

Vidéoprotection intelligente

Conditions d'efficacité et critères d'évaluation

Vidéoprotection intelligente – conditions d'efficacité et critères d'évaluation

Historique des versions du document

Version	Date	Commentaire
V1.0	13/01/14	Création du document
V2.0	27/03/14	Version envoyée pour relecture
V2.1	03/04/14	Relecture L. Khoudour et T. Durlin, ajout cadre de l'étude et conclusion

Affaire suivie par

Violina Iordanova - CEREMA/DTer NP/TM/ST
<i>Tél. : 03 20 49 62 21 / Fax : 03 20 49 63 69</i>
<i>Courriel : violina.iordanova@cerema.fr</i>

Rédacteur

Violina Iordanova - CEREMA/DTer NP/TM/STS

Rellecteurs

Thomas Durlin – CEREMA/DTer NP/TM/STS

Louahdi Khoudour – CEREMA/DTer SO/DALETT/ESAD-ZELT

Sommaire

1 Préambule.....	3
1.1 Cadre de l'étude.....	3
1.2 Objectifs et démarche.....	3
2 Introduction.....	4
2.1 Définition d'un système de vidéoprotection.....	4
2.2 Cadre juridique de la vidéoprotection.....	4
2.3 Définition de la vidéoprotection intelligente	4
2.4 Principales fonctionnalités de la vidéoprotection intelligente routière.....	5
2.5 Bénéfices de la vidéoprotection intelligente.....	6
2.6 Difficultés de la vidéoprotection intelligente.....	6
2.7 Architecture fonctionnelles de vidéoprotection intelligente.....	9
2.8 Problématique des algorithmes de traitement d'images.....	13
3 Conditions d'une exploitation efficace.....	15
3.1 Diagnostic de sécurité.....	15
3.2 Définition d'une stratégie globale.....	16
3.3 Gestion du matériel.....	17
3.4 Choix des implantations.....	17
3.5 Personnel.....	18
3.6 Partenariats ou profils des utilisateurs.....	20
3.7 Systèmes en interface.....	21
4 Évaluation.....	22
4.1 L'évaluation des dispositifs de vidéoprotection.....	22
4.2 Besoin d'évaluation dans les procédés logiciels.....	23
4.3 Besoins en méthodes d'évaluation centrées utilisateur.....	24
4.4 Évaluation des performances du dispositif.....	26
5 Conclusions et perspectives.....	30
6 Références.....	31

1 Préambule

1.1 Cadre de l'étude

Cette étude a été réalisée dans le cadre de l'ORSI SERRES (Solutions pour une exploitation de la route respectueuse de l'environnement et de la sécurité) IFSTTAR / CEREMA, et plus particulièrement de son action 3 consacrée à l'évaluation pluri-critère.

Les retours opérationnels de systèmes de vidéoprotection intelligente, comme dans le cas de la DIR Nord [34], ont récemment identifié que les performances théoriques de ces systèmes annoncées par les constructeurs pourraient différer fortement des performances réelles dans les conditions d'exploitation : contraintes des situations terrain observées, intégration dans l'environnement technique de l'exploitant, prise en compte des contraintes et des besoins des agents en charge de la surveillance des réseaux, ...

Il apparaît donc nécessaire de pouvoir évaluer ces dispositifs, d'une part pour apprécier la pertinence des investissements effectués, et d'autre part pour proposer des pistes d'amélioration pour les systèmes en place et à venir.

Toutefois, les systèmes de vidéoprotection intelligente agissent à différents niveaux techniques (algorithmie, équipements, ...) et humains (interface homme / machine). Cette complexité rend la démarche d'évaluation délicate.

1.2 Objectifs et démarche

Elle a donc pour objectifs de :

- 1) proposer un état de l'art général de l'évaluation des systèmes de vidéoprotection intelligente dans une optique opérationnelle,
- 2) d'identifier les axes de recherche à investiguer sur cette thématique,
- 3) alimenter les réflexions dans le cadre de l'action 3 de SERRES en travaillant sur l'évaluation d'un sujet complexe multi-thématique : technique / humain, impacts sécurité / trafic / acceptabilité, ...

Elle s'appuie pour cela sur l'analyse de communications scientifiques, documents de référence (normes, ...), documentations techniques commerciales, dossiers de spécification (notamment les cas de la DIRIF et de la DIR Nord), rapports d'étude et d'évaluation.

2 Introduction

2.1 Définition d'un système de vidéoprotection

Un système de vidéoprotection¹ est défini généralement comme un ensemble comprenant une ou plusieurs caméras fixes ou mobiles surveillant une scène donnée. Ce système permet de visualiser et/ou d'enregistrer dans un lieu centralisé ou non, les images issues des caméras utilisées. En fonction des besoins, il peut :

- fonctionner de manière permanente ou à la demande,
- être exploité en temps réel ou en différé (données sauvegardées et traitées ultérieurement),
- fonctionner en fusion ou coopération avec un capteur de nature différente (détecteur de présence, détecteur de fumée, etc.).

Appliqué au trafic, il est utilisé essentiellement pour :

- la surveillance du trafic routier,
- la surveillance des zones sensibles des routes (rampes proches ou supérieures à 4%, des zones de congères, des zones de formation de verglas, etc.),
- la surveillance des équipements et des ouvrages sensibles (barrières physiques, éclairage, issues de secours des tunnels (intrusions abusives), tunnels, etc.),
- le secours aux personnes et la défense contre l'incendie dans les tunnels (informations sur l'usager utilisant le téléphone de sécurité, le déroulement des évacuations dans les issues de secours, etc).

2.2 Cadre juridique de la vidéoprotection

La vidéoprotection publique en France est encadrée par des lois et des règlements spécifiques qui autorisent la vidéoprotection sur les voies publiques et dans les lieux ouverts au public, sous certaines conditions limitatives. Tous les textes législatifs et réglementaires relatifs à la vidéoprotection sont consultables sur le site du ministère de l'intérieur : <http://www.videoprotection.interieur.gouv.fr>.

Il est important de rappeler que :

- Les spécifications techniques minimales des images des systèmes de vidéoprotection sont définies par l'arrêté interministériel du 3 août 2007, complété par une annexe technique parue le 21 août 2007. Ces spécifications techniques doivent être respectées par tout nouveau système de vidéoprotection.
- L'autorisation préfectorale est nécessaire pour toute installation de vidéoprotection dans les lieux publics et mixtes ainsi que sur les voies publiques.
- Les usagers de la route doivent être informés de la vidéoprotection par le biais d'un panneau de vidéoprotection comportant un pictogramme représentant une caméra.

2.3 Définition de la vidéoprotection intelligente

Quand le nombre de caméras à surveiller est important, les capacités d'analyse des vidéos et des transmissions des informations d'une machine dépassent les capacités humaines surtout pour des scènes présentant peu de changements, alors qu'un surveillant humain surpasse la machine pour des

¹ Sous réserve des dispositions de la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure le mot « vidéosurveillance » est remplacé par le mot « vidéoprotection ».

scènes très actives présentant beaucoup d'occlusions². Afin de fournir un environnement sûr et sécurisé pour les usagers et le personnel, les organismes d'état et les sociétés d'autoroutes s'orientent vers des systèmes de vidéoprotection intelligente où la détection d'un certain nombre d'événements prédéfinis est automatique. Des études, notamment britanniques, ont montré que les opérateurs de transport devant leurs écrans, deviennent quasiment aveugles quant à la détection visuelle de tel ou tel événement au bout de 45 minutes. Il y a donc lieu d'automatiser toutes ces tâches.

La vidéoprotection intelligente est utilisée pour :

- identifier automatiquement dans des séquences vidéos, des événements particuliers définis préalablement par l'opérateur dans le poste de contrôle du trafic et des tunnels (PCTT) ou dans le Centre d'Ingénierie et de Gestion du Trafic (CIGT),
- avertir l'opérateur en générant des alarmes sonores et visuelles en temps réel,
- transmettre toutes les informations permettant le diagnostic et la vérification du lieu de l'incident et les circonstances avant et après l'occurrence de l'incident,
- consigner dans une base de données les attributs de tous les événements suspects détectés et leurs propriétés contextuelles spécifiques.

La vidéoprotection intelligente peut être utilisée en mode différé pour visualiser les archives vidéos. Des algorithmes d'indexation d'images sont parfois utilisés pour réduire le temps passé à la visualisation et réduire donc le coût de cette exploitation..

Il est à noter que pour qu'un système soit qualifié d'intelligent, il est couramment admis qu'il présente les caractéristiques suivantes [9] :

- présence d'un microprocesseur embarqué et d'un logiciel de détection d'événements dédié (ou un « analyseur » au pied des caméras), afin d'optimiser la capacité de collecter les données et d'effectuer localement les traitements et les calculs,
- capacité de communication bidirectionnelle avec des systèmes extérieurs et des opérateurs humains (envoi des alarmes, des informations de statut, validation des mesures, diagnostic avancé, reconfiguration dynamique, etc).

L'architecture de la vidéoprotection tend actuellement vers un système IP « distribué » à faible « flux ». Modularité et forte capacité d'échanges sont les maîtres mots caractérisant la vidéoprotection aujourd'hui.

Concernant les capteurs DAI, pour qu'ils soient qualifiés d'intelligents, ils doivent s'accorder avec la norme NF EN 60770-3 pour l'évaluation des performances des capteurs intelligents.

2.4 Principales fonctionnalités de la vidéoprotection intelligente routière

Les principales fonctionnalités de la vidéoprotection intelligente routière sont récapitulées dans le tableau 1.

² Certaines études [32] rapportent qu'un individu ne peut suivre attentivement 9 à 12 caméras plus de 15 minutes. Ainsi la probabilité de réagir à un événement capté par un système vidéosurveillance est estimé à 1 sur 1000. A ce titre, la vidéo a été utilisée historiquement comme un outil d'enquête après un événement. Néanmoins, d'après [33] moins de 0,01% des vidéos enregistrées sont visionnées.

Fonctionnalités	Description
Détection d'événements	Circulation et arrêt sur la BAU Formation de congestion Activités des piétons (intrusion dans des zones interdites aux piétons) Circulation dans des zones interdites (voies de bus) Infraction aux règles de la circulation (contresens) Détection d'incendie (tunnels)
Recueil de données de trafic	La collecte, pour chaque voie de circulation, des trois variables fondamentales du flux de trafic : le débit (nombre de véhicules/temps) ; la densité (nombre de véhicules/distance) ; la vitesse (km/h).
Classification des véhicules	La classification des véhicules est réalisée le plus souvent, de la façon suivante : poids lourds et véhicules légers. Des classifications plus élaborées sont également possibles en fonction des besoins d'exploitation de la route et de la gestion du trafic.

Tableau 1 : Fonctionnalités principales de la vidéoprotection intelligente

2.5 Bénéfices de la vidéoprotection intelligente

Les principaux bénéfices de la vidéoprotection intelligente sont regroupés dans le tableau ci-dessous :

Bénéfices	Description
Fonctionnement continu	La vidéoprotection intelligente peut fonctionner 24 heures par jour, sept jours par semaine. Elle fournit des moyens d'extraire visuellement des informations contextuelles en direct comme en différé.
Fonctionnement en temps réel	La vidéoprotection intelligente permet d'identifier en temps réel des situations dans une scène et de suivre leur évolution. L'enclenchement d'une alarme permet à un opérateur humain la prise en compte de l'événement en temps réel.
Contrôle visuel	Le retour visuel émis par le système de vidéoprotection intelligente garantit son bon fonctionnement. L'opérateur se trouvant dans le centre de contrôle du trafic est en mesure de vérifier sur l'écran si la détection et la transmission fonctionnent correctement.
Économie des moyens ³	La vidéoprotection intelligente permet de réduire le câblage, la bande passante et l'espace d'archivage nécessaires en ne transmettant ou n'enregistrant que les données sur les événements pertinents. Concernant le recueil de données : - le système vidéo réduit le nombre de détecteurs par voie ⁴ , - les recherches sur les systèmes de vidéoprotection intelligente ont été encouragées par le coût élevé des systèmes de détection dits « intrusifs » associé à la nécessaire fermeture des voies de circulation pour leur installation.

Tableau 2. Bénéfices de la vidéoprotection intelligente

2.6 Difficultés de la vidéoprotection intelligente

Les principales difficultés de la vidéoprotection intelligente sont récapitulées dans le tableau ci-dessous :

³ Il ne s'agit pas du coût global du système, mais seulement de la réduction des coûts énumérés.

⁴ Un seul capteur optique bien positionné avec la focale adéquate peut surveiller plusieurs voies de circulation.

Difficultés	Description
Robustesse des algorithmes	Les problèmes récurrents des algorithmes de traitement d'images sont : - les bouchons et le trafic dense (occultation des véhicules), - le trafic hétérogène (tailles, formes et couleurs variables des véhicules), - les conditions météorologiques difficiles (pluie, neige, etc.), - les variations brutales de la luminosité, - les occultations entre véhicules ou provoquées par l'environnement ambiant, - les vibrations de la caméra, - l'imprécision du calibrage.
Fiabilité	Les critères de conception des systèmes de vidéoprotection intelligente ne font pas référence à des normes, attestant la sûreté de leur fonctionnement et permettant aux utilisateurs du système de placer une confiance justifiée dans le service rendu. Par conséquent, chaque alarme délivrée par un système de vidéoprotection intelligente doit être évaluée par l'opérateur de surveillance du trafic.
Peu d'études comparant formellement les performances des différents algorithmes en vertu des problèmes récurrents	Il n'existe pas d'algorithmes de référence reconnus pour les applications dans le domaine du trafic routier. Si l'architecture est similaire, chaque constructeur a ses propres algorithmes de détection d'évènements qu'il ne diffuse pas. La comparaison est alors difficile.
Produits « mono-constructeur »	En l'absence de méthodes objectives et systématiques pour évaluer et comparer les performances des systèmes de vidéoprotection intelligente et par conséquent des normes, la vidéoprotection intelligente reste un produit « mono-constructeur ».
Peu d'information disponibles sur les logiciels de gestion vidéo	Les principales entreprises de conception et d'installation des systèmes de vidéoprotection intelligente n'offrent pas suffisamment d'informations sur les logiciels de gestion vidéo (algorithmes, paramétrage, ...).
Coûts élevés	Le coût de déploiement initial est élevé. De plus, les coûts récurrents supplémentaires pour maintenir le système (calibrage au fil du temps, licences) doivent être prévus par les utilisateurs.
Interopérabilité	Les systèmes de vidéoprotection intelligente sont évolutifs et il est évident qu'une attention particulière doit être portée à l'interopérabilité des systèmes en prenant en compte l'évolutivité des formats propriétaires des données et des métadonnées, l'incessante mise à jour logicielle et l'obsolescence accélérée des équipements qui augmente le risque de difficultés de connectivité entre les différents équipements.

Tableau 3. Difficultés de la vidéoprotection intelligente

La difficulté majeure de tout système de vidéoprotection intelligente est son incapacité à prendre en compte correctement les changements soudains d'environnements lumineux. Il n'est pas rare que des algorithmes qui fonctionnent bien dans la journée voient leur précision diminuer en période de baisse de luminosité. Les moments les plus difficiles, sont à l'aube et au crépuscule quand le soleil est très bas à l'horizon, car il provoque soit des ombres artificielles, soit des éblouissements sévères lorsque la caméra est orientée dans sa direction. Presque toujours, les caméras passent automatiquement du mode couleur pendant la journée en mode à faible sensibilité, noir et blanc, lorsque la lumière ambiante est réduite en dessous d'un seuil, au soleil couchant, et inversement lorsque le soleil se lève à nouveau le matin. Bien que le mode à faible sensibilité permet à un observateur humain de mieux voir la scène, cette fonction entraîne souvent des phénomènes de blooming (flou) autour des phares des véhicules et des réflexions sur la chaussée, néfastes pour les algorithmes de traitement d'images. Enfin, les conditions environnementales telles que la pluie, la glace et la neige provoquent d'importants changements dans l'apparence visuelle des objets à détecter, produisant ainsi de nouveaux défis pour les algorithmes.

La précision des systèmes est également affectée par la hauteur de la caméra, par la distance focale

entre la caméra et les voies de circulation et par l'angle d'inclinaison de la caméra [27]. Si l'appareil n'est pas monté suffisamment haut, alors l'image d'un véhicule « *déborde* » sur les voies voisines et entraîne, soit un double comptage, soit des occultations. Si, comme souvent dans les tunnels, la position des caméras est assez basse, il est impossible de différencier les limites de deux véhicules circulant de front [28]. À noter que dans les tunnels, gérés par la DiRIF, chaque caméra permet une distance de détection de 20 fois sa hauteur d'implantation. Cette approximation implique une caméra avec un angle d'inclinaison d'environ 3° par rapport à l'horizontal [11].

Concernant le recueil des données, les comparaisons effectuées avec les boucles électromagnétiques sont unanimes sur la meilleure précision de ces détecteurs, et ceci indépendamment de la hauteur des caméras [27].

En France, Traficon (acquis par FLIR system le 29/12/12, <http://www.traficon.com/>), Citilog (<http://www.citilog.com/>) et NEAVIA (<http://www.neavia.com/>) sont les principales entreprises de conception et d'installation des systèmes de vidéosurveillance intelligente dans le domaine du trafic routier. Certains de leurs produits ont été évalués par le MEDDE.

Pour les besoins de la présente étude sur les systèmes commercialisés aux USA, les résultats des évaluations d'Autoscope (le premier système commercialisé en 1984) et PEEK VideoTrak 900 seront cités [26, 27].

En France, au sein du MEDDE, deux rapports d'évaluations ([29] et [30]) ont été produits concernant les produits NEAVIA par le CEREMA/DTer SO/DALETT/ESAD-ZELT. En termes de mesures de trafic (débit, vitesse, taux d'occupation), la comparaison avec la station SIREDO montre :

- des écarts de débits dont la moyenne se situe entre 2,5% et -1,2%,
- des écarts de vitesse (6 min) de l'ordre de 5 km/h en dessous de 50 km/h et de 5% au-dessus de 50 km/h, les vitesses de NEAVIA étant supérieures aux vitesses SIREDO,
- des taux d'occupation (6 min) inférieurs en général pour NEAVIA, l'écart se situant en moyenne à -0,7 point.

Lors des chutes de neige, la qualité des mesures du trafic a été fortement dégradée.

Concernant la détection des congestions, environ la moitié des congestions n'ont pas fait l'objet d'alarmes. Parmi les congestions tracées, une moitié seulement le sont correctement au début et à la fin de l'événement, l'autre moitié omettant l'une ou l'autre des informations. Les fausses détections de bouchons sont peu nombreuses, mais la vérification à l'aide des photos remontées de façon systématique (toutes les 6 minutes hors incident ou bouchon) ou avec une fréquence accrue en cas de bouchon, s'est avérée difficile.

D'après [27], les algorithmes de la vidéoprotection intelligente ne sont pas en mesure de maintenir un niveau d'efficacité souhaitée dans la détection d'incidents.

Le CEREMA/DTerIF est chargé de l'évaluation des produits Traficon (Traficam) et Citilog (Xcam) . Les résultats de ces évaluations n'ont pas été publiés à ce jour.

La plupart des technologies de détection évaluées aux USA présentent une erreur inférieure à 5% en moyenne concernant le débit. Cette précision se dégrade légèrement concernant la vitesse et la classification des véhicules. Pour la classification des véhicules, les évaluations ne sont pas normalisées en termes de catégorie de véhicules. Le nombre de classes peut varier selon l'application. L'évaluation d'Autoscope pour la classification des véhicules selon 5 classes a démontré divers degrés de précision, avec une moyenne allant de 65 à 90% selon le type d'installation et le nombre de voie. Les sites hors autoroute donnent de meilleurs résultats que les sites autoroutiers. L'étude a démontré que la présence d'ombres ou un temps pluvieux dégradent la précision moyenne de 10% supplémentaires [26].

Pour combler les insuffisances des algorithmes de traitement d'images, les efforts des entreprises se sont portés sur la qualité des caméras selon plusieurs directions :

- La fonction de détection de fumées denses dans [11] s'appuie sur l'évolution de la qualité de contraste dans une zone de détection, d'où la nécessité, pour une analyse efficace, de disposer de caméras de bonne qualité, assurant un contraste optimal,
- l'acquisition de Traficon par FLIR Systems, spécialisé dans les caméras thermiques.

Il est à noter que concernant la détection d'incendie à l'aide des systèmes de vidéoprotection intelligente, il n'existe pas de programme national de tests standards pour la protection des tunnels routiers. Le seul document, essentiellement d'information est le [11] et est basé sur le marché de DAI-Réseaux, mené par la DIRIF.

Des améliorations algorithmiques seront, par conséquent, nécessaires pour surmonter les difficultés actuelles et maintenir le coût des systèmes relativement bas en les rendant relativement indépendants des conditions environnementales et du matériel utilisé.

2.7 Architecture fonctionnelles de vidéoprotection intelligente

D'une manière générale, les systèmes de vidéoprotection intelligente comprennent plusieurs modules fonctionnels dédiés à l'acquisition, au traitement, à l'encodage, à la transmission, au décodage, à l'enregistrement et à la visualisation des images. Un système d'information⁵ (SI) DAI⁶ simplifie la maintenance du système et/ou sa gestion.

Dans la plupart des systèmes mis en œuvre par les DIR, des serveurs dédiés (analyseurs DAI) sont utilisés pour exécuter l'analyse des flux vidéos provenant le plus souvent des caméras analogiques. Un distributeur assure :

- la remontée des signaux vidéos et de télémétrie analogiques de la caméra vers un encodeur qui les convertit en signaux numériques pour être transportés sur le réseau IP (le plus souvent, filaire) vers le système de vidéosurveillance (SI vidéo),
- la remontée des signaux vidéos analogiques vers un analyseur vidéo qui transmet des alarmes sur le réseau IP vers le centre de contrôle (SI DAI).

À titre d'exemple, l'architecture du système de vidéoprotection de la DiRIF, peut être citée (figure 1).

5 Un SI peut être défini comme « un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, traiter, stocker, communiquer des informations (sous forme de données, textes, images, sons, etc.) au sein d'une organisation » [1].

6 Au sein des DIR, le terme DAI (Détection Automatique d'Incidents) est utilisé pour désigner les systèmes de vidéoprotection intelligente.

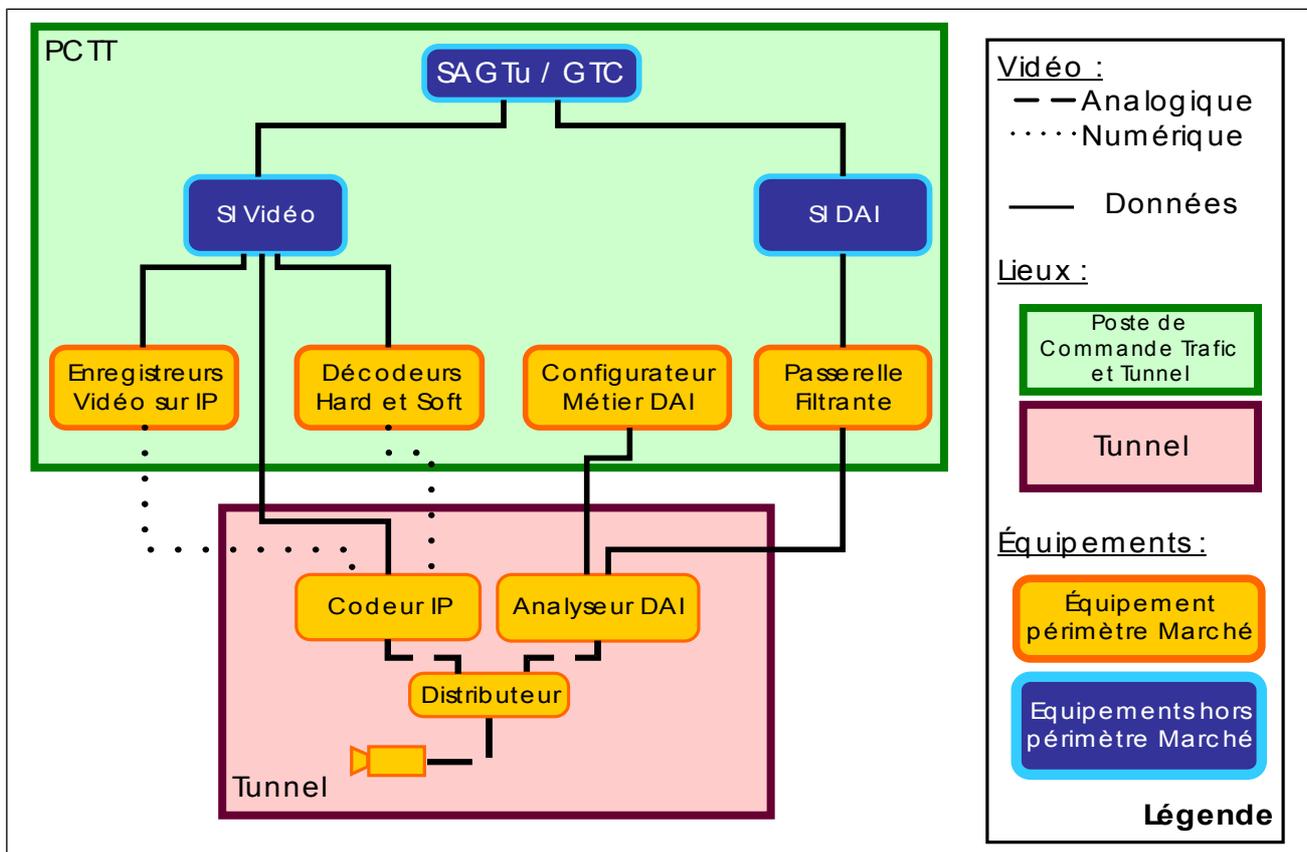


Figure 1 : Architecture de principe d'un système de vidéoprotection intelligente en tunnel

2.7.1 Module d'acquisition

Pour l'acquisition des images, les caméras analogiques sont moins chères, mais engagent des coûts de travaux et d'infrastructure plus élevés, car elles utilisent une technologie en train de devenir obsolète.

Les caméras numériques (caméras IP) sont plus chères, mais plus flexibles, gérables sur le réseau IP et faciles à déployer, ce qui réduit considérablement les coûts d'installation.

Les caractéristiques de l'optique et du capteur sont essentielles pour l'efficacité de l'ensemble du système. La plupart des caméras de vidéoprotection du trafic routier fonctionnent en plan large. Comme mentionné dans le paragraphe 2.6, les scènes de surveillance du trafic contiennent des changements brusques de luminosité, il est alors recommandé d'utiliser des caméras avec une large plage dynamique et passage automatique en noir et blanc pour la surveillance des scènes de nuit. Les systèmes de vidéoprotection routière utilisent des capteurs relativement grands (1/3" ou 1/2"). La résolution et la fréquence d'images sont les deux autres paramètres importants pour une caméra. Pour les systèmes de vidéoprotection, le choix est porté sur des formats d'images de taille minimale, mais offrant une qualité acceptable : VGA (640x480), CIF (352 x288) et 4CIF (704x576).

Pour pouvoir détecter tout événement en temps réel, la cadence d'au minimum 12 images par seconde est recommandée, en particulier pour un traitement automatique. D'après l'annexe technique de l'arrêté interministériel du 3 août 2007, parue le 21 août 2007, les caméras fonctionnant en plan large doivent fournir une cadence minimale réelle des images de 6 images par seconde, cadence nécessaire pour une visualisation correcte et la lever de doute.

Il est important de noter que la contrainte électrique est une contrainte de conception majeure pour les caméras fonctionnant avec des sources énergétiques autonomes (énergie solaire). Un autre aspect important est la dissipation de la chaleur qui doit être faible afin d'éviter le refroidissement actif.

Les caméras installées à l'extérieur ont également des contraintes d'exploitation telles que la taille,

la gamme de température, l'humidité, etc. Elles sont protégées par des caissons, qui sont choisis en fonction des indices de protections IP (IP66 ou IP67), IK (IK08 (en tunnel IdF) et la résistance à la corrosion.

Concernant la vidéoprotection intelligente, l'installateur doit indiquer la sensibilité des algorithmes à la température et à l'humidité et les moyens à mettre en œuvre pour endiguer ces problèmes. Par exemple, l'efficacité de l'algorithme de détection de PEEK VideoTrak (PEEK Traffic Corporation, 2007) diminue à mesure que la température dans le caisson dépasse 74°C et lorsque l'humidité dépasse 95% [27].

2.7.2 Module de traitements des images

Le **module de traitement** d'images réalise les tâches suivantes : la compression du flux vidéo, la conversion du signal analogique en signal numérique, l'analyse du signal numérique pour la détection d'un événement et/ou pour le recueil de données. Le micrologiciel embarqué dans ce module contrôle tous les périphériques, la gestion de toutes les tâches logicielles, la reconfiguration via l'interface réseau.

Il est actuellement possible de réaliser **le traitement** des images au sein même de la caméra IP et de réduire drastiquement la charge du réseau et l'espace du déploiement. Il s'agit des caméras intelligentes ou smart caméras, définies comme suit : « *Une caméra intelligente (CCD ou CMOS) filme une scène et réalise le traitement des images et l'analyse du contenu des données. Elle peut être configurée pour envoyer des flux vidéos sur le réseau de transmission pour une visualisation en direct et/ou un enregistrement selon une certaine planification, lorsqu'un événement se produit ou sur demande d'un utilisateur autorisé. Les images capturées sont transmises aux formats vidéos Motion JPEG et H.264 à l'aide de différents protocoles, comme : TCP/IP. UDP, FTP/HTTP/HTTPS/SMTP/POP3/MMS* ».

Par conséquent, une caméra intelligente regroupe en son sein, les trois modules fonctionnels principaux : le module d'acquisition, le module de traitement et le module de communication.

2.7.3 Module de communication

Les fonctionnalités du **module de communication** sont les suivantes : PoE (IEEE 802.3af), IGMPv3 (et possibilité de forcer le mode IGMPv2), SNMPv3, HTTPS (pour le cryptage des flux vidéos avant leur transmission sur le réseau), filtrage d'adresse IP (qui accorde ou refuse des droits d'accès aux adresses IP spécifiques), Norme IEEE802,1x (pour le contrôle d'accès à un réseau), fonctionnalités sans fil.

Pour sécuriser les communications via Internet, l'adressage IP des équipements routiers se fait au sein d'un VPN (Virtual Private Network). Deux options sont possibles pour la mise en place d'un VPN :

- Des réseaux opérés de bout en bout : l'opérateur de télécommunications prend en charge l'ensemble de l'ingénierie de trafic, de déploiement, de gestion et de maintenance du VPN sécurisé.
- Des réseaux privés ou autogérés : la DIR élabore, construit et gère elle-même son réseau VPN.

Le risque de piratage informatique des images au niveau de la caméra existe mais reste marginal. Le risque principal est de perdre les images par destruction de la caméra et de son stockage local. Par conséquent, il est souvent recommandé de mettre en place un test automatique régulier de bon fonctionnement des liaisons avec la caméra et il est également recommandé le rapatriement des images au centre de contrôle du trafic pendant les heures creuses, afin d'avoir une sauvegarde supplémentaire des images (caméras sans fil).

Dans le cas de la surveillance d'espaces étendus et des zones de travaux, lorsque l'installation de câbles s'avère trop coûteuse ou lorsque les zones sensibles à surveiller sont impossibles à relier par

câble, les systèmes de vidéoprotection sans fil, type GSM, peuvent être utilisés. Ils permettent de fournir un service à distance et un faible coût de construction via Internet⁷. Ils offrent des possibilités d'intégration dans les systèmes centraux de gestion du trafic et dans leur base de données. Parallèlement, les utilisateurs peuvent obtenir les alarmes et les images sur leurs téléphones mobiles dans la mesure où l'authentification des mobiles GSM entre eux peut être vérifiée lors de la connexion.

2.7.4 Module de stockage

Les solutions de stockage sont de deux types et sont récapitulées dans le tableau ci-dessous :

Type	Description
Internes	<p>Les disques durs intégrés aux enregistreurs vidéos numériques ou aux serveurs représentent la forme d'archivage la plus répandue.</p> <p>Certaines caméras IP disposent d'une carte mémoire flash longue durée (carte MicroSD) permettant d'enregistrer des heures, voire des jours de vidéo.</p> <p>Les solutions internes d'archivage conviennent pour les systèmes de taille modeste comprenant jusqu'à 50 caméras.</p>
Rattachées	<p>L'archivage se fait sur des appareils externes aux enregistreurs ou aux serveurs vidéos. De types NAS ou SAN, ces systèmes offrent un espace de stockage partagé entre les différents clients du réseau.</p> <p>Ces solutions d'archivage sont préconisées pour des grands réseaux de vidéoprotection comportant un grand nombre de caméras.</p> <p>Elles sont supérieures aux systèmes internes en termes d'extensibilité, de flexibilité et de redondance.</p>

Tableau 4. Solution de stockage

Au sein des DIR, les enregistreurs des flux vidéos sont disposés dans les CIGT ou dans les PCTT. Sur le réseau IP, ils sont de type NVR (Network Video Recorder) et permettent, en temps réel, en permanence et sur l'ensemble des caméras d'enregistrer les flux vidéos IP issus des codeurs, et sur commande de relire des flux vidéos dans la pile FIFO (First In First Out) d'enregistrements. Ils transmettent les flux vidéo aux SI Vidéo afin d'élaborer les séquences d'incidents.

A la DiRIF, par exemple, chaque enregistreur a la capacité d'enregistrer 32 flux vidéos IP en simultané et de stocker ces données, en qualité 4CIF à 25 images par seconde, sur une période de 72 heures, et ce indépendamment du nombre de flux lus par les utilisateurs du système. Les enregistreurs sont dimensionnés pour assurer la redondance des enregistrements de deux PCTT, et ceci, en plus de la redondance locale assurée par le biais du RAID 5 : en prenant les caractéristiques du système de vidéoprotection, qui sont les suivantes :

- compression : MPEG-4,
- fréquence : 25 IMPS (images par seconde),
- résolution : 1/2D1 (352x576 pixels),
- bande passante : 2Mb/s,
- durée de stockage : 3 jours (72 heures),

le calcul de la capacité de stockage pour une caméra et pour trois jours est le suivant :

$$\text{Capacité de stockage par caméra} = (2/8) * 72 * 3\ 600 = 64\ 800 \text{ Mo.}$$

Ce qui donne, pour 32 flux vidéos IP de base plus 32 flux IP de redondance :

$$\text{Capacité par enregistreur} = 64 * 64\ 800 = 4\ 147\ 200 \text{ Mo} = 4,2 \text{ To utiles}$$

⁷ Les connexions via Internet sont interdites au sein du MEDDE à l'exclusion de celles prévues via Moréa. La connexion des équipements extérieurs nécessite une dérogation, accordée à condition de respecter des architectures dérogatoires type.

Le nombre minimal des caméras installées est environ 1697, le nombre minimal de NVR de base est 27, le nombre minimal de NVR de base redondance est 27.

Il serait intéressant d'évaluer l'utilisation réelle de toute cette quantité d'enregistrements ainsi que son utilisation conjointe avec le SI DAI, car rapporté aux exigences réglementaires, le système décrit ci-dessus semble surdimensionné.

2.7.5 Module de décodage

Concernant le **décodage**, le décodeur doit implémenter toutes les parties requises d'une norme pour pouvoir décoder un flux binaire conforme. La norme spécifie la façon exacte dont un algorithme de décompression doit rétablir chaque bit d'une vidéo compressée.

Il est souvent recommandé de comparer les résultats sur les images temps réel et sur les images enregistrées.

Il est à noter que les caméras, encodeurs et enregistreurs proposant une compression MPEG-4 uniquement et non spécifiquement labellisée H.264 ou MPEG AVC dans la documentation technique, ne compressent les vidéos qu'avec les anciennes implémentations de la norme MPEG-4.

Les logiciels de décodage, lorsque le nombre de distributions est très élevé sont, le plus souvent, compatibles avec les environnements Windows XP et Vista.

2.7.6 Module de visualisation

Dans les PCTT ou dans les CIGT, les images sont visualisées en continu et en temps réel sur des moniteurs analogiques dédiés ou sur des murs d'écrans (analogiques ou numériques). La visualisation des images peut être répartie sur plusieurs postes informatiques grâce aux droits de visualisation précis par caméra qui sont donnés à chaque utilisateur distant.

Sur les réseaux IP, les images peuvent être aussi regardées à distance sur un téléphone ou un dispositif portable (dans la mesure où l'authentification des mobiles GSM entre eux peut être vérifiée lors de la connexion).

La visualisation des images est dépendante des caractéristiques d'encodage. Dans les PCTT, les images sont diffusées à raison de 25 IMPS, chacune ayant une résolution 4CIF ou D1.

En conclusion, l'architecture fonctionnelle d'un système de vidéoprotection dépend des besoins du gestionnaire du trafic. Elle peut refléter différentes solutions :

- solutions personnalisées et adaptées au type de système à surveiller et à sa complexité,
- solutions de base où la vidéo est enregistrée dans les caméras et aucun autre dispositif d'enregistrement n'est requis,
- solutions complètes où la vidéo est enregistrée sur le serveur du système ou sur des appareils externes aux enregistreurs ou aux serveurs vidéos dans le cas de grands réseaux de vidéoprotection,
- surveillance fournie comme service basé sur le Cloud du fournisseur du système vidéo.

L'analyse des solutions mises en place par les DIR permettra de mettre en évidence les principales caractéristiques de l'état actuel des systèmes, les démarches suivies pour le choix de la solution et les problèmes rencontrés. Pour avoir une vision plus complète, il est nécessaire de décrire les résultats des évaluations des systèmes de vidéoprotection. Une telle démarche couplée à la veille technologique permettra l'élaboration des architectures en fonction des besoins réels des utilisateurs et dans un souci de sobriété des moyens tout en assurant l'efficacité désirée.

2.8 Problématique des algorithmes de traitement d'images

La vidéoprotection intelligente appliquée au domaine routier est étroitement liée au développement des technologies vidéos. Actuellement, les techniques d'analyse d'images dépendent des performances de la caméra, de sa configuration et de son implantation. La plupart des algorithmes sont conçus pour traiter des images provenant d'une caméra fixe afin d'avoir un « calibrage » du

système relativement simple. Différentes techniques de traitement d'images sont utilisées pour la détection des événements, le recueil de données et la classification des véhicules. Ces techniques sont généralement bien connues des scientifiques travaillant dans des domaines connexes de la recherche. Une description détaillée des algorithmes peut être trouvée dans de nombreux articles scientifiques, incluant les articles de [12] à [23]. Néanmoins, peu d'études comparent formellement les performances des différents algorithmes. Par conséquent, il n'existe pas d'algorithmes de référence reconnus pour les applications dans le domaine du trafic routier, sauf peut-être pour les algorithmes exploitant la stéréovision pour la reconstruction tridimensionnelle de scènes, pour lesquels une base de données commune d'images artificielles est mise à disposition (base Middlebury spécifique contenant des paires d'images fixes naturelles ou artificielles). Dans cette base, les chercheurs en stéréovision peuvent comparer leurs algorithmes de mise en correspondance et de reconstruction 3D, grâce à des vérités terrain existantes aussi dans cette base.

Il est important de souligner que le développement d'algorithmes de traitement d'images par le biais de la recherche font rarement partie des projets de mise en place des systèmes de vidéoprotection intelligente sur les autoroutes et les routes en France. Par conséquent, ces projets ne bénéficient pas d'expérience antérieure sur les algorithmes de traitement d'images, sur le système complet et sur les nouvelles avancées dans le domaine. La plupart, des systèmes implantés en France sont des systèmes commercialisés dont la nature des algorithmes n'est pas documentée. Rares sont aussi les publications sur les résultats d'évaluations de ces systèmes. En règle générale, ces systèmes sont approuvés par le MEDDE sur les performances annoncées et utilisés dans le domaine routier sans être testés en profondeur.

Les performances annoncées des systèmes commercialisés sont globalement : une probabilité de détection supérieure à 90%, une probabilité de fausses alarmes inférieure à 1 fausse alarme/jour/caméra/fonctionnalité et un temps moyen de détection compris entre 10 et 20 secondes. Exemple [11] :

Détection d'événement	DR	TMD
PL	95,00%	de 12 s à 15 s
Contresens	95,00%	de 2 s à 10 s
Piéton ⁸	90,00%	de 5 s à 10 s
Fumée dense	95,00%	10 s
Véhicule arrêté sur BAU	98,00%	15 s
Véhicule arrêté en pleine voie en circulation fluide	98,00%	15 s
Objets immobile ⁹	90,00%	15 s
Véhicule arrêté en pleine voie en circulation fluide	90,00%	30 s

Tableau 5. Performances annoncées des systèmes commercialisés

8 La distance de détection sera limitée à la moitié de la distance entre les caméras ou 10 fois la hauteur.

9 Pour des objets de surface visible supérieure à 0,5 m². La distance de détection sera limitée à la moitié de la distance entre les caméras ou 10 fois la hauteur.

3 Conditions d'une exploitation efficace

Pour la description des conditions d'une exploitation efficace, la présente étude s'inspire de « *l'évaluation des dispositifs de vidéoprotection dans la lutte contre la criminalité, le terrorisme et la prévention de la délinquance* » [25], réalisée par l'Institut National des Hautes Etudes de Sécurité. Cette étude a rassemblé les conditions préalables à l'exploitation optimale de l'outil. La même démarche est entreprise, dans ce chapitre, en l'appliquant aux dispositifs de vidéoprotection pour la gestion du trafic routier et la sécurité des usagers en attendant de disposer au sein du MEDDE d'une somme de travaux d'évaluation conséquent permettant de cerner les modalités adéquates pour la construction d'un plan d'évaluation de l'impact de la vidéoprotection dans les politiques de sécurité et de gestion du trafic routier.

Pour compléter le travail entrepris, réalisé essentiellement à partir de documents disponibles sur Internet, une recherche plus approfondie doit être envisagée, incluant des visites sur sites et des entretiens avec les utilisateurs et les responsables d'exploitation des systèmes de vidéoprotection.

Les principales conditions d'une exploitation efficace de la vidéoprotection intelligente, appliquée au trafic routier sont :

- un bon diagnostic de sécurité,
- la définition d'une stratégie d'exploitation globale,
- le choix des implantations,
- la gestion du matériel,
- le personnel qualifié,
- l'identification des partenaires,
- la gestion des interfaces avec les autres systèmes de gestion du trafic et/ou de sécurité.

3.1 Diagnostic de sécurité

Afin d'optimiser la phase préparatoire aux études d'installation d'un système de vidéoprotection, il convient que le Maître d'ouvrage, en concertation avec l'exploitant du réseau routier, établisse un diagnostic et une analyse des besoins de sécurité portant sur :

- la connaissance exacte de la situation en termes de sécurité (zone sensible de la route, ouvrage sensible, zone interdite aux piétons, zone réservée à un type d'usagers, etc.),
- l'établissement d'un état des moyens disponibles et des actions de prévention déjà mises en œuvre,
- la liste des attentes de l'exploitant,
- la définition des actions devant être conduites et pour lesquelles l'installation d'un dispositif de vidéoprotection est pertinente.

L'analyse de la situation en termes de sécurité peut être réalisée sur la base des indicateurs suivants :

- types de perturbations (incidents) constatées (perturbation récurrentes, perturbations non récurrentes mais prévisibles, perturbations non récurrentes et non prévisibles),
- nombre des perturbations et/ou incidents relevé(e)s,
- étude de la répartition temporelle et géographique des perturbations (des incidents),
- efficacité de la détection préalable aux interventions.

Pour rappel, l'analyse des perturbations récurrentes est souvent menée en utilisant :

- les courbes débit-vitesse (diagramme fondamental) des sections sensibles,

- le niveau de service local de circulation (NSC) sur les sections sensibles,
- la vitesse moyenne,
- le temps de parcours (élaboré par les systèmes informatiques de gestion du trafic),
- la cartographie des congestions (élaborée par les systèmes informatiques de gestion du trafic),
- les indicateurs globaux de circulation (volume de trafic (véh_xkm), temps total passé en circulation (véh_xh), volume d'encombrement (hx_xkm) issus des systèmes informatiques du gestionnaire.

Les données d'accidentologie (BAAC), les bulletins de météo France, la main courante, la base de données incidents des SAGT des exploitants et les procédures d'accidents (PV) rédigées par les forces de l'ordre pour chaque période du temps doivent être analysés principalement en fonction de leurs références temporelles, kilométriques, météorologiques ainsi qu'en fonction du type des véhicules impliqués. Les données vidéo pour l'observation des zones à risques peuvent compléter le diagnostic de l'accidentologie.

Le diagnostic doit comprendre des zones « témoins » sans vidéoprotection et présentant les mêmes caractéristiques que les zones équipées, afin de mieux évaluer l'effet de la seule vidéoprotection.

3.2 Définition d'une stratégie globale

À l'issue du diagnostic, les lieux les plus appropriés pour y installer les caméras sont déterminés et l'architecture fonctionnelle est choisie en fonction :

- des besoins réels de l'exploitant,
- de l'environnement humain (profils des utilisateurs),
- de l'environnement matériel (type et géométrie de l'ouvrage, réseaux d'énergie et de télécommunications, langage de communication, système informatique d'exploitation en temps réel, etc.),
- de l'environnement logiciel.

Le plus souvent, la vidéosurveillance intelligente est exploitée en temps réel. Les alarmes sont censées déclencher une intervention rapide et une organisation adéquate. Néanmoins, tous les événements n'ont pas le même niveau d'importance. Ce niveau dépend de leur vocation : gestion du trafic ou secours aux personnes. Ainsi, la seule vocation à la gestion du flux de trafic ou à la surveillance du matériel ne nécessite pas à priori un dispositif aussi conséquent que le secours aux personnes et la défense contre l'incendie dans les tunnels et elle ne requiert pas une coopération aussi étroite avec les forces de l'ordre et de lutte contre les incendies.

Il est important de rappeler que l'instruction technique relative aux dispositions de sécurité dans les nouveaux tunnels routiers, annexée à la circulaire 2000-63 du 25 août 2000, précise que : « *Un réseau de surveillance par télévision couvrant la totalité de l'intérieur du tunnel et ses abords immédiats ainsi qu'un système de détection automatique d'incidents sont obligatoires lorsqu'une surveillance humaine permanente ou non est assurée ...* ».

Malheureusement, l'instruction technique ne précise ni la nature du système de détection automatique des incidents, ni le type d'événement à détecter par ce système. Elle impose la vidéoprotection et annule l'étape de diagnostic de sécurité la concernant. Pour combler cette lacune, [11] propose de classer les événements à détecter de la manière suivante :

- événements de niveau 1 : véhicule arrêté, apparition de fumée,
- événements de niveau 2 : qualification du trafic (trafic fluide, trafic congestionné), véhicule en contre-sens,
- événements de niveau 3 : piéton,

- événements de niveau 4 : objet, véhicule lent,

et rappelle l'importance du choix des événements à détecter, car les événements détectés modélisent la stratégie générale d'action des services de gestion du trafic.

3.3 Gestion du matériel

Le choix du matériel est essentiellement fonction des objectifs poursuivis, des équipements préexistants, de l'environnement immédiat, des besoins en termes de qualité et de débit et surtout des finances disponibles. Il est constamment recommandé de choisir des systèmes pouvant fonctionner avec des hauteurs des caméras différentes, permettant la réutilisation des caméras existantes ou ayant une interopérabilité entre les dispositifs de « vidéosurveillance » et de « DAI ». Dans la réalité, l'installation d'un système de « DAI » est systématiquement accompagnée de la dépose des caméras existantes et de leurs systèmes de soutien. Dans les tunnels, par exemple, les deux systèmes utilisent les mêmes caméras, mais la « DAI » fonctionne de manière indépendante de la « vidéosurveillance ».

Le CIGT doit établir très régulièrement un diagnostic d'utilisation de chaque caméra, afin de connaître les raisons pour lesquelles certaines sont sous-utilisées et, au besoin de les déployer ailleurs.

Pour un meilleur diagnostic, il peut être couplé à l'établissement des cartographies des congestions et des incidents, fournies par le système de vidéoprotection intelligente et mise à jour en temps réel ainsi qu'à la géolocalisation précise des véhicules d'intervention. Cette cartographie permettra d'obtenir également une plus grande réactivité des entités d'intervention.

3.4 Choix des implantations

Le positionnement de la caméra est aussi important que la technologie utilisée. Même avec une meilleure technologie, une caméra mal positionnée (trop loin ou dans une zone mal éclairée) sera moins efficace. Le positionnement des caméras doit tenir compte des points suivants, récapitulés dans le tableau 4 :

	Description
<i>La luminosité</i>	La luminosité naturelle de jour et le niveau d'éclairage artificiel de nuit.
<i>La hauteur de positionnement de la caméra</i>	Positionnée trop haut, la caméra souffrira d'un mauvais angle de vue à son pied et d'un déficit du niveau de détail dû à l'éloignement de la caméra par rapport à la scène filmée. Positionnée trop bas elle sera exposée au vandalisme et sera inefficace pour la prise de vues distantes. De plus si elle est trop basse, des phénomènes d'occultation peuvent apparaître par des objets qui n'intéressent pas la scène filmée. C'est très souvent un compromis qu'il faut chercher.
<i>La saisonnalité</i>	Arbres à feuilles, hauteur du soleil.
<i>L'éblouissement</i>	Soleil bas, contre-jours, lampadaires à proximité, phares des véhicules.
<i>Les intempéries</i>	Brouillard, neige, pluie d'orage, vent.
<i>La propreté de la caméra</i>	Il est important de respecter les recommandations du constructeur sur le nettoyage régulier.
<i>Les zones privées</i>	Obligation de positionnement d'un nombre de masques numériques nuisibles à l'efficacité de la caméra.
<i>Les algorithmes de détection</i>	La position optimale de la caméra dépend des algorithmes de détection vidéo intelligents implémentés.

Tableau 6. Points à prendre en compte dans le choix des implantations

La réalisation de prises de vues en position réelle est fortement conseillée lors des études d'implantation de la caméra. Les prises de vue doivent confirmer le fonctionnement désiré du

système dans des conditions très variables de circulation (trafic fluide, trafic congestionné) et selon une très grande diversité des conditions lumineuses (soleil, nuages, crépuscule, nuit, pluie).

Le choix de positionnement des caméras a un impact direct sur le coût de réalisation des travaux : l'implantation des caméras est toujours conditionnée par la proximité des artères de communications et des sources d'alimentation.

3.5 Personnel

3.5.1 Recrutement adapté

L'emploi d'un personnel qualifié et réactif constitue une des conditions essentielles pour transformer la vidéoprotection en un outil efficace en matière de gestion du trafic, de secours aux personnes et de défense contre l'incendie. Pour cela, l'opérateur doit réunir des compétences avérées. Il doit connaître parfaitement les lieux vidéosurveillés et les différents types de perturbations susceptibles d'apparaître afin d'anticiper le comportement du flux de trafic et/ou des usagers. En d'autres termes, il doit réagir rapidement aux diverses perturbations repérées sur l'écran et aux alarmes envoyées par la vidéoprotection intelligente. Il est important de souligner que les systèmes de vidéoprotection font partie d'un ensemble de systèmes implantés dans un CIGT. Ces systèmes fonctionnent, le plus souvent de manière indépendante, même si des interfaces fonctionnelles sont parfois recherchées avec, par exemple, la mise en place des SAGTu et GTC pour l'aide à la décision et la gestion centralisée des tunnels. Les architectures fonctionnelles de ses systèmes sont rarement prises en compte dans la description des missions des opérateurs des CIGT et des opérateurs de sécurité des tunnels (OST), qui sont principalement, les suivantes :

- surveiller le réseau et gérer le trafic en temps réel : surveillance, déclenchement et suivi des interventions,
- informer les usagers, les institutionnels et les partenaires,
- mettre en œuvre des plans de gestion de trafic,
- activer des équipements d'exploitation, diffuser les bulletins météo d'alerte,
- suivre les dysfonctionnements des équipements et des systèmes et vérifier notamment leur niveau de disponibilité,
- en période hivernale : diffuser la synthèse des remontées d'informations des états de conduite hivernale et des conditions météorologiques,
- réaliser et diffuser la synthèse des prévisions de travaux, les tableaux des astreintes et élaborer les bilans statistiques.

Par conséquent, l'opérateur n'est pas tenu à l'analyse permanente des écrans vidéos.

Pour compléter les conditions d'efficacité du système, une description des concours de recrutement des opérateurs et de la démarche utilisée pour évaluer le profil des candidats recherchés semble nécessaire.

En conclusion sur ce point, la dimension formation est essentielle car le frein à l'utilisation du système est souvent d'ordre humain. Il est important que le personnel soit formé à l'utilisation du système mais aussi à la façon de traiter et de réagir face aux informations de détection fournies par les algorithmes du système.

3.5.2 Gestion des opérateurs par objectifs

D'après [3], une gestion active des opérateurs est préconisée là où les dimensions du dispositif de vidéosurveillance dépassent une certaine taille (au-delà de 10 caméras) : c'est le cas des DIR.

Le paragraphe précédent a énuméré les missions multiples et variées de l'opérateur. Les sections courantes (ou les ouvrages) devant faire l'objet d'une attention particulière ne sont pas les mêmes selon les horaires, les saisons et les priorités de gestion. Les objectifs redéfinis à la semaine peuvent

évoluer en fonction des événements sur le réseau adjacent ou en fonction des activités des partenaires externes (SAMU, Pompier, Gendarmerie, CRS, CISGT voisins, etc.). Si certaines des tâches des opérateurs sont facilement déductibles, leur formalisation et leur suivi par les instances et les services de gestion du trafic permet d'en avoir une approche dynamique, renouvelée et motivante pour les opérateurs.

Concrètement, ce suivi est réalisé par les chefs de salle des CIGT qui supervisent les opérateurs. Ils ont accès aux mêmes fonctions temps réel que les opérateurs qu'ils dirigent, et ils peuvent consulter en plus les images enregistrées par le système informatique. Ils sont chargés de générer les DVD contenant les séquences vidéos que peut demander, sur commission rogatoire, un officier de police judiciaire.

Les « missions » des différents acteurs des CIGT au sein d'une DIR, facilitent la collaboration entre les différents services et les partenaires. .

3.5.3 Formation cohérente

Pour la mise en place de conditions d'exploitation efficaces, l'épineux problème de la formation des opérateurs CIGT se pose. Actuellement, aucune formation initiale ne forme au métier d'opérateurs CIGT. En vue de la professionnalisation des métiers d'exploitation, le CVRH de Mâcon organise, depuis 2008, une formation des « Opérateurs de CIGT » avec deux modules de trois jours. Elle ne porte pas spécifiquement sur la vidéoprotection. Des formations spécifiques concernant ce système sont prévues dans les marchés publics d'installation des systèmes de vidéoprotection.

Par conséquent, l'instruction des opérateurs peut être qualifiée d'empirique. Les opérateurs novices en plus d'un apprentissage technique des systèmes de vidéoprotection (SI vidéo, SI DAI) et des autres systèmes d'information des CIGT ont besoin des notions de droit, de connaissances des institutions, des savoirs de base dans le domaine de la gestion du trafic, des connaissances des enjeux de leur poste et de leur responsabilité, afin de développer des capacités à mettre en place différentes procédures adaptées aux situations simultanées, d'en estimer les conséquences, d'en prioriser le traitement et d'en informer les bons interlocuteurs.

Pour la vidéoprotection intelligente, en particulier, des fiches d'aide à la décision pour chaque alarme (ou plans d'action PAC), intégrées dans le SI DAI, sont souvent recommandées afin d'augmenter la réactivité des opérateurs.

Pour prévoir une formation cohérente, des études d'évaluation sont nécessaires sur les systèmes d'aide à la gestion mis en place dans les CIGT.

Il est à noter que la présence dans les CIGT des agents assermentés et formés à la déontologie policière peut servir de garant à une certaine éthique dans l'utilisation des images.

L'évolution du métier d'opérateur de CIGT est une piste de recherche permanente. D'après [25], certaines contraintes (attention soutenue, fatigue oculaire, espace confiné, horaire décalés, etc.) ne permettent pas d'envisager des carrières complètes dans des CIGT et pose la question de la reconversion, étroitement liée aux avantages financiers liés à ce type d'emploi (travail de nuit, de dimanche et de jours fériés).

3.5.4 Respect de la confidentialité

Afin de garantir la discrétion, les services de vidéoprotection rédigent généralement une charte de confidentialité signée par tous les opérateurs CIGT et parfois affichées en bonne place dans les centres de supervision. Il est fortement recommandé de généraliser cette pratique afin de contribuer à la préservation des libertés publiques.

De même, l'accès au CIGT doit être restreint aux seules personnes habilitées et doit être contrôlé. Parallèlement, le nombre d'agents autorisés à pratiquer des extractions doit être strictement limité, afin de garantir le caractère secret des images stockées.

Enfin, l'installation d'un comité d'éthique chargé de piloter l'implantation du dispositif et de recueillir les possibles protestations permet d'éviter tout éventuel dérapage et de susciter un

consensus parmi les usagers.

A compléter avec les dispositions mises en place par le MEDDE.

3.6 Partenariats ou profils des utilisateurs

La typologie des utilisateurs et des partenaires est souvent mise en avant lorsqu'il s'agit de la définition des conditions d'une exploitation efficace ou des conditions d'une évaluation du système. Les fonctionnalités d'un système s'adressent à différents utilisateurs. Des situations très variées peuvent être rencontrées par les différents utilisateurs, des situations normales qu'anormales débouchant sur des actions différentes.

Le présent paragraphe répertorie globalement les différents profils des partenaires et utilisateurs du système de vidéosurveillance. Un répertoire plus détaillé doit être réalisé lors des futures recherches sur ce système.

3.6.1 Partenaires externes

3.6.1.1 Partenaires d'exploitation

Il s'agit des organisations externes aux DIR, qui exploitent des sections de voirie limitrophes aux zones de responsabilité des DIR et disposant de leurs propres systèmes de vidéoprotection.

Des flux vidéo issus des caméras gérées par les partenaires peuvent potentiellement intéresser les DIR. À l'inverse, les DIR peuvent mettre à disposition des partenaires des flux issus de leurs propres caméras.

Ces partenariats d'exploitation sont formalisés sous la forme de « conventions de partenariat relatif à la vidéosurveillance » entre une DIR et un centre de gestion du trafic urbain, par exemple. Elles prévoient, notamment, l'organisation des réunions régulières, la réalisation des analyses et des plans stratégiques, la transmission des consignes opérationnelles à l'intention des opérateurs.

Dans les architectures existantes, il est convenu que les flux soient fournis par les partenaires sous la forme de flux analogiques, encodés dans le bon format à leur entrée sur le réseau d'une DIR, et inversement, les flux vidéos issues d'une DIR soient transformés en flux analogiques pour être acheminés vers les partenaires. Cette architecture mettant en vis-à-vis le décodeur d'un partenaire avec le codeur d'une DIR, et réciproquement, implique une limitation du nombre de flux pouvant transiter entre les entités. Le nombre de flux pouvant être échangés est limité par le nombre de paires codeurs/décodeurs ainsi mis en place.

Par ailleurs, les partenaires ne peuvent pas piloter les caméras d'une DIR. De même, leurs caméras ne peuvent pas être pilotées par la DIR.

3.6.1.2 Partenaires de maintenance

Il s'agit d'entreprises privées externes des DIR. Certaines de ces sociétés sont amenées à entreprendre des actions de maintenance sur le système de vidéoprotection installé. Il est souhaitable, dans ce cas, que ces personnes disposent des IHM du SI Vidéo et du SI DAI, installées sur un poste nomade, et permettant un accès aux fonctions de base temps réel des systèmes. Ces accès aux systèmes leur permettront notamment de contrôler les actions de maintenance qu'ils effectuent.

3.6.2 Partenaires internes

3.6.2.1 Unités d'exploitation de la route (UER)

Les UER sont localisées dans les centres d'entretien et d'intervention (CEI). Il s'agit de personnels d'une DIR chargés de toutes les interventions sur la voirie (balisage, ramassage d'objet, assistance aux usagers, etc.).

Généralement les CEI disposent d'un ou de deux moniteurs permettant de visualiser des secteurs situés sur leur périmètre d'intervention. Les CEI disposent également d'une IHM du SI Vidéo installée sur un PC. Cette IHM permet essentiellement un accès aux fonctions temps réel du système de vidéoprotection (matriçage et pilotage des caméras).

La liste des caméras accessibles depuis un CEI peut éventuellement être restreinte par paramétrage. Logiquement, les conditions d'exploitation devront être les mêmes concernant la vidéoprotection intelligente, mais les documents examinés lors de cette étude ne permettent pas d'affirmer la présence d'une IHM du SI DAI dans les CEI. Concernant ce dernier point des vérifications auprès de la DiRIF sont nécessaires.

3.6.2.2 Maintenance interne

Il s'agit des personnels DIR chargés de la maintenance des équipements.

Il existe deux acteurs de cette catégorie :

- les techniciens de maintenance (TDM) ou des personnels DIR qui effectuent les interventions de premier niveau, ils sont les premiers informés des problèmes techniques. Ils disposent d'un poste de supervision technique leur permettant d'avoir une vue d'ensemble des équipements routiers (et des équipements tunnels). Pour affiner les diagnostics depuis le module de supervision du système de gestion centrale, il est souhaitable qu'ils puissent lancer une IHM du SI Vidéo (concernant la DAI des vérifications doivent être faites auprès de la DiRIF). Les TDM sont présents en heures ouvrées et sont mobilisables en dehors de ces heures par l'intermédiaire d'astreinte.
- Les services de maintenance centralisée : il s'agit des personnels DIR qui gèrent les TDM.

Les mainteneurs internes sont les premiers utilisateurs des fonctions de supervision de l'installation de vidéoprotection.

3.6.3 Autres partenaires/utilisateurs

Il s'agit de toutes les autres personnes ayant besoin d'accéder ponctuellement ou régulièrement aux fonctions proposées par le SI Vidéo. Ces personnes peuvent, normalement, accéder au système depuis un poste banalisé, après le paramétrage des profils et des droits des différents profils d'utilisateurs.

3.7 Systèmes en interface

Un SI Vidéo doit communiquer avec tous les systèmes informatiques externes pour la mise en œuvre des fonctions dont il a la charge. Par exemple, le SI DAI fournit des alarmes dans l'objectif d'un affichage et/ou d'un enregistrement d'une séquence vidéo et d'autres demandent la disponibilité fonctionnelle et technique des équipements vidéos.

Les protocoles d'échange avec ces systèmes sont définis au cas par cas.

4 Évaluation

4.1 L'évaluation des dispositifs de vidéoprotection

Le besoin en démarches rigoureuses et systématiques pour la conception et pour l'évaluation des systèmes d'information (SI) développés pour la gestion et la supervision du trafic routier a été mise en évidence avec la généralisation de ces systèmes sur les routes et les autoroutes de l'état.

4.1.1 Approches orientées fonction et orientées objet

Pour la modélisation d'un tel système, deux approches principales se distinguent : les approches orientées fonctions et les approches orientées objets.

Les spécifications fonctionnelles permettent la décomposition hiérarchique des fonctionnalités d'un système et la représentation de leurs interactions (architectures fonctionnelles). Parmi les méthodes classiques d'analyse fonctionnelle sont souvent citées : SADT, MERISE, etc. Dans les dossiers des ouvrages exécutés des DIR, les spécifications fonctionnelles sont regroupées dans le dossier des spécifications générales (DSG) et le dossier des spécifications détaillées (DSD).

Les modèles orientés objets centrent les études sur les composants (objets) du système, reliés entre eux pour réaliser un service (ou des services) à un niveau hiérarchique supérieur. Les objets peuvent aussi être assimilés aux éléments matériels ou physiques du système (architectures structurelles). Le langage le plus connu pour les modèles objets est l'UML (Unified Modeling Language). Il est à noter que les méthodes orientées objets prédominent dans la conception et l'analyse des logiciels.

Les modèles comportementaux (ou opérationnels) font le lien entre l'architecture fonctionnelle et l'architecture structurelle.

Par conséquent, le développement d'un plan d'évaluation des dispositifs de vidéoprotection peut prendre de nombreuses formes. Il semble pertinent, de les évaluer comme des SI en prenant en compte leur complexité et interconnexions ; le fait qu'ils utilisent différentes technologies et soutiennent l'activité quotidienne de différentes catégorie d'utilisateurs.

Cette évaluation est indispensable pour les DIR qui doivent assurer la performance et la qualité des systèmes qu'elles utilisent et pour leur permettre une gestion efficace et efficiente des systèmes.

4.1.2 État de l'art général

Pour pouvoir évaluer un système, il est nécessaire de repérer d'abord les éléments à considérer avec attention lors de l'évaluation. Par exemple, pour avoir un SI fiable qui répond aux besoins de l'utilisateur il est souvent préconisé de l'évaluer en termes :

- de qualité des modules applicatifs centrés procédé,
- de l'interface homme-machine réalisée,
- de l'utilité des données obtenues par le système.

Pour que cette évaluation soit rigoureuse, elle doit être faite tout au long de la conception et de la réalisation du système. Il s'agit souvent d'évaluations a priori et a posteriori.

Concernant la vidéoprotection intelligente, il n'existe pas d'étude et d'outils d'évaluation des IHM. Les méthodes d'évaluation des IHM et leurs exploitations, décrites dans [1] par exemple, offrent un potentiel important pour aborder l'évaluation des SI de vidéoprotection intelligente, car la plupart des méthodes sont génériques et peuvent a priori être exploitées dans ce domaine concret. Un résumé des besoins en évaluation des IHM est proposé dans le paragraphe 4.3.

Concernant les modules applicatifs centrés procédé, les besoins d'évaluation dans les procédés logiciels sont résumés dans le paragraphe 4.2 et le programme de recherche ETISEO pour l'évaluation des algorithmes de la vidéoprotection intelligente est décrit au paragraphe 4.3.1.2.

Un autre aspect de l'évaluation est la bonne pratique nécessaire aux évaluateurs pour interpréter les résultats qu'ils soient qualitatifs ou quantitatifs, objectifs (taux d'erreurs enregistrées automatiquement) ou subjectifs (issues des questionnaires ou d'interviews). En règle générale, l'évaluation d'un SI nécessite des équipes pluridisciplinaires d'évaluateurs : spécialistes des facteurs humains, utilisateurs, concepteurs, et chercheurs.

Afin de regrouper les compétences nécessaires pour l'établissement d'une démarche adaptée pour l'évaluation des SI de vidéoprotection, un travail de recherche doit être effectué afin de lister les programmes de recherche en France qui ont fortement contribué au développement des méthodes et des outils d'évaluation des systèmes de vidéoprotection intelligente.

En règle générale, les méthodes et les outils d'évaluation dépendent de l'état de développement du système à évaluer : réalisé concrètement ou envisagé pour une réalisation future, et doivent intégrer les conditions souvent variables au cours de la vie du système.

L'objectif de ce paragraphe est de décrire les besoins d'évaluations au cours de la vie d'un SI, afin de déterminer un cadre d'évaluation pour les SI de vidéoprotection intelligente dans les CIGT.

Il est important de souligner le rôle essentiel de la documentation des systèmes, sa mise à jour tout au long de la vie d'un projet et son intégration correcte dans le DOE (Dossier des Ouvrages Exécutés). Bien souvent, les premières étapes d'une évaluation consistent à rassembler les données du système et ses différentes contraintes techniques et fonctionnelles et à effectuer une analyse approfondie du système, en s'appuyant sur le DOE, les opérateurs en salle de contrôle et le service de maintenance.

4.2 Besoin d'évaluation dans les procédés logiciels

Les procédés logiciels décrivent les bonnes pratiques que doit suivre une entreprise pour mener à bien les tâches de développement d'un logiciel (interface et/ou procédé). Ces méthodes sont utilisées lorsque le système à évaluer n'existe pas. Dans l'ingénierie du logiciel, les modèles de cycle de vie se sont imposés. Ils sont essentiellement utilisés dans la définition de l'organisation, de la planification, ou encore dans la détermination des coûts d'un projet. Leur rôle est également d'imposer aux développeurs de respecter l'ordre d'exécution des activités : expression des besoins (maîtrise de contenu, connaissance des utilisateurs, cahier des charges), spécification des modules du système, conception préliminaire des modules du système, spécification logicielle, conception préliminaire, conception détaillée et codage, ainsi que d'assurer que le logiciel délivre des artefacts corrects. Une manière de s'en assurer est de procéder à différents tests.

Le tableau ci-dessous récapitule les tests habituellement rencontrés dans les CC (Cahier des charges). Ils correspondent au modèle de cycle de vie logiciel en V :

Tests	Description
Cas de test	Chemin fonctionnel à mettre en œuvre pour atteindre un objectif de test. Un cas de test est défini par le jeu d'essai à mettre en œuvre, le scénario de test à exécuter et les résultats attendus.
Scénario de test	Procédé à suivre par le testeur pour exécuter le cas de test : manipulation à effectuer, dialogue homme/machine ... Le même scénario peut être utilisé dans plusieurs cas de test.
Tests d'intégration	Ils permettent de vérifier progressivement que l'ensemble constitué par les composants logiciels assemblés répond aux spécifications fonctionnelles et techniques. Ils doivent, s'il y a lieu, activer les interfaces avec les applications connexes. Ils sont exécutés lors de la phase de conception du système et/ou pendant la conception préliminaire.
Tests de non-régression	Dans le cas de changement de version, ils permettent de vérifier que les modifications apportées n'ont pas entraîné d'effets de bord non prévus qui pourraient dégrader le comportement du logiciel antérieurement validé. Ils portent sur l'exécution de tests déjà joués afin de s'assurer que le système répond toujours aux exigences spécifiées.
Tests de performances	Ils permettent de vérifier des contraintes de temps de réponse et d'occupation mémoire. Ils peuvent faire partie des tests de validation ou de non-régression.
Tests unitaires	Ils permettent de vérifier le fonctionnement de chaque composant logiciel modifié ou nouveau dans des cas de fonctionnement normal, aux limites ou dégradé. Ils s'appuient sur la structure interne du composant (tests « boîte blanche »). Les vérifications portent sur l'initialisation des rubriques, les contrôles de saisie, les règles de gestion, les messages d'erreur, la gestion du curseur, la gestion des touches fonctions, l'enchaînement des écrans, ... Ces tests sont exécutés lors de la phase de conception détaillée et codage.
Test de validation	Ils permettent de vérifier que les exigences fonctionnelles et techniques du CC sont respectées. Ils s'effectuent sans connaissance de la structure interne. Ils sont effectués lors de la phase de spécification logicielle.

Tableau 7. Tests cycle de vie logiciel en V

Concernant la vidéoprotection intelligente, il n'y a pas de développement de logiciels spécifiques dans les marchés publics ; les logiciels installés sont des logiciels commercialisés, répondant à un cahier des charges, le plus souvent réalisé dans le cadre d'un marché public de MOE pour les études et les travaux.

Dans la pratique, il n'y a pas d'évaluation des procédés logiciels. Les critères de performance et les tests de validation du système, décrits dans le cahier des charges des marchés d'installation et réalisés en phase OPR sont centrés utilisateur. Dans cette démarche, les interactions hommes-machine sont laissées à l'appréciation du concepteur, les utilisateurs ne sont pas concernés explicitement et les tâches humaines ne sont pas décrites.

Les tests ne permettent pas d'identifier les faiblesses des algorithmes en fonction de leurs conditions d'utilisation.

Il paraît évident que l'élaboration des méthodes d'évaluation unifiées des procédés logiciels pour la vidéoprotection intelligente mérite un effort de recherche afin d'identifier les actions appropriées pour introduire dans les marchés publics les attentes réelles du système tant sur la partie interactive que sur la partie applicative, et ceci à tous les stades du projet.

4.3 Besoins en méthodes d'évaluation centrées utilisateur

Ces méthodes sont utilisées le plus souvent lorsque le système existe. Les méthodes les plus utilisées sont recensées par la norme ISO/TR 16982:2002 « Ergonomie de l'interaction homme-système – Méthodes d'utilisabilité pour la conception centrée sur l'opérateur humain ». Elles sont le plus

souvent centrées sur les critères d'utilité et d'utilisabilité [2] et sont fondées sur le recueil et l'analyse des données comportementales provenant de l'utilisation du système et de son IHM par des utilisateurs représentatifs de la population des utilisateurs. L'évaluation est souvent expérimentale et doit être effectuée dans un environnement le plus proche possible de la réalité. Il est à noter que l'efficacité d'une IHM est lié à la capacité de l'utilisateur à percevoir, à interpréter les informations, à raisonner sur celles-ci et agir en conséquence.

Il est à noter que les normes ISO 9126 et ISO 9141 proposent une définition de l'utilisabilité comme facteur de qualité du logiciel.

4.3.1 Évaluation de l'utilisabilité

L'utilisabilité rend compte de la qualité de l'interaction homme-machine, en termes de facilité d'apprentissage et d'utilisation, ainsi que de qualité de documentation. Par définition, elle est le rapport entre l'utilité potentielle d'un produit et son utilité réelle. Il est important de rappeler que toute évaluation consiste à comparer un modèle de l'objet évalué à un modèle de référence permettant d'établir des conclusions. La méthode de modélisation choisie dessinera le cadre de la future démarche d'évaluation des SI de vidéoprotection intelligente.

L'évaluation de l'utilisabilité doit inclure aussi les dysfonctionnements du système (ou les modes dégradés), car l'absence d'informations adéquates aux contextes anormaux rendra la tâche des utilisateurs plus difficile et leur niveau de stress plus important. Une analyse des dysfonctionnements débouchera principalement sur l'ensemble des variables pertinentes et significatives de l'ensemble des causes possibles d'un dysfonctionnement donné, afin de pouvoir aider l'utilisateur qualifié à localiser la cause de la panne et à rétablir une situation de fonctionnement normale [7].

4.3.1.1 Approches empiriques

Elles concernent essentiellement l'IHM. Les techniques et méthodes associées à cette classe peuvent être utilisées pour l'évaluation de l'IHM du SI de vidéoprotection intelligente lorsque des utilisateurs expérimentés sont disponibles. Certaines de ces méthodes exigent une interaction directe entre les évaluateurs et des utilisateurs expérimentés, alors que d'autres méthodes consistent à recueillir des données représentatives de l'interaction à l'aide d'observations, puis d'analyser les traces de l'activité des utilisateurs expérimentés.

Lorsque des utilisateurs expérimentés ne peuvent pas intervenir dès le début du projet, l'évaluation du système et de son IHM nécessite obligatoirement une analyse qualifiée d'expert.

Pour l'évaluation d'une IHM, certains préconisent le respect de recommandations ergonomiques centralisées dans des grilles, d'autres sont fondées sur l'implication personnelle et le jugement d'experts en communication homme-machine.

Ces techniques peuvent être envisagées a priori dès les étapes d'expression des besoins et introduire, de cette façon, le cadre de l'évaluation dès l'étape de spécification.

Pour chacune des approches empiriques, il s'agit d'une analyse de données recueillies a posteriori. Elles permettent d'en tirer les conclusions avec les utilisateurs pour les spécifications du système interactif futur (ou modèle a priori basé sur l'expertise humaine), l'amélioration de l'existant ou la précision des besoins en aide ou en formation [5].

4.3.1.2 Approches analytiques

Ces approches sont basées sur des modèles formels (informatisés ou non) ainsi que sur la mise en œuvre de métriques objectives. Ils peuvent être utilisés a priori dès les étapes d'analyse et de spécifications. De plus, ils servent de support de dialogue entre les intervenants du projet.

	Description
<i>Analyse et modélisation du système</i>	<p>Pour l'évaluation de l'utilisabilité, il est nécessaire d'analyser et modéliser finement les systèmes mis en place, leurs problématiques, leurs contraintes, et leurs caractéristiques selon différentes dimensions (structurelles, fonctionnelle, etc.). Une telle modélisation permettra le recensement des différentes situations normales et anormales pour lesquelles des tâches sont effectuées par les utilisateurs de l'IHM et/ou les algorithmes [4], afin de détecter des erreurs de conception et de déterminer jusqu'à quel point le système interactif est adapté pour les tâches pour lesquels il a été conçu.</p> <p>Pour appliquer cette approche, un modèle de référence est nécessaire sur lequel se basera la comparaison. En termes d'analyse et de modélisation, le domaine est très riche, de nombreuses techniques et méthodes sont disponibles [4]. Pour la vidéoprotection, le travail de recherche consiste en l'élaboration de la démarche permettant de qualifier et certifier les systèmes de vidéoprotection intelligente.</p>
<i>Analyse et modélisation des tâches humaines</i>	<p>L'analyse et la modélisation des tâches humaines font l'objet de recherches actives depuis une vingtaine d'années [4]. Dans le domaine de la gestion du trafic routier, un travail de recherche est nécessaire pour déterminer les méthodes appropriées à l'évaluation des tâches humaines relatives à la vidéoprotection intelligente. L'analyse des tâches humaines est un travail d'équipe et doit susciter les démarches participatives des DIR et de ses partenaires. Elle contribuera à faire ressortir de manière fine les objectifs, les stratégies, les besoins des utilisateurs impliqués dans différentes situations normales et anormales, apportant ainsi des informations précieuses pour les spécifications des systèmes interactifs, leur amélioration et/ou des outils d'aide à mettre à disposition des utilisateurs.</p>
Tableau 8. Exemples d'approches analytiques	

4.3.2 Évaluation de l'utilité

Il est possible d'évaluer l'utilité par une analyse de la tâche et/ou des activités en se basant sur deux critères principaux : l'adéquation à la tâche et la répartition du travail. L'adéquation à la tâche consiste à vérifier si les procédures cognitives développées par l'utilisateur sont similaires à celles initialement développées par le concepteur et donc à estimer si la tâche (réelle) redéfinie par l'utilisateur est en accord avec la tâche (prescrite) à effectuer. Concernant le critère de répartition du travail, il s'agit d'analyser la façon dont est organisé le travail entre l'homme et la machine [5].

Dans les systèmes industriels, les critères de répartition sont généralement la performance, la charge de travail et la sécurité [6].

4.4 Évaluation des performances du dispositif

Dans la pratique des procédures d'évaluations à posteriori sont utilisées. Elles sont de deux types :

- Mise en place d'un plan expérimental complet comprenant toutes les composantes importantes inhérentes au traitement des images vidéo : position des caméras, paramètres d'installation, distances focales, luminosités différentes, jours de semaine, week-end, heures pleines, heures creuses, météo variée, etc... Par la suite les algorithmes vidéo sont mis en place et appliqués à toutes ces situations. Les événements à détecter sont le plus souvent simulés en conditions réelles par des humains. Ensuite une comparaison des résultats des algorithmes avec la vérité terrain vidéo permet de fournir des performances.
- Par ailleurs, les données collectées par une boucle de type SIREDO sont comparées aux données collectées par le système de vidéoprotection intelligente.

Ces procédures dépendent de la séquence vidéo de test, des métriques et des vérités terrains. Il est souvent impossible de prédire les performances d'un algorithme si l'un de ces paramètres change [31].

Constatant l'état actuel des procédures d'évaluation, il paraît nécessaire d'identifier les recherches

lancées actuellement dans le but de définir les connaissances scientifiques et techniques nécessaires pour mettre en place une plate-forme permettant de qualifier et certifier les systèmes de vidéoprotection intelligente. Le procédé classique d'évaluation d'un système de vidéoprotection intelligente s'appuie sur les trois piliers suivants [31] : bases de données de vidéos, vérités de terrain et critères d'évaluation (indicateurs).

Données d'entrée	Descriptions
Base de données vidéo	<p>Les systèmes de vidéoprotection intelligente doivent être testés sur des séquences vidéos différentes. Ces séquences doivent être aussi représentatives que possible des situations réelles du système évalué. Si le contexte est variable et complexe, les séquences de tests doivent représenter ces variations. Les données doivent être réparties en deux ensembles : l'un, pour configurer les algorithmes et le second, pour l'évaluation.</p> <p>Le problème auquel les évaluateurs sont souvent confrontés est que la tâche d'acquisition et d'annotation des séquences exige beaucoup de temps et d'efforts humains. Pour cette raison, cette tâche onéreuse ne peut pas être intégrée dans les marchés publics, d'où l'importance d'une base de données. La gestion et le partage de cette base seront déterminés au sein du MEDDE.</p>
Annotation	<p>L'annotation ou la réalité du terrain décrit les propriétés véritables d'une séquence vidéo. Le processus d'annotation dépend du degré de détail et peut être très long. Il peut décrire les variables fondamentales du trafic ou la description détaillée des événements qui se déroulent dans la séquence avec une précision de fraction-de-seconde.</p> <p>Il existe de nombreuses façons d'acquérir cette réalité terrain :</p> <ul style="list-style-type: none"> – manuellement : cette approche est minutieuse et peut introduire un certain biais, car deux personnes qui annotent la même séquence ne produiront pas exactement les mêmes données. Par conséquent, des règles d'annotation seront nécessaires afin de limiter ce biais. – Acquisitions semi-automatiques : Un algorithme d'analyse vidéo est utilisé pour produire un ensemble de données annotées initiales. Les résultats sont ensuite corrigés par un être humain et la réalité de terrain est construite sur la base de ces corrections. Cette démarche peut être utilisée uniquement quand la sortie de l'algorithme à évaluer est compatible avec la sortie de l'algorithme de référence. – Capteurs auxiliaires : les données des capteurs autres que les caméras vidéos sont utilisées (station SIREDO). Cette approche signifie que le système d'acquisition est complexe et nécessite la synchronisation et la référence spatiale et il est impossible d'automatiser l'annotation de toutes les propriétés. – Les autres moyens pour faciliter et accélérer le processus d'annotation sont résumés dans [31]. <p>Pour les besoins de l'état d'art des moyens d'annotation employés dans les systèmes déployés (calendrier, boîtes englobantes), une analyse des manuels d'utilisations s'impose.</p> <p>En conclusion, il n'y a pas de normes définissant le contenu et le format d'une réalité terrain. Pour utiliser des vérités de terrain produites par différents outils, une conversion de données est, par conséquent, nécessaire.</p>
Critères de performance	<p>Taux de vrais positifs : événements correctement détectés/nombre total d'évènements</p> <p>taux de faux négatifs : évènements non déclarés alors qu'ils existent/nombre total d'évènements</p> <p>taux de faux positifs : évènements détecté à tort /nombre total d'évènements</p> <p>taux de vrais négatifs : évènements non détectés à raison/nombre total d'évènements</p> <p>Rappel et précision</p> <p>Rappel = nombre d'évènements correctement détectés d'un type particulier/ nombre d'évènements de ce type</p> <p>précision = nombre d'évènements correctement détectés d'un type particulier/ nombre total d'évènements</p> <p>Courbes ROC croisant les variables Rappel et Précision</p>

Tableau 9 : Données d'entrées pour l'évaluation

Les critères de performances, cités dans le tableau 9, mettent l'accent uniquement sur le point de vue des utilisateurs. Ils ne permettent pas d'identifier les faiblesses des algorithmes en fonction de leurs conditions d'utilisation. Pour combler ce besoin, le programme de recherche ETISEO a été

lancé pour évaluer les algorithmes de traitement vidéo en se concentrant sur une tâche dans le procédé (par exemple, la détection et le suivi d'objet), en fonction du type de séquence (scène de route) et un obstacle général (présence des ombres). Les principes de base de la méthodologie élaborée dans ce programme sont récapitulés dans le tableau suivant :

Principes	Descriptions
Typologie des tâches (ou ontologies)	Les tâches correspondent aux principales tâches d'un système d'analyse vidéo : détection de l'objet, suivi de l'objet, classification de l'objet, reconnaissance de l'événement.
Typologie des problèmes	Les différents problèmes sont dûment définis, classés et sont traités séparément. Par exemple, le problème de l'ombre peut être divisé en plusieurs sous-problèmes : l'ombre avec différents niveaux d'intensité (peu ou fortement contrastée), l'ombre avec le même niveau d'intensité mais avec un autre fond en termes de couleurs et textures, l'ombres avec différentes sources de lumière en termes de position ou de longueur d'onde).
Compilation d'une base de données représentative des problèmes	Chaque séquence vidéo est spécifique à un problème. Il est préférable que les séquences compilées proviennent de plusieurs caméras différentes.
Annotation des séquences	Trois types de données sont collectées pour chaque séquence : <ul style="list-style-type: none"> - la réalité du terrain, y compris les annotations nécessaires pour les quatre tâches identifiées (boîtes englobantes sur les objets, le type d'objet, les événements). La réalité du terrain est produite à l'aide de l'outil VIPER (http://homepages.inf.ed.ac.uk/rbf/), - la difficulté particulière de la vidéo (présence d'une ombre légère), - les conditions d'acquisition (conditions météorologiques, vibrations de la caméra, etc.), - les paramètres d'étalonnage de la caméra et de la topologie de la scène.
Critères d'évaluation	ETISEO a défini différentes mesures pour évaluer chacune des tâches identifiées. Elles sont détaillées dans [31].
Analyse de la sensibilité des algorithmes	Outil de visualisation et d'évaluation ViSEvAI, disponible sous licence AGPL.

Tableau 10. Principes de base de la méthodologie d'évaluation des algorithmes

5 Conclusions et perspectives

Cette étude a mis en évidence la complexité des systèmes de vidéoprotection intelligente, qui reposent sur :

- des algorithmes d'analyse d'images, qui manquent encore de cadres d'évaluation de référence et dont les implémentations dans les produits commerciaux restent peu renseignées,
- des équipements (caméras, analyseurs, réseaux, ...) soumis à des fortes contraintes terrain et devant s'intégrer dans des environnements d'exploitation variés,
- une interface homme-machine sensible - la charge des opérateurs étant déjà déjà forte - sur laquelle repose toute la pertinence du dispositif mais insuffisamment prise en compte.

Si, pour certaines briques de ces systèmes, les travaux d'évaluation et de formalisation de l'évaluation sont déjà plus ou moins défrichés ou tout du moins initiés (transmission, algorithmie), d'autres demeurent encore à investiguer. Plus largement, cela limite directement la vision globale de la performance de la vidéoprotection intelligente appliquée au domaine routier.

Compte tenu des enjeux en termes d'investissements, déjà déployés ou à venir (nouveaux sites, renouvellements d'équipements), ainsi que des besoins de structuration de l'offre du marché, il apparaît pertinent de poursuivre l'exploration de cette thématique.

De nombreuses actions sont proposées dans ce rapport. Des états de l'art sur les différents outils et programmes de recherche doivent être menés au sein du MEDDE, afin de proposer les bases d'une méthodologie d'évaluation des systèmes de vidéoprotection intelligente. En complément, un programme de recherche pourrait permettre :

- la mise en place d'une vaste base de données,
- la définition des métriques pour évaluer les algorithmes d'analyse vidéo,
- la conception (ou l'adaptation) d'un outil d'évaluation de ces algorithmes, spécifique pour le flux du trafic.

Un tel outil facilitera la communication entre les différents acteurs : chercheurs, développeurs et utilisateurs finaux. En plus d'améliorer directement les dispositifs de vidéoprotection intelligente, cette démarche permettrait également de proposer un outillage adapté (formation, ...) à même d'améliorer l'acceptabilité auprès des utilisateurs finaux.

6 Références

1. Christophe Kolski, Houcine Ezzedine, Marie-Pierre Gervais, Kathia Marcal de Oliveira, Ahmed Seffah, Evaluation des SI, Besoins en méthodes et outils provenant de l'ergonomie et de l'IHM.
2. Nielsen J., Usability Engineering. Academic Press, Boston, 1993.
3. INHES, La vidéoprotection, Conditions d'efficacité et critères d'évaluation, Juillet 2008.
4. Christophe Kolski, Houcine Ezzedine, Conception et évaluation des IHM de supervision : éléments méthodologiques, Revue Génie Logiciel, 65, pp. 2-11, 2003.
5. Martial Grislin, Christophe Kolski, Evaluation des interfaces hommes-machine lors du développement des systèmes interactifs, Technique et Sciences Informatiques (TSI), 1996.
6. Ezzedine Houcine, Kolski Christophe, Démarche d'évaluation d'IHM dans les systèmes complexes, application à un poste de supervision du trafic ferroviaire, RIHM, vol. 5, num. 2, pp. 91-122.
7. Fauozi Moussa, Christophe Kolski, Meriem Riahi, Analyse des dysfonctionnements des systèmes complexes en amont de la conception des IHM : apports, difficultés et étude de cas, RIHM, volume 7, n.2, pp. 79-111.
8. Rania Bahloul, Mounir Ben Ayed, Adel M Alimi, Vers une méthode d'évaluation de Système Interactif d'aide à la décision basée sur le processus d'ECD, EvalECD, 2010.
9. F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, Capteurs intelligents : nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement, Maîtrise des risques et de Sûreté de fonctionnement, Lambda-Mu 16, Avignon, 2008.
10. Julie Beugin, Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé, thèse, 2006.
11. Jérémie Bossu, Détection Automatique d'Incidents (DAI) par analyse d'images en tunnel, document d'information, CETU, septembre 2013.
12. Cheng-Chang Lien and Ming-Hsiu Tsai, Real-Time Traffic Flow Analysis without Background Modeling, *Journal of Information Technology and Applications* Vol. 5, No. 1, pp. 1-14 2011
13. Brendan Morris and Mohan Trivedi, Real-Time Video based Highway Traffic Measurement and Performance Monitoring.
14. H. S. Mohana, Aswatha Kumar. M, G. Shivakumar, Vehicle Counting and classification using Kalman filter and pixel scanner technique and its verification with optical flow estimation, Global journal of computer science and technology, 2010.
15. Jian Wu, A survey on video-based vehicle behavior analysis algorithms, Journal of multimedia, 2012.
16. Erhan Bas, Road and Traffic Analysis from video, these, 2007.
17. Pablo Augusto Negri, Détection et reconnaissance d'objets structurés : application aux Transports Intelligents, thèse, 2008.
18. Neeraj Krantiveer Kanhere, Vision-based detection, tracking and classification of vehicles using stable features with automatic camera calibration, these, 2009.
19. Stopped Vehicle Detection System for Outdoor Traffic Surveillance, Gonçalo Monteiro, Joao Marcos, and Jorge Batista, Stopped Vehicle Detection System for Outdoor Traffic Surveillance.
20. CHUNG-CHENG CHIU, MIN-YU KU AND CHUN-YI WANG, Automatic Traffic Surveillance System for Vision-Based Vehicle Recognition and Tracking, JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, 611-629 (2010).
21. Jun-Wei Hsieh, Shih-Hao Yu, Yung-Sheng Chen, and Wen-Fong Hu, An Automatic Traffic Surveillance System for Vehicle Tracking and Classification, *IEEE*, Vol. 7, No. 2, 175-187, 2006.
22. P. Rajesh, M. Kalaiselvi Geetha and R. Ramu, Traffic density estimation, vehicle classification and stopped vehicle detection for traffic surveillance system using predefined traffic videos, *Elixir Comp. Sci. & Engg.* 56A (2013) 13671-13676
23. Luis Unzueta, Marcos Nieto, Andoni Cortés, Javier Barandiaran, Oihana Otaegui, and Pedro Sánchez, Adaptive Multicue Background Subtraction for Robust Vehicle Counting and Classification.
24. Violina Iordanova, Louahdi Khoudour, Pierre-Yves Tanniou, Thomas Durlin, Vidéoprotection intelligente sur les réseaux mobiles 3G appliquée au trafic routier, ATEC, 2014.
25. INHES, La vidéoprotection, Condition d'efficacité et critère d'évaluation, juillet 2008.
26. Neeraj K. Kanhere, Evaluation of a Computer-Vision Tracking System for Collecting Traffic Data, TRB Paper Number: 11-4162
27. Robert Lewis Graham, Jr., EVALUATION OF A COMPUTER VISION TRAFFIC

- SURVEILLANCE SYSTEM, A Thesis Presented to the Graduate School of Clemson University, December 2007.
28. Marché DAI-Réseaux, Tunnels routiers franciliens, ÎdF, Spécifications fonctionnelles Analyseur AVS400 FARECO, 25 octobre 2011.
 29. Catherine Barthe, NEAVIA, Test d'un système de comptage et de détection d'incident, ZELT, 2006.
 30. Catherine Barthe, Expérimentation du système de mesure de trafic NEAVIA sur la RN83 à Besançon, Rapport d'évaluation, ESAD-ZELT, 2011.
 31. Sous la direction de Jean-Yves Dufour, Outils d'analyse vidéo, pour une pleine exploitation des données de vidéoprotection, Lavoisier.
 32. Valérie Gouaillier, Aude-Emmanuelle Fleurant, La vidéosurveillance intelligente : promesses et défis, rapport de veille technologique et commerciale, mars 2009.
 33. IndigoVision, Détection vidéo intelligente – mythes et limites.
 34. Patrick Palmier, Evaluation des délais d'alerte suite à un accident dans le système ALLEGRO, rapport d'évaluation, ESAD, 2011