.

29.2 La connexion aux fonctions du MAD doit se faire par :

(a) un code d'utilisateur (NIP) attribué à chaque titulaire de carte;

(b) lecture d'une carte à un lecteur associé au MAD;

(c) lecture d'une carte valide à un lecteur associé au MAD et saisie d'un NIP à 4 ou 6 chiffres sur ce module.

29.3 Les titulaires de cartes autorisés doivent pouvoir :

(a) activer et désactivez toutes les zones d'alarme d'intrusion ou seulement celles attribuées à un MAD précis;

(b) accuser réception des alarmes;

(c) détourner les entrées de zones d'alarme;

(d) afficher un résumé de l'état de tous les périphériques associés au MAD.

(e) consulter et utiliser les données appropriées à la zone d'alarme à laquelle ils ont accès.

29.4 Le système doit permettre d'attribuer les titulaires et les groupes de titulaires à un nombre arbitraire de modules d'activation à distance.

29.5 Les communications entre les modules d'activation à distance et les contrôleurs doivent être chiffrées (au minimum, AES 40 bits).

29.6 Les modules d'activation à distance doivent pouvoir prendre en charge 30 zones d'alarme et 100 entrées connexes dans un système complet.

29.7 Le système doit permettre l'utilisation de plusieurs modules d'activation à distance à n'importe quel point pour gérer à distance les zones d'alarme d'intrusion attribuées.

29.8 Les modules d'activation à distance doivent pouvoir armer et désarmer les zones périmétriques clôturées.

30 Notifications

30.1 Le système doit permettre de configurer des messages d'événements et d'alarmes précis à transmettre aux utilisateurs désignés par courrier électronique ou messages texte (SMS).

30.2 Ceux qui reçoivent ces messages d'alarme doivent pouvoir accuser réception de ceux-ci par courrier électronique ou messages texte (SMS).

30.3 Le système doit pouvoir envoyer un avis d'expiration imminente d'une carte ou d'une compétence à un titulaire, à son gestionnaire ou à toute autre personne désignée. Consulter les sections 13 et 39.

30.4 Le système doit intégrer une fonction de filtrage complète pour gérer la transmission des notifications.

31 Piste de vérification

31.1 Aux fins d'archivage, le serveur de contrôle central doit enregistrer sur son disque toutes les activités du système. Il doit aussi empêcher toute modification des données enregistrées.

31.2 Chaque événement survenu dans le système et tous les détails pertinents, notamment, mais sans s'y limiter la liste suivante, doivent être horodatés à la seconde près et doivent être enregistrés dans le journal des activités du système.

(a) toutes les tentatives d'accès (accès accordé ou refusé);

(b) événements d'alarme;

(c) événements système;

(d) activités des opérateurs.

31.3 Le système de contrôle central doit comprendre un système d'archivage en ligne des données du système et les événements dans un fichier d'archive afin de libérer de l'espace sur le disque dur local et ainsi permettre l'enregistrement d'autres activités.

31.4 Le processus d'archivage doit être déclenché soit manuellement, soit automatiquement après un délai réglable.

31.5 Il doit être possible de préciser le nombre de jours dont les données sont laissées sur le serveur après archivage.

31.6 Le système doit permettre à un opérateur d'afficher une piste d'événements filtrée; tous les événements visant les éléments choisis d'un site, par exemple.

32 Rapports

32.1 Le système de contrôle central doit produire des rapports historiques à partir des sources d'information suivantes :

(a) données d'activité du système;

(b) données d'accès des titulaires de cartes;

(c) champs de données personnelles des titulaires;

(d) données de configuration et de réglage des sites.

32.2 La fonction de création de rapports doit être facile à utiliser et fondée sur des assistants qui aident l'utilisateur à régler les paramètres des rapports. Les assistants doivent pouvoir simplifier la création de rapports en incorporant des choix comme des rapports sur la veille, la dernière semaine, le dernier mois, etc. Ces fonctions visent à permettre de créer rapidement des rapports récurrents d'un format uniforme.

32.3 Les paramètres de création des rapports doivent être entièrement réglables par l'utilisateur; on doit pouvoir effectuer des recherches sur n'importe quel titulaire de carte ou événement d'accès.

32.4 Il doit être possible de créer automatiquement les rapports énumérés ici. Les méthodes de création des rapports sont décrites ci-dessus.

(a) Activités — Toute activité du site.

(b) Évacuation — Dernier emplacement connu de tous les détenteurs de carte sur place.

(c) Exceptions — Alarmes non traitées, alarmes non reçues et portes sécurisées mises temporairement en mode d'accès libre.

32.5 Le rapport est produit par l'un des moyens suivants, selon les besoins de l'opérateur :

(a) exécution d'une macro par l'opérateur;

(b) déclenchement d'un d'événement d'alarme;

(c) selon un échéancier récurrent.

32.6 Le système de contrôle central doit créer et mettre en forme les rapports en arrière-plan; en d'autres termes, l'opérateur doit être en mesure de traiter les alarmes, de modifier les paramètres de la base de données et d'apporter d'autres modifications au système pendant la création des rapports. La création de rapports doit se poursuivre si l'opérateur décide d'effectuer d'autres tâches.

32.7 Le système de contrôle central doit pouvoir afficher les rapports à l'écran avant leur impression.

32.8 Le système doit pouvoir envoyer des rapports par courrier électronique aux personnes ou groupes de personnes désignés.

32.9 Il doit être possible d'enregistrer la mise en forme des rapports pour l'appliquer plus tard à d'autres rapports.

32.10 Le système de contrôle central doit intégrer une file d'attente, afin de pouvoir imprimer des rapports sur toutes les imprimantes connectées au système et prises en charge par le réseau.

32.11 Le système de contrôle central doit intégrer une file d'attente d'impression, afin de mettre les rapports en file d'attente si l'imprimante cible est hors ligne, utilisée, non connectée ou défectueuse.

32.12 Le système de contrôle central doit pouvoir créer des rapports de tension pour surveiller la tension des clôtures périmétriques électrifiées.

32.13 Les rapports de gestion sur les visiteurs doivent comprendre les suivants :

(a) état des visiteurs (attendus, sur place, partis);

(b) visites prévues;

(c) visites antérieures (qui a visité qui, qui a escorté un visiteur).

33 Communications et dépannage

33.1 Le système de contrôle central doit relancer automatiquement le fonctionnement complet et intégral du système après une panne de courant.

33.2 Le système de contrôle central doit tenir un journal complet des diagnostics de rendement, pour permettre aux ingénieurs système de surveiller le rendement du système en cas de panne ou de défaillance du système.

33.3 Le journal des diagnostics de rendement doit être stocké sur le disque dur dans un fichier distinct de tous les autres fichiers de données.

33.4 On doit pouvoir consulter les diagnostics de rendement sans devoir interrompre ni désactiver le système.

33.5 Le système de contrôle central doit intégrer des fonctions de diagnostic en ligne qui permettent aux opérateurs ou aux ingénieurs système autorisés de surveiller et de régler en conséquence les paramètres de rendement du système (réglage de la capacité du réseau de communications, par exemple).