Spécifications de Paxton

Section 1
Contrôle d'accès et gestion vidéo
Paxton10

PARTIE 1 GÉNÉRALITÉS

1.1 RÉSUMÉ

A. La section comprend

1. Contrôle d’accès électronique et gestion vidéo

B. Sections connexes

1. 28 10 00 Contrôle d’accès électronique et détection d’intrusion
2. 28 13 00 Contrôle d’accès
3. 28 23 00 Vidéosurveillance

C. Produits

{Choisissez d’utiliser le nom du produit Paxton ou un nom général pour chaque}

1. Un [serveur] [serveur Paxton10] qui doit contenir la base de données centrale du système, héberger le logiciel et fournir un stockage pour les événements système et les événements utilisateur.
2. Un [contrôleur de porte] [contrôleur de porte Paxton10], qui doit s’interfacer avec les périphériques de point d’accès et les dispositifs de collecte d’identité, fournissant de la logique et de la prise de décision pour gérer un point d’accès.
3. Un [contrôleur vidéo] [contrôleur vidéo Paxton10], qui, en plus de l’interfaçage avec les périphériques de point d’accès, doit également traiter et enregistrer des séquences vidéo provenant de caméras vidéo réseau.
4. Une [carte d’alarme] [connecteur d’alarme Paxton10], qui doit contenir des périphériques d’entrée et de sortie pour surveiller et contrôler l’état des alarmes anti-intrusion et incendie.
5. Une [carte d’interface sans fil] [connecteur sans fil Paxton10], qui doit communiquer via la technologie sans fil Z-Wave pour communiquer avec les dispositifs Z-Wave et les contrôler.
6. Une [caméra de vidéosurveillance] [caméra Paxton10], qui doit être capable d’enregistrer des vidéos en résolution 4K et contenir une mémoire intégrée pour le stockage Edge.
7. Un bloc d’alimentation (PSU), qui doit fournir l’alimentation nécessaire pour alimenter les contrôleurs.
8. Un [lecteur de proximité] [Lecteur Paxton10] qui doit lire une variété d’identifiants de proximité pour vérifier et valider les utilisateurs.
9. Un [lecteur de proximité résistant au vandalisme] [Lecteur anti-vandale Paxton10] qui doit lire une variété d’identifiants de proximité pour vérifier et valider les utilisateurs, contenus dans un boîtier résistant au vandalisme.
10. Un [lecteur de proximité du clavier] [lecteur de clavier Paxton10] qui doit lire une variété d’identifiants de proximité, en plus de fournir le code et le code PIN, afin de vérifier et de valider les utilisateurs.
11. Un [lecteur de bureau] [Lecteur de bureau Paxton10] qui doit fournir la méthode d’inscription des badges de proximité au système à associer aux utilisateurs.
12. Le [logiciel de gestion] [logiciel Paxton10] qui permet l’interaction et la configuration du matériel système, ainsi que la gestion des utilisateurs et du système.

D. Système

1. Les produits ci-dessus doivent constituer un système complet de contrôle d’accès (ACS), assurant le contrôle et la surveillance des points d’accès sur le site installé.
2. Les produits ci-dessus doivent constituer un système de gestion vidéo (VMS) complet, assurant l’enregistrement vidéo et la vidéosurveillance sur le site installé.

3. Le système doit être évolutif, ce qui doit permettre la mise en place d'un matériel supplémentaire provenant du même fabricant.
4. Tout le matériel fourni par le fabricant doit être plug-and-play.
5. Le système doit contenir plusieurs points d'accès.
6. Le système doit contenir plusieurs dispositifs contrôlables.
7. Le système doit contenir plusieurs dispositifs pouvant être surveillés.
8. Le système doit contenir des avertisseurs intrusion et incendie.
9. Le système doit contenir des caméras de vidéosurveillance.

1.2 EXIGENCES DU PROJET

A. Le système doit surveiller et contrôler l'accès aux installations au moyen de contrôleurs d'accès électroniques utilisant des lecteurs de cartes, des dispositifs clavier et des smartphones. Il doit être implémenté au moyen d'une architecture TCP/IP utilisant l'approche du contrôleur électronique à porte unique via l'infrastructure PoE.
B. Le système doit être capable de surveiller les points d'alarme, de contrôler les dispositifs de sortie et de gérer les commandes d'étages des ascenseurs. Le système doit maintenir une piste d'audit de l'activité de l'opérateur et de toutes les activités de contrôle d'accès et d'alarme.
C. Le système doit pouvoir commencer par une seule porte et augmenter d'une porte à la fois jusqu'à un maximum de 1000 portes.
D. Chaque contrôleur doit pouvoir gérer le matériel nécessaire pour sécuriser une porte. Si l'entrée et la sortie sont requises, un seul contrôleur est requis.
E. Chaque contrôleur doit tenir à jour une base de données d'informations complète permettant de prendre des décisions distribuées et hors ligne, sans point de défaillance unique.
F. Les contrôleurs doivent utiliser la technologie IPv6, prenant en charge la détection et l'adressage automatiques et le plug-n-play.
G. Le système doit permettre un nombre illimité de postes de travail pour la programmation et l'administration du système, y compris la gestion des bases de données, la production de rapports et la surveillance en temps réel de l'activité.
H. Aucune clé de licence ni aucun frais ne sera exigé pour accéder au logiciel d'administration, et aucune installation ne sera requise sur le serveur ou sur un poste de travail.
I. Le système doit prendre en charge au moins 50 000 identifiants uniques.
J. Le système doit fournir au minimum les éléments suivants :

1. Contrôle d'accès
2. Contrôle de l'état de la porte (Porte forcée, porte restée ouverte)
3. Vidéosurveillance
4. Gestion de la vidéo
5. Rapport d'événement
6. Synoptiques / Cartes graphiques
7. Déclencheurs et actions
8. Anti-passback
9. Intégration des alarmes intrusion
10. Surveillance de l'alarme incendie

11. Rapports d'appel et de rassemblement
12. Accès à distance
13. Application smartphone pour le contrôle du système
14. Application smartphone pour l'administration des utilisateurs
15. Lecteur d'inscription des identifiants
16. Diverses technologies de lecteur de proximité, y compris Bluetooth
17. Logiciels sans licence et mises à jour à vie sans frais
18. Interphone / Station d'entrée vidéo
19. Serrures de porte sans fil

1.3 DÉFINITIONS

A. Anti-Passback : terme qui empêche le partage ou le transfert d'un badge dans le but de permettre aux utilisateurs non autorisés d'accéder à un site.
B. AWG (American Wire Gauge) : unité de mesure pour le diamètre des fils.
C. Navigateur : programme informatique utilisé pour visualiser et interagir de manière graphique avec les données à un endroit sur le réseau connecté.
D. Client : un PC qui peut visualiser et gérer la base de données système.
E. COM (Common) : un contact sur un relais de connecteur d'E/S.
F. Contrôleur : unité de commande périphérique intelligente qui fournit l'interface entre le sous système de gestion et de surveillance et les dispositifs installés, dans le but de restreindre l'accès, de contrôler et de surveiller l'activité de l'utilisateur et de l'appareil.
G. DDR3 (Double Data Rate type 3) : type de RAM avec une interface à bande passante élevée.
H. Dispositif : Une caméra vidéo, une lumière, une alarme, un point d'accès ou tout autre élément avec lequel on peut interagir, soit en contrôlant l'action ou le résultat, soit en surveillant sa sortie ou son état.
I. Stockage à la périphérie : l'enregistrement de séquences vidéo directement sur la caméra.
J. EMC : compatibilité électromagnétique.
K. Système d'entrée (système d'entrée audio/vidéo) : Système autonome ou intégré, composé de panneaux et de moniteurs pour autoriser l'accès via la communication vidéo et audio.
L. FCC : commission fédérale des communications.
M. E/S : entrée/sortie, se rapportant aux périphériques où une entrée est utilisée pour surveiller l'état élevé/faible d'un signal, et une sortie est constituée d'un relais capable de mettre en marche ou arrêter un dispositif.
N. IC : Industrie Canada.
O. IP : protocole Internet intégré dans Microsoft Windows.
P. LAN : réseau local.
Q. Mbit/s : mégabits par seconde
R. Moniteur : périphérique de matériel qui permet à un occupant de valider l'entrée d'un utilisateur via une confirmation audio ou vidéo.
S. N.C. (Normalement fermé) : un contact sur un relais de connecteur d'E/S.
T. N.O. (Normalement ouvert) : un contact sur un relais de connecteur d'E/S.
U. Occupant/résident : l'utilisateur d'un moniteur ou l'utilisateur d'un lecteur.

V. Air libre : sans obstruction ni interférence.
W. Panneau : périphérique de matériel utilisé pour déterminer si un utilisateur connu est autorisé à accéder, et comme moyen de communication permettant aux utilisateurs inconnus de communiquer avec les occupants d'un bâtiment.
X. PC : ordinateur personnel, utilisé comme station de travail, pour accéder au logiciel système.
Y. PoE : alimentation par Ethernet.
Z. RAM (Random Access Memory) : type de stockage utilisé pour le logiciel pour stocker les données temporaires, requis pour le bon fonctionnement et l'utilisation du logiciel.
AA. Lecteur : lecteur de proximité, clavier ou lecteur biométrique qui capture les informations d'identification utilisées pour identifier un utilisateur.
BB. RoHS : restriction des substances dangereuses.
CC. Appel : liste de contrôle de présence des utilisateurs connus pour avoir été dans une zone spécifiée.
DD. RS-485 : norme TIA/EIA pour les communications multipoints.
EE. CNR-210 : norme IC pour les appareils radio exemptés de licence.
FF. CNR-GEN : norme IC pour les exigences générales et les renseignements relatifs à la certification des appareils radio.
GG. Serveur : PC qui contient la base de données des utilisateurs et de la configuration du système, qui exécute le logiciel système.
HH. SIP : protocole d'initiation de session.
II. Disque SSD (Solid State Drive) : périphérique de stockage qui utilise une mémoire flash et n'a pas de pièces mobiles.
JJ. Système : le matériel et les logiciels à installer, combinés à tout matériel et logiciel existant, pour répondre aux exigences du projet.
KK. TCP : protocole de contrôle du transport intégré à Microsoft Windows.
LL. Badge : les informations d'identification délivrées à une personne. Il peut s'agir d'un code PIN, ou d'un périphérique contenant un numéro encodé, utilisé pour déterminer si l'accès sera accordé ou refusé.
MM. Déclencheurs et actions : composant logiciel qui permet de créer des règles pour effectuer des fonctionnalités sur mesure.
NN. UDP : protocole de datagramme utilisateur intégré à Microsoft Windows.
OO. UL : laboratoires des assureurs.
PP. Unicast : communication où l'information est adressée à un seul destinataire.
QQ. UPS : alimentation sans intérruptions.
RR. USB : bus série universel. Port de communication trouvé sur la plupart des ordinateurs.
SS. Résistant au vandalisme (anti-vandale) : propriété d'un article qui identifie l'article comme étant durable et résistant aux attaques.
TT. Visiteur : utilisateur non autorisé/inconnu. Ou l'utilisateur d'un panneau.
UU. WAN : réseau étendu.
VV. Wiegand : principe magnétique breveté qui utilise des fils spécialement traités intégrés dans la carte d'identification. Également connu sous le nom de format de sortie de données de lecteur et signal Wiegand.

WW. Windows : système d'exploitation de Microsoft Corporation.

XX. Station de travail : PC utilisé pour accéder au logiciel système.

YY. Site : l'emplacement, ou les emplacements, dans lesquels le système est installé.

1.4 DESCRIPTION DU SYSTÈME

A. Généralités

1. Le système doit surveiller et restreindre les déplacements des utilisateurs à travers les points d'accès.

2. Le système doit enregistrer et gérer les enregistrements des caméras vidéo IP situées autour du site

3. Les utilisateurs doivent être identifiés et traités par l'un de ces moyens :

    a. Présentation d'un badge à un lecteur

    b. Présentation d'un smartphone ou d'une tablette à un lecteur

    c. Saisie d'un code PIN unique sur un clavier

    d. Confirmation visuelle et/ou audio de la part d'un occupant des lieux

    e. Combinaison de ce qui précède

4. Le système ne doit pas exiger de codes d'installation pour les informations d'identification des cartes. Chaque badge/identifiant doit avoir un cryptage unique pour une sécurité élevée.

5. Le système doit prévoir des numéros de série de cartes uniques, de sorte que l'utilisateur n'aura pas besoin de déterminer la prochaine séquence de cartes à acheter.

6. Un PC doit être utilisé pour administrer le système de contrôle d'accès.

    a. Un mot de passe doit être requis pour se connecter et doit limiter les activités qu'un opérateur est autorisé à effectuer.

7. Des applications mobiles doivent être disponibles pour le contrôle du système et l'administration des utilisateurs.

    a. Les applications mobiles seront disponibles pour les appareils Android et iOS.

B. Matériel

1. Le matériel doit être composé de :

    a. Un serveur

    b. Contrôleurs de porte

    c. Contrôleurs vidéo

    d. Caméras vidéo

    e. Panneaux périphériques d'alarme

    f. Cartes d'interface sans fil {Requis pour PaxLock}

    g. Lecteurs de proximité

    h. Lecteurs de clavier

    i. Lecteurs de bureau

    j. Unités d'alimentation

2. Tout le matériel doit être plug-and-play.

3. Tous les périphériques matériels doivent être clairement étiquetés et identifiés pour faciliter l'installation.

4. L’équipement utilisé doit recevoir des mises à jour du firmware par le fabricant gratuitement.

C. Logiciel

1. La base de données système contenant toutes les informations relatives au matériel et aux utilisateurs doit être conservée sur le serveur.

2. Le serveur héberge le logiciel du système et fournit un lien Web permettant d’accéder au système et de le configurer.

a. Le logiciel doit être accessible à un nombre illimité de postes de travail sans installation.

b. Le logiciel doit être accessible à l’aide de la dernière version des navigateurs suivants :

(i) Google Chrome

(ii) Apple Safari

3. L’accès au logiciel doit être restreint à l’aide d’une connexion d’opérateur protégée par mot de passe.

4. L’accès au logiciel doit être autorisé en fonction des besoins et du rôle de chaque administrateur.

5. Le logiciel doit comprendre :

a. Une interface utilisateur graphique.

b. Des info-bulles sur chaque commande pour l’information utilisateur.

c. Prise en charge des appareils mobiles, tablettes et ordinateurs de bureau.

d. Multi-utilisateurs et multi-tâches pour permettre des activités indépendantes et une surveillance simultanée sur différents postes de travail.

6. La licence du système doit porter sur l’ensemble du système et doit inclure la capacité pour les ajouts futurs qui respectent les limites de taille du système indiquées dans la présente section. Il n’y aura pas de frais de licence ou de renouvellement annuel.

D. Ensemble de fonctionnalités

1. Le système et les logiciels associés doivent fournir au minimum les éléments suivants :

a. Contrôle d’accès

b. Enregistrement et gestion vidéo

c. Intégration de caméras IP tierces

d. Prise en charge des caméras PTZ

e. Mur vidéo

f. Exportation de vidéo

g. Exportation d’un instantané vidéo

h. Signets vidéo

i. Recherche intelligente

j. Recherche dans la vidéo

k. Contrôle de la vitesse de lecture de la vidéo

l. Intégration d’alarme d’intrus

m. Intégration d’alarme incendie

n. Importation d’utilisateur

o. Cartes graphiques

p. Tableaux de bord personnalisés

q. Favoris de l'utilisateur

r. Affichage automatique de l'image utilisateur sur PC à l'utilisation de la carte

s. Appel et regroupement

t. Notifications d'appel par e-mail

u. Rapports d'appel sur smartphone

v. Déclencheurs et actions pour obtenir des fonctionnalités personnalisées et uniques

w. Anti-passback

x. Permissions multi-sociétés

y. Prise en charge de plusieurs technologies de lecture, y compris Bluetooth

z. Gestion du site à distance

aa. Application mobile Android et iOS pour la gestion de site

bb. Application mobile Android et iOS pour l'identification de l'utilisateur (badge Bluetooth)

cc. Connexion logicielle sécurisée à l'aide de HTTPS

dd. Paramètres de gestion des données pour gérer la protection des données

ee. Logiciels disponibles en plusieurs langues

2. Ces fonctionnalités doivent être fournies sans frais supplémentaires ni abonnement

1.5 EXIGENCES DE PERFORMANCE

A. Toute modification apportée au logiciel est automatiquement communiquée à tout le matériel de contrôle d'accès intelligent, les modifications appropriées prenant effet immédiatement.

B. Traitement distribué :

1. Le système est un système de traitement entièrement distribué de sorte que les informations (y compris l'heure, la date, les codes valides, les niveaux d'accès et les données similaires) soient téléchargées auprès des contrôleurs de telle manière que chaque contrôleur prend des décisions de contrôle d'accès pour cet emplacement.

2. Si les communications vers le serveur sont perdues, tous les contrôleurs doivent automatiquement mettre en mémoire tampon les transactions d'événements jusqu'à ce que les communications soient restaurées, et les événements mis en mémoire tampon seront téléchargés sur le serveur.

C. Capacités du système :

1. Le système doit prendre en charge au maximum :

a. 1 000 points d'accès.

b. 1 000 caméras vidéo.

c. 50 000 utilisateurs, chacun avec une identification unique.

d. Niveaux d'accès et règles illimités.

e. Rapports illimités

D. Configuration réseau système requise

1. Les PC clients communiquent avec le serveur via HTTPS, en utilisant le chiffrement SSL sécurisé.

a. Les événements système enregistrés par le serveur doivent être communiqués aux clients.

b. Les modifications apportées à la base de données sur un poste client doivent être communiquées au serveur.

2. Le serveur doit communiquer avec le matériel de contrôle d'accès via HTTPS.
    a. Les événements de contrôle d'accès doivent être communiqués au serveur.
    b. Les modifications apportées à la base de données doivent être communiquées au matériel de contrôle d'accès.
3. Le système utilise des protocoles de mise en réseau standard pour permettre l'installation sur l'infrastructure de l'entreprise.
4. Aucun adressage manuel n'est requis.

1.6 ASSURANCE DE LA QUALITÉ

A. Le logiciel doit recevoir les mises à jour du fabricant à vie gratuitement.

B. Tous les équipements fournis doivent être couverts par une garantie du fabricant pendant au moins 5 ans, à l'exception du serveur, qui doit être couvert pendant au moins trois ans. Les aspects suivants sont couverts :

1. Électrique
2. Électronique
3. Composant
4. Mécanique

C. Tout le matériel fourni doit recevoir gratuitement les mises à jour du firmware du fabricant.

1.7 DOCUMENTS CONNEXES

A. Fabricant acceptable : Paxton {Supprimer si nécessaire}

1. Adresse e-mail : {Supprimer les options qui ne sont pas obligatoires}
    a. {UK} [support@paxton.co.uk]
    b. {FR} [support@paxtonaccess.fr]
    c. {US} [supportUS@paxton-access.com]
    d. {DE} [verkauf@paxton-gmbh.de]
    e. {NL} [support@paxton-benelux.com]
2. Numéro de téléphone :
    a. {UK} [01273 811011]
    b. {FR} [01 57 32 93 56]
    c. {US} [877.438.7298]
    d. {DE} [0251 2080 6900]
    e. {NL} [076 3333 999]
3. Skype :
    a. {UK} [Paxton.support]
    b. {FR} [Paxton.benelux.support]
    c. {US} [USAaxton.support]
    d. {DE} [Paxton.gmbh.support]

B. Substitutions : Non autorisées. {Supprimer si nécessaire}

C. Les composants du système doivent être disponibles auprès d'un fabricant unique afin d'assurer la compatibilité des produits.

D. Le fabricant du lecteur doit également fournir un système de contrôle d'accès.

E. Le fabricant du lecteur doit également fournir un système d'entrée de porte.

F. Limites de substitution

1. Il doit être possible d'installer un lecteur dans un système [Paxton10] existant.
2. Il doit être possible d'installer un lecteur en remplacement fonctionnel d'un lecteur existant.

1.8 CONFORMITÉ

A. Le système doit respecter les conditions suivantes :

1. Le Règlement Général sur la Protection des Données (RGDP) 2018
2. EN60839-11-1 Grade 1
3. EN60839-11-1 Grade 2

B. Les lecteurs doivent respecter les normes suivantes :

1. EN 301 489-1 pour EMC {UE}
2. EN 300 330 pour la radio {UE}
3. EN 60950-1 pour la sécurité {UE}
4. IEC/EN 60950-1 pour la sécurité {ROW}
5. FCC Partie 15C pour la radio {US}
6. UL294 pour la sécurité {US}
7. CNR-GEN, 210 pour Radio {Canada}
8. CS C22.2 NO 205-M1983 pour la sécurité {Canada}
9. IP67 pour résistance à l’humidité

C. Les lecteurs résistants au vandalisme doivent respecter les normes suivantes :

1. EN 301 489-1 pour EMC {UE}
2. EN 300 330 pour la radio {UE}
3. EN 60950-1 pour la sécurité {UE}
4. IEC/EN 60950-1 pour la sécurité {ROW}
5. FCC Partie 15C pour la radio {US}
6. UL294 pour la sécurité {US}
7. CNR-GEN, 210 pour Radio {Canada}
8. CS C22.2 NO 205-M1983 pour la sécurité {Canada}
9. IP67 pour résistance à l’humidité
10. IK10 pour résistance aux chocs

D. Les connecteurs d’alarme doivent respecter les aux normes suivantes :

1. EN 55032 pour EMC {UE}
2. EN 50130-4 pour EMC {UE}
3. EN 60950-1 pour la sécurité {UE}
4. FCC Partie 15B pour EMC {US}
5. UL 294 pour la sécurité {US}
6. ICES-003 pour EMC {Canada}
7. CSA C22.2 NO 205-M1983 pour la sécurité {Canada}

E. Les connecteurs sans fil doivent respecter les normes suivantes :

1. EN 301 489-1 pour EMC {UE}

2. EN 300 328 pour la radio {UE}
3. EN 60950-1 pour la sécurité {UE}
4. UL/CSA 60950-1 pour la sécurité {US/Canada}
5. CEI 60950-1 pour le régime CB
6. FCC Partie 15C pour la radio {US}
7. CNR-GEN, 210 pour Radio {Canada}

F. Le serveur doit respecter les normes suivantes :

1. EN 60950-1 pour la sécurité {UE}
2. EN 55022 pour EMC {UE}
3. EN 55024 pour EMC {UE}
4. EN 61000-3-2 pour EMC {UE}
5. EN 61000-3-3 pour EMC {UE}
6. Europe RoHS pour la conformité environnementale {UE}
7. FCC 47 CFR partie 15, sous-partie B pour EMC {US}
8. UL/CSA 60950-1 pour la sécurité {US/Canada}
9. ICES-003 pour EMC {Canada}
10. CEI 60950-1 pour la sécurité
11. CISPR 22 pour EMC
12. CIPSR 24 pour CEM
13. Série IEC/EN 61000-4 pour EMC

G. Les contrôleurs doivent respecter les normes suivantes :

1. EN 55032 pour EMC {UE}
2. EN 55024 pour EMC {UE}
3. IEC/EN 62368-1 pour la sécurité {UE}
4. FCC partie 15B pour EMC {US}
5. UL 294 pour la sécurité {US}
6. CSA C22.2 NO 205-M1983 pour la sécurité {Canada}
7. ICES-003 pour EMC {Canada}
8. CEI 62368-1 pour le régime CB

H. Les lecteurs de bureau doivent respecter les normes suivantes :

1. EN 301 489-1 pour EMC {UE}
2. EN 300 330 pour la radio {UE}
3. IEC/EN 60950-1 pour la sécurité {UE}
4. FCC Partie 15C pour la radio {US}
5. CNR-GEN, 210 pour Radio {Canada}
6. UL/CSA 62368-1 pour la sécurité {US/Canada}

I. Les caméras doivent respecter les normes suivantes :

1. RoH53 2015/863 {UE}
2. EN 55032 pour les émissions {UE}
3. EN 50130-4 pour la sécurité {UE}
4. EN 60950-1 pour la sécurité {UE}

5. FCC partie 15B pour EMC {US}
6. ICES-003 {Canada}
7. UL/CSA 60950-1 pour la sécurité {US/Canada}

1.9 EXIGENCES GÉNÉRALES DE FONCTIONNALITÉ

A. Par l'utilisation d'un contrôleur, il doit être possible de :

1. Contrôler l'état de verrouillage d'un point d'accès.
2. Surveiller l'état actuel d'ouverture/fermeture d'un point d'accès.
3. Surveiller les contacts de porte forcée.
4. Communiquer les événements et la configuration avec le serveur.
5. Interfacer avec des connecteurs de matériel pour fournir des périphé ecteurs de matériel pour fournir des périphériques supplémentaires.

C. Il doit être possible de commander et de surveiller des dispositifs supplémentaires en utilisant toutes les entrées/sorties d'un contrôleur qui ne sont pas utilisées pour sécuriser un point d'accès.

D. Grâce à l'utilisation d'un connecteur d'alarme, il doit être possible de :

1. Interfacer avec les alarmes intrusion et incendie :
    a. Contrôler l'état d'armement d'une alarme intrusion.
    b. Surveiller l'état d'armement d'une alarme intrusion.
    c. Surveiller l'état actif d'une alarme intrusion.
    d. Surveiller l'état actif d'une alarme incendie.

E. Il doit être possible de commander et de surveiller les dispositifs supplémentaires en utilisant toutes les entrées/sorties libres d'un connecteur d'alarme qui ne sont pas utilisées pour surveiller ou contrôler une alarme.

F. Grâce à l'utilisation d'un lecteur de proximité, il doit être possible de lire les identifiants d'un utilisateur.

1. Un titulaire d'identifiant doit pouvoir présenter son badge ou son dispositif intelligent au lecteur pour obtenir un accès valide à un point d'accès.
    a. La présentation d'un identifiant non valide ne doit pas permettre l'accès.
2. Un titulaire d'identifiant doit pouvoir présenter son badge au lecteur pour contrôler un appareil.
    a. La présentation d'un identifiant non valide ne doit pas agir sur l'appareil.
3. Une rétroaction visuelle doit être fournie à l'utilisateur lors de la présentation d'un identifiant.
    a. La rétroaction doit indiquer si l'identifiant est valide ou non pour l'action envisagée.
4. Une rétroaction audible doit être fournie à l'utilisateur sur présentation d'un identifiant.
    a. La rétroaction doit indiquer si l'identifiant est valide ou non pour l'action envisagée.

G. Grâce à un lecteur de clavier, l'utilisateur doit pouvoir saisir un code PIN ou un code générale pour s'identifier.

1. Il doit être possible d'utiliser un code PIN ou un code générale conjointement avec un badge de proximité ou un dispositif intelligent afin d'améliorer la sécurité davantage.

2. Le système doit requérir un mode d'authentification de l'utilisateur approprié pour l'appareil ou le point d'accès avec lequel l'interaction se fera. Le mode de fonctionnement doit changer automatiquement à différents moments de la journée ou des jours de la semaine en fonction de sa configuration.

H. Par l'utilisation d'un serveur, il doit être possible de :

1. Accéder au logiciel pour la configuration, la maintenance et la surveillance du système.
2. Stocker la base de données système à un emplacement central.
3. Enregistrer les événements système à afficher à un utilisateur en direct ou à une date ultérieure.

I. Il doit être possible de combiner le matériel pour répondre aux exigences du projet :

J. Le système doit utiliser les capacités existantes du réseau du site. {Supprimer si ce n'est pas vrai pour le projet}

K. Le système doit être polyvalent :

1. Le système reste opérationnel tant que le serveur est hors ligne.
2. Chaque contrôleur et ses connecteurs doivent rester opérationnels tant que le réseau ou les autres contrôleurs ne sont pas disponibles.
3. Chaque contrôleur doit être muni d'une batterie de secours, afin de maintenir le fonctionnement de celui-ci et de ses connecteurs en cas de panne de courant. {Retirez si aucune batterie n'est installée}
    a. La batterie doit être surveillée par le système et doit fournir l'état actuel de la batterie et son niveau de charge dans l'interface utilisateur.

1.10 EXIGENCES GÉNÉRALES RELATIVES AUX COMMUNICATIONS

A. Le serveur doit être connecté au réseau TCP/IP local.

1. Une URL locale doit être fournie depuis laquelle le logiciel doit être accessible sur n'importe quel ordinateur sur le même réseau.
2. Une URL distante est générée si nécessaire depuis laquelle le logiciel doit être accessible sur n'importe quel ordinateur doté d'une connexion Internet, à condition que le serveur dispose également d'un accès Internet.
3. Les communications au serveur doivent utiliser HTTPS sécurisé, chiffré à l'aide de SSL.
4. Le serveur doit être adressable par les clients utilisant un DNS convivial.

B. Les contrôleurs doivent être connectés au réseau TCP/IP local.

1. Les contrôleurs doivent utiliser IPv6 link-local.
2. Les contrôleurs doivent communiquer avec le serveur.
3. Les contrôleurs doivent communiquer avec d'autres contrôleurs (pair à pair).
4. Les contrôleurs doivent être automatiquement détectés par le serveur.

C. Les caméras doivent être connectées au réseau TCP/IP local. {Si vous utilisez des caméras Paxton10}

1. Les caméras doivent utiliser IPv6 link-local.
2. Les caméras doivent communiquer avec le serveur pour fournir des informations, la configuration et l'interaction de l'utilisateur.
3. Les caméras doivent communiquer la vidéo directement au client, ce qui réduit les besoins de bande passante via le serveur.
4. La vidéo et la configuration de la caméra doivent être protégées par mot de passe.
    a. Le mot de passe de la caméra ne doit être connu uniquement du système et ne doit pas nécessiter la saisie de l'utilisateur.

D. Les caméras doivent être connectées au réseau TCP/IP local. {Si vous utilisez des caméras ONVIF}

1. Les caméras doivent être détectées automatiquement à l'aide de la découverte du ONVIF profil S.
2. Les caméras doivent communiquer avec un contrôleur vidéo.

E. Les caméras doivent être connectées à un réseau TCP/IP. {Si vous utilisez des caméras RTSP}

1. Les caméras doivent être adressées manuellement à l'aide de leur adresse RTSP.
2. Les caméras doivent communiquer avec un contrôleur vidéo.

F. Les lecteurs doivent se connecter à un contrôleur.

1. Un seul câble à paires torsadées de 22 AWG à 4 noyaux doit être utilisé par lecteur.
    a. 5m de câble doit être fourni avec chaque lecteur.
    b. Le type de câble pour les rallonges doit être de 22 AWG, 4 noyaux avec paires torsadées.
    c. La longueur maximale du câble doit être 100m.
2. Les lecteurs doivent être automatiquement détectés par le système.
3. Chaque contrôleur doit prendre en charge au moins deux lecteurs filaires.

G. Le lecteur de bureau doit se connecter à un ordinateur client.

1. Le lecteur de bureau doit entrer des données dans le logiciel Paxton10 via un PC client.
2. Le lecteur de bureau doit se connecter à un PC client via un câble mini USB vers USB.
3. Le lecteur de bureau doit être plug-and-play, utilisant la sortie clavier.

H. Tous les contrôleurs adressables sur le réseau doivent prendre en charge l'IPv6 pour la détection automatique et la fonctionnalité plug-and-play.

I. Toutes les caméras utilisées doivent produire deux flux vidéo : un flux « principal » haute résolution et un « sous » flux basse résolution. Le sous-flux doit être utilisé pour économiser la bande passante du réseau lors de la diffusion de plusieurs flux vidéo.

J. Le système doit utiliser des protocoles de mise en réseau normalisés pour permettre l'installation sur l'infrastructure de l'entreprise.

PARTIE 2 PRODUITS

2.1 FABRICANTS

A. Fabricant acceptable : Paxton {Supprimer si nécessaire}

1. Adresse e-mail : {Supprimer les options qui ne sont pas obligatoires}
    a. {UK} [support@paxton.co.uk]
    b. {FR} [support@paxtonaccess.fr]
    c. {US} [supportUS@paxton-access.com]
    d. {DE} [verkauf@paxton-gmbh.de]
    e. {NL} [support@paxton-benelux.com]
2. Numéro de téléphone :
    a. {UK} [01273 811011]
    b. {FR} [01 57 32 93 56]
    c. {US} [877.438.7298]
    d. {DE} [0251 2080 6900]
    e. {NL} [076 3333 999]

3. Skype :
    a. {UK} [Paxton.support]
    b. {FR} [Paxton.benelux.support]
    c. {US} [usaPaxton.support]
    d. {DE} [Paxton.gmbh.support]

B. Substitutions : Non autorisées. {Supprimer si nécessaire}

C. Les composants du système doivent être disponibles auprès d'un fabricant unique afin d'assurer la compatibilité des produits.

D. Les composants doivent être constitués de :

1. Logiciel système. Le fabricant doit avoir à son emploi le personnel d'ingénieurs logiciel qui rédigent et gèrent le code du système et doit conserver toutes les licences requises.

2. Contrôleurs. Le fabricant doit fournir des contrôleurs de porte et des contrôleurs vidéo pour une solution plug-and-play permettant de sécuriser un bâtiment et contrôler des dispositifs.

3. Lecteurs. Le fabricant doit fournir des lecteurs de proximité, des lecteurs digicode et des variantes résistantes au vandalisme pour identifier et valider un utilisateur.

4. Badges / identifiants. Le fabricant doit fournir une gamme de badges de proximité pour répondre aux exigences du projet.

5. Caméras. Le fabricant doit fournir sa propre gamme de caméras de vidéosurveillance plug-and-play, en réseau, avec une résolution de 4K. Les caméras doivent être disponibles sous une série de facteurs de forme.

6. Interphone d'entrée de porte. Si cela est nécessaire maintenant ou à une date ultérieure, le fabricant doit fournir des moniteurs d'entrée et des panneaux d'entrée plug-and-play pour permettre aux occupants d'un bâtiment de communiquer avec les visiteurs et de leur permettre l'accès. L'interphone d'entrée de porte doit s'ajouter à un système nouveau ou existant sans refonte ni réarchitecture.

7. Poignées de porte sans fil. Si cela est nécessaire maintenant ou à une date ultérieure, le fabricant doit fournir des poignées de porte sans fil pour les solutions de contrôle d'accès lorsqu'une solution filaire n'est pas réalisable. La poignée de porte sans fil doit pouvoir être ajoutée à tout moment, quelle que soit la quantité, sans réarchitecture du système.

E. Limites de substitution

1. Pas de substitutions.

2.2 EXIGENCES SPÉCIFIQUES POUR LES BADGES

A. Le fabricant du système doit être en mesure de fournir des badges Paxton HiTag2 125kHz.

1. Les badges fournis doivent contenir une méthode d'authentification pour dissuader la copie et l'utilisation non autorisée de badges.

2.3 EXIGENCES SPÉCIFIQUES POUR LE SERVEUR [PAXTON10]

A. Caractéristiques

1. Le serveur doit stocker et gérer la base de données centrale du système.
2. Le serveur doit être intégré sur un ordinateur puissant fourni par le fabricant.
    a. Le matériel doit être une plateforme NUC (Next Unit of Computing) conçue par Intel®.
3. Le fabricant doit fournir un dispositif de stockage USB pour les sauvegardes externes de la base de données.
    a. Cela doit être fourni sans frais supplémentaires.
    b. La capacité du périphérique de stockage USB doit être d'au moins 32 Go.
    c. Les sauvegardes de base de données doivent être automatiques.
4. Le serveur doit être plug-and-play.
5. Le serveur doit mettre à jour tout le matériel du système sur le réseau en fonction des modifications apportées à la base de données.
6. Le logiciel de gestion du système doit être préinstallé sur le serveur.
    a. Le logiciel doit être accessible à partir de n'importe quel poste de travail situé sur le même réseau.

B. Interaction des utilisateurs

1. L'ordinateur doit être plug and play.
2. Après l'installation, aucune autre interaction avec le matériel ne doit être requise.

C. Le serveur doit tenir à jour la base de données système contenant au minimum, mais sans s'y limiter :

1. Dossiers utilisateur :
    a. Nom
    b. Adresse électronique
    c. Date de validité à partir de / valide jusqu'à
    d. Image
    e. Adhésion au groupe
    f. Autorisations
    g. Champs personnalisés
    h. Préférences de l'utilisateur
2. Rapports :
    a. Un journal de tous les événements système et utilisateur
    3. Tableaux de bord
4. Plans du site
5. Appareils :
    a. Nom
    b. Mappage du matériel
    c. Configuration
    d. Adhésion au groupe
    e. Autorisations
6. Règles
    a. Règles et comportements personnalisés

b. Autorisations utilisateur

c. Profils horaires / programmes

d. Configuration de l'appel

e. Comportement anti-passback

D. Spécifications matérielles du serveur :

1. L'ordinateur doit contenir au minimum un processeur Intel i3.
2. L'ordinateur doit contenir au moins 8 Go de RAM.
    a. La RAM doit être DDR3.
3. L'ordinateur doit contenir un disque dur interne permettant de stocker la base de données système :
    a. Le disque dur doit être un disque SSD (Solid State Drive).
    b. Le disque dur doit avoir une capacité de stockage d'au moins 60 Go.
4. L'ordinateur doit contenir au minimum une carte graphique Intel® HD Graphics 4000.

E. Alimentation

1. L'ordinateur doit être alimenté par un adaptateur secteur CA-DC de 19 V 65 W.
    a. Cela doit être fourni par le fabricant sans frais supplémentaires.
2. L'ordinateur doit consommer au maximum 25 W.
3. L'ordinateur doit comporter un capteur de tension.
4. L'ordinateur doit contenir un contrôle de gestion de l'alimentation conforme à l'ACPI.

F. Température

1. L'ordinateur doit conformer aux normes de température requises pour un produit interne.
    a. L'ordinateur doit fonctionner de manière fiable dans la plage de température comprise entre 32 °F et +122 °F (0 °C à +50 °C)

G. Boîtier

1. La conception du boîtier doit être élégante et moderne.
2. Le boîtier doit être en aluminium et en plastique.
3. Il ne doit pas y avoir de fixations visibles sur les faces affichées.
4. L'article doit être disponible en noir.

H. Dimensions

1. Les dimensions du serveur ne doivent pas dépasser :
    a. Une largeur de 4,6" (116 mm)
    b. Une hauteur de 4,4" (112 mm)
    c. Une profondeur de 1,7" (42 mm)

2.4 EXIGENCES SPÉCIFIQUES POUR LE CONTRÔLEUR DE PORTE [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. Le contrôleur doit permettre le contrôle et la surveillance d'un point d'accès unique.
2. Le contrôleur doit pouvoir déverrouiller automatiquement les points d'accès pendant des périodes spécifiées.
3. Le contrôleur doit stocker localement la base de données système pour une recherche plus rapide et hors ligne.

4. Le contrôleur doit permettre le raccordement de connecteurs supplémentaires au système, augmentant ainsi ses connexions E/S disponibles.

5. Le contrôleur doit fournir la prise de décision et la logique à un système.

6. Le contrôleur doit être muni d'une batterie de secours externe.

a. Le système doit rester fonctionnel pendant une période de temps au cours d'une panne de courant.

b. Le système doit signaler l'état et le niveau de charge de la batterie pour le diagnostic et la notification de l'utilisateur.

7. Toutes les données doivent être conservées lors d'une perte de puissance.

8. Le contrôleur doit être muni de bornes détachables pour un entretien rapide et facile.

B. Interaction des utilisateurs

1. Le contrôleur doit être plug and play.

2. Après l'installation, aucune autre interaction avec le matériel ne doit être requise.

C. Affichage

1. Le contrôleur doit avoir une représentation de codage couleur pour le lecteur, le dispositif de sortie, les communications et les connexions d'alimentation afin de simplifier l'installation, l'entretien et le dépannage.

2. L'unité doit comprendre des voyants d'installation indiquant l'état du relais de sortie, l'état d'entrée et l'état des communications TCP/IP.

D. Alimentation

1. Il doit être possible de mettre le contrôleur sous tension par :

a. Alimentation par Ethernet (PoE/PoE+)

b. Un bloc d'alimentation (bloc d'alimentation) de 12 V, 2 A

2. La consommation électrique au ralenti ne doit pas dépasser 3,0 W.

3. La consommation d'énergie maximale ne doit pas dépasser 5,6 W.

4. Le contrôleur doit être équipé d'une batterie de secours au plomb de 12 V.

E. Température

1. Le contrôleur doit conformer aux normes de température requises pour un produit interne.

a. Le contrôleur doit fonctionner de manière fiable dans la plage de température comprise entre 32 °F et +113 °F (0 °C à +45 °C).

F. Boîtier

1. Un boîtier mural doit être disponible.

2. Le boîtier doit être disponible en blanc.

3. Le contrôleur doit comporter des connecteurs amovibles pour faciliter l'installation et l'échange de carte si nécessaire. Les points de connexion ne doivent pas nécessiter d'outils spéciaux pour être terminés.

G. Dimensions

1. Les dimensions du contrôleur, en boîtier, ne doivent pas dépasser :

a. Une largeur de 9,3" (236 mm)

b. Une hauteur de 12,7" (322 mm)

c. Une profondeur de 3,1" (77 mm)

H. Périphériques

1. Le contrôleur doit fournir les périphériques pour contrôler et sécuriser un point d'accès

unique. Les connexions matérielles suivantes doivent être disponibles :

a. 1 x sortie de verrou alimentée

i) La sortie de verrou doit fournir la puissance nécessaire pour fixer et contrôler une seule serrure magnétique

(ii) La sortie de verrou doit fournir 1A à 12V CC

iii) La sortie de verrou doit être configurable en tant que verrou à ouverture ou fermeture sur coupure de courant

b. 1 x contact de porte

i) Le contact de porte doit surveiller l'état actuel d'ouverture/fermeture d'un point d'accès

c. 1 x bouton de sortie alimenté

i) Un bouton de sortie doit permettre la libre circulation par le point d'accès

ii) Le périphérique du bouton de sortie doit fournir une sortie de 12 V pour fournir une indication visuelle et un retour d'information au niveau du bouton de sortie.

iii) Le périphérique du bouton de sortie peut être désactivé dans le logiciel système s'il n'est pas utilisé, afin d'éviter que l'accès ne soit effectué par la manipulation matérielle.

d. 2 x relais

(i) Chaque relais doit être muni de contacts N.O. (normalement ouvert) et N.C. (normalement fermé)

ii) Les contacts de relais doivent être libres de potentiel.

(iii) Chaque relais doit pouvoir commuter une charge résistive d'au moins 2 A à 30 V CC.

(iv) Un relais doit pouvoir être configuré comme sortie d'alarme

(v) Un relais doit pouvoir être configuré comme sortie de verrou

vi) Un relais doit pouvoir être utilisé pour des dispositifs autres que le point d'accès sécurisé

e. 2 ports de lecteur

(i) Il doit être possible d'utiliser une combinaison de lecteurs de proximité, de lecteurs de proximité clavier et de lecteurs résistants au vandalisme.

(ii) Les périphériques de lecteur doivent fournir les données et l'alimentation aux lecteurs connectés.

(iii) Le périphérique du lecteur ne doit pas être limité à une entrée de données fixes, et doit plutôt accepter des données lues à partir de divers types de badges de différentes longueurs, y compris, mais sans s'y limiter, aux éléments suivants :

1. PIN
2. Code
3. ID de badge
4. ID d'identification Bluetooth

(iv) Le périphérique du lecteur doit émettre des états de courant pertinents pour le dispositif à contrôler pour fournir une rétroaction au détenteur du badge sous la forme d'une LED et d'un haut-parleur.

(v) Le périphérique du lecteur doit fournir la puissance dont le lecteur a besoin pour fonctionner.

(vi) Un lecteur peut être utilisé pour des dispositifs autres que le point d'accès sécurisé

f. 1 x entrée numérique

(i) Une entrée numérique doit pouvoir être configurée comme un bouton de sortie

(ii) Une entrée numérique doit pouvoir être configurée pour surveiller un bloc d'alimentation externe

(iii) Une entrée numérique doit pouvoir être utilisée pour des dispositifs autres que le point d'accès sécurisé

2. Il doit être possible d'assigner n'importe quel périphérique à différents dispositifs ou de fournir des fonctionnalités personnalisées.

3. Le contrôleur doit fournir un port de connecteur.

a. Les connecteurs doivent communiquer avec le système par l'intermédiaire du contrôleur.

b. Le contrôleur doit fournir la PoE aux connecteurs.

4. Le contrôleur doit fournir un interrupteur d'autoprotection libre de potentiel.

a. Le système doit déclencher un événement d'alarme lorsqu'un interrupteur d'autoprotection est déclenché.

5. Le contrôleur doit fournir des bornes de batterie.

a. Une batterie de 12 V CC 7Ah doit être installée.

b. Le contrôleur doit surveiller l'état et le niveau de charge de la batterie.

2.5 EXIGENCES SPÉCIFIQUES POUR LE CONTRÔLEUR VIDÉO [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. Le contrôleur doit permettre le contrôle et la surveillance d'un point d'accès unique.

2. Le contrôleur doit pouvoir déverrouiller automatiquement les points d'accès pendant des périodes spécifiées.

3. Le contrôleur assure le traitement et la gestion du stockage d'au moins quatre caméras réseau.

4. Le contrôleur doit traiter et enregistrer au moins 2 flux vidéo de chaque caméra, en plus d'une image QCIF périodique régulière. Le contrôleur doit fournir au système :

a. Un flux vidéo haute résolution, jusqu'à une résolution 4K à 20 IPS

b. Un flux vidéo basse résolution, jusqu'à 640 x 480 résolution à 15 IPS

c. Une image QCIF basse résolution, enregistrée à 1 IPS

5. Le contrôleur doit fournir une interface et une alimentation à deux disques de stockage pour le stockage vidéo.

6. Le contrôleur doit stocker localement la base de données système pour une recherche plus rapide et hors ligne.

7. Le contrôleur doit permettre le raccordement de connecteurs supplémentaires au système, augmentant ainsi ses connexions E/S disponibles.

8. Le contrôleur doit fournir la prise de décision et la logique à un système.

9. Le contrôleur doit être muni d'une batterie de secours externe.

a. Le système doit rester fonctionnel pendant une période de temps au cours d'une panne de courant.

b. Le système doit signaler l'état et le niveau de charge de la batterie pour le diagnostic et la notification de l'utilisateur.

10. Toutes les données doivent être conservées lors d'une perte de puissance.

11. Le contrôleur doit être muni de bornes détachables pour un entretien rapide et facile.

B. Interaction des utilisateurs

1. Le contrôleur doit être plug and play.

2. Après l'installation, aucune autre interaction avec le matériel ne doit être requise.

C. Affichage

1. Le contrôleur doit avoir une représentation de codage couleur pour le lecteur, le dispositif de sortie, les communications et les connexions d'alimentation afin de simplifier l'installation, l'entretien et le dépannage.

2. L'unité doit comprendre des voyants d'installation indiquant l'état du relais de sortie, l'état d'entrée et l'état des communications TCP/IP.

D. Alimentation

1. Il doit être possible de mettre le contrôleur sous tension avec :

a. Alimentation par Ethernet (PoE+)

b. Un bloc d'alimentation (bloc d'alimentation) de 12 V, 4 A

2. La consommation électrique au ralenti ne doit pas dépasser 3,9 W.

3. La consommation d'énergie maximale ne doit pas dépasser 8,3 W.

4. Le contrôleur doit être équipé d'une batterie de secours au plomb de 12 V.

E. Température

1. Le contrôleur doit satisfaire aux normes de température requises pour un produit interne.

a. Le contrôleur doit fonctionner de manière fiable dans la plage de température comprise entre 32 °F et +113 °F (0 °C à +45 °C).

F. Boîtier

1. Un boîtier mural doit être disponible.

2. Le boîtier doit être disponible en blanc.

3. Le contrôleur doit comporter des connecteurs amovibles pour faciliter l'installation et l'échange de carte si nécessaire. Les points de connexion ne doivent pas nécessiter d'outils spéciaux pour être terminés.

G. Dimensions

1. Les dimensions du contrôleur, en boîtier, ne doivent pas dépasser :

a. Une largeur de 10,8" (275 mm)

b. Une hauteur de 12,6" (320 mm)

c. Une profondeur de 2,8" (70 mm)

H. Périphériques

1. Le contrôleur doit fournir les périphériques pour contrôler et sécuriser un point d'accès unique. Les connexions matérielles suivantes doivent être disponibles :

a. 1 x sortie de verrou alimentée

(i) La sortie de verrou doit fournir la puissance nécessaire pour fixer et contrôler une seule serrure magnétique

(ii) La sortie de verrou doit fournir 1A à 12V CC

(iii) La sortie de verrou doit être configurable en tant que verrou à ouverture ou fermeture sur coupure de courant

b. 1 x contact de porte

(i) Le contact de la porte doit surveiller l'état actuel d'ouverture/fermeture d'un point d'accès

c. 1 x bouton de sortie alimenté

(i) Un bouton de sortie doit permettre la libre circulation par le point d'accès

(ii) Le périphérique du bouton de sortie doit fournir une sortie de 12 V pour fournir une indication visuelle et un retour d'information au niveau du bouton de sortie.

(iii) Le périphérique du bouton de sortie doit pouvoir être désactivé dans le logiciel système s'il n'est pas utilisé, afin d'éviter que l'accès ne soit effectué par la manipulation matérielle.

d. 2 x relais

(i) Chaque relais doit être muni de contacts N.O. (normalement ouvert) et N.C. (normalement fermé)

(ii) Les contacts de relais doivent être libres de potentiel.

(iii) Chaque relais doit pouvoir commuter une charge résistive d'au moins 2 A à 30 V CC.

(iv) Un relais doit pouvoir être configuré comme sortie d'alarme

(v) Un relais doit pouvoir être configuré comme sortie de verrouillage

(vi) Un relais doit pouvoir être utilisé pour des dispositifs autres que le point d'accès sécurisé

e. 2 ports de lecteur

i) Il doit être possible d'utiliser une combinaison de lecteurs de proximité, de lecteurs de proximité clavier et de lecteurs résistants au vandalisme.

ii) Les périphériques de lecteur doivent fournir les données et l'alimentation aux lecteurs connectés.

(iii) Le périphérique du lecteur ne doit pas être limité à une entrée de données fixe, et accepte à la place les données lues à partir de divers types de badges de différentes longueurs, y compris, mais sans s'y limiter, aux données suivantes :

1. PIN
2. Code
3. ID de badge
4. ID d'identification Bluetooth

(iv) Le périphérique du lecteur doit émettre des états de courant pertinents pour le dispositif à contrôler afin de fournir une rétroaction au détenteur de badge sous la forme d'une LED et d'un haut-parleur.

(v) Le périphérique du lecteur doit fournir la puissance dont le lecteur a besoin pour fonctionner.

(vi) Un lecteur doit pouvoir être utilisé pour des dispositifs autres que le point d'accès sécurisé

f. 1 x entrée numérique

(i) Une entrée numérique doit pouvoir être configurée comme un bouton de sortie

(ii) Une entrée numérique doit pouvoir être configurée pour surveiller un bloc d'alimentation externe

(iii) Une entrée numérique doit pouvoir être utilisée pour des dispositifs autres que le point d'accès sécurisé

2. Il doit être possible d'assigner n'importe quel périphérique à différents dispositifs ou de fournir des fonctionnalités personnalisées.

3. Le contrôleur doit fournir deux ports SATA pour connecter des disques durs externes.

a. Le contrôleur doit fournir une sortie MOLEX alimentée

b. Le contrôleur doit fournir 2 ports SATA

c. Le contrôleur doit enregistrer la vidéo sur les disques en utilisant la configuration RAID
1.

4. Le contrôleur doit fournir un port de connecteur.

a. Les connecteurs doivent communiquer avec le système par l'intermédiaire du contrôleur.

b. Le contrôleur doit fournir PoE aux connecteurs.

5. Le contrôleur doit fournir un interrupteur de violation sans tension.

a. Le système doit déclencher un événement d'alarme lorsqu'un interrupteur de violation est déclenché.

6. Le contrôleur doit fournir des bornes de batterie.

a. Une batterie de 12 V CC 7Ah doit être installée.

b. Le contrôleur doit surveiller l'état et la charge de la batterie.

2.6 EXIGENCES SPÉCIFIQUES POUR LE CONNECTEUR D'ALARME [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. Le connecteur doit permettre le contrôle et la surveillance d'une alarme intrus.

2. Le connecteur doit permettre la surveillance d'une alarme incendie.

3. Le connecteur doit être petit et compact, destiné à être installé dans une armoire d'alarme existante.

4. Le connecteur doit comporter des voyants de détection des défauts.

5. Le connecteur doit être muni de bornes détachables pour un entretien rapide et simple.

B. Communications

1. Le connecteur doit comprendre une interface TCP/IP pour les communications réseau directement dans la carte de traitement (contrôleur) via un connecteur RJ45. Les modules complémentaires ne sont pas approuvés.

C. Alimentation électrique

1. L'article doit fonctionner à partir de l'alimentation en courant continu fournie par le contrôleur.

a. Aucune source d'alimentation supplémentaire ne doit être requise.

b. Les données et l'alimentation doivent utiliser le même câble, ce qui réduit au minimum les coûts d'installation et d'installation.

2. La tension de fonctionnement doit être de 30 V.

3. La consommation électrique au ralenti ne doit pas dépasser 0,6 W.

D. Affichage

1. Les périphériques doivent être étiquetés clairement et intuitivement.

a. Les étiquettes doivent être graphiques.

2. L'article doit comporter des LED pour la détection des défauts.

3. Les états périphériques suivants doivent être indiqués :

a. État du relais

b. État d'entrée (pour chaque entrée)

4. Une LED doit indiquer quand l'article est sous tension.

E. Température

1. L'article doit fonctionner de manière fiable dans la plage de température comprise entre +32 °F et +131 °F

(0°C à +55°C).

F. Boîtier

1. L'article doit être petit et compact de telle sorte qu'il puisse être installé dans un boîtier existant utilisé pour l'alarme correspondante.

G. Dimensions

1. Les dimensions du connecteur d'E/S ne doivent pas dépasser :
    a. Une largeur de 51mm (2 po)
    b. Une hauteur de 2,7 po (68 mm)
    c. Une profondeur de 1,3 po (34 mm)

H. Périphériques

1. Le connecteur d'alarme doit comporter un seul relais contrôlable.
    a. Chaque relais doit être muni de contacts COM, N.O. et N.C.
    b. Les contacts de relais doivent être exempts de tension.
    c. Chaque relais doit pouvoir commuter une charge résistive d'au moins :
    (i) 2A @ 24V CC
    (ii) 0,5 A à 125 V CA
    d. Chaque relais doit conserver son état lorsque le connecteur d'alarme perd sa puissance.
    e. La fonctionnalité du relais doit être configurable dans le logiciel de contrôle d'accès fourni avec le système.
2. Le connecteur d'alarme doit comporter 2 entrées numériques.
    a. Chaque entrée doit être formée de 2 terminaux.
    b. Chaque entrée doit pouvoir supporter au moins 14V.
    c. Les seuils que le système doit associer à chaque état sont les suivants :
    i) Faible : < 0,8 V
    ii) Élevé : > 3,0 V
    d. Chaque entrée doit être configurable pour déclencher une règle de déclencheur et d'action pour effectuer des tâches automatisées et un comportement personnalisé.
3. Le connecteur d'alarme ne doit pas contenir d'entrée de commutateur de falsification.
    a. Le connecteur d'alarme doit être installé à l'intérieur du boîtier d'une alarme ou d'un autre connecteur, dont le dispositif doit contenir son propre dispositif de violation.
    b. Il doit être possible d'utiliser une entrée de rechange sur le connecteur d'alarme ou sur un autre connecteur pour générer des événements d'alarme à l'intérieur du système si une entrée de violation est requise.

2.7 EXIGENCES SPÉCIFIQUES POUR LE CONNECTEUR SANS FIL [PAXTON10] {Supprimer au besoin — Connecteur sans fil requis pour PaxLock}

A. Caractéristiques

1. Le connecteur doit assurer la communication avec les poignées de porte sans fil.
2. Le connecteur doit assurer la communication avec les dispositifs Z-Wave.

3. Le connecteur doit être cascadable, ce qui permet de connecter des connecteurs sans fil supplémentaires les uns aux autres, ce qui étend leur couverture sans fil.

4. Le connecteur doit comporter des LEDs de détection des défauts.

B. Communications

1. Le connecteur doit comprendre une interface TCP/IP pour les communications réseau directement dans la carte de traitement (contrôleur) via un connecteur RJ45. Les modules complémentaires ne sont pas approuvés.

2. Le connecteur doit contenir une interface Bluetooth permettant de communiquer avec les poignées de porte électroniques.

a. Le connecteur doit communiquer en utilisant Bluetooth à faible consommation (BLE) 2,4 GHz

3. Le connecteur doit contenir une interface Z-Wave permettant de communiquer avec les dispositifs certifiés Z-Wave.

a. Le connecteur doit communiquer en utilisant Z-Wave 868,40 MHz et 869,85 MHz.

C. Alimentation électrique

1. L'article doit fonctionner à partir de l'alimentation en courant continu fournie par le contrôleur.

a. Aucune source d'alimentation supplémentaire ne doit être requise.

b. Les données et l'alimentation doivent utiliser le même câble, ce qui réduit au minimum les coûts d'installation et d'installation.

2. La tension de fonctionnement doit être de 30 V.

3. La consommation électrique au ralenti ne doit pas dépasser 0,7 W.

4. La consommation électrique pendant l'activité Bluetooth ne doit pas dépasser 0,8 W.

D. Affichage

1. L'article doit héberger des LED pour la détection des défauts. Les états suivants doivent être indiqués :

a. Santé et communication

b. Activité Bluetooth

c. Activité Z-Wave

E. Température

1. L'article doit fonctionner de manière fiable dans la plage de température comprise entre +32°F et +113 °F

(0°C à +45°C).

F. Boîtier

1. L'article doit être visiblement attrayant pour une installation à la vue des utilisateurs, réduisant ainsi les obstacles entre le connecteur et ses dispositifs de communication.

2. Le boîtier de l'article doit être blanc.

3. L'article doit être adapté pour le montage :

a. Sur un mur

b. Sur un plafond

c. Sur plaques de plâtre

d. Sur un boîtier arrière

G. Dimensions

1. Les dimensions du connecteur ne doivent pas dépasser :

a. Une largeur de 6,5 po (164 mm)

b. Une hauteur de 6,4 po (163 mm)

c. Une profondeur de 1,3 po (34 mm)

H. Périphériques

1. Le connecteur sans fil doit contenir un port RS485 pour le raccordement en série à des connecteurs supplémentaires.

a. Jusqu'à 3 connecteurs doivent être enchaînés en série à partir d'un contrôleur

b. Le pouvoir et la communication doivent être enchaînés en série.

2.8 EXIGENCES SPÉCIFIQUES POUR LES CAMÉRAS [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. Toutes les caméras doivent être capables de fournir une résolution 4K.

2. Toutes les caméras doivent contenir des capteurs à très faible luminosité pour l'enregistrement en faible luminosité.

a. La portée IR des caméras doit être d'au moins 30 mètres.

3. Toutes les caméras doivent contenir un stockage intégré pour l'enregistrement direct sur la caméra (stockage de bord).

4. Toutes les caméras doivent pouvoir enregistrer du son.

5. Chaque caméra doit fournir au système plusieurs flux vidéo de qualités différentes :

a. Un flux vidéo haute résolution, jusqu'à une résolution 4K à 20 FPS

b. Un flux vidéo basse résolution, jusqu'à 640 x 480 résolution à 15 IPS

c. Une image QCIF basse résolution, enregistrée à 1 IPS

6. La vidéo ne doit être enregistrée que lorsque du mouvement est détecté, ce qui maximise l'efficacité du stockage et réduit au minimum les séquences vidéo des scènes non impliquées.

7. Le fabricant doit fournir 4 variantes de caméra :

a. Caméra mini-bullet

b. Caméra mini-dôme

c. Caméra bullet à focale variable

d. Caméra dôme à focale variable

8. Toutes les caméras doivent être plug-and-play.

9. Toutes les caméras doivent communiquer sur un réseau IP.

10. Toutes les données doivent être conservées lors d'une perte de puissance.

B. Communication

1. La caméra doit traiter et enregistrer sa propre vidéo, sans nécessiter de communication constante avec un enregistreur vidéo externe.

2. La caméra doit communiquer avec le serveur et les clients via TCP/IP.

3. La bande passante vidéo maximale doit être configurable pour répondre aux exigences du réseau.

C. Interaction des utilisateurs

1. Toutes les caméras doivent être plug and play.

a. Par défaut, les caméras doivent enregistrer en 1080p à 20 IPS.

b. Par défaut, les caméras doivent enregistrer les séquences vidéo dans leur stockage interne.

2. Les paramètres de caméra suivants doivent être configurables :
    a. Rotation vidéo
    b. Norme vidéo (PAL/NTSC)
    c. Résolution vidéo
    d. Fréquence d'images (FPS)
    e. Débit binaire maximal (Kbit/s)
3. Pour les caméras à focale variable, la configuration supplémentaire suivante doit être disponible :
    a. Distance focale
4. Les paramètres d'enregistrement vidéo suivants doivent être configurables :
    a. Emplacement de stockage vidéo
    (i) Interne — Enregistrer sur la caméra
    (ii) Externe — Enregistrer sur un emplacement du réseau
    b. Période de stockage vidéo/Suppression automatique de la vidéo après une période de temps définie
5. Après l'installation, aucune autre interaction avec le matériel ne doit être requise.

D. Alimentation
1. Chaque caméra doit être alimentée par PoE.
2. La consommation d'énergie maximale de toute caméra ne doit pas dépasser 15W.

E. Température
1. Chaque caméra doit satisfaire aux normes de température requises pour un produit externe.
    a. La caméra doit fonctionner de manière fiable dans la plage de température comprise entre -22 °F et +140 °F (-30 °C à +60 °C).

F. Boîtier
1. Chaque caméra doit être adaptée au montage :
    a. Sur un mur
    b. Sur un plafond
2. Chaque caméra doit être résistante au vandalisme à l'IK10.
    a. Le boîtier extérieur du boîtier principal de la caméra doit être en métal.
3. Chaque caméra doit être étanche aux intempéries conformément à la norme IP66.

G. Dimensions
1. Les dimensions de la caméra min-bullet ne doivent pas dépasser :
    a. Une largeur de 2,8 po (70 mm)
    b. Une hauteur de 2,7 po (68 mm)
    c. Une profondeur de 6,7 po (171 mm)
2. Les dimensions de la caméra mini-dôme ne doivent pas dépasser :
    a. Un diamètre de 4,4 po (111 mm)
    b. Une profondeur de 3,2 po (82,4 mm)
3. Les dimensions de la caméra bullet à focale variable ne doivent pas dépasser :
    a. Un diamètre de 5,67 po (144,13 mm)
    b. Une profondeur de 13,10 po (332,73 mm)

4. Les dimensions de la caméra dôme à focale variable ne doivent pas dépasser :
    a. Un diamètre de 6 po (153,4)
    b. Une profondeur de 5,2 po (133,1 mm)

H. Périphériques

1. Chaque caméra doit contenir un emplacement pour carte mémoire pour le stockage vidéo interne.
    a. La caméra doit prendre en charge les cartes mémoire suivantes :
    i) Micro SD
    ii) Micro SDHC
    iii) Micro SDXC
    b. La caméra doit prendre en charge les cartes mémoire jusqu'à une capacité de 128 Go.
    c. La vitesse de lecture de la mémoire doit être d'au moins 25 Mo/s.
    d. La vitesse de lecture de la mémoire doit être d'au moins 95 Mo/s.

2.9 EXIGENCES SPÉCIFIQUES POUR LE LOGICIEL [PAXTON10]

A. Interface utilisateur Web

1. Le logiciel doit être hébergé sur le serveur.
2. Le logiciel doit être accessible à partir de tout ordinateur doté d'un accès au réseau.
3. Aucune installation ne doit être requise à un poste de travail client.
4. Le logiciel doit être gratuit.
5. Le fabricant du logiciel doit fournir gratuitement les mises à jour et mises à niveau.
6. Le logiciel doit offrir toutes les fonctionnalités nécessaires à la gestion d'un système de contrôle d'accès.
7. Le logiciel doit offrir toutes les fonctionnalités nécessaires à la gestion d'un système de gestion vidéo.

B. Accès à distance

1. Il doit être possible d'accéder au logiciel depuis n'importe où dans le monde grâce à une connexion Internet.
2. Cela peut être autorisé dans le logiciel afin de restreindre l'accès à distance aux utilisateurs sélectionnés.

C. Exigences relatives aux postes de travail

1. Il doit être possible d'accéder au logiciel à partir de tout ordinateur ou dispositif exécutant la dernière version de :
    a. Google Chrome.
    b. Apple Safari
2. Il doit être possible d'accéder au logiciel depuis n'importe quel smartphone ou tablette à l'aide d'une application dédiée.
    a. L'application doit être disponible sur les systèmes d'exploitation suivants :
    (i) iOS
    (ii) Android
    b. L'application doit être gratuite.

D. Affichage

1. Le logiciel doit fournir une interface utilisateur propre et simple.

2. La navigation doit être visible sur tous les écrans, afin de permettre une navigation rapide dans toutes les zones du logiciel.

3. Un ruban en tête de page doit être prévu pour offrir d'autres commandes.

a. Il doit être possible de réduire le ruban, afin d'augmenter la surface de travail.

b. Pour préserver la simplicité, le ruban doit être rempli avec les commandes pertinentes pour l'élément actuellement consulté.

4. Il doit être possible d'ajuster la façon dont les entités sont présentées :

a. Grandes icônes, idéales pour les appareils à écran tactile et également utiles pour la recherche graphique. Les images de l'utilisateur et d'autres entités doivent être affichées lors de la visualisation de grandes icônes.

b. Détails, qui doivent fournir des informations supplémentaires le cas échéant et permettre le tri des entités en vue d'une utilisation plus avancée.

5. La façon dont le logiciel est visualisé doit être sauvegardé pour chaque utilisateur du logiciel, de sorte que ses préférences en matière de conception et de mise en page soient mémorisées chaque fois qu'il se connecte.

E. Interaction

1. Le logiciel doit prendre en charge l'interaction avec l'écran tactile.

2. Le logiciel doit prendre en charge les appareils mobiles.

3. Des infobulles doivent être fournies pour chaque commande afin d'informer le comportement.

F. Regroupement

1. Le logiciel doit fournir une méthode simple mais efficace pour l'organisation des entités du logiciel.

2. Le logiciel doit permettre une segmentation et un agencement adaptés aux schémas du département et du bâtiment.

G. Gestion des données

1. Le logiciel doit fournir les capacités nécessaires pour se conformer aux réglementations en matière de protection des données.

2. Tous les utilisateurs du logiciel doivent être forcés de créer un mot de passe sécurisé.

3. Le logiciel doit permettre de :

a. Supprimer des utilisateurs

b. Supprimer des rapports

c. Supprimer des événements

d. Supprimer automatiquement des événements après une période de temps spécifiée

e. Effacer une vidéo

f. Effacer automatiquement une vidéo après une période de temps spécifiée

H. Langue

1. Le logiciel doit être disponible dans les langues suivantes :

a. Anglais (Royaume-Uni)

b. Anglais (États-Unis)

c. Français

d. Allemand

e. Espagnol

I. Aide et assistance

1. Le logiciel doit fournir une aide aux utilisateurs du logiciel sous la forme d'info-bulles, d'assistants, de vidéos et de documentation.

a. Les assistants devront guider les utilisateurs à travers des tâches spécifiques, donnant à l'utilisateur la possibilité d'accomplir sa tâche au fur et à mesure qu'il apprend les étapes requises.

b. Les vidéos doivent fournir des instructions et des informations à l'appui pour accomplir les tâches et explorer les zones de l'interface utilisateur.

c. La documentation doit se composer de notes d'application, d'instructions et de fiches techniques.

d. Des infobulles doivent être disponibles lors du survol d'un curseur sur les commandes et les options.

(i) Lorsqu'elles sont disponibles, les info-bulles doivent contenir un lien permettant d'orienter l'utilisateur vers des informations complémentaires.

2. Un outil d'aide intégré doit permettre à l'utilisateur de localiser les informations d'assistance dont il a besoin.

a. L'outil d'aide doit être accessible à partir de tous les emplacements du logiciel.

J. Notes de mise à jour

1. Lorsqu'une mise à jour logicielle est disponible, les notes de mise à jour doivent être présentées à l'utilisateur.

2. Les notes de mise à jour doivent informer l'utilisateur de ce que la mise à jour contiendra, ainsi que toute information importante relative à la mise à jour.

2.10 EXIGENCES SPÉCIFIQUES POUR LES FONCTIONNALITÉS LOGICIELLES [PAXTON10]

A. Personnes

1. Les utilisateurs doivent être ajoutés au système à l'aide du logiciel.

a. Il doit être possible de créer au moins 50 000 utilisateurs.

b. Il doit être possible d'attribuer au moins 50 000 identifiants uniques aux utilisateurs.

2. Les utilisateurs doivent se voir attribuer des autorisations pour déterminer ce que chaque utilisateur peut actionner, configurer ou afficher.

a. Les utilisateurs n'ont accès qu'aux points d'accès et au contrôle des périphériques qui sont dans les limites des autorisations qui leur sont attribuées.

b. Les utilisateurs doivent pouvoir se connecter au logiciel et visualiser/modifier les zones qui sont dans les limites des autorisations qui leur sont attribuées.

3. Chaque enregistrement utilisateur doit contenir des champs de saisie pour stocker les données de l'utilisateur.

a. Les champs suivants sont disponibles par défaut :

(i) Adresse électronique

(ii) Date de début de validité

(iii) Date d'expiration

b. D'autres champs doivent être disponibles, le cas échéant, pour saisir des informations supplémentaires :

(i) Numéro de téléphone portable

(ii) Immatriculation des voitures

(iii) Adresse 1

(iv) Adresse 2

(v) Ville

(vi) Pays

(vii) Code postal

c. Il doit être possible de créer des champs de saisie personnalisés lorsque les données ci-dessus ne couvrent pas les données à stocker pour chaque utilisateur. Une étiquette à afficher et le type de données à saisir ou à stocker doivent être sélectionnables.
Les types de données suivants doivent être pris en charge :

(i) Booléen — case à cocher

(ii) Date

(iii) E-mail

(iv) Nombre

(v) Texte

4. Il doit être possible de télécharger une image de chaque utilisateur.

a. Chaque enregistrement utilisateur doit avoir une silhouette de personne comme image par défaut.

b. Il doit être possible de télécharger une image pour remplacer l'image par défaut.

c. Le logiciel doit permettre le téléchargement d'images jusqu'à 4 Mo.

d. Au minimum, les formats d'image suivants doivent être pris en charge :

(i) JPEG

(ii) JPG

(iii) GIF

(iv) PNG

e. Il doit être possible de modifier l'image téléchargée dans le logiciel. Au minimum, il doit être possible de réaliser les objectifs suivants :

(i) Recadrer l'image téléchargée.

(ii) Placer une bordure autour de l'image téléchargée.

(iii) Ajouter une ombre à l'image téléchargée.

f. L'image doit être utilisée :

(i) Comme moyen d'identifier un utilisateur

(ii) Comme méthode de recherche d'utilisateurs à côté de leur nom

(iii) Dans les plans du site pour associer un utilisateur à un identifiant en cours de lecture

(iv) Dans les rapports vidéo pour associer un utilisateur à un identifiant en cours de lecture

(v) Dans les tableaux de bord pour identifier un utilisateur

(vi) Dans les rapports d'appel comme confirmation visuelle

5. Il doit être possible d'attribuer des informations d'identification à un utilisateur.

a. Les types d'identifiants suivants doivent être pris en charge :

(i) Mot de passe

(ii) Badge

(iii) Identifiant intelligent

(iv) PIN

b. Les mots de passe doivent être requis pour que l'utilisateur puisse accéder au logiciel.

(i) Les utilisateurs sont limités à avoir un seul mot de passe.

(ii) Les mots de passe doivent être créés par l'utilisateur lorsqu'il tente de se connecter pour la première fois.

(iii) Le logiciel doit appliquer les mots de passe pour répondre à un critère de sécurité.

(iv) Les mots de passe doivent :

1. Comporter au moins 7 caractères.
2. Comporter au moins 3 types de caractères différents : majuscules/minuscules/nombre/ponctuation

c. Des badges doivent être exigés pour qu'un utilisateur ait accès et contrôle des points d'accès et des dispositifs d'accès sur un système.

(i) Il doit être possible d'attribuer plusieurs badges à chaque utilisateur.

(ii) Les badges sont ajoutés au système au moyen des éléments suivants :

1. Un lecteur de bureau fourni par le fabricant du logiciel.
2. Un événement d'accès non valide

(iii) Plusieurs types d'identifiants doivent être pris en charge. Il doit être possible pour les utilisateurs de sélectionner un type et de donner un nom à l'identifiant à des fins de convivialité et de référence.

(iv) Chaque type de badge doit être distingué par une image unique.

(v) Il doit être possible de marquer un badge comme perdu, ce qui supprimera tous les droits d'accès de ce badge tout en permettant à l'utilisateur de rester actif avec d'autres badges.

d. Les identifiants intelligents permettent aux utilisateurs d'utiliser leur smartphone ou tablette pour accéder aux points d'accès et aux dispositifs d'accès d'un système et le contrôle de ceux-ci.

(i) Il doit être possible d'attribuer plusieurs identifiants intelligents à chaque utilisateur.

(ii) Les identifiants intelligents doivent exister en tant qu'application enregistrée sur l'appareil intelligent d'un utilisateur.

(iii) Les systèmes d'exploitation mobiles suivants doivent être pris en charge :

1. Android
2. iOS

(iv) Les identifiants intelligents doivent être gratuitement émettables et utilisables.

(v) Les identifiants intelligents doivent être émis à partir du logiciel via e-mail.

(vi) L'e-mail d'identifiant intelligent doit contenir des instructions, un lien de téléchargement et un identifiant d'enregistrement unique pour l'utilisateur adressé.

(vii) Le numéro d'inscription ne doit être valide que pour un seul appareil.

(viii) Il sera possible de marquer un identifiant intelligent comme perdu, ce qui supprimera tous les droits d'accès de ce badge tout en permettant à l'utilisateur de rester actif avec d'autres badges.

(ix) Il doit être possible d'exiger une vérification lors de l'utilisation des identifiants intelligents. Lorsqu'une vérification est requise, l'utilisateur doit s'authentifier en utilisant :

1. Empreintes digitales, à l'aide du lecteur biométrique intégré à leurs appareils

2. Code d'accès ou motif, en utilisant le verrouillage sécurisé intégré à leurs appareils

(x) Il doit être possible de saisir un profil horaire durant lequel la vérification est requise.

e. Les PIN fournissent un moyen sans badge de valider et d'identifier un utilisateur.

(i) Les utilisateurs ne doivent avoir qu'un seul code PIN.

(ii) La longueur du PIN doit être configurée dans le logiciel pour répondre aux exigences de sécurité du projet.

(iii) Le système génère un événement d'alarme de pirate clé lorsque plusieurs tentatives échouées sont effectuées sur un lecteur digicode, ce qui protège contre les pirates informatiques et les tentatives d'accès non autorisées.

f. Il doit être possible d'exiger une combinaison d'identifiants d'un utilisateur, telles que badge + PIN, pour assurer la sécurité du site.

6. Il doit être possible d'interdire un utilisateur.

a. Interdire un utilisateur supprimera son accès et le contrôle de tous les points d'accès et dispositifs.

b. Interdire un utilisateur supprimera son accès au logiciel.

c. Il doit être possible de réautoriser un utilisateur pour restaurer toutes ses autorisations précédentes.

B. Dispositifs

1. Le matériel doit être représenté et configuré en tant qu'entités logicielles, dénommées « dispositifs ».

2. Le logiciel doit prendre en charge les types de dispositifs suivants :

a. Point d'accès

b. Dispositif contrôlable

c. Dispositif d'entrée numérique

d. Alarme intrusion

e. Alarme incendie

f. Caméra

g. Enregistreur vidéo

3. Il doit être possible d'associer le dispositif logiciel créé au matériel qu'il doit représenter.

a. La configuration à l'intérieur du dispositif logiciel doit avoir une incidence sur le matériel pour effectuer le comportement souhaité.

4. Les points d'accès doivent fournir la configuration suivante :

a. Mode de fonctionnement :

1. Temporisé, déverrouille le point d'accès pendant une durée déterminée à chaque fois que chaque identifiant valide est lu.

2. Bascule, inverse l'état du verrou à chaque identifiant valide lu.

b. Temps d'ouverture de la porte, détermine pendant combien de temps le point d'accès reste déverrouillé lorsqu'il fonctionne en mode temporisé.

c. Programmation de déverrouillage, permet au point d'accès de rester déverrouillé pendant des périodes spécifiées.

d. LED de lecteur, permet à tous les lecteurs mappés d'avoir leurs LED activées ou désactivées.

e. Son du lecteur, permet à tous les lecteurs mappés d'avoir leur son coupé ou activé

f. Toujours autoriser la sortie, lorsqu'il est activé ceci permet aux utilisateurs valides de sortir, même en dehors de leur temps autorisé.

g. Options d'authentification, configuration du type d'identifiant que les utilisateurs doivent fournir pour accéder à la zone.

h. Plage de lecture Bluetooth, configuration du fonctionnement des identifiants intelligents et des badges Bluetooth.

i. Alarmes au son :

1. Porte laissée ouverte
2. Porte forcée
3. Échec du bloc d'alimentation

j. Caméras, qui doivent associer les images de la caméra aux événements relatifs au point d'accès.

5. Les dispositifs contrôlables doivent fournir la configuration suivante :

a. Mode de fonctionnement :

1. Temporisé, allume l'appareil pendant une durée spécifiée à chaque fois que des identifiants valides sont lus.
2. Bascule, inverse l'état de l'appareil à chaque fois que des identifiants valides sont lus.
3. Momentané, change l'état de la sortie pendant une fraction de seconde, avant de revenir en arrière.

b. À temps, détermine la durée de fonctionnement du dispositif en mode temporisé.

c. Selon le programme, permet à l'appareil de rester en fonctionnement pendant des périodes spécifiées.

d. LED de lecteur, permet à tous les lecteurs mappés d'avoir leurs LED activées ou désactivées.

e. Son du lecteur, permet à tous les lecteurs mappés d'avoir leur son coupé ou activé

f. Toujours autoriser l'arrêt, lorsqu'il est activé, permet aux utilisateurs valides d'éteindre l'appareil, même en dehors de l'heure autorisée.

g. Options d'authentification, configuration du type d'identification que les utilisateurs doivent fournir pour contrôler l'appareil.

h. Plage de lecture Bluetooth, configuration du fonctionnement des identifiants intelligents et des badges Bluetooth.

i. Caméras, qui doivent associer les images de la caméra à des événements relatifs à l'appareil.

6. Les dispositifs d'entrée numériques doivent fournir la configuration suivante :

a. Événement, permet à l'utilisateur de définir un événement qui doit être déclenché lorsque l'entrée change d'état.

b. Caméras, qui doivent associer les images de la caméra à des événements se rapportant à l'appareil.

c. Les alarmes intrusion doivent fournir la configuration suivante :

d. Dans quelle condition d'entrée l'alarme est armée.

e. Dans quelle condition d'entrée l'alarme est active.

f. Durée d'impulsion requise pour changer l'état d'armement de l'alarme.

g. Portes extérieures, permet à certaines portes de rester verrouillées lorsque l'alarme intrusion est armée.

h. Désarmement des portes, permet de désarmer l'alarme intrusion aux portes sélectionnées.

i. LED du lecteur, permet à tous les lecteurs mappés d'avoir leurs LED activées ou désactivées.

j. Son du lecteur, permet à tous les lecteurs mappés d'avoir leur son coupé ou activé

k. Options d'authentification, configuration du type d'identification que les utilisateurs doivent fournir pour contrôler l'alarme.

l. Plage de lecture Bluetooth, configuration de la façon dont les identifiants intelligents et les badges Bluetooth fonctionnent.

m. Caméras, qui doivent associer les images de la caméra à des événements liés à l'alarme.

n. Les alarmes d'incendie doivent fournir la configuration suivante :

o. Dans quelle condition d'entrée l'alarme est active.

p. Portes coupe-feu, s'assure que les portes sélectionnées sont déverrouillées lorsque l'alarme incendie est active.

q. Les caméras, qui doivent associer les images de la caméra à des événements liés à l'alarme.

7. Les caméras et les enregistreurs vidéo doivent fournir la configuration suivante :

a. Calendrier d'enregistrement, configuration pendant laquelle la caméra doit enregistrer les périodes de temps.

b. Emplacement de l'enregistrement, permet d'enregistrer la vidéo sur un emplacement réseau ou sur la caméra ou l'enregistreur vidéo.

c. Période de stockage vidéo, permet l'effacement automatique de la vidéo après un nombre défini de jours.

d. Rotation vidéo, permet la rotation de la vidéo {Caméras Paxton10 seulement}

e. La distance focale de la caméra, qui doit permettre de régler la distance focale de la caméra {Caméras vari-focales Paxton10 seulement}

f. Qualité vidéo, permettant au système de visualiser, et pour certaines caméras configurer, la résolution vidéo, la fréquence d'images et le débit binaire maximal.

g. Un aperçu vidéo doit être fourni en fonction de la configuration de la caméra.

(i) Dispositifs, qui doivent associer des séquences vidéo à des événements survenus sur les dispositifs sélectionnés.

C. Rapports sur les événements

1. Les rapports d'événements doivent être utilisés pour afficher l'activité du système.
2. Les événements doivent être générés pour, mais sans s'y limiter :

a. Lecture valide d'identifiant

b. Lecture d'identifiant non valide (identifiant inconnu, autorisations non valides, identifiant marqué comme perdu)

c. Point d'accès déverrouillé/verrouillé

d. Dispositif allumé/éteint

e. Changement d'état en entrée

f. Alarme à un point d'accès (porte forcée, laissée ouverte, falsification)

g. Alarme d'intrusion armée / désarmée

h. Alarme d'intrusion active

i. Alarme incendie active

j. Événements système (matériel en ligne/hors ligne, événements serveur)

k. Événements logiciels (personne/appareil modifié)

3. Il doit être possible de filtrer les événements selon les critères suivants :

a. L'utilisateur auquel l'événement se rapporte.

b. Le dispositif auquel l'événement se rapporte.

c. L'heure à laquelle l'événement s'est produit.

d. Le type d'événement (lecture des identifiants, alarme, système/logiciel)

e. Contient des séquences vidéo

4. Il existe une sélection de rapports de défaillance pour indiquer les domaines d'intérêt communs, y compris les suivants :

a. Tous les événements

b. Tous les événements de la semaine dernière

c. Tous les événements cette semaine

d. Tous les événements d'aujourd'hui

e. Tous les événements hier

f. Badges expirés

g. Premiers et derniers événements

h. Dernière position connue

i. Liste de tous les utilisateurs

j. Badges perdus

k. Autorisations

l. Badge utilisé pour la dernière fois

m. Badges inutilisés

n. Qui est entré aujourd'hui

5. L'utilisateur doit être en mesure de créer des rapports personnalisés pour répondre à ses propres besoins.

6. L'interaction d'événement suivante doit être disponible :

a. Afficher la vidéo associée à un événement.

b. Visualiser le profil de la personne auquel un événement se rapporte.

c. Confirmer une alarme et laisser un commentaire sur l'événement.

d. Ajouter une information d'identification au système à partir d'un événement d'accès refusé.

e. Marquer un utilisateur comme en sécurité ou pas en sécurité dans un rapport d'appel.

7. Les événements affichés dans un rapport doivent être filtrés pour ne montrer que ceux que le spectateur a la permission de voir.

D. Rapports vidéo

1. Les rapports vidéo doivent être utilisés pour afficher des vidéos en direct et archivées enregistrées par des caméras du système.

2. Les rapports vidéo doivent être évolutifs, offrant une vue à partir d'une caméra, jusqu'à un maximum de 20 caméras.

a. L'affichage doit être ajusté dynamiquement pour permettre une visualisation optimale du nombre de caméras figurant dans le rapport.

b. Le flux vidéo affiché doit être ajusté en fonction du nombre de caméras actuellement affichées, en optimisant l'utilisation de la bande passante du réseau et la zone de visualisation du client.

3. Il doit être possible de visualiser les événements dans un rapport vidéo.

a. Les événements doivent être pré-filtrés pour ne montrer que les événements qui se rapportent aux dispositifs qui peuvent être vus par les caméras figurant dans le rapport.

b. Il doit être possible de filtrer les événements affichés.

c. Les événements liés à l'appareil et les détails de l'utilisateur doivent être superposés sur la vidéo, le cas échéant.

4. Une sélection d'options de lecture doit être disponible, y compris :

a. Lecture/pause

b. Modifier la vitesse de lecture

c. Aller en avant / en arrière de 15 secondes

d. Aller à la vidéo en direct

e. Recherche avec aperçu QCIF

5. Les commandes de vue par caméra doivent être disponibles, y compris :

a. Activer/couper le volume

b. Afficher/masquer le nom de la caméra

c. Afficher/masquer l'heure de la caméra

d. Ces réglages ne doivent pas affecter la caméra elle-même ou l'enregistrement vidéo, ils ne doivent affecter que la lecture et la vue pour le client actuel.

6. Il doit être possible d'exporter un clip vidéo vers un emplacement réseau.

a. La période d'exportation doit être identifiée à l'aide d'une interface utilisateur simple et graphique.

b. Par défaut, 5 minutes de clip vidéo sont sélectionnées.

(i) La durée minimale du clip doit être d'une minute.

(ii) La durée maximale du clip doit être de 30 minutes.

c. Le clip exporté doit contenir du son

d. Le clip doit être téléchargé au format MP4.

7. Il doit être possible d'exporter un instantané fixe de la vidéo vers un emplacement réseau.

a. Le système doit fournir une sélection d'images instantanées entourant l'heure choisie.

b. L'instantané doit être téléchargé au format JPEG.

8. Il doit être possible de marquer un moment dans le temps pour référence future.

a. Il doit être possible de donner un nom ou une description à un signet.

b. Les signets doivent être clairement identifiés sur la chronologie vidéo.

c. Les signets doivent être automatiquement supprimés lorsque la vidéo est supprimée.

d. Des commandes doivent être disponibles pour naviguer facilement à travers tous les signets.

e. Il n'y a pas de limite au nombre de signets pouvant être créés.

9. La recherche intelligente doit être disponible pour la recherche de mouvement dans la vidéo enregistrée.

a. La recherche intelligente doit permettre aux utilisateurs de localiser facilement le moment où un élément a été déplacé ou quand une activité a eu lieu.

b. L'utilisateur doit être en mesure de mettre en évidence des zones sur plusieurs flux vidéo, qui doit rechercher dans les flux vidéo le moment où le mouvement s'est produit dans les zones spécifiées.

10. Le zoom numérique doit permettre aux utilisateurs de zoomer sur un flux vidéo pour afficher des détails supplémentaires.

a. Lorsque vous effectuez un zoom avant sur un flux vidéo, le système doit passer au flux de résolution la plus élevée dont il dispose pour la caméra spécifiée.

b. Le zoom numérique ne doit pas affecter l'enregistrement de la vidéo, ni l'affichage pour les autres utilisateurs.

c. Le zoom numérique doit être disponible à l'aide des commandes à l'écran, de la molette de la souris et de l'écran tactile.

11. Plein écran et affichage modal pour une visualisation élargie.

a. Il doit être possible de placer chaque caméra individuellement en plein écran ou en mode modal.

b. Lorsqu'il est affiché en plein écran ou en mode modal, le système doit passer au flux de résolution la plus élevée dont il dispose pour la caméra spécifiée.

12. Il n'y a pas de limite au nombre de rapports vidéo pouvant être créés.

13. La visualisation d'un rapport vidéo est autorisée de telle sorte que chaque utilisateur du logiciel ne puisse visionner que la vidéo qu'il est autorisé à voir.

E. Tableaux de bord

1. Les tableaux de bord fournissent une vue personnalisée avec des contrôles spécifiques à l'utilisateur, configurés pour répondre aux exigences de chaque utilisateur.

2. Les tableaux de bord sont constitués d'une combinaison des widgets suivants :

a. Événements

(i) Lorsqu'il est ajouté à un tableau de bord, un widget d'événements doit afficher tous les événements et toutes les activités du système.

(ii) Il doit être possible de filtrer le widget événements pour ne montrer que des événements spécifiques.

b. Alertes système

(i) Lorsqu'il est ajouté à un tableau de bord, un widget d'alerte système surveille le système et les alarmes d'accès.

(ii) Il doit être possible de configurer le widget pour afficher des alarmes pour des dispositifs spécifiques ou des types d'alarme.

(iii) Le widget doit fournir des informations sur les événements d'alarme les plus récents.

(iv) Il doit être possible de visionner une vidéo d'un événement d'alarme.

c. Systèmes d'alarme

(i) Lorsqu'il est ajouté à un tableau de bord, un widget de systèmes d'alarme doit surveiller l'état actuel des alarmes incendie sélectionnées ou des alarmes intrusion.

d. Vidéo

(i) Le widget vidéo doit ajouter des caméras vidéo à un tableau de bord, permettant de visionner des vidéos en direct et archivées.

(ii) Chaque widget vidéo doit permettre de visualiser la vidéo d'une seule caméra.

(iii) Les commandes suivantes doivent être prises en charge lorsqu'elles sont vues dans un tableau de bord :

1. Plein écran/modal
2. Modifier la vitesse de lecture
3. Revenir 15 secondes en arrière
4. Aller à la vidéo en direct
5. Recherche avec aperçu QCIF
6. Zoom numérique
7. Exporter l'élément
8. Exporter l'instantané
9. Afficher/masquer le nom de la caméra
10. Afficher/masquer l'heure de la caméra
11. Activer/Désactiver l'audio

e. Boutons programmables

(i) Les boutons programmables doivent permettre des actions définies sur mesure à partir d'un clic sur un bouton.

(ii) Le comportement du bouton programmable doit être configuré et géré dans un emplacement central.

(iii) Les boutons programmables doivent être graphiques et indiquer quand ils ont été pressés.

(iv) Un seul widget doit contenir un nombre de boutons programmables.

f. Carte de visite

(i) Lorsqu'il est ajouté à un tableau de bord, un widget de carte de visite doit afficher l'image et les détails de chaque utilisateur lorsqu'ils interagissent avec le système.

(ii) Le widget de carte de visite doit afficher l'image de l'utilisateur à mesure que l'utilisateur entre dans une zone.

(iii) Le widget de carte de visite doit afficher les coordonnées de l'utilisateur à mesure que l'utilisateur entre dans une zone.

(iv) Le widget doit être configurable sur le dispositif ou point d'accès à surveiller, et les événements à afficher.

(v) Il doit être possible de visionner la vidéo de l'interaction d'un utilisateur.

g. Plan du site

(i) Lorsqu'il est ajouté à un tableau de bord, un widget de plan de site doit fournir une carte graphique interactive du site.

(ii) Le widget doit afficher un plan de site à partir du système.

(iii) Le plan du site doit être créé et géré dans un espace dédié du logiciel.

(iv) Le widget doit permettre la navigation vers d'autres plans de site.

(v) Le widget doit fournir les fonctionnalités et interactions suivantes :

1. Déverrouiller la porte

2. Dispositif de commande
3. Armer/désarmer l'alarme
4. Confirmer l'alarme
5. Accéder à la configuration du périphérique
6. Afficher les événements de l'appareil
7. Voir la vidéo de l'appareil
8. Voir la vidéo de la caméra

h. Qui est là aujourd'hui

(i) Le widget doit fournir un appel des utilisateurs qui ont été enregistrés sur place le jour actuel.

(ii) Le widget doit fournir les détails suivants :

1. Nom de la personne
2. Groupe de personnes ou département
3. Date et heure de leur enregistrement
4. Emplacement (appareil) où ils ont été enregistrés

i. Météo

(i) Un widget de météo doit fournir une prévision météorologique pour un endroit déterminé.

(ii) Le widget doit permettre la recherche d'emplacement en texte libre.

3. Les tableaux de bord doivent être composés de 1 à 16 widgets.
4. Les widgets et leur disposition doivent être définis par le client.
5. Il ne doit pas y avoir de limite au nombre de tableaux de bord pouvant être créés.
6. Les tableaux de bord doivent permettre les autorisations de telle sorte que chaque utilisateur du logiciel ne voit que les tableaux de bord appropriés à ses tâches et à son rôle.

F. Plans des sites

1. Les plans du site doivent fournir une visualisation graphique et une interaction avec le site.
2. Il doit être possible de télécharger une image à utiliser comme plan de site.

(i) Le logiciel doit permettre le téléchargement d'images jusqu'à 4 Mo.

(ii) Au minimum, les formats d'image suivants doivent être pris en charge :

1. JPEG
2. JPG
3. GIF
4. PNG

(iii) Il doit être possible de recadrer l'image téléchargée dans le logiciel.

3. Des dispositifs doivent être ajoutés à un plan de site pour représenter le point d'accès physique ou le dispositif.

a. Les icônes de l'appareil doivent indiquer l'état actuel du dispositif en changeant de couleur et en clignotant.

b. Les icônes de l'appareil doivent afficher les événements associés à l'appareil au fur et à mesure qu'ils se produisent.

c. Il doit être possible d'interagir avec l'icône du dispositif pour commander le dispositif ou déverrouiller la porte.

d. Il doit être possible de visualiser la vidéo d'une caméra à partir d'un plan de site.

4. Des icônes de navigation doivent être ajoutées à un plan de site pour fournir des liens vers d'autres plans de site, permettant la navigation entre différents sites ou plusieurs étages d'un bâtiment.

a. Lorsqu'ils sont cliqués, les icônes de navigation dirigent l'utilisateur vers un plan de site défini.

b. Les icônes de navigation doivent afficher des icônes d'événement pour représenter les événements survenant sur les appareils du site lié.

c. La transition utilisée lors de la commutation des plans de site doit imiter l'emplacement du site en perspective.

5. Des boutons programmables doivent être ajoutés à un plan de site pour fournir des actions définies personnalisées à partir d'un clic de bouton.

a. Les boutons programmables doivent être configurables par l'utilisateur pour effectuer diverses actions lorsqu'il clique dessus.

b. Le comportement des boutons programmables doit être configuré et géré dans un emplacement central.

c. Les boutons programmables doivent être graphiques et indiquer quand ils ont été pressés.

6. Des zones d'alarme doivent être ajoutées à un plan de site afin de mettre en évidence les activités importantes.

a. Les zones d'alarme doivent indiquer les événements d'alarme pour certains dispositifs, tels que les sondes d'alarme d'intrus.

b. Les zones d'alarme doivent mettre en évidence une partie ou la totalité d'un plan de site pour alerter l'utilisateur.

c. L'utilisateur doit pouvoir définir la zone que représente l'alarme.

7. Des étiquettes doivent être ajoutées à un plan de site afin de fournir des instructions à l'utilisateur et des titres de zone.

a. Les étiquettes doivent être des étiquettes textuelles simples qui peuvent fournir des renseignements et des notes supplémentaires au plan du site.

8. Un plan de site doit être visualisable en 2D et 3D.

a. En 3D, il doit être possible de faire pivoter le plan du site.

G. Autorisations d'accès aux bâtiments

1. Les autorisations d'accès aux bâtiments doivent être utilisées pour gérer l'accès des utilisateurs aux périphériques.

2. Il n'y a pas de limite au nombre d'autorisations d'accès aux bâtiments qui peuvent être créées.

3. Il doit être possible d'attribuer aux utilisateurs plusieurs autorisations d'accès aux bâtiments.

4. Il doit être possible d'attribuer des appareils à plusieurs autorisations d'accès aux bâtiments.

5. Il doit être possible d'attribuer des profils horaires à plusieurs autorisations d'accès aux bâtiments.

6. L'utilisateur n'a accès à un appareil que s'il est combiné en autorisation d'accès aux bâtiments avec un planning actif.

H. Autorisations logicielles

1. Les autorisations logicielles doivent être utilisées pour gérer l'accès des utilisateurs au logiciel.

2. Il n'y a pas de limite au nombre d'autorisations logicielles pouvant être créées.

3. Il doit être possible d'attribuer aux utilisateurs plusieurs autorisations logicielles.

4. Il doit être possible de sélectionner différents niveaux d'autorisations pour chaque section logicielle. Les niveaux suivants doivent être possibles :

a. Complet — accès à la création/modification/suppression

b. Lecture — accès à la vue

c. Événements — accès à la consultation des événements

5. Un utilisateur n'a accès au logiciel que s'il est inclus dans une autorisation logicielle.

a. L'utilisateur n'a accès qu'aux zones du logiciel spécifiées dans l'autorisation logicielle.

6. Les zones logicielles suivantes peuvent être individuellement autorisées :

a. Tableaux de bord ou groupes de tableaux de bord spécifiés

b. Rapports ou groupes de rapports spécifiés

c. Plans de site ou groupes de plans de sites spécifiés

d. Personnes ou groupes de personnes spécifiés

e. Règles, ou groupes de règles spécifiés

f. Dispositifs, ou groupes de dispositifs spécifiés

g. Gestion du matériel

h. Options

i. Événements logiciels

j. Événements matériels

k. Accès à distance

I. Profils horaire

1. Les profils horaires doivent être utilisés pour permettre des fonctionnalités et des comportements différents pour différents moments de la journée ou jours de la semaine.

2. Il n'y a pas de limite au nombre de profils horaires pouvant être créés.

3. Il doit être possible d'attribuer un calendrier différent pour au moins 28 jours dans un seul profil horaire.

4. Les jours personnalisés doivent être utilisés pour fournir une fonctionnalité unique ou anormale de jours spécifiés.

a. Il n'y a pas de limite au nombre de jours personnalisés pouvant être créés.

b. Il doit être possible d'attribuer un calendrier différent pour les jours personnalisés.

c. Lorsque les jours personnalisés ont lieu, les horaires doivent être remplacés par ceux définis pour le jour personnalisé.

5. La mise en page doit être graphique et facile à utiliser, consistant en commandes cliquer-glisser.

J. Déclencheurs et actions

1. Les règles de déclencheur et d'action doivent fournir au système une fonctionnalité sur mesure, définie par configuration.

2. Le logiciel doit permettre la création de règles de déclencheur et d'action afin d'effectuer un comportement unique et de fournir des fonctionnalités supplémentaires au système.

3. Il ne doit pas y avoir de limite au nombre de règles de déclencheur et d'action pouvant être créées.

4. Il doit être possible d'effectuer une action lorsqu'un déclencheur sélectionné se produit. La

liste des déclencheurs doit comprendre, mais sans s'y limiter :

a. Lecture d'identifiant valide
b. Lecture d'identifiant non valide
c. Entrée ouverte
d. Entrée fermée
e. Changement d'état en entrée
f. Demande de sortie/bouton de sortie enfoncée
g. Alarme de porte forcée
h. Alarme de porte ouverte
i. Alarme intrusion armée
j. Alarme d'intrusion désarmée
k. Alarme d'intrusion activée
l. Alarme incendie activée
m. Début du profil horaire
n. Fin du profil horaire
o. Bouton programmable enfoncé

5. Il doit être possible de restreindre lorsqu'une règle est exécutée par l'état des autres dispositifs du système. La liste des contraintes comprend, mais sans s'y limiter :

a. Entrée élevée
b. Entrée faible
c. Alarme intrusion armée
d. Alarme intrusion désarmée
e. Alarme intrusion active
f. Alarme intrusion inactive
g. Alarme incendie active
h. Alarme incendie inactive
i. Point d'accès ouvert
j. Point d'accès fermé
k. Sortie activée
l. Sortie désactivée

6. Lorsqu'un déclencheur se produit et que toutes les contraintes sont satisfaites, plusieurs actions peuvent se produire. La liste des actions comprend, mais sans s'y limiter :

a. Déverrouiller le point d'accès
b. Verrouiller le point d'accès
c. Basculer le point d'accès
d. Allumer l'appareil
e. Arrêter l'appareil
f. Basculer l'appareil
g. Armer l'alarme intrusion
h. Désarmer l'alarme intrusion
i. Exécuter le rapport d'appel

7. Il ne doit pas y avoir de limite au nombre de déclencheurs, de contraintes et d'actions qu'une règle peut consister.

K. Anti-passback

1. Les règles anti-passback doivent permettre de surveiller et de restreindre les tentatives d'accès séquentielles.

2. Il doit y avoir deux types d'anti-passback disponibles :

3. Il doit être possible de préciser les personnes qui sont appliquées par une règle anti-passback.

4. Il doit être possible de spécifier les points d'accès auxquels s'applique une règle anti-passback.

a. Traditionnel

(i) Une fois qu'un utilisateur est entré par l'un des points d'accès définis, il ne peut pas entrer à nouveau tant qu'il n'a pas été vu en train de sortir.

(ii) L'oubli est possible, en réinitialisant tous les états entrées/sorties à une heure définie chaque jour.

b. Chronométré

(i) Une fois qu'un utilisateur est entré par l'un des points d'accès définis, il ne peut pas entrer de nouveau pendant une période définie.

(ii) Il doit être possible de permettre aux utilisateurs d'entrer de nouveau dans ce délai s'ils ont été vus en train de sortir.

5. Il y a deux types de restriction d'accès :

a. Anti-passback dur — le fait d'être non conforme à la règle restreint l'accès de l'utilisateur.

b. Anti-passback souple — le fait d'être non conforme à la règle permet l'accès selon les autorisations de l'utilisateur, tout en déclenchant un événement pour informer les administrateurs de la violation.

6. Il n'y a pas de limite au nombre de règles anti-passback qui peuvent être créées.

L. Appel

1. Le logiciel doit fournir une fonctionnalité d'appel.

2. Les règles d'appel doivent être utilisées pour configurer la fonctionnalité d'appel.

a. Chaque règle doit définir les points d'accès qui composent une zone.

b. Chaque règle doit définir les lecteurs de point de rassemblement situés à chaque point de rassemblement de la zone.

3. Les rapports d'appel sont utilisés pour répertorier tous les utilisateurs dans une zone au point de génération du rapport.

a. Le rapport doit être généré suivant la configuration d'une règle d'appel individuel.

b. Il doit être possible d'automatiser la génération d'un rapport d'appel en cas d'urgence.

c. Il doit être possible d'envoyer automatiquement par courrier électronique un rapport d'appel dès la génération.

4. Le rapport d'appel doit être visualisable dans le logiciel.

5. Le rapport d'appel doit fournir :

a. Affichage de tous les utilisateurs d'une zone.

b. Informations sur l'utilisateur, y compris le nom, l'adresse e-mail et toute information stockée pour les utilisateurs.

c. Image de l'utilisateur.

d. Dernier emplacement connu de chaque utilisateur.

e. État en sécurité / pas en sécurité

(i) Les utilisateurs peuvent être marqués comme en sécurité dans le rapport.

(ii) Les utilisateurs peuvent se marquer comme étant en sécurité en présentant leur badge à un lecteur de point de rassemblement désigné.

6. Seuls les utilisateurs connus pour se trouver dans une zone seront inclus dans le rapport lorsqu'il est généré.

a. Il doit être possible d'effacer le rapport à une heure définie chaque jour.

b. Il doit être possible de retirer les utilisateurs du rapport après avoir été inactifs pendant une durée déterminée.

M. Gestion du matériel

1. Le matériel doit être mappé au logiciel à l'aide d'un simple clic et glissement.
2. Le matériel doit être géré dans un emplacement central.
3. Le logiciel doit fournir des informations détaillées sur tout le matériel lié, y compris :

a. Type de matériel

b. Numéro de série ou identifiant unique

c. Sous-réseau

d. Adresse IP

e. État de la batterie

f. Version du microprogramme

g. Statut en ligne

4. La gestion du matériel doit être permise aux utilisateurs de logiciels spécifiés.
5. La cartographie des périphériques matériels aux appareils doit être flexible et polyvalente, ce qui permet aux dispositifs de se composer de plusieurs composants provenant d'un certain nombre de matériels

a. Il doit être possible d'associer tout périphérique de sortie (relais) à :

(i) Verrouillage d'un point d'accès

(ii) Alarme pour un point d'accès

(iii) Sortie contrôlée pour un dispositif

(iv) Contrôle de l'armement d'une alarme intrus

b. Il doit être possible d'associer tout périphérique d'entrée numérique à :

(i) Bouton de sortie pour un point d'accès

(ii) Contact de porte pour un point d'accès

(iii) Entrée numérique pour un dispositif

(iv) État de l'armement de d'alarme pour une alarme intrusion

(v) État actif de l'alarme pour une alarme intrusion

(vi) État actif de l'alarme pour une alarme incendie

c. Il doit être possible d'associer tout lecteur à un :

(i) Point d'accès pour surveiller et restreindre l'accès

(ii) Dispositif contrôlable pour surveiller et restreindre l'utilisation

(iii) Alarme d'intrusion pour surveiller et restreindre l'armement/désarmement.

N. Dispositif de commande

1. Le logiciel doit permettre de contrôler à distance le matériel du système à partir du logiciel.

2. Au minimum, les éléments suivants doivent être possibles à partir du logiciel :

a. Déverrouiller un point d'accès

b. Activer/Désactiver/Basculer l'état d'un périphérique contrôlable

c. Armer/Désarmer une alarme intrus.

3. Les utilisateurs de logiciels doivent être limités à n'avoir accès qu'à contrôler à distance les dispositifs qu'ils seraient en mesure de contrôler s'ils avaient présenté leur badge à un lecteur.

O. Accès à distance

1. Le logiciel doit être accessible de n'importe où grâce à une connexion Internet.

a. Il doit être possible d'activer/désactiver cette fonction.

b. Il doit être possible de restreindre la connexion à distance à tout groupe ou individu.

2. Lorsque vous accédez à distance, aucune installation logicielle ou un adressage manuel complexe ne doit être requis.

3. Lorsque vous accédez à distance, l'interface utilisateur doit être identique à celle de l'accès local.

P. Page d'accueil

1. Une page d'accueil fournit aux utilisateurs un endroit central pour visualiser et gérer leur système.

2. La page d'accueil doit permettre d'accéder à :

a. Création de nouvelles entités sur le système

b. Favoris.

3. La page d'accueil fournit un résumé du système et de son activité, y compris :

a. Résumé

(i) Nombre d'utilisateurs actifs

(ii) Nombre total d'utilisateurs

(iii) Nombre total de dispositifs

b. Notifications

(i) Nombre d'événements d'alarme non reconnus

(ii) Nombre d'appareils hors ligne

iii) Nombre d'utilisateurs connectés

c. Activité du système

(i) Graphique des événements d'accès par jour, au cours des 7 derniers jours

Q. Favoris

1. Le logiciel doit fournir à chaque utilisateur un ruban personnalisable pour les raccourcis de contrôle et de navigation.

2. L'utilisateur doit pouvoir ajouter ce qui suit au ruban de son favori :

a. Liens — pour naviguer rapidement vers les zones du logiciel.

b. Actions — pour exécuter l'action par défaut d'un périphérique.

3. L'utilisateur doit pouvoir organiser des raccourcis et des actions sur le ruban du favori.

a. Il doit être présenté sous forme d'interface graphique par glisser-déposer.

4. Les utilisateurs ont la possibilité d'ouvrir une zone spécifique du logiciel par défaut lorsqu'ils se connectent.

5. Tous les favoris et options sont stockés par utilisateur, de sorte que chaque utilisateur du logiciel puisse avoir ses propres favoris et paramètres personnalisés.

R. Importation utilisateur

1. Il est possible d'importer des données utilisateur dans le système.
2. Le fichier suivant pour

2.11 CONDITIONS SPÉCIFIQUES POUR LE LECTEUR DE BUREAU

A. Caractéristiques

1. Le lecteur de bureau doit faciliter l'attribution de badges aux utilisateurs.
2. Le lecteur de bureau doit lire plusieurs types et formats de badges de proximité.
3. Le lecteur de bureau doit identifier les badges/identifiants qui ont déjà été attribuées aux utilisateurs.
4. Le lecteur de bureau élimine le besoin de connaître le numéro de chaque badge.
5. Dans les systèmes comportant plusieurs PC clients, le système doit pouvoir prendre en charge plusieurs lecteurs de bureau.
6. Le lecteur de bureau doit générer un ID unique à partir de chaque badge présenté.
7. Le lecteur de bureau doit produire un ID unique à partir d'une variété de formats et de longueurs.

B. Interaction des utilisateurs

1. Le lecteur de bureau doit fonctionner en mode intuitif :
    a. Lorsqu'un badge/identifiant non attribué est présenté, le logiciel système crée automatiquement l'enregistrement de l'utilisateur et l'écran utilisateur pour entrer les informations de l'utilisateur ainsi que d'autres paramètres de sécurité.
    b. Lorsque l'opérateur est déjà dans une fiche d'utilisateur et qu'un badge/identifiant non attribué est présenté, le logiciel doit afficher l'option permettant d'ajouter le badge/identifiant à la fiche affichée.
    c. Lorsqu'un badge/identifiant existant est présenté au lecteur de bureau, le logiciel récupère et affiche automatiquement la fiche utilisateur associé à cet utilisateur. Si plusieurs badges/identifiants sont attribués à cet utilisateur, le logiciel doit mettre en évidence celui présenté.
2. Le lecteur doit être plug & play.

C. Lecteur de proximité

1. L'article doit contenir un lecteur de proximité.
    a. Au minimum, la technologie de badge suivante doit être prise en charge :
    (i) Paxton HiTag2 125KHz
    (ii) HID 125KHz
    (iii) EM4100/02
    (iv) EM4200
    (v) Sony FeliCa Lite-S
    (vi) MIFARE 1K
    (vii) MIFARE 4K
    (viii) MIFARE Ultralight / C
    (ix) MIFARE DESFire / EV1
    (x) MIFARE Mini

b. Toutes les technologies de badges ci-dessus doivent être prises en charge simultanément.

c. Les formats d'identifiants suivants doivent être pris en charge :

(i) Carte ISO

(ii) Clamshell

(iii) Minifob / keyfob

(iv) Proxidisc

(v) Watchprox

(vi) Badge mains libres

D. Alimentation

1. L'article doit être alimenté par USB.

E. Communication

1. Le lecteur de bureau doit se connecter à un PC via un câble mini USB vers USB.

F. Affichage

1. L'article doit être doté d'un affichage LED élégant.
2. Les LED doivent indiquer les états suivants :
    a. Article alimenté ou prêt à l'emploi
    b. Lecture des identifiants

G. Température

1. L'article doit satisfaire aux normes de température requises pour un produit interne.
    a. L'article doit fonctionner de manière fiable dans la plage de température comprise entre 0 °C et +49 °C (32 °F à 120 °F)

H. Boîtier

1. L'article doit être élégant et moderne.
2. Le produit doit être disponible en noir

I. Dimensions

1. Les dimensions du lecteur de bureau ne doivent pas dépasser :
    a. Une largeur de 115 mm (4,5 po)
    b. Une hauteur de 19 mm (0,7 po)
    c. Une profondeur de 75 mm (3 po)

FIN DE LA SECTION