

**MARCHE PUBLIC DE TECHNIQUES DE L'INFORMATION ET
DE LA COMMUNICATION**

**CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES
(CCTP)**

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

CHAPITRE 1	Objet et dispositions générales.....	3
ARTICLE 1.1	Présentation de la DIR Est – Services concernés	3
ARTICLE 1.2	Description générale	4
ARTICLE 1.3	Description de l'ouvrage.....	5
ARTICLE 1.4	Normes et règlements applicables.....	6
ARTICLE 1.5	Système DAI actuel.....	7
1.5.1	Caméras DAI.....	7
1.5.2	système de la gestion de détection automatique d'incident (DAI)	7
CHAPITRE 2	nouvelle DAI.....	9
ARTICLE 2.1	Périmètre technique	9
2.1.1	Objectif de la nouvelle DAI	9
2.1.2	Redondance souhaitée du système à mettre en œuvre	9
2.1.3	Solution applicative	10
2.1.4	Proposition matérielle	10
ARTICLE 2.2	Transfert de compétence et formation	11
ARTICLE 2.3	Garanties	11
ARTICLE 2.4	Ouverture à variantes.....	11
CHAPITRE 3	Besoin fonctionnel du système DAI.....	12
ARTICLE 3.1	Principe de la DAI.....	12
3.1.1	Définition des détections.....	12
3.1.2	Performances des détections	13
3.1.3	Fausse alarmes.....	13
3.1.4	Taux de détection.....	13
3.1.5	Bougé caméra.....	14
3.1.6	Dégradation de la qualité de l'image	14
3.1.7	Perte ou dégradation du signal vidéo	14
3.1.8	Défauts fonctionnels et techniques.....	14
3.1.9	Réinitialisation	14
ARTICLE 3.2	Affectation des détections en fonction des caméras	15
3.2.1	Tunnel de bois de Peu	15
3.2.2	Tunnel de Fontain	15
3.2.3	Fonctionnement en exploitation.....	16
CHAPITRE 4	Essais et contrôles.....	17
4.1.1	Recettes de contrôle et essai	18
ARTICLE 4.2	Opération de révision à 6 mois	22
ARTICLE 4.3	Documentation	22
CHAPITRE 5	Préparation, coordination et exécution de la prestation	22
ARTICLE 5.1		22

ARTICLE 5.2	Période de préparation - Programme d'exécution de la prestation	22
ARTICLE 5.3	Contraintes d'exploitation	23
ARTICLE 5.4	Hygiène et sécurité.....	23
5.4.1	PPSPS	23
CHAPITRE 6	Cybersécurité	24
ARTICLE 6.1	COMPOSANTS COMMUNS D'ADMINISTRATION	24
6.1.1	Collecteur de logs	24
6.1.2	Sauvegarde des données opérationnelles	24
6.1.3	Synchronisation horaire – serveur ntp.....	24
6.1.4	Authentification des utilisateurs	24
6.1.5	Antivirus	25
ARTICLE 6.2	Documents et fichiers relatifs à la cybersécurité à fournir par le titulaire	25
6.2.1	Données confidentielles.....	25
6.2.2	Fonctionnement sans média USB	25
6.2.3	Plan d'Assurance Sécurité Projet	25
6.2.4	Documentation des actions de configuration	25
6.2.5	Procédures d'installation, sauvegarde et restauration	26
6.2.6	Inventaire et cartographie des livrables.....	26
6.2.7	Risques résiduels.....	26
6.2.8	Comptes et mots de passe configurés	26
6.2.9	Cahier de recette des fonctions de sécurité	26
6.2.10	Maintien en conditions de sécurité	26
6.2.11	EXIGENCES CYBERSÉCURITÉ	27
ARTICLE 6.3		28

CHAPITRE 1 Objet et dispositions générales

ARTICLE 1.1 Présentation de la DIR Est – Services concernés

La voie des Mercureaux fait partie du réseau routier national couvert par la DIR Est représentée par le Service Régional d'Exploitation et d'Ingénierie Franche-Comté (SREI FC). En tant qu'exploitant de la RN57 dans le Doubs, le SREI FC assure l'entretien et l'exploitation de la voie des Mercureaux et des deux tunnels (Bois de Peu et Fontain) qui la composent.

Le CISGT Vauban :

- assure la surveillance 24h/24 et 7j/7, et la maintenance des équipements dynamiques de la voie des Mercureaux ;
- organise la maintenance préventive et curative de ces mêmes équipements ;
- accueille le PC Trafic dont le rôle est de collecter, traiter et redistribuer toute l'information liée à l'exploitation ;

Le Service systèmes et réseaux (SeSyR) organise et coordonne l'administration des systèmes et réseaux de l'ensemble des tunnels de la DIR Est.

Le District de Besançon, représenté par le CEI de la Vèze assure l'entretien et l'exploitation de la RN 57 sur la voie des Mercureaux.

ARTICLE 1.2 Description générale

La DIR Est a pour projet de rénover la partie logiciel et serveur de son système de vidéo-surveillance et détection automatique d'incident (DAI) pour les deux tunnels de la voie des Mercureaux (25), notamment pour une problématique d'obsolescence.

Le présent Cahier des Clauses Techniques Particulières (CCTP) est relatif aux travaux de renouvellement de la DAI de la voie des Mercureaux, dont les principaux objectifs sont les suivants :

- la fourniture et le paramétrage des nouveaux serveurs, analyseurs et enregistreurs
- la fourniture des systèmes applicatifs ;
- la configuration de la solution ainsi que sa vérification et la validation des performances pour l'adapter aux spécificités de la section ;

Des interventions seront par ailleurs nécessaires dans le CISGT et dans les locaux techniques associés situés à proximité immédiate des tunnels : l'un à la tête « Doubs » du Tunnel de Bois de Peu et l'autre à la tête « Ouest » du Tunnel de Fontain.



Figure 1: implantation des locaux techniques

Les baies pouvant accueillir les différents serveurs sont situées dans les locaux techniques :

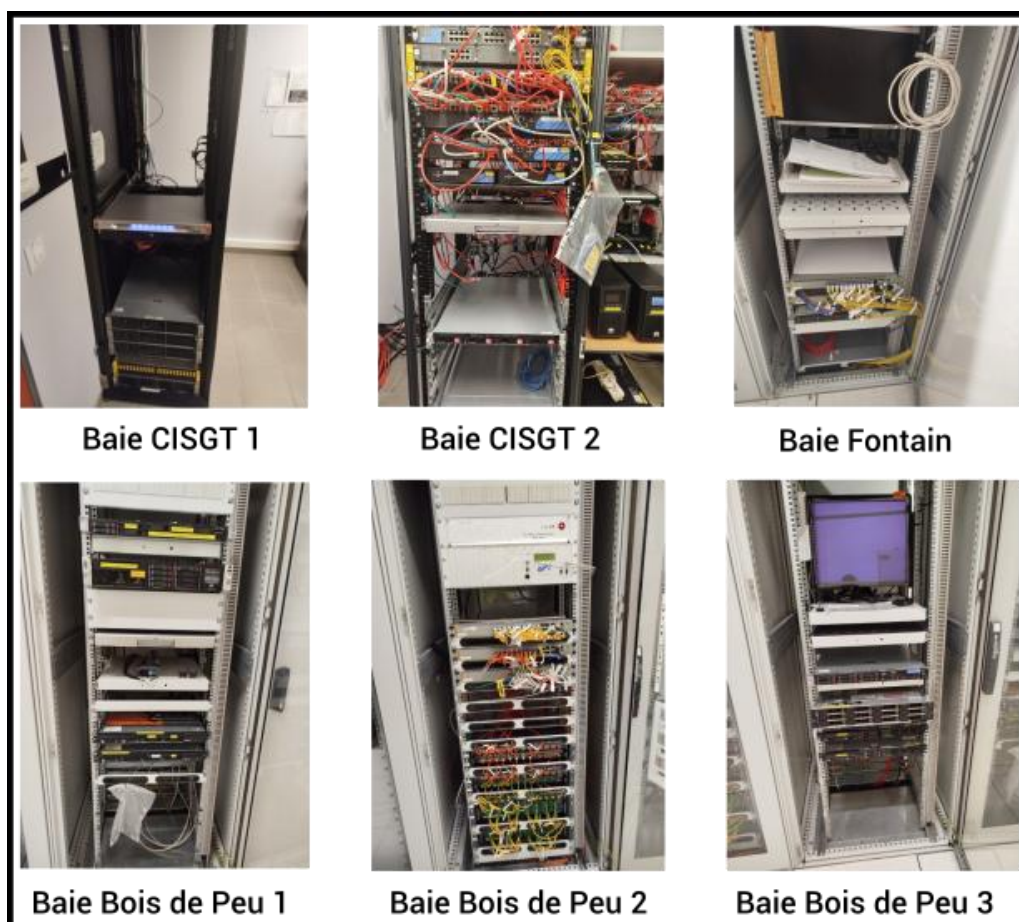


Figure 2: Baies

techniques de la voie des Mercureaux

Les éléments suivants ne sont pas intégrés aux prestations demandées dans le cadre de cette consultation :

- intervention ou remplacement des caméras de la DAI
- modification du réseau de fibre optique
- intervention sur les autres solutions logicielles utilisées par le CISGT Vauban (surveillance video Genetec, système d'assistance à la gestion du trafic, gestion technique centralisée...)

ARTICLE 1.3 Description de l'ouvrage

Les ouvrages concernés par le présent marché sont situés dans le département du Doubs à proximité de Besançon, sur la Voie des Mercureaux (N57) entre l'échangeur de Beure et l'échangeur de La Vèze. Le tunnel de Bois de Peu a une longueur de l'ordre de 570 m.

Au sens de l'annexe 2 de la Circulaire 2006-20 relative à la sécurité des tunnels routiers du réseau national, le tunnel de Bois de Peu est classé de la façon suivante :

- tunnel non urbain de moins de 800 m ;
- 2 tubes à circulation unidirectionnelle ;
- trafic non faible ;
- gabarit supérieur à 3,50 m ;
- autorisé au transport des marchandises dangereuses (TMD) ;
- degré de permanence et de surveillance : D4 – surveillance humaine permanente depuis la salle de contrôle Vauban.

Le tunnel de Fontain, d'une longueur inférieure à 300 m est lié au tunnel de Bois de Peu par une logique d'itinéraire.

Par conséquent, au sens de l'annexe 2 de la circulaire 2000-63 relative à la sécurité des tunnels routiers du réseau national, le tunnel de Fontain est classé de la façon suivante :

- tunnel non urbain de moins de 300 m ;
- 2 tubes à circulation unidirectionnelle ;
- trafic non faible ;
- gabarit supérieur à 3,50 m ;
- autorisé au transport des marchandises dangereuses (TMD).

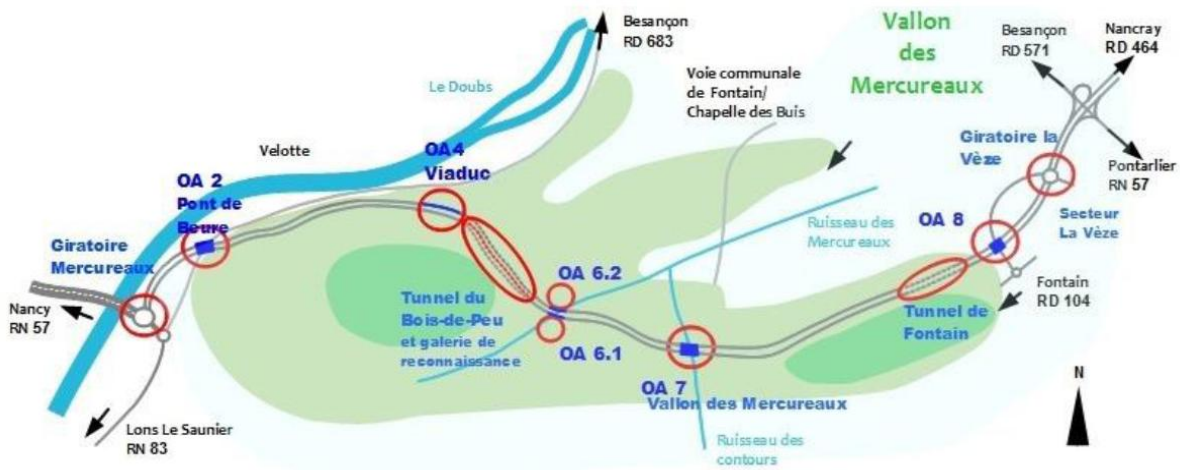


Figure 3: synoptique des ouvrages de la voie des Mercureaux – la DAI couvre les 2 tunnels

ARTICLE 1.4 Normes et règlements applicables

L'installation sera conforme aux normes et décrets en vigueur en date du présent CCTP.

Le présent projet détaillé prend en compte les lois, décrets, arrêtés, circulaires, normes, règlements et textes généraux applicables à ce type de projet, en particulier :

- Règlement Général sur la Protection des Données (RGPD – 25 mai 2018)
- Loi n°2011-167 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI 2),
- Articles L.223-1 à L.223-9, L.251-1 à L.255-1 et R.223-1 à R.223-2 du Code de la sécurité Intérieure,
- le décret n° 2005-701 du 24 juin 2005 relatif à la sécurité d'ouvrages du réseau routier,
- la circulaire interministérielle n°2006-20 du 29 mars 2006 relative à la sécurité des tunnels routiers d'une longueur supérieure à 300 mètres
- l'annexe n°2 à la circulaire interministérielle n° 2000-63 du 25 août 2000 relative à la sécurité dans les tunnels du réseau routier national : « Instruction technique relative aux dispositions de sécurité dans les nouveaux tunnels routiers (conception et exploitation) »
- le décret n°96-926 modifié du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité
- les arrêtés des 3 et 21 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance
- Vidéoprotection « classique » – Synthèse des références juridiques applicables – 18 novembre 2024 -
- document de la Commission Nationale de l'Informatique et des Libertés (CNIL)
- Analyser le statut d'un modèle d'IA au regard du RGPD – 22 juillet 2025 – document de la Commission Nationale de l'Informatique et des Libertés (CNIL)
- la norme NF C 15 100 : installations électriques à basse tension

- la norme NF EN 60529 : degrés de protection procurés par les enveloppes
- toutes normes relatives à la protection des travailleurs dans les établissements qui mettent en œuvre des courants électriques
- le guide du CETU de mai 2015 intitulé « Détection Automatique d'Incidents par analyse d'image en tunnel » ou nouveau document en vigueur à la date de publication de la consultation,
- l'arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité
- le PSSIE (POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT)
- le Guide d'hygiène informatique de l'ANSSI

Les équipements installés à l'intérieur des tunnels sont soumis à l'annexe n°2 à la circulaire interministérielle n° 2000-63 du 25 août 2000 relative à la sécurité dans les tunnels du réseau routier national et notamment le chapitre 4 « comportement au feu ». Lorsque l'interprétation du présent document et des textes officiels aboutit à une contradiction, la DIRE se réserve le droit de définir la solution qu'elle jugera la plus appropriée sans modification du prix ou de délai.

Les matériels et logiciels installés devront être soumis à l'accord préalable du maître d'œuvre

ARTICLE 1.5 Système DAI actuel

1.5.1 Caméras DAI

Les caméras DAI ont une double fonction : d'une part visualiser le trafic routier dans le tunnel, d'autre part analyser les images et envoyer une alarme en cas de détection d'incident particulier (voiture arrêtée, accident, piéton, ...). Ces alarmes sont transmises à l'opérateur situé en salle opérationnelle du CISGT Vauban de façon à pouvoir déclencher les mesures de sécurité adéquates. Les flux vidéos DAI sont visualisables en continu depuis la salle opérationnelle du CISGT Vauban. Les flux vidéos continus sont conservés dans le local technique du tunnel de Bois de Peu, sur une période de 7 jours glissants. L'ensemble pour les 2 tunnels est constitué de 28 caméras fixes et de 4 caméras thermiques.

Tunnel Bois de Peu

- 16 caméras fixes (8 par tube) -Hanwha XNB 6000 - flux H264 Résolution 800x448 (16/9) 5ips
- 2 caméras fixes thermiques sur chaque entrée du tube - Axis Q1941-E-PT – flux H264 , résolution 768x576 (4/3) , 30ips ;

Tunnel de Fontain

- 12 caméras fixes (6 par tube)-Hanwha XNB 6000 - flux H264 Résolution 800x448 (16/9) 5ips,
- 2 caméras fixes thermiques sur chaque entrée du tube - Axis Q1941-E-PT – flux H264 , résolution 768x576 (4/3) , 30ips ;

Les implantations ainsi que les vues caméra sont disponibles en annexe 3, 4, 5 et 6 au CCTP.

1.5.2 système de la gestion de détection automatique d'incident (DAI)

Le système est supporté par :

- 1 serveur DAI qui assure la centralisation des alarmes, des séquences d'incidents, des configurations du système DAI et l'enregistrement. Il est situé dans le local technique de Bois de Peu

- 1 analyseur pour les flux vidéo numériques en provenance des caméras de vidéosurveillance avec applicatif propriétaire CITILOG (version 8 - 2016) permettant la détection et analyse d'incident routier. Ils sont situés dans le local technique de Bois de Peu.

Ce système est composé de 2 serveurs HPE proliant dl20 gen 9 xeon e3-1240V.

- 1 ordinateur poste client, permettant le pilotage à distance du serveur et l'affichage d'incident en temps réel. Actuellement ce poste accueille la DAI et le système de vidéosurveillance Genetec ;
- 1 écran déporté en salle se déclenchant en cas de détection ;
- 1 réseau fibre en étoile permettant de connecter l'ensemble du système (connection sur les switchs via SFP en 1Gbit/s).

Les enregistrements vidéo sont assurés en parallèle par un enregistreur Vidéo Genetec, qui ne fait pas l'objet de la présente consultation.

Le système DAI ne dispose pas d'interfaces avec les dispositifs suivants :

- Mur d'image Genetec ;
- Système d'Aide à la Gestion du Trafic (SAGT Vauban) ;
- Gestion Technique Centralisée Tunnels (GTC) qui va être renouvelée en 2026 - 2027. Une communication devra cependant être assurée entre la DAI et la future GTC : ceci sera fait par le futur titulaire du marché GTC.

En tunnel le système DAI permet la détection :

- De fumée, de perte de visibilité (fumée+brouillard) ;
- De véhicule arrêté en pleine voie en trafic fluide,
- Du trafic congestionné « STOP C » ;
- Des véhicules en contre sens ;
- Des piétons ;
- Des objets sur la chaussée (> 0.5m3) ;
- Des véhicules lents sur voie circulée ;
- Bougé caméra et d'autres défauts techniques.

les zones de détection sont définies en distinguant les voies de circulation et les trottoirs.

1.5.2.1 Modes de gestion dégradés

D'une longueur supérieure à 300 m, le tunnel de Bois de Peu fait l'objet d'un Dossier de Sécurité mis à jour annuellement. Dans ce dossier, le Plan d'Intervention de Secours définit la politique d'exploitation de la voie des Mercureaux, l'organisation de l'exploitant et des intervenants externes en cas d'incident, afin d'assurer la sécurité du parcours. Il décrit des modalités d'exploitation des équipements à appliquer en cas de défaillance (modes dégradés, conditions minimales d'exploitation (CME), et conditions de fermeture (CF)) dont certaine, rappelées ci-dessous, concerne la DAI.

Les modes d'exploitation du tunnel de Fontain sont un peu différents, et peuvent donner lieu à des CME différentes, celles-ci sont spécifiées le cas échéant ci-dessous, et présenté plus largement en annexe 2 au CCTP :

S'agissant des modes dégradés relatifs à la DAI, la situation actuelle est la suivante :

- - la perte de la fonction d'analyse sans perte de la fonction vidéosurveillance associée, correspond au mode dégradé 2 à savoir solution à trouver dans la semaine.
- - la perte totale de la vidéo DAI (analyse + flux vidéo) correspond à une condition de fermeture.

Concernant ceux relatifs à la vidéosurveillance :

- - la perte des images d'une caméra en tunnel (Bois de Peu ou Fontain) correspond au mode dégradé 1 (solution dans le mois) ;
- - la perte des images de 2 caméras non successives dans le même tube d'un tunnel (Bois de Peu ou Fontain) hors galerie correspond au mode dégradé 2 (solution à trouver dans la semaine) ;
- - la perte des images de 3 caméras (ou plus) successives dans le même tube (tubes de Fontain) correspond au mode dégradé 2 (solution à trouver dans la semaine) ;
- - la perte des images de 2 caméras successives dans le même tube du tunnel de Bois de Peu (hors galerie) correspond à l'atteinte de la condition minimale d'exploitation (solution à trouver dans les 48h) ;
- - la perte des images de 3 caméras (ou plus) successives dans le même tube (hors galerie) – tunnel Bois de Peu correspond à la condition de fermeture.

Pour information, le calepinage actuel des caméras DAI permet une couverture complète de l'ensemble des 2 tunnels.

Les plans de l'architecture réseau et le schéma de l'infrastructure sont fournis en annexe au CCTP.

CHAPITRE 2 nouvelle DAI

ARTICLE 2.1 Périmètre technique

Le présent marché est relatif à la fourniture et mise en œuvre d'un nouveau système (analyseur , serveur, IHM et solution applicative) de Détection Automatique d'Incidents (DAI) permettant de répondre aux exigences d'une surveillance D4 d'un ouvrage routier.

2.1.1 Objectif de la nouvelle DAI

Les objectifs du nouveau système de vidéosurveillance et DAI sont :

- d'analyser les images des caméras DAI des 2 tunnels et de transmettre les alarmes DAI au serveur DAI et à la GTC Supervision, d'optimiser les délais, de minimiser les fausses alarmes et d'améliorer le taux de détection,
- d'enregistrer les séquences associées à un événement,
- de permettre de consulter les séquences vidéo associées à un événement ,à posteriori,
- de surveiller la disponibilité des équipements du système-de DAI et de remonter les indisponibilité et problèmes techniques sur la future GTC,
- d'exploiter et d'administrer le système de DAI,
- d'avoir accès à un journal d'évènements et des actions,
- d'extraire des rapports sur les détections et le fonctionnement du système
- de permettre la lecture de signalétique sur véhicule dont notamment les codes ADR et plaques minéralogiques

2.1.2 Redondance souhaitée du système à mettre en œuvre

Une redondance des serveurs et analyseurs DAI avec la mise en œuvre d'une solution redondée dans au moins deux locaux techniques différents est demandée (parmi les locaux techniques Bois de Peu, Fontain et CISGT Vauban). Cette redondance permet d'assurer une sécurisation complète de la chaîne d'acquisition et de traitement, analyseurs / serveur DAI, sans perte d'exploitation (redondance dite « à chaud »).

2.1.3 Solution applicative

Le titulaire présentera dans son mémoire technique les caractéristiques techniques de sa solution applicative en répondant point par point aux besoins évoqués dans le présent CCTP. L'utilisation de solution utilisant des modules d'intelligence artificielle n'est pas interdit pour la présente consultation.

Le titulaire précisera les caractéristiques de sa solution concernant une éventuelle interface avec les autres outils utilisés pour la supervision du réseau routier au sein du CISGT Vauban (GTC – SAGT), notamment les matrices de flux, les protocoles supportés ainsi que les entrées et sorties nécessaires à l'échange de données avec son applicatif.

Les licences associées à la solution applicative seront prévues pour l'ensemble du cycle de vie du matériel (10 années) et dimensionnées pour le parc de caméras, serveurs, analyseurs et postes opérateurs (1 licence), technicien de maintenance (2 licences minimum) du CISGT Vauban et entreprise (1 licence).

Le périmètre du présent marché n'inclut pas les mises à jours qui sont prévues dans le marché spécifique de maintenance en vigueur. Cependant le mémoire technique du soumissionnaire devra le cas échéant préciser le coût annuel prévisionnel des licences.

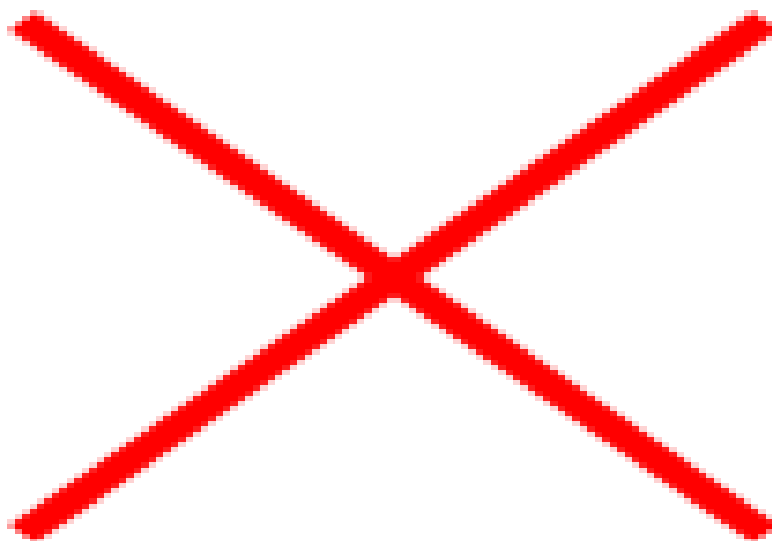
2.1.4 Proposition matérielle

2.1.4.1 Serveurs et analyseurs

L'acquisition des serveurs de stockage, de gestion et d'analyse sont partie intégrante de la présente consultation. **Le candidat devra dans son mémoire technique préciser les caractéristiques des matériels nécessaires au bon fonctionnement de la solution proposée en intégrant la notion de redondance, de cybersécurité et de continuité de service malgré la perte d'un équipement (respect des conditions minimales d'exploitation cf §1.5.2). Les appareils devront disposer d'une double alimentation et d'une carte de management (type ILO ou équivalent).** La proposition devra permettre le fonctionnement optimal dans la configuration actuelle (32 caméras actuellement) et devra pouvoir supporter des équipements supplémentaires sans modifications matérielles jusqu'à 40 caméras.

La proposition intégrera la fourniture, la mise en œuvre dans le respect des règles de cybersécurité de la DIRE, la pose et la formation pour les équipes du CISGT de ces équipements.

Les caractéristiques matérielles attendues sont les suivantes :



2.1.4.2 Poste client DAI

Le titulaire fournira un poste client DAI en salle opérateur au CISGT Vauban. Ce poste client sera l'IHM avec la solution applicative du titulaire. Elle sera équipée d'un système avertisseur sonore configurable et permettra l'affichage des alarmes sur écrans secondaires déportés. Il devra supporter la présence d'un client de vidéosurveillance Genetec sur la même machine (spécifications recommandée, windows 11, processeur i7 14700, 32 Go de RAM en DDR5, carte graphique NVIDIA RTX 4070(12Go) et disque SSD avec 6 Go de stockage disponible pour le client).

Les postes des techniciens de maintenance (3) devront pouvoir accéder à la solution logiciel (web ou client lourd).

La solution applicative devra permettre la configuration de macros permettant de définir rapidement des modes d'exploitation (ex : inhibition des détections lors de maintenance dans un tube spécifique). Les macros seront à définir avec l'exploitant.

ARTICLE 2.2 Transfert de compétence et formation

Il est prévu une formation scindée en 2 modules pour le personnel de maintenance et le personnel d'exploitation de la DIRE.

S'agissant de la maintenance : la formation comprend une assistance au démarrage de l'ensemble des matériels installés, la fourniture de la documentation technique et d'exploitation relative aux différents matériels et logiciels installés.

Ce document en langue française comprendra les éléments permettant la configuration, l'exploitation et la maintenance du système de DAI.

S'agissant des opérateurs, la formation visera à présenter le fonctionnement et la spécificité des équipements et logiciels mis en œuvre. Les périodes de formations seront adaptées au cycle de travail des opérateurs (formation des 8 gents par groupes de 2 personnes pour respecter le cycle de travail en 3x8).

ARTICLE 2.3 Garanties

L'ensemble des matériels et logiciels installés sera garanti deux ans. Durant cette période, le titulaire assurera le maintien des performances du système, y compris en terme de cybersécurité, telle que définies dans le présent CCTP. Il devra s'assurer de conserver sur cette période la sauvegarde des configurations logicielles lors de la mise en service et à chaque modification majeure de configuration. Cette sauvegarde sera remise au terme de la garantie à la DIRE.

ARTICLE 2.4 Ouverture à variantes

Des variantes pourront être proposées concernant les propositions matériels, à condition de respecter les spécifications de l'article 2.1.1 et de garantir une redondance des systèmes informatiques permettant une continuité de service malgré la défaillance d'un maillon de la chaîne technique équivalent aux spécifications de l'article 2.1.2.

Les variantes pourront également porter sur la nature des licences logiciels (licence à vie plutôt que licence annuelle, par exemple).

CHAPITRE 3 Besoin fonctionnel du système DAI

Le présent chapitre expose dans un premier temps les incidents à détecter, les performances attendues, les défauts à éviter qui conduisent à la dégradation de la performance du système. Ensuite est présenté le détail pour chacune des caméras. Enfin il présente le fonctionnement en Exploitation.

ARTICLE 3.1 Principe de la DAI

L'installation permet à minima l'horodatage, identification de la zone, identification de la voie concernée, la relecture du clip vidéo par l'opérateur et type d'incident détecté ci-dessous

- véhicules arrêtés sur les voies et Bande d'Arrêt d'Urgence quand elles existent
- incendie (apparition de fumées pour les caméras standards et de flammes pour les caméras thermiques)
- véhicules circulant à contre sens
- objet sur la chaussée
- piétons ou cyclistes.
- Véhicules lents

D'autres types de détections et d'autres fonctionnalités pourront être proposées en compléments de celles présentées ci-dessus par les candidats dans leur mémoire technique.

3.1.1 Définition des détections

Véhicule arrêté : Le système DAI considérera un véhicule comme arrêté, tout véhicule immobile pendant une période d'au moins 10 secondes, en tout point de la chaussée y compris BAU. Le système d'analyse devra prendre en considération les véhicules légers, les deux-roues et les Poids lourds, il n'est cependant pas demandé de distinguer le type de véhicule arrêté. L'arrêt devra être d'une durée supérieure ou égale au temps de détection.

Incendie(apparition de fumée): le système de DAI doit détecter une perte significative du niveau de contraste sur une partie significative de la surface de l'image, persistant pendant au moins 10 secondes.

Incendie(apparition de flamme): le système de DAI doit détecter une flamme, et cela en tout point de la chaussée, (persistant pendant au moins 10 secondes) » dans tout le champ de vision d'une caméra thermique.

Véhicules-en contre sens : Le système DAI devra détecter un véhicule à contre sens circulant à plus de 30KM/h, en tout point de la chaussée.

Objet : Le système DAI devra détecter un objet de plus de 0,5 mètre cube, en tout point de la chaussée.

Piétons : Le système DAI devra détecter un piéton se déplaçant à moins de 5 km/h, en tout point de la chaussée et des trottoirs. Cette détection doit prendre en considération un piéton à partir du moment où il est entièrement visible à l'image, quelle que soit sa taille ou la couleur de ses habits. Il sera possible de définir les zones de l'image dans lesquelles les piétons pourront être détectés.

Véhicule lent : Avec cette fonction, le système de DAI devra détecter comme lent tout véhicule roulant à une vitesse paramétrable en tout point de la chaussée. Un second seuil est généralement utilisé de façon à ne générer l'alarme que si la vitesse du véhicule est significativement inférieure à la vitesse moyenne du trafic.

3.1.2 Performances des détections

Actuellement, une sonnerie est générée lors d'une détection et le flux vidéo de la caméra sur laquelle il y a détection s'affiche sur un écran dédié.

Ce fonctionnement est à conserver ou un fonctionnement équivalent est à proposer. L'alarme sonore doit pouvoir être paramétrable (type de son et volume)

Temps de détection :

De manière générale, le temps de détection sera décomposé en 2 temps : le temps d'analyse et de détection proprement dit, entre l'apparition réelle de l'événement et la détection par l'analyseur, le temps global de traitement et de remontée à travers tous les éléments du système entre la détection par l'analyseur et l'affichage de la caméra impliquée sur le moniteur au CISGT.

Les différents temps maximums sont définis dans le tableau suivant.

Type d'événement	Analyse et détection	Traitement et affichage	Taux de détection
Véhicules arrêtés	10 s	2 s	98 %
incendie	10 s	2 s	95 %
Véhicules circulant à contre sens	2 s	2 s	95 %
Objet sur la chaussée	10 s	2 s	90 %
Piéton	10 s	2 s	90 %

3.1.3 Fausses alarmes

Les fausses alarmes concernent les alarmes émises alors qu'il n'y a pas d'événements liés à l'exploitation. La fréquence des fausses alarmes devra être inférieure à 9 fausses alarmes par jour en moyenne sur l'ensemble de la Voie des Mercureaux et ce pour tout type d'incident confondus.

3.1.4 Taux de détection

Les performances d'un système de DAI sont évaluées selon les classes d'alarmes définies ci-après :

- la vraie alarme (VA) : le système remonte une alarme à l'opérateur, et l'observateur humain, après consultation de la séquence vidéo, valide le fait que l'incident détecté a effectivement eu lieu et correspond bien à l'alarme. Par exemple, un véhicule arrêté est bien détecté comme alarme « véhicule arrêté » ;

- la fausse alarme (FA) : le système remonte une alarme à l'opérateur, mais l'observateur humain, après consultation de la séquence vidéo, ne constate pas d'incident, ou le phénomène constaté ne fait pas partie de ceux à détecter. Par exemple, une ombre en tunnel est identifiée comme un « véhicule arrêté ». Ce type d'alarme est classé en fausse alarme ;
- l'alarme mal qualifiée (AMQ) : le système remonte une alarme à l'opérateur, mais l'observateur humain, après consultation de la séquence vidéo, constate que le type d'incident ne correspond pas à l'alarme remontée tout en faisant néanmoins partie de ceux à détecter. Par exemple, un piéton est identifié comme un véhicule lent. La fonction d'alerte étant remplie, cette alarme de typage erroné est néanmoins comptabilisée parmi les vraies alarmes.
- la non-détection (ND) : le système ne remonte aucune alarme alors qu'un incident, faisant partie de la liste de ceux à détecter, a eu lieu.

Les incidents détectables par le système correspondent à la somme des VA et des ND et des AMQ, c'est-à-dire à l'ensemble des incidents que le système de DAI, s'il a été parfaitement programmé et fonctionne à 100 % de ses capacités, doit être capable de détecter. Au sens de cette définition, tout incident n'est pas un « incident détectable ».

Le classement des détections en tant que vraies alarmes, fausses alarmes ou alarmes mal qualifiées, doit être apprécié par un œil humain, à savoir celui du maître d'œuvre ou de l'entrepreneur en phase de tests et celui de l'opérateur en phase d'exploitation. Ce classement, appliqué à un échantillon statistique d'incidents représentatifs, permet d'évaluer les performances principales du système.

3.1.5 Bougé caméra

Le système remonte une alarme à la supervision lorsqu'il repère un déplacement de la caméra susceptible de détériorer la performance de détection. Cette alarme ne doit cependant pas être remontée en cas de faibles vibrations occasionnées par exemple par le passage de véhicules à proximité de la caméra, dès lors que celles-ci ne remettent pas en cause les paramètres de l'analyse.

3.1.6 Dégradation de la qualité de l'image

Le système remonte une alarme à la supervision lorsque l'image n'a plus la qualité suffisante pour assurer la détection d'incident et tenir les performances exigées. Il s'agit par exemple de détecter l'encrassement de la vitre d'un caisson ou le desserrement d'un objectif.

3.1.7 Perte ou dégradation du signal vidéo

Le système signale à la supervision l'absence ou la dégradation du flux en entrée.

3.1.8 Défauts fonctionnels et techniques

Les défauts logiciel et matériel génèrent une alarme technique. Il s'agit généralement de défauts techniques (température du processeur trop élevée ou tout défaut entraînant une perte de disponibilité fonctionnelle) ou de défauts fonctionnels (dysfonctionnement d'une fonction d'analyse, de la fonction d'inhibition...).

3.1.9 Réinitialisation

Entre deux détections successives sur la même caméra, le temps de réinitialisation ne devra pas excéder 30 secondes.

Conditions particulières :

La détection devra être indépendante des véhicules , de leur état et de leur sens de circulation. Compte tenu de passage de véhicules sans feux de croisement, la détection ne devra pas être altérée par ces phénomènes. L'installation devra permettre la détection d'incident intervenant sur des véhicules circulant sans feux (ni croisement ni position).

ARTICLE 3.2 Affectation des détections en fonction des caméras

Afin de garantir une exploitation rationnelle des incidents au niveau du CISGT, les caméras doivent pouvoir détecter l'ensemble des fonctionnalités. Le tableau suivant donne, une fois l'implantation définie, en fonction des caméras , les détections à réaliser. Pour les caméras non thermiques en tête d'ouvrage, il faudra vérifier que les détections de fumée et d'objet ne conduisent pas dans certains cas à une dégradation des performances du système, qui est parfois observable sur des systèmes similaires et proposer des adaptations des affectations de détection au besoin.

3.2.1 Tunnel de bois de Peu

Caméra	Arrêt	Incendie	Contresens	Objet	Piéton	Véhicules lents
C1BN	oui	oui	oui	oui	oui	40km/h
C2BN	oui	oui	oui	oui	oui	40km/h
C3BN	oui	oui	oui	oui	oui	40km/h
C4BN	oui	oui	oui	oui	oui	40km/h
C5BN	oui	oui	oui	oui	oui	40km/h
C6BN	oui	oui	oui	oui	oui	40km/h
C7BN	oui	oui	oui	oui	oui	40km/h
C8BN	oui	oui	oui	oui	oui	40km/h
C8BNTH	oui	oui	oui	oui	oui	40km/h
C1BS	oui	oui	oui	oui	oui	30km/h
C1BSTH	oui	oui	oui	oui	oui	30km/h
C2BS	oui	oui	oui	oui	oui	30km/h
C3BS	oui	oui	oui	oui	oui	30km/h
C4BS	oui	oui	oui	oui	oui	30km/h
C5BS	oui	oui	oui	oui	oui	30km/h
C6BS	oui	oui	oui	oui	oui	30km/h
C7BS	oui	oui	oui	oui	oui	30km/h
C8BS	oui	oui	oui	oui	oui	30km/h

3.2.2 Tunnel de Fontain

Caméra	Arrêt	Incendie	Contresens	Objet	Piéton	Véhicules lents
--------	-------	----------	------------	-------	--------	-----------------

C1FN	oui	oui	oui	oui	oui	40km/h
C2FN	oui	oui	oui	oui	oui	40km/h
C3FN	oui	oui	oui	oui	oui	40km/h
C4FN	oui	oui	oui	oui	oui	40km/h
C5FN	oui	oui	oui	oui	oui	40km/h
C6FN	oui	oui	oui	oui	oui	40km/h
C6FNTH	oui	oui	oui	oui	oui	40km/h
C1FS	oui	oui	oui	oui	oui	40km/h
C1FSTH	oui	oui	oui	oui	oui	40km/h
C2FS	oui	oui	oui	oui	oui	40km/h
C3FS	oui	oui	oui	oui	oui	40km/h
C4FS	oui	oui	oui	oui	oui	40km/h
C5FS	oui	oui	oui	oui	oui	40km/h
C6FS	oui	oui	oui	oui	oui	40km/h

3.2.3 Fonctionnement en exploitation

3.2.3.1 Fonctionnement « normal »

- En l'absence d'incident, le moniteur du PC alarme DAI affectés à la Pop-up DAI au CISGT sera en veille.

3.2.3.2 En cas de détection d'incident

- Pour chaque type d'incident, dans le temps défini précédemment :
- l'analyseur DAI communique au serveur DAI le numéro de la caméra ayant détecté l'incident ainsi que la nature de cette détection
- le serveur DAI vérifie s'il y a une alarme à émettre en fonction de la détection et communique au PC DAI le numéro de la caméra ayant détecté l'incident ainsi que le type de détection
- le serveur DAI prélève dans l'enregistrement numérique la séquence correspondant à l'évènement sur une durée paramétrable (généralement 30s avant et 2mn après la détection de l'incident) sur l'enregistreur DAI
- une alarme sonore est déclenchée au PC DAI (paramétrable)
- par ailleurs , le serveur DAI affiche automatiquement les images de la caméra ayant détecté l'incident sur le PC DAI ainsi que sur le moniteur du PC Alarme DAI dédiés à la pop-up DAI
- les clips vidéos numériques des incidents enregistrés par l'enregistreur DAI sont visualisables à tout moment depuis le PC DAI pendant 31 jours.

En cas de détection d'incident n'entraînant pas de problématique d'exploitation ou de fausse alarme , après détection automatique de l'incident , l'opérateur du CISGT pourra acquitter le défaut depuis le PC DAI , ce qui ramènera le moniteur du PC Alarme DAI en état de veille, sauf si d'autres alarmes sont encore présentes.

Sur demande, l'opérateur pourra visualiser les enregistrements correspondant aux détections depuis le PC DAI. Il pourra alors acquitter un ou plusieurs incidents et libérer de la « pile » ces incidents.

Le PC DAI permet l'inhibition de chaque type de détection, par caméra, par voie et par tube. Ces inhibitions sont possibles unitairement ou groupées.

Quelle que soit l'inhibition mise en place, le système d'analyse devra se réactiver automatiquement au bout d'une durée paramétrable. Cette inhibition peut être utilisée notamment dans le cas d'opérations de maintenance ou de travaux devant une caméra, afin de ne pas générer d'alarme DAI inutile. Un symbole visible devra apparaître quand une caméra sera inhibée sur un bandeau de la DAI avec un rappel sur la vignette caméra concernée.

3.2.3.3 *Fonction d'aide à l'exploitation*

Le PC DAI permet l'inhibition de chaque type de détection, par caméra, par voie et par tube. Ces inhibitions sont possibles unitairement ou groupées. Quelle que soit l'inhibition mise en place, le système d'analyse devra se réactiver automatiquement au bout d'une durée paramétrable. Cette inhibition peut être utilisée notamment dans le cas d'opérations de maintenance ou de travaux devant une caméra, afin de ne pas générer d'alarme DAI inutile. Un symbole visible devra apparaître quand une caméra sera inhibée sur un bandeau de la DAI avec un rappel sur la vignette caméra concernée.

« activation/inhibition des détections par type et par voie et par caméra : cette fonction est très utile à l'exploitant quand le tunnel n'est pas exploité de façon normale (travaux, etc.). »

3.2.3.4 *Fonctions de maintenance et d'administration*

Les paramètres d'administration et de maintenance du système DAI devront inclure à minima les éléments suivants :

- définitions des droits utilisateurs (administrateur, maintenance, chef de salle, opérateurs)
- définition ou recalage des zones à surveiller cette fonction permet à la personne chargée de la maintenance de recalibrer les masques par exemple en cas de bougé caméra
- édition de rapport de fonctionnement et de détection configurable par période, caméra, type d'alarme, événement
- configuration des filtres (pour éviter les avalanches d'alarmes par exemple pour les véhicules à contre-sens)
- étalonnage et calibrage de la DAI
- activation/inhibition des détections par type et par voie et par caméra : cette fonction est très utile à l'exploitant quand le tunnel n'est pas exploité de façon normale (travaux, etc.)
- consulter et éditer le journal des événements
- archiver des données
- recharger le paramétrage de référence sauvegardé
- afficher l'état de fonctionnement des appareils DAI

CHAPITRE 4 Essais et contrôles

Les contrôles seront réalisés par le titulaire en présence du représentant de la DIRE :

- Contrôles des zones de vision
- Contrôles et essais de performance du système DAI sur site.

La mise au point du fonctionnement de la DAI par le prestataire concerne tous les essais et la mise en service des équipements d'exploitation (serveurs, moniteurs, affichages, alertes visuelles et sonores, enregistrement...). Cette phase comprend également toutes les prestations nécessaires à la mise au point complète et les réglages de tous les équipements liés au système DAI.

Les contrôles et essais de performance du système DAI sur site seront réalisés lors des opérations préalables à la réception.

4.1.1 Recettes de contrôle et essai

4.1.1.1 Contrôle et essai sur site

Le titulaire établit et soumet à la validation du maître d'œuvre, un **programme de contrôle ainsi qu'un cahier de recette associé** de l'installation de détection automatique d'incident et des serveurs. La production et la validation de ce document conditionnent le démarrage des travaux d'installation de ces équipements sur le site.

Le programme de contrôle du titulaire décrit le contenu des tests et vérifications qu'il va mettre en œuvre sur le site, leur étendue et les critères d'acceptation. Le cahier de recette permet de suivre la réalisation de l'ensemble des points contrôlés. Le programme s'articule autour des phases suivantes :

- tests des matériels participant à la DAI
- tests des fonctions d'aide à la maintenance (exemple : bougé caméra)
- tests des fonctions de détection prescrites dans le CCTP.

La réussite de l'ensemble des tests d'une phase conditionne le démarrage de la suivante. La nature et l'étendue des contrôles à réaliser par le titulaire sont décrites ci-dessous.

4.1.1.2 Tests des matériels participants à la DAI

Le titulaire réalisera à minima les tests suivants sur l'installation DAI:

Tests	Actions à réaliser
Démarrer le serveur DAI	Se connecter avec les différents profils utilisateurs. Vérifier le bon démarrage des services DAI (analyse, administration, visualisation, enregistrement...). Vérifier l'absence d'alarme technique.
Afficher les flux des caméras sur l'IHM	Vérifier que les flux vidéo de l'ensemble des caméras sont visibles sur l'interface DAI. Et que pour une caméra donnée avec une vidéo sans alarme de trafic, la fréquence d'affichage en DAI soit la même que celle envoyée par les caméras avec un minimum de 5 images par secondes et qu'aucune alarme ne s'affiche (état appelé « normal »).
Contrôler la qualité des images	Vérifier visuellement la qualité de l'image provenant de chaque caméra, ainsi que la bonne incrustation de leur identification et de l'horodatage.

Tester la perte d'un flux vidéo	Vérifier que la perte d'un flux vidéo remonte bien à l'opérateur une alarme. Vérifier que l'alarme disparaît lorsque le flux est de nouveau disponible.
Tester la communication entre analyseur et serveur	Vérifier que lors de la détection d'un incident, une alarme remonte bien à l'opérateur.
Tester la perte de la fonction d'analyse	Vérifier que la perte totale ou partielle de la fonction d'analyse remonte bien une alarme à l'opérateur. Vérifier que l'alarme disparaît lorsque la fonction est de nouveau disponible.
Tester la perte du serveur	Vérifier que la perte d'un des serveurs remonte une alarme à l'opérateur. Vérifier que l'alarme disparaît lorsque le serveur est de nouveau disponible. Vérifier que lors de la perte du serveur maître, le basculement sur le serveur esclave s'opère et que le serveur est opérationnel.
Tester les fonctions de redondance	Vérifier que lors de la perte d'un analyseur, que la redondance s'opère et que la fonction d'analyse reste fonctionnelle.
Tester l'interaction avec les systèmes connexes	Vérifier la possibilité de communication entre système DAI et un système de supervision/GTC (remontées d'informations, passages de commande). Vérifier que lors d'une remontée d'alarme DAI, le flux vidéo de la caméra concernée s'affiche sur l'écran dédié en salle de contrôle.
Tester le défaut « bougé caméra »	Vérifier que la modification de l'orientation d'une caméra remonte bien une alarme à l'opérateur.
Tester la dégradation de la qualité de l'image	Vérifier que la dégradation des images remonte bien une alarme à l'opérateur.
Tester les fonctions d'inhibition	Vérifier l'inhibition des fonctions de détection (par caméra, par zone, par type d'incident). Vérifier le retour d'information d'inhibition à l'opérateur. Vérifier le retour à l'état initial lorsque les fonctions de détection sont réactivées. Vérifier le fonctionnement des presets
Tester les règles de filtrage	Vérifier les fonctions de filtrage des alarmes récurrentes.
Tester les fonctions d'enregistrement, d'archivage et d'export	Vérifier qu'une détection d'incident provoque bien l'enregistrement d'une séquence vidéo. Vérifier l'archivage et la possibilité de relecture des séquences.

Vérifier la possibilité d'export de la séquence et/ou l'édition d'un rapport de détection.
--

4.1.1.3 Validation des fonctions de détection

La validation des performances de détection du système DAI concernera l'ensemble des caméras et l'ensemble des fonctions telles que définies ci-après. Les taux de détection seront calculés en établissant la moyenne des résultats pour l'ensemble des caméras équipées en DAI.

4.1.1.4 Réalisation des tests des fonctions de détection

Le titulaire déterminera les actions nécessaires à la réalisation des essais.

Ces tests demanderont la mise en œuvre d'un certain nombre de moyens (génération et évacuation de fumée, changements de régime d'éclairages, différents régimes d'éclairage, etc.) : le titulaire établira la liste de ces besoins et se donnera les moyens de les mettre en œuvre.

4.1.1.4.1 Incendie (apparition de Fumée)

- performances attendues : le taux de détection attendu est de 95 %,
- mise en œuvre de la détection « fumée » via un véhicule équipé d'un générateur de fumée (équivalent au dégagement d'un feu de VL) qui circule dans le sens de circulation, à une allure approximative inférieure à 15 km/h
 - au moins un test de fumée par caméra sera réalisé,
 - la localisation précise de ces tests sera définie en concertation avec la maîtrise d'œuvre. En cas de non-réussite du test, la localisation pourra être modifiée pour la réalisation d'un nouvel essai après reprise de paramétrages,
 - le temps de détection est fixé à 10 secondes,
- les départs de fumées simulés devront être détectés notamment pour différents régimes d'éclairages.

4.1.1.4.2 Incendie (apparition de flamme)

- performances attendues : le taux de détection attendu est de 95 %,
- mise en œuvre de la détection « flamme » via un générateur de flammes
 - au moins un test de flamme par caméra thermique sera réalisé,
 - la localisation précise de ces tests sera définie en concertation avec la maîtrise d'œuvre. En cas de non-réussite du test, la localisation pourra être modifiée pour la réalisation d'un nouvel essai après reprise de paramétrages,
 - le temps de détection est fixé à 10 secondes,
- les départs de flammes simulés devront être détectés notamment pour différents régimes d'éclairages.

4.1.1.4.3 Véhicule arrêté

- performances attendues : un taux de détection de 98 % sera exigé,
- mise en œuvre : les tests de validation se feront la nuit de la migration, sur chacune des voies de circulation. Les essais seront envisagés comme suit :
 - les véhicules auront les feux de croisement et feux de position allumés, les feux-stop en état de marche (ils ne seront pas équipés de gyrophares ou bandes blanches et seront de type VL blanc pour l'un et sombre pour l'autre)
 - le temps de détection est fixé à 10 secondes,

- 1 arrêt sera réalisé par caméra soit 64 arrêts au total par voie et quelques arrêts sur BAU selon les cas selon calepinage préalable validé par le CISGT. Le titulaire proposera un plan sur lequel sont mentionnés ces arrêts qui mixeront les arrêts en début, milieu et fin de champ

4.1.1.4.4 Véhicule lent

- performances attendues : un taux de détection de 98 % sera exigé,
- mise en œuvre : les tests de validation se feront à la fin des travaux, sur chacune des voies de circulation.
- Les essais seront envisagés comme suit :
- les véhicules auront les feux de croisement et feux de position allumés, les feux-stop en état de marche (ils ne seront pas équipés de gyrophares ou bandes blanches et seront de type VL blanc pour l'un et sombre pour l'autre),
- ils circuleront à moins de 30 km/h dans le sens montant de Bois de Peu , 40 km/h pour les autres tubes)
- le temps de détection est fixé à 10 secondes,

4.1.1.4.5 Piétons

- performances attendues : un taux de détection de 90 % sera exigé,
- Les zones de détection sont les trottoirs et les voies de circulation.
- mise en œuvre :
 - Le piéton portera des vêtements civils (pas de dispositif rétroréfléchissant)
 - Le piéton circulera dans le tunnel sur les trottoirs puis sur les voies
 - Le temps de détection sera fixé à 10 secondes par défaut à partir de l'apparition totale du piéton dans l'image.

4.1.1.4.6 Contre sens

- performances attendues : un taux de détection de 95 % sera exigé,
- Les zones de détection sont toutes les voies de circulation.
- mise en œuvre :
 - Le véhicule circulera à contre sens en empruntant successivement chacune des voies
 - au moins 2 tests par tube et par voie sera réalisé (la vitesse du véhicule sera de 70 km/h et de 30 kmh pour le second test)
 - Le temps de détection sera fixé à 2 secondes par défaut à partir de l'apparition totale du véhicule dans l'image.

4.1.1.4.7 Objet sur la chaussée

- performances attendues : un taux de détection de 90 % sera exigé,
- Les zones de détection sont les voies de circulation et les trottoirs.
- mise en œuvre :
 - un objet d'au moins 0,8x0,8x0,8 m³ soit 0,5 m³ est déposé au sol depuis le véhicule en circulation sur chacune des 2 voies et pour chacune des caméras pour les tests, prévoir plusieurs objets, pour optimiser le temps de réalisation de ce test. Le véhicule devra rouler à plus de 30 km/h pour ne pas générer une alarme véhicule lent
 - Le temps de détection sera fixé à 10 secondes par défaut à partir de l'apparition totale de l'objet dans l'image.

Lorsque toutes les fonctions auront été testées, le titulaire calculera les performances réelles obtenues par le système. Pour cela seront regroupés tous les résultats obtenus individuellement sur chaque caméra pour chaque type de détection afin d'en déduire les taux de détections. Les temps de détections correspondront à une moyenne des essais réussis pour chaque type de détection.

Si les performances mesurées sont supérieures ou égales à celles définies au niveau du CCTP, la réception est validée. Dans le cas contraire, des réserves sont émises sur les types de détections. Ces éventuelles non conformités devront être corrigées afin de lever les réserves.

ARTICLE 4.2 Opération de révision à 6 mois

Dans un délai de six (6) mois (période de vérification de service régulier – VSR) suivant la validation de la phase d'essais, le titulaire réalisera une opération de révision de la solution applicative. Cette intervention aura pour objet d'ajuster les paramètres de fonctionnement en fonction des retours du CISGT liés à l'usage quotidien de la DAI notamment sur le volet fausses alarmes.

ARTICLE 4.3 Documentation

Le titulaire fournira toute documentation utile à la bonne utilisation et configuration des solutions logiciels et matériel installées :

- Manuels d'exploitation et d'utilisation
- Manuel de maintenance et d'administration du système
- Manuel de maintenance des matériels fournis

Le titulaire préparera également des fiches réflexes présentant les principales actions courantes de maintenance et de configuration du système spécifique à l'installation du CISGT Vauban (redémarrage du système, mise à jour, configuration des alarmes...)

CHAPITRE 5 Préparation, coordination et exécution de la prestation

ARTICLE 5.1

ARTICLE 5.2 Période de préparation - Programme d'exécution de la prestation

Le titulaire devra prévoir, dans son mémoire technique, un **planning prévisionnel détaillé** des interventions nécessaires à l'installation du matériel et de la solution applicative, en tenant compte des contraintes spécifiques du projet, notamment l'absence d'interruption du trafic routier en dehors des plages programmées de nuits (cf article 5.2).

Ce planning prévisionnel devra inclure les phases suivantes :

- une réunion de démarrage
- Proposition de l'architecture par le titulaire
 - Le titulaire proposera une architecture détaillée, incluant les spécifications techniques des matériels requis (serveurs, équipements annexes) et leur compatibilité avec la solution applicative.
- Installation des matériels
 - installations des différents serveurs et de l'Interface Homme Machine en salle opérateur en parallèle de l'existant.
- Mise en œuvre de la solution logicielle en parallèle de l'existant
 - Préparation de la solution applicative sur les nouveaux équipements, tout en assurant le maintien de la continuité de service de la solution existante.
- Phase de tests
 - Planification et réalisation de tests fonctionnels et techniques sur la base minimale des éléments présentés dans ce CCTP.
- Bascule et validation finale

- Description des étapes et procédures nécessaires à la bascule de l'ancienne solution vers la nouvelle, après validation complète des tests.
- Enlèvement des anciens matériels
 - Enlèvement en lien avec le CISGT et le Service Système et Réseau de la DIRE des anciens équipements (serveurs et IHM).
- Réunion de fin d'opération
- Préparation et planification des modules de formation et de la documentation technique opérateur et maintenance
- opération de révision à six mois.

Le titulaire devra soumettre le planning d'exécution mise à jour à validation par le maître d'ouvrage dans un délai de 10 jours après le lancement de la période de préparation. Ce planning devra intégrer les contraintes d'exploitation de la DIRE sur la voie des Mercureaux précisées lors de la réunion de démarrage.

ARTICLE 5.3 Contraintes d'exploitation

La modification du logiciel ainsi que la migration sur les nouveaux serveurs devront être organisées de façon à minimiser les pertes d'exploitation.

La migration consistera à préparer la solution logiciel de contrôle, de suivi et d'enregistrement des données conformément à la réglementation, au paramétrage des détections par les analyseurs pour l'ensemble des caméras des tunnels.

Les interventions qui ont un impact sur l'exploitation (exemple : migration du système) seront à réaliser lors des fermetures de nuit (21h – 5h). Les Conditions Minimales d'Exploitations (CME) devront impérativement être respectées lors de la réouverture à 5 h.

Les essais pour chaque tunnel devront être réalisés de nuit , du lundi au jeudi de 21h à 4h30, lors des fermetures planifiées par la DIR Est . L'ensemble des contraintes d'exploitations devront être planifiées et validées par le responsable du CISGT. Le titulaire précisera le nombre de nuit nécessaire à la réalisation des essais selon son programme de contrôle et son cahier de recette (cf 4.1.1). les nuits supplémentaires potentiellement nécessaires sont réputées prise en charge dans le forfait.

Si des interventions sont planifiées lors des périodes de viabilité hivernale(1er novembre au 15 mars), l'exploitant se réserve le droit de faire reporter ces interventions en cas d'intempéries.

- Les périodes d'intervention dans les locaux techniques ne sont pas contraintes. Les périodes d'intervention dans la salle opérationnelle (intégration caméra au logiciel DAI) ne sont pas contraintes, mais ne devront pas entraîner de CME pendant l'exploitation.

Si le dispositif ne permet pas d'assurer l'exploitation avec un niveau de sécurité satisfaisant à la réouverture de la circulation (cf supra.), il devra être possible à tout moment de revenir sur la solution technique actuelle jusqu'à validation de sa dépose par le CISGT.

ARTICLE 5.4 Hygiène et sécurité

5.4.1 PPSPS

Pour l'exécution des travaux d'installation de matériel et d'intervention d'essais et contrôles, l'entreprise est tenue de se conformer aux mesures particulières de sécurité et de protection de la santé prescrites par la réglementation en vigueur dans les chantiers du bâtiment et des travaux publics.

L'établissement d'un plan de prévention ou du PPSPS sera réalisé selon l'article 28.3 du CCAG, la loi n°93-1418 du 31 décembre 1993 et ses décrets d'application.

CHAPITRE 6 Cybersécurité

ARTICLE 6.1 COMPOSANTS COMMUNS D'ADMINISTRATION

6.1.1 Collecteur de logs

Actuellement, la DIR Est ne possède pas de collecteur de logs, mais a exprimé le besoin de mettre en place un serveur de logs pour la traçabilité des accès et des actions sur le réseau. Il est demandé au Titulaire de fournir des machines capables de générer des logs pour assurer la traçabilité.

Le PASR prendra en charge l'installation et l'hébergement du serveur de logs. Le collecteur sera proposé par le Titulaire.

Le collecteur sera compatible avec le standard SYSLOG. En revanche, l'ensemble des machines déployées devront être configurées par le Titulaire pour transmettre leurs logs via des protocoles réseau sécurisés (SSL/TLS).

Tous les équipements seront néanmoins configurés pour retransmettre leur log via le protocole syslog. Ces transmissions devront être sécurisées. (TCP / TLS) Le prestataire se coordonnera avec les équipes PASR DIR Est afin de configurer son environnement pour être compatible.

Le Titulaire devra mettre en œuvre le paramétrage de chaque machine (serveurs, postes) pour générer des logs complets, selon les exigences de la DIR Est (événements système, connexions, incidents, modifications...). Il devra également prévoir un journal d'exploitation clair permettant l'analyse par la MOA (exploitation + cybersécurité). Le collecteur de logs proposé devra être documenté dans le Plan d'Assurance Sécurité. Il devra répondre à l'ensemble des exigences NIS2.

6.1.2 Sauvegarde des données opérationnelles

L'archivage de restauration doit permettre la restauration des données système à un état antérieur en cas de défaillance ou de corruption des données (panne matérielle, cybersécurité), et ainsi garantir la continuité des opérations de surveillance et de service d'exploitation du CISGT.

Il devra donc être mis en place un système de sauvegarde complète, et automatique, assurant une redondance du stockage des données (RAID1E ou RAID5E), Tous les serveurs doivent assurer un niveau élevé de tolérance aux pannes matérielles.

Le Titulaire devra donc :

- Établir une procédure d'archivage des données (métier et paramétrage) et des systèmes
- Établir une méthodologie de restauration système (dans son manuel d'installation ou de maintenance)
- Mettre en œuvre ces procédures, sur site, en présence des personnels DIR Est
- La DIR Est prendra en charge la réalisation des actions de sauvegardes régulières, selon les procédures ainsi éprouvées.

6.1.3 Synchronisation horaire – serveur ntp

Toutes les machines raccordées au réseau doivent supporter le protocole NTP. Le serveur NTP primaire sera mis à disposition par la DIR Est.

6.1.4 Authentification des utilisateurs

Le Titulaire doit la fourniture de toute information (utilisateurs, groupes de sécurité, GPOs...) nécessaire à la réalisation de la configuration et mise en service de ce composant d'authentification des utilisateurs par les équipes de la DIR Est. Il est demandé au titulaire concernant l'authentification des utilisateurs de la DAI que celle-ci soit possible de deux manières :

- Authentification sur la solution d'authentification des utilisateurs,

- Authentification par module logiciel propre par utilisateur et sans mot de passe générique ni commun.

6.1.5 Antivirus

Les postes sur lesquels la solution DAI sera installée devront être munis d'antivirus dernière génération type EDR.

La solution choisie devra pouvoir être mise à jour sans connexion à internet.

Cette solution devra être validée par la DIR Est et être compatible du système DAI mis en œuvre.

ARTICLE 6.2 Documents et fichiers relatifs à la cybersécurité à fournir par le titulaire

6.2.1 Données confidentielles

Toutes les données concernant les infrastructures de la DIR Est (équipements, réseaux) et les codes, plans, documentations générées lors de la réalisation des études, développement et installation sont considérées comme confidentielles, et doivent être stockées de manière sécurisée par le titulaire du marché et les sous-traitant (ex : pas sur clé USB non chiffrée, non accessible en cas de perte de PC portable etc...)

La diffusion et l'accès doivent être restreintes aux personnels ayant besoin d'y accéder. Les documents sensibles devront être cryptés et le cas échéant les données cloud seront hébergées en Europe.

6.2.2 Fonctionnement sans média USB

La DIR Est ne souhaite pas que soit utilisé des « dongles » pour la gestion des licences. Pour des raisons liées à la cybersécurité, et d'une manière générale, l'utilisation des clés USB (stockage) ne sera pas autorisée sur l'ensemble du réseau.

6.2.3 Plan d'Assurance Sécurité Projet

Le Plan d'Assurance Sécurité (PAS) décrit l'ensemble des dispositions spécifiques que l'Entreprise s'engage à mettre en œuvre pour garantir le respect des exigences de cybersécurité de la DIRE. L'Entreprise doit élaborer un PAS en accord avec le PSSI de la DIRE.

Les obligations nées de la transposition française de la Directive NIS2 devront être prises en compte par le titulaire du marché dans le cas où celle-ci serait publiée avant le lancement de la consultation

Il est donc nécessaire de prévoir une étroite collaboration avec le RSSI de la DIRE pour l'élaboration de ce plan.

Ce plan doit être réalisé au démarrage du projet et visé par la DIR Est. Il décline au niveau de l'organisation et des sous-traitants le plan de cybersécurité. La déclinaison des moyens de sécurisation des données (stockage, contrôle d'accès, communication) doit être indiquée.

La liste des personnes ayant accès aux documents confidentiels est précisée et mise à jour.

Les règles et informations (utilisateurs) sont susceptibles d'être auditées sans préavis par la maîtrise d'ouvrage, conformément à l'arrêté du 18 sep 2018, dont on rappelle les points clés :

Article 3 - Contrôles et audits

3.1. Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.

3.2. Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc).

6.2.4 Documentation des actions de configuration

Les actions nécessaires pour respecter les différentes règles de sécurité (durcissement, configuration...) doivent figurer soit dans la documentation générale soit dans un document spécifique. Le document doit

être exhaustif de manière à permettre le remplacement d'un équipement en panne sans perte de niveau de cybersécurité.

6.2.5 Procédures d'installation, sauvegarde et restauration

Le titulaire fournira les supports (ou sources sécurisées) et les procédures et/ou scripts nécessaires à la sauvegarde, installation à partir de postes et serveurs non configurés, et restauration à partir des sauvegardes ; Toutes ces procédures, supports, manuels devront être les plus descriptifs et détaillés possible.

6.2.6 Inventaire et cartographie des livrables

Les documents ci-dessous devront être mis à jour au fur et à mesure des évolutions des installations afin qu'ils correspondent à la réalité des systèmes en fonctionnement, permettant ainsi les audits.

Une description fonctionnelle des installations, comprenant en particulier :

- Les noms et les fonctions des applications,
- Les lieux d'installation des équipements.

Un inventaire des biens, comprenant notamment :

- La liste des plages d'adresses IP des sous réseaux et des points de sortie des sites,
- La liste des serveurs, des postes de travail,
- La liste des équipements réseau et sécurité (routeurs, switches, pare-feu, etc.),
- La liste des dispositifs d'administration (équipements dédiés).

Un schéma d'architecture physique, comprenant :

- Les réseaux locaux,
- Les accès distants
- Les interconnexions avec le réseau bureautique, Internet ou des réseaux tiers,
- Les routeurs et commutateurs réseau,
- Les accès d'administration.

Un schéma d'architecture logique représentant les flux avec le détail des protocoles.

Un inventaire des comptes, comprenant notamment :

- La description des profils utilisateurs ainsi que la liste de leurs droits sur le réseau,
- La liste des comptes utilisateurs par profil, y compris les comptes d'administration,
- La liste des comptes de service.

6.2.7 Risques résiduels

La liste des exceptions aux règles (firmware pas à jour, fonctions non désactivables etc.), leur justification et l'accord de la DIR Est sont consignés dans ce document.

6.2.8 Comptes et mots de passe configurés

La liste des comptes et mots de passes configurés est fournie dans un conteneur Keepass2 et le mot de passe du conteneur communiqué directement au responsable projet DIR Est.

6.2.9 Cahier de recette des fonctions de sécurité

Le cahier de recette des fonctions de sécurité doit permettre de vérifier tous les éléments de configuration et moyens techniques mis en œuvre. La plupart des points de contrôles sont des actions manuelles, par exemple :

- Vérification de la désactivation de comptes génériques, du fonctionnement avec un compte non administrateur,
- Vérification et test des autres points de durcissement : services désactivés, pas de logiciel inutile etc...
- Vérification de l'inventaire (modèles, versions...) via audit d'au moins un composant par type

6.2.10 Maintenance en conditions de sécurité

Des actions de maintenance seront nécessaires afin de maintenir le niveau de cybersécurité de l'installation, et sont à décrire dans un document de "Maintenance en conditions de sécurité".

Le document précise les actions à mener par le mainteneur afin de :

- Mettre en place les mises à jour régulières préventives (ex : mise à jour des signatures anti-virus, des systèmes d'exploitation...) hors limitations éventuelles consignées dans le document risques résiduels
- Vérifier régulièrement (période à préciser) le bon fonctionnement des configurations de sécurité : journalisation, filtrage d'accès (le cas échéant)
- Vérifier le non-engorgement (ressources mémoires, processeur, disque)
- Vérifier régulièrement l'absence de vulnérabilités
 - Soit par consultation de sources à indiquer
 - Soit par exécution d'un outil en phase de maintenance (à préciser également)
- Auditer les comptes configurés et les autres éléments de configuration
- Vérifier la cartographie, l'inventaire (y compris niveaux de firmware), les flux
- Revoir le document des risques résiduels et identifier de possibles solutions (équipement équivalent pouvant remplacer à fonctionnalité identiques, solution technique additionnelle...)

Ces actions seront réalisées au moins une fois durant la période de garantie de parfait achèvement.

6.2.11 EXIGENCES CYBERSÉCURITÉ

Les exigences en matière de cybersécurité sont encadrées par des réglementations nationales et européennes, telles que la directive NIS2, PSSI-E, RGPD, etc. Ces normes visent à assurer l'intégrité, la confidentialité et la disponibilité des données et des systèmes de contrôle, tout en prenant en compte les spécificités du secteur routier et des tunnels. L'objectif est de mettre en œuvre des solutions techniques et organisationnelles adaptées pour prévenir, détecter et répondre efficacement aux incidents de sécurité, tout en maintenant la fluidité et la sécurité du trafic routier.

En conformité avec les obligations de l'Arrêté du 18 septembre, la directive NIS2 et le PSSI-E, Les exigences suivantes sont à respecter :

- Nomination d'un responsable sur le projet pour les sujets de cybersécurité (formé, expérimenté, idéalement avec certification)
- Gestion sécurisée des données projet : Hébergement obligatoire des données sensibles en France, accès contrôlé et limité aux intervenants sur le projet, traçabilité
- Antécédents en termes de cybersécurité : expérience de gestion des exigences sur projet similaire, indication des incidents passés
- Existence d'une charte de sécurité informatique et d'une sensibilisation à la cybersécurité pour tous les intervenants (employés et autres). Formation pour les développeurs, chefs de projets...
- Engagement à donner visibilité sur la chaîne de sous-traitance et à répercuter et garantir le respect des exigences présentes NIS2
- Sélection de produit avec une durée de vie > 5 ans à minima pour les mises à jour de sécurité. Engagement à signaler toute vulnérabilité découverte post-livraison et à fournir des solutions dans des délais contractuellement
- Les livrables ne doivent pas comporter de faille de sécurité connue et pouvoir être mis à jour
- Les réseaux et systèmes utilisés dans le cadre du projet (développement, test, programmation...) sont dédiés au travail sur le projet et ne sont pas également utilisés pour des activités de bureautique. Ils sont à jour de sécurité et dispose d'une solution anti-virus à jour
- L'utilisation éventuel de média amovibles (clés USB etc...) est faite selon des règles de sécurité à préciser
- Les livrables doivent respecter l'état de l'art notamment en ce qui concernant la documentation (mesure de sécurités, flux...), l'administration (consoles dédiées), les sauvegardes (3-2-1 : 3 copies, 2 technologies, 1 exemplaire hors site principal avec chiffrement)
- Une documentation décrit les moyens d'assurer le maintien en condition de sécurité des livrables
- Les livrables incluent les éléments logiciels et procédures permettant d'effectuer des sauvegardes, réinstallation et restauration à partir des sauvegardes
- Le cahier de recette explicite les tests de cybersécurité permettant de vérifier le respect des exigences
- Les équipements munis de système d'exploitation standards sont durcis comme préconisé par les bonnes pratiques de l'ANSSI, et le fonctionnement nominal (logiciels IHM, SCADA...) doit utiliser un compte sans privilège d'administration
- Un inventaire détaillé des composants livrés et une cartographie des flux est fournie et vérifiée lors de la recette

- Un plan d'assurance sécurité est développé et soumis au client par le titulaire, et respecte l'état de l'art
- Le titulaire signale immédiatement tout incident de sécurité via le responsable sécurité à celui du client. Les sous-traitants ont la même obligation
- Les titulaires peuvent être audités sans préavis pour vérifier le respect des clauses de cyber sécurité

La Maîtrise d'Ouvrage (MOA) a déjà mis en œuvre plusieurs mesures de cybersécurité et poursuit actuellement ses efforts dans ce domaine. Néanmoins, l'entrepreneur aura la responsabilité de mener des vérifications et des contrôles approfondis pour s'assurer que les exigences et recommandations en matière de cybersécurité sont effectivement appliquées. Concernant les exigences non encore satisfaites, il incombe à l'entrepreneur d'en informer la MOA et de collaborer étroitement avec elle pour suivre la mise en œuvre de ces actions cruciales en termes de cybersécurité. Cette approche proactive et collaborative vise à garantir une protection optimale des systèmes et des données sensibles du centre de gestion de trafic et des ouvrages à tunnels.

ARTICLE 6.3