

CCTP PROJET MIGRATION VIDEOPROTECTION EN GENETEC SECURITY CENTER

Musée des Arts Décoratifs Paris
107 rue de Rivoli - 75001 Paris



Maitre d'Ouvrage	AC2S CONSULTING Ave DANTZIG 77340 Pontault-Combault	Tel : Email :	06.11.15.13.95 ndaine@ac2s-consulting.com
Assistant Maitre d'Ouvrage	AC2S CONSULTING Ave DANTZIG 77340 Pontault-Combault	Tel : Email :	06.07.37.04.03 Gino.anoumantou@madparis.fr

SOMMAIRE

1.1	OBJET DU MARCHÉ	3
1.2	CONFORMITÉ DES OFFRES	3
1.2.1	Conformité technique.....	3
1.2.2	Capacités de candidature.....	4
1.2.3	Conformité financière de l'offre	4
1.2.4	Assurances	4
1.2.5	Offres inacceptables, irrégulières ou inappropriées.....	5
1.3	DOCUMENTS A FOURNIR	5
1.3.1	Avec l'offre	5
1.3.2	Avec les études d'exécution.....	5
1.3.3	A la réception des travaux.....	6
1.4	NORMES ET REGLEMENTS DE REFERENCE	6
1.5	PRINCIPE DE BASE	6
1.5.1	Pérennité et évolutivité	6
1.6	ARCHITECTURE DE LA PLATEFORME UNIFIEE DE SURETE.....	7
1.6.1	Ouverture	8
1.6.2	Les Interfaces	8
1.6.3	Gestionnaire de Configuration et de Traitement (GCT).....	8
1.6.4	Gestion de la Sécurité Centralisée (GSC)	8
1.6.5	Gestion Mobile (GM).....	9
1.7	FONCTIONNALITES D'ADMINISTRATION	9
1.7.1	Les entités	9
1.7.2	Les serveurs et les rôles	9
1.7.3	La fédération de sites	9
1.7.4	La cartographie	9
1.7.5	Outils de maintenance et diagnostique	10
1.7.6	Situations de crise	10
1.8	FONCTIONNALITES D'EXPLOITATION	10
1.8.1	Les tâches de surveillance	10
1.8.2	Les tâches de rapport et d'investigation	11
1.8.3	Les tableaux de bords.....	12
2	SYSTEME DE CONTROLE D'ACCES SYNERGIS	13
2.1	PRINCIPE DE BASE	13
2.1.1	Pérennité et évolutivité	13
2.1.2	Le rôle du Gestionnaire d'Accès	13
2.1.3	Maintien en condition opérationnelle terrain	13
2.1.4	Automatismes terrain	14
2.2	FONCTIONNALITES	14
2.2.1	Les titulaires de carte	14
2.2.2	Définition des règles d'accès	14
2.2.3	Définition des horaires	15
2.2.4	Utilisations des accès	15
2.2.5	Gestion d'impression des badges	15
2.2.6	Gestion d'enrôlement et d'encodage de badge	16
2.2.7	Antiretour (Anti Pass Back)	16
2.3	FONCTIONNALITES COMPLEMENTAIRES	16
2.3.1	Gestion des communications	16
2.3.2	Gestion d'ascenseur	16
2.3.3	Gestion des visiteurs.....	17
2.3.4	Gestion avancée des visiteurs	17
2.3.5	Gestion de comptage et occupation	17
2.3.6	Gestion d'accès sans fil online.....	17
2.3.7	Gestion d'accès autonome Offline	18
2.4	ARCHITECTURE DE LA SOLUTION DE CONTROLE D'ACCES.....	18
2.5	DESCRIPTIONS TECHNIQUES.....	19

2.5.1	Les contrôleurs	19
2.5.2	L'environnement de porte	20
2.5.3	Les lecteurs.....	20
2.5.4	Les identifiants	21
2.6	FORMATIONS.....	22
2.7	DEPLOIEMENT ET MISE EN SERVICE.....	22
2.8	FONCTIONNALITES COMPLEMENTAIRES EN OPTION	22
2.9	FORMATIONS.....	22
2.10	DEPLOIEMENT ET MISE EN SERVICE.....	22
3	SYSTEME DE VIDÉOPROTECTION OMNICAST	23
3.1	PRINCIPE DE BASE	23
3.1.1	Pérennité et évolutivité	23
3.1.2	Le rôle de l'archivageur.....	23
3.1.3	Haute disponibilité et maintien en condition opérationnelle	24
3.2	FONCTIONNALITES	24
3.2.1	Communication et réseau	24
3.2.2	Enregistrement et détection d'activité.....	24
3.2.3	Rapport d'archive vidéo	25
3.2.4	Recherche en direct.....	25
3.2.5	Recherche rapide.....	25
3.2.6	Filature visuelle	25
3.2.7	Fonction de mur d'images.....	25
3.2.8	Exports vidéo et marqueurs	26
3.2.9	Protection contre le piratage des images	26
3.3	ARCHITECTURE DE LA SOLUTION DE VIDEOPROTECTION	27
3.4	DESCRIPTIONS TECHNIQUES.....	28
3.4.1	Gestion et centralisation	28
3.4.2	Enregistrement vidéo principal	28
3.4.3	L'infrastructure réseau	29
3.4.4	Les terminaux.....	29
3.5	FORMATIONS.....	30
3.6	DEPLOIEMENT ET MISE EN SERVICE.....	30

1.1 Objet du marché

Le présent marché a pour objet la reprise de l'intégralité des caméras présente sur le site du Musée des Arts Décoratif dans un objectif d'une migration totale sur la plateforme unifiée de sûreté sur IP **Genetec Security Center** existante en exploitation actuellement, le système contrôle d'accès **Synergis** en exploitation, vidéophonie et de localisation opérationnelle.

La première partie des caméras est intégrée sur Security center, la deuxième partie est actuellement sur un logiciel tiers (VPRO) de Videoconsult dont il faudra assurer la migration totale vers Genetec.

La troisième partie concerne uniquement la reprise du contrôle d'accès actuel sur Genetec et en assurer la parfaite assimilation dans le cadre de la plateforme unifiée de Security Center.

Etendue et limite des prestations

Le contrat est conclu sur la base d'un prix global et forfaitaire, et comprend l'ensemble des prestations et fournitures nécessaires au parfait achèvement des ouvrages mentionnés dans le présent CCTP. Le prestataire ne pourra invoquer l'absence de description d'un équipement, d'un matériel ou de travaux annexes, pour se prévaloir de prestations complémentaires. Il est entendu que les prescriptions techniques représentent un minimum des performances et fonctionnalités attendues, mais ne constituent en aucun cas une description exhaustive des ouvrages à réaliser. En complément du cahier des charges, la visite du site permettra l'établissement d'une offre prenant en compte l'intégralité des prestations et fournitures nécessaires au bon fonctionnement des systèmes.

Le marché prévoit l'ensemble des prestations suivantes :

- Réalisation des études de conception ayant pour objet d'assurer la cohérence de la solution proposée avec les besoins de la maîtrise d'ouvrage (Hardware informatique, environnement réseau, cohérence des solutions proposées, interopérabilité avec des systèmes tiers, ...),
- Réalisation des démarches administratives nécessitant des autorisations légales,
- Réalisation des études d'exécution des ouvrages (méthodologie, planning et détails des travaux de pose, fourniture des plans d'exécution, échantillons des matériels proposés, ...)
- Réalisation des ouvrages (travaux de pose, câblage, raccordement, paramétrage, configuration, mise en service, ...),
- Tests et essais de fonctionnement nécessaires à la recette des installations,
- Fourniture des livrables : Plans et schémas, mémoire technique, analyse fonctionnelle, et autres, associés à l'élaboration complète du Dossier D'ouvrage Exécuté,
- Formation des exploitants et utilisateurs de la solution proposée,
- La proposition d'un contrat de maintenance annuel comprenant les prestations de maintenance du fabricant et/ou éditeur de la solution, y compris la mise à disposition des mises à jour logicielles.

1.2 Conformité des offres

1.2.1 Conformité technique

L'offre des candidats est établie en conformités avec les recommandations techniques des éditeurs et fabricants, et selon les règles de l'art définie dans les normes et réglementations applicables.

Devoir de conseil

Les candidats se doivent de prévenir le Maître d'ouvrage de toute erreur éventuelle qu'ils ont pu relever sur les plans et/ou pièces écrites qui leurs ont été fournis. Pendant toute la durée de son engagement et jusqu'à ce que soit prononcée la réception définitive de l'ouvrage, le titulaire du marché reste soumis au même devoir de conseil.

Respect des prescriptions techniques

Sous peine d'être rejetée, l'offre formulée par le candidat doit obligatoirement respecter l'intégralité des prescriptions techniques et fonctionnelles du présent CCTP, définies selon une étude de besoins de la maîtrise d'ouvrage.

Préalablement à la validation de la solution proposée, le prestataire doit démontrer la pertinence de celle-ci et remettra des échantillons du matériel associé prévu en veillant systématiquement à :

- Spécifier l'éditeur et/ou fabricant des solutions proposées,
- Indiquer la présence d'un support technique en France,
- Préciser les marques, les noms et références précises du matériel,
- Fournir une documentation technique complète.

Il pourra être demandé une démonstration de la solution en collaboration avec l'éditeur et/ou le fabricant afin de confirmer la conformité aux besoins du client final.

Il est rappelé que l'appréciation d'équivalence des matériels présentés par le prestataire, avec les fonctions et performances décrites au présent CCTP, appartient à la maîtrise d'œuvre. En cas de désaccord, le prestataire doit procéder à toutes les modifications demandées par le maître d'œuvre ou le maître d'ouvrage (conception et travaux) jusqu'à un accord complet.

Aucune variante ne sera acceptée.

1.2.2 Capacités de candidature

En garantie du respect des recommandations techniques des éditeurs et fabricants, il est demandé aux candidats de justifier de certifications sur la solution **Genetec** proposée. En cas de nécessité, il pourra être demandé aux éditeurs et fabricants de valider la conception technique. Le candidat s'engage à disposer des capacités de réalisation des prestations suivantes :

- Etudes de conception,
- Etudes d'exécution, calcul de bande passante, Besoin en stockage, budget POE, ... etc.
- Installation, pose et raccordement
- Paramétrage, configuration et mise en service,
- Tests et essais de fonctionnement,
- Formation des exploitants et utilisateurs,
- Garantie et Maintenance du système.

1.2.3 Conformité financière de l'offre

Il est rappelé que le présent dossier est un marché global et forfaitaire et que l'entreprise ne pourra prétendre à une quelconque réclamation financière complémentaire pour quelque raison que ce soit autre que pour des modifications issues de la volonté du maître d'ouvrage lui-même.

1.2.4 Assurances

L'entrepreneur doit être titulaire :

- D'une assurance Responsabilité Civile Entreprise garantissant les conséquences financières encourues en raison de dommages causés aux tiers du fait de son activité.
- D'un contrat d'assurance Décennale ayant pour objet de garantir les ouvrages réalisés suivant des procédés ou avec des matériaux ou produits de technique courante.
- Il est rappelé à l'ensemble des candidats qu'il s'agit d'un établissement sensible impliquant un travail soigné et méticuleux nécessitant des précautions d'usages nécessaires à la réalisation des travaux.

1.2.5 Offres inacceptables, irrégulières ou inappropriées

Il est rappelé aux candidats que les offres systématiquement écartées sont :

- Celles dont les conditions prévues pour leur exécution méconnaissent la législation en vigueur, ou hors budget,
- Celles qui tout en apportant une réponse au besoin du maître d'ouvrage, sont incomplètes ou ne respectent pas les exigences formulées dans les documents de la consultation.
- Celles qui apportent une réponse sans rapport avec le besoin du maître d'ouvrage et peuvent en conséquence être assimilée à une absence d'offre.

Visite de site :

Sous peine d'être rejetée, l'offre formulée par le candidat doit obligatoirement justifier de la participation à une visite de site. L'attestation de visite sera jointe à l'offre du candidat.

1.3 Documents à fournir

Afin de pouvoir juger correctement la pertinence et la qualité des candidatures, l'entrepreneur doit fournir les documents suivants :

1.3.1 Avec l'offre

- Un devis avec descriptif technique détaillé en harmonie avec les descriptions de ce CCTP,
- Une proposition estimative de contrat de maintenance évolutive, y compris le support,
- Les fiches techniques du logiciel et du matériel proposé,
- La description de la méthodologie de réalisation des ouvrages et les dispositions prises pour gérer la qualité du projet,
- Tous les justificatifs permettant de juger de la capacité de l'entreprise et de ses personnels à réaliser l'ouvrage,
- Un planning estimatif reprenant les études de conception, les études d'exécution, et le déploiement des ouvrages.

Nota :

Les documents manquants peuvent être éliminatoires.

1.3.2 Avec les études d'exécution

- Une analyse fonctionnelle de la plateforme unifiée proposée,
- Les manuels utilisateurs pour l'exploitation et l'administration,
- Les plans détaillés de l'architecture générale du système,
- Les fiches techniques et schémas de câblage,
- Les plans d'exécution avec implantation et repérage de l'ensemble des ouvrages,
- La méthodologie détaillée de réalisation des ouvrages en site occupé
- Le planning détaillé de la réalisation des ouvrages

1.3.3 A la réception des travaux

- Le décompte général et définitif,
- Les DOE, constitués de la synthèse des tous les éléments comprenant :
 - Mot de passe admin de tous les composants de l'installation (Caméras, switch, serveurs, pc d'exploitation, ...etc.)
- Les consignes générales et intervention d'entretien sur l'ouvrage à effectuer,
- La proposition de maintenance annuelle en association avec le fabricant et/ou éditeur de la solution fournie.

1.4 Normes et règlements de référence

Normes et règlements de référence :

- Référentiel APSAD D83 Contrôle d'accès 09/2012
- Référentiel APSAD R82 Vidéosurveillance 02/2016
- La loi n°95-73 du 21 janvier 1995 relative à la sécurité,
- Le décret n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance,
- La circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n°95-73
- La loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme,
- Le décret n°2006-929 du 28 juillet 2006 relatif à la vidéosurveillance modifiant le décret n°96-926,
- L'arrêté du 03 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance,
- ANSSI – Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - v2.0 du 04/03/2020

L'entreprise mandataire a connaissance de ces documents afin d'appliquer le respect des règles de l'art et d'avoir la connaissance technique en la matière.

Il est souligné que certaines caractéristiques sont considérées comme essentielles à la conformité de la solution technique proposée, et il appartient à la maîtrise d'œuvre le jugement des équivalences pour la maîtrise d'ouvrage.

UNIFICATION DES SYSTEMES DE SURETE

1.5 Principe de base

La simplification de l'utilisation globale des systèmes de sûreté est vitale pour que les exploitants s'approprient la solution comme un outil indispensable à la sécurisation du site. Pour améliorer la pertinence de la globalité de la solution, il est prévu une plateforme unifiée de sûreté. A chaque exploitant ou à chaque besoin d'utilisation, la même interface proposée doit être adaptée.

1.5.1 Pérennité et évolutivité

Le choix de la solution par la maîtrise d'ouvrage est un investissement durable. La pérennité du système et l'évolutivité de la solution sont des points importants. La plateforme unifiée de sûreté **Genetec Security Center** est une solution logicielle en environnement Microsoft Windows. L'infrastructure informatique et réseau IP, de type serveur-client, doit se baser sur du matériel standard non-propriétaire du marché, conforme aux recommandations de l'éditeur.

La solution est de type éditeur, c'est-à-dire qu'une entité logicielle gère le matériel terrain, de divers fabricants, intégrant nativement un maximum de terminaux répertoriés sur une liste de matériel compatible. En effet, la maîtrise d'ouvrage se laisse le choix de choisir différents matériels terrain, selon les besoins techniques et/ou l'évolution du marché.

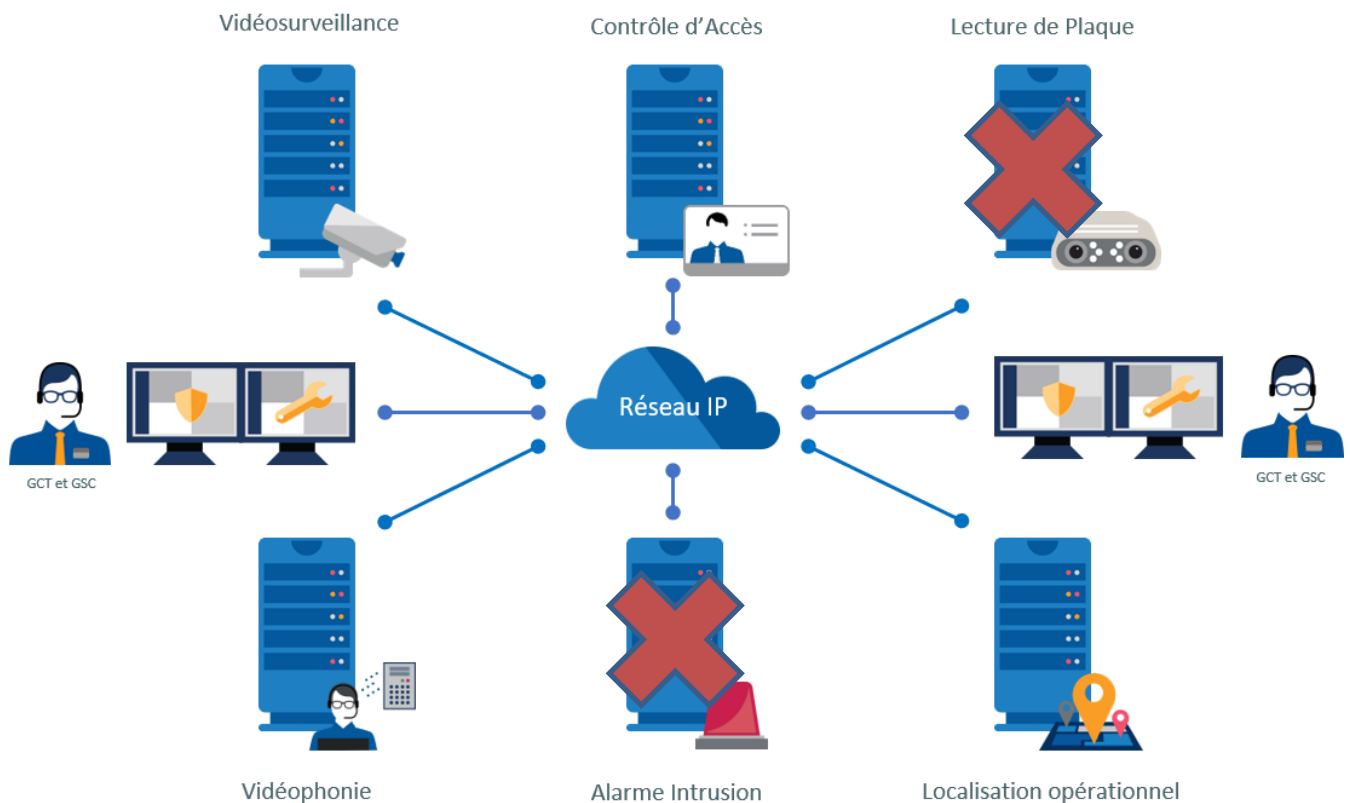
L'entreprise mandataire doit justifier de son niveau de formation et de certification sur la solution déployée. Le cas échéant, il peut être demandé les certifications du personnel qui intervient sur le système.

L'éditeur **Genetec** de la solution choisie dispose d'une gamme de versions évolutives de logiciel, permettant une souplesse de l'installation et des évolutions futurs. Dans ce cadre, mais également pour garder le système toujours à jour car c'est un gage d'une protection optimale contre les cyberattaques, l'entreprise doit prévoir avec son offre, 3 ans de services auprès de l'éditeur, comprenant à minima le support 24/24 et les mises à jour du logiciel y compris celle des composants dans un objectif d'une parfaite garantie de la sécurité des installations.

1.6 Architecture de la plateforme unifiée de sûreté

La plateforme unifiée sur IP, étant dédiée à la sûreté, ne nécessite pas de couche logicielle supplémentaire de type Hypervision, pour simplifier l'architecture globale. Ainsi, les mises à jour logicielles ne concernent qu'un seul logiciel, évitant ainsi toutes les problématiques de compatibilités de version et d'intégration, pour disposer d'une solution toujours dans la dernière version recommandée par l'éditeur. Cette plateforme unifiée doit être capable de gérer les métiers de :

- Contrôle d'Accès **Synergis**,
- Détection Intrusion, non prévue au marché,
- Vidéophonie, non prévu au marché,
- Service de localisation opérationnel sur plan Manager de la plateforme,
- Vidéoprotection **Omnicast**.



L'administration et l'exploitations de tous ces métiers unifiés est faite par la plateforme unifiée. L'architecture basée sur IP est établie sur le principe de l'intelligence répartie pour chaque rôle. Il est ainsi possible de répartir les ressources sur plusieurs machines informatiques ou en environnement virtualisé pour une performance optimale sur mesure, et évolutive. De plus, il est possible de secourir les rôles les plus critiques de la solution, notamment la gestion de la base de données, afin de garantir le fonctionnement optimisé dans les meilleures conditions d'exploitation.

1.6.1 Ouverture

La maitrise d'ouvrage précisera les informations et/ou synthèses qu'elle souhaite récupérer sur la plateforme unifiée. Pour cela, l'application doit être ouverte et communicante avec des bases de données ou d'autres systèmes tiers : GTB/GTC, SSI, ... Il doit être disponible par simple ajout de licence, différents connecteurs logiciels standards paramétrables : ModBusTCP, OPC, BACnet, API, ... L'interfaçage avec un hyperviseur doit être possible.

Concernant les systèmes tiers, qui peuvent apporter des fonctionnalités spécifiques supplémentaires, la solution retenue doit avoir une liste de partenaires technologiques intégrés, suffisamment étoffé pour que la maitrise d'ouvrage trouve réponse à ses besoins actuels et futurs.

1.6.2 Les Interfaces

Pour ce projet, il est distingué trois types d'utilisations :

- L'administration : via le Gestionnaire de Configuration et de Traitement (GCT)
- L'exploitation locale : via le client de Gestion de la Sécurité Centralisée (GSC)
- La Gestion Mobile : via un client web ou une application mobile. (GM)

1.6.3 Gestionnaire de Configuration et de Traitement (GCT)

Dans le cadre de l'administration, une application avec une interface dédiée au paramétrage peut être utilisée pour gérer tous les systèmes unifiés. Celle-ci permet aux administrateurs du système de gérer le paramétrage et la configuration de la plateforme unifiée, ainsi que les différents privilèges associés aux différents exploitants ou administrateurs. Cette interface se doit être ergonomiquement basée sur le même principe que le GSC afin de permettre aux administrateurs de comprendre la logique. Il y sera accessible entre autres, la gestion des secteurs, des rôles, des utilisateurs et du matériel. L'outils de configuration est installé sur des postes informatiques du réseau permettant à un administrateur d'accéder au paramétrage et à la configuration n'importe où.

1.6.4 Gestion de la Sécurité Centralisée (GSC)

L'interface dans cadre de l'exploitation des systèmes de sûreté est entendue comme l'application logicielle permettant la supervision de l'ensemble des dispositifs participant à la sécurisation du site. Elle a pour but permettre un accès à toutes les fonctionnalités des différents systèmes unifiés. Cette interface doit être personnalisable à l'aide de différentes tâches ou tableau de bords, permettant à chaque exploitant de s'approprier son poste de travail. Ces taches seront personnelles ou partagées entre les opérateurs. Véritable gestion graphique, elle permet de gérer des plans organisés avec une navigation aisée, affichant des symboles dynamiques et interactifs des entités : caméras, détecteurs, portes, ... En complément, un fil de l'eau des événements d'alarmes, d'accès ou autre, complété d'une zone d'affichage de type mosaïque. Les mosaïques permettent d'afficher des portes, des caméras, de la lecture de plaque minéralogiques, de l'intrusion, des plans, des pages web, des résultats de rapports et tous autres éléments disponibles dans le système. Il est alors possible d'avoir des informations visuelles temps réel de toutes les composantes de sûreté, ainsi que d'effectuer des actions depuis les plans, le fil d'événements et les images vidéo, ou via la barre d'outils adaptative, donnant accès aux fonctions de l'entité sélectionnée. Il est prévu d'un à quatre moniteurs d'affichage pour une bonne ergonomie d'utilisation sur les postes GSC, en fonction de l'utilisation ciblée.

1.6.5 Gestion Mobile (GM)

Pour répondre au besoin de mobilité des exploitants, la plateforme unifiée dispose d'une gestion via un client web ou une application mobile. Cette interface est accessible depuis un smartphone, une tablette, ou un navigateur web. Une application disponible sur l'Apple App Store et le Google Play Store sont disponibles. Pour des questions de sécurité, l'administration et l'accès au paramétrage du système ne doivent en aucun cas être réalisés à partir de cette interface, elle permet les fonctionnalités suivantes d'exploitation globale :

- Interface cartographique
- Vidéoprotection, surveillance et investigation
- Contrôle d'accès, pilotage distant et levée de doute
- Actions éclair et notification push
- Partage de la vidéo de la caméra de l'appareil
- Localisation de l'exploitant mobile sur le plan et messagerie

La fonction logicielle nécessite uniquement une extension de licence du système déployé, et ne remet pas en cause l'installation, mis à part la mise en place d'une ressource informatique correspondante. La gestion mobile n'est pas prévue dans le cadre de ce marché mais pourra être ajouté à la demande de la maîtrise d'ouvrage.

1.7 Fonctionnalités d'administration

Ces différentes fonctionnalités sont disponibles pour les exploitants ou les administrateurs dans le GCT ou le GSC. En fonction des privilèges, ils ont plus ou moins d'autorisation à l'utilisation. Lorsqu'une fonction n'est pas disponible pour un opérateur, il ne peut tout simplement pas la voir afin d'épurer l'interface.

1.7.1 Les entités

Les entités sont les composants de base de la plateforme unifiée. Tout ce qui requiert une configuration est représenté par une entité. Les entités peuvent représenter un objet physique, comme une caméra ou une porte, ou une notion abstraite, comme une alarme, un horaire, un utilisateur, un rôle, un module externe ou un composant logiciel.

1.7.2 Les serveurs et les rôles

Les serveurs sont un type d'entité qui représente une ressource informatique sur lequel le logiciel de la plateforme unifiée de sûreté est installé. Fonction de la performance de traitement nécessaire, la solution peut se déployer sur une quantité plus ou moins importante de machine. La scalabilité de la solution est un critère de choix important.

1.7.3 La fédération de sites

La fonctionnalité de fédération relie plusieurs systèmes de sécurité sur IP indépendants pour former un seul système virtuel. Grâce à cette fonctionnalité, les administrateurs et les exploitants peuvent afficher et contrôler les entités qui appartiennent aux systèmes fédérés directement depuis leur système hôte local.

L'unification pour la plateforme unifiée s'assure également en multisite. La solution doit permettre ces fonctionnalités afin de pouvoir rapatrier des éléments d'autres sites distants. Aucun site fédéré n'est prévu dans ce marché.

1.7.4 La cartographie

La solution apporte des plans dynamiques pour visualiser et parcourir l'installation en temps réel, pour gérer toutes les entités du système : caméras, portes, détecteur ou autres... Les cartes permettent d'effectuer les

tâches suivantes :

- Navigation panoramique et zoom / Parcourir les différentes cartes
- Étendre une même carte à plusieurs moniteurs
- Gérer toutes les entités de la plateforme unifiée de sûreté
- Surveiller et répondre aux alarmes et événements en temps réel
- Ajouter des entités locales et fédérées
- Afficher des informations sur les objets cartographiques dans des bulles de texte
- Rechercher les entités sur les cartes et voir les entités à proximité
- Repérer les points d'intérêt
- Surveiller l'état de points

1.7.5 Outils de maintenance et diagnostique

À des fins de dépannage, un outil de collecte de données de diagnostic recueille et prépare les informations système pour que l'administrateur puisse facilement les envoyer support. Le système dispose notamment de rapport d'état de santé du système permettant à l'administrateur de toujours avoir rapidement un œil sur l'état de fonctionnement de son système.

1.7.6 Situations de crise

Il est nécessaire de pouvoir paramétrer des scénarii correspondant à des situations de crise pour lesquelles l'ensemble du fonctionnement du système sera modifié, soit pour faciliter l'évacuation du site, soit pour renforcer le contrôle et restreindre les accès. Une fonction de gestion des niveaux de crise doit permettre de façon simple et rapide, de changer les autorisations d'accès du site. Plutôt que de modifier les droits d'accès pour les utilisateurs individuellement, la fonction fournit un paramètre pour l'ensemble de l'installation de la sécurité générale, qui peut être modifié par une seule action en utilisant l'écran niveau de crise.

Chaque groupe d'accès ou utilisateur dispose d'un niveau de crise, est dispose de ces droits valides, tant que le niveau de crise du site reste égal ou inférieur. Un minimum de 8 niveaux est paramétrable dans la solution technique proposée.

1.8 Fonctionnalités d'exploitation

Le GSC est de base un client lourd, fonctionnant sous Microsoft Windows. L'interface graphique est parfaitement intégrée dans cet environnement, avec une gestion multi tâches sous forme d'onglets, permettant une navigation intuitive et simplifiée. Via une page d'accueil représentant toutes les tâches, il est facilement repérable par un code couleur les fonctions dédiées aux différents métiers. Pour simplifier l'exploitation de l'interface, les manipulations ne requièrent que la sélection d'icônes ou l'accès à des menu contextuel au moyen de la souris, et la conception est faite pour accéder à l'objectif avec le moins de clics possibles. Un utilisateur lambda de l'outil informatique doit pouvoir accéder aux principales fonctions sans formation, de manière totalement intuitive.

Pour y accéder, chaque exploitant dispose de son nom d'utilisateur et de son mot de passe. En fonction de l'exploitant et de ces privilèges, il a accès aux tâches du GSC qui lui sont autorisées. Celui-ci peut configurer son environnement de travail et le sauvegarder pour lui-même, ou le partager avec ses homologues. Seul l'administrateur du système, peut accéder à l'ensemble des droits, et notamment celui de définir les droits des autres utilisateurs.

1.8.1 Les tâches de surveillance

Parmi les tâches proposées via une page d'accueil ergonomique, le GSC propose une des tâches de surveillance en temps réels. Celles-ci permettent aux exploitants de garder un œil sur le fonctionnement de l'installation afin de veiller à la sécurité du site.

Evénements

Un fil des événements, ou fil de l'eau, interactif et paramétrable, permet de visualiser en temps réel tous les événements liés au système. Il est possible de séparer les événements de type accès et de type alarme, et de cliquer sur un événement quelconque pour accéder au menu contextuel délivrant les différentes fonctions associées.

Ce menu contextuel permet d'accéder aux fonctionnalités liées à chaque événement. En cas d'alarme associée à une caméra vidéo par exemple, le menu contextuel permet d'ouvrir la séquence enregistrée et la prise en compte de l'alarme.

La surcharge d'information dans les fils de l'eau entraîne la plupart du temps une inefficacité à long terme. Pour prévenir cela, la solution dispose d'une fonction de surveillance permettant aux exploitants de sélectionner les entités pour lesquelles, ils souhaitent avoir les remontées d'événements en temps réels.

Cartographie dynamique

Afin d'optimiser l'investigation en temps réel, le GSC dispose d'un outil de gestions de plans, avec l'implantations des entités représentatives du fonctionnement du système. Ces entités seront dynamiques et les plans seront vectoriels, afin de garantir une bonne qualité même en zoom sur des grands plans, sans être volumineux.

La gestion de plans est importante pour la localisation simple et efficace de tous les événements. Elle se présente sous la forme d'un écran de plan, associé à un bandeau d'événements et a une liste de plans du site. Il est ainsi très aisé de passer d'un plan à l'autre, soit par la liste, soit par clic dans le plan.

Le plan est interactif en temps réel, c'est-à-dire que les symboles représentant les terminaux ou accès sont dynamiques, informant de leur état. Une action par double clic est paramétrable sur les symboles, ainsi que le clic droit qui permet d'ouvrir le menu contextuel offrant les différentes possibilités suivant le type d'entités.

Les alarmes sont visibles par un repérage coloré et il est possible de faire switcher automatiquement les plans. Sans aucune action de l'exploitant, le plan correspondant à un déclenchement d'alarme vient automatiquement s'afficher, pour une meilleure efficacité.

La gestion graphique permet également de créer des boutons ou des afficheurs, entièrement paramétrables, à l'image de la programmation réalisée sur le système. Une bibliothèque de symbole ainsi qu'un éditeur sont disponibles pour une personnalisation totale par les exploitants.

Levée de doute

Une gestion des vidéos permet d'avoir un visuel associé à chaque événement pour mieux en déterminer la cause, ou encore pour valider visuellement ce qui se passe. Elle se présente sous la forme d'un écran d'affichage mosaïque paramétrable, associé à un bandeau d'événements et a une liste des caméras du site. Il est très simple de configurer son affichage par cliquer déposer de la liste des caméras vers la mosaïque.

La mosaïque paramétrable permet également d'afficher automatiquement les caméras associées aux événements de la plateforme unifiée. La vidéo ainsi affichée est visuellement associée à l'événement dans l'affichage avec une incrustation dans l'image, pour distinguer facilement les événements autres vidéos de surveillance.

Barre d'outils dynamique

Une plateforme unifiée proposant de nombreuses fonctionnalités multi métiers, il peut y avoir trop de fonctionnalité pour l'opérateur. Afin d'optimiser l'utilisation et de guider les exploitant, le GSC propose une barre d'outils dynamique, qui change automatiquement en fonction des entités sélectionnées.

1.8.2 Les tâches de rapport et d'investigation

Le besoin d'établir des rapports spécifiques ou statistiques étant important pour la maîtrise d'ouvrage dans l'utilisation de la solution, un assistant de rapport sophistiqué est intégré à la solution. Il établit des rapports prédéfinis sur tous les éléments du système, et permet à l'exploitant d'ajouter ou de supprimer des catégories d'information, et de filtrer les données pour produire des rapports plus spécifiques sur mesure, si nécessaire. Les rapports couvrent tous les types de transactions du système, et peuvent également dresser la liste des informations matérielles et les paramètres de configuration.

Un mode de prévisualisation permet à l'utilisateur construire et de voir l'ensemble de son rapport avant l'impression ou l'export. Les nouvelles définitions de rapport de l'exploitant peuvent être enregistrées comme rapports personnalisés, et peuvent être réutilisés sans exiger une nouvelle définition.

Une palette complète d'outils graphiques permet à l'exploitant une exploitation visuelle des données filtrées et pertinentes. Elle permet de réaliser des camembert, nuages de points, graphique de barres, et autres...

1.8.3 Les tableaux de bords

Les tableaux de bord correspondent une tâche d'exploitation qui fournit un tableau vierge entièrement personnalisable, sur lequel il peut se fixer des widgets afin d'obtenir une interface GSC sur mesure. Plusieurs types de widgets doivent être disponibles : des graphiques, des résultats de rapports, des vignettes vidéo ou de portes, des compteurs, du texte, des pages web, des plans, et autres... Ces widgets apportent une supervision des indicateurs clés de la plateforme unifiée et fournissent un aperçu de l'activité et des événements enregistrés par le système.

De base, un tableau de bord type est créé et prêt à l'exploitation pour la supervision de l'état de l'installation, avec le score de sécurité et les indicateurs de performance clés.

2 SYSTEME DE CONTROLE D'ACCES SYNERGIS

2.1 Principe de base

Afin de sécuriser le site et de limiter la circulation dans les différents secteurs, en fonction des niveaux d'autorisations de chacun, les accès aux différentes zones sont contrôlés aux moyens d'un système centralisé de contrôle d'accès **Synergis** permettant de :

- Contrôler et identifier les différentes circulations du personnel dans les locaux en limitant les accès aux zones autorisées,
- Traiter et mettre en forme des informations temps réelles en vue de leur utilisation immédiate et ultérieure. À tout moment, un état des personnes présentes sur les différentes zones du site, doit être consultable,
- Superviser les alarmes et les défauts locaux en provenance des terminaux.

Des organes de contrôle associés à des environnements de porte, sont mis en place afin de bloquer ou d'autoriser physiquement, la circulation du personnel. Associés à des contrôleurs répartis et autonomes en tous points, les accès sont supervisés en temps réel, avec une visualisation adaptée à chaque profil d'exploitant, le site dispose d'une partie en contrôle d'accès, le titulaire devra s'assurer du parfait fonctionnement de celle-ci dans le cadre de la migration du système.

2.1.1 Pérennité et évolutivité

Il est rappelé que la solution retenue est de type éditeur, c'est-à-dire qu'une entité logicielle gère le matériel terrain, de divers fabricants. La possibilité de mettre différents contrôleurs issus de différents fabricants est une prérogative de choix de la solution. La solution proposée doit intégrer des contrôleurs d'au moins 3 fabricants reconnus sur le marché.

Les terminaux gérés par les différents contrôleurs répartis sur sites, sont définis comme les éléments constituant l'environnement de contrôle, de verrouillage et de détection, associés à l'obstacle physique limitant la circulation d'un espace à l'autre. Ils sont choisis parmi les standards reconnus du marché selon les caractéristiques décrites et sont soumis à validation de la maîtrise d'œuvre. Ils doivent impérativement se baser sur des technologies ouvertes et non propriétaires, afin que la maîtrise d'ouvrage reste libre des approvisionnements et de la maintenance.

2.1.2 Le rôle du Gestionnaire d'Accès

Le rôle du gestionnaire d'accès gère et surveille les unités de contrôle d'accès du système. Le gestionnaire d'accès assure la mise à jour des réglages sur les unités, en temps réel ou sur horaire, afin qu'elles puissent prendre des décisions de contrôle d'accès de manière autonome, qu'elles soient connectées ou non à celui-ci. Le Gestionnaire d'accès consigne également les événements de contrôle d'accès dans la base de données à des fins d'investigation ou de maintenance. Tous les événements générés par les unités (accès accordé, accès refusé, porte ouverte, etc.) sont transmis par le gestionnaire d'accès, par l'intermédiaire du rôle répertoire, aux composants concernés du système. Plusieurs instances de ce rôle peuvent être créées au sein du système pour gérer la ressource informatique en fonction de la performance.

2.1.3 Maintien en condition opérationnelle terrain

L'application de contrôle d'accès doit s'organiser sur une architecture logique comprenant une base de données répertoire : configuration et utilisateurs, et une base pour les événements. Pour disposer d'une redondance dans le cadre du projet, la solution retenue dispose nativement d'un mécanisme de redondance intégré du répertoire.

La redondance souhaitée correspond à la mise en place d'un répertoire sur deux salles. Pour éviter un aspect trop coûteux de la redondance, il est prévu un répertoire principal, et un répertoire de secours. Le basculement est automatique en cas de défaillance, est le retour à la normal se fait manuellement, selon la méthode dite du backup and restore.

Toutes solutions ne disposant pas de ces fonctionnalités nativement ne sont pas envisageables.

Dans un souci de maintien en condition opérationnelle terrain, il est important que le système soit capable d'assurer ses fonctions propres, sur le principe de l'intelligence répartie. Une perte de serveur, une perte réseau ou une perte de bus, ne remettra aucunement en cause le bon fonctionnement de l'installation terrain. A ce titre les contrôleurs déployés doivent être autonomes, tant au niveau de la communication, qu'au niveau de l'alimentation. **Afin de répondre à la répartition des portes et à l'implantation des coffrets, l'utilisation de modules déportés est acceptable dans la mesure où la perte d'un bus terrain n'entraîne pas la perte d'un nombre de porte n'excédant pas 8 portes.** Les coffrets sont tous secourus par batterie sans exception, quel que soit le mode d'alimentation utilisé.

2.1.4 Automatismes terrain

Dans certaines situations et à partir des informations collectées par le système, il est nécessaire de générer des actions automatiques d'exploitation. Le système de contrôle d'accès proposé doit donc permettre de créer librement ces automatismes déclenchés sur événements, avec la possibilité pour les exploitants de définir :

- Les automatismes : Logiciel ou terrain, sous un mode Actions / Événements
- Les exploitants concernés : Pour voir l'activation de ces automatismes ou déclencher un processus.

Les automatismes dit terrain, seront chargés vers les contrôleurs, qui assureront le fonctionnement sans avoir recours à une interrogation du serveur.

2.2 Fonctionnalités

Ces différentes fonctionnalités sont disponibles pour les exploitants ou les administrateurs dans le GCT ou le GSC. En fonction des privilèges, ils ont plus ou moins d'autorisation à l'utilisation. Lorsqu'une fonction n'est pas disponible pour un opérateur, il ne peut tout simplement pas la voir afin d'épurer l'interface.

2.2.1 Les titulaires de carte

Un titulaire de carte est un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées.

Groupes de titulaires de cartes

Un groupe de titulaires de cartes sert à configurer des droits d'accès et les propriétés communes à un ensemble de titulaires de cartes. Dans le cadre d'un système de contrôle d'accès de taille importante, les titulaires de cartes et les règles d'accès sont bien plus faciles à gérer quand les titulaires de cartes sont membres de groupes de titulaires.

La maîtrise d'ouvrage souhaite retenir un système gérant une arborescence des utilisateurs, permettant une synchronisation des titulaires de cartes par Active Directory (ou annuaire LDAP). L'objectif est d'entretenir la base de données du contrôle d'accès, via la gestion du personnel par les ressources humaines.

Il conviendra de mettre en place un organigramme en concertation avec le maître d'ouvrage.

2.2.2 Définition des règles d'accès

Une règle d'accès définit une liste de titulaires de cartes auxquels un accès est accordé ou refusé en fonction d'un horaire. Les règles d'accès peuvent être appliquées aux secteurs sécurisés et aux portes d'entrée et de sortie, ou aux secteurs de détection d'intrusion pour l'armement et le désarmement.

Les règles d'accès sont soit permanentes, soit temporaires. Les règles d'accès temporaires sont adaptées aux situations qui nécessitent d'accorder aux titulaires de cartes un accès temporaire ou saisonnier à des secteurs sécurisés. Ces règles d'accès sont automatiquement supprimées sept jours après leur expiration afin d'éviter d'encombrer le système. Les règles d'accès temporaires sont typiquement utilisées pour les titulaires de cartes externes, ou pour les titulaires de cartes permanents qui ont besoin d'un accès à court terme à une zone sécurisée, comme les techniciens de maintenance qui interviennent sur le système.

La configuration quotidienne se fait dans le GSC, alors que des règles avec une gestion plus globale et personnalisées, se fait plutôt dans le GCT.

La programmation des droits d'accès est associée à chaque utilisateur, et non à chaque identifiant, ce qui établit une libre circulation à l'intérieur des espaces autorisés, quel que soit le dispositif de contrôle. Chaque utilisateur peut avoir différents identifiants, sous différentes formes, qui lui sont attribués : Badges physique RFID, badge virtuel Bluetooth ou NFC, Ainsi, l'utilisateur utilise ses différents identifiants aux différents modes de contrôle, de manière totalement transparente pour les exploitants.

2.2.3 Définition des horaires

En association au groupe d'accès ou en individuel, les programmes journaliers et hebdomadaires permettent de définir les plages horaires sur lesquelles les utilisateurs bénéficient des droits d'accès. Cette gestion intègre les jours fériés.

Les horaires sont des contraintes de temps qui peuvent être appliquées à de nombreuses situations au sein du système. Chaque contrainte horaire est décrite par une plage de dates (quotidien, hebdomadaire, mensuel, annuel ou à dates spécifiques) et par une plage horaire (toute la journée, plage fixe, journée ou nuit). Chaque contrainte horaire est caractérisée par des dates (périodicité ou dates particulières couvertes par l'horaire) et des heures (périodicité à l'échelle de 24 heures).

2.2.4 Utilisations des accès

Dans le but de permettre une souplesse dans la vie quotidienne du contrôle d'accès, ou en cas d'événements spécifiques, il est nécessaire qu'en exploitation, les accès permettent diverses utilisations configurables :

- Accès contrôlé : La porte est en état de fonctionnement, un voyant signale que le lecteur est en attente d'une lecture. Après contrôle de l'utilisateur, l'accès est refusé ou accordé en fonction des droits qui lui sont attribués.
- Accès libre : La porte est ouverte, l'accès n'est pas contrôlé.
- Accès bloqué : La porte est bloquée, l'accès n'est pas contrôlé.
- Accès sous escorte : La porte est en état de fonctionnement normal. Certains utilisateurs pourront être définie comme superviseur, permettant ainsi de s'identifier sur l'organe de contrôle afin d'autoriser l'accès à une personne autorisée sous escorte.
- Accès à valider : La porte est en état de fonctionnement normal. Certain accès sont surveillés en permanence par un exploitant. Lors du contrôle d'un utilisateur, ce dernier, effectue une vérification visuelle, et déclenche ou non, l'ouverture de l'accès. Cette fonction pourra être associée à la vidéo.

2.2.5 Gestion d'impression des badges

Les badges des utilisateurs doivent être personnalisés. La solution de contrôle d'accès doit donc permettre une gestion intégrée d'impression de badge. Les exploitants peuvent définir de multiples modèles de fond de badge, et les imprimer directement depuis le GSC. Une imprimante à badge doit être directement raccordée au poste. Il peut être intégré sur les modèles :

- Des textes : Champs de la fiche détenteur de badge, Champs personnalisables, ...
- La photo : Correspondante à l'utilisateur,
- Des logos, Images : De l'entreprise par exemple.
- Un modèle déjà fourni par la maîtrise d'ouvrage

2.2.6 Gestion d'enrôlement et d'encodage de badge

Dans le cadre d'un déploiement de badges sécurisés, il est prévu un poste client dédié à l'encodage des badges. Celui-ci dispose d'un lecteur de table USB permettant de programmer ou de reprogrammer l'encodage de la mémoire des badges. Il permet également de créer des badges de reconfiguration pour les lecteurs de badges afin de laisser la possibilité à la maîtrise d'ouvrage de gérer sa sécurité en totale liberté.

Il doit être également prévu des lecteurs de table USB enrôleurs pour, permettant aux exploitants d'associer ou de lire facilement le badge d'un utilisateur, sur les postes ou cela est nécessaire, comme l'accueil pour les visiteurs par exemple.

2.2.7 Antiretour (Anti Pass Back)

Dans le but de renforcer le niveau de sécurité, ou simplement d'éviter les prêts de badge, certains accès de zone sont dits antiretour. Cette fonction permet d'éviter à un même titulaire de carte de pénétrer dans une même zone plusieurs fois.

Il existe deux types de remontée d'information d'antiretour, le logique et le physique :

- Logique : L'antiretour Souple ne fait que consigner les événements antiretours dans la base de données. Il ne bloque pas le déverrouillage de la porte en cas d'événement antiretour.
- Physique : L'antiretour strict consigne les événements antiretours dans la base de données et bloque le déverrouillage de la porte en cas d'événement antiretour.

Délai d'expiration de présence

Cela définit la durée durant laquelle la présence du titulaire de cartes est mémorisée pour la détection antiretour. Une fois la période écoulée, un titulaire de cartes qui n'a jamais quitté le secteur peut à nouveau entrer sans déclencher d'événement antiretour. Ce délai peut être nul avoir un antiretour permanent.

2.3 Fonctionnalités complémentaires

2.3.1 Gestion des communications

Afin de gérer les interphone et visiophone du site, la plateforme unifiée de sûreté dispose d'une solution **Sipelia** pour la gestion des communications sur IP. Cette solution est basée sur l'intégration de terminaux compatible avec le protocole standard et ouvert SIP. Nativement intégrée dans le GSC, l'exploitant peut prendre les appels et communiquer avec l'interlocuteur en toute simplicité depuis son poste. Le cas échéant, un visuel de la caméra est disponible, est les fonctions associées à la porte également, permettant le déverrouillage à distance par exemple.

2.3.2 Gestion d'ascenseur

Le site disposant d'ascenseurs, il est prévu la mise en place d'une gestion de ceux-ci par le contrôle d'accès. Le logiciel doit fournir de manière complètement intégrée, le contrôle des accès pour les ascenseurs, en gérant les différents niveaux autorisés. Pour cela, il doit être placé des lecteurs dans les cabines, afin de permettre aux utilisateurs d'accéder uniquement aux niveaux autorisés après avoir été contrôlé. Les contrôleurs associés, placés en machinerie, doivent s'interfacer par relais ou autres avec les ascenseurs. L'entreprise doit prévoir l'intervention la prestation en coordination avec l'ascensoriste.

2.3.3 Gestion des visiteurs

Un visiteur est un utilisateur occasionnel du système du contrôle d'accès, ayant des droits d'accès limités dans les espaces, mais également dans le temps. Le système permet de définir et de planifier temporairement des visites, avec au minimum les informations suivantes :

- Personne visitée : Sélectionner parmi la liste des détenteurs de badge, la personne visitée
- Coordonnées du visiteur : Spécifier les coordonnées pour joindre la personne
- Motif de la visite : Spécifier le motif de la visite.

En renforcement de la sécurité sur des visiteurs identifiés comme profil sensible, il peut être associé le mode escorte, et il est possible de joindre des documents lors de la création. La création et la planification doit être effectuée depuis le GSC, par un exploitant.

2.3.4 Gestion avancée des visiteurs

En complément de la gestion de base d'écrite, le système dispose d'une interface web accessible en intranet pour le pré enregistrement des visiteurs afin de planifier leurs visites. Cette interface permet l'entrée les informations personnelles du visiteur par un utilisateur loggé sur la page, ainsi que les informations concernant sa visite :

- Lieu de visite : Lieu géographique, bâtiment, service, ...
- Événement ou invitation : Pour la gestion d'événements ponctuels.

Cette solution permet de gérer des listes d'invitations, ainsi que l'envoi de courriel aux visiteurs planifiés, en y associant un QR Code ou autre identifiant dématérialisé permettant un accès direct au site pour se rendre à l'accueil, point de passage obligatoire pour des raison de sécurité : contrôle d'identité et authentification de la personne. Cette fonction permet notamment la réservation d'une place et d'un accès au parking géré par le contrôle d'accès.

Pour un accès sans fil d'attente ou en cas d'événements spécifiques, il est prévu une borne d'accueil permettant un pré contrôle du visiteur afin que celui-ci s'enregistre lui-même. Pour disposer d'un badge physique permettant de pénétrer l'enceinte sécurisée du site, le visiteur devra dans tous les cas passer par l'accueil pour un contrôle d'identité.

2.3.5 Gestion de comptage et occupation

Afin d'être capable de déterminer le nombre d'utilisateurs présents dans les zones sensibles ou dans la globalité du bâtiment, il doit être déployé une gestion de comptage. Celle-ci est un programme qui permet d'incrémenter ou de décrémenter un compteur quand des conditions prédéfinies sont satisfaites. Les computers peuvent être utilisés de différentes manières, notamment en comparaison avec des valeurs minimum et maximum de référence, qui déclenchent un automatisme quand elles sont atteintes. Il est possible par exemple de déterminer des seuils de présence, à partir desquels le système appliquera automatiquement des décisions pré programmées par le responsable de sécurité.

Suivant les zones à comptabiliser, il doit être mis en place aux accès périphériques des lecteurs en entré et en sortie. Pour garantir des résultats satisfaisants, un système garantissant l'unicité de passage doit être mis en place.

2.3.6 Gestion d'accès sans fil online

Dans un objectif d'éviter des coûts trop importants de câblage et de faire des économies en réduisant le nombre de clés physiques sur le site, il est prévu de mettre en place sur les locaux peu sensibles un contrôle d'accès sans fil, en complément du contrôle d'accès câblé, fonctionnant avec les mêmes badges. Ce contrôle d'accès sans fil est online, c'est-à-dire qu'il est supervisé en temps réel depuis la supervision du contrôle d'accès. L'architecture doit rester la même, lecteur sans fil sur contrôleur, afin de garantir l'autonomie de fonctionnement. Le déploiement se fait sur la base d'un maximum de quatre accès sans fil pour un récepteur, et de huit accès par contrôleur, pour garantir un minimum de perte en cas de défaillance.

2.3.7 Gestion d'accès autonome Offline

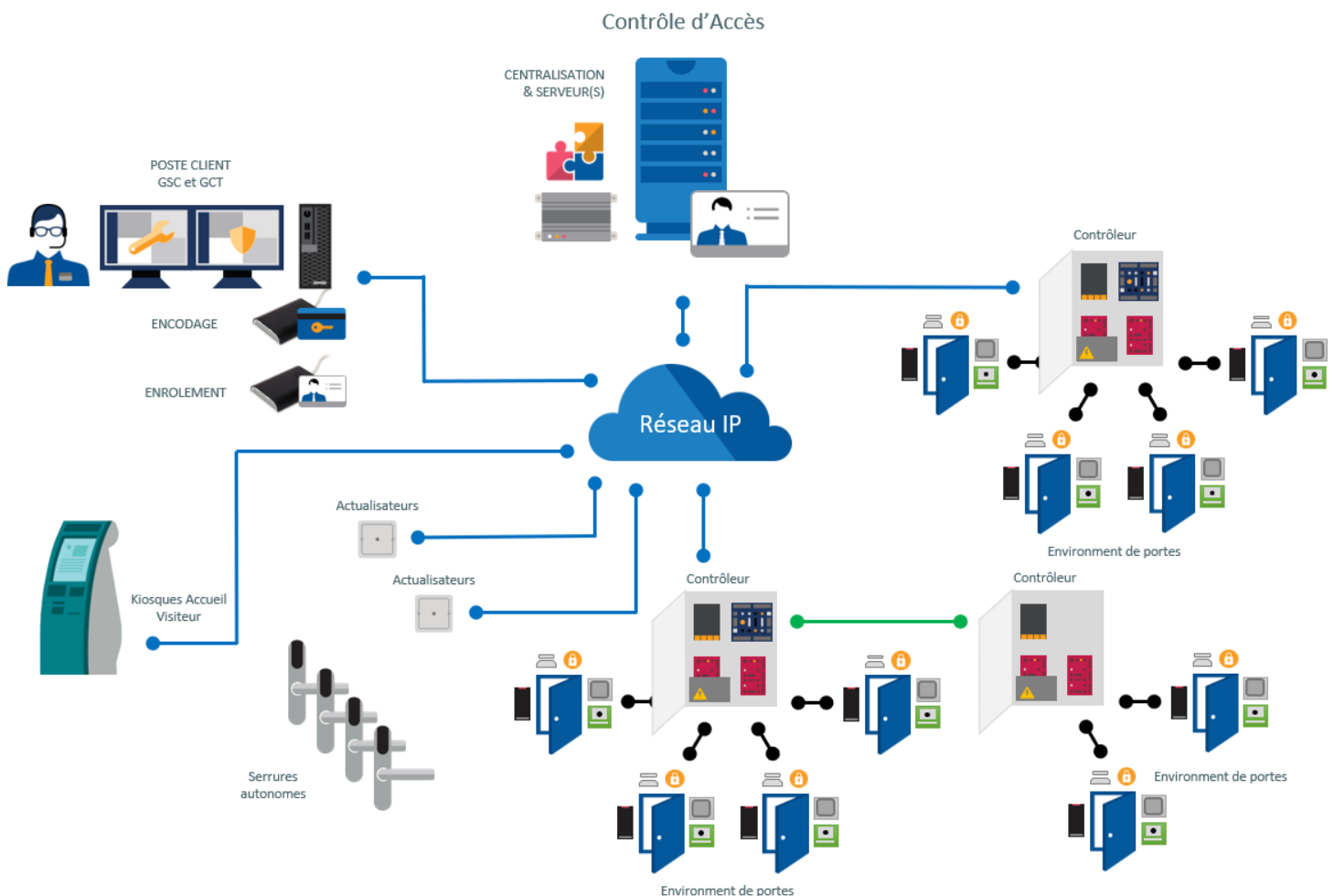
Dans un objectif d'éviter des coûts trop importants de câblage et de faire des économies en réduisant le nombre de clés physiques sur le site, il est prévu de mettre en place sur les locaux peu sensibles un contrôle d'accès autonome, en complément du contrôle d'accès câblé, fonctionnant avec les mêmes badges. Ce contrôle d'accès autonome est Offline, c'est-à-dire qu'il est supervisé en temps différé par la supervision du contrôle d'accès.

L'architecture est basée sur des serrures autonomes réparties sur les différents accès, et des lecteurs actualisateurs. La gestion des droits et des événements se fait par le mémoire du badge, qui transportent et assurent la communication entre les serrures autonomes et les lecteurs actualisateurs. Ces informations sont remontées et redescendues à la supervision via ces lecteurs.

2.4 Architecture de la solution de Contrôle d'Accès

La structure de la solution de contrôle d'accès **Synergis** s'organise donc selon trois niveaux :

- La centralisation : Serveurs, applications, base de données, Postes Client.
- Les contrôleurs : Organes de gestion autonomes et secourus.
- Les environnements de portes : Lecteurs, détecteurs, bouton poussoir, verrouillage.



2.5 Descriptions Techniques

2.5.1 Les contrôleurs

Les contrôleurs sont entendus comme les éléments matériels constituant les organes terrain, autonomes et secours, de la solution de contrôle d'accès. Ces contrôleurs comportent des UTL intelligentes, ainsi que des modules lecteurs dépendants, pour câbler au plus près des portes en cas de nécessité. Il doit être privilégié au maximum, d'avoir une UTL intelligente par coffret afin de garantir l'autonomie. Toutefois, l'entreprise propose son étude d'implantation pour une répartition idéale, tout en garantissant un maximum de 16 portes par UTL intelligente, pour éviter une perte trop importante en cas de panne ou de coupure de communication.

Le système proposé doit impérativement fonctionner sur le réseau IP, mais avec la possibilité de fonctionner sur bus RS485, afin de s'adapter à tout type d'environnement et proposer une architecture souple et modulable.

Les contrôleurs prévus sont de la **gamme LP / MR, de marque Mercury**. Les UTL intelligentes sont les briques matérielles principales du système garantissant un fonctionnement autonome avec le stockage local des utilisateurs, mais aussi de l'historique des événements en cas de coupure de communication. Les événements stockés sont restitués à la plateforme unifiée lorsque la communication est rétablie. Les alimentations des contrôleurs sont toutes secours par batterie sans exception. Les contrôleurs sont intégrés en coffrets sécurisés avec autoprotection intégrée.

Dans tous les cas, il doit être supervisé au minimum les défauts de : communication, alimentation, et autoprotection.

- UTL intelligente : assure la gestion autonome du contrôle d'accès, pilote les modules et les éventuels environnements de portes associés. Ils communiquent en temps réel avec la centralisation, et stock en local toutes les informations liées à la base de données les concernant, pour la gestion de modules déportés, selon les caractéristiques techniques suivantes :
 - Contrôleur d'accès 100% autonome
 - 1 ou 2 portes / 1 ou 2 Lecteurs de badge
 - Communication IP sécurisée
 - Communication RS485 pour les modules complémentaires
 - Coffret sécurisé avec autoprotection
 - Alimentation 230V intégrée avec batterie et défauts
 - 1 ou 2 liaisons lecteurs Wiegand ou RS485 (OSDP retenu)
 - Mémoire 150k détenteurs de badges, et 50k événements
 - De 3 à 10 Entrées / de 2 à 4 Sorties pour les terminaux
 - De 16 à 32 modules complémentaires
- Module complémentaire Lecteurs : assure la gestion des portes et leur environnement. Il communique en temps réel avec l'UTL intelligente et dépend de son autonomie. Il gère 1 ou 2 lecteurs, selon les caractéristiques techniques suivantes :
 - Module dépendant de l'UTL intelligente
 - 1 ou 2 portes / 1 ou 2 Lecteurs de badge
 - Communication RS485 avec l'UTL intelligente
 - Coffret sécurisé avec autoprotection
 - 1 ou 2 liaisons lecteurs Wiegand ou RS485, ...
 - De 3 à 10 Entrées / de 2 à 4 Sorties pour les terminaux

- **Module complémentaire Entrées/Sorties** : assure la gestion d'entrées et de sorties complémentaires. Il communique en temps réel avec l'UTL intelligente et dépend de son autonomie. Il peut servir à gérer la remontée d'information de capteurs ou piloter des ascenseurs par exemple, selon les caractéristiques techniques suivantes :
 - Module dépendant de l'UTL intelligente
 - Communication RS485 avec l'UTL intelligente
 - Coffret sécurisé avec autoprotection
 - 16 Entrées / 16 Sorties

2.5.2 L'environnement de porte

Il est défini par les terminaux qui sont les éléments constituant l'environnement de contrôle, de verrouillage et de détection associés à l'obstacle physique limitant la circulation d'un espace à l'autre. Ils comprennent le plus souvent les lecteurs, les organes de verrouillage, les détecteurs, les boutons poussoir, et les boîtiers bris de vitre.

- **Boîtiers Bris de Glace Vert deux contact** : Les Boîtiers Bris de Glace Vert ou Déclencheurs Manuel Vert, sont à membrane déformable, double contact et capot de protection plastique si nécessaire. L'un des deux contacts sert à la coupure de l'alimentation, l'autre est repris sur les contrôleurs pour la supervision. Ce dernier génère une alarme.
- **Détecteur d'Ouverture** : Chaque détecteur d'ouverture de porte est principalement composé de deux éléments. Un premier élément positionné sur la partie fixe de la porte est constitué d'un interrupteur à lame souple. Un second élément positionné sur l'ouvrant de la porte et constitué d'un simple aimant. Chaque détecteur est auto-protégé.
- **Bouton poussoir** : Il est prévu des boutons poussoir, en cas de besoin pour les sorties libres, de type plastique en saillie. Les boutons disposent d'une indication claire indiquant leur fonction (écrit porte, dessin clé, ...)
- **Organes de verrouillage** : Les accès doivent être équipés d'organe de verrouillage à rupture et doivent respecter la norme NFS 61 937 pour les issues de secours. Ils sont de type gâches électriques ou ventouses électromagnétiques. Ces organes de verrouillages sont alimentés par les contrôleurs dans la limite de 12V/500mA maximum par verrouillage. Des alimentations secourues indépendantes du contrôle d'accès doivent être prévues par le présent lot pour des consommations supérieures ou des tensions différentes de 12V. Ces alimentations doivent être asservies à l'incendie dans le cas des issues de secours, et si nécessaire, le titulaire doit mettre en place un interfaçage de puissance pour libérer les portes en cas de détection incendie en agissant directement sur l'alimentation des ouvrants indépendamment du système de contrôle d'accès. Le titulaire doit, pour chaque accès contrôlé, la fourniture d'un ferme-porte, et prendre en compte la consommation des organes de verrouillages pour dimensionner et définir, les alimentations séparées ou non, nécessaires au bon fonctionnement du contrôle d'accès.

2.5.3 Les lecteurs

Dans un souci d'évolutivité et de compatibilité, les lecteurs choisis sont multi technologie et évolutifs, permettant la lecture de différents types d'identifiants et la reprogrammation et parfaitement compatible avec la solution Genetec.

- Lecteur de badge sécurisé multi-technologie : Ils assurent la lecture sécurisée des identifiants, badges dans ce cas, et communiquent avec les contrôleurs de manière sécurisée selon le protocole OSDP sur bus RS485. Le mode de sécurisation retenue est 13.56 MHz Mifare Desfire EV1 en AES 128 bits, signé et chiffré. Les lecteurs assurent le protocole de cryptographie et contiennent les éléments secrets, type clé de cryptage, de manière protégée. Ils ont les caractéristiques techniques suivantes :
 - 13.56 MHz. ISO14443 types A & B, ISO18092
 - MIFARE Ultralight® et Ultralight® C, MIFARE® Classic et EV1, MIFARE Plus®, MIFARE® DESFire® EV1 et EV2, NFC, SMART MX, CPS3, iCLASS®, PicoPass®
 - Lecture sécurisée de fichiers ou secteurs
 - Jusqu'à 6 cm avec un badge MIFARE DESFire® EV1
 - Sortie bus RS485 / Protocole OSDP V2 pour communication protégée
 - Buzzer intégré et LEDs RVB couleurs entièrement personnalisables
 - IP65 et IK10 : Protection intérieure et extérieure anti vandale
 - Murale en applique avec design soigné
 - Montage sur tout type de support y compris sur métal
- Lecteur QR Code : Ces lecteurs permettent la lecture des identifiants dématérialisés tel que le QR Code pour la gestion de visiteurs. Ils disposent des mêmes caractéristiques que les lecteurs de badge sécurisé multi-technologie, avec les fonctions complémentaires suivantes pour les autres technologies :
 - Bluetooth et NFC : Identifiants dématérialisés pour smartphone
 - Code matriciel : Codes 1D & 2D ; QR Code versions 1, 2 et 3 ; Micro QR Code ; code 128 ; Aztec et Data M
 - Montage sur tout type de support y compris sur métal

L'implantation et le choix du modèle doit être justifié par l'entreprise avec une étude, en fonction des éléments et du contexte terrain, garantissant une lecture optimale.

- Serrure autonome : Ces serrures disposent d'un lecteur de badge intégré permettent la lecture et l'écriture des badges de manière sécurisée. La lecture permet de vérifier l'autorisation d'accès et l'écriture permet le retour des événements. Ils disposent des mêmes caractéristiques que les lecteurs de badge sécurisé multi-technologie.

2.5.4 Les identifiants

Les identifiants correspondent aux supports accueillant les numéros personnels des utilisateurs du système de contrôle d'accès. Ils peuvent se présenter sous plusieurs formes : Badges physiques plastique, porte clé, tags, badges virtuels NFC ou Bluetooth.

- Badge physique : Le badge étant le support permettant l'identification, il nécessite une gestion sécurisée des informations personnelles de l'utilisateur qu'il contient. Il est donc demandé une programmation des badges par l'inscription en mémoire d'un identifiant personnel issu, soit d'un champ de la fiche usager, soit directement calculé par le système. Il doit être totalement sécurisé, chiffré et signé, par cryptage. Il assure le protocole de cryptographie et d'authentification avec le dispositif de contrôle. Il est multi application selon un standard international permettant à la maîtrise d'ouvrage de garder sa totale autonomie, tant en approvisionnement, tant qu'en reprogrammation et utilisation multiple. Le numéro de série UID reste disponible en cas de besoin pour une utilisation non sécurisée, mais ne doit en aucun cas, être utilisé par le contrôle d'accès. Toute solution proposant l'utilisation du numéro de série UID sont directement rejetées.

2.6 Formations

L'entreprise doit impérativement prévoir la formation des personnels administrateurs et utilisateurs du système avec pour objectif, qu'à l'issue de la formation, les personnels des différentes administrations et des différents services soient pleinement opérationnels sur le système **Synergis**. Une formation à l'encodage des badges est également prévue au présent lot.

Le titulaire propose le contenu ainsi que la durée et le nombre de sessions de formations, qui est adapté au nombre de participants dans chaque domaine, et à la complexité de la solution.

2.7 Déploiement et mise en service

Le paramétrage de l'installation doit être réalisé par l'entreprise titulaire du présent lot en coordination avec les utilisateurs afin de livrer un ensemble en ordre de marche.

La Maîtrise d'Ouvrage communiquera tous les éléments nécessaires au paramétrage et à la mise en service expressément demandé, aux moins 3 semaines à l'avance, pendant la période de réalisation de l'installation.

Le déploiement et la mise en service doit être effectué par du personnel formé et certifié sur la solution déployée. L'entreprise doit le justifier.

2.8 Fonctionnalités complémentaires en option

Les fonctionnalités de la plateforme unifiée de sûreté décrites précédemment sont disponibles pour l'utilisation et la supervision de la centrale intrusion, tel que :

- Les tâches de surveillance
- Les tâches de rapport et d'investigation
- Les tableaux de bords

2.9 Formations

L'entreprise doit impérativement prévoir la formation des personnels administrateurs et utilisateurs du système avec pour objectif, qu'à l'issue de la formation, les personnels des différentes administrations et des différents services soient pleinement opérationnels sur le système.

Le titulaire propose le contenu ainsi que la durée et le nombre de sessions de formations, qui est adapté au nombre de participants dans chaque domaine.

2.10 Déploiement et mise en service

Le paramétrage de l'installation doit être réalisé par l'entreprise titulaire du présent lot en coordination avec les utilisateurs afin de livrer un ensemble en ordre de marche.

La Maîtrise d'Ouvrage communiquera tous les éléments nécessaires au paramétrage et à la mise en service expressément demandé, aux moins 3 semaines à l'avance, pendant la période de réalisation de l'installation.

3 SYSTEME DE VIDÉOPROTECTION OMNICAST

3.1 Principe de base

Afin de surveiller les volumes intérieurs et de la périphérie des bâtiments, la maîtrise d'ouvrage d'une installation comprenant :

Des caméras IP (voir marque dans l'annexe)

Des caméras analogiques en turbo HD (voir marque dans l'annexe)

Ces caméras sont réparties en partie sur Genetec en sa version 5.10 et la seconde partie est intégré dans uns VMS déployés sur petit serveurs de marque Windows avec l'utilisation du VMS VPRO de la société Videoconsult.

Le titulaire du lot devra prévoir la récupération de l'ensemble de caméras sur la plateforme unifiée de Genetec en s'assurant des points suivants :

La compatibilité de celle-ci avec une parfaite intégration sur le Security center avec la version actuelle,

La disponibilité du stockage nécessaires a cette migration,

La parfaite intégration du matériel avec une architecture totalement en IP

La parfaite adéquation des ressources informatique nécessaires à la réalisation.

Ce système de vidéoprotection managé sur IP, permettant de :

- Visualiser en temps réel les événements et mouvements dans les bâtiments, aux abords extérieurs des bâtiments et du périmètre du site,
- Contrôler visuellement les divers événements qui de produisent sur site,
- Rechercher en investigation les vidéos en cas de besoin,
- Alerter en générant des alarmes sur des vidéos anormales.

Des terminaux de visualisation sur IP associés à une centralisation, sont mis en place de manière stratégique sur le site, afin de pouvoir disposer des vidéos nécessaires à la protection des zones sensibles ou à la simple levée de doute visuelle. La centralisation permet le management et les enregistrements de tous les flux vidéo, et permet une supervision en temps réel de la vidéoprotection selon les besoins des exploitants.

3.1.1 Pérennité et évolutivité

La solution de vidéoprotection **Omnicast** est une fonction de la plateforme unifiée de sureté **Genetec Security Center**. Aucun logiciel complémentaire ne sera accepté.

La version choisie dispose parmi une gamme de versions évolutives de logiciel, permet de répondre aux besoins exprimés.

Les terminaux de visualisation gérés sur le réseau IP, sont définis comme les éléments de prise de vue générant un flux vidéo. Ils sont choisis parmi les standards reconnus du marché avec des drivers ouverts à l'intégration de toutes les fonctionnalités selon les caractéristiques décrites, et sont soumis à validation de la maîtrise d'œuvre, afin que la maîtrise d'ouvrage reste libre des approvisionnements et de la maintenance.

La maîtrise d'œuvre souhaite recommander un choix de matériel réseau et caméra, issu de fabricants de confiance hors polémique, afin de garantir à la maîtrise d'ouvrage l'intégrité des données. Il peut être demandé au titulaire de varier les marques proposées.

3.1.2 Le rôle de l'archiviste

C'est le rôle responsable de la découverte, la vérification d'état et le contrôle des unités vidéo. L'Archiveur gère également l'archivage vidéo, et effectue la détection de mouvement si elle n'est pas réalisée la caméra elle-même. Toutes les communications entre le système et les unités vidéo sont établies par le biais de ce rôle. Tous les événements générés par les unités (mouvement, analyse vidéo, etc.) sont transmis par l'Archiveur aux utilisateurs concernés. Plusieurs instances du rôle Archiveur peuvent être créées au sein du système, à définir par l'entreprise.

3.1.3 Haute disponibilité et maintien en condition opérationnelle

L'application centrale de vidéoprotection doit s'organiser sur une architecture logique comprenant la base, la gestion des enregistrements, et les enregistreurs avec stockage. Pour disposer d'une redondance dans le cadre du projet, la solution retenue dispose nativement d'un mécanisme de redondance intégré, sans aucune application tierce.

La redondance souhaitée correspond à la mise en place d'enregistrement sur deux salles. Pour éviter un aspect trop coûteux de la redondance, il est prévu un enregistrement principal pleine résolution, et un enregistrement secondaire réduit.

3.2 Fonctionnalités

Ces différentes fonctionnalités sont disponibles pour les exploitants ou les administrateurs dans le GCT ou le GSC. En fonction des privilèges, ils ont plus ou moins d'autorisation à l'utilisation. Lorsqu'une fonction n'est pas disponible pour un opérateur, il ne peut tout simplement pas la voir afin d'épurer l'interface.

3.2.1 Communication et réseau

Afin de pouvoir optimiser la communication et le réseau, la solution de vidéoprotection s'articule autour d'une technologie unicast et multicast complète. Le multicast permettant d'envoyer un flux vidéo temps réel unique simultanément vers plusieurs clients tout en optimisant la charge du serveur et la bande passante. Il n'est pas prévu un déploiement multicast, mais la solution doit être capable de le proposer par un ajustement de la configuration et un ajustement réseau.

Pour sécuriser les échanges de données entre les différents composants de la solution, il est prévu un cryptage AES 256-bits de toutes les communications entre les serveurs et les clients. Également, les flux avec les caméras (images, administration) doivent être chiffrés et authentifiés par des protocoles tels que TLS (Transport Layer Security) supporté par de nombreuses caméras.

La maîtrise d'ouvrage désire rester libre de ces choix de caméras, et souhaite également pouvoir bénéficier des dernières nouveautés. Pour cela, la solution intègre nativement un maximum de drivers de caméras tel que Axis, Bosch, Hanwha, Mobotix, Panasonic, Sony, Vivotek et d'autres... La solution doit être également capable d'utiliser des drivers standards de type Onvif, pour une ouverture maximum de la solution.

Il est toujours privilégié l'intégration native du driver de la caméra plutôt que l'Onvif.

3.2.2 Enregistrement et détection d'activité

La sensibilité du site nécessite la garantie d'obtenir les images à n'importe quel moment de la journée. L'activité étant moins forte mais plus sensible la nuit, la maîtrise d'ouvrage souhaite mettre en place un enregistrement permanent. Il est prévu un enregistrement 24h/24, 7j/7, et ce pendant 30 jours. L'entreprise doit fournir son calcul de stockage et bande passant complet, et détaillé, en justifiant la correspondance avec les prérequis de l'éditeur.

Aucune détection d'activité n'est prévue coté serveur ou coté caméra, cependant, certaines caméras nécessiteront le paramétrage de masquage dynamique pour éviter d'enregistrer des zones non autorisées. L'entreprise doit prévoir tous ces paramétrages.

3.2.3 Rapport d'archive vidéo

Un outil dynamique d'aide à l'investigation doit être à disposition des exploitants de la vidéoprotection. Il a pour but de permettre en un temps réduit, de pouvoir retrouver des séquences vidéo sur une longue période d'enregistrement, à l'aide de rapport d'archives vidéo. Il permet de rechercher les séquences vidéo archivées lors d'une période donnée ou par une caméra à une date particulière. Lorsqu'un incident de sécurité important survient, il sert à effectuer une recherche dans les archives vidéo pour étudier les enregistrements, puis les partager avec des collègues ou les forces de l'ordre.

3.2.4 Recherche en direct

Une frise chronologique dynamique incrustée dans l'image de chaque caméra, donne une vue d'ensemble claire, des enregistrements sur une durée ajustable. Elle permet une navigation rapide et intuitive par simple cliquer-glisser, comme une lecture avant ou arrière à différentes vitesses, sur les enregistrements. Une fonction peut être utilisée pour revoir simultanément des images vidéo de plusieurs caméras synchronisées. Il est possible de créer directement des marqueurs sur cette frise de temps.

3.2.5 Recherche rapide

L'outil recherche rapide permet aux exploitants de facilement et rapidement, accéder à la séquence vidéo d'un incident, par la génération automatique de vidéo miniature à intervalles égaux d'une caméra. Une fois l'incident visible sur une bande miniature, l'exploitant peut affiner ses intervalles de temps jusqu'à obtenir une séquence de l'exact moment où commence et se termine l'incident. Si vous savez quelle caméra a enregistré un événement et où l'événement a eu lieu (comme lorsqu'un sac a été retiré d'une table), vous pouvez utiliser la Recherche rapide de la tâche Surveillance pour retrouver la séquence vidéo précise qui contient l'événement, très rapidement.

3.2.6 Filature visuelle

La filature visuelle permet de suivre un individu en mode vidéo en direct ou enregistrée entre les diverses caméras de votre installation. Cette fonction est très importante car elle offre un gain de temps et simplifie les tâches de surveillance et d'enquête. Grâce à celle-ci, il est facile de suivre une personne rapidement sans perdre de temps à rechercher la caméra pertinente. Il n'est pas nécessaire de connaître les caméras pour les enchaîner, car elles sont toutes liées entre elles. L'association de caméras permet de former rapidement de nouveaux opérateurs, et réduit le stress de l'opérateur lors de situations à haut niveau d'alerte.

3.2.7 Fonction de mur d'images

L'exploitation en temps réel pour un nombre important de caméras peut s'avérer peu pratique pour les exploitants. C'est pourquoi le logiciel de vidéoprotection intègre nativement, sans ajout de licences complémentaires et sans remettre en cause la solution déployée, la gestion de multiples murs d'images, d'un nombre illimité de caméras et de moniteurs. Il est doté d'une interface graphique avec une représentation virtuelle des écrans, depuis n'importe quel poste client. Véritable outil d'exploitation en temps réel, les vidéos y sont diffusées instantanément de 4 à 16 flux maximum par écran suivant la taille, pour garder un visuel correct. La configuration du mur d'images est modifiable en permanence sans quitter l'exploitation. Il offre de nombreuses fonctionnalités :

- Affichage de tous types de caméras
- Affichage de tous types de vues complètes
- Affichage de moniteurs d'alarme
- Prise de contrôle d'une caméra en temps réel
- Direct investigation sur des caméras affichées

- Gestion graphique et représentation virtuelle des écrans
- Fonction glisser-déposer ou sélection pour affichage

La fonction mur d'images est indispensable pour le pilotage dynamique des écrans du PCS depuis un poste d'exploitation (GSC). Chaque exploitant doit pouvoir piloter et prendre en main le mur d'image comme une extension de son propre poste de travail.

3.2.8 Exports vidéo et marqueurs

L'export des preuves peut se faire sous différentes formes : vidéo simple ou multiple, au format avi ou base de données, capture d'image jpeg ou rapport imprimable, et sur différents supports : CD, DVD, clé USB, disque dur ou Cloud. Pour cela, l'exploitant doit uniquement définir un point de début et de fin dans le temps, directement depuis l'interface d'investigation. Il est ensuite proposé les différentes possibilités par une fenêtre adaptée avec menu déroulant.

Un logiciel de visualisation des vidéos au format base de données protégé doit être disponible pour la mise à disposition aux autorités en cas de fourniture de preuves vidéo.

Une fonctionnalité de marqueurs correspond simplement à la mise en place de marque page permettant de retrouver facilement les séquences vidéo d'incident dans le rapport de recherche. Il est possible de créer des marqueurs personnalisés pour guider l'exploitant dans sa classification d'incident.

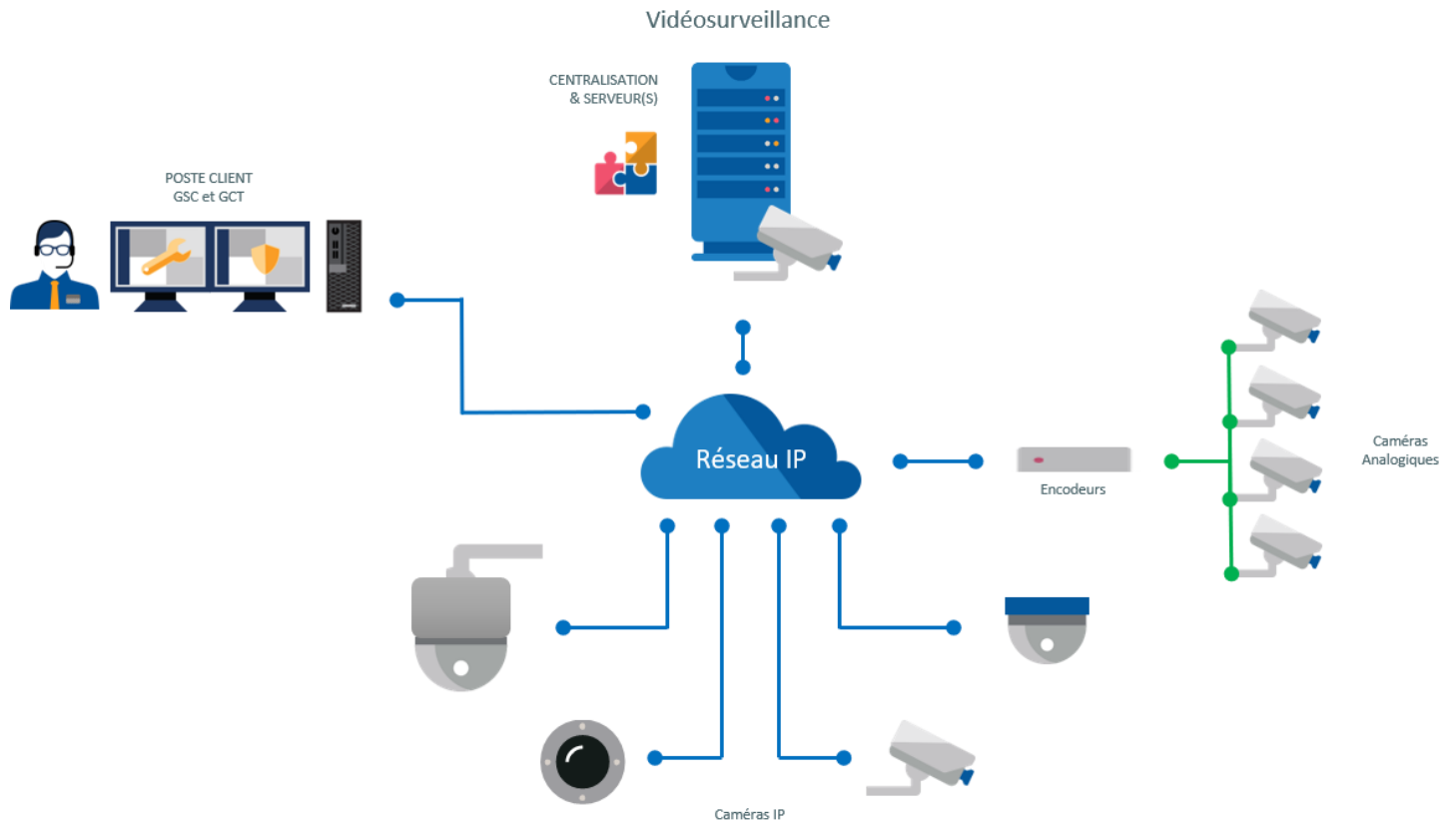
3.2.9 Protection contre le piratage des images

Pour lutter contre les smartphones qui filment les écrans de vidéosurveillance, le système est capable de mettre en place un tatouage vidéo selon le profil connecté au GSC. Le tatouage vidéo superpose du texte visible sur la vidéo en direct, enregistrée ou exportée traitée par Security Center. Ce texte comprend des informations d'identification de l'exploitant, destinées à dissuader les utilisateurs non autorisés de pirater les enregistrements vidéo. Le tatouage vidéo est incrusté sur la vidéo en direct et enregistrée. Ces incrustations statiques ne sont pas redessinées lors du zoom numérique ou du redressement de l'image.

3.3 Architecture de la solution de Vidéoprotection

La structure de la solution de vidéoprotection **Omnicast** s'organise donc selon deux niveaux :

- La gestion et centralisation : Serveurs, Applications, stockage, Clients.
- Les terminaux : Caméras, encodeurs, modules d'entrées sorties.



3.4 Descriptions Techniques

3.4.1 Gestion et centralisation

Dans le cadre de ce projet, l'intégralité du matériel informatique est à la charge du titulaire du lot, les serveurs d'enregistrement doivent parfaitement s'intégrer dans l'environnement actuel pour le bon fonctionnement de la solution. L'entreprise mandataire doit la mise en service de la solution, ainsi que tout le paramétrage associé sur les serveurs.

L'entreprise doit fournir les archiveurs selon les prérequis de l'éditeur, en termes de performances, mais également en préparation et paramétrage, afin de garantir un fonctionnement adéquat. Ils sont impérativement tous issus d'un unique fabricant reconnu, selon les standards du marché et non propriétaire, afin de simplifier la maintenance du parc informatique homogène.

- Pour le (ou les) serveur(s) d'enregistrement (Archiveur):
 - Processeur : Intel Xeon Xeon Silver 4210 - 10C/20T - 3,2 GHz turbo - 13,75MB Cache
 - Mémoire : 32 ou 64 GB
 - Stockage / Raid : 2x 240Go SSD M2 + n x 4-8-12-16 To SATA 7.2k / Raid1+Raid6
 - n correspond au nombre de HDD nécessaires selon la capacité calculée de stockage.
 - Graphique : Graphique intégré
 - Réseau : 2x Ports 1 Gbit/s et 2x Ports 10 Gbit/s SFP+
 - Alimentation : Double blocs d'alimentation 1100W
 - Système d'Exploitation : Microsoft Windows Server 2012 R2
 - Serveur Streamvault Dell R740xd optimisé et préparé par l'éditeur

3.4.2 Enregistrement vidéo principal

Dans le cadre de ce projet, l'entreprise doit fournir le (ou les) archiveur(s) vidéo et doit mettre à disposition le stockage nécessaire.

Afin que l'enregistrement principale du système de vidéoprotection soit capable d'enregistrer les flux vidéo pendant la durée de 30 jours définie par le maître d'ouvrage, les données utilisées pour le calcul de stockage à justifier, sont les suivantes :

- Durée : 30 jours
- Fréquence d'images : 25 Images par seconde
- Compression : H264
- Résolution : HD1080p 1920x1080p
- Qualité d'images : Haute
- Pourcentage d'enregistrement : 100%
- Complexité des images et mouvements : Aux dessus de la normale

Le prestataire doit alors donner la quantité exacte de stockage Brut et Net prévu avec la sécurisation RAID6 minimum, afin de garantir au maître d'ouvrage la conformité au besoin et le bon fonctionnement de la vidéosurveillance. Il en est de même pour la capacité et le nombre de serveurs nécessaires.

3.4.3 L'infrastructure réseau

Dans le cadre de ce projet, l'intégralité du matériel informatique est à la charge du titulaire du lot. L'entreprise mandataire doit la mise en service de la solution, ainsi que tout le paramétrage associé au réseau pour la solution déployée.

L'ensemble de la solution s'articulant autour du réseau IP, il doit être adaptés aux prérequis informatiques de l'éditeur, en termes de performances, mais également en préparation, afin de garantir un fonctionnement adéquat.

3.4.4 Les terminaux

Les terminaux de visualisation gérés sur le réseau IP, sont définis comme les éléments de prise de vue générant un flux vidéo. Ils comprennent le plus souvent des caméras fixes et mobiles, IP ou analogiques, des encodeurs et des modules d'entrées sorties. Dans un souci d'évolutivité et de compatibilité, les terminaux choisis sont multi-protocole et multi-flux, permettant l'évolutivité de la solution envisagée.

Caméra Mini Dôme / Tube fixe Anti vandale intérieur – extérieur

- Type mini dôme / tube fixe Anti Vandale
- IP66 et IK10 pour l'extérieur
- IR LED 30m
- Réseau Ethernet 10/100 Base-T
- Capteur 1/3"
- Résolution 1920x1080 (Full HD) à 25ips
- Objectif Vari-focal, 2.8 - 12 mm
- Encodeur H 264
- POE Class IEEE802.3af
- Fonction jour / nuit automatique
- Support mural possible

Caméra Multidirectionnelles Anti vandale intérieur – extérieur

- Type multidirectionnelle 2 ou 4 caméras (180° ou 360°)
- IP66 et IK10 pour l'extérieur
- IR LED 15m
- Réseau Ethernet 10/100 Base-T
- Capteur 1/3"
- Résolution 1920x1080 (Full HD) à 25ips
- Objectif Vari-focal, 3 - 6 mm
- Encodeur H 264
- POE Class IEEE802.3at
- Fonction jour / nuit automatique
- Support mural possible

3.5 Formations

L'entreprise doit impérativement prévoir la formation des personnels administrateurs et utilisateurs du système avec pour objectif, qu'à l'issue de la formation, les personnels des différentes administrations et des différents services soient pleinement opérationnels sur le système **Omnicast**.

Le titulaire propose le contenu ainsi que la durée et le nombre de sessions de formations, qui est adapté au nombre de participants dans chaque domaine.

3.6 Déploiement et mise en service

Le paramétrage de l'installation doit être réalisé par l'entreprise titulaire du présent lot en coordination avec les utilisateurs afin de livrer un ensemble en ordre de marche.

Le Maître d'Ouvrage communiquera tous les éléments nécessaires au paramétrage et à la mise en service expressément demandé, aux moins 3 semaines à l'avance, pendant la période de réalisation de l'installation.

Le déploiement et la mise en service doit être effectué par du personnel formé et certifié sur la solution déployée. L'entreprise doit le justifier.