

**INSTITUT D'ETUDES POLITIQUES
D'AIX EN PROVENCE
Espace Philippe Séguin**

**Mise en œuvre d'une infrastructure
de sécurisation**

MAITRE D'OUVRAGE

**INSTITUT D'ETUDES POLITIQUES D'AIX-EN-
PROVENCE (SCIENCES PO AIX)**



25 rue Gaston de Saporta
13625 AIX-EN-PROVENCE CEDEX 1
Tél : 04 65 04 70 00

hugues.meri@sciencespo-aix.fr

MAITRE D'ŒUVRE

GROUPE CETAB



61, rue du Professeur Lannelongue
BP 80033
33041 BORDEAUX CEDEX
Tél : 05 57 19 12 00

cetab.bx@cetab.fr

BUREAU DE CONTROLE

QUALICONSLT



Domaine de l'Escapade
Bâtiment E
203 avenue Paul Jullien (DN7N)
13100 LE THOLONET
Tél : 04 42 37 09 80

**CCTP
Lot « Sécurisation »**

PHASE : DCE	Date : Septembre 2024	Affaire n°2231	Rédaction : FMo/VM	Indice			
				A	B	C	D
				E	F	G	H
Date	Indice	Modifications					
01/12/2024	A	Modifications suite à relance marché					
16/12/2024	B	Modifications suite aux remarques MOA					

SOMMAIRE

1 - CADRE DU PROJET	4
1.1 - PRESENTATION DU PROJET	4
1.2 - PRESENTATION DU SITE	4
1.2.1 - Généralité	4
1.2.2 - Effectif du site	5
1.3 - ASPECTS REGLEMENTAIRES & LEGISLATIFS - VIDEOPROTECTION	6
1.3.1 - Lois applicables	6
1.3.2 - Règles CNIL	6
1.4 - REGLES TECHNIQUES – VIDEOPROTECTION	8
1.4.2 - Normes	10
1.5 - INFORMATION DES PERSONNES	12
1.6 - ASPECTS REGLEMENTAIRES & LEGISLATIFS – CONTROLE D'ACCES	12
1.6.1 - Niveau de sûreté et types de menaces	12
1.6.2 - Choix du système	14
2 - ORGANISATION ET PLANIFICATION	17
2.1 - VISITE DES LIEUX	17
2.2 - PLANNING	17
2.3 - RENDEZ-VOUS DE CHANTIER	17
2.4 - SECURITE DU CHANTIER ET NETTOYAGE + BASE VIE	17
2.5 - QUALIFICATIONS	18
2.6 - ETUDES D'EXECUTION	18
2.7 - CONTRAINTES PARTICULIERES LIEES AUX TRAVAUX EN MILIEU OCCUPE	18
2.7.1 - Travaux en milieu occupé	18
2.7.2 - Maintien en service des bâtiments existants	19
2.7.3 - Déroulement des opérations	19
2.7.4 - Pénétration dans les bâtiments occupés	19
2.7.5 - Déplacement de mobilier - Protection	19
2.7.6 - Approvisionnement des matériaux	19
2.7.7 - Protection contre le bruit et la poussière	20
2.7.8 - Sécurité des tiers	20
2.8 - RECEPTION ET CONTROLE DES INSTALLATIONS	20
2.9 - DOE	20
2.9.1 - Plans	20
2.9.2 - Notices d'entretien	21
2.9.3 - Fiches techniques et références des matériels	21
2.9.4 - Liste des matériaux et équipements mise en œuvre	21
2.9.5 - Nombre d'exemplaires	21
2.10 - DECOMPOSITION DES PRIX FORFAITAIRES	22
2.11 - FORMATION DU PERSONNEL	22
2.12 - AFFICHAGE REGLEMENTAIRE	22
2.13 - GARANTIE	22
3 - DESCRIPTIF DES PRESTATIONS	24
3.1 - PRESENTATION GENERALE	24

3.1.1 - Plan de sécurisation de principe	24
3.1.2 - Sécurisation des accès périmétriques piétons	25
3.1.3 - Sécurisation de l'accès véhicules – AS3	26
3.1.4 - Compartimentage des entités IEP et CAEC	27
3.1.5 - SépAration de la zone jardin partagée et IEP	28
3.1.6 - Implantations.....	28
3.2 - TERRASSEMENT	29
3.2.1 - Démolition	29
3.2.2 - Terrassement de la terre végétale.....	29
3.2.3 - Terrassements généraux.....	30
3.2.4 - Protection équipement existant.....	31
3.3 - TRAVAUX DE GENIE CIVIL	31
3.4 - CARACTERISTIQUES DES TRANCHEES.....	32
3.5 - REMBLAIS	32
3.6 - DESCRIPTION DES TRAVAUX.....	32
3.6.1 - VRD	33
3.6.2 - Tranchée.....	33
3.6.3 - Fourreaux.....	33
3.6.4 - Dispositif avertisseur.....	33
3.6.5 - Chambre de tirage.....	33
3.7 - RESEAU DE SURETE.....	34
3.7.1 - Objectif général.....	34
3.7.2 - Création des points d'accès réseau <90ml.....	35
3.7.3 - Caractérisitiques techniques des matériels réseau.....	35
3.7.4 - Implantations RG et SR (suivant plans).....	40
3.8 - VIDEOPROTECTION	40
3.8.1 - Objectifs généraux.....	40
3.8.2 - Technologie	41
3.8.3 - Généralités cybersécurité des caméras	42
3.8.4 - Caractéristiques techniques minimales des caméras	43
3.8.5 - Visualisation et traitement des images	50
3.8.6 - Caractéristiques fonctionnelles du poste d'exploitation.....	50
3.8.7 - Station de travail (Gestion des d'images).....	51
3.8.8 - Dispositifs d'identification des images	52
3.8.9 - Affichettes de signalisation.....	52
3.9 - CONTROLE D'ACCES	52
3.9.1 - Descriptif des matériels.....	53
3.9.2 - Pincipe de câblage d'une porte de contrôle d'accès	55
3.10 - VISIOPHONIE	57
3.10.1 - Descriptif.....	58
3.11 - PROTECTION MECANIQUE.....	60
3.11.1 - Portillon automatique.....	60
3.11.2 - Barrière automatique AS3	60
3.11.3 - Panneaux grillage à mailles rigides.	61
3.11.4 - Potelet VL.....	61

1 - CADRE DU PROJET

1.1 - PRÉSENTATION DU PROJET

Depuis 2016, l'Institut d'Études Politiques d'Aix en Provence (IEP), s'est engagé dans un ambitieux projet de modernisation des infrastructures de sécurité de ses bâtiments. Ce programme pluriannuel vise à renforcer la protection électronique de ses installations, notamment en matière de séparation de flux (contrôle d'accès et visiophonie) et de vidéoprotection.

À ce jour, deux des trois sites principaux de l'IEP d'Aix-en-Provence ont déjà bénéficié de ces améliorations : le site de Saporta et celui de l'Espace Marceau Long.

L'espace Philippe Séguin (EPS) représente le troisième site à traiter dans ce contexte.

Le présent projet prend donc en compte la mise à niveau de la sûreté et des équipements :

- La mise en sûreté des accès périmétriques du site.
- La séparation des flux dans l'enceinte du site.
- La séparation de la zone « jardin partagé ».

1.2 - PRÉSENTATION DU SITE

1.2.1 - GÉNÉRALITÉ

L'IEP d'Aix-en-Provence, également appelé « Sciences Po Aix », est un établissement public français d'enseignement supérieur fondé en 1956, situé à Aix-en-Provence dans le département français des Bouches-du-Rhône en région Provence-Alpes-Côte d'Azur.

C'est l'un des dix Instituts d'Études Politiques de France et il fait à ce titre partie des grandes écoles. Il est depuis mars 2018 l'un des huit Instituts d'Études Politiques à faire partie de la Conférence des grandes écoles.

L'école occupe trois espaces distincts :

- Le siège historique de l'école, installé dans un hôtel particulier du XVIII^e siècle, rue Gaston de Saporta.
- L'espace Marceau Long accueille des salles de cours et des bureaux administratifs.

Depuis 2009, l'IEP occupe en plus de son siège historique de nouveaux locaux dans l'ancien hospice des Petites Sœurs des Pauvres, avenue Jean-Dalmas.

Cette extension permet à l'école de disposer de nouvelles salles de cours, de bureaux ainsi que d'une bibliothèque installée dans une ancienne chapelle. En mai 2016, après des rénovations, l'extension sera renommée l'Espace Philippe Séguin pour faire partie intégrante de l'Institut.

La mission d'audit concerne l'Espace Philippe Séguin. Le site est occupé par deux autres entités :

- Le CAEC : centre d'examen et de concours, géré par le Rectorat de l'académie d'Aix-Marseille.
- Le CROUS : Centre régional des œuvres universitaires et scolaires, qui assure le service des repas.

Le site dispose d'un parking en interne. Le site est situé dans une zone urbaine, il est desservi par plusieurs lignes de bus.

Délimitation du périmètre du site.



1.2.2 - EFFECTIF DU SITE

Agents du Ministère de l'Éducation Nationale et du Ministère de l'Enseignement Supérieur et de la Recherche

- Institut d'Études Politiques - de 7h30 à 20h30 - 25 max.
- CAEC - de 7h30 à 19h30 - nombre d'agents différent entre 2 et 45 (en fonction des sessions d'examens, concours organisés sur le site.).
- CROUS – 1 à 2 personnes

Étudiants

- Institut d'Études Politiques – de 8h00 à 19h30 - 250 max.
- CAEC – de 8h à 20h30 - jusqu'à 1200 max pour les épreuves les plus importantes.

Visiteurs (sur invitation)

- De 8h30 à 18h30

1.3 - ASPECTS RÉGLEMENTAIRES & LÉGISLATIFS - VIDÉOPROTECTION

1.3.1 - LOIS APPLICABLES

L'article 9 du Code Civil : « Droit au respect de la vie privée ».

Loi Informatique et liberté du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiées par la loi du 6 août 2004.

Loi n° 95-73 du 21 Janvier 1995 « Article 10 de la LOPS » déclaration préalable à l'installation auprès d'une commission préfectorale :

- Circulaire du 14 septembre 2011 relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part.

Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) qui concerne de la police et de la gendarmerie nationale.

L'arrêté du 6 mars 2009 qui fixe les conditions de certification des installateurs de vidéoprotection.

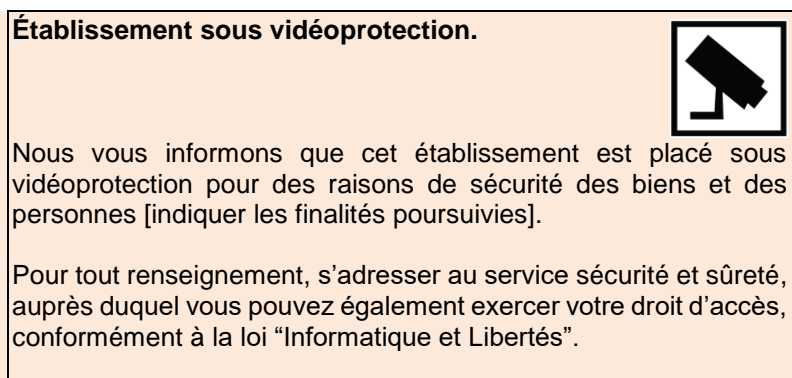
1.3.2 - RÈGLES CNIL

Pour respecter les exigences de la CNIL, toutes les garanties doivent être mises en œuvre :

- Une réflexion préalable indispensable.
- Le nécessaire respect du principe de proportionnalité.
- L'obligation d'information.
- L'élaboration d'un document de référence.
- Une visualisation des images restreinte aux seuls destinataires habilités.
- Une durée de conservation des images limitée.
- Et bien sûr, la déclaration auprès de la CNIL.

	Lieu ouvert au public	Lieu non ouvert au public
Sans enregistrement d'images numériques	Autorisation préfectorale	Aucune démarche
Avec enregistrement d'images numériques	Autorisation préfectorale	Déclaration normale auprès de la CNIL
Avec alimentation d'un fichier	Déclaration normale auprès de la CNIL	Déclaration normale auprès de la CNIL
Avec constitution d'un fichier d'infraction	Autorisation auprès de la CNIL	Autorisation auprès de la CNIL
Avec reconnaissance faciale ou analyse comportementale	Autorisation auprès de la CNIL	Autorisation auprès de la CNIL

Exemple d'affichage à mettre en place :



À la suite de la déclaration CNIL du système, vous pourrez informer les services de l'Etat et mettre à disposition les images.

L'accès aux données est possible non seulement en cas de procédure judiciaire par la voie de la réquisition d'un officier de police judiciaire, mais également, dans le cadre de la police administrative, dès lors que l'autorisation préfectorale désigne les services habilités ou que le chef du service de la police ou le commandant de gendarmerie procède à cette désignation sous la forme d'une habilitation individuelle.

C'est d'ailleurs pour que ce droit d'accès des services de police et gendarmerie ait une portée concrète que des normes techniques imposent une qualité minimum des images. Cette disposition résultant de l'arrêté du 3 août 2007 s'applique pour les systèmes déjà autorisés à partir du 22 août 2009 et immédiatement pour les nouvelles déclarations.

1.3.2.1 - CONFORMITÉ DES ENREGISTREURS NUMÉRIQUES PAR RAPPORT AU CSI

Le système d'enregistrement numérique des images devra être parfaitement conforme aux dispositions du Code de la Sécurité Intérieure, portant définition des normes techniques des systèmes de vidéoprotection, et en particulier, présentera les fonctionnalités suivantes :

- Tout flux vidéo enregistré numériquement est stocké avec des informations permettant de déterminer à tout moment de la séquence vidéo sa date, son heure et l'emplacement de la caméra.
- L'enregistrement numérique garantit l'intégrité des flux vidéo et des données associées relatives à la date, à l'heure et à l'emplacement de la caméra.
- Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo. Pour les systèmes numériques, ce journal est généré automatiquement sous forme électronique.
- Un journal électronique des exportations, indiquant la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation, est généré automatiquement.
- Le système d'enregistrement reste en fonctionnement lors de ces opérations d'exportation.
- Le support physique d'exportation est un support numérique non réinscriptible et à accès direct, compatible avec le volume de données à exporter. Dans le cas de volumes importants de données à exporter, des disques durs utilisant une connectique standard pourront être utilisés. Pour les systèmes numériques de vidéosurveillance, un logiciel permettant l'exploitation des images est fourni sur support numérique, disjoint du support des données.

Le logiciel doit permettre :

- La lecture des flux vidéo sans dégradation de la qualité de l'image.
- La lecture des flux vidéo en accéléré, en arrière, au ralenti.

- La lecture image par image des flux vidéo, l'arrêt sur une image, la sauvegarde d'une image et d'une séquence, dans un format standard sans perte d'information.
- L'affichage sur l'écran de l'identifiant de la caméra, de la date et de l'heure de l'enregistrement.
- La recherche par caméra, date et heure.

1.4 - RÈGLES TECHNIQUES – VIDEOPROTECTION

Sur la base des recommandations de l'ANSSI.

Analyse succincte des menaces

Les risques liés à l'exploitation d'éventuelles vulnérabilités dans les dispositifs de vidéoprotection relèvent pour l'essentiel des trois catégories suivantes :

Atteinte à la confidentialité des données de vidéoprotection

Les flux vidéo et éventuellement audio captés par les caméras peuvent être interceptés, par écoute passive sur le réseau support ou interception de rayonnements parasites compromettants. La sensibilité des flux qui sont susceptibles d'être interceptés dépend naturellement du positionnement des caméras à l'intérieur ou à l'extérieur des locaux qu'elles contribuent à protéger.

Atteinte à la disponibilité de la vidéoprotection

L'exploitation de vulnérabilités logiques dans les différents équipements actifs du réseau de vidéoprotection (caméras, équipements de routage, serveurs de collecte) peut permettre à un attaquant de désactiver tout ou partie du dispositif. Une attaque de ce type peut par ailleurs être dissimulée par l'injection de flux vidéo illégitimes créés par l'attaquant ou le rejeu de flux légitimes antérieurs.

Intrusion dans le reste du système d'information

Lorsque le réseau support des équipements de vidéoprotection est mutualisé avec le système d'information de l'entité utilisatrice (réseau bureautique, serveurs internes ou externes), la prise de contrôle d'un équipement de vidéoprotection par un attaquant peut permettre à ce dernier de mener dans un second temps une intrusion plus générale au sein du système d'information. Ce risque est d'autant plus significatif que, de par la nature même de leur fonction, les caméras de vidéoprotection sont souvent plus exposées à des attaques physiques que les autres équipements du système d'information (caméras déployées à l'extérieur des bâtiments, ou dans des zones peu fréquentées).

Architecture du réseau support

Afin de contrer les risques d'intrusion au sein du système d'information et de limiter les possibilités d'atteinte généralisée à l'ensemble du dispositif de vidéoprotection, il est primordial d'isoler le réseau de support associé, et de mettre en œuvre un cloisonnement adapté au sein de ce dernier. Ce principe d'isolation et de cloisonnement se décline selon plusieurs modalités pratiques :

- **Une connectivité filaire est requise pour les équipements de vidéoprotection.**
 - En effet, bien que certaines caméras récentes offrent la possibilité de communiquer via différents modes sans fil (principalement le wifi ou la téléphonie 3G), l'activation de ces fonctionnalités accroît considérablement la vulnérabilité des équipements face aux attaques logiques. Il est donc impératif que les caméras soient connectées par câble. Si les équipements sont dotés de fonctionnalités sans fil, celles-ci doivent être désactivées, documentées et assorties d'un mot de passe administrateur spécifique.
- **Le dispositif de vidéoprotection ne doit pas être directement accessible depuis Internet.**
 - En particulier, les éventuelles interfaces d'administration des équipements ne doivent pas être accessibles depuis Internet.

- **Il est recommandé, lorsque cela est possible, d'isoler entre eux les réseaux de vidéoprotection interne et externe.**
 - Lorsque des caméras sont positionnées aussi bien à l'intérieur des bâtiments protégés que dans leur périmètre extérieur. En effet, les caméras extérieures sont naturellement plus exposées, et une action malveillante sur celles-ci ne doit pas permettre de porter atteinte à la confidentialité des flux intérieurs. Lorsque cela est possible, l'emploi d'équipements différents au sein des deux dispositifs de vidéoprotection apporte une sécurité supplémentaire, en limitant les risques de voir une même vulnérabilité exploitée sur les deux réseaux.
- **Un fort cloisonnement logique doit être établi au sein du réseau.**
 - Chaque site doit être pourvu d'un VLAN Vidéo dédié. Ce VLAN sera attribué aux caméras, au contrôleur du site, ainsi qu'à tout équipement IP dédié à la vidéo.
- **Il est souhaitable de contrôler les accès directs au réseau support.**
 - La prévention des accès illégitimes doit s'appuyer sur un contrôle des points d'accès physiques, en évitant de laisser les apparents et accessibles des ports d'accès au réseau.

Choix et configuration des équipements de vidéoprotection

Les considérations de sécurité doivent également intervenir dans le choix des capteurs de vidéoprotection, ainsi que dans la configuration de ces équipements. Il est rappelé ici que les modèles récents de caméras IP s'apparentent très largement, en dépit d'un facteur de forme différent, à des ordinateurs classiques, aussi bien au niveau du matériel lui-même (microprocesseurs usuels, connectivité standard de type USB ou port série, etc.) que des composants logiciels qu'il exécute (système d'exploitation de type Linux, serveur web ou console d'accès distant, etc.). A ce titre, les recommandations de sécurité portant sur ces équipements rejoignent largement celles qui sont plus généralement conseillées pour des matériels informatiques de type PC. On retiendra plus particulièrement les mesures suivantes :

- **Les flux réseau émis et reçus par les équipements doivent autant que possible être chiffrés et authentifiés, avec un protocole cryptographique interdisant le replay de flux antérieurs.**
 - Cette mesure doit porter aussi bien sur les flux de remontée vidéo que sur les connexions d'administration distante des caméras. De nombreux modèles, de caméras IP, supportent des options de protection cryptographique des flux réseau, mais il est en général nécessaire de les activer spécifiquement dans la configuration des équipements. Il est par ailleurs souhaitable de privilégier dans ce cadre des protocoles cryptographiques génériques et éprouvés, comme TLS ou IP sec, plutôt que des protocoles propriétaires spécifiques à un type d'équipement, dont il est difficile de vérifier la robustesse a priori.
- **On veillera à désactiver, si cela est possible, les interfaces locales d'administration des équipements déployés, lorsque de telles interfaces existent.**
 - Il est notamment courant que les caméras IP proposent une administration par port série, avec ou sans authentification. Si de telles interfaces trouvent toute leur utilité dans la configuration initiale des équipements, il est en revanche souhaitable, au regard des possibilités d'accès physique que pourrait avoir un attaquant, de les désactiver logiquement lors du déploiement effectif des capteurs.
- **De manière générale, il est recommandé de désactiver les fonctions et interfaces d'administration qui ne sont pas réellement utilisées dans le cadre du déploiement considéré.**
 - Il est en effet courant pour les équipements récents de proposer un ensemble de fonctionnalités avancées (par exemple la réorientation de la caméra) dont la mise en œuvre n'est pas forcément nécessaire dans un cadre donné. Dans ce cas, la désactivation de ces fonctionnalités, lorsqu'elle est possible, réduira d'autant la surface d'attaque des équipements.

En plus des mesures classiques de sécurité physique, le système fera l'objet d'une isolation par rapport au reste du système d'information et **d'une application stricte des règles classiques d'hygiène informatique.**

On veillera ainsi plus particulièrement :

- À l'authentification nominative et sur la base de mécanismes robustes des utilisateurs.
- À l'utilisation d'un réseau dédié à l'administration des équipements, si ceux-ci sont administrés par le réseau.
- À la mise en œuvre d'une politique adaptée de suivi des versions et de mise à jour des composants logiciels.
- Au strict contrôle des branchements de périphériques amovibles.
- Et enfin à la journalisation des opérations, notamment celles portant sur l'administration du parc de caméras et des serveurs de collecte des flux, et au contrôle régulier de ces journaux.

1.4.1.1 - LOPPSI ET VIDÉOPROTECTION (LOI N°2011-267 DU 14 MARS 2011)

L'un des changements majeurs apportés par la LOPPSI est l'attribution de nouvelles compétences de contrôle à la CNIL. Celle-ci dispose dorénavant d'un pouvoir de contrôle de tous les dispositifs de vidéoprotection installés sur le territoire national.

Elle peut également mettre en demeure les responsables de ces systèmes si elle constate des manquements aux obligations qui s'imposent à eux (information du public, respect de la durée de conservation des enregistrements, limitation des destinataires des images, etc.). Elle peut enfin proposer au préfet d'ordonner des mesures de suspension ou de suppression du système contrôlé.

Elle a également prévu un nouveau pouvoir du préfet, qui peut désormais inciter une commune, sous certaines conditions, à s'équiper aux fins de prévention du terrorisme.

Si les caméras filment un lieu **non ouvert au public** (lieux de stockage, réserves, zones dédiées au personnel comme le fournil d'une boulangerie), **aucune formalité auprès de la CNIL** n'est nécessaire. Si l'organisme qui a mis en place des caméras a désigné dans le cadre du RGPD un Délégué à la protection des données (DPO), ce dernier doit être associé à la mise en œuvre des caméras. Si le dispositif doit faire l'objet d'une analyse d'impact (AIPD), le DPO doit y être associé. L'employeur doit inscrire ce dispositif de vidéosurveillance dans le registre des traitements de données qu'il doit tenir.

Fiche CNIL « La vidéosurveillance vidéoprotection au travail »

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf

1.4.2 - NORMES

Les matériels et installations devront être conformes aux normes, règlements et décrets (éditions en vigueur à la date de signature du marché) et respecteront les règles de l'art et les documents ci-après applicables dans leur dernière édition complétée de leurs additifs (cette liste n'est pas limitative).

1.4.2.1 - VIDÉOPROTECTION

Code de la sécurité intérieure (titre V chapitre 1 à 5, article L223-1 à L223-9).

Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Loi n°95-73 du 21 janvier 1995 modifiée - loi d'orientation et de programmation relative à la sécurité. Elle pose les bases du régime juridique de la vidéoprotection de la voie publique et des lieux ou établissements ouverts au public.

Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

Décret n° 2009-86 du 22 janvier 2009 relatif à la vidéosurveillance.

Arrêté du 03 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

Arrêté du 6 mars 2009 fixant les conditions de certification des installateurs de vidéosurveillance.

Circulaire INTD0900057C du 12 mars 2009 relative aux conditions de déploiement des systèmes de vidéoprotection et ses annexes.

Guide méthodologique de la vidéoprotection publié par le Ministère de l'Intérieur sur le site www.interieur.gouv.fr/Videoprotection.

1.4.2.2 - RÉSEAUX ET CÂBLAGE

Norme NF C 12 100 – Protection des travailleurs qui mettent en œuvre des courants électriques.

Norme NF C 13 100 – Post de livraison établi à l'intérieur d'un bâtiment et alimenté par un réseau de distribution public de 2e catégorie.

Norme NF C 13 200 – Installations électriques à haute tension.

Norme NF C 14 100 – Installation de branchement à basse tension.

Norme NF C 15 100 – Installations électriques BT – Règles et additifs.

Norme NF C 17 200 – Installations d'éclairage public.

Norme NF C 32 024 – méthodes d'essais communes pour les matériaux d'isolation et de gainage des câbles électriques.

Norme NF C 32 060 – polyéthylène pour enveloppes isolantes et gaines de câbles de télécommunication.

Norme NF C 32 070 – conducteurs et câbles isolés pour installations (+additif 1 et 2).

Normes NF C 46 020 /21/22 en ce qui concerne la compatibilité et les rayonnements électromagnétiques.

Décret 72-1120 du 14 décembre 1972 en ce qui concerne les attestations de conformité des travaux électriques.

Normes NF EN 50081 et 55022 relatives à l'émission.

Norme NF EN 50082 relative à l'immunité.

Norme EN 55.024 concernant l'immunité aux décharges électrostatiques (CEI 801.2) aux champs électrostatiques (CEI 801.3) aux impulsions à front raides (CEI 801.4) aux parasites (CEI 801.6).

Normes réseau Ethernet : IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.1d Spanning Tree Protocol, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3z, IEEE 802.3x, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.1Q VLAN, IEEE 802.1p QoS Prioritization, 1000Base LX/LH, 1000Base ZX

Configuration Guideline for DiffServ Services Classes.

Norme SNMP v3.

[RFC 3569] - PIM Source Specific Multicast (PIM-SSM).

[RFC 3376] – IGMP v3.

Compatibilité électromagnétique : marquage CE, FCC part 15 Class A (EN 55022 Class A), EN 50082-1, VCCI Class A.

1.5 - INFORMATION DES PERSONNES

Les personnes concernées doivent être informées par un panneau de l'existence du dispositif et des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant.

Cette information sera réalisée par affichage au format A5, sous forme d'autocollant et par panneau métallique d'information à chaque entrée de parking, comportant un **pictogramme de caméra** et reprenant l'ensemble du texte ci-dessous :

Exemple d'affichette A5 à installer :



1.6 - ASPECTS RÉGLEMENTAIRES & LÉGISLATIFS – CONTRÔLE D'ACCES

1.6.1 - NIVEAU DE SÛRETÉ ET TYPES DE MENACES :

Le niveau de sûreté des équipements et des installations de contrôle des accès physiques correspond à un niveau de résistance à l'effraction et à la fraude. Le niveau de sûreté découle directement du type de menaces redouté pour chaque niveau de sensibilité des zones précédemment définies. Ces niveaux de sûreté et types de menaces ont été définis en lien avec le CNPP. Ce même tableau est reproduit dans le référentiel « APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation » :

Menaces potentielles			Niveaux de sûreté
	Quels moyens ?	Quelles connaissances ?	
Franchissement « naturel » d'un point d'accès			
Pénétrations involontaires ou de curieux	Pas de matériel ou matériel basique (marteau léger, téléphone portable...)	Pas de connaissance	I
Franchissement par attaque mécanique et/ou logique « simple »			
Pénétrations préméditées de personnes faiblement équipées	Matériel et méthode obtenus dans le commerce ou sur Internet.	Connaissance basique du système acquise au travers de documents publicitaires ou technico-commerciaux émis par le fabricant ou les distributeurs.	II
Franchissement par attaque mécanique et/ou logique « évoluée »			
Pénétrations préméditées de personnes initiées et équipées.	Matériel ou maquette électronique spécifique facilement réalisable.	Connaissances recueillies à partir de l'examen d'un dispositif.	III
Franchissement par attaque mécanique et/ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées.	Matériel comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.	Connaissances sur la conception et l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant.	IV

Ce tableau ne prend pas en compte l'impact de filtrages réalisés par des moyens humains ou non, tels que de la surveillance humaine ou de la vidéo surveillance 24h/24, et qui sont susceptibles de réduire le besoin de sûreté des équipements et des installations de contrôle des accès physiques nécessaires.

Flux de circulation des individus :

L'analyse des flux de circulation des individus permet de connaître les besoins de chaque point d'accès à contrôler. Il s'agit de répondre aux questions : Qui ? Quand ? Comment ? Combien ?

Il est pour cela utile de définir :

- Les différentes catégories de personnel autorisées (personnel interne, intérimaire, agent de surveillance, prestataires de services, clients, visiteurs, services d'urgences, etc.).
- Les plages horaires.
- Le type de passage à contrôler (simple porte, sas, entrée de véhicules).
- Les exigences de circulation particulières et contraintes spécifiques (sorties de secours).
- La quantité prévisionnelle de passages.

Identification des acteurs :

Les différents acteurs et responsables doivent être clairement identifiés. On distingue plusieurs types d'acteurs pouvant intervenir dans les processus organisationnels de gestion des accès physiques :

- Les demandeurs (Collaborateurs, mainteneur, services, supports, etc.) qui font les demandes d'attribution de badges et droits associés.
- Les responsables de validation (Responsables du système (locaux ou au siège), qui valident ou non les différents droits demandés.
- Les informés, qui ont connaissance des attributions et révocations de badges et de droits à différentes fins.
- Les opérateurs du système de contrôle des accès physiques (Responsables et filtrage à l'accueil).
- Les opérateurs de sauvegarde du système.
- Les mainteneurs des matériels physiques.
- Les mainteneurs applicatifs.
- Les utilisateurs finaux, à qui sont attribués les badges.

Selon la situation, plusieurs rôles peuvent être assurés par les mêmes personnes. Il convient de s'assurer que ce cumul ne confère pas tous les droits à une seule personne et que des mécanismes d'approbation et de contrôle indépendants sont mis en place et respectés.

Processus organisationnels :

Les flux organisationnels doivent être clairement déterminés dès l'expression des besoins. Il s'agit de représenter les échanges nécessaires entre les acteurs pour réaliser un objectif particulier. Ces échanges peuvent être informatisés ou non. On distingue communément les processus suivants :

- Demande de badge.
- Délivrance de badge.
- Révocation de badge.
- Modification de droits.

Continuité de service :

Il est nécessaire d'avoir une réflexion sur le niveau de continuité de service souhaité : tolérance aux pannes, autonomie en cas de coupure électrique, délais de remplacement du matériel dans le contrat de maintenance, etc. Le besoin doit être exprimé de manière rationnelle afin de ne pas engendrer des coûts inutilement démultipliés.

1.6.2 - CHOIX DU SYSTÈME

Le choix d'un système nécessite de prendre en compte plusieurs critères, liés à sa conception même (architecture et sécurité des éléments support) et aux contraintes réglementaires.

Sécurité des éléments supports :

- **Badges : niveaux de sûreté, résistance aux attaques logiques.**

Le Tableau 2 ci-dessous établit le lien entre les niveaux de sûreté et des niveaux de résistance aux attaques logiques.

Niveau de sûreté	Résistance aux attaques logiques	Méthode	Technologie	Caractéristiques
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement répliquable

II	L1	Authentification du badge.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clé commune ; Algorithmes et protocoles d'authentification connus et réputés (AES).
III	L2	Authentification du badge, clé dérivée recommandée.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clé dérivée d'une clé maîtresse ; Algorithmes et protocoles d'authentification connus et réputés (AES).
IV	L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clé dérivée.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clé dérivée d'une clé maîtresse ; Algorithmes et protocoles d'authentification connus et réputés (AES).

Pour répondre aux principes exposés ici, une demande d'autorisation devra être faite selon les procédures complètes de la CNIL.

Ces procédures visent la protection des données personnelles, et non pas celle du système de contrôle d'accès.

La procédure simplifiée impose le stockage d'informations sur le badge et non pas sur un serveur.

Il est recommandé que les badges soient visuellement les plus neutres possibles. Ils ne doivent pas indiquer :

- D'informations sur l'établissement ou le service (nom, adresse).
- D'informations sur le porteur (nom, prénom, poste), en dehors de sa photo.
- Les accès qu'ils permettent.

La photographie est tolérée, car elle permet de vérifier rapidement que le badge appartient bien au porteur.

Têtes de lecture : protection des éléments chiffrés.

Les parties du système situées hors de la zone de sécurité délimitée par le contrôle des accès, dont les têtes de lecture font partie, ne doivent pas être source de vulnérabilités.

Dans le cas des architectures où les têtes de lecture renferment des éléments secrets, celles-ci doivent comporter des mécanismes de protection, tels que l'effacement des clés et éventuellement le déclenchement d'une alarme en cas d'arrachement. Malheureusement ces dispositifs ne sont pas totalement sûrs : pour la plupart des produits proposant ces fonctionnalités, il demeure possible d'accéder à l'intérieur de la tête avec un espacement très réduit (moins de 5mm) sans les déclencher. Bien que ce mode d'attaque soit d'un niveau déjà avancé, il confirme la nécessité d'exercer une surveillance des points d'accès permettant de déceler toute activité suspecte sur les lecteurs. (Couplage vidéoprotection).

Ces architectures requièrent également une méthode de mise à la clé sécurisée.

En outre, du fait du nombre restreint de fabricants de lecteurs et de badges, certains modèles sont facilement reconnaissables et peuvent révéler la technologie employée. Il est donc conseillé d'utiliser des lecteurs à façades standard ou anonymes (soit, totalement dépourvus d'un quelconque sigle de société ou de marque).

Enfin, il est nécessaire de connaître les personnes habilitées à effectuer le paramétrage et les opérations d'entretien des lecteurs (mise à la clé, maintenance, etc.) et d'assurer un suivi des opérations requérant ces accès.

Unités de traitement local : accès physique réservé, Secure Access Module et redondance.

L'unité de traitement local (UTL) se présente généralement sous la forme d'une carte à circuits imprimés, que l'on peut considérer comme un automate, et qui gère un groupe de têtes de lecture, généralement chacune associée à un ouvrant.

C'est un élément particulièrement sensible du système de contrôle d'accès : il détient un cache de la base des droits d'accès, ainsi que d'autres informations, telles que les derniers journaux d'événements. Dans la plupart des architectures, l'UTL détient aussi les éléments secrets cryptographiques permettant l'identification/l'authentification et la sécurisation de la communication avec le badge ou les têtes de lecture. Enfin l'UTL contient les relais qui commandent l'ouverture des ouvrants.

Les UTL doivent donc impérativement être situées à l'intérieur de la zone physique pour laquelle elles commandent l'accès et ne doivent pas être accessibles facilement (idéalement, elles doivent être à l'abri de tout accès frauduleux, dans un local technique ou tout autre type d'emplacement sécurisé).

Dans le cadre de la maintenance globale du système, la batterie de l'alimentation de secours de l'UTL doit être régulièrement vérifiée. Cette alimentation de secours et la réplication de la base des droits d'accès dans chaque UTL sont le gage d'une grande résilience du système.

Comme pour la maintenance des têtes de lecture, il est impératif de disposer de la liste des personnes autorisées à accéder physiquement aux UTL et d'assurer également la surveillance de ces opérations.

Liaisons filaires : dans le périmètre de sécurité.

Autant que possible, les liaisons filaires doivent être situées dans la zone de sécurité délimitée par le contrôle des accès, et non pas à l'extérieur de cette zone.

2 - ORGANISATION ET PLANIFICATION

2.1 - VISITE DES LIEUX

Dans le cadre de la consultation, la visite du site est obligatoire. Elle se déroulera selon les conditions indiquées, dans le règlement de la consultation.

Aucune plus-value basée sur la méconnaissance des lieux ne pourra être prise en compte.

2.2 - PLANNING

Le titulaire, dès la notification du marché, proposera un planning faisant apparaître :

- Le délai d'étude.
- Le délai de fabrication ou d'approvisionnement des matériels.
- Les phases de préparation avec le Maître d'ouvrage.
- Le délai de réalisation des prestations (exécution de chaque prestation technique comme pose des caméras, réseau, etc...).
- Le délai des essais et la mise en service.
- La date prévisionnelle de réception du système.

Les phases de pose, réglages et essais préciseront notamment l'effectif prévu sur le chantier en main-d'œuvre et encadrement. Toutes les notes de calculs, les synoptiques de chaque installation et les documentations techniques sont à la charge de l'entreprise titulaire.

L'entreprise devra fournir le dossier technique avant le démarrage des prestations. Les documents d'exécution devront obligatoirement être visés par le Maître d'Ouvrage ou son assistant pour validation.

2.3 - RENDEZ-VOUS DE CHANTIER

Une réunion de lancement et de coordination des prestations sera organisée avant le démarrage du projet à laquelle participera le titulaire afin de s'assurer de la synchronisation des chantiers.

Le Maître d'ouvrage et son assistant organisent les rendez-vous de chantier hebdomadaires et éventuellement exceptionnels.

Le titulaire est tenu de se faire représenter à ces rendez-vous au minimum par le responsable du chantier, habilité à prendre toutes les décisions à la demande du Maître d'ouvrage.

2.4 - SÉCURITÉ DU CHANTIER ET NETTOYAGE + BASE VIE

Le prestataire devra respecter toutes les mesures de prévention nécessaires à la sécurité des prestations et au bon déroulement des chantiers :

- Une signalisation adaptée pour toutes les zones de travail, notamment sur les zones de circulations, piétonnes et véhicules.

- Port obligatoire des équipements de protection individuelle pour chaque agent travaillant sur le chantier.
- Nettoyage des chantiers après chaque zone traitée.
- Les espaces de stockage de matériel seront définis par le MOA : le titulaire du présent marché devra amener ses propres containers de stockage et les déposer en fin de chantier.
- Le titulaire du présent marché devra gérer ses installations de vestiaire et de restauration.
- Des sanitaires seront mis à disposition par Science Po, et le titulaire du présent marché devra faire réaliser à ses frais un nettoyage hebdomadaire des sanitaires.
- Les emprises de chantier devront être compatibles avec l'exploitation des locaux.

2.5 - QUALIFICATIONS

Le titulaire du marché doit avoir suivi la formation du fabricant et obtenu la certification technique pour le système proposé au titre du marché.

Le titulaire du marché doit être un partenaire certifié avec les niveaux de qualification nécessaire pour l'installation, le paramétrage et la mise en service du système proposé.

Le titulaire du marché doit fournir la preuve de l'obtention des certifications nominatives des intervenants des prestations pour la réalisation des installations.

2.6 - ETUDES D'EXECUTION

A partir des documents d'Appel d'Offres, l'Entrepreneur devra remettre :

- 1 - Les plans de réalisation des installations et synoptiques des systèmes de sûreté.
- 2 - La nomenclature complète des ensembles et de leurs composants avec les notices des constructeurs des différents appareils installés, réapprovisionnement ultérieur des pièces de rechange nécessaires à l'entretien des installations.
- 3 - L'état des besoins en points d'accès au réseau informatique.
- 4 - Les plans mis à jour après exécution de la totalité des installations.

Les documents cités en 1-2 seront fournis avant exécution, en 3 exemplaires, destinés à être approuvés, avant toute commande de matériel.

Les différents documents 1-2-3 seront fournis après exécution sous forme de fichiers informatiques DWG ou DXF et des exemplaires papiers conformément au cahier des prescriptions complémentaires.

La libération du cautionnement ou de la retenue de garantie est subordonnée à la production des documents définitifs cités ci-dessus.

2.7 - CONTRAINTES PARTICULIERES LIEES AUX TRAVAUX EN MILIEU OCCUPE

2.7.1 - TRAVAUX EN MILIEU OCCUPÉ

Les travaux seront réalisés en milieu occupé pour le site EPS. Ils ne pourront être exécutés qu'après information des usagers et accord du maître de l'ouvrage.

2.7.2 - MAINTIEN EN SERVICE DES BÂTIMENTS EXISTANTS

Les mesures conservatoires ont pour objet d'assurer la continuité de service du bâtiment durant toute la durée des travaux et comprendront :

- **Le maintien en service des alimentations /courants forts et faibles.**
- **Toutes dispositions provisoires induites par le phasage et nécessaires au bon fonctionnement.**

Les travaux seront chronologiquement réalisés, à partir des investigations nécessaires à la connaissance des installations, découleront les principales tâches à réaliser pour le maintien en service des installations.

Le titulaire aura à sa charge, toutes les mesures conservatoires permettant de maintenir les installations fonctionnelles : liaisons provisoires, réalimentations provisoires, déposes et poses...

2.7.3 - DÉROULEMENT DES OPÉRATIONS

Les travaux devant être réalisés sur un site occupé, toutes les mesures doivent être prises pour ne générer qu'une moindre gêne aux habitants.

A cet effet :

- Le nombre et la durée des interventions relatives à chaque zone sont limités au strict minimum.
- Les déchets, gravats et emballages sont évacués au fur et à mesure de leur production, et en tout cas, au moins une fois par jour,
- Dans l'attente de leur mise en œuvre, les matériaux et matériels ne doivent pas être stockés à l'intérieur des bureaux ou dans les circulations communes.

A la remise de sa proposition, les entrepreneurs doivent indiquer les moyens et modes d'intervention qu'il se propose d'utiliser pour l'obtention de ces résultats.

2.7.4 - PÉNÉTRATION DANS LES BÂTIMENTS OCCUPÉS

Le Maître d'Ouvrage se charge de la campagne d'information nécessaire auprès de ses occupants pour annoncer la réalisation des travaux.

Les entrepreneurs préciseront les jours et heures d'intervention de leur personnel aux différents occupants des bâtiments et assureront l'organisation des rendez-vous ou des réunions d'information nécessaires à la bonne marche des travaux.

2.7.5 - DÉPLACEMENT DE MOBILIER - PROTECTION

Le Maître d'Ouvrage aura à sa charge de déplacer les éléments de rangement, les objets et le mobilier gênant l'avancement des travaux.

L'Entrepreneur devra prendre toutes les dispositions nécessaires à la protection des mobiliers, objets et biens appartenant aux usagers, avec des bâches, couvertures, etc...., afin d'éviter toute contestation et procédure à son encontre en cours ou à la fin des travaux.

2.7.6 - APPROVISIONNEMENT DES MATÉRIAUX

L'entrepreneur a à sa charge tous les frais relatifs aux installations nécessaires à l'exécution des travaux (location, pose, dépose, transport, etc.).

Les opérations de levage ne doivent causer aucune dégradation des bâtiments existants, et être conduites de façon à assurer la sécurité absolue des personnes travaillant sur le chantier, ainsi que des tiers.

2.7.7 - PROTECTION CONTRE LE BRUIT ET LA POUSSIÈRE

L'entrepreneur prendra toutes les dispositions pour ne pas occasionner de gêne auditive à l'égard des usagers des bâtiments.

Le plus grand soin sera apporté au respect des conditions de vie et de tranquillité des bâtiments, en réduisant au maximum les nuisances inhérentes au déroulement du chantier (utilisation de matériel insonorisé, aménagement des horaires de travail, etc.).

2.7.8 - SÉCURITÉ DES TIERS

Pendant la durée des travaux, l'Entreprise devra prendre toutes les dispositions nécessaires afin de ne causer aucun dommage aux bâtiments.

Dans le cas contraire, elles seront tenues pour seules responsables des dommages causés et devront en supporter les conséquences.

2.8 - RECEPTION ET CONTROLE DES INSTALLATIONS

L'entreprise titulaire devra procéder aux essais et vérifications de fonctionnement des installations conformément aux dispositions figurant dans les documents techniques COPREC N°1 paru dans le cahier spécial du Moniteur du Bâtiment et des Travaux Publics n° 4899 du 17 Octobre 1997.

En même temps qu'il formule sa demande de réception, l'entrepreneur devra fournir les procès-verbaux établis à la suite de ces essais conformément au Document Technique COPREC N° 2, paru dans le cahier spécial du Moniteur du Bâtiment et des Travaux Publics n° 4899 du 17 Octobre 1997 et devront être transmis préalablement à la réception des travaux, au Bureau de Contrôle pour l'établissement de son rapport.

Les dossiers de plans des ouvrages exécutés seront soumis à l'approbation de la Maîtrise d'œuvre avant la transmission au Maître d'Ouvrage.

2.9 - DOE

Après validation de la réception et dans un délai de 20 jours ouvrables, l'entreprise devra fournir en deux exemplaires papiers et un exemplaire sur support informatique, le D.O.E (Dossier d'Ouvrage Exécuté) comprenant :

- Le synoptique de l'installation mis à jour.
- Les plans de récolement du site (la numération des caméras existantes devra être conservée pour les caméras de remplacement afin de ne pas changer les repères des agents).
- Les fiches techniques des produits installés.
- Les photos des prestations réalisées.
- Le PV de réception.

2.9.1 - PLANS

Le titulaire devra transmettre entre autres les documents ci-dessous concernant les ouvrages dont elle a eu la réalisation :

- Plans de tous les ouvrages réalisés, correspondant aux plans de détail d'exécution élaborés pendant le chantier et ayant reçu les visas du contrôleur technique et du Maître d'œuvre.
- Ces plans devront comporter l'emplacement et le tracé de tous les ouvrages, canalisations, tableaux et organes de commande, de coupure, etc...
- Ces ouvrages devront être cotés, tant en dimension qu'en position de niveaux, par rapport, soit au niveau de référence du bâtiment, soit au N.G.F. pour les éléments extérieurs.

2.9.2 - NOTICES D'ENTRETIEN

L'entrepreneur devra fournir :

- Les schémas généraux des installations techniques.
- Les notices techniques et d'entretien nécessaires pour la conduite des installations et l'entretien du matériel ou des ouvrages.

Faute d'avoir fourni les renseignements, l'entrepreneur ne pourra se prévaloir contre le Maître d'Ouvrage d'un mauvais entretien des ouvrages sous garantie.

L'entreprise devra en outre, à la remise de ces documents, procéder à l'information et la formation du personnel désignée par le Maître d'Ouvrage et ayant à charge pour celui-ci la maintenance des installations.

Le planning de formation sera établi avec le Maître d'Ouvrage après la réception des travaux.

2.9.3 - FICHES TECHNIQUES ET RÉFÉRENCES DES MATÉRIELS

L'entrepreneur devra fournir :

- Les fiches techniques pour tout le matériel mis en œuvre permettant une identification précise de tout organe pouvant être remplacé par le Maître d'Ouvrage au-delà de la durée de garantie.
- Ces fiches techniques et références devront comporter tous les procès-verbaux et avis techniques correspondant aux spécifications du descriptif, ou ayant été demandés pendant le chantier, tant par le contrôleur technique que par le Maître d'œuvre.
- Ces documents devront être reliés en volumes et également communiqués sur CD Rom.

2.9.4 - LISTE DES MATÉRIAUX ET ÉQUIPEMENTS MISE EN ŒUVRE

Cette liste comportera dans l'ordre :

- 1) - La référence de l'article CCTP
- 2) - La nature
- 3) - La provenance ; fournisseur, adresses...
- 4) - Le classement
- 5) - L'avis technique
- 6) - Les observations
- 7) - Le PV de classement au feu

2.9.5 - NOMBRE D'EXEMPLAIRES

Les documents seront fournis en deux exemplaires et sur support informatique (plan sous autocad) sur clé USB.

L'ensemble des plans et divers documents sera remis dans un ou des classeurs blancs rigides deux trous avec intercalaires.

2.10 - DECOMPOSITION DES PRIX FORFAITAIRES

L'entreprise devra remettre, en même temps que sa soumission, la décomposition des prix globale et forfaitaire détaillée, en quantités et prix unitaires sous la forme du bordereau quantitatif joint au présent descriptif.

L'entrepreneur ne portera aucune rectification à la numérotation des articles ni à la pagination, le non-respect de cette clause sera éliminatoire.

2.11 - FORMATION DU PERSONNEL

L'entreprise aura, comme prestations incluses dans ce marché, l'élaboration de modules de formation complémentaires dans le cadre de l'exécution de ce marché. La formation se déroulera sur site, pendant la phase d'essais des installations.

La formation des exploitants sera effectuée par l'entreprise et coordonnée par le Maître d'Ouvrage.

Les formations seront dispensées aux responsables et opérateurs.

Il sera prévu deux formations spécifiques :

- Une formation à l'exploitation des équipements.
- Une formation destinée au mainteneur des équipements.

Le titulaire devra présenter dans son offre des modèles de programmes de formation concernant les installations de vidéosurveillance.

2.12 - AFFICHAGE RÉGLEMENTAIRE

La fourniture et l'installation des panneaux d'information du public sont à la charge du titulaire du marché.

Les panneaux devront être installés sur l'espace public avant la mise en exploitation du système à proximité de chacune des zones équipées de sorte que chaque personne filmée « soit en situation de s'y attendre ».

L'entreprise soumettra une maquette au Maître d'Ouvrage pour validation et devra prévoir l'ensemble des dispositifs nécessaires à la fixation des panneaux.

Les emplacements de panneaux et des affichettes seront définis lors de la première réunion de chantier.
- 20 affiches à prévoir/ parking.

2.13 - GARANTIE

La garantie de parfait achèvement sera d'un an à partir de la réception conforme de l'installation (hors dégradation volontaire, mauvaise utilisation et intempéries).

Elle portera sur les prestations, le fonctionnement des installations et leur conservation.

La garantie constructeur sera de deux ans pour les fournitures et matériels.

La mise en œuvre de ces garanties impliquent :

- Le remplacement ou la réparation des matériels.
- Les études nouvelles s'il y a lieu.

- La main-d'œuvre nécessaire.
- Les frais annexes pouvant découler des interventions au titre des garanties.

Par remplacement des matériels, on entend toute pièce défectueuse, ou présentant des vices de construction, ou ne correspondant pas ou plus aux caractéristiques définies, ou présentant une usure anormale.

L'entreprise restera responsable des installations jusqu'à l'expiration des délais de garantie.

3 - DESCRIPTIF DES PRESTATIONS

3.1 - PRÉSENTATION GÉNÉRALE

3.1.1 - PLAN DE SÉCURISATION DE PRINCIPE



3.1.2 - SÉCURISATION DES ACCÈS PÉRIMÉTRIQUES PIÉTONS

3.1.2.1 - Accès AS1, AS2, AS5, AS6

Voir plan de principe en page précédente.

L'entrée sur le site sera organisée en fonction du type d'usager. Cela permettra de différencier et de répartir les flux **en y associant les contrôles correspondants**.

Définition des usagers :

- U1 - Enseignants, agents techniques et administratifs (IEP, Rectorat, CAEC, CROUS), prestataires réguliers (ménage...).
- U2 - Etudiants inscrits à l'IEP, enseignants vacataires.
- U3 - Candidats aux examens et concours CAEC.
- U4 - Prestataires ponctuels (espaces verts...), fournisseurs, rendez-vous, futurs usagers des espaces partagés (jardin, amphi, expositions...).

Pour les piétons, l'objectif d'organisation devrait être :

L'accès AS1, dans le cadre de la sécurisation, **pas d'intervention particulière**, le portail devra rester un accès pompiers et il devra rester fermé dans l'usage.

- Tranche optionnelle pour l'AS1 : mise en œuvre d'une caméra sur mât de 7 m (voir tranches optionnelles T02 et T03).

L'accès AS2 pour les usagers U1 (sachant que la majorité de ces usagers viennent en véhicule) sera équipé dans le cadre de **la tranche ferme** comme suit :

- Mise en œuvre d'un accès contrôlé par badges en entrée et en sortie, sur l'accès existant.
- Mise en œuvre d'un verrouillage à serrure électronique extérieur.
- Mise en œuvre d'un visiophone en entrée avec transfert des appels à l'accueil.
- Ferme porte.
- Mise en œuvre d'une caméra (à placer sur le local transformateur désaffecté).

Dans le périmètre d'AS2 se trouve le transformateur désaffecté dans lequel il y sera mis en œuvre (à la charge de la DSISN) un coffret 19 pouces, un commutateur POE et un tiroir optique dédié à la sûreté.

- Mise en œuvre d'un accès contrôlé par badges en entrée et sortie libres, sur l'accès existant.
- Mise en œuvre d'un verrouillage à serrure électronique extérieur.
- Mise en œuvre d'un ferme porte.

A ce titre, ce local devra être protégé par de la détection d'intrusion (hors périmètre).

L'accès AS5, sa réfection est **hors périmètre du marché**. Hors période d'examens et de concours par le CAEC, le portail pompier restera maintenu fermé comme AS1.

Pour les usagers U3, **l'accès AS5** pourra être équipé dans le cadre de **la tranche optionnelle TO 01** et sera équipé comme suit :

- Mise en œuvre d'un visiophone en entrée et transmission des appels au poste de réception du CAEC.
- Mise en œuvre d'une caméra sur mât de 7 m.

L'accès AS6 (accès piétons depuis la place Philippe Séguin), il est réservé aux usagers U2 et U4, il sera traité dans le cadre **des tranches optionnelles TO 02 et TO 03**, il pourra être équipé comme suit :

TO 02 :

- La mise en œuvre en retrait de la voie publique, d'un accès à unicité de passage conforme PMR, passage vélos et piétons type ONYX outdoor avec auvent de protection du constructeur Bolloré ou équivalent.
- La mise en œuvre en œuvre en retrait de la voie publique, de deux tourniquets de sécurité à unicité de passage de type TF1000-EVO du constructeur Bolloré ou équivalent
- La mise en œuvre d'un contrôle d'accès par badges en entrée et sortie.
- La mise en œuvre de visiophone à bouton en entrée et sortie avec appel aboutissant à l'accueil et débordement sur l'astreinte.
- La mise en œuvre de caméra en entrée et en sortie des accès à unicité de passage.
- Le mise en œuvre de la caméra, sur mât, d'AS1.
- La mise en œuvre des alimentations électriques nécessaires,
- L'ensemble des câblages courant faible devront être tirés à proximité du coffret n°6 DSISN.
- Le système de contrôle d'accès devra être placé sous coffret et autoprotégé. (les autoprotections seront reprises ultérieurement par le projet de rénovation de l'intrusion, hors périmètre).

TO 03 :

- La mise en œuvre en retrait de la voie publique, de trois accès à unicité de passage conforme PMR, passage vélos et piétons type ONYX outdoor avec auvent de protection du constructeur Bolloré ou équivalent.
- La mise en œuvre d'un contrôle d'accès par badges en entrée et sortie.
- La mise en œuvre de visiophone à bouton en entrée et sortie avec appel aboutissant à l'accueil et débordement sur l'astreinte.
- La mise en œuvre de caméra en entrée et en sortie des accès à unicité de passage.
- La mise en œuvre de la caméra, sur mât, d'AS1.
- La mise en œuvre des alimentations électriques nécessaires.
- L'ensemble des câblages courant faible devront être tirés à proximité du coffret n°6 DSISN.
- Le système de contrôle d'accès devra être placé sous coffret et autoprotégé. (les autoprotections seront reprises ultérieurement par le projet de rénovation de l'intrusion, hors marché).

Pour les usagers U4, ils devront donner leur identité et le motif de la visite par l'accès AS6 via les visiophones mis en œuvre.

Hors périmètre du projet :

- Le génie civil nécessaire au raccordement des portillons automatiques avec le bâtiment.
- La clôture de part et d'autre, des unicités de passage qui seront mis en œuvre en retrait de la voie publique.
- L'ouverture de l'accès piéton AS6, dans la murette de séparation de la place Philippe Séguin et du jardin de l'établissement.
- Le remodelage des terrains nécessaire à l'implantation des portillons automatiques (le titulaire devra fournir ces besoins à la MOA).

3.1.3 - SÉCURISATION DE L'ACCÈS VÉHICULES – AS3

L'accès AS3, pour les usagers U1, sera équipé dans le cadre de **la tranche ferme** et sera équipé comme suit :

- Le portail véhicule coulissant motorisé (existant et conservé) commandé à distance à partir de l'accueil et au CROUS pour la gestion des livraisons :
 - Mise en œuvre d'un contrôle d'accès en entrée et sortie libre par boucle magnétique au sol.
 - Suppression de bouton de sortie du portail motorisé.

- Remplacement de visiophone d'entrée portail par un visiophone à défilement pour les appels vers l'accueil Science Po, le CROUS et le CAEC.
 - Mise en œuvre d'un poste de réception audio et vidéo à l'accueil IEP, au CROUS et au CAEC
-
- Mise en œuvre de deux barrières automatiques à lisses équipées de herse haute et basse, asservissement par effet de sas, afin d'éviter le franchissement de piétons et les entrées de véhicule par effet dit « de petit train ». L'espacement entre les deux barrières, le portail motorisé et la première barrière devra permettre l'accès des véhicules de livraison du CROUS type 20 mètres cube.
 - Mise en œuvre d'un contrôle d'accès dans le sens de l'entrée, pour la barrière automatique, sur potelet pour les VL. Entrée par asservissement à effet de sas avec la deuxième barrière.
 - Mise en œuvre d'un contrôle d'accès dans le sens de la sortie, pour la deuxième barrière automatique, pour les VL. Sortie par asservissement à effet de sas avec la première barrière.
 - Une boîte à boutons de commande manuelle des barrières devra être mise en œuvre à l'accueil, pour gérer l'accès véhicule visiteurs.
 - Mise en place de visiophone, sur potelet, pour les VL, dans le sens de l'entrée et le sens de sortie des barrières automatiques avec transfert des appels à l'accueil l'IEP.
 - Mise en œuvre d'un visiophone, sur potelet VL, entre les deux barrières automatiques, avec transfert des appels à l'accueil de l'IEP.
 - Création du génie civil nécessaire au raccordement des systèmes (ELEC et CFA) au local transformateur désaffecté.
 - Remodelage des terrains nécessaire à la VRD et à l'implantation de la barrière automatique.
 - Mise en œuvre d'une clôture de part et d'autre des barrières automatiques afin de délimiter la zone du sas d'accès véhicule et d'éviter les franchissements de piétons :
 - Mise en œuvre d'une clôture en treillis soudé de type Gantois d'une hauteur de 2m.
 - Mise en œuvre d'une caméra sur mât de 7 m.

Cette organisation devra permettre d'adapter le niveau de contrainte en mettant en œuvre la fonction « sas » ou non, entre les barrières automatiques et le portail motorisé.

Exemple :

- En période d'heure d'ouverture du site, le portail coulissant sera ouvert, les barrières seront contrôlées par badges et visiophones :
 - Dans le sens de l'entrée au site, ouverture de la première barrière par badge, ouverture automatique de la deuxième barrière lorsque la première barrière sera fermée.
 - Dans le sens de la sortie du site, ouverture de la deuxième barrière par badge, ouverture automatique de la première barrière lorsque la deuxième barrière sera fermée.
- Sur événement majeur, le portail motorisé pourra être contrôlé manuellement afin de fermer l'accès au site depuis la voie publique.

3.1.4 - COMPARTIMENTAGE DES ENTITÉS IEP ET CAEC

3.1.4.1 - SÉPARATION SP1

La **séparation SP1**, hors périmètre du projet, sera une délimitation « douce » entre les entités (CROUS/CAEC et IEP), l'objectif étant de séparer les zones et de ne pas créer un sentiment de fermeture, le parc doit rester un endroit de quiétude.

L'accès par **la séparation SP1**, sera traité dans le cadre de **la tranche optionnelle TO 04**, il pourra être équipé comme suit :

- Mise en œuvre d'un contrôle d'accès en entrée et sortie (portillon).
- Mise en œuvre d'un verrouillage à serrure électronique extérieur.

- Mise en œuvre d'une caméra.

Hors périmètre du présent marché :

- Un portail métallique dédié aux pompiers et aux livraisons, doubles battants, ouverture à la française, avec une serrure mécanique type A2P** ou équivalent, carré pompiers.
- Un portillon métallique et ferme porte.
- Une clôture de délimitation douce.

3.1.4.2 - SÉPARATION SP2

La **séparation SP2**, qui reste hors périmètre du projet, permettra de maintenir une étanchéité des flux avec le CAEC/CROUS et limiter l'accès aux usagers de la catégorie U4.

L'accès par **la séparation SP2**, sera traité dans le cadre **la tranche optionnelle TO 05**, il pourra être équipé comme suit :

- D'un visiophone à un bouton, pour les livraisons, aboutissant au CROUS.
- Poste de réception audio et vidéo au CROUS (déjà prévue sur AS3).
- Mise en œuvre d'une caméra.

Hors périmètre du marché

- Un portail métallique dédié aux pompiers et aux livraisons, doubles battants, ouverture à la française, avec une serrure mécanique type A2P** ou équivalent, carré pompiers.
- Une clôture de part et d'autre du portail, de mêmes hauteurs que le portail.

3.1.4.3 - SÉPARATION SP3 :

La séparation SP3, qui reste hors périmètre du projet, pour les usagers U1 permettra de maintenir une étanchéité entre les flux de l'IEP et du CAEC.

L'accès par **la séparation SP3**, sera traité dans le cadre de la tranche optionnelle **TO 06**, il pourra être équipé comme suit :

- Mise en œuvre d'un contrôle d'accès en entrée et sortie.
- Mise en œuvre d'un verrouillage à serrure électronique extérieur.

Hors périmètre du présent marché :

- Un portillon métallique et ferme porte.
- Une clôture de part et d'autre du portillon.

3.1.5 - SÉPARATION DE LA ZONE JARDIN PARTAGEE ET IEP

L' accès AS4 qui reste hors périmètre du présent marché, est réservé pour l'accès au jardin partagé comme seul accès au public :

- Remplacement de l'accès existant par un portillon métallique avec serrure mécanique type A2P** ou équivalent.
- Reprise de la voute de passage.

3.1.6 - IMPLANTATIONS

Les plans fournis en annexe présentent les implantations théoriques des équipements et sont donnés à titre indicatif.

Le titulaire devra faire valider l'implantation définitive, des équipements, à la maîtrise d'ouvrage et à son assistant.

3.2 - TERRASSEMENT

La prestation comprend :

- L'intégralité des besoins en remblais par apport de grave extérieur (GNT) ou autres matériaux validés par la maîtrise d'œuvre.
- L'intégralité de l'évacuation des déblais excédentaires.
- L'intégralité de l'évacuation des déblais liés au décapage (y compris s'il s'agit de « terre végétale ») et des déchets verts (défrichage, arbres, souches).
- Le réemploi de terres ou grave du site ne pourra être envisagé que sur accord du Maître d'œuvre et de la maîtrise d'ouvrage.
- La reprise de la bordure.

3.2.1 - DÉMOLITION

Démolition des constructions existantes et des ouvrages enterrés (fondations, rochers, etc.). Avant de procéder à leur enlèvement, l'entreprise doit s'assurer de leur non-utilisation et prévenir la maîtrise d'œuvre.

Démolitions des revêtements, des clôtures et des bordures existantes en limite de projet pour réalisation d'une liaison de finition propre et soignée :

- Sciage.
- Décroulage.
- Rabotage.
- Marteau piqueur.
- Dépose de bordures.
- Evacuation.

3.2.2 - TERRASSEMENT DE LA TERRE VÉGÉTALE

3.2.2.1 - DÉCAPAGE

Sur toutes les surfaces des travaux de terrassement pour voirie, il est procédé au préalable au décapage de la terre végétale .

Les zones de remblais pour mouvements de terre doivent également être décapées.

L'ensemble du produit de décapage de la terre végétale est stocké sur le chantier en un ou plusieurs lieux de stockage définis en accord avec le Maître d'Œuvre. L'entreprise est tenue d'assurer la protection et la sauvegarde des terres végétales en stock, qui devront être protégées de toute pollution.

L'épaisseur moyenne de décapage est de : 20 cm.

3.2.2.2 - RÉEMPLOI

Les terres végétales, stockées, préalablement et parfaitement protégées, sont reprises et mises en œuvre en couverture définitive sur une épaisseur moyenne de 20 cm. L'excédent sera évacué à la décharge.

L'Entrepreneur doit le modelage final qui doit permettre le réglage.

Epaisseurs minimales à obtenir après tassements :

- 0.30 m pour les engazonnements, massifs de fleurs et plantes vivaces.
- 0,50 m pour les arbustes en massif et pour les haies.
- Jusqu'à 5 cm des bords dans les jardinières.

3.2.3 - TERRASSEMENTS GÉNÉRAUX

Les travaux comprennent les terrassements en terrain de toutes natures, pour mise à niveau et modelage du terrain comprenant les pentes pour l'éloignement des eaux des ouvrages ainsi que les noues supprimant toute stagnation d'eau.

Les terres excédentaires ainsi que celles dont la nature ne permet pas un réemploi en remblai, les rochers et gravois, sont évacués vers la filière de gestion appropriée.

La tolérance en altitude doit être de deux centimètres (0,02 m) aussi bien au-dessus qu'en dessous des cotes prescrites.

Niveau altimétrique des plateformes :

- **Sous chaussée** : suivant les différents revêtements de sols.
- **Sous-espace vert** : - 20 cm par rapport au niveau fini.

3.2.3.1 - TERRASSEMENT EN DÉBLAIS

Terrassements en pleine masse exécutés mécaniquement et si besoin au BRH :

- Terrassements en déblai pour obtenir les plateformes des voiries et des bâtiments. Les plateformes des bâtiments devront avoir une emprise minimum de 3 m en plus de l'emprise du bâtiment afin de permettre la circulation autour du bâtiment pendant la phase de chantier.
- Pente des talus déterminée par l'entrepreneur étant précisé qu'il sera responsable de tous les incidents découlant d'un manque de précautions ; Protection nécessaire des talus.
- Confection de rampes d'accès et enlèvement en fin de travaux.
- Enlèvement des débris de masse inférieure à 0,5m³ compris dans le forfait.
- Purge soignée du fond de fouille. Comblement des trous en sable tout-venant.
- Fossés et drainages pour évacuation des eaux de ruissellement avec tous les relevages nécessaires.
- Manutention des terres excavées et mises en dépôt sur la parcelle.
- Évacuation des terres excavées vers la filière de gestion appropriée.

3.2.3.2 - TERRASSEMENT EN REMBLAI

Réalisation des plateformes :

- Terrassements en remblai pour obtenir les niveaux des plateformes.
- Purge soignée des poches de mauvaises terres.
- Rampe d'accès en sol compacté, supprimée en fin de travaux.
- Drainages si nécessaires.
- Dressement, chargement et enlèvement des excédents aux décharges.
- Compactage par couches de 20 cm maximum suivant la prescription du SETRA.

3.2.4 - PROTECTION EQUIPEMENT EXISTANT

Les équipements existants à proximité des zones de travaux seront protégés pendant la durée des travaux (exemple : candélabre).

3.3 - TRAVAUX DE GÉNIE CIVIL

Les stipulations du présent document concernent les travaux de :

- Les travaux préparatoires.
- Les travaux de terrassement généraux.
- Les travaux de voirie.
- Les travaux de réseaux secs.

Les études et travaux devront être réalisés en conformité avec les règles, règlements et normes en vigueur le jour de la soumission.

L'ensemble des travaux décrits ou non décrits au présent corps d'état et nécessaires au total et parfait achèvement de l'ouvrage, devra être prévu, aucune plus-value en cours de chantier ne pouvant être prise en considération.

Pour toutes tranchées réalisées en terre végétale, l'évitement des systèmes racinaires sera à prendre en compte pour ne pas blesser les arbres des zones végétalisées et s'assurer de la pérennité des passages de câble qui seront réalisés (Vidéo, Energie, câbles de détection enterrés).

Les travaux comprendront :

- L'intégralité des besoins en remblais par apport de grave extérieur (GNT) ou autres matériaux validés par la maîtrise d'œuvre.
- L'intégralité de l'évacuation des déblais excédentaires.
- L'intégralité de l'évacuation des déblais liés au décapage (y compris s'il s'agit de « terre végétale ») et des déchets verts (défrichage, arbres, souches).
- Le réemploi de terres ou grave du site ne pourra être envisagé que sur accord du Maître d'œuvre et de la maîtrise d'ouvrage.
- Démolitions des revêtements, des clôtures et des bordures existantes en limite de projet pour réalisation d'une liaison de finition propre et soignée :
 - Sciage.
 - Décroulage.
 - Rabotage.
 - Marteau piqueur.
 - Dépose de bordures.
 - Evacuation.
- L'exécution des fouilles sous chaussée, trottoir ou espaces verts, soit à la tranchée ou fonceuse mécanique, soit à la pelle mécanique, soit à la main avec toutes sujétions inhérentes à ce type de prestations (purge de tout corps saillant et régalinge de fond de fouille), quelle que soit la nature du sol (terre, béton, cailloux, roche, etc...).
- La fourniture et la pose des canalisations et de leur protection (grillage avertisseur) ; les canalisations seront réalisées avec des fourreaux Ø63mm TPC conformes à la norme NF T 54-018 ; ils seront emboîtés au fur et à mesure de l'avancement des travaux ; ils seront aiguillés à l'aide d'un filin imputrescible de résistance minimale à la traction de 100daN.

Toutes les canalisations seront posées en double parallèle suivant le principe un Fourreau Courant Faible, un Fourreau Energie.

- La remise en état des chaussées et trottoirs à l'identique, sauf cas de réfection provisoire imposée par les gestionnaires de voirie.

- La fourniture et pose des chambres de tirage.
- La fourniture et la pose des bornes et coffrets.

L'Entreprise devra repérer soigneusement les réseaux existants et devra supporter toutes les sujétions résultant de la présence de ceux-ci.

3.4 - CARACTÉRISTIQUES DES TRANCHÉES

Les tranchées seront de dimensions nécessaires pour respecter les profondeurs et écartements réglementaires entre les diverses canalisations.

- FIBRE OPTIQUE, profondeur minimum 60cm : remblai de protection en sablon sur 20cm au-dessus de la génératrice la plus haute ; grillage avertisseur de coloris vert ; remblaiement complémentaire en tout-venant sous voirie et en terre fine sous-espaces verts.
- CABLE DETECTEUR, profondeur de 25cm, remblai en terre végétale, grillage avertisseur de coloris vert.

Si des canalisations de natures différentes sont placées dans une même tranchée, elles respecteront les distances suivantes :

- Distance minimale de 20cm entre les canalisations électriques B.T. sous gaine isolante et les canalisations d'eau, de gaz, de vapeur et de télécommunication, en réseaux parallèles ou croisés.
- Cette distance minimale est portée à 50 cm pour les câbles H.T.

3.5 - REMBLAIS

Les remblais employés seront constitués de sols homogènes. Les remblais seront exempts de plâtras, gravier hétérogène, tourbe, vase, terre fluente ou argile. Les matériaux gelés ou susceptibles d'être altérés par le gel ne pourront être utilisés. Les blocs rocheux et les déblais de carrière seront autorisés sous réserve que les vides soient remplis par un remblai de bonne nature.

Seules les couches supérieures pourront être composées par des terres légères, tufeuses ou graveleuses extraites des fouilles.

Avant le début des travaux, l'entreprise indiquera la nature et la provenance des matériaux qu'il propose de mettre en œuvre et fournira les résultats des essais de convenance exécutés dans un laboratoire agréé (Classement au GTR).

Les déblais provenant des fouilles serviront aux remblais, après nettoyage (élimination des gravois, des cailloux et des pierres les plus volumineuses), et à condition qu'ils soient de qualité requise.

Les remblais au contact des bâtiments seront constitués par des matériaux assurant le drainage au voisinage des fondations : leur mise en place s'effectuera de telle sorte que les fondations, sous-sols ou murs de soutènement ne subissent aucun dommage.

3.6 - DESCRIPTION DES TRAVAUX

Les travaux prévus au présent marché sont définis par point caméra dans les fiches descriptives ci-dessus.

3.6.1 - VRD

La prestation VRD comprend :

- La mise en œuvre de la tranchée (y compris la mise en place du grillage avertisseur).
- La mise en œuvre de la tranchée du câble de détection enterré.
- La mise en œuvre des regards et chambres de tirage.
- La mise en œuvre des fourreaux ainsi que l'aiguillage.
- La mise en œuvre du câble détecteur.
- La mise en œuvre des mâts, y compris massif et fondation.

3.6.2 - TRANCHÉE

Les terrassements comprendront :

- Fouilles en tranchée dans terrain de toute nature, y compris démolitions éventuelles dans l'emprise de la fouille.
- Évacuation des déblais non réutilisables aux décharges publiques.
- Évacuation des venues d'eau si nécessaire par pompage ou rabattement de nappe, avec blindage des fouilles.
- Aménagement du fond de fouille comprenant le compactage et réglage du lit de pose.
- Lit de pose en sable sur 0.10 m d'épaisseur pour pose des tuyaux.
- Remblais d'apport en sable jusqu'à 0,20 m au-dessus de la génératrice supérieure.
- Mise en place d'un grillage avertisseur de couleur conventionnel.
- Remblais complémentaires en grave sableuse 0/31.5 et compactage soigné jusqu'à la base des structures voiries et allées piétonnes.
- Réfection de la voirie quand nécessaire (une découpe préalable de la chaussée s'effectuera avant ouverture pour des raccords propres).

3.6.3 - FOURREAUX

Les fourreaux seront en polyéthylène basse densité de première fusion conforme à la norme 68 171 du 20 février 1988. Ils seront aiguillés avec un cordon imputrescible.

Le rayon de courbure doit être égal à 15 fois minimum le diamètre extérieur de la gaine TPC.

La prestation comprend :

- Fourniture et pose de fourreaux TPC annelés de Ø63mm de couleur verte.
- Y compris coude, raccord et manchon et aiguillage.

3.6.4 - DISPOSITIF AVERTISSEUR

Un grillage avertisseur de couleur vert conforme à la norme NF EN 12613 sera positionné à environ 0.30cm au-dessus des fourreaux fibre optiques.

3.6.5 - CHAMBRE DE TIRAGE

Fourniture et pose de chambres de tirage préfabriquées :

- Terrassements nécessaires.
- Béton de propreté de 5cm.
- Regard préfabriqué en béton L0T, L1T, L2T ou L3T, conforme aux normes applicables.

- Les masques devront être réalisés proprement, les fourreaux devront être arasés aux parois.
- Nettoyage des fonds de chambre.

Leur fermeture sera assurée par un tampon fonte sur cadre fonte ou acier. Leur classe de résistance sera la suivante :

- Sous voirie accessible, véhicule D400.
- Sous voirie accessible aux piétons C250.
- Sous-espace vert B125.

3.7 - RÉSEAU DE SÛRETÉ

3.7.1 - OBJECTIF GÉNÉRAL

Dans le cadre du projet, un réseau dédié à la sûreté devra être déployé afin de mettre en communication les systèmes tout en conservant une étanchéité avec le réseau de fonctionnement de l'établissement.

Le local transformateur désaffecté servira de sous-répartiteur informatique industriel dédié à la sûreté et la mise en place des coffrets de contrôle d'accès, pour AS2 et AS3.

La création du réseau de sûreté devra utiliser les infrastructures courantes faibles existantes pour le cheminement des câbles dans l'établissement.

La DSISN se chargera de la fourniture, de l'administration et de la maintenance du commutateur du cœur de réseau de la sûreté au R+3. La Direction des Systèmes d'Informations et de la Stratégie Numérique (DSISN), service informatique de l'IEP, configurera le réseau de sûreté dédié et entièrement autonome sur le site d'EPS :

- Les coffrets (coffret n°6, n°7, n°8 et n°9, voir plan d'implantation).
 - **L'alimentation des coffrets et les onduleurs seront à la charge du titulaire.**
- Les points d'accès réseau.
- Les transceivers.
- Les actifs réseau en salle serveur.
- Les configurations réseau.

Une partie des câblages seront à la charge de la DSISN et la VRD sera hors périmètre.

Répartition de la création des réseaux :

- Un lien fibre optique devra être créé entre le local transformateur désaffecté (coffret N°7) et le local serveur du R+3 un utilisant la VRD existante (voir plan) et les infrastructures courant faible existant du bâtiment, à la charge de la DSISN. Dans ce local, la DSISN devra la mise en œuvre d'un coffret 19 pouces, d'un tiroir optique.
Le titulaire devra la fourniture et la mise en place du commutateur POE, niveau 2, durcie, et des modules SFP dans le coffret N°7 (mis à disposition par la DSISN), l'alimentation électrique et l'onduleur.
- Un lien devra être créé entre AS3 et le local transformateur :
 - Création de la VRD à la charge du titulaire.
 - Alimentation électrique des barrières automatiques à la charge du titulaire.
 - Liens cuivre, contrôle d'accès et informatiques (visiophones et caméras) sont à la charge du titulaire.
- Un lien cuivre devra être crée entre AS6, AS1 et le coffret n°6, les alimentations électriques et l'onduleur sont à la charge du titulaire.

- La VRD nécessaire est hors périmètre. Le titulaire devra préciser ces besoins à la MOA.
- Un lien fibre devra être crée entre SP1 et le coffret n°8 est à la charge de la DSISN, l'alimentation électrique et l'onduleur sont à la charge du titulaire.
La VRD nécessaire est hors périmètre. Le titulaire devra préciser ces besoins à la MOA.
- Un lien fibre devra être créée entre le R+3 et le coffret n°9 à la charge de de la DSISN, l'alimentation électrique est la charge du titulaire en tranche optionnelle TO 06.
La VRD nécessaire est hors périmètre. Le titulaire devra préciser ces besoins à la MOA.
- Les liens cuivre de chaque caméra mise en œuvre sur l'emprise du bâtiment seront à la charge de la DSISN.

Le présent document concerne la conception, la fourniture, l'installation, les tests et la réception d'un système de câblage fournis par le titulaire:

- De catégorie 6a et de classe Ea.
- Électrique pour l'alimentation électrique des matériels de sûreté et la création de points d'accès réseau pour ceux-ci.

Ce système de câblage assurera le transport des signaux vidéo, sûreté et contrôle télémétrique, le tout de manière transparente. Pour répondre aux besoins futurs, il devra permettre la réalisation aisée de la maintenance ainsi que d'éventuelles extensions.

Le système de câblage réalisé devra permettre de supporter tous les protocoles IEEE, EIA/TIA et ISO existants définis comme fonctionnant sur ce support, et ce pour une durée minimale de 15 ans.

Le système de câblage devra intégrer la compatibilité de bout en bout avec la norme IEEE 802.3af, à savoir permettre la transmission de courants « basse tension » (PoE) sur les liaisons de câble en cuivre.

//tous les câbles seront repérés (tenant-aboutissant).

3.7.2 - CRÉATION DES POINTS D'ACCÈS RÉSEAU <90ML

Chacun de ces points aura les caractéristiques suivantes :

- Tenant, commutateur réseau le plus proche et TD le plus proches.
- Composante :
 - Multipaires Ethernet catégorie 6a suivant caractéristiques décrites ci-après, connectorisées, lovées en attente dans l'emprise de la fixation caméra, raccordée au commutateur indiqué.

3.7.3 - CARACTÉRISTIQUES TECHNIQUES DES MATÉRIELS RESEAU

3.7.3.1 - CONTRAINTES D'ENVIRONNEMENT ÉLECTROMAGNÉTIQUE

Le respect des contraintes d'environnement ci-après conditionne directement les performances de l'infrastructure de câblage.

La séparation entre les câbles de transmission de données et les câbles d'alimentation électrique doit être au minimum conforme à la norme EN 50174, partie 2, afin de garantir le bon fonctionnement des équipements.

Il est demandé de respecter une distance de séparation minimale de :

- 12 cm avec les éclairages incandescents.
- 60 cm avec les éclairages fluorescents.
- 1 mètre avec les sources d'énergie supérieures à 10 kVa.

- 2 mètres avec les moteurs électriques.
- 3 mètres avec les lignes à haute tension ou les sources émettrices rayonnantes en HF, VHF, UHF et SHF.

En cas de cheminement parallèle, les câbles seront au moins éloignés de :

Longueur du chemin parallèle	Source < 2KVA	Source de 2 à 5 KVA	Source > 5 KVA
3 m	10 mm	20 mm	40 mm
5 m	15 mm	40 mm	80 mm
10 m	30 mm	70 mm	140 mm
15 m	50 mm	120 mm	240 mm
20 m	60 mm	150 mm	300 mm
> 30 m	120 mm	300 mm	600 mm

Le croisement perpendiculaire est autorisé à l'exception du croisement avec les éclairages fluorescents.

Dans un environnement fortement perturbé, il conviendra de prévoir une protection électromagnétique renforcée pour le passage des câbles (dalles marines capotées, par exemple).

Le système de câblage proposé doit respecter les exigences de compatibilité électromagnétique décrites dans la norme EN 50288 et ISO 11801 2e édition qui stipule que le câblage installé ne devra en aucun cas détériorer le bon fonctionnement des équipements qui y sont reliés. Le titulaire devra garantir cette conformité.

3.7.3.2 - CHEMINEMENT DES CÂBLES

Tous les chemins de câbles, distributions primaires et secondaires, tube MRB, goulottes, passages de murs, etc., seront dimensionnés pour qu'aucun câble ne dépasse et pour offrir une réserve de place et de poids de 30 % minimum en vue d'éventuelles extensions.

Quels que soient les dispositifs de passage retenus, ils devront respecter les contraintes d'environnement du chapitre 3.1.

En aucun cas les câbles ne devront reposer sur un faux plafond ni être collés, agrafés ou attachés sur des matériaux.

Les câbles devront toujours être posés dans un chemin de câble, sous tube, sous goulotte ou fourreau. Quel que soit le cas de figure rencontré, un câble doit toujours être posé et protégé dans un support adapté à la configuration des lieux.

// La fermeture des faux plafonds et des goulottes ne pourra être effectuée qu'après contrôle du respect du présent C.C.T.P.

3.7.3.3 - CHEMINS DE CÂBLES

Les câbles seront posés et fixés dans des chemins de câbles.

La pose des chemins de câble "vidéo" et/ou le respect des préconisations qui y sont associées se font sous la responsabilité du titulaire.

Les chemins de câbles prévus pour les câbles de courants faibles ne devront en aucun cas être partagés avec d'autres ressources.

Les chemins de câbles horizontaux seront obligatoirement en tôle galvanisée ajourée de type "dalle marine" à bords non coupants, les chemins de câbles verticaux seront en fils d'acier soudé ou de type "dalle marine".

Les changements de direction seront réalisés à l'aide de pièces préformées pour les dalles, et de pliages et de découpes effectuées aux coupes de boulon avec mâchoires dites "coupe d'angle tondeuse". Les bords abrasifs résultant des découpes seront limés.

Pour assembler 2 sections différentes de chemins de câbles, il sera utilisé les systèmes conçus, testés mécaniquement et fournis par le fabricant de chemins de câbles. La résistance électrique des jonctions n'excédera pas 50 mΩ et sera testée conformément à la procédure décrite dans la norme CEI 61537.

Lorsque la configuration des lieux nécessite une interruption du cheminement, l'espace entre les 2 chemins de câbles ne devra en aucun cas excéder 1 mètre et les câbles devront être protégés dans un fourreau de type CAPRIPLAST.

Tous les chemins de câbles seront mis à la terre d'une façon continue, par un conducteur de cuivre nu (non gainé) d'au moins 16 mm² de section, circulant sur l'aile extérieure des chemins de câbles. Ce conducteur sera fixé par bornes de laiton non isolées à chaque changement de section, de direction et au minimum tous les 5 m, et par collier plastique à chaque mètre.

Les chemins de câbles suspendus le seront par l'intermédiaire de pendards avec semelles et consoles de support. Si nécessaire, pour éviter l'inclinaison des pendards, ceux-ci seront renforcés par une jambe de renfort.

Les moyens de fixation des chemins de câbles doivent être également prévus pour supporter le surplus de poids engendré par les éventuelles extensions. Les écartements entre les fixations des chemins de câble devront garantir la rigidité de l'ensemble, y compris avec le poids maximum pouvant être en mis en place.

Tous les accessoires d'assemblage et de mise à la terre seront dus.

Des précautions particulières seront prises au droit des joints de dilatation des bâtiments afin que les chemins de câbles et les canalisations qu'ils supportent puissent subir sans dommage les déplacements résultant du jeu normal des bâtiments.

Les chemins de câbles dans les locaux ouverts au public devront être clos par un couvercle lorsqu'ils sont visibles.

Pour les lieux où l'installation des chemins de câbles n'est pas possible, les câbles devront être supportés et protégés par des aménagements adaptés, validés par le maître d'œuvre.

3.7.3.4 - GOULOTTES

Les goulottes seront composées :

- D'un corps ou partie arrière.
- De couvercles.
- De joints de couvercles.
- D'éclipses de jonction.
- D'angles préformés d'une seule pièce.
- D'embouts de fermeture.
- De joints de traversée de paroi.

Dans le cas où le chantier prévoit la pose de goulottes mixtes (courants forts/courants faibles), les goulottes devront avoir :

- Le compartiment du haut sera réservé aux câbles de courants faibles.
- Le compartiment du bas sera réservé aux câbles de courants forts.
- En cas d'installation en plinthe (directement au sol) le premier compartiment devra être surélevé d'au moins 30 mm pour permettre l'installation des fiches électriques coudées (conformément à la norme NF C 15-100 § 555.2.8 : l'axe des alvéoles doit se trouver à au moins 50 mm au-dessus du sol fini).

- En cas de traversée de paroi, un joint de traversée de paroi sera utilisé.
- Une éclipse de jonction sera utilisée entre 2 sections de goulotte.
- Un joint de couvercle sera utilisé entre 2 sections de couvercle.
- Les goulottes seront fixées aux parois à l'aide de vis et chevilles adaptées au support.

// les descentes verticales depuis le faux plafond se feront par le même type de goulotte.

3.7.3.5 - FOURREAUX

Il convient de protéger les câbles dans des fourreaux de type MRB ou Capri Plast, notamment dans le cas de :

- De traversées de cloison accessible au public.
- De jonction entre 2 chemins de câbles discontinus accessible au public.
- De jonction entre un chemin de câble et une goulotte accessible au public.
- De configuration empêchant la pose d'un chemin de câble ou d'une goulotte.

3.7.3.6 - PROTECTION CONTRE LES INCENDIES

Le titulaire devra se conformer aux directives nationales et locales en vigueur concernant la protection contre les incendies. Il devra en particulier sceller les coupe-feux qu'il a dû ouvrir afin de poser le câblage.

3.7.3.7 - GAINÉ MÉTALLIQUE TYPE MRB

Conduits rigides en acier zingué ou inoxydable blindé :

- Pose apparente.
- Manchons pour raccord de tubes par filetage.
- Finition : acier inox ou zingué.

Y compris accessoires.

//Pour les parties terminales et courbes, le tube rigide sera remplacé par de la gaine souple métallique.

3.7.3.8 - CÂBLES ETHERNET

Les câbles Ethernet présenteront au minimum les caractéristiques suivantes :

- Câble droit, blindé.
- Câble PIMF (paires dans un feuillard métal)
- Prévu pour les applications gigabit / 10 gigabit.
- Support 10/100/1000Base-TX.
- Catégorie 6 (A) ou plus.
- 26 AWG.
- 4 paires.

Y compris les connecteurs RJ45 anti-arrachement installé en saillie (étanche en extérieur).

3.7.3.9 - COMMUTATEURS RÉSEAU

Les commutateurs dédiés au réseau de sûreté seront à la charge de la DSISN.

Le titulaire aura à sa charge la transmission de tous les éléments techniques nécessaires au dimensionnement des commutateurs par la DSISN (nombre et localisation de points d'accès, bilan de puissance des équipements à raccordement POE).

3.7.3.10 - ALIMENTATION ÉLECTRIQUE

3.7.3.10.1 - Protection électrique

Les installations (matériels actifs branchés sur le secteur 220V) seront protégées en tête par des disjoncteurs différentiels 30mA. **Ils devront être étiquetés.** Ils seront dédiés uniquement à la protection du système de vidéoprotection.

3.7.3.10.2 - Prises électriques

Les prises électriques installées en gaine technique devront être étanches. Celles installées sous coffret, baie 19 pouces ou cache-borne pourront être de type modulaire.

Prévoir une prise supplémentaire (pour la servitude et/ou maintenance).

3.7.3.10.3 - Terres

La mise à la terre des matériels actifs, de la baie ou des grilles de fond de coffret sera effectuée avec un câble vert/jaune de section minimum de 2,5mm².

Les câbles de terre (matériels actifs) seront reliés à la terre du bâtiment.

Nota : Prévoir la mise en place de toutes les fournitures pour mener à bien cette mise en conformité électrique (câbles électriques, fourreaux, coffret cache-borne, DPN ...).

Toutes les alimentations seront protégées par un 30mA, dédié uniquement au système de sûreté. Les câbles électriques utilisés (RO2V) seront de diamètre 3x2.5mm² et seront directement raccordés aux différents tableaux divisionnaires. Ils seront conformes pour une utilisation intérieure et/ou extérieure.

3.7.3.11 - RÉSEAU DE TERRE

Le problème de la mise à la terre est un problème complexe qui met en jeu la sécurité des personnes et influe directement sur les performances du câblage.

La mise à la terre du système de câblage doit être réalisée en conformité avec les recommandations du constructeur et les normes EN50303, EN50174-2 et TIA/EIA-607.

Toutes les terres du réseau support créé doivent être interconnectées (réseau maillé, unique et équipotentiel) et liées à la terre du bâtiment. Une mesure de la valeur de terre du bâtiment devra être effectuée pour s'assurer de sa bonne qualité.

3.7.3.12 - MESURES ET RECETTES DES CÂBLAGES

Cette procédure est lancée quand les prestations de câblages sont terminées afin d'assurer qu'ils ont été correctement exécutés, qu'aucune erreur de câblage ne subsiste et qu'aucun n'a été endommagé pendant sa mise en place.

Cette phase ultime de l'installation sera effectuée par un organisme indépendant et reconnu autre que le titulaire du marché, les frais inhérents à ces mesures sont à la charge du présent marché.

Toutes les mesures effectuées auront pour but de certifier les câblages conformes au projet de norme ISO/IEC DIS 11 801.

3.7.3.12.1 - Mesures statiques

L'ensemble des liaisons sera testé, afin de vérifier que chaque paire torsadée :

- Est correctement connectée à chaque extrémité.
- N'est pas croisée avec une autre paire du même câble.
- N'est pas en court-circuit.
- Respecte les polarités.
- Est bien isolée par rapport aux autres paires et par rapport à la terre.
- Ne dépasse pas la longueur maximale autorisée.

3.7.3.12.2 - Mesures dynamiques

Afin de qualifier l'installation par rapport à des caractéristiques de débit souhaitées, il sera effectué des tests de transmission, d'atténuation et de paradiaphonie.

Ces mesures seront réalisées au moyen d'un testeur WIRESCOPE 250 MHz d'EXPERDATA ou équivalent et devront permettre de vérifier le respect des caractéristiques minimales imposées par le projet de norme ISO/IEC DIS 11 801.

Ces contrôles seront effectués sur les liaisons commutateurs <---> points de livraison.

REMARQUE :

Aucun matériel électronique ne devra être connecté sur le réseau durant les tests.

Le contrôle d'une liaison se fait de bout en bout, y compris le connecteur terminal.

Les résultats de tests sont inscrits sur des bordereaux de mesures.

Les extensions de ce réseau vers les systèmes de détection, intrusion et contrôle des accès seront réalisées par câble bus adapté.

3.7.4 - IMPLANTATIONS RG ET SR (SUIVANT PLANS)

Suivant les plans.

3.8 - VIDÉOPROTECTION

3.8.1 - OBJECTIFS GÉNÉRAUX

Le système de vidéoprotection au sein des parkings pourra poursuivre trois objectifs distincts ou complémentaires :

- La vidéoprotection par dissuasion, implantation de caméras visibles ayant pour objectif d'empêcher le passage à l'acte délictuel.
- La vidéoprotection intervient dès la détection d'une anomalie par un opérateur ou par un Détecteur Automatique d'Anomalie (DAA) et peut apporter un soutien aux salariés intervenants. Cette étape peut également être utilisée en exploitation.
- La vidéo d'élucidation est utilisée uniquement en post-traitement dans, par exemple, un cadre d'enquête judiciaire.

Les caméras selon leurs implantations pourront répondre à trois buts :

- Soit les caméras visionnent des champs larges comme des niveaux de parking.
- Soit les caméras visionnent des champs étroits comme des accès, des escaliers mécaniques ou des couloirs et sont utilisées en identification.
- Soit les caméras dotées d'analyse d'images (embarquée dans les caméras) des champs particuliers comme des lieux sensibles, tels que des points d'attentes (ascenseurs).

Les généralités vidéo principales seront les suivantes :

- Système de vidéoprotection reconnu comme un grand standard dans l'écosystème de la vidéo, compatible, pérenne et efficace, de **conception ouverte** de manière à laisser le libre choix des intégrateurs (mise en œuvre et maintenance) autre que le concepteur (non-propriétaire).
 - Le système VMS devra être entièrement compatible avec le logiciel Milestones déjà en place, dans établissements de Science Po site Saporta et l'Espace Marceau Long.
 - Mise à jour des licences vidéo Milestone Xprotect PRO+ 2019 R3 et des 15 licences caméras associées (ID : M01- C05-133-6C4F3)
 - Architecture serveurs/clients.
 - Une interconnexion devra être fonctionnelle entre les sites de l'IEP,
 - Cartographie (caméras, alarmes, défaut).
 - Communication selon le protocole TCP/IP.
 - Mise en œuvre de machines informatiques correspondant à des machines de constructeurs réputés dans l'écosystème informatiques.
 - Mise en œuvre de caméras de nouvelle génération, nativement IP.
 - Remplacement des caméras analogiques existantes ainsi que le câblage qui restera à la charge de la DSISN (la caméra PTZ existante devra être remplacée par deux caméras fixes).
 - Toutes les caméras seront enregistrées en 24h/24, avec un enregistrement sur détection dans l'image en 25 IPS Full HD sur événement.
-
- Le système de vidéoprotection pourra être fortement communicant avec des Hyperviseurs pour des extensions futures des éléments de sûreté.
 - La DSISN réalisera l'interconnexion entre les sites EPS/SAPORTA et véhiculera les réseaux nécessaires pour le bon fonctionnement d'interconnexion entre les serveurs de vidéo.
 - La matrice des flux du système devra être transmise au plus tôt à la DSISN afin de préparer l'administration du réseau de sûreté.

// une analyse fonctionnelle devra être organisée avec la MOA et les utilisateurs finaux afin de déterminer le mode de fonctionnement.

// une attention particulière devra être apportée sur la mise en œuvre des caméras extérieures, elles ne devront être en aucun cas accessibles au public (pas d'accès à hauteur d'hommes).

3.8.2 - TECHNOLOGIE

Le système sera basé sur le réseau de sûreté, avec communications suivant le protocole TCP/IP.

Le système sera basé sur une architecture client-serveur. Pour des questions de sûreté, les clients seront des clients lourds avec obligation de connexion pour accéder aux données.

Chaque caméra sera adressée et en lien avec le serveur de supervision/enregistrement, installée dans le local vidéo.

L'enregistrement des images issues des caméras sera réalisé sur détection de présence sur disques durs « vidéo » du marché.

Il sera basé sur un logiciel de gestion de vidéoprotection et de gestion vidéo numérique ouverte.

- Plateforme permettant de fonctionner avec une importante palette de constructeurs technologique (caméras, encodeur numérique, enregistreurs numériques,) laissant souplesse, libre choix des marques de matériel et de prestataires (installation et maintenance). Elle sera reconnue comme un grand standard de l'écosystème VMS mondiaux.
- Intégration de fonctionnalité logicielle par brique (ex : analyse d'image).
- Interopérabilité avec des systèmes de sûreté connexes (ex : hyperviseur) :
 - Logiciel basé sur architecture client-serveur :
 - Communicant sur protocole TCP/IP.
 - Base de données SQL.
 - Fonctionnement natif Windows 64 bit,
 - Conforme à la réglementation NDAA.
- Mode de gestion et de diffusion des flux vidéo numériques :
 - Unicast, connexion réseau point à point entre un serveur et un poste informatique qui demande les flux vidéo des caméras. Connexion point à point à multiplier autant de fois qu'il y a de demande.
 - Multicast, connexion réseau, diffusion multipoint, d'un seul point d'émission vers tous les destinataires qui le demande.
- Evolution illimitée :
 - Ajout de serveurs (management/redondance, enregistrement/secours).
 - Ajout de caméras vidéo.
- Prise en charge de l'accélération graphique (GPU).
- Prise en charge de la compression vidéo H 265.
- Gestion de mur d'images, selon les licences et l'éditeur :
 - Logiciel qui reste une toile de fond de collaboration qui facilite l'échange efficace d'informations et la coordination des réponses et activités dans les salles de contrôle.
 - Ils prennent en charge une large gamme d'informations, notamment des vidéos, plans, liens hypertextes, alarmes et messages.
 - Le logiciel de mur d'images est entièrement intégré aux outils de vidéoprotection. Les agents peuvent ainsi partager instantanément des contenus avec d'autres agents sur le mur vidéo, en toute simplicité. Les informations peuvent également être publiées automatiquement sur le mur d'images en fonction d'événements et alarmes déclenchées dans les systèmes VMS.
 - Une prise en charge de toute quantité ou combinaison d'écrans, indépendamment du fabricant. Ils fonctionnent sur des postes informatiques et affichages ordinaires, donnant ainsi la liberté de choisir le matériel répondant le mieux aux besoins et au budget. Ces logiciels emploient également du matériel d'accélération du décodage, pour une performance vidéo de haute qualité et une charge grandement réduite sur l'unité centrale.
 - Grande souplesse d'architecture, car, étant basée sur de simples postes informatiques et brassage informatique, elle permet de modifier ou déplacer le mur d'images.
 - Cette typologie de mur d'images logiciel pourra être gérée par un hyperviseur.

3.8.3 - GÉNÉRALITÉS CYBERSÉCURITÉ DES CAMÉRAS

Toutes les caméras doivent adopter les généralités techniques suivantes :

- L'aspect cybersécurité.
- La certification ONVIF.

- L'analyse d'image intégrée des caméras, sans serveur ni licence supplémentaire facilitant la flexibilité des utilisateurs par les règles d'alertes, la recherche contextuelle à travers la relecture d'image (grâce aux métadonnées qui remontent parfaitement dans les VMS du marché).
- La qualité d'image (Starlight, WDR ou HDR dynamique, excellente résolution...).
- Un système de gestion centralisée doit simplifier le processus de mise à jour des firmwares des caméras et de tous les équipements intervenant dans le périmètre vidéo. Cela inclut la récupération automatique des packages de mise à jour et la gestion du déploiement de manières aussi automatisée que possible.
- Conforme aux réglementations NDAA (National Defense Authorization Act)

La sécurité des données

- Les caméras sont accessibles au travers du protocole HTTP, mais les clients web doivent être réorientés vers le protocole HTTPS grâce au protocole HSTS. Le protocole HTTP peut être désactivé au profit du protocole HTTPS.
- Le protocole Telnet ainsi que le protocole propre au fabricant doivent pouvoir également être désactivés.
- Les flux vidéo doivent être chiffrés et compatibles au format SRTP et RTSPS.
- Les caméras ne doivent pouvoir accepter que les micrologiciels (firmware) signés par le constructeur afin de garantir l'absence de logiciels malveillants (malware).

3.8.4 - CARACTÉRISTIQUES TECHNIQUES MINIMALES DES CAMERAS

3.8.4.1 - CAMÉRA BULLET

Les caméras fixes IP présenteront au minimum les caractéristiques suivantes :

- Résolution vidéo : 5 MP - 2592 x 1944 à 30 images/sec.
- 3 flux vidéo réglables individuellement en H264 et H265.
- Objectif avec une focale variable motorisée de 3.2 à 10.5 mm avec un contrôle de type P-iris.
- Champ de vision réglable Wide-Télé : W (95°x 71°), T (29° x 2°) – Rotation possible à 90° (réglage en mode couloir).
- Plage dynamique de 105 dB WDR minimum (mesurée en accord avec la norme CEI-62676 partie 5) – plage dynamique étendue à 120dB.
- Conformité ONVIF Profil S, G, T, M (EN 50132-5-2, EN 62676-2).
- Les métadonnées seront accessibles via le protocole MQTT présent nativement dans la caméra.
- La caméra sera équipée d'un slot microSD permettant d'enregistrer sur des cartes mémoires jusqu'à 2To.
- Température de fonctionnement : -40°C à +55°C.
- Protection contre l'eau et la poussière : IP 67 (EN 60529).
- Résistance aux chocs : IK10 (EN 62262).
- Montages possibles : plafond, mural, mât.
- Alimentation IP POE+ type 2.
- Fonctions d'analyse vidéo intégrées nativement.

3.8.4.2 - CAMÉRA DÔME

Les caméras dômes extérieures et intérieures présenteront au minimum les caractéristiques suivantes :

- Résolution vidéo : 5 MP - 2592 x 1944 à 30 images/sec.
- 4 flux vidéo H.265 réglables individuellement.
- Objectif avec une focale variable motorisée de 3.4 à 10.2 mm avec un contrôle de type P-iris
- Champ de vision réglable H (29° à 95°), V (22° à 71°) – Rotation à 90° (réglage en mode couloir).

- Plage dynamique de 105 dB WDR minimum (mesurée en accord avec la norme CEI-62676) plage dynamique étendue à 120dB.
- Conformité ONVIF Profil S, G, T, M (EN 50132-5-2, EN 62676-2).
- Les métadonnées doivent être accessibles via le protocole MQTT présent nativement dans la caméra.
- Fonctions d'analyse vidéo intelligente intégrées nativement.
- La caméra doit être équipée d'un slot microSD permettant d'accepter des cartes mémoire jusqu'à 2To.
- Température de fonctionnement : -40°C à +50°C
- Protection contre l'eau et la poussière : IP66 & NEMA type 4X, IK10 pour les caméras extérieures.
- Alimentation IP POE+ type 2.

3.8.4.3 - ALIMENTATION ÉLECTRIQUE

3.8.4.3.1 - Protection électrique

Les installations (matériels actifs branchés sur le secteur 220V) seront protégées en tête par des disjoncteurs différentiels 30mA. Ils devront être étiquetés. Ils seront dédiés uniquement à la protection du système de vidéoprotection.

3.8.4.3.2 - Prises électriques

Les prises électriques installées en gaine technique devront être étanches. Celles installées sous coffret, baie 19 pouces ou cache-borne pourront être de type modulaire.

Prévoir une prise supplémentaire (pour la servitude et/ou maintenance).

3.8.4.3.3 - Terres

La mise à la terre des mâts des aériens (antenne radio) sera réalisée avec un câble vert/jaune de section minimum de 6mm². Celui-ci sera obligatoirement mis sous fourreaux en intérieur et extérieur (norme NF C15-100).

La mise à la terre des matériels actifs, de la baie ou des grilles de fond de coffret sera effectuée avec un câble vert/jaune de section minimum de 2,5mm².

Les câbles de terre (aériens et matériels actifs) seront reliés à la terre du bâtiment ou à la terre des candélabres (suivant l'implantation).

Nota : Les matériels d'enregistrement d'images seront alimentés par une ligne ondulée.

3.8.4.4 - ONDULEUR

Chaque baie équipée, de serveur et/ d'élément actif, se verra équipée d'onduleur rackable. Les onduleurs seront de type **ON-LINE (rackable)** et implanté dans la baie 19 pouces.

Les caractéristiques des onduleurs devront tenir compte des consommations électriques de tous les éléments installés.

3.8.4.5 - BAIE 19''

La baie de sûreté fera 24 U, 800x1000 pour accueillir, les alimentations, les commutateurs, serveur vidéo, poste de gestion vidéo, poste de gestion de contrôles d'accès (y compris tous les accessoires

permettant un fonctionnement optimum du système). En ce qui concerne les bandeaux RJ45, ils restent à la charge de la DSISN. Le titulaire aura à sa charge la réservation des bandeaux RJ45 de la DSISN dans la baie de sûreté.

Elle sera équipée d'une porte ventilée (type nid d'abeilles) avec serrure, d'un système de ventilation actif, d'un porte-document et d'un plateau pour disposer les accessoires.

Elle sera raccordée à la terre du bâtiment.

La charge admissible permettra d'installer la globalité du système de vidéoprotection et le poste de gestion. L'entreprise devra calculer le poids total du matériel.

Cette baie sera installée dans le local serveur au R+3 du bâtiment principal.

3.8.4.6 - ENREGISTREMENT

Le système d'enregistrement numérique devra permettre d'enregistrer en permanence les images de l'ensemble des caméras de vidéoprotection. Les serveurs d'enregistrement numériques des caméras seront installés dans la salle serveur sécurisée.

Le dispositif d'enregistrement numérique permettra d'archiver sur une architecture de disques durs de type RAID 6 la totalité des sources vidéo des caméras du projet, y compris la réserve de capacité.

Le système d'enregistrement numérique, de chaque parking, devra être surdimensionné afin de permettre au système d'évoluer (**6 flux issus de caméras Full HD supplémentaires**).

Seuls les responsables d'exploitation pourront rechercher et visionner les enregistrements (accès par mot de passe).

Afin de respecter l'arrêté de 2007 portant définition des normes techniques des systèmes de vidéoprotection) :

- L'accès aux images enregistrées sera sécurisé par mots de passe personnels sur le logiciel afin que seules les personnes habilitées puissent consulter les enregistrements.
- Les images enregistrées seront automatiquement effacées au-delà du délai légal de 30 jours.
- Un historique d'exploitation consignera automatiquement toutes les opérations de stockage, consultation, effacement d'enregistrement et copie d'image.

3.8.4.7 - FRÉQUENCE ET DURÉE D'ENREGISTREMENT

Les dispositifs d'enregistrements numériques devront être conformes au Code de la Sécurité Intérieure portant définition des normes techniques des systèmes de vidéoprotection.

Les images de l'ensemble des caméras doivent être enregistrées en permanence (sur détection de mouvements 24h/24) avec un enregistrement local en 4CIF, 12ips, quand il ne se passe rien (exemple pas de détection de piéton), en full résolution en 25ips quand un mouvement est détecté (exemple, détection de piéton), sur une durée de 10 jours.

L'enregistrement des images sera réalisé en boucle, les dernières images écrasant automatiquement les premières images.

Cette fonction permettra de conserver les images enregistrées sur une durée déterminée.

Les enregistrements archivés sous format numérique seront donc systématiquement détruits au bout d'une durée maximale de 10 jours, sauf dans le cas d'une enquête judiciaire (réquisition).

En fonction de ces données, l'entreprise devra dimensionner le nombre et la capacité des disques durs de type RAID 6 à installer.

Les images enregistrées seront automatiquement écrasées en fin de capacité mémoire allouée (10 jours de conservation).

3.8.4.8 - SPÉCIFICITÉS DES MATÉRIELS D'ENREGISTREMENT NUMÉRIQUE

3.8.4.8.1 - Spécifications fonctionnelles

Flux multiples :

- Les flux pourront être encodés aux formats de compression numérique MPEG-4, MPEG-2, MJPEG, H.264, H.265, Wavelet ou JPEG2000 permettant un enregistrement en temps réel de chaque caméra ou encodeur.
- Plusieurs flux vidéo, provenant d'une seule ou plusieurs caméras, seront pris en charge.

Multi-diffusions :

- Le système permettra également à une caméra d'être vue simultanément par plusieurs utilisateurs en même temps en utilisant une seule fois la bande passante.
- Le système intégrera une surveillance d'événements unifiés en temps réel.

Stockage :

- Le dispositif d'enregistrement devra permettre d'archiver sur disques durs la totalité des sources vidéo en permanence.
- Le système de vidéoprotection s'appuiera sur une architecture ouverte qui permettra l'utilisation de matériel de stockage non propriétaire et qui n'impose aucune limite sur la capacité de stockage permettant de l'augmenter à tout moment.
- Le système de vidéoprotection possédera des capacités de stockage à long terme sur toute unité de sauvegarde prise en charge par Windows ou Linux.
- Toutes les unités de stockage ou disques de stockage connectés à des PC ou à un réseau pourront être intégrées au système de stockage centralisé :
 - Stockage en réseau (NAS) sur un réseau local ou étendu.
 - Réseaux de stockage (SAN).
 - Disques SCSI/Fibre Channel.
- Ces dispositifs seront paramétrables via l'IHM (interface homme-machine) sur le poste d'exploitation du système.
- Le système offrira également plusieurs solutions pour parer à la perte accidentelle de données. Le système assurera une disponibilité des archives en combinant les solutions suivantes : le système de stockage prendra en charge les serveurs vidéo possédant des capacités d'enregistrement sur périphérique (carte SD, clé USB...) et permettra le transfert automatique et/ou manuel de ces données sur le serveur de stockage.

Les enregistrements pourront être consultés selon plusieurs critères :

- Intervalle de temps.
- Demande de lecture.
- Événements d'analyse vidéo.
- Détection de mouvement.
- Signets.
- Alarmes.
- Événements d'unité hors ligne.

// Le système de vidéoprotection ne requerra aucun matériel de gestion, d'enregistrement, d'exploitation, de sauvegarde et de virtualisation propriétaire pour l'enregistrement et la surveillance vidéo.

3.8.4.9 - ARCHITECTURE DE FONCTIONNEMENT

L'architecture des serveurs et des stockeurs sera de type RAID 6, ou techniquement équivalent.

En cas de défaillance d'un disque, le fonctionnement normal du système devra être maintenu sur les autres disques durs. Le disque défectueux sera extrait et remplacé. Cette opération pourra s'effectuer rapidement et simplement en conservant le fonctionnement normal des autres disques durs.

En cas de panne, les éléments seront redondants et échangeables à chaud (sous tension) :

- Disques durs.
- Alimentation.
- Ventilateurs...

En cas de dysfonctionnement d'un disque dur, le disque de rechange disponible en stock sera utilisé et la reconstruction du groupe de disques durs RAID sera réalisée automatiquement.

Le système sera un environnement multi-utilisateur et multitâche.

Le système prendra en charge un environnement réseau distribué sur IP.

Toutes les communications entre les serveurs, les postes clients et les contrôleurs matériels seront basés sur le protocole TCP/IP.

L'architecture distribuée permettra :

- Un haut niveau de fiabilité.
- Une évolutivité maximale.
- Une indépendance matérielle.

La solution doit disposer d'un système de sauvegarde de son disque système.

Les fichiers contenant les paramètres de configurations des équipements doivent également être sauvegardés.

La solution devra pouvoir disposer d'un système de restauration de la sauvegarde.

Les procédures relatives à ces opérations seront fournies par le titulaire du présent marché.

3.8.4.10 - CARACTÉRISTIQUE TECHNIQUE MINIMUM

Quelle que soit la configuration du système choisie : serveurs distincts (serveur de gestion + serveur enregistreur) ou un serveur regroupant toutes les fonctions, les serveurs doivent satisfaire aux prérequis minimums matériels suivants :

Ils seront de type rackable de :

- Microprocesseur de type Intel Xeon E5 ou supérieur.
- Disques durs système montés en « raid 1 » SSD.
- Disques durs de données montés en « raid 6 » HDD.
- Possibilité d'extension par adjonction d'une alvéole supplémentaire.
- 32 Go mémoire RAM.
- Double alimentation.
- Carte réseau multiport gigabit Ethernet.
- Carte graphique standard multiport (VGA, DVI, HDMI, DP).
- ...

3.8.4.11 - SÉCURITÉ DU SYSTÈME

Les communications entre les serveurs et postes clients (serveur vers client et client vers serveur) sont chiffrées. La méthode de chiffrement est au minimum un algorithme de chiffrement AES sur 128 bits ou équivalent.

Les applications client seront protégées par mot de passe. Les mots de passe sont stockés sous forme chiffrée dans la base de données du serveur de configuration.

Le système devra intégrer un service de surveillance. Le service de surveillance devra analyser en permanence l'état de l'installation (services, serveurs, caméras...).

En cas de dysfonctionnement ou de panne sur un des éléments de l'installation, le service de surveillance devra mettre en œuvre un processus d'avertissement, y compris en surveillance réseau (SNMP).

L'interface utilisateur (IHM) intégrée à la plateforme unifiée de sécurité devra fournir à l'utilisateur un état global et détaillé du système et de ces sous-systèmes.

L'interface de surveillance devra fournir une interface graphique pour contrôler et surveiller la plateforme unifiée de sécurité.

3.8.4.12 - APPLICATION SERVEUR

Le système doit être structuré autour d'une architecture de type clients / serveur.

Le serveur d'application doit disposer d'une interface horaire synchronisée sur une source de référence fournie par le client. Il sera serveur d'horloge de tous les équipements installés sur le réseau.

Les applications serveur doivent être compatibles avec plusieurs systèmes d'exploitation 64 bits, dont Windows 11, Windows Server 2019 **et 2022**. Les serveurs virtuels doivent être implémentés avec Windows Server 2019 au minimum.

Les serveurs de base de données du système doivent être conçus pour fonctionner avec SQL Server ou MySQL. Les applications du système de vidéoprotection ne doivent imposer aucune limite sur le nombre de machines pouvant être connectées en réseau afin de constituer un système de serveur d'archivage distribué.

Le système doit être constitué des éléments suivants :

Serveur de management

Le serveur de management doit pouvoir établir des connexions, afficher et recevoir des informations de configuration centralisées. Il aura la capacité d'être redondé et virtualisé.

Système d'archivage

- Les serveurs d'archivage sont physiques et localisés dans les locaux techniques sécurisés des parkings placés sous vidéoprotection.
- Il doit prendre en charge l'exploitation centralisée des unités vidéo (encodeurs et décodeurs) du système.
- Il doit être capable de détecter automatiquement les nouvelles unités qui sont ajoutées au système.
- Il doit enregistrer les flux vidéo en fonction des horaires spécifiés par les utilisateurs.
- Il doit gérer également un index des événements, des repères de mouvement et des signets dans une base de données relationnelle pour aider l'utilisateur à trouver rapidement et facilement toute séquence vidéo ayant un intérêt.

- Il doit intégrer des fonctionnalités comme le chiffrement des commandes et des signatures électroniques.
- Il doit permettre la relecture des sauvegardes sur bande ou dans des dossiers.
- Il doit comporter un archivage complémentaire.

Supervision système

- Le système doit intégrer un service de surveillance qui doit analyser en permanence l'état de l'installation (services, serveurs, caméras, postes clients...).

3.8.4.13 - CAPACITÉS DU SYSTÈME DE VIDÉOPROTECTION SUR IP

L'interface utilisateur doit être composée d'une seule interface de configuration client et d'une seule interface de surveillance client (Exploitation).

Les modules serveur du système doivent être compatibles avec plusieurs systèmes d'exploitation 64 bits, dont Windows 11, Windows Server 2019 à minima et ultérieur.

Les modules clients du système doivent s'exécuter sous Windows 11, 64 bits.

Le système est conçu avec des outils de conception les plus récents et les plus performants.

Les serveurs de base de données du système sont conçus pour fonctionner avec SQL Server ou MySQL.

Capacité et évolutivité du système

Le système doit pouvoir évoluer d'une unité à la fois, par exemple : 1 identifiant à la fois, 1 caméra à la fois, etc.

Le système doit permettre de prendre en charge un nombre illimité de caméras. Chaque serveur vidéo prendra en charge plusieurs connexions caméras.

3.8.4.14 - DEMANDE AUTORISATIONS

Afin de garantir la possibilité de déploiement des systèmes sur l'établissement, une demande d'autorisation préfectorale sera initiée par le maître d'ouvrage, dès lors que des caméras visualisent la voie publique ou un espace ouvert au public.

Le titulaire devra remettre les éléments nécessaires (plan d'implantation et de couverture des caméras, dimension des affichettes) au maître d'ouvrage afin qu'il puisse réaliser la demande auprès de la Préfecture.

Cette demande d'autorisation précisera :

- L'adresse du site (parking concerné).
- Un rapport de présentation du projet (type APD) comportant :
 - Le nombre de caméras prévues.
 - Leurs implantations.
 - Leurs champs visuels.
 - La localisation du local d'enregistrement.
 - Les moyens de conservation des images.
 - Les moyens de sécurisation de l'accès au local.
 - La durée de conservation des images.
 - La désignation des personnes susceptibles d'accéder aux images.
 - Le type d'affichage d'information du public.

- Un plan masse.
- Un plan de détail avec implantations et champs visuels.

3.8.5 - VISUALISATION ET TRAITEMENT DES IMAGES

3.8.5.1 - MONITEUR D'IMAGES LCD 27"

Résolution Full HD 1 920 x 1 080 pixels.
Filtre en peigne numérique 3D avec désentrelacement pour une vidéo de grande qualité.
Rapport de contraste élevé.
Adaptés aux applications 24h/24 7j/7.
VGA, DVI, S-Vidéo, BNC et HDMI.
Désentrelacement du mouvement.
Incrustation d'image (PIP).
Angle de visualisation : H178° / V 178°.
Surface antireflet.

Il sera possible d'afficher, une mosaïque d'images ou de choisir d'afficher une image en plein écran sur l'écran LCD 27'.

La composition de l'affichage des images (quadra-vision, multi-vision, image plein écran) sur l'écran LCD 27" sera configurable par l'opérateur.

Implantation : 2 écrans 27" pour le poste d'extraction au local serveur R+3 et 2 écrans 27" pour le poste de gestion dans le bureau d'accueil du site (poste de travail logistique) au RDC du bâtiment.

3.8.6 - CARACTÉRISTIQUES FONCTIONNELLES DU POSTE D'EXPLOITATION

Le poste d'exploitation permettra de superviser le système de vidéoprotection et d'accéder aux enregistrements vidéo sur la station de travail.

Au titre du marché, le titulaire devra la mise en œuvre et la programmation des postes d'exploitation.

Des plans graphiques représenteront les lieux où sont installées les caméras.

La navigation entre les plans sera sélectionnable à la souris par les icônes. Les actions sur ces icônes seront transmises directement au système.

La représentation graphique fera apparaître l'état du matériel actif, en défaut, en alarme...

Les modes opératoires, utilisant notamment des icônes, devront être particulièrement simples et efficaces pour afficher une caméra sur un moniteur, contrôler une séquence sur un moniteur vidéo, contrôler des salves de commutation de caméras sur plusieurs moniteurs, piloter les télécommandes ou les prépositions des caméras avec gestion de priorité, passer dans un mode pré configuré de gestion de crise ou de ronde d'une caméra dôme.

Des reports d'alarmes seront disponibles pour reprendre toutes les informations ² équipements installés : défaut de signal vidéo, défaut d'alimentation caméra, passage en mode secours, alarme distante, défaut disque dur, défaut liaison réseau ...

Des historiques horodatés de tous les événements seront disponibles.

L'exportation d'images ou de séquences vidéo sera possible.

Plusieurs niveaux hiérarchiques permettront d'accorder des droits d'utilisateurs selon des mots de passe (logins personnels et non pas commun aux opérateurs). Un mode administrateur, un mode système réservé aux techniciens et un mode opérateur seront notamment disponibles.

En mode administrateur, les fonctions suivantes seront disponibles :

- Configuration de tous les équipements du système.
- Gestion profil et droit d'accès de chaque poste.
- Attribution et personnalisation des objets qu'un poste d'opérateur peut accéder.
- Paramétrage des macros et des scripts pour créer des fonctions.
- Définition de calendrier type pour actions automatisées.
- Gestion du masquage dynamique des caméras.

Le logiciel sera interfacé avec les enregistreurs numériques pour rechercher et consulter des séquences avec sélection de dates et horaire, de sites, d'événements ...

Le logiciel développé sous un environnement convivial de type Windows devra les fonctionnalités suivantes :

- Cartographie : gestion d'une arborescence de plans en format couramment utilisé (fichier DWG, DXF). Ces plans concerneront les zones visualisables par les caméras.
- La sélection automatique des images d'une caméra sur un moniteur à partir des plans graphiques au moyen de la souris. L'opérateur cliquera simplement sur l'espace exact qu'il souhaite visualiser ou sur la caméra sur le plan graphique et le logiciel choisira et sélectionnera automatiquement la caméra permettant de visualiser la zone choisie.
- Afin de faciliter et d'automatiser l'exploitation des opérateurs, l'exécution automatique de cycles et de prépositionnements sera disponible.
- Le pilotage des caméras mobiles au moyen d'un joystick (aussi de la souris et du clavier).
- Poursuite automatique.

Le logiciel permettra :

- Un encodage au format H.265, H264.
- Wise Stream.
- Tous les événements d'alarme, notamment la classification sonore, le maraudage et la gestion des files d'attente.
- Réglage de la mise au point automatique.
- Prise en charge des caméras multidirectionnelles.
- Mode Couloir.
- HTTPS.
- Réglage de l'heure.
- Configuration du profil de caméra / de l'image.
- Synchronisation des préréglages PTZ.

3.8.7 - STATION DE TRAVAIL (GESTION DES D'IMAGES)

La station de travail présentera au minimum les caractéristiques suivantes :

- Processeur I7 minimum ou équivalent, 3,7 GHz Turbo, multi-cœurs HT.
- Carte graphique type Quadro, équipée d'au minimum 2Go de mémoire et 4 sorties HDMI et/ou Display Port.
- SDRAM DDR3 16 Go à 1866 MHz.
- Disque dur SSD.

La station permettra :

- Le pilotage de l'ensemble des caméras et l'affichage des images en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic de souris,
- L'affichage de la cartographie avec emplacement des équipements
- La gestion de la main courante des événements.

Implantation : Un poste d'extraction des vidéos placées dans le local serveur du R+3 et dans le bureau d'accueil du site (poste de travail logistique) au RDC du bâtiment .

3.8.8 - DISPOSITIFS D'IDENTIFICATION DES IMAGES

Chaque image des caméras sera identifiée par l'indication en clair de la zone visualisée (adresse, bâtiment...). Cette indication sera dynamiquement asservie à la position de l'axe optique de la caméra. Le nombre de libellés ne sera pas limité et chaque libellé comprendra au moins 16 caractères alphanumériques, y compris les espaces.

3.8.9 - AFFICHETTES DE SIGNALISATION

Affichettes plastifiées autocollantes.

Dimensions 150x200.

La signalétique sera définie par le MOA, mais respectera les préconisations CNIL./RGPD.

3.9 - CONTRÔLE D'ACCÈS

Le contrôle d'accès sera réalisé en prenant en compte les prescriptions particulières suivantes :

- Le système de contrôle d'accès sera de type iPerflex du constructeur SECURE Sytems & Services ou équivalent. Le système devra être totalement compatible avec le système de contrôle d'accès déjà en place (BDD et système) des établissements de Science Po, le site Saporta et l'Espace Marceau Long.
- Les lecteurs de badges utilisés seront de type Mifare Desfire EV3 et compatible avec les badges Mifare déjà déployés.
- Les UTL devront être équipées au maximum à 85% de leur capacité.
- Les UTL devront être placés dans des locaux sécurisés, étant eux même sous contrôle d'accès (local serveur au R+3, local transformateur...) ou coffrets DSISN (coffret n° 6, 7, 8, 9).
- Le zonage du site répondra au principe fonctionnel,
- Le système sera en mesure de gérer les deux types d'ouverture des portillons automatique dans les deux sens de circulation, soit l'ouverture à 600 mm et l'ouverture à 900 mm,
- L'exploitation des retours d'alarmes du contrôle d'accès sera gérée par serveur situé à Saporta.
- Le système de contrôle d'accès fonctionnera exclusivement sur le réseau sécurisé de fonctionnement de Science Po,
- Fourniture de 500 badges au format Mifare Desfire.
- La transmission des informations d'alarmes (badges non autorisés, porte forcée, porte ouverte trop longtemps, badge perdue, volé non valide, inconnu, appui bouton poussoir, activation BBG vert) sera gérée par un poste client placé dans le local serveur.
- La DSISN réalisera l'interconnexion entre les sites EPS/SAPORTA et véhiculera les réseaux nécessaires pour le bon fonctionnement des boîtiers UTL du contrôle d'accès.
- La matrice des flux du système devra être transmise au plutôt à la DSISN afin de préparer l'administration du réseau de sûreté.

Récapitulatif des accès à placer sous contrôle :

Tranche ferme :

- Local serveur R+3.

- Local transformateur désaffecté.
- Accès AS2.
- Accès AS3.

Tranches optionnelles :

- Accès AS6.
- Séparation SP1.
- Séparation SP2
- Séparation SP3.

// Une analyse fonctionnelle devra être organisée avec la MOA et les utilisateurs finaux afin de déterminer le mode de fonctionnement.

3.9.1 - DESCRIPTIF DES MATÉRIELS

Le système sera constitué de plusieurs entités de différents niveaux.

Niveau 0 : Capteurs, relais

- Les détecteurs d'ouverture.
- Boîtier Bris de Glace vert.
- Les lecteurs de badges.
- Verrouillages.

Niveau 1 : Automate réseau Ethernet, Automates de terrain

- Réseau Ethernet :
 - Unité de Traitement Local des informations (U.T.L).
- Bus de terrain :
 - Module de porte.
 - Hub Radio.

Niveau 2 : Système de supervision Serveur et les postes clients.

3.9.1.1 - U.T.L

Les UTL seront raccordées directement sur un réseau Ethernet sécurisé de Science Po. Sur ce réseau seront raccordés aussi le serveur centralisé, et les postes clients de gestion des badges.

Les U.T.L devront être en mesure de communiquer entre elles par le biais du réseau pour assurer toutes interactions ou asservissements.

Les capacités de base

- Contrôleur d'accès (jusqu'à 110 000 badges).
- Fonctionnement autonome avec ses périphériques propres (modules de gestion des accès).
- Liaison temps réel avec le système par le réseau Ethernet en http ou https.
- Mise en œuvre rapide, facile et sécurisée, web serveur embarqué.
- Permet de contrôler en direct jusqu'à 4 accès, 8 lecteurs/claviers de technologies multiples.
- (1 des 4 bus RS485 servant de liaison avec le module de porte).
- Gestion de 12 entrées (2, 4 ou 6 états).

Cette carte se déclinera en 2 versions :

- UTL 4, qui gère seul sans esclave jusqu'à 4 accès (jusqu'à 8 lecteurs) et 12 Entrées/ 10 Sorties (dont 6 transistorisées).
- UTL 32, qui gère jusqu'à 32 accès au travers de ces esclaves (module de portes). Il gère 268 entrées (2, 4 ou 6 états) et 170 sorties.

Il est possible également d'utiliser un de ces 4 bus de terrain pour gérer un ou plusieurs accès localement.

Un upgrade logiciel pourra transformer une UTL 4 en UTL 32 est possible.
Physiquement ce sont les mêmes cartes, il n'y a donc pas de contrainte sur le matériel de maintenance.

Les UTL 4 et UTL 32 pourront être mis en œuvre :

- En coffret PVC, avec ou sans alimentation et avec ou sans batteries.
- Sur rail DIN ou rack.

3.9.1.2 - MODULE DE PORTE

Le module de porte déportée esclave de l'automate « maître » UTL pour la gestion des accès de porte.

Cette carte se déclinera en 2 versions :

- Module de porte 4 accès: Contrôle de 4 accès en entrée/sortie ou sortie libre.
- Module de porte 2 accès : Contrôle de 2 accès en entrée/sortie ou sortie libre.
- Liaison vers UTL et autre module de porte par bus RS485 dédié.
- Permet de raccorder 4 accès, 8 lecteurs/claviers/biométrique de technologies multiples (si les lecteurs sont adressables).
- Gestion de 8 entrées (2, 4 ou 6 états).
- Pilotage de 10 sorties (4 relais, 6 transistors).
- Fonctionnement de la carte et du bornier standard : - 10°C, + 55°C.

3.9.1.3 - LECTEUR DE BADGES

Les lecteurs seront positionnés pour permettre une ouverture en entrée seulement ou en entrée et sortie.

Le lecteur de badges devra être fixé à 1.3 m par rapport au sol.

Les lecteurs de badges :

- Ils devront utiliser le protocole de communication RS485.
- Compatible Mifare Desfire EV3 et Mifare Classic.
- De 13,56 MHz qui associe la distance de lecture offerte par la proximité et la sécurisation des échanges entre la carte et le lecteur.
- De type proximité passif avec une distance de lecture de l'ordre de 8 cm maximum pour les accès piétons.

3.9.1.4 - VERROUILLAGE

Les verrouillages pourront être de différents types en fonction des ouvrants à contrôler :

- Serrure électromécanique outdoor pour le portillon métallique :
 - Avec retour d'information porte fermée, mais pas verrouillée.
 - Avec retour d'information porte forcée.

- Avec retour d'information déverrouillage par cylindre.

3.9.1.5 - AVEC RETOUR D'INFORMATION PORTE FORCÉE. BBG VERT (BOÎTIER BRIS DE GLACE)

Les Boîtier Bris de Glace seront conformes à la norme EN 54-11 et la NFS61-936.

Déclencheurs manuels à membrane déformables avec indicateur d'alarme (visuel et sonore).

Le BBG devra être fixé à 1.3 m par rapport au sol et de couleur verte.

Il comportera deux contacts :

- Un contact pour la coupure de l'alimentation de la serrure libérant la porte.
- Un contact d'information pour un report vers la supervision du contrôle d'accès.

3.9.1.6 - DÉTECTEUR D'OUVERTURE PORTE (DO)

Chaque ouvrant devra avoir son D.O intégré au système de verrouillage (serrure, ventouse) ou en supplément sur l'accès si non existant pour être relié à une entrée du système de contrôle d'accès qu'il pourra contrôler, superviser l'état de l'accès et déclencher les alarmes type « effraction porte » et « porte ouverte trop longtemps ».

3.9.2 - PRINCIPE DE CÂBLAGE D'UNE PORTE DE CONTRÔLE D'ACCÈS

Un lecteur implanté à proximité de la porte à une hauteur d'environ 1,30m du sol.

Un automate UTL et un module de porte contrôlant ce lecteur, implanté soit dans un faux plafond soit dans une zone technique dédiée.

Dans tous les cas le module électronique devra être situé dans la zone protégée par le lecteur de badges.

Il est donc indispensable de raccorder ce module à l'automate UTL et de s'assurer que celui-ci n'est pas déjà complet en capacité de gestion de lecteurs de badges.

Attention il est important de noter que le lecteur de badges est raccordé uniquement via son module de porte.

Prendre en compte :

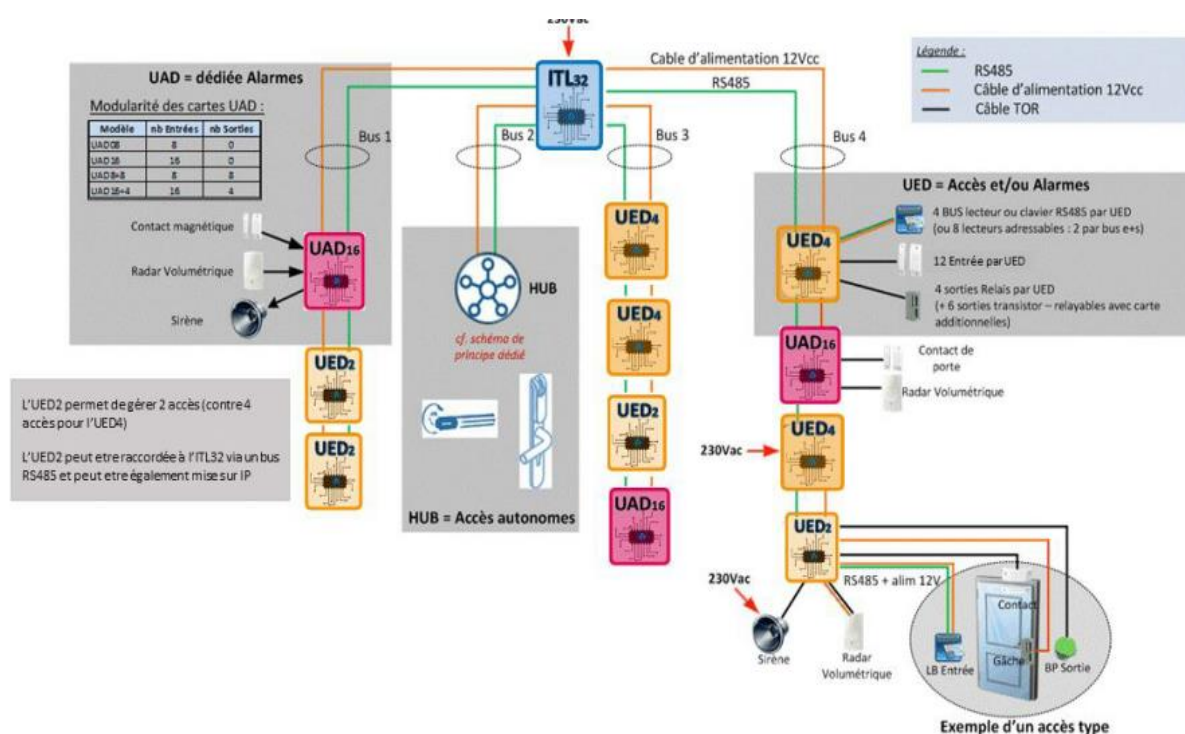
- Les coffrets d'intégration.
- Les alimentations des modules, des lecteurs et des capteurs.
- Les alimentations des serrures électriques (prévoir des alimentations séparées entre les serrures, les UTL et les lecteurs).
- Les batteries.

Conseils/ Précautions :

- Ne pas faire passer dans un seul et même câble multipaire la commande de la serrure, la remontée d'informations et le dialogue UTL/Lecteur de badges.
- Pour éviter les perturbations et préserver la durée de vie des relais lors de la commande de charges celtiques (Gâches électriques, Ventouses, Relais de commande...), il est obligatoire d'installer des diodes de roue libre (pour les organes alimentés en tension continue uniquement) ou des varistances pour supprimer les parasites générés lors de la commande de ces organes. Les protections doivent être installées au plus près des organes de verrouillage.

- Dans beaucoup d'environnements, les câbles bus peuvent être parasités par des éléments tels que des tubes « fluo », il est obligatoire d'utiliser du câble blindé type Belden ou équivalent.
- Les sections et longueurs doivent faire l'objet de calculs précis pour éviter les fortes chutes dues à d'importantes longueurs et/ou consommations.
- Le Boîtier Bris de Glace (BBG) doit agir directement sur la commande de l'organe de verrouillage. En effet, c'est un organe de sécurité des personnes, il doit permettre d'ouvrir, même en cas de panne de l'électronique d'ouverture de la porte. Il est demandé de remonter l'état du contact BBG sur le logiciel de supervision, alors un BBG double contact est nécessaire.
- **Toutes portes contrôlées par badges doivent être asservies par le système SSI du bâtiment concerné. Cette commande coupera directement l'alimentation du moyen de verrouillage et sans passer par système tiers intermédiaire.**
- Tous les câbles de liaison avec le verrouillage (commande, remontée d'informations, etc.), lorsqu'ils sont reliés à la partie mobile de la porte (ils passent donc dans un manchon de protection), doivent être des câbles multibrins souples, pour éviter qu'ils ne cassent.
- Les alimentations des organes de verrouillage ne doivent pas être les mêmes que les alimentations des organes de commande. Il est indispensable de prévoir des alimentations séparées, dont les caractéristiques de puissance sont adaptées à ou aux organes de verrouillage. Ces alimentations devront notamment être capables de délivrer les pics de courant éventuels créés lors des commandes.

3.9.2.1 - SCHÉMA DE PRINCIPE D'ARCHITECTURE DE TERRAIN



3.9.2.2 - ALIMENTATION ÉLECTRIQUE

Protection électrique

Les installations (matériels actifs branchés sur le secteur 220V) doivent protéger en tête par des disjoncteurs différentiels 30mA. **Ils devront être étiquetés.** Ils seront dédiés uniquement à la protection du système de contrôle d'accès.

Terres

La mise à la terre des matériels actifs, de la baie ou des grilles de fond de coffret sera effectuée avec un câble vert/jaune de section minimum de 2,5mm².

Les câbles de terre (aériens et matériels actifs) seront reliés à la terre du bâtiment ou à la terre des candélabres (suivant leur implantation).

Nota : Prévoir la mise en place de toutes les fournitures pour mener à bien cette mise en conformité électrique (câbles électriques, fourreaux, coffret cache-borne, DPN ...).

3.9.2.3 - TOUTES LES ALIMENTATIONS SERONT PROTÉGÉES PAR UN 30mA, DÉDIÉ UNIQUEMENT AU SYSTÈME DE SÛRETÉ. LES CÂBLES ÉLECTRIQUES UTILISÉS (RO2V) SERONT DE DIAMÈTRE 3x2.5MM² ET SERONT DIRECTEMENT RACCORDÉS AUX DIFFÉRENTS TABLEAUX DIVISIONNAIRES. ILS SERONT CONFORMES POUR UNE UTILISATION INTÉRIEURE ET/OU EXTÉRIEURE. RÉSEAU DE TERRE

Le problème de la mise à la terre est un problème complexe qui met en jeu la sécurité des personnes et influe directement sur les performances du câblage.

La mise à la terre du système de câblage doit être réalisée en conformité avec les recommandations du constructeur et les normes EN50303, EN50174-2 et TIA/EIA-607.

Toutes les terres du réseau support créé doivent être interconnectées (réseau maillé, unique et équipotentiel) et liées à la terre du bâtiment. Une mesure de la valeur de terre du bâtiment devra être effectuée pour s'assurer de sa bonne qualité.

3.10 - VISIOPHONIE

Dans le cadre du projet de sécurisation, il sera déployé de la visiophonie sur les accès périmétriques principaux. Le système devra être de technologie IP qui aura les organes suivants :

- Platine Vidéo,
- Moniteur de réception.

Le système peut comporter plusieurs platines ou plusieurs moniteurs. L'ensemble sera programmable à l'aide d'une interface Web.

Les adresses IP seront modifiées suivant le plan applicatif fourni par DSISN.

Récapitulatif des accès placés sous contrôle :

Tranche ferme :

- Accès AS2.

Tranche opérationnelle :

- Accès AS3.
- Accès AS6.
- Séparation SP2.
- Séparation SP3.

3.10.1 - DESCRIPTIF

Le système de gestion de l'accès global au bâtiment permettant de gérer la visiophonie PHMR par bouton des services à appeler. La réception sera réalisée sur poste chef à écran LCD tactile qui permettra l'ouverture à distance de l'accès contrôlé correspondant à l'appel.

- Portier IP POE+ sur une connexion RJ45.
- Poste de réception IP sur RJ 45, audio/vidéo tactile.

Le portier audio/vidéo permettra de faire des appels directs (SIP natif), de gérer les horaires d'accès (ouverture libre à certains moments de la journée) sans l'utilisation d'un serveur d'interphonie.

Pour plus de souplesse dans la gestion des appels, la même platine d'appel vidéo PHMR pourra permettre d'appeler en cascade ou en simultanée les éléments suivants :

- Des moniteurs en direct dans les bureaux.
- Sur les postes informatiques de bureau via un logiciel en POP-UP et le réseau de l'établissement (réseau de sûreté dédié).
- Des appels téléphoniques audio avec déverrouillage par code (appel aboutissant par l'intermédiaire d'autocommutateur IPBX et déverrouillage par clavier numérique du téléphone).

Le principe général étant qu'un bouton d'appel ou un nom dans la liste du défilement devra faire sonner au moins 5 éléments en cascade ou en simultané dans le but de ne pas perdre d'appel.

Pour la partie moniteur, aucune solution avec centrale ou convertisseur réseau ne sera acceptée. La solution devra obligatoirement fonctionner sans centrale et en s'appuyant sur le câblage VDI banalisé pour éviter une panne générale en cas de défaut de centrale, et faciliter les extensions futures.

3.10.1.1 - POSTE DE RÉCEPTION

Les postes de réception d'appels de bureaux devront être de type **écran LCD tactile**, PHMR et seront conçus pour recevoir les appels audio/vidéo des portiers des différents accès et pour les commander.

Intuitifs et facile d'utilisation, ils devront être mains libres et auront des boutons de commande explicites et non sensitifs (bouton porte, validation).

Afin d'augmenter la sécurité des personnes, le moniteur devra pouvoir visualiser une caméra IP de l'installation de vidéo de protection fournissant un angle de visualisation complémentaire au portier d'accès.

Alimenté en POE, un seul câble réseau sera nécessaire à leur bon fonctionnement. Ils devront obligatoirement fonctionner sur le réseau de sûreté pour une meilleure évolutivité (comme déplacer le moniteur sans avoir retiré de câble).

Un poste de réception dans le bureau d'accueil du site (poste de travail logistique) au RDC du bâtiment et un poste au CROUS.

Caractéristiques minimums :

- Ecran LED de 7 pouces minimum.
- Technologie IP, POE.
- PHMR.
- Authentification 802.1X (EAP-TLS, EAP-LEAP).
- Protocole SRTP, HTTPS.
- Support mural ou de bureau.
- Commandes de portes par touches dédiées ou écran tactile.

3.10.1.2 - VISIOPHONE (PORTIER)

Les portiers audio/vidéo seront de type **portier de rue audio/vidéo à bouton** d'appel ou **à défilement en fonction** du besoin. Ils devront être placés à une hauteur de 1,30 m.

Ils permettront de faire des appels directs, de gérer les horaires d'accès (ouverture libre à certains moments de la journée).

Ils seront alimentés en POE ou POE+ avec une seule connexion réseau (RJ 45), et devront intégrer des fonctions de traitement du son comme la suppression de bruit ambiant et l'anti-écho ainsi qu'une fréquence d'échantillonnage de 16Khz.

En réponse à la réglementation PMR, ils intégreront au minimum les fonctions : synthèse vocale, pictogrammes avec signalisation de fonctionnement (sonnerie, en communication, porte ouverte), un délai du relais de déverrouillage configurable, un son de qualité HIFI, une caméra couleur HD et une boucle à induction auditive intégrée.

Afin de voir une personne assise ou debout, la caméra du vidéo portier devra obligatoirement être de type grand-angle de type fish-eye avec un angle d'au moins 170 degrés.

Afin de mutualiser les systèmes de sûreté, le flux de caméra du portier devra pouvoir s'intégrer dans l'architecture de vidéoprotection via le protocole ONVIF au même titre que les autres caméras.

Pour faciliter la maintenance du système et pour limiter le coût du vandalisme pour la maîtrise d'œuvre, le Makrolon de protection de la caméra vidéo du portier sera remplaçable par la face avant, sans démontage de la platine et la platine devra être en inox 816L.

Ils délivreront minimum deux contacts TOR pour couper l'alimentation du verrouillage électrique.

Une extension de contacts TOR sera possible afin de pouvoir contrôler trois accès avec un même visiophone.

Caractéristiques minimums :

- Platine anti-vandale, de préférence encastrée si la configuration du site le permet.
- Impérativement muni de LED IR.
- Objectif grand-angle et zoom.
- Technologie IP, POE.
- Authentification 802.1X (EAP-TLS, EAP-LEAP).
- Protocole SRTP, HTTPS.
- Compatible ONVIF.
- Portier pourra être associé à une caméra IP de l'installation.

De plus, la platine vidéo de rue, installée à l'entrée du public, sera conforme à la norme d'accessibilité des ERP (Loi 2014-789 du 10 juillet 2014).

- Boucle magnétique conforme à la norme NF EN 60118-4 :2007.
- Pictogrammes (appel en cours, parler, ouverture porte).
- Synthèse vocale (appel en cours, parler, ouverture porte).

Implantation : Voir plans

3.11 - PROTECTION MÉCANIQUE

3.11.1 - PORTILLON AUTOMATIQUE

3.11.1.1 - PORTILLONS AUTOMATIQUES MOTORISÉS AS6

Les portillons automatiques à ouverture dans les deux sens seront de type « ONYX Outdoor » du constructeur Bolloré ou équivalent :

- Conforme PMR.
- Ouverture type papillon des vantaux dans le sens de passage.
 - Fonction 600/900mm.
- Motorisation :
 - Deux motoréducteurs freins réversibles.
 - Dispositif d'autolimitations de couple.
 - Frein à émission de courant (sécurité positive) ou à rupture de courant (sécurité négative).
- Unicité de passage : Cellules IR dans les montants de porte.
- Ouverture automatique sur contact incendie.
- Débrayage manuel double sens possible vers le côté opposé au danger.
- Verrouillage mécanique par béquille au sol (en bas de battant), condamnable par clés.
- Flux de passage, 20 à 25 personnes/ min.
- Portes pivotantes, barreaudage vertical.
- Acier thermolaqué.
- RAL au choix (à valider avec la MOA).

Les portillons automatiques devront être équipés de paravent de protection.

Les portillons automatiques permettront des largeurs d'ouvertures en fonction des droits attribués,

Exemple :

- Piéton PMR, droit PMR, ouverture à 900 mm.
- Piéton, droit piéton, ouverture à 600 mm.
- Piéton/vélos, droit piéton/vélos, ouverture à 600 mm ou 900 mm.

3.11.2 - BARRIÈRE AUTOMATIQUE AS3

Barrière automatique type « BLXX » ou équivalent :

- Lisse déportée ronde en aluminium, laquée blanc avec bandes réfléchissantes rouges, composées de 2 ou 3 segments emboîtés. La lisse sera équipée en standard d'une herse articulée en aluminium haute et basse.
- Arbre d'entraînement de la lisse pleine, de diamètre 50 mm, montées sur 2 paliers lubrifiés à vie.
- Groupe électromécanique : Motoréducteur asynchrone triphasé réversible, assurant la protection du mécanisme en cas de relevage forcé de la lisse par malveillance. Transmission secondaire par pignon et roue dentée.
- Alimentation 230 v.

3.11.3 - PANNEAUX GRILLAGE A MAILLES RIGIDES.

3.11.3.1 - DE PART ET D'AUTRE ACCÈS AS6 ET AS3

La clôture devra être réalisée en panneaux de treillis soudés indéformables et indémaillables, renforcés par des nervures horizontales avec plis renforcés.

Hauteur de la Clôture : de 1,50m à 2,50m.

Maille du treillis : 200x55 mm.

Diamètre des fils : 5 mm.

Panneau soudé selon norme EN 10223-7.

Poteau profilé selon norme EN 10162.

Fil d'acier galvanisé selon norme NF EN 10244-2.

Panneau plastifié Haute adhérence polyester selon norme EN 13438.

Feuillard galvanisé selon norme EN 10223-7.

Poteau plastifié haute adhérence polyester selon norme EN 13438.

Coloris en RAL, au choix de la MOA.

Espacement des poteaux : 2.53m.

Enfoncement en sol : 0.50m. Bétonnés.

Compris travaux de maçonnerie pour ancrage, et toutes sujétions de mise en œuvre pour une finition soignée.

Avant toute fabrication l'entreprise devra fournir les notes de calcul et les plans (les détails d'exécution et d'ancrage) au Maître d'Œuvre et bureau de contrôle pour approbation.

3.11.4 - POTELET VL

3.11.4.1 - POTELET VL ACCÈS BARRIÈRE AUTOMATIQUE AS3

Type potelet P 800 de chez TGO ou équivalent.

Largeur utile plane de 200 mm.

La profondeur maximum d'intégration est de 95 mm.

La plaque de fermeture haute est dévissable.

Coloris en RAL, au choix de la MOA.

Hauteur : 1,80 mm.