

**SPÉCIFICATIONS A&I**

<b>DIVISION 28</b>		<b>SÛRETÉ ET SÉCURITÉ ÉLECTRONIQUE</b>
NIVEAU 1	28 10 00	CONTRÔLE D'ACCÈS ÉLECTRONIQUE ET DÉTECTION D'INTRUSION
NIVEAU 2	28 13 00	CONTRÔLE D'ACCÈS
<b>NIVEAU 3</b>	<b>28 13 16</b>	<b>SYSTÈMES DE CONTRÔLE D'ACCÈS ET GESTION DE BASES DE DONNÉES</b>
NIVEAU 4	28 13 16.00	NON APPLICABLE
NIVEAU 5	28 13 16.00.TP1.5	NUMÉRO DE RÉFÉRENCE UNIQUEMENT

Cette spécification A&I est conforme au Répertoire normatif du CSI 2004.

Le niveau en **gras** ci-dessus identifie le niveau auquel cette spécification se trouve dans la hiérarchie du Répertoire normatif du CSI.

Ne pas hésiter à contater Interlogix à propos des exigences spécifiques du projet. Pour des informations et de l'aide, contacter :

Interlogix  
3211 Progress Drive, Lincolnton, NC 28092, États-Unis d'Amérique  
Internet : <http://www.interlogix.com>

[AUTEUR]  
[NOM DU FICHIER]

SYSTÈMES DE CONTRÔLE D'ACCÈS ET GESTION DE BASES DE DONNÉES  
28 13 16

**INFORMATIONS CONFIDENTIELLES INTERLOGIX™ – Pour les utilisateurs potentiels et utilisateurs actuels de TruPortal™ et leurs consultants autorisés. Toute utilisation tierce est interdite sans l'autorisation écrite d'Interlogix.**

## TABLE DES MATIÈRES

PARTIE 1 GÉNÉRAL .....	3
1.1 RÉSUMÉ.....	3
1.2 RÉFÉRENCES.....	3
1.3 PROPOSITIONS.....	3
1.4 PROPOSITIONS DE FERMETURE .....	3
1.5 GARANTIE.....	4
PARTIE 2 PRODUITS.....	5
2.1 MATÉRIEL FOURNI PAR LE PROPRIÉTAIRE .....	5
2.2 SYSTÈME.....	5
2.3 CRITÈRES DE PERFORMANCE.....	5
PARTIE 3 EXÉCUTION .....	16
3.1 INSTALLATEURS.....	16
3.2 INSPECTION .....	16
3.3 PRÉPARATION .....	16
3.4 INSTALLATION.....	16
3.5 CONTRÔLE QUALITÉ.....	17
3.6 DÉMARRAGE DU SYSTÈME .....	18
3.7 ACTIVITÉS DE CLÔTURE .....	18

## SECTION 28 13 16

### PARTIE 1 GÉNÉRAL

#### 1.1 RÉSUMÉ

- A. La section comprend
  - 1. Critères de performances des systèmes intégrés de gestion de la sécurité
  - 2. Critères de performance des stations de travail d'opérateurs des systèmes intégrés de gestion de la sécurité
- B. Critères associés
  - 1. Systèmes intégrés et options
    - a. 28 06 00 Programmations pour la sécurité et la sûreté électronique
    - b. 28 13 00 Contrôle d'accès (la présente section non incluse)
    - c. 28 20 00 Surveillance électronique
    - d. 28 30 00 Détection électronique d'alarmes
  - 2. Sections associées
    - a. 26 33 53 Bloc d'alimentation permanente statique
    - b. 27 20 00 Communications de données

#### 1.2 RÉFÉRENCES

- A. NFPA 70 - Code électrique national
- B. NFPA 101 - Code de sécurité des personnes
- C. UL 294 - Systèmes de contrôle d'accès
- D. UL 1076 - Unités et systèmes d'alarmes antivols propriétaires
- E. Loi américaine en faveur des personnes handicapées (ADA) - Loi publique 101.336
- F. FCC
- G. RoHS - Restriction d'utilisation de certaines substances dangereuses sur le matériel électrique et électronique
- H. CE - Conformité européenne

#### 1.3 PROPOSITIONS

- A. Diagramme de bloc unifilaire affichant toutes les interfaces d'équipement associées
- B. Fiches techniques des fabricants
- C. Dessins d'atelier
- D. Logiciel : un ensemble de logiciels dans l'emballage original du fabricant

#### 1.4 PROPOSITIONS DE FERMETURE

- A. Contrats de maintenance
- B. Données ou manuels d'utilisation et de maintenance
- C. Documentation de garantie
- D. Documentation d'enregistrements
- E. Logiciel
- F. Documentation de mise en service et liste de vérification
- G. Schémas de pose

[AUTEUR]  
[NOM DU FICHIER]

SYSTÈMES DE CONTRÔLE D'ACCÈS ET GESTION DE BASES DE DONNÉES  
28 13 16

**INFORMATIONS CONFIDENTIELLES INTERLOGIX™ – Pour les utilisateurs potentiels et utilisateurs actuels de TruPortal™ et leurs consultants autorisés. Toute utilisation tierce est interdite sans l'autorisation écrite d'Interlogix.**

- H. Matériel de cours de formation
- I. Présentations de formation
- J. Fichiers vidéo de cours de formation

## 1.5 GARANTIE

- A. Garantie  
<http://www.interlogix.com/support>

## PARTIE 2 PRODUITS

### 2.1 MATÉRIEL FOURNI PAR LE PROPRIÉTAIRE

- A. Ordinateur (configuration minimum requise) :
1. Processeur Intel Pentium 4.2.8 GHz
  2. 1 Go de RAM
  3. Carte vidéo 512 Mo
  4. 1 Go d'espace libre
  5. Carte d'interface réseau Ethernet 10/100 Mo
  6. Résolution de l'écran 1 024 x 768
  7. Clavier standard 101 touches et souris à molette à deux boutons
- B. Logiciel informatique :
1. Système d'exploitation : Microsoft Windows XP SP3 32 bits, Windows 7 (32 ou 64 bits), Windows 8 64 bits Classic ou Macintosh Operating System X Mountain Lion
- C. Client Web de la station de travail de l'opérateur :
1. Navigateur Internet : Internet Explorer 8, 9, 10 ou 10 Desktop, Mozilla Firefox 16, Google Chrome 22 et Apple Safari 6.02
    - a. Contrôle vidéo supporté uniquement avec utilisation d'ActiveX sur Internet Explorer

### 2.2 SYSTÈME

- A. Fabricant
1. Fournir tous les logiciels de contrôle d'accès aux systèmes et le matériel associé sous la forme d'une offre de produits sur catalogue standard du fabricant.
  2. Exception : les serveurs, stations de travail et autres équipements informatiques associés doivent avoir des caractéristiques spécifiques produites de manière régulière par un fabricant informatique reconnu par l'industrie, tant que les composants remplaçables sont disponibles auprès de sources tierces.
  3. Exception : les équipements contrôlés, tels que les serrures électroniques, les commandes de portes, les capteurs, etc., sont spécifiés à un autre endroit.
  4. Cette spécification est basée sur TruPortal 1.5 fabriqué par Interlogix, 3211 Progress Drive, Lincolnton, NC 28092, États-Unis d'Amérique. <http://www.interlogix.com>
- B. Description
1. Le système est un équipement de contrôle d'accès IP.
  2. Le système est un système de sécurité à lecteurs de carte permettant de contrôler l'accès aux bâtiments.
  3. Le système est un système de contrôle d'accès autonome.
  4. Le système est un système de contrôle d'accès de base prêt à l'emploi et tout-en-un fourni dans un package Internet.
  5. Utilise un contrôleur et les équipements associés.
  6. Offre la gestion, le contrôle et la surveillance des composants d'accès et d'alarmes.
  7. Définition et configuration de l'application et de la base de données système.

### 2.3 CRITÈRES DE PERFORMANCE

- A. Architecture du système :

1. Application Internet intégrant de nombreuses fonctions de sécurité, notamment la gestion, le contrôle et la surveillance :
  - a. du contrôle d'accès
  - b. De la gestion des alarmes
  - c. De l'interface de surveillance vidéo
2. Fonctionne sur les systèmes d'exploitation Microsoft Windows XP SP3 32 bits, Windows 7 (32 ou 64 bits) et Windows 8 (64 bits) Classic.
  - a. Capacité multi-utilisateurs
3. Protocole de communication réseau standard Transmission Control Protocol (TCP/IP) entre les stations clients, le(s) système(s) de surveillance vidéo et les sous-systèmes de la base de données
  - a. Support de la connectivité 10/100/1000 Mo Ethernet sur topologies de réseau local (LAN)/étendu (WAN)
4. Support du protocole Dynamic Host Configuration Protocol (DHCP) ou de l'adresse IP fixe
  - a. Le contrôleur propose des solutions à programmer via le protocole DHCP ou avec une adresse IP fixe
5. Support de la configuration réseau
6. Le contrôleur supporte le protocole Network Time Protocol (NTP)
7. Support des communications codées Secure Socket Layer (SSL) entre le client navigateur Web et le contrôleur.
8. Support des communications codées Advanced Encryption Standard (AES) entre le contrôleur et les contrôleurs de porte
9. Support des capacités permettant aux utilisateurs de créer des demandes de signature due certificat (CSR) et d'importer des certificats signés ou de générer et installer des certificats auto-signés.
  - a. Fully Qualified Domain Name (FQDN) ou SSL peuvent être utilisés dans les certificats
10. Réglié pour observer automatiquement l'heure d'été (DST) (si le fuseau horaire sélectionné prend en charge l'heure d'été)
11. Interface des lecteurs
  - a. Le contrôleur prend uniquement en charge l'interface Wiegand
  - b. L'interface lecteur entre les contrôleur et le lecteur doit être une interface Wiegand
12. Prend en charge jusqu'à dix champs personnels définis par l'utilisateur
13. Support d'un maximum de 10 000 photos de personnes aux formats GIF, JPG et PNG
  - a. Les photos d'une taille maximale de 200 Ko peuvent être téléchargées
  - b. Les photos sont automatiquement redimensionnées à 10 Ko ou moins
  - c. Taille maximale du stockage photo : 40 Mo
14. Support de la visualisation des 65 535 derniers événements
15. Support de la gâche de porte et des durées de porte restée ouverte conformément à la réglementation ADA
  - a. La fonction d'activation ou de désactivation des durées supplémentaires est définie en fonction des justificatifs d'identité
  - b. Les durées supplémentaires sont définies par porte
16. Permettre la sauvegarde des paramètres et données système actuels comme paramètres personnalisés
17. Prend en charge la recherche automatique des contrôleurs et des modules en aval
18. Assistants utilisateur
  - a. Guide étape par étape pour certaines tâches utilisateurs courantes
19. Recherche d'événements et de personnes
  - a. Support de la recherche (filtrage) des enregistrements
20. Permet à l'utilisateur de créer un nouvel enregistrement en fonction d'un enregistrement existant
21. Prend en charge les info-bulles lorsque l'utilisateur passe au-dessus de certains éléments de l'interface utilisateur

22. Indicateur de statut du système
    - a. Visible depuis n'importe quel écran
  23. Support de la génération de rapports
- B. Contrôleur de porte
1. Support du module d'interface double porte
    - a. Les modules prennent en charge deux (2) portes et peuvent être configurés pour un ou deux lecteurs par porte
    - b. Support de 64 lecteurs
      - 1) 64 portes câblées pour lecteur d'entrée uniquement
      - 2) 32 portes câblées pour lecteur d'entrée/sortie
  2. Support des contrôleurs de porte unique basés sur IP
    - a. Les modules prennent en charge une porte et peuvent être configurés pour un ou deux lecteurs par porte
      - 1) Supporte 62 contrôleurs de porte unique basés sur IP
      - 2) Supporter 64 portes câblées pour lecteur d'entrée/sortie
  3. Support des serrures autonomes sortie Wiegand
    - a. Schlage AD-400 (exige d'utiliser PIM-400 TD2)
    - b. Assa Abloy Aperio™ (exige d'utiliser le concentrateur de communication interface Wiegand standard AH20)
  4. Support des entrées numériques via carte d'expansion d'entrée
    - a. Chaque module prend en charge 16 entrées
      - 1) Support de quatre entrées auxiliaires sur le contrôleur
      - 2) Support de deux entrées auxiliaires sur le contrôleur
  5. Support des sorties de relai via les cartes de circuit de sortie de relai connectées à une carte d'expansion de huit sorties de relai via l'interface de bus RS-485 SNAPP
    - a. Chaque module de sortie prend en charge huit sorties
  6. Support de modules en aval via communications RS-485 multipoints
  7. Support de borniers amovibles pour toutes les connexions entre les modules en aval et les entrées numériques, sorties de relai et lecteurs
  8. Support des diodes de diagnostic sur le contrôleur
  9. Résistances de supervision de fin de ligne
    - a. Configurables
    - b. Simples ou doubles
    - c. 1K ou 4K7
  10. Rapport sur les alarmes Porte forcée
  11. Rapport sur les alarmes Porte restée ouverte
  12. Rapport sur les alarmes système
  13. Rapport sur les alarmes d'autoprotection
- C. Assistant d'installation
1. Utilitaire d'installation indépendant
  2. Supporté par le système d'exploitation Windows 7 (32 ou 64 bits) ou Windows 8 (64 bits) Classic
  3. Supportera plusieurs langues
  4. Permettra à l'utilisateur d'effectuer la configuration initiale
    - a. Permettra à l'utilisateur d'installer Microsoft .NET Framework 4.5 et les composants préalables Bonjour
    - b. Permettra à l'utilisateur de changer le mot de passe de l'administrateur par défaut pour une meilleure sécurité
    - c. Permettra à l'utilisateur de paramétrer kes table horaire, date et heure
    - d. Permettra à l'utilisateur de définir l'adresse IP du contrôleur et le protocole DHCP ou l'IP statique

- e. Permettra à l'utilisateur de sélectionner les options du réseau y compris : statique ou DHCP, adresse IP, port de service, protocole HTTP ou HTTPS
  5. Détectera le contrôleur sur le réseau local
  6. Proposera un lien pour lancer l'application du système pour le contrôleur sélectionné
- D. Assistant d'importation/exportation
1. Utilitaire autonome pour importation et exportation des données dans un format CSV
  2. Supporté par le système d'exploitation Windows 7 (32 ou 64 bits) ou Windows 8 (64 bits) Classic
  3. Supportera plusieurs langues
  4. Permettra à l'utilisateur d'importer les personnes et données de justificatif d'identité dans un format CSV
    - a. Chargement d'un fichier CSV dans lequel chaque enregistrement contient les données de personne et données optionnelles d'un justificatif d'identité
    - b. Permettra de lier les champs CSV aux données du système
    - c. Permettra à l'utilisateur de demander que le fichier CSV soit utilisé pour une opération d'ajout, de mise à jour ou de suppression (par fichier et non par enregistrement)
    - d. Permettra de sauvegarder ou restaurer tous les paramètres depuis ou vers un fichier
    - e. Permettra de traiter tous les enregistrements dans un fichier CSV sans interaction de l'utilisateur
    - f. Permettra de lier les noms des niveaux d'accès dans le fichier CSV aux noms des niveaux d'accès existants dans le système
    - g. Supportera l'importation des données de photo d'une personne via des fichiers accessibles localement et dont le chemin d'accès est un champ du fichier CSV
    - h. Supportera la sélection des champs qui identifieront de façon unique un enregistrement
  5. Permettra à l'utilisateur d'exporter les personnes et données de justificatif d'identité dans un format CSV
    - a. Permettra à l'utilisateur de sélectionner les données de personne et de justificatif d'identité pour exportation
    - b. Exportation systématique de tous les enregistrements disponibles
    - c. Sélection par l'utilisateur des champs ou de l'ordre des champs (dans un enregistrement) à exporter
    - d. Supportera l'exportation des photos de personne
    - e. Production des enregistrements dans un ordre de tri prédéfini
    - f. Permettra de sauvegarder ou restaurer tous les paramètres depuis ou vers un fichier
    - g. Production de tous les enregistrements dans un fichier CSV sans interaction de l'utilisateur
  6. Support des caractères spéciaux
  7. Produira un rapport dans un format HTML avec informations récapitulatives sur l'importation ou l'exportation
  8. Permettra à l'utilisateur d'effacer les personnes et données de justificatif d'identité par lot
  9. Permettra à l'utilisateur d'exporter les événements fournissant un enregistrement historique de l'activité du système
  10. Support de la migration des données depuis l'application Topaz
    - a. Support de la migration des enregistrements de personne, enregistrements de justificatif d'identité et photos via fichiers CSV
    - b. L'outil de migration de Topaz, Topaz Migration Tool, est disponible dans le DVD du produit des distributeurs
    - c. Les données peuvent être extraites vers un dossier pour l'importation dans TruPortal via l'assistant d'importation/exportation
- E. Assistant de mise à niveau



1. L'utilitaire autonome permet à l'utilisateur de mettre le contrôleur à niveau depuis une version antérieure
  2. Supporté par le système d'exploitation Windows 7 (32 ou 64 bits) ou Windows 8 (64 bits) Classic
  3. Supportera plusieurs langues
  4. Supportera les mises à niveau distantes
  5. Actualisera le micrologiciel et le code source du contrôleur
  6. Permettra à l'utilisateur de sauvegarder les données avant la mise à niveau et de restaurer ensuite les données
    - a. Ne sauvegarde pas les événements historiques à des fins de tenue d'archives uniquement
- F. Support du courriel
1. Supportera la configuration d'un serveur SMTP (Simple Mail Transfer Protocol) interne ou externe
  2. Permettra à l'utilisateur de créer des listes de distribution électronique
  3. Des courriels automatiques peuvent être générés après :
    - a. Des sauvegardes programmées se produisent
    - b. Des déclencheurs d'action sont exécutés
- G. Sauvegarde et restauration
1. Support de la sauvegarde et restauration complètes de la base de données depuis ou vers un fichier
  2. Codage du fichier de sauvegarde
  3. Les sauvegardes peuvent être programmées pour se produire automatiquement
    - a. Supportera les courriels automatiques pour notifier les utilisateurs des sauvegardes réussies ou échouées
    - b. Supportera la copie de fichiers de sauvegarde dans des ressources réseau partagées
  4. La sauvegarde et la restauration comprennent tous les enregistrements et paramètres qu'un utilisateur peut configurer avec l'interface utilisateur à l'exception des :
    - a. Paramètres de configuration du réseau
    - b. États des porte/lecteur paramétrés manuellement via la page Porte
    - c. Événements
  5. Support de la sauvegarde autonome des événements dans un fichier à des fins de tenue d'archives
  6. Support de la capacité à restaurer le contrôleur à ses paramètres d'usine par défaut
- H. Diagnostics
1. Diagnostics d'informations simples
  2. Indicateurs visuels pour les modes d'échec courants qui permettent aux utilisateurs finaux de résoudre le problème
  3. Statut de l'alimentation et du matériel
  4. Utilisation des ressources
  5. Capacités du système et de l'équipement
  6. Supporte la capacité à placer les informations du système et des fichiers journal dans un fichier crypté pouvant être envoyé au support technique
- I. Fonctions du système
1. Effectuer un scan pour voir les changements au niveau du matériel
  2. Contrôler l'accès aux portes en fonction des horaires de contrôle d'accès définis par l'utilisateur
  3. Créer et configurer les programmations, congés et niveaux d'accès
  4. Gérer les personnes et justificatifs d'identité
  5. Contrôler à distance les fonctions du système

- a. Surveiller les événements, vidéo de l'événement et alarmes
  - b. Entrées et sorties
  - c. Déclencheurs d'action
  - d. Programmations
  - e. Sécuriser, verrouiller et ouvrir les portes
  - f. Réinitialiser l'Anti-passback (APB)
6. Gèrent les alarmes
  7. Configurer les portes et lecteurs
  8. Autorise l'accès aux utilisateurs en fonction de l'heure et du lieu
  9. Mettent à jour les droits d'accès
  10. Envoyer des courriels automatisés
  11. Configurer les politiques de permission de groupe
  12. Configurer les déclencheurs d'action automatiques qui sont exécutés lorsqu'un ensemble de conditions est satisfait.
  13. Configurer les ressources du réseau partagées dans lesquelles envoyer les fichier de sauvegarde programmée.
- J. Capacité du système :
1. Propose un maximum de 10 000 personnes
  2. Propose un maximum de 10 000 justificatifs d'identité
  3. Propose un maximum de cinq justificatifs d'identité par personne
  4. Propose un maximum de 64 niveaux d'accès
  5. Propose un maximum de huit niveaux d'accès par justificatif d'identité
  6. Propose un maximum de 64 programmations
  7. Propose un maximum de six intervalles horaires par programmation
  8. Propose un maximum de huit groupes de congés par programmation
  9. Propose un maximum de huit groupes de congés
  10. Propose un maximum de 32 congés par groupe de congés
  11. Propose un maximum de 255 congés
  12. Propose un maximum de 64 secteurs
  13. Propose un maximum de 64 groupes de lecteurs
  14. Propose un maximum de 32 rôles d'opérateur
  15. Propose un maximum de dix champs définis par l'utilisateur
  16. Propose un maximum de 64 gabarits vidéo
  17. Propose un maximum de huit formats de carte
  18. Propose un maximum de 10 listes de courriel
  19. Propose un maximum de 32 déclencheurs d'action
  20. Propose un maximum de 32 modules d'interface double porte
  21. Propose un maximum de 62 contrôleurs de porte unique basés sur IP
  22. Propose un maximum de 64 portes
  23. Propose un maximum de 64 lecteurs
  24. Propose un maximum de huit modules de carte d'expansion d'entrée
  25. Propose un maximum d'une carte d'expansion de sortie huit relais par carte d'expansion d'entrée
  26. Support d'un maximum de cinq clients actifs concurrents
  27. Maximum de quatre DVR et 64 caméras
  28. Maximum de quatre ports de bus SNAPP RS-485
- K. Interface d'opérateur :
1. Utilise une interface utilisateur Internet pour la configuration, l'administration, la gestion du système et le contrôle des opérations
    - a. Plugiciel Flash requis pour client sur navigateur

2. Propose des fichiers d'aide contextuels en ligne pour aider les opérateurs à configurer et mettre en route le système
3. Support de plusieurs langues
  - a. L'interface utilisateur, les événements et la documentation en ligne peuvent être localisés dans les langues suivantes :
    - 1) Anglais (en-US) disponible comme configuration de base
    - 2) Espagnol (es-ES) disponible comme configuration de base
    - 3) Français (fr-FR) disponible comme configuration de base
    - 4) Néerlandais (nl-NL) disponible comme configuration de base
    - 5) Portugais (pt-PB) disponible via téléchargement du langage pack depuis le site Web
    - 6) Allemand (de-DE) disponible via téléchargement du langage pack depuis le site Web
    - 7) Italien (it-IT) disponible via téléchargement du langage pack depuis le site Web
    - 8) Suédois (sv-SE) disponible via téléchargement du langage pack depuis le site Web
    - 9) Turc (tr-TR) disponible via téléchargement du langage pack depuis le site Web
    - 10) Finlandais (fi-FI) disponible via téléchargement du langage pack depuis le site Web
  - b. La langue principale du système détermine la langue utilisée pour les fonctions du système, comme l'attribution de nom d'équipement par défaut, sauvegarde programmée et courriels automatiques.
  - c. Les langues peuvent être ajoutées ou supprimées ; un maximum de quatre langues actives à la fois dans un système est permis
  - d. Les utilisateurs peuvent faire leur choix parmi les langues actives.
- L. Rôles opérateur
  1. Jusqu'à 32 rôles d'opérateur
  2. Chaque rôle dispose d'un nombre de permissions défini et sera configuré pour différents niveaux de permission
  3. Contient cinq rôles prédéfinis
- M. Cartes
  1. Support des formats de carte avec une longueur de bits totale de 20 à 200 bits (longueur totale de la carte et contient des bits pour le numéro de carte, le code sécurité, le code édition et les bits de parité)
  2. Numéro de carte maximum limité à 128 bits
  3. La valeur de l'ID de justificatif d'identité maximum qu'un utilisateur peut saisir lorsqu'il crée un justificatif d'identité dépend des formats de carte définis dans le système
  4. Si aucun format n'est défini, la valeur maximum sera basée sur le numéro de la carte 128 bits et autorisera des chiffres entre un et  $2^{128}-1$
  5. Si aucun format n'est défini, l'utilisateur peut saisir des chiffres entre 1 et  $2^N-1$ , où N est la plus grande longueur de bit de numéro de carte de tous les formats définis
  6. Le système inclura des types de formats de carte prédéfinis :
    - a. Code sécurité 200 Weigand 26 bits (H10301)
    - b. 14443 cascade 1 32 bits
    - c. (I10304) code sécurité 40 37 bits
    - d. CASI 4002 40 bits
  7. Support des lecteurs avec clavier pour accès par carte ou code confidentiel
  8. Support des dates d'expiration pour les justificatifs d'identité
- N. Détenteurs de badge :
  1. Support d'un maximum de 10 000 personnes et justificatifs d'identité

2. Tous les justificatifs d'identité du système doivent être attribués à une personne
  3. Supporte les lecteurs de justificatif d'identité RF Ideas pouvant être utilisés pour lire les données de badge et insérer les informations relatives aux justificatifs d'identité dans l'interface utilisateur
- O. Gestion de contrôle d'accès :
1. contrôle tous les secteurs sécurisés et génère des notifications d'alarme lors d'un accès non autorisé aux portes contrôlées par les lecteurs
  2. Autorise les portes sécurisées à s'ouvrir sans générer de condition d'alarme lors de :
    - a. la lecture d'une carte valide
    - b. Une demande de sortie avec équipement de sortie
    - c. Déverrouillage manuel de la porte via une commande à distance autorisée
  3. Événements
    - a. Affichage des événements s'étant produits sur le système
    - b. Accès autorisé, accès refusé, accès autorisé - Porte déverrouillée et accès refusé - Porte verrouillée
    - c. Listera le détenteur de badge qui a initialisé l'événement ainsi que l'heure à laquelle ce dernier s'est produit, la description de l'événement, l'équipement, les date/heure (dans le format du langage pack) et la photo si disponible.
    - d. Affichage et tri des événements
    - e. Exportation des événements dans l'ordre de tri
    - f. Affichage des événements en fonction de l'activité des portes
    - g. Supportera le filtrage des événements
    - h. Localisation du texte relatif à l'événement dans la langue du système
  4. Durée normale autorisation accès
    - a. Durée pendant laquelle une porte s'ouvre lorsque l'accès est autorisé
  5. Durée supplémentaire autorisation accès
    - a. Durée pendant laquelle une porte s'ouvre lorsqu'une personne dispose de durées supplémentaires d'ouverture de porte sur son badge
  6. Durée ouverture
    - a. Durée pendant laquelle une porte s'ouvre après qu'un événement RTE (demande de sortie) se produit
  7. Fonctionnalité de gâche de porte supprimant une demande de sortie
    - a. Permet à l'administrateur d'empêcher d'alimenter la gâche de porte lors de la fermeture du contact de la demande de sortie
  8. Durée Porte restée ouverte
    - a. Durée pendant laquelle une porte peut rester ouverte après un accès autorisé ou une demande de sortie (RTE)
  9. Option d'alarme activée
    - a. Autorise l'administrateur système à choisir si les événements d'alarme de portes restées ouvertes ou de portes forcées sont déclenchés
  10. Entrées RTE
    - a. Pourra choisir comment gérer les entrées RTE
  11. Entrée de contrôle de porte
    - a. Possibilité de choisir comment gérer les entrées de contrôle de porte
  12. Expiration code confidentiel
    - a. Possibilité de définir l'expiration du code confidentiel
  13. Limite tentatives accès
    - a. Possibilité de définir la limite de tentatives d'accès
  14. Heure verrouillage tentative d'accès échouée
    - a. Possibilité de définir l'heure de verrouillage de tentative d'accès échouée
  15. Méthode d'accès
    - a. Possibilité de définir la méthode d'accès

16. Verrouillages et déverrouillages programmés
    - a. Support de la fonctionnalité de verrouillage et déverrouillage des portes via des programmations pouvant être attribuées aux portes de manière indépendante
  17. Déverrouillage temporisé
    - a. Support des déverrouillages temporisés pour des durées définies par l'utilisateur
    - b. La porte se déverrouille lorsque l'accès est autorisé et reste verrouillée jusqu'à l'heure de déverrouillage spécifiée
  18. Verrouiller sur fermeture
    - a. Support du verrouillage sur fermeture
    - b. La porte se déverrouille lorsque l'accès est autorisé et reste déverrouillée jusqu'à l'heure de déverrouillage spécifiée ou la porte s'ouvre et se ferme, suivant l'action qui arrive en premier
  19. Indépendance totale de l'hôte ou opération hors ligne
  20. Déverrouille toutes les portes en cas d'incendie
    - a. Support du déverrouillage des portes en fonction des entrées ou en fonction de l'action de l'opérateur
  21. Opération en mode dégradé
    - a. Support d'un mode dégradé pour les contrôleurs de porte hors ligne
    - b. Le mode sélectionné est commun à toutes les portes et doit être configuré au niveau du contrôleur
    - c. Modes disponibles :
      - 1) Pas d'accès = Pas d'accès (par défaut)
      - 2) Accès code du site = Accès si le code de site du justificatif d'identité correspond au code de site défini dans les formats de carte
      - 3) Accès à tout = Accès si le format du justificatif d'identité est reconnu
      - 4) Utiliser table cache local = (Pour les contrôleurs de porte unique basés sur IP uniquement) Accès si le justificatif d'identité correspond à un des 100 derniers justificatifs d'identité utilisé pour obtenir l'accès
  22. Congés
    - a. Date unique
    - b. Date récurrente annuelle
    - c. Jour, semaine ou mois récurrent chaque année
  23. Groupes de lecteurs
    - a. Les groupes sont regroupés de manière logique pour faciliter la création de niveaux d'accès
  24. Anti-passback (APB)
    - a. Les utilisateurs peuvent définir les secteurs et les assigner en tant que secteurs d'entrée ou de sortie aux lecteurs, et définir le mode APB pour les secteurs.
    - b. Le système effectue un suivi du secteur actuel du justificatif d'identité (l'APB est suivi et est appliqué par justificatif d'identité et non par personne)
    - c. L'imposition de l'APB soft et hard sera permise
      - 1) L'anti-passback hard nécessite la réinitialisation manuelle du justificatif d'identité
      - 2) L'Anti-passback soft enregistre simplement l'événement
    - d. Supportera la réinitialisation automatique configurable de l'APB par secteur
- P. Programmations:
1. Support d'un nombre défini de programmations horaires
  2. Chaque programmation peut définir un ou plusieurs intervalles horaires hebdomadaires et un ou plusieurs groupes de congés
  3. Le système inclura des programmations prédéfinies que l'utilisateur peut effacer :
    - a. Tous les jours 24h/24 7j/7
    - b. Jours de la semaine de 8 heures à 17 heures
    - c. Jours de la semaine de 9 heures à 18 heures

d. Jours de la semaine de 7 heures à 19 heures

Q. Exécution de rapports

1. Le système propose des rapports prédéfinis
2. Des rapports prédéfinis sont fournis
  - a. Historiques
    - 1) Historique des accès
  - b. Temporaire
    - 1) Personne ou liste
    - 2) Justificatif d'identité
    - 3) Accès au lecteur
    - 4) Appel
3. Permettre le filtrage limité en fonction du type de rapport
4. Généré en format HTML et affiché dans une instance (ou onglet) de navigateur indépendante de l'interface utilisateur du système
5. Champs de sorties fixes et disposition
6. Imprimable via la fonction de navigateur Internet
7. Exportation en fichier CSV
8. Permission contrôlée

R. Intégration vidéo :

1. Support des vidéos en temps réel et enregistrées
2. Support de la création de clips vidéo
3. Support du contrôle PTZ des caméras depuis la fenêtre de l'application
4. Les équipements d'enregistrement supportés incluent :
  - a. TVN 20
  - b. TVN 21
  - c. TVN 50
  - d. TVR 10
  - e. TVR 11
  - f. TVR 11-C
  - g. TVR 30
  - h. TVR 31
  - i. TVR 41
  - j. TVR 60
5. Support de l'intégration des systèmes de surveillance vidéo
  - a. Enregistreurs vidéo :
    - 1) Proposer une interface vidéo numérique intégrée et une interface de gestion des caméras pour la commande et le contrôle de la vidéo
    - 2) Proposer une console de gestion de la vidéo dans plusieurs fenêtres pour le contrôle et la surveillance des équipements vidéo en temps réel depuis n'importe quelle station client d'opérateur
    - 3) Affichage des enregistreurs vidéo, caméras et des préparamétrages attribués dans une sous-fenêtre de navigation pour un accès par l'opérateur
    - 4) Support des demandes de transmission de la vidéo en temps réel et vidéo enregistrée depuis les unités d'enregistrement vidéo à différentes résolutions et tailles d'affichage, indépendamment des paramètres de résolution actuels de la vidéo enregistrée locale, configurables par l'utilisateur pour faciliter l'adaptabilité au réseau
    - 5) Support de plusieurs équipements d'enregistrement vidéo
6. Nécessite Internet Explorer pour l'installation du contrôle ActiveX
7. Les vidéos seront associées aux alarmes de porte et de lecteur

8. Les vidéos seront lues selon le tampon horaire enregistré dans l'événement de porte ou de lecteur
- S. Support d'équipement mobile
  1. Support des équipements iOS6, y compris iPad 2 ou plus récent et iPhone 3GS ou plus récent
    - a. Applications disponibles via iTunes® et le magasin Apple® App Store
  2. Support des téléphones Android supportant support Android 2.2 ou plus récent
    - a. Application disponible via le magasin Google Play
  3. L'application TruVision Mobile permet d'afficher la vidéo en temps réel et enregistrée
    - a. Application disponible via iTunes et les magasins App Store ou Google Play

## PARTIE 3 EXÉCUTION

### 3.1 INSTALLATEURS

- A. Exigences concernant les entrepreneurs :
  - 1. Installation locale et organisation des services.
  - 2. Doivent fournir trois références (minimum) ayant des systèmes du même niveau de complexité
    - a. Installé par cet entrepreneur au cours des cinq dernières années.
    - b. Entretenu par cet entrepreneur.
  - 3. Doivent fournir des preuves tangibles d'assurance en responsabilité et d'indemnisation des travailleurs en cas d'accident du travail pour le personnel employé conformément à la loi en vigueur.
- B. Doivent garantir que tout le personnel travaillant sur le projet est enregistré auprès du bureau d'accréditation national et local conformément aux textes réglementaires nationaux ou municipaux.
  - 1. Au moment de l'appel d'offre, l'entrepreneur doit avoir un permis au niveau national ou local d'exécuter des tâches de sécurité dans le pays.
  - 2. Les entrepreneurs qui ont des licences ou permis de services de sécurité en attente ne pourront être acceptés pour répondre à ce projet.
- C. Exigences concernant les installateurs et des techniciens :
  - 1. Doivent être expérimentés et qualifiés pour accomplir tout le travail demandé rapidement et de manière satisfaisante.
  - 2. Doivent fournir des preuves que le personnel de support et de service désigné a bien effectué la formation matérielle et logicielle proposée par le fabricant et a reçu la certification d'installation, de service et de maintenance pour le système spécifié.
  - 3. Doivent établir une liste écrite au propriétaire de tout le personnel de service et support désigné responsable de l'installation et du service avant et après garantie.

### 3.2 INSPECTION

- A. Inspecter le site d'installation avant d'effectuer l'appel d'offre.
- B. Signaler toute divergence entre les spécifications du projet et la documentation d'appel d'offre et l'inspection du site avant la date d'ouverture de l'appel d'offre.

### 3.3 PRÉPARATION

- A. Commander toutes les pièces et matériel requis dès l'attribution de l'appel d'offre.
- B. Tester tout le matériel avant la livraison sur le site du projet.
- C. Vérifier la disponibilité de l'alimentation aux endroits nécessaires. Si une nouvelle source d'alimentation est nécessaire, un électricien agréé sera commandité pour l'installation.
- D. Vérifier la disponibilité des infrastructures de communication aux endroits nécessaires.
- E. Faire le nécessaire pour obtenir toutes les informations de programmation y compris les durées d'accès, les durées d'accès gratuit, les groupes de portes, les niveaux des opérateurs, etc.

### 3.4 INSTALLATION

- A. Exigences
  - 1. Installer tous les composants et équipements système conformément aux spécifications du fabricant, pratiques référencées, règles et codes applicables.



2. Fournir toutes les interconnexions, services et réglages nécessaires à la mise en place et au fonctionnement du système comme spécifié.
  3. Les lignes de transmission des signaux de contrôle, des communications et des données devront être installées selon les besoins pour éviter que les boucles de terre, les interférences et les surtensions n'affectent le fonctionnement du système.
  4. Suivre scrupuleusement les expressions du manuel d'installation du fabricant pour garantir que toutes les étapes ont été suivies et proposer un système fiable et simple à utiliser.
  5. Effectuer toutes les tâches comme indiqué dans les spécifications du projet et dans la documentation d'appel d'offre.
  6. Préprogrammer le système et charger sur l'ordinateur hôte du propriétaire.
- B. Intégration des systèmes :
1. Se coordonner avec le service IT du propriétaire avant de se connecter au réseau du propriétaire.
  2. Travailler en harmonie avec tous les autres secteurs.
  3. Intégrer les systèmes et sous-systèmes associés.

### 3.5 CONTRÔLE QUALITÉ

- A. Qualité de la main-d'œuvre
1. Se conformer aux plus hautes normes de l'industrie, sauf lorsque des exigences spécifiques indiquent des normes plus strictes ou plus précises.
  2. Effectuer le travail avec du personnel expérimenté et qualifié pour accomplir les tâches spécifiées.
  3. Maintenir le contrôle qualité des fournisseurs et sous-traitants.
  4. La qualité de la main-d'œuvre est importante. Le représentant du propriétaire aura le droit de refuser le travail non conforme à la documentation du projet.
- B. Tests et inspections des sites
1. Exécuter les tests appropriés du système pour garantir un fonctionnement correct.
  2. Une fois l'achèvement substantiel de l'ouvrage atteint, effectuer un test et une inspection complète du système. Si l'installation et le fonctionnement sont corrects, avertir [Client] qu'il est maintenant possible d'effectuer le test et l'inspection officiels du système complet.
  3. Soumettre l'historique des performances (plans de récolement) au représentant du propriétaire pour qu'il le consulte avant l'inspection.
  4. Pendant le test et l'inspection officiels (mise en service) du système, du personnel doit être présent avec à sa disposition les outils et le matériel permettant de démonter les équipements afin d'inspecter les connexions électriques. Fournir des diagrammes de câblage et d'étiquette pour correctement identifier tout le câblage.
  5. Si des modifications sont nécessaires, l'entrepreneur fournira une liste de toutes les malfaçons apparentes. Effectuer les modifications nécessaires en temps et en heure.
  6. Avertir le propriétaire une fois prêt à effectuer une nouvelle inspection de l'installation.
- C. Support technique des logiciels et du matériel
1. Services de support logiciel et matériel pour aider le propriétaire à coordonner les interfaces entre le système de gestion de la sécurité et les bases de données du personnel ou d'autres systèmes à distance.
  2. Le support technique des logiciels et du matériel doit être certifié par ou employé par le fabricant du système et doit parfaitement maîtriser les applications du système.
  3. Le support technique des logiciels et du matériel doit se trouver sur le site et doit pouvoir rencontrer les représentants du propriétaire pendant deux jours consécutifs minimum. Les visites sur site doivent être programmées selon les disponibilités du propriétaire.

### 3.6 DÉMARRAGE DU SYSTÈME

- A. Fournir la programmation et la configuration initiales du système de gestion de la sécurité.
- B. La programmation doit comprendre la définition du matériel, des portes, des points de surveillance, des codes d'autorisation, des codes horaires, des groupes de portes, des groupes d'alarmes, des séquences opérationnelles, des commandes de caméra, etc. Toutes les entrées de données doivent être faites par l'entrepreneur. Consulter le représentant du propriétaire pour définir les paramètres de fonctionnement.
- C. Le propriétaire, avec la coopération et l'assistance de l'entrepreneur, entrera les données des détenteurs de badge pour chaque carte d'accès.
- D. Conserver des fiches techniques papier qui illustrent entièrement le programme et la configuration du système.
  - 1. Les fiches techniques doivent être mises à jour quotidiennement jusqu'à l'accord final du propriétaire.
  - 2. Les fiches techniques doivent pouvoir être consultées et acceptées par le propriétaire.
  - 3. Fournir les copies finales au propriétaire avant la clôture du projet.
- E. Conserver une sauvegarde complète et à jour de la configuration du système et de la base de données des détenteurs de badges.
  - 1. La sauvegarde doit être conservée pendant toute la période de programmation jusqu'à l'accord final du propriétaire.
  - 2. Donner le support de sauvegarde au propriétaire lors de l'accord final.
- F. Fournir une assistance de suivi de la configuration système pendant 60 jours après le démarrage du système comme demandé par le propriétaire. Inclure une allocation forfaitaire de main-d'œuvre pour l'assistance de suivi dans le prix de base.

### 3.7 ACTIVITÉS DE CLÔTURE

- A. Mise en service
  - 1. Faire correctement et entièrement fonctionner le système comme spécifié.
  - 2. Vérifier que tous les composants matériels sont correctement installés et connectés et qu'ils communiquent et fonctionnent correctement.
  - 3. Vérifier que tous les logiciels du système sont installés, configurés et conformes aux exigences de fonctionnement spécifiées.
  - 4. Effectuer le test d'accord final en présence du représentant du propriétaire, en exécutant une inspection point par point en fonction d'un plan de test documenté qui démontre la conformité avec les exigences système comme spécifié.
  - 5. Soumettre le plan de test documenté au propriétaire au moins 14 jours avant le test d'accord, l'inspection et la vérification.
  - 6. Effectuer les tests d'accord final en présence du représentant du propriétaire, en vérifiant que chaque point d'équipement et séquence fonctionnent correctement et communique correctement avec le panneau de configuration et le centre de contrôle.
  - 7. L'accord du propriétaire est soumis à l'acceptation de la vérification. Si la vérification est incomplète en raison de travail supplémentaire nécessaire, reprogrammer et effectuer une nouvelle vérification jusqu'à ce qu'elle soit acceptée en une seule fois, sauf si des parties du système ne sont pas affectées par du travail supplémentaire.
  - 8. Le système ne sera pas considéré comme accepté tant que tous les éléments du test de contrôle n'auront pas été acceptés sur la liste de contrôle. L'utilisation de parties ou de tout le système ne sera pas considérée comme un accord.
- B. Formation
  - 1. Fournir la formation à la maintenance, à l'administration et au fonctionnement du système par du personnel formé et qualifié.

- a. La formation devra être orientée vers le système spécifique en cours d'installation conformément au présent contrat comme spécifié.
  - b. Fournir des sessions de formation dans les locaux du propriétaire programmées en fonction des disponibilités du propriétaire.
  - c. Fournir des plans et des calendriers de formation pour chaque session de formation avant leur programmation.
  - d. Enregistrer et fournir des copies des programmes de formation pour la base de connaissances du propriétaire.
2. Le propriétaire désignera le personnel à former.
- a. Fournir des expressions sur les salles de classe aux personnes sélectionnées par le propriétaire.
  - b. Proposer deux heures de formation pratique individuelle à chaque personne.
    - 1) La formation pratique devra permettre à chaque personne de faire fonctionner le système.
    - 2) La formation pratique devra inclure la pratique de chaque opération qu'un opérateur est supposé effectuer.
  - c. Fournir du matériel de formation imprimé à chaque stagiaire, y compris les manuels de produits, les plans de cours, les cahiers d'exercices ou guides de l'étudiant et les examens écrits pour la certification.
3. Traiter de toutes les fonctions du système, y compris les fonctions suivantes :
- a. mise en place du système et configuration de la base de données des détenteurs de badge.
  - b. Fonctionnalités de contrôle d'accès.
  - c. Fonctionnalités de contrôle des alarmes.
  - d. Génération et recherche de rapports.
  - e. Gestion des cartes.
  - f. Procédures de sauvegarde des bases de données.
  - g. Procédures de maintenance courante et de réglage.

## FIN DE SECTION

TruPortal™ 1.5 Spécifications A&I, Version A

Droits d'auteur © 7OCTOBRE2013 United Technologies Corporation, Inc. Interlogix fait partie de UTC Climate Controls & Security, une unité de United Technologies Corporation. Tous droits réservés.

Les informations contenues dans ce document peuvent être modifiées sans préavis.

Interlogix, TruPortal et le logo sont des marques de Interlogix. Microsoft et Windows sont des marques déposées ou des marques de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Les autres noms utilisés dans ce document peuvent être des marques commerciales ou déposées des fabricants ou fournisseurs de leurs produits respectifs.