

C.C.T.P.
Cahier des Clauses Techniques Particulières

Dossier de Consultation des Entreprises

Sécurisation de la DISP
123 rue Nationale BP 765 à LILLE 59034



Maître d'ouvrage :
Direction Interrégionale des Services Pénitentiaires de Lille 123
rue Nationale - BP 765 à LILLE 59034

**Lot 1 : VIDEO SURVEILLANCE, CONTROLE D'ACCES,
INCENDIE, ANTI INTRUSION**

Edition du 13/04/2026
Rédacteur : Kévin LAURENT

Sommaire

01.1	DOCUMENTS DE REFERENCE.....	3
01.2	NETTOYAGES.....	3
01.3	PROTECTION DES OUVRAGES EXECUTES	3
01.4	CONTROLE INTERNE.....	3
01.5	CONDITIONS TECHNIQUES D'EXECUTION DES TRAVAUX.....	3
01.6	PLANS D'EXECUTION ET DE RECOLEMENT	4
01.7	PRESTATIONS GENERALES A LA CHARGE DES ENTREPRISES	5
01.8	RELATIONS AVEC LES ADMINISTRATIONS ET SERVICES	5
01.9	QUALITE DES MATERIAUX, STOCKAGES ET MISES EN OEUVRE	5
01.10	SECURITE ET PROTECTION DE LA SANTE SUR LE CHANTIER.....	5
01.11	TRANCHES DE TRAVAUX.....	6
01.12	NOTATIONS UTILISEES DANS LE CCTP.....	6
01.13	DEFINITION DU CCTP.....	7
01.14	GARANTIES ANNUELLE, BIENNALE ET/OU DECENNALE	7
02.2	DESCRIPTION DES TRAVAUX	7
02.2.2	ETUDES DE CHANTIER.....	7
02.2.3:	EXIGENCES RELATIVES A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL (RGPD)	7
02.2.4:	EXIGENCES DEMANDE PAR LA DGAP	9
02.2.5	LOT 1 MISE EN SECURITE DE LA DISP (VIDEO SURVEILLANCE, CONTROLE D'ACCES, INCENDIE, ANTI INTRUSION) (TRANCHE FERME).....	15
	ANNEXES.....	42

01.1 DOCUMENTS DE REFERENCE

Les travaux seront exécutés conformément aux règles de l'art et à la réglementation française telle qu'elles se trouveront être en vigueur un mois avant la date d'établissement de l'offre.

En particulier, les travaux seront conformes aux prescriptions techniques contenues dans les lois, décrets, arrêtés et circulaires applicables en France, ainsi que dans les cahiers des clauses techniques générales, les documents techniques unifiés (cahier des charges, cahier des clauses spéciales, cahier des clauses techniques, mémento), les normes, les DTU, les avis techniques, les exemples de solutions.

01.2 NETTOYAGES

Au cours des travaux, le chantier devra être tenu en parfait état de propreté par chaque intervenant. Chaque entrepreneur est chargé de l'enlèvement de ses gravois, chaque fois que leur volume l'exigera ou à la demande du maître d'œuvre ou du maître de l'ouvrage. Il doit le nettoyage parfait des locaux dans lesquels il travaille ou qu'il emprunte pour l'exécution de ses travaux. En fin de travaux, les nettoyages définitifs seront faits par l'entreprise.

01.3 PROTECTION DES OUVRAGES EXECUTES

L'entrepreneur est tenu pour responsable des ouvrages de son lot et en doit la protection jusqu'à la réception. Il doit donc les protéger contre les risques de détérioration, de vol ou de détournement. De plus, pendant l'exécution de ses propres travaux, il doit prendre les précautions nécessaires pour ne pas causer de dégradation aux matériaux ou ouvrages des autres entrepreneurs, ni au reste des locaux.

Si des détériorations sont constatées en cours de chantier elles seront réparées aux frais de l'entrepreneur responsable, à charge pour lui de se faire couvrir par son assurance.

Si l'auteur des dégradations ne peut être identifié, la remise en état sera à la charge du compte prorata. Ces réparations ou remises en état, quoique étant exécutées pendant le délai contractuel, n'entraîneront pas d'augmentation de ce délai.

01.4 CONTROLE INTERNE

En début de chantier, l'entrepreneur donnera le nom de la personne chargée d'assurer le contrôle des matériaux et de leur mise en œuvre. Le contrôle interne auquel sont assujetties les entreprises doit être réalisé à différents niveaux :

- Au niveau des fournitures, quel que soit leur degré de finition, l'entrepreneur s'assurera que les produits commandés et livrés sont conformes aux normes et spécifications complémentaires éventuelles du marché.
- Au niveau du stockage, l'entrepreneur s'assurera que celles de ses fournitures qui sont sensibles aux agressions des agents atmosphériques et aux déformations mécaniques sont convenablement protégées.
- Au niveau de l'interface entre corps d'état, l'entrepreneur vérifiera tant au niveau de la conception que de l'exécution, que les ouvrages à réaliser ou à exécuter par d'autres corps d'état permettent une bonne réalisation de ses propres prestations.

01.5 CONDITIONS TECHNIQUES D'EXECUTION DES TRAVAUX

Tous les ouvrages doivent être réalisés avec les matériaux ou fournitures de la meilleure qualité dans l'espèce indiquée avec mise en œuvre dans les règles de l'art, tant au point de vue technique qu'au point de vue esthétique.

01.5.1 ACCES CHANTIER

Les travaux seront réalisés en site occupé, et soumis aux contrôles de sécurité par les personnels de l'établissements

Une copie des cartes d'identité des intervenants sera demandée au moins 1 semaine avant tout accès pour contrôle.

Les personnels des entreprises retenues devront être identifiables à tout moment par leurs vêtements et de leurs cartes professionnelles

Le site ayant un nombre de places très limité pour le stationnement des véhicules, la priorité sera donnée aux véhicules devant décharger les matériaux en quantité, lourds et encombrants. Les autres véhicules devront stationner sur l'espace public.

01.5.2 SECURITE DES MATERIELS ET MATERIAUX

La zone des travaux étant dans un site à risque particulier, il est important de prendre en compte que tout matériel ou matériaux peut être considéré sensible. Un local sera mis à disposition pour stocker les matériels ou matériaux. Des stockages journaliers seront autorisés sur les zones d'intervention avec le balisage autour.

01.5.3 ECHAFAUDAGES- NACELLES - MONTAGE DES MATERIAUX

Le prix global proposé par les entrepreneurs comprendra la valeur des échafaudages, agrès, engins d'élévations, etc., nécessaires à l'exécution des travaux de leur propre lot. Il prendra également compte des contraintes dues au cheminement de la conception du bâtiment. Pour toutes utilisation d'espace sur la voie publique l'entreprise aura en charge l'ensemble des démarches administratives.

01.5.4 TROUS, SCCELLEMENT ET MENUS OUVRAGES

L'entreprise doit prévoir toutes les incorporations au gros-œuvre. Elle réserve, à ses frais, tous les percements, scellements, dégradations dues aux travaux, etc.. et remises en état le cas échéant y compris calfeutrement réglementaire.

01.5.5 TRAITS DE NIVEAU

L'entreprise de gros-œuvre a la charge et la responsabilité des traits de niveau, de l'implantation et de la borne repère jusqu'à l'achèvement de l'ouvrage.

01.6 PLANS D'EXECUTION ET DE RECOLEMENT

L'entrepreneur respectera la charte graphique de la DISP fournie dans le dossier de consultation.

01.6.1 PLANS D'EXECUTION

Tous les plans d'exécution sont à la charge des entreprises. Ces plans devront être établis en coordination avec les autres lots et suffisamment tôt pour qu'ils soient examinés et approuvés par le maître d'œuvre de la réalisation et le Bureau de Contrôle. Ces plans d'exécution devront d'autre part respecter très fidèlement les côtes du dossier d'appel d'offres, sauf dérogation. Toute erreur ou omission affectant ce dossier devra être signalée au Maître d'Ouvrage dans l'offre initiale, faute de quoi leurs conséquences financières éventuelles seront à la charge exclusive de l'entreprise.

01.6.2 PLANS DE RECOLEMENT

Après exécution de ses travaux, l'entrepreneur de chaque lot technique devra remettre au Maître d'Ouvrage un tirage d'un dossier complet des ouvrages exécutés et la fourniture du même dossier sur clef USB, y compris fiches techniques notice descriptive de fonctionnement des équipements. (DOE)

01.7 PRESTATIONS GENERALES A LA CHARGE DES ENTREPRISES

Qu'elles figurent ou non dans le corps du descriptif détaillé, les prestations ci-après sont dues par les entreprises attributaires et sont réputées comprises dans le montant du marché :

- La visite des lieux et la prise en compte de toutes les sujétions d'exécution
- La prise en compte de tous les éléments relatifs à l'ensemble du lot
- Les installations de chantier propres à chaque entreprise, y compris baraques de chantier, hangars de stockage, etc.
- Si le CCTP le prévoit, l'établissement et la fourniture d'un exemplaire papier et un numérique des plans de récolement des ouvrages exécutés selon les prescriptions du maître d'œuvre.
- La participation aux réunions de chantier dès lors que l'entrepreneur y aura été invité par la MOE.
- La participation aux réunions de chantier dès lors que l'entrepreneur y aura été invité par le maître de l'ouvrage

01.8 RELATIONS AVEC LES ADMINISTRATIONS ET SERVICES

Toutes démarches ou déclarations auprès des services de la CNIL, d'électricité de France, gaz de France, opérateur téléphonique, Compagnie des Eaux, Services Techniques de la Ville, etc. sont à la charge de l'entreprise, y compris les travaux demandés par ces mêmes services pour permettre le bon déroulement et l'achèvement complet de la réalisation.

Le prestataire participera et devra assistance de la maîtrise d'ouvrage à la rédaction des dossiers administratifs réglementaires auprès des autorités de référence

Les frais de dossiers éventuellement demandés par ces Services sont à la charge de l'entreprise.

01.9 QUALITE DES MATERIAUX, STOCKAGES ET MISES EN OEUVRE

01.9.1 MATERIAUX

Il ne sera prévu que des matériaux traditionnels ou des matériaux non traditionnels ayant fait l'objet d'un avis technique du C.S.T.B ou d'une enquête spécialisée d'un bureau de contrôle et acceptés en garantie par le S.T.FC

01.9.2 ESSAIS COPREC

L'entrepreneur ne pourra exécuter ses travaux qu'après accord du Bureau de Contrôle sur la conception de ses ouvrages.

Il procédera au contrôle interne auquel il est assujéti au niveau des fournitures, du stockage et de la mise en œuvre ainsi qu'aux essais et vérifications figurant sur la liste en vigueur établie par le COPREC et en accord avec les assurances.

Les résultats de ces vérifications et essais devront être consignés dans des procès-verbaux suivant les formes prévues par le document technique n° 2 COPREC (octobre 1998, Moniteur du 6 novembre 1998). Ces procès-verbaux devront être envoyés, pour examen, au Bureau de Contrôle, en double exemplaire.

01.10 SECURITE ET PROTECTION DE LA SANTE SUR LE CHANTIER

01.10.1 GENERALITES

Les entrepreneurs veilleront scrupuleusement au respect des règles de sécurité concernant le travail des ouvriers, la protection des baies libres, trémies, etc. Les dispositions réglementaires de protection, d'hygiène et de sécurité seront conformes aux prescriptions des lois, décrets, arrêtés et règlements en vigueur.

Les indications figurant dans les documents établis par le coordonnateur S.P.S. seront rigoureusement respectées. Tous les travaux nécessaires au respect des spécifications concernant la sécurité et la santé sont réputés compris dans l'offre de l'entreprise

La mission globale du coordonnateur SPS pour une opération de construction comprend les éléments de mission conformes à la loi n° 93-1418 du 31 décembre 1993 et aux décrets n° 94-1159 du 26 décembre 1994 et n° 95-543 du 4 mai 1995.

La mission confiée au coordonnateur SPS par le maître d'ouvrage se décompose en éléments de mission précisés au présent chapitre.

Le coordonnateur SPS de conception assure le passage des consignes et la transmission des documents au coordonnateur SPS de réalisation de l'ouvrage lorsque celui-ci est différent. La mission du coordonnateur SPS comprend les éléments mentionnés au paragraphe ci-dessous.

01.10.2 MISSIONS POUR UNE OPERATION DE 3° CATEGORIE

01.10.2.1 Phase Conception

- Coordination de la mise en œuvre des principes généraux de prévention,
- Création et tenue du Registre Journal (RJ) de la coordination définie à l'article R.238.19,
- Constitution et mise au point du Dossier d'Intervention Ulérieure (DIU) sur l'ouvrage, défini aux articles L.235.15 et R.238.37 à R.238.39,
- Examen des dispositions à prendre par les entreprises pour que seules les personnes autorisées puissent accéder au chantier.

01.10.2.2 Phase Réalisation

- Coordination de la mise en œuvre des principes généraux de prévention,
- Organisation des inspections communes avec les différentes entreprises, y compris sous-traitantes, qu'elles se trouvent ou non présentes ensemble sur le chantier, où sont traités la coordination de leurs activités simultanées ou successives, les modalités de leur utilisation en commun des installations, matériels et circulations verticales et horizontales, leur information mutuelle ainsi que l'échange entre elles des consignes en matière de sécurité et de protection de la santé,
- Mise à jour et tenue du Registre Journal de la coordination au fur et à mesure du déroulement de l'opération, définies à l'article R.238.19,
- Mise à jour et adaptation du Dossier d'Intervention Ulérieure sur l'ouvrage, définies aux articles L. 235.15 et R.238.37 à R.238.39 et remise finale contre procès-verbal, accompagné du dossier de maintenance des lieux de travail fourni par le maître d'ouvrage (art. R.235.5).

01.11 TRANCHES DE TRAVAUX

La décomposition en tranches de travaux suivante est prévue :

	Sans objet

0

01.12 NOTATIONS UTILISEES DANS LE CCTP

Le présent CCTP fait appel aux conventions de notation suivantes :

01.12.1 MARQUES COMMERCIALES

Il est parfois indiqué, dans le corps du descriptif, des noms de marques commerciales. Les entreprises sont tenues de s'en tenir aux produits spécifiés. Cependant, dans le cadre de marchés publics, les entreprises ont le droit de proposer et de mettre en œuvre des produits qui soient techniquement et esthétiquement équivalents aux ouvrages décrits dans le CCTP Sauf accord préalable du Maître Ouvrage, toute autre modification des prestations sera refusée, tous les frais de remplacement étant à la charge de l'entreprise défaillante.

01.13 DEFINITION DU CCTP

Le Cahier des Clauses techniques Particulières (CCTP) vient préciser l'ensemble des prestations que l'entrepreneur doit prévoir dans son offre. L'entreprise devra notamment comprendre dans son offre, sous peine de nullité :

- L'ensemble des études et travaux nécessaires au parfait achèvement des ouvrages
- La découverte d'erreurs ou d'omissions dans le descriptif établi par le maître d'œuvre, celui-ci devant être immédiatement informé de ces erreurs ou omissions ; dans tous les cas, l'entreprise s'engage à effectuer l'intégralité des travaux prévus au devis descriptif ou représentés sur les plans.
- Lorsque le quantitatif est établi par le maître d'œuvre, le contrôle des quantités. Si aucune observation n'est présentée à ce sujet à ce sujet lors de la remise des offres, l'entreprise ne pourra prétendre à quelque réajustement que ce soit concernant les quantités effectivement mises en œuvre. Toute omission en limite de prestations entre corps d'état sera à la charge de l'entreprise. Dans le cas d'une réhabilitation, toutes les cotes portées aux plans sont à vérifier sur place avant commande de fourniture ou travaux.

01.14 GARANTIES ANNUELLE, BIENNALE ET/OU DECENNALE

L'entrepreneur garantit formellement la conformité de ses ouvrages à la réglementation nationale en matière de construction.

Cette garantie, d'une durée d'un an, implique le remplacement dans les plus brefs délais, de toute partie d'ouvrage reconnue défectueuse, ainsi que la remise en état pendant cette période de tout élément qui se serait détérioré dans des conditions d'utilisation normale.

Les fournitures et les réparations faites seront garanties pendant un nouveau délai d'un an, et dans les mêmes conditions que lors des travaux initiaux.

Par ailleurs, la date de réception avec ou sans réserve constitue l'origine de la garantie biennale et/ ou décennale des ouvrages, pour application des articles 1792 et 2270 du Code Civil

02.2 DESCRIPTION DES TRAVAUX

Lot 01 mise en sécurité de la Disp (vidéo surveillance, contrôle d'accès, incendie, anti intrusion)

02.2.1 INSTALLATION DE CHANTIER

- Un espace commun aux entreprises sera mis a disposition par la DISP celui-ci servira de bureau et de vestiaire. Pour se restaurer un réfectoire est disponible sur place afin permettre de réchauffer ses aliments par micro-onde et de s'asseoir. Distributeur et machine a café son disponible également. Le bâtiment dispose également de douches et sanitaires qui seront mis a disposition. Pour toutes réunion une demande devra être faite en amont au chargé d'opération afin que celui-ci consulte la disponibilité des salles.

02.2.2 ETUDES DE CHANTIER

Les plans d'implantation souhaité vous seront fourni exclusivement le jour de la visite obligatoire

02.2.2.1 Plans d'exécution des ouvrages

- Réalisation des plans d'exécutions des ouvrages
- Ceux-ci seront à faire valider avant réalisation des
- travaux

02.2.3: Exigences relatives à la protection des données à caractère personnel (RGPD)

Le soumissionnaire devra démontrer que la solution proposée est, **dans sa globalité**, conçue pour garantir une conformité totale avec le cadre légal relatif à la protection des données à caractère personnel. Cela inclut le respect des principes fondamentaux du Règlement (UE) 2016/679 (RGPD) dès la conception (by

design) et par défaut (*by default*), de la loi n° 78-17 modifiée, ainsi que des délibérations et recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL).

À ce titre, le présent article détaille les exigences techniques et fonctionnelles impératives sur lesquelles la DISP de Lille porte une attention **particulière**. Le soumissionnaire devra fournir, dans son mémoire technique, un **dossier de conformité RGPD** détaillé démontrant, point par point, comment sa solution répond non seulement à ces exigences spécifiques, mais aussi, plus largement, à l'ensemble des obligations du RGPD applicables au contexte du traitement. Ce dossier inclura la documentation technique, les certifications éventuelles, les schémas d'architecture et toute preuve jugée utile.

02.2.31 Exigences spécifiques aux dispositifs de vidéosurveillance

Le soumissionnaire devra démontrer que la solution proposée garantit le respect des principes suivants :

1. Sécurité et intégrité du système :

- Le soumissionnaire décrira précisément les mesures mises en œuvre pour assurer la **sécurité physique** des installations (ex: protection des caméras contre le vandalisme, sécurisation du câblage, préconisations pour l'installation des serveurs en local technique sécurisé).
- Il détaillera les mesures de **sécurité logique** visant à protéger l'intégrité du système et des données contre toute ingérence ou accès non autorisé. Celles-ci devront inclure, à minima :
 - Le **chiffrement des flux vidéo** entre les caméras et les serveurs d'enregistrement (chiffrement de bout en bout).
 - Le **chiffrement des données stockées** sur les serveurs.
 - Une politique de **mots de passe robustes** et de renouvellement régulier pour l'administration du système.
 - La possibilité de **segmenter le réseau** pour isoler le système de vidéosurveillance.
 - La **journalisation** de tous les accès et opérations sur le système.

2. Gestion de la captation sonore :

- Le soumissionnaire devra prouver que la captation sonore est **désactivée par défaut** sur l'ensemble des dispositifs.
- Il décrira le mécanisme technique permettant une **activation ponctuelle, manuelle et tracée** de l'enregistrement audio par un agent spécifiquement habilité, uniquement en cas d'événement exceptionnel le justifiant (ex: agression). La solution doit garantir qu'une activation automatique ou permanente est techniquement impossible.

3. Gestion de la durée de conservation :

- Le système devra permettre un **paramétrage strict de la durée de conservation** des images, qui ne pourra excéder 30 jours. Le soumissionnaire démontrera que la purge des données est **automatique et irréversible** à l'issue de la durée configurée.
- Il prouvera que la durée de conservation est indépendante de la capacité de stockage technique du système.
- La solution devra intégrer une fonctionnalité d'**extraction sécurisée et tracée** des enregistrements, permettant de les conserver pour la durée d'une procédure disciplinaire ou pénale, après consignation de l'opération.

02.2.32 Exigences spécifiques aux dispositifs de contrôle d'accès biométrique

Le soumissionnaire devra démontrer que sa solution est conçue pour respecter les exigences les plus strictes en matière de biométrie, conformément à la délibération CNIL n° 2019-001 et aux recommandations de l'ANSSI.

1. Stockage des gabarits biométriques :

- La solution devra impérativement reposer sur un **stockage des gabarits sous la maîtrise exclusive de la personne concernée** (stockage dit « de type 1 »). Le soumissionnaire précisera les supports proposés (ex: carte à puce, badge sécurisé).
- Il devra prouver que le support individuel (badge) est conçu pour qu'il soit **techniquement impossible d'extraire, de copier ou de reconstituer le gabarit biométrique** qui y est stocké. Il fournira les certifications de sécurité associées (ex: Critères Communs EAL4+).

2. Architecture et traitement des données :

- Le soumissionnaire devra prouver que l'architecture proposée **exclut toute base de données biométriques centralisée**. Le serveur de contrôle d'accès se limitera à la gestion des droits associés aux identifiants des badges, sans jamais avoir accès aux gabarits.
- Il démontrera que l'image de l'empreinte captée par le lecteur pour la comparaison est **immédiatement et automatiquement effacée de toute mémoire volatile** après l'opération de vérification, conformément à l'article 6.1 de la délibération CNIL n° 2019-001.

3. Processus de comparaison ("Match") :

- Le processus de vérification biométrique devra s'effectuer localement. Le soumissionnaire devra privilégier une architecture de type « **Match-on-Card** » (comparaison réalisée au sein de la puce sécurisée du badge).
- Si une architecture « Match-on-Reader » est proposée, le soumissionnaire devra apporter la preuve formelle que le gabarit n'est jamais exposé en clair et ne transite pas sur le réseau.

4. Sécurité des communications :

- Conformément à l'Article 32 du RGPD et aux bonnes pratiques de sécurité, le soumissionnaire devra garantir l'intégrité et la confidentialité de la chaîne de communication.
- L'utilisation du protocole **OSDP v2 (ou supérieur) avec canal sécurisé (Secure Channel) activé est impérative** pour chiffrer les échanges entre les lecteurs biométriques et les contrôleurs de porte (UCP). Le soumissionnaire devra prouver la compatibilité de son matériel avec cette exigence.

02.2.4: Exigences demandé par la DGAP

02.2.4.1 la VIDEOSURVEILLANCE :

- EXG_PHY_085

Aucun support amovible, à l'exception des supports vierges tels que CD-ROM ou DVDROM, ne peut être introduit par les utilisateurs dans les postes d'exploitation des systèmes de sûreté. Une protection physique sera mise en place sur le poste ou le poste sera déporté dans un local technique non accessible aux utilisateurs.

- EXG_CAC_051

Chaque utilisateur doit posséder un compte d'accès qui dispose des droits et privilèges strictement nécessaires à son profil sur les systèmes de sûreté.

En gros, par ces deux exigences, je souhaite que l'accès aux ports USB ne soit accessible qu'à certains utilisateurs, pour ma part il y a 3 types d'utilisateurs :

- L'administrateur qui a accès à tout le système
- Un compte qui permet de brancher une clé USB pour faire des extractions
- Un compte d'utilisation et de relecture simple

Dans Windows on peut gérer différents utilisateurs appartenant à ces groupes.

On peut adapter le fait de ne pas utiliser de compte nominatif par cette exigence :

- EXG_CAC_065

Les modalités d'utilisation d'un compte générique doivent garantir qu'un compte générique ne peut pas être utilisé sans qu'on puisse identifier, à posteriori, la personne ayant réalisé une action par le biais de ce compte.

Donc en gros, il faudra la mise en place d'un registre à notre niveau et respecter :

- EXG_CAC_066

- Ainsi, ces comptes génériques techniques et fonctionnels doivent être assignés aux seuls groupes de personnes autorisées et leur utilisation doit être strictement encadrée avec l'application des exigences suivantes :
- La liste exhaustive de ces comptes doit être consignée, accompagnée des mots de passe, et doit être mis sous scellé et au coffre du responsable du site pour en garantir la disponibilité, l'intégrité et la confidentialité ;

- EXG_VDS_04

Les interfaces d'administration locale des caméras doivent être désactivées.

- EXG_PHY_087

Les postes d'exploitation sont des écrans déportés ou des postes fixes. Les postes nomades ne sont pas autorisés comme postes d'exploitation.

- EXG_EXP_151

- Un contrôle antivirus local doit être effectué sur tous les serveurs, recevant des fichiers depuis l'extérieur (support amovible, réseaux externes...), et les postes de d'exploitation.
- Les fichiers de signatures pourront être mis à jour une fois par mois si la connexion avec l'extérieur est une connexion temporaire. Les fichiers de signature d'un système connecté en permanence à l'extérieur devront, en revanche, être mis à jour quotidiennement.

- EXG_EXP_351

Toutes les actions portées sur les systèmes doivent être journalisées.

- EXG_EXP_357

Un système de supervision doit permettre de détecter les dysfonctionnements d'un équipement ou d'un système dédié au SI, notamment si cet équipement ou ce système est utilisé pour une application d'une disponibilité supérieur ou égal au niveau D2.

- EXG_EXP_358

Le temps d'archivage des journaux des applications doit être défini pour chaque application.

- EXG_EXP_354

Toutes les actions d'administration sur les systèmes de sûreté doivent être journalisées.

- EXG_EXP_256

L'administration à distance (hors site) des postes d'exploitation et des serveurs utilisés pour les systèmes de sûreté n'est pas autorisée.

- EXG_CAC_151

Les outils de prise de main à distance sont interdits sur les systèmes de sûreté.

- EXG_CAC_153

Pour se prémunir de tentatives d'usurpation d'une connexion réseau filaire active, un contrôle des ports des commutateurs réseaux basé sur l'adresse réseau bas niveau (adresse MAC) de la ressource connectée est mis en œuvre avec le blocage temporaire du port en cas de changement intempestif de la ressource connectée.

- EXG_EXP_251

Les réseaux dédiés à la « sûreté pénitentiaire » (vidéosurveillance, remontées d'alarmes, Biométrie, etc.) doivent physiquement être séparés des réseaux dits réseaux de « gestion » (RPVJ).

- EXG_EXP_252

Chaque système de sûreté doit être isolé sur un réseau logique (VLAN) qui lui est propre afin de ne pas perturber les autres systèmes en cas de dysfonctionnement et de pouvoir assurer une qualité de service de certains systèmes.

- EXG_EXP_253

Les équipements actifs, ne sont pas situés dans les mêmes baies que les équipements actifs utilisés pour les réseaux de gestion, doivent être sécurisés par les services gestionnaires de ces équipements par un contrôle d'accès réseau adapté à la maturité de l'établissement (notamment blocage des ports de l'équipement actif par MAC ADRESS).

- EXG_VDS_11

L'architecture en série est proscrite.

- EXG_VDS_12

L'architecture à plat est proscrite.

- EXG_VDS_13

Les communications sans fils (Wifi, Bluetooth, non exclusivement) des caméras doit obligatoirement être désactivé (physiquement ou matériellement).

- EXG_VDS_14

Le système doit être totalement hermétique aux réseaux externes

- EXG_EXP_051

Les clauses du contrat liant le service gestionnaire à l'AP doivent intégrer à minima les exigences de sécurité suivantes et le respect des besoins de sécurité du système tel qu'identifié par la DAP :

- Intégrité : Le système ou les données mis à la disposition ou sous la responsabilité du prestataire ne doivent pas être modifiés sans autorisation ;

- Disponibilité : Le système ou les données mis à la disposition ou sous la responsabilité du prestataire ne doivent pas être rendus indisponibles sans autorisation ;
- Confidentialité : Le système ou les données mis à la disposition ou sous la responsabilité du prestataire ne doivent pas être divulgués sans autorisation ;
- Traçabilité : Les modifications apportées sur le système doivent pouvoir être détectées et revues.

02.2.4.2 LE CONTROLE D'ACCES :

- EXG_CAP_01

Les têtes de lecture doivent comporter des éléments de protection tels que l'effacement des clés ou le déclenchement d'une alarme en cas d'arrachement.

- EXG_CAP_02

L'administration directe des têtes de lecture doit être désactivée.

- EXG_CAP_03

Les données relatives au droit d'accès et les périodes de validité ne doivent pas être stockées sur le badge.

- EXG_CAP_04

Le badge doit pouvoir être réaffecté à une autre personne sans perte de traçabilité.

- EXG_CAP_05

Le numéro unique de traçabilité du badge doit être visible sur le support.

- EXG_CLA_001

Pour chaque système dont la durée de conservation n'est pas détaillée, le commanditaire doit fixer le délai pendant lequel les journaux d'événement doivent être conservés et la nature des informations à conserver, après consultation du Correspondant Informatique et Liberté (CIL) de la DAP et déclaration auprès de la CNIL si ces traces contiennent des données nominatives (identifiant de connexion, adresse IP d'une machine du réseau...).

- EXG_CLA_002

Par défaut, ou pour tout système sensible, les journaux d'événements sont conservés au minimum durant 6 mois.

- EXG_CAC_051

Chaque utilisateur doit posséder un compte d'accès qui dispose des droits et privilèges strictement nécessaires à son profil sur les systèmes de sûreté.

En gros, par ces deux exigences, je souhaite que l'accès aux ports USB ne soit accessible qu'à certains utilisateurs, pour ma part il y a 3 types d'utilisateurs :

- L'administrateur qui a accès à tout le système
- Un compte qui permet de brancher une clé USB pour faire des extractions
- Un compte d'utilisation et de relecture simple

Dans Windows on peut gérer différents utilisateurs appartenant à ces groupes.

On peut adapter le fait de ne pas utiliser de compte nominatif par cette exigence :

- EXG_CAC_065

Les modalités d'utilisation d'un compte générique doivent garantir qu'un compte générique ne peut pas être utilisé sans qu'on puisse identifier, à posteriori, la personne ayant réalisé une action par le biais de ce compte.

Donc en gros, il faudra la mise en place d'un registre à notre niveau et respecter :

- EXG_CAC_066

- Ainsi, ces comptes génériques techniques et fonctionnels doivent être assignés aux seuls groupes de personnes autorisées et leur utilisation doit être strictement encadrée avec l'application des exigences suivantes :
- La liste exhaustive de ces comptes doit être consignée, accompagnée des mots de passe, et doit être mis sous scellé et au coffre du responsable du site pour en garantir la disponibilité, l'intégrité et la confidentialité ;

02.2.4.3 Travail dans les zones sécurisées (salle serveur)

- EXG_PHY_009

Tous les accès doivent être journalisés (en entrée et si possible en sortie), les personnes qui accèdent à ces salles doivent être identifiées nominativement.

- EXG_PHY_010

La liste des personnes ayant accédé aux locaux techniques doit être contrôlée périodiquement par le responsable du local et au minimum une fois par an, en interne AP par le RISSI.

- EXG_PHY_011

Les locaux techniques hébergeant des serveurs de systèmes de sûreté doivent voir l'accès restreint aux seules personnes autorisées. Un système d'ouverture par badge en entrée et en sortie doit être mis en place.

- EXG_PHY_012

Un sas à entrer unique doit être prévu afin de garantir la traçabilité des personnes présentes dans les locaux techniques.

- EXG_PHY_013

Les interventions de personnes autorisées de façon ponctuelle dans les salles informatiques hébergeant les composants critiques et sensibles du système d'information doivent se faire accompagner d'une personne habilitée qui doit, en particulier, s'assurer que ces personnes n'effectuent que les actions pour lesquelles l'accès à la salle leur a été donné.

- EXG_PHY_014

Le contrôle d'accès aux bâtiments hébergeant des ressources informatiques ou des points d'accès à ces ressources est régi par les dispositions correspondantes de la PSO de la DAP sur le contrôle d'accès physique aux bâtiments.

- EXG_PHY_019

Les prises réseaux doivent empêcher toute connexion d'un équipement non autorisé. Pour cela une protection de reconnaissance des adresse NAC (Network Access Control) ou MAC (Media Access Control -selon la maturité du site-) devra être envisagée sur les différentes prises réseaux.

- EXG_PHY_051

Le câblage informatique doit être protégé contre tout accès malveillant pouvant conduire à des écoutes ou des dégradations.

- EXG_CAP_06

Les têtes de lecture ne doivent fonctionner qu'avec une distance maximale de 5cm.

- EXG_CAC_151

Les outils de prise de main à distance sont interdits sur les systèmes de sûreté.

- EXG_CAC_153

Pour se prémunir de tentatives d'usurpation d'une connexion réseau filaire active, un contrôle des ports des commutateurs réseaux basé sur l'adresse réseau bas niveau (adresse MAC) de la ressource connectée est mis en œuvre avec le blocage temporaire du port en cas de changement intempestif de la ressource connectée.

- EXG_EXP_252

Chaque système de sûreté doit être isolé sur un réseau logique (VLAN) qui lui est propre afin de ne pas perturber les autres systèmes en cas de dysfonctionnement et de pouvoir assurer une qualité de service de certains systèmes.

- EXG_EXP_253

Les équipements actifs, ne sont pas situés dans les mêmes baies que les équipements actifs utilisés pour les réseaux de gestion doivent être sécurisés par les services gestionnaires de ces équipements par un contrôle d'accès réseau adapté à la maturité de l'établissement (notamment blocage des ports de l'équipement actif par MAC ADRESS).

- EXG_EXP_053

Le développement des systèmes les plus critiques doivent être homologués à minima CSPN qui peut être étendue à une qualification EAL3+ (critères communs, fiabilité des fonctionnements) sur demande du comité d'homologation, ainsi qu'une homologation SIL2 (sûreté de fonctionnement).

- EXG_CAP_08

Le badge doit être homologué EAL4+ a minima.

02.2.5 lot 1 MISE EN SECURITE DE LA DISP (VIDEO SURVEILLANCE, CONTROLE D'ACCES, INCENDIE, ANTI INTRUSION) (Tranche ferme)

Le système de contrôle d'accès (interphonie compris de l'entrée du site) et de vidéo surveillance devra être opérable depuis plusieurs postes repartis sur le bâtiment.

Le contrôle d'accès des portes ou grilles devant être modifié ou ajouté, une coordination et collaboration avec le titulaire du lot 2 menuiserie métallique et l'ascensoriste sera obligatoire.

- Grille extérieur accès sous-sol / RDC 1 ventouse 300Kg + 1 bouton de sortie + DM + 1 lecteur carte
- Grille d'entrée piéton, ventouse de 600 kg + renforcement du support ventouse+ 1 bouton de sortie + DM + 1 lecteur carte
- Par poste prévoir 2 prises 230 v + une RJ 45 (une prise pour l'écran, une pour le PC)
4 écrans sont repartis sur différents niveaux 1 écrans 43" et 3 de 65"-70 "
- Les caméras sont en 360° sauf 3, un fixe et deux motorisé, pour la couverture de toutes les circulations
- La porte d'entrée du local serveur se fermera avec deux ventouses de type vortex, + 1 bouton de sortie + DM + 1 lecteur carte
- La grille du local serveur sera sur 2 ventouses de type vortex + 1 bouton de sortie + DM + 1 lecteur biométrique
- Porte (dsi/desp) sera sur 2 ventouses de type vortex + 1 bouton de sortie + DM + 1 lecteur biométrique + un interphone avec un récepteur par service pour avertir la DESP ET LE DSI DEV
- Mise en place d'un contrôle d'accès ventouse 300kg avec équerre sur chaque porte palière et des bureaux désignés.
- Remplacement des bandeaux ventouse existant par des nouveaux bandeaux en 2 x 300kg et remplacement également de toutes les ventouses simples déjà existante
- Des têtes incendie seront à ajouter sur un bureau au 1^{er} étage : 4 têtes incendie dans le pôle PSE
- Les ascenseurs seront compris dans le protocole de contrôle d'accès
- Mise en place d'une alarme sonore en cas d'ouverture de la porte de secours du DPIPFR et du RDC
- L'interphonie contrôlable des postes jumelé avec la vidéo et le contrôle d'accès.
- 400 cartes vierge, 300 type biométrique et 100 classiques seront fournies
- Prévoir câblerie informatique en CAT 7 de couleur Orange pour la vidéo et violet pour le contrôle d'accès
- Pour le soir et Week end et jour férié prévoir mettre signal sonore quand une caméra détecte quelqu'un dans des zones définies sur des plages horaires définies.
- Switch pilotable dédié pour le système de sécurité
- Création d'un protocole pour mettre le contrôle d'accès sur les cartes professionnelles de l'administration pénitentiaire
- Les ventouses de la salle serveur, porte entrée DSI/DESP, portes de bureau du 1^{er} ; 2 -ème étage et du 6eme devront être secourues sur batteries
- Pour 3 des portes en contrôle d'accès un DM vert par porte sera à rajouté dans un coffret fermant à clef dans un local sécurisé
- Un extracteur d'air simple sera à installer afin de ventiler un local onduleur
- Le rideau métallique et toutes portes choisies devront être commandables à distance via l'interface du contrôle d'accès.
- Un bouton numérique de maintien d'ouverte du sas sera à créer sur l'interface du contrôle d'accès. En plus des commandes physiques existantes.
- L'alarme intrusion actuelle sera à changer, des points supplémentaires en plus de l'existant seront à ajouter
- Un module GSM de transmission des alarmes incendie et intrusion sera à installer
- Petits travaux de CFO/CFA afin de bouger des équipements existants dans la nouvelle organisation.
- Les switch seront à programmer avec les consignes fournis par le service du DSI
- Le titulaire du lot devra prévoir quelques lots de dalles de faux plafond afin de remplacer les dalles endommager par l'ancienne installation ou d'éventuelles problématiques lors de l'installation du nouveau système
- En cas d'incendie les portes palières devront être automatiquement libérées.

L'entreprise titulaire du lot, devra garantir le fonctionnement du contrôle des accès à chaque fin de journée sur les entrées et sorties du bâtiment.

Le titulaire du lot devra inclure dans son chiffrage le démontage et retrait des anciens équipements, la Disp récupérera la station de sauvegarde et l'écran de contrôle.

Le titulaire du lot aura à charge la totalité des modifications de l'installation CFO/CFA et travaux connexes nécessaires au fonctionnement du nouveau système et installation et devra les inclure à son offre.

Pour le contrôle d'accès DM = déclencheur manuel vert + vitre + plombs plastique

02.2.5.1 La Vidéo Surveillance.

La typologie de caméra souhaité sera en annexe.

Attendu pour la vidéo surveillance :

1. Introduction

Ce cahier des charges définit les exigences pour une solution logicielle de gestion vidéo (VMS) basée sur la plateforme Network Optix Nx VMS, version 6.0.x/24.1.x. Cette solution doit répondre aux besoins spécifiques du projet de la DISP en assurant la surveillance et la gestion des vidéos provenant de caméras IP.

2. Exigences Générales

- **Plateforme ouverte et extensible:** La solution VMS doit être une plateforme ouverte et extensible, compatible avec une variété d'appareils et de systèmes tiers.
- **Intégration transparente:** La solution doit inclure des APIs et des SDK pour faciliter l'intégration d'appareils et de systèmes tiers.
- **Architecture multiplateforme:** L'architecture de la solution doit comprendre des applications de bureau, de serveur et mobiles pour une accessibilité et une gestion flexibles.
- **Assurance qualité:** Le fournisseur doit fournir une documentation technique complète sur les produits et les données techniques, accessible en ligne.
- **Soumissions de propositions:** Les propositions de solution doivent inclure une documentation technique complète sur tous les matériaux et équipements utilisés dans le projet.
- **Soutien et garantie:** La solution doit être garantie pour les pièces, le matériel et la main d'oeuvre pendant au moins un an à compter de la date d'acceptation finale du système de vidéosurveillance.

3. VMS

3.1 Vue d'ensemble

La solution VMS doit être composée de trois applications logicielles qui fonctionnent de manière transparente :

- **Serveur:** Un service multiplateforme léger et performant chargé de la découverte des appareils, de l'enregistrement des flux, de la diffusion vidéo et d'autres données aux clients, et de l'établissement de connexions sécurisées.
- **Client Bureau:** Une application client multiplateforme légère et performante capable d'agir comme un lecteur multimédia autonome, un client connecté pour configurer et gérer des appareils et des données, ou un mur vidéo.
- **Client Mobile:** Une application mobile légère avec des capacités limitées de configuration, de gestion et de visualisation des appareils et des données.

3.2 Outils de développement et d'intégration VMS

La solution VMS doit disposer d'outils de développement intégrés :

- **Générateur d'événements génériques:** Permet de construire des appels d'événements génériques HTTP pour déclencher des actions système dans le VMS.

- **API Serveur:** Une API HTTP CRUD REST permettant d'accéder aux données du système, du serveur, de la vidéo, de l'audio, du proxy, de WebSocket, et de gérer l'authentification et le cryptage.
- **Client (API Java Script):** Permet aux développeurs d'intégrer des applications web dans le navigateur intégré.
- **SDK d'intégration des sources vidéo:** Permet d'intégrer pratiquement n'importe quelle source vidéo dans le VMS.
- **SDK de stockage:** Permet d'intégrer n'importe quel type de stockage dans un système.
- **SDK de métadonnées:** Permet d'intégrer l'analyse vidéo pilotée par l'objet pour obtenir les coordonnées de l'objet et les métadonnées associées.

3.3 Architecture VMS

- **Architecture en ruche de serveurs:** Tous les serveurs d'un système sont égaux et synchronisent les bases de données en temps réel.
- **Mises à jour en un seul clic:** Les administrateurs de système doivent pouvoir mettre à niveau un système entier à l'aide d'un seul bouton.
- **Sécurité des communications:** Le VMS doit utiliser des technologies sécurisées pour la communication et la sécurité entre les applications.
- **Licences:** Le VMS ne doit pas nécessiter de licences supplémentaires pour augmenter le nombre de dispositifs, d'utilisateurs ou de serveurs.
- **Capacités du système:** Le système doit s'adapter aux tailles maximales recommandées sans assistance technique ni licence supplémentaire.

4. Application VMS Serveur

4.1 Systèmes d'exploitation pris en charge:

- Microsoft Windows (Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022)
- Ubuntu Linux (Ubuntu 20.04 LTS, Ubuntu 22.04 LTS)
- macOS (Client de bureau uniquement)
- Cartes de développement ARM / Debian (Appareils NVIDIA Jetson, Périphériques Raspberry Pi à partir de Raspberry Pi 4)
- Plateformes de virtualisation / conteneurisation (VMWare, VirtualBox, Docker)

4.2 Exigences matérielles minimales:

- Le serveur VMS doit pouvoir enregistrer 256 caméras IP à double flux sur un seul coeur de processeur Intel Core i3.

4.3 Installation et Configuration:

- L'application VMS Server doit pouvoir être téléchargée gratuitement et être accessible au public.
- L'application du serveur VMS ne doit pas nécessiter de logiciel propriétaire ou tiers lors de l'installation.
- Le processus d'installation doit être simple et ne nécessiter aucune intervention de l'utilisateur.

4.4 Fonctionnalités:

- **Découverte automatique des appareils:** L'application serveur doit découvrir automatiquement les caméras IP ONVIF pro fil S sur le même sous-réseau.
- **Support des flux RTSP, HTTP ou UDP:** L'application serveur doit découvrir et enregistrer des flux RTSP, HTTP ou UDP manuellement.
- **Connexions simultanées:** L'application serveur doit prendre en charge jusqu'à 1 000 connexions TCP simultanées.
- **Enregistrement et diffusion vidéo:** L'application serveur doit enregistrer et diffuser en continu des vidéos de n'importe quelle résolution et fréquence d'images, limitées uniquement par le matériel.

- **Basculement automatique des caméras:** L'application serveur doit prendre en charge le basculement automatique des caméras sans licence supplémentaire.
 - **Gestion des utilisateurs et des rôles:** L'application VMS Server prend en charge un nombre illimité d'utilisateurs et de rôles d'utilisateurs personnalisés.
 - **Support du stockage:** L'application VMS Server prend en charge tout type de support de stockage - disques durs, disques SSD, cartes SD, DAS, NAS ou autres dispositifs de stockage connectés au réseau.
 - **Intégration LDAP / Active Directory / OpenLDAP:** L'application serveur doit prendre en charge l'intégration pour la gestion des identifiants de connexion des utilisateurs.
 - **Enregistrement et diffusion audio:** L'application serveur doit enregistrer et diffuser des flux audio AAC, PCM (Mu-Law, A-law), g726 et MP3.
 - **Transcodage à la demande:** L'application serveur doit transcoder les flux à la demande.
 - **Stockage des index d'archives:** L'application serveur doit stocker les index d'archives au même endroit que les fichiers vidéo enregistrés.
 - **Réindexation des archives:** L'application serveur doit permettre aux administrateurs système de récupérer les archives à partir de n'importe quel support de stockage.
 - **Moteur d'événements booléens:** L'application serveur doit contenir un moteur d'événements booléens permettant aux opérateurs de programmer et de déclencher des actions du système.
 - **Requêtes HTTP:** L'application serveur doit pouvoir envoyer des requêtes HTTP PUT ou GET à des systèmes ou dispositifs tiers.
 - **IPv4 ou IPv6:** L'application serveur doit prendre en charge l'adressage IPv4 ou IPv6.
 - **Configuration d'acheminement réseau:** L'application serveur doit permettre aux opérateurs de définir des configurations d'acheminement réseau personnalisées.
 - **Surveillance de l'état du serveur:** L'application VMS Server doit permettre aux opérateurs de surveiller en temps réel l'utilisation du CPU, de la RAM, du NIC et du HDD.
 - **Suivi des actions de l'opérateur:** L'application VMS Server doit permettre de suivre toutes les actions de l'opérateur.
 - **Fichiers de crash automatiques:** L'application VMS Server doit générer des fichiers de crash automatiques en cas de crash inattendu.
-
- **Gestion de l'espace disque:** L'application VMS Server doit permettre aux opérateurs de modifier la taille de l'espace disque réservé aux unités de stockage.
 - **Désactivation automatique des lecteurs système:** L'application VMS Server doit automatiquement désactiver tout lecteur système dans le matériel informatique comportant plus d'un lecteur.
 - **Contacts d'E/S binaires:** L'application VMS Server doit prendre en charge la configuration et les événements provenant de contacts d'E/S binaires sur les dispositifs pris en charge.
 - **Notifications par courrier électronique:** L'application VMS Server doit prendre en charge l'envoi de notifications par courrier électronique via SMTP.
 - **Sauvegarde programmée des archives:** L'application VMS Server doit prendre en charge la sauvegarde programmée des archives d'enregistrement.
 - **Sauvegarde à la demande des archives:** L'application VMS Server doit permettre la sauvegarde à la demande des archives d'enregistrement.
 - **Enregistrement simultané sur plusieurs serveurs:** L'application VMS Server doit permettre l'enregistrement simultané de toutes les caméras et de tous les flux connectés sur deux (2) serveurs en temps réel.
 - **Analyse de mouvement côté serveur:** L'application VMS Server doit permettre l'analyse de mouvement côté serveur, basée sur le processeur, pour toutes les caméras IP connectées.
 - **Interface d'administration web:** L'application VMS Server doit disposer d'une interface d'administration web qui permet aux utilisateurs de visionner des vidéos en direct ou enregistrées.

- **Surveillance de l'état du serveur (interface web):** L'application VMS Server doit disposer d'une interface d'administration web qui permet aux administrateurs système de visualiser en temps réel les statistiques de surveillance de l'état du serveur.
- **Gestion des serveurs (interface web):** L'application VMS Server doit disposer d'une interface d'administration web qui permet aux utilisateurs de visualiser tous les serveurs disponibles dans le système.
- **Paramètres avancés du système (interface web):** L'application VMS Server doit disposer d'une page avancée cachée qui permet aux administrateurs de système de modifier les paramètres avancés du système.
- **Support des configurations RAID:** L'application VMS Server doit prendre en charge toute configuration RAID du stockage.
- **Acquisition et stockage de métadonnées:** Le serveur VMS doit prendre en charge l'acquisition et le stockage de métadonnées orientées objet.
- **Cryptage des archives:** Le serveur VMS doit prendre en charge le cryptage des archives à l'aide d'une clé définie par l'utilisateur et d'un cryptage AES 128 bits.
- **Épinglage de certificats SSL/TLS:** Toutes les connexions au serveur VMS doivent utiliser l'épinglage de certificats SSL/TLS.

5. Application VMS Client

5.1 Systèmes d'exploitation pris en charge:

- Microsoft Windows (Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022)
- Ubuntu Linux (Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS)
- Apple macOS (macOS 11, macOS 12, macOS 13)
- ARM / Debian Developer Boards (NVIDIA Jetson Devices)

5.2 Exigences matérielles minimales:

- L'application VMS Client doit pouvoir fonctionner sur tout matériel capable d'exécuter un système d'exploitation compatible avec un processeur supportant OpenGL 2.1 et Intel HD Graphics 3000 (ou plus).
- L'application VMS Client ne doit pas nécessiter de lecteur graphique dédié pour fonctionner à pleine capacité.

5.3 Installation et Configuration:

- L'application VMS Client doit pouvoir être téléchargée gratuitement et être accessible au public.
- L'application VMS Client ne doit pas nécessiter de logiciels propriétaires ou de tiers lors de l'installation.
- Le processus d'installation doit être simple et ne nécessiter aucune intervention de l'utilisateur.

5.4 Fonctionnalités:

- **Structure de base de l'interface:** L'application VMS Client doit présenter une structure de base avec un panneau de navigation, un panneau des ressources, un panneau des notifications, un panneau chronologique et une grille de visualisation.
- **Support des types de médias:** L'application VMS Client doit permettre aux opérateurs de visualiser et d'interagir avec les types de médias suivants : flux en direct, médias hors ligne, dispositifs d'E/S et serveur.
- **Défilement et zoom:** L'application VMS Client doit permettre à l'opérateur de faire défiler l'écran pour zoomer sur n'importe quelle partie de la grille de visualisation.
- **Glisser-déposer des caméras:** L'application VMS Client doit permettre à l'opérateur de réaffecter des caméras d'un serveur à un autre par glisser-déposer.
- **Calendrier flexible:** L'application VMS Client doit disposer d'un calendrier flexible permettant aux opérateurs de visualiser les dates de toutes les vidéos archivées.

- **Signets:** L'application VMS Client doit permettre aux opérateurs de créer des signets manuellement ou automatiquement à l'aide du moteur de règles.
- **Moteur de règles:** L'application VMS Client doit permettre aux opérateurs de créer des automatismes à l'aide du moteur de règles avec les événements et actions suivants : événements définis par l'utilisateur, événements par défaut, événements générés par le système, signets, sorties d'appareils, enregistrements de panique, sons, courriels, notifications mobiles, notifications sur le bureau, schémas d'alarme, texte superposé, parler, écriture dans le journal.
- **Déclencheurs logiciels:** L'application VMS Client doit permettre aux opérateurs de créer des déclencheurs logiciels pour déclencher toute action disponible dans le système.
- **Icônes de contrôle des caméras:** L'application VMS Client doit comporter des icônes permettant aux opérateurs de déformer les caméras fixe, de contrôler les caméras PTZ, d'appliquer une amélioration de l'image côté client, d'exécuter une recherche de mouvement intelligente, de créer des fenêtres de zoom, de faire pivoter les éléments et d'activer les informations sur les flux ou les fichiers.
- **Fenêtres de zoom:** L'application VMS Client doit permettre aux opérateurs de créer des fenêtres de zoom.
- **Recherche Smart Motion:** L'application VMS Client doit permettre aux opérateurs d'effectuer une recherche Smart Motion.
- **Recherche des caméras:** L'application VMS Client doit permettre aux utilisateurs de rechercher des caméras en direct par nom, fabricant, adresse IP, adresse MAC et état.
- **Recherche dans les archives vidéo:** L'application VMS Client doit permettre aux opérateurs d'effectuer des recherches dans les archives vidéo par date et heure.
- **Personnalisation de l'image d'arrière-plan:** L'application VMS Client doit permettre aux opérateurs de personnaliser l'image d'arrière-plan de l'application.
- **Cartographie numérique:** L'application VMS Client doit prendre en charge la cartographie numérique.
- **Mise à l'échelle adaptative:** L'application VMS Client doit utiliser une technologie de mise à l'échelle adaptative pour basculer automatiquement entre les flux haute et basse résolution.
- **Passage rapide d'un système à l'autre:** L'application VMS Client doit permettre aux opérateurs de passer rapidement d'un système à l'autre.
- **Analyse du stockage:** L'application VMS Client doit disposer d'une fonction d'analyse du stockage permettant aux opérateurs d'analyser la capacité de stockage du système.
- **Gestion des dispositifs, utilisateurs et ressources:** L'application VMS Client doit permettre de gérer et de configurer tous les dispositifs, utilisateurs et ressources du système dans une interface unique et unifiée.
- **Avance et retour rapide des vidéos archivées:** L'application VMS Client doit permettre l'avance et le retour rapide des vidéos archivées.
- **Indication du serveur de connexion:** L'application VMS Client doit indiquer aux opérateurs à quel serveur du système ils sont connectés.
- **Connexions à des versions antérieures:** L'application VMS Client doit permettre aux opérateurs de se connecter à des versions antérieures.
- **Découverte automatique des systèmes:** L'application VMS Client doit découvrir automatiquement les systèmes disponibles sur le même réseau que l'ordinateur qui exécute l'application client.
- **Reconnect automatique:** L'application VMS Client doit récupérer automatiquement et se reconnecter à un système dans le cas où le serveur auquel l'opérateur est connecté devient inaccessible.
- **Vignettes adaptatives:** L'application VMS Client doit permettre aux opérateurs d'afficher ou de masquer les vignettes adaptatives dans le panneau de la chronologie.
- **Synchronisation des éléments d'une disposition:** L'application VMS Client doit permettre de synchroniser tous les éléments d'une disposition ou de désactiver la synchronisation.
- **Boîtes de dialogue adaptatives:** L'application VMS Client doit disposer de boîtes de dialogue de paramétrage adaptatives.

- **Configuration par lots des caméras:** L'application VMS Client doit permettre de configurer par lots les horaires d'enregistrement des caméras, le nombre d'images par seconde et la qualité.
 - **Glisser-déposer de plusieurs ressources:** L'application VMS Client doit permettre de faire glisser et de déposer simultanément plusieurs ressources système sur la grille de visualisation.
 - **Synchronisation de l'heure:** L'application VMS Client doit permettre aux administrateurs de modifier les paramètres de synchronisation de l'heure.
 - **Liste des caméras et dispositifs:** L'application VMS Client doit permettre aux administrateurs du système de visualiser une liste complète des caméras et des dispositifs du système.
 - **Visualisation et exportation des événements:** L'application VMS Client doit permettre aux opérateurs de visualiser, de rechercher et d'exporter tous les événements du système.
 - **Visualisation et exportation des signets:** L'application VMS Client doit permettre aux opérateurs de visualiser, de rechercher et d'exporter tous les signets du système.
 - **Visualisation et exportation des journaux:** L'application VMS Client doit permettre aux opérateurs de visualiser, de rechercher et d'exporter les journaux du système.
 - **Piste d'audit des actions de l'opérateur:** L'application VMS Client doit permettre aux opérateurs de visualiser, de rechercher et d'exporter une piste d'audit de toutes les actions de l'opérateur.
 - **Sauvegarde et restauration de la base de données:** L'application VMS Client doit permettre aux administrateurs de sauvegarder et de restaurer la base de données du système.
 - **Remplacement d'une caméra:** L'application VMS Client doit permettre aux administrateurs de remplacer une caméra tout en conservant les archives de la précédente.
 - **Groupes d'utilisateurs prédéfinis:** L'application VMS Client doit fournir des groupes d'utilisateurs prédéfinis.
 - **Accès invité:** L'application VMS Client doit permettre aux invités d'accéder temporairement au système avec des autorisations limitées.
 - **Groupes d'utilisateurs personnalisés:** L'application VMS Client doit permettre aux administrateurs de créer un nombre illimité de groupes d'utilisateurs personnalisés et de définir les autorisations.
-
- **Layouts verrouillables:** L'application VMS Client doit permettre aux administrateurs de créer et de partager des layouts verrouillables.
 - **Mises à jour en temps réel des présentations:** L'application VMS Client doit permettre aux administrateurs de mettre à jour les présentations en temps réel.
 - **Enregistrement d'écran:** L'application VMS Client doit permettre aux utilisateurs d'enregistrer leur écran.
 - **Dossier local pour les fichiers locaux:** L'application VMS Client doit permettre aux utilisateurs d'ajouter un dossier local pour ajouter des fichiers locaux.
 - **Mode mur d'images:** L'application VMS Client doit disposer d'un mode mur d'images.
 - **Mode lecteur multimédia:** L'application VMS Client doit disposer d'un mode lecteur multimédia.
 - **Souvenirs des connexions antérieures:** L'application VMS Client doit se souvenir des connexions antérieures au système et des informations d'identification de l'utilisateur.
 - **Réglage du rapport hauteur/largeur et de la qualité des flux:** L'application VMS Client doit permettre aux opérateurs de régler le rapport hauteur/largeur et la qualité des flux des éléments affichés sur la grille de visualisation.
 - **Affichage des dispositifs d'E/S:** L'application VMS Client doit afficher les dispositifs d'E/S en tant qu'éléments individuels sur la grille de visualisation.
 - **Personnalisation des panneaux d'E/S:** L'application VMS Client doit permettre aux utilisateurs de personnaliser la disposition des panneaux d'E/S sur l'élément de la grille de visualisation.
 - **Déformation des objectifs fisheye:** L'application VMS Client doit permettre aux utilisateurs de déformer n'importe quel objectif fisheye.
 - **Circuits de visualisation personnalisables:** L'application VMS Client doit permettre de créer des circuits de visualisation entièrement personnalisables.

- **Présentation partagée:** L'application VMS Client doit permettre aux administrateurs système de modifier et d'enregistrer une présentation partagée.
- **Audio bidirectionnel:** L'application VMS Client doit prendre en charge l'audio bidirectionnel.
- **Alertes audio:** L'application VMS Client doit prendre en charge les alertes audio.
- **Préréglages et visites PTZ:** L'application VMS Client doit prendre en charge les préréglages et les visites PTZ.
- **Suivi d'objets en temps réel:** L'application VMS Client doit prendre en charge le suivi d'objets en temps réel.
- **Programmation d'enregistrement:** L'application VMS Client doit permettre aux opérateurs de programmer l'enregistrement pour les caméras et les appareils connectés.
- **Pré-enregistrement et post-enregistrement:** L'application VMS Client doit permettre aux opérateurs de configurer le pré-enregistrement et le post-enregistrement.
- **Optimisation de la qualité de diffusion:** L'application VMS Client doit permettre aux opérateurs d'optimiser la qualité de diffusion des caméras.
- **Exportation de vidéos:** L'application VMS Client doit permettre aux utilisateurs d'exporter des vidéos.
- **Fonction d'exportation rapide:** L'application VMS Client doit disposer d'une fonction d'exportation rapide.
- **Activation et désactivation des licences système:** L'application VMS Client doit permettre aux administrateurs système d'activer ou de désactiver les licences système.
- **Ouverture d'une présentation d'alarme:** L'application VMS Client doit permettre aux utilisateurs de forcer l'ouverture d'une présentation d'alarme déclenchée par un système ou un événement tiers.
- **Augmentation du nombre d'éléments sur la grille de visualisation:** L'application VMS Client doit disposer d'une méthode configurable cachée permettant d'augmenter le nombre d'éléments autorisés sur la grille de visualisation.
- **Configuration des dispositifs:** L'application VMS Client doit permettre aux utilisateurs de régler la configuration des dispositifs.
- **Raccourcis clavier:** L'application VMS Client doit prendre en charge les raccourcis clavier.
- **Analyse à partir de Wisenet et d'autres dispositifs compatibles:** Le VMS doit permettre l'analyse à partir de Wisenet et d'autres dispositifs compatibles.
- **Authentification initiale pour les caméras Wisenet:** L'application VMS Client doit obliger les utilisateurs à définir un mot de passe initial pour la caméra Wisenet.
- **Notifications push personnalisées:** L'application VMS Client doit permettre aux opérateurs de créer et d'envoyer des notifications push personnalisées.
- **Accès à la page web de la caméra:** L'application VMS Client doit permettre aux opérateurs d'accéder à une page web de la caméra.
- **Décodage Intel Quicksync côté client:** L'application VMS Client doit permettre aux utilisateurs d'activer le décodage Intel Quicksync côté client.
- **Connexions cryptées et archivage:** L'application VMS Client doit permettre aux opérateurs d'activer les connexions cryptées et l'archivage.

6. Application VMS - Client Mobile

6.1 Systèmes d'exploitation pris en charge:

- Google Android (Android 9, Android 10, Android 11, Android 12, Android 13, Android 14)
- Apple iOS (iOS 16, iOS 17, iPadOS 16, iPadOS 17)

6.2 Installation:

- L'application VMS Mobile doit être téléchargeable gratuitement sur Google Play ou Apple iTunes stores.

6.3 Fonctionnalités:

- **Découverte automatique des systèmes:** L'application VMS Mobile doit découvrir automatiquement les systèmes disponibles sur un réseau local (LAN).
- **Stockage des connexions et des identifiants:** L'application VMS Mobile doit stocker les connexions et les identifiants des systèmes précédents.
- **Flux adaptatif:** L'application VMS Mobile doit disposer d'un flux adaptatif et ajuster automatiquement le flux affiché en fonction de la vitesse du réseau.
- **Ajustement manuel de la résolution:** L'application VMS Mobile doit permettre aux utilisateurs d'ajuster manuellement la résolution des flux.
- **Recherche des caméras par nom:** L'application VMS Mobile doit permettre aux utilisateurs de rechercher des caméras par leur nom.
- **Dewarping fisheye:** L'application VMS Mobile doit permettre le dewarping fi sheye de n'importe quel objectif fi sheye.
- **Visualisation des vidéos en direct:** L'application VMS Mobile doit permettre aux utilisateurs de visionner des vidéos en direct.
- **Lecteur multimédia personnalisé:** L'application VMS Mobile doit utiliser un lecteur multimédia personnalisé.
- **Recherche des vidéos:** L'application VMS Mobile doit permettre aux utilisateurs de rechercher des vidéos à l'aide d'un calendrier et d'une chronologie flexible.
- **Smart Motion Search:** L'application VMS Mobile doit permettre la « Smart Motion Search ».
- **Contrôle des caméras à l'aide de déclencheurs logiciels:** L'application VMS Mobile doit permettre aux utilisateurs de contrôler les caméras à l'aide de déclencheurs logiciels.
- **Audio bidirectionnel:** L'application VMS Mobile doit prendre en charge l'audio bidirectionnel.
- **Navigation à l'aide de schémas partagés:** L'application VMS Mobile doit permettre aux opérateurs de naviguer à l'aide de schémas partagés.
- **Vignettes en direct:** L'application VMS Mobile doit présenter des vignettes en direct.
- **Contrôle des caméras PTZ:** L'application VMS Mobile doit permettre aux utilisateurs de contrôler les caméras PTZ.
- **Navigation dans les signets:** L'application VMS Mobile doit permettre aux utilisateurs de naviguer dans les signets.
- **8. Conclusion**
- Ce cahier des charges présente les exigences minimales pour la solution logicielle de gestion vidéo basée sur Network Optix Nx VMS. La solution doit répondre à tous les critères spécifiés pour garantir une surveillance et une gestion vidéo performantes et sécurisées.
- **9. Annexes**
- Liste des caméras IP et des dispositifs à intégrer dans le système.
- Schéma d'implantation du système.
- Calcul des exigences en matière de largeur de bande du réseau et de stockage.
-

02.2.5.2 Le contrôle d'accès/ anti intrusion/ interphonie

1. Description de la demande

Le présent descriptif a pour objet de décrire l'ensemble des prestations de fourniture et de mise en œuvre d'une solution de gestion globale des accès d'un site de type "Sensible".

La solution proposée devra être qualifiée par l'ANSSI.

Le site sera muni d'un système de contrôle d'accès, de détection intrusion et d'un outil de supervision global qui sera commun à l'ensemble des sous-systèmes de sûreté. Les dispositifs de contrôle d'accès et de détection intrusion répondront à une logique de zonage du site et de hiérarchisation des droits d'accès.

Le site intégrera également un système de vidéophonie IP.

L'objectif étant de permettre aux différents opérateurs, spécialisés ou non, de réaliser indifféremment de manière simple et transversale, toutes les fonctions liées :

- A l'exploitation des accès du site,
- Au maintien de sûreté des locaux,
- A la sécurité des personnes.

Elle sera dimensionnée de façon suffisante pour permettre la prise en charge et le traitement de différents types de population tel que :

- Visiteurs standard
- Visiteurs VIP
- Collaborateurs
- Mainteneurs
- Agents de sécurité
- Agents d'entretien
- Etc....

Le système proposé sera de marque **Synchronic** ou techniquement équivalent et sera impérativement un système centralisé temps réel.

Le système sera impérativement capable de centraliser la gestion de la sécurité, de plusieurs sites distants géographiquement.

Son exploitation offrira la simplicité d'un système dans l'optimisation des tâches et sera paramétrable par l'exploitant. Le système devra être particulièrement modulaire et extensible et devra aussi bien fonctionner sur une architecture de type BUS de terrain (RS485) que sur une architecture native TCP/IP.

Il sera basé sur une architecture à différents niveaux :

- Niveau 1 : Les terminaux terrain (têtes de lecture pour le contrôle d'accès, contacts, radars anti-intrusion, barrières Infra Rouges,...). Ce matériel ne pourra être propriétaire, il sera impérativement basé sur des standards du marché
- Niveau 2 : Les Concentrateurs et/ou Centrales permettant la gestion des périphériques en local et garantissant une autonomie de fonctionnement en cas de perte de réseau d'exploitation ou de serveur
- Niveau 3 : Le logiciel d'exploitation qui se devra convivial et permettra le paramétrage du système dans sa globalité et l'exploitation temps réel des différents « métiers » de la Sûreté souhaités (Contrôle d'accès, détection intrusion, GTB, Vidéosurveillance,...)

Les systèmes quelle que soit leur version devront être compatibles avec la suite logiciel Air'Evolution de marque Synchronic et devront pouvoir fonctionner nativement en mode MODBUS/TCP.

Les soumissionnaires veilleront donc à proposer une véritable suite logicielle dont les interfaces systèmes partagent une ergonomie, une structure, une iconographie et une signalétique identiques. Ces interfaces seront complétées par des scénarios configurables secondant l'opérateur par des tâches automatiques et/ou planifiées.

Les événements remontant d'un équipement lié à la sûreté comme le contrôle d'accès ou la vidéophonie devront avoir la capacité de générer des actions automatiques ou non avec l'ensemble des équipements de sûreté et de sécurité.

Dans ce but, il est demandé à l'Entreprise et au fournisseur industriel de la gestion des accès de s'engager dans sa disponibilité complète auprès du Maître d'Ouvrage jusqu'en phase de réception.

1.1. Acceptation des matériels et conformité des ouvrages

Tous les équipements constitutifs de la solution globale, logicielle et matériel terrain devront fournir une interopérabilité complète, avec notamment :

Pour la supervision :

- Interagir avec le contrôle d'accès
- Interagir avec la vidéophonie IP
- Interagir avec l'interphonie de sécurité
- Interagir avec l'anti-intrusion
- Interagir avec la vidéosurveillance
- Visualiser l'infrastructure SI des sous-systèmes de sûreté,
- ...

1.2. Documents à fournir

L'entreprise veillera à fournir les documents suivants.

Avec son offre :

- La marque et le type des matériels proposés,
- Les notices et documentations techniques se rapportant à ces matériels,
- Les fiches techniques démontrant l'interopérabilité des systèmes.
- Qualification ANSSI valide à la date de rendu de l'offre

Avant les travaux :

- Les échantillons de matériels proposés à la validation accompagnés de leurs FDES,
- Les notices techniques et notices de pose des matériels,
- Les P.V. de conformité aux normes et aux textes législatifs,
- Les plans d'exécutions et de calepinages,
- Le détail des ouvrages avec lesquels ils sont en contact ou avec lesquels ils s'intègrent et comprenant : organes de liaison, de fixation, etc.
- L'analyse fonctionnelle comprenant les différents scénarios et automatismes des sous-systèmes validés par le Maître d'Ouvrage.
- Qualification ANSSI valide à la date du lancement des travaux

A la réception des travaux :

- Notices d'entretien,
- Les plans d'exécution,
- Au titre des D.O.E. : Les P.V, rapports d'essais établis par le CNPP, notices techniques du fabricant, avis techniques, etc.
- Attestation de conformité d'installation et de paramétrage des ouvrages par le/les fabricants des sous-systèmes.

1.3. Nature des prestations

Au titre de son marché, le titulaire doit les prestations suivantes :

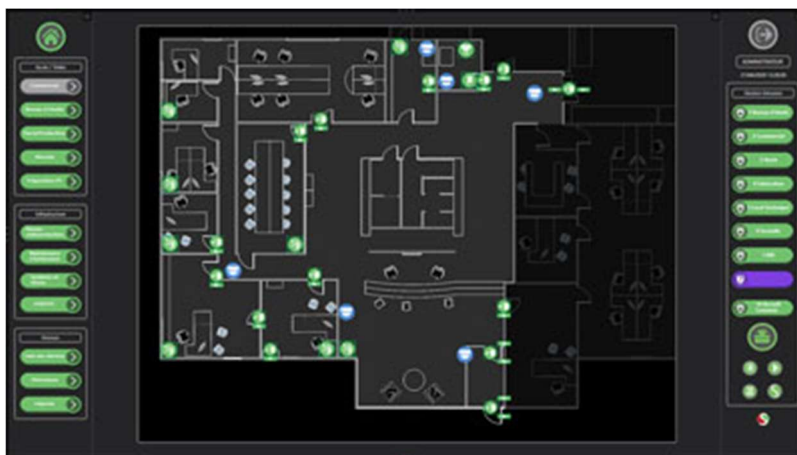
- Réalisation des études d'exécution, échantillons des matériels proposés,
- Définition et validation de l'implantation de l'ensemble des composants du système,
- Réalisation des démarches administratives nécessaires,
- Mise en place des procédures de communication externes,
- Interfaçage avec l'ensemble des systèmes neufs et existant (si besoin),
- Pose des systèmes,
- Réalisation des essais, tests préalables à la réception,
- Réception des ouvrages,
- Remise d'une analyse fonctionnelle du projet,

2. Solutions logicielles

Les logiciels proposés devront impérativement être compatibles avec les logiciels de la suite Air'Evolution de Synchronic (XT Manager, Horizon Evolution, Vision Evolution)

2.1. L'outil de supervision

Le poste de gestion et de supervision sûreté sera installé dans le PC sûreté. Il sera commun à l'ensemble des sous-systèmes de sûreté (contrôle d'accès, intrusion et vidéo surveillance). Le logiciel **Horizon Evolution** de marque **Synchronic** sera proposé (ou autre logiciel techniquement équivalent). Il offrira une interface de gestion unique pour l'opérateur afin de gérer l'ensemble des informations en provenance des différents équipements de sûreté.



Le logiciel devra impérativement permettre un nombre de plans illimités.

Il répondra aux spécifications techniques suivantes :

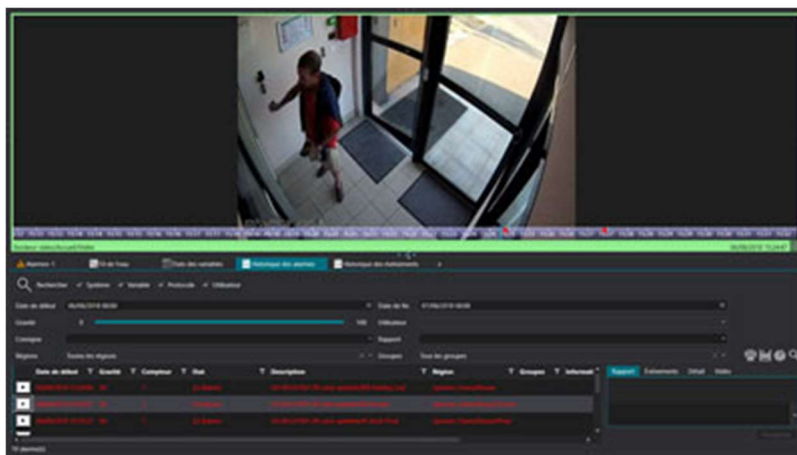
- Créer des vues graphiques sophistiquées pour visualiser l'état de l'installation,
- Archiver les événements dans une base de données pour pouvoir les analyser ultérieurement,
- Visualiser et contrôler la liste des alarmes en cours,
- Visualiser l'évolution des variables de supervision sous forme de courbes, en temps réel ou à partir des données enregistrées dans l'historique des événements,
- Calculer des statistiques sur les valeurs des variables supervisées,
- Importer et exporter des états et des historiques.

2.1.1. Le logiciel de supervision devra également intégrer les fonctionnalités suivantes :

Interfaçage vidéosurveillance

Une extension module vidéo pour Horizon Evolution, sera proposée. Elle permettra entre autres de réaliser les fonctionnalités suivantes :

- Visualiser sur une même interface les alarmes intrusions, les accès par badges et les caméras de vidéosurveillance,
- D'associer et de visualiser automatiquement sur alarme une ou plusieurs caméras de vidéo
- D'asservir les caméras motorisées aux alarmes,
- Relire les séquences vidéo associées aux déclenchements d'alarmes.



Interfaçage autres systèmes

Le superviseur graphique permettra un interfaçage des systèmes suivants :

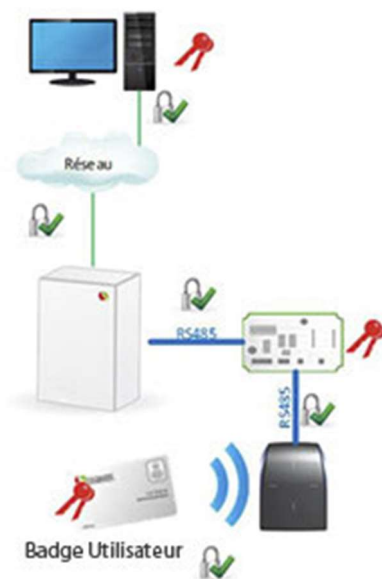
- Détection incendie
- Interphonie
- Alarme NFA2P

2.2. Le contrôle d'accès

2.2.1. La solution devra être conforme aux préconisations ANSSI

Le système proposé devra répondre en tout point aux préconisations de l'ANSSI qui précise entre autres les éléments suivants :

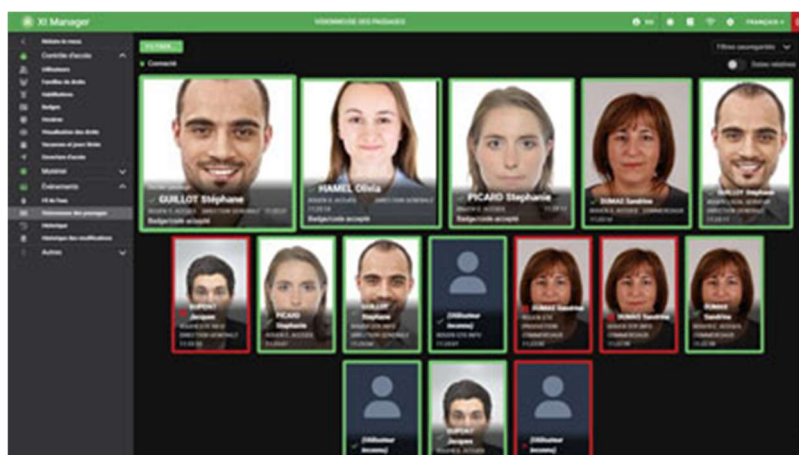
- L'authentification du badge doit reposer sur une clé commune ou une clé dérivée d'une clé maîtresse l'utilisation d'une puce Mifare DESFire est donc la solution la plus adaptée.
- Aucune information ne doit circuler en clair sur le canal sans fil et la liaison filaire, les liaisons de type Data-Clock/Wiegand sont donc à proscrire.
- La tête de lecture ne doit contenir aucun secret (niveau 1 ANSSI).



Architecture ANSSI n°1

Le logiciel d'administration du contrôle d'accès devra être fourni avec un module Secur'Evolution de marque Synchronic, ou techniquement équivalent. L'administration et le transfert des clés de chiffrements vers les lecteurs se feront de manière centralisée depuis le poste d'administration, toutes les solutions à base de badge de configuration à présenter devant chaque lecteur seront à proscrire. La solution devra permettre de gérer simultanément deux types de badge encodé différemment, soit avec deux applications distincts (AID) soit deux fichiers différents dans la même application, et ceci afin de permettre, de s'affranchir de toute compromission clé ou de renouvellement de clé. Il sera livré avec un lecteur USB pour l'enrôlement et l'encodage des badges utilisateurs.

2.2.2. Le logiciel d'administration



Le système devra être administré par une application web client/serveur de type **XT Manager de marque Synchronic** ou techniquement équivalent. Il devra fonctionner exclusivement depuis un navigateur web. Toute solution nécessitant l'installation d'une application client lourd ne sera pas retenue.

Il devra disposer d'une interface graphique conviviale et intuitive, en français et devra proposer une interface avec un thème clair et un thème sombre au choix de l'utilisateur.

L'encodage et l'enrôlement des badges devra obligatoirement être intégré depuis le client web.

Afin de garantir une interopérabilité du système, le logiciel de contrôle d'accès devra impérativement disposer d'une API REST via Webservice.

L'application de contrôle d'accès devra permettre la gestion centralisée du système de contrôle d'accès. Il devra être possible d'administrer depuis un point unique, un système dispersé sur plusieurs bâtiments ou plusieurs sites.

Les fonctionnalités essentielles du contrôle d'accès telles que :

- Connecteur à une base de données tierces , exemple LDAP(S)
- Comptage

Devront être native dans l'application et non soumises à licence

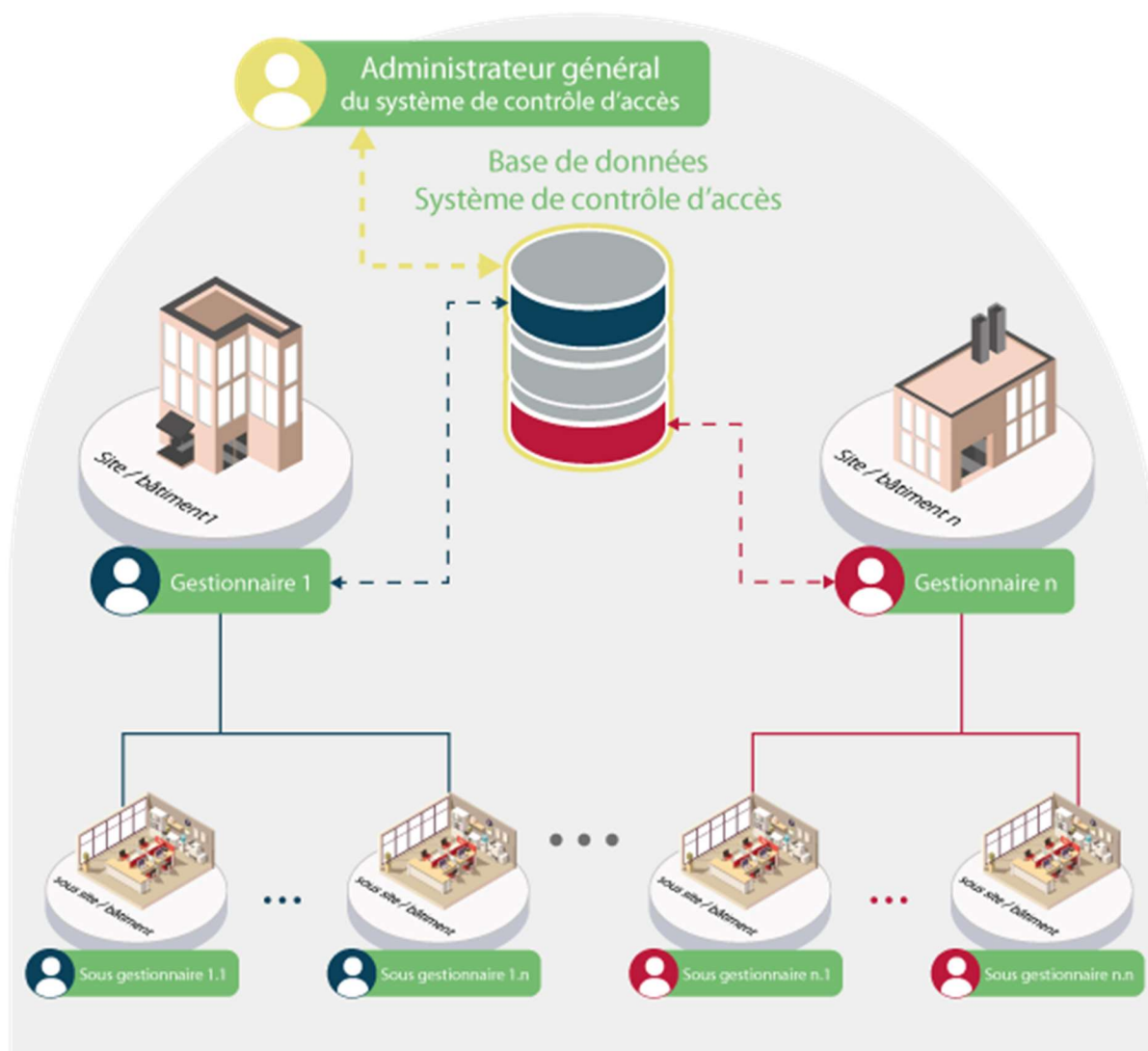
Chaque lecteur ne fera pas l'objet d'une licence spécifique dépendant du niveau de sécurité, l'application intégrera nativement tous les niveaux requis.

Il devra obligatoirement être possible pour chaque utilisateur de définir plusieurs identifiants appartenant à plusieurs technologies d'identification.

- MIFARE Classic / Ultralight C / MIFARE Plus
- MIFARE DESFire
- Biométrie, Lecteur de plaques minéralogiques
- etc.

L'application devra obligatoirement intégrer une visualisation de passage et un fil de l'eau en temps réel.

L'application devra obligatoirement permettre de hiérarchiser les profils exploitants pour l'administration du contrôle d'accès. Il devra être possible de définir un administrateur général, ayant un accès total à la base de données et des gestionnaires, ayant un accès limité à leurs zones d'action. Ce système d'administration, pourra être adapté à tous types de fonctionnements. (administration par zone géographique, site, bâtiment, métier, service...)



2.2.3. Extensions logiciels

Le logiciel de contrôle d'accès devra également intégrer les fonctionnalités suivantes :

Interfaçage base LDAP, AD

Le système de contrôle d'accès devra obligatoirement s'interfacer sur l'annuaire LDAP de l'entreprise afin de permettre une synchronisation en temps réel de la base de données du contrôle d'accès sur l'annuaire de LDAP de l'entreprise.

2.3. Equipements informatiques

La suite logicielle sera installée sur un serveur en format rack 19'', il disposera des caractéristiques techniques suivantes :

- UC Serveur rackable de Marque DELL ou équivalent,
- CPU : benchmark 10000 type E3-1240v6 3.7GHz
- Mémoire RAM (Min / Reco) : 8 Go / 16 Go
- Espace disque disponible (Min / Reco) : 100 Go / 250 Go
- Systèmes d'exploitation recommandés : Windows 10, Windows Server 2019
- Systèmes d'exploitation compatibles : Windows 8 - 8.1, Windows 10, Windows Server

- 2012 R2, Windows Server 2016, Windows Server 2019 à compter des versions 2.23.x.x de la suite logicielle Synchronic
- Compatibilité virtualisation : Hyper-V, VMWare, Citrix

Il sera prévu un poste d'exploitation avec 2 moniteurs 24", il disposera des caractéristiques techniques suivantes :

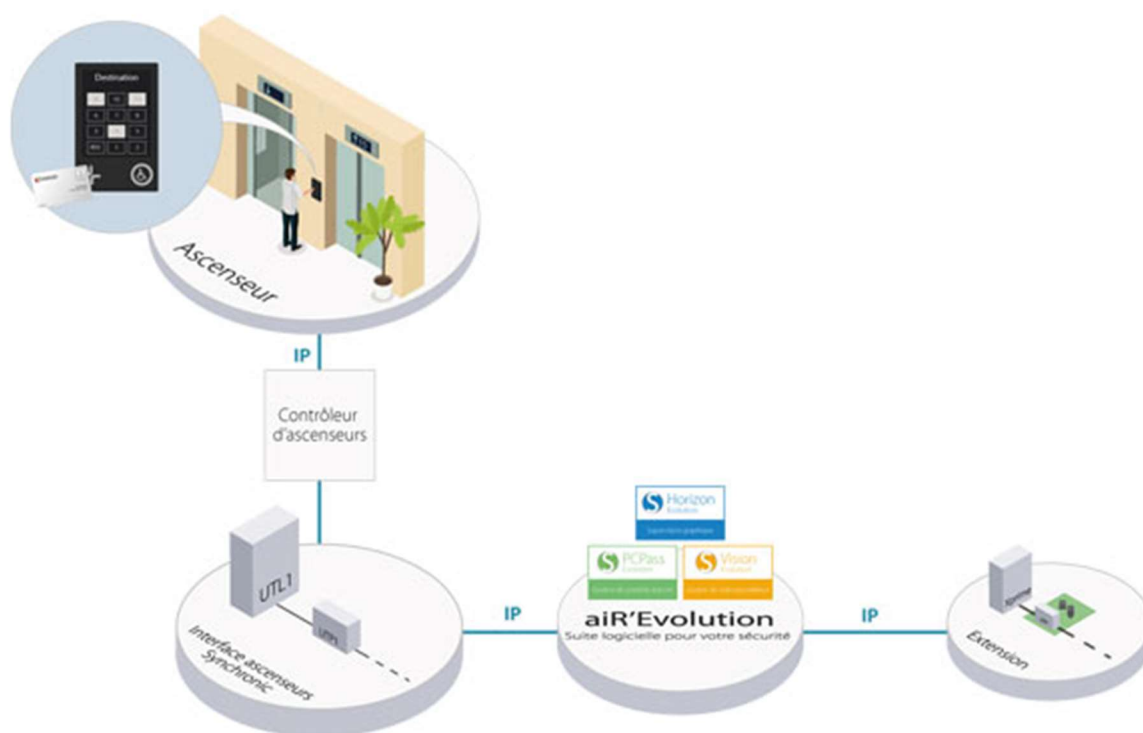
- UC de marque DELL ou équivalent,
- CPU : benchmark 8000 points, type i3-10100
- Mémoire RAM (Min / Reco) : 4 Go / 8 Go
- Espace disque disponible (Min / Reco) : 40 Go / 100 Go
- Système d'exploitation recommandé : Windows 10
- Systèmes d'exploitation compatibles : Windows 8 - 8.1, Windows 10, Windows 11

3. Fonctions spécifiques

Le système de contrôle d'accès devra gérer les fonctions spécifiques suivantes :

3.0.1. Gestion ascenseur

Le système de contrôle d'accès devra permettre la gestion d'ascenseurs (Prédestination des étages suivant le profil utilisateur) et être compatible à minima avec les deux ascensoristes KONE et OTIS, avec un interfaçage direct entre l'UTL et l'automate ascenseur.



3.0.2. Anti Passback / Anti Timeback

Les contrôleurs devront gérer nativement les fonctionnalités d'antipassback / antitimeback sur au minimum 2 zones distinctes. Une même zone antibassback pouvant être sur un même contrôleur ou répartie sur plusieurs contrôleur. Dans ce dernier cas, la fonctionnalité se fera directement via les contrôleurs sans passer par le serveur de contrôle d'accès.

4. UTL de contrôle d'accès et d'alarme intrusion - Qualifiée ANSSI

Le système proposé reposera sur une ou plusieurs UTL **Xsecur'-Evo de marque Synchronic**, qualifiée par l'ANSSI et permettant la gestion simultanée du contrôle d'accès et de la détection intrusion.

Le système devra donc supporter la technologie DESFire, et être conforme aux préconisations de l'ANSSI dans le cadre de l'architecture n°1 (gestion du lecteur en mode transparent)

Le système devra impérativement résister aux attaques logiques L2 ou L3 du guide de l'ANSSI, avec la prise en charge obligatoire de l'authentification du badge via des clés dérivées.

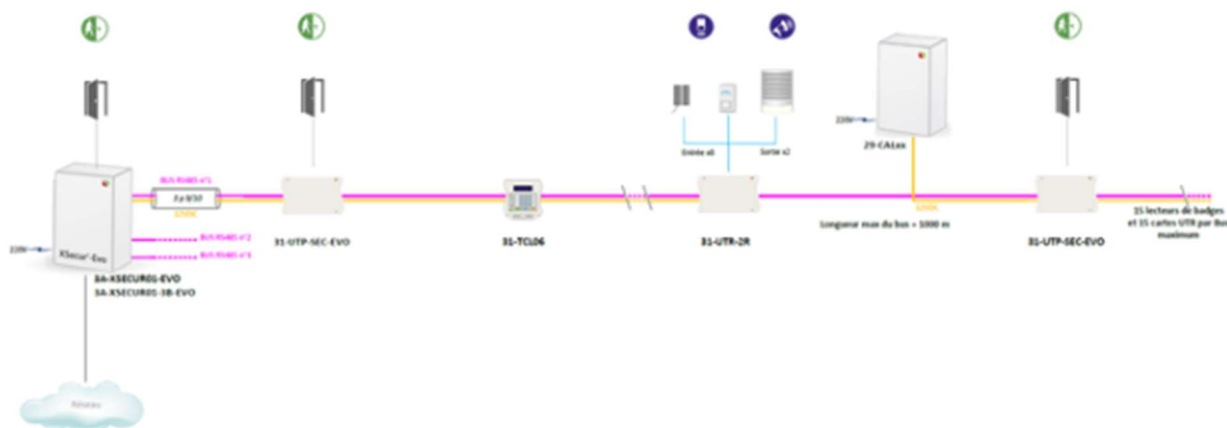
Caractéristiques principales :

- Nombre de bus : 1 à 3 bus
- Nombre de lecteurs de base sur carte mère : 1 ou 2 lecteurs pour 1 porte (E/S)
- Nombre max de lecteurs : 15 à 45
- Nombre de familles CA : 300
- Nombre de plages horaires CA : 128
- Nombre identifiants (badges/codes) maximum : 200 000
- Nombre de points d'alarmes : 0 à 360
- Transmission IP : Oui - Natif - chiffrée AES128 et AES256 - protocole TLS
- Transmission LTE/4G : Option
- Module SAM : Amovible EAL6+
- Authentification 802.1x : Oui
- Protection des firmwares : signés, chiffrés, authentifiés
- TCP / IP : Oui - Natif
- Événements mémoire : 32 000
- Lignes de programmation : 2 000
- Dialogue inter UTL : Oui
- Alimentation : 1,7A - 5A suivant boîtier
- Batterie (non fournie) : de 7 Ah à 38Ah

En plus de ces fonctionnalités le système proposé pourra également permettre :

- la gestion du contrôle d'accès pour les ascenseurs
- la gestion de SAS
- la gestion de fonctionnalités d'antipassback / antitimeback sur au minimum 2 zones distinctes
- le raccordement de lecteur biométrique
- le raccordement de lecteur / clavier
- la transmission des alarmes via LTE/4G
- la transmission vocale des alarmes
- le secours GSM pour la transmission des alarmes

Ces UTL permettront la garantie d'un fonctionnement en mode dégradé en cas de rupture du réseau de communication avec le serveur d'exploitation.



4.1. Gestion de clés de chiffrement

La clé de chiffrement devra être amovible au format SE. Elle garantira une sécurité optimum par un cryptage de ses informations en EAL6+ et un confort d'utilisation dans la gestion des secrets.

L'administration des clés de chiffrement devra être centralisée via le logiciel Secur'Evolution de marque Synchronic ou équivalent. Le chargement des secrets dans les modules SAM peut être réalisé de 2 façons :

- Depuis la station d'encodage des modules SAM, raccordée sur un port USB du poste de gestion
- Téléchargé de manière sécurisée depuis le serveur vers les automates Xsecur'Evo

La 2ème solution offre l'avantage de s'affranchir des problématiques de logistique de transport des modules SAM dans les configurations multi-sites.

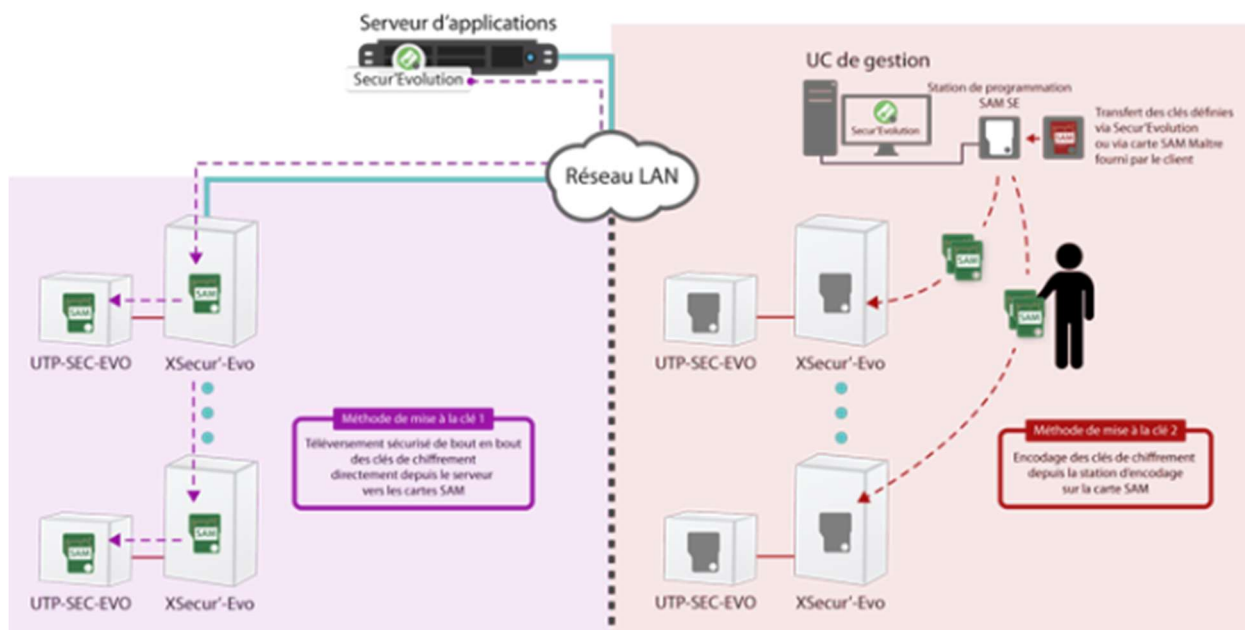
La solution permet également :

- Une saisie des clés en direct ou via cérémonie (plusieurs personnes apportent une partie du secret)
- Gestion des clés diversifiées (permet d'avoir des clés uniques pour chaque badge)
- Le support simultané de 2 configurations MIFARE® DESFire® par lecteur (ex: badge entreprise + badge visiteur, badge Agent + badge blanc)
- Suppression des clés et/ou identifiant sur autoprotection coffret, manuellement, à distance ou via procédure matérielle
- Le client final a la maîtrise totale des secrets

Il sera interdit à l'Entreprise d'avoir accès ou visualiser la ou les clés de chiffrement, dont seul l'exploitant en aura la connaissance.

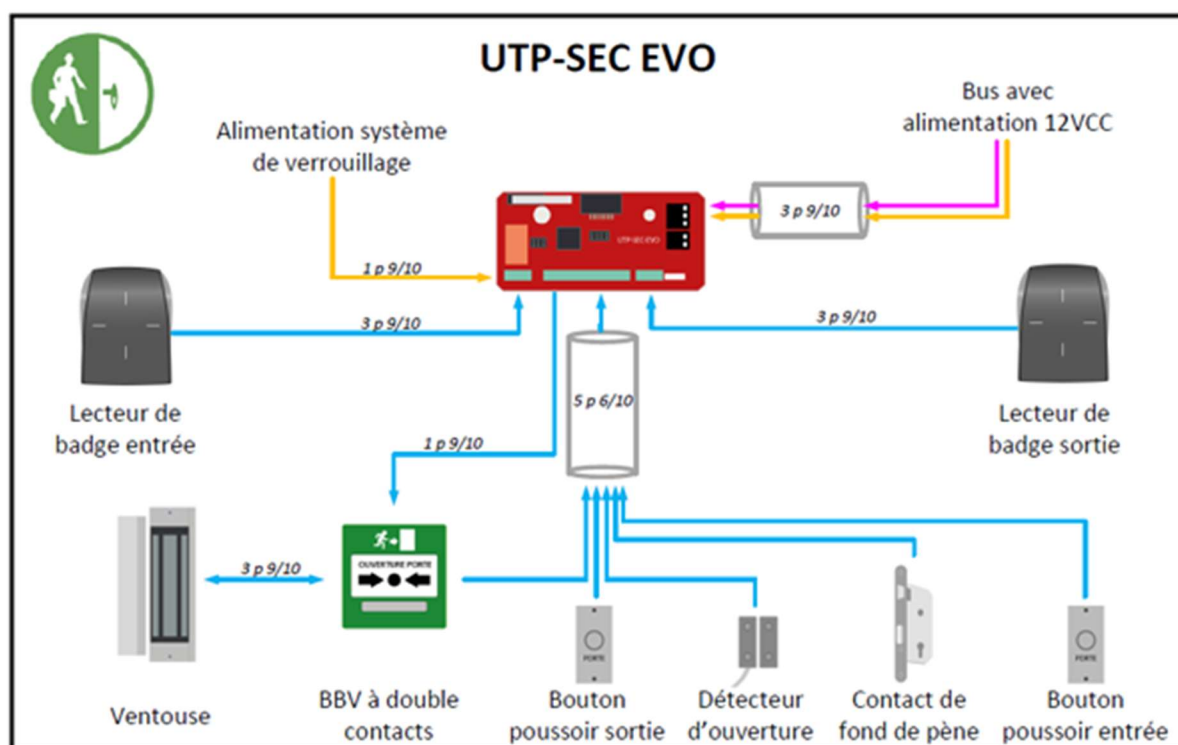
Dans le cas, du secret corrompu ou à risque, il sera possible d'administrer la gestion du secret en local via une unité de gestion complètement détachée du réseau, localisé dans un local sécurisé ou à travers le serveur d'applications via le réseau WAN dédié pour être distribué sur bus sécurisé jusqu'au équipements de sûretés. Cette gestion sera réservée au choix de l'exploitant.

Tout secret stocké sur clé de type HSM sera refusé.



5. Equipement contrôle d'accès

5.1. Module UTP-SEC-EVO - Unité de traitement de Porte sécurisé



Il sera prévu, selon le nombre de portes à contrôler, des Unité de traitement de porte - UTP-SEC-EVO - permettant de gérer une porte avec 1 ou 2 lecteurs. En cas d'indisponibilité de l'UTL, le module de porte devra impérativement disposer d'un mode secours permettant l'ouverture de l'accès avec des badge stockés dans sa mémoire. Le module de porte disposera au minium de 10 badges de secours. Le module de porte devra obligatoirement gérer l'état fermé et verrouillé de la porte, par deux contacts distincts.

Ils auront pour autres caractéristiques :

- BUS RS-485 chiffré / 1 module = 2 lecteurs (1 porte)
- Gestion des secrets sur carte SAM SE (certification EAL 6+)
- 5 Entrées natives et programmées : Boutons poussoirs (entrée – sortie) - Etat du BBG - Contact de position de porte - Contact d'état de verrouillage de porte
- Possibilité de mémoriser 10 badges de secours par UTP en cas de non réponse de l'UTL
- Intégration en coffret auto protégé alimenté ou non, avec possibilité de pré-montage en atelier.
- jusqu'à 15 lecteurs par BUS

5.2. Les lecteurs de badges

5.2.1. Mifare DESFire

Les lecteurs de badges proposés seront de technologie Mifare DESFire.

Lecteur mode "transparent"

Les lecteurs de badges proposés devront être ceux présent dans la cible de sécurité présentée à l'ANSSI dans le cadre de la certification du constructeur.

Ils devront fonctionner en mode dit "Transparent" (le lecteur ne doit pas intervenir dans le chiffrement des données), de type 31-TPRDS485 de chez Synchronic ou techniquement équivalent. Ils auront pour autres caractéristiques :

- Liaison RS485 haute sécurité avec l'UTP-SEC
- Système anti arrachement
- Fonctionne avec les puces Mifare, Mifare DESFire
- Bornier de raccordement
- Compatible plot d'encastrement
- Antivandale(IK10) / IP65



Dans le cadre d'accès nécessitant un haut niveau de sécurité, des lecteurs/claviers RS485 de type TCLDS485 de marque Synchronic ou techniquement équivalent, pourront être proposés afin d'être conforme aux recommandations L3 du chapitre "tête de lecture" du guide de l'ANSSI. Ils auront pour autres caractéristiques :

- Liaison RS485 haute sécurité avec l'UTP-SEC
- Double authentification badge + code
- Système anti arrachement
- Fonctionne avec les puces Mifare, Mifare DESFire
- Bornier de raccordement
- Compatible plot d'encastrement
- Antivandale(IK10) / IP65



Badges format carte de crédits

Les badges seront au format cartes de crédits.

Ils devront être multi applications et comporter une puce au format MIFARE® DESFire® EV2, avec 2Ko de stockage minimum. Le lecteur ne devra en aucun cas utiliser le numéro de série du badge comme identifiant.

5.3. Autres technologies d'identifications

5.3.1. Biométrie

Le système de contrôle d'accès devra permettre la mise en place d'une solution d'identification via biométrie. Cette solution devra respecter les directives de la CNIL.

- La mise en place d'un système de contrôle accès doit se faire en accord avec le CODE DU TRAVAIL.
- La Direction doit donc informer de son intention et demander l'avis des instances représentatives du personnel notamment le Comité d'Entreprise et le Comité d'Hygiène, de Sécurité et des Conditions du travail (CHSCT).
- La mise en place d'un système de contrôle d'accès doit aussi respecter la loi "INFORMATIQUE ET LIBERTÉ".
- La loi du 6 Janvier 1978, stipule que toute entreprise qui met en place puis gère un fichier informatisé de données nominatives est tenue de le déclarer.
- Les données personnelles recueillies doivent être accessibles par l'individu qui conserve un droit de modification sur celles-ci.
- La Direction doit donc obtenir l'accord de la Commission Nationale Informatique et Liberté (CNIL).
- De plus, la mise en place d'un contrôle d'accès ne doit pas faire obstacle au bon fonctionnement des issues de secours et d'une façon plus générale à la sécurité des personnes. Il sera donc nécessaire de tenir compte des préconisations des commissions de sécurité ou pompiers (Asservissements liés au SSI (Système de Sécurité Incendie)).

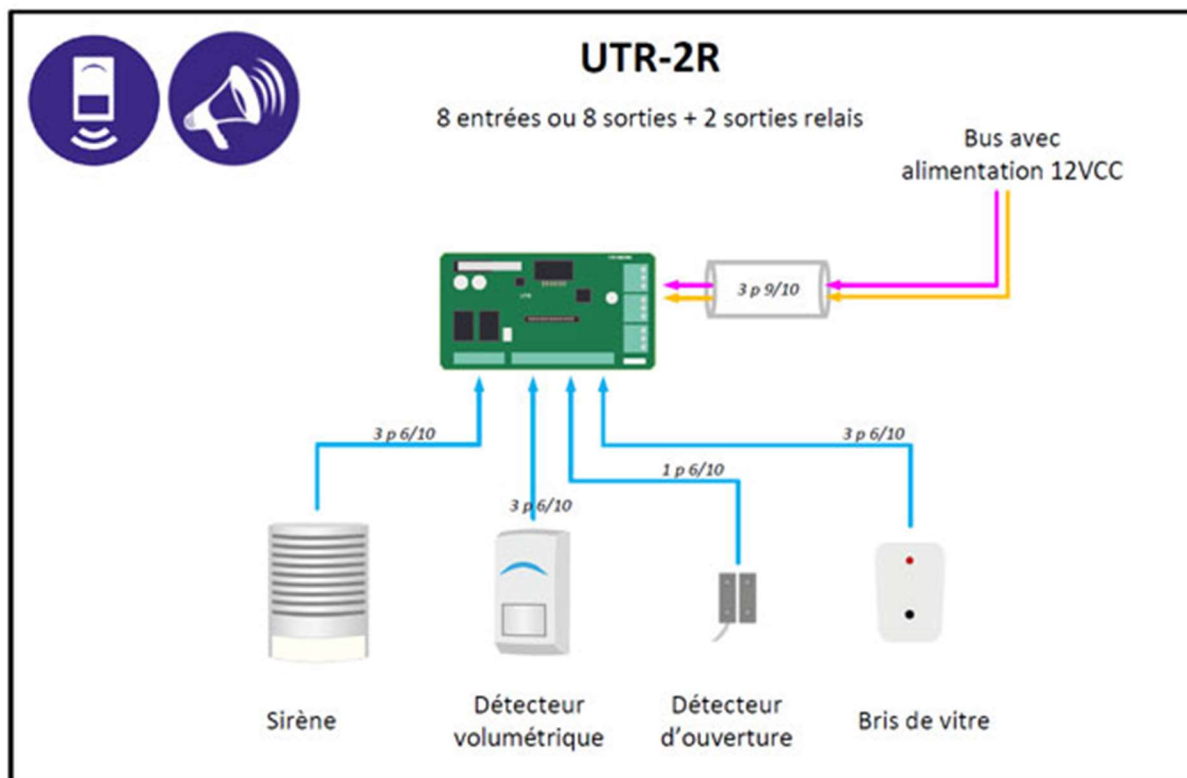
Des lecteurs du type 31-TBIO-485 de marque Synchronic, ou techniquement équivalent, seront mis en place pour la sécurité des accès sensibles.



6. Equipement intrusion

6.1. Modules déportés

6.1.1. Module UTR - Unité de traitement ressources



Le matériel proposé devra permettre de gérer les ressources de l'installation, comme des entrées et des sorties :

Entrées :

- Alarme intrusion
- GTC
- Alarme Technique
- Alarme Incendie
- Etc...

Sorties :

- Sirènes,
- Asservissements vidéo,
- Télécommande lumière,
- Etc...

Ces informations seront issues des cartes connectées sur le bus RS485 de type UTR de marque Synchronic ou équivalent, sur lesquelles viennent se raccorder des détecteurs. Chaque carte UTR devra disposer au minimum de 8 ressources. Ces 8 ressources pourront être indifféremment configurées comme soit des entrées soit des sorties afin de minimiser le nombre de cartes à installer. Ainsi il sera possible de configurer chaque carte UTR comme pouvant gérer 8 entrées d'alarmes, ou 8 télécommandes ou 4 entrées et 4 télécommandes. Les détecteurs seront obligatoirement raccordés sur les UTR en mode équilibré par une double résistance afin d'assurer une supervision de la boucle de

détection. Les détecteurs utilisés seront liés aux différentes fonctions souhaitées pour assurer la sécurité du site, à savoir :

- Périmètre
- Volumétrie
- Périphérie
- Et plus généralement tous détecteurs

Le système devra permettre :

- l'association des droits d'accès aux droits d'intrusions.
- L'asservissement du contrôle d'accès aux informations d'alarme.
- Piloter des process d'asservissements de type GTC grâce à un module intégré permettant des paramétrages spécifiques afin de s'adapter aux besoins d'évolution éventuels.

6.2. Transmission

6.2.1. Transmission LTE/4G/5G

Le système devra permettre la transmission des alarmes sur réseau IP via le réseau mobile LTE/4G. Il sera donc prévu un module CN-XPE-4G, transmetteur SIA/CID DC-09, pour les UGL Synchronic.

6.3. Clavier

Il sera possible de raccorder directement sur le BUS RS485 des claviers qui seront de type TCL06 ou TCL11 de marque Synchronic ou équivalent pour une utilisation intérieure ou extérieure. Ces claviers permettront la gestion locale et l'exploitation de la détection intrusion.

6.3.1. Clavier intérieur

Le ou les claviers intérieurs seront de type 31-TCL06 de marque Synchronic ou techniquement équivalent. Ils auront pour caractéristiques :

- Raccordable sur bus RS485
- 1 voyant rouge, 1 voyant vert, pilotés directement par la centrale,
- 1 buzzer piloté directement par la centrale,
- Ecran LCD 2 lignes 16 caractères
- Boîtier ABS haute résistance



6.4. Pupitre tactile de gestion



Il sera prévu un pupitre tactile de gestion, de type Pupitre XTC de marque Synchronic. Il devra communiquer en temps réel avec l'installation de sécurité. Il permettra :

- de consulter les alarmes en cours
- de consulter l'historiques des alarmes
- l'affichage des points en défaut, avec éjection
- la visualisation des droits d'accès
- l'ouverture de porte à distance
- le déclenchement de télécommande personnalisables (lumière, portail...)
- la diffusion de messages vocaux personnalisables (depuis le pupitre ou depuis des modules de type 26-MHP-PAU, déportés).

Il aura pour caractéristiques :

- écran tactile de 7"
- interface personnalisable
- accès hiérarchisé via badge Mifare ou code sur clavier aléatoire
- raccordable sur réseau TCP/IP
- possibilité d'alimentation POE

6.5. Sirène

Il sera possible de raccorder sur les cartes UTR des sirènes pour une utilisation intérieure ou extérieure.

6.5.1. Sirène intérieure

Il sera prévu des sirènes intérieures en ABS - NF-A2P type 3 - d'une puissance sonore de 114dB, devant être secourue par une batterie 12v de 2Ah.

6.6. Technologie de détection

6.6.1. Détection volumétrique

Détecteurs volumétriques

Il sera prévu des détecteurs bivolumétriques IR + hyperfréquences, selon les caractéristiques :

- 12m x 12 m - NFA2P type 2
- ou
- 15m x 18 m - fonction antimasque - NFA2P type 3

7. Interphonie

7.1. Les portiers

Il sera mis en place un système d'interphonie intégrant le contrôle d'accès dans la platine, avec identification par badge et/ou QR CODE, sans câblage supplémentaire.

Les lecteurs de badges devront être directement compatible avec le système de contrôle d'accès.

Les interphones seront de type XELLIP de marque CASTEL ou équivalent.



Ils auront pour caractéristiques principales :

- Caméra FULL HD grand angle 110° vertical et 170° horizontal
- Haut-parleur de 10W minimum
- IP65 et à minima IK08
- Sortie bus RS485
- 2 ports Ethernet :
 - Débit 10/100/1000MB
 - Fonction bridge pour la connexion d'un produit tiers comme une caméra IP,
 - Boucle IP
- Support VLAN
- Gestion de notification ASCII
- Intégration du protocole SNMP (Simple Network Management Protocol)
- Sécurisation des connexions Ethernet via le protocole 802.1X (radius)
- Serveur Web embarqué (français / anglais)
- 6 contacts sec
- 2 sorties relais paramétrables
- Fonction SIP TLS natif
- Lecteur intégré compatible :
 - Mifare Plus® Sécurisé

- Mifare DesFire®
 - Mifare Bluetooth® BLE
- Lecteur de QR CODE
- Possibilité d'un clavier à code (compatible braille et en inox)
- Bouton en inox à contraste tactile
- Façade en inox de qualité marine pour environnement difficile
- Visserie en inox anti-vandale
- Démontage de la protection de la caméra sans retirer la façade avance
- Couleur de la face avant personnalisable suivant un RAL fourni par l'architecte.
- Ecran couleur de 2.8 pouces (si vidéophone à défilement) ou pictogramme PHMR par LED.
- Possibilité d'appeler nativement sur un Smartphone ou un PC via le Cloud SIP CASTEL
- Alimentation par POE+ ou 24V DC

02.2.5.3 Extension du système incendie actuel et alarme d'ouverture de porte Independent

La Disp dispose actuellement d'une SSI de marque FINSECUR de modèle BALTIC 512, sur la zone du 1^{er} étage. Nous voulons rajouter 4 points de détection dans les bureaux.

Lors d'un déclenchement de l'alarme incendie, certaines portes déterminées par la Disp devront être libérées du contrôle d'accès le temps de l'alarme.

Sur un système indépendant, la DISP de Lille souhaite une alarme pour détecter l'ouverture de deux portes avec une temporisation de quelques secondes situées au 1^{er} étage et au RDC. Sur cette réalisation, il faudra prévoir un inhibiteur des capteurs par clef.

02.2.5.4 Remplacement du système de télétransmission

Le transmetteur d'alarme actuel sera à remplacer, relocaliser et à connecter avec l'alarme incendie et intrusion. Celui-ci devra être remplacé par un transmetteur d'alarme GSM 4/5 G.

02.2.5.5 Petit travaux CFA CFO

Suite à la réalisation de ce chantier. Le copieur du service DSI doit être repositionné dans un autre espace. Il vous est demandé de créer l'alimentation et le point de connexion du copieur. Ainsi que mettre de la détection de mouvements sur l'éclairage afin de couvrir toute la circulation de la zone du copieur pour l'éclairage. Le titulaire du lot 1 devra effectuer la dépose, la repose ou la pose des éléments de CFO CFA nécessaires à la bonne installation des matériaux du lot 2, en coordination avec le titulaire du lot 2 menuiserie métallique.

02.2.6 Planning

- Les délais offerts à cette opération de travaux sont assez restreints. L'étude du planning fera l'objet d'une attention toute particulière, et offre peu de place aux aléas. Toute optimisation sera attendue.

Annexes



31-TBIO-485

Lecteur Mifare DESFire + biométrie

Lecteur haute sécurité design + Biométrie - Nécessite UTP-SEC - Mode transparent - Conforme préconisations ANSSI
- Empreinte stockée dans le badge, conforme à la législation (CNIL)

Fréquence / Normes	13.56 MHz / ISO14443 A
Puce	MIFARE® DESFire® EV1/EV2, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
Fonctions	Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur) + Empreintes digitales
Identification biométrique	Optique (GAGEM MorphoSmart™) / Durée d'identification ≤ 1 seconde pour une authentification 1:1 / Zone de reconnaissance 14 x 22 mm
Interface	RQ485
Distance de lecture	0 - 5 cm
Connectique	Bornier débrochable 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F - Indicateur d'état d'arrachement
Indicateur lumineux	2 LEDs RVB - 360 couleurs
Indicateur sonore	Buzzer intégré
Consommation	100 mA/12 VDC typique
Alimentation	7 - 28 VDC
Matériaux	ABS-PC UL-V0 (noir)
Dimensions (h x l x p)	167 x 80 x 62 mm
Températures de fonctionnement	- 10°C / + 50°C
Fonction anti-arrachement	Détection arrachement par accéléromètre avec possibilité d'effacement des clefs (brevet déposé)
Indice Protection / Résistance	IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
Fixation	Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
Certifications	CE & FCC



31-TPRDS-485

Lecteur haute sécurité

Lecteur haute sécurité design - Nécessite UTP-SEC - Mode transparent - Conforme préconisations ANSSI

Fréquence	13.56 MHz
Normes	ISO14443 types A
Puce	MIFARE® DESFire® EV2/EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
Fonctions	Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur)
Interface	RS485
Distance de lecture	0 - 6 cm
Connectique	Bornier débrochable 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F - Indicateur d'état d'arrachement
Indicateur lumineux	2 LEDs RVB - 360 couleurs
Indicateur sonore	Buzzer
Consommation	130 mA/12 VDC typique
Alimentation	7 - 28 VDC
Matériaux	ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
Dimensions (h x l x p)	107 x 80 x 26 mm
Températures de fonctionnement	- 20°C / + 70°C
Fonction anti-arrachement	Détection arrachement par accéléromètre avec possibilité d'effacement des clés (brevet déposé)
Indice Protection / Résistance	IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandalisme IK10
Fixation	Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
Certifications	CE

XSECUR'-EVO

UTL QUALIFIÉE PAR L'ANSSI

- Bus RS485 haute sécurité, chiffrement basé sur le standard TLS
- Jusqu'à 45 lecteurs par automate de sécurité
- Jusqu'à 200 000 badges
- Module SAM amovible EAL6+
- Protection des firmwares (signés, chiffrés, authentifiés)
- Communication IP chiffrée TLS
- Mécanismes de cryptographie conformes au RGS
- Prise en charge de l'authentification RADIUS 802.1x



La solution de contrôle d'accès XSecur'-Evo répond aux nouvelles problématiques de sécurité et de cyber-sécurité. À ce titre l'UTL XSecur'-Evo est qualifiée par l'ANSSI. Cette qualification, vaut recommandation par l'État français.

Polyvalence et performance

Avec 1 à 3 bus terrains, la solution XSecur'-Evo peut gérer par automate jusqu'à 45 lecteurs et 200 000 identifiants (badges / codes). Les automates XSecur'-Evo intègrent également des fonctions d'intrusion, avec jusqu'à 360 points d'alarmes par automate.

Pensée pour la sécurité du client final

XSecur'-Evo est une solution pensée pour la sécurité du client final. La sécurité n'est pas remise en cause en cas d'intervention de l'agent de maintenance, qui doit être formé sur nos produits (compétent), mais ne nécessite pas « d'habilitation de sécurité » (niveau de confiance faible, pas d'accès aux secrets).

Très haut niveau de sécurité

Avec un bus RS485 haute sécurité (chiffrement basé sur le standard TLS) et un module SAM amovible EAL6+, la solution XSecur'-Evo fait partie des plus hauts niveaux de sécurité du marché.

La solution intègre également une protection des firmwares (signés, chiffrés, authentifiés).

Gestion de clés de chiffrement

L'administration des clés de chiffrement est centralisée via le logiciel Secur'Evo. Le chargement des secrets dans les modules SAM peut être réalisé de 2 façons :

- Depuis la station d'encodage des modules SAM, raccordée sur un port USB du poste de gestion
 - Téléchargé de manière sécurisée depuis le serveur vers les automates XSecur'Evo
- La 2^{ème} solution offre l'avantage de s'affranchir des problématiques de logistique de transport des modules SAM dans les configurations multi-sites.

La solution permet également :

- Une saisie des clés en direct ou via cérémonie (plusieurs personnes apportent une partie du secret)
- Gestion des clés diversifiées (permet d'avoir des clés uniques pour chaque badge)
- Le support simultané de 2 configurations MIFARE® DESFire® par lecteur (ex: badge entreprise + badge visiteur, badge Agent + badge blanc)
- Suppression des clés et/ou identifiant sur autoprotection coffret, manuellement, à distance ou via procédure matérielle

Le client final a la maîtrise totale des secrets.



Sécurité & Sûreté, Notre Priorité

La technologie VORTEX

Le Vortex est un verrouillage hybride (magnétique et mécanique) plus petit qu'une ventouse magnétique. Il garantit un verrouillage extrêmement puissant (jusqu'à dix fois plus performant que les ventouses basiques du marché). Sa force de maintien testée est de 15000 N.

L'exclusivité de ce verrouillage hybride réside dans un « diabolito » usiné dans un alliage à haute résistance. Ce dernier est capturé au sein d'un puits grâce à l'action d'un vortex de forces électromagnétiques. Le verrouillage est, à ce stade, assuré par la cinétique du bloc magnétique.

En cas de tentative d'intrusion, le verrouillage mécanique entre en action. Le « diabolito » se retrouve prisonnier du puits par le déploiement des billes métalliques contenues dans ce dernier. Le VORTEX est ainsi capable de résister à une pression/traction supérieure à 15 000N (1 500kgf) se rapportant au « grade 6++ »!

Technologie unique de pré-alarme (EW)

Le Vortex est équipé d'un capteur de pression/traction: Cette technologie permet au Vortex de déclencher une alarme AVANT même que l'accès ne soit forcé. Il s'agit d'un système unique dans le monde de la sécurité.

CARACTÉRISTIQUES

- Montage: En applique
- Tension: 12/24V DC
- Courant: 330 / 170 mA
- Contrôle de verrouillage: Contact reed
- Contrôle de position de porte: Contact reed
- Technologie Early Warning: Senseur dynamique incorporé détectant toute pression/traction anormale sur la porte
- Circuit MOV intégré protégeant des sur-tension (Peak)
- Protection enveloppe: IP 43 (Sous linteau)
- Dimensions: LxHxP: 218 x 36 x 30 mm
- Poids: ~1,3 kg
- Température d'utilisation: -20°C à +60°C

¹ Les raccordements électriques doivent être protégés en fonction de l'environnement de l'installation.

PERFORMANCES¹

- Catégorie de Maintien: Grade 6++ (15 000N)
- Catégorie d'utilisation: Grade 3 (Public - Fréquence élevée)
- Endurance: Grade 9 (> 1 000 000 de cycles)
- Résistance à la corrosion: Grade 3 (EN 1670, EN ISO 9227)

VX2400LP

VERROUILLAGE HYBRIDE



ÉTIQUETTE NORMALISÉE

Les caractéristiques de nos produits HQMAG sont reprises sur ces derniers, à l'aide d'une étiquette normalisée conforme à la norme EN 13637, chap 7.

3	9	9	1	2	6++	6++	0	0	D
---	---	---	---	---	-----	-----	---	---	---

Réf: EN 13637: + Corrosion EN ISO 9227: Grade 3



NS 561 937



Dimension des Ecrans

Diagonale en pouces	Diagonale en centimètres	Largeur (cm)	Hauteur (cm)	Surface écran (cm ² - m ²)	
40 pouces	101,6 cm	88,55 cm	49,81 cm	0,44 m ²	16/9
41 pouces	104,14 cm	90,77 cm	51,06 cm	0,46 m ²	16/9
42 pouces	106,68 cm	92,98 cm	52,30 cm	0,49 m ²	16/9
43 pouces	109,22 cm	95,19 cm	53,66 cm	0,51 m ²	16/9
44 pouces	111,76 cm	97,41 cm	54,79 cm	0,53 m ²	16/9
45 pouces	114,3 cm	99,62 cm	56,04 cm	0,56 m ²	16/9
46 pouces	116,84 cm	101,83 cm	57,28 cm	0,58 m ²	16/9
47 pouces	119,38 cm	104,05 cm	58,53 cm	0,61 m ²	16/9
48 pouces	121,92 cm	106,26 cm	59,77 cm	0,64 m ²	16/9
49 pouces	124,46 cm	108,48 cm	61,02 cm	0,66 m ²	16/9
50 pouces	127 cm	110,69 cm	62,26 cm	0,69 m ²	16/9
51 pouces	129,54 cm	112,90 cm	63,51 cm	0,72 m ²	16/9
52 pouces	132,08 cm	115,12 cm	64,75 cm	0,75 m ²	16/9
53 pouces	134,62 cm	117,33 cm	66,00 cm	0,77 m ²	16/9
54 pouces	137,16 cm	119,55 cm	67,24 cm	0,80 m ²	16/9
55 pouces	139,7 cm	121,76 cm	68,49 cm	0,83 m ²	16/9
56 pouces	142,24 cm	123,97 cm	69,73 cm	0,86 m ²	16/9
57 pouces	144,78 cm	126,19 cm	70,98 cm	0,90 m ²	16/9
58 pouces	147,32 cm	128,40 cm	72,23 cm	0,93 m ²	16/9
59 pouces	149,86 cm	130,61 cm	73,47 cm	0,96 m ²	16/9
60 pouces	152,4 cm	132,83 cm	74,72 cm	0,99 m ²	16/9
61 pouces	154,94 cm	135,04 cm	75,96 cm	1,03 m ²	16/9
62 pouces	157,48 cm	137,26 cm	77,21 cm	1,06 m ²	16/9
63 pouces	160,02 cm	139,47 cm	78,45 cm	1,09 m ²	16/9
64 pouces	162,56 cm	141,68 cm	79,70 cm	1,13 m ²	16/9
65 pouces	165,1 cm	143,90 cm	80,94 cm	1,16 m ²	16/9
66 pouces	167,64 cm	146,11 cm	82,18 cm	1,20 m ²	16/9
67 pouces	170,18 cm	148,32 cm	83,43 cm	1,24 m ²	16/9
68 pouces	172,72 cm	150,54 cm	84,68 cm	1,27 m ²	16/9
69 pouces	175,26 cm	152,75 cm	85,92 cm	1,31 m ²	16/9
70 pouces	177,8 cm	154,97 cm	87,17 cm	1,35 m ²	16/9
71 pouces	180,34 cm	157,18 cm	88,41 cm	1,39 m ²	16/9
72 pouces	182,88 cm	159,39 cm	89,66 cm	1,43 m ²	16/9
73 pouces	185,42 cm	161,61 cm	90,90 cm	1,47 m ²	16/9
74 pouces	187,96 cm	163,82 cm	92,15 cm	1,51 m ²	16/9
75 pouces	190,5 cm	166,04 cm	93,39 cm	1,56 m ²	16/9
80 pouces	203,2 cm	177,10 cm	99,62 cm	1,76 m ²	16/9