

RECTORAT D'ACADEMIE DE BRETAGNE

Division Régionale De l'Immobilier de l'Etat

RENOUVELLEMENT DES INSTALLATIONS DE SURETE DES BATIMENTS AFFECTES AU SITE DE RENNES

PHASE DCE

CCTP Lot unique Surêté

Maître d'ouvrage

RECTORAT D'ACADEMIE DE BRETAGNE
Division Régionale de l'Immobilier de l'Etat
96 rue d'Antrain
35705 RENNES Cedex 7

Maîtrise d'œuvre

Bureau d'Études

Egis Bâtiments Centre-Ouest
Zac de la Courrouze - Immeuble Eolios – 1er étage
3, rue Louis Braille – 35136 St-Jacques-de-la-Lande
(adresse postale : TSA 50851 - 35208 RENNES Cédex 2)

SOMMAIRE

1	DISPOSITIONS GENERALES.....	5
1.1	PRÉAMBULE	5
1.2	CLASSEMENT DES DIFFÉRENTS BÂTIMENTS	6
1.3	PIÈCES CONSTITUTIVES DU LOT ÉLECTRICITÉ	6
1.4	DECOMPOSITION DU MARCHE	7
1.5	CONSISTANCE DES TRAVAUX.....	7
1.6	NORMES ET RÈGLEMENTS APPLICABLES.....	8
1.7	OBLIGATIONS DE L'ENTREPRISE.....	10
1.7.1	Généralités	10
1.7.2	Connaissance et appréciation du projet.....	11
1.7.3	Relation de l'entrepreneur avec les services de distribution	11
1.7.4	Relation avec les autres corps d'état	11
1.8	DOCUMENTS À FOURNIR PAR L'ENTREPRISE	11
1.8.1	Dossier de chantier	11
1.8.2	Dossier des ouvrages exécutés	12
1.8.3	Dossier de maintenance	12
1.9	LIMITES DE PRESTATIONS.....	13
1.10	FOURNITURES – PROTOTYPES - ECHANTILLONS	13
1.10.1	Qualité des fournitures	13
1.10.2	Choix des fournitures	13
1.10.3	Maquettes - Prototypes	14
1.10.4	Approvisionnement.....	14
1.11	ESSAIS - RÉCEPTION	14
1.11.1	Organisation des essais	14
1.11.2	Essais et contrôles en usine	14
1.11.3	Autocontrôles	14
1.11.4	Essais et contrôles sur le site.....	15
1.11.5	Consuel	15
1.11.6	Démarche pour les essais en configuration définitive.....	15
1.11.7	Réception	15
1.11.8	Garantie.....	15
1.12	FORMATION.....	15
2	DESCRIPTION DES OUVRAGES DE SURETE.....	17
2.1	ETAT DES LIEUX DES INSTALLATIONS EXISTANTES	17
2.1.1	Contrôle d'accès.....	17
2.1.2	Alarme intrusion	17
2.1.3	Video surveillance	17
2.1.4	Sécurité incendie.....	17
2.2	HYPOTHÈSES DE CONCEPTION	18
2.2.1	Prescriptions particulières (limites de prescriptions).....	18
2.2.2	Fiabilité des systèmes	19

2.2.3	Gestion des versions et mises à jour	19
2.2.4	Fondement du contrôle d'accès	21
2.2.5	Fondement de l'anti-intrusion	26
2.2.6	Fondement de la vidéosurveillance	27
2.2.7	Réseau Sûreté	30
2.3	SUPERVISION	30
2.3.1	Poste principal d'exploitation et poste secondaire	30
2.3.2	Logiciels	33
2.3.3	Monitoring et supervision	34
2.3.4	Animation de synoptiques graphiques (Prestation supplémentaire éventuelle)	36
2.3.5	Supervision vidéo	37
2.3.6	Gestion des utilisateurs	38
2.3.7	Gestion des annuaires LDAP/Active directory	39
2.3.8	Gestion multi-sites / multi clients	39
2.3.9	Programmation, essais et mise en service	40
2.3.10	Formation des utilisateurs	41
2.4	CONTRÔLE D'ACCES	42
2.4.1	Rappel du cadre réglementaire et assureur	42
2.4.2	Généralités	42
2.4.3	Différents niveaux de sécurité	43
2.4.4	Spécification matérielle du système	44
2.4.5	Architecture envisagée	44
2.4.6	Capacité du système à respecter	46
2.4.7	Attribution des droits d'accès aux usagers	46
2.4.8	Historiques	47
2.4.9	Richesse fonctionnelle de la solution	47
2.4.10	Automate	53
2.4.11	UTL	53
2.4.12	Badges	54
2.4.13	Lecteur enrôleur de table	54
2.4.14	Environnement de la porte	54
2.4.15	Lecteurs de badges	57
2.4.16	Câblage du système	58
2.4.17	Programmation, essais et mise en service	58
2.4.18	Contrat de service (prestation supplémentaire éventuelle-PSE N°2 TF / PSE N°3 T01 / PSE N°5 T02)	59
2.5	ALARME INTRUSION	59
2.5.1	Rappel du cadre réglementaire et assureur	59
2.5.2	Généralités	59
2.5.3	Description du système	60
2.5.4	Centrale d'Alarme	60
2.5.5	Modules Entrées/Sorties	61
2.5.6	Alimentation déportée	62
2.5.7	Terminale d'exploitation	62
2.5.8	Détection intrusion	62
2.5.9	Détecteurs périmétriques	62
2.5.10	Détecteurs Bi-volumétriques	63
2.5.11	Sirènes intérieures	63
2.5.12	Câblage du système	64
2.5.13	Secteur de surveillance	64
2.5.14	Transmission d'événements	64
2.5.15	Exploitation fonctionnelle	65
2.5.16	Programmation, essais et mise en service	66
2.6	VIDÉOSURVEILLANCE	66
2.6.1	Rappel du cadre réglementaire	66
2.6.2	Spécification matérielle du système	69

2.6.3	Ouverture du système	69
2.6.4	Gestion des caméras	70
2.6.5	Gestion des murs d'images	70
2.6.6	Gestion de l'affichage	71
2.6.7	Gestion de plans interactifs (prestation supplémentaire eventuelle-PSE N°1 TF / PSE N°3 T01 / PSE N°5 TO2)	71
2.6.8	Recherche sur archives	71
2.6.9	Export de séquences	71
2.6.10	Gestion d'alarmes	72
2.6.11	Paramétrage des masques des caméras	72
2.6.12	Paramétrages des enregistrements	72
2.6.13	Le bloc enregistrement	72
2.6.14	Surveillance de l'état des enregistreurs	73
2.6.15	Spécifications du matériel informatique	73
2.6.16	Caractéristiques des caméras	75
2.6.17	Spécification logicielle du système	78
2.6.18	Interface avec des applications tierces	79
2.6.19	Interopérabilité avec les caméras du marché (ONVIF)	79
2.6.20	Calcul de stockage	79

3 DESCRIPTION DES OUVRAGES COURANTS FAIBLES.....86

3.1	EXTENSION DU PRÉCABLAGE BANALISÉ VDI	86
3.1.1	Principe	86
3.1.2	Généralités	86
3.1.3	Conformité de l'installation	86
3.1.4	Principe des travaux à réaliser	87
3.1.5	Equipement des baies informatiques	87
3.1.6	Câblage cuivre	87
3.1.7	Tests à réaliser	89
3.1.8	Fournitures hors marché	90
3.2	MODIFICATION DU SYSTEME DE SECURITE INCENDIE	90

4 DESCRIPTION DES OUVRAGES COURANTS FORTS.....91

4.1	RÉSEAU DE TERRE.....	91
4.2	ALIMENTATION COURANTS FORTS	91
4.3	EXTENSION DES TABLEAUX ELECTRIQUES	91
4.4	RÉSEAU HAUTE QUALITÉ	91
4.5	CANALISATIONS.....	92
4.6	GOULOTTE DE DISTRIBUTION	92
4.7	BOUCHAGE DES PERCEMENTS.....	92
4.8	EQUIPEMENT DES LOCAUX	92
4.8.1	Appareil d'éclairage intérieur.....	93
4.8.2	Appareillage	93

5 DESCRIPTION DU MOBILIER DU PCS.....95

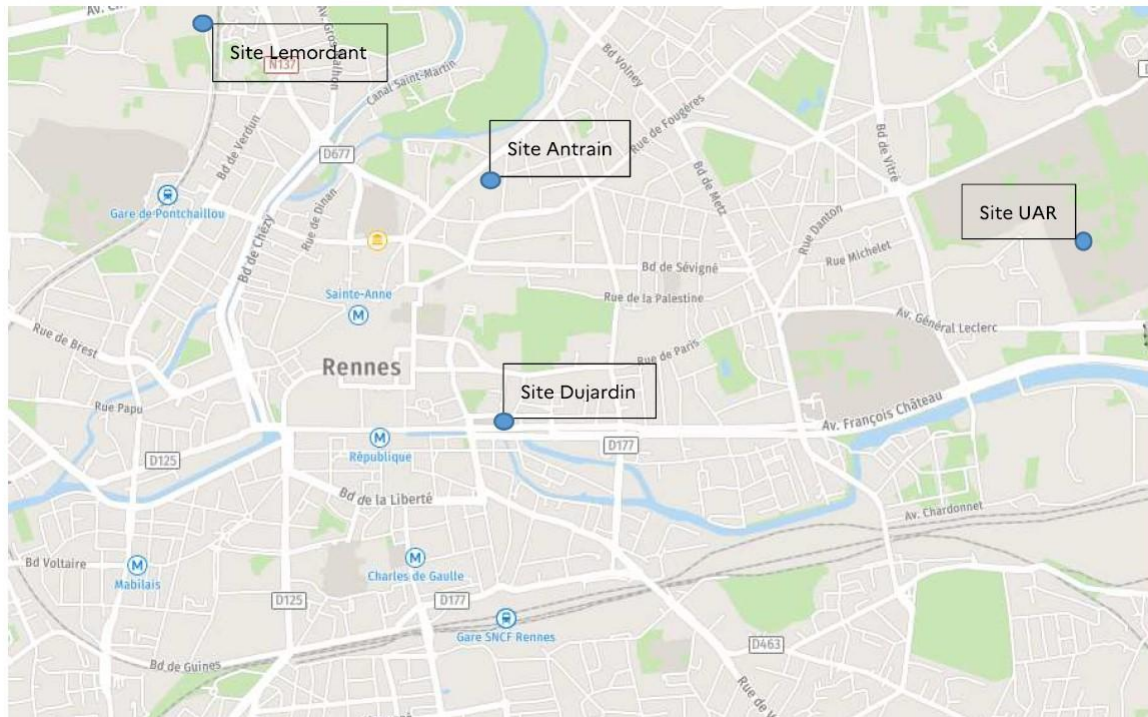
6 TRAVAUX DE DEPOSE97

1 DISPOSITIONS GENERALES

1.1 PRÉAMBULE

La présent cahier des charges a pour objet la définition des travaux nécessaires au renouvellement des installations de sureté sur plusieurs sites du rectorat d'académie de Bretagne localisés à Rennes à savoir :

- Les bâtiments du Rectorat au 92, 96 et 108 Rue d'Antrain.
- Le bâtiment de la DSDEN au 1 quai Dujardin.
- Le bâtiment UAR allée Perrin Rennes (dans l'enceinte de l'université de Rennes I).
- Le bâtiment de la DSII rue Jean Julien Lemordant.



Les systèmes de sûreté à mettre en œuvre dans le cadre du projet comprendront :

- Le Contrôle d'Accès par lecteurs de badges,
- La Détection Intrusion,
- La Vidéosurveillance.
- Les divers travaux d'adaptation nécessaires (alimentation électrique, verrouillage de porte, aménagement d'un local PC de sécurité)

Ces différents systèmes seront exploités depuis un PC Sécurité localisé au RDC du bâtiment de la DSDEN et d'un bureau de la DAGE au rdc du 96 Rue d'Antrain.

Afin de faciliter la convergence et les interactions entre les différents systèmes de sûreté, les équipements de contrôle d'accès, de détection intrusion et de vidéosurveillance à mettre en œuvre utiliseront majoritairement la technologie IP (Internet Protocol).

Les équipements IP de ces systèmes seront fédérés sur un même réseau informatique dédié Sûreté (LAN spécifique) par l'intermédiaire des liaisons informatiques décrites au paragraphe « Câblage VDI ».

Ce réseau sera appelé dans la suite du document « réseau Sûreté ».

Les équipements IP qui seront raccordés au réseau seront les suivants :

- Contrôle d'accès :

- Serveur
- Postes d'exploitation
- Automate ou Unités de Traitement Locales (UTL) de contrôle d'accès
- Détection intrusion :
 - Centrales intrusions
- Vidéosurveillance :
 - Serveurs
 - Stockeurs
 - Postes d'exploitation
 - Caméras

Pour pallier toute évolution, et sauf spécification contraire dans la suite du document, chaque système de sûreté mis en œuvre sera dimensionné avec 30% de réserve sur les équipements centraux, logiciels, et licences afin de permettre le raccordement et la gestion de terminaux supplémentaires.

Sont entendus par « terminaux » les équipements suivants :

- Pour le contrôle d'accès : les UTL et lecteurs de badges associés
- Pour la détection intrusion : les modules d'entrées-sorties déportés et capteurs associés
- Pour la vidéosurveillance : les caméras

1.2 CLASSEMENT DES DIFFÉRENTS BÂTIMENTS

Les différents bâtiments sont classés de la façon suivante :

- Le bâtiment au 96 Rue d'Antrain : bâtiment principal de type administratif en R+4 avec sous-sol classé ERP de type W 5ème catégorie
- Le bâtiment au 92 Rue d'Antrain : bâtiment secondaire de type administratif en R+3 avec sous-sol classé ERP de type W-R 3ème catégorie
- Le bâtiment au 108 Rue d'Antrain : bâtiment de restauration pour le personnel du rectorat sur un seul niveau classé ERT de type N 5ème catégorie.
- Le bâtiment de la DSDEN 1 quai Dujardin : bâtiment administratif en R+4 avec sous-sol classé ERP de type W-R-L 2ème catégorie. Il est associé à un amphithéâtre (Donzelot) rue Kleber dont les deux ensembles sont indissociables.
- Le bâtiment de l'UAR : bâtiment administratif (service de reprographie du Rectorat) en rdc classé ERT de type W catégorie 5. Il est localisé dans l'enceinte de Beaulieu de l'université de Rennes I, allée Perrin Rennes
- Le bâtiment de la DSII (service informatique du rectorat) : bâtiment type administratif (service informatique du Rectorat d'Académie de Bretagne) en R+2 avec sous-sol partiel classé ERT de type W catégorie 5. Ce bâtiment partage une entrée commune avec l'Office Français de l'immigration et de l'intégration (OFII).

1.3 PIÈCES CONSTITUTIVES

En complément au CCTP, le présent dossier comporte une série de documents graphiques.

Ils ont pour but de définir et de préciser avec le CCTP les prestations à réaliser.

Liste des plans fournis

NUMERO PLANS	DESIGNATION	ECHELLE
DCE-ELE001	Carnet de plans de sûreté	sans



DCE-ELE002	Carnet étude vidéosurveillance	sans
DCE-ELE004	Carnet synoptique architecture sureté	sans

1.4 DECOMPOSITION DU MARCHE

Le présent marché se décompose en trois tranches:

Une tranche ferme:

- Les bâtiments du rectorat au 92 et 96 Rue d'Antrain.
- Le bâtiment de la DSDEN 1 quai Dujardin (aménagement pour recevoir le PC de Sécurité uniquement).

Une tranche optionnelle N°1:

- Le bâtiment de la DSDEN 1 quai Dujardin (dans sa globalité).
- Le bâtiment de la DSII rue Jean Julien Lemordant.

Une tranche optionnelle N°2:

- Le bâtiment de l'UAR allée Perrin Rennes.
- Le bâtiment restaurant du rectorat au 108 Rue d'Antrain

1.5 CONSISTANCE DES TRAVAUX

Les installations seront livrées en parfait état d'achèvement et en bon ordre de marche. A cet effet, l'Entrepreneur devra inclure dans son prix l'intégralité des fournitures, de la main d'œuvre et des prestations diverses nécessaires à une réalisation complète de bonne qualité suivant les conditions fixées dans le présent marché et dans le respect des normes, règlements et règles de l'art.

Les prestations du présent lot comprennent :

- Les études et la production des documents d'exécution nécessaires à la réalisation des ouvrages (plans, schémas, synoptiques, scénarios, etc.).
- La participation aux réunions de mise au point
- La fourniture, le transport à pied d'œuvre, le montage, le réglage et les essais de tout le matériel.
- La modifications des installations existantes (tableaux électriques, baies informatiques)
- La fourniture, la pose, la fixation et le raccordement de tous les câbles pour les équipements de sureté
- L'équipement des menuiseries existantes sous contrôle d'accès
- Les mises à la terre nécessaire
- Les alimentations électriques pour les besoins du projet
- Les essais et le maintien en bon état de fonctionnement de l'installation pendant la période de garantie,
- L'enlèvement des gravats provenant des travaux du présent lot.
- Les frais de transport, d'emballage, d'entrepose provisoire concernant le présent lot ainsi que tous les frais de main d'œuvre auxiliaire s'y rattachant.
- Tous les percements, scellements, saignées, rebouchage et raccords en cloisons maçonnées nécessaires pour le présent lot, en particulier les calfeutrements des réservations de passage en matériaux coupe-feu (traversées de compartiment coupe-feu), acoustique et thermique.
- Toutes les saignées dans le béton ou le plâtre, les incorporations dans le béton, les parpaings pour le présent lot.

- Les câblages, fourreaux, goulottes, chemins de câbles, travaux accessoires et annexes nécessaires à la réalisation de l'ensemble.
- Toutes sujétions de transport, stockage, manutention et pose.
- La protection par peinture ou tout autre procédé des éléments susceptibles d'être corrodés, compte tenu en particulier des conditions climatiques du lieu d'installation.
- La peinture de finition des matériels apparents.
- Les essais en atelier et sur le site, y compris fourniture de la main d'œuvre qualifiée, des équipements provisoires et matières consommables éventuellement indispensables.
- Les réglages, équilibrages et mise en service des installations.
- La participation active aux opérations préalables à la réception.
- La mise en place des marques signalétiques et repères sur les canalisations et matériels suivant les plans et schémas des ouvrages exécutés.
- L'information et la formation du personnel du Maître d'Ouvrage.
- La garantie des installations pièces et main d'œuvre dans les conditions définies dans le CCAP, inclus extension de garantie fournisseur s'il y a lieu.
- Entretien durant la période de garantie de parfait achèvement des matériels désignés.

NOTA IMPORTANT : Les travaux sont réalisés en site occupé et ne doivent pas entraver la continuité d'activité. L'entreprise devra donc proposer une méthodologie d'intervention qui soit compatible avec le phasage envisagé pour maintenir le niveau de sécurité du système actuel avant basculement sur le nouveau système.

1.6 NORMES ET RÈGLEMENTS APPLICABLES

Les matériels et installations devront satisfaire aux normes et règlements (édition en vigueur à la date précisée dans les pièces administratives) et respecteront notamment :

- L'arrêté du 01/08/06 applicable au 01/01/07 relatif à l'accessibilité handicapés.
- Le Code du Travail.
- Le décret 2010-1017 du 30/08/2010 : Obligation des Maîtres d'Ouvrage pour prévenir les risques électriques dans la construction ou modification de bâtiments à usage professionnel.
- Le décret 2010-1016 du 30/08/2010 : Obligation de l'employeur pour l'utilisation des installations électriques et de leurs modifications ou entretien.
- Le décret 2010-1118 du 22/09/2010 : Règles de sécurité relatives aux opérations sur ou au voisinage des installations électriques.
- Le décret 2010-1018 du 30/08/2010 : Dispositions relatives à la prévention des risques électriques dans les lieux de travail.
- L'arrêté du 14 décembre 2011 relatif aux installations d'éclairage de sécurité.
- L'arrêté du 25 juin 1980 modifié et l'arrêté du 19 novembre 2001 relatifs au règlement de sécurité contre les risques d'incendie et de panique dans les ERP,
- Le Code de la Construction et de l'Habitation (Partie Réglementaire) : Chapitre 6 Infrastructures pour la recharge des véhicules électriques dans les bâtiments et le stationnement sécurisé des vélos - Articles R136-1 à R136-4.
- L'arrêté du 20 février 2012 relatif à l'application des articles R. 111-14-2 à R. 111-14-5 du code de la construction et de l'habitation.
- La norme NF C14-100 relative aux installations de branchement à basse tension,

- La norme NF C15-100 et additifs, relative aux installations à basse tension, ainsi que les fiches d'interprétation permanentes de l'UTE.
- Le guide pratique UTE C15-103 relatif au choix des matériels électriques en fonction des influences externes.
- Le guide pratique UTE C15-105 relatif à la détermination des sections des conducteurs et au choix des dispositifs de protection.
- Le guide pratique UTE C15-106 relatif à la détermination des sections des conducteurs de protection, des conducteurs de terre et des conducteurs de liaison équipotentielle.
- Le guide pratique UTE C15-402 relatif à l'installation des Alimentations sans Interruption (ASI) de type statique,
- Le guide pratique UTE C15-443 relatif à la protection des installations basse tension contre les surtensions d'origine atmosphérique et détaillant les méthodes de choix et d'installation des parafoudres.
- Le guide pratique UTE C15-476 relatif au sectionnement à la commande et à la coupure des installations électriques à basse tension.
- Le guide pratique UTE C15-520 relatif aux modes de pose et aux connexions des installations électriques à basse tension.
- Le guide pratique UTE C15-559 relatif aux installations d'éclairage en TBT,
- Le guide pratique UTE C15-755 relatif aux installations électriques d'origines différentes dans un même local et dont les exploitations sont placées sous des responsabilités différentes,
- La norme NF C17-102 relative à la protection contre la foudre et aux installations de paratonnerre à dispositifs d'amorçage.
- La norme NF EN 62305-1 Protection contre la foudre -partie 1 : principes généraux.
- La norme NF EN 62305-2 Protection contre la foudre -partie 2 : Evaluation du risque.
- La norme NF EN 62305-3 Protection contre la foudre - partie 3 : Dommages physiques sur les structures et risques humains.
- La norme NF EN 62305-4 Protection contre la foudre - partie 4 : Réseaux de puissance et de communication dans les structures.
- Les prescriptions de la norme NF EN60-439 concernant les enveloppes et les indices de protection.
- La norme NF C63-421 relative aux ensembles d'appareillage à basse tension - Ensembles de série et ensembles dérivés de série.
- Les normes NF C71-800, NF C71-801, NF C71-805, NF C71-805, NF C71-810, NF C71-815, NF C71-815 et le guide pratique UTE 71-820 relatifs aux blocs autonomes d'éclairage de sécurité.
- La série des normes NF S61-930 à NF S61-970 pour celles qui sont applicables aux prestations du présent lot.
- Les directives européennes relatives à la compatibilité électromagnétique, ainsi que la guide pratique UTE C 15.900 relatif à la cohabitation entre réseaux de communication et d'énergie.
- La norme NF EN 62471 relative à la sécurité photobiologique des lampes et systèmes à lampes (LED).
- IEC/PAS 62717 – Exigences de performances – Modules de LED pour l'éclairage général.
- IEC/PAS 62722 – Exigences de performances – Luminaires LED pour l'éclairage général.
- Norme française NF C 15.100 et ses additifs, concernant les installations électriques à basse tension
- Norme française NF C 14-100 concernant les installations de branchement à basse tension
- UTE C18-510 : Recueil d'instructions générales de sécurité d'ordre électrique

- La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, lorsque les caméras filment des lieux non ouverts au public
- Articles L223-1 et suivants (lutte contre le terrorisme)
- Articles L251-1 et suivants, lorsque les caméras filment des lieux ouverts au public.
- Article L2323-32 (information/consultation des instances représentatives du personnel)
- Articles L1221-9 et L1222-4 (information individuelle des salariés)
- Article L1121-1 (principe de proportionnalité)
- Article 226-1 (enregistrement de l'image d'une personne à son insu dans un lieu privé)
- Article 226-16 (non déclaration auprès de la CNIL)
- Article 226-18 (collecte déloyale ou illicite)
- Article 226-20 (durée de conservation excessive)
- Article 226-21 (détournement de la finalité du dispositif)
- Article R625-10 (absence d'information des personnes)
- L'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.
- Les recommandations de l'ANSSI sur la sécurité des systèmes informatiques
- Directives NIS 2
- Les règles APSAD relatives à la sûreté du bâtiment, notamment :
 - R81 – Règle d'installation de la détection intrusion
 - D83 – Document technique pour la conception et l'installation du contrôle d'accès
 - R82 – Règle d'installation de la vidéosurveillance
- Les normes ISO15693, ISO 14443A et ISO 14443B
- Les normes IEEE 802.X
- Les normes de câblages ISO / IEC 11 801 et l'EIA / TIA

Cette liste n'est pas exhaustive.

Pour les normes, les fiches d'interprétation sont applicables

1.7 OBLIGATIONS DE L'ENTREPRISE

1.7.1 GENERALITES

Dans la description qui va suivre, le MOE s'est efforcé de renseigner l'Entreprise sur la nature des travaux, sur le nombre de matériels à mettre en œuvre, leurs dimensions et leur emplacement, mais il convient de signaler que cette description n'a pas un caractère limitatif et que l'Entreprise devra exécuter, comme compris dans son prix, sans exception ni réserve, tous les travaux nécessaires et indispensables pour l'achèvement complet des ouvrages projetés.

En conséquence, l'Entreprise ne pourra jamais arguer que des erreurs ou omissions aux plans et devis puissent la dispenser d'exécuter tous les travaux de son corps d'état ou fassent l'objet d'une demande de supplément de prix.

Tous les documents graphiques remis à l'Entreprise pour l'exécution des ouvrages doivent être considérés comme une proposition qu'elle devra vérifier avant la remise de son offre.

Elle devra signaler au Maître d'Œuvre les dispositions qui ne lui paraîtraient pas en rapport avec la solidité et la conservation des ouvrages, l'usage auquel ils sont destinés ou l'inobservation des règles de l'art.

L'Entreprise sera considérée avoir pris connaissance des travaux à réaliser et avoir estimé elle-même les quantités, définitions d'ouvrages et conditions d'exécution nécessaires à la parfaite réalisation des travaux.

Aucune incidence financière ne pourra être accordée pour une sous-estimation des difficultés ou des dépassements de temps de main d'œuvre, dus au non-respect de cette règle.

L'Entreprise devra prendre toutes les dispositions nécessaires afin de ne pas perturber le fonctionnement du site pendant les travaux (travaux de nuit, le week-end, etc.). Notamment les travaux de raccordement des câbles existants pourront être exécutés sur une installation en service. Elle devra donc tenir compte de ces impératifs dans le montant de son offre.

1.7.2 CONNAISSANCE ET APPRECIATION DU PROJET

L'Entreprise sera supposée connaître l'ensemble du projet . Elle vérifiera les éléments mis à sa disposition au moment de l'établissement de sa proposition.

En cas d'omission, de divergences ou d'impossibilités techniques de réalisation du projet, elle devra, de par ses connaissances techniques et professionnelles, y remédier d'office et en avertir obligatoirement le Maître d'Œuvre au plus tard lors de la remise de son offre.

Sans observation de sa part, sa proposition sera considérée comme acceptant l'exécution des travaux dans leur intégralité sans aucune réserve, ni restriction et sans qu'il puisse être demandé des suppléments.

L'Entreprise devra se conformer aux exigences de la notice acoustique relative au présent projet notamment en ce qui concerne les rebouchages et les calfeutrements. .

1.7.3 RELATION DE L'ENTREPRENEUR AVEC LES SERVICES DE DISTRIBUTION

Sans objet.

1.7.4 RELATION AVEC LES AUTRES CORPS D'ETAT

Sans objet.

1.8 DOCUMENTS À FOURNIR PAR L'ENTREPRISE

Au cours de la phase de préparation des travaux, l'Entrepreneur établira à ses frais en complément aux études remises dans le DCE par la Maîtrise d'Œuvre, les études, plans et tout document indispensable à la réalisation des ouvrages et demandés dans le présent document.

1.8.1 DOSSIER DE CHANTIER

1.8.1.1 DOCUMENTS GENERAUX

L'Entreprise doit remettre après l'approbation du marché et dans les délais définis dans le CCAP marché principal :

- Les synoptiques généraux et détaillés par bâtiment.
- Les plans de cheminement des câbles fournis.
- Les plans d'implantation des équipements par bâtiments et par système.
- Plan d'aménagement détaillé des locaux spécifiques (PC de sécurité)
- Le plan de couverture des caméras de vidéosurveillance
- La mise à jour des schémas unifilaires des tableaux principaux, armoires divisionnaires.
- La mise à jour des plans des baies informatiques
- La nomenclature et fiches techniques de tout le matériel (sûreté et électricité)
- La liste des câbles et les conduits.
- Les analyses fonctionnelles détaillées par système.

- La liste des adresses IP et les tables d'échange de communication
- Les consignes de conduite des installations (mode normal, mode dégradé).
- Les listes de points du système de supervision.
- Les documents administratifs auprès des autorités compétentes (préfecture, CNIL)
- Etc

1.8.1.2 DIVERS

Tous ces documents devront également être communiqués au Contrôleur Technique pour avis.

Tous les documents d'exécution de l'Entreprise devront être réalisés sur support informatique AUTOCAD dernière version). Les procédures de codification des documents, des « couches » et des couleurs, les valeurs des paramètres systèmes et des styles seront définies par le Maître d'Ouvrage à la notification du marché. Les fonds de plans seront fournis sous AUTOCAD à l'Entreprise, sur demande écrite au chef de projet.

Aucune modification ne pourra être apportée au projet décrit dans le présent CCTP et les plans joints sans l'autorisation écrite du Maître d'Œuvre.

Pour toute modification demandée par l'Entreprise et approuvée par le Maître d'Ouvrage et le Maître d'Œuvre, l'Entreprise prendra à sa charge toutes les mises à jour des plans d'exécution liées à cette modification, et ceci sans se prévaloir d'une réclamation sur ses forfaits d'étude ou d'exécution.

Tout désaccord avec les dimensions des équipements ou avec les conditions climatiques des locaux mis à la disposition de l'Entreprise doit être signalé avant signature des offres et être indiqué dans l'offre de l'Entreprise. Dans le cas contraire, l'Entreprise est réputée avoir accepté les conditions d'implantations prévues.

1.8.2 DOSSIER DES OUVRAGES EXECUTES

L'Entreprise doit remettre, après constat d'achèvement des travaux et dans les délais définis dans le CCAP du marché principal tous les documents cités précédemment dans le dossier de chantier (à l'exception des plans de réservations) et compléter des documents suivants :

- Une notice de fonctionnement général de l'installation.
- Les plans d'équipement des armoires et coffrets.
- Les synoptiques détaillés par type d'installation,
- Les notices techniques des équipements installés.
- La liste définitive des câbles posés.
- Les fiches d'autocontrôle de toutes les installations effectuées.
- Le procès-verbal d'essais des matériels conformément aux normes et décrets en vigueur.
- Le dossier de maintenance.

L'entreprise devra soumettre au Maître d'œuvre au préalable pour validation le sommaire du dossier DOE.

1.8.3 DOSSIER DE MAINTENANCE

L'Entreprise doit remettre dans les mêmes conditions que le Dossier des Ouvrages Exécutés :

- La liste détaillée des pièces de rechange nécessaires à la maintenance courante et le chiffrage de leur coût.
- Les notices des constructeurs.
- La documentation utilisateur (notices d'exploitation, d'entretien et de dépannage).
- Un support de sauvegarde des systèmes d'exploitation, progiciels et de la dernière version des paramétrages.

- Une édition sur papier des paramètres de configuration et de fonctionnement.
- Les licences d'exploitation des matériels et procédés brevetés ainsi que les droits d'usage afférent aux logiciels.

1.9 LIMITES DE PRESTATIONS

Sauf indications contraires dûment précisées "hors fourniture" ou "hors mise en place", tout matériel mentionné dans le CCTP, le DPGF, et sur les plans et schémas est sous-entendu fourni, posé, fixé et raccordé y compris toutes sujétions de mise en œuvre.

1.10 FOURNITURES – PROTOTYPES - ECHANTILLONS

1.10.1 QUALITE DES FOURNITURES

Il sera fait exclusivement usage de matériels neufs de première qualité, standard, de marque notoirement connue et facilement remplaçable par approvisionnement local dans des délais rapides.

Les matériaux éléments ou ensembles utilisés doivent être conformes aux stipulations contenues dans les pièces du marché, ainsi que dans les ordres de service. S'ils font l'objet de normes, ils devront également être conformes à celles-ci et d'une façon générale porter le label NF et le marquage CE correspondants.

Lorsque, exceptionnellement, il n'existerait pas de marque de qualité, il pourra être demandé la garantie de la conformité aux normes et aux spécifications du marché par un procès-verbal d'essais effectué par un organisme qualifié aux frais de l'entrepreneur.

Tous les matériels devront avoir l'indice de protection et le degré de réaction au feu (essai au fil incandescent) requis selon l'utilisation des locaux et les risques présentés aux lieux où ils seront installés (Influences externes selon guide UTE C 15-103).

Toutes les précautions nécessaires doivent être mises en œuvre au cours des travaux pour assurer leur bon état de conservation, tant pendant le transport, le stockage sur le chantier que durant le montage.

Les parties métalliques posées avec leur revêtement définitif (couches premières anticorrosion et peinture de finition) devront être efficacement protégées jusqu'à la livraison de l'installation.

Elles ne devront présenter aucune détérioration susceptible d'être le siège d'une corrosion ultérieure. Toute résurgence de tache de rouille entraînera le refus de la réception de la partie d'ouvrage correspondante. La visserie et la boulonnerie seront entièrement traitées.

1.10.2 CHOIX DES FOURNITURES

Les types et marques des matériels mentionnés dans les pièces du DCE seront données à titre indicatif de référence. Ils ont servi de base à l'étude de la maîtrise d'œuvre pour obtenir les performances attendues. L'entrepreneur pourra proposer des matériels équivalents de son choix, tout en restant engagé par l'obligation d'obtenir au moins le même niveau de performances.

Les matériels proposés devront être précisés à l'appui de la remise de l'offre suivant cadre joint en annexe du DPGF.

L'entrepreneur devra fournir les catalogues, croquis et dessins qui pourraient lui paraître indispensables pour l'appréciation de son offre.

Toute proposition ne correspondant pas techniquement, dimensionnellement, qualitativement ou esthétiquement au matériel prévu pourra être refusée.

Pour les équivalences de matériel qu'elle proposera, l'entreprise fournira la fiche technique et un échantillon du matériel prescrit en base, la fiche technique et un échantillon du matériel proposé en variante et ce de manière à apporter tous les éléments permettant de statuer sur l'équivalence ; pour les luminaires, les échantillons seront comparés éteints et allumés et dans des conditions de mise en œuvre aussi proches que possible de la mise en œuvre définitive.

1.10.3 MAQUETTES - PROTOTYPES

Des maquettes, prototypes, échantillons ou montages témoins provisoires sur le site pourront être demandés selon les besoins par le Maître d'œuvre pour permettre la vérification de certaines fournitures vis-à-vis de :

- Leur conformité aux normes et spécifications du marché.
- Leur mise en service.
- Leur intégration avec d'autres éléments.

Des échantillons de petits matériels seront fournis par l'entreprise. Ils serviront de témoin approuvé pour la réalisation des travaux.

1.10.4 APPROVISIONNEMENT

Tous les matériels seront neufs et de bonne qualité. Ils devront être conformes aux normes qui leur sont propres et porteront les estampilles d'agréments et labels de qualité chaque fois qu'ils font l'objet d'essais ou de contrôles réglementaires.

Avant le démarrage de ses travaux, l'Entreprise devra soumettre les références exactes des fournitures qu'elle se propose de mettre en œuvre à l'approbation du Maître d'Œuvre qui appréciera s'il y a concordance et équivalence avec les prescriptions des pièces du marché. Dans le cas contraire, le Maître d'Œuvre se réserve le droit d'exiger les marques et types cités en référence dans le CCTP.

L'Entreprise du présent lot présentera au Maître d'Œuvre, après la réception de l'ordre de service de notification de marché, et avant commencement des travaux, un tableau comportant un échantillon des appareils à installer. Chaque échantillon comportera une étiquette comportant la marque et les références de l'appareil, ainsi que les endroits d'utilisation envisagés.

Après accord, ce tableau restera sur le chantier jusqu'à la réception.

Aucune commande de matériel ne pourra être passée par l'entreprise, sinon à ses risques et périls, tant que l'échantillon, la maquette ou le prototype correspondant n'aura pas été agréé par le Maître d'Œuvre et le Maître d'Ouvrage.

1.11 ESSAIS - RÉCEPTION

1.11.1 ORGANISATION DES ESSAIS

Les essais définis ci-après seront réalisés sur le site.

La liste des essais prescrits n'est donnée qu'à titre indicatif et n'est pas limitative.

Les modalités des essais ou contrôles sont établies d'un commun accord entre le Maître d'Œuvre et l'Entreprise.

L'Entreprise rédige les procès-verbaux d'essais sur lesquels doivent figurer pour chaque essai les résultats des mesures effectuées ou de vérifications réalisées. Les procès-verbaux seront remis au Maître d'Œuvre et au Maître d'Ouvrage (la non remise de ces procès-verbaux entraînera le refus de réception des installations par le Maître d'Ouvrage).

Tous les frais afférents à ces travaux sont réputés être inclus au prix porté dans l'offre de l'Entreprise.

Les essais doivent être effectués en respectant scrupuleusement les consignes de protection du matériel et du personnel.

1.11.2 ESSAIS ET CONTROLES EN USINE

Sans objet

1.11.3 AUTOCONTROLES

L'Entreprise doit procéder aux autocontrôles techniques de ses installations conformément aux dispositions figurant dans les documents techniques

L'Entreprise est tenue de fournir au Maître d'Œuvre :

- Un programme des essais et des vérifications.
- Des fiches des autocontrôles attestant la réalité de ces vérifications.

Enfin, il doit organiser son chantier de telle sorte que l'autocontrôle de la mise en œuvre soit systématiquement assuré.

- Ces essais comprennent au minimum les autocontrôles de l'entreprise pour les points suivants
 - Les essais de bon fonctionnement de chaque sous-système point à point .
 - La vérification du paramétrage de l'installation.
 - La vérification du bon fonctionnement de l'installation.

1.11.4 ESSAIS ET CONTROLES SUR LE SITE

Avant la réception, le Maître d'Œuvre se réserve le droit de contrôler par sondage les résultats des vérifications exécutées par l'Entreprise.

Ces contrôles consistent à vérifier que les installations sont conformes aux dispositions réglementaires et aux prescriptions du présent CCTP et qu'elles satisfont aux performances demandées.

Dans le cas où les contrôles de conformité et les essais révéleraient un élément non conforme ou l'impossibilité d'obtenir toutes les caractéristiques exigées dans le présent document, l'Entreprise devra remplacer ou modifier à ses frais et sans augmentation des délais contractuels les pièces ou éléments de l'installation incriminée.

1.11.5 CONSUEL

Sans objet

1.11.6 DEMARCHE POUR LES ESSAIS EN CONFIGURATION DEFINITIVE

Les essais interviendront une fois que l'entreprise aura effectué ses propres autocontrôles à la fin de chaque phase de travaux.

1.11.7 RECEPTION

La réception n'est prononcée qu'après remise par l'Entreprise du Dossier des Ouvrages Exécutés, des procès-verbaux d'essais sans observations réhibitoires, des notices d'exploitation et d'entretien des matériels installés et d'une attestation de conformité établie par le Contrôleur Technique.

1.11.8 GARANTIE

La période de garantie des équipements ne commence qu'à compter du jour de la réception "in situ" des installations en ordre de marche.

Il est exigé que tous les matériels et équipements prévus et installés soient aptes à satisfaire à la fonction qui leur est destinée et donnent les résultats attendus.

De ce fait, et pendant toute la durée de la période de garantie (un an de parfait achèvement et deux ans de bon fonctionnement) l'Entreprise doit à ses seuls frais, quelle que soit l'importance des travaux, effectuer tout renforcement, adjonction, remplacement de matériels ou équipements mal dimensionnés, mal adaptés ou défectueux.

1.12 FORMATION

Dès la prise de possession de l'installation par le Maître d'Ouvrage et à une date fixée en accord avec lui, l'Entreprise déléguera des représentants qualifiés pour les formations dans le but de former le personnel qualifié désigné et ce afin que ce personnel puisse assurer la prise en main courante de toute l'installation.

Les formations seront prévues pour un maximum de 5 à 6 représentants du personnel d'exploitation par session. Cette prestation fait partie intégrante du présent marché.

L'Entreprise proposera un programme de formation qu'elle soumettra à l'approbation de la Maîtrise d'Œuvre et de la Maîtrise d'Ouvrage au minimum un mois avant la réception des ouvrages.

La formation devra se faire sur site en utilisant les systèmes mis en place, sur la base des documents DOE. Elle fera l'objet d'un compte-rendu mentionnant les noms et qualités des personnels formés par systèmes. Les frais de déplacements du personnel chargé de la formation devront être inclus dans le prix.

Dans les cas de fourniture de systèmes d'automatismes complexes prévoir une session de formation spécifique et la décrire.

Le présent devra se reporter au chapitre concerné détaillant le nombre de sessions à prévoir dans les différents chapitres de la description des ouvrages.

2 DESCRIPTION DES OUVRAGES DE SURETE

2.1 ETAT DES LIEUX DES INSTALLATIONS EXISTANTES

Les différents sites du rectorat sont suivant le cas équipés d'installations de sureté qui seront à déposer en fin de chantier, à conserver et/ou à étendre suivant la vétusté du matériel en place.

Le présent lot devra prendre en compte la possibilité ou non de conserver certaines centrales intrusion afin que celles-ci soient compatibles avec le superviseur sans développement spécifique de "connecteur". Dans le cas contraire le présent lot à l'obligation de développer le(s) connecteurs nécessaires afin d'assurer les remontées des informations depuis le réseau IP depuis chaque centrale conservée ou dans le cas contraire de prévoir le remplacement.

Nota : les installations obsolètes devront être déposées en fin de chantier une fois les nouveaux systèmes opérationnels.

2.1.1 CONTRÔLE D'ACCÈS

Une installation de contrôle d'accès architecturée autour d'un matériel de marque URMET modèle Pyramid (centrale, lecteur de badge) est existante sur les sites suivants à savoir :

- Bâtiments du rectorat au 92 et 96 Rue d'Antrain.
- Bâtiment DSDEN 1 quai Dujardin.
- Bâtiment DSII Rue Jean Julien Lemordant.

2.1.2 ALARME INTRUSION

Une installation d'alarme intrusion qui pour certains bâtiments devra être remplacée entièrement et pour d'autres complétée par des points de détection à savoir :

- Bâtiments du rectorat au 92 et 96 Rue d'Antrain – Installation existante avec centrale Aritech modèle ATS1201 NFA2P grade 2
- Bâtiment UAR allée Perrin – Installation existante récente avec centrale Aritech modèle ATS1500A IP NFA2P grade2
- Bâtiment DSII Rue Jean Julien Lemordant – Installation existante récente avec centrale Septam modèle Harmonia NFA2P grade 3

NOTA : L'entreprise devra préciser dans son offre en fonction de la solution envisagée et de l'existence ou non de connecteurs sur le logiciel de supervision, les centrales qu'elle prévoit de conserver et/ou de remplacer. Dans tous les cas la solution retenue devra être opérationnelle à 100%.

2.1.3 VIDEO SURVEILLANCE

Seul le bâtiment du rectorat au 92 Rue d'Antrain est équipé d'une installation de vidéo-surveillance hors service au sous-sol avec enregistreur vidéo HIKVision + 4 caméras.

2.1.4 SÉCURITÉ INCENDIE

Chaque bâtiment ou ensemble de bâtiment est équipé d'un système de sécurité incendie suivant son classement vis-à-vis de la réglementation en vigueur.

- Bâtiments du rectorat au 92 et 96 rue d'Antrain – Installation existante commune de catégorie A avec équipement d'alarme type 1 adressable Algorex CI1142 Siemens + d'un CMSI collectif SST2240 Siemens
- Bâtiment du rectorat au 108 rue d'Antrain – SSI de catégorie E avec équipement d'alarme type 4 de marque Nugelec
- Bâtiment DSDEN 1 qui Dujardin - SSI de catégorie B avec un CMSI adressable modèle ANTARES IV de marque DEF

- Bâtiment UAR Allée Jean Perrin - SSI de catégorie E avec équipement d'alarme type 4 de marque Nugelec
- Bâtiment DSII Rue Jean Julien Lemordant- SSI de catégorie E avec équipement d'alarme type 4 de marque Eaton

Nota : Seule des adaptations seront nécessaires sur certains SSI afin d'assurer le déverrouillage des issues verrouillées par le contrôle d'accès en cas du déclenchement de l'alarme incendie.

2.2 HYPOTHÈSES DE CONCEPTION

2.2.1 PRESCRIPTIONS PARTICULIERES (LIMITES DE PRESCRIPTIONS)

2.2.1.1 A CHARGE DU MAITRE D'OUVRAGE

- Fourniture des serveurs/enregistreur avec les capacités de stockage et les solutions logicielles associés avec licences (hors logiciel métier)
- Fourniture des accès sécurisée sur le réseau du rectorat (configuration de réseau LAN)
- L'entreprise précisera :
 - Quelles sont les caractéristiques physiques des serveurs à prévoir (matériel et logiciel).
 - La capacité de stockage nécessaires des données (sauvegarde) suivant les tranches de travaux.
 - Les mesures visant à assurer la haute disponibilité (alimentation, redondance des serveurs, systèmes de secours des disques de type RAID, ...)
 - Le type de services d'annuaires avec le protocole.
- Le service d'annuaire du personnel du rectorat au protocole LDAP

2.2.1.2 A CHARGE DU PRESENT LOT

- La fourniture des postes de travail les solutions logicielles, il indiquera :
 - Quelles sont les caractéristiques physiques des postes de travail (matériel et logiciel)
 - Quelles sont les conditions de remplacement en cas de panne (délai d'intervention, durée de garantie, termes du contrat de maintenance).
- Il décrira le paramétrage du système visant à garantir la sécurité:
 - Système d'exploitation,
 - Anti-virus,
 - etc
- Il devra s'assurer que la durée de support des composants de sa solution soit au moins égale à celle de la garantie.
- Il décrira les fréquences et modes de mise à jour des composants (notamment patches système et anti-virus)
- Administration et maintenance des postes informatiques
- L'entrepreneur indiquera comment est effectuée l'administration (processus et responsabilités, en installation et en fonctionnement),
 - Des postes de travail,
 - Des composants logiciels.

L'entrepreneur indiquera comment sont réalisés les moyens de sécurisation de l'administration (chiffrement, authentification forte...).

Il est souhaité que l'administration de la solution et son service soient accessibles sur des interfaces de raccordement différenciées.

Il indiquera si des solutions de télémaintenance sont déployées, le cas échéant leur mode de fonctionnement et le processus de prise de main à distance (avec les éléments relatifs à la sécurisation de l'accès en télémaintenance qui devra être compatible).

- Contrôle et surveillance du serveur.

L'entrepreneur indiquera sous quelles conditions la DSII du Rectorat devra déployer sur ces serveurs et son système de stockage des solutions de contrôle et surveillance et précisera notamment :

- Les possibilités et moyens d'accès aux logs des équipements (envoi au fil de l'eau, accès à la demande, possibilité de déployer un agent de collecte ...),
- La possibilité d'auditer les serveurs concernés, soit en propre soit par un prestataire choisi par elle, sachant que ces audits pourront prendre la forme, entre autres, de tests d'intrusion, revue de configuration, etc.
- Les engagements de remédiation du prestataire en cas de faille publiée ou remontée lors des audits.

2.2.2 FIABILITE DES SYSTEMES

Les équipements seront soumis à des essais (exercice de faille de sécurité). L'adjudicataire devra prévoir la mise à disposition de moyens (matériels, logiciels, plateformes, licences) permettant aux services du rectorat de réaliser les essais.

Certains périphériques (caméra, capteurs Bluetooth, autres) subiront des tests de robustesse, de véracité, de fiabilité, de sécurité, sur la base des produits proposés par les fournisseurs et en sus des tests réalisés lors de la recette, dans un cadre d'utilisation nominale et dans des contextes liés à des scénarios envisagés.

Les essais de fiabilité pourront être réalisés après la réception sur les équipements suivants :

- Caméra,
- Lecteur de badge,
- UTL,
- Liste non exhaustive.

Les processus de tests se dérouleront après finalisation du dossier d'études. La MOA/MOE s'engage à un délai pour donner un accord ou un refus sur les produits proposés.

Le titulaire devra prévoir un calendrier d'études en fonction des dates de livraison des fiches techniques et à réception des matériels le cas échéant. Il pourra aussi être émis un premier visa "VAO-Sous réserve des tests de sécurité".

Si le matériel répond aux exigences de sécurité et de fiabilité, les documents seront diffusés par le titulaire afin d'être validés.

2.2.3 GESTION DES VERSIONS ET MISES A JOUR

Le titulaire devra préciser dans une analyse fonctionnelle les capacités (matérielles et logicielles) pour la gestion des mises à jour (sens ascendant), afin d'assurer le maintien en condition opérationnelle et de sécurité.

Le titulaire précisera également la fin de vie, la fin de support matériel et logicielle de chaque brique de la solution.

2.2.3.1 MATRICE DES FLUX

Le titulaire devra élaborer et transmettre une trame de tableau Excel contenant les indications permettant de localiser précisément l'équipement IP à raccorder au réseau informatique du rectorat (à valider avec les services de la DSII du rectorat)

- Libellé de l'équipement,
- Niveau,
- Local,
- L'adresse IP,
- Les ports de connexion,
- Les configurations particulières (802.1x, la version de Firmware, etc.)
- Toutes autres informations utiles et nécessaires.

2.2.3.2 GESTION ET SECURITE DES DROITS D'ACCES

L'accès à chaque machine informatique sera sécurisé par « Login » et « Mot de passe » associé au domaine réseau pour chacune des applications.

Le titulaire devra prévoir une rotation des mots de passe d'accès aux systèmes d'informations.

A l'ouverture de la session Windows, l'opérateur saisira son « Login » puis « Mot de passe » et lui donnera accès à l'application en fonction de son profil (Opérateur – Administrateur, Maintenance, etc).

La stratégie des mots de passe sera définie par le Maître d'Ouvrage et son exploitant (association de chiffres, caractères alphabétiques et caractères spéciaux) sur une durée définie.

L'ensemble des systèmes d'informations sera compatible avec le protocole d'authentification SAML V2. Cependant les futurs systèmes mis en œuvre par le présent lot seront exploités par différents acteurs (multi-tenant) et par conséquent les systèmes informatiques devront être compatibles avec les sources standards d'annuaires (LDAP, Microsoft. NET – Active Directory, etc.), tout en respectant la sécurité et la confidentialité.

2.2.3.3 RISQUE DES CONNEXIONS EXTERIEURES

Pour les équipements extérieurs ou accessibles raccordés au réseau informatique, le titulaire devra :

- Mise en œuvre de socles anti-vandalisme,
- Mise en œuvre de fourreaux de protection sur les câbles,
- Accessibilité démontage maintenance depuis l'intérieur du bâtiment, sans nacelle, et pas de démontage possible depuis l'extérieur (décrire les modalités de maintenance).
- Configuration d'une segmentation forte avec l'ajout d'un VLAN spécifique aux équipements
 - Mise en place d'un PVLAN par équipement au niveau architecture réseau pour éviter le rebond d'un équipement sur un autre ou la saturation de la bande passante (DDoS).
- Configurations du protocole d'authentification 802.1x par certificats.

2.2.3.4 OUTILS DE TEST ET DE DIAGNOSTIC

Les logiciels doivent fournir en standard tous les outils permettant de vérifier le bon fonctionnement de l'application et de diagnostiquer le mieux possible les comportements anormaux.

2.2.3.5 PRODUITS CERTIFIES CSPN

Dans le cadre du présent projet, certains matériels et équipements proposés par l'entreprise devront être certifiés de premier niveau par l'Agence nationale de la sécurité des systèmes d'information.

2.2.4 FONDEMENT DU CONTROLE D'ACCES

2.2.4.1 DEFINITION

Un système de contrôle d'accès physiques est un dispositif ayant pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local. Il est constitué de moyens permettant d'autoriser les entrées et sorties de zones sensibles aux seules personnes qui ont droit d'y accéder.

Un système de contrôle d'accès assure trois fonctions :

- L'identification et l'authentification,
- Le traitement des données,
- Le déverrouillage.
- Ces fonctions sont assurées en chaque point où l'accès est contrôlé.

Dans le cas d'un contrôle d'accès utilisant des technologies sans-contact, quatre éléments support interviennent :

- Le badge,
- Le lecteur (Tête de lecture),
- L'unité de traitement local (désignée par UTL),
- Le serveur de gestion du système.

Il convient de prendre en considération la sécurité des liaisons filaires entre les éléments ainsi que la sécurité du serveur de gestion du système de contrôle d'accès et des postes de travail utilisés pour le paramétrage et la programmation.

2.2.4.1.1 La phase d'identification / authentification

Pour mémoire :

- S'identifier, c'est le fait de communiquer une identité
- S'authentifier c'est apporter la preuve de son identité : c'est donc un élément complémentaire à l'identification.

Dans le contexte des systèmes de contrôles d'accès, et en fonction de la technologie choisie, la phase dite d'identification/authentification peut se réduire à l'identification du badge, ou à l'identification et l'authentification du badge seulement.

2.2.4.1.2 Identification

Dans un système reposant sur une technologie sans-contact, l'identification est la présentation d'un badge à un lecteur.

2.2.4.1.3 Authentification du badge

L'authentification du badge consiste à prouver qu'il est valide.

Pour un système de contrôle d'accès reposant sur des technologies sans-contact, l'authentification du badge se fait le plus souvent par un échange cryptographique permettant au badge de prouver qu'il détient des éléments secrets sans les révéler. Si les fonctions cryptographiques sont suffisamment robustes, il n'est pas possible de cloner un tel badge tant que les éléments secrets restent protégés. Néanmoins le badge, support physique, peut être volé. Dans ce cas, il faut que le porteur du badge le signale à l'administrateur du système pour supprimer les accès.

2.2.4.1.4 Authentification du porteur

Le badge étant préalablement authentifié, il s'agit pour le porteur du badge de prouver qu'il en est le détenteur légitime.

Le système sera compatible pour réaliser une authentification à deux facteurs. En effet, l'authentification du porteur se fait par l'usage d'un second élément sélectionné parmi ce que l'on est et ce que l'on sait. Elle peut se faire par exemple par la saisie d'un mot de passe, d'un code que seul le détenteur légitime du badge connaît ou par l'usage de la biométrie (compatibilité du système à prévoir).

2.2.4.2 EXPRESSION DES BESOINS FONCTIONNELS

Selon l'usage qui en est fait et selon leur localisation, les portes doivent plus ou moins répondre aux critères suivants.

2.2.4.2.1 Type d'accès

- Accès libre
- Accès par clef
- Accès par badge + clef
- Accès par badge ou code
- Accès par badge et/ou Qrcode

2.2.4.2.2 Sécurité des personnes

- Entrée possible en cas de feu
- Sortie possible en cas de feu

2.2.4.2.3 Sûreté requise pour le local

- Résistance à l'effraction
- Indifférent à la panne de courant

2.2.4.3 TRAITEMENTS DES DONNEES

Le traitement des données est assuré en premier lieu par l'unité de traitement local (UTL). Le matériel proposé sera configuré afin qu'aucune donnée ne soit sauvegardée sur l'UTL en cas de fonctionnement anormal. Dans le cas où des données sont maintenues sur les équipements, les données seront automatiquement chiffrées.

Cette unité assure la gestion de toutes les demandes d'accès, compare ces demandes par rapport à un ensemble de droits stockés dans sa base de données, et délivre les commandes de libération des verrouillages.

Le serveur de gestion du système :

- Centralise les journaux d'événements,
- Remonte les événements au gestionnaire,
- Héberge la base de données centrale tenue à jour (Droits, utilisateurs, groupes, badges, etc.)
- Pilote l'ensemble des UTL en leur transmettant la base de données nécessaire à leur traitement d'accès.
- Echange base de données salariés et base de données authentification,
- Echange de variables en OPC ou API (Client/serveur).

2.2.4.4 VERROUILLAGE / DEVERROUILLAGE

Le dispositif de verrouillage permet de réaliser le blocage mécanique du point d'accès pour empêcher le passage des personnes non autorisées. Le contrôle d'accès autorise le déverrouillage.

Dans le cadre de l'analyse des risques, il conviendra de prendre en compte les situations dégradées (coupure électrique, gestion de crise, etc) et le cas d'ouverture automatique (incendie) pour les issues de secours.

2.2.4.5 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 (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 véhicule),
- Les exigences de circulation particulières et contraintes spécifiques (sortie de secours),
- La quantité prévisionnelle de passage.

Le présent projet offre différents types d'espaces à destination de différents publics, notamment :

- Zone publique (noté ZPUB)
- Il s'agit de la zone ouverte au grand public pour laquelle aucune identification n'est requise, parmi ces zones :
 - Les zones ERP,
 - Les espaces multifonctionnels lorsque les accès vers la zone ERP sont ouverts,
 - Les Halls.
- Zone intermédiaire de stationnement – parkings voitures, motos et vélos (ZSTA)
 - Il s'agit des espaces qui ne sont pas publiques (accès contrôlé par badge) mais qui ne sont pas des « zones de vie », ces zones potentiellement disjointes sont uniquement destinées au stationnement de véhicules (automobiles, motos, vélos) et à la circulation de personnes à cet effet.
- Zone commune (ZCOM)
 - Il s'agit de l'ensemble des zones menant aux espaces de travail (escaliers, ascenseurs, paliers et zones de circulation ne permettant pas un filtrage « fin »). Les espaces convivialité et salle de pause sont inclus dans ce zonage.
- Il existe des zones communes intérieures, mais aussi extérieures (terrasses). Il est possible de les décrire ZCOM-I et ZCOM-E.
- Ces zones se distinguent par des besoins spécifiques soit en termes de bâtiment, soit en termes de sécurité :
 - Zones métiers spécifiques ;
 - Zones liées à ces activités
 - etc
- On distinguera dans cette catégorie plusieurs zones avec des règles distinctes, en particulier la zone sensible « ZS ».
- Zones Techniques (ZTECH)
 - On trouve ici les locaux techniques informatiques.

Le public identifié accédant aux espaces est :

- Grand public ;

- Visiteurs extérieurs;
- Salariés ;
- Prestataires ;
- Etc.

Une hiérarchisation peut être établie sur les zones en fonction du besoin de sécurité nécessaire, ainsi sur chaque type de zone les besoins de sécurité peuvent s'additionner.

- Niveau 1 : Abords immédiats et ZERP
- Niveau 2 : ZLOC et ZLPT
- Niveau 3 : ZLPS et ZTECH
- etc

Le passage d'une zone à une autre ne peut se faire que par le passage au niveau immédiatement supérieur ou inférieur.

En fonction de la hiérarchie des niveaux, il sera utilisé différentes clés d'accès suivant la zone (clé bleu, clé rouge, clé verte), afin de physiquement s'assurer de cette hiérarchie de sécurité. De plus, l'objectif étant d'ouvrir les champs des possibilités en termes de développement (biométrie, accès par Bluetooth, etc.) et il n'est pas envisageable que la clé d'identification soit commune à l'ensemble des zones.

2.2.4.6 IDENTIFICATION DES ACTEURS

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

- Les demandeurs (chef de services, managers, etc.) qui font les demandes d'attribution de badges et droits associés,
- Les responsables de validation (responsables de sites ou de zones), 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 d'accès physiques,
- Les opérateurs de sauvegarde du système,
- Les opérateurs d'exploitation des journaux d'évènements du système,
- Les mainteneurs des installations techniques
- 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'approbations et de contrôle indépendants sont mis en place et respectés.

2.2.4.7 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 badge,
- Délivrance de badge,
- Révocation de badge,

- Modifications de droits.

2.2.4.8 CONTINUITE 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, délai 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.

2.2.4.9 INTERFACES OU INTERCONNEXIONS

Les interconnexions avec d'autres systèmes (vidéosurveillance, système de gestion ressources humaines, Annuaire LDAP, active directory, etc.) doivent être référencées et/ou exprimées au préalable car elles ont un impact sur le projet de mise en place d'un système de contrôle d'accès. La nature de ces interconnexions doit être détaillée afin que les réponses aux appels d'offres soient cohérentes en regard des systèmes existant ou à intégrer.

2.2.4.10 BADGE MULTISERVICE

Le système de contrôle d'accès sera configuré afin d'être compatible multiservice. Le badge permettra notamment de gérer :

- L'accès aux locaux,
- L'accès aux parkings,
- Accès à la session imprimante
- Autres.

Le titulaire devra prévoir l'ensemble des réunions d'interface avec le maître d'ouvrage et le développement de l'interface :

- Définition de la charte d'encodage,
- Définition de la structure des usages,
- Définition des emplacements/secteurs,
- Définition des critères de sécurité : chiffrement /clé,
- Définition des identifiants : N° Série /Matricule / Identifiant unique.

Dans le principe où le badge sera multiservice et sera donc compatible avec l'AMC - Application Multi-services Citoyenne. Cette application fait appel à la notion de secteur, référencé par la norme : XP P99-508 (Juin 2018).

2.2.4.10.1 Niveau de sûreté et résistance aux attaques logiques

La technologie du badge devra être :

- conforme à la norme internationale ISO/IEC 14 443-1, 14 443-2,
- communiquer avec des cartes sans contact du type A, du type B et B' Niveau 1 à 4,
- Identifiants tous badge 13,56 MHz (Mifare Classic, Mifare +, Desfire).

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

- D'informations sur l'entreprise (Nom, adresse),
- D'informations sur le porteur (Nom, prénom, poste),
- Les accès qu'ils permettent.

2.2.5 FONDEMENT DE L'ANTI-INTRUSION

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

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

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

Les applications logicielles seront installées sur le poste de travail principal. L'administrateur informatique donnera les droits aux profils ayant besoin d'un accès à l'application.

Les systèmes de détection extérieure qui sont disponibles sur le marché utilisent différentes technologies. Cette variété permet de couvrir l'ensemble des besoins de sécurisation d'un site de façon la plus adaptée possible.

Nous considérons que la conception de chaque dispositif de protection extérieure peut se faire selon quatre couches concentriques, déployées seules ou en combinaison. Ces choix doivent permettre de disposer d'un système adapté à la topographie, à l'environnement et au niveau de risque de chaque site.

- Le premier niveau de détection concerne le moment de l'escalade ou de la destruction de la clôture qui délimite la propriété,
- Le deuxième niveau concerne le périmètre intérieur, typiquement situé à proximité de la clôture,
- Le troisième niveau concerne les espaces compris entre le périmètre de propriété et les bâtiments ou plus spécifiquement certains espaces extérieurs où les risques sont les plus élevés.
- Le quatrième niveau concerne la protection des façades des bâtiments, des murs ou des ouvertures afin de déclencher une alerte avant l'intrusion dans les bâtiments,

Chaque dispositif de détection doit être choisi pour obtenir le meilleur compromis entre la certitude et la fiabilité de détection. Ceux-ci seront d'autant plus efficaces à exploiter que le ou les systèmes déployés fournissent une information d'alarme qualifiée.

Les choix technologiques proposés dans notre étude, reposent sur le principe d'obstacle pour :

- Dissuader
- Retarder, empêcher,
- Détecter,
- Lever de doute.

2.2.5.1 DISSUADER – RETARDER - EMPECHER

La résistance mécanique et la hauteur doit représenter un élément non seulement dissuasif mais également retardateur.

La clôture doit être définie en fonction des différents types de franchissement :

- Franchissement par-dessus : Escalade, saut,
- Passage à travers : Découpe, démontage, enfoncement, arrachement,
- Passage par-dessous : Déblaiement sous clôture, soulèvement.

2.2.5.1.1 Franchissement par le dessus

Il faut choisir la hauteur de la clôture par rapport aux possibilités de franchissement lié à l'environnement.

La proximité de route – chemin à proximité de la clôture et sa hauteur est un facteur aggravant vis-à-vis de la possibilité d'intrusion sans toucher à celle-ci (« Risque intrusion nacelle » ou « véhicule collé à la clôture »)

2.2.5.1.2 Franchissement à travers

L'enfoncement ou l'arrachement est à prendre en compte pour le choix des panneaux et le dimensionnement des poteaux. La structure des panneaux ne doit pas permettre la découpe à l'aide en outre de pinces coupantes ou de scies (Cas pour les panneaux alvéolaires ou treillis soudés). Les systèmes de fixations doivent être « indémontables ».

2.2.5.1.3 Franchissement par le dessous

Le franchissement par-dessous peut être réalisé soit par soulèvement (Structure souple à simple torsion) soit par déblaiement sous grillage.

2.2.6 FONDEMENT DE LA VIDEOSURVEILLANCE

- Vidéoprotection = Caméras filmant des lieux ouverts au public (ou la voie publique).
- Vidéosurveillance = Caméras filmant des lieux non accessibles au public.

Ces deux termes ne sont pas synonymes et ne peuvent pas être utilisés l'un pour l'autre :

- La vidéosurveillance concerne les locaux non accessibles aux publics : zones sensibles, etc.
- La vidéoprotection concerne la voie publique et l'ensemble des locaux ouverts au public (abords et périphérique des locaux, halls d'accueil, ...).

Le cadre juridique de ces deux dispositifs est différent, même si les règles qui les régissent se rejoignent en partie. Schématiquement, la vidéosurveillance est soumise à la loi n°78-17 du 6 janvier 1978 modifiée (dite loi CNIL) alors que la vidéoprotection est régie par le Code de la sécurité intérieure.

Il faut identifier l'expression de besoin du client en s'appuyant sur les éléments de base décrit ci-dessous.

- Quel est l'objectif à atteindre (Répression – Prévention – Sécurité) ?
- Quels sont les événements qui poussent le client à mettre en œuvre un tel système (Vol, intrusion, filtrage d'accès (véhicules), etc.) ?
- Quels sont les périmètres à surveiller (Extérieur, intérieur) ?
- Souhaite-t-il exploiter les images en local (nécessite du personnel) ou à distance ?
- Surveillance jour et nuit ?
- Enregistrement souhaité ?
- Fonction d'analyse d'image ?

Afin de mener à bien ce projet, il est crucial pour le client d'avoir une vision stratégique globale du dispositif à mettre en place : notion de schéma directeur, permettant le déploiement de cette phase à court terme, tout en s'interrogeant sur les évolutions futures, et de ce fait, sur des phases de déploiements ultérieures afin de mesurer et identifier les avantages et inconvénients des dispositifs déployés.

La définition de la fonction finale de la vidéosurveillance, les usages types pouvant être fixés pour le premier déploiement, mais également pour des objectifs futurs :

- Détection de :
 - Surveillance,
 - Sécurité des personnes et des biens,
 - Reconnaissance d'objets abandonnés (voiture, sacs, valises),
 - Gestion de trafic automobile,
 - Contrôle d'accès (borne escamotable) – levée de doute sur "qui tente d'entrer ?",
 - Reconnaissance de plaque minéralogique,

L'outil est particulièrement efficace dans les endroits clos qui ont fait l'objet d'un traitement complet de sécurisation (Obstacle physique pour « retarder » et équipements électroniques de détection précoce pour intervenir « Pré alerte »

- Définition de la salle de visualisation
 - Quel moniteur au niveau du PC de sécurité?
 - Autre moniteur en dehors du PC de sécurité?
 - Quelle stratégie retenir pour les masques numériques (Voie public) ?
- Définition du type de logiciel à déployer
 - Quelles sont les fonctionnalités de l'IHM (Interface Homme/Machine) nécessaires et suffisantes qui correspondent au mieux, aux opérateurs ?
- Définition de la stratégie de transport des images :
 - Quel transport : analogique (jusqu'où ?), numérique (à partir d'où ?)
 - Analogique bande de base : Coaxial, FO analogique, laser, multiplexage,
 - Numérique: FH, ADSL, CPL, SDSL, WIFI, WIMAX, 3G, GPRS, Bluetooth, Ethernet, RPV IP, Internet...
 - QoS (Quality of Services : les paramètres à respecter... débit, temps, TEB)
 - 3 paramètres clés pour la Vidéosurveillance :
 - Qualité surfacique d'une image (résolution/netteté/contraste/couleur/luminance)
 - Fluidité (Nombre d'image par seconde)
 - Contrainte Temporelle (pour la réception de la vidéo pour l'opérateur ; délai moyen, variance maximale... et pour la télécommande de la caméra dans l'autre sens) – Télémétrie
- La continuité de service
 - Comme tout équipement, un système de vidéo protection est susceptible de connaître des pannes, quelle que soit la qualité du matériel et de la maintenance. Ces pannes peuvent conduire à des interruptions de service. Pour des applications sécuritaires, une interruption de service n'est pas acceptable. En fonction de ces contraintes particulières, il faudra :
 - Doubler les équipements,
 - Redondance du réseau de transport des données,
 - Redondance des alimentations électriques,
 - Redondance des enregistrements,
 - Prévoir un contrat de maintenance adapté à l'exigence.

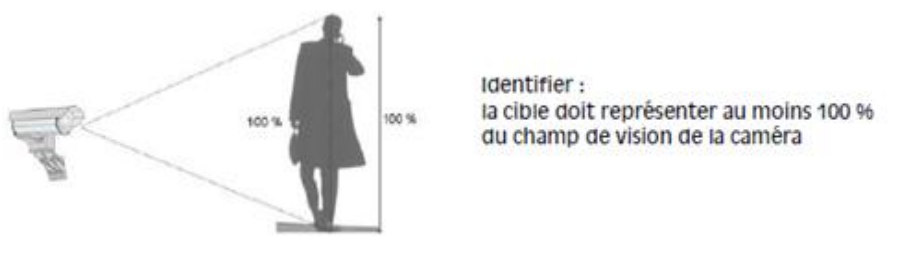
2.2.6.1 LE NIVEAU D'EXPLOITATION DE LA VIDEOSURVEILLANCE ET LES OBJECTIFS ATTENDUS

Il est important de noter qu'en fonction de l'exploitation que l'on veut faire des images vidéo, les matériels qui vont être mise en jeu, notamment au niveau des caméras de prise de vue :

- Identification
- Reconnaissance
- Détection
- Surveillance

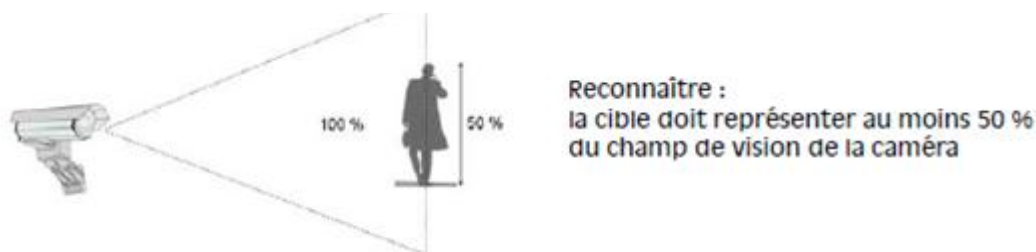
2.2.6.1.1 L'identification

Pour permettre l'identification d'un individu et donc fournir des éléments de preuve aux forces de l'ordre, il est nécessaire de disposer d'une résolution linéaire minimale de 250 px/m (pixel/mètre). Cette résolution linéaire autorise l'extraction d'une vignette de visage de taille 90 x 60 pixels conformément aux prescriptions de l'arrêté du 3 août 2007.



2.2.6.1.2 La reconnaissance

L'observateur peut s'assurer avec certitude si l'individu présent sur l'image est le même qu'une personne qu'il a déjà vue auparavant. Pour permettre la reconnaissance d'un individu, il est nécessaire de disposer d'une résolution linéaire minimale de 125 px/m (pixel/mètre).

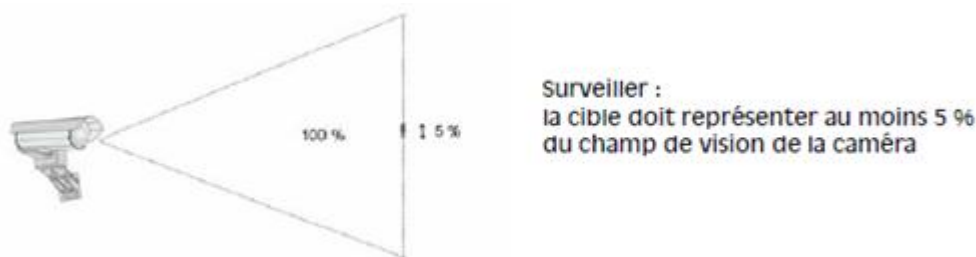


2.2.6.1.3 La détection

À la suite d'une alarme, l'observateur peut, après une recherche, s'assurer avec un grand degré de certitude s'il y a une personne visible sur l'image vidéo qui lui est présentée. Pour permettre la détection d'une personne, il est nécessaire de disposer d'une résolution linéaire minimale de 25 px/m (pixel/mètre).

2.2.6.1.4 La surveillance

Son but est de visualiser un champ assez large, afin d'effectuer une surveillance très sommaire d'un site, c'est-à-dire de surveiller globalement que rien d'anormal ne se passe à l'intérieur du site (Présence d'individus ou de véhicules, leur nombre, leur direction et leurs mouvements par exemple). Pour permettre la surveillance d'une cible, il est nécessaire de disposer d'une résolution linéaire minimale de 12,5 px/m (pixel/mètre).



2.2.7 RESEAU SURETE

2.2.7.1 GENERALITES

Un réseau informatique de type Ethernet-IP et sera mis en œuvre par le service de la DSII afin de fédérer les équipements IP des systèmes suivants :

- Contrôle d'accès,
- Détection-intrusion,
- Vidéosurveillance

Ce réseau est constitué :

- Des équipements principaux cœur de réseau installé dans les locaux de la DSII
- Des équipements déportés répartis dans les locaux VDI des différents bâtiments.
- D'un maillage par des liaisons fibres optiques

À partir de réseau, le titulaire devra raccorder les différents matériels IP par l'intermédiaire des liaisons capillaires détaillées au paragraphe « Câblage VDI ».

La fourniture des jarretières optiques et cordons de brassage nécessaires aux systèmes de sûreté ainsi que le brassage des équipements de sûreté sera à la charge du présent lot.

2.2.7.2 PARAMETRAGES RESEAU

Le paramétrage du réseau informatique « Sûreté » sera dû par les services de la DSII.

Le choix des équipements IP raccordés au réseau Sûreté sera fait de manière à privilégier les échanges de données sécurisés. Les protocoles de chiffrement de type HTTPS ou SSL/TLS seront privilégiés. Si les équipements IP n'utilisent pas de communication sécurisée, leurs communications seront complètement cloisonnées.

Il sera notamment prévu un VLAN (réseau virtuel) spécifique par application.

2.2.7.3 ALIMENTATION POE DES TERMINAUX

Certains terminaux raccordés sur le réseau Sûreté seront alimentés en PoE (Power over Ethernet) depuis le matériel actif.

2.3 SUPERVISION

2.3.1 POSTE PRINCIPAL D'EXPLOITATION ET POSTE SECONDAIRE

Le système proposé aura une architecture logicielle Client / Serveur. Le poste principal sera raccordé sur le réseau de type Ethernet TCP/IP du rectorat. Il supervisera le dialogue avec les UTL /centrales et le poste client raccordé aussi sur même réseau.

Le logiciel de contrôle d'accès, intrusion et supervision sera installé sur ces deux postes, permettant à la fois de paramétrer, d'exploiter les badges et de visualiser des alarmes, défauts et états de fonctionnement du système.

Dans un souci de pérennité, le logiciel retenu devra fonctionner obligatoirement sur un système d'exploitation type Windows Serveur 2022 et une base de données SQL serveur 2022 64 bits.

Le matériel informatique (PC, serveur, postes clients) respectera les prérequis, recommandations du constructeur de la solution.

Le système de supervision assurera une sauvegarde automatique et périodique de la base de données sur un répertoire donnée à définir. Il permettra de définir et de paramétrer la date, l'heure, le chemin et la fréquence des sauvegardes.

2.3.1.1 CONFIGURATION DES POSTES INFORMATIQUES (A CHARGE DU PRESENT LOT)

Dans le cadre du présent projet, il sera mis en place :

- Un poste d'administration et d'exploitation au niveau du PC de sécurité (poste principal)
- Un poste d'exploitation au niveau du bureau DAGE (poste secondaire)

Le modèle proposé par le titulaire sera confirmé durant sa phase d'exécution mais sera de marque DELL ou de qualité équivalente.

Les spécifications techniques précisées ci-dessous respecteront au minimum les prérequis du logiciel d'exploitation (à confirmer par l'adjudicataire du lot) :

2.3.1.1.1 Poste d'exploitation du PC sécurité (Poste principal)

Ce poste sera constitué de :

- Unité centrale de type mini tour
- 1 carte mère avec processeur, performances adaptées aux traitements à réaliser
- 1 carte graphique multi - écrans
- 1 disque dur SSD intégré de 500 Go minimum
- Mémoire vive de capacité adaptée aux traitements à réaliser
- 1 clavier Azerty,
- 1 souris optique,
- 1 carte Ethernet 10/100/1000 Mbit/s avec agent SNMP v3
- 1 écrans couleur 27 pouces LCD format 16/9^{ème}
- 1 système d'exploitation Windows ou équivalent
- Logiciel anti-virus avec mise à jour automatique des définitions de virus via le cloud inclus pendant 2 ans
- Alimentations 230 V secourue par onduleur

Ce poste sera équipé :

- Du module logiciel permettant la visualisation des images des caméras
- 1 écran sera dédié à l'affichage du fil de l'eau et aux diverses fonctionnalités du contrôle d'accès
- 2 écrans dédiés à l'affichage des caméras

2.3.1.2 Console de pilotage

La console de pilotage sera connectée en IP au réseau Sûreté et sera équipée :

- De boutons permettant :
 - La sélection de la caméra à piloter
 - La commutation des vues sur les moniteurs,
 - La relecture des événements,
 - La sélection de prépositions ou de rondes enregistrées.

2.3.1.2.1 Poste de création des badges (Poste principal)

Ce poste sera constitué de :

- Unité centrale de type mini tour
- 1 carte mère avec processeur, performances adaptées aux traitements à réaliser

- 1 carte graphique
- 1 disque dur SSD intégré de 500 Go minimum
- Mémoire vive de capacité adaptée aux traitements à réaliser
- 1 clavier Azerty,
- 1 souris optique,
- 1 carte Ethernet 10/100/1000 Mbit/s avec agent SNMP v3
- 1 écran couleur 23 pouces LCD format 16/9ème
- 1 système d'exploitation Windows ou équivalent
- Logiciel anti-virus avec mise à jour automatique des définitions de virus via le cloud inclus pendant 2 ans
- Alimentations 230 V

Ce poste sera équipé :

- D'un lecteur encodeur de badges
- Du module logiciel permettant la création des badges

2.3.1.3 MUR D'IMAGES

Le mur d'images sera constitué de 2 écrans vidéo LCD permettront la visualisation rapprochée, en temps réel, des images des caméras du système et à l'exploitation du système

Ils seront fixés sur un des cloisons du local selon une disposition qui devra être validée au cours des études d'exécution.

Leur angle de vision permettra d'assurer le confort visuel des utilisateurs dans la pièce. Ils permettront des temps d'apparition de l'image compatibles avec une exploitation en temps réel des caméras.

Caractéristiques :

- Moniteur de type LED
- Taille : 40 pouces
- Bords ultra-fins
- Format 16/9ème
- Définition Ultra HD 3840 x 2160 pixels minimum
- Technologie anti-reflet et anti-poussière
- Luminosité de 500 cd/m² minimum
- Connectique DVI, USB, HDMI, VGA et RJ45
- Hauts parleurs intégrés
- Matériel de gamme professionnelle, garanti par le fabricant pour un fonctionnement 7j/7 et 24h/24
- Marque SAMSUNG ou équivalent

Tous les supports muraux nécessaires à l'intégration et à la fixation des moniteurs seront à prévoir. Les moniteurs devront être orientables verticalement et horizontalement grâce aux supports de fixation.

Le mur d'images permettra l'affichage d'un minimum de 32 flux vidéo.

2.3.1.4 POSTE D'EXPLOITATION BUREAU DAGE (POSTE PRINCIPAL)

Ce poste sera constitué de :

- Unité centrale de type mini tour ou intégrée dans l'écran
- 1 carte mère avec processeur, performances adaptées aux traitements à réaliser
- 1 carte graphique
- 1 disque dur SSD intégré de 500 Go minimum
- Mémoire vive de capacité adaptée aux traitements à réaliser
- 1 clavier Azerty,
- 1 souris optique,
- 1 carte Ethernet 10/100/1000 Mbit/s avec agent SNMP v3
- 1 écran couleur 23 pouces LCD format 16/9ème
- 1 système d'exploitation Windows ou équivalent
- Logiciel anti-virus avec mise à jour automatique des définitions de virus via le cloud inclus pendant 2 ans
- Alimentations 230 V

Ce poste sera équipé :

- Du module logiciel permettant la gestion des visiteurs
- Du module logiciel permettant la visualisation des images des caméras

2.3.2 LOGICIELS

Le système intégré de sûreté permettra le paramétrage et la supervision du contrôle d'accès, de la détection intrusion, de la levée de doute vidéo ou de la relecture sur alarmes.

Il devra être évolutif, et pouvoir offrir des modules fonctionnelles (ex gestion des visiteurs) et des passerelles avec différents systèmes tiers via des protocoles ouverts (ex MODBUS IP, OPC UA, API Web Services, LDAP) supplémentaires.

En tant que superviseur, le logiciel devra permettre également de réaliser des passerelles suivantes :

- Synchronisation automatique & périodique des usagers avec le logiciel RH (ou autre) avec règles d'attribution d'accès automatiques possibles pour simplifier, aider le client final via des fichiers CSV ou par web services
- Gestion des opérateurs et de leurs profils opérateurs à travers l'annuaire active directory du client final via LDAP. Il sera possible d'attribuer plusieurs profils par opérateur par ce mécanisme. Le système devra avoir une finesse des profils opérateur suffisante pour pouvoir gérer les profils suivants :
 - Droit d'enrôler/attribuer des badges aux usagers uniquement sans pouvoir modifier les autres informations usagers
 - Droit d'attribuer des accès aux usagers uniquement sans pouvoir modifier les autres informations usagers
 - Droit de visualiser les codes claviers personnalisés des accès renforcés sans pouvoir modifier les autres informations usagers
 - Droit de créer / modifier / supprimer des badges aux usagers uniquement sans pouvoir modifier les informations usagers
 - Droit de visualisation de la photo des usagers ainsi que modifier celle-ci uniquement sans pouvoir modifier les autres informations usagers

2.3.3 MONITORING ET SUPERVISION

Le logiciel devra permettre la surveillance des événements, alarmes, défauts du contrôle d'accès, intrusion, flux vidéo, de la gestion techniques et de lancer des actions associées (acquiescement, commandes diverses, visionner les flux vidéo, ...) grâce à ces fonctions :

- Moniteur d'événements et d'alarme
- Surveillances des zones
- Animateur de synoptique (optionnel)

2.3.3.1 ERGONOMIE GENERALE

- L'ergonomie de l'interface doit être étudiée pour offrir une exploitation facile, rapide avec :
 - Une seule IHM unifiée pour gérer toute la sûreté
 - L'opérateur ne voit pas les fonctions, ni les données qui lui sont interdites
 - Gestion multi-langues des IHM
 - Chaque IHM dédiée à certaines fonctions (identifiés, POI, moniteur, synoptique, ...)
 - Fonctions utilisées par une grande population accessibles en WEB (RDV, ...)
 - Navigation et couleur séparée des applications : Exploitation – Paramétrage – Maintenance
 - Un champ de recherche du Menu permet de retrouver facilement les fonctions disponibles
 - Affichage de l'opérateur connecté sur la barre du haut
- Notion de favori, raccourcis et liste des dernières applications récentes ouvertes dans le menu principal pour un accès rapide aux fonctions courantes
- Gestion de l'autocomplétions permettant à l'utilisateur de limiter la quantité d'informations qu'il saisit avec son clavier, en se voyant proposer un complément qui pourrait convenir à la chaîne de caractères qu'il a commencé à taper
- Contrôle de cohérence des données en cours d'écriture selon le champ de saisies
- Notification aux opérateurs des erreurs, oublis selon saisie faite
- Possibilité de personnaliser la majorité des colonnes des formulaires de résultats :
 - Sélection des champs & données souhaités à l'affichage
 - Sauvegarde de leur position
 - Modification possible par l'exploitant à tout moment

2.3.3.2 MONITEUR INTERACTIF DES EVENEMENTS D'ALARME

Le Moniteur interactif d'événements centralise la surveillance de tous les événements, alarmes, défauts reçus par le logiciel, les affiche en temps réel au fil de l'eau, et permet d'acquiescer les alarmes, lancer des actions & télécommandes, forcer l'état des propriétés, ...

Chaque opérateur ne voit que les catégories d'événements autorisés. Dans tous les cas, toutes les apparitions, les acquiescements et les effacements d'alarme sont horodatés et archivés en base de données pour consultation ultérieure (voir chapitres Historique & opérateur).

2.3.3.3 FIL DE L'EAU

L'onglet « Fil de l'eau » remonte en temps réel tous les événements de manière chronologique selon un filtrage dynamique.

Il est possible de désactiver le défilement automatique des événements pour laisser le temps à l'utilisateur de visualiser les événements intervenus avant et après celui étudié.

Que la liste d'événements soit importante ou pas, il est toujours possible de les filtrer en dynamique selon :

- Le site (en gestion multisites)
- Le type d'évènements (passage autorisé ou interdit, alarmes, télécommandes, système, le dernier passage d'un identifié)
- Un mot clé dans la recherche rapide (nom,...)

2.3.3.4 DETAILS

Lors de la sélection d'un évènement affiché dans le fil de l'eau, la zone « Détails » permet de consulter des informations supplémentaires sur l'évènement et de voir les actions disponibles associées :

- Acquitter l'alarme : L'acquiescement d'une alarme, permet de s'assurer que l'opérateur l'a prise en compte. La nécessité ou pas d'avoir à l'acquiescer est paramétrable pour chaque évènement typé en alarme.
 - Acquiescement unitaire / multiples sur alarmes par 1 ou X d'opérateurs autorisés selon les catégories des alarmes (CA, AI, ...) et leurs niveaux d'acquiescement (masque). Une alarme peut nécessiter d'être acquiescée par plusieurs intervenants.
 - Choix d'un clignotement ou pas sur les alarmes à acquiescer
- Lire une consigne,
- Visualiser la caméra en live
- Visualiser l'enregistrement d'une séquence vidéo de l'alarme ou du passage de badge
- Afficher le synoptique associé à une alarme
- Sur passage de badge, accéder rapidement aux informations de l'identifié en ouvrant sa fiche et débloquent la sortie temporairement en cas d'alarme antipassback/anti-retour
- Sur changement d'une valeur, connaître l'état, forcer l'état, lancer une télécommande ...
- Affichage de la photo associée au dernier passage
- Ouvrir l'interface de prise de notes (libres ou liées à un évènement variable)

On peut distinguer les alarmes en fonction d'un niveau de gravité de 0 (le moins important) à 512 (le plus élevé).

Les codes couleurs des alarmes sont :

- Couleur de fond rouge et texte blanc : alarme en cours non acquiescée (Couleur par défaut, et personnalisable). On peut distinguer ces alarmes à acquiescer en fonction de leur niveau de gravité de 0 qui est personnalisable par :
 - Des couleurs de texte et fond de texte au choix et/ou
 - Des audios, sons au choix (synthèse vocale de Windows, fichier audio)
- Couleur de fond blanc et texte en noir : Une alarme non acquiesable en cours
- Couleur de fond blanc et texte rouge : Alarme acquiescée mais toujours en cours

2.3.3.5 ONGLET ALARMES

Donne une vue exhaustive des alarmes en cours ou qui n'ont pas encore été acquiescées. Les alarmes acquiescées et qui ne sont plus en cours disparaissent.

Les alarmes sont d'abord triées par ordre de gravité. La majeure partie des actions disponibles dans le fil de l'eau à propos des alarmes sont aussi disponibles dans cette vue avec en plus :

- Afficher la fenêtre courbe d'historique d'une alarme
- Accéder rapidement au paramétrage d'une propriété associée à l'alarme

2.3.3.6 ONGLET PROPRIETES

Permet de surveiller, rechercher les différents types de propriétés, de surveiller leurs états (notification lorsqu'une porte ouverte est détectée, par exemple), de les éditer et interagir avec.

Un objet représente un élément installé sur site qui génère des informations (ex : une porte).

Les propriétés de supervision sont les différents états, télécommandes qui s'appliquent au sein d'un même objet (ex pour un objet porte : BP, Ventouse, Contact porte, effraction, commande ouverture) et qui permettent de les piloter dans la supervision.

Cette vue est utile à l'exploitant mais aussi à l'intégrateur lorsqu'il paramètre un site car elle permet de diagnostiquer son installation (ex: passer une télécommande, regarder un état, passer une autre télécommande, ouvrir un synoptique...).

Les actions possibles sur ces propriétés selon leurs types sont :

- Forcer : permet d'inhiber les propriétés, par exemple temporairement dans les cas d'une maintenance, d'un détecteur défaillant ...,
- Envoyer une commande ou une impulsion,
- Visualiser la courbe associée,
- Voir le synoptique associé,
- Editer la propriété

Les propriétés peuvent être affichées avec différents couleurs : Fond jaune texte marron si l'état d'une propriété a été forcé.

2.3.4 ANIMATION DE SYNOPTIQUES GRAPHIQUES (PRESTATION SUPPLEMENTAIRE EVENTUELLE)

Le système permettra la supervision des équipements sur des synoptiques représentant des vues et des niveaux des bâtiments ou des tableaux dynamiques. Pour cela, le système proposera un éditeur de synoptiques intégré permettant de personnaliser des plans (par bâtiment et par niveau). Chaque vue représentera un plan dynamique permettant une exploitation conviviale avec icônes, animations, clignotement si non acquitté, télécommandes, changement de couleurs selon état (alarme en rouge, repos en vert), notion d'arborescence de vues, Widgets alarme/usager/lecteur, etc,...

Sur apparition d'une alarme, en 1 clic, l'opérateur pourra afficher le synoptique correspondant à cette alarme avec une consigne et pourra ajouter des commentaires/tickets dans une main courante qui les enregistre pour un suivi facile de l'apparition et la fin de l'alarme. Cette main courante sera disponible pour toutes les alarmes acquittables.

Un éditeur et animateur de synoptiques intégrés nativement, rapidement configurables et hautement personnalisables devra être prévu afin d'assurer les fonctionnalités suivants :

- La notion d'objets avec leurs propriétés (informations, états, commandes)
- Une bibliothèque de modèles d'objets prédéfinis, livrée avec le logiciel (UTL, porte, MAXIRIS, ...) qui intègrent la configuration métier et celle de supervision :
 - Paramétrage facile, rapide en glissant-déposant un objet à partir d'un modèle
 - Attribue automatiquement les automatismes, les entrées, sorties à câbler selon un schéma type avec des choix possibles à sélectionner par simple clic
 - Possibilité de changer l'image de l'objet en gardant toute la configuration
 - Ex avec l'objet « portes standards » : choix d'activer en entrée : contact position porte, commande, contact BBG, ou contact porte verrouillée
- La possibilité de créer, importer, copier des objets/propriétés personnalisés sur projet
- Le support du .SVG qui facilite l'import et l'export de plans de construction,
- La simulation possible depuis l'éditeur pour avoir un aperçu,
- Animer les objets selon les états des équipements (couleur, clignotement, message audio...)

- Réaliser des télécommandes, actions diverses depuis des objets, boutons par les opérateurs
- Utiliser la fenêtre des synoptiques pour naviguer d'un synoptique à l'autre conçus en arborescence (ex : une vue globale du site puis clic pour zoomer sur chaque bâtiment, puis une vue par étage du bâtiment, etc.)
- Disposer des fonctions de zoom avant et arrière sur un synoptique
- Ajuster rapidement le synoptique à l'écran ou de passer en mode plein écran par 2 raccourcis
- Gérer et superviser les alarmes directement depuis les synoptiques grâce à :
 - La possibilité d'acquitter les alarmes
 - L'ouverture des propriétés d'un objet
 - La visualisation des courbes correspondantes
 - Une fenêtre spécifique détachable des alarmes avec widget / compteur et liste des alarmes (comme depuis le moniteur d'évènements) avec les différentes couleurs d'affichage selon leur état et leur acquittement
 - Exemple ci-dessous de Widgets, objets (Porte, Interphone, caméra, ...) avec photo et information temps réel de la personne qui badge...

2.3.5 SUPERVISION VIDEO

La fonction logicielle devra permettre de :

- Dialoguer, dans les 2 sens, avec de nombreux VMS logiciels et enregistreurs vidéo via des connecteurs intégrés dans le logiciel
- Piloter toutes les fonctions de sécurité depuis un superviseur unique, commun à tous les systèmes du bâtiment (contrôle d'accès, intrusion, incendie, gestion technique).
- Effectuer la majorité des opérations courantes de la vidéosurveillance depuis n'importe quel poste client avec un ou plusieurs VMS à la fois :
 - Visualisation du direct
 - Déclenchement de l'enregistrement
 - Réception, émission des événements & alarmes
 - Consultation des images enregistrées
 - Pilotage des dômes

Avec l'intégration native vidéo dans le logiciel, l'exploitation devient beaucoup plus simple pour l'utilisateur. Les interactions entre la vidéo et les autres systèmes pouvant être complètement automatisées (actions sur alarmes ou sur événements), la rapidité et l'efficacité des traitements sont garanties. Afin d'assurer le meilleur fonctionnement, le poste client utilisant doit posséder deux écrans d'affichage.

Exemple de flux de données entre le VMS et le logiciel :

- La caméra de vidéosurveillance détecte des images à enregistrer
- L'enregistreur numérique enregistre les images détectées
- Le poste principal consulte directement les images en temps réel ou les images enregistrées en provenance de l'enregistreur, sans passer par le serveur, en fonction du paramétrage dans le serveur auquel le poste principal accède .
- Les images vidéo ne sont pas stockées sur le serveur mais uniquement sur les enregistreurs des VMS.

2.3.5.1 FONCTIONNALITES NATIVES

- Réception et émission d'évènements, alarmes avec plusieurs VMS

- Logiciel -> VMS : déclenchement/ arrêt enregistrement, pilotage dôme avec choix préposition et zoom, ...
- VMS -> logiciel : alarme détection, défaut caméra, défaut enregistrement, enregistreur connecté, caméra connectée...
- Réduction du temps de paramétrage (important liée à la fonction Vidéo) avec :
 - Les connecteurs intégrés et/ou optionnels dans utilisent les SDK des VMS et des objets/propriétés natifs pour un paramétrage rapide et facile
 - La notion d'objet « Caméra » dans l'éditeur des synoptiques
 - L'import des libellés caméras des VMS
- Supervision des alarmes opérationnelles (détection d'activité par vidéo) et des alarmes de fonctionnement (perte de signaux vidéo ou autres pannes) en provenance des enregistreurs avec le moniteur d'événements, le bandeau d'alarme, temps réel comme toutes les autres
- Une fenêtre d'architecture matérielles dédiée peut être peut éventuellement s'afficher sur demande
- Pilotage des caméras dômes (zoom, choix d'une préposition prédéfinie) par une fenêtre dédiée
- Zone de visualisation des caméras entièrement personnalisables elon des scénarios prédéfinis qui positionnent un ou plusieurs moniteurs dans différentes positions et différentes tailles (3 x 3, 2x 2,...). Il est possible d'ajouter autant de moniteurs que de sources. Les couleurs de la barre de titre du moniteur renseignent sur son contenu et son état.
- Visualisation de flux vidéo en direct (Live) simultanés de plusieurs VMS en parallèle sur sélection d'icônes sur synoptiques d'exploitation, sur alarmes
- Déclenchement d'enregistrements automatique qui peut être réalisé par un événement (badgeage sur un lecteur donné), une alarme, un asservissement complexe, une commande manuelle opérateur depuis le synoptique en cliquant sur un bouton ou objet graphique, une commande depuis le Moniteur d'événements
- Gestion de mur d'images (fonction matrice) qui permet de gérer un mur d'images constitué de plusieurs écrans et d'afficher une caméra dans une zone (appelée tuile).

2.3.5.2 VMS INTERFACES VIA DES CONNECTEURS

La liste des solutions, des versions compatibles et des fonctionnalités accessibles devra être en constante évolution avec des connecteurs intégrés avec leurs objets/propriétés, et des passerelles interfacées optionnelles.

2.3.6 GESTION DES UTILISATEURS

Un opérateur est une personne physique, autorisée à utiliser l'interface de supervision. Cet utilisateur, selon sa fonction, son niveau hiérarchique ou sa situation géographique, peut accéder à la totalité ou à une partie des différentes fonctions, données disponibles dans le logiciel de supervision.

Pour affecter à chaque opérateur uniquement les droits qui lui sont nécessaires, et le faire rapidement par type d'opérateurs, le logiciel doit intégrer une notion de "profils opérateurs". Ces profils sont définis par un système de cases à cocher représentant les droits accessibles avec finesse dans chacune des grandes fonctions suivantes et en visualisation, création, modification, suppression :

- Droits liés au contrôle d'accès.
- Droits liés à l'exploitation.
- Droits liés à l'historique
- Droits liés aux identifiés (dont quelles données personnelles).
- Droits liés aux visites.

- Droits liés à la supervision (dont catégories des propriétés par ex : accès, intrusion, incendie, ..., masque / niveau d'acquiescement des alarmes).
- Droits liés au paramétrage (dont filtrage pour les projets multi-sites selon sites lecteurs, sites des objets synoptiques, entités identifiées, classification de chaque accès dont la finesse est supérieure à la notion de site).
- Droits liés à la sécurité.

Pour chaque opérateur créé, il suffit ensuite de lui attribuer un ou plusieurs profils opérateurs pré définis.

La gestion des droits est sécurisée, facilitée, prévue pour une grande population, et simplifie l'exploitation la maintenance et la mise en œuvre car :

- Une modification des profils opérateurs modifie automatiquement tous les opérateurs qui y sont associés.
- On peut associer un ou plusieurs profils à l'opérateur pour permettre à ce dernier de se mettre dans les mêmes conditions d'un autre opérateur qu'il souhaiterait aider par exemple.
- Un opérateur est d'abord un "Identifiés" qui a des droits d'accès physique et que l'on a déclaré en plus comme opérateur du logiciel. Cela évite une double saisie des données personnelles et des fiches.
- Hiérarchie entre opérateurs : Afin de modifier les droits des opérateurs, le niveau hiérarchique de l'opérateur réalisant la modification doit être supérieur aux opérateurs modifiés (niveau hiérarchique et profil).
- Les mots de passe opérateur sont protégés en BDD par un HASH SHA-512 + SEL de 512 caractères aléatoires.
- Traçabilité et historique des actions opérateurs (avec valeurs/champs modifiés) qui est une exigence réglementaire dans de nombreux secteurs d'activité (Agro-alimentaire, pharmaceutique, transport, nucléaire...).
- Gestion centralisée des droits opérateurs dans le logiciel pour tous les types de postes clients (.
- Un login et mot de passe par défaut est donné à chaque opérateur. Ces données devront être modifiées par l'opérateur lors de sa première connexion, ainsi elles ne seront connues que de lui.
- Déconnexion automatique des opérateurs après un temps d'inutilisation trop long ou au redémarrage du serveur.

2.3.7 GESTION DES ANNUAIRES LDAP/ACTIVE DIRECTORY

La gestion des opérateurs est possible sur le système ou depuis un annuaire centralisé Active Directory (A.D) du client final géré par son service informatique ou RH et interfacé par une passerelle au protocole LDAP. Cela permet :

- D'avoir un seul annuaire référent pour tous les utilisateurs des applications d'une société qui simplifie la création, modification, suppression des opérateurs. La mise à jour est facilitée et automatique.
- D'attribuer dans cet A.D le ou les profils opérateur prédéfinis qui portent le métier. Prise en compte du multi-profil opérateur avec l'authentification LDAP.
- De gérer des mots de passe complexes et time out (déconnexion auto) par la puissance de l'A.D.
- De gérer les opérateurs en mode sécurisé avec LDAPs.

2.3.8 GESTION MULTI-SITES / MULTI CLIENTS

Le logiciel devra permettre de gérer jusqu'à 256 sites différents à partir du même système. Cette fonction est intéressante dans plusieurs cas

- La gestion de bâtiments disséminés géographiquement :bâtiments d'une collectivité locale, sites de depuis un seul serveur central.

- La nécessité, au sein d'un même site, d'une maîtrise de droits différents au niveau de chaque service.
- Le partage d'un même bâtiment par plusieurs locataires et différencier les accès communs et ses accès propres.
- Le choix au niveau des serveurs : 1 serveur national pour tous les sites ou 1 serveur par site selon les contraintes (qualité du réseau) et organisation prévues (centralisée, décentralisée...).
- Le choix au niveau de l'administration des badges avec :
 - Personnalisation & encodage centralisé au siège.
 - Encodage générique centralisé au siège et personnalisation sur chaque site.
 - Personnalisation & encodage sur chaque site.

L'utilisation de la fonction multisite exige un gestionnaire / administrateur principal afin :

D'administrer la base de données unique centralisée.

- Définir les sites, le site le plus petit étant un UTL :
 - Il faut bien prendre en compte que l'UTL est mono-site dans l'architecture, le choix et localisation des UTL et l'impact câblage associé.
- Définir les entités d'affectation des personnes.
- Définir les droits opérateurs et les opérateurs par site selon l'organisation & procédures.
- De créer des gestionnaires par site, services, société, ... qui peuvent recevoir sa délégation, grâce à la notion de hiérarchie d'opérateur, pour gérer finement chaque site dont :
 - Les droits d'accès de leur personnel / entité sur les lecteurs de leur site et, s'il y en a, sur les lecteurs communs (accueil, parkings, ascenseurs...).
 - La consultation des historiques et mouvements de leur personnel.

Ils ne verront ni les lecteurs & droits d'accès des autres sites, ni les personnes et leur historique des autres entités

Chaque site possède 256 plages horaires indépendantes, utilisées soit dans le cadre du contrôle d'accès, soit de l'intrusion, soit dans le cadre de la gestion technique des bâtiments (système d'alarme, arrosage automatique...). Le système central peut créer jusqu'à 256 sites et 256 x 256 plages horaires au total pour tous les sites.

Pour la sécurité des clés des badges, l'utilitaire KSM, les outils d'encodage et les UTL permettent à l'officier central de sécurité de gérer, si besoin, des clés badges différentes par site avec la notion de périmètre, comme demandé dans le guide ANSSI.

2.3.9 PROGRAMMATION, ESSAIS ET MISE EN SERVICE

2.3.9.1 PARAMETRAGE

Le paramétrage et la mise en service de l'ensemble de l'installation devra être assuré en étroite collaboration avec le support technique du(es) fabricants.

L'entreprise doit le paramétrage, la programmation, la mise en service et les essais de l'ensemble de l'installation. Pour cela elle devra établir et fournir un plan de contrôle.

Le titulaire doit :

- La configuration de chaque centrale pour connexion au réseau TC/IP
- La configuration des tables d'échanges avec la supervision,
- L'installation et le paramétrage des postes informatiques et des serveurs,
- L'installation et paramétrage de la base de données,
- Le paramétrage des plages horaires,

- Le transfert de la programmation vers les équipements
- L'intégration et l'animation des symboles graphiques des équipements, des alarmes, des fonctions (inhibition, etc.), etc.
- Toutes sujétions utiles et nécessaires.

2.3.9.2 ESSAIS ET MISE EN SERVICE

La réception définitive des ouvrages aura lieu lorsque l'ensemble des travaux sera terminé.

Les essais fonctionnels à réaliser pour le système porteront sur :

- Les essais fonctionnels de l'installation lors des phases d'autocontrôle,
- Les essais de chaque point (intrusion, contrôle d'accès, vidéo)
- Les essais de réception avec la maîtrise d'œuvre et le maître d'ouvrage/exploitant.

2.3.10 FORMATION DES UTILISATEURS

Le présent lot devra dans sa proposition, comprendre la formation à l'utilisation de l'ensemble du système du personnel chargé de la surveillance de l'établissement (supervision, contrôle d'accès, alarme intrusion et vidéo-surveillance)

Cette formation devra être programmée par session de 5 à 6 personnes maximum et comprendra au minimum les aspects suivants :

- La connaissance du site,
- La manipulation des éléments constitutifs du système et les automatismes associés.

Le titulaire du marché devra obligatoirement avoir avec une certification de formation du constructeur de la solution retenue attestant de sa bonne maîtrise.

Le titulaire du marché devra pouvoir proposer sur site et sur le système déployé les formations suivantes au client final.

TRANCHE FERME		
FORMATION	DUREE	NOMBRE DE CESSIONS / PERSONNES
Administrateur/ gestionnaire système	2 jours	1 / 5
Exploitant, Utilisateur système	1 jour	1 / 5 à 6
6 mois après la mise en service (révision, questions/réponses)	1 jour	1 / 5

TRANCHE OPTIONNELLE 1		
FORMATION	DUREE	NOMBRE DE CESSIONS / PERSONNES
Administrateur/ gestionnaire système	1 jours	1 / 5
Exploitant, Utilisateur système	0.5 jour	1 / 5 à 6
TRANCHE OPTIONNELLE 2		
FORMATION	DUREE	NOMBRE DE CESSIONS / PERSONNES
Administrateur/ gestionnaire système	1 jours	1 / 5
Exploitant, Utilisateur système	0.5 jour	1 / 5 à 6

2.4 CONTRÔLE D'ACCES

2.4.1 RAPPEL DU CADRE REGLEMENTAIRE ET ASSUREUR

- Guide « Sécurité des technologies sans-contact pour le contrôle des accès physiques » de l'ANSSI,
- CNIL (Commission nationale de l'informatique et des libertés)
- La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,
- La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense
- Le règlement général sur la protection des données de mai 2018,

2.4.2 GENERALITES

Un système de contrôle d'accès centralisé par lecteurs de badges sera prévu afin de permettre l'accès à certaines zones ou locaux aux seules personnes autorisées.

Le système aura pour objectif :

- L'identification des badges
- Le traitement des données compris traçabilité des événements
- Le déverrouillage des accès contrôlés par lecteurs de badges

Le système permettra la visualisation en temps réel des passages de badges, la désactivation de badges (badges perdus, date de validité dépassée...) ainsi que le filtrage des accès suivant les autorisations qui seront définies pour chaque personne.

Le système qui sera mis en œuvre devra être totalement compatible avec le système de vidéosurveillance mis en œuvre (caméras, logiciels, serveurs et stockeurs vidéo).

Le système sera de marque TILL, NEDAP, SYNCHRONIC ou strictement équivalent. Le système sera obligatoirement d'une marque connue, largement répandue sur le marché, et présentant des références similaires en termes de nombre de lecteurs et de type de bâtiment.

Le niveau de surveillance par contrôle des accès physiques de l'établissement sera relatif à la surveillance d'un ou plusieurs accès du bâtiment par une installation de contrôle d'accès suivant la règle D83 APSAD

Les badges pourront être programmés individuellement pour permettre de restreindre ou d'autoriser l'accès à certains secteurs du bâtiment, mais aussi d'activer et désactiver l'alarme intrusion.

Le contrôle d'accès sera centralisé et commandera les portes extérieures/intérieures par l'intermédiaire de bandeau ventouse sur les menuiseries ou par contact sec pour les portes motorisées.

L'équipement de contrôle d'accès se composera principalement:

- Des postes d'exploitation :
 - un poste d'exploitation principal au PC Sûreté (supervision totale et paramétrage du système)
 - un poste d'exploitation pour la création des badges
- un poste d'exploitation secondaire dans le bureau de la DAGE
- Unités centrales (Automate, UTL maître, ou autres)
- Des unités de traitement locales (UTL) sur lesquelles seront raccordés les environnements de portes (lecteurs de badges, systèmes de verrouillage, détecteurs d'ouverture, boutons poussoirs et boîtiers de demande d'ouverture)
- De lecteurs de badges (proximité, Qrcode, et suivant le cas avec clavier à code)

- Encodeur de badge
- De badges
- De systèmes de verrouillage avec de détecteurs d'ouverture (à charge de chaque lot fournissant les portes)
- Des boutons poussoirs de sortie et de boîtiers de demande d'ouverture (BBG vert)
- Licences nécessaires
- Réseau de câblage,
- Programmation et mise en service

L'architecture du système sera de type IP et sera construite sur 3 niveaux fonctionnels :

- Niveau 1 : la supervision,
- Niveau 2 : les Unités de Traitement Locales (UTL),
- Niveau 3 : les capteurs, les détecteurs et les lecteurs de badges.

2.4.3 DIFFERENTS NIVEAUX DE SECURITE

Le réseau Ethernet et obstacles physiques resteront à la charge et sous la responsabilité du maître d'ouvrage qui décidera s'il s'agit d'un réseau sûreté dédié, d'un VLAN, ou d'un réseau mutualisé. Ils ne sont pas inclus dans ce dossier.

- **Niveau 0** : Périphériques, capteurs, actionneurs : les détecteurs intrusion, serrures, obstacles physiques, sirènes, lecteurs de badges, autres, seront raccordés sur des modules
- **Niveau 1** : Automates de terrain : Les UTL / centrales d'alarmes seront raccordées directement sur un réseau Ethernet et auront des bus de terrain pour les modules déportés
- **Niveau 2** : Système de supervision Serveur (GAC) et les postes clients seront raccordés directement sur le même réseau Ethernet et communiqueront avec les UTL/centrales

La solution sera apte à assurer de base, à minima, les tâches suivantes :

- Contrôle des accès, levée de doute vidéo et détection-intrusion sur un seul logiciel
- Gestion des autorisations d'accès et calendriers horaires,
- Gestion de badges permanents et temporaires,
- Gestion de QR code pour des accès ponctuels ou limités dans le temps (pour des accès limités)
- Gestion des utilisateurs accompagnés et accompagnants,
- Enregistrement de tous les événements
- Dispose d'une application mobile permettant l'exploitation des fonctions majeures du logiciel
- Envoie email avec leurs QR code, identifiant virtuel pour permettre aux permanents d'accéder aux parkings sur site avant accueil

En complément elle pourra à l'avenir assurer sans que cela soit prévu de base:

- Gestion des accès au niveau des ascenseurs,
- Edition et traitement des différents compteurs,
- Gestion des entrées/sorties des zones de stationnement de véhicules,
- Détection et gestion des alarmes techniques et d'intrusion,
- Représentation graphique dynamique selon typologie des bâtiments,
- Gestion et pilotage des équipements de vidéosurveillance tiers,
- Edition d'automatismes permettant des procédures sur mesure pour l'utilisateur.

- Enregistrement de tous les événements
- La solution assurera le contrôle permanent du fonctionnement du système, y compris de chaque élément « adressable » intelligent
- À travers la programmation de réactions automatiques, toutes entrées ou sorties d'un porteur de badge, toutes détections d'anomalie et/ou d'alarme peut engendrer diverses actions pour obtenir une stratégie globale de sécurité. Contrôle vidéo des accès : à la suite d'un badgeage demandant un accès sur une porte sensible, un opérateur devra donner son accord en un clic sur un IHM dédié du système.

2.4.4 SPECIFICATION MATERIELLE DU SYSTEME

L'architecture mis en place devra pouvoir respecter l'architecture de niveau 1 de l'ANSSI (tête de lecture dite "transparente"). Le matériel proposé par le présent lot devra pouvoir obligatoirement bénéficier d'une certification reconnu et qualifié ANSSI à termes.

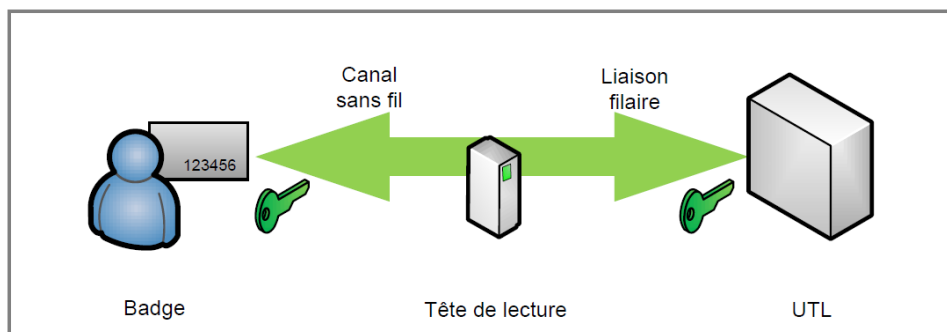


Figure 7 : Architecture n°1 : tête de lecture transparente, authentification de bout en bout

Dans un premier temps la certification ANSSI n'est pas demandée, mais il devra être possible d'y répondre sans remettre en cause l'installation (matériel ou câblage). La mise à niveau devra se faire par une « upgradation » de licence complémentaire ou par clé physique type « dongle » complémentaire.

NOTA : Toute proposition qui ne sera pas établie avec un matériel répondant à cette demande sera déclarée non conforme.

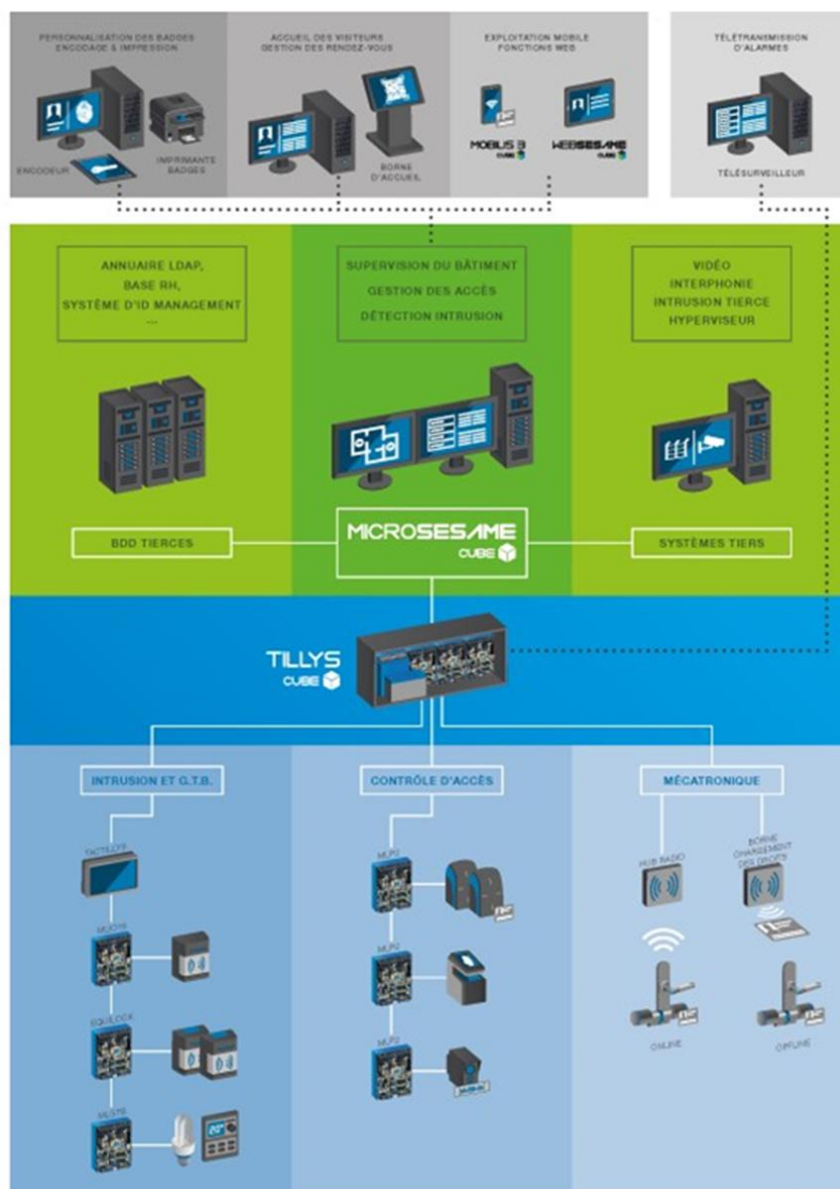
2.4.5 ARCHITECTURE ENVISAGE

Le système sera composé d'une unité centrale raccordé sur le réseau informatique du client.

Pour une architecture homogène, les unités de traitement local seront directement raccordées sur l'unité centrale. Ces unités de traitement assureront une décision locale des accès et entrées/sorties raccordés.

La solution proposée sera dotée d'une grande souplesse de raccordement (mise en œuvre de liaisons adaptées) et d'outils garantissant le niveau de performances requis.

Le système sera basé sur une architecture **TiL technologie** ou strictement équivalent.





2.4.6 CAPACITE DU SYSTEME A RESPECTER

Le système devra être évolutif par ajout de licences, options, modules hardware mais avoir les capacités finales minimales suivantes pour permettre des extensions ultérieures sans remettre en cause toute l'installation existante :

- 1000 UTL / centrales sur IP
- 10 000 lecteurs de badges
- 40 000 entrées / sorties
- 256 postes clients
- 10 000 opérateurs
- 100 000 usagers et 200 000 identifiants (badges, plaque,...)
- 1024 profils d'accès (somme de groupes de lecteurs + lecteurs + niveaux ascenseur)

2.4.7 ATTRIBUTION DES DROITS D'ACCES AUX USAGERS

A chaque usager, il sera possible d'associer plus de 100 droits d'accès pérennes et/ou provisoires dont :

- Plusieurs profil(s) d'accès +
- Plusieurs groupes de lecteurs +
- Plusieurs lecteurs

Pour chaque choix, on pourra associer une date de début – fin possible pour des missions temporaires

Pour chaque choix de groupes de lecteur, lecteurs, on pourra associer une plage horaire parmi 250 possibles qui sont des semainiers intégrant jusqu'à 32 jours fériés & spéciaux (inventaire, ...)

Quand une fiche usager intégrant des droits d'accès et un numéro de badge est validée par un opérateur, la liste dite blanche de ces droits d'accès et son numéro de badge devra être téléchargée automatiquement en moins de 30 sec vers les seuls UTL où la personne a le droits d'accéder en une seule opération.

2.4.8 HISTORIQUES

Le logiciel offrira une IHM dédiée & intégrée conviviale de recherche d'événements, alarmes.

Les critères de recherche devront être :

- Des périodes de recherches (dates et jours),
- Evénements badges : autorisés, interdits, liste noire, anti-retour avec le choix du badge, du profil, du lecteur, du groupe de lecteurs,
- Evénements type alarmes
- Evénements des opérateurs : connexion/déconnexion, acquittement, télécommandes, forçages de voies, connexions/déconnexions avec le choix de l'opérateur. En effet le système devra offrir la traçabilité des actions opérateurs

Les historiques peuvent être exportés pour une exploitation ultérieure. Les requêtes extraites des historiques peuvent également être imprimées. Afin d'optimiser le stockage des historiques du système de contrôle d'accès/intrusion, celui-ci permettra la purge intelligente des historiques périodiquement.

2.4.9 RICHESSE FONCTIONNELLE DE LA SOLUTION

Au-delà des fonctions déjà décrites, le système installé devra disposer des fonctionnalités suivantes, de façon native ou par ajout de licences optionnelles sans impact technique sur la solution déployée, pour un besoin qui pourrait apparaître ultérieurement :

- Gestion des temps de repos (11h),
- Localisation, comptage, liste de présents en zones, assistance au plan d'évacuation POI,
- Lecteur Mobile type Smartphone durci avec lecteur intégré de badge et/ou QR code pour contrôle inopiné sur site et contrôle d'accès sur l'entrée du site des usagers. Il fonctionnera soit en offline / autonome avec sa base de données intégrée soit en online avec une connexion sécurisée avec le système central. Pour éviter les éventuelles conséquences d'un vol et le respect du RGPD, il devra avoir sa propre sécurité intrinsèque avec au minimum :
 - Pas de clés badge,
 - Anonymisation des fiches usagers en n'affichant que la photo et la validité sur lecture d'un badge ou QR Code,
 - Suppression des données se trouvant dans le lecteur mobile après X heures paramétrables de déconnexion au serveur,
 - Chiffrement de la base de données locale.
- Notion d'habilitations (électrique, chimique) possible en option avec impact ou pas sur les droits d'accès selon accès
- Gestion de lecteurs de plaque avec X voitures possibles par personne, sans système supplémentaire
- Gestion de niveaux de crise / Mode crise / Vigipirate
- Envoie email avec leurs QR code, identifiant virtuel pour permettre aux permanents d'accéder aux parkings sur site avant accueil
- Contrôle vidéo des accès : à la suite d'un badgeage demandant un accès sur une porte sensible, un opérateur devra donner son accord en un clic sur un IHM dédié du système
- Surveillance de liste noire

- Gestion de quarantaine : le système devra être capable d'interdire l'accès à certaines zones après une durée configurable depuis le passage dans certaines zones
- Gestion des parcours de rondes
- Gestion des niveaux d'ascenseurs autorisés par usagers

2.4.9.1 GESTION DES ACCES

La fiche Identifié/Identifiants regroupe et définit :

- Les informations de l'identifié: dates de validité, société, service, coordonnées, ainsi que 16 libellés personnalisables supplémentaires. Des pièces jointes peuvent également être associées (contrat de travail, photo...).
- Les identifiants de l'identifié: jusqu'à 4 technologies différentes d'identifiants sont possibles (ex : badge 13,56 MHz, badge 125kHz, code clavier, plaque minéralogique, QRCode...), pour chaque Identifié on peut stocker jusqu'à 99 identifiants par technologie. Les identifiants peuvent avoir plusieurs statuts : cassé, perdu, volé, non rendu pour expliquer le motif d'interdiction. Ainsi, on ne crée qu'une seule personne même avec pour plusieurs identifiants.
- Des attributs spécifiques : anti-retour, liste noire (pour surveillance spécifique), niveau d'accréditation (mode crise), possibilité de recevoir des visites, d'être accompagnant, ...
- Période de validité: qui est associée à chaque identifié et permet d'invalider (ou revalider) rapidement et temporairement un identifiant, sans détruire la liste de ses autorisations
- La gestion des droits d'accès qui offre une souplesse de visualisation et rapidité d'attribution des droits : vue commune, filtre textuel, sélection de droits multiples dans une liste regroupant les profils, les lecteurs online/offlines, les groupes de lecteurs, les étages d'ascenseurs, les clés & groupes de clés des armoires connectées. Les droits d'accès sont attribués à la personne, pas aux identifiants (badges). Ainsi, même si on perd un badge et qu'on en réattribue un autre, cela ne change pas les droits d'accès.

2.4.9.2 GESTION DES ACCES INDIVIDUELS

L'attribution d'un droit d'accès permet d'autoriser le passage d'un identifié sur un lecteur, ou un groupe de lecteurs, en fonction d'un programme horaire défini (128 programmes horaires).

Les UTL devront être périodiquement mises à l'heure, pour s'assurer qu'il n'y a pas de dérive entre les UTL et le serveur et bien respecter les plages horaires.

2.4.9.3 GESTION DES ACCES PAR PROFILS

Le profil d'accès permet de prédéfinir les droits d'accès pour une catégorie d'identifiés, sur un ou plusieurs sites. Le profil est composé d'une liste de :

- Lecteurs online/offlines et/ou
- Groupes de lecteurs et/ou
- Clés des armoires connectées et/ou
- Groupes de clés et/ou
- Niveaux d'ascenseur

Chaque lecteur ou groupe pouvant être associé à une plage horaire différente. A chaque identifié, il est possible d'associer un ou plusieurs profils d'accès.

Il est possible de créer des exceptions pour une personne particulière en utilisant la gestion individuelle des accès par lecteurs et/ou groupes de lecteurs.

On pourra par exemple associer un profil « général » pour les accès communs, un profil « service » pour l'accès à certaines zones et des particularités propres à la personne, liée à sa fonction ou à son niveau hiérarchique.

Le logiciel doit intégrer une notion de profils d'accès « tous lecteurs » pour chaque site qui englobe tous les lecteurs existants et futurs du site. Ce profil est pratique quand on veut donner à un identifié tous les lecteurs d'un site sans avoir à modifier le profil à chaque ajout de nouveaux lecteurs pour un site donné.

La gestion des droits d'accès des Identifiés est d'une très grande souplesse. Elle permet une visualisation et une attribution rapides des droits d'accès : vue complète des accès, filtre textuel, sélection d'accès multiples dans une liste regroupant les profils, les lecteurs, les groupes de lecteurs et les étages d'ascenseurs.

Une fonctionnalité de la gestion des Identifiés affiche en permanence les « accès résultants » issus de l'attribution de tous les droits d'accès affectés à l'Identifié.

2.4.9.4 GESTION DES ZONES

Le logiciel doit intégrer une gestion de zones. Une zone est délimitée par deux groupes de lecteurs : un groupe permettant d'entrer dans la zone et un groupe permettant de sortir de la zone. Un groupe de lecteurs peut contenir un nombre quelconque de lecteurs d'une installation.

Il est possible de connaître exactement le nombre de personnes présentes dans chaque zone et d'en établir la liste, par ordre alphabétique, par ordre chronologique d'arrivée ou d'autres critères de tri comme la société etc.

Très utilisée par certains établissements, cette gestion des zones est indispensable à la mise en place de l'application spécifique de type Plan d'Opération Interne.

Il est possible d'envoyer par mail la liste des présents dans une zone en cas de déclenchement d'un POI.

La gestion des zones permet également la mise en place d'un contrôle précis des circulations.

La possibilité d'imbriquer une zone dans une autre et l'activation de lecteurs en fonction de la sortie d'une autre zone créant, de fait, un « passage obligé », appelé notion de dépendance.

2.4.9.5 GESTION DES HABILITATIONS

Les autorisations d'accès d'un identifié, sur certaines zones ou certains lecteurs, peuvent être conditionnées par la possession d'une habilitation, externe au contrôle d'accès, en cours de validité : habilitation électrique, zone sensible, etc...

Cette condition de validité peut être gérée par des personnes différentes, par exemple le service RH ou n'importe quel responsable fonctionnel concerné.

Cette fonctionnalité permet jusqu'à 256 habilitations.

Chaque identifié peut cumuler plusieurs habilitations, possédant chacune sa propre période de validité.

L'accès à un lecteur donné peut être soumis à la validité d'une ou plusieurs habilitations.

2.4.9.6 FONCTIONS DE SECURITE RENFORCE

- Anti-retour : Sur des accès avec lecteurs en entrée et sortie, la gestion des zones permet de mettre en place un mécanisme "anti-retour" afin d'empêcher un identifié d'entrer plusieurs fois de suite dans une zone, sans en être préalablement sorti.
- Gestion de SAS: La force de la programmation du système permet également de personnaliser l'asservissement de plusieurs portes entre elles selon les besoins projets. Cette programmation permet de combiner plusieurs technologies : tapis contact, tapis d'unicité, caméra vidéo, lecteur biométrique....
- Contrôle renforcé : possibilité de déclarer certains lecteurs avec double contrôle : passage d'un badge autorisé et saisie d'un code secret sur un clavier. Ce contrôle renforcé permet une authentification forte du porteur du badge pour les accès sensibles. Le code secret peut être identique pour tous les identifiants et personnalisé pour chaque identifié.

- Code contrainte: prend en compte un code clavier saisi sous contrainte. Une alarme silencieuse est alors générée immédiatement sur le poste opérateur et l'accès s'ouvre normalement sans alarme sonore.
- Surveillance de la « liste noire » : Cette fonction permet de déclencher une alarme dès qu'un badge inscrit en "liste noire" est présenté sur l'un des lecteurs du site. Par exemple pour intervenir sur le terrain en cas de tentative d'utilisation frauduleuse d'un badge perdu ou volé.
- Mode crise: permet de gérer des seuils de crise. Basés sur des critères propres à chaque site, 7 niveaux sont attribuables, aussi bien aux personnes (selon la hiérarchie, les habilitations...) qu'aux lecteurs (selon les zones, les types d'alarmes...).

Lorsqu'un mode crise est déclenché, chaque UTL du système reçoit l'ordre de changement de seuil et gère automatiquement les correspondances entre les niveaux d'accréditation des personnes et les niveaux de sécurité des lecteurs. Une personne d'un niveau inférieur à celui du lecteur ne pourra plus entrer et/ou accéder à un étage via l'ascenseur. En effet le mode crise agit sur tous les droits d'accès des lecteur online y compris lecteur cabine de gestion des étages.

Il est possible de générer plusieurs scénarios de crises par :

- Des asservissements automatiques selon des combinaisons d'entrées
- Des actions opérateurs autorisés par un simple clic sur des boutons sur synoptiques préalablement configurés par l'intégrateur : un scénario X va mettre les lecteurs définis dans un niveau de crise souhaité

2.4.9.7 QUARANTAINE (NON PREVU AU MARCHE)

Une gestion des durées de mise en quarantaine hautement configurable (à partir du firmware TILLYS NGv2.3) doit être possible.

Il est recommandé d'utiliser une UTL par zone de quarantaine.

Pour chaque accès sur un lecteur donné par une personne X (lecteur de mise en quarantaine), on peut définir des durées paramétrables vers des lecteurs dépendants de la quarantaine pour la personne X (2 Heures sur lecteur 1; 5 jours sur lecteur 2; etc...).

Une alarme sur le moniteur d'événements apparaît quand la personne X, après avoir passé sur le lecteur déclenchant la mise en quarantaine, tente d'entrer sur un accès dépendant, sans respecter les durées de mise en quarantaine.

Dans ce cas d'interdiction d'accès pour non-respect de la quarantaine par la personne X, le message indique qu'elle pourra rentrer sur les lecteurs dépendants concernés, à partir d'une durée exprimée en jours/heures.

L'autonomie des UTL est complète car elles communiquent directement entre elles.

Sur coupure réseau, chaque UTL mémorise les messages et l'heure de badgeage et les envoie automatiquement aux autres UTL au rétablissement du réseau.

2.4.9.8 GESTION D'ASCENSEUR (NON PREVU AU MARCHE)

La mise en place de lecteurs de badges dans les ascenseurs d'un bâtiment devra permettre de limiter l'accès à certains étages en fonction de droits individuels, de profils de personnel ou des sociétés d'appartenance, dans le cas d'un immeuble multisite.

Le logiciel devra être capable de gérer nativement cette fonctionnalité, directement dans les droits des identifiés. Les étages ou groupes d'étages sont vus comme des lecteurs de badges du bâtiment et peuvent donc être intégrés dans des groupes de lecteurs ou des profils d'accès.

La gestion multisite dans un immeuble à plusieurs locataires permet de filtrer quel étage est géré par quel opérateur en rappelant qu'un UTL est mono-site. On peut par exemple organiser les étages ainsi :

- Le promoteur, gestionnaire principal peut gérer les droits d'accès de tous les étages.

- Chaque locataire gère les droits d'accès uniquement à ces étages loués et aux étages communs (RDC/accueil, parkings, cantine...) et que pour son personnel grâce aux entités.

Une UTL dédiée à la gestion d'ascenseurs est requise pour bénéficier de cette fonctionnalité.

2.4.9.9 ACCES VEHICULES ET GESTION DES PARKINGS (NON PREVU AU MARCHE)

Le logiciel devra pouvoir superviser à distance (à télécommande ou à badges actifs) ou des lecteurs de plaques minéralogiques ou de QR Code.

Ces équipements facilitent la gestion des flux de véhicules, notamment aux heures de forte affluence, et apportent un plus grand confort pour les utilisateurs.

L'intégration devra être transparente : les télécommandes ou les badges à longue portée font remonter un numéro comme n'importe quel autre badge, les plaques d'immatriculation sont directement gérées dans la fiche Identifié/Identifiant (jusqu'à 99 plaques minéralogiques par identifié).

Plus que contrôler les accès, cette gestion intégrée des identifiants permet aussi, par exemple de connaître :

- Le nombre total de véhicules.
- Les taux d'occupation par type de personnel, service ou société si parking commun.
- Les volumes et durées d'occupation pour imputations ou refacturations...

2.4.9.10 GESTION WEB DES IDENTIFIES (NON PREVU AU MARCHE)

Pour une exploitation simplifiée du contrôle d'accès, en plus des interfaces serveur et client, des interfaces web « légères » devront être disponibles pour la gestion des identifiés et des visiteurs.

Depuis n'importe quel PC ou appareil mobile équipé d'un navigateur internet et d'une connexion, une interface WEB devra permettre :

- La recherche et l'affichage de fiches « Identifiés » selon plusieurs critères.
- La création ou modification de fiches, et notamment l'association d'une photo (prise rapide par smartphone ou tablette).
- L'attribution de profils d'accès et d'identifiants préexistants.
- L'import/export d'identifiés/identifiants.

Ces mêmes fonctions sont disponibles pour la gestion des fiches visiteurs (externes au site).

D'autres interfaces de contrôle d'accès sont également disponibles en mode web, comme la gestion des rendez-vous (visiteurs externes) ou la consultation de l'historique de contrôle d'accès.

L'ergonomie devra être optimisée pour une utilisation sur tablettes et smartphones (responsive):

- Ecrans auto-adaptatifs (résolution et orientation).
- Auto-complétion des champs et affichage photo.
- Boutons à cocher.

2.4.9.11 GESTION DES VISITEURS

Sur un site équipé en contrôle d'accès, les personnes extérieures doivent pouvoir être enregistrées, accompagnées, voire munies d'un identifiant, pour pouvoir circuler dans les zones qui lui sont autorisées. Cet objectif est demandé dans la politique de sécurité du client final ou imposé par la législation (guide ANSSI pour les OIV, OSE...).

La gestion des visiteurs doit permettre la planification, la gestion des flux des visiteurs l'optimisation des procédures d'accueil et allie flexibilité et sécurité. Pour s'adapter au mieux aux besoins, procédures et organisation du client final, la solution offre des paramètres généraux à prédéfinir (ex, limiter la durée d'un rendez-vous par défaut) et des limites fonctionnelles selon le profil opérateur de chaque demandeur, valideur, hôte d'accueil.

Cette fonction logicielle est réalisée au moins au travers 2 interfaces dédiées :

- L'interface web
- Des postes d'exploitation
- Lecteurs de badge+Qrcode

L'ergonomie de ces interfaces a été étudiée pour offrir une IHM épurée, un traitement accéléré avec :

- Accès aux onglets fonctionnels filtrés selon les droits opérateurs et données par défaut proposées ou imposées
- Ecrans web auto-adaptatifs à la résolution et à la navigation (portrait/paysage, disposition des champs selon largeur...)
- Saisie et recherche de visiteurs avec auto-complétion.

L'interface WEB est accessible à tous les utilisateurs autorisés avec leurs PC bureautiques munis d'un navigateur web depuis l'intranet de l'entreprise. Elle permet de créer des visiteurs, de planifier et/ou valider des rendez-vous et compléter les informations nécessaires (plage horaire, profil d'accès, accompagnant, fiche visiteur...).

Les lecteurs de badge avec Scanner QR code intégré, offre 2 choix sur son écran :

- Pour le visiteur attendu qui scanne son QR code reçu par email.

Cette solution offre les avantages suivants :

- Gérer des visiteurs par un workflow complet & intégré à la gestion des accès.
- Optimiser, fluidifier, sécuriser l'accueil des visiteurs et leurs accès aux sites.
- Offrir des visites libres ou accompagnées / escorté avec double badgeage.
- Valider les RDV selon critères personnalisables par client :
 - Notifications email automatiques avec fichier ICS joint vers les visités, visiteurs, accompagnants pour enregistrer RDV dans Outlook en 1 clic
- Autoriser les visiteurs sur des accès anticipés (parkings...).
- Créer des visites par les visités autorisés depuis leurs PC bureautiques.
- Respecter les exigences de l'ANSSI (guide du sans contact).
- Offrir 2 types d'accueil visiteur pour 2 problématiques (sécurité, coût).
- Edition de badges visiteurs personnalisés par client (charte graphique, nom, codes couleur...).
- Permettre de créer des rendez-vous inopinés.

La gestion des visiteurs doit permettre la saisie de toutes les informations requises afin de créer les visiteurs éventuellement autorisés à circuler sur le site seul ou accompagné. La désignation des champs obligatoires à renseigner par les utilisateurs est paramétrable par les opérateurs. Les possibilités de gestion d'accès sont limitées volontairement, par rapport à un poste d'exploitation, pour les adapter aux fonctions utiles à la gestion des visiteurs et au personnel qui utilisera l'interface (personnel hors accueil et service sécurité) :

- Profils d'accès parmi ceux autorisés pour les visiteurs.
- Attribution d'un identifiant (badge) libre, parmi ceux créés pour les visiteurs.
- Validité, Anti-retour, passe-partout, liste noire...
- Notion de « statut » visiteur que l'on peut rendre visible qu'aux opérateurs spécifiques.

Cela permet de créer des droits d'accès limités pendant une période donnée

2.4.9.12 ENCODAGE DES BADGES

Le logiciel devra gérer l'encodage de la plupart des formats : Mifare Classic, Mifare Desfire EV1/EV2, en définissant notamment l'emplacement (ex : secteur Mifare Classic, applications et fichiers Mifare Desfire) et le format des identifiants (décimal, hexadécimal, alphanumérique...).

Plusieurs applications avec de multiples Identifiants peuvent être encodés en une seule fois.

L'identifiant peut être généré par le logiciel ou fourni par une application tierce.

L'encodage physique devra être réalisé individuellement ou par série de badges, sur un encodeur de table. Dans ce cas, il est possible de réaliser simultanément, en automatique pour une population de personnes :

- L'encodage multi-applications
- L'enrôlement de chaque badge à la personne associée

NOTA : Il n'est pas prévu de personnalisation des badges.

2.4.10 AUTOMATE

L'automate programmable IP devra intégrer nativement les fonctions de contrôle d'accès, intrusion et GTB.

Il s'intègre dans un système centralisé MICROSESAME CUBE et doit être associés à des modules spécialisés pour superviser et commander des portes, capteurs ou tous types d'automatismes.

Le système devra pouvoir gérer 24 lecteurs de contrôle d'accès, répartis sur 3 bus, et jusqu'à 600 000 identifiants.

Il est compatible avec un très grand nombre de protocoles et technologies d'identification : Desfire, QR code, plaque d'immatriculation, Bluetooth...

Il propose également une grande richesse fonctionnelle liée aux droits d'accès : anti-retour géographique & temporel, badge + code, double badgeage, accès sous contrainte, mode crise, filtrage d'étages (lecteur de cabine ascenseur), etc.

Caractéristiques

- Alimentation 12 ou 24 VDC pour plus de flexibilité et de distance de raccordement.
- 3 bus RS485, dont 1 reporté sur nappe de connexion rapide, avec propagation de l'alimentation.
- 3 entrées paramétrables (TOR, Equilibrée...) dont 1 prédisposée pour l'autoprotection.
- Entrées et bus RS485 protégés contre les courts-circuits, surtensions et inversions de polarités.
- 1 seul mode fonctionnel par bus : MD(V2); ML(NG), ML sécurisé (NG ou CUBE) ou APERIO.
- Paramétrage simplifié par serveur web embarqué.



2.4.11 UTL

Toutes les automates, UTL (Unité de traitement locale) et modules d'extension devront être de véritables automates industriels.

Il gère 2 lecteurs, sur 2 accès ou sur 1 accès avec lecteurs entrée/sortie. Les entrées paramétrables du MLP2 permettent de remonter aussi bien des informations surveillées de contrôle d'accès (état de porte, bouton poussoir, boîtier bris de glace) que des points intrusion.

Montage en coffret avec alimentation et batterie de secours. Le boîtier sera équipé d'un contact d'autoprotection à l'ouverture.

Ce module est conçu pour répondre aux préconisations de sécurité de l'ANSSI qui l'a certifié CSPN et qualifié.



Il permet de gérer le mode « lecteur transparent » où les clés sont stockées dans le module SAM/HSM du MLP2 CUBE, assurant leur secret.

Les lecteurs ne contiennent plus de clés (ANSSI architecture 1). Ils savent lire simultanément jusqu'à 4 types de badges DESFIRE EV1/2/3 pour 4 types de populations (ex : badges employés, badges prestataires, badges visiteurs,)

Caractéristiques

- Alimentation 12 ou 24 VDC pour plus de flexibilité et de distance de raccordement
- Nappe de connexion rapide pour simplifier le raccordement du bus et de l'alimentation
- Bus lecteurs de badges RS485
- 9 Entrées paramétrables (TOR, équilibrée...) dont 1 prédisposée pour l'autoprotection
- 2 relais NO ou NF
- Firmware et pilote lecteur téléchargeables par le bus RS485 depuis l'automate TILLYS CUBE
- Led sur toutes les entrées, sorties et bus RS485 pour faciliter la mise en service et la maintenance
- Borniers débrochables positionnés en haut et bas de carte pour faciliter le câblage et la maintenance

Les modules de porte seront montés dans un coffret spécifique commun à l'automate installé soit dans un local technique, gaine technique ou au plus près des portes dans un volume protégé.

Modèle MLP2 CUBE TiL technologie ou strictement équivalent.

2.4.12 BADGES

Les badges seront de type carte format ISO en PVC, avec puce MIFARE® DESFire® EV3 4ko sans impression (badge neutre)

Quantité prévue

- Tranche ferme : 500 unités
- Tranche optionnelle 1 : 350 unités

2.4.13 LECTEUR ENROLEUR DE TABLE

Un lecteur enrôleur de table à connexion par port USB permettra l'encodage des badges ainsi que la lecture. Il sera connecté au poste principal d'exploitation.

2.4.14 ENVIRONNEMENT DE LA PORTE

Chaque porte suivant sa localisation devra recevoir les équipements suivants :

- En entrée : lecteurs de différentes technologies
- En sortie : des boutons poussoirs (porte standard), béquille, barre antipanique ou des lecteurs (porte sensible)
- BBG Vert (bris de glace) de sortie d'urgence : Conforme aux normes en cours. Il comportera deux contacts :
 - Un contact pour la coupure de l'alimentation de la serrure libérant la porte et relié au SSI
 - Un contact d'information pour un report vers la supervision du contrôle d'accès
- Détecteur d'Ouverture porte (DO) : Chaque ouvrant devra avoir son détecteur d'Ouverture (intégré au système de verrouillage, ou contact en supplément sur l'accès) pour être relié à une entrée du module de porte qui pourra contrôler, superviser l'état de l'accès et déclencher les alarmes type « effraction porte », « porte ouverte trop longtemps », et « Antipassback »

2.4.14.1 LECTEUR DE BADGES

Les lecteurs de badges seront de marque identique à l'ensemble du système de contrôle d'accès.

En fonction de leur lieu d'installation, ils ne doivent pas être source de vulnérabilité. Les lecteurs de badges seront multi-technologies, à savoir :

- RFID MIFARE (Ultralight®, Classic, Plus, DESFire® EV1 & EV2, etc.),

Suivant les préconisations ANSSI, les têtes de lectures auront les caractéristiques techniques minimales suivantes :

- Distance de lecture 5 cm,
- Fréquence d'émission 13,56 MHz,
- Interface communication RS485 Crypté AES128 ou AES256.

Caractéristiques

- Anti-arrachement par accéléromètre et signal de vie, remontés via les Modules TiL.
- Boîtiers polycarbonate renforcé anti-vandale (IK10), imperméable aux jets d'eau et à la poussière (IP65)
- Capots disponibles en plusieurs couleurs ou motifs et éclairage d'ambiance réglable 360 couleurs
- **4 modules additionnels disponibles : biométrie, QR code, clavier à codes et lecteur 125 kHz**

NOTA : Les modules additionnels QR code et claviers sont à prévoir de base sur quelque accès uniquement (Bâtiments Rectorat du 92 et 96 Rue d'Antrain suivant plans)

Gamme Evolution TiL technologie ou strictement équivalent.

2.4.14.2 BOUTON POUSSOIR DE SORTIE

Le présent devra dans sa prestation un bouton poussoir inox, agréé IP67 IK08 (dimensions 90 x 90mm LxH) associé au système de contrôle d'accès.

Il sera conforme à la loi sur l'accessibilité aux personnes handicapées.

Il possédera un marquage en braille et une gravure du mot « PORTE »

L'état de fonctionnement sera identifié par un voyant vert ainsi que par un buzzer.

2.4.14.3 DECLENCHEUR MANUEL VERT POUR ISSUE DE SECOURS

Conformément à l'Article CO46 du règlement de sécurité incendie, le verrouillage des portes des sorties de secours sera réalisé sous réserve du respect des mesures suivantes :

- Chaque porte doit être équipée d'un dispositif de verrouillage électromagnétique conforme à la norme NFS 61-937 – Annexe A / Fiche XIV.
- Chaque porte ne peut être commandée selon l'un des deux principes suivants :
 - Par un dispositif de commande manuelle à fonction d'interrupteur intercalé sur la ligne de télécommande et situé près de l'issue équipée,
 - Le déverrouillage automatique des issues de secours doit être obtenu dans les conditions prévues à l'article MS 60, c'est à dire dès le déclenchement du processus d'alarme (début de l'alarme restreinte, s'il existe une temporisation).



La télécommande de ces DAS est donc toujours réalisée par rupture de courant.

Le présent devra prévoir un déclencheur manuel de type à double action et à membrane déformable, réarmable par clef, de couleur verte, sera installé à 1,30 m de hauteur côté intérieur, à proximité de la porte afin que celle-ci soit déverrouillable localement

Ce déclencheur est intercalé sur la ligne d'alimentation du dispositif de verrouillage de la porte fonctionnement à sécurité positive.

2.4.14.4 CONTACTS DE POSITION

Les informations de position des ouvrants seront à reprendre depuis soit les contacts intégrés au système de verrouillage ou soit par des contacts à prévoir sur les vantaux des portes à charge du présent par le présent lot (matériel similaire à l'alarme intrusion)

Des contacts magnétiques d'ouverture seront installés sur les portes équipées de lecteurs de badges.

Les portes à plusieurs vantaux seront équipées d'un contact magnétique par vantail (contacts câblés en série).

Ces capteurs sont composés de deux éléments :

- Un boîtier comportant un aimant sur l'ouvrant,
- Un boîtier de contact autoprotégé raccordé à l'UTL.

Ils devront fonctionner sans perturbation pour des températures allant jusqu'à +50°C et seront adaptés à la nature des portes (bois, métal...).

2.4.14.5 BOITES DE RACCORDEMENT LOCALES (BRL)

Les boîtes de raccordement locales seront mises en œuvre pour le raccordement local des câbles des environnements de portes (contacts d'ouverture, bouton poussoir, boîtier de décondamnation d'urgence, système de verrouillage...), les boîtes seront implantées au-dessus des portes (en faux-plafond le cas échéant) côté zone contrôlée.

Chaque boîte intégrera un bornier à vis et sera équipée d'un contact d'autoprotection qui sera traité comme une alarme et remonté à la supervision.

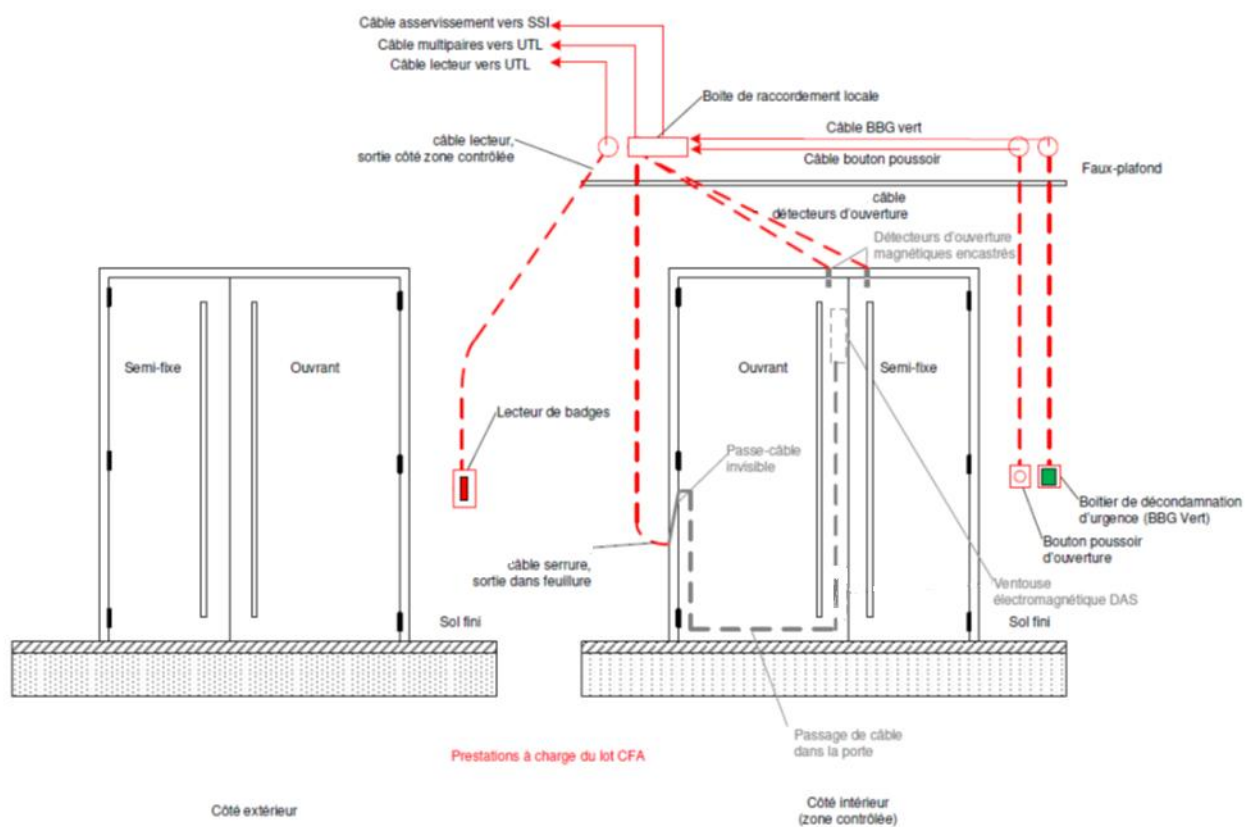
2.4.14.6 SYSTEME DE VERROUILLAGE

Le titulaire du présent lot devra les systèmes de verrouillage pour assurer le contrôle d'accès de chaque porte. Le système de verrouillage sera de type ventouse électromagnétique en applique avec voyant en applique avec une force de maintien de 500 kg avec contact de position pour les portes extérieures et 300kg pour les portes intérieures.

Grâce à ses propriétés multi-fixes et à son profil étroit, elle conviendra pour des portes simples battantes ou va et vient. L'aimant basse consommation sera alimenté en 12 ou 24 VDC et sera équipé d'un contact de position de porte. L'entreprise devra adapter le modèle aux différentes typologies de porte avec obligation de résultat.

Elle devra répondre à la norme NFS 61.937.

Principe de câblage d'une porte



2.4.14.7 ALIMENTATION ELECTRIQUE SECOURUE

L'ensemble des alimentations électriques nécessaires aux équipements de contrôle d'accès (UTL, systèmes de verrouillages) seront reprises soit depuis les TD les plus proches.

Ces alimentations seront à la charge du présent lot depuis les départs disjoncteurs à créer. Le système sera sécurisé par l'intermédiaire d'ensembles chargeur / batterie, assurant une autonomie de fonctionnement minimum de 48 heures tout en assurant un minimum de 100 commandes de serrure. Les batteries seront de type étanche au Cadmium-Nickel.

2.4.14.8 ACCES PARTICULIERS

Pour ces accès particuliers, le présent lot aura à sa charge la mise en œuvre et le raccordement des informations de pilotage par contact sec pour :

- Barrières levantes
- Portiques de sécurité à l'accueil des bâtiments du rectorat

Les deux portes de garages motorisées du Rectorat au sous-sol du 92 Rue d'Antrain sont actuellement équipés de télécommande HF. Cette installation est conservée

2.4.15 LECTEURS DE BADGES

Afin d'assurer une compatibilité avec les différentes technologies de badges, les lecteurs de badges devront être multi-technologies et multi-fréquences. Il devra posséder toutes les fonctionnalités suivantes :

- Supporter simultanément les fréquences de transmission de 13,56 MHz et de 125 KHz
- Pouvoir lire simultanément les badges (cartes) conformément aux normes ISO
- Doit pouvoir être mis à jour sans désinstallation pour supporter les évolutions des badges conformes aux normes ISO 14443A, ISO 14443B et ISO 15693

- Les fonctionnalités de lecture doivent pouvoir être mises à jour indépendamment du firmware du lecteur
- Pouvoir être connecté avec une connexion filaire ou connecteur
- Être équipé d'un « Élément Sécurisé » certifié EAL5+ pour héberger les clés secrètes et effectuer les opérations cryptographiques
- Doit supporter les algorithmes standards tels que 3DES ou AES
- Doit supporter le chiffrement des communications et l'authentification mutuelle badge / lecteur
- Doit pouvoir lire des données encapsulées appariées au support quel qu'il soit (badge, périphérique NFC ...)
- Avoir une interface Wiegand, Clock & data et RS485 pour les communications bidirectionnelles sécurisées entre le lecteur et le contrôleur
- Pouvoir être équipé d'un module optionnel pour supporter le protocole de communication OSDP-SC via RS485.
- Posséder 8 couleurs de LED pouvant être configurées pour indiquer les différents états du lecteur
- Pouvoir indiquer s'il est défaillant par une séquence LED dédiée
- Être fonctionnel jusqu'à des températures de -35°C
- Avoir un dispositif anti malveillance
- Doit pouvoir être identifié dans le système par un numéro de série électronique unique

Dans le cas où un clavier serait demandé association avec la lecture sans contact, les fonctionnalités additionnelles devront être intégrées :

- Le clavier du lecteur doit être conforme aux recommandations européennes sur l'accessibilité, il devra comporter une touche « 5 » marquée ainsi que des touches sur trois colonnes
- Le clavier du lecteur doit être rétroéclairé

2.4.16 CABLAGE DU SYSTEME

L'ensemble des canalisations nécessaires à cette installation sera réalisé par câble spécifique 6 et 9/10^è dissimulées à la vue, c'est à dire intégralement posées sous fourreaux encastrés et sur chemins de câbles courants faibles.

- Liaison réseau en câble 1x4P 6/10 catégorie 6A identique au câble VDI ou RS485
- Liaisons vers chaque lecteur de badge, système de verrouillage (BP et BG Vert)
- Liaison entre le système de contrôle d'accès et l'alarme intrusion
- Fourreaux encastrés ICTA et apparent IRL suivant le type de local.

Tous les câbles mis en œuvre devront être repérés de façon durable aux deux extrémités de façon à faciliter l'intervention du prestataire.

Se reporter aux plans d'implantations et synoptique sureté.

2.4.17 PROGRAMMATION, ESSAIS ET MISE EN SERVICE

2.4.17.1 PROGRAMMATION

Le paramétrage et la mise en service de l'ensemble du système de contrôle d'accès devra être assuré en étroite collaboration avec le support technique du fabricant.

Le présent lot devra collecter les besoins auprès du maître d'ouvrage ou de l'exploitant et lui proposer les scénarii sous forme de tableau de programmation pour validation.

2.4.17.2 ESSAIS ET MISE EN SERVICE

La réception définitive des ouvrages aura lieu lorsque l'ensemble des travaux sera terminé.

Les essais fonctionnels à réaliser pour le système porteront sur :

- Les essais fonctionnels de l'installation lors des phases d'autocontrôle,
- Les essais de chaque point de contrôle d'accès
- Les essais de chaque porte ou accès contrôlé,
- Les essais de réception avec la maîtrise d'œuvre et le maître d'ouvrage/exploitant.

2.4.18 CONTRAT DE SERVICE (PRESTATION SUPPLEMENTAIRE EVENTUELLE-PSE N°2 TF / PSE N°3 T01 / PSE N°5 T02)

Le constructeur du système devra pouvoir proposer un contrat de service à ses partenaires intégrateurs agréés ou au client final dans le cadre d'un forfait annuel de mise à disposition des évolutions logicielles & patches. Ce contrat aura pour objectif d'assurer les services suivants sur ses logiciels :

- Maintenance de sécurité : mise à disposition des correctifs de sécurité des vulnérabilités connues (CVE) des composants techniques utilisés par le constructeur (linux, algorithmes de cryptage, ...) permettant un maintien en condition de sécurité (MCS) éditeur de la solution technique.
- Maintenance curative : Mise à disposition des correctifs /patches (corrections de bug)
- Maintenance évolutive : Mise à disposition des nouvelles versions & firmwares automatés
- Fournir les informations synthétiques des évolutions de chaque version

Le titulaire du marché devra mettre à jour le système déployé chez le client final avec les éventuelles patches, correctifs de l'éditeur au moins une fois par an. Il devra également faire une migration le système déployé une fois tous les 3 ans.

Le constructeur, avec un support technique obligatoirement en France composé de 5 personnes minimum, associé avec les compétences du partenaire agréé devront pouvoir offrir le choix des services optionnels supplémentaires suivants aux clients finaux à travers un contrat :

- Accès à un support téléphonique en heures ouvrées et non limité,
- Prise en main du site à distance depuis le support téléphonique, avec l'accord du client final,
- Diagnostic et recherche des dysfonctionnements à distance
- Assistance à l'exploitation du client final.

2.5 ALARME INTRUSION

2.5.1 RAPPEL DU CADRE REGLEMENTAIRE ET ASSUREUR

- CNIL (Commission nationale de l'informatique et des libertés)
- La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,
- La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense,
- Le règlement général sur la protection des données de mai 2018,

2.5.2 GENERALITES

Chaque bâtiment sera pourvu d'un système d'alarme anti-intrusion raccordé à un terminal de télésurveillance. Le matériel sera certifié NF A2P. L'ensemble de l'installation anti-intrusion sera secouru par batteries permettant une autonomie de 72 heures en fonctionnement et d'une heure en alarme.

Le système d'intrusion viendra en complément au contrôle d'accès dans les locaux non contrôlés en accès. Le titulaire devra proposer un matériel totalement compatible avec le matériel de contrôle d'accès et son logiciel de supervision. Il sera donc possible d'y associer des fonctionnalités de protection à l'intrusion :

- Forçage d'un local contrôlé en entrée / en sortie, (état anormale),
- Ouverture anormale d'un local contrôlé en entrée / en sortie,
- Ouverture trop longtemps d'un local contrôlé en entrée / en sortie,
- Liste non exhaustive.

Dans tous les cas :

- Le matériel devra être pour l'ensemble de l'établissement d'une seule marque compatible avec le superviseur,
- Chaque entité devra pouvoir gérer indépendamment la programmation, et ses zones de détection.
- En cas d'alarme, la société de télésurveillance devra connaître précisément l'origine de celle-ci pour intervenir (adressage des détecteurs)
- Le système sera couplé avec le système de contrôle d'accès afin de désactiver l'installation lors du badgeage
- Le système permettra l'allumage de l'éclairage extérieur (sur détection des zones du niveau RDC)

L'alarme sera traitée par zone et par bâtiment (à se faire confirmer le découpage avant exécution).

2.5.3 DESCRIPTION DU SYSTEME

L'équipement d'alarme intrusion se composera principalement :

- Centrale adressable avec module de transmission téléphonique IP
- Modules entrées/sorties
- Claviers d'exploitation
- Détecteurs d'ouverture
- Détecteurs volumétriques
- Sirènes de diffusion
- Réseau de câblage,
- Programmation et mise en service

La mise en/hors service se fera soit par les claviers tactiles spécifiques ou depuis les lecteurs de badges qui devront neutraliseront les zones par badgeage.

2.5.4 CENTRALE D'ALARME

Le système sera construit autour d'une centrale à bus sur laquelle seront raccordés des modules périphériques.

La centrale à enveloppe métallique, protégée à l'ouverture et à l'arrachement, sera certifiée conforme au référentiel NFA2P 2 ou 3 boucliers suivant le niveau de risque.

Le bus sera de type RS485, réalisé avec du câble alarme comportant au minimum 2 paires torsadées 9/10. Le Bus pourra être rebouclé afin d'assurer le fonctionnement de l'intégralité de l'installation en cas de coupure de celui-ci.

L'alimentation du système devra être secourue par une batterie en cas de coupure de l'alimentation principale 230V avec une autonomie sur batterie d'au moins 60 heures.

Il sera prévu la fourniture, la pose et le raccordement d'une centrale entièrement électronique à microprocesseur de type adressable, permettant de gérer un fractionnement par zone à passage JOUR/NUIT indépendants (minimum 8 de base). Elle sera positionnée dans le local RGI.

Elle devra intégrer une connexion Ethernet native permettant au moins 10 communications IP simultanées avec diverses applications telles que logiciel de paramétrage, frontaux de télésurveillance, web browser, DMS, GTC, etc.

Un dialogue via une liaison protocolaire entre la centrale et d'autres applicatifs (DMS, GTC, superviseur) devra être possible. Dans le cas où certains applicatifs tiers ne seraient pas compatibles, le constructeur de la centrale aura obligation de fournir le protocole ainsi que son SDK pour intégration.

Elle permettra de gérer au maximum en intrusion :

- Jusqu'à 32 groupes protégés indépendants
- Jusqu'à 520 groupes de détection
- Jusqu'à 64 portes
- Jusqu'à 1000 détenteurs de cartes par système
- Jusqu'à 67 programmations hebdomadaires
- Jusqu'à 32 claviers pris en charge
- Prise en charge de claviers tactiles graphiques (4)
- Journaux d'événements consignants les accès et les intrusions (jusqu'à 1000 et 1500 événements respectivement)
- Prise en charge de plusieurs modes de communication (PSTN, ISDN, Ethernet)
- Jusqu'à 32 canaux de levée de doute audio
- Solution de gestion centralisée depuis un seul PC
- Protocole d'interface amélioré pour l'intégration du système
- Conformité aux normes européennes en vigueur et à NF&A2P type 3



La centrale à prévoir sera de marque Galaxy Honeywell et compatible sans développement supplémentaire avec le logiciel de supervision.

Les zones d'alarmes pour accéder au terminal déporté seront temporisées (tempo réglable).

Le transmetteur téléphonique multi protocole permettant le renvoi d'information vers une société de surveillance extérieure, il sera équipé d'un module de transmission par synthèse vocale, interrogeable à distance par téléphone et sera raccordé directement au réseau téléphonique. Il permettra d'indiquer l'adresse exacte du détecteur ou de la zone en alarme.

En complément la centrale pourra remonter via le logiciel de supervision une alarme vers le télésurveilleur (SMS ou autre)

2.5.5 MODULES ENTREES/SORTIES

Ils seront montés en coffrets déportés auto-protégés intégrant toute la connectique nécessaire aux raccordements du bus et des câbles venant et allant aux points adressés.

Ils seront placés dans les locaux technique et/ou éventuellement dans les gaines techniques courants faibles. Chaque coffret sera équipé de sa propre alimentation secourue par batterie.

Ils seront de type modulo 16 entrées/sorties maximum par module raccordés sur le bus du système. Chaque module devra gérer et transmettre à la centrale, en plus des informations propres aux éléments raccordés sur ses entrées, une alarme d'autosurveillance à l'ouverture et à l'arrachement. La perte de communication entre la centrale et les modules E/S générera une alarme autosurveillance clairement identifiée sur la centrale.

Caractéristiques

- 8 entrées
- 4 ou 8 sorties

Module 8E/4S Galaxy Honeywell.

2.5.6 ALIMENTATION DEPORTEE

Si l'alimentation fournie par la centrale est insuffisante, le système devra permettre de raccorder des coffrets chargeurs sur le Bus de la centrale qui seront supervisés par la centrale et secourus sur batterie.

Toute information de défaut batterie, défaut fusible, autoprotection ou coupure Bus survenant sur un chargeur sera affichée sur les claviers et transmise à la centrale.

Les coffrets chargeurs intégreront le module d'entrées/sorties.

2.5.7 TERMINALE D'EXPLOITATION

L'armement et le désarmement du système sera opéré au moyen d'un clavier LCD à l'entrée de chaque zone d'intrusion suivant plans

Ils posséderont un afficheur LCD rétro éclairé avec au minimum 2 lignes de 16 caractères alphanumériques et des voyants qui donneront un aperçu rapide de l'état de tout ou d'une partie du système.

Il sera possible de programmer les claviers pour limiter l'accès des utilisateurs aux seules fonctions autorisées pour chacun.

Une temporisation paramétrable permettra au personnel autorisé, d'accéder au clavier et taper son code de Mise Hors Service de la ou des zones programmées. Au-delà du temps paramétrés, l'alarme sera enclenchée et transmise.

Les claviers devront également intégrer une synthèse vocale pour confirmer l'état en service et hors service de la centrale d'alarme.

Modèle gamme Galaxy Honeywell ou équivalent

2.5.8 DETECTION INTRUSION

La détection s'articulera autour de divers équipements paramétrés de manière à déclencher une alarme en temps réel dès la moindre tentative d'intrusion ou d'actes de malveillance dans les zones surveillées.

- Détection périphérique : par contacts d'ouverture sur les portes extérieures (portes simples et doubles battants ou portes sectionnelles)
- Détection intérieure : par détecteurs de mouvements, acoustiques, chocs ou sismiques.

2.5.9 DETECTEURS PERIMETRIQUES

Ils seront raccordés individuellement sur les modules déportés d'entrées/sorties de la centrale par câblage en mode dit « équilibré 2 résistances » et assureront la surveillance de tous types d'ouvrants. Ils seront livrés et installés avec leurs conduits de raccordement armés.

Il sera prévu la mise en place de contacts d'ouverture sur les accès contrôlés ainsi que sur les Issues de Secours (IS) donnant sur l'extérieur.

Ils seront de type NF&A2P 3 Boucliers.

Ces contacts seront de type et de technologies appropriées à chaque type d'ouvrant à protéger, de dimensions les plus réduites possibles :

- Contacts sabot pour les ouvrants métalliques de type portes sectionnelles et à rouleaux, en boîtier aluminium grand écartement montés en saillie.
- Contact d'ouverture pour des ouvrants aluminium, PVC ou bois, les contacts seront en boîtier polycarbonate, dit tout support. Ils pourront être montés en saillie ou encastrés lorsque l'esthétique de la pièce devra être préservée.



2.5.10 DETECTEURS BI-VOLUMETRIQUES

Parfaitement adaptés à la surveillance intérieure des locaux étant donné leurs fonctionnalités avancées et leur faible consommation, les détecteurs seront certifiés NFA2P 2 ou 3 boucliers, EN50131-2-2 grade 2 classe B, et seront protégés à l'ouverture et à l'arrachement.



Il sera prévu la fourniture, la pose et le raccordement de détecteurs aux caractéristiques suivantes :

- Détecteur à double technologie avec fonction anti-masque équipé d'une lentille de Fresnel plate (cylindrique) interchangeable,
- Le capteur IRP est complètement protégé des perturbations causées par l'éventuel accès d'insectes et/ou de courants d'air pouvant déclencher des fausses alarmes.
- Protection anti-arrachement.
- Deux modes de fonctionnement possibles : AND : l'alarme est déclenchée si les deux sections (I.R. et H.F.) sont sollicitées. OR : l'alarme est déclenchée si au moins une section est sollicitée.

Les détecteurs de type bi-volumétrique détecteront une présence humaine en mouvement dans un volume, par mesure de variations de températures et par la technologie infrarouge / hyperfréquence.

Les caractéristiques principales sont :

- Portée de 8/11/13/15 grande angle et longue portée 45ml type rideau (suivant besoin)
- Montage mural avec angle 90° ou encastré avec angle 360°
- Détection infrarouge passive avec ou sans détection hyperfréquence
- Optique à double miroir de précision
- Fonction anti-masquage
- Immunité aux animaux
- Réglage de la sensibilité de détection en fonction de l'environnement
- Faible consommation à partir de 2,5mA au repos
- Résistances d'équilibrages 4,7Kohms prémontées en usine

Le titulaire du présent lot devra intégrer pour chaque détecteur le ou les accessoires suivant pour chaque situation :

- Rotule de montage
- Embase d'encastrement
- Embase métallisée

Les détecteurs placés dans les zones publiques devront avoir une fonction d'anti-masquage performante permettant de détecter les tentatives de neutralisation par pulvérisation de laque ou de vernis sur la fenêtre du détecteur.

Le choix des détecteurs dépendra de l'exigence de sécurité du site et des contraintes de surveillance. Ils seront de type infra-rouge passif ou double technologie et compatible avec la centrale.

Le présent lot devra déterminer le modèle et type de détecteur à prévoir suivant les zones à protéger.

2.5.11 SIRENES INTERIEURES

Il sera prévu, en cas d'intrusion, le fonctionnement des sirènes autonomes avec batterie pour un fonctionnement temporisé et répétitif en cas de nouvelles anomalies.

Les sirènes de dissuasion seront placées à l'intérieur du bâtiment et éventuellement à l'extérieure. Elles seront avec flash intégré.

Elles seront de dimensions les plus réduites possibles, montées en coffrets auto-protégés à l'ouverture et à l'arrachement intégrant les batteries d'auto-alimentation.

Puissance 110 à 115 dba à 1 mètre.

2.5.12 CABLAGE DU SYSTEME

L'ensemble des canalisations nécessaires à cette installation sera réalisé par câble spécifique 6 et 9/10^e dissimulées à la vue, c'est à dire intégralement posées sous fourreaux encastrés, moulure PVC et sur chemins de câbles courants faibles.

Autant que possible, les liaisons filaires doivent être situées dans des zones de sécurité pour éviter les actes de malveillance et seront conformes aux prescriptions du fabricant.

Le titulaire doit l'ensemble du câblage :

- Liaison vers le clavier
- Liaisons vers chaque organe de détection
- Liaison vers chaque diffuseur
- Liaisons d'asservissements de l'alarme intrusion pour la commande des scénarii
- Fourreaux encastrés ICTA, et apparent type moulure, tube IRL suivant le type de local.

Toutes les canalisations seront auto-protégées et surveillées en permanence, l'autoprotection sera câblée sur tous les organes boîtes et coffrets de raccordement de l'installation.

2.5.13 SECTEUR DE SURVEILLANCE

La centrale devra permettre de gérer plusieurs secteurs de surveillance distincts avec possibilité de créer des liens entre chacun. Un secteur devra pouvoir être commun à 2 secteurs minimum.

Exemples de scénarii réalisables :

- Mise en surveillance d'un secteur commun pourra entraîner la mise en surveillance des secteurs dépendants du commun
- Mise en surveillance de tous les secteurs dépendants du commun pourra entraîner la mise en surveillance du secteur commun
- Mise hors surveillance d'un secteur commun pourra entraîner la mise hors surveillance de tous les secteurs dépendants du commun
- Mise hors surveillance d'un des secteurs dépendants du commun pourra entraîner la mise hors surveillance du commun

Dans chaque secteur, il devra être possible de choisir entre une protection totale ou une protection partielle, avec deux modes de protection partielle possibles.

2.5.14 TRANSMISSION D'EVENEMENTS

La centrale disposera nativement d'une connexion Ethernet qui permettra la transmission d'alarme par TCP/IP point par point et GPRS.

Le transmetteur numérique (Ethernet, GPRS) supportera l'envoi d'informations d'alarmes correctement réceptionnées par le télésurveilleur, en utilisant un protocole sécurisé d'une cryptographie symétrique en protocole EDP SIA.

Dans le cas de l'utilisation des 2 types de transmetteurs (Ethernet et GPRS), le transmetteur GPRS devra secourir le transmetteur Ethernet (en cas d'échec de transmission sur le réseau Ethernet, l'information d'alarme sera alors transmise via le réseau GPRS).

De plus chaque centrale sera dans la capacité de remonter les alarmes sur les postes de supervision afin que depuis ceux-ci une alarme puisse être envoyée par mail ou autres supports (notifications, SMS, etc)

2.5.15 EXPLOITATION FONCTIONNELLE

2.5.15.1 UTILISATEURS

La centrale devra permettre de gérer jusqu'à 2500 utilisateurs avec des profils différents et adaptés aux besoins de l'exploitation du site.

Chaque utilisateur pourra être identifié par son nom propre, et chacune de ses actions sera clairement identifiée dans le journal de bord. Un même utilisateur pourra se voir doté d'un code (de 4 à 8 chiffres)

Quel que soit le mode de badgeage employé par l'utilisateur pour accéder au système, il devra être identifié de la même manière dans l'historique du système.

Il sera possible de limiter dans le temps la validité des droits d'accès d'un utilisateur. Une fois la date limite dépassée, ses droits seront invalidés, mais l'utilisateur devra rester enregistré dans la centrale. Une simple modification des dates de validité revalidera automatiquement ses droits, sans autre paramétrage nécessaire.

Le système proposera l'import/export des utilisateurs à travers le navigateur web à partir d'un fichier Excel ou Word.

Les commandes de mise En/Hors service de territoires intrusion devront être réalisables sur action de l'opérateur.

2.5.15.2 JOURNAL DE BORD

La centrale devra être pourvue de 3 journaux de bord dissociés, avec chacun une capacité de stockage de 10.000 évènements.

- 1 dédié au système
- 1 dédié à la fonction contrôle des accès
- 1 dédié aux alarmes

Même en cas de remise à zéro de la centrale, il est impératif que l'historique des évènements demeure consultable.

2.5.15.3 GESTION HORAIRE

La centrale gèrera des scénarii horaires programmables (ou calendriers) qui seront associés aux zones surveillées, aux utilisateurs, aux entrées, aux sorties, aux portes.

Ces calendriers devront permettre une gestion horaire quotidienne : à cet effet, ils disposeront de 4 plages horaires ON/OFF journalières, potentiellement différentes chaque jour de la semaine, autorisant ainsi la création de 3 semaines types associés ensuite aux 53 semaines de l'année

Ces calendriers pourront être associés aux composants suivants de l'installation :

- Utilisateur : invalidation des droits utilisateurs en dehors des plages actives du calendrier
- Sorties : Activation de la sortie pendant les plages actives du calendrier
- Zones de surveillance : Mise en et/ou hors surveillance en fonction des plages horaires du calendrier
- Portes : Verrouillage ou déverrouillage des portes en fonction des plages du calendrier

Lors de la mise en surveillance automatique par calendrier, une pré-signalisation sonore et/ou visuelle informera l'utilisateur de l'imminence de la mise sous surveillance de la zone dans laquelle il se trouve. La fonction de dérogation horaire permettra à l'utilisateur de différer l'horaire de mise en surveillance automatique.

2.5.15.4 GESTION D'ASSERVISSEMENTS

La centrale disposera également des fonctions annexes à la détection d'intrusion, en permettant sur combinaisons de différents événements de l'installation (cause à effet), d'activer des dispositifs externes par le biais des sorties de la centrale.

Le type de déclencheur sera :

- L'état d'une entrée

- L'état d'une zone de surveillance
- L'état des défauts techniques
- Une action utilisateur (saisie d'un code spécifique, utilisation d'une radiocommande spécifique)

2.5.16 PROGRAMMATION, ESSAIS ET MISE EN SERVICE

2.5.16.1 PROGRAMMATION

Le paramétrage et la mise en service de l'ensemble du système d'anti-intrusion devra être assuré en étroite collaboration avec le support technique du fabricant.

Le présent lot devra collecter les besoins auprès du maître d'ouvrage ou de l'exploitant et lui proposer les scénarii sous forme de tableau de programmation pour validation.

L'entreprise doit la programmation, la mise en service et les essais de l'ensemble de l'installation. Pour cela elle devra établir et fournir un plan de contrôle.

Le titulaire doit :

- La configuration de chaque centrale pour connexion au réseau TC/IP
- La configuration des tables d'échanges avec la supervision,
- L'installation et le paramétrage du serveur,
- L'installation et paramétrage de la base de données,
- Le paramétrage des plages horaires,
- Le transfert de la programmation dans les centrales
- L'intégration et l'animation des symboles graphiques des équipements, des alarmes, des fonctions (inhibition, etc.), etc.
- Toutes sujétions utiles et nécessaires.

2.5.16.2 ESSAIS ET MISE EN SERVICE

La réception définitive des ouvrages aura lieu lorsque l'ensemble des travaux sera terminé.

Les essais fonctionnels à réaliser pour le système porteront sur :

- Les essais fonctionnels de l'installation lors des phases d'autocontrôle,
- Les essais de chaque point de détection,
- Les essais de réception avec la maîtrise d'œuvre et le maître d'ouvrage/exploitant.

2.6 VIDÉOSURVEILLANCE

2.6.1 RAPPEL DU CADRE REGLEMENTAIRE

- CNIL (Commission nationale de l'informatique et des libertés)
- La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,
- La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense
- Le règlement général sur la protection des données de mai 2018,
- La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense

- La loi du 21 janvier 1995 prévoit et impose des dispositifs garantissant le respect de la vie privée des sujets filmés :
 - Les images enregistrées ne doivent être accessibles que par un personnel habilité et seront impérativement protégées par un code d'accès,
 - Au-delà d'une durée définie par la Préfecture, les images enregistrées devront être automatiquement effacées,
 - Un dispositif de type « main courante » devra garantir la traçabilité de toutes les opérations effectuées (consultation, effacement, copie, ...) sur la base de données constituée par l'ensemble des images enregistrées.
- Conformité au décret du 3 août 2007 :
 - Le matériel devra être conforme à l'extrait de l'annexe technique de l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance (rectificatif) NOR : IOCD0762353Z
 - 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.
 - Le nom de la caméra, la date et l'heure de l'enregistrement doivent être intégrés de manière logicielle dans chaque image du fichier vidéo.
 - 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 format des fichiers vidéo devra être non-propriétaire et standard.
 - Les flux vidéo stockés issus des caméras qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit, à l'exclusion de celles de régulation du trafic routier, ont un format d'image supérieur ou égal à 704 × 576 pixels. Ce format pourra être inférieur si le système permet l'extraction de vignettes de visage d'une résolution minimum de 90 × 60 pixels.
 - Tous les flux vidéo seront enregistrés à une résolution minimum de 704x576 pixels (soit 4CIF).
 - Une fréquence minimale de douze images par seconde est requise pour l'enregistrement des flux vidéo issus de caméras installées pour une des finalités mentionnées au II de l'article 10 de la loi du 21 janvier 1995 susvisée, à l'exclusion de celles de régulation du trafic routier, et qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit et filment principalement des flux d'individus en déplacement rapide.
 - Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo.
 - Un journal de toutes les opérations devra être enregistré, indiquant la caméra, la date et l'heure de la séquence exportée, la date et l'heure de l'export et la personne ayant fait cet export.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 1
 - Un rapport de présentation dans lequel sont exposés les finalités du projet au regard des objectifs définis par ladite loi et les techniques mises en œuvre, eu égard à la nature de l'activité exercée, aux risques d'agression ou de vol présentés par le lieu où l'établissement a été créé.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 2
 - Un plan de masse des lieux montrant les bâtiments du pétitionnaire et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et leurs ouvertures.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 3

- Un plan de détail à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 4
 - La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 5
 - La description des mesures de sécurité qui seront prises pour la sauvegarde et la protection des images éventuellement enregistrées.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 7
 - Délai de conservation des images, s'il y a lieu, avec les justifications nécessaires.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 8
 - Désignation de la personne ou du service responsable du système et, s'il s'agit d'une personne ou d'un service différent, la désignation du responsable et de sa maintenance, ainsi que toute indication sur la qualité des personnes chargées de l'exploitation du système susceptibles de visionner les images.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 9
 - Les consignes générales données aux personnels d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images.
- Décret n°96-926 du 17 octobre 1996 – Article 1er – Paragraphe 10
 - Modalités du droit d'accès des personnes intéressées.

2.6.1.1 DOSSIER DE DEMANDE D'AUTORISATION D'EXPLOITATION

Le titulaire aura en charge de rédiger les dossiers administratifs de demande d'autorisation d'exploitation du système de vidéosurveillance pour la préfecture et la CNIL.

Il sera transmis au Maître d'Ouvrage. A charge du Maître d'Ouvrage de le compléter et de le transmettre aux institutions concernées (Préfecture et CNIL).

2.6.1.2 MODALITE D'INFORMATION DU PUBLIC

Afin d'informer le public de son entrée dans un espace sous vidéosurveillance et de lui laisser la possibilité d'y consentir, un système d'information par voies d'affichage sera mis en place.

Ce principe repose sur des panneaux d'information du public d'une dimension minimale de 35cm par 20cm environ.

Ils seront répartis sur l'ensemble des sites de la manière suivante :

- A chaque accès véhicules pour les parkings,
- A chaque entrée piétonne.



Le titulaire doit la fourniture et pose de l'ensemble des panneaux.

2.6.1.3 DECLARATION APSAD R82

Le titulaire devra se conformer aux préconisations ANSSI.

2.6.2 SPECIFICATION MATERIELLE DU SYSTEME

L'appel à un installateur certifié garantit l'assurance de la mise en œuvre des systèmes de sécurité performants :

- Une conception adaptée au besoin de l'utilisateur,
- Un matériel de qualité,
- Un installateur compétent,
- Un mainteneur / vérificateur compétent pour des installations fiables et pérennes.

L'architecture d'un système de Vidéosurveillance sur le plan fonctionnel est constituée de 4 blocs :

- Bloc acquisition
- Bloc transport
- Bloc enregistrement
- Bloc exploitation

Dans le cadre du présent projet, les prestations de vidéosurveillance se limite à

- L'étude de couverture de vidéosurveillance afin de confirmer le type et l'emplacement des caméras ainsi que les points RJ45 ou connexion fibre optique,
- La constitution du dossier de demande d'autorisation auprès de la CNIL, de la déclaration en préfecture et les affichages réglementaires (signalétiques),
- L'intégration des caméras IP dans le bâti, suivant implantation précisée sur les plans,
- La mise en place et le raccordement des équipements informatiques dans les baies informatiques.

2.6.3 OUVERTURE DU SYSTEME

Le système n'utilisant aucun matériel hardware propriétaire mais exclusivement des PC sur base Windows, moniteurs et stockeurs réseau du marché.

Le système de vidéosurveillance répondra aux caractéristiques générales suivantes :

- Fonctionnement avec des caméras IP et/ou analogiques (via encodeurs IP)
- Utilisation simultanée de caméras IP choisies parmi la majorité des modèles de caméras IP de marques mondialement reconnues et non propriétaires : AXIS, HANWHA...
- Évolutivité du système (compléments de caméras, de serveurs d'enregistrements, de moniteurs de visualisation...) ne nécessitant que l'ajout de licences logicielles.
- Pas de limitation du nombre de caméras pouvant être gérées (plusieurs milliers)

Le système sera ouvert avec des systèmes tiers (API et SDK pour intégration de toutes les fonctionnalités principales du système avec applications tierces).

Le système devra permettre d'intégrer ultérieurement des fonctions d'analyses d'images.

Les applications logicielles devront fonctionner sur les versions Windows actuelle et sur une architecture informatique disponible sur le marché indépendamment du fabricant ou de l'éditeur de la plateforme de vidéosurveillance sur IP.

Un journal intégré au système gardera une trace de toutes les activités réalisées sur le système : changement de paramétrage, de mode d'opération, copie de fichiers, exports, effacements ou modification etc.

Le logiciel d'exploitation permettra les fonctionnalités de gestion et d'administration suivantes :

- Gestion des caméras
- Gestion du mur d'images
- Gestion de l'affichage
- Gestion des plans interactifs
- Recherche sur archives
- Export de séquence
- Gestion des alarmes

2.6.4 GESTION DES CAMERAS

Pour chacune des caméras :

- Contrôle de la qualité de l'image.
- Contrôle de la bande passante maximale utilisée
- Définition du codec à utiliser : MJPEG, MPEG4, H264, H265
- Gestion des doubles flux pour enregistrement et/ou visualisation à fréquence et résolution différente
- Gestion des métadonnées générées par les caméras intelligentes
- Définition du mode d'enregistrement : continu, sur détection de mouvements ou sur détection par l'analyse d'image
- Définition du mode d'enregistrement en fonction de plages horaires hebdomadaires.
- Définition des paramètres de la détection de mouvements :
 - Paramétrage du seuil de sensibilité.
 - Paramétrage de la quantité de mouvement minimale pour déclenchement.
- Masquage de zones :
 - Possibilité de définir jusqu'à 1024 zones par caméra.
 - Possibilité d'ignorer les mouvements sur toute l'image et ne détecter que les mouvements sur une zone à marquer. Exemple : seulement les entrées et sorties par une porte.
- Gestion de la pré et post alarme avec définition de la durée du tampon.
- Définition de l'événement déclencheur.
- Définition de l'événement qui arrête l'enregistrement.
- Le contrôle de la motorisation des caméras PTZ se fera directement en IP et n'utilisera pas de connexion supplémentaire dédiée.
- Possibilité d'accès simultané aux images d'une même caméra en live ou en relecture par de nombreux utilisateurs sans aucune dégradation de la qualité des images et de leur fréquence.

2.6.5 GESTION DES MURS D'IMAGES

Le logiciel de vidéo protection intégrera la gestion de murs d'images (au minimum 2x16 caméras par mur d'images) et de moniteurs avec une représentation schématique des écrans du mur d'images depuis n'importe quel poste client.

- Envoi d'une caméra ou d'une vue complète depuis un poste client vers n'importe quel moniteur du mur d'images.
- Pour chaque caméra affichée :
 - Pause sur image, lecture avant arrière à vitesse variable en relecture d'enregistrements
 - Affichage simultané sur un même moniteur d'une même caméra en pause en lecture avant et en lecture arrière (vitesse normale, ralentie, accélérée)
 - Zoom numérique et optique en live possible
 - Zoom numérique en relecture.
- Gestion des événements pour affichage des alarmes sur un écran dédié

2.6.6 GESTION DE L’AFFICHAGE

Le système proposé devra permettre de gérer l’affichage de la façon suivante :

- Affichage simultané d’images archivées sur différents stockeurs.
- Affichage d’un QUAD (4 caméras) en résolution Full HD.
- Affichages jusqu’à 32 caméras par moniteur.
- Définition de la position et de la taille d’affichage de chaque caméra sur l’écran par l’utilisateur.
- Possibilité de contrôle des caméras motorisées par joystick et/ou par clic dans l’image.
- Pré positionnement des caméras motorisées accessibles par clic sur un bouton.

2.6.7 GESTION DE PLANS INTERACTIFS (PRESTATION SUPPLEMENTAIRE EVENTUELLE-PSE N°1 TF / PSE N°3 T01 / PSE N°5 T02)

Afin de garantir une exploitation conviviale, le système devra afficher des plans avec des icônes positionnées pour chaque caméra. Les vues graphiques seront réalisées sur la base de plans épurés du bâtiment au format AUTOCAD en JPEG. Ces vues seront impérativement dynamiques et permettront :

- L’affichage d’une caméra ou d’une vue complète en direct par simple « Clic » sur une icône
- Le déclenchement manuel d’enregistrements par simple clic sur un bouton
- De zoomer sur les vues caméras lives et sur les archives.
- La représentation virtuelle des murs d’images.

2.6.8 RECHERCHE SUR ARCHIVES

La recherche sur archives devra se faire de la manière suivante :

- Par date et heure de l’enregistrement.
- Par le nom de la caméra.
- Par type d’événement déclencheur de l’enregistrement.
- Par nom du détecteur ou de l’alarme déclencheur de l’enregistrement.
- Par filtre

2.6.9 EXPORT DE SEQUENCES

L’export de séquences vidéo devra se faire à partir des postes de travail, sous format AVI, MPEG, MKV, ... avec possibilité de cryptage et d’ajout de mot de passe. Il sera également possible de faire des exports de la base de données au format propriétaire avec une visionneuse attachée.

Toute manipulation des enregistrements devra rendre instantanément les enregistrements inexploitable.

2.6.10 GESTION D'ALARMES

Le système permettra l'affichage automatique des caméras en alarme en superposition à toute autre application active afin de faciliter l'exploitation du système par l'exploitant

2.6.11 PARAMETRAGE DES MASQUES DES CAMERAS

Des masques seront paramétrés sur les images des caméras visualisant des zones publiques (logements, parties privatives des tiers...).

Pour les caméras PTZ, les masques seront gérés dynamiquement en fonction du champ de vision de la caméra et du facteur de zoom.

2.6.12 PARAMETRAGES DES ENREGISTREMENTS

L'enregistrement des caméras devra être réalisé en continu 24h/24. Les images devront être sauvegardées pendant 30 jours suivant qualité vidéo détaillée ci-après.

Le système sera paramétré comme suit :

- Caméra en alarme :
 - Enregistrement au format H.264 ; sans dégradation des détails en mouvement,
 - A la résolution maximale de la caméra,
 - A une fréquence de 25 images par secondes.
- Caméra hors alarme :
 - Enregistrement au format H.264 ; sans dégradation des détails en mouvement,
 - A la résolution maximale de la caméra,
 - A une fréquence de 12 images par secondes.

Les caméras passeront en mode alarme :

- En cas de détection d'activité sur la caméra
- En cas d'alarme intrusion (interface avec le système intrusion)
- En cas d'alarme contrôle d'accès (interface avec le système de contrôle d'accès : porte forcée, boîtier de décondamnation d'urgence activé...)

Les images enregistrées seront signées numériquement et le logiciel sera capable d'en vérifier l'intégrité.

2.6.13 LE BLOC ENREGISTREMENT

Le bloc fonctionnel « Enregistrement » concerne le stockage des images vidéo en vue d'une exploitation à postériori et donc en temps différé.

La localisation du ou des dispositifs de stockage sera décentralisé au niveau du bâtiment de la DSII

- La solution technique de stockage sera de type:
 - NVR, NAS, SAAS, SAN, Etc.
- Le niveau de disponibilité recherché : stockage simple ou stockage à haute disponibilité

Quel que soit la solution retenue, elle devra autoriser :

- L'enregistrement de chaque caméra avec la résolution maximale et une fluidité de 12 images par seconde,

- La relecture simultanément à l'enregistrement à l'enregistrement des flux.

2.6.14 SURVEILLANCE DE L'ETAT DES ENREGISTREURS

L'état des enregistreurs sera monitoré via SNMP, les infos remontées devront au minimum être les suivantes (Liste non exhaustive) :

- Pertes de base de données,
- Disques saturés,
- Impossibilité d'écriture disques,
- Perte de connexion IP,
- Archivage arrêté,
- État du RAID,
- État des alimentations électrique (perte de redondance),
- Etc.

Il est important que le matériel de stockage soit contrôlé, afin qu'une éventuelle panne soit immédiatement détectée pour remplacer l'élément défaillant.

Ces états devront être intégrés nativement dans le SDK du constructeur du serveur pour mise à disposition.

2.6.15 SPECIFICATIONS DU MATERIEL INFORMATIQUE

Le présent devra transmettre au début de l'opération transmettre ou confirmer les prérequis pour le matériel suivant à la charge du maître d'ouvrage (matériel et logiciel d'exploitation).

La fourniture et l'installation des logiciels spécifiques liés aux applications de sûreté reste à la charge du présent lot.

2.6.15.1 SERVEUR DE MANAGEMENT

Le serveur de management sera fourni par les services du rectorat (DSII) et sera configuré suivant les prérequis par le présent lot. L'ensemble des applications mis en œuvre (à l'exception du contrôle d'accès et de l'anti-intrusion) seront virtualisées. Le serveur sera hébergé dans le bâtiment de la DSII rue Jean Julien Lemordant à Rennes.

Ce serveur permettra de gérer les authentifications des utilisateurs au système vidéo, il est l'interface pour le SDK et aiguille les différents flux vidéo.

Après une coupure secteur, le serveur sera en mesure de redémarrer automatiquement « procédure Auto log on ».

Les capacités du serveur de management devront être confirmées par l'adjudicataire afin de réaliser les fonctions d'exploitation et de redondance (redondance d'un serveur d'enregistrement en cas de perte n-1). Les services de la DSII devra configurer cette redondance, afin que cela soit totalement transparent par les utilisateurs.

Le serveur sera constitué de :

- Serveur Rack 1U type DELL POWEREDGE R530 ou techniquement équivalent (ou version plus à jour),
- Système d'exploitation Windows serveur ou équivalent
- Processeurs Intel XEON E5-2620 (ou version plus à jour),
- RAM 16 Go, 2 x 1 DD 500 Go SATA en RAID 1 pour le système d'exploitation et X DD 1To SATA RAID 5 pour le système d'archivage
- Deux Cartes réseau Ethernet PCI Gigabits,

- Logiciel anti-virus

2.6.15.2 SERVEUR D'ENREGISTREMENT VIDEO

Le serveur d'enregistrement sera fourni par les services du rectorat (DSII) et sera configuré suivant les prérequis par le présent lot. L'ensemble des applications mis en œuvre (à l'exception du contrôle d'accès et de l'anti-intrusion) seront virtualisées. Le serveur sera hébergé dans le bâtiment de la DSII.

Les principales caractéristiques du serveur d'enregistrement aura au minimum les suivantes et devront être confirmé par le présent lot :

- Serveur Rack 1U type DELL POWEREDGE ou techniquement équivalent (version la plus à jour),
- Windows server (version la plus à jour),
- Base de données SQL Serveur,
- Processeurs Intel XEON ,
- Disques durs enfichables à chaud,
- Blocs d'alimentation redondants enfichables à chaud,
- RAM 16 Go, 2 x 1 DD 500 Go SATA en RAID 1 pour le système d'exploitation et X DD 1To SATA RAID 5 pour le système d'archivage
 - Tranche ferme (92 et 96 Rue d'Antrain Rennes) : 8 To minimum sur une base 12 images par seconde (à confirmer par le présent lot)
 - Tranche optionnelle 1 (DSDEN et DSII) : 6 To minimum sur une base 12 images par seconde (à confirmer par le présent lot)
 - Tranche optionnelle2 (UAR et Restaurant) : 4 To minimum sur une base 12 images par seconde (à confirmer par le présent lot)
- Cartes réseau Ethernet PCI Gigabits – 2 unités
- Clavier, souris,
- 2 à 4 ports USB,

Les principales fonctionnalités des serveurs d'enregistrements doivent être au minimum les suivantes :

- Enregistrer des signaux vidéo à 12 images/secondes,
- Supporter plusieurs relectures simultanées,
- Disposer du tatouage numérique (Watermarked),
- 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,
- Une alimentation redondante afin d'éviter une possibilité de panne (Une alimentation sur source normale, une alimentation sur source secourue),
- Procédé de compression M-JPEG – H264 – H264CCTV – MPEG4CCTV.
- Le nombre de serveurs dépendra du nombre de caméras à gérer (Charge CPU et flux d'enregistrement maximum par serveur). Le titulaire devra indiquer le nombre de serveurs qu'il a prévu.
- Après une coupure secteur, le serveur sera en mesure de redémarrer automatiquement « procédure Auto log on ».

2.6.16 CARACTERISTIQUES DES CAMERAS

2.6.16.1 LE BLOC ACQUISITION

Le bloc acquisition correspond à la capture des images vidéo par les équipements adaptés que sont les caméras de vidéosurveillance :

- Les caméras fixes pour surveiller un champ de vision bien défini et ciblé avec ou sans reconnaissance faciale.

Toutes les caméras seront de type couleur numérique Full HD. Certaines caméras devront assurée une reconnaissance faciale par conséquent leurs caractéristiques devront être prévues dans ce but.

Toutes les caméras comporteront une détection d'activité réglable par le logiciel. Elles disposeront toutes de fonction jour/nuit et apparaitront obligatoirement dans la liste du matériel supporté par le logiciel de vidéosurveillance.

Les modèles et références proposés sont données à titre indicatif et l'entreprise devra définir les modèles exactes à prévoir suivants les zones à surveiller.

2.6.16.1.1 Caméra Dôme fixe intérieur pour reconnaissance faciale :

Les caméras dôme fixe 4MP intérieur disposeront des caractéristiques suivantes :

- Type dôme fixe anti vandale
- Indice de protection : IP66, IK10
- Compatibilité ONVIF (version en cours au moment de la consultation)
- Port réseau Ethernet 10/100 Base-TX
- Capteur 1/2.7" CMOS
- Sensibilité couleur 0,18 à 0,03 lux N/B
- Résolution 2304x1728
- Objectif Vari-focal
- Iris automatique
- Encodeur H264, H265
- Alimentation PoE (802.3af)
- Fonction jour / nuit automatique avec filtre infrarouge débrayable
- Microphone intégré
- Mise au point à distance
- Fonctionnement de -30°C à +60°C

Modèle AXIS P4216V ou équivalent

2.6.16.1.2 Caméra Dôme fixe intérieur pour couloir étroit :

Les caméras dôme fixe 8MP intérieur disposeront des caractéristiques suivantes :

- Type dôme fixe anti vandale
- Indice de protection : IP66, IK10
- Compatibilité ONVIF (version en cours au moment de la consultation)
- Port réseau Ethernet 10/100 Base-TX
- Capteur 1/2.8" CMOS

- Sensibilité couleur 0,24 à 0,04 lux N/B
- Résolution 3840x2160 à 320x240
- Objectif Vari-focal
- Iris automatique
- Encodeur H264, H265
- Alimentation PoE (802.3af)
- Fonction jour / nuit automatique avec filtre infrarouge débrayable
- Microphone intégré
- Mise au point à distance
- Fonctionnement de -30°C à +60°C

Modèle AXIS M4218V ou équivalent

2.6.16.1.3 Caméra Dôme fixe intérieur pour couloir étroit :

Les caméras dôme fixe 2MP intérieur disposeront des caractéristiques suivantes :

- Type dôme fixe anti vandale
- Indice de protection : IP66, IK10
- Compatibilité ONVIF (version en cours au moment de la consultation)
- Port réseau Ethernet 10/100 Base-TX
- Capteur 1/2.8" CMOS
- Sensibilité couleur 0,24 à 0,04 lux N/B
- Résolution 1920x1080 à 160x90
- Objectif Vari-focal
- Iris automatique
- Encodeur H264, H265
- Alimentation PoE (802.3af)
- Fonction jour / nuit automatique avec filtre infrarouge débrayable
- Microphone intégré
- Mise au point à distance
- Fonctionnement de -30°C à +60°C

Modèle AXIS P3265V ou équivalent

2.6.16.1.4 Caméra « bullet » extérieure :

Les caméras « bullet » disposeront des caractéristiques suivantes :

- Type mini caisson (tube)
- Projecteur infra-rouge à LED intégré (distance : 20m)
- Indice de protection : IP66, IK10
- Compatibilité ONVIF (version en cours au moment de la consultation)
- Port réseau Ethernet 10/100 Base-TX

- Capteur 1/3" CMOS
- Sensibilité couleur 0,13 à 0 lux N/B
- Résolution 2592/1944
- Objectif Vari-focal
- Iris automatique
- Encodeur H264, H265
- Alimentation PoE (802.3af)
- Fonction jour / nuit automatique avec filtre infrarouge débrayable
- Microphone intégré
- Mise au point à distance
- Fonctionnement de -30°C à +60°C

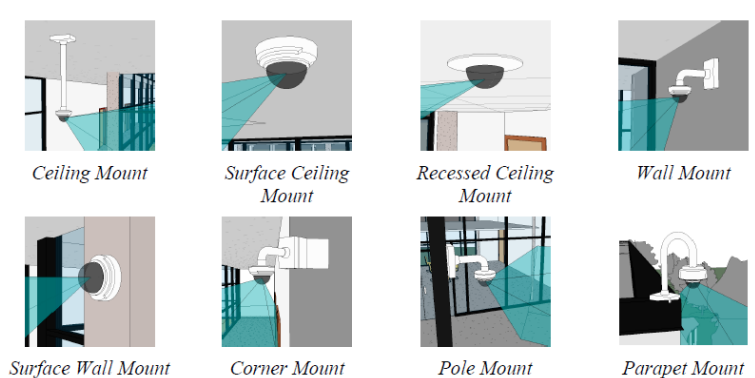
Modèle AXIS P1467-LE ou équivalent

2.6.16.1.5 Supports caméras

En fonction du mode de pose, le titulaire doit l'ensemble des accessoires de support (Mural – Plafond – Angle à 90° - Mât – Mât candélabre, etc.)

Le titulaire doit l'ensemble des supports adaptés pour la fixation des caméras.

Le mode de pose sera soit mural, soit en dalle plafond mais avec potence pour fixation sous dalle (Exemple ci-dessous pour le modèle mini dôme).



2.6.16.1.6 Configuration et paramétrage

Le titulaire doit l'ensemble des prestations de paramétrage et configuration des caméras :

- Le paramétrage à partir des serveurs WEB (Adresse IP, trap SNMP, NTP), dont les paramètres de configuration seront donnés par le MOA durant la phase d'exécution,
- La déclaration des caméras,
- Les échanges de données par SDK avec les serveurs d'enregistrements
- Le réglage des champs des caméras (Pan – tilt – Focale),
- Le libellé des caméras suivant la codification imposée par le client.

2.6.16.1.7 Réglage des caméras

Le titulaire aura à sa charge le réglage des caméras, comprenant réglage des champs de vision, objectifs, sensibilité, focale, format d'image (16/9, 4/3)...

2.6.16.1.8 Tests des caméras

Chaque caméra devra être testée. Ce test comprendra :

- Vérification de la communication avec chaque caméra
- Vérification de la qualité des images
- Vérification du fonctionnement des motorisations (caméras dômes PTZ)
- Une capture d'image attestant du champ de vision de chaque caméra devra être réalisée.

Chaque caméra fera l'objet d'une fiche de recette attestant de son bon fonctionnement et intégrant :

- Son repère (référence aux plans d'implantation),
- Son adresse IP,
- Son adresse MAC,
- Le modèle de la caméra (marque et référence),
- Le format et la résolution de l'image,
- Le repère du commutateur sur lequel elle est raccordée ainsi que le repère de sa prise RJ45,
- Une capture d'image de la caméra,
- Une ou plusieurs photos des conditions de mise en œuvre de la caméra,
- Un extrait du plan d'implantation DOE associé

2.6.16.1.9 Licences caméras

Le titulaire doit intégrer les licences par caméras.

2.6.16.2 LE BLOC TRANSPORT

Le bloc fonctionnel « Transport » concerne l'acheminement des images vidéo et leur commutation, depuis les postes d'acquisition jusqu'au(x) poste(s) d'exploitation et/ou enregistrement.

Cet acheminement doit se faire sans altération significative des images afin que celles-ci puissent être visualisées et exploitées correctement.

2.6.16.2.1 Les câbles

Dans une solution vidéo numérique, le bloc transport est composé de câbles cuivre ou fibres optiques et de commutateur Ethernet multicast.

2.6.16.2.2 Les équipements actifs réseaux

Les switches de commutation seront fournis par le MOA et mis à disposition par les utilisateurs. Le titulaire devra fournir l'inventaires des équipements raccordés sur le réseau informatique.

Le débit ou flux vidéo est composé d'une succession d'images, 12 ou 25 images par seconde constituant l'illusion du mouvement. Les facteurs impactant sont les suivants :

- Résolution initiale de l'image,
- Format de compression appliqué (H264, etc.),
- Nombre d'image par seconde.

2.6.17 SPECIFICATION LOGICIELLE DU SYSTEME

Les applications du système de vidéosurveillance n'imposeront aucune limite sur le nombre de machines pouvant être connectées en réseau afin de constituer un système de serveur d'archivage distribué.

2.6.18 INTERFACE AVEC DES APPLICATIONS TIERCES

Les serveurs devront pouvoir être supervisé par des systèmes tiers (Superviseur) et transmettre les flux vidéo grâce au SDK ou serveur RTSP fourni par le constructeur.

2.6.19 INTEROPERABILITE AVEC LES CAMERAS DU MARCHE (ONVIF)

Le serveur doit intégrer les caméras pour transmettre les états, via SDK, des caméras :

- Perte d'image de référence
- Masquage caméra
- D'autres états futurs (Détection de mouvements – Sens de passage par une ligne virtuelle programmée dans la caméra, etc.)
- Perte de connexion IP,
- Etc.

2.6.20 CALCUL DE STOCKAGE

Le titulaire devra fournir lors de ses études d'exécution le calcul de la capacité de stockage de chaque serveur. Le calcul de la capacité disque dépend des critères suivants :

- Nombre de caméras,
- Enregistrement continu
- Nombre d'heures d'enregistrement quotidien par caméra (24h/24),
- Nombre d'image par seconde (12ips),
- Résolution d'image,
- Type de compression vidéo (H264),
- Complexité de l'image, conditions d'éclairage et quantité de mouvement,
- Durée de conservation souhaitée des données (10 jours).

2.6.20.1 CALCUL BANDE PASSANTE

Le titulaire devra fournir lors de ses études d'exécution le calcul de bande passante pour chaque serveur en fonction des caméras qui leurs sont rattachés.

Le titulaire devra prendre en compte que les caméras diffuseront un double flux :

- Live en résolution Full HD en 25 ips,
- Enregistrement en résolution Full HD en 12 ips.

2.6.20.2 CONFIGURATION ET PARAMETRAGE

Le titulaire doit l'ensemble des prestations de paramétrage et configuration (Liste non exhaustive) :

- L'adressage IP
- L'installation des applications logicielles,
- La déclaration des caméras,
- Les échanges de données par SDK.

2.6.20.3 LE BLOC EXPLOITATION

2.6.20.4 GENERALITES

Ce dernier bloc fonctionnel correspond aux équipements, matériels et logiciels mis à disposition des opérateurs pour assurer les opérations liées à :

- La visualisation des images temps réels,
- La consultation des images enregistrées,
- L'affichage de caméra sur événements (appel interphone – contact intrusion – etc.)
- Nous retrouverons dans ce bloc :
 - Les logiciels liés au système de gestion vidéo,
 - Les postes opérateurs informatisés,
 - Les écrans autorisant les différents scénarios d'affichage.

Le logiciel proposé devra être mutualiser aux usages suivants :

- Contrôle d'accès,
- Anti-intrusion,
- Vidéoprotection,

Le système de gestion Vidéosurveillance possédera une architecture modulaire et utilisera des protocoles de communications standardisés permettant ainsi de garantir l'ouverture et l'évolutivité du système :

- Ajout de caméras,
- Ajout de serveurs de stockage,
- Montée en charge du nombre d'opérateur,
- Ajout de nouvelles fonctionnalités de type ouvert et totalement évolutif,
- Interface avec d'autres systèmes (Passerelle logicielle, API/SDK, etc.)

L'exploitation au quotidien du système de Vidéosurveillance se fera dans le local PCS et éventuellement en consultation depuis le poste secondaire.

La sécurisation et la protection de l'accès au système, sera assurée par des mécanismes adaptés (https, authentification, gestion des flux, etc.). Le titulaire fournira un descriptif permettant d'apporter les justifications des choix techniques.

2.6.20.5 LOGICIEL D'EXPLOITATION

2.6.20.6 GESTION ET SECURITE DES DROITS D'ACCES

L'accès à chaque machine informatique sera sécurisé par « Login » et « Mot de passe » associé au Domaine réseau pour l'application de Vidéosurveillance.

A l'ouverture de la session Windows, l'opérateur saisira son « Login » puis « Mot de passe » et lui donnera accès à l'application en fonction de son profil (Opérateur – Administrateur, Maintenance, etc.).

Les ports et les lecteurs (USB, SD, etc.) des postes d'exploitations et des serveurs non utilisés seront verrouillés.

2.6.20.7 APPLICATION LOGICIELLE

2.6.20.8 PRINCIPALES FONCTIONNALITES DE L'IHM

L'IHM doit permettre à un opérateur de se concentrer sur ces objectifs et missions en s'affranchissant complètement des aspects techniques. Les principales fonctionnalités auxquels l'IHM doit répondre sont les suivantes :

- Gestion de la cartographie
 - La base de travail est constituée usuellement par un fond de plan couvrant la zone à surveiller, avec fonction de zoom avant et arrière et hiérarchisation. Ce fond de plan peut être une simple image (cartographie statique) ou une source issue d'un système d'information géographique (Autocad ou Révit)
- Sélection des caméras :
 - Toutes les caméras raccordées doivent pouvoir être sélectionnées à partir de l'interface graphique de l'IHM.
- Gestion de l'affichage :
 - Affectation des caméras à visualiser depuis la carte ou une liste hiérarchisée des caméras vers le système d'affichage (Ecran poste de travail et Mur d'images).
- Gestion d'une arborescence :
 - Regroupement de caméras par zone géographique sous forme arborescente de manière que l'opérateur puisse accéder rapidement à l'ensemble des caméras correspondant à la zone géographique choisie.
- Gestion des cycles :
 - Sur une même vignette, affichage en cycle de plusieurs caméras avec une temporisation de changement paramétrable.
- Caméra postée :
 - Possibilité, pour les opérateurs, de désactiver les cycles d'une caméra et de la figer volontairement sur un cadrage.
- Relecture d'images enregistrées

2.6.20.8.1 Fonction de visualisation

L'utilisateur a la possibilité de sélectionner les sources vidéo à afficher :

- A partir d'une liste de caméras organisées dans une arborescence,
- Par glisser - déplacer à partir de la liste des caméras,
- Par glisser - déplacer à partir de plans graphiques,
- Par simple clic à partir de plans graphiques,
- Par menu contextuel à partir de plans graphiques,
- Par sélection d'un contexte d'affichage pré enregistré,

Les sources vidéo peuvent être affichées simultanément dans un des formats multi vision disponible : 2x2, 3x3, 4x4, 5+1, 12+1, 8+2. Le format multi vision pourra aussi être totalement paramétrable.

L'affichage des sources vidéo s'effectue en live ou en playback si des enregistreurs sont raccordés à l'IHM.

L'affichage des sources vidéo peut être automatisé en fonction de différent mode :

- Commutation de caméra sur alarme ou sur événement.
- Possibilité de définir un cyclique automatique sur alarme,

- Possibilité de définir des cycliques prés programmés : liste de caméras avec temporisation et avec préposition (uniquement pour les caméras dôme),
- Commutation de caméra sur alarme,
- Basculement du mode d'affichage multi vision en affichage plein écran par double clic sur l'image.

Les modes d'affichage décrit ci-dessus s'appliquent sur les afficheurs internes (intégrés à l'application) et également aux afficheurs externes : moniteurs, décodeurs IP, ou système de mur d'images.

L'interface graphique permettant d'intégrer des plans au format standard (BMP, JPG, GIF, WMF, EMF, DXF) est complètement personnalisable avec une bibliothèque de symboles qu'il est possible d'enrichir ou de modifier à volonté avec un éditeur graphique vectoriel intégré à l'IHM Il est aussi possible de configurer les plans graphiques pour qu'ils intègrent sous forme d'incrustation les afficheurs vidéo avec possibilité de commutation automatique.

Autres fonctions :

- Fonction pause (arrêt sur image),
- Relecture instantanée (uniquement sur enregistreur),
- Commande d'enregistrement,
- Capture d'image,
- Impression d'image.

L'appel des synoptique se fera à partir de bouton préprogrammé ou d'une liste déroulante.

2.6.20.8.2 Les incrustations vidéo

Le logiciel permettra la gestion des textes incrustés sur la vidéo ainsi que l'heure et la date. Afin de faciliter le repérage d'une image visualisée par une caméra sur un écran, les incrustations vidéo indiqueront à la place du nom de la caméra, le texte correspondant à la zone visualisée.

Les textes incrustés seront ceux des zones géographiques qui seront dessinés sur le plan sur lequel est implantée chaque caméra.

2.6.20.8.3 Fonction de visualisation et de mémorisation

Afin de faciliter et automatiser l'exploitation, des séquences d'exploitation (visualisation et/ou mémorisation) seront gérées par l'IHM. Ces scénarii vidéo seront ceux préalablement définies par le responsable d'exploitation.

Ceux-ci pourront être déclenchés de la manière suivante :

- Choix de l'opérateur dans une liste ou des boutons spécifiques,
- Apparition d'un événement d'alarme,
- Heure de déclenchement planifiée, dans un agenda journalier et hebdomadaire intégrant les jours fériés et des jours ou heures particuliers.

Les séquences exécutables dans un scénario seront au minimum les suivantes :

- Affichage d'une caméra sur un écran (ou plusieurs caméras sur plusieurs écrans).
- Positionnement automatique d'une caméra,
- Mémorisation des images d'une ou plusieurs caméras,
- Affichage d'un plan,
- Affichage de messages de consigne,
- Incrustation de textes dans l'image,
- Incrustation du nom de la zone visualisée.

2.6.20.8.4 Fonction « Pixéliser / Flouter »

Le logiciel devra nativement permettre de pixéliser, flouter ou de masquer, selon les cas, pour la visualisation et/ou l'extraction et devra être compatible pour un floutage en mouvement en vue de certaines extractions réglementaires.

2.6.20.8.5 Fonctions de consultation

Ces fonctions ne sont disponibles qu'à partir des enregistreurs.

L'utilisateur a la possibilité de sélectionner les séquences vidéo enregistrées :

- En sélectionnant des sources vidéo puis en sélectionnant une période de temps : date/heure,
- Ou à partir de l'historique des alarmes ou des événements en sélectionnant la vidéo associée.

Dans ce dernier cas les alarmes ou événements rattachés à des séquences vidéo sont affichés, par exemple, dans la liste avec un icône « vidéo ».

Lors de l'accès à un enregistrement sur alarme, la période d'affichage est automatiquement positionnée sur la période de pré alarme.

L'interface de l'IHM pour consulter les séquences enregistrées dispose des fonctions suivantes :

- Affichage en playback de plusieurs sources simultanées avec possibilité de synchronisation de la lecture,
- Possibilité de lecture en vitesse accélérée et en lecture arrière,
- Fonction pause,
- Relecture instantanée,
- Avance/recule image par image,
- Export des séquences vidéo dans un format standard,
- Capture d'image,
- Impression d'image.

2.6.20.8.6 La consultation des images

La consultation des images fera sans arrêt des enregistrements en cours, sera protégée par un code d'accès (loi de 1995) et devra se faire selon différents critères, à savoir :

- La date et l'heure,
- Le type d'enregistrement,
- Le numéro d'une ou plusieurs caméras,
- Un mode localisation géographique (dessin sur plan ou zone d'incrustation de texte) permettant de ne rechercher que les images correspondant à des positionnements de caméras lorsqu'elles visualisent uniquement la zone où l'événement est recherché.

2.6.20.8.7 Fonctions d'acquisition d'événement

L'IHM est capable de contrôler l'infrastructure du système et d'exploiter les événements ou alarmes produits par les systèmes vidéo (Liste non exhaustive) :

- Pertes de base de données,
- Disques saturés,
- Impossibilité d'écriture disques,
- Perte de connexion IP,
- Archivage arrêté,

- état du RAID,
- état des alimentations électrique (perte de redondance),
- Perte d'image de référence
- Masquage caméra
- D'autres états futurs (Détection de mouvements – Sens de passage par une ligne virtuelle programmée dans la caméra, etc.)
- Perte de connexion IP,
- Liste non exhaustive.

Avec la possibilité d'intégrer dans les plans graphiques l'animation correspondant à ces événements.

Ces événements seront disponibles dans le SDK du constructeur pour être exploité par une application tierce.

2.6.20.8.8 Fonctions d'administration

L'IHM intègre une gestion des utilisateurs organisée par profil ce qui permet de définir finement les droits d'accès aux fonctionnalités :

- Accès à l'affichage en live,
- Accès à l'affichage en playback,
- Commande des dômes,
- Filtrage sur les sources vidéo accessibles,
- Filtrage sur la période de temps accessible pour la consultation des séquences enregistrées,
- Filtrage sur la période de temps accessible pour la consultation des historiques des alarmes et événements,
- Configuration des cycliques et des prépositions,
- Impression,
- Capture d'image ou de vidéo,
- Configuration de l'IHM,
- Gestion des utilisateurs et profils,

D'autre part l'IHM enregistre toutes les actions utilisateur :

- Connexion/déconnexion,
- Acquiescement d'alarme,
- Rapport sur alarme,
- Demande de lecture en live,
- Demande de lecture en playback,
- Affichage de cyclique,
- Capture photo,
- Capture vidéo,

2.6.20.8.9 Auto-commutation vidéo sur événements alarmes

Des événements alarmes nécessiteront une auto-commutation vidéo permettant :

- Lever un doute,
- Organiser l'intervention,

- Mieux informer les services de sécurité sur les infractions,
- Etc.

Il sera prévu à minima les auto-commutations suivantes :

- Intrusion extérieur (1 par façade),
- Intrusion intérieur (1 par niveau),
- Intrusion locaux sensibles

3 DESCRIPTION DES OUVRAGES COURANTS FAIBLES

3.1 EXTENSION DU PRÉCABLAGE BANALISÉ VDI

3.1.1 PRINCIPE

L'objectif est d'étendre le réseau de câblage VDI existant afin d'assurer la connexion des équipements de sûreté.

Le réseau VDI doit permettre d'assurer :

- La connexion du contrôle d'accès, l'alarme intrusion et la vidéo-surveillance
- L'équipement des locaux hébergeant les postes d'exploitation (principal et secondaire)
- Serveurs et système de stockage

3.1.2 GENERALITES

Le présent document a pour objet de définir l'ensemble des prestations et fournitures nécessaires à la réalisation du précâblage banalisé (voix/données/images) pouvant recevoir un système de supervision dynamique de la couche physique cuivre et fibre optique en temps réel.

Les caractéristiques du système de câblage doivent permettre un débit le plus important possible, et ainsi supporter toutes les applications IEEE 802.x (10M/100M/1000M/10G Ethernet).

En conséquence, les locaux du présent projet seront irrigués par un câblage polyvalent dont la conception et la réalisation de mise en œuvre sera conforme aux tests et normes en vigueur aux niveaux européens et internationaux définis par ISO/IEC 11801 1.0 Edition 2017, les normes de la série EN 50-173, EN 50-174, EN 55-022, IEC 61754-19, et EIA/TIA 568-B.2.1, et de plus compatible CEM EN 50-167, 50-168, 50-169 et 50-174.

3.1.3 CONFORMITE DE L'INSTALLATION

Le présent lot devra assurer toutes les démarches nécessaires en temps voulu auprès du service informatique chargée des équipements informatiques et de vérifier que le précâblage envisagé comprend bien toutes les prestations nécessaires au bon fonctionnement de ces équipements.

Fournir tous les éléments certifiant que l'ensemble des composants (prise terminale, câble de distribution horizontal, cordon de brassage et de liaison) du système de câblage sont bien conformes aux normes composants par exemple la norme ISO/IEC 60603-7-51 pour les connecteurs de catégorie 6A permettent la réalisation de liaisons conformes à la classe EA ISO/IEC 11801-1 édition 2017:

- Perte d'insertion jusqu'à 500Mhz
- NEXT jusqu'à 500Mhz
- Perte en Retour ou RL jusqu'à 500Mhz
- Tous les « POWER SUM » jusqu'à 500Mhz
- Tous les autres paramètres définis dans la norme
- Déséquilibre résistif : Pour assurer la transmission des applications de télé alimentation (PoE/PoE+ et 4PPOE jusqu'à 90 W respectivement IEEE 802.3af, 802.3at et 802.3bt)

Le système de câblage sera également en mesure d'être certifié selon l'ISO/IEC 11801-1 édition 2017 en lien Permanent 2 ou 3 connecteurs suivant la configuration retenue pour le projet. Un test cuivre dont les mesures en Lien Permanent 2 ou 3 connecteurs (Permanent Link) sont conformes à la norme ISO le sera également en Canal (Channel) dès lors que les cordons de brassage sont aussi conformes à la norme.

3.1.4 PRINCIPE DES TRAVAUX A REALISER

Les équipements connectés au réseau informatique en IP (PC, caméra, contrôle d'accès, intrusion) le seront depuis des liaisons à prévoir depuis les baies informatiques existantes sur les différents sites par extension du câble existant.

3.1.5 EQUIPEMENT DES BAIES INFORMATIQUES

Chaque baie recevra les équipements suivants:

- x panneaux 24 ports RJ45
- x panneau passe cordons à raison d'un par panneau optique et cuivre
- Les cordons de brassage cuivre RJ45/RJ45 4 paires droits

3.1.5.1.1 Panneaux de brassage

Le panneau de brassage intégrera le même type de connecteur RJ45 que le poste de travail. Il sera modulaire et pourra intégrer jusqu'à 24 ports RJ45 sur 1U.

La mise à la terre des connecteurs RJ45 sur le châssis 19" sera automatiquement réalisée lors du clipsage des modules RJ45.

L'identification des ports se fera par étiquette placée sous fenêtre transparente.



3.1.5.1.2 Passe cordons

Les passe-cordons seront équipés de 4 anneaux métalliques de dimensions 52/74 mm.

Les cordons peuvent aussi être gérés en passage arrière par le biais de passe cordons à balais.

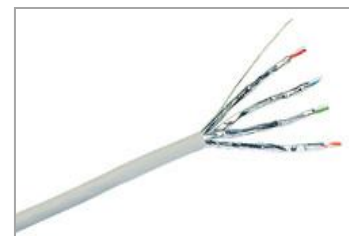


3.1.6 CABLAGE CUIVRE

3.1.6.1.1 La distribution capillaire

La distribution capillaire cheminera principalement sur chemins-de-câble en dalles pleines perforées spécifiques, sous fourreaux encastrés en cloisons ou doublages, et en apparent sous tube IRL/goulotte ou tube acier inox.

Les chemins de dalles seront distants de 30 cm par rapport aux chemins de câbles courants forts d'électricité. Les câbles capillaires issues des chemins de câbles chemineront à 30 cm de tout câble électrique parallèle à son parcours.



A chaque fois qu'un câble descendra sous fourreau ou tube depuis le chemin-de-câble ce dernier sera attaché à celui-ci puis sera ininterrompu jusqu'à la prise terminale ou la plinthe électrique compartimentée Courants forts et courants faibles.

Le câble utilisé pour le raccordement des prises RJ45 sera en 1x4 ou 2x4 paires torsadées, AWG 23 minimum, **catégorie 6a** et de structure blindée par paire avec un écran individuel autour de chaque paires type F/FTP 500 MHz. Il sera Euroclasse Dca minimum selon la norme RPC EN50575 compatible PoE, PoE+ et 4PPoE (55W-90W). La gaine sera de couleur grise avec le marquage de la NVP.

NOTA : dans le cas la longueur nécessaire pour connecter un équipement dépasse la longueur de 90m, le présent lot devra prévoir en remplacement une liaison fibre optique et les convertisseurs FO/CU aux extrémités.

3.1.6.1.2 Les prises ou points d'accès

Les prises terminales seront adaptées à l'appareillage électrique 45 x 45 pour poste de travail en montage encastré ou sailli avec boîtier adapté.

Le module RJ45 Catégorie 6A utilisé pour le raccordement sera avec capot de blindage métallique pour assurer une meilleure efficacité du blindage. Il sera de type PowerSafe, compatible 4PPoE (55W-90W) selon la norme IEEE 802.3bt.



La zone de contact de fonctionnement sera distincte de la zone de déconnexion lors du débranchement Plug (protection PoE).

Le connecteur acceptera pour le raccordement de câbles monobrins et multibrins.

Le raccordement des 4 paires du câble sera réalisé sans outil spécifique en câblage EIA/TIA 568A/B et la reprise du blindage sera réalisée par un système automatique cranté en périphérie de gaine.

Il sera important d'utiliser des boîtiers ou des plinthes de profondeur suffisante pour assurer un rayon de courbure correct du câble et de maintenir ainsi les performances dynamiques de l'ensemble. Il sera multi-positionnable avec des accroches sur les quatre côtés.

Certaines prises devront être intégrées dans des boîtiers étanches avec volet transparent.

Elles seront câblées suivant la convention EIA/TIA 568 B (à faire valider par le Maître d'ouvrage), sans outil de câblage spécifique.

L'étiquette de repérage sera protégée par une fenêtre transparente. Chaque prise sera repérée par étiquetage inaltérable et indécollable DYMO. Cet étiquetage ne sera mis en place définitivement qu'après contrôle final du réseau, un étiquetage provisoire de chantier est donc à prévoir.

3.1.6.1.3 Equipement des postes de travail (Poste principal et poste secondaire)

Les prises seront fonctionnellement disposées et en nombre suffisant dans les locaux. Leurs positions devront être étudiées par rapport à l'aménagement des postes de travail.

3.1.6.1.4 Cordons de brassage

Les cordons de brassage utilisés pour les liaisons seront en 4 paires, catégorie 6A d'impédance 100 Ohms et de structure blindé par paire S/FTP avec une gaine extérieure LSFROH.

La technologie du Plug RJ45 sera de type CAD PowerSafe (perçement d'isolant interdit)) et garantira les applications de télé-alimentation IEEE 802.3af, 802.3at et 802.3bt (4PPoE 55W-90W) sans risque d'échauffement.



La conception du manchon sera adaptée à un rayon de courbure supérieur à 90° (Sertissage métallique du câble à 360°).

Ils seront munis d'un système de repérage visuel par clips de couleur interchangeable (8 au total).

La gaine extérieure pourra être aussi de couleur. Diamètre global du câble de 6mm et conducteur AWG26/7.

Les couleurs seront à valider avec le service informatique

3.1.6.1.5 Repérage et étiquetage

Le repérage sera effectué sur les équipements et sur les plans d'exécutions. Il devra être validé par le Maître d'Ouvrage avant mise en œuvre. A cet égard, Un listing avec le numéro des locaux et leurs noms sera fourni par l'entrepreneur.

Le repère de chaque baie doit être indiqué sur une étiquette collée sur la porte du coffret ou de la baie.

Toutes les prises réseau de l'établissement doivent être étiquetées suivant la codification du Maître d'ouvrage.

3.1.7 TESTS A REALISER

Un contrôle statique et dynamique du câblage (tests à effectuer dans les deux sens) sera effectué systématiquement sur l'ensemble des composants suivant la norme ISO/IEC 11 801 - dernière édition.

L'entreprise devra procéder au test de 100% des liens installés et/ou modifiés, ce, en « Permanent-Link », au regard des valeurs du tableau de la norme ISO/IEC 11 801 - dernière édition.

Le testeur utilisé devra disposer d'un jeu de cordons adéquat au précâblage mis en œuvre pour un test en Permanent Link et Channel permettant de valider chaque liaison suivant les valeurs minimales ISO / IEC de la classe demandée.

Avant démarrage des tests « un certificat de calibrage », de moins d'un an, des appareils de mesure devra être présenté pour accord.

Tel que le préconise la norme, l'ensemble des tests devra être effectué avec un même et unique jeu de cordons.

3.1.7.1 RECETTE DE L'INSTALLATION CUIVRE

La référence normative sera l'ISO/IEC 11801-1 : 2017 :

- Pour un test Permanent Link (PL) Classe EA
- Pour un test Canal Classe EA (Channel)

Ces mesures seront consignées dans un dossier précisant pour chaque liaison :

- | | | |
|-------------------------|-----------------------|------------|
| • Longueur | Perte d'Insertion | NEXT |
| • PS NEXT | Return Loss) | ACR-N |
| • ACR-F | PSACR-N | PSACR-F |
| • PS ACR | Délais de propagation | Delay Skew |
| • Déséquilibre résistif | | |

Les mesures seront réalisées avec un certificateur de câblage de précision niveau III minimum (ex : Fluke DSX 8000, WireXpert 4500, Ideal LanTEK III...) et seront transmises sous le format natif de l'appareil de test utilisé.

Pour les rocade téléphoniques, un test de continuité et de plan de câblage sera demandé.

La mesure de la performance du blindage en courant alternatif et localisation de sa coupure sur le lien est obligatoire afin de détecter une éventuelle mauvaise mise à la terre des baies de brassage.

Les mesures seront réalisées avec un certificateur de câblage de précision minimum de niveau IIIe validée par un laboratoire indépendant avec fourniture du certificat.

Dans le cas où le débit est supérieur à 1Gbps (soit 10Gbps, 25 voire 40Gbps), il est important de vérifier l'immunité de l'installation par rapport aux perturbations qui pourraient traverser le blindage. Les mesures de TCL et ELTTCL permettent le contrôle d'une bonne immunité.

3.1.8 FOURNITURES HORS MARCHÉ

Matériel informatique nécessaire au fonctionnement du réseau du rectorat (Routeur, switch).

3.2 MODIFICATION DU SYSTÈME DE SÉCURITÉ INCENDIE

Dans le cadre de la mise en sécurité des différents bâtiments, le présent lot doit assurer le déverrouillage des issues de secours verrouillées pour des raisons de sûreté.

3.2.1.1 DEVERROUILLAGE DES ISSUES DE SECOURS

Certaines portes extérieures et intérieures à fonction d'issues de secours, indiquées sur les plans, sont équipées de dispositifs de verrouillages électriques qui doivent être asservis au système de sécurité incendie (SSI).

Les lignes de commande et de contrôle aboutissent sur bloc porte commandé (dispositif de fermeture hors lot).

Chaque bloc porte est commandé par :

- Un déclencheur manuel de couleur vert, à fonction d'interrupteur de ligne de type avec membrane déformable avec clapet de protection (double action avec plombage),

Les déclencheurs manuels seront placés à 1 m 30 du sol. Le mode de commande sera de type sécurité positive.

LES PORTES DEVERROUILLEES SONT INDIQUEES SUR LES PLANS ET CORRESPONDENT A CELLES CONTROLEES PAR LE SYSTÈME DE CONTRÔLE D'ACCÈS.

3.2.1.2 CANALISATIONS DU SSI

Les câbles respecteront les données du constructeur et les normes en vigueur (en particulier les normes NFC 15-100, NF S 61-970 et NF S 61-932).

Les sections et les natures des câbles sont donnés à titre indicatif, il est nécessaire de tenir compte de leur longueur, de la puissance installée et de leurs implantations (traversées de locaux à risques par exemple).

3.2.1.3 PROGRAMMATION

Le présent lot doit assurer la programmation ou la modification de la programmation de chaque centrale incendie afin d'assurer la fonction déverrouillage. Si besoin elle fera intervenir le fabricant pour assurer les modifications.

Les listings de programmation devront être transmis à la maîtrise d'œuvre.

3.2.1.4 AUTOCONTROLES

Le présent lot de vérifier le bon fonctionnement du déverrouillage des issues de secours sur déclenchement de l'alarme.

3.2.1.5 RECEPTION

Préalablement à la réception technique, l'installateur réalise ses propres essais par autocontrôle tels que définis dans les normes NF S 61-932 et NF S 61-970 et, d'autre part, des vérifications de mise en œuvre.

Il doit établir une déclaration d'installation attestant de la conformité de ses travaux et un document indiquant les résultats obtenus lors des essais par autocontrôle pour chacun des matériels dont il a la responsabilité d'installation.

4 DESCRIPTION DES OUVRAGES COURANTS FORTS

4.1 RÉSEAU DE TERRE

Le présent lot devra réaliser la mise à la terre de toutes les masses métalliques mises en place dans le cadre de ses travaux.

Tous les matériels spécifiés dans la norme NF C15-100 devront être mis à la terre. Cette mise à la terre sera réalisée par le lot fournissant le matériel à mettre à la terre à partir des attentes de terre mises à disposition

4.2 ALIMENTATION COURANTS FORTS

Le présent lot devra assurer l'alimentation électrique de ses installations depuis les tableaux généraux en basse tension de chaque site ou des tableaux divisionnaires dans le cas d'aménagement des locaux (PC de sécurité

4.3 EXTENSION DES TABLEAUX ELECTRIQUES

Les disjoncteurs de protection seront du type modulaire équipé de déclencheurs magnétothermiques de même marque que l'existant. Le type de disjoncteur sera déterminé en fonction du courant de court-circuit pouvant se développer à l'intérieur du tableau. Le type de déclencheur sera déterminé de façon à assurer en priorité la protection des personnes.

Le câblage au niveau de chaque tableau est à prévoir depuis le jeu de barres ou répartiteur jusqu'aux bornes de distribution.

Il sera prévu une sélectivité totale sur l'ensemble de la chaîne de distribution électrique.

DEPART	DISJONCTEURS	LIMITES
Eclairage	2 x10 A-DDR 300 mA	10 points lumineux max.
PC standard	2x16 A-DDR 30 mA	8 PC max.
PC détournée poste de travail	2 x16 A-DDR 30 mA type Si/Hpi	6 PC max.
Equipement de sureté	2 ou 4 pôles DDR 300mA (Pour les alimentations directes),	1 disjoncteur par équipement
	2 ou 4 pôles DR 30 mA (pour les alimentations sur des PC).	1 disjoncteur par équipement

Les schémas des armoires devront être mis à jour à la fin des travaux.

En complément des dispositifs de protection contre les effets indirects de la foudre par protections parafoudres suivant le guide UTE 15-443 sont à prévoir

Les parafoudres modulaires seront fournis, posés et câblés avec protection par coupe-circuit, assurant la protection des équipements électriques et électroniques contre les surtensions transitoires d'origine atmosphérique et industrielle.

Le circuit alimentant le parafoudre doit être protégé contre les courts circuits et les surcharges par un disjoncteur, respectant les sélectivités.

Les parafoudres répondant à la norme NF EN 61643-11 et permettant d'utiliser la totalité de la protection foudre sont précisés dans le tableau de fonctionnement suivant.

Les équipements sensibles sont à équiper de protection foudre (parafoudre) de type 3.

4.4 RÉSEAU HAUTE QUALITÉ

Les équipement des deux postes de travail (principal et secondaire) seront équipées d'une alimentation sans interruption de type onduleur permettant de couvrir les besoins avec une autonomie 15 minutes à pleine charge.

Localisation

- Au rdc dans le local PCS – Bâtiment DSDEN 1 quai Dujardin.
- Au rdc service DAGE – Bâtiment du rectorat 96 rue d'Antrain.

4.5 CANALISATIONS

La distribution comprendra les éléments suivants :

- Les alimentations depuis les tableaux électriques TD seront réalisées par des câbles sans halogène FR-N1 X1 G1-1000V

Les sections de câbles et les conditions de mise en œuvre seront conformes aux prescriptions de la norme NF C15-100.

Ils seront fixés sur chemins de câbles existants présents dans les plénum des plafonds (démontage ou accessible depuis des trappes). Dans le cas contraire les câbles sont installés sous conduits rigides de type IRL dans les locaux techniques et sous moulure PVC dans les locaux nobles ou circulations sans faux-plafond.

Des plinthes ou goulottes multi-compartiments de type préfabriquée en PVC blanche 9010, 2 ou 3 compartiments, section 130/160x50 mm, 2/3 couvercles en PVC de même nature seront utilisées dans le cadre de l'aménagement du local PCS ou dans les locaux recevant les équipements centraux du contrôle d'accès et de l'alarme intrusion.

4.6 GOULOTTE DE DISTRIBUTION

Les goulottes électriques seront de type monobloc type Ensto ou équivalent avec les caractéristiques suivantes :

- Goulotte préfabriquée en PVC blanche 9010, 2 compartiments, section 130x50 mm, 2 couvercles en PVC de même nature.
- Accessoires associés de la gamme (embouts, angles variables, cloisons de séparation, tés, agrafes, jonctions de fond et de couvercle, joints ...).
- Clipsage direct de l'appareillage au format 45x45. Pour garantir une utilisation optimum l'appareillage sera format 45x45, conforme à la norme IEC 60884-1, simple, double ou triple, à 33° ou 90° d'inclinaison, couleurs au choix ainsi que la possibilité de format détrompé.
- Conforme CE, catégorie M1, IP40 et IK09.



Cette goulotte électrique pourra être fixée en plinthe ou en allège dans les différents locaux possédant des postes de travail. Elle permettra le passage des différents courants forts et faibles, sera symétrique, garantira l'anti-arrachement de l'appareillage de même marque, et sera livrée avec un film de protection intégrale.

L'entreprise devra se rapprocher du lot cloison afin d'apporter le plus grand soin quant à la mise en place des plinthes électriques afin qu'elles soient alignées par rapport aux supports muraux.

4.7 BOUCHAGE DES PERCEMENTS

Pour l'ensemble des percements, le présent lot doit le rebouchage avec un produit coupe-feu, le calfeutrement devra reconstituer le degré coupe-feu de la paroi traversée par un produit agréé compatible avec le support.

4.8 EQUIPEMENT DES LOCAUX

Le présent lot devra l'aménagement du local PC sécurité de la DSDEN comprenant:

- Les disjoncteurs de protection dédié pour ce local (éclairage et PC) depuis le tableau électrique de zone rdc y compris le câblage associé.
- L'éclairage normal
- L'équipement du local (appareil d'éclairage, commande d'éclairage et prises de courant)
- L'éclairage de sécurité (en ambiance)

- Les prises courants faibles (RJ45) – Se référer au chapitre câble VDI.
- Le mobilier recevant le matériel constituant le poste principal d'exploitation

4.8.1 APPAREIL D'ÉCLAIRAGE INTERIEUR


L'éclairage devra répondre aux règles en vigueur et, notamment les recommandations de l'AFE, les règles AFNOR et le règlement de sécurité contre l'incendie dans les Etablissements recevant du public.

Les terminaux seront de technologie à LED et s'intégreront parfaitement dans les trames de faux plafond (600*600mm). Les luminaires seront raccordés/asservis à des détecteurs de présence de type infrarouge dont le flux lumineux sera régulé sur un niveau d'éclairement déterminé par un dispositif de régulation embarqué au sein du luminaire. Les niveaux d'éclairement proposés dans le cadre du projet sont par défaut ceux de la norme NF EN 12464-1.

Le niveau d'éclairement est le suivant:

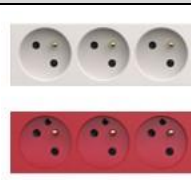
DESIGNATION DU LOCAL			
	ECLAIREMENT MOYEN (LUX)	SURFACE DE CALCUL PLAN DE RÉFÉRENCE	FACTEUR D'UNIFORMITE D'ÉCLAIREMENT
Bureau poste de sécurité	300 niveau général 500 sur le plan de travail	Plan utile 0.7m	0.6


L'éclairage devra garantir une uniformité supérieure à 0,7 (E min. / E moy.) à hauteur du « plan de travail » et un rendu des couleurs supérieur à 0,80. Le taux d'éblouissement unifié (U.G.R.) sera inférieur à 19 dans tous les locaux (hors locaux techniques).

DESIGNATION	LOCALISATION	PHOTO
Encastré pour plafond 600x600, 24w, 3400 lumens, 4000K, UGR16, IRC>80, SDCM<3, convertisseur Dali. Modèle Powerbalance GEN2 Philips ou équivalent	Bureau PCS – Encastré en plafond	

4.8.2 APPAREILLAGE

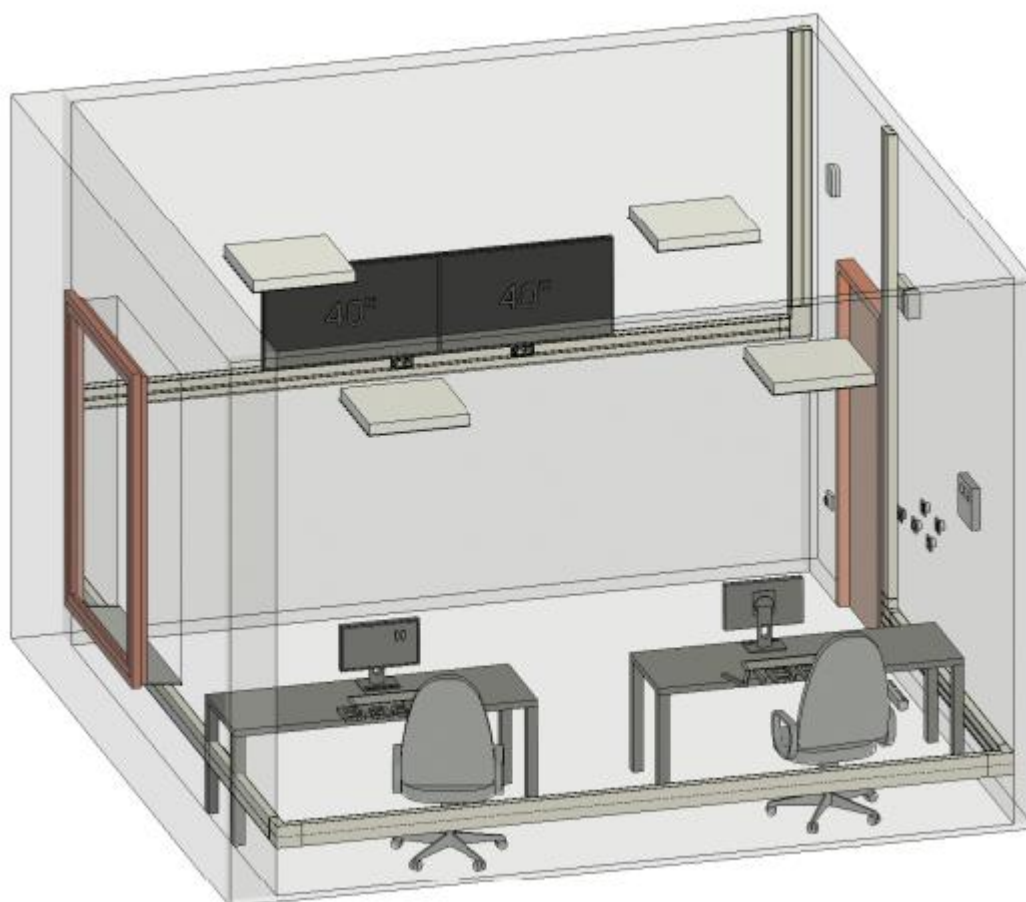
L'appareillage comprend les prises de courant et les organes de commande de l'éclairage.

DESIGNATION	LOCALISATION	PHOTO
Appareillage blanc à clipsage directe 45 x 45 33° : IP 40, IK04. Modèle Mosaic 45 Legrand ou équivalent	Appareillage monté sur goulottes, boîtier de sol.	

DESIGNATION	LOCALISATION	PHOTO
Appareillage standard blanc : IP21D, IK 04 Modèle Mosaic 45 Legrand	Appareillage mural	

5 DESCRIPTION DU MOBILIER DU PCS

L'équipement en mobilier à prévoir dans le local PC de sécurité permettra de regrouper l'ensemble du matériel d'exploitation du matériel de sûreté (poste informatique, écrans d'exploitation et de visualisation), clavier, souris et encodeur de badge.



Caractéristiques des pupitres fixe :

- Structure et porte en métal avec plateau en dérivé de bois
- Longueur de 1200 mm de longueur (la longueur exacte sera définie en fonction de l'implantation).
- Profondeur 750mm (la profondeur exacte sera définie en fonction des besoins)
- Hauteur : 750mm fixe
- Mât support écran pour aligner des écrans verticalement (2 unités)
- Passages de câble intégré
- Coloris blanc

Modèle FIX EVO1 Augeron ou équivalent



Caractéristiques des fauteuils:

- Fauteuil ergonomique réglable en hauteur par vérin gaz,
- Angle d'inclinaison de -6° à +19°,

- Coussin d'assise interchangeable, rembourrage confort plus pour une confort d'assise optimal pour de longues périodes (8 heures)
- Piètement 6 branches en étoile avec roulettes de grande taille,
- Garantie 5 ans.

Modèle OP85 Nexee ou équivalent

6 TRAVAUX DE DEPOSE

Le present lot devra la depose de l'ensemble des installations existantes non conservées à savoir:

- Alarme intrusion
- Contrôle d'accès
- Vidéo-surveillance
- Canalisation et câble de toute nature,
- Etc

Elle devra le rebouchage soignée de les trous ou percements occasionnés pour les travaux de dépose compris enduit de finition.

Cette liste est non exhaustive et l'entreprise devra se rendre sur place pour évaluer la nature de cette prestation.

L'entreprise ne devra pas perdre de vue que les travaux seront réalisés dans un établissement en activité. De ce fait, les travaux devront être planifiés avec la Maîtrise d'œuvre et les exploitants, afin de minimiser les gênes occasionnées par les travaux à réaliser, de même que les installations devront être réalisées de sorte qu'elles puissent, à l'avenir, être reprises et réorganisées aisément, mais aussi s'intégrer et intégrer les équipements et câblages déjà existants sur le site.

L'exécution de ces travaux devra tenir compte des exigences de l'établissement, des règles de sécurité vis à vis du public, afin de ne pas entraver l'accès à certains locaux ou les issues de secours.

Tous les travaux de coupure électrique que ce soit au niveau des sources d'alimentation (TGBT, tableaux électriques) ou sur chaque départ devront se faire suivant une planification qui devra recevoir l'accord avec la Maîtrise d'œuvre et les exploitants.