Maître d'ouvrage :

AÉROPORT LA RÉUNION ROLAND GARROS

Commune Sainte-Marie

ACCORD-CADRE MONO-ATTRIBUTAIRE RELATIF AU REMPLACEMENT, EXTENSION ET A LA MAINTENANCE DU SYSTEME DE VIDEOPROTECTION

2025AS008

CCTP

Cahier des Clauses Techniques Particulières

Maîtrise d'œuvre :

BET Fluides
INSET SAS
8, rue Henri Cornu
CS 61071 - 97495 STE-CLOTILDE Cedex
02.62.21.54.43
Email : bet.inset@inset.fr

Date : **Mai 2025** Indice : **2** **Dossier : N° 22-070 / LH**	Phase : **DCE**

SOMMAIRE

1. GENERALITES

1.1 PREAMBULE

Depuis juin 2011, la Société Anonyme Aéroport de La Réunion Roland GARROS (SA ARRG) est titulaire du contrat de concession de l'Aéroport de La Réunion Roland GARROS pour une durée de 38 ans.

Son capital est détenu par l'Etat (60%), la CCI Réunion (25%), la Région Réunion (10%), et la commune de Sainte-Marie (5%), sur laquelle est située la plate-forme de 200 Ha.

Le présent accord-cadre, d'une durée de deux ans renouvelables trois fois, a pour objet de confier à un prestataire la fourniture et mise en œuvre d'équipement de vidéoprotection dans le cadre du projet de remplacement, d'extension et de maintenance SVP destiné à assurer la sûreté de l'ARRG.

Le domaine aéroportuaire est soumis à autorisation d'accès pour les zones en accès direct avec les aéronefs. Le soumissionnaire sera assujetti à l'ensemble des mesures de sûreté de l'ARRG.

1.2 OBJET DE L'ACCORD-CADRE

L'accord-cadre a pour objet la dépose des anciens équipements jugés obsolètes, la conception, la fourniture, l'installation et la maintenance du matériel de vidéoprotection.

Conformément au CCAP, des marchés subséquents seront passé avec le titulaire du présent accord cadre.

1.3 LISTE DES PLANS

-	Niveau 0 – Aérogare Est & Ouest	A – Mars 2025	- VID-01
-	Niveau 1 – Aérogare Est & Ouest	A – Mars 2025	- VID-02
-	Niveau 2 – Aérogare Est & Ouest	A – Mars 2025	- VID-03
-	Plan de Masse	A – Mars 2025	- VID-04
-	Plan Parking & Entrée Aérogare	A – Mars 2025	- VID-05
-	Plan Centrale de Secours Electrique	A – Mars 2025	- VID-06
-	Plan Fret Hangar et Station Animalière	A – Mars 2025	- VID-07

1.4 PRINCIPES GENERAUX

Les zones à contrôler dans le domaine de la sûreté sont scindés en deux groupes :

- Côté Ville, ce groupe représente les zones accessibles au public depuis l'extérieur sans être passé par un poste d'inspection et de filtrage (PIF).
- Côté Piste, ce groupe représente les zones accessibles aux passagers ou personnels habilités et ayant passé avec succès une zone de filtrage.

Les circulations à contrôler dans le domaine de la sûreté sont scindés en deux typologies de circuits :

- Circuit de départ, c'est-à-dire de l'extérieur vers l'aéronef.
- Circuit d'arrivée, c'est-à-dire de l'aéronef vers l'extérieur.

Annexe 1 transmis à la phase d'offre

Le présent accord-cadre définit la surveillance des points sensibles couvert en vidéoprotection extérieure comme intérieure.

1.5 LIMITES DE PRESTATIONS

1.5.1 Généralités

Le titulaire du présent accord-cadre devra prévoir à sa charge de façon non exhaustive :

- La fourniture, le transport, la manutention y compris les moyens de levage pour le gros matériel, la pose, le montage et le réglage de tous les appareils et les régulations nécessaires au bon fonctionnement des installations,
- Stockage, gardiennage et protection des matériels, matériaux et outillages nécessaires au présent accord-cadre, installés ou non, et cela jusqu'à réception des travaux,
- L'amenée, l'installation et l'enlèvement de tout le matériel et personnel nécessaires aux travaux de son accord-cadre,
- Les essais pendant la durée des travaux,
- La programmation et le paramétrage de l'ensemble des équipements fournis
- Les accessoires de fixation pour la pose des appareils et appareillages,
- Les moyens d'accessibilité pour la pose du matériel,
- Le nettoyage du chantier et l'évacuation des déchets pendant toute la durée des travaux,
- Les dossiers de DOE y compris autocontrôle.

1.6 DOCUMENTS DE REFERENCE

- Code du travail,
- Normes NFC 15-100 et additifs (dernières éditions),
- NF P 98-331 : Chaussées et dépendances – Tranchées : ouverture, remblayage, réfection,
- Le décret du 14 novembre 1988 concernant la protection des travailleurs,
- Le décret n°72-1120 du 14 décembre 1972 relatif au contrôle et attestation de la conformité des installations électriques intérieures aux normes de sécurité en vigueur,
- La directive CEM 89/336/CEE relative aux perturbations électriques,
- Les normes CEI 435, ISO IEC 11801, EN 50173,
- Règlements de sécurité relatifs aux Établissements Recevant du Public (ERP),
- Certifications Spécifications (C.S.) et Guidance Materials (G.M.) de l'European Aviation Safety Agency (EASA)
- Arrêté portant sur les conditions d'homologation et procédures d'exploitation des aérodromes du 28 août 2003 (C.H.E.A.), dernière édition du 14 mars 2007
- Spécifications techniques de l'Organisation de l'Aviation Civile Internationale Annexe 14, dernière édition.
- Marquage CE.
- DO 160, Environnemental Conditions and test Procédures for Airborne Equipment
- Le Code de la Sécurité Intérieure (articles L.223-1 à L.223-9, L251-1 à L255-1, L.613-13, R.251-1 à R.253-4),
- L'article 1er du décret n°96 926 du 17 octobre 1996, décret d'application de l'article 10 de la loi 95-73,
- La circulaire du 22 octobre 1996, relative à l'application de la loi 95-73,

- Le décret n° 2006-929 du 29 juillet 2006, portant définition des normes techniques des systèmes de vidéoprotection,
- L'arrêté du 3 août 2007 portant modification du décret précédent pour la définition des normes techniques des systèmes de vidéoprotection,
- Le décret du 15 novembre 1973, n° 73-048 (J.O. du 21.11.1973), fixant la partie réglementaire du Code du Travail, et notamment les articles concernant le cadre réglementaire pour la prévention des risques liés à l'exposition au bruit dans les lieux de travail,
- L'ensemble des documents techniques unifiés (DTU), y compris les additifs, modifications ou erratas,
- Les recommandations ANSSI concernant la sécurisation de l'ensemble des réseaux constituant le dispositif de vidéoprotection.
- Le Réglementation européen UE 2019/1583. Mise en vigueur au 31/12/2021 - Cyber sûreté
- Cadre de conformité de cyber France (C3F) publié par DGAC en septembre 2021
- Le Règlement européen (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- Le règlement d'exécution (UE] 2019/1583 de la commission du 25 septembre modifiant le règlement d'exécution (UE) 2015/1988 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, en ce qui concerne les mesures de cybersécurité
- Network and Information Systems Directive

En aucun cas, l'Entreprise ne pourra se soustraire aux obligations contenues dans ces documents. Cette liste est non exhaustive.

1.7 MODULARITE DES EXIGENCES ET DES CONTRAINTES

1.7.1 Variantes non acceptées

Aucune variante ne sera acceptée.

2. PRESCRIPTIONS TECHNIQUES PARTICULIERES

2.1 PRESENTATION DU SITE

2.1.1 Plan de l'aéroport

Le site aéroportuaire est situé sur la commune de Sainte-Marie et les limites de la concession sont matérialisées par la ligne en pointillé blanc sur l'image ci-dessous.

2.1.2 Réseau Cuivre existant

L'ARRG possède déjà des précâblages informatiques de type Cat.6a minimum qui seront réutilisés après accord de la direction informatique de l'ARRG (DSI).

Le titulaire veillera à ce que l'ensemble des ports utilisés pour la connexion des systèmes de vidéoprotection soient sur un switch destiné uniquement à un usage de vidéoprotection. Dans le cas où aucun port dédié ne soit disponible, le titulaire de l'accord-cadre devra en informer le maitre d'ouvrage qui aura à sa charge la mise en place et le déploiement d'un switch supplémentaire dans la baie liée à l'équipement installé. Le prestataire tiendra compte des délais de commande et d'installation de la DSI.

3. EXIGENCES DU TITULAIRE

3.1 PRESTATIONS SYSTEMATIQUEMENT INCLUSES

Sans qu'il soit nécessaire de le rappeler, la prestation du titulaire comprend tout ce qui est nécessaire pour le parfait respect de l'ensemble des exigences et des contraintes, dans une logique **d'obligation de résultat**.

Ces prestations incluent donc, sans que cette liste soit limitative :

- Toutes les études et plans de réalisation des tranchées et fourreaux à destination des services techniques de l'aéroport pour réalisation des travaux.
- La réalisation du génie civil sur les zones en dehors des terre-pleins soumis à la validation des services techniques.
- Les frais et taxes en tous genres liés à l'importation des matériels à la Réunion,
- La fourniture, la pose, le paramétrage et la mise en service des matériels nécessaires à l'atteinte des exigences :
    - Le câblage courant faible et courant fort des équipements proposés
    - L'ensemble du câblage cuivre, optique ou toutes autres technologies qui seraient nécessaires en plus de l'infra existante.
    - Le raccordement au réseau électrique pour l'alimentation des caméras, détecteurs et systèmes à partir du point tableau le plus proche et la pose d'un disjoncteur qui seraient nécessaires en plus de l'infra existante.
- La mise à la terre des équipements.
- L'obtention des autorisations nécessaires.
- L'ensemble des sujétions liées à la sécurité et à l'inaccessibilité en hauteur qui impose l'utilisation d'une nacelle.
- L'ensemble des sujétions liées au respect des exigences et des contraintes liées au domaine de l'ARRG.
- La participation aux échanges et aux différentes réunions.

Sont inclus dans les fournitures dès lors que l'existant ne serait pas suffisant, sans que cette liste ne soit limitative :

- Les supports de toutes natures (poteaux, fixations, etc..),
- Les réseaux informatique et électriques, y compris leurs cheminements,
- Les borniers de raccordement au réseau de transmission,
- L'ensemble des matériels nécessaires à la réalisation des ouvrages tels que prévus dans des prescriptions fonctionnelles et techniques du présent document,
- L'ensemble du matériel de raccordement et de réseau.

La prestation comprend la parfaite continuité des cheminements, entre les différents points à raccorder, y compris la pénétration dans les bâtiments lorsque cela est nécessaire.

Le prestataire prend en compte tous les paramètres pour une mise en œuvre efficiente du système attendu par les besoins du maître d'ouvrage en adéquation avec l'étude de l'AMO (Annexe).

Le titulaire doit au titre de l'accord-cadre l'étude de débit binaire de la caméra et la couverture du champ de vision en fonction du positionnement des caméras sur les zones à surveiller.

Le titulaire :

- Établit un plan d'implantation général et des plans de détails qui spécifient l'implantation des caméras,
- Définit les supports, mâts, candélabres,

- Prévoit l'installation d'une protection adaptée sur le point d'alimentation électrique, nécessaire à l'installation.
- Précise les dimensions exactes et l'intégration des coffrets de raccordement, connexions de distribution et de transmission.
- Etablit un plan des définitions en pixel/cm des équipements en fonction de leurs positionnements.

3.1.1 Dimensionnement

Il appartient au titulaire de s'assurer que les équipements techniques qui sont en relation directe avec les siens soient compatible. Le titulaire doit notamment s'assurer de façon non exhaustive :

- Des puissances et des intensités pour les livraisons de courant électrique ;
- Des localisations exactes des points de livraison de puissance et des points de rj VDI ;
- De la compatibilité des nombres et sections des conducteurs avec les points de connexion en prenant connaissance des câbles arrivant sur les équipements et en communiquant les caractéristiques des câbles qu'elle prévoit, de la compatibilité des renvois d'informations en vérifiant les intensités et tensions, polarisations, nature de contacts (ouverture, fermeture, inverseur), caractéristiques des câbles, situation exacte des points de raccordement... ;
- Des capacités, limites techniques et recommandations pour l'intégration d'équipements.

Toute incohérence ou incompatibilité non signalée à la Maîtrise d'ouvrage et son Maitre d'œuvre avant approvisionnement et exécution engage la responsabilité du titulaire.

3.2 LIMITES DE PRESTATIONS : PRESTATIONS ET FOURNITURES A LA CHARGE DE L'ARRG

Cette liste est strictement limitative. Tout ce qui n'y est pas inclus spécifiquement est à la charge du prestataire.

3.2.1 Système d'information

Pour des raisons de responsabilité du système d'information les prestations suivantes sont à la charge de la DSI de l'ARRG :

- La fourniture, pose et paramétrage des réseaux de fibres optique fédératrices en double adduction.
- La fourniture et paramétrage des switchs nécessaires au prestataire.
- La fourniture des plans d'adressages nécessaires à la mise en œuvre du projet
- Toutes les décisions techniques sur les réseaux de distributions des systèmes d'informations sûreté.
- Les équipements routeur, firewall et le cœur du réseau
- La configuration des logins et VPN

3.2.2 Autres limites de fournitures :

Ne sont pas à la charge du prestataire :

- Le mobilier sur lequel le PC est posé ;
- Les locaux sécurisés,

3.3 DOCUMENTATION A FOURNIR

3.3.1 Généralités

Chaque document doit être fourni en français et réactualisé à chaque changement de version des applications ou ajout/suppression de matériels.

L'ARRG souhaite une documentation sur les services déployés, leur version, les services à monitorer, ainsi qu'un schéma de l'architecture mis en place.

L'ARRG souhaite aussi une documentation d'exploitation regroupant les principaux problèmes et les procédures de résolution associées.

Le titulaire devra indiquer la documentation de PRI/PCI de la solution.

Les documents mis à disposition pourront faire l'objet d'un audit documentaire.

Chaque livrable devra être remis au format dématérialisé :

- PDF ;
- DWG version 2024
- Modifiable par les logiciels de bureautique courant (Word, Excel, LibreOffice, etc.).

3.3.2 DOE et DIUO

Ces deux dossiers seront remis à l'approbation du maître d'ouvrage et/ou l'assistant en un exemplaire papier et un exemplaire informatique modifiable sous 8 jours après les OPR.

La validation par le maître d'ouvrage et/ou son assistant s'effectuera tout au long de la période des clauses de vérification de servie régulier (VSR), laissant ainsi le temps à l'entreprise de compléter et finaliser le contenu de ses dossiers pour une remise définitive avant l'étape 3 de réception définitive des ouvrages.

Ces dossiers comprendront notamment :

- La nomenclature de tous les équipements mis en œuvre avec les notices techniques,
- La nomenclature des versions logiciels, licences, firmware,…
- Les plans et schémas d'exécution "certifiés conformes" à la réalisation, (plans de positionnement des équipements, plans de cheminement des réseaux, supports, fixations…) seront réalisés à minima sous AutoCAD (version à jour), géo-référencés et à la structure et/ou charte graphique de la collectivité. Les fichiers graphiques seront au format DGN et les relevés du prestataire se feront en planimétrie et en altimétrie (x,y,z), selon le système de projection RGF93CC45 et le système altimétrique IGN normal.
- Les carnets de câbles,
- Les procès-verbaux de l'organisme de contrôle pour l'ensemble des équipements concernés,
- Les consignes détaillées de fonctionnement des installations permettant à toute personne chargée de la maintenance et/ou de son utilisation courante, d'intervenir sans erreur ni omission, et notamment :

- le niveau de compétence technique requis,
- les notices d'exploitation et de maintenance,
- les recommandations sur la nature et la fréquence des interventions de maintenance par type d'équipement,
- les éventuelles contraintes d'exploitation,

- La documentation précisant les procédures d'installation, de désinstallation, de sauvegarde et de restauration,
- Les codes utilisateurs et mots de passe (Usine ou Maître et Administrateur),

Suite à validation par le maître d'ouvrage et/ou l'assistant, l'entreprise éditera :

- Un DOE et DIUO global en un exemplaire définitif et numéroté au format papier et une copie informatique modifiable

3.4 ORGANISATION DU CHANTIER

Ces prestations sont réalisées dans le strict respect de la méthodologie suivante :

- Constitution d'une équipe projet avec un interlocuteur unique
- Réunion de lancement.
- Réunions hebdomadaires de suivi de chantier ordonnées et pilotées par la Maitrise d'Œuvre (MOE).

3.5 PROGRAMMATION DES TRAVAUX.

Un programme d'intervention est établi lors de la réunion de lancement par l'entreprise qui précise :

- Les méthodes d'intervention sur la voirie et dans le bâtiment.
- Les périodes calendaires d'intervention.
- Les moyens techniques mis en œuvre dans chaque zone d'intervention.

Les EXE et Fiches Techniques sont tous soumis à VISA. Sans l'obtention de ces derniers, les travaux ne sont pas autorisés.

3.6 GESTION DES RISQUES

3.6.1 Risques opérationnels.

Une analyse globale des risques du projet, identifiés par le titulaire, est réalisée dès le début du projet pendant la période de préparation et d'étude d'EXE et actualisée tout au long de son déroulement.
Le titulaire alerte sans délai le comité technique de tout retard ou glissement qui surviendrait lors d'une phase ou d'une étape du projet et explicite ses éventuelles conséquences ou mesures palliatives.
Quelques risques identifiés qui pourraient être liés à ce dossier :

- la non-atteinte des objectifs des projets,
- le dépassement des délais,

- le dépassement des budgets,
- la complexité technique,
- le manque de mobilisation des ressources internes
- la non tenue de délais de livraison de fournitures

Elle est fournie de manière formalisée à chaque réunion de chantier.

3.6.2 Plan de prévention

Le titulaire et l'ARRG réalisent ensemble un plan de prévention préalablement aux travaux.
Le titulaire ne peut demander aucun supplément à ce titre pour le chantier.
Si nécessaire, l'ARRG nomme un SPS à ses frais. La collaboration du titulaire avec ce SPS est à la charge du titulaire.

3.6.3 Signalisation en zone publique

Les coûts intègrent également les moyens de signalisation et de sécurité prévus pour l'exécution des travaux en zone publique, et notamment si cela est nécessaire, sur les routes d'accès.

3.6.4 Travaux en zone exploitée

Les travaux s'effectuent en zone exploitée, ce qui nécessite un phasage des travaux en fonction des contraintes d'exploitation. Le titulaire en tient compte dans ses coûts. Les travaux sur les mâts se font en journée, et le prestataire garantit la fonctionnalité d'éclairage nocturne de tous les mâts sur lesquels il intervient.
Le prestataire prend en compte un haut niveau de protection en zones exploitées (ex : barrières, surveillance humaine supplémentaire, permis de feu, zones ATEX, etc…), pour ses travaux comme pour ceux réalisé par son ou ses sous-traitants.

3.7 ASPECTS ETUDES.

L'entreprise a à sa charge les études relatives aux sujets suivants :

- Les emplacements des caméras et les procédés de fixation des équipements de vidéo protection,
- Les solutions de raccordements des divers équipements entre eux, aux réseaux de transmission sécurisé,
- Les méthodes d'intervention sur la voirie et dans les bâtiments.

Un programme d'intervention est établi le moment venu par l'entreprise qui précise :

- Les périodes calendaires d'intervention,
- Les moyens techniques mis en œuvre dans chaque zone d'intervention,
- Les moyens de signalisation et de sécurité prévus pour l'exécution des travaux en zone publique.
- Les démarches à effectuer auprès des différents services (Commission de Sécurité, DGAC, Service de l'État, …), les plans, contre-calques à remettre pour l'obtention du certificat de conformité et de la mise sous tension, ainsi que tous les frais afférents, sont à la charge du titulaire.

- Autorisation de travailler sur le domaine public ;
- Arrêté de mise en place de signalisation provisoire ;
- Demande de renseignements auprès des concessionnaires ;
- Déclaration d'Intention de Commencement de Travaux (DICT) ;
- Demande d'arrêté de circulation et/ou de stationnement sont à la charge du titulaire avant tout commencement d'exécution de tout ou partie de son chantier

Toutes ces demandes prennent en compte, sans surcoût, les délais de réponses du maître d'ouvrage et prévoient pour cela un minimum de 15 jours.

3.8 PARAMETRAGE

Au titre de son accord-cadre, le titulaire fournit à l'ARRG pour approbation, un plan de paramétrage, c'est-à-dire les dispositions qu'il entend mettre en œuvre. L'aéroport se réserve le droit de lui demander de les adapter autant que nécessaire jusqu'à acceptation du plan de paramétrage définitif. Il assure ensuite la totalité des paramétrages nécessaires à l'exploitation du dispositif

L'approbation du plan de paramétrage n'exonère pas le titulaire du respect des fonctions et des performances de vidéoprotection.

3.9 EXIGENCES EN MATIERE DE SECURITE DES SYSTEMES D'INFORMATIONS

L'Aéroport de la Réunion Roland Garros (SA ARRG) est dans l'obligation de respecter un certain nombre d'exigences en matière de sécurité des systèmes d'information.

Le titulaire s'engage à justifier de la mise en place de mesures de sécurité et des règles sur lesquelles il s'est engagé dans son offre.

La Sécurité du système d'information du pouvoir adjudicateur est particulièrement sensible.

3.9.1 Exigences générales

Le titulaire conçoit, met en œuvre et exploite les systèmes d'information sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière.

Ainsi, pour chaque composant déployé, le titulaire doit respecter les guides de durcissement fournis par la SA ARRG et adapté à chaque composant déployé.

À la livraison du système, tous les services et logiciels non nécessaires sont désinstallés par le titulaire :

- Tous les services non utilisés sont techniquement désactivés ou désinstallés. Ceci concerne tous les services ouverts ou en écoute sur le réseau (FTP, TFTP, HTTP, RDP, SSH, etc.).
- Toutes les applications et logiciels non nécessaires au fonctionnement des composants sont désinstallés/désactivés.

3.9.2 Clausier contractuel de Sécurité des Systèmes d'Information

Le Titulaire de l'accord-cadre devra signer le clausier contractuel en Sécurité des Système d'Information présent en annexe de ce CCTP. Ce clausier présente les responsabilités et obligations en matière de sécurité des systèmes d'information à la charge du Titulaire.

Tout candidat au présent accord-cadre est considéré sachant du clausier contractuel en Sécurité des Système d'Information en annexe.

3.9.3 Fourniture d'un plan d'assurance Sécurité

Le titulaire respecte le Plan d'Assurance Sécurité (PAS) qu'il devra fournir dans son offre, présentant les mécanismes et procédures qu'il s'engage à mettre en œuvre pour garantir une sécurité optimale de sa solution et le respect du niveau d'exigences définies ci-dessous, aussi bien au niveau de la solution fournie que de son système d'information utilisé pour l'administrer. Le PAS et ses éventuels compléments constituent l'ensemble des mesures de sécurité techniques, humaines et organisationnelles que le titulaire s'engage à mettre en œuvre et à maintenir tout au long de la prestation

Le titulaire est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité définies ci-dessous, pendant toute la durée de l'accord-cadre.

Tout candidat devra joindre à sa candidature le PAS en annexe. Il pourra à sa convenance proposer les mesures complémentaires qu'il jugera nécessaire.

3.9.4 Fourniture de la cartographie

Le pouvoir adjudicateur souhaite maîtriser les composants matériels et logiciels installés au niveau de son parc. Pour satisfaire ce besoin, le titulaire doit fournir un inventaire sous format Excel qui décrit l'ensemble des composants qui constituent le système objet de l'accord-cadre.

Pour chaque composant logiciel, le titulaire fournit à minima les informations suivantes :

- L'éditeur, la marque et le modèle du composant logiciel
- Le nom et la version du logiciel/de l'application
- L'interface et le protocole d'accès : URL, adresse IP, Port réseau, module d'authentification mise en place (intégration avec l'Active Directory ou authentification locale) ;

Pour chaque composant matériel, le titulaire fournit à minima les informations suivantes :

- Le fabricant, le type, le modèle
- La version du Firmware
- Protocole de management (interface d'administration)
- Emplacement physique aux bâtiments du pouvoir adjudicateur.

Le titulaire fournit la cartographie technique du système qu'il déploiera lors de la recette du serveur.

Le titulaire peut utiliser le guide de l'ANSSI si besoin : https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/

La cartographie contient au minimum :

- Une vue application : décrit les solutions technologiques qui supportent les processus métiers, principalement les applications.
- Une vue logique : Cette vue correspond à la répartition logique du réseau. Elle illustre le cloisonnement des réseaux et les liens logiques entre eux, en outre, elle répertorie les équipements réseau en charge du trafic.
- Une vue physique : La vue des infrastructures physiques permet de décrire les équipements physiques qui composent le système d'information ou qui sont utilisés par celui-ci. Cette vue correspond à la répartition géographique des équipements réseau au sein des différents sites de l'organisme. Elle offre une vision d'ensemble des actifs connectés au réseau de télécommunication du pouvoir adjudicateur.
- La Matrice des Flux.

3.9.5 Evolutions fonctionnelles.

Les évolutions fonctionnelles ou techniques ne remettent pas en cause le respect des exigences contractuelles et de sécurité, ou ne compromet pas une éventuelle opération de réversibilité. En cas d'évolution, le titulaire doit vérifier que sa mise en œuvre est conforme aux exigences et en apporter la justification auprès du pouvoir adjudicateur.

Le pouvoir adjudicateur se réserve le droit de refuser toute évolution s'il s'avérait qu'elle rendrait la solution non conforme.

3.9.6 Sécurité

Le titulaire s'engage à ce que les produits du contrat soient, au jour de leur mise en production pour le pouvoir adjudicateur, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations. Ces produits doivent en particulier être livrés avec la dernière version supportée par l'éditeur. Aucun produit OPEN SOURCE non sécurisé ne sera toléré.

La vérification de service régulier (VSR) est refusée si des composants ne sont pas à jour des correctifs de failles de sécurité publiés depuis un délai supérieur à 15 jours à compter de la date de livraison finale du système.

Le titulaire doit n'utiliser que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée de l'accord cadre, à minima 2 ans renouvelable 3 fois. Si la durée de l'accord-cadre dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

3.9.7 Engagement de confidentialité

L'ensemble des informations qui seront communiquées au cours des prestations restent confidentielles, elles ne peuvent faire l'objet d'aucune divulgation à des tiers ou à des membres du personnel du titulaire non appelés à participer à l'exécution des prestations, sauf si la divulgation est nécessaire en raison d'obligations légales, comptables ou règlementaires échappant au contrôle du titulaire retenu.

Un engagement de confidentialité doit être complété et signé par le Titulaire avant toute mise en œuvre des prestations. Le modèle est fourni en annexe.

3.9.8 Conformité RGPD

L'ensemble des systèmes installés par le titulaire devra être conforme au Règlement Général sur la Protection des Données (RGPD - n°2016/679) du le 27 avril 2016 et qui est en vigueur le 25 mai 2018.

Si le dispositif mis en œuvre participe à un traitement de données à caractère personnel (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...) alors la SA ARRG doit être tenu informée de la nature et de la raison de ce traitement.

Il conviendra alors de prendre les dispositions nécessaires en matière de protection des données à caractère personnel sur les axes juridiques, contractuels et techniques pour assurer un niveau de sécurité suffisant de ces données. Le Prestataire doit notamment s'engager à prévenir la SA ARRG de toute violation de données à caractère personnel dès qu'il en aura connaissance.

Le Titulaire de l'accord-cadre devra signer le clausier clausier RGPD fournis par l'ARRG.

3.9.9 Charte prestataire

Une charte prestataire sera signée par chaque agent du titulaire qui sera amener à effectuer des tâches de maintenance, d'exploitation, d'installation et de gestion informatique sur le système STB. Cette charte permet d'encadrer les actions du prestataire et de responsabiliser chaque individu sur les actions qu'il réalise.

Le titulaire devra faire signer à chacun de ses agents cette charte.

La SA ARRG pour accéder aux documents signés sur demande.

3.9.10 Intervention sur site

Le prestataire utilisera un PC portables, qui restera à demeure à l'aéroport afin de réaliser les tâches de maintenance des équipements. Ces postes déjà paramétrés par le prestataire contiendra tous les logiciels nécessaires à la maintenance et à l'administration informatique.

Avant chaque intervention, le titulaire devra préparer et anticiper les actions afin de fournir au préalable les éléments nécessaires (nouvelle version d'un logiciel ou d'un système d'exploitation, ISO d'installation, fichier de configuration …)
En cas d'utilisation de clés USB ou de tout support de stockage de masse amovible, ces périphériques devront être vérifiés (analyse antivirus) via la station blanche (KUB) mise à disposition par l'aéroport avant toute connexion aux PC de maintenance ou aux systèmes de l'aéroport.

3.9.11 Intervention à distance

Le titulaire de l'accord-cadre aura l'obligation d'utiliser l'accès VPN fournis par la MOA pour tout accès à distance.

En cas de d'accès à distance pour réaliser les tâches de maintenance ou d'administration informatique, le titulaire doit utiliser les moyens de connexion à distance fournis par l'aéroport. Il doit présenter des

mesures de sécurité renforcées sur le poste à partir duquel l'accès à distance va être réalisé. A minima, les mesures de sécurité suivantes doivent être respectées par le titulaire et ses salariés :

- Cet accès à distance sera ouvert à la demande.
- Accès VPN avec authentification via compte nominatif
- Connexion aux systèmes de l'aéroport via le bastion d'administration de l'aéroport
- Authentification forte (lorsque cela sera mis en place)
- Signer la charte des prestataires externes fournie par la SA ARRG (chaque salarié du titulaire intervenant sur les systèmes doit signer la charte) ;
- Informer la SA ARRG en cas de départ ou de changement de fonction d'un salarié ayant intervenu pour la SA ARRG ;
- Durcir les postes de travail utilisés par le titulaire pour l'accès à distance
    - Activer le chiffrement du disque dur
    - Disposer d'un antivirus à jour
    - Disposer d'un pare-feu local au niveau du poste de travail
    - Installer les mises à jour de sécurité.

En particulier, le titulaire prend toutes les précautions nécessaires pour éviter l'introduction de tout Programme Malveillant dans le système d'information du pouvoir adjudicateur et adopte les mesures adéquates s'il constate l'existence d'un tel Programme Malveillant.

Il prend en compte toutes les conséquences de défaillance de la sécurité du fait d'un dysfonctionnement de la sécurité pendant une opération de télémaintenance.

3.9.12 Exigences réglementaires et cybersécurité

Le système objet de ce CCTP est soumis à des règlementations très strictes en matière de cyber sécurité.

L'annexe « 6.1 exigences réglementaires en cybersécurité » contient les règles de sécurité à déployer/respecter par rapport à la réglementation.

Le candidat doit faire une réponse pour chaque règle dans le document XLS fourni en annexe :

- Statut (conforme/non conforme/partiellement conforme)
- Justification/explication/commentaires

L'annexe « 6.2 exigences cybersécurité SVP » en cybersécurité contient les règles de sécurité spécifique au système SVP.

Le candidat doit faire une réponse pour chaque règle dans le document XLS fourni en annexe :

- Statut (conforme/non conforme/partiellement conforme)
- Justification/explication/commentaires

3.9.13 Architecture TCP/IP du SVP

Un pare-feu en haute disponibilité sera mis en œuvre par la SA ARRG. Il permettra d'isoler le système SVP du reste du SI ARRG.

Un cloisonnement par vlan sera également appliqué au sein du système SVP. Tous les flux inter-vlan seront filtrés par le pare-feu selon le principe du moindre privilège.

A minima, il convient de mettre en place les VLANs suivants :

- VLAN pour les serveurs vidéoprotection
- VLAN pour les postes de travail vidéoprotection
- VLAN pour les caméras intérieures de sûreté
- VLAN pour les caméras extérieures de sûreté
- VLAN pour les caméras intérieures hors sûreté
- VLAN pour les caméras extérieures hors sûreté

Le schéma annexé 1 au présent CCTP montre un exemple d'architecture qui peut être déployé sur la plateforme aéroportuaire.

Annexe 2 transmis à la phase d'offre

3.10 ARCHITECTURE SI, SPECIFICATIONS ET INTEGRATION AU SI ARRG

Le système de vidéoprotection sera intégré dans un SI dédié aux systèmes sensibles.

Sauf précision contraire, toutes les solutions demandées/proposées dans cet accord-cadre (ci-dessous) devront être installées et configurées par le titulaire de l'accord-cadre. Pour toutes les solutions, le candidat devra argumenter et justifier ses choix/décisions.

Toutes les licences, sauf mention contraire, devront être fournies par le titulaire de l'accord-cadre.

Tous les équipements fournis devront être neufs, avec étiquettes et livrés dans leur emballage d'origine.

La SA ARRG souhaite à tout moment pouvoir acquérir du matériel ou des licences supplémentaires. Le titulaire devra donc indiquer dans son bordereau de prix unitaire, à titre d'information, tous les prix des composants matériels, des logiciels et des prestations.

Les équipements du Système de Vidéo Protection seront interconnectés via le réseau Sensible mise en place par la SA ARRG.

Le titulaire de l'accord-cadre devra :

- Fournir tout type de câbles (RJ45, jarretière optiques, …) et de petits matériels (transceiver, adaptateur, etc.) nécessaire au raccordement et à l'installation en LSI (Locaux Système d'Information) des équipements.
- Etiqueter ses équipements et les raccordements courants forts et courants faibles (électrique, RJ45, fibre optique, …) avec source et destination de chaque côté du câble

- A titre informatif, les switchs mis à disposition seront de la marque Aruba gamme 6300M et 8360 series.

Afin d'identifier les besoins réseau, le candidat devra préciser le nombre de ports RJ45, fibres optique (monomode), le type de connectique fibre optique, ainsi que le débit nécessaire. De plus, il devra présenter un schéma d'architecture détaillé pendant la période de préparation, pour validation.

Pour rappel, toutes les licences nécessaires à la mise en place de l'infrastructure seront à la charge du prestataire sauf précision contraire. Toutes les licences devront être acquise au nom de l'Aéroport Réunion Roland Garros avec un espace au support associé.

La date de fin de commercialisation de chaque élément proposé doit être supérieure à 3 ans, à compter de la date de publication de l'accord-cadre.

3.10.1 Segmentation réseau et gestion des flux de communication :

Afin de simplifier la gestion du réseau, la SA ARRG souhaite fortement privilégier l'utilisation de l'unicast pour l'ensemble des flux vidéo de l'architecture. Dans cette configuration l'idée étant que les caméras remontent toutes en unicast vers l'infrastructure serveur et les postes clients récupèrent les flux vidéo en unicast depuis l'infrastructure serveur.

Si nécessaire, le candidat présentera un scénario alternatif avec l'utilisation partielle ou totale du multicast, avec les gains et impacts potentiels.

Dans tous les cas, le candidat présentera le principe de fonctionnement de sa solution en démontrant les différents flux réseaux, les protocoles et le routage utilisés.

L'aéroport souhaite une segmentation VLAN comme représenté en annexe 2 du présent CCTP :

Annexe 3 transmis à la phase d'offre

L'isolation et la segmentation des réseaux étant un enjeu crucial de cybersécurité, l'Aéroport a pour habitude de filtrer et n'autoriser que les flux de communication nécessaire. De ce fait, le titulaire devra fournir à l'aéroport une matrice des flux de l'ensemble de son système et le sens (source, destination, port).

- **Equipements terrain**
  - Le titulaire devra fournir et paramétrer les caméras
  - Les équipements terrain seront précâblés en cuivre FFTP au LSI le plus proche du même niveau.
    - Dans le cas exceptionnel où la distance de câblage de l'équipement ne permet pas une connexion dans le LSI le plus proche. Le candidat doit proposer dans son offre une architecture et configuration matérielle évolutive qui permet de s'intégrer proprement dans un LSI (par exemple : coffret mural contenant les convertisseurs ou rack de convertisseurs dans la baie). Le titulaire fournira l'ensemble des éléments nécessaire à l'intégration de l'équipement dans le LSI (alimentation, câblage et convertisseur fibre-cuivre).

- Tous les équipements terrain installés par le titulaire devront être référencés dans la fiche LSI (selon le modèle en annexe) et étiquetés dans le but de faciliter le suivi et gestion de la maintenance / exploitation de la SA ARRG.
- A titre informatif, les cordons de brassage utilisés dans les baies sont de couleur rouge afin de respecter le code couleur des systèmes installés sur la plateforme.

- **Poste de maintenance (PC portable)**
  - Le titulaire devra utiliser un poste de maintenance dédiée pour toute intervention. En aucun cas le titulaire ne pourra utiliser son propre PC.
  - Le titulaire devra fournir et paramétrer un PC de maintenance durci selon le guide fourni par l'aéroport. Un 2ième PC de secours sera fourni par le titulaire.
  - Ce PC restera à demeure à l'aéroport
  - Ce PC sera intégré au SI d'administration de la SA ARRG et ne sera utilisé que dans le cas de la maintenance du système par le titulaire lui-même.
  - Ce poste restera à la SA ARRG et sera déconnecté après chaque intervention. Il n'a pas vocation à être connecté à internet.
  - Lors d'une intervention nécessitant l'utilisation d'une clé USB, la clé devra être au préalablement scannée en station blanche avant d'être connectée sur le PC de maintenance. La SA ARRG dispose de plusieurs stations blanches notamment dans le bâtiment APAX et dans le bâtiment de la Direction Technique. La SA ARRG se chargera de l'installation de l'agent nécessaire au fonctionnement de la clé USB.
  - Le titulaire devra fournir et installer le système d'exploitation de type Windows Long Time Support le plus récent « LTSC » en Français. La DSI de la SA ARRG se chargera d'intégrer le PC au SI ARRG (Active Directory, antivirus, GPO de durcissement…). Le titulaire fournira les licences nécessaires et installera les logiciels liés à la maintenance de son SI

Exigences d'intégration communes :

- Les équipements actifs (notamment switch) seront fournis et paramétrés par la DSI de l'ARRG. Le titulaire ne doit pas installer d'équipements actifs sans autorisation préalable de la DSI de l'ARRG
- Les équipements installés par le titulaire devront être impérativement connectés aux switchs de la SA ARRG de manière directe. Toute exception devra être vue avec et validée par la DSI de l'ARRG.
- Le brassage des équipements terrain se fera par la DSI à partir du moment où la fiche LSI a bien été renseignée.
- De manière générale, tous les composants IP de la solution du titulaire doivent être intégrés dans le Système d'Informations (SI) de l'aéroport selon les exigences de la DSI.
- En fonction des besoins du titulaire (liste à fournir), la DSI de l'ARRG fournira à l'entreprise le plan d'adressage à utiliser pour la configuration des cartes d'interfaces de leurs équipements réseau (automates, cartes I/O…).
- Tous les équipements déployés dans le cadre de cet accord-cadre devront s'appuyer sur le serveur NTP mis en place par l'aéroport. Dans le cas de serveurs Windows, ces derniers s'appuieront sur l'horaire du serveur Active Directory de l'aéroport.
- En cas de maintenance à distance, le titulaire devra passer par les accès à distance de la SA ARRG. En fonction des besoins du titulaire, les ressources seront autorisés/mise en œuvre (accès IHM web, accès RDP, comptes nominatifs sur l'AD,…). Les ouvertures se feront sur demande.
- L'authentification des utilisateurs se fera via l'annuaire Active Directory de l'aéroport

- A noter que les serveurs et ordinateurs de la solution (hors poste de maintenance) seront intégrés dans le domaine active Directory de l'aéroport. Les postes et serveurs Windows se mettront à jour selon les indications mentionnées dans l'annexe « maintenance informatique et maintien en condition de sécurité du Système de Vidéoprotection » ci-dessous.
- A noter que l'antivirus Eset et des politiques de sécurité (GPOs Active Directory, stratégies antivirus,…) seront déployés sur les serveurs et ordinateurs mis en œuvre.
- La solution mise en œuvre devra produire des journaux d'évènements (logs). Ces logs devront pouvoir être envoyés vers un serveur de centralisation de logs via le protocole syslog ou encore SNMP.

3.11 FORMATION DES GESTIONNAIRES

Le titulaire assure la formation de l'ensemble du personnel jugé susceptible d'utiliser les prestations et matériels objet de l'accord-cadre conformément aux stipulations du CCTP.

Le titulaire élabore le plan de formation qui devra être validé par la MOA.

Ces utilisateurs doivent pouvoir recevoir les informations nécessaires sur la maintenance et le câblage, les réseaux, les documents d'exécution transmis, les matériels installés.

La formation sera dispensée pour un maximum de 8 personnes par session.

Les formations se déroulent dans les locaux de l'Aéroport et/ou dans les locaux du titulaire sans coût supplémentaire.

Le formateur fournit pour cela :

- Les supports de formation
- Le programme de formation
- Le matériel sur lequel la formation se déroule.

L'Aéroport fournit la salle de formation équipée d'un réseau et d'un moyen de projection par HDMI.

4. CONTRAINTE LIÉE À LA MISE EN ŒUVRE

4.1 L'ENTREPRISE DOIT AU TITRE DE LA MISE EN ŒUVRE

Avant tout démarrage des travaux, l'entreprise devra :

- Faire valider le dossier d'exécution par la maitrise d'œuvre ;
- Consulter et se synchroniser avec les différents services du maître d'ouvrage et autres tiers, notamment sur site, pour la réalisation des traçages ou piquetages permettant de situer l'implantation précise des systèmes de vidéoprotection.

L'entreprise devra au titre de son accord-cadre :

- Réaliser l'ensemble des infrastructures nécessaires à la mise en œuvre de ses équipements
- Réaliser l'ensemble des percements et/ou découpes, carottages,
- La mise en œuvre de l'ensemble des équipements constituant les dispositifs demandés et nécessaires à la bonne fin des ouvrages,
- Réaliser la mise en œuvre l'ensemble des canalisations nécessaires aux équipements,
- Réaliser le rebouchage des percements des parois et trémies des gaines techniques avec le même matériau ou un matériau compatible aux performances équivalentes, notamment lorsque la paroi traversée est Coupe Feu,
- Réaliser le raccord d'enduit sur rebouchage,
- Réaliser les liaisons concernant les alimentations électriques et basse tension de l'ensemble des équipements constituant les systèmes,
- Réaliser la mise en œuvre des protections adaptées à chaque typologie d'équipements contre tous les effets de surtension (courant forts et courants faibles),
- Réaliser la mise en œuvre des équipements de communication, de centralisation, d'enregistrement et d'exploitation dédiés aux dispositifs.
- Réaliser la mise en œuvre des terminaux,
- Réaliser la mise en œuvre du nouveau coffret d'alimentation nécessaire à la distribution électrique des équipements
- Réaliser les raccordements de l'ensemble des équipements,
- Réaliser la validation de l'ensemble des contrôles des performances des réseaux mis à disposition (si mis à disposition),
- Réaliser la validation de l'ensemble des contrôles des performances des nouveaux réseaux mis en œuvre,
- Réaliser le paramétrage des logiciels des dispositifs en conformité avec les prescriptions, recommandations de l'éditeur de la solution choisie,
- Réaliser la programmation globale, paramétrages, réglages, de l'ensemble des équipements,
- Réaliser le repérage et/ou étiquetage des équipements,
- Réaliser le nettoyage des installations et locaux et évacuation des emballages,
- Respecter et faire valider l'environnement des postes informatiques en coordination avec la structure informatique locale du maître d'ouvrage,
- Réaliser le paramétrage de l'ensemble du dispositif aux conditions d'exploitation des utilisateurs et administrateurs,
- Réaliser la formation à l'exploitation des utilisateurs, administrateurs et techniciens,
- Réaliser le basculement fonctionnel entre l'ancien et les nouveaux dispositifs.

Nota 1: Pour chaque intervention sur site, l'entreprise s'engage à respecter l'ensemble des procédures, consignes de sécurité et à s'astreindre aux contraintes spécifiques du lieu concerné.

Nota 2 : Si les travaux nécessitent de modifier ou démonter des ouvrages (percement, carottage, encastrement, dalle ou autre finition de faux plafond, …), l'entreprise doit une remise en l'état à l'identique de l'existant (revêtement, dalles de faux plafond, … et embellissements,). Avant tous travaux de ce genre l'entreprise doit établir un état des lieux avec le maître d'ouvrage ou son représentant. Faute de l'avoir fait, l'entreprise ne pourra se prévaloir d'un quelconque désengagement de sa responsabilité.

4.2 CANALISATIONS

La nature et le mode de pose des canalisations seront conformes aux prescriptions du paragraphe 52 de la norme NFC 15.100.

Tous les conducteurs et câbles seront démontables sans démolition.

Les câbles de tensions et d'utilisations différentes BT, TBT, courants faibles etc. empruntant des parcours communs seront isolés par groupe (tablette de chemins de câbles ou conduits différents).

Le titulaire devra au titre de son accord-cadre toutes les notes de calculs relatives au dimensionnement des sections de câbles des alimentations des équipements.

4.2.1 Hypothèse de calcul

Sauf indications contraires, les notes calcul seront réalisées par défaut avec les hypothèses suivantes :

- Taux de pollution harmonique H3 : <15%
- Coefficient k3 (température ambiante canalisation à l'air libre) : 30°C
- Coefficient k7 (température ambiante canalisation enterrées) : 20°C
- Facteur de symétrie fs = 0,8 sauf à pouvoir justifier du respect des conditions de symétrie
- TGBT et liaison principale BT dimensionnés sur la base de la puissance de livraison
- Autres canalisations dimensionnées avec le courant d'emploi des armoires électriques + réserve

4.2.2 Nature

Sauf exception précisée, les canalisations principales seront en câble de la série U1000 R2V ou AR2V, le neutre ayant **la même section que les phases**. Conformément au paragraphe 523.6 de la N FC 15-100, au-delà de 4 câbles mono conducteurs par phase, il sera mis en œuvre des canalisations préfabriquées.

Les lignes secondaires seront en câble de la série U1000 R2V.

Les parties sous fourreau encastré pourront être en fil du type H07 VU à partir des boîtes de dérivation.

4.2.3 Mode de pose

4.2.3.1 Distribution en enterrée

La distribution en enterré concerne les liaisons notamment :

- Les liaisons inter-bâtiment

- Les attentes extérieures (caméra sur portail et portillon automatique, caméra sur mat, …)

Les canalisations seront réalisées en câble sous fourreaux type TPC pour les liaisons principales.

4.2.3.2 Distribution en extérieur

La distribution des équipements extérieurs, en toiture terrasse, en façade de bâtiment, etc., sera réalisée impérativement en câble de type RO2V ou similaire.

Les câbles courants faibles seront également protégés efficacement contre les UV.

Le présent lot prévoira un coffret étanche IP 65 - IK10, polyester avec visserie antivandalisme pour y positionner les équipements courants faibles soumis aux UV et notamment :

- Les convertisseur fibre cuivre

4.2.3.3 Distribution en encastré

Câble sous fourreau type ICTA encastré dans les cloisons

A charge de l'entreprise les saignées éventuelles et leur rebouchage.

***NOTA** : La distribution en encastrée sera obligatoire :*

- Dans les zones accessibles au public
- Pour les appareillages isolés avec cheminement vertical

4.2.3.4 Distribution en apparent

Câbles posés selon les cas :

- sur chemin de câble avec colliers de fixation dans les circulation, sous faux-plafond, pour la distribution principale,
- maintenus à l'horizontale sous faux plafonds par arcs de fixation pour la distribution terminale.
- sous goulottes PVC dans les locaux suivant plans
- sous moulure pour les cloisons existantes (hors zone publique)
- sous tube IRL 5 en apparent pour les locaux techniques et/ou zones exposées.

4.2.3.5 Distribution en faux plafond Coupe-Feu

Dans le cas particulier de la mise en œuvre de faux plafond coupe-feu, l'encastrement des appareils d'éclairage n'est pas autorisé. Les câbles chemineront sous fourreaux fixés à la structure. Les boîtes de dérivation seront interdites.

4.2.3.6 Distribution en cloison Coupe-Feu

Les boites d'encastrement dans les cloisons coupe-feu ne devront pas altérer les performances de la cloison en termes de résistance au feu. Cette obligation impose l'utilisation de boite coupe-feu.

4.2.3.7 Calfeutrements

Les traversées de mur béton et de cloison placo seront réalisées systématiquement sous fourreau type ICTA ou PVC. Elles seront calfeutrées avec un matériau permettant de restituer le degré CF des parois et d'assurer l'isolation acoustique entre locaux et/ ou circulations.

4.2.4 Sections des conducteurs

Les sections des conducteurs actifs seront calculées de façon à ne jamais dépasser leur contrainte thermique admissible conformément au paragraphe 523 de la norme NFC 15.100.

4.3 SPECIFICITES LIEES AUX RESEAUX CUIVRE A CREER

Afin d'éviter les perturbations des données analogiques ou numériques à hauts débits, les câbles courants faibles sont éloignés le plus possible des sources de perturbations externes ou internes (tubes fluorescents, moteurs électriques, réseau de distribution du secteur 220 V, etc..).

D'une manière générale, courants forts et courants faibles doivent être séparés par une distance supérieure à 30 cm dans tous les cas le long des cheminements parallèles. Pour les cheminements courts de quelques mètres, par exemple en plinthe, la séparation peut être réduite à 3 cm. Les croisements sont autorisés.

La longueur totale du câble cuivre entre la prise RJ45 du point d'accès et la source est inférieure à 90 mètres.

L'ensemble de l'installation est constitué avec la même catégorie de câble de structure F/FTP Cat6a.

Le câble est utilisé pour la distribution des points d'accès et le raccordement des prises RJ45.

Il est de type 4 paires torsadées, catégorie 6a, d'impédance caractéristique 100 Ohms et blindé par paire type F/FTP.

La gaine extérieure est de type LSOH selon les critères inflammabilité IEC 332-1.

Le câble est en conformité avec les standards EN 50173, IOS 11801.2002/A1, EIA/TIA 568B2.10, IEEE 802.3af et 802.3at.

Descriptif :

- F/FTP
- 4 paires, les câbles 2x4 paires ou 3x4 paires seront prohibés
- Impédance 100 Ohms
- Gaine : LSOH
- Bande passante minimale 500 Mhz
- Conducteur AWG 23

4.4 CONTRAINTES LIEES AUX RESEAU FIBRES OPTIQUES A CREER :

D'une manière générale, les constituants des câbles sont compatibles entre eux. Ils sont conformes aux normes NF et/ou à d'autres spécifications en vigueur à la date du présent accord-cadre. Le support de transmission est composé de câbles à fibres optiques monomodes à poser en conduite avec gaine armée non métallique.

Les câbles à fournir et à poser sous conduite sont des câbles étanches, non métalliques et parfaitement adaptés à la pose sous conduite.

Les câbles fibres optiques à poser en bâtiment sont des câbles sans halogène (LSZH). Les matières premières, les conditions de mise en œuvre et d'emploi qui ne sont pas prévues dans ce cahier des charges sont conformes à la spécification CEI 793.2. Au préalable à la commande des câbles fibres optiques, l'entreprise si nécessaire, réalise une visite de piquetage systématique des fourreaux existants et du réseau d'assainissement afin de valider les cheminements des câbles optiques.

Les caractéristiques des éléments des câbles sont compatibles avec les protections d'épissure, les dispositifs de raccordement et d'épanouissement spécifiés dans le présent CCTP. L'âme optique est constituée de plusieurs modules assemblés de type « tube ». La structure de l'âme et la nature des matériaux doivent permettre au câble de satisfaire aux caractéristiques fonctionnelles et aux essais.

Module Optique :

Le module optique est de type « tube ». La nature, la géométrie et le dimensionnement des éléments constitutifs du module doivent être tels que, pour un bon positionnement des fibres (sur longueur), celles-ci ne subissent ni contrainte mécanique, ni modification de leurs caractéristiques optiques lors des tolérances admises, des essais mécaniques, thermiques et mise en œuvre spécifiées dans le présent CCTP.

La fibre optique de type monomode OS2 9/125 µm est définie aux longueurs d'ondes suivantes :

- Longueurs d'ondes 850 nm / 1300 nm
- Atténuation max (en dB/km) 3,2 1,2
- BP mini en Mhz/km 400 600
- Ouverture numérique 0,2 0,2
- Diamètre du cœur 9 µm
- Diamètre de la gaine 125 µm

Les fibres optiques utilisées dans les câbles répondent aux conditions techniques relatives aux fibres optiques monomodes des normes UIT-T G 652 et CEI 793-2.

Les câbles des fibres optiques ont les caractéristiques suivantes :

- Structure libre, multitubes modularité des brins optiques ;
- Porteur central non métallique (aramide, …) ;
- Gaine intérieure assurant l'étanchéité longitudinale ;
- Gaine extérieure PEHD, la qualité ignifugée ou FRNC (retardant la flamme) est un plus;
- Gaine anti-rongeur ;
- Câble non armé résistant aux conditions sévères : totalement diélectrique ;
- Câblage sur connecteur LC-APC.

Les dimensions des coffrets sont optimisées par le titulaire de l'accord-cadre pour limiter l'encombrement des coffrets.

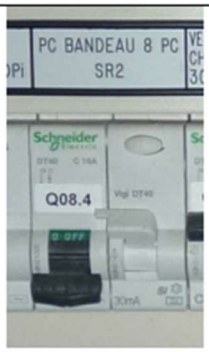
Les coffrets de vidéoprotection devront être obligatoire de minimum IP65 et Ik10 avec vis anti-vandalisme.

4.5 REPERAGE ET ETIQUETAGE

Tous les tableaux, coffrets de raccordement, boîtes de dérivation, boîtiers, etc., seront repérés par des étiquettes.

Les conducteurs électriques seront repérés sur toute leur longueur de façon continue par les teintes conventionnelles fixées par la NFC 04.200.

L'ensemble des étiquetages et repérage devront respecter les standards de l'ARRG ci-dessous.

	Repérage sur câbles : Tous les conducteurs ou câbles seront repérés au moyen d'étiquettes rigides gravées fixées au moyen de 2 colliers minimum. Les étiquettes possèderont : Un code couleur ou symbolique Un numéro Un tenant et un aboutissant Les couleurs privilégiées retenues : La couleur blanche pour les réseaux CFO "normal" ; La couleur verte pour les réseaux "communication" ; La couleur rouge pour les réseaux "incendie" ; Le principe de repérage tenant /aboutissant avec N° d'ordre. La titulaire remettra lors de la phase étude, le carnet de câbles comprenant les appellations des repérages des câbles.
	Repère des boites : **<u>Aucune</u>** boîte ne pourra être implantée dans une zone non démontable, si tel est le cas, le présent lot devra et ce à sa charge prévoir les systèmes d'accès aux équipements tout en respectant l'esthétisme et le degré coupe-feu de l'environnement (à valider par l'équipe de maîtrise d'œuvre). Elles seront obligatoirement repérées au moyen d'étiquettes. Le repérage devra comporter : Un code couleur. Une désignation (exemple : circuit éclairage). Un tenant, un aboutissant, (exemple : TGBT / PC16A+N+T). Un numéro de circuit (exemple : PC01). Toutes les boites de jonctions seront repérées au moyen d'un plan spécifique à joindre au DOE. Dans un objectif de simplification de gestion et de maintenance ; les boites de jonctions devront être regroupées dans une même zone.
	Repérage des départs dans les armoires électriques : Au sein des armoires électriques, il sera fait usage de deux types de repérage : Repérage du départ par une étiquette gravée et montée sur glissière, correspondant à désignation du circuit. Repérage du départ par une étiquette collé sur le départ correspondant à l'identification de ce départ sur les schémas électriques, Nota : l'identification du départ doit permettre le repérage des protections même avec le (ou les) plastron(s) enlevé(s)

4.6 DERIVATIONS

Les dérivations seront réalisées à partir des boites de dérivations avec un maximum de trois conducteurs par bornes.

Les boîtes seront facilement accessibles (boite interdite dans les faux plafonds non démontables).

Afin de faciliter les dépannages, les boîtes de dérivations seront fixées sur les ailes des chemins de câble dans les circulations sauf justification impérative.

Pour tout élément extérieur les boites de dérivation seront impérativement à vis IK10 type anti vandale.

4.7 LE RESPECT DES NORMES ET REGLEMENTATIONS

Dans le cadre contractuel de son accord-cadre, le titulaire est soumis à une obligation de résultat, c'est-à-dire qu'il devra livrer au maître d'ouvrage l'ensemble des installations en parfait état de fonctionnement, et répondant :

- à toutes les réglementations et normes qui leur sont applicables,
- aux prescriptions et instructions des distributeurs.

4.8 DESIGNATION D'UN REFERENT POUR LE SUIVI DU PROJET ET LA CONDUITE DES TRAVAUX

Au cours de l'exécution des travaux, l'entreprise devra détacher à titre permanent un ou plusieurs conducteurs de travaux et chefs de chantiers capables de conduire les travaux dont un ayant la qualité pour le représenter dans toutes opérations, réunions, ...

Le titulaire devra participer aux instances de pilotage du projet, du démarrage du projet suite à sa sélection jusqu'au déploiement.

Ces personnes seront indiquées dans le projet d'installation de chantier.

La fréquence des réunions de suivi des travaux sera à minima d'une réunion hebdomadaire.

L'entreprise veillera au bon déroulement du chantier. Si elle s'aperçoit en cours de chantier d'un quelconque problème, elle en référera immédiatement au maître d'ouvrage et ou son maitre d'œuvre.

Il appartiendra à l'entreprise de s'assurer auprès des autres entreprises dont les équipements techniques sont en relations directes avec les siens, du dimensionnement et de la compatibilité des installations. L'entreprise devra notamment s'assurer :

- des puissances et des intensités pour les livraisons de courant,
- des situations exactes des points de livraison de puissance et les confirmer aux autres entrepreneurs,
- de la compatibilité des nombres et sections des conducteurs avec les points de connexion en prenant connaissance des câbles arrivant sur les équipements et en communiquant les caractéristiques des câbles qu'elle prévoit, de la compatibilité des renvois d'informations en vérifiant les intensités, tensions, polarisations, nature de contacts (ouverture, fermeture, inverseur), caractéristiques des câbles, situation exacte des points de raccordement,
- des capacités, des limites techniques et recommandations pour l'intégration d'équipements,

En outre, l'entreprise communiquera ses plans aux entreprises intéressées, et se fera communiquer les plans des autres entrepreneurs, …

Toute incohérence ou incompatibilité non signalée avant l'approvisionnement et l'exécution engagera la responsabilité de l'entreprise. Dans ce cas, les modifications pour assurer la compatibilité et la cohérence des installations entre elles, seront imposées aux entreprises par le maître d'ouvrage. Elles en supporteront les frais, chacune sur sa propre installation, les décisions du maître d'ouvrage étant sans appel.

L'entreprise assurera pendant tout le chantier, le maintien en bon état des différentes alimentations ou évacuations.

L'entreprise évitera toute souillure des abords du chantier. Elle assurera le nettoiement de la voie publique à chaque fois que des souillures auront lieu du fait du chantier. En cas de carence, le maître d'ouvrage fera procéder au nettoiement au lieu et place du titulaire et à ses frais.

D'une façon générale, le chantier sera tenu dans un bon état de propreté. Les déchets, gravats et terre seront évacués au fur et à mesure de l'avancement des travaux.

4.9 CONTINUITE DE SERVICE DE L'AEROGARE

Les travaux seront réalisés en site occupé et en exploitation. En effet, et conformément aux règles en vigueur, le fonctionnement du dispositif vidéoprotection ne peut être interrompu pendant les périodes d'exploitation de l'aérogare.

En complément, les études menées sur le dispositif révèlent que les réseaux (câbles) existants sont à remplacer et que l'arborescence du nouveau réseau SI de sûreté avec l'existant, ne correspond plus totalement aux nouveaux besoins.

Le maître d'ouvrage a donc décidé de faire réaliser un nouveau câblage pour l'ensemble des nouveaux terminaux.

Cela entraîne que le nouveau dispositif sera mis en œuvre en parallèle de l'existant.

4.10 DROIT D'UTILISATION DES LICENCES

Le titulaire fournit et accorde au maître d'ouvrage une licence d'utilisation de chacun des logiciels lui conférant le droit d'usage de ces logiciels pour chacun des utilisateurs et en devient propriétaire.

La licence fournie sans limite dans le temps est inaliénable. Les logiciels fournis par le titulaire restent en toutes circonstances sa propriété exclusive ou celle de leur fabricant d'origine. Le maître d'ouvrage ne pourra les céder, en concéder la jouissance, ou plus généralement les mettre à disposition d'un tiers. Toutefois, le maître d'ouvrage est autorisé, par mesure de sauvegarde et de protection contre une mauvaise utilisation, à copier les logiciels standards concédés.

Il pourra tester, étudier ou observer le fonctionnement desdits logiciels conformément à l'article L.122-6-1 du Code de la propriété intellectuelle, tel qu'il a été modifié par la Loi n°94-361 du 10 mai 1994.

Pour les parties logicielles, le titulaire doit fournir la preuve de sa propriété sur les produits fournis, ou de sa capacité à les commercialiser, attesté de la stabilité du produit et de son mode de programmation.

4.11 PROPRIETE INTELLECTUELLE

Le titulaire déclare qu'il a bien et dûment la propriété industrielle des systèmes et/ou usage, procédés ou objets qu'il emploie ou à défaut, s'engage vis-à-vis du maître d'ouvrage, tant en ce qui concerne lui-même que ses sous-traitants et cotraitants, à acquérir sous sa responsabilité et à ses frais, toutes les licences nécessaires relatives aux brevets qui les concernent.

Il garantit en conséquence le maître d'ouvrage contre tous les recours qui pourraient être exercés à ce sujet par des tiers au cas où lui seraient contestés soit la propriété industrielle des systèmes, procédés ou objets mentionnés, soit le droit de les employer s'ils sont couverts par des brevets.

Le titulaire garantit le maître d'ouvrage de tous les dommages dont il pourrait être rendu responsable par la seule existence du chantier, notamment ceux causés aux divers ouvrages, construction, qu'ils aient été réceptionnés ou non par le maître d'ouvrage.

D'une manière générale, le candidat doit l'ensemble des matériels et prestations nécessaires à la bonne fin de la mise en œuvre de l'ouvrage

4.12 ESSAIS ET CONTROLES

L'entreprise remettra un cahier de recette interne de chaque dispositif qu'il soumettra pour avis au maître d'ouvrage et au maitre d'œuvre.

L'entreprise réalisera l'ensemble de ses essais et contrôle en interne sur la base de son cahier de recette validé.

Le Maître d'ouvrage se garde la possibilité de vérifier son contenu par des tests similaires ou complémentaires.

Le contrôle du respect des règles de l'Art, et la bonne exécution des travaux sera effectué scrupuleusement :

- Vis-à-vis des réseaux de transmission (en fonction de type de liaisons) et notamment :
    - Contrôle des performances des réseaux numériques (bande passante, analyse des perturbations …),
    - Contrôle de la simultanéité de la transmission des données vers les serveurs et les unités centrales dédiées à la vidéoprotection.

L'entreprise aura à sa charge la validation de l'ensemble des contrôles des performances des nouveaux réseaux optiques et cuivres mis en œuvre (Recette, …).

L'entreprise réalisera l'ensemble des contrôles qui lui semblent indispensables et nécessaires à cette validation.

L'entreprise remettra l'ensemble des documents constituant ces mesures et indiquera précisément la marge ou tolérance à ne pas dépasser. Elle validera l'ensemble de ces mesures et en sera tenue pour seule responsable.

4.13 RECEPTION DES OUVRAGES

La réception est l'acte par lequel le maître d'ouvrage déclare accepter l'ouvrage avec ou sans réserve. La date de réception est le point de départ des responsabilités et garanties notamment instituées par les articles 1792 et 1792-4 à 1792-4-3 du code civil.

5. VIDEOSURVEILLANCE

5.1 OBJECTIFS

Le présent accord-cadre est relatif au remplacement et à la maintenance du système de vidéoprotection de la concession de la SA ARRG. Le système de vidéoprotection remplit les rôles suivants :

- Visualisation en temps des usagers, services et locaux
- Visualisation en temps différés sous 30j minimum des usagers, services et locaux
- Aide à la surveillance.
- Détermine l'origine d'un acte de malveillance.
- Levée de doute.
- Assiste le contrôle des flux (véhicules ou personnes).
- Détecte le déplacement d'objets ou d'individus.
- Identifie des comportement, actes ou objet suspect.

Le système de vidéoprotection permet à l'ARRG de déceler des situations anormales ou non autorisées dans les secteurs visualisés ou sous détections.

5.1.1 Définition de la Vidéoprotection

La vidéoprotection est constituée de l'ensemble des moyens d'acquisition, de transmission, de gestion et d'enregistrement d'images ayant pour objectif la protection de sites, de bâtiments ou de locaux à distance. Il assure les fonctionnalités suivantes :

- Prise de vues ;
- Gestion et visualisation des images ;
- Enregistrement et rendu des images ;
- Gestion des alarmes ;
- Journalisation des activités ;
- Analyse des images.

Elle permet de prévenir et identifier des atteintes à la sécurité des personnes et des biens dans des lieux exposés à des risques d'agression, de vol ou de trafic de stupéfiants, des actes de terrorisme, dans les conditions prévues par l'article L.251-2 du code de la sécurité intérieure.

Ces dispositifs également permettent de constater des infractions aux règles de la circulation, réguler les flux de transport, protéger des bâtiments et installations de l'ARRG et leurs abords, prévenir des risques naturels ou technologiques, faciliter le secours aux personnes ou encore lutter contre les incendies et assurer la sécurité des installations accueillant du public.

5.2 MATERIEL EXISTANT ACTUELLEMENT

Une partie du matériel de l'ARRG est considéré comme obsolète, le titulaire de l'accord-cadre devra faire la dépollution d'une zone lorsque celle-ci est couverte par le nouveau système de vidéoprotection.

5.3 ZONES A SURVEILLER ET CARACTERISTIQUES

Le titulaire devra prendre en compte les spécificités liées à l'illumination des scènes vidéo à surveiller lors du choix des caméras. En effet, s'il s'agit de pouvoir enregistrer des images de qualité en vision nocturne donc il convient soit d'utiliser des caméras à haute sensibilité soit de prévoir un éclairage d'appoint, infrarouge par exemple.

Les prises de vue sont stables dans le temps, et le système n'autorise pas de jaunissement de l'optique, ni de présence d'humidité ou de moisissures pendant la durée de l'accord cadre de 2 ans renouvelable.

Les spécifications caméras en fonction de leurs usages sont définie par le pôle judiciaire de la gendarmerie nationale :

- Les caméras visant à prévenir ou dissuader doivent assurer obligatoirement une résolution spatial minimal de 10 pixels/cm.
- Les caméras visant à détecter une activité suspecte doivent assurer obligatoirement une résolution spatial minimal de 30 pixels/cm.
- Les caméras visant à déclencher et guider une intervention doivent assurer obligatoirement une résolution spatial minimal de 100 pixels/cm.
- Les caméras visant à matérialiser une infraction doivent assurer obligatoirement une résolution spatial minimal de 100 pixels/cm.
- Les caméras visant à lire une plaque d'immatriculation doivent assurer obligatoirement une résolution spatial minimal de 200 pixels/cm
- Les caméras visant à Identifier des auteurs doivent assurer obligatoirement une résolution spatial minimal de 400 pixels/cm.

Une intelligence artificielle est intégrée au serveur de stockage et analyse d'image, cette IA devant permettre de détecter et avertir en cas de :

- Franchissement de ligne virtuelle
- Maraudage
- Apparition/disparition d'objets
- Objet laissé seul
- Regroupement d'individus / stationnement interdits
- Flux de passagers
- Indentification Individu
- Indentification Véhicule
- Flux de personnes et flux isolé
- Mesure de vitesse de véhicule

Les caméras multi capteurs visant la gestion des flux de passager assurent obligatoirement via leurs 4 objectifs couvrants les 360° sans rupture un nombre de pixels sur la cible de minimum 400 pixels par centimètre en lecture directe comme en enregistrement afin d'atteindre un niveau de détection via l'IA intégrée ou déportée.

Les caméra fixe, avec zoom numérique ou optique assurent la visualisation des zones suivantes :

- Limite Côté Piste et Côté Ville
- Les complexes entrées sorties, en permanence, dont le portillon, portails et barrière levante
- Les locaux et bâtiments techniques.
- Les linéaires des aérogares Est et Ouest

- Voir photos annexes pour l'ensemble des vues et des plans.

Les caméras PTZ visant la visualisation d'élément distant, permettront d'effectuer des pan pour pivoter, des Tilt pour s'incliner et du Zoom pour zoomer.

5.4 QUALITE DU SYSTEME ATTENDUE

5.4.1 Exigences liées aux Caméras

Le titulaire devra proposer à minima des équipements répondant aux caractéristiques décrites dans les chapitres suivants, cependant les caractéristiques en fonction des zones à surveiller devront être respecter. L'ensemble des caméras disposeront d'un moyen de stockage de masse amovible type carte SD. Les données devront être chiffrées sur la carte SD afin d'éviter toute fuite d'information en cas de vol ou de perte des cartes SD. L'ensemble des caméras disposeront d'un système de traitement de donnée par Intelligence Artificielle intégrée.

L'ensemble du système de vidéoprotection devra être équipé de boitier et fixation anti vandalisme. Une attention particulière devra être porté par le titulaire de l'accord-cadre dans l'intégration architecturale du système de vidéoprotection, les règles d'installation à respecter architecturalement sont les suivantes :

- Equipement en intérieur devra être confondu avec l'élément sur lequel il est installé
- Equipement en extérieur devra être visible dans un objectif de dissuasion

L'ensemble des caméras devront disposer d'Analytics compatibles avec l'ensemble des VMS ANSSI.

De plus, elles devront être conforme à la norme ONVIF et répondre aux spécifications ci-dessous :

AU MINIMUM :

- **Profil S**

Pour le streaming vidéo

Le profil S de l'ONVIF permet à un client conforme de configurer, demander et contrôler le flux de données vidéo sur un réseau IP à partir d'un périphérique conforme. Ce profil prend également en charge le contrôle PTZ, la réception de flux audio et de métadonnées et les sorties relais si ces fonctions sont prises en charge par le client.

- **Profil G**

Pour le stockage et l'enregistrement des bords

Les clients et les dispositifs conformes au profil G de l'ONVIF prennent en charge la configuration, la recherche, la lecture et la récupération des enregistrements sur le stockage embarqué/rattaché au réseau.

- **Profil T**

Pour un streaming vidéo avancé

Le profil T prend en charge les fonctions de diffusion vidéo telles que l'utilisation des formats d'encodage H.264 et H.265, les paramètres d'imagerie et les événements tels que la détection de mouvement et de sabotage. Les fonctionnalités obligatoires pour les périphériques comprennent également l'affichage à l'écran et le streaming de métadonnées. Le profil T couvre également les spécifications ONVIF pour le streaming HTTPS, la configuration PTZ, la configuration des régions de mouvement, les entrées numériques et les sorties relais, ainsi que l'audio bidirectionnel pour les appareils et les clients conformes qui prennent en charge ces fonctions.

- **Profil M**

Pour les métadonnées provenant d'applications d'analyse le profil M prend en charge un flux de métadonnées normalisé pour la communication des données d'analyse, des événements et de la position PTZ. Il offre des interfaces pour la classification générique des objets et des métadonnées spécifiques comme le véhicule et le corps humain.

Les caméras seront directement alimentées par les équipements actifs PoE++ type 3.

Dans les cas où la puissance délivrée par le Switch (PoE++ type 3) ne serait pas suffisante, le titulaire prévoira la fourniture et pose d'un injecteur PoE adapté.

Si des caméras devaient être alimentées en 230V, cette alimentation serait due par le présent lot depuis l'armoire électrique ondulée la plus proche.

5.4.1.1 Caméras fixes

Les caméras fixe seront de type IP « Box » pour les caméras en extérieur et de type « Bullet » pour les caméras en intérieur. Les caméras devront être adaptées aux conditions climatiques de la Réunion.

Les caméras embarquent dans leur processeur des systèmes intelligents tels que :

- Analyse du comportement (Apparition, disparition, vagabondage)
- Croisement (Ligne virtuelle, entrée/sortie, détection de direction)
- Amélioration de la qualité d'image (Détection de perte de mise au point, détection du brouillard)
- Détection (Détection de mouvement, sabotage, détection de visage, Détection audio)

Les caméras devront pouvoir être équipé d'un système de stockage de masse externe (carte SD avec données chiffrées)

Un système de réduction des distorsions d'objectif supprime l'effet bombé sur les bords des vidéos.

Les caméras possèdent à minimum les caractéristiques suivantes :

- Objectif vari focal motorisé de 2,8 ~ 12 mm (4,3x) ou numérique en fonction du besoin
- Résolution minimale de 2 mégapixels (2560 x 1920)
- Max. 60 ips toutes les résolutions (H.265/H.264)

- Compatible codec H.265, H.264 et MJPEG, multi-flux
- Jour/nuit (ICR), WDR (150 dB), dénébulisation
- Fonction Maraudage, détection directionnelle, détection de brouillard,
- Détection audio, auto-tracking digital, classification sonore, sabotage
- Détection de mouvement, relais
- Mode couloir
- Correction de distorsion d'objectif (LDC)
- PoE / 24 V CA, 12 V CC, compatible audio bidirectionnel

5 configurations de caméra fixe :

- Type 1 : Caméra fixe extérieure pour de la surveillance de ligne (100 pxl/cm)
- Type 2 : Caméra fixe extérieure pour de la lecture de plaque (200 pxl/cm)
- Type 3 : Caméra fixe extérieure pour de l'identification (400pxl /cm)
- Type 4 : Caméra fixe intérieur pour de la surveillance de ligne ou matérialisation d'infraction (100 pxl/cm)
- Type 5 : Caméra fixe intérieur pour de l'identification (400pxl /cm)

5.4.1.2 Cameras multi-capteurs

Les caméras multi-capteurs doivent pouvoir fonctionner à des températures allant jusqu'à 50 ˚ ainsi que dans des environnements exposés à l'eau ou très humides plus de 80% d'humidité.

Les caméras multi capteurs sont pourvues de trois ou quatre capteurs selon le besoin.

En utilisant une seule caméra au lieu de quatre, les caméras multi capteurs filment des vidéos avec un angle considérablement étendu.

Elles peuvent créer une seule vidéo en combinant les vidéos de chaque capteur jusqu'à 360° sans aucune marque de fusion.

Les caméras devront pouvoir être équipé d'un système de stockage de masse externe.

Caractéristiques techniques minimum :

- 3x ou 4x résolution 2560 x 1920 minimum
- 3x ou 4x objectifs vari focal motorisés
- 3x ou 4x 60 ips max. 5 Mpx (H.265, H.264)
- Stabilisation d'image numérique avec capteur gyroscopique intégré
- Compatible codec H.265, H.264, MJPEG
- Jour/nuit (ICR), WDR (120 dB)
- Détection de mouvement, sabotage, analyse vidéo avancée

5 configurations de caméra multi-capteurs :

- Type 6 : Caméra multi-capteurs extérieure pour de la surveillance de ligne (100 pxl/cm)
- Type 7 : Caméra multi-capteurs extérieure pour de la lecture de plaque (200 pxl/cm)
- Type 8 : Caméra multi-capteurs extérieure pour de l'identification (400pxl /cm)
- Type 9 : Caméra multi-capteurs intérieur pour de la surveillance de ligne ou matérialisation d'infraction (100 pxl/cm)
- Type 10 : Caméra multi-capteurs intérieur pour de l'identification (400pxl /cm)

5.4.1.3 Cameras PTZ extérieures

Les caméras PTZ doivent pouvoir fonctionner à des températures allant jusqu'à 50 ˚ ainsi que dans des environnements exposés à l'eau ou très humides plus de 80% d'humidité.

Les caméras sont dotées d'une résolution minimale de 4 MP et d'un zoom optique 40x pour des vues d'ensemble et des détails excellents.

Les caméras PTZ d'extérieurs haute performance permettent de lancer le suivi d'un simple clic, ainsi qu'une aide à l'orientation pour le suivi actif des objets et un positionnement rapide.

Un système d'amélioration de l'image produit des images aux couleurs plus saturées dans des environnements à faible luminosité et des images plus nettes des objets en mouvement.

Les fonctions de sécurité améliorées telles que le firmware signé et le démarrage sécurisé garantissent l'intégrité et l'authenticité du firmware.

Un système d'optimisation avec H.264/H.265 ou équivalent réduit considérablement les besoins en bande passante et en stockage.

Caractéristiques minimums :

- Capteur d'image CMOS progressive scan 1/2,8"
- Objectif 4,25–170 mm, F1.6–4.95
- Champ de vision horizontal : 65,1°–2,00° (2 Mp minimum)
- Champ de vision vertical : 39,1°–1,18° (2 Mp minimum)
- Mise au point automatique, iris automatique Jour et nuit
- Filtre infrarouge à retrait automatique
- Obscurité jusqu'à 0,3 lux
- Vitesse d'obturation 1/11000 s à 1/3 s avec 50 Hz 1/11000 s à 1/3 s avec 60 Hz
- Panoramique/Inclinaison/Zoom Panoramique : 360° infini, 0,05°–450°/s Inclinaison : 180°, 0,05°–450°/s
- Zoom : zoom optique 40x, numérique 12x, total 480x E-flip, 256 positions préréglées,
- Enregistrement de tour de garde (10 max., durée maximale de 16 minutes chacun),
- Ronde de contrôle (100 max.),
- Vitesse de zoom réglable,
- Rappel de mise au point

- Type 11 : Caméra PTZ extérieure

5.4.1.4 Caméras dômes :

CAMERA FIXE ANTIVANDALE (DOME) INTERIEUR

Les caractéristiques minimales seront les suivantes :

- Antivandale IK10
- Indice de protection IP52
- Champ de vision vertical 53-20°
- Optique avec focale variable
- Ajustement et réglage optique suivant la zone à surveiller
- Fonction identification possible

➢ Référence caméra : type 12

CAMERA DOME FISHEYE 360°

Il sera utilisé pour certaines zones de surveillance des caméras avec vision 360°.
Les caractéristiques minimales seront les suivantes :

- Antivandale IK10
- Indice de protection IP66
- Surveillance sur 360° avec une résolution de 8MP ou 12MP
- Capteur CMOS 1/1,7"
- Conversion à faible taux de distorsion d'images/différents flux
- Double résolutions full-HD
- Champ de vision vertical 181°
- Champ de vision horizontal 181°

➢ Référence caméra : type 13 (caméra vidéo fixe 360°)

CAMERA MOTORISEE PTZ ANTIVANDALE (DOME) ZOOM X30

Les caractéristiques minimales seront les suivantes :

- Caméra 1080P motorisée
- Antivandale IK08
- Indice de protection IP66
- Zoom optique 32x
- Mise au point instantanée
- Zoom progressif avec mise au point en continue
- Live 25im/s mini
- Minimum de 15 masques dynamiques
- Commutation jour/nuit automatique
- Orientation PTZ
- Alimentation POE

➢ Référence caméra : type 14

CAMÉRA MOTORISÉE PTZ ANTIVANDALE (DÔME) ZOOM X10

Les caractéristiques minimales seront les suivantes :

- Caméra 1080P motorisée
- Anti vandale IK08
- Indice de protection IP66
- Zoom optique 10x
- Mise au point instantanée
- Zoom progressif avec mise au point en continue
- Live 25im/s mini
- Minimum de 15 masques dynamiques
- Commutation jour/nuit automatique
- Orientation PTZ
- Alimentation POE

➢ Référence caméra : type 15

5.4.1.5 Dispositifs d'éclairage de scènes

Pour chaque point vidéo où cela nécessaire, le titulaire fournit et installe des dispositifs infrarouges pour l'éclairage de nuit. Ces dispositifs sont fixés de manière à éclairer correctement le périmètre de visualisation en privilégiant si possible les mâts et les bâtiments supports pour les équipements de vidéo ou de transmission.

Ces projecteurs infrarouges sont asservis à un système de détection de la luminosité permettant leur déclenchement et leur arrêt automatique.

Dans tous les cas, l'angle du faisceau doit être ajustable.

Les projecteurs peuvent être si nécessaire intégrés dans la caméra.

Dans le cas de projecteur séparé, la distance d'écartement entre la caméra et le projecteur dépasse 30 cm.

Tous les projecteurs doivent respecter la norme anti-vandale.

Les projecteurs doivent respecter la norme IP66.

Le système de refroidissement des LED doit être optimisé afin de maximiser la durabilité du dispositif.

La longueur d'onde utilisée doit être à minima de 850 nm.

La puissance des projecteurs doit être réglable.

La télémétrie doit être ajustable.

Les dispositifs doivent être équipés d'une cellule photoélectrique réglable.

Les dispositifs de fixation sont spécialement conçus et adaptés aux supports.

6. ANNEXE

6.1 EXIGENCES REGLEMENTAIRES EN CYBERSECURITE

Le système objet de ce CCTP est soumis à des règlementations très strictes en matière de cyber sécurité. Ci- dessous les règles de sécurité à déployer/respecter.

Le candidat doit faire une réponse pour chaque règle dans le document XLS fourni en annexe

- Statut (conforme/non conforme/partiellement conforme)
- Justification/explication/commentaires

Règles de sécurité	
Règles	Descriptif
Politique de sécurité SI	Le titulaire devra se conformer à la Politique de Sécurité des Systèmes d'Information de l'aéroport. Des adaptations ou des dérogations pourront être accordées en fonction des contraintes techniques, organisationnelles et métiers suite à validation du RSSI de l'aéroport
Homologation de sécurité	Des audits de sécurité et des analyses de risques seront réalisées sur le système fourni. Le titulaire devra collaborer avec l'aéroport (interview, fourniture des certifications, agréments ou tout autre justificatif attestant d'un certain niveau de Sécurité du titulaire et/ou du système fourni)
Cartographie	Le titulaire devra fournir les inventaires (matériel et logiciel), les schémas, la matrices de flux… Au démarrage du projet le titulaire devra fournir et/ou compléter les documents : - ARRG_Collecte_Renseignements_editeur.xlsx - ARRG_collecte_Securite_SI.xlsx - Architecture physique - Architecture logique TCP/IP (vlan, réseau IP) - Architecture applicative simplifiée Les inventaires et cartographies devront être maintenus à jour par le titulaire.

Règles de sécurité	
Règles	Descriptif
Maintien en condition opérationnelle et de sécurité	Le titulaire doit assurer un maintien en condition opérationnelle et de sécurité du système fourni : - Les matériels et logiciels fournis doivent être supportés, sous garantie et non obsolètes - Les matériels et logiciels doivent être maintenus à jour (mise à jour annuelle a minima) L'aéroport dispose d'un serveur de mise à jour Windows (WSUS). Le titulaire doit s'appuyer sur ce serveur pour mettre à jour automatiquement les composants Windows de son système. Le titulaire doit indiquer si les mises à jour WINDOWS automatiques peuvent poser problème. Si tel est le cas, il doit décrire les dispositifs et modes opératoires qui seront mis en place pour la mise à jour régulière des postes et serveurs Windows de son système. Cela doit être validé par le RSSI ARRG. A noter que les postes et serveurs Windows/Linux devront avoir un antimalware (fourni par la SA ARRG). Cet anti-malware sera configuré pour avoir des mises à jour automatiques des bases de signature anti-malware et des scans hebdomadaires de recherche de malwares. La SA ARRG fournira la procédure « PR-08-16_V4_procédure de maintien en condition de sécurité » à respecter. Le titulaire devra respecter les délais contractuels définis dans le contrat de maintenance pour les maintenances préventives et les maintenances correctives (panne ou dysfonctionnement à résoudre, vulnérabilités à corriger). De manière générale, si des mises à jour régulières ne peuvent pas être réalisées sur des composants du système (exemple : caméras), le titulaire devra à minima proposer des mesures pour limiter les risques liés à des vulnérabilités critiques.
Journalisation	Le système doit générer des journaux d'évènements avec possibilité d'archivage et export des journaux. Le système doit activer les logs sur l'ensemble des composants du système (serveurs, applications, switch, pare-feu, automate…) et renvoyer ses journaux d'évènements vers le serveur de centralisation de logs de l'aéroport (via le protocole syslog ou autre). Le socle minimal (relevé des connexions réussies/échouées,

Règles de sécurité	
Règles	Descriptif
	administration et changement de programme) à journaliser est fourni par la SA ARRG.
Corrélation et analyse des journaux	L'aéroport mettra en œuvre un serveur de type corrélation de logs (SIEM). Le titulaire devra fournir à l'aéroport la liste, la description et la composition (champs) des journaux d'évènements qui seront générés à partir du système fourni. Il devra également fournir l'emplacement et les procédures d'extraction des journaux.
Détection	L'aéroport souhaite que les composants Windows et linux du système soient protégés par un anti-malware avec base de signature maintenue à jour automatiquement et scan hebdomadaire. Les paramétrages et stratégies antimalwares seront réalisées par la SA ARRG. L'IPS/IDS sera activé sur le pare-feu ARRG pour tous les flux entrants/sortant du système. Dans l'idéal l'IPS/IDS doit être activé sur tous les flux internes du système (flux inter vlans). Le titulaire devra préciser s'il y a des contre-indications et documenter les éventuelles exceptions qui seront configurés dans les stratégies anti-malware et IPS/IDS.
Traitement des Incidents de sécurité Gestion des crises	Le titulaire doit collaborer avec l'aéroport en cas d'incident de sécurité ou de crise lié au système fourni.
Traitements des alertes	Dans le cadre de la maintenance préventive, le titulaire doit effectuer une revue régulière des alertes et journaux d'évènements et apporter les corrections appropriées.
Identification Authentification Droit d'accès	Des comptes nominatifs doivent être utilisés pour l'ensemble des utilisateurs et administrateurs du système. Les mots de passe doivent respecter la politique de mot de passe ARRG. L'authentification doit se faire via le compte et mot de passe de l'annuaire Active Directory de la SA ARRG. Cela permet d'avoir une gestion centralisée des identités et des accès.

Règles de sécurité	
Règles	Descriptif
Compte d'administration	Des comptes nominatifs et dédiés aux tâches d'administrations doivent être utilisés. Les mots de passe par défaut des comptes d'administration ou des comptes génériques doivent être modifiés. Les mots de passe d'administration doivent respecter la politique de mot de passe ARRG.
Environnement d'administration	L'aéroport a mis en œuvre un SI d'administration. Toutes les tâches d'administration informatique devront se faire via ce SI d'administration (bastion d'administration)
Cloisonnement	Le système fourni doit être isolé des autres systèmes ARRG. Un cloisonnement interne au sein du système SVP doit également être mis en place selon les préconisations de la SA ARRG
Filtrage	Les flux internes aux systèmes ou externes avec d'autres systèmes doivent être connus. Des règles de sécurité seront déployés sur les pare-feu afin d'autoriser uniquement les flux nécessaires. Le titulaire devra fournir la matrice des flux de son système.
Accès à distance	Le titulaire devra passer par la solution d'accès à distance de la SA ARRG. Cet accès à distance sera ouvert à la demande. Le titulaire ne pourra pas mettre en œuvre son propre accès à distance (sauf sur dérogation du RSSI ARRG).
Durcissement	Le système fourni doit être durci afin de limiter la surface d'attaque : uniquement les composants ou logiciels nécessaires doivent être installés, des restrictions de l'environnement utilisateur doivent être mis en place (exemple : pas d'accès au paramètres du système d'exploitation, pas d'accès aux paramètres de sécurité, impossibilité de désactiver des modules ou outils de sécurité, désactivation des outils de prise en main à distance,…), uniquement des protocoles sécurisés doivent être utilisés (SSH, https,…),… Le titulaire devra décrire l'ensemble des mesures de durcissement et de sécurité mis en œuvre sur les composants du système.
	A noter que les serveurs et postes de travail seront durcis avec les GPO, guides et politiques de l'aéroport.

Règles de sécurité	
Règles	Descriptif
Indicateurs	Des indicateurs annuels doivent être fournis à l'ANSSI. Le titulaire devra collaborer avec l'aéroport pour compléter ces indicateurs : - Pourcentage de postes et de serveurs non supportés - Pourcentage de postes et de serveurs non mis à jour - Pourcentage d'utilisateurs avec accès privilégiés - Pourcentage d'utilisateurs avec accès partagés - Pourcentage de secret ou mot de passe non modifiable - Pourcentage de ressources administrées via compte d'administration - Pourcentage de ressources administrées hors environnement d'administration - Pourcentage de ressources administrées via liaison non sécurisée

6.2 SPECIFICATION DE SECURITE DU SVP

Le système objet de ce CCTP est soumis à des règlementations très strictes en matière de cyber sécurité. Ci- dessous les règles de sécurité à déployer/respecter.

Le candidat doit faire une réponse pour chaque règle dans le document XLS fourni en annexe

- Statut (conforme/non conforme/partiellement conforme)
- Justification/explication/commentaires

Thématique	Description
Confidentialité	Chiffrer et authentifier les flux émis et reçus par les caméras : Les flux émis et reçus par les caméras (images, administration) doivent être chiffrés et authentifiés par des protocoles tels que TLS (1.2 minimum) ou IPsec. Une PKI de la SA ARRG permet de générer des certificats.
Durcissement	Les interfaces locales d'administration des caméras doivent être désactivées (exemple : via connectique USB ou via port console). De manière générale, il faut désactiver les fonctions qui ne sont pas réellement utilisées dans le cadre du SVP.
Gestion des comptes	Remplacer les mots de passe par défaut des caméras. Utiliser des mots de passe robuste qui respectent la politique de mot de passe de l'aéroport. Indiquer s'il est possible d'intégrer l'authentification au niveau des caméras à l'AD.
Gestion des comptes	Utiliser des comptes nominatifs pour se connecter à l'application de vidéosurveillance et l'enregistreur. L'authentification doit être intégrée à l'Active Directory de la SA ARRG.
Gestion des comptes	Remplacer les certificats installés par défaut dans le SVP (caméra, serveur VMS, logiciel client du poste vidéo) par des certificats générés par la PKI dédiée de la SA ARRG
Mise au rebut	Une attention particulière doit être portée sur les dispositifs en panne susceptibles de contenir des éléments cryptographiques ou des données du SVP (Caméras, carte SD) Il est recommandé, lorsque cela est possible, d'effacer voire de supprimer ces éléments avant envoi du dispositif pour réparation chez un prestataire. Lors d'une mise au rebut d'un dispositif, il faut s'assurer que ces éléments cryptographiques ne pourront pas être extraits. Dans le cas où ces éléments ne peuvent pas être effacés, il convient de procéder à la destruction physique du dispositif.
Physique	Installer les caméras à une hauteur hors portée des personnes et s'assurer que le câble n'est pas visible.
Sécurité de l'application	Les obligations de maintien en condition de sécurité (MCS) sont définies dans le contrat de maintenance et doit couvrir les composants techniques de l'application métier (Base de données, Serveur d'application, librairie de développement, etc.), l'application métier (identification et correction des vulnérabilités applicatives) et les composants industriels (les firmwares des caméras).
Sécurité de l'application	Les flux entre les clients (Postes de supervision) et les serveurs de vidéosurveillance doivent être chiffrés (exemple : TLS 1.2 minimum ou IPSEC)

Sécurité de l'application	Les logs applicatifs du SVP doivent être remontés à un serveur Syslog ARRG.
Accès aux interfaces d'exploitation et/ou d'administration	L'accès aux interfaces d'exploitation et/ou d'administration devra se faire via un navigateur. Cette interface devra obligatoirement être sécurisée via le protocole HTTPS avec du chiffrement TLS de version 1.2 au minimum.
Accès aux interfaces d'exploitation et/ou d'administration	Si un client lourd doit être déployé pour l'administration et/ou l'exploitation de la solution, ce client devra être sécurisé (chiffrement des flux client/serveur). Le titulaire devra : -> Préciser les mécanismes de sécurité mis en œuvre entre le logiciel client lourd et le serveur (exemples : type de chiffrement mis en place, type d'authentification mis en place,…) -> Préciser les fonctionnalités fournies par la ou les interfaces d'administration et/ou d'exploitation. -> Préciser les prérequis d'installation de ce logiciel (CPU, RAM, disque dur, connectiques,…).
Mode kiosque poste vidéo	Hormis le poste client du service sûreté qui sera seul autorisé à réaliser des extractions d'images, les postes vidéo devront fonctionner en mode kiosque : - Le poste doit se lancer et démarrer automatiquement et de manière transparente pour l'agent (sans saisie d'un login/mot de passe de session Windows par l'agent). - Le logiciel de visualisation VMS devra se lancer en mode kiosque de manière automatique. Ce sera le seul logiciel accessible par l'agent - L'agent utilisera un compte pour accéder au logiciel VMS (mire d'authentification du logiciel VMS) Le poste vidéo fonctionnera en mode kiosque et permettra de limiter les interactions de l'agent (pas d'accès à la session Windows). Le candidat doit fournir un descriptif ou une documentation sur le paramétrage du mode kiosque pour les postes vidéo.
authentification/Identification	Pour des raisons organisationnelles la SA ARRG souhaite que la gestion des comptes sur le logiciel VMS puisse faire de la façon suivante : -> accès des externes (exemple: sous-traitant sûreté) avec des comptes configurés dans la base locale du VMS. Le service sûreté est autonome pour la création/modification/suppression des comptes de sous-traitant sûreté.

	-> accès des utilisateurs de la SA ARRG avec leur compte Active Directory. Les comptes AD sont créés/modifiés/supprimé par la DSI ARRG
Authentification/Identification	Une politique de mot de passe doit pouvoir être configurée sur le logiciel VMS afin de forcer les comptes locaux à respecter la politique ARRG: nombre caractère minimum, types de caractères exigées (minuscule, majuscule, chiffre, caractère spéciaux), duré d'expiration du mot de passe, nombre d'échec de mot de passe autorisé, historique des mots de passe , obligation de changer son mot de passe à la première connexion, déconnexion de la session applicative sur le VMS au bout d'un délai d'inactivité.
authentification/Identification	Les authentifiants ne doivent pas être stockés en clair (sans chiffrement ou condensation) quelle que soit la méthode de stockage (fichier, base de données, scripts …). Des droits doivent être positionnés afin qu'aucun authentifiant ne soit accessible en lecture, même sous forme chiffrée, aux utilisateurs.
authentification/Identification	Le chiffrement des authentifiants doit utiliser des algorithmes éprouvés (ex : http://www.ssi.gouv.fr/administration/guide/cryptographie-les-regles-du-rgs/). Le transport des authentifiants doit être chiffré (https, LDAPS, Kerberos, ssh …). Ces règles sont valables aussi bien côté client que serveur. Aucun algorithme propriétaire d'authentification et de chiffrement ne sera autorisé
authentification/Identification	Tous les comptes (système et applicatif) doivent être configurés de manière sécurisée ; les points suivants sont à prendre en compte : • désactivation des comptes par défaut, • désactivation des comptes sans mot de passe • modification des mots de passe par défaut • renommage des comptes privilégiés, • mise en place de comptes nominatifs avec identifiant unique, • blocage au bout d'un certain nombre de tentatives infructueuses, Tous les comptes (système et applicatif) devront être conforme à la politique de gestion des comptes et des mots de passe de l'ARRG.

Gestion des droits	Les systèmes et applications devront être configurés afin que : - chaque profil d'utilisateurs n'ait accès qu'aux fonctions qui lui sont nécessaires pour remplir sa mission. - chaque profil d'utilisateurs n'ait accès qu'aux Postes Opérateurs nécessaires pour remplir sa mission - chaque utilisateur n'ait accès qu'au profil qui lui est attribué Pour compléter, ces droits peuvent être: - Droit de lecture : les utilisateurs auront différents accès à l'information - Droit de contrôle : les utilisateurs auront différents niveaux de contrôle selon leurs fonctions et responsabilités. - Droit d'administration : les utilisateurs auront différents niveaux d'administration de l'outil. Le paramétrage de l'outil pourra être modifié dans une certaine mesure par des acteurs de l'aéroport disposant des droits d'administrateurs nécessaires. - Droit de développement : certains utilisateurs pourront réaliser des développements spécifiques selon le niveau d'autonomie souhaité par l'aéroport. Les droits pourront être déclinés en fonction du poste, des vues, des usages, de la zone géographique. Pour simplifier l'attribution des droits, des profils types ou groupe de profil pourront être créés avec des droits spécifiques.
Accès physique	Les liaisons filaires de télécommunications et électrique transmettant des données ou assurant la sureté de l'aéroport doit être protégé contre les dommages (faiblesse physique, déconnection, section volontaire…).
Accès physique	La solution devra de limiter les points d'accès et protéger contre l'accès physiques lors des raccordements des caméras notamment pour les équipements exposés côté ville. Le titulaire devra décrire les moyens mis en œuvre pour protéger l'accès à ces équipements.
Sécurité des réseaux	La solution devra garantir l'intégrité et l'authenticité des flux émis et reçus par la couche terrain. Le titulaire devra décrire les protocoles de communication utilisés ainsi que les principes de sécurité applicables.
Sécurité des réseaux	Le titulaire devra s'assurer que la solution permet le cloisonnement logique des équipements selon les différentes zones de sécurité et l'exposition des équipements. Pour information, il était identifié 6 VLANs différents : 1 val serveur, 1 vlan poste vidéo, 4 vlan caméras. Le titulaire devra être force de proposition pour l'architecture du cloisonnement dans le respect des bonnes pratiques.
Sécurité des réseaux	Tous les équipements devront être synchronisés à l'aide du protocole NTP via les serveurs de temps mis à disposition par l'ARRG.
Sécurité des réseaux	Les caméras devront être authentifiées au travers certificats respectant la norme 802.1X quel que soit la connectivité. Les certificats seront gérés par la PKI de l'ARRG. Dans le cas où les équipements sont dans l'incapacité de gérer les certificats, la vérification par adresse MAC devient obligatoire et sera soumis à dérogation.

Sécurité des réseaux	La connectivité filaire pour les dispositifs de vidéosurveillance et de contrôle d'accès physique est obligatoire.
Sécurité des réseaux	L'utilisation de connectivité sans fil devra faire l'objet d'une dérogation (exemple : contraire géographique du bâtiment). Le titulaire devra confirmer que la solution SVP permettra de sécuriser la connectivité (ex : TLS ou IPSEC) ou a minima d'être compatible avec une solution de sécurité de type encapsulation IPSEC.
Sécurité des systèmes	Tout import de données sur site via support de stockage USB devra être contrôlé sur la station blanche de la SA ARRG Cette règle est valable : - quelle que soit la source de données : clé USB, disque de dur externe - quelle que soit la phase du projet : conception, déploiement, exploitation courante, opération de maintenance
Sécurité des systèmes	Le titulaire devra fournir la liste des clés USB utilisées dans le cadre de l'accord-cadre (revendeur, modèle, ID de série). Seule cette liste sera autorisée sur les systèmes.
Sécurité des systèmes	L'intégrité et l'authenticité des matériels, des logiciels et des données livrées par le titulaire doivent être garantis ainsi que les mises à jour. Exemple : Par récupération des correctifs sur les sites officiels des éditeurs et vérification de leur signature électronique si disponible.
Sécurité de la donnée	Les données sensibles ne doivent être stockées en clair (sans chiffrement ou condensation) quelle que soit la méthode de stockage (fichier, base de données, scripts …). Des droits doivent être positionnés afin qu'aucun authentifiant ne soit accessible en lecture, même sous forme chiffrée, aux utilisateurs. Le chiffrement des authentifiants doit utiliser des algorithmes éprouvés (ex : http://www.ssi.gouv.fr/administration/guide/cryptographie-les-regles-du-rgs/).
Stockage et archivage	La solution doit permettre d'effectuer des archivages et stockages avec identification précise des périodes correspondant aux données.
Stockage et archivage	Le titulaire doit superviser l'espace disque local des équipements (ex : caméras) qui génèrent et stockent les journaux. Les serveurs et poste de travail seront supervisés par les systèmes centralisés de l'ARRG basé sur CENTREON.
Stockage et archivage	Les mécanismes de gestion des traces, système et applicatif, doivent réaliser une sauvegarde régulière des enregistrements afin de prévenir une perte de ces enregistrements provoquée par un dysfonctionnement du système. La durée de rétention des données doit être de 6 mois glissant
Stockage et archivage	Les données sauvegardées sont idéalement stockées dans une base de données d'un format non-propriétaire.

Stockage et archivage	Le titulaire devra fournir les procédures de sauvegarde et restauration de la solution.
Résilience	Tous les équipements serveurs et stockeurs doivent disposer d'une double alimentation afin de pourvoir pallier une perte de l'énergie principale via une alimentation de secours
Résilience	En cas de perte de liaison, la solution doit être en capacité de stocker temporairement des vidéos/images sur une durée de 24 heures sur chaque caméra. Une carte SD ou un stockage local peut être déployé à cet effet. A noter que les données doivent être chiffrées en local afin d'éviter des fuites de données en cas de perte ou de vol de la caméra ou de la carte SD
Horodatage	Tous les équipements devront être synchronisés à l'aide du protocole NTP via les serveurs de temps mis à disposition par l'aéroport.
Journaux	La solution fournie par le titulaire devra produire des journaux d'évènements (logs). Les journaux doivent si possible être générés dans un format interprétable, c'est-à-dire compréhensible à la lecture et facilement analysable de manière automatique par des outils informatiques.
Journaux	Il doit ainsi être possible d'enregistrer des évènements des systèmes d'exploitation et des applications liés à : - l'authentification (réussites et échecs d'authentification, élévations de privilèges, etc.) - gestion des comptes et des droits (ajouts/ suppressions de comptes/groupes/rôles, etc.) - accès aux ressources (accès ou tentatives d'accès en lecture/écriture/exécution aux ressources) - Modification des stratégies de sécurité (éditions, applications, réinitialisations de configurations, etc.) - activité des processus (démarrages/arrêts, dysfonctionnements, etc.) - activité des systèmes (démarrages/arrêts, dysfonctionnements/surcharges du système, etc.) - la sécurité - l'activité correspondant au service fourni par l'applicatif (par exemple l'accès à une ressource).
Journaux	L'accès aux journaux des événements doit être strictement réservé aux personnes habilitées.
Journaux	Un évènement doit contenir en particulier une source identifiable permettant de déterminer avec le plus de précision possible son origine : date, heure, identité de l'utilisateur, adresse de l'équipement d'origine et résultat de l'authentification.
Journaux	Ces logs devront également être envoyés vers un serveur de centralisation de logs (fourni par la SA ARRG) via le protocole syslog ou encore snmp.

Journaux	Des rapports réguliers sur la base des journaux d'événements métier devront être disponibles afin de pouvoir générer des rapports. Le titulaire devra fournir la liste des rapports disponible par la solution tel que : - les caméras n'ayant pas communiqué ; - dégradation des images selon les caméras;
Journaux	Afin d'éviter la saturation des disques des équipements qui produisent ou centralisent des journaux, il est demandé de créer une partition dédiée aux journaux d'évènements et disposant de droits d'accès restreints. Cette mesure permet d'éviter la défaillance du système ou de certains services qui n'auraient pas d'espace disque suffisant pour fonctionner correctement. Cependant des journaux pourraient être perdus si la partition dédiée venait à être saturée à son tour. C'est la raison pour laquelle une politique de rotation adéquate des journaux doit être mise en œuvre en complément de cette mesure.
Alertes	Le titulaire doit s'assurer que les alertes remontent en temps réel au centre de supervision
Alertes	En parallèle de rapports réguliers sur la base des journaux d'événements métier, il est demandé de configurer des alertes en temps réel qui peuvent être rapidement prises en compte par le gestionnaire du système. Ces alertes concernant la vidéosurveillance doivent être configurées pour tout événement d'un niveau de criticité important. Par exemple : • Défectuosité d'un élément support (caméra, alertes systèmes et applicatives du serveur de gestion) ; • Saturation de l'espace de sauvegarde des vidéos ;

6.3 MAINTENANCE SI ET MAINTIEN EN CONDITION DE SECURITE DU SVP

Dans le cadre de la maintenance, le titulaire doit assurer un maintien en condition opérationnelle et de sécurité des équipements et logiciels déployés.

- Il doit s'assurer que les matériels et logiciels fournis soient supportés, sous garantie et non obsolètes tout au long du cycle de vie du système à maintenir
- Il doit assurer une veille concernant les matériels et logiciels fournis. Il doit prévenir sans délai l'ARRG si des vulnérabilités de sécurité sont découvertes sur les versions systèmes ou logicielles de la solution mise en œuvre. Le Titulaire doit corriger sans délai ces vulnérabilités tout en garantissant le bon fonctionnement du système.

Ces prestations visent à permettre le maintien en condition opérationnelle du système fourni à titre préventif ou correctif.

- Par « préventif », on entend les mesures d'entretien exécutées pour éviter la survenance d'anomalies.
- Par « correctif », on entend les mesures consistant à corriger des anomalies ou à appliquer des mises à jour critiques.

A noter qu'une maintenance trimestrielle est demandée sur les aspects SI.

Ainsi, les prestations de maintenances attendues sont :

- La maintenance corrective ;
- La maintenance préventive.

6.3.1 Prestation de maintenance préventive

Au titre de la maintenance préventive, il sera demandé au prestataire d'effectuer un contrôle trimestriel afin de contrôler le bon fonctionnement de la solution :

- Audit des journaux systèmes et/ou applicatifs
- Mise à jour des documents décrivant le système : inventaire des équipements, schémas, synoptiques, matrice des flux…
- De vérifier et de mettre à jour les logiciels (patch de sécurité) si nécessaire ;
- Vérifier le bon fonctionnement global et unitaire de la solution ;
- De relever d'éventuels dysfonctionnements liés au matériel ou aux applications ;
- Vérifier le bon fonctionnement des PC de maintenance/administration (y compris mise à jour du poste : OS et base de signature antivirus)

Le titulaire devra prévoir une mise à jour complète de la solution a minima une fois par an. Cela comprend :

- Firmware des équipements terrain (caméras,…)
- Version des applications et composants logiciels

L'aéroport dispose d'un serveur de mise à jour Windows (WSUS). Le titulaire doit s'appuyer sur ce serveur pour mettre à jour automatiquement les composants Windows de son système. Le titulaire doit indiquer si les mises à jour WINDOWS automatiques peuvent poser problème. Si tel est le cas, il doit décrire les dispositifs et modes opératoires qui seront mis en place pour la mise à jour régulière des postes et serveurs Windows de son système.

Si la mise à jour automatique n'est pas préconisée par le titulaire, ce dernier devra se charger de sa mise à jour par un autre moyen et informer la DSI de son intervention.

Un procès-verbal d'intervention incluant les mises à jour qui ont été réalisées devra être communiqué à la DSI.

Les interventions du Titulaire, devront s'effectuer sans perturber le fonctionnement des services rendus et suivant un calendrier coordonné avec les services de la SA ARRG (Informatique / Technique / Sûreté / exploitation aéroportuaire).

Afin d'éviter tout risque d'arrêt ou de perturbation du système, le prestataire retenu devra indiquer dès sa prise de connaissance de l'existant et de manière systématique après interventions, ses préconisations, contrôles réguliers à effectuer et préconisation de surveillance.

6.3.2 Prestation de maintenance corrective

6.3.2.1 Incident / Panne et GTI/GTR

Le titulaire prendra en compte les incidents à partir du constat du défaut ou de la demande d'intervention de la SA ARRG et jusqu'à leurs résolutions.

Le prestataire devra fournir un rapport après chaque intervention de maintenance préventive. Il devra se conformer et utiliser le modèle de rapport fourni par la SA ARRG.

Trois niveaux de gravité sont définis :

- Gravité 1 : incident ou dégradation du service bloquant tout ou partie du fonctionnement.

  Exemple : caméra non fonctionnelle mettant en jeux la sûreté.

- Gravité 2 : incident ou dégradation du service ayant un impact significatif sur tout ou partie du fonctionnement qui entraine une dégradation de la qualité de service.

  Exemple : anomalie sur un ou plusieurs des logiciels installés suite à une mise à jour logicielle ou hors mise à jour logicielle, entrainant l'impossibilité d'accéder au service

- Gravité 3 : dysfonctionnement ou dégradation du service mineur rendant certaines fonctionnalités non importantes indisponibles.

  Exemple : anomalie d'affichage

Le niveau de gravité d'un incident sera défini par la SA ARRG.

En fonction de la nature du problème rencontré, un appel à un guichet unique de prise en charge des incidents pourra déclencher l'intervention afin de diagnostiquer et corriger le dysfonctionnement constaté.

Le tableau ci-après résume les délais demandés :

Gravité	GTI*	GTR*	Jours	Amplitude horaire
1	1 Heure	4 Heures	7 jours /7	24 Heures / 24
2	2 Heures	8 Heures	7 jours /7	24 Heures / 24
3	8 Heures	10 Jours	5 jours /7	8:00 H – 18:00 H

* GTI : Garantie de temps d'intervention

* GTR : Garantie de temps de rétablissement

6.3.2.2 Sécurité des produits et services fournis par le prestataire

Le prestataire doit assurer une veille concernant les matériels et logiciels fournis. Il doit prévenir sans délai l'ARRG si des vulnérabilités de sécurité sont découvertes sur les versions systèmes ou logicielles de la solution mise en œuvre. Le Titulaire doit corriger ces vulnérabilités selon les engagements de délais définis ci-dessous tout en garantissant le bon fonctionnement du système.

Type de vulnérabilité	A compter de la mise en évidence de la vulnérabilité, délai de mise à disposition d'une analyse d'impact et d'un plan de correction	Délai de mise en œuvre d'une solution palliative ou de contournement ne modifiant en rien le prix et les fonctionnalités des produits et services fournis au titre du Contrat	Délai de mise en œuvre de la correction de la vulnérabilité
Vulnérabilité majeure**	2 jours ouvrés	5 jours ouvrés	10 jours ouvrés
Vulnérabilité mineure	15 jours ouvrés	30 jours ouvrés	40 jours ouvrés

La prestation de correction sera faite sur demande de l'aéroport. Le prestataire fournira un devis en fonction de la complexité et de la charge de travail nécessaire. Un bon de commande sera alors établi selon les coûts en vigueur dans le Bordereau de Prix Unitaires.

** Vulnérabilité majeure : désigne une Vulnérabilité, pouvant avoir des conséquences significatives sur les données et/ou le système d'information du Client/Bénéficiaire

6.4 FICHE TECHNIQUE LSI (POUR LE REPERAGE)

FICHE TECHNIQUE Page 31/65	LSI	Aéroport de La Réunion Roland Garros S.A. ARRG

LSI 2.1 XXXXX

Les fibres optiques

Les prises	Description
A01 à A06	Vers XX
A07 à A12	Vers XX
B01 à B06	Vers XX
B07 à B12	Vers XX

Les RJ45

Les prises	Localisation
A01	Equipement XX
A02	
A03	
A04	
A05	
A06	
A07	
A08	
A09	
A10	
A11	
A12	
A13	
A14	
A15	
A16	
B01	
B02	
B03	
B04	
B05	
B06	
B07	
B08	
B09	
B10	
B11	
B12	
B13	
B14	
B15	
B16	

6.5 LISTE DU FICHIER « ANNEXE SI CCTP »

- ARRG_Charte prestataires SI
- ARRG_Clausier-RGPD_accord-cadre-SVP
- ARRG_Clausier-SSI_accord-cadre-SVP
- ARRG_Conformité Sécurité SI_accord-cadre-SVP
- ARRG_Plan-assurance-securite_PAS__accord-cadre-SVP