Cahier des charges : Gestion du Contrôle d'accès & de l'Intrusion

Système de sûreté sur réseau IP

- Contrôle d'accès
- Intrusion
- Supervision graphique
- Interface GTB
- Supervision vidéo

Bureau	Interlocuteurs	Téléphone	Fax
▪ **Agence IDF** **France Nord** Imm. ATRIA 2, rue du Centre 93885 Noisy-le-Grand Cedex	Christophe LARCHER Karim AOUADHI Quentin ROIRET David KOITA Lee ANG Frédéric HELAINE	01 48 15 04 30	01 48 15 04 32
▪ **Siège social** **Agence France Sud** Parc du Golf - Bât 43 CS 60481 350, avenue de la Lauzière 13592 Aix-en-Provence Cedex 3	Patrice BARBERA Hervé ALPHAND Hervé LE MEUR	04 42 37 11 77	04 42 24 28 98
▪ **Bureau** **Bordeaux Mérignac** Centre d'Affaires BBS Aéroport Le Lindbergh - 6 avenue Neil Armstrong 33962 Mérignac Cedex	Christophe DAVID	05 56 18 11 70	05 56 18 91 11

Sommaire

I. Philosophie générale

Ce document définit un système de sûreté dont les caractéristiques correspondent à une approche cohérente et **intégrée** de la sûreté avec la mise en œuvre des fonctions de **Contrôle d'Accès, de Détection Intrusion et supervision de la Vidéo Surveillance.**

Le système possèdera offrira obligatoirement les possibilités suivantes :

1. Caractéristiques fonctionnelles : intégration, ouverture et flexibilité

- **Convivialité** : Le système permettra de superviser le contrôle d'accès, l'intrusion et la vidéo surveillance à partir d'un **poste unique** disposant d'une interface graphique conviviale. Pour certaines fonctions (gestion de visiteurs), une interface WEB permettra l'exploitation à partir d'un poste client léger raccordé en réseau INTRANET.

- **Compatibilité et ouverture** : Le système sera compatible avec toutes les technologies d'identification (badges, biométrie etc.). Il permettra également de gérer les alarmes techniques et de superviser des automates et autres équipements techniques en protocole JBUS/MODBUS ou OPC.

- **Flexibilité** : Les fonctions de sécurité avancée (anti-retour, contrôle renforcé, code sous contrainte, etc.) seront pré-programmées mais le système possèdera une capacité de programmation pour permettre la mise en œuvre d'automatismes adaptés à chaque site et à chaque client. Ces automatismes pourront avoir un caractère permanent ou conditionnel (par exemple : gestion de mode crise, etc.).

- **Modularité** : Le système pourra assurer une gestion multi-site et multi-client/multi-entité. Les fonctions de gestion des accès, de gestion d'intrusion, d'animation des synoptiques, de gestion des visiteurs, de traçage de courbes, de gestion des rondes, de personnalisation des badges, d'exploitation vidéo et de communication inter-systèmes seront assurées par des modules logiciels provenant du même constructeur et donc parfaitement intégrés. Les logiciels de parties tierces ne seront pas admis.

- **Fiabilité :** Le système permettra une gestion intelligente de la maintenance (envoi de messages SMS, télé-maintenance, etc.)

- **Intégration horizontale et verticale** : Des interfaces ou passerelles vers d'autres systèmes (incendie, GTB) permettront une meilleure intégration des fonctions de sûreté/sécurité. Des passerelles informatiques permettront d'aligner automatiquement la base de données des badges avec celle du service du personnel afin d'éviter les doubles saisies.

2. Caractéristiques techniques des Unités de Traitement Local

- **Intégration et autonomie** : Les Unités de Traitement Local (UTL) gèreront les accès et l'intrusion. Elles assureront également des asservissements particuliers tels que la gestion de sas ou d'ouvrants et la gestion des alarmes techniques. Elles seront parfaitement autonomes et continueront d'assurer la totalité de leurs fonctions en cas d'arrêt du serveur (autorisation de passage, anti-retour, gestion de plages horaires, stockage des informations et événements, broadcast et partage d'information etc.).

- **Intégration sécurisée dans un réseau à haut débit** : Les UTL supporteront les protocoles TCP/IP et UDP/IP ***en mode natif***. La connexion sur réseau IP sera directe et ne demandera pas d'interface ou de passerelle. Le réseau IP pourra être un réseau d'entreprise ou un réseau dédié. Le fonctionnement en mode UDP garantira une très faible utilisation de la bande passante.

- **Sécurité et Détection d'Intrusion** : Les UTL seront dotées ***d'entrées équilibrées*** pour la surveillance de ligne (alarme et autoprotection) et pourront gérer des cartes d'extension réparties sur des bus secondaires. Les UTL ***communiqueront directement entre elles, en mode crypté*****,** sur le réseau Ethernet, même en cas d'arrêt du serveur. En fonction de l'architecture retenue, la fonction de détection intrusion pourra être concentrée sur certaines UTL qui assureront de manière autonome la fonction de **centrale d'alarme à bus** ou bien réparties sur plusieurs UTL raccordées en réseau VLAN.

- **Fiabilité** : Les UTL seront capables de surveiller leur alimentation électrique et d'identifier non seulement les défauts d'alimentation (coupure secteur) mais également les défauts de la batterie (absence de batterie, fusible claqué, batterie déchargée, recharge impossible, etc.).

II. Généralités

Ce document présente le Cahier des Clauses Techniques Particulières (CCTP) des équipements de mise en sûreté du site, à savoir :

- Le contrôle d'accès
- Le système de détection intrusion
- Les alarmes techniques GTB
- La supervision graphique

L'objectif de la mise en place du dispositif de sûreté du site est :

- De contrôler et filtrer le flux de personnes en gérant les accès (contrôle d'accès)
- D'empêcher la pénétration des personnes indésirables sur le site (intrusion)
- D'acquérir et d'exploiter ou centraliser un ensemble d'informations ou d'alarmes provenant d'autres dispositifs de sécurité ou techniques (système CVC, GTB, système incendie etc.)

Enfin, le système proposé devra permettre une exploitation simple et conviviale, alliant pérennité et évolution. *Pour cela, le fournisseur du système devra être le développeur et le concepteur tant sur la partie logicielle que matérielle.*

1. Généralités

Ce chapitre présente le Cahier des Clauses Techniques Particulières (CCTP) des équipements de mise en sûreté du site, à savoir le système contrôle d'accès et de détection intrusion.

L'objectif de la mise en place du dispositif de sûreté du site est d'assurer la protection des biens et des personnes en permettant l'acquisition et la centralisation d'un ensemble d'informations ou d'alarmes

provenant d'autres dispositifs de sûreté : lecteur, serrure, radar, contact de position, alarme technique, etc.

Le système proposé devra permettre une exploitation simple et conviviale du logiciel, alliant pérennité et évolution.

III. Architecture matérielle intrusion et contrôle d'accès

Le système sera constitué de plusieurs entités de différents niveaux

- **Niveau 0 :** Capteurs, relais : Les détecteurs d'ouverture, volumétrique, bris de vitre, sirène, lecteurs de badges, autres
- **Niveau 1 :** Automates de terrain sur réseau Ethernet : ici les Unités de Traitement Locales des informations et/ ou les centrales d'alarmes
- **Niveau 2 :** Système de supervision Serveur et les postes clients éventuels.

Le réseau de sûreté de type Ethernet est dédié à la sûreté, l'entrepreneur devra prévoir le câblage, les éléments actifs et chemins de câbles nécessaires à sa mise en œuvre.

Les lecteurs de badges seront connectés sur les UTL, qui sont raccordées directement sur un réseau Ethernet dédié ou pas. Sur ce réseau seront raccordés aussi le serveur, et les postes clients.

Si le réseau de sûreté de type Ethernet est dédié à la sûreté, l'entrepreneur devra prévoir le câblage, les éléments actifs et chemins de câbles nécessaires à sa mise en œuvre.

Si le réseau de sûreté est celui du client, donc existant, l'entrepreneur devra prévoir les liaisons de chaque UTL vers les éléments actifs du client en réalisant un cheminement des câbles tenant compte des contraintes liées au réseau Ethernet (distance, etc.).

Dans ce dernier cas, (réseau du client), il pourra être envisagé de mettre en place un VLAN (réseau local virtuel) afin que le système soit sur un réseau indépendant, mais en restant administré par le client.

Les Unités de Traitement Local (UTL) en contrôle d'accès et intrusion

Les UTL seront natives IP c'est-à-dire raccordées directement sur le réseau informatique Ethernet (sans convertisseur intermédiaire). Elles assureront une mémorisation locale de la liste des badges autorisés, la classe des badges, les plages horaires et les historiques et une gestion autonome des accès - même en cas de déconnexion du réseau Ethernet. Lors de la reconnexion du réseau, les informations seront restituées automatiquement au PC serveur.

Les UTL devront dialoguer avec le PC serveur mais aussi entre elles pour assurer les interactions, asservissements ou fonctions réparties sur plusieurs UTL, leurs dialogues, et les données échangées seront sécurisées par un cryptage de données AES 128 bits.

Les UTL devront être Auto négociable et auto MDI afin de fonctionner dans un maximum de configuration réseau.

Les échanges de données entre UTL et le serveur se feront par des trames UDP afin d'optimiser les échanges et l'encombrement du réseau informatique. Les UTL posséderont et pourront traiter la totalité des informations nécessaires à un fonctionnement autonome.

Elles assureront :

- L'acquisition d'entrées logiques (Tout ou Rien ou équilibrées avec surveillance de lignes) et analogiques permettant la gestion des points de détection de l'installation : radars, contacts d'ouvertures, bris de vitres, etc…
- L'acquisition et la gestion locale des données et commandes nécessaires au contrôle d'accès permettant la gestion de lecteurs de badges.
- La commande sous forme de sorties logiques à relais ou transistors permettant de commander des serrures électriques.
- La mémorisation et l'horodatage des événements, avec restitution « au fil de l'eau » ou suivant une périodicité contrôlée (pour optimiser les communications réseau).
- La mise en oeuvre d'automatismes locaux tels que gestion de sas, ou d'ouvrants, asservissements etc.

L'UTL ou centrale intrusion, pourra fonctionner de manière autonome et/ou intégré dans un système centralisé en réseau IP. Les fonctions anti-intrusion minimales de la centrale sont :

- 32 groupes
- 220 entrées équilibrées et 300 entrées TOR
- 82 sorties relais
- 1 transmetteur digital sur RTC avec gestion de l'écoute et de l'interpellation (16 micros HP adressés individuellement)
- 1 transmetteur IP pour la télésurveillance compatible F1
- 16 claviers d'exploitation (fonctions de mise en marche totale et/ ou partielle, éjection de points, consultations des historiques, gestion de codes utilisateurs, etc.…)
- 16 lecteurs de badges multi technologies

La centrale permettra ainsi la gestion du contrôle d'accès et de l'intrusion.

La centrale sera équipée d'une alimentation continue et régulée 12 volts 3A. Elle devra fournir les informations de défaut secteur et batterie basse. Pour cela l'alimentation du coffret devra fournir une information de défaut secteur ainsi qu'une synthèse pour les défauts suivants : absence de batterie, batterie déchargée ou défaut sur fusible de la batterie. Le coffret disposera d'un contact d'autoprotection à l'ouverture, et d'un bornier sectionnable pour le raccordement du secteur 220 volts monophasés.

La centrale disposera d'extensions locales internes et d'extensions sur deux bus déporté type RS 485.

La centrale disposera deux bus RS485 d'une longueur de 600 mètres chacun, acceptant le câblage en série et/ou en étoile.

L'ensemble des points d'intrusion devra posséder sont adresse unique et être raccordé en bus crypté.

Caractéristiques TILLYS	
Alimentation : 12 VDC/100Ma ***Horloge calendrier*** : secourue par pile lithium débrochable, 32 jours fériés, 64 programmes horaires ***Nbre de badges*** **:** 5000 ***Microprogramme :*** 6000 instructions environ ***Rétrospective*** : 4000 événements ***Communication réseau*** **:** carte réseau ETHERNET 100baseT, connecteur RJ45, 2 voyants d'états ***Autres connexions :*** borniers débrochables à vis, ***Voyants*** **:** sur l'alimentation et sur chaque entrée/sortie ***Dimensions*** **:** HxLxP = 110x125x50 ***Humidité :*** 0 - 95 % sans condensation ***Température d'utilisation :*** 0° à + 50° C	***1 ou 2 lecteurs de badges*** **:** connexion RJ45 ou par module bornier à vis N.B. : jusqu'à 16 lecteurs peuvent être gérés avec des modules d'extensions déportées (voir ci-dessous) ***7 entrées ToR :*** 5 à 30 VDC ou contact sec (1 commun pour 2 entrées) ***4 entrées équilibrées :*** entrées ToR avec surveillance de ligne par résistance ***2 Sorties relais :*** NO/NF 6A/48V= ou 10A/48V~ ***Extensions locales :*** apposées et reliées par connecteur HE10 ***Extensions déportées :*** disposées de deux bus secondaires RS485 d'une longueur de 600 mètres

1.1. Les extensions locales

Elles sont montées sur rails DIN dans le coffret de l'UTL et se raccordent physiquement sur le bornier de celle-ci ou celui d'une autre extension locale.

- Module permettant l'acquisition et la gestion de 8 entrées de type TOR opto-isolées 12V à 24V, afin de gérer des informations de position, de comptage ainsi que des alarmes techniques.
- Module permettant l'acquisition et la gestion de 12 entrées équilibrées avec surveillance de lignes afin de gérer des alarmes intrusion (surveillance de 4 états sur la même entrée).
- Module permettant l'acquisition et la gestion de 4 entrées analogiques 12 bits - 4-20 mA ; 0-4V ou 0-10 v afin de gérer des informations relatives à la GTB (mesure de température ou comptage par exemple).
- Module disposant de 8 sorties transistors 12 à 24 V 500mA à 1,4 A maxi afin de réaliser des asservissements de caméras vidéos, de sirènes ou d'indicateurs lumineux.
- Module disposant de 8 sorties relais NO/NF 6A/ 48V ou 10A/48V afin de commander des organes de fermeture ou des équipements techniques (par exemple : commande d'ascenseur ou de sas).
- Module disposant de 4 sorties relais statiques 230 VAC afin de piloter des commandes d'éclairages (par exemple : asservissement de l'éclairage sur intrusion).

1.2. Les extensions déportées

Déportées sur le(s) bus secondaire(s) RS485 de l'UTL, elles peuvent être montées sur rail DIN pour intégration dans un coffret alimenté ou dans un simple boîtier mural téléalimenté.

- Module Déporté Intrusion permettant de gérer 6 entrées équilibrées, 3 entrées TOR, et 2 sorties transistors.
- Module EQUILOCK permettant la mise série des points d'intrusion sur bus (distance max du Bus 300 mètre).
- Clavier Déporté avec afficheur permettant la gestion de fonctions intrusion (mise en marche/arrêt, consultation d'alarmes en cours, derniers événements, etc.).

Caractéristiques communes des claviers 17 touches TACTILLYS	
Alimentation : 12 VDC ***Température d'utilisation*** : de -10°C à + 50°C ***Connectique*** : Bornier débrochable à vis ***Consommation (hors lecteur) :*** ▪ Clavier actif : 140 mA ▪ Clavier en veille : 50 mA ***Fixation :*** En saillie par 4 vis **Auto protégé à l'ouverture**	***Distance entre le clavier et l'UTL*** : 600 mètres ***Couleur blanche*** ***16 Touches sensitives*** ***2 lignes de 20 caractères*** ***3 voyants programmables***

- Module Déporté pour Porte permettant de gérer un lecteur de badge : 1 entrée lecteur, 3 entrées TOR, 2 entrées équilibrées, 1 sortie relais, 1 sortie transistor, 1 buzzer.
- Module Déporté pour Lecteur entrée et sortie: 2 entrées lecteurs, 3 entrées TOR, 2 entrées équilibrées, 1 sortie relais, 1 sortie transistor, 1 buzzer.
- Module Déporté GTB permettant de gérer 8 entrées TOR et 2 sorties relais.
- Module Déporté disposant de 4 sorties relais statiques.
- Module Déporté disposant de 8 sorties relais.
- Module Déporté de Gestion de plaques minéralogiques

Les Unités de Traitement Local (UTL) en contrôle d'accès

Les UTL devront pouvoir se fixer sur rail DIN à intégrer dans une armoire spécifique ou dans un coffret à alimenter en 220 volts. Ces coffrets techniques seront répartis dans les placards courants faibles implantés dans le bâtiment à chaque niveau ou zone, à proximité des chemins de câbles. Dans certain cas, il pourra également être envisagé de mettre les coffrets en faux plafonds ou en local technique.

Les coffrets seront équipés d'une alimentation continue et régulée 12 volts 3A se fixant sur le rail DIN du coffret. Le système de sûreté devra fournir les informations de défaut secteur et batterie basse. Pour cela l'alimentation du coffret devra fournir une information de défaut secteur ainsi qu'une synthèse pour les défauts suivants : absence de batterie, batterie déchargée ou défaut sur fusible de la batterie.

Ces informations seront remontées au superviseur sous forme de deux contacts TOR repris par l'UTL. Le coffret disposera de un ou deux rails DIN permettant la fixation de l'UTL et des modules d'extension, ainsi que d'un contact d'autoprotection à l'ouverture, et d'un bornier sectionnable pour le raccordement du secteur 220 volts monophasés.

Fonctionnalité très importante : lors d'un téléchargement les UTL devront continuées à fonctionner normalement, c'est à dire lire les badges, exécution des automatismes embarqués dans l'UTL (commande de la gâche par exemple), et remontées les événements sur le superviseur en temps réel. Tout système ne permettant pas d'assurer cette fonctionnalité ne sera pas retenu.

Le coffret sera de type BTE40 (un rail DIN) ou BTE80 (2 rails DIN) de marque TIL Technologies. Dans certains cas, les modules peuvent être intégrés directement dans des armoires ou baies.

Dans un but de flexibilité et d'évolutivité, l'UTL devra impérativement disposer d'extensions locales et d'extensions sur bus déportés type RS 485. Les extensions permettront les fonctions suivantes, de base, les capacités minimum des UTL seront :

- 2 lecteurs de badges multi-technologies extensibles à 8.
- 7 entrées TOR.
- 4 entrées équilibrées.
- 2 sorties relais.
- 19 000 badges extensibles à 40000 en configuration 2 lecteurs uniquement.

La faculté des UTL à pouvoir gérer des entrées de différents types directement ou via des modules d'extension permettra de faire l'acquisition d'alarmes techniques, intrusion, et autres.

L'UTL pourra gérer jusqu'à 8 lecteurs de badges, 32 entrées analogiques, 16 entrées vidéo analogiques et 8 sorties vidéo analogiques.

Véritable automate, chaque UTL sera entièrement programmable permettant souplesse et adaptation du système aux besoins présents et futurs du client.

Les caractéristiques techniques des UTL devront être conformes au tableau ci-dessous :

Caractéristiques UTiL	
Alimentation : 12 VDC/100Ma ***Horloge calendrier*** : secourue par pile lithium débrochable, 32 jours fériés, 64 programmes horaires ***Nombre de badges*** : 19000 pour UTIL8 ou 40000 pour UTILMX ***Microprogramme :*** 6000 instructions environ ***Rétrospective*** : 4000 événements ***Communication réseau*** : carte réseau ETHERNET 100baseT, connecteur RJ45, 2 voyants d'états ***Autres connexions :*** borniers débrochables à vis, ***Voyants*** : sur l'alimentation et sur chaque entrée/sortie ***Dimensions*** : HxLxP = 110x125x50 ***Humidité :*** 0 - 95 % sans condensation ***Température d'utilisation :*** 0° à + 50° C	***1 ou 2 lecteurs de badges*** : connexion RJ45 ou par module bornier à vis N.B. : jusqu'à 8 lecteurs peuvent être gérés avec des modules d'extensions déportées (voir ci-dessous) ***7 entrées ToR :*** 5 à 30 VDC ou contact sec (1 commun pour 2 entrées) ***4 entrées équilibrées :*** entrées ToR avec surveillance de ligne par résistance ***2 Sorties relais :*** NO/NF 6A/48V= ou 10A/48V~ ***Extensions locales :*** apposées et reliées par connecteur HE10 ***Extensions déportées :*** disposées de deux bus secondaires RS485 d'une longueur de 600 mètres

1.1. Les extensions déportées

Déportées sur le(s) bus secondaire(s) RS485 de l'UTL, elles peuvent être montées sur rail DIN pour intégration dans un coffret alimenté ou dans un simple boîtier mural téléalimenté.

- Module Déporté pour Porte permettant de gérer un lecteur de badge : 1 entrée lecteur, 3 entrées TOR, 2 entrées équilibrées, 1 sortie relais, 1 sortie transistor, 1 buzzer.
- Module Déporté pour Lecteur entrée et sortie: 2 entrées lecteurs, 3 entrées TOR, 2 entrées équilibrées, 1 sortie relais, 1 sortie transistor, 1 buzzer.
- Module Déporté disposant de 4 sorties relais statiques.
- Module Déporté disposant de 8 sorties relais.
- Module déporté de Gestion de plaques minéralogiques

Les lecteurs de badges

Les lecteurs de badges seront de type multi technologies et universel dans la gamme 13.56 MHz. Il permettront de lire plusieurs technologies : Mifare, Desfire, Calypso, Icao, etc…selon les normes ISO 14443-A part 3, ISO15693.

Le lecteur devra avoir une consommation très faible (0,25W), le client pourra choisir la couleur de son lecteur selon un RAL fourni par ce dernier.

L'entreprise devra proposer des lecteurs carrés à installer sur des pots d'encastrement pour les lecteurs intérieurs, et des lecteurs longs pour les accès extérieurs.

Les lecteurs de badges seront de type proximité passif avec une distance de lecture de l'ordre de 3 à 5 cm. Ils pourront être installés jusqu'à une distance d'environ 100 mètres de l'UTL. Le protocole de dialogue sera RS485, cette liaison lecteur – UTL sera sécurisée par un cryptage. Par conséquent le lecteur sera en mesure de donner à l'UTL le signe de vie. Cette information sera superviser dans le système d'exploitation.

Les lecteurs devront avoir un aspect soigné ainsi qu'une bonne résistance aux intempéries et aux dégradations extérieures.

Une version lecteur de table (lecteur enrôleur avec liaison série RS232 et boîtier) sera disponible pour le (ou les) poste(s) de supervision.

Les badges MIFARE devront être compatibles avec les spécifications des lecteurs (voir ci-dessus). Ils auront une mémoire de 4 K octets. Leur dimension sera 85 X 54 X 2.2mm.

Caractéristiques PROXILIS	
Alimentation : *12 VDC (9 à 15 VDC)* ***Consommation moyenne :*** *0,25 W* ***Fréquence d'émission :*** *13.56 MHz* ***Distance maximale entre le module et le lecteur :*** *600 m* ***Interface de communication :*** *RS485 crypté, signe de vie* ***Connectique :*** *Bornier 4 points inclus* ***Matériaux :*** *ABS* ***Dimensions :*** *86 x 86 x 16 mm* ***Fixation :*** *2 vis, sur boite d'encastrement 80mm ou en applique*	***Distance de lecture :*** *jusqu'à 8 cm selon la technologie du badge* ***Signalisation :*** *Eclairage d'ambiance blanc* *Leds rouge/vert pilotables* *Buzzer intégré* ***Température de fonctionnement:*** *de +5°C à +40°C* ***Poids :*** *0.10 Kg* ***Disponibles en 3 versions : Proxilis-Standard, Proxilis-Pro et Proxilis-Sante***

Lecteur MIFARE type cylindre européen - Apério

Le lecteur Mifare sera de type cylindre européen avec un bouton mécanique intérieur à sortie toujours libre. Il sera équipé d'un bouton extérieur intégrant une antenne Mifare pour la lecture des badges répondant à la norme ISO 14443A.

Le bouton extérieur sera équipé d'une signalisation lumineuse tri couleur indiquant la prise en compte puis la validation ou non du badge, cette led devra être visible sur la périmétrie du bouton pour garantir une acquisition malgré la présence du badge devant le bouton

Il devra communiquer en temps réel via une liaison sans fil dans un rayon de 5 mètres et suivant la norme IEEE 802.15.4 vers son Hub.

L'UTL (ou le contrôleur de porte) du système de contrôle d'accès devra être capable de communiquer avec le Hub du lecteur via une liaison RS485.

La sécurité des données transitant sur la liaison sans fil entre le hub et le lecteur sera réalisée avec un encryptage 128 bits de type AES.

La liaison entre le HUB et le système de contrôle d'accès permettra la gestion des droits et la gestion d'évènements en temps réel par un seul et unique système de contrôle d'accès.

Lecteur MIFARE ensemble béquilles - Apério

Le lecteur Mifare sera de type ensemble plaque béquille, dont la plaque extérieure serra munie de la tête de lecture des badges répondant à la norme ISO 14443A. Il permettra, par un embrayage motorisé, une action sur la béquille pour la décondamnation de la porte.

Cette tête de lecture sera équipée d'une signalisation tri couleur indiquant la prise en compte puis la validation ou non du badge.

Il devra communiquer en temps réel via une liaison sans fil dans un rayon de 5 mètres et suivant la norme IEEE 802.15.4 vers son Hub.

L'UTL (ou le contrôleur de porte) du système de contrôle d'accès devra être capable de communiquer avec le Hub du lecteur via une liaison RS485.

La sécurité des données transitant sur la liaison sans fil entre le hub et le lecteur sera réalisée avec un encryptage 128 bits de type AES.

La liaison entre le HUB et le système de contrôle d'accès permettra la gestion des droits et la gestion d'évènements en temps réel par un seul et unique système de contrôle d'accès.

OPTION : Verrouillage automatique de la porte

Les portes avec lecteur Mifare cylindre européen ou ensemble béquilles seront équipées d'une serrure mécanique à verrouillage automatique et sortie d'urgence.

Les serrures présenteront les caractéristiques suivantes :

- Résistance à l'effraction d'une valeur supérieure à 1000 kg.
- Réversibilité toutes mains (droite/gauche et poussant/tirant) pour une maintenance ultérieure par un modèle unique.
- Verrouillage automatique sur 2 points sécurisés :
    - Un contre pêne de sécurité et un pêne demi-tour afin d'empêcher les sorties de pêne accidentelles.
- Axe et entraxe, respectivement à 50mm/70 mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés)

La mise en œuvre des serrures sera adaptée au support de la porte (bois, métal ou verre).

Il appartient au présent lot de s'assurer que les bloc-portes assurent le degré coupe-feu ou pare-flamme demandé, et que les équipements sont mis en place conformément au procès verbal du fabricant de serrure.

IV. Architecture Informatique et Logicielle

1. Le poste serveur

Le système proposé aura une architecture logicielle Client /Serveur. Le poste principal serveur sera dédié à la sûreté de la ville. Il sera raccordé sur un réseau de type Ethernet TCP/IP. Il supervisera le dialogue avec les centrales et les postes clients raccordés sur le réseau Ethernet TCP/IP. Il disposera d'une capacité de stockage mémoire permettant le bon fonctionnement des applications.

Le logiciel de contrôle d'accès, intrusion et supervision sera installé sur ce poste, permettant à la fois de paramétrer, d'exploiter les badges et de visualiser des alarmes, défauts et états de fonctionnement du système sur des vues IHM représentant les plans du bâtiment par niveaux et par zones.

Le système pourra gérer au minimum 4096 lecteurs de badges avec une capacité d'extension de 200% et surveiller jusqu'à 40 000 points logiques ou analogiques répartis sur un ou plusieurs sites. En configuration de base, le système devra pouvoir gérer au moins 128 postes clients.

Configuration requise pour le serveur pour installation moyenne :

- Micro-ordinateur compatible PC (type PENTIUM IV – 3 GHz)
- Carte Ethernet 100Mbits
- 4 Go de RAM
- Disque dur 160 Go minimum
- Ecran plat TFT 19''
- Clavier, souris, Windows Serveur 2003, 2008
- 2 ports série au minimum
- 2 ports USB

L'application du système proposé permettra de virtualisation avec vmware.

Le système de supervision assurera une sauvegarde automatique et périodique de la base de données sur un poste client ou sur un media à définir. Il permettra de définir et de paramétrer la date, l'heure et le chemin de la sauvegarde.

2. Les postes clients

Le ou les postes clients seront raccordés sur le même réseau sûreté que le poste serveur. Ils auront les mêmes capacités de gestion que le poste serveur.

Configuration typique pour le poste client d'une installation moyenne :

- Micro-ordinateur compatible PC (type PENTIUM IV – 3 GHz)
- Carte Ethernet 100 Mbits
- 2 Go de RAM,
- Disque dur 80 Go minimum,
- Ecran plat TFT 19''
- Clavier, souris, Windows XP PRO, Win 7
- 1 port série au minimum
- 2 ports USB

3. Le logiciel de contrôle d'accès, intrusion, exploitation vidéo et supervision

Le logiciel de supervision permettra la mise en œuvre des fonctionnalités suivantes à partir d'un poste d'exploitation unique ou de n'importe lequel des postes d'exploitation dans une architecture serveur client :

- Paramétrage général du système
- Attribution des droits des opérateurs
- Toutes les fonctions de gestion du contrôle d'accès, depuis la création ou l'importation du fichiers de usagers jusqu'à l'exploitation des historiques
- Création, personnalisation et impression de badges
- Fonctions de sûreté intrusion, y compris gestion de télétransmission d'alarmes

- Gestion de rondes
- Fonction de gestion technique de bâtiment (supervision d'automates programmables en protocole MODBUS/JBUS, comptages, alarmes techniques, gestion et affichage de valeurs analogiques, traitement des variables par lots etc.)
- Interface et échanges de données avec d'autres systèmes (incendie, GTB etc).
- Envoi d'emails à un serveur SMTP
- Sauvegardes et restauration du système (éventuellement avec des outils externes pour les bases SQL)
- Maintenance du système

Le logiciel permettra également l'encodage des secteurs des badges Mifare et Desfire.

Le logiciel fonctionnera sous un environnement Windows multitâche et multi-utilisateurs. Il sera modulaire, convivial, et évolutif. Le système permettra la gestion de sites déportés par réseau informatique, ligne spécialisée ou RTC.

Afin d'assurer l'ouverture et l'évolutivité du système, le logiciel devra être multi base de données, c'est à dire être disponible en base avec une base de données simple du type MSDE. Ainsi le système supportera au minimum les bases de données de type SQL SERVER 2003, 2008 et ORACLE 10G.

Tous les systèmes fonctionnant avec des bases de données propriétaires ou de type Access seront exclus.

Le logiciel, de part son ouverture, devra être capable de proposer des interfaces ou passerelles optionnelles permettront l'interfaçage du système avec les équipements suivants :

- Informatique de gestion pour alignement de la base badges de contrôle d'accès avec celle du personnel.
- Annuaire Activ Directory, LDAP.
- Système de sécurité incendie.
- GTB, etc.

Le système devra être capable de superviser des automates industriels ou d'autres équipements techniques tels que systèmes de CVC ou détection incendie en protocole Modbus.

Le système devra être capable de superviser des automates industriels ou d'autres équipements techniques tels que systèmes de CVC ou détection incendie en protocole Modbus ou Bacnet.

Le système devra permettre la gestion de SAS, d'ascenseurs, la gestion de parking, la gestion de parcours et la gestion de l'intrusion. L'interaction entre l'intrusion et le contrôle d'accès sera simple et conviviale grâce à l'interface graphique.

Tout événement sur le système sera tracé, les événements pourront être d'origine différente, à savoir :

- Les autorisations et les interdictions de badges.
- Les erreurs de manipulation.
- Les tentatives de fraudes.
- Les modifications, suppression, ajouts de badges.
- Les modifications, suppression, ajouts d'accès à un porteur de badges.

V. Utilisation du système

1. L'accès au logiciel

L'accès des agents sur le logiciel sera contrôlé par mots de passe. Il sera possible de gérer jusqu'à 64 agents différents. Les droits d'accès de chacun sont personnalisables par définition des droits : accès aux historiques, au paramétrage, modifications de badges, à la visualisation, etc.

Chaque intervention dans le système est archivée dans l'historique avec le nom de l'opérateur et l'heure. La durée d'accès au système est paramétrable.

2. Plages horaires

Le système pourra gérer au minimum 64 plages horaires différentes par site. Elles auront les particularités suivantes :

- Jusqu'à 2 ou 4 créneaux par jour.
- Plages communes au contrôle d'accès et à la GTB ou plages distinctes.
- Prise en compte des jours fériés.
- Définition du type de plage (quotidienne, hebdomadaire.).
- Plage active ou inactive.

3. Groupes de lecteurs

Le système permettra de créer jusqu'à 1024 groupes de lecteurs. Un groupe de lecteurs est un ensemble regroupant de un à 1024 lecteurs Il permet de simplifier la gestion des droits d'accès des usagers et de créer des zones géographiques particulières (voir ci-dessous *Gestion des zones et anti-retour*).

4. Attribution des droits d'accès des usagers

Le profil d'accès permet de prédéfinir les accès pour une catégorie d'usagers sur un ou plusieurs sites. L'attribution des droits d'accès aux usagers pourra se faire de deux façons différentes :

A. Gestion Individuelle

L'attribution des droits d'un individu se fera badge par badge sur des lecteurs ou groupes de lecteurs avec attribution d'une plage horaire pour chaque lecteur ou groupe de lecteurs, avec un début et une fin de date de validité pour chaque attribution de droits.

B. Gestion Multi-Profils

A chaque badge, il sera possible d'associer un (ou plusieurs) **profil d'accès**. On pourra ainsi associer un profil général (droit d'accès à plusieurs lecteurs) à plusieurs personnes, facilitant ainsi la création des profils d'un groupe de personnes ayant les mêmes droits d'accès.

La fenêtre de gestion des accès devra être modifiée en conséquence, on observera :

- La disparition de la liste affichant le détail des accès d'un profil
- La disparition des contrôles associés à cette liste
- L'apparition d'un nouveau bouton permettant d'ajouter un ou plusieurs profils au badge
- L'apparition de nouveaux boutons permettant de modifier la priorité des accès les uns par rapport aux autres (la liste est alors affichée par ordre de priorité)
- L'apparition d'un nouveau bouton permettant de spécifier les dates de début et de fin de validité d'un accès particulier.

Chaque profil pourra être défini par une date de début et de fin de validité. Un porteur de badge pourra ainsi avoir plusieurs profils actifs en même temps. Un niveau de priorité permettra de définir les accès autorisés.

Dans le cas de la gestion par profil, il sera possible de gérer des exceptions et d'attribuer ou d'enlever des droits spécifiques à un badge particulier. On modifiera individuellement les accès d'un porteur de badges en utilisant la gestion des accès par lecteurs et/ou groupes de lecteurs.

5. La fiche utilisateur

Elle permettra d'identifier chaque usager (porteur de badge, etc..) et de gérer ses droits. Elle devra au minimum contenir les fonctions et champs suivants :

- Les nom et prénom de l'utilisateur.
- 16 champs personnalisables : N° de matricule, véhicule, adresse, date de naissance, etc.
- Un champ de commentaires : intérimaire, etc.
- L'agent créateur, ainsi que la date de création.
- Sites d'appartenance (pour la gestion multi-site uniquement).
- Validité et date de fin de validité du badge.
- Le profil de base attribué au badge si la gestion des profils est utilisé.
- La fonction badges :
    - passe partout,
    - liste rouge (fonction qui garantit la confidentialité lors de l'utilisation des badges : le nom des titulaires n'apparaîtra pas),
    - liste noire (fonction qui permet de surveiller particulièrement le badge : badge déclaré volé par exemple),
    - visiteur (voir également la fonction gestion des visiteurs ci-dessous).
- La classe du badge (65536 possibilités) qui permet une gestion catégorielle permanente ou conditionnelle. Par exemple : comptage ou gestion de crise.
- Acquisition automatique du numéro de badge via un lecteur- enrôleur de badges.
- 4 champs pour autoriser jusqu'à 4 numéros de badges différents par fiche. Ces champs pourront contenir des numéros de plaque d'immatriculation nécessaires au contrôle d'accès automobile.
- Acquisition automatique de l'empreinte digitale (enrôlement)
- Un onglet permettant de lire (ou de définir) les habilitations du titulaire de la fiche utilisateur, celle-ci auront une période de validité à définir. Le système acceptera 256 habilitations différentes, un même badge pouvant cumuler plusieurs habilitations.
- Code secret pour les fonctions intrusion ou double sécurité (badge + code).
- Personnalisation du badge depuis la fiche utilisateur : préparation du fond de carte + personnalisation du badge directement sur une imprimante.

Pour faciliter l'exploitation, le système possédera une fonction de gestion avancée des badges. Celle-ci permettra de rechercher les badge puis de modifier leur propriétés en utilisant plusieurs critères d'extraction tels que :

- La date de validité
- La date de création
- Les profils
- Le contenu d'un champ de la fiche badge
- La classe du badge
- Les affectations et droits particuliers : avec/ou sans anti-retour, passe partout, liste noire, liste rouge.

Tout changement intervenant sur la fiche badge est tracé (ajout, modification, ou suppression) sur un ou plusieurs champs de la fiche. Il sera également notifié le nom de l'opérateur ayant réalisé la manipulation.

Lors de l'extraction, il sera possible de sélectionner les champs à extraire de la fiche utilisateur, à savoir : date de naissance, adresse, ville, code postal, profession, entreprise.
A partir du résultat de l'extraction, il sera possible de modifier les droits des badges dans la même fenêtre, en cochant simplement les cases à modifier. Les données extraites pourront être sauvegardées sur un fichier texte.

Cette fonctionnalité permet l'exploitation du système de façon et convivial. Par conséquent, cette fonction sera obligatoire dans le système retenu.

6. Multi Site / Multi Client / Multi Entité

A. Principe

Cette fonction permettra de cloisonner un système de contrôle d'accès en plusieurs entités (ou sites) bénéficiant d'une gestion autonome du contrôle d'accès. Les entités pourront être d'ordre géographiques (un étage, un bâtiment, un parking…) et/ou fonctionnelles (service administratif, service production, locataires A et B…).

Le système pourra gérer 64 entités et permettra à chacune d'avoir une maîtrise différenciée de ses accès. Chaque entité disposera de 64 plages horaires indépendantes utilisées soit dans le cadre du contrôle d'accès, soit dans le cadre de la gestion technique de bâtiment.

B. Gestionnaire principal et agent gestionnaire

Le système devra nécessairement comporter un gestionnaire principal. Ce dernier sera le seul qui aura accès à la totalité de la base de donnée commune aux différents sites. Le gestionnaire principal verra tous les badges, pourra les créer, les supprimer, ou les modifier. Il aura aussi la fonction d'administrateur général et devra dans ce cadre attribué les droits de chaque agent gestionnaire.

L'agent gestionnaire, quant à lui, devra pouvoir gérer uniquement les lecteurs de son site. Dans un souci d'autonomie et de confidentialité, l'agent gestionnaire ne verra ni les lecteurs, ni les badges, ni les historiques de passages des autres sites. L'agent gestionnaire doté, par le gestionnaire principal, du droit de gestion des accès pourra créer des badges pour le personnel de son service uniquement sur les lecteurs pour lesquels il aura été qualifié.

C. Zones ou communes

Cette configuration devra prendre en compte la possibilité de gestion de zones communes à plusieurs clients. Ce cas de figure implique nécessairement la gestion d'une base de donnée unique et commune (détenu intégralement par le seul gestionnaire principal).

Certains lecteurs pourront en effet être gérés en communs par plusieurs agents gestionnaires. De même un badge devra pouvoir appartenir à plusieurs entités et pourra de ce fait avoir accès à plusieurs sites. Un tel badge (donnant accès à plusieurs sites) ne pourra être délivré et supprimé que par un opérateur ayant capacité à gérer tous les sites concernés.

7. Gestion des zones et anti-retour

Le système sera capable de gérer 128 zones géographiques. Une zone est définie par un groupe de lecteurs d'entrée et un groupe de lecteurs de sortie. La création de zones permettra de gérer les fonctions suivantes :

- Fonction anti-retour sur l'entrée et/ou la sortie
- Comptage automatique du nombre de personnes présentes dans la zone
- Possibilité d'exclure un badge de la zone au bout d'une durée à définir
- Possibilité de connaître la liste des personnes présentes dans la zone en dynamique

Plusieurs modes de fonctionnement seront possibles :

- En cas de badgeage ***en entrée seulement***, le fonctionnement de l'anti-retour sera basé sur une simple temporisation déclenchée par le passage du badge sur le lecteur. Le badge ne sera plus autorisé sur ce lecteur avant expiration de la temporisation.
- Si un badgeage est nécessaire ***en entrée et en sortie de zone***, le système empêchera un usager de retourner dans une zone avant l'expiration d'une temporisation déclenchée par son entrée ou qu'il ait badgé en sortie. Il pourra également interdire de sortir à un usager qui n'aura pas badgé en entrée au préalable.
- Enfin une fonction de verrouillage par asservissement permettra d'interdire le badgeage sur tous les lecteurs situés dans une zone si l'usager n'a pas badgé en pénétrant dans cette zone.

8. Supervision des alarmes et Gestion des catégories de variables

Pour tout événement (changement d'état d'une entrée ou d'une sortie, alarme, passage de badge, action d'un agent…), un message horodaté pourra apparaître au fil de l'eau et sera archivé dans l'historique.

Les alarmes – et d'une manière générale les variables surveillées par le système - pourront être classées par catégories suivant leur type (contrôle d'accès, incendie, intrusion ou techniques) et/ou suivant leur localisation géographique. Le fil de l'eau permettra de tracer les événements horodatés suivants :

- ***pour un changement d'état ou une alarme***
  - la désignation de la voie (le libellé en clair)
  - son état (normal, défaut, etc.)
- ***pour un passage de badge***
  - le nom de la personne
  - l'heure
  - l'état d'autorisation du badge (autorisé, inconnu, hors plage horaire, anti-retour…)
- ***pour les actions d'un agent***
  - l'opération effectuée
  - le nom de l'agent
  - le poste concerné
- ***pour les autres événements***
  - le type d'événement
  - le nom de l'organe du système concerné
  - le poste concerné

Les fenêtres de surveillance devront permettre une gestion des alarmes en temps réel. Toute voie logique pourra être déclarée comme une alarme avec des conditions sur son acquittement et son niveau. Des messages de différentes couleurs apparaîtront selon que l'alarme est acquittable ou non, si elle a été acquittée avant ou après un nouveau changement d'état :

- Message d'apparition d'alarme :
  - en rouge sur fond blanc : alarme non acquittable (défaut)
  - blanc sur fond rouge : alarme à acquitter (alerte)
- Message de changement d'état d'alarme à acquitter : jaune sur fond rouge (le défaut a disparu avant acquittement).
- Après acquittement, l'alarme est visualisée en rouge sur fond blanc (si le défaut persiste).

Les apparitions, acquittements et effacements d'alarmes sont tous horodatés et archivés en base de données.

Envoi de télécommande tout ou rien

Depuis l'unité centrale, il est possible d'effectuer des télécommandes logiques par différents moyens :

- En cliquant directement sur le **nom de la voie** dans la fenêtre de télécommande du logiciel
- En agissant directement sur un **objet graphique ou un bouton de commande dans les synoptiques**.

Toutes les télécommandes seront horodatées et archivées avec le nom de l'opérateur qui les aura effectuées.

9. Les historiques

La capacité de stockage du système ne sera pas limitée (plus 1 million d'événements). Deux requêtes d'extraction des historiques seront disponibles :

- ***Critères d'extraction simples*** *:* Période de recherches (dates & jours), alarmes, changements d'états, télécommandes, badges interdits, badges autorisés.
- ***Critères d'extraction détaillés*** *:*
    - Evénements badges : autorisés, interdits, liste noire, anti-retour avec le choix du badge, du profil, du lecteur, du groupe de lecteurs.
    - Evénements voies : alarmes, logiques ou numériques avec sélection de la voie.
    - Evénements modules : connexion/déconnexion, reset avec sélection du module et de la ligne.
    - Evénements de lignes : début/fin de scrutation et téléchargement.
    - Evénements des agents : Acquittement, télécommandes, forçages de voies, connexions/déconnexions avec le choix de l'agent.

Les historiques peuvent être exportés dans un fichier texte pour une exploitation ultérieure. Les requêtes extraites des historiques peuvent être imprimées sur l'imprimante du P.C. de sûreté.

Afin d'optimiser le stockage des historiques du système de contrôle d'accès/intrusion, celui-ci permettra la purge intelligente des historiques, soit périodiquement, soit sur un volume d'événements différenciés voie par voie.

10. Traitement par lot

Les historiques devront permettre l'édition de données par voies afin d'effectuer des traitements par lots. Cette fonction permet de connaître la valeur moyenne, la somme, la valeur mini, la valeur maxi pour une ou plusieurs voies prédéfinies sur une période déterminée. Exemple : nombre moyen d'utilisateurs dans un parking, température moyenne de bureaux sur 1 mois avec les valeurs minimum et maximum, temps de fonctionnement d'un équipement, etc.

Cette fonctionnalité permettra également d'éditer des statistiques d'alarmes, afin de connaître le nombre d'alarmes intrusion (volumétrie, périmétrie, ou autres) sur une période déterminée.

11. Journal de bord

Le système intégrera la fonction *journal de bord* permettant à l'opérateur de saisir librement en main courante un commentaire pour chaque événement survenu sur le système de contrôle d'accès et d'intrusion. Ce journal sera ensuite archivé. Il pourra être consulté et imprimé.

12. Animation de synoptiques – supervision graphique

Le système permettra la supervision des équipements sur des synoptiques représentant des vues et des niveaux des bâtiments ou des tableaux dynamiques. Pour cela, le système proposera un éditeur de synoptiques permettant de personnaliser des plans existants sous forme de fichiers. L'éditeur aura des fonctions de dessin ce qui permettra la personnalisation de chaque plan. Chaque vue représentera un tableau ou plan dynamique permettant une exploitation conviviale avec icônes, animations, télécommandes, changement de couleurs, etc.

Sur apparition d'une alarme, le système devra afficher le synoptique correspondant à cette alarme (localisation physique ou tableau de synthèse) avec une gestion de consigne et de priorité.

La mise en place des synoptiques rendra l'exploitation des alarmes plus conviviale pour l'exploitant grâce à des vues détaillées et personnalisées de l'installation. A partir de la page d'accueil, l'exploitant pourra appeler des menus lui permettant de superviser et de télé-agir sur l'ensemble de son installation. Il pourra également appeler des menus du programme de supervision à partir de n'importe quel synoptique (par exemple gestion des badges, gestion des zones ou gestion des visiteurs).

Afin d'optimiser l'exploitation du système, il sera prévu une vue par niveau et par bâtiment. Toutefois, le système ne devra pas être limité dans le nombre de synoptiques ou de vues. Chaque synoptique

pourra commander n'importe quel autre synoptique, afin que l'opérateur puisse obtenir le détail de l'alarme s'il le souhaite par des « sous plans» permettant un effet de zoom, en cliquant simplement sur le plan (le nombre de sous plan ne sera pas limité).

Depuis le PC sûreté, l'exploitant pourra effectuer les mises en marche et à l'arrêt du système intrusion simplement en agissant sur les plans ou les animations définis sur les vues. Les changements d'états du système intrusion seront signalés sur le synoptique (clignotement, texte ou changement de couleur de la zone ou de l'icône.)

Le principe « d'info bulle » sera mis en place pour permettre de faciliter l'utilisation du synoptique. Le passage à proximité d'un élément actif (icône ou plans) entraînera l'ouverture d'une bulle d'information renseignant l'opérateur sur la fonction associée à cet élément. Enfin, l'opérateur devra pouvoir exécuter certaines fonctions à définir (tel que l'éjection de points en mode intrusion) simplement par un clic droit de la souris. Cette action entraînera l'apparition d'un menu local et permettra une gestion aisée du synoptique.

13. Gestion des habilitations (option)

Les contraintes et obligation du site imposent la mise en place d'habilitations professionnelles conditionnant les droits d'accès des usagers sur le site.

Les autorisations d'accès d'un badge devront être conditionnées par l'obtention d'une habilitation. Cette condition de validité, limité dans l'espace et dans le temps, pourra être attribuée et renouvelée par des agents différents.

L'accès à certains lecteurs du système pourra être conditionné par la détention d'une habilitation valide, pour un badge donné.

Le système acceptera 256 habilitations différentes, chacune d'entre elle concernera des lecteurs ou des groupes de lecteurs différents, sur des périodes différentes impliquant des consignes de sécurités différentes. En outre, un même badge pourra cumuler plusieurs habilitations.

Enfin, une gestion avancée des badges, par lots, sera possible permettant ainsi de faciliter les traitements sur les conditions de validité supplémentaire (attribution, report, contrôle) pour un groupe de personnes.

Les habilitations seront embarquées dans les UTL une semaine avant l'échéance de cette dernière – la gestion des habilitations ne dépendra donc pas du PC serveur – tout système ne répondant pas à cette fonctionnalité ne sera pas retenu.

14. Personnalisation de badges

Afin de simplifier l'exploitation des badges et leur paramétrage, le système de contrôle d'accès intégrera une fonction de personnalisation de badges ce qui permettra de travailler sur la même base de données que celle du contrôle d'accès et sur le même PC.

La personnalisation des badges proposés devra être donc impérativement être issue du même constructeur que le logiciel de contrôle d'accès et supervision. Le module de personnalisation devra posséder les fonctionnalités suivantes :

La personnalisation graphique :

- Préparation du fond de carte (possibilité de modification grâce à l'éditeur intégré)
- Importation du logo, nom, prénom, numéro de matricule, etc..
- Acquisition de photo à partir d'une source vidéo extérieure : Webcam, appareil numérique, caméra IP motorisée, etc…
- Encodage de piste magnétique ou code à barres.
- Impression directe sur l'imprimante à sublimation.
- Impression de pictogrammes.

La personnalisation électrique : Dans le cas de gestion de badges de type MIFARE secteurs.

- Définition des secteurs MIFARE
- Définition et gestion des clés de lecture et écriture MIFARE
- Définition et gestion de la MAD

- Définition du type d'identifiant (format hexadécimal, alphanumérique, décimal) qui sera encodé dans les badges. Cet identifiant pourra être générer par le système avec garantit d'unicité ou importé par le client depuis une base tierce.

La personnalisation graphique et électrique se fera à partir d'une imprimante à badges permettant de réaliser en une seule opération l'impression et l'encodage du badge.
La personnalisation de badges pourra être faite individuellement ou par série de badges depuis la gestion avancée de badges.

15. Gestion de rondes et parcours (option)

Le système permettra l'utilisation des lecteurs de badges du contrôle d'accès pour la gestion de rondes. Le gardien devra effectuer un parcours pré-établi dans le logiciel (64 parcours possibles). Le début du parcours pourra se faire sur un créneau horaire, sur décision du gardien ou sur commande. En cas de non-respect du parcours ou du temps imparti, une alarme sera envoyée sur le superviseur et /ou sur un transmetteur téléphonique.
Tous les événements seront archivés et il sera possible de consulter l'historique des parcours (personne, état, alarme….).

16. Envoi d'alarmes SMTP (option)

Le système devra disposer d'une fonction d'envoi d'alarmes par messagerie SMTP. Une alarme détectée sur le système (intrusion, contrôle d'accès, alarmes techniques) pourra être envoyée par mail ou par SMS.

17. Exploitation Intégrée de la Vidéo (option)

Le système devra permettre de gérer le système de vidéo surveillance de manière conviviale, l'objectif étant que l'opérateur n'utilise qu'un seul poste d'exploitation pour effecteur la majorité des opérations d'exploitation courantes. En particulier, le système procurera les fonctionnalités suivantes :

- Sélection et visualisation d'images en provenance d'une ou plusieurs caméras spécifiques à partir d'un simple clic sur un synoptique d'exploitation. L'image sera transmise sur le réseau IP avec une qualité de niveau MPEG4. L'accès sera simplifié et uniforme pour tous les enregistreurs numériques utilisés sur le site.
- Asservissement d'une action « vidéo » à un événement ou à une télécommande d'un opérateur. L'évènement déclencheur pourra être le passage d'un badge interdit ou hors plage, la détection d'une tentative d'intrusion ou tout autre événement détectable par le système : alarme technique, alarme incendie, ronde etc. L'action vidéo résultante pourra être un enregistrement - ou un changement du mode d'enregistrement – d'images ou bien la commande de positionnement d'un dôme ou d'une tourelle.
- Commandes de positionnement asservi dites de « télémétrie » permettant le positionnement précis de la caméra par l'opérateur en cliquant directement sur la fenêtre de consultation du superviseur. Cette commande ou « clic image » sera intuitive et permettra à l'opérateur d'orienter la caméra suivant tous les degrés de liberté et de commander le zoom.
- Association d'un événement à une source vidéo.
- Consultation et accès direct aux images enregistrées au moment de la survenue d'un événement depuis la fonction « historique » du superviseur. Le système devra impérativement regrouper tous les événements dans un fichier d'historique unique afin de permettre une exploitation aisée et d'éviter les problèmes de synchronisation ou d'horodatage.
- Gestion des alarmes opérationnelles (détection d'activité par vidéo) et des alarmes de fonctionnement (perte de signaux vidéo ou autres pannes) en provenance des enregistreurs.

Ces fonctions seront disponibles grâce à la mise en réseau IP du superviseur et des postes d'exploitation d'une part et du ou des enregistreurs numériques du système vidéo d'autre part.

La communication entre supervision et enregistreurs numériques sera bi-directionnelle afin d'assurer la totalité des fonctions décrites ci-dessus. Tout autre mode d'interconnexion (câblage direct, liaison série

etc.) ne sera pas acceptable car il ne permettra pas de mettre en œuvre les fonctionnalités demandées dans de bonnes conditions d'exploitation (quantité et qualité des informations échangées, flexibilité, optimisation de la bande passante utilisée etc.)

18. Gestion des accès automobiles par lecture des plaques minéralogiques (option)

Le logiciel de supervision devra intégrer un outil de reconnaissance de plaques minéralogiques permettant l'accès automatique de véhicules. L'outil devra se comporter comme un lecteur de badge (niveau 0) et devra pouvoir être configuré, géré et utilisé par le superviseur commun. Pour des questions de simplicité d'utilisation et de maintenance, en aucun cas le système de reconnaissance de plaque ne doit nécessiter un fonctionnement en parallèle avec le reste de la gestion d'accès.

Ce système de lecture des plaques minéralogiques devra permettre :

- Le contrôle des informations liées à la plaque minéralogique (nom du propriétaire, département, accès limités…)
- La surveillance des accès (actions associées à une plaque minéralogique, levée de doute, interdiction ou forçage de l'accès).
- La gestion des différents temps de permission des véhicules.
- L'administration de parking (comptage des places libres, mise en place de voitures prioritaires…). Cette fonctionnalité devra pouvoir se retrouver visuellement dans les synoptiques du logiciel de supervision.
- La recherche de véhicule par l'intermédiaire d'un historique et la sortie d'informations en base de donnée.
- L'adaptation aux systèmes de vidéosurveillance déjà existants.

La gestion des plaques d'immatriculation et en particulier les droits d'accès seront gérés directement depuis l'UTL gérant les accès à contrôler. Donc tout système ne permettant pas d'assurer ce mode de fonctionnement ne sera pas retenu.

19. Contrôle vidéo des accès (option)

Le système devra permettre l'affichage du trombinoscope des porteurs de badges au moment ou une personne badge sur un accès surveillé. Ce trombinoscope sera associé à une levée de doute vidéo intégrée dans le même fenêtre. Cette fonctionnalité pourra être activée manuellement, ou automatiquement sur plage horaire. L'opérateur pourra également avoir une fonction «autorisation d'accès» pour ouvrir la porte ou «refus d'accès» pour ne pas ouvrir la porte.

20. Gestion des POI (option)

Le système devra permettre la gestion de POI (plan d'opération interne) afin de connaître en temps réel la liste des personnes présentent en zones sécurisées et la liste des personnes présentent en zones non sécurisées. Le système intègrera le début et la fin de POI. Le recensement se fera à partir des bornes mises place aux points de rassemblement du site.

Ce dispositif permettra en autre :

- Fourniture de la liste des personnes présentent sur le site en temps réel (gestion de zones).
- Suivi en temps réel de la migration du personnel des zones de travail vers les zones sécurisées après le déclenchement du POI
- Recherche de personnes pour connaître leur localisation
- Edition des noms des personnes avec trombinoscope

21. Le contrat de service AMCO (conseillé)

TIL Technologies propose et conseil un contrat de service AMCO à ceux clients partenaires agréés dans le cadre d'un contrat de maintenance avec le client final. Ce contrat a pour objectif d'assurer un service maximum à l'exploitant en associant les compétences de l'installateur agréé et le support technique de TIL. TIL propose ainsi les services suivants :

- Accès à la hot line téléphonique prioritaire et non limité
- Prise en main du site depuis la hot line (si le client permet la connexion)

- Fourniture de la dernière version logicielle du système (1 fois par an)
- Audit et inspection du serveur de contrôle d'accès (1 fois par an)

Ce contrat est proposé aux installateurs partenaires agrées par TIL Technologies dans le cadre de la maintenance des sites installés en TIL Technologies.

Normes et règlements applicables

Les propositions de l'Entreprise devront être conformes aux clauses de l'ensemble des lois, décrets, arrêtés, règlements, circulaires, normes et tous les textes nationaux ou locaux applicables aux ouvrages de la présente opération.

Les documents, ci-après, sont applicables dans leur dernière édition, cette liste n'est pas exhaustive.

- norme NFC15.100 : installations électriques à basse tension-règles,
- norme C18.510 : installations courants faibles et forts,
- norme NF C 63.410 : ensembles d'appareillages basse tension montés en usine,
- norme NF C91.101 : perturbations radioélectriques et systèmes d'antiparasitage, textes officiels concernant le matériel alimenté en réseau de première catégorie et dont le rayonnement direct est faible,
- norme NF C91.104. : perturbations radioélectriques et systèmes d'antiparasitage et textes officiels concernant les appareils servant aux réceptions individuelles ou collectives des émissions et radiodiffusion sonore ou visuelle,
- norme NF C92.130 : appareils électroniques et appareils associés à usage domestique ou à usage général analogue, reliés à un réseau de règles de sécurité.
- norme NF P 25-362 : Fermetures pour baies libres et portails, Spécifications techniques, Règles de sécurité,
- norme C32-321 : Conformité des câbles de distribution basse tension,
- norme C32-201 : Conformité du conducteur de protection,
- norme C32-310 : Conformité des câbles basse tension résistant au feu.