

Cahier des clauses techniques particulières



Lot Sûreté

- *Contrôle d'accès*
- *Intrusion*
- *Supervision graphique*

Sommaire

SOMMAIRE	2
I. PHILOSOPHIE GENERALE	4
II. ARCHITECTURE MATERIELLE	5
1. LE SYSTEME SERA CONSTITUE DE PLUSIEURS ENTITES DE DIFFERENTS NIVEAUX	5
2. LES UNITES DE TRAITEMENT LOCAL (UTL) EN CONTROLE D'ACCES ET INTRUSION	5
LES CAPACITES DE BASE	5
LES CAPACITES AVEC EXTENSION	6
LES CLAVIERS DEPORTES	7
LE RACCORDEMENT DES CAPTEURS INTRUSION	7
LE FONCTIONNEMENT EN MODE DEGRADE	7
SECURITE	7
COMMUNICATION & CRYPTAGE	8
MONTAGE & RACCORDEMENT	8
3. LES LECTEURS DE BADGES	9
4. LES SERRURES	9
III. ARCHITECTURE INFORMATIQUE & LOGICIELLE	10
1. LE POSTE SERVEUR	11
IV. DESCRIPTION DU LOGICIEL	12
1. GENERALITES	12
L'ACCES AU LOGICIEL	12
PLAGES HORAIRES	12
GROUPES DE LECTEURS	12
ATTRIBUTION DES DROITS D'ACCES DES USAGERS	12
LA FICHE UTILISATEUR	13
UTILISATION DE PLUSIEURS TECHNOLOGIES D'IDENTIFICATION	14
MULTI-SITE / MULTI-CLIENT / MULTI-ENTITE	14
GESTION DES ZONES ET ANTI-RETOUR	14
SUPERVISION DES ALARMES ET GESTION DES CATEGORIES DE VARIABLES	15
HISTORIQUES	16
GENERATEUR DE RAPPORTS	16
TRAITEMENT PAR LOT	16
JOURNAL DE BORD	17
ANIMATION DE SYNOPTIQUES – SUPERVISION GRAPHIQUE	17
V. LE CONTRAT DE SERVICE	18
VI. NORMES ET REGLEMENTS APPLICABLES	19

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, de G.T.B. et de supervision de la Vidéosurveillance**.

Le système devra se connecter nativement (sans passerelle) au serveur de contrôle d'accès, alarme intrusion et supervision MICRO-SESAME de TIL-TECHNOLOGIES présent à l'Université de Bordeaux.

Les objectifs principaux de la mise en place du dispositif de sûreté du site sont :

- De contrôler et filtrer le flux de personnes en gérant les accès (contrôle d'accès),
- De détecter la pénétration des personnes indésirables sur le site (détection intrusion),

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.

Une préférence sera donnée aux systèmes conçus et fabriqués en France.

- **Convivialité** : Le système permettra de superviser le contrôle d'accès, l'intrusion et la vidéosurveillance à partir d'un **poste unique** disposant d'une interface graphique conviviale.
- **Compatibilité et ouverture** : Le système sera compatible avec toutes les technologies d'identification (badges, biométrie, lecture de plaques minéralogiques, etc...). Il permettra également de gérer les alarmes techniques et de superviser des automates et autres équipements techniques en protocole MODBUS RTU ou OPC.
- **Flexibilité** : Les fonctions de sécurité avancée (anti-retour, contrôle renforcé, code sous contrainte, etc...) seront préprogrammées 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 de la détection 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, télémaintenance, etc...).
- **Intégration horizontale et verticale** : Des interfaces ou passerelles vers d'autres systèmes (incendie, G.T.B.) 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.

II. Architecture matérielle

1. 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.

Les UTL seront raccordées directement sur un réseau Ethernet. Sur ce réseau seront raccordés aussi le serveur, et les postes clients.

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

Si le réseau Ethernet 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...).

Un VLAN (réseau local virtuel) sûreté a été créé afin que le système soit sur un réseau indépendant, mais en restant administré par le client.

Les lecteurs de badges et autres accessoires (détecteurs intrusion, etc...) seront raccordés sur des modules déportés, eux-mêmes raccordés aux UTL par un bus de terrain RS485.

Pour limiter les contraintes de câblage, et **ce bus RS485 aura obligatoirement une topologie ouverte** : il pourra être installé en étoile, en bus ou en toile d'araignée.

2. Les Unités de Traitement Local (UTL) en Contrôle d'Accès et Intrusion

Les UTL proposées devront permettre la **gestion combinée du contrôle d'accès et de la détection intrusion**, permettant ainsi des automatismes et des asservissements optimisés entre les deux fonctions.

Elles assureront également des asservissements particuliers tels que la gestion de sas ou d'ouvrants et la gestion des alarmes techniques.

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

Les capacités de base

De base, les capacités minimum des UTL seront :

- 2 lecteurs de badges multi-technologies extensibles à 16,
- 7 entrées ToR,
- 4 entrées équilibrées,
- 2 sorties relais,
- 5 000 badges,
- 150 utilisateurs répartis en 64 profils et sous-profils,
- 32 jours fériés et 64 programmes horaires
- 6 000 instructions (microprogramme),
- 8 192 événements intrusion (historique),
- 284 points et 32 groupes de points intrusion,
- Gestion de 16 claviers déportés (exploitation de la détection intrusion).

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 : détecteurs volumétriques, 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...
- **La gestion combinée du Contrôle d'Accès et de l'Intrusion.**

Les capacités avec extension

Dans un but de flexibilité et d'évolutivité, l'UTL devra impérativement disposer d'extensions sur bus déportés. Ces extensions auront la forme de modules montables sur rail DIN pour intégration dans un coffret alimenté, ou disponibles sous la forme de boîtiers muraux téléalimentés.

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.

Grâce à ces extensions, l'UTL pourra ainsi gérer jusqu'à :

- 16 lecteurs de badges,
- 32 entrées analogiques,
- 256 entrées équilibrées et 480 entrées TOR,
- 256 sorties relais.

Les modules déportés disponibles seront :

- Module Transmetteur Digital sur RTC avec gestion de l'écoute et de l'interpellation (16 micros HP adressés individuellement), protocoles ID Contact et CESA 200, possibilité de secours,
- Module Déporté Intrusion permettant chacun de gérer 6 entrées équilibrées, 3 entrées ToR, et 2 sorties transistors,
- Module Transpondeur permettant la mise série des points d'intrusion sur bus (distance maximale du bus 300 mètres),
- 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 G.T.B. 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,

Les claviers déportés

Des claviers déportés avec afficheur seront mis en place afin de permettre la gestion des fonctions intrusion (directement sur le clavier) :

- Mise en / hors service du système de détection intrusion,
- Gestion des zones (groupes de points),
- Consultation des alarmes en temps réel,
- Arrêt sirènes, éjection des points,
- Consultation de l'historique (derniers événements),
- Déclaration / modification des utilisateurs,
- Possibilité d'intégrer un lecteur de badges sans contact pour faciliter l'identification de l'utilisateur.

Caractéristiques communes des claviers 17 touches	
Alimentation : 12 VDC Température d'utilisation : de - 10°C à + 50°C Connectique : bornier débrochable à vis Consommation (hors lecteur) : <ul style="list-style-type: none"> ■ Clavier actif : 140 mA ■ Clavier en veille : 50 mA Fixation : en saillie par 4 vis Auto-protégé à l'ouverture	Distance max. entre le clavier et l'UTL : 600 m 16 touches sensibles 2 lignes de 20 caractères 3 voyants programmables

Ces claviers seront raccordés directement sur le bus RS485 de l'UTL.

Le raccordement des capteurs intrusion

Dans une logique de réduction des coûts de câblage et d'économie d'énergie, les capteurs (contacts de porte, détecteurs volumétriques...) seront raccordés à un ou plusieurs modules d'acquisition, **via des bus RS485 sécurisés et auto-alimentés**.

Chaque module d'acquisition comportera 2 bus RS485, permettant chacun le raccordement de 32 capteurs.

Le bus pourra être bouclé afin de limiter le risque de perte de connexion en cas de rupture physique. Le module d'acquisition devra être en mesure de détecter la coupure et le court-circuit du bus.

Pour le raccordement des capteurs, le constructeur mettra à disposition des transpondeurs, facilement intégrables dans les contacts et radars en lieu et place des résistances d'équilibrage. Chaque transpondeur aura un numéro d'identification unique, la transmission entre le transpondeur et le module d'acquisition sera cryptée. Toute tentative de sabotage sera immédiatement détectée.

Le fonctionnement en mode dégradé

Les UTL posséderont et pourront traiter toutes les informations nécessaires à un fonctionnement autonome.

Les autorisations de passage, anti-retour, gestion de plages horaires, stockage des informations et événements, broadcast et partage d'informations seront assurés **même en cas de déconnexion du réseau Ethernet**. Lors de la reconnexion du réseau, les informations seront restituées automatiquement au PC serveur.

Sécurité

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

Communication & Cryptage

Les UTL seront natives IP c'est-à-dire raccordées directement sur le réseau informatique Ethernet (sans convertisseur intermédiaire). 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 devront dialoguer avec le PC serveur **mais aussi entre elles**, permettant ainsi d'assurer les interactions, les asservissements ou les fonctions réparties sur plusieurs UTL. Les données échangées seront sécurisées par un cryptage de données AES 128 bits.

Les UTL devront pouvoir fonctionner dans un maximum de configurations réseau. Pour cela, elles seront :

- Auto-négociables (configuration automatique en fonction de la vitesse du réseau, de 10 à 100 Mb/s),
- et Auto-MDI (configuration automatique en fonction du type de câble réseau : droit ou croisé).

Montage & Raccordement

Les UTL disposeront de deux bus RS485 d'une longueur de 600 mètres chacun, acceptant le câblage en série et / ou en étoile.

Les UTL devront pouvoir se fixer sur rail DIN à intégrer dans une armoire spécifique ou dans un coffret à alimenter en 220 V. Ces coffrets techniques seront répartis dans les locaux techniques courants faibles implantés dans le bâtiment.

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 V monophasé. Les coffrets seront équipés d'une alimentation continue et régulée 12 V 6A minimum secouru par batterie.

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.

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

Caractéristiques UTL IP	
Alimentation : 12 VDC / 100 mA Horloge calendrier : secourue par pile lithium débrochable, 32 jours fériés, 64 programmes horaires Nombre de badges : 5 000 Microprogramme : 6 000 instructions environ Rétrospective intrusion : 8 192 évènements Communication réseau : carte réseau Ethernet 100 baseT, connecteur RJ45, 2 voyants d'état Autres connexions : borniers débrochables à vis Voyants : sur l'alimentation sur chaque entrée / sortie Dimensions : H 110 x L 125 x P 50 mm Humidité : 0 – 95% sans condensation Température d'utilisation : 0°C à + 40°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 déportés (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 : disposent de deux bus secondaires RS485 d'une longueur de 600 m maximum

3. Les lecteurs de badges

Les lecteurs de badges seront multi technologies et universel dans la gamme 13,56 MHz. Ils permettront de lire plusieurs technologies : MIFARE, DESFire, ICAO, etc...selon la norme ISO 14443-A part 3.

Le lecteur devra avoir une consommation très faible (0,25 W).

L'entreprise devra proposer des lecteurs longs à installer sur les montants de portes, et des lecteurs anti-vandales pour les accès extérieurs.

Les lecteurs de badges seront de type proximité passifs 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 obligatoirement supervisée dans le système d'exploitation.

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

Le lecteur choisi devant être universel dans la gamme 13,56 MHz, il devra être reprogrammable sans devoir être démonté et sans connexion physique (reprogrammation radio par badge ou par programmeur sans contact).

Caractéristiques lecteurs intérieurs	
Alimentation : 12 VDC (9 à 15 VDC) Consommation moyenne : 0,25 W Fréquence d'émission : 13,56 MHz Distance max. entre le module et le lecteur : 600 m Interface de communication : RS485 crypté, signe de vie Connectique : bornier 4 points inclus Matériaux : ABS Dimensions : H 86 x L 86 x P 16 mm Fixation : 2 vis, sur boîte d'encastrement 80 mm ou en applique	Distance de lecture : de 3 à 5 cm Signalisation : <ul style="list-style-type: none"> ▪ Eclairage d'ambiance blanc ▪ LEDs rouge / verte pilotables ▪ Buzzer intégré Température de fonctionnement : de + 5°C à + 40°C Poids : 0,10 kg

Caractéristiques lecteurs anti-vandale	
Alimentation : 12 VDC (9 à 15 VDC) Consommation moyenne : 0,25 W Fréquence d'émission : 13,56 MHz Distance max. entre le module et le lecteur : 600 m Interface de communication : RS485 crypté, signe de vie Connectique : bornier 4 points inclus Matériaux : plastique renforcé Dimensions : H 125 x L 43 x P 18 mm Fixation : 2 vis, en applique	Distance de lecture : jusqu'à 6 cm Signalisation : <ul style="list-style-type: none"> ▪ LEDs rouge / verte pilotables ▪ Buzzer intégré Température de fonctionnement : de - 25°C à + 40°C Poids : 0,18 kg Etanchéité : IP65 Résistance aux chocs : IK8 (résistance aux projectiles et à la flamme d'un briquet)

--	--

4. Les serrures

Les portes extérieures devront être équipées de bandeau de ventouses conforme avec la hauteur de la porte à savoir minimum 2500mm. Le Ral de couleur des bandeaux devra être au choix du client.

Les portes intérieures devront être équipées, si les PV coupe-feu le permettent, de bandeau de ventouse 400 à 600mm centré au milieu de la porte.

Cas échéant, la validation devra être effectuée par la direction du patrimoine de l'université dans un souci de maîtrise des coûts de maintenance.

Pour la conformité avec les normes appliquées à la réception de public aux universités les portes seront associées avec bouton poussoir de sortie et bris de glace vert.

L'asservissement de chaque issue de secours à la détection incendie sera **obligatoire**.

En effet l'université mettra à disposition la liste des entreprises SSI habilitées sur le(s) site(s) concerné(s), l'entreprise devra ordonner et suivre ces travaux d'asservissements afin que la conformité incendie du bâtiment soit décernée.

III. Architecture Informatique & Logicielle

1. Le poste serveur

Les bâtiments Talence Pessac seront à raccorder obligatoirement sur le serveur université existant. En effet le PC sécurité université possède une supervision unique et ne prendra pas en compte de nouvelles architectures.

Au cas où le système ne serait pas raccordé sur le serveur existant et donc au PC sécurité, les universités se refuse d'accepter de nouveau site après coup.

Dans le cas d'un site distant ou l'installation d'un nouveau serveur indépendant est obligatoire, le système proposé aura une architecture logicielle Client / Serveur. Ce poste serveur 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 4 096 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 lourd ou bien dynamique et léger en connexion TSE.

2. Les postes clients

Le ou les postes clients lourd 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 (3 GHz),
- Carte Ethernet 100 Mb/s,
- 4 Go de RAM,
- Disque dur 100 Go minimum,
- 1 lecteur DVD (pour l'installation du logiciel),
- Ecran plat TFT 21", résolution 1920 x 1024 au minimum,
- Clavier, souris, Windows 7 Professional,
- 1 port série au minimum,
- 2 ports USB,
- Licence client Microsoft SQL.

IV. Description du logiciel

1. Généralités

En cas de raccordement sur serveur existant des extensions de licences du logiciel MICRO-SESAME de TIL TECHNOLOGIES devront être prévues.

Il permettra le paramétrage et la supervision du contrôle d'accès, de la détection intrusion, de la GTB, des enregistreurs vidéo, et des différents systèmes tiers présents sur le site via des protocoles ouverts comme MODBUS RTU ou OPC.

Il fonctionnera sous un environnement Windows et sera modulaire, convivial et évolutif.

Il communiquera avec les UTL par liaison IP, ce qui permettra notamment la gestion d'UTL déportées (via XDSL, GSM...).

Afin d'assurer l'ouverture et l'évolutivité du système, il sera multi base de données : il sera compatible au minimum avec des bases de type SQL Server 2008 et Oracle 11.2g.

Les systèmes fonctionnant avec des bases de données propriétaires seront exclus.

L'accès au logiciel

L'accès des opérateurs sur le logiciel sera contrôlé par l'intermédiaire de l'annuaire LDAP. Les droits de chacun sont personnalisables par définition des droits : accès aux historiques, au paramétrage, modifications de badges, à la visualisation, etc...

Il sera possible de créer des profils opérateurs prédéfinis, facilitant la gestion des droits d'un grand nombre d'opérateurs.

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.

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 G.T.B. ou plages distinctes,
- Prise en compte des jours fériés,
- Définition du type de plage (quotidienne, hebdomadaire),
- Plage active ou inactive.

Groupes de lecteurs

Le système permettra de créer jusqu'à 1 024 groupes de lecteurs. Un groupe de lecteurs est un ensemble regroupant de un à 1 024 lecteurs Il permet de créer des zones géographiques particulières (voir ci-dessous Gestion des zones et anti-retour).

Profil d'accès

Le système permettra de créer jusqu'à 1 024 profil d'accès. Un profil d'accès est l'association d'un lecteur et/ou groupe de lecteurs à une plage horaire. Il permet de simplifier la gestion des droits d'accès des usagers.

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.

Attribution des droits d'accès des usagers

Gestion par logiciel sésame

L'université a développé une interface web appelée Sésame. Elle répertorie dans une base de données tous les badges Aquipass possédés par les étudiants et employés des universités.

Des référents contrôle d'accès sont désignés par l'université.

En effet ces référents affectent aux porteurs de badges des **profils d'accès** préalablement créés pour chaque site depuis le portail Web.

A chaque badge, il sera possible d'associer un (ou plusieurs) profil(s) 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.

Sur le serveur existant Micro-sésame une passerelle d'importation a été créée afin de récupérer les informations saisies par les habilitateurs, ainsi aucune action n'est obligatoire par les utilisateurs directement sur le logiciel.

Evidemment, dans le cas d'un rajout de serveur, il devra être rendu compatible avec cette passerelle.

La fiche utilisateur

Elle permettra d'identifier chaque usager (porteur de badge, etc...) et de gérer en second lieu 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'opérateur 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 utilisée,
- 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 (65 536 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,
- Le système permettra la gestion de 4 identifiants par utilisateur, permettant ainsi de mixer plusieurs technologies sur le site. Par exemple, il sera possible d'attribuer une plaque minéralogique pour les accès véhicules à une personne sur la même fiche badge.
- 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 badges 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 doit être 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.

Utilisation de plusieurs technologies d'identification

Le système permettra la gestion de 4 identifiants distincts par utilisateur, sur une même fiche badge.

Ceci permettra d'utiliser simultanément plusieurs technologies de contrôle d'accès sur un même site, sans créer de doublons.

Par exemple, il sera possible d'attribuer à une même fiche badge un identifiant de badge MIFARE, un numéro de plaque minéralogique et une empreinte biométrique.

Multi-site / Multi-client / Multi-entité

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.

Gestionnaire principal et opérateur gestionnaire

Le système devra nécessairement comporter un gestionnaire principal. Ce dernier sera le seul qui aura accès à la totalité de la base de données 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 attribuer les droits de chaque opérateur gestionnaire.

L'opérateur gestionnaire, quant à lui, devra pouvoir gérer uniquement les lecteurs de son site. Dans un souci d'autonomie et de confidentialité, l'opérateur gestionnaire ne verra ni les lecteurs, ni les badges, ni les historiques de passages des autres sites. L'opérateur 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.

Zones 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 données unique et commune (détenue intégralement par le seul gestionnaire principal).

Certains lecteurs pourront en effet être gérés en communs par plusieurs opérateurs 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.

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'utilisateur n'a pas badgé en pénétrant dans cette zone.

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 opérateur...), 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 opérateur**
 - l'opération effectuée,
 - le nom de l'opérateur,
 - le poste concerné,
- **pour les autres événements**
 - le type d'événement,
 - le nom de l'organe du système concerné,
 - le poste concerné.

Le fil de l'eau affichera les événements par couleur, selon leur nature.

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.

Historiques

La capacité de stockage du système ne sera pas limitée (plus 1 million d'événements).

Les critères d'extraction pourront être :

- Des périodes de recherches (dates et jours),
- Événements badges : autorisés, interdits, liste noire, anti-retour avec le choix du badge, du profil, du lecteur, du groupe de lecteurs,
- Événements voies : alarmes, logiques ou numériques avec sélection de la voie,
- Événements modules : connexion/déconnexion, reset avec sélection du module et de la ligne,
- Événements de lignes : début/fin de scrutation et téléchargement,
- Événements des opérateurs : acquittement, télécommandes, forçages de voies, connexions/déconnexions avec le choix de l'opérateur.

L'interface facilitera les recherches en permettant la différenciation par fonction de sécurité (onglets contrôle d'accès, GTB, actions opérateurs, événements système...). Des recherches types pourront être enregistrées.

Les historiques peuvent être exportés pour une exploitation ultérieure. Les requêtes extraites des historiques peuvent également être imprimées.

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.

Générateur de rapports

Le superviseur devra intégrer un générateur de rapports graphiques basé sur la solution Crystal Reports.

Un certain nombre de rapports prédéfinis seront fournis (état de l'architecture système, passages de badges par lecteur, etc...). Ces rapports pourront être édités au format PDF (avec graphiques) ou exportés au format CSV.

Des rapports personnalisés pourront être créés sous réserve de la détention d'une licence Crystal Reports Developer. Le concepteur du système de sûreté devra également être en mesure de proposer la création de rapports personnalisés correspondant aux besoins de l'exploitant.

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.

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.

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 plan dynamique permettant une exploitation conviviale avec icônes, animations, télécommandes, changement de couleurs, etc...

La charte graphique étant existante, le référent contrôle d'accès de la DSI doit valider que chaque variable soit conforme à la demande.

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 piloter l'ensemble de son installation.

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 P.C. 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).

L'exploitant pourra également piloter les différentes sorties du système et matériels interfacés par de simples clics sur le synoptique : pilotage d'un éclairage, affichage d'une caméra vidéo, recherche d'enregistrement vidéo, réponse à un appel interphone, etc...

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).

V. Le contrat de service

Le constructeur du système proposera un contrat de service à ses clients partenaires agréés dans le cadre d'un contrat de maintenance avec le client final. Ce contrat aura pour objectif d'assurer un service maximum à l'exploitant en associant les compétences de l'installateur agréé et le support technique du constructeur. Ce contrat inclura ainsi les services suivants :

- Accès à un support téléphonique prioritaire et non limité,
- Prise en main du site depuis le support téléphonique (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).

VI. 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 NF C15.100** : installations électriques à basse tension,
- **norme C18.510** : installations courants faibles et forts,
- **norme NF C63.410** : 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 P25.362** : 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.