CETU

Guides

# DOSSIER PILOTE ÉQUIPEMENTS

## Fascicule : Détection automatique d'incidents par analyse d'images en tunnel routier


décembre 2025

Centre d'Études des Tunnels

www.cetu.developpement-durable.gouv.fr

MINISTÈRE DES TRANSPORTS

*Liberté*
*Égalité*
*Fraternité*

## LES GUIDES

Les guides sont l'aboutissement de travaux méthodologiques pilotés par le CETU. Ils ont pour but de servir de référence pour la conception, la réalisation ou l'exploitation des ouvrages souterrains. Quoique pertinent au moment de sa rédaction, tout guide peut devenir obsolète, notamment du fait des évolutions réglementaires ou techniques. Chaque utilisateur est responsable de sa juste application.
Ces documents sont téléchargeables sur le site Internet du CETU.

# *DOSSIER PILOTE ÉQUIPEMENTS*

*Fascicule :*
*Détection automatique d'incidents par analyse d'images en tunnel routier*

**décembre 2025**

**Centre d'Études des Tunnels**
25, avenue François Mitterrand
69500 BRON – France
Tél. 33 (0)1 40 81 30 30

cetu@developpement-durable.gouv.fr
www.cetu.developpement-durable.gouv.fr

# TABLE DES MATIÈRES

# ANNEXES

# 1 INTRODUCTION

## 1.1 CONTEXTE

Depuis une trentaine d'années, les tunnels routiers longs ou à trafic élevé sont équipés de systèmes de détection automatique d'incidents par analyse d'images (DAI). Un système de DAI assiste l'opérateur au Poste de Contrôle-Commande (PCC) dans ses missions de contrôle des ouvrages en l'informant de l'apparition d'un incident pouvant être à l'origine d'une situation potentiellement dangereuse pour les usagers.

L'opérateur peut alors déclencher le scénario d'intervention le mieux adapté dans les délais les plus brefs. La DAI par analyse d'images n'est pas le seul moyen permettant d'assurer la fonction de détection d'incidents et n'a pas vocation à se substituer aux opérateurs ni à tous les autres systèmes, mais elle constitue un moyen essentiel de détection dans les tunnels routiers surveillés en permanence.


*Figure 1 : Mur d'images du Poste de Contrôle Commande du Centre d'Ingénierie de Sécurité et de Gestion du Trafic de Moulin-les-Metz*

## 1.2 ENJEUX

La DAI par analyse d'images tient une place très importante dans l'aide à l'exploitation des tunnels routiers et de très nombreux ouvrages en sont aujourd'hui dotés. Cet équipement concourt aux fonctions « détecter » et « qualifier » un incident au sens de la note d'information n°23 du CETU[1]. Si elle n'est pas le seul moyen permettant d'assurer la fonction de détection, elle demeure un équipement important, car il peut permettre de gagner du temps dans des situations où la rapidité de réaction est cruciale pour la sécurité des usagers.

Les retours d'expérience montrent que la vidéosurveillance couplée à un système de DAI est le premier moyen de détection des incidents significatifs. Suivant les années, entre 40 et 60 % des incidents sont détectés avec cet équipement.[2]

Compte tenu des enjeux reposant sur ce système, il doit être conçu avec soin et faire l'objet d'un réglage judicieux afin de demeurer fiable dans le temps et constituer un outil de confiance pour l'exploitant.

En effet, un système de DAI mal conçu ou mal réglé est susceptible de remonter un trop grand nombre de fausses alarmes, ce qui est une source de perturbations pour les opérateurs. Inversement, un système mal conçu ou mal réglé peut ne pas détecter un incident avéré, tarder à le faire, ou mal le qualifier, ce qui décrédibilise le système et réduit la confiance que les opérateurs peuvent avoir en lui.

Par ailleurs, les tests de DAI réalisés entre 2011 et 2023 par le CETU sur plus de 40 ouvrages, à l'occasion d'inspections détaillées, ont montré un écart non négligeable entre les performances constatées et celles attendues, mettant ainsi en évidence l'attention à porter à ce système pour qu'il livre ses meilleures performances.

## 1.3 OBJECTIFS DU DOCUMENT

Ce guide propose des recommandations pour la conception, l'installation, la validation et la maintenance des systèmes de DAI en tunnel routier afin d'aider à en assurer la performance dans le temps. Il annule et remplace le document d'information publié en 2015.

Son élaboration s'est appuyée sur des échanges avec des maîtres d'ouvrages, maîtres d'œuvre, exploitants, fabricants et intégrateurs. Les évolutions par rapport au document de 2015 portent sur les nouvelles technologies de capteurs (caméras thermiques) et systèmes d'analyse, les architectures réseau, ainsi que la cybersécurité. Certains chapitres ont été largement complétés, comme celui traitant des phases de conception et d'installation ou celui relatif à la phase d'exploitation de l'ouvrage. Des évolutions de doctrine ont en outre été apportées, en particulier en ce qui concerne la classification des incidents qui a été complétée et dotée d'une nouvelle terminologie. Enfin, de nouveaux indicateurs sont proposés pour qualifier la performance globale du système.

Organisé en sept chapitres, ce document définit dans un premier temps les incidents à détecter, puis décrit les équipements de DAI et ses modes de fonctionnement. Il donne également des éléments sur les performances attendues et sur des principes généraux de cybersécurité et de sûreté de fonctionnement. La conception, l'installation et les tests de validation des performances du système sont ensuite abordés. Pour finir, la dernière partie est consacrée aux opérations à réaliser durant la vie de l'ouvrage, qui sont primordiales pour maintenir le bon fonctionnement et le meilleur niveau de confiance en ce système.

1. Note d'information n°23, *Définition des fonctions de sécurité – Application aux modes d'exploitation dégradée et aux conditions minimales d'exploitation*.
2. Source : base de données pannes/accidents du CETU – Rex 2014-2020.

2

# ÉLÉMENTS RÉGLEMENTAIRES

## 2.1 VIDÉOPROTECTION DES ESPACES PUBLICS

L'utilisation de la vidéoprotection est principalement régie par les articles 17 à 25 de la section IV de la Loi n°2011-167 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI 2).

La loi ne se prononce pas sur la technologie utilisée mais définit seulement les principales modalités de fonctionnement des systèmes et fixe des normes techniques (par arrêté du 3 août 2007 mis à jour le 16 mars 2011 – annexes techniques publiées au Journal Officiel du 25 août 2007) qui portent d'une part sur les caméras et sur les systèmes de transmission et de stockage, et d'autre part sur l'interopérabilité des systèmes de stockage et d'exportation des données vers les forces de police et de gendarmerie.

Les dispositions de la LOPPSI 2 ont été transposées dans le Code de la Sécurité Intérieure (CSI). Le document de la Commission Nationale de l'Informatique et des Libertés (CNIL) du 18 novembre 2024 intitulé *La vidéoprotection classique* synthétise les textes applicables et rappelle les règles à respecter[3].

La vidéoprotection en tunnels routiers, au titre de la prévention des risques, la sécurité des personnes et la gestion des flux, est encadrée par les articles L.223-1 à L.223-9 et R.223-1 à R.223-2 du CSI. Ces articles mentionnent notamment :

- l'installation requiert une autorisation préfectorale après dépôt d'un dossier technique incluant, si nécessaire, une Analyse d'Impact sur la Protection des Données (AIPD) ;
- les données collectées se limitent aux images utiles pour la détection des incidents (excluant sons et reconnaissance faciale), avec une conservation maximale d'un mois ;
- l'accès aux images est strictement réservé aux agents habilités ;
- les personnes filmées doivent être informées par affichage ;
- les droits d'accès aux données sont encadrés avec des restrictions possibles pour la sécurité publique.

Les administrations, sociétés et associations traitant des données à caractère personnel, mais aussi leurs prestataires et sous-traitants, sont désormais pleinement responsables de la protection des données qu'ils traitent.

Il leur appartient d'assurer la conformité au Règlement Général sur la Protection des Données (RGPD – 25 mai 2018) de leurs traitements de données personnelles tout au long de leur cycle de vie et d'être en mesure de démontrer cette conformité.

En particulier, la CNIL précise que « les modèles d'IA peuvent relever du RGPD s'ils mémorisent des données personnelles issues de leur entraînement. La CNIL propose une méthode à destination des fournisseurs pour évaluer si leurs modèles sont soumis au RGPD ou non »[4]. Les fournisseurs de DAI doivent donc s'assurer qu'ils respectent ces règles.

## 2.2 DÉTECTION AUTOMATIQUE D'INCIDENTS EN TUNNEL ROUTIER

Dans le cas où une surveillance humaine est assurée, l'Instruction Technique (IT) relative aux dispositions de sécurité dans les nouveaux tunnels du réseau routier national, figurant en annexe 2 de la circulaire 2000-63 du 25 août 2000, impose l'installation d'un réseau de vidéosurveillance ainsi qu'un système de détection automatique d'incidents. En effet, le paragraphe 3.9 de l'IT 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 (degrés D3 ou D4 de permanence et surveillance…). En cas d'alarme susceptible d'être la conséquence d'un incident ou accident, les images télévisées montrant la zone d'où provient l'alarme doivent être enregistrées automatiquement de façon à permettre l'analyse ultérieure de l'incident ou de l'accident éventuel. Il s'agit d'une prescription minimale : un système comportant un enregistrement systématique de toutes les images et leur conservation pendant quelques minutes en temps normal et pendant une durée indéfinie en cas d'alarme offre bien sûr de meilleures possibilités d'analyse ultérieure…* ».

3. Source : *Vidéoprotection « classique » – Synthèse des références juridiques applicables*, 18 novembre 2024, document de la Commission Nationale de l'Informatique et des Libertés (CNIL).
4. Source : *IA : analyser le statut d'un modèle d'IA au regard du RGPD*, 22 juillet 2025, document de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Les tunnels pour lesquels l'IT impose un système permettant de détecter les incidents doivent donc être aussi équipés d'un système de vidéosurveillance. Cette détection d'incident est par conséquent généralement réalisée par une analyse des images issues des caméras de vidéosurveillance.

L'IT ne précise pas le type d'incident que doit détecter le système de DAI.

Des exigences similaires sont imposées par l'arrêté du 9 novembre 2007 modifiant l'arrêté du 8 novembre 2006 et fixant les exigences de sécurité minimales applicables aux tunnels de plus de 500 mètres du réseau transeuropéen.

Les tunnels répondant à ce critère doivent satisfaire aux exigences de sécurité minimales prévues à l'alinéa m de l'article 2 qui indique :

« *Des systèmes de vidéosurveillance et un système capable de détecter automatiquement les incidents de la circulation ou les incendies sont installés dans tous les tunnels équipés d'un poste de contrôle-commande.*
*Des systèmes de détection automatique des incendies sont installés dans tous les tunnels ne disposant pas d'un poste de contrôle-commande, lorsque la mise en œuvre de la ventilation mécanique pour la maîtrise des fumées est différente de la mise en œuvre automatique de la ventilation pour la maîtrise des polluants* ».

## 2.3 CYBERSÉCURITÉ

Les systèmes de vidéosurveillance et la DAI font partie des systèmes d'information particulièrement sensibles aux enjeux de cybersécurité.

Le cadre réglementaire national et européen s'appliquant à la sécurité de l'information est constitué de l'ensemble des directives européennes, textes de lois et décrets depuis plusieurs décennies. Parmi ces textes, citons notamment la Loi Informatique et Libertés (LIL)[5], les Lois de Programmation Militaire (LPM) 2014-2019 et 2024-2030, la directive *Network and Information Security* (NIS), et le Règlement Général de Protection des Données européen UE 2016/679 (RGPD).

Par ailleurs, la série des normes ISO 27000, en particulier la norme NF EN ISO/IEC 27001:2023[6], contient les exigences relatives à la certification d'un Système de Management de la Sécurité de l'Information (SMSI).

En application de ces textes, le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le service informatique de l'établissement édictent une Politique de Sécurité des Systèmes d'Information (PSSI) comportant un volet spécifiquement adapté aux systèmes métiers opérationnels. La Procédure d'Exploitation et de Sécurité (PES) doit être établie pour le système de DAI dans le respect de la PSSI.

5. Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
6. NF EN ISO/IEC 27001:2023 Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences.

# 3 INCIDENTS À DÉTECTER

## 3.1 DÉFINITION D'UN INCIDENT

Le terme **incident** caractérise un événement anormal et imprévu présentant un effet défavorable sur l'exploitation et la sécurité d'un tunnel[7].

Il est primordial pour un exploitant de détecter les situations anormales le plus tôt possible afin de pouvoir réagir très rapidement.

Dans un tunnel peuvent se produire des incidents présentant des risques directs élevés, comme les accidents ou les incendies, et d'autres qui peuvent être précurseurs d'événements plus graves. Dans cette seconde catégorie, se trouvent par exemple les ralentissements, les arrêts de véhicules en chaussée, ou encore la présence de piétons dans les tunnels qui leur sont interdits.

La détection d'un incident peut être soit directe soit indirecte. Dans le premier cas, l'incident lui-même est détecté. Dans le second cas, ce sont les conséquences de l'incident sur la circulation qui sont détectées.

## 3.2 CLASSIFICATION ET CHOIX DES INCIDENTS À DÉTECTER

La réglementation ne précise pas parmi les incidents pouvant survenir en tunnel, de types très variés, ceux qu'il convient de détecter.

Ce chapitre propose donc une liste des types d'incidents à détecter.

Chaque exploitant souhaite naturellement pouvoir détecter le maximum d'incidents. Toutefois, même si les capacités de détection d'une DAI sont en constante progression, plus le nombre d'incidents à détecter est important, plus le système est difficile à paramétrer et ses performances susceptibles d'être dégradées. Dans certains cas, souvent liés à une maintenance préventive insuffisante, la dégradation est telle qu'elle peut conduire les opérateurs à être submergés de fausses alarmes, avec le risque d'un discrédit du système de DAI. Il convient donc de procéder à une sélection judicieuse du type d'incidents à détecter.

Pour cela, une liste des incidents les plus courants a été établie. Elle est **hiérarchisée en trois niveaux** : du niveau 1 (estimé prioritaire) au niveau 3 (détection intéressante mais pas primordiale). Bien évidemment, ces différents niveaux peuvent être modulés en fonction des caractéristiques de l'ouvrage et de son environnement, de son type d'exploitation et du service attendu.

La priorisation des types d'incidents peut être effectuée en fonction :

- de leur gravité et de leur occurrence ;
- de la capacité du système à pouvoir les détecter ;
- de l'existence ou non d'un moyen d'action en réponse à leur survenance.

Le tableau 1 ci-après présente cette hiérarchisation des incidents les plus courants (leur description détaillée est donnée en annexe A). Ce tableau peut être complété, au regard des risques spécifiques à chaque ouvrage, par d'autres types d'incidents à définir au cas pas cas.

| Niveau de l'incident | Incident |
|---|---|
| 1 | Véhicule arrêté |
| | Incendie[8] |
| 2 | Congestion[9] |
| | Véhicule arrêté en situation de congestion |
| | Véhicule en contre-sens |
| | Piétons |
| 3 | Objet |
| | Véhicule lent |

7. Définition de l'Association Mondiale de la Route (PIARC).
8. Le système peut détecter soit une perte de visibilité (fumée), soit la présence d'une flamme.
9. Congestion : phénomène qui survient lorsque la demande est supérieure à la capacité de cette infrastructure (source : *Comprendre le trafic routier – Méthodes et calculs*, 2010, Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques, CERTU).

Un véhicule arrêté et un incendie[10] sont les deux incidents à détecter systématiquement dans l'ensemble de l'ouvrage.

Pour les autres incidents, il convient de réaliser une analyse pour déterminer s'ils doivent être détectés et, dans cette hypothèse, les zones de l'ouvrage dans lesquelles ils doivent l'être.

Il est possible de s'appuyer sur les éléments suivants pour mener cette analyse :

- il faut éviter autant que possible d'effectuer de la détection de fumée et d'objet à partir des caméras situées en tête d'ouvrage car cela peut conduire dans certains cas à une dégradation des performances du système ;
- la détection de contresens peut être pertinente pour les tunnels de longueur supérieure à 1 km ou situés sur des itinéraires équipés de moyens d'action ;
- en cas de détection de piétons, il peut s'avérer pertinent, outre une détection en tête, de prolonger celle-ci à l'intérieur de l'ouvrage pour les piétons provenant de « dépose-minutes » sauvages ou d'intrusion par des accès divers (issues, bretelles…) ;
- la détection d'objets en tunnel n'est pertinente que si le trafic est faible. En effet, pour des tunnels à trafic élevé, il est fort probable que l'objet ait causé un autre incident lui-même détectable ou ait été déplacé par un véhicule avant qu'une mesure n'ait pu être prise par le Poste de Contrôle Commande (PCC). Enfin, les retours d'expérience auprès d'exploitants démontrent que ce type de détection peut être générateur de fausses alarmes récurrentes. Il est donc conseillé de ne le prévoir que dans des cas bien particuliers et après une analyse fine des objectifs visés ;
- la détection des véhicules lents est plus rarement demandée. Elle peut par exemple s'avérer utile dans les tunnels où la vitesse minimale des véhicules constitue un enjeu particulier (cas des grands ouvrages transfrontaliers…).

Ainsi, selon le type d'ouvrage et son contexte, il est possible de retenir un ou plusieurs types d'incidents de chaque niveau.

10. L'ancienne désignation « Apparition de fumées » qui figurait dans le document d'information de 2015 a été remplacée par « Incendie », qui peut être détecté soit par une perte de visibilité soit par des fonctionnalités de détection de flamme offertes aujourd'hui par les caméras thermiques.

4

# ÉQUIPEMENTS DE DAI

La fonction DAI par analyse d'images repose sur un système de captation de la scène généralement issu des caméras de vidéo-protection du tunnel, qui requiert des caractéristiques particulières. Le flux vidéo généré est analysé par un logiciel dédié qui fait appel à plusieurs types d'algorithmes. Lorsqu'un incident est identifié par ce système, une alarme est générée et transmise à l'opérateur.

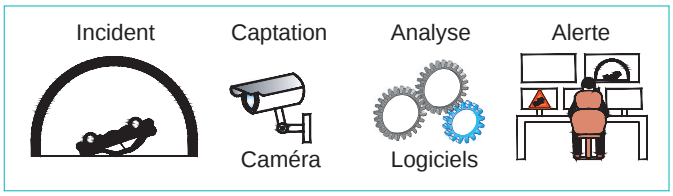



*Figure 2 : Synoptique d'une DAI*

## 4.1 LES CAMÉRAS

Une DAI par analyse d'images utilise les images captées par une caméra généralement fixe.

On entend par caméra l'ensemble comprenant le capteur, l'objectif, le caisson et son système de fixation.

L'image obtenue dépend des caractéristiques du capteur de la caméra.

Deux types de caméras sont utilisés : **les caméras classiques**, sensibles à la lumière visible, et **les caméras thermiques**, sensibles au rayonnement infrarouge (voir encadré ci-contre). Chaque technologie présente des avantages et inconvénients.

Quelques systèmes avec caméras analogiques existent encore, mais ils sont en fin de vie par manque de matériel de rechange et sont voués à évoluer vers les technologies numériques « caméras IP » (Internet Protocol).

### Caractéristiques des capteurs

***Spectre électromagnétique***

Suivant le type de caméra, la plage de fonctionnement peut se situer sur des longueurs d'onde différentes du spectre électromagnétique. Le spectre électromagnétique est défini comme le classement des rayons électromagnétiques par longueur d'onde (de zéro à l'infini) dans le vide. Il est divisé en plusieurs classes, dans lesquelles le rayonnement s'étudie par des moyens particuliers. Une représentation de ce spectre est présentée en figure 3.

***Résolution***

La résolution du capteur correspond au nombre de pixels total.

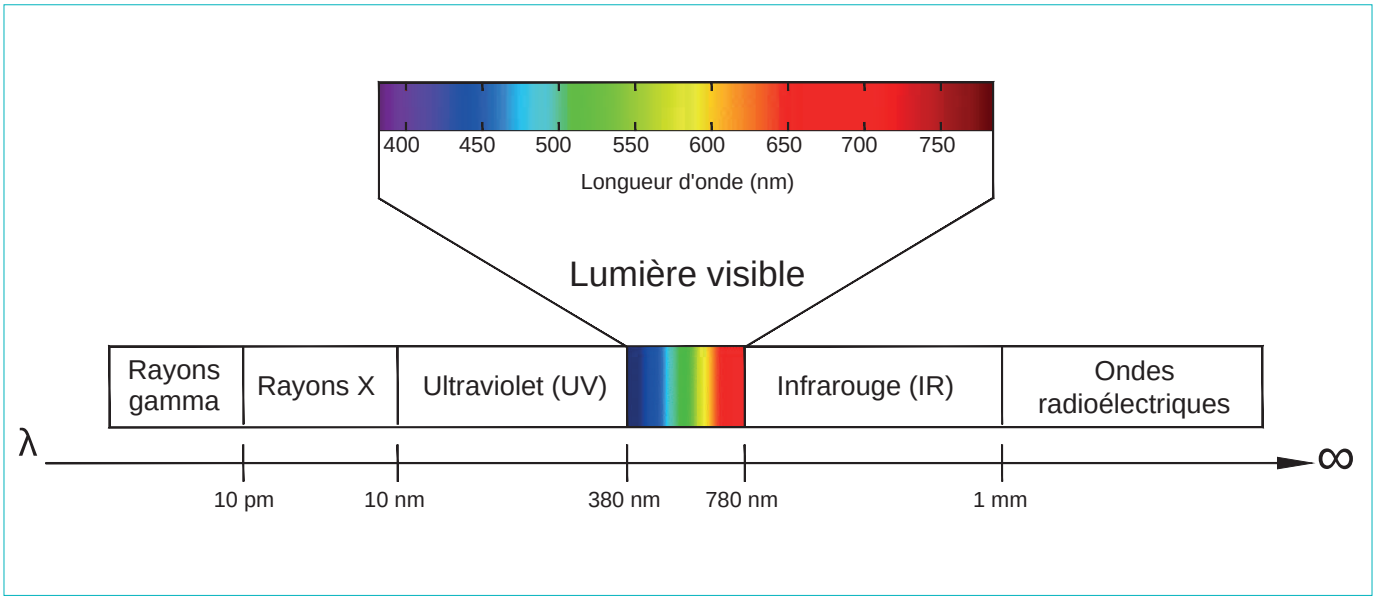



*Figure 3 : Représentation du spectre électromagnétique (© Cerema DTecITM)*

## 4.1.1 Caméras classiques

Les caméras classiques utilisent un capteur électronique photosensible (utilisation de photodiodes, technologie Complementary Metal Oxyde Semiconductor CMOS) fonctionnant sur le phénomène de la réflexion. Il permet la conversion d'un rayonnement électromagnétique en un signal électrique.

Ce capteur, en fonction de son utilisation, peut travailler dans les classes de longueurs d'ondes suivantes :

- ultraviolet (10-380 nm), qui ne présente aucun intérêt pour de la DAI ;
- visible (380-780 nm) ;
- infrarouge proche (700-1 500 nm), *near infrared*, NIR sur la figure 4.

Les caméras travaillant dans la classe des longueurs d'ondes visibles sont très utilisées dans les tunnels.

Les avantages liés à cette technologie sont les suivants :

- retour visuel immédiat en vraies couleurs de l'incident (confort pour l'opérateur) ;
- résolution du capteur pouvant atteindre 4k, ce qui est très utile pour la qualification de l'incident ;
- détection de fumée possible ;
- prix inférieur à celui d'un système doté d'une technologie thermique.

Les inconvénients liés aux caméras travaillant dans la classe des longueurs d'ondes visibles sont les suivants :

- sensibilité aux facteurs météorologiques tels que la pluie ou le brouillard ;
- sensibilité aux variations de luminosité et aux conditions de visibilité comme l'éblouissement en tête d'ouvrage ; utilisation impossible dans le noir (hormis les caméras jour/nuit) ou dans un tunnel enfumé ;
- sensibilité à la projection d'ombres ;
- sensibilité aux défauts intrinsèques et extrinsèques de la caméra (reflets sur son objectif par exemple).

Les caméras travaillant dans le proche infrarouge ne sont actuellement pas utilisées pour la DAI en tunnel.

Leurs caractéristiques et usages possibles sont décrits en annexe B.

## 4.1.2 Caméras thermiques

Les caméras thermiques, généralement mises en œuvre en tunnel, utilisent un capteur de type micro-bolomètre sensible aux rayonnements infrarouges compris entre 7,5 et 14 µm.

Ce capteur permet d'observer une image qui correspond aux gradients thermiques présents dans la scène observée. Il travaille à l'intérieur des longueurs d'ondes LWIR (7-15 µm).

Ces caméras peuvent produire des images soit en fausses couleurs, soit en noir et blanc.

Bandes spectrales de l'infrarouge ;

- NIR, *near infrared* : infrarouge proche ;
- SWIR, *short wave infrared* : infrarouge de courte longueur d'onde ;
- MWIR, *medium wave infrared* : infrarouge moyen ;
- (V)LWIR, *(very) long wave infrared* : infrarouge de (très) grande longueur d'onde.

Ces bandes sont représentées dans la figure 4.

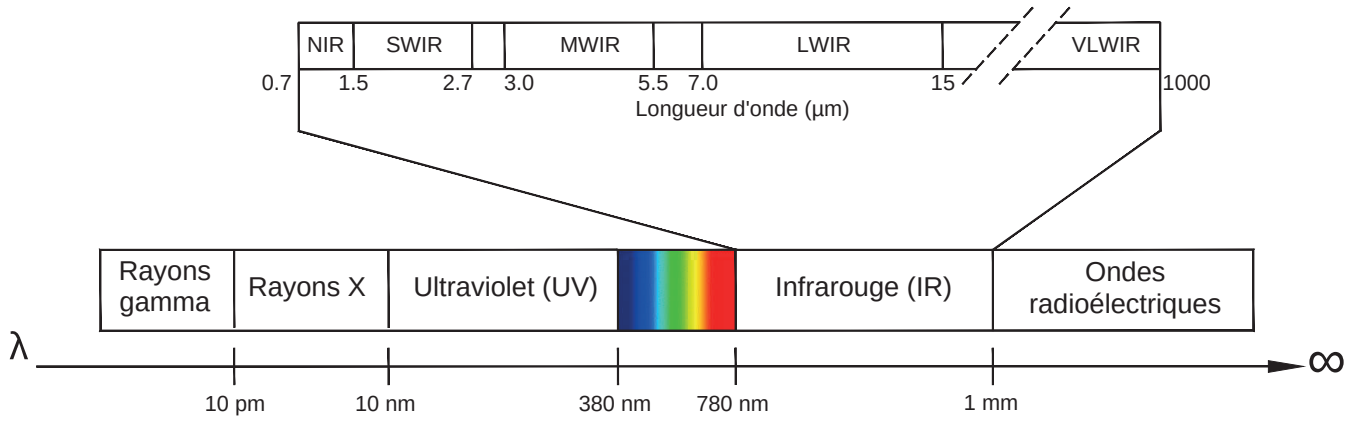



*Figure 4 : Les différentes bandes de fréquences dans l'infrarouge (© Cerema DTecITM)*

Cette technologie étant peu sensible aux variations de luminosité et de conditions de visibilité, ses principaux avantages sont les suivants :

- faible sensibilité aux facteurs météorologiques comme le brouillard ;
- non sensibilité aux reflets des phares et aux réflexions lumineuses sur chaussée humide ;
- détection possible d'objets à travers la fumée (en fonction de la sensibilité de la caméra) ;
- faible sensibilité aux projections d'ombres (surtout en tunnel) ;
- détection de flamme possible (en fonction des longueurs d'ondes utilisées par la caméra).

Les inconvénients liés à ce type de technologie sont les suivants :

- non adaptée à la surveillance du trafic et au contrôle visuel des incidents par l'opérateur[11] ;
- non adaptée à la détection des corps ayant un rayonnement proche de celui de l'environnement de l'ouvrage comme les fumées froides ou les objets qui ne dégagent pas de chaleur ;
- capacité de résolution du capteur actuellement moindre que celle des capteurs utilisés en technologie classique ;
- prix supérieur à celui des caméras classiques.

### Transformation globale

Dans un système de DAI par analyse d'images, les incidents à détecter ne s'analysent pas sur un volume mais sur une surface de projection.

L'action de transformation globale consiste en une projection en perspective qui transforme un point de l'espace à trois dimensions, en un point de l'image à deux dimensions.

Cette projection est très dépendante des paramètres du système optique (caméra positionnée et orientée dans son environnement) qui sont de deux ordres :

- paramètres correspondant aux caractéristiques propres de la caméra (taille du capteur, résolution du capteur, focale de l'objectif, distorsion optique…) ;
- paramètres dépendants de la position et de l'orientation de la caméra dans le tunnel (implantation, inclinaison et azimut) directement liés à la géométrie du tunnel (nombre de voies, courbes, gabarit).

Ces différents paramètres impactent **la définition** de l'image, c'est-à-dire le rapport pixels par mètre (plus petite partie d'une image discrétisée).

## 4.1.3 Couverture et implantation

Les paramètres du système optique (voir encadré *Transformation globale* ci-contre) sont à prendre en compte pour réaliser la couverture DAI souhaitée dans le tunnel.

En effet, selon sa position, son inclinaison et la focale utilisée (généralement 8 mm ou 16 mm), une caméra peut couvrir une plus ou moins grande partie du tunnel en ligne droite (allant de 60 à 100 mètres) ; mais avec l'inconvénient que plus la zone étudiée est éloignée de la caméra, plus le rapport pixels/mètre est faible.

L'image obtenue par la caméra est généralement divisée en trois parties dans le sens de la hauteur (voir figure 5 ci-après) :

- la première moitié de l'image, avec la meilleure définition, représente le début de champ ;
- les deux tiers de la deuxième moitié, de définition moyenne, représentent le milieu de champ ;
- le tiers restant de la deuxième moitié, de basse définition, représente la fin de champ.

Dans la fin de champ, l'image des objets étant de moins bonne qualité, il est possible que les performances de détection du système de DAI soient dégradées.

Un **recouvrement** entre caméras est nécessaire pour permettre au système de détecter en tout point de la chaussée les incidents demandés. Cela s'applique également aux bandes dérasées, bandes d'arrêts d'urgence et trottoirs s'ils existent.

Une **étude préalable d'implantation** des caméras est indispensable afin de s'assurer de la couverture souhaitée (cf. paragraphe 8.1 – Études de conception). On remarque que la mise au point d'un système de DAI conduit souvent à augmenter le nombre de caméras par rapport à celui requis pour les seuls besoins de la vidéosurveillance. Bien évidemment, plus l'ouvrage présente une géométrie compliquée (courbes, déclivités...), plus le positionnement des caméras est complexe et plus leur nombre doit augmenter.

L'étude d'implantation doit prendre en compte, également, les effets des différentes perturbations décrites au paragraphe 4.3 – Dispositions particulières.

Lorsque le gabarit le permet, il convient de privilégier un positionnement des caméras dans l'axe central du tunnel, pour éviter les problèmes de masquage par les poids lourds.

11. Ce type de caméra peut très bien compléter un système de surveillance mais peut difficilement le remplacer. En effet, les caméras classiques sont généralement nécessaires pour que l'opérateur puisse visualiser et analyser les événements.

## 4.2 L'ANALYSEUR DAI

L'analyseur DAI est l'outil qui traite les images captées dans le tunnel. Il peut être intégré à la caméra, ou déporté et mutualisé pour plusieurs caméras. Ses analyses reposent sur des algorithmes.

### 4.2.1 Les algorithmes d'analyse d'images

Une DAI par analyse d'images vise à reproduire la surveillance visuelle que ferait un opérateur pour identifier un incident dans le tunnel.

Pour cela, les fabricants combinent plusieurs types d'algorithmes. Les premiers algorithmes – appelés algorithmes « historiques » dans la suite du document, qui ont été utilisés et qui sont encore utilisés de nos jours – sont ceux de type « *background extraction* » (également appelé « *foreground / background algorithm* »), « *tripwire* » et « *tracking* ». Ces algorithmes permettent de qualifier les déplacements dans l'ouvrage et de détecter des situations anormales synonymes d'incidents (véhicule arrêté, contre-sens…).

La méthode **« *background extraction* »** consiste à mémoriser comme référence la partie figée de la scène (« *background* ») et à analyser les changements dans l'image qui pourraient être interprétés comme un incident.

La méthode **« *tripwire* »** consiste à définir un zonage précis dans l'image, chacune des zones étant limitée par des lignes transversales et longitudinales. La mesure de la vitesse de la variation de luminosité sur les lignes est alors interprétée comme le passage d'un véhicule. Cette mesure permet de calculer une vitesse moyenne et de déterminer un sens de circulation.

La méthode **« *tracking* »** repose sur la reconnaissance de forme et le suivi d'objets. L'analyse de la taille de l'objet, de son sens de déplacement ainsi que de sa vitesse, permet de différencier les éléments présents sur l'image.

Plus récemment, avec le développement des systèmes de transports intelligents (STI), de nouvelles méthodes d'extraction d'images de personnes ou d'objets dans des séquences vidéo ont été développées. Elles sont basées sur l'intelligence artificielle[12] (IA) et plus particulièrement sur l'utilisation de l'apprentissage profond (« *deep learning* »).

La méthode **« *deep learning* »** fait appel à des techniques de réseaux de neurones artificiels. Afin de bien fonctionner, ces réseaux doivent apprendre à reconnaître une grande quantité d'objets présents dans les scènes étudiées. La puissance de ces algorithmes dépend fortement du nombre de neurones par couche, du nombre de couches de neurones artificiels utilisés ainsi que du volume et de la qualité de la base de données[13].

Il est possible de combiner ces différentes méthodes pour améliorer la robustesse du système.

Des algorithmes complémentaires sont également mis en œuvre afin de traiter les perturbations décrites au paragraphe 4.3 – Dispositions particulières.

### 4.2.2 Notion de masque

Quel que soit le principe de fonctionnement retenu, l'image issue d'une caméra est décomposée en plusieurs zones d'analyse appelées masques.

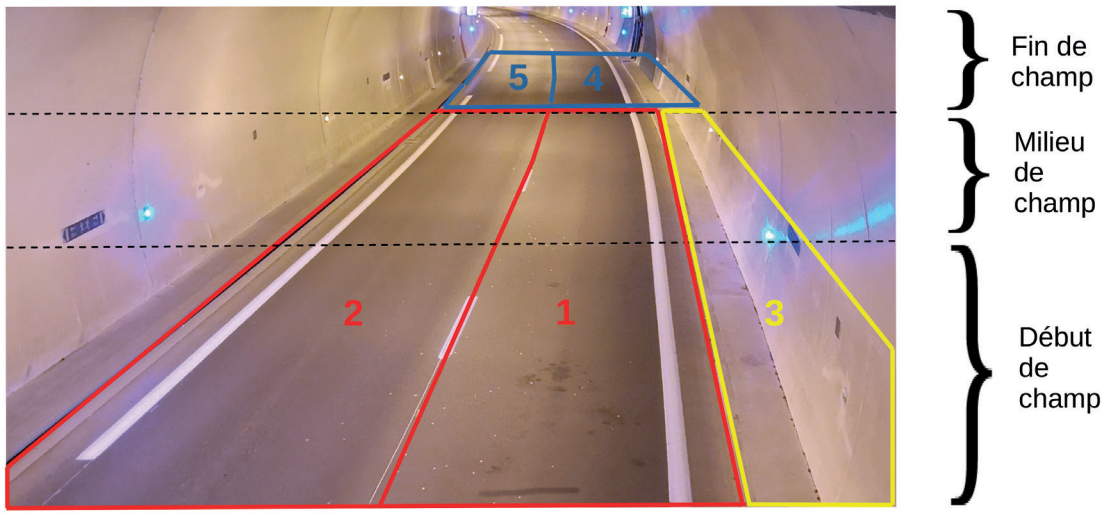



*Figure 5 : Exemple de représentation des masques et des différents champs*

12. L'IA est un champ de recherche qui regroupe l'ensemble des techniques et méthodes qui tendent à comprendre et reproduire le fonctionnement d'un cerveau humain. Le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établit des règles harmonisées concernant l'intelligence artificielle.
13. Les performances du système sont directement liées à la cohérence du jeu de données utilisé qui doit être adapté aux incidents à détecter dans l'ouvrage.

Le but principal du masque est de pouvoir relier l'incident détecté aux différentes zones de trafic du tunnel (voies, sens, trottoir, BAU, garage...). Par extension, il permet également de définir des zones d'intérêt en fonction des types d'incidents qui peuvent s'y produire, avec des règles de détection qui leur sont propres.

La figure 5 montre un exemple de décomposition d'image en masques. Les masques 1 et 2 correspondent à la chaussée. Il peut y avoir autant de masques que de voies : le masque 1 correspond à la voie lente y compris la bande dérasée, et le masque 2 à la voie rapide. Dans ces zones, l'objectif est de détecter des incidents relatifs à la circulation de véhicules et éventuellement de piétons, ou la présence d'objets.

Le masque 3 correspond au trottoir où l'on cherche généralement à détecter la présence de piétons et éventuellement d'objets.

Les masques 4 et 5 correspondent à la zone la plus éloignée de la caméra dans laquelle le rapport pixels/mètre est faible, comme expliqué au paragraphe 4.1.3 – Couverture et implantation. Il est ainsi préférable de réaliser les détections d'incidents survenant dans cette zone avec la caméra suivante, pour laquelle ils se retrouveront en début de champ.

Enfin, s'il est tentant d'augmenter le nombre de masques pour affecter à chacun des fonctionnalités ciblées, il faut savoir que plus ce nombre augmente, plus le système d'analyse devient complexe et peut induire soit une dégradation de la qualité de détection, soit une augmentation du nombre de fausses alarmes.

Il est à noter que l'usage des masques a évolué depuis les algorithmes historiques. En effet, les algorithmes maintenant basés sur la méthode « *deep learning* » détectent les incidents sur la totalité de l'image et utilisent cette notion de masque pour simplement caractériser l'emplacement de l'incident détecté.

## 4.3 DISPOSITIONS PARTICULIÈRES

En tunnel routier, les éléments constitutifs des systèmes de DAI sont soumis à des contraintes propres à cet environnement particulier. Ces contraintes peuvent aussi bien provoquer des dommages sur le matériel qu'une dégradation de la qualité de captation. Des dispositions particulières doivent donc être prises en conséquence.

### 4.3.1 Protection des matériels

Les caméras sont soumises à de nombreuses contraintes (hygrométrie, pollution, vibration, salissures, variation de température…).

C'est pourquoi elles sont généralement placées dans un caisson chauffé vitré, étanche, et résistant à la corrosion, lui-même fixé sur un support dont l'orientation est réglable. Ce système doit être suffisamment robuste dans le temps pour assurer la stabilité et le bon fonctionnement des caméras.

Suivant l'environnement (proximité des ventilateurs par exemple), il peut être également intéressant de prévoir un système de stabilisation des images.

### 4.3.2 Adaptation aux perturbations extérieures

Les capteurs optiques sont soumis à plusieurs types de perturbations, qui peuvent être à l'origine de fausses alarmes ou de non-détections. Les principales perturbations en tunnel sont les suivantes :

- l'occultation optique : ce phénomène se produit lorsqu'un véhicule en cache partiellement ou totalement un autre. Un mauvais positionnement de la caméra peut amplifier ce phénomène (exemple des caméras installées en piédroit dans un tunnel bidirectionnel). Ce problème peut être évité par une étude d'implantation rigoureuse ;
- les intempéries : le ruissellement des eaux pluviales ou le brouillard peuvent pénétrer à l'intérieur du tunnel et perturber les fonctions d'analyse ;
- les niveaux d'éclairement : des variations rapides des niveaux d'éclairement peuvent, suivant la sensibilité du capteur, fausser l'analyse, notamment :
  - en situation de pénétration du soleil dans les zones d'entrée du tunnel,
  - lors des changements de régime de l'éclairage de renforcement ou de base,
  - en situation d'éclairage non homogène créant une alternance de zones sombres et claires,
  - en cas d'éclairage insuffisant, c'est-à-dire n'offrant pas un contraste suffisant entre un objet à détecter et son environnement.

Les nouvelles générations de caméras permettent de s'affranchir efficacement de certaines de ces perturbations (voir avantages et inconvénients des différentes technologies au paragraphe 4.1 – Les caméras).

La détection doit aussi être garantie quelles que soient les conditions d'éclairage. Les informations de changement de régime de l'éclairage doivent ainsi être transmises au système de DAI par la Gestion Technique Centralisée (GTC), afin qu'il s'adapte en temps réel aux nouvelles conditions, sans dégradation de ses performances.

## 4.4 ARCHITECTURES

Un système de vidéosurveillance possède trois fonctions :

- l'acquisition,
- la gestion,
- la visualisation.

Le système de DAI vient compléter ces fonctions par une analyse d'images et une alerte à l'opérateur. Le schéma ci-dessous présente les matériels associés aux fonctions. Dans les faits plusieurs fonctions peuvent être regroupées dans un même matériel. En particulier, grâce à la technique de virtualisation, plusieurs serveurs virtuels peuvent être regroupés dans un même serveur physique.

Les systèmes de vidéosurveillance sont aujourd'hui dotés de caméras numériques, qui ont remplacé celles de type analogique (voir 4.1 – Les caméras).

Elles sont raccordées au réseau fédérateur[14] du tunnel. Ce réseau est pour cela généralement organisé en réseaux locaux virtuels ou *Virtual Local Area Networks* (VLAN)[15].

La pluralité des matériels présents dans un système de DAI par vidéosurveillance, associée à la variété des fonctions offertes, ouvre la possibilité à de nombreuses architectures pour ce système. Leur évolution vers des technologies toujours plus puissantes et miniaturisées accroît encore les possibilités.

L'architecture de l'ensemble reste toutefois fortement dépendante de l'architecture du système de vidéosurveillance du tunnel.

Le choix de l'architecture du système de DAI doit prendre en compte différents critères, qui sont :

- le nombre de caméras ;
- le débit du flux vidéo qui est fonction de la qualité des images choisie ;
- les capacités des réseaux de communication ;
- le nombre de locaux techniques et leur positionnement ;
- l'espace disponible dans le ou les locaux techniques et au(x) PCC ;
- le niveau de sûreté de fonctionnement et de cybersécurité à atteindre en fonction des enjeux de l'ouvrage.

En fonction de l'architecture choisie, le positionnement des équipements diffère.

Dans tous les cas, l'acquisition se fait à l'intérieur du tunnel – par l'intermédiaire des caméras – et la visualisation au niveau du PCC – sur les écrans du mur d'images, sur la supervision[16] ou sur le client DAI[17].

Pour la gestion des flux vidéos et leur analyse, différentes solutions sont envisageables : au plus près de l'acquisition avec l'intégration de l'analyse d'images dans la caméra jusqu'à une analyse déportée et centralisée plus ou moins loin du tunnel.

Des architectures-types de DAI en tunnel sont présentées ci-après. Il ne s'agit que d'exemples. Des architectures combinant celles présentées sont aussi possibles.

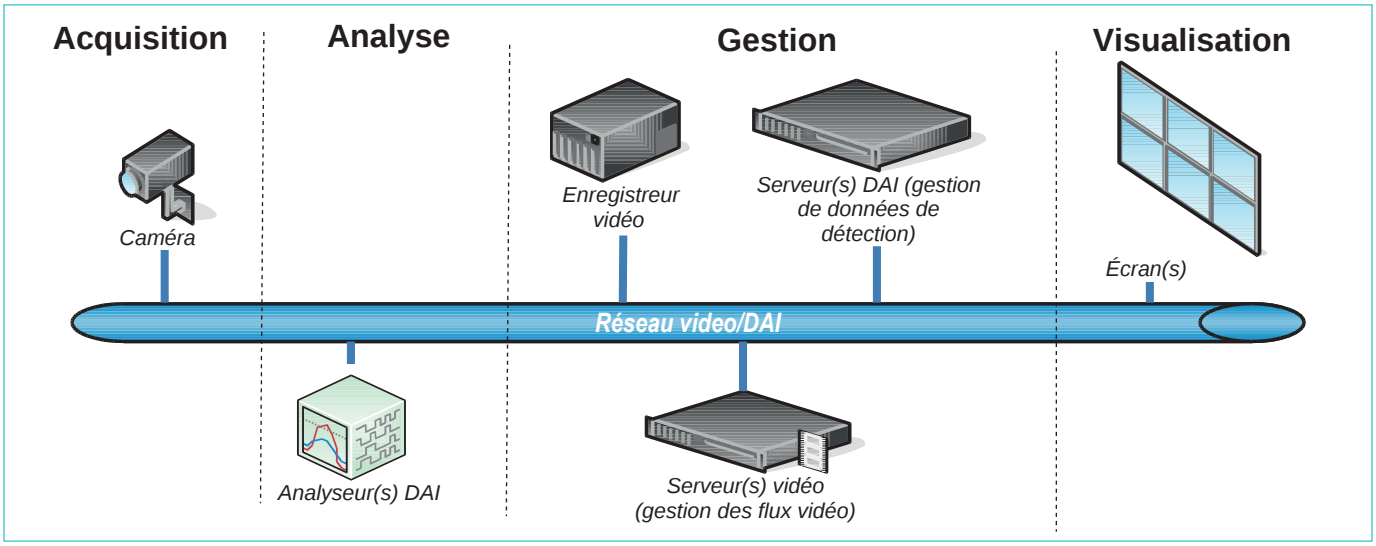



*Figure 6 : Synoptique-type d'une DAI*

14. Le réseau fédérateur est le réseau où transitent les échanges de données entre systèmes (GTC, vidéosurveillance, DAI, Réseau d'Appel d'Urgence - RAU, signalisation extérieure...) au niveau du tunnel.
15. Réseau local informatique regroupant un ensemble de machines de manière logique et non physique.
16. Interface homme machine permettant à l'exploitant de suivre et piloter les équipements du tunnel.
17. Logiciel de gestion et de supervision développé par le fabricant du système de la DAI.

## Exemple d'architecture n°1 : analyseurs en local technique tunnel

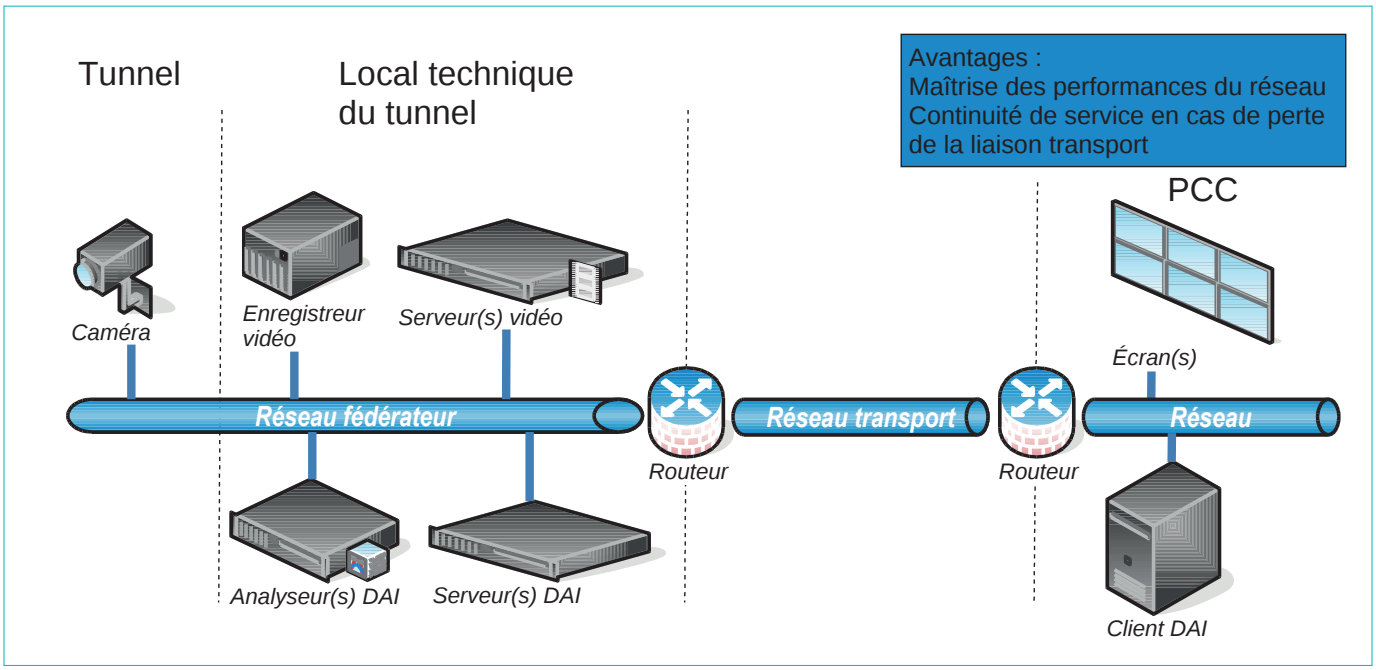



*Figure 7 : Synoptique d'une DAI avec analyseurs en local technique*

Cette architecture est souvent rencontrée en tunnel : l'ensemble des serveurs et analyseurs sont installés dans un local technique du tunnel. Les phases d'acquisition et d'analyse sont tributaires du seul réseau fédérateur, qui est maîtrisé par le gestionnaire (fiabilité et débit). Cette configuration permet également d'utiliser le système en mode local indépendamment de la liaison avec le PCC. Cette configuration est aussi un avantage pour assurer la continuité de service depuis le ou les PCC de secours en cas de dysfonctionnement du PCC principal.

## Exemple d'architecture n°2 : analyse intégrée dans la caméra

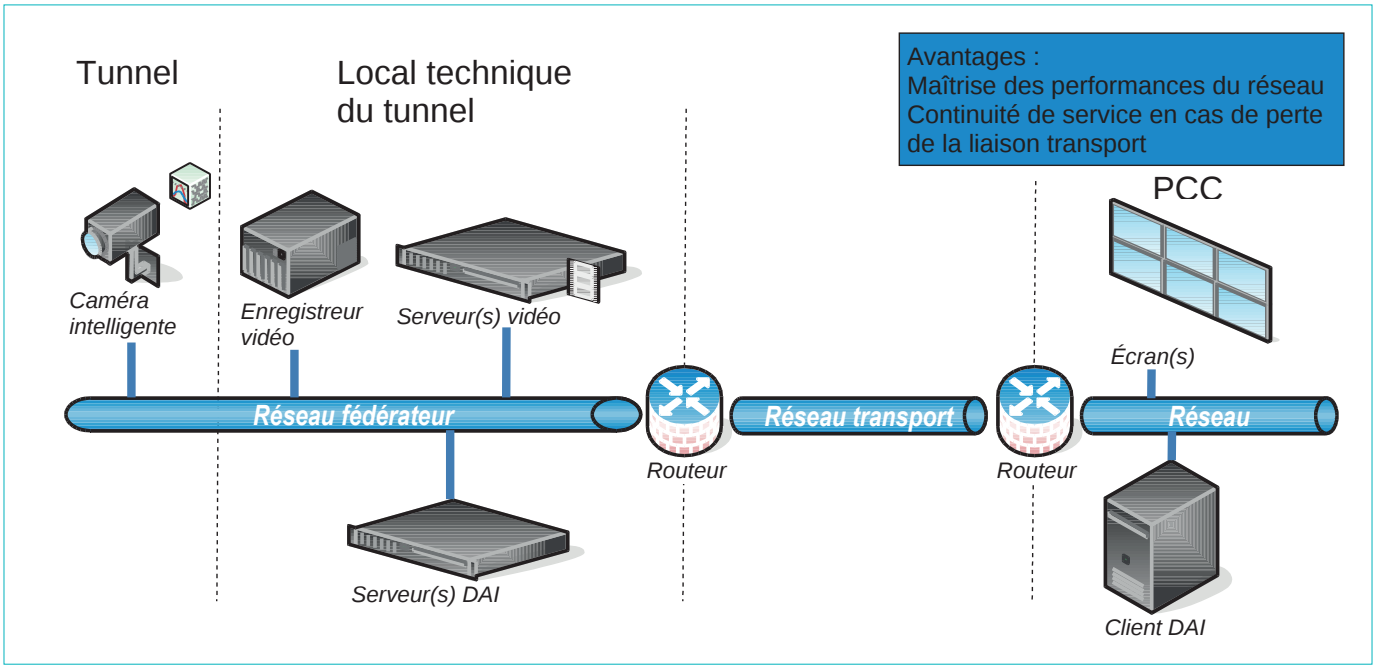



*Figure 8 : Synoptique d'une DAI avec analyse intégrée dans la caméra*

Dans cette architecture la fonction d'analyse est intégrée dans la caméra. Les avantages sont similaires à ceux de la solution 1.

## Exemple d'architecture n°3 : serveurs et analyseurs déportés au PCC

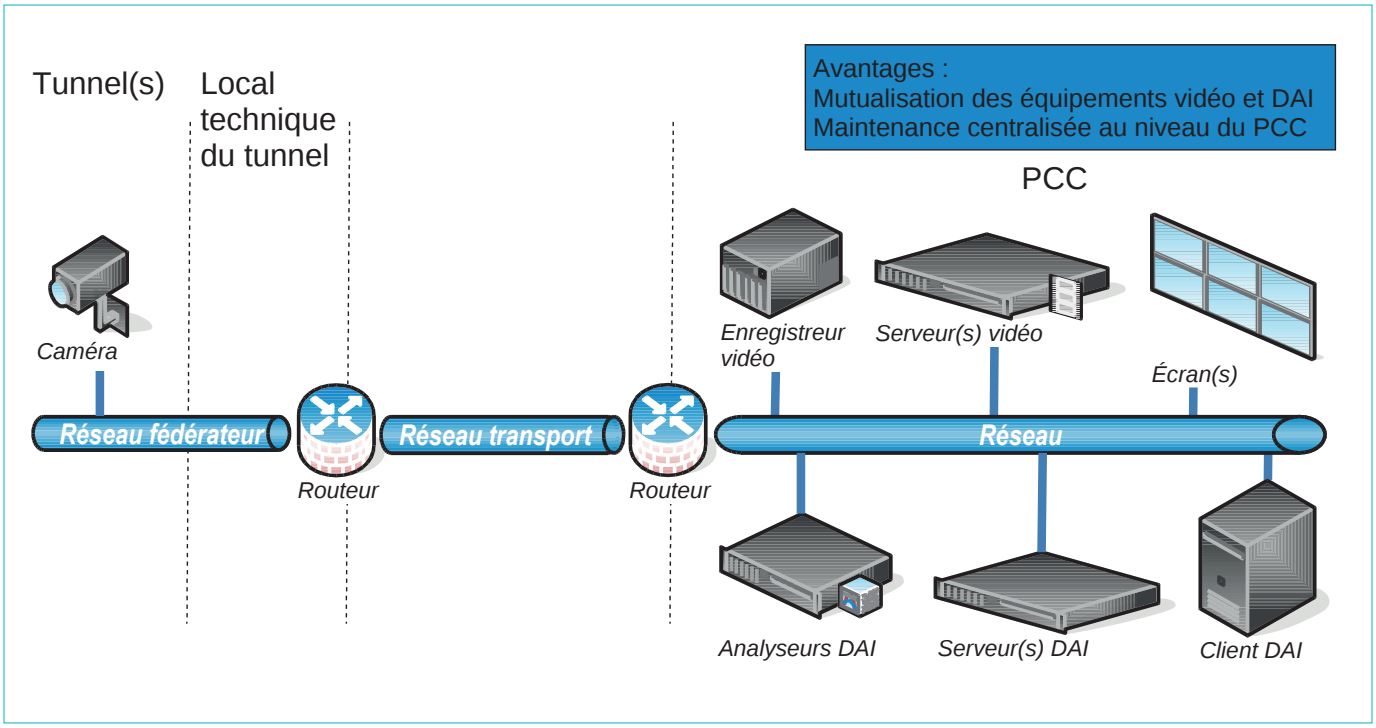



*Figure 9 : Synoptique d'une DAI avec serveurs déportés au PCC*

Cette dernière architecture regroupe l'ensemble des éléments de gestion et d'analyse au niveau du PCC.

Bien qu'au premier regard cette solution semble offrir de nombreux avantages en termes financiers et de maintenance, des études approfondies du système dans son ensemble sont à mener avant son déploiement en prenant en compte la capacité des réseaux de transport (cf. chapitre 7 – Cybersécurité et sûreté de fonctionnement) et leur fiabilité.

Pour les architectures 1 et 3, il est également possible de mutualiser certaines ressources (analyseurs en spare[18] entre tunnels, virtualisation de serveurs…) pour améliorer la résilience globale d'analyse du système.
L'architecture 2 limite la perte de la fonction DAI à une zone réduite du tunnel en cas de défaut d'un des analyseurs (caméra).

Quelle que soit l'architecture choisie par le maître d'ouvrage, la résilience doit être étudiée en fonction des enjeux de sécurité de l'ouvrage (cf. chapitre 7 – Cybersécurité et sûreté de fonctionnement).
Il est également important de bien prendre en compte les sujétions liées à l'entretien et la maintenance.

18. Matériel surnuméraire qui permet la reprise d'activité rapide.

5

# MODES DE FONCTIONNEMENT

Un système de DAI a pour rôle de détecter des situations anormales se produisant dans un tunnel. Il s'agit de sa fonction première, devant être assurée en permanence dans un tunnel en exploitation, comme aide aux opérateurs chargés de la surveillance du tunnel. C'est aussi une fonction obligatoire selon la réglementation (voir chapitre 2 – Éléments réglementaires).

Les systèmes de DAI sont toutefois dotés d'autres fonctionnalités, destinées notamment à faciliter son utilisation et sa maintenance.

Ces différentes fonctionnalités sont présentées dans ce chapitre.

## 5.1 FONCTIONNEMENT EN EXPLOITATION

Au PCC, en l'absence d'incident, les écrans affectés à la DAI peuvent être soit en mode veille, soit en mode affichage. S'il est utilisé en exploitation, le client DAI est actif.

En règle générale, dès l'apparition d'un incident, les séquences détaillées ci-dessous s'enchaînent. Ce séquencement peut différer d'un système à un autre. Par ailleurs, certaines séquences peuvent être conduites en parallèle.

Ces séquences sont les suivantes :

- l'analyseur DAI détecte l'incident, procède à son horodatage en spécifiant au serveur DAI la caméra, la zone/voie et le type d'incident ;
- le serveur DAI filtre éventuellement l'incident suivant des règles prédéfinies (paragraphe 5.2), et applique des règles de priorisation ;
- l'incident est affiché sur le client DAI avec l'ensemble des informations qui le caractérisent ;
- le serveur vidéo affiche automatiquement les images de la caméra ayant détecté l'incident sur l'écran dédié à la DAI ;
- le serveur DAI prélève dans l'enregistrement numérique vidéo, la séquence correspondant à l'incident (durée paramétrable qui, généralement, commence 30 secondes avant et se termine 2 minutes après l'incident) ;
- le serveur DAI remonte éventuellement les alarmes relatives à l'incident à la GTC. La vue d'exploitation correspondante est activée sur la supervision. L'incident est localisé sur le synoptique ;
- une alarme sonore et visuelle est déclenchée au PCC ;
- la vidéo de l'incident peut être revisionnée pour analyser la situation ;
- soit l'incident est confirmé et l'opérateur déclenche le scénario d'exploitation adapté (fermeture, incendie…), soit il s'agit d'une fausse alarme ;
- l'opérateur qualifie et acquitte l'alarme.

## 5.2 FONCTIONS OPTIONNELLES D'AIDE À L'EXPLOITATION

Plusieurs fonctions optionnelles sont proposées et peuvent faciliter l'exploitation.

En cas de détection d'incidents simultanés ou successifs, une « pile » est créée. Elle est consultable sur le client DAI où les incidents peuvent être sélectionnés de façon unitaire pour être affichés sur les écrans dédiés à la DAI.

Des dispositifs de filtrage sur une durée paramétrable sont introduits dans les algorithmes afin d'éviter que le même incident ne donne lieu à une succession de détections, que ce soit sur la même caméra, ou sur des caméras successives. La notion de caméras voisines s'étend jusqu'à deux caméras en amont et deux en aval de la caméra courante. Elle peut aussi concerner les caméras proches mais pas dans le même alignement.

Ces fonctionnalités permettent de limiter les alarmes sans intérêt pour l'opérateur (par exemple, arrêts successifs de véhicules dans une congestion déjà détectée).

Le serveur DAI permet l'inhibition de chaque type de détection par caméra, par voie et par tube. Ces inhibitions sont possibles de manière individuelle ou par groupe ou zone. Cette fonction est très utile quand le tunnel n'est pas exploité de façon normale (travaux) et peut être préconfigurée sous forme de scénario.

Les durées d'affichage des alarmes de détection et de réapparition d'un incident non acquitté peuvent également être paramétrées par l'exploitant depuis le serveur DAI.

## 5.3 FONCTIONS D'AIDE À LA MAINTENANCE

Les fonctions d'aide à la maintenance permettent d'alerter l'exploitant en cas de défaut du système. Un système de DAI peut faire son auto-diagnostic en interrogeant les constituants de l'installation sur leurs états techniques et fonctionnels.

Le système de DAI peut ainsi remonter les alarmes suivantes :

- **bougé caméra :** le système remonte une alarme à la supervision lorsqu'il repère un déplacement de la caméra susceptible de détériorer la performance de détection. Cette alarme ne doit cependant pas être remontée en cas de faibles vibrations occasionnées par exemple par le passage de véhicules à proximité de la caméra, dès lors que celles-ci ne remettent pas en cause les paramètres de l'analyse ;
- **dégradation de la qualité de l'image :** le système remonte une alarme à la supervision lorsque l'image n'a plus la qualité suffisante pour assurer la détection d'incident et tenir les performances exigées. Il s'agit par exemple de détecter l'encrassement de la vitre d'un caisson ou le desserrement d'un objectif ;
- **perte ou dégradation du flux vidéo :** le système signale à la supervision l'absence ou la dégradation du flux en entrée ;
- **défauts fonctionnels et techniques :** les défauts logiciel et matériel génèrent une alarme technique. Il s'agit généralement de défauts techniques (température du processeur trop élevée ou tout défaut entraînant une perte de disponibilité fonctionnelle) ou de défauts fonctionnels (dysfonctionnement d'une fonction d'analyse, de la fonction d'inhibition…).

L'objectif de ces fonctions d'aide à la maintenance est de déclencher une intervention afin de corriger le défaut.

Suivant l'ampleur de l'intervention effectuée, des tests de non régression[19] du système peuvent s'avérer nécessaires.

## 5.4 FONCTIONS D'ADMINISTRATION

Le serveur DAI permet à l'exploitant d'accéder à certaines fonctions d'administration. Suivant les systèmes et ses fonctions d'administrateur, l'exploitant a la possibilité de :

- définir ou recaler les zones à surveiller ;
- définir ou modifier les règles de filtrage ;
- activer ou inhiber des détections par type d'incident, par voie et/ou par tube ;
- définir et gérer des utilisateurs du système ;
- archiver des données ;
- consulter et éditer le journal des événements ;
- recharger le paramétrage de référence sauvegardé, ce qui peut être utile après une mise à jour du logiciel ;
- afficher l'état de fonctionnement des appareils DAI (caméras, serveurs…).

19. Tests visant à s'assurer que les fonctionnalités et leurs performances avant modification sont a minima maintenues.

# 6 PERFORMANCES DE DÉTECTION

Le niveau de performance d'une DAI, à savoir sa capacité à détecter des incidents et les qualifier correctement, s'apprécie au travers de plusieurs indicateurs.

L'obtention d'un système de DAI performant consiste à rechercher le meilleur compromis entre taux de détection, fausses alarmes et délais de détection, qui sont des paramètres interdépendants.

## 6.1 CLASSES D'ALARMES

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

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

**Les incidents détectables** par le système correspondent à la somme des **VA** et des **ND** et éventuellement des **AMQ**, c'est-à-dire à l'ensemble des incidents que le système de DAI, s'il a été parfaitement programmé et fonctionne à 100 % de ses capacités, doit être capable de détecter.

Au sens de cette définition, tout incident n'est pas un « incident détectable ». Ainsi l'exploitant peut souhaiter que l'algorithme du système de DAI inhibe toute détection d'un incident survenant sur la même caméra dans les 2 minutes suivant une première détection. Il est alors normal que cet incident ne soit pas détecté.

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

## 6.2 INDICATEURS

Les indicateurs définis ci-après sont calculés à partir du nombre de vraies alarmes, fausses alarmes, alarmes mal qualifiées et non-détections.

### 6.2.1 Définitions

Les indicateurs permettant de définir les performances d'un système de DAI sont au nombre de six :

- **le taux de détection général (TDG)** qui permet de mesurer la sensibilité du système tout incident confondu. Il est égal à :

$$TDG = \frac{VA + AMQ}{VA + AMQ + ND} \times 100$$

- **le taux de fausse alarme général (TFAG)** qui permet de mesurer la probabilité qu'une alarme, tout type d'incident confondu, soit fausse. Ce taux est dépendant du nombre d'alarmes total remonté et nécessite un échantillon suffisant pour être représentatif. Il est égal à :

$$TFAG = \frac{FA}{FA + AMQ + VA} \times 100$$

- **le taux de détection (TD)**[20] qui permet de mesurer la sensibilité du système par type d'incident. Il est égal à :

$$TD = \frac{VA}{VA + ND} \times 100$$

20. Pour cette formule, les AMQ doivent être intégrées dans les FA ou les VA suivant le choix de l'exploitant.

- **le taux de fausses alarmes (TFA)** qui permet de mesurer la probabilité qu'une alarme par type d'incident soit fausse. Ce taux est dépendant du nombre d'alarmes total remonté et nécessite un échantillon suffisant pour être représentatif. Il est égal à :

$$TFA = \frac{FA}{FA + VA} \times 100$$

- **la fréquence de fausses alarmes (FFA)** qui représente le nombre de fausses alarmes par type d'incidents rapporté à la durée de l'échantillon en jours et par caméra. Ce taux rapporté au nombre de caméras dans l'ouvrage est représentatif de la gêne occasionnée à l'opérateur par les fausses alarmes.
  On peut en outre définir une **fréquence de fausses alarmes général (FFAG)** correspondant à la somme des différentes FFA des types d'incidents à détecter ;
- **le délai de détection moyen (DDM)** qui est défini comme la moyenne des laps de temps qui s'écoulent entre la survenue des incidents et leur détection par le système de DAI. Il est égal à :

$$DDM = \frac{\sum_{i=1}^{N_{det}} (t_d - t_i)}{N_{det}}$$

avec :

– $N_{det}$ : le nombre d'incidents détectés,

– $t_d$ : l'instant $t$ auquel l'incident a été détecté,

– $t_i$ : l'instant $t$ auquel l'incident est survenu.

Il est important de signaler que l'instant auquel l'incident a été détecté peut être très différent selon qu'il est observé au plus près du tunnel (client DAI en local technique) ou au niveau de l'opérateur (remontée d'alarme sur la supervision). Suivant l'objectif recherché (réception de l'installation de DAI, inspection durant la vie de l'ouvrage), on privilégiera donc l'un ou l'autre.

### 6.2.2 Lien entre taux de détection et taux de fausses alarmes

Les indicateurs que sont le taux de détection (TD), le délai de détection moyen (DDM) et le taux de fausses alarmes (TFA) ne sont pas indépendants. Privilégier le taux de détection ou une détection rapide conduit à une plus grande fréquence de fausses alarmes et inversement. La calibration du système de DAI est donc une étape importante qui vise à trouver le meilleur compromis entre le minimum de non-détections, le minimum de fausses alarmes et un délai de détection approprié. Ce réglage doit être très minutieux.

En termes de paramétrage, un équilibre est donc à trouver entre des réglages qui permettent de détecter quasiment tous les incidents mais qui génèrent beaucoup de fausses alarmes, et des réglages qui ne permettent pas de détecter tous les incidents souhaités mais qui limitent le nombre de fausses alarmes.

Pour un délai de détection fixé, le taux de fausses alarmes (TFA) croît au fur et à mesure que le taux de détection (TD) augmente. Une relation identique existe entre le taux de détection générale (TDG) et le taux de fausse alarme générale (TFAG).

## 6.3 FACTEURS INFLUANT SUR LES PERFORMANCES

De nombreux facteurs peuvent influencer les performances d'un système de DAI :

- les caractéristiques du site (géométrie du tunnel, type et volume de trafic, exposition des têtes, pénétration de la lumière naturelle, conditions d'éclairage, qualité du réseau de transmission entre le tunnel et le PCC…) ;
- la conception du système de DAI du point de vue matériel et logiciel (technologies utilisées, disposition des caméras, conception et paramétrage des algorithmes). Cette conception doit être adaptée aux caractéristiques particulières du site (voir chapitre 4 – Équipements de DAI) ;
- le nombre de caméras DAI, car le nombre de FA augmente avec le nombre de caméras, qui est lui-même dépendant de la longueur de l'ouvrage et du nombre d'ouvrages surveillés par le PCC ;
- le choix des types d'incidents à détecter, car chaque type d'incident à détecter étant associé à une FFA, augmenter le nombre d'incidents à détecter provoque une augmentation de l'apparition de FA et dégrade ainsi la crédibilité du système ;
- le nombre de fonctionnalités proposées, qui est susceptible de croître avec les évolutions technologiques, mais qui doit cependant être maîtrisé et restreint à ce qui est indispensable pour assurer la sécurité des usagers ;
- l'ergonomie du logiciel et son appropriation par les opérateurs ;
- le défaut de maintenance préventive et corrective (voir paragraphe 9.3 – Actions de maintenance et de contrôle).

Pour les systèmes DAI communiquant avec la supervision du tunnel, il faut noter que les caractéristiques du réseau et de la GTC ont une influence sur les performances globales de la fonction de sécurité « détection ». En effet, d'éventuelles latences dans la transmission d'information par le réseau et dans le traitement des alarmes de supervision par la GTC peuvent impacter les performances perçues du système, notamment le délai de détection.

# 7 CYBERSÉCURITÉ ET SÛRETÉ DE FONCTIONNEMENT

La DAI fait partie des équipements de sécurité indispensables afin que les usagers puissent se mettre hors de danger et que les premiers secours puissent intervenir en cas d'incident ou d'accident. Elle est, pour cette raison, alimentée par une alimentation électrique secourue sans coupure afin de préserver son fonctionnement même en cas de défaillance de l'alimentation électrique extérieure (voir 3.1.1 de l'IT).

Les systèmes de DAI sont en outre des systèmes sensibles qui peuvent faire l'objet de défaillances ou de cyberattaques, mettant en péril leur intégrité.

S'agissant donc de systèmes d'information étendus et critiques, les systèmes de DAI doivent être résilients du point de vue de la sûreté de fonctionnement et protégés contre les cyber-menaces.

Ce chapitre présente les principes généraux de cybersécurité et de sûreté de fonctionnement à appliquer aux installations de DAI.

Les textes réglementaires applicables sont présentés au paragraphe 2.3 – Cybersécurité. Des informations complémentaires sont données en annexe F.

## 7.1 SÉCURISATION DES RÉSEAUX DE TRANSMISSION

Pour sécuriser les architectures DAI telles que décrites au paragraphe 4.4 – Architectures, des principes de sûreté de fonctionnement conjugués à des principes de cybersécurité doivent être mis en œuvre afin de sécuriser l'ensemble des réseaux de transmission utilisés par le système.

### 7.1.1 Principes communs

Afin d'éviter qu'une défaillance se traduise par une perte d'exploitation du système de DAI, et finalement un dépassement des Conditions Minimales d'Exploitation (CME), il faut accroître la disponibilité du système de transmission (réseau, switch, routeur…).

L'architecture doit donc être construite avec des **redondances**, sans mode commun de défaillance (*single point of failure* – SPOF). En particulier, les réseaux de transmission doivent être conçus avec des redondances de « chemins » au niveau 2 (couche liaison de données - Ethernet) et des redondances de « routes » au niveau 3 (couche réseau - IP) du modèle OSI[21].

Par ailleurs, les pare-feux assurant la connexion de différents réseaux ou servant à l'établissement de liaisons sécurisées doivent être en redondance de haute disponibilité (*High availability* – HA) c'est-à-dire conçus pour minimiser les interruptions de service.

Suivant la sensibilité du tunnel, les serveurs de DAI peuvent être regroupés en cluster[22] ou en machines virtuelles sur un système hôte en cluster.

### 7.1.2 Sécurisation du réseau fédérateur

L'ensemble des équipements du réseau fédérateur étant implantés sur le terrain, une protection et une surveillance des accès physiques à ces équipements (locaux techniques, armoires…) sont indispensables.

En matière de transmission locale, des architectures sur des boucles sont généralement utilisées ; elles permettent de supporter la perte d'un équipement. Au niveau terrain, on utilise des redondances de niveau 2 ; il existe pour cela des protocoles standardisés (comme le *rapid spanning tree* – RSTP) ou propriétaires (*hyperring*, *turbochain*…), permettant la reconfiguration d'un réseau en cas de perte d'un lien.

### 7.1.3 Sécurisation du réseau de transport

La protection des accès physiques est plus difficile pour le réseau de transport que pour le réseau fédérateur. Pour assurer l'intégrité et la confidentialité des données transitant sur le réseau de transport, on utilise donc des **protections logicielles** telles que les tunnels *Virtual Private Network* (VPN) avec le protocole *Internet Protocol Security* (IPSec[23]) montés depuis les extrémités sécurisées.

21. Modèle OSI (*Open Systems Interconnection*) défini par la norme ISO/CEI 7498-1-1994:1994.
22. Groupe d'objets. Notamment pour assurer la haute disponibilité. Si un équipement est indisponible, l'autre peut reprendre le fonctionnement de manière complètement transparente pour les utilisateurs. Cela permet également une répartition de charge.
23. Protocole de sécurisation des données IP, permettant notamment d'assurer le chiffrement des données dans un tunnel VPN.

Le mode de sécurisation de ce réseau varie selon l'architecture du réseau global dans lequel il s'intègre. La sécurisation peut être obtenue au moyen de redondances de niveau 2 (du même type que pour le réseau fédérateur) et de niveau 3 (protocoles *Open Shortest Path First* – OSPF et *Virtual Router Redundancy Protocol* – VRRP). Une liaison redondante peut être gérée par l'exploitant ou par un opérateur de télécommunication fournissant un accès à internet ou au travers de celui-ci.

Un exemple d'architecture de transmission est donné sur la figure 10 ci-dessous.

## 7.1.4 Coordination des protections

De simples redondances de chemins (niveau 2) et de routes (niveau 3) n'interagissent pas forcément de concert et peuvent mener à des conflits. Il faut donc veiller à la bonne coordination des protections en place (cf. annexe F).

## 7.1.5 Modalités d'accès pour les opérations de maintenance

Un accès à distance aux équipements et serveurs peut être nécessaire, tant pour l'installateur en phase de mise en service et de réglage de l'installation, que pour les techniciens de maintenance (exploitant ou tiers).

Ces accès, qu'ils soient permanents (exploitant) ou ponctuels (tiers), doivent être attribués avec la plus grande prudence, en cohérence avec la PSSI.

Il est primordial de mettre en place un portail d'accès distant, accessible par exemple au moyen d'un VPN chiffré (IPSec ou protocole *Transport Layer Security* – TLS[24]) avec authentification mutuelle des machines qui participent à la connexion. Une authentification forte et multifactorielle sur le portail doit être demandée à l'utilisateur, à qui les accès aux différentes machines sont autorisés, en fonction de son identité.

Il faut noter que les équipements et serveurs ne devraient jamais être directement accessibles depuis Internet. Les connexions web chiffrées sortantes – donc généralement autorisées par les pare-feux – vers le serveur distant ne sont pas souhaitables, d'une part parce qu'elles ne respectent pas les critères d'authentification multi-étapes et multi-factorielle préconisée par l'ANSSI, et d'autre part parce qu'elles ne sont pas qualifiées telles qu'on les attend sur une pare-feu externe.

Dans une version très sécurisée, qui est recommandée, l'utilisateur distant n'est pas autorisé à charger ou téléverser directement des fichiers : il les fait transiter par une machine dédiée sur le réseau technique, avec intervention de l'opérateur présent au PCC pour les relayer depuis ou vers l'Internet.

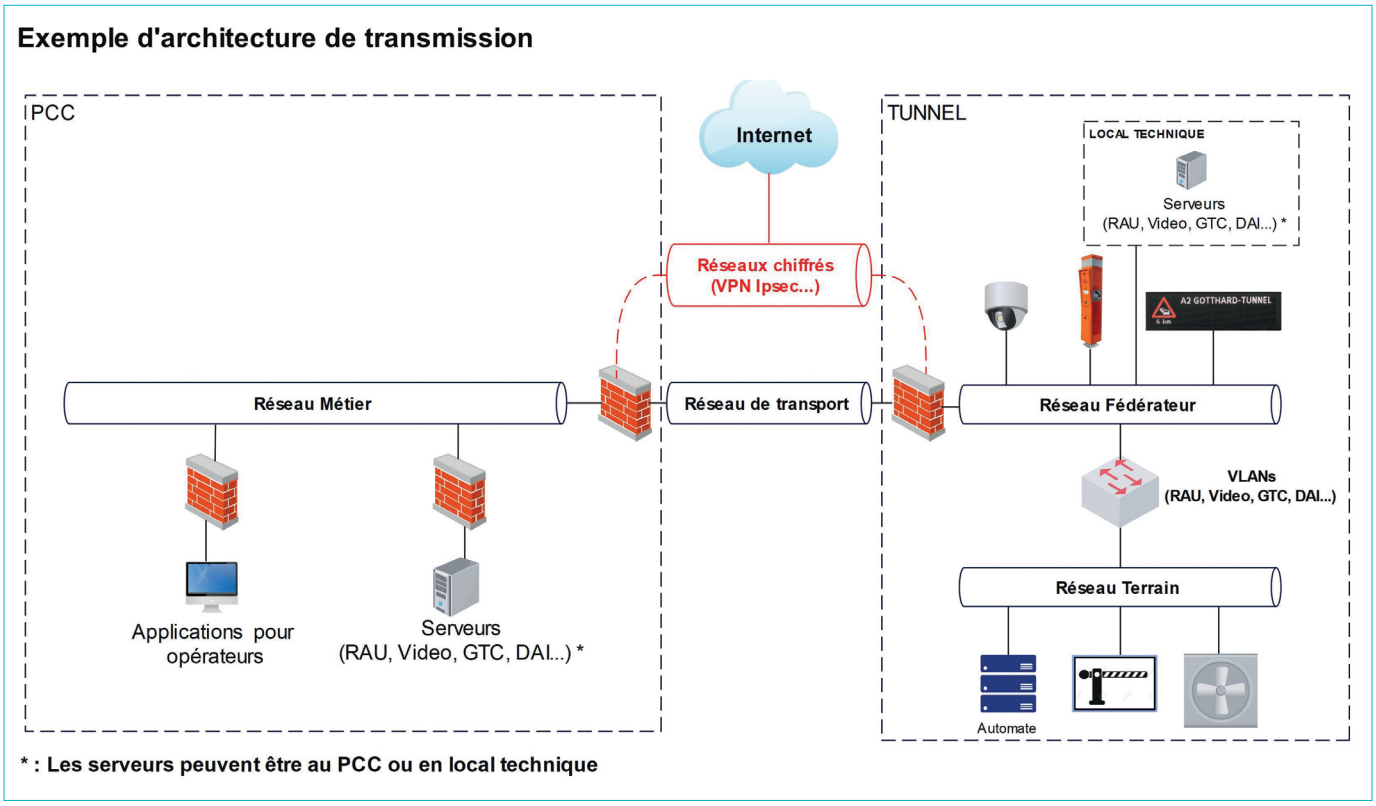



*Figure 10 : Exemple d'architecture de transmission (© Cerema Sud-Ouest)*

24. Protocole pour une communication sécurisée entre un client et un serveur afin d'assurer la confidentialité (chiffrement) et l'intégrité des données.

### 7.1.6 Fonctionnement sans accès à Internet

Pour réduire le risque d'intrusion par cyberattaque, l'ensemble des équipements de terrain et les serveurs doivent fonctionner en mode nominal sans avoir besoin d'accéder à des services ou serveurs sur Internet (fonctionnement « *on premice* »).

Dans ce cadre, certains équipements sont toujours nécessaires au fonctionnement du système, et notamment les serveurs de temps et de noms. Les serveurs de temps (*Network Time Protocol* – NTP[25]) et de noms (*Domain Name Server* – DNS[26]) sont des équipements locaux ou relais fondamentaux utilisés couramment. Lors de la configuration de ces serveurs, il est important d'être attentif à leurs paramétrages pour fonctionner sans Internet.

## 7.2 MISES À JOUR DU SYSTÈME

Les logiciels de DAI sont potentiellement vulnérables, ce qui implique leur mise à jour régulière et l'application rigoureuse des correctifs publiés par les éditeurs. Il n'est pas prudent de laisser le système sans mise à jour.

Dans la mesure du possible, il faut tester la compatibilité des mises à jour sur une réplique partielle du système fonctionnant hors exploitation avec machines dédiées, qu'elles soient physiques ou virtuelles.

Lorsqu'une partie du système est obsolète et ne dispose plus de mises à jour de sécurité, l'exploitant doit définir des mesures de sécurité supplémentaires (déconnexion, ajout de machines mandataires en *Demilitarized Zone* – DMZ[27]…) afin de compenser le risque d'exposition, en attendant le remplacement du système.

Il est également important de noter qu'en cybersécurité, le risque zéro n'existe pas, notamment en raison des vulnérabilités « *ZERO DAY* », à savoir des failles d'un logiciel ou d'un système qui sont découvertes par un attaquant et pour lesquels il n'y a encore pas de correctif connu. Une vulnérabilité de ce type n'est pas à exclure dans un système de DAI.

Des plans de continuité d'activité (PCA) et de reprise d'activité (PRA) doivent, pour cette raison, être élaborés en cohérence avec la PSSI, et testés lors d'exercices.

25. Protocole permettant la synchronisation du temps entre plusieurs machines.
26. Service informatique permettant d'associer des noms de domaine internet (adresse web) à leurs adresses IP respectives.
27. Emplacement réseau situé généralement entre deux pare-feux pour sécuriser un réseau local du trafic internet. Cette zone héberge des machines devant assurer une communication directe vers Internet.

# 8 DE LA CONCEPTION À LA RÉCEPTION LES ÉTAPES DE DÉPLOIEMENT D'UN SYSTÈME DE DAI

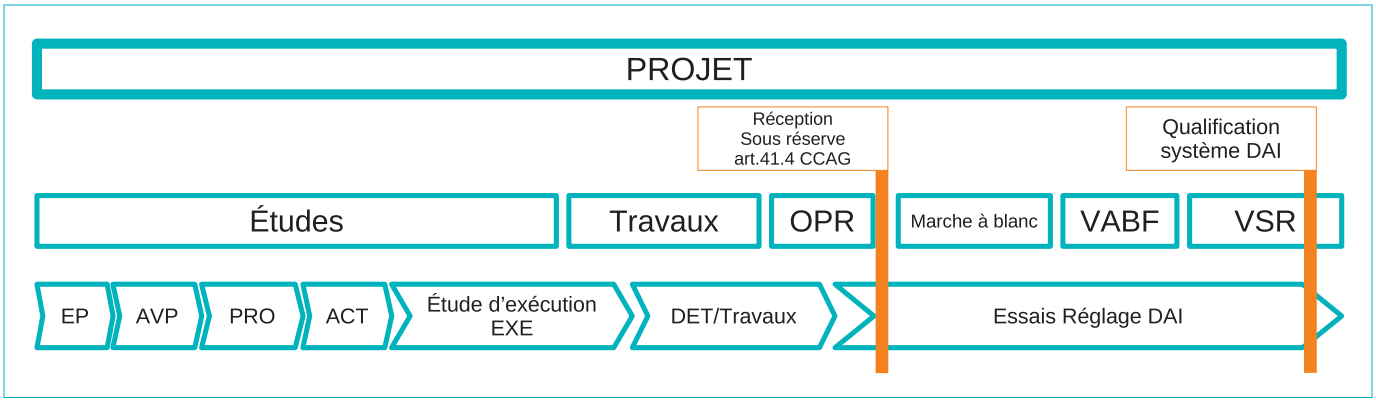



*Figure 11 : Diagramme des différentes phases d'un projet*

Les performances d'un système de DAI dépendent en premier lieu du soin apporté à sa conception, qui doit être intégrée et anticipée, et prendre en compte les interactions avec les autres systèmes de sécurité du tunnel.

La phase d'essais, qui démarre à la fin des travaux, est une autre phase cruciale, car elle valide le bon fonctionnement du système. Cette validation s'articule en trois étapes :

1. **Les Opérations Préalables à la Réception (OPR)**, qui consistent en la vérification des fonctionnalités techniques et logicielles, ainsi que des détections sur incidents. Dans le cas des ouvrages en exploitation, elle est généralement effectuée lors d'une fermeture du tunnel. Une fois les travaux jugés conformes au marché, la réception est prononcée sous réserve de la validation des performances de détection, ce qui a pour conséquence le transfert de la propriété du système au maître d'ouvrage[28].
2. **La Vérification en Service Régulier (VSR)**, lors de laquelle l'entreprise qui a réalisé les travaux procède aux réglages du système en conditions réelles de circulation, en collaboration avec le fabricant, notamment pour réduire les fausses alarmes.
3. **La validation des performances de détection**, qui consiste en la simulation d'incidents sous fermeture pour vérifier les performances atteintes en fin de VSR, et doit permettre *in fine* de lever les réserves.

Le suivi scrupuleux de ces étapes est une condition nécessaire pour garantir la conformité aux prescriptions du marché et l'efficacité du système avant sa mise en service définitive (cf. guide du CETU, *Équipements des tunnels routiers et des transports guidés urbains – Essais, réceptions et garanties*, 2019).

## 8.1 ÉTUDES DE CONCEPTION

Les études de conception recouvrent successivement les études préalables (EP), les études d'avant-projet (AVP) et les études de projet (PRO). Dès lors qu'il est connu, il est nécessaire d'associer l'exploitant à ces différentes étapes.

À l'issue des études de conception, au moins les éléments suivants doivent avoir été définis :

- **les contraintes d'implantation** (géométrie de l'ouvrage, points singuliers, caractéristiques de la structure...) ;
- **les contraintes d'exploitation** (gabarit routier autorisé, modalités d'intervention en tunnel pour le mainteneur, autres contraintes opérationnelles) ; par souci de sécurité et de durabilité, aucune caméra ne doit engager la hauteur libre ni les revanches latérales de protection de l'ouvrage (voir *Dossier Pilote – Géométrie* du CETU, décembre 1990) ;
- **l'étude de trafic** (typologie et volume des véhicules empruntant le tunnel) ;
- **les modalités de fonctionnement avec le système de vidéosurveillance** (en particulier, si les prestataires ou les temporalités d'installation diffèrent entre les systèmes de DAI et de vidéosurveillance, une description détaillée du système de vidéosurveillance – emplacement des caméras, caractéristiques techniques – doit être fournie) ;

28. Article 41.4 du Cahier des Clauses Administratives Générales (CCAG) : « *Dans le cas où certaines épreuves doivent, conformément aux stipulations du CCAP, être exécutées après une durée déterminée de service des ouvrages ou à certaines périodes de l'année, la réception ne peut être prononcée que sous réserve de l'exécution concluante de ces épreuves.* »

- **les règles de gestion des défauts** (liste des anomalies techniques et fonctionnelles qui doivent déclencher une alarme pour faciliter la maintenance – cf. paragraphe 5.3) ;
- **les modalités d'intégration à la GTC / Supervision** (informations nécessaires à l'intégration, incluant les protocoles de communication et les alarmes associées aux incidents techniques et d'exploitation) ;
- **les spécifications de détection** (liste des incidents à détecter – cf. chapitre 3 –, avec des exigences précises en matière de taux de détections, de fréquence de fausses alarmes et de délai de détection – cf. paragraphe 6.2. Pour établir cette liste, le tableau suivant peut servir d'exemple.

**Les valeurs cibles doivent être fixées selon les spécificités de l'ouvrage (caractéristiques géométriques, trafic…).**

**À titre indicatif, le taux de détection** à atteindre est généralement compris entre 80 et 98 %. Pour rappel, plus on cherche à atteindre un taux proche de 100 % sur un type d'incident, plus on risque de dégrader le taux de fausses alarmes.

**La fréquence de fausses alarmes** maximale admise à retenir est généralement comprise entre 0,025 et 0,150 par caméra, par jour et par type d'incident. Ce paramètre doit être ajusté en fonction de la configuration du PCC (nombre de caméras DAI remontant au PCC, tous ouvrages confondus et types d'incidents à détecter, nombre d'opérateurs en poste, etc.) pour que le nombre total de fausses alarmes (cumul des fausses alarmes au PCC sur une journée) puisse être acceptable pour le ou les opérateurs.

Enfin, **le délai de détection** maximal attendu peut être compris entre 2 et 20 secondes.

| Incident | Taux de détection (%) minimal à atteindre (TDG ou TD) | Fréquence de fausses alarmes maximale admise (FA/caméra/jour) | Délai de détection maximal attendu (en secondes) |
|---|---|---|---|
| Véhicule arrêté | | | |
| Incendie | | | |
| … | | | |

*Figure 12 : Table des exigences de performance à atteindre*

## 8.2 DOSSIER DE CONSULTATION DES ENTREPRISES

Les caractéristiques techniques du système de DAI y compris le tableau des performances minimales à atteindre qui ont été définies durant les études de conception, sont intégrées au dossier de consultation des entreprises. Ces éléments sont complétés par la liste des documents que le titulaire doit fournir à l'appui de son offre. Il s'agit notamment de :

- **la justification de la couverture vidéo et DAI**, qui doit inclure un plan d'implantation des caméras et les coupes associées ; elle doit tenir compte des points sensibles (niches, issues, garages, etc.) pour leur assurer une visibilité optimale, en les positionnant en début ou en milieu de champ d'image (paragraphe 4.1.3 – Couverture et implantation) ;
- **le Plan d'Assurance Sécurité (PAS)**, document contractuel qui décrit les mesures que le candidat s'engage à appliquer pour respecter les exigences de cybersécurité. Chaque co-traitant ou sous-traitant concerné doit élaborer un PAS conforme au PSSI du maître d'ouvrage (chapitre 7 – Cybersécurité et sûreté de fonctionnement). Une fois le prestataire sélectionné, le PAS est annexé au contrat et remplace d'éventuelles clauses génériques ;
- **les spécifications fonctionnelles générales** du système de vidéosurveillance et de DAI ;
- **la description des moyens humains et matériels mobilisés** par le titulaire pour la réalisation des différents essais, et notamment des tests de performance.

## 8.3 ÉTUDES D'EXÉCUTION

Une fois le contrat signé, le titulaire du marché conduit les études d'exécution. Dès la phase de préparation des travaux, il doit fournir :

- **l'étude de couverture détaillée avec prises de vue sur le terrain** (paragraphe 4.1.3 – Couverture et implantation), qui prend en compte les équipements installés ou projetés dans le tunnel afin de limiter les effets de masquage ;
- **l'étude de piquetage des caméras**, qui doit privilégier une implantation des caméras en voûte, en tenant compte du gabarit et des revanches pour réduire les phénomènes de masquage par les poids lourds ;
- **les spécifications fonctionnelles détaillées**, qui décrivent les fonctionnalités précises des systèmes de vidéosurveillance, DAI et enregistrement ;
- **les Spécifications Techniques des Matériels (STM)**, qui concernent l'ensemble des équipements prévus ;
- **les spécifications d'interface**, qui définissent les connexions avec le réseau fédérateur, le réseau de transport et la GTC / Supervision ;
- **les schémas d'architecture**, qui présentent l'intégration de la vidéosurveillance et de la DAI, tant au niveau des équipements en tunnel que des systèmes installés en locaux techniques ;
- **le plan d'intégration et d'implantation**, qui détaille l'implantation des équipements dans le tunnel, les locaux annexes et le PCC, ainsi que les cheminements.

Le démarrage des travaux d'installation des caméras est fortement déconseillé tant que les deux premiers documents (étude de piquetage et spécifications fonctionnelles détaillées) n'ont pas été validés. Un point d'arrêt doit être explicitement prévu dans le marché pour garantir cette validation préalable.

## 8.4 TRAVAUX

Pendant la phase de travaux, il est essentiel de vérifier la conformité des travaux réalisés aux documents contractuels et techniques préalablement validés.

Cette vérification porte notamment sur les points suivants :

- **implantation des caméras** (contrôle de leur positionnement, en veillant à leur adéquation avec le gabarit de circulation de l'ouvrage) ;
- **champs de vision et masquages éventuels** (validation des angles de vue pour garantir une couverture optimale et identifier les éventuelles zones d'obstruction) ;
- **cheminement des câbles** (inspection des trajets empruntés par les câbles, en conformité avec les plans d'installation et les normes en vigueur) ;
- **fixation des caissons** (vérification de la solidité et de la stabilité des fixations, de la résistance à la corrosion pour assurer la durabilité et la sécurité des installations).

## 8.5 ESSAIS SPÉCIFIQUES DU SYSTÈME DE DAI

Le système global de vidéosurveillance/DAI doit faire l'objet d'essais rigoureux, afin de valider le bon fonctionnement du système de DAI.

Ces essais sont effectués en présence du maître d'œuvre, du titulaire du marché, du fabricant du système de DAI et si possible de l'exploitant.

Pour un suivi rigoureux, des cahiers de recette validés en amont par le maître d'œuvre sont complétés au fur et à mesure :

- cahiers de recette en usine ;
- cahiers de recette sur plateforme ;
- cahiers d'installation des matériels ;
- cahiers des essais de qualification DAI.

Les essais se déroulent en différents lieux (usine, plateforme ou site) et suivent une progression : essais statiques, puis essais d'acceptation partielle, essais d'acceptation système et enfin essais d'acceptation globale, qui permettent de vérifier l'ensemble des matériels et des fonctions d'aide à la maintenance et de détection, d'abord sous fermeture du tunnel, puis en circulation durant la VSR.

À l'issue des essais d'acceptation globale, les vérifications de pré-OPR (tests qui précèdent les OPR), conduites par le maître d'œuvre, ont pour objectif de déterminer si le système de DAI peut être réceptionné, ou pas, par le maître d'ouvrage.

Si les vérifications de pré-OPR ne sont pas concluantes, la réception n'est pas prononcée et l'entreprise doit procéder à des travaux correctifs, jusqu'à ce que le système puisse être réceptionné.

Cette réception est prononcée sous réserve de la réalisation de la VSR, lors de laquelle l'entreprise procède aux réglages du système en conditions réelles de circulation.

C'est à l'issue de la VSR, lorsque toutes les réserves ont été levées, que la validation finale du système de DAI peut être prononcée.

### 8.5.1 Vérifications en vue des OPR

#### Tests fonctionnels

Les vérifications commencent par des tests fonctionnels, qui ont pour objectif de vérifier le fonctionnement des matériels et des fonctions support définies ci-après.

Des exemples de tests sont fournis en annexe C. Les tests décrits constituent un cadre à adapter en fonction des spécificités de chaque installation, étant donné la variabilité des systèmes DAI.

Une partie des tests peut être effectuée en usine ou sur plate-forme d'essais pour valider les interfaces et le bon fonctionnement du système avant son déploiement dans l'ouvrage.

Chaque équipement composant le système de DAI doit être testé individuellement. Les vérifications consistent à s'assurer que les caméras, analyseurs, serveurs, client DAI, réseaux de transport et de communication sont tous bien alimentés et opérationnels.

Les fonctions support élémentaires que doit assurer le système doivent également être vérifiées, dont notamment :

- la communication interne entre les équipements du système ;
- la communication entre le système de DAI et les systèmes connexes (GTC, mur d'images…) ;
- les fonctions d'administration et de configuration de la DAI ;
- les fonctions d'aide à la maintenance des équipements DAI (bougé caméra…) ;
- l'enregistrement, la gestion, la consultation et l'archivage des séquences vidéos numériques ;
- le fonctionnement des redondances (serveurs, analyseurs…) ;
- la remontée des alarmes techniques du système.

Il convient de procéder à ces vérifications depuis le client DAI en local, mais aussi en distant (PC de maintenance, PC d'exploitation, PC de secours…).

### Tests de performance

Après validation des essais fonctionnels, une phase de test des performances de détection doit être menée pour s'assurer que l'installation de DAI est conforme aux niveaux de performance définis au marché.

Dans le cas d'un ouvrage neuf ou existant pour lequel la rénovation comprend la vidéo et la DAI, ces tests ne peuvent démarrer qu'après la fin des essais du système de vidéo-surveillance et des réseaux de communication du tunnel (Essais d'Acceptation Partielle, Essais d'Acceptation Système). En effet la couverture vidéo, la qualité des images et la qualité du réseau fédérateur sont un prérequis aux tests de DAI.

Les tests de performance sont essentiels et leur durée ne doit pas être sous-estimée. Cette phase peut nécessiter des moyens notables en personnels et en matériels : véhicules légers, piétons, conducteurs, générateur de fumée et son alimentation, etc. Elle demande également du temps, car les essais doivent être réalisés pour chaque type d'incident, sur chaque caméra et pour chacune des voies. De plus, pour calculer des taux de détection, il est nécessaire de faire plusieurs fois les mêmes essais.

Les remontées d'alarme sont vérifiées depuis le poste client DAI pour évaluer les performances intrinsèques, puis depuis les systèmes de supervision/hypervision pour qualifier l'intégrité des transmissions.

L'annexe D présente des propositions de test des fonctions de détection par incident, suivant la classification établie au paragraphe 3.2.

En outre, il faut vérifier que le fonctionnement des autres systèmes d'équipements installés dans l'ouvrage (changement des régimes d'éclairage, de l'état de panneaux dynamiques, etc.) ne provoque pas de fausses alarmes.

Aucune modification de réglage – à l'exception de l'inhibition de fonctions de détection et de règles de filtrage – ne doit être effectuée durant cette phase. Lors des tests d'un fonction donnée, toutes les autres fonctions de détection doivent être inhibées.

Pour chaque incident à détecter, les performances sont calculées en établissant la moyenne des résultats obtenus pour l'ensemble des caméras. Elles sont ensuite comparées aux exigences définies dans le marché.

Un nombre minimal d'essais doit être réalisé. Il est déterminé en fonction des caractéristiques du tunnel : nombre de voies, géométrie du tunnel, nombre de caméras, fonctions retenues…

Certains tests peuvent concerner simultanément plusieurs caméras. Par exemple, dans le cas du test de la fonction « arrêt véhicule » en début de champ de la caméra *n*, le véhicule arrêté peut être détecté également en fin de champ de la caméra *n* – 1.

En section courante, les tests peuvent être réalisés de jour ou de nuit. Le régime d'éclairage du tunnel peut être le régime le plus faible.

Aux entrées et sorties d'ouvrage, il peut être intéressant de privilégier les tests de jour pour couvrir le plus possible des conditions d'utilisation défavorables. En effet, l'analyse d'images peut être influencée par les conditions météorologiques à l'extérieur de l'ouvrage : lumière du soleil pénétrante, chaussée humide en tête…

Il faut noter que si le système de DAI est doté de la fonction d'analyse d'enregistrements vidéo, il est conseillé de sauvegarder les séquences des tests. Ces vidéos de référence pourront être utilisées ultérieurement pour s'assurer d'une absence de régression du système lors des opérations de maintenance (cf. paragraphe 9.3.6 – Maintenance logicielle).

En guise d'illustration, l'annexe E présente un exemple de fiche de test pour un arrêt de véhicule et la fiche de synthèse des performances observées.

Les résultats obtenus sur l'ensemble des incidents permettent de calculer les taux de détection pour chaque type d'incident. Une synthèse par caméra est un moyen d'identifier d'éventuels dysfonctionnements. Si les performances respectent les prescriptions du marché, la réception peut être prononcée sous réserve de la validation des performances à l'issue de la VSR. Sinon, des correctifs doivent être apportés, et les tests réitérés. Toute modification sur une caméra nécessite une reprise intégrale des tests correspondants.

## 8.5.2 Réglages du système en VSR

Une fois la réception prononcée, sous réserve comme vu ci-dessus, débute la marche à blanc générale des équipements de sécurité du tunnel (cas des tunnels neufs) ponctuée par la Vérification d'Aptitude au Bon Fonctionnement (VABF) à l'issue de laquelle l'installation de DAI est mise en exploitation (cf. guide du CETU *Équipements des tunnels routiers et des transports guidés urbains – Essais, réceptions et garanties*, 2019).

La VSR débute ensuite, pour les installations neuves comme pour celles rénovées. Elle vise à constater que les prestations fournies sont capables d'assurer un service régulier dans les conditions normales d'exploitation prévues dans le marché.

La durée de la VSR, qui dépend de la complexité du système de DAI, est en général de trois mois. Si des problèmes sont rencontrés lors de cette phase, elle peut être étendue par exemple jusqu'à six mois.

Durant cette période, les données de fonctionnement de la DAI sont recueillies et, après analyse, fournissent les performances réelles du système. Ces constats de terrain permettent de vérifier avec certitude les vraies alarmes, les fausses alarmes et les alarmes mal qualifiées, et par conséquent, de définir le taux et la fréquence de fausses alarmes. Les éventuels défauts du système sont ainsi identifiées précisément et leur correction peut être engagée.

L'identification des non-détections est particulièrement complexe, car les non-détections n'engendrent ni séquence ni alarme remontée par le système. Elles peuvent néanmoins être détectées par les opérateurs ou grâce à des systèmes complémentaires à la DAI, tels qu'un opacimètre signalant la présence de fumée.

Une autre méthode consiste en l'analyse visuelle d'enregistrements vidéo effectués en continu sur une période donnée (une ou plusieurs semaines). Ces enregistrements permettent d'identifier les incidents potentiellement détectables par la DAI durant cette période. La liste des incidents ainsi établie est ensuite comparée aux détections effectivement remontées par le système de DAI.

Idéalement, cette approche nécessite que chaque enregistrement d'une durée suffisante soit visionné attentivement par un observateur, afin d'assurer une évaluation fiable. Toutefois, en raison des ressources importantes qu'elle mobilise, cette méthode est rarement applicable.

Pour alléger ce processus, il est envisageable de solliciter le fabricant du système de DAI pour la réalisation d'un audit de performance mené conjointement avec l'exploitant. Il s'agit d'une période de surveillance de quelques semaines, durant laquelle l'exploitant consigne dans un document dédié toutes les anomalies constatées, y compris les non-détections et les fausses alarmes, détaillées par caméra. Chaque incident génère une séquence sous forme de fichier vidéo comprenant des images avant et après l'incident. Ces séquences sont souvent suffisantes pour comprendre les anomalies du type fausse alarme. En s'appuyant sur les résultats de cet audit, les configurations inadaptées du système de DAI sont modifiées. Dans le cas de modifications substantielles, une nouvelle phase de tests de performances doit être menée (cf. paragraphe 8.5.1 – Vérifications en vue des OPR).

Durant toute cette période de VSR, les modifications peuvent être effectuées soit localement, soit à distance par l'intermédiaire d'un réseau virtuel privé chiffré (VPN) conforme aux recommandations de l'ANSSI (voir paragraphe 7.1.5 – Modalités d'accès pour les opérations de maintenance), à partir des fonctions d'administration du système.

## 8.5.3 Validation des performances

Lorsque l'ensemble des essais réalisés selon la méthode décrite dans ce chapitre sont concluants, la validation du système peut être prononcée par la levée des réserves émises lors de la réception.

La figure 13 ci-contre récapitule les étapes conduisant à la validation du système.

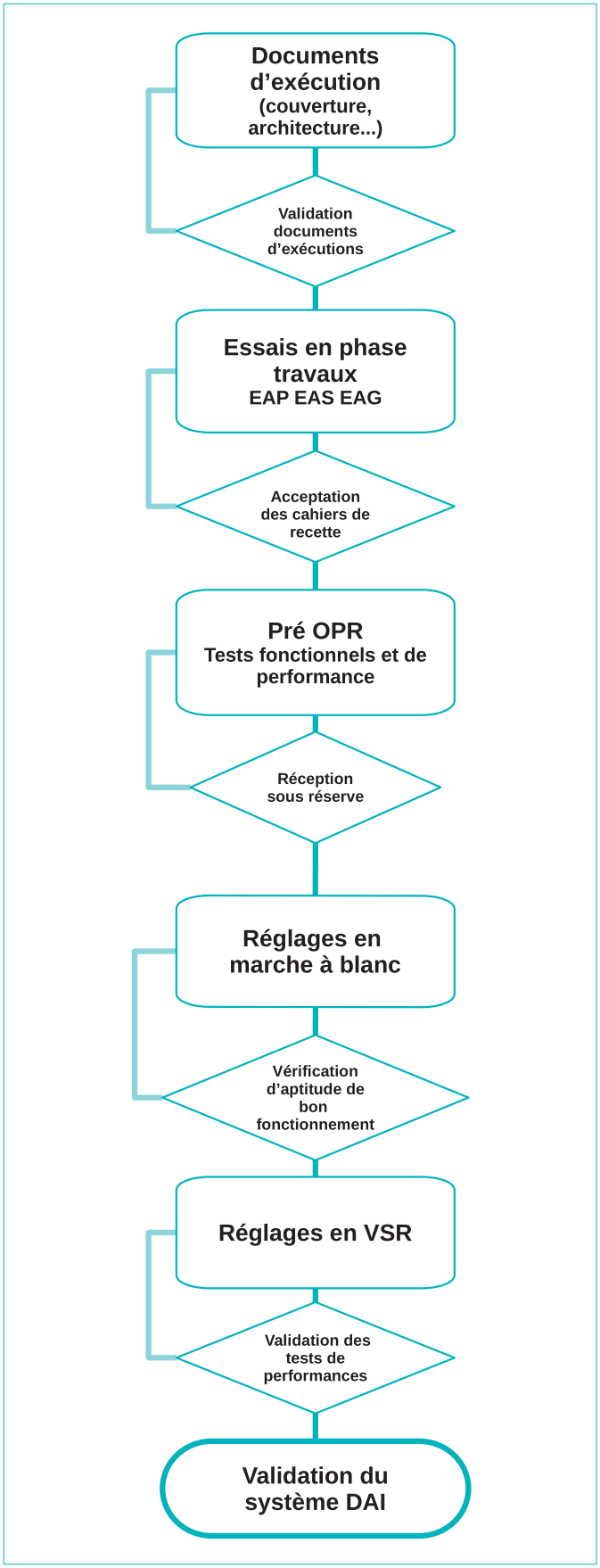



*Figure 13 : Étapes de validation du système de DAI*

9

# ACTIONS À MENER EN PHASE D'EXPLOITATION

## 9.1 GÉNÉRALITÉS

Le maintien de l'état et des performances des systèmes de DAI durant toute leur durée de vie est un enjeu majeur pour les exploitants de tunnels.

Une défaillance de cet équipement qui concourt à plusieurs fonctions de sécurité peut, pour certains ouvrages, entraîner un dépassement des conditions minimales d'exploitation et donc la fermeture du tunnel.

Une défaillance, ou une simple baisse des performances du système de DAI, peut aussi conduire à des situations critiques pour la sécurité des personnes, si un événement en principe détectable par la DAI n'est pas détecté.

La perte totale de la DAI est la plupart du temps facilement identifiable en exploitation courante.

Le retour d'expérience des tests menés depuis 2010 par le CETU, en particulier lors d'Inspections Détaillées Périodiques (IDP), a montré qu'une dégradation significative des performances de ce système peut, quant à elle, rester inconnue de l'exploitant très longtemps. Cette situation augmente le risque qu'un incident échappe à la vigilance de l'opérateur, retardant les actions rapides qui s'imposent dans cette situation.

Afin que ses utilisateurs gardent confiance en ce système au cours du temps, il est important de vérifier régulièrement, tout au long de sa vie, qu'il demeure en capacité de remplir ses fonctions en cas d'incident.

Les actions de vérification à mener comme indiqué dans la figure ci-dessous, sont détaillées dans les paragraphes 9.3 – Actions de maintenance et de contrôle et 9.4 – Inspections détaillées.

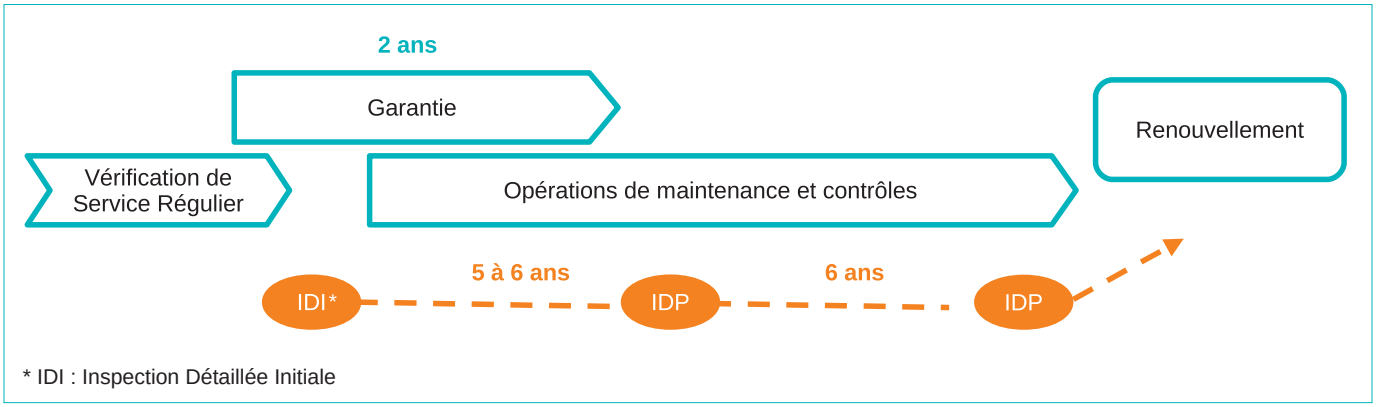



*Figure 14 : Synoptique des actions durant l'exploitation de l'installation*

## 9.2 GARANTIES

Le document *Équipements des tunnels routiers et de transports guidés urbains essais, réceptions et garantie* publié en juin 2019, donne dans son chapitre 5 des recommandations concernant les garanties contractuelles du marché de travaux. Le délai de garantie commence à courir dès la réception de l'installation.

On distingue les garanties réglementaires définies dans le CCAG Travaux, comme la garantie de parfait achèvement, et les garanties particulières qui peuvent être prévues dans le marché de travaux. À ce titre, il peut être prévu de prolonger les garanties des matériels de DAI : caméras, caissons, analyseurs, serveurs, logiciels… Sans dispositions particulières, ce matériel est couvert par la garantie légale de conformité portant sur les matériels et les produits numériques. Ces dispositions couvrent également la partie logicielle (cf. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043511875)

# 9.3 ACTIONS DE MAINTENANCE ET DE CONTRÔLE

## 9.3.1 Maintien des performances

L'objectif principal de la maintenance est de garantir la pérennité du système en évitant une dérive des performances au cours du temps.

Le maintien des performances repose sur le bon fonctionnement de chaque composant du système (caméras, analyseurs, logiciel de DAI…) ainsi que sur celui des équipements « support » (alimentation électrique, réseaux et supervision). Il est donc important de vérifier l'état et le bon fonctionnement de ces équipements.

Comme vu précédemment, les performances d'une DAI sont un compromis entre les détections (taux et temps de détection, non-détections) et les fausses alarmes. Pour maintenir un bon niveau de performance du système, il convient de veiller à ce que les niveaux de performance de ces paramètres interdépendants ne dérivent pas dans le temps.

L'augmentation de la fréquence de fausses alarmes est généralement facile à constater du fait de la nuisance occasionnée à l'opérateur dans l'exploitation courante d'un ouvrage. Par contre, seule la comparaison avec la réalité des événements sur le terrain permet de constater une dégradation de la capacité du système à détecter des incidents. Des non-détections peuvent être identifiées en exploitation courante, par confrontation avec des données issues d'autres systèmes tels que le RAU, les remontées d'état GTC (ouverture de porte de niche, d'issue, capteurs de pollution…), ou de la « main courante », voire le signalement d'un opérateur suite à la constatation visuelle d'un incident non détecté.

Toutes les non-détections ne pouvant être identifiées de cette façon, il est malgré tout nécessaire de simuler des incidents en intervenant spécifiquement dans l'ouvrage. La simulation d'incidents dans les tunnels est une opération qui demande, en plus des moyens humains et matériels, une fermeture de l'ouvrage pouvant s'avérer difficile à mettre en œuvre. Dans ce contexte, l'exploitation d'« incidents » générés dans le cadre de manœuvres d'exploitation courante, de travaux ou de maintenance peut être une alternative partielle intéressante. Par exemple, l'arrêt d'un patrouilleur pour une opération ponctuelle ou le balisage/débalisage peut être utilisé comme « incident » pour s'assurer que le système détecte bien un arrêt ou un contre-sens.

Pour optimiser l'exploitation de ces données, une traçabilité « au fil de l'eau » de tout incident survenu dans l'ouvrage, y compris les incidents d'exploitation courante (l'arrêt d'un patrouilleur par exemple) doit être mise en place.

Cette traçabilité permet, tout en minimisant la gêne à l'exploitation, de capitaliser un maximum d'« incidents » réels liés à la circulation des usagers, mais aussi aux actions de maintenance ou aux chantiers dans l'ouvrage et de constituer une base de données « d'incidents ». Pour qu'elle reste acceptée, crédible et pérenne, la mise en œuvre de cette traçabilité ne doit pas être trop lourde. Son niveau de détail et le temps imparti doivent être adaptés au contexte (nombre de tunnels exploités par le PCC par exemple), mais aussi en fonction des résultats des analyses.

## 9.3.2 Principes des maintenances corrective et préventive

Deux grands types de maintenance peuvent être distingués pour une installation de vidéo/DAI : la maintenance corrective et la maintenance préventive.

La maintenance corrective intervient lorsqu'un équipement devient inopinément défectueux. Afin de pouvoir rapidement pallier le problème d'indisponibilité de tout ou partie du système, un lot de pièces de rechange adapté à l'architecture de l'installation doit être prévu (voir l'annexe G1 – Lot de maintenance).

La maintenance préventive consiste en des opérations programmées d'entretien courant, de vérification, de tests, de remplacement des éléments matériels et des équipements « support », et de mises à jour des logiciels. Un exemple de programme de maintenance préventive est donné dans l'annexe G2. Il est rappelé qu'une maintenance préventive est à privilégier car cela permet de planifier les interventions et d'avoir des équipements en bon état de marche tout au long de leur durée de vie[29].

En outre, il convient de privilégier des vérifications « légères » mais fréquentes (quotidiennes, hebdomadaires, mensuelles), à des campagnes lourdes très espacées dans le temps (pluriannuelles) qui peuvent conduire à détecter tardivement les dérives du système.

Certaines de ces opérations de maintenance sur l'installation de vidéo/DAI peuvent être réalisées en régie pour les plus simples, les plus complexes pouvant être sous-traitées à des prestataires spécialisés. À noter que l'opportunité de l'ouverture d'accès à distance pour ces opérations doit être évaluée du point de vue des risques liés à la cybersécurité (voir paragraphe 7.1.5 – Modalités d'accès pour les opérations de maintenance).

29. L'annexe C du fascicule 40 *Tableaux des interventions de maintenance préventive* détaille les différentes interventions de maintenance préventive et les périodicités à mener sur les systèmes en tunnel.

## 9.3.3 Entretien courant et contrôle continu

L'entretien courant, premier niveau de la maintenance préventive, repose sur le nettoyage et la vérification périodique de l'état des équipements de prise de vue (niveau d'encrassement des vitres des caissons des caméras, non-mobilité des caissons…) et du réseau vidéo/DAI (état d'empoussièrement des serveurs, bonne ventilation des baies…).

Le contrôle continu du fonctionnement peut être réalisé en premier lieu grâce aux fonctions d'aide à la maintenance qui permettent de vérifier et de tester en permanence les états techniques des équipements concourant au système de DAI (cf. paragraphe 5.3 – Fonctions d'aide à la maintenance). Des alarmes techniques peuvent également être remontées sur l'Interface Homme-Machine (IHM) de supervision du tunnel. En outre, des vérifications visuelles du bon fonctionnement doivent être menées depuis les frontaux disponibles (contrôle de la présence de flux et de la qualité des images, vérification de la cohérence des masques de détection dans l'image…). Des connexions régulières avec les matériels permettent de contrôler les charges des processeurs, la mémoire utilisée, les espaces disques restants… et d'identifier des signes précurseurs de dysfonctionnements.

## 9.3.4 Audit des performances

Un audit des performances du système de vidéo/DAI, similaire à celui conduit pendant la VSR, permet d'objectiver le nombre de fausses alarmes – et donc la fréquence de fausses alarmes – et d'identifier, éventuellement, une problématique de non-détection.

L'analyse du journal des alarmes DAI permet de faire l'inventaire des vraies et des fausses alarmes. En visionnant les séquences relatives aux alarmes, leur classement (vraie, mal qualifiée ou fausse) et la connaissance de leur nombre peuvent être fiabilisés. La mise en place d'un suivi comparatif dans le temps permet également d'identifier des anomalies d'analyse pour certaines caméras.

La comparaison du journal des alarmes DAI avec l'inventaire des incidents issu des données de sources externes (main courante, données GTC…) permet d'alerter sur une problématique de non-détections.

Cet audit ne permet néanmoins pas de disposer de données suffisantes pour évaluer globalement la performance sur l'ensemble des caméras et des types de détection. La programmation d'essais spécifiques reste nécessaire.

*Figure 15 : Encrassement d'une vitre de caisson de caméra DAI*


*Figure 16 : Mauvaise qualité d'image issue d'une caméra dont la vitre de caisson est encrassée*


*Figure 17 : Flux vidéo d'une caméra ayant bougé (décalage des masques)*

### 9.3.5 Essais programmés

Des essais programmés doivent venir compléter les autres vérifications.

Tout d'abord, afin de vérifier régulièrement la capacité de détection d'un des premiers niveaux prioritaire d'incident, des tests de « véhicule arrêté » peuvent être réalisés dans des zones spécifiques de l'ouvrage (au droit des issues de secours ou des niches de sécurité par exemple). Il peut être opportun de mutualiser ce test avec d'autres opérations de maintenance menées périodiquement dans l'ouvrage. Par exemple, le stationnement d'un véhicule au droit d'un lieu où une tâche de maintenance récurrente est à réaliser peut représenter un « incident » permettant de vérifier régulièrement la fonction de détection. Le contrôle de la génération de l'alarme peut être fait en temps différé.

En outre, l'ensemble des fonctions de détection doit être vérifié lors de campagnes de tests de détection plus conséquentes. L'objectif est de simuler *in situ* tous les types d'incident, y compris ceux peu fréquents (incendie, contresens) et de vérifier la détection sur un échantillon représentatif de caméras sans toutefois être aussi complet que lors de la phase de réception initiale. La fonction de détection « véhicule arrêté » est, par exemple, testée une fois sur chaque caméra.

Ces vérifications de performance de la DAI doivent tenir compte de l'ensemble de la chaîne, qui inclut l'interface utilisée par l'opérateur, et ne pas se limiter à un examen du seul client DAI. En effet, il est courant de constater, lors des phases de maintenance, que les performances du système global sont inférieures à celles du système de DAI seul.

### 9.3.6 Maintenance logicielle

La maintenance logicielle consiste à réaliser :

- les opérations de purge de données, les mises à jour des versions de logiciels (mise à jour de sécurité des systèmes d'exploitation, des firmwares, des drivers…). Ces actions peuvent être réalisées en régie ou par un sous-traitant tiers ;
- des réglages fins des algorithmes suite à des constats de dérives de performances. Ces réglages sont implémentés sous forme de patchs. Il est recommandé de conclure un contrat de maintenance qui couvre ce volet de la maintenance. Ce contrat doit démarrer dès la fin de la période de garantie. Il est généralement conclu avec le fournisseur du système de DAI.

Lorsque les résultats des opérations de maintenance préventive (vérifications fonctionnelles, audit de performances, essais programmés) font apparaître des dysfonctionnements ou une dérive des performances, il convient de transmettre au titulaire du contrat de maintenance les données recueillies afin qu'il réalise des réglages et propose des mises à jour logicielles.

Ces mises à jour logicielles, en particulier sur les analyseurs, nécessitent des tests de non-régression. Ces opérations consistent à simuler quelques incidents *in situ* afin de s'assurer que des alarmes sont bien générées et qu'elles remontent toujours au niveau de l'opérateur. Si la configuration matérielle n'a pas évolué (pas de modification optique, pas de réorientation de caméras…), et si le système le permet, le rejeu d'images d'incidents sur les analyseurs peut servir pour la vérification de non-régression.

| Action de maintenance | Paramètre « évaluable » | Sources | Échantillon concerné |
|---|---|---|---|
| Audit de performances | Fréquence de fausses alarmes<br>Non-détection | « Incidents » identifiés en phase d'exploitation, chantier : journal d'alarmes DAI, sources externes (RAU, GTC…) | Quelques caméras et seulement les types d'incidents courants (véhicules arrêtés) |
| Essais programmés | Taux et temps de détection<br>Non-détection | « Incidents » simulés : journal d'alarmes | Toutes caméras et tout type de détection |

*Figure 18 : Paramètres évalués lors des opérations de maintenance et de contrôle*

## 9.4 INSPECTIONS DÉTAILLÉES

Selon les recommandations du Fascicule 40[30], des Inspections Détaillées Initiale (IDI) et Périodiques (IDP) des équipements doivent être réalisées par un organisme extérieur au gestionnaire pendant la vie de l'ouvrage.

Ces interventions sont complémentaires au contrôle continu réalisé par le gestionnaire.

L'IDI consiste à établir l'état de référence pour l'état et les performances des équipements. Elle concerne les installations neuves ou ayant bénéficié d'une rénovation substantielle. Cette intervention ne se substitue pas aux opérations de contrôle effectuées dans le cadre du marché de travaux (cf. paragraphe 8.3 – Études d'exécution). Ainsi, le retour d'expérience montre qu'il est préférable qu'elle se déroule

30. *Guide d'application de l'ITSEOA Fascicule 40 : Tunnels Génie civil et équipements*.

quelques mois après la mise en service pour que le fonctionnement du système soit stabilisé et les dernières levées de réserve aient été prononcées.

L'IDI se décompose en une analyse documentaire du Dossier des Ouvrages Exécutés complétée par une visite du tunnel, durant laquelle sont réalisés un examen de l'état des équipements, des essais fonctionnels et des mesures de performances similaires à ce qui est réalisé lors d'une IDP.

L'IDP, réalisée tous les six ans, comprend une visite du tunnel permettant d'obtenir un état des lieux ponctuel de l'état et des performances des équipements. Les opérations suivantes sont menées par les inspecteurs sur les systèmes vidéo et DAI :

- un contrôle visuel de l'état des équipements (caméras suspendues dans l'ouvrage, analyseurs et serveurs dans les locaux techniques, mur d'images au poste de contrôle-commande…) avec des moyens d'accès adaptés ;
- une vérification du fonctionnement du système (remontée d'alarme sur détection, affichage automatique des images sur moniteur, stockage et visionnage des séquences DAI…) ;
- des tests de performance (taux et temps de détection) sur quelques incidents faciles à simuler.

Pour la réalisation des tests de performances, plusieurs principes sont à prendre en compte :

- l'absence de coactivité – au moins dans les zones où sont réalisés les tests – est nécessaire, afin de ne pas perturber les résultats avec des « incidents parasites » ;
- la performance doit être examinée en prenant en compte la chaîne d'alerte dans son ensemble, en se plaçant dans les conditions réelles d'exploitation du système de DAI. Ainsi, les remontées d'alarme doivent être vérifiées sur l'interface utilisée par les opérateurs au quotidien avec la configuration d'exploitation courante, y compris les filtres appliqués (l'analyse des résultats doit les prendre en compte). Un inspecteur doit donc être présent au poste de contrôle-commande ;
- concernant l'échantillonnage (type de détection et emplacement), il convient de vérifier en priorité les fonctions de détection de niveau 1 (véhicule arrêté, incendie). Cela consiste à réaliser, au moins sur chaque caméra, un test pour chacune de ces fonctions et pour chaque voie.

Pour la fonction « véhicule arrêté », il peut être pertinent de réaliser les tests au droit des équipements destinés aux usagers (issues de secours, niches de sécurité).

De plus, il peut être intéressant de simuler les arrêts en fin de champ de caméra, avant l'apparition du véhicule dans le champ de la caméra suivante.

Les fonctions de détection des incidents de niveaux 2 et 3 les plus faciles à simuler doivent également être vérifiées sur quelques zones présentant un enjeu.

L'évaluation des équipements du tunnel fait partie intégrante du bilan des inspections détaillées, et est proposée au gestionnaire sous la forme d'une notation par famille. Selon les préconisations du fascicule 40, deux notes sont attribuées : une note « E » pour l'appréciation de l'état, et une autre, « P », pour celle du fonctionnement et de la performance.

Deux compléments littéraux permettent d'alerter sur des problématiques liées à la maintenabilité du système – mention « M » –, ou lorsque la sécurité est directement engagée – mention « S ».

Les problèmes de maintenabilité (mention « M ») couramment constatés sur le terrain sont liés entre autres à des dégradations de matériels (par exemple, système de réglage de l'orientation d'un caisson de caméra bloqué par la corrosion) ou à l'indisponibilité de pièces de rechange sur le marché (par exemple, indisponibilité de pièces de rechange pour des réseaux vidéo analogiques).

La sécurité (mention « S ») peut indifféremment être engagée par des désordres liés à l'état ou au fonctionnement d'un système. Citons notamment les risques de chute d'éléments suite à des chocs ou des dégradations provoquées par la corrosion de fixations (par exemple, corrosion caverneuse d'assemblages boulonnés) ou des performances très insuffisantes pour une fonction de détection de niveau 1.

Les résultats des inspections détaillées permettent à l'exploitant d'améliorer son programme de maintenance et alimentent sa réflexion dans le cadre de la programmation du renouvellement de l'installation.

Pour aller plus loin sur le sujet des inspections détaillées des équipements, le lecteur peut se référer aux documents suivants :

- « Annexe A – Contrôles et essais à réaliser lors d'une inspection détaillée initiale des équipements (hors contrôles de conception) » du fascicule 40 ;
- « Annexe D1 – Contrôles et essais à réaliser lors d'une inspection détaillée périodique des équipements » du fascicule 40 ;
- « Annexe D2 – Référentiel pour l'évaluation des équipements » du fascicule 40.

## 9.5 RENOUVELLEMENT ET RÉNOVATION

Le renouvellement est un remplacement complet de l'installation, tandis qu'une rénovation consiste à remplacer une partie seulement du système (conservation des supports, des caissons, des câbles, caméras, etc.).

Le renouvellement ou la rénovation du matériel ou du logiciel peuvent être déclenchés par différents signaux :

- lorsque la durée de vie du système est atteinte ou qu'il est devenu obsolète ;
- lorsque les informations remontées des IDP et des actions de maintenance montrent que l'état du système et ses performances sont trop fortement altérées.

Une piste pour réaliser des optimisations budgétaires et pour réduire les impacts environnementaux peut être de recourir à des rénovations partielles plutôt qu'à des renouvellements systématiques.

Il est rappelé que, avant toute intervention sur l'installation, il convient de s'interroger sur la nécessité qu'il y aura de vérifier ensuite la performance du système par des tests de détection dans l'ouvrage. Ces tests sont obligatoires lorsque ce sont des caméras ou des analyseurs qui sont renouvelés.

Le fascicule 40 indique des durées de vie type pour les principaux constituants d'un système de DAI. Ces données sont à relativiser au regard des retours d'expérience récents. Pour les caméras, par exemple, la durée de vie constatée est proche de 10 ans. Les logiciels quant à eux, peuvent être obsolètes au bout de 4 à 5 ans, les problématiques liées à la cybersécurité pouvant accélérer leur renouvellement.

| Équipements | Durées de vie type |
|---|---|
| Caméras | 10 ans |
| Écrans | 10 ans |
| Câbles | 30 ans |
| Logiciels | 10 ans - pouvant être obsolètes au bout de 4 à 5 ans |

*Figure 19 : Durées de vie type des équipements de DAI*

# 10 CONCLUSION

La détection automatique d'incidents par analyse d'images est le premier moyen de détection des incidents significatifs dans les tunnels routiers surveillés. Afin d'assurer leur exploitation en sécurité, il est donc indispensable de disposer d'un système de DAI fiable, performant et pérenne.

Pour permettre d'atteindre tous ces objectifs, le présent document comporte des informations et recommandations concernant toutes les phases de vie du système : conception, réalisation, réception et maintenance.

Au regard du retour d'expérience, certains points sont fondamentaux et méritent d'être soulignés.

Le choix des types d'incidents à détecter doit être effectué en fonction des enjeux de sécurité propres au tunnel étudié, en cherchant à en limiter le nombre. De même, les objectifs de performance à atteindre doivent être fixés en prenant en compte les spécificités de l'ouvrage.

En phase de conception, il est nécessaire de porter une attention particulière à la couverture vidéo complète de l'ouvrage, à la qualité des images, au choix des technologies de caméras et à l'architecture du système, qui conditionnent l'atteinte des performances.

En phase de réalisation, le système doit faire l'objet de réglages fins pour atteindre le meilleur compromis entre de bonnes performances de détection et la limitation du nombre de fausses alarmes. Les étapes progressives d'essai et de qualification doivent être scrupuleusement respectées.

En exploitation, il est indispensable de s'assurer que le système reste performant pour que les opérateurs conservent la confiance en cet équipement. Pour cela, il convient de mettre en œuvre des actions préventives régulières de maintenance, dont notamment des tests périodiques simples pour vérifier ses bonnes performances, et si nécessaire apporter des correctifs.

Enfin, la DAI étant un système d'information étendu et critique, il convient de s'assurer que la politique globale de cybersécurité et de sûreté de fonctionnement a bien été prise en compte durant toutes les phases précitées.

11

# LISTE D'ABRÉVIATIONS

| | |
|---|---|
| **ANSSI** | Agence Nationale de la Sécurité des Systèmes d'Information |
| **AMQ** | Alarmes Mal Qualifiées |
| **BAU** | Bande d'Arrêt d'Urgence |
| **CCAG** | Cahier des Clauses Administratives Générales |
| **DAI** | Détection Automatique d'Incidents par analyse d'images |
| **DMZ** | Demilitarized Zone |
| **DDM** | Délai de Détection Moyen |
| **FA** | Fausses Alarmes |
| **FFA** | Fréquence de Fausses Alarmes |
| **FFAG** | Fréquence de Fausses Alarmes Générales |
| **IA** | Intelligence Artificielle |
| **IDI** | Inspection Détaillée Initiale |
| **IDP** | Inspection Détaillée Périodique |
| **IP** | Internet Protocol |
| **IPSec** | Internet Protocol Security |
| **IT** | Instruction Technique |
| **GTC** | Gestion Technique Centralisée |
| **ND** | Non-Détection |
| **OPR** | Opérations Préalables à la Réception |
| **PCC** | Poste de Contrôle-Commande |
| **PSSI** | Politique de Sécurité des Systèmes d'Information |
| **RAU** | Réseau d'Appel d'Urgence |
| **RGPD** | Règlement Général sur la Protection des Données |
| **RSSI** | Responsable de la Sécurité des Systèmes d'Information |
| **SI** | Système d'Information |
| **TD** | Taux de Détection |
| **TDG** | Taux de Détection Générale |
| **TFA** | Taux de Fausses Alarmes |
| **TFAG** | Taux de Fausses Alarmes Générales |
| **VA** | Vraies Alarmes |
| **VABF** | Vérification d'Aptitude au Bon Fonctionnement |
| **VLAN** | Virtual Local Area Network |
| **VPN** | Virtual Private Network |
| **VSR** | Vérification de Service Régulier |

# A ANNEXE A CLASSIFICATION DES INCIDENTS À DÉTECTER

Pour rappel (cf. paragraphe 3.2 – Classification et choix des incidents à détecter), il convient de procéder à une sélection judicieuse du type d'incidents à détecter en fonction de leur gravité et de leur occurrence, de la capacité du système à pouvoir les détecter et de l'existence ou non, d'un moyen d'action en réponse à leur survenance.

## A.1 INCIDENTS DE NIVEAU 1

### A.1.1 Véhicule arrêté en trafic fluide

Le système de DAI doit détecter tout véhicule immobile, et cela en tout point de la chaussée ; les arrêts fugitifs, c'est-à-dire lorsqu'un véhicule s'arrête puis redémarre aussitôt, ne sont pas à prendre en compte.

### A.1.2 Incendie

Détection de perte de visibilité (apparition de fumées) : le système de DAI doit détecter une perte significative du niveau de contraste sur une partie significative de la surface de l'image.

Détection de flamme : le système de DAI doit détecter une flamme, et cela en tout point de l'image.

## A.2 INCIDENTS DE NIVEAU 2

### A.2.1 Congestion

Le système de DAI doit détecter un flot de véhicules circulant à faible vitesse ou proche de l'arrêt.

### A.2.2 Véhicule arrêté en situation de congestion

Le système de DAI doit détecter tout véhicule immobile dans une circulation congestionnée et cela en tout point de la chaussée ; cette fonction ne doit pas détecter les arrêts fugitifs liés à la congestion (lorsqu'un véhicule s'arrête puis redémarre aussitôt).

### A.2.3 Véhicule en contre-sens

Le système de DAI doit détecter un véhicule circulant en sens inverse de la circulation de la voie sur laquelle il est positionné.

### A.2.4 Piéton

Le système de DAI doit détecter un piéton se déplaçant sur la chaussée et/ou sur les trottoirs (en tout point) quelle que soit sa vitesse (marche, course) et sa trajectoire de déplacement (rectiligne ou non).

## A.3 INCIDENTS DE NIVEAU 3

### A.3.1 Objet

Le système de DAI doit détecter un objet immobile sur la chaussée pouvant provoquer un accident de véhicule. L'objet pouvant être de toute forme et toute taille, il est difficile de définir des caractéristiques minimales. À titre indicatif, les essais sont réalisés usuellement avec un cube d'arête 0,8 m, soit 0,5 m³.

Il est à noter qu'étant donné les faibles dimensions de l'objet, sa détection peut conditionner grandement la distance entre caméras. Si l'on souhaite détecter un objet en tout point de la chaussée, il convient de prévoir le calepinage en conséquence.

### A.3.2 Véhicule lent

Le système de DAI doit détecter comme lent tout véhicule roulant à une vitesse paramétrable (qui dépend de la vitesse réglementaire dans l'ouvrage) en tout point de la chaussée.

B

# ANNEXE B
# CAMÉRAS VISIBLES DONT LA SENSIBILITÉ EST ÉTENDUE DANS L'INFRAROUGE

En tunnel, du fait de la présence d'un l'éclairage artificiel permanent, des caméras sensibles dans le visible sont généralement utilisées.

Toutefois, l'utilisation de caméras dont le capteur est sensible à la fois dans le visible et dans le proche infrarouge (NIR) peut être envisagée dans certains cas particuliers.

Ces caméras pourraient par exemple être utilisées pour des ouvrages non éclairés et dans lesquels l'exploitant souhaite pouvoir détecter la présence de piétons.

Elles produisent de jour des images en couleur et de nuit des images en noir et blanc. Pour cela, elles comportent un filtre infrarouge amovible afin que la lumière infrarouge n'atteigne pas, de jour, le capteur. En effet, de jour, lorsque la lumière infrarouge passe à travers les trois filtres de couleurs (*Red Green Blue* – RGB, ou Rouge Vert Bleu RVB) du capteur, les informations relatives aux couleurs sont perdues et la caméra ne peut plus offrir une image en couleurs. Ce filtre est bien sûr paramétrable et automatique afin qu'il ne soit en place que sur une certaine plage horaire en journée et ainsi profiter de l'information couleur. Le reste du temps il n'est pas utilisé et seule une information en noir et blanc est fournie.

L'utilisation en mode NIR requiert généralement l'utilisation d'un illuminant infrarouge (IR) de type *Infrared Light Emitting Diode* (LED-IR). Cet illuminant est un moyen discret (car non visible par l'œil humain et donc l'usager), et à faible consommation d'énergie, de surveiller un tunnel dans le noir.

C

# ANNEXE C
# EXEMPLES DE TESTS DE MATÉRIELS ET DE FONCTIONS SUPPORT

Le tableau ci-dessous fournit des exemples de tests de matériels et de fonctions support pouvant être réalisés afin de s'assurer de leur bon fonctionnement au stade des essais et OPR (liste non exhaustive à compléter et à adapter au système installé).

Il est recommandé de procéder à ces vérifications depuis le client DAI local ou distant (PC maintenance, PC d'exploitation, PC de secours…).

| Tests | Actions à réaliser |
|---|---|
| Affichage sur serveur DAI | Démarrer le serveur DAI<br>Se connecter avec les différents profils utilisateurs.<br>Vérifier le bon démarrage des services DAI (analyse, administration, visualisation, enregistrement…).<br>Vérifier l'absence d'alarme technique. |
| Afficher les flux des caméras sur le client DAI | Vérifier que les flux vidéo de l'ensemble des caméras sont visibles sur l'interface DAI. |
| Contrôler la qualité des images | Vérifier visuellement la qualité de l'image provenant de chaque caméra, ainsi que la bonne incrustation de leur identification et de l'horodatage. |
| Tester la perte d'un flux vidéo | Vérifier que la perte d'un flux vidéo remonte bien à l'opérateur une alarme.<br>Vérifier que l'alarme disparaît lorsque le flux est de nouveau disponible. |
| Tester la communication entre analyseur et serveur | Vérifier que lors de la détection d'un incident, une alarme remonte bien à l'opérateur. |
| Tester la perte de la fonction d'analyse | Vérifier que la perte totale ou partielle de la fonction d'analyse remonte bien une alarme à l'opérateur.<br>Vérifier que l'alarme disparaît lorsque la fonction est de nouveau disponible. |
| Tester la perte du serveur | Vérifier que la perte du serveur remonte bien une alarme à l'opérateur.<br>Vérifier que l'alarme disparaît lorsque le serveur est de nouveau disponible. |
| Tester les fonctions de redondance | Vérifier que lors de la perte d'un analyseur, le basculement sur l'analyseur en secours s'opère et que la fonction d'analyse reste fonctionnelle.<br>Vérifier que lors de la perte du serveur maître, le basculement sur le serveur esclave s'opère et que le serveur est opérationnel. |
| Tester l'interaction avec les systèmes connexes | Vérifier la bonne communication entre système de DAI et supervision/GTC (remontées d'informations, passages de commande).<br>Vérifier que lors d'une remontée d'alarme DAI, le flux vidéo de la caméra concernée s'affiche sur l'écran dédié au PCC. |
| Tester le défaut « bougé caméra » | Vérifier que la modification de l'orientation d'une caméra remonte bien une alarme à l'opérateur. |
| Tester le défaut de dégradation de la qualité de l'image | Vérifier que la dégradation des images remonte bien une alarme à l'opérateur. |
| Tester les fonctions d'inhibition | Vérifier l'inhibition des fonctions de détection (par caméra, par zone, par type d'incident).<br>Vérifier le retour d'information d'inhibition à l'opérateur.<br>Vérifier le retour à l'état initial lorsque les fonctions de détection sont réactivées. |
| Tester les règles de filtrage | Vérifier les fonctions de filtrage des alarmes récurrentes. |
| Tester les fonctions d'enregistrement, d'archivage et d'export | Vérifier qu'une détection d'incident provoque bien l'enregistrement d'une séquence vidéo.<br>Vérifier l'archivage et la possibilité de relecture des séquences.<br>Vérifier la possibilité d'export de la séquence et/ou l'édition d'un rapport de détection. |

# D ANNEXE D
# DÉTAIL DES TESTS DES FONCTIONS DE DÉTECTION PAR INCIDENTS POUR LA QUALIFICATION D'UN SYSTÈME DE DAI

La phase de test des fonctions de détection par incidents pour la qualification d'un système de DAI est essentielle (voir paragraphe 8.5 – Essais spécifiques du système de DAI). Les moyens et le temps à consacrer à cette phase ne doivent pas être sous-estimés. Ils doivent être explicités dans le marché, pour chaque essai.

Le détail des tests à réaliser est successivement donné, dans les paragraphes qui suivent, pour chaque fonction de détection.

Les moyens destinés à assurer la sécurité des personnes et de l'infrastructure (extincteurs, EPI, etc) dont il faut disposer pour la réalisation de ces tests ne sont pas décrits dans ce document.

## D.1 TEST DE LA FONCTION DE DÉTECTION « VÉHICULE ARRÊTÉ »

| | |
|---|---|
| **Moyens requis** | Un véhicule léger de couleur blanche.<br>Un véhicule léger de couleur sombre. |
| **Procédure** | Un véhicule circule dans le tunnel à une vitesse supérieure à 30 km/h, avec arrêt dans la zone prévue selon le plan de tests.<br>Le véhicule doit rester à l'arrêt pendant une durée égale à 2 fois le temps de détection défini dans le marché.<br>Les feux de croisement et de position des véhicules utilisés devront être allumés et il faudra s'assurer que leurs feux stop fonctionnent. |
| **Nombre de tests conseillé** | Un arrêt est fait dans le champ de chaque caméra en début, milieu et fin de champ.<br>Un test est fait pour chaque véhicule, pour chacune des voies de circulation et le cas échéant pour la bande d'arrêt d'urgence (BAU) ou la bande dérasée droite (BDD).<br>Il est préférable de faire les tests plusieurs fois pour avoir un échantillon représentatif. Des tests doivent être réalisés au droit de chaque point singulier de l'ouvrage (niches de sécurité, issues de secours, garages). |
| **Résultat** | Le test est réussi si l'incident est détecté en un temps inférieur ou égal au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

## D.2 TEST DE LA FONCTION DE DÉTECTION « INCENDIE »

Pour la réalisation du test de détection d'incendie, trois méthodes peuvent être envisagées : la méthode par production de fumées froides, celle par production de fumées tièdes et celle par apparition de flamme.

Pour ce qui concerne les fumées :

- les fumées froides, plus faciles à produire, permettent par exemple de simuler une casse de moteur turbo de poids lourd. Il est assez facile d'obtenir des fumées froides de forte opacité, mais il est impossible de simuler les comportements de véritables fumées d'incendie (stratification par exemple) dictés par des effets thermiques ;
- les fumées tièdes sont plus représentatives des fumées réellement émises lors d'incendies en tunnel (écoulement, opacité), mais leur mise en œuvre nécessite des moyens plus lourds et certaines précautions.

Quelle que soit la méthode, pour les fumées, le retour d'expérience montre que la vitesse de courant d'air souhaitable pour la réalisation des essais doit être inférieure à 2 m/s si l'on dispose d'une seule machine à fumée.

Il faut s'assurer que le tunnel est doté de moyens permettant de respecter cette condition.

À défaut, des moyens complémentaires doivent être prévus, par exemple des générateurs de fumée multiples (ou de simples fumigènes) ou des ventilateurs portables permettant de contrôler le courant d'air.

Lors des tests de fumées, les démarrages automatiques du désenfumage doivent être inhibés afin de ne pas perturber les tests.

## D.2.1 Test de la détection d'incendie par production de fumées froides

| | |
|---|---|
| **Moyens requis** | Un générateur de fumée froide.<br>Un groupe électrogène ou les prises pompiers présentes dans les niches de sécurité.<br>Un véhicule porteur pour le déplacement du générateur. |
| **Procédure** | Deux méthodes peuvent être envisagées :<br>1) Le générateur de fumée est installé sur le véhicule porteur qui parcourt la totalité du tunnel sur une voie dans le sens du courant d'air avec une allure adaptée à la diffusion de la fumée (5 à 15 km/h environ).<br>À noter que, suivant les conditions de courant d'air naturel ou forcé, la propagation des fumées peut se faire sans déplacer le véhicule porteur.<br>2) Le générateur est alimenté depuis les prises pompiers ; il doit donc être déplacé de niche en niche afin de couvrir l'intégralité des caméras.<br>À noter que, suivant les conditions de courant d'air naturel ou forcé, la propagation des fumées peut se faire sans déplacer le dispositif. |
| **Nombre de tests conseillé** | Un test est fait dans le champ de chaque caméra.<br>Il est préférable de refaire trois fois le test de chaque caméra avec des positions différentes dans l'image pour avoir un échantillon représentatif. |
| **Résultat** | Le test est positif si l'incident est détecté en une durée inférieure au temps de détection défini dans le marché.<br>Calcul du taux de détection à la fin des différents tests. |

## D.2.2 Test de la détection d'incendie par production de fumées tièdes

| | |
|---|---|
| **Moyens requis** | Un bac à combustible permettant d'obtenir un départ de fumée assez rapide et suffisamment dense.<br>La préparation de ce bac exige des compétences spécifiques. Ce test est mis en œuvre par des professionnels formés et équipés. |
| **Procédure** | Arrêter la ventilation pendant le test.<br>Procéder à la mise à feu et ne pas stationner à proximité du nuage de fumée à cause de la nature irritante de la fumée émise.<br>Évacuer les fumées par la ventilation à la fin de chaque essai.<br>Positionner le bac à combustible sur la chaussée dans le champ de vision d'une caméra.<br>À noter que, suivant les conditions de courant d'air naturel ou forcé, la propagation des fumées pourra se faire sans déplacer le dispositif. |
| **Nombre de tests conseillé** | Du fait d'une mise en œuvre complexe, le nombre de tests sera défini au cas par cas. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure au temps de détection défini dans le marché.<br>Calcul du taux de détection à la fin des différents tests. |

## D.2.3 Test de la détection d'incendie par apparition de flammes

| | |
|---|---|
| **Moyens requis** | Un générateur de flammes.<br>Un extincteur (sécurité). |
| **Procédure** | Procéder à la mise à feu et ne pas stationner à proximité du générateur à cause de la chaleur générée.<br>Positionner le générateur de flammes sur la chaussée dans le champ de vision d'une caméra. |
| **Nombre de tests conseillé** | Un test est fait dans le champ de chaque caméra.<br>Il est préférable de refaire trois chaque test avec des positions différentes dans l'image pour avoir un échantillon représentatif. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure au temps de détection défini dans le marché.<br>Calcul du taux de détection à la fin des différents tests. |

## D.3 TEST DE LA FONCTION DE DÉTECTION DE CONGESTION

La mise en œuvre du test de détection de congestion est relativement contraignante en termes de moyens humains et matériels. Pour cette raison, il est recommandé de réaliser ce test en conditions réelles de circulation, en utilisant une situation de congestion survenant dans l'ouvrage durant la VSR.

Les feux de croisement et de position des véhicules utilisés doivent être allumés, ce qui est normalement le cas en exploitation réelle.

| | |
|---|---|
| **Moyens requis** | Plusieurs véhicules peuvent être mobilisés. Le nombre de véhicules et leur vitesse sont définies par le maître d'ouvrage en fonction des caractéristiques de l'ouvrage lors de la rédaction du marché. |
| **Procédure** | Un groupe de véhicules roule à une vitesse inférieure à la valeur paramétrée pour l'incident. |
| **Nombre de tests conseillé** | Un test est fait pour chacune des voies de circulation et la bande d'arrêt d'urgence (BAU) éventuelle.<br>Il est préférable de refaire plusieurs fois les tests pour avoir un échantillon représentatif. |
| **Résultat** | Le test est réussi si la congestion est détectée en une durée inférieure ou égale au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

## D.4 TEST DE LA FONCTION DE DÉTECTION D'UN VÉHICULE ARRÊTÉ EN SITUATION DE CONGESTION

La mise en œuvre d'un test de détection d'un véhicule arrêté en situation de congestion par arrêt volontaire d'un véhicule envoyé pour le test est déconseillée pour des raisons de sécurité (risque d'accrochage). La vérification du bon fonctionnement de cette fonction est à prévoir uniquement à l'occasion d'incidents survenus en conditions réelles de circulation durant la VSR.

## D.5 TEST DE LA FONCTION DE DÉTECTION D'UN VÉHICULE EN CONTRE-SENS

Pour le test de la fonction de détection d'un véhicule en contre-sens, comme pour les autres tests, les feux de croisement et de position des véhicules utilisés doivent être allumés.

| | |
|---|---|
| **Moyens requis** | Un véhicule léger de couleur blanche.<br>Un véhicule léger de couleur sombre. |
| **Procédure** | Le véhicule roule à contresens, à une vitesse comprise entre 30 km/h et la vitesse maximale autorisée dans le tunnel, sur toute la longueur du tunnel, sur la voie faisant l'objet du test.<br>Il est conseillé de faire les tests à la vitesse maximale autorisée en veillant à ce que les conditions de sécurité dans l'ouvrage soient garanties (absence de co-activité...).<br>Le test est fait pour chaque de véhicule et pour chacune des voies de circulation.<br>Le test est réussi si l'incident est détecté en une durée inférieure ou égale au temps de détection défini dans le marché. |
| **Nombre de tests conseillé** | Un test est fait pour chaque de véhicule, pour chacune des voies de circulation et la bande d'arrêt d'urgence (BAU) éventuelle.<br>Il est préférable de refaire plusieurs fois les tests à différentes vitesses pour avoir un échantillon représentatif. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

## D.6 TEST DE LA FONCTION DE DÉTECTION D'UN PIÉTON

| | |
|---|---|
| **Moyens requis** | Un piéton. |
| **Procédure** | Le piéton marche sans s'arrêter sur une voie de circulation pour laquelle la fonction est activée, et parcourt la totalité de l'ouvrage. |
| **Nombre de tests conseillé en réception** | Un test est fait pour chaque caméra et chaque voie sur lesquelles la fonction de détection est activée.<br>Le nombre de tests est égal au nombre de caméras participant à la détection multiplié par le nombre de voies de circulation sur lesquelles la fonction de détection d'un piéton est activée. La BAU (ou BDD selon les cas) et les trottoirs sont à considérer comme des voies de circulation à part entière.<br>Un test supplémentaire avec piéton ayant une trajectoire erratique est souhaitable. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure ou égale au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

## D.7 TEST DE LA FONCTION DE DÉTECTION D'UN OBJET

| | |
|---|---|
| **Moyens requis** | Deux objets d'un volume d'environ 0,5 m³.<br>Un objet de couleur claire.<br>Un objet de couleur sombre. |
| **Procédure** | L'objet doit rester dans le champ de la caméra pendant une durée de 2 fois le temps de détection défini dans le marché.<br>Le test est fait pour chaque caméra et chaque voie sur lesquelles la fonction de détection est activée. |
| **Nombre de tests conseillé** | Un test est fait dans le champ de chaque caméra en début, milieu et fin de champ.<br>Un test est fait pour chaque objet, pour chacune des voies de circulation et la bande d'arrêt d'urgence (BAU) éventuelle.<br>Il est préférable de refaire les tests plusieurs fois pour avoir un échantillon représentatif. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure ou égale au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

## D.8 TEST DE LA FONCTION DE DÉTECTION D'UN VÉHICULE LENT

Pour le test de la fonction de détection d'un véhicule lent, comme pour les autres tests, les feux de croisement et de position des véhicules utilisés doivent être allumés.

| | |
|---|---|
| **Moyens requis** | Un véhicule léger de couleur blanche.<br>Un véhicule léger de couleur sombre. |
| **Procédure** | Le véhicule roule à une vitesse inférieure à la valeur paramétrée pour l'incident, sur toute la longueur d'une voie.<br>Le test est fait sur chacune des voies de circulation et pour chaque véhicule. |
| **Nombre de tests conseillé** | Un test est fait pour chaque véhicule, pour chacune des voies de circulation et la bande d'arrêt d'urgence (BAU) éventuelle.<br>Il est préférable de refaire plusieurs fois les tests pour avoir un échantillon représentatif. |
| **Résultat** | Le test est réussi si l'incident est détecté en une durée inférieure ou égale au temps de détection défini dans le marché.<br>Calcul du taux de détection global pour la fonction de détection. |

# E ANNEXE E
# EXEMPLES DE FICHES DE RÉSULTAT DE TEST DES FONCTIONS DE DÉTECTION

| **Véhicule léger de couleur claire** | | | | | | |
|---|---|---|---|---|---|---|
| Date : | Heure : | | | Régime d'éclairage : | | Courant d'air (GTC) : |
| **TYPE DE DÉTECTION** | | | | | | |
| **SENS/TUBE** | | | | | | |
| **N° de test** | **N° de caméra** | **Résultat du test** | **Délai de détection(s)** | **Voie** | **Champ** | **Remarque** |
| 12 | 345 | 1 | 12 | Voie lente | Fin | |
| 13 | 346 | 0 | | Voie lente | Milieu | |
| 14 | 347 | 1 | 15 | Voie médiane | Début | |
| 15 | 348 | 1 | 13 | Voie médiane | Milieu | |
| 16 | 349 | 0 | | Voie rapide | Fin | |
| 17 | 350 | 1 | 25 | Voie rapide | Fin | |

Un exemple de fiche récapitulative des performances obtenues, établie à partir des tests réalisés, est donné ci-dessous.

| | | **Arrêt véhicule : récapitulatif général, toutes voies confondues** | | | |
|---|---|---|---|---|---|
| | | **Pourcentage demandé** | **Pourcentage de réussite** | **Temps de détection demandé en secondes** | **Temps moyen de détection en secondes** |
| **Nombre de tests** | 68 | 92,00 % | 100,00 % | 15 | 7,23 |
| **Nombre de résultats positifs obtenus** | 68 | | | | |

| | | **Piéton : récapitulatif général, tous trottoirs confondus** | | | |
|---|---|---|---|---|---|
| | | **Pourcentage demandé** | **Pourcentage de réussite** | **Temps de détection demandé en secondes** | **Temps moyen de détection en secondes** |
| **Nombre de tests** | 59 | 75,00 % | 93,22 % | 15 | 6,4 |
| **Nombre de résultats positifs obtenus** | 55 | | | | |

| | | **Véhicule lent : récapitulatif général** | | | |
|---|---|---|---|---|---|
| | | **Pourcentage demandé** | **Pourcentage de réussite** | **Temps de détection demandé en secondes** | **Temps moyen de détection en secondes** |
| **Nombre de tests** | 21 | 92,00 % | 71,43 % | 12 | 5,83 |
| **Nombre de résultats positifs obtenus** | 15 | | | | |

| | | **Incendie : récapitulatif général** | | | |
|---|---|---|---|---|---|
| | | **Pourcentage demandé** | **Pourcentage de réussite** | **Temps de détection demandé en secondes** | **Temps moyen de détection en secondes** |
| **Nombre de tests** | 33 | 80,00 % | 84,85 % | 15 | 6,46 |
| **Nombre de résultats positifs obtenus** | 28 | | | | |

F

# ANNEXE F
# ÉLÉMENTS D'INFORMATION CONCERNANT LA CYBERSÉCURITÉ

L'annexe explicite des concepts et mesures en complément du chapitre 7. Elle rappelle en particulier des notions fondamentales concernant la cybersécurité en tunnel routier (composantes de la sécurité, types de menaces, concept de défense en profondeur) et donne le détail des mesures de sécurité pouvant être mises en œuvre au niveau matériel et logiciel (authentification, protection des accès physiques, pare-feu, supervision et machines informatiques).

## F.1 COMPOSANTES DE LA SÉCURITÉ

### F.1.1 Présentation des composantes

La sécurité d'un Système d'Information (SI) est généralement considérée selon les quatre composantes que sont la disponibilité, l'intégrité, la confidentialité et la traçabilité.

Une illustration des enjeux que revêtent ces quatre composantes pour le cas particulier d'un système de DAI en tunnel est donnée ci-dessous à travers des exemples :

- disponibilité : le fonctionnement du système de DAI doit être protégé contre les défaillances, car cet outil est nécessaire à la détection précoce d'incidents dont l'évolution pourrait mettre en danger les utilisateurs de l'ouvrage ;
- intégrité : la falsification des données, ou la génération de faux incidents, peut masquer l'évolution de la situation ou conduire l'exploitant à mobiliser inutilement des moyens ;
- confidentialité : les images et séquences vidéo produites par le système contiennent des données personnelles. Elles ne peuvent être visualisées ou consultées que par des personnes spécifiquement et individuellement habilitées ;
- traçabilité : les accès au système, les consultations et extractions de données doivent être tracées.

### F.1.2 Types de menaces

On distingue quatre principaux types de motivations à l'origine des attaques portées aux SI :

- idéologiques : interruptions de service pour faire passer un message, détournement ou divulgation d'informations (exemple : attaque de l'État Islamique sur TV5 Monde, prise des sites web d'administrations françaises par Anonymous) ;
- financières : vols de données personnelles, bancaires ou stratégiques ; demandes de rançon pour que la victime puisse récupérer les données volées ou relancer l'activité du SI compromis ;
- pour espionnage d'État : écoutes, vol de données confidentielles ;
- pour espionnage industriel : vol de données et de codes sources.

Une grande majorité des attaques sur un SI sont portées en utilisant l'ingénierie sociale. Ce terme représente l'art de la manipulation des personnes en exploitant leur naïveté pour leur faire divulguer des informations permettant d'infiltrer le SI. La méthode la plus répandue est l'hameçonnage (*phishing*), consistant à envoyer un courriel demandant de cliquer sur un lien corrompu ou d'envoyer ses identifiants de connexion. D'autres moyens peuvent être employés lorsqu'un groupe d'attaquants dispose déjà d'informations (appels, SMS, lettres, applications web ou mobiles).

Ces dernières années, les attaques sur les systèmes d'information ont été très médiatisées, notamment celles visant les établissements de santé. Dans la plupart des cas, un rançongiciel (*ransomware*) crypte l'ensemble des données d'un SI et demande le paiement d'une rançon en cryptomonnaie pour décrypter les informations. Il ne faut jamais payer la rançon et il faut déposer plainte auprès de la Gendarmerie ou de la Police le plus vite possible afin d'entamer les procédures pour gérer la crise associée. D'autres démarches peuvent être mises en place, avec notamment l'aide de l'ANSSI.

Au-delà des rançongiciels, les chiffres sur les fuites de données (données de comptes utilisateur après vol des logins et mots de passe) démontrent l'ampleur de ce phénomène : 533 millions de comptes pour Facebook en 2022, 250 millions pour Microsoft en 2021.

L'arrivée de nouvelles technologies et de nouveaux usages informatiques devrait encore renforcer les besoins en cybersécurité du fait d'une surface d'exposition au risque encore plus grande : objets connectés, environnements Cloud, données massives (*big data*) et intelligence artificielle par apprentissage profond (*deep learning*) qui à elle seule génère une grande incertitude en termes de cybersécurité.

# F.2 DÉFENSE EN PROFONDEUR

La cyber-protection doit passer par différents niveaux de protection afin d'assurer une défense en profondeur ; cela signifie qu'il ne faut pas se contenter d'un seul élément de protection, mais superposer les mécanismes défensifs : si l'un échoue ou est contourné, un autre est encore présent pour déjouer l'attaque.

Au-delà des publications régulières de correctifs concernant l'exposition aux dernières menaces de cybersécurité sur les systèmes et équipements, des failles peuvent rester présentes.

La défense en profondeur ne doit pas être que logicielle : elle commence avec la protection des accès physiques aux matériels.

## F.2.1 Authentification

Il est indispensable que les équipements ne supportent que des protocoles et modalités d'accès suffisamment sécurisés. Bien sûr, les protocoles tels que telnet[31], HTTP[32], FTP[33] doivent être bannis (liste non-exhaustive), au profit de protocoles tels que SSH[34], HTTPS[35], SFTP[36] (liste non-exhaustive). De même, tout protocole ou dispositif de sécurisation ou chiffrement propre à un constructeur doit être banni : la sécurisation doit reposer sur des mécanismes connus, auditables, standardisés et surveillés par une large communauté.

Même si les flux sont protégés par une méthode de chiffrement, les simples identifications par mots de passe devraient également être évitées, au bénéfice d'une authentification par certificat[37] et si possible une authentification mutuelle. Celle-ci est nécessaire pour se prémunir contre les attaques d'interception dites *man in the middle* (type de cyberattaque où un attaquant parvient à s'introduire entre un expéditeur et un destinataire, en prenant notamment la main sur un équipement, par exemple un routeur Wi-Fi public, leur permettant de communiquer).

Tous les éléments d'authentification d'origine (certificats fournis par les constructeurs, mots de passe par défaut), pratiques pour tester les fonctionnalités des matériels et commencer les mises en services, doivent être remplacés par des éléments d'authentification établis et renouvelés selon la politique des identifiants définie par l'exploitant (longueur et contraintes de complexité des mots de passe, hiérarchie des certificats, fréquences de renouvellement…).

Il faut également être vigilant vis-à-vis des processus d'authentification qui seraient sécurisés dans le fonctionnement courant du système, mais qui pourraient se retrouver diminués ou dégradés (*downgradable*).

## F.2.2 Protection des accès physiques

La protection physique est généralement assurée pour le centre d'exploitation, sa salle informatique et les locaux techniques.

Sur une infrastructure étendue, il est illusoire de vouloir réaliser une protection contre les intrusions physiques de personnes décidées et préparées (équipées et entraînées). Néanmoins, il semble nécessaire de mettre en œuvre des moyens simples et peu coûteux qui permettent d'obtenir :

- un niveau de protection qui évite les intrusions de simples curieux ou des hackers en herbe qui n'ont pas forcément de compétences sur l'accès physique ;
- une remontée d'informations dans tous les cas d'accès : des procédures doivent être mises en place pour que le centre puisse décider si cet accès est potentiellement une intrusion, et prendre des mesures le cas échéant.

Tous les locaux et sites d'installation doivent donc d'une part être physiquement protégés, d'autre part être sous alarme pour que les intrusions physiques soient détectées avant que les intrus aient pu prendre la main sur les équipements et les systèmes de protection.

Cette protection ne s'applique pas seulement aux locaux de tête de tunnel qui abriteraient les nœuds de communication principaux, mais à tout site ou armoire de terrain contenant un équipement de communication. Une communication dans un VPN de type tunnel sécurisé (typiquement IPsec) peut permettre de ne pas faire peser cette contrainte sur les sites intermédiaires.

Une politique de sécurité des accès est indispensable pour l'ensemble du personnel exploitant : toujours demander l'identité d'une tierce personne sur site, privilégier si possible un accès par badges, interdire certaines pratiques (mots de passes visibles sur les bureaux, utilisation d'une clé USB non identifiée…).

---

31. Protocole de communication entre un client et un serveur, aujourd'hui obsolète.
32. *HyperText Transfer Protocol*, protocole de communication entre serveurs et navigateur web, autorisant le transfert de fichiers avec des informations d'authentification en clair.
33. *File Transfer Protocol*, protocole de transfert de fichier avec des informations d'authentification en clair.
34. *Secure SHell*, protocole de transmission sécurisée fonctionnant avec une interface de commande à distance.
35. *HyperText Transport Secure*, combinaison des protocoles HTTP et TLS – *Transport Layer Security*. Permet une navigation web avec un niveau accru de sécurité.
36. *Secure File Transfer Protocol*, protocole de transfert de fichiers permettant des communications sécurisées à un ordinateur distant.
37. Processus d'authentification entre un utilisateur et une ressource protégée. L'échange de ces certificats permet de disposer d'une sécurité accrue en comparaison d'une authentification par login et mot de passe. Ce processus nécessite l'implantation d'une autorité de certificat connectée à la ressource pour garantir la validité des certificats.

## F.2.3 Pare-feu

### Séparation des réseaux

Même si la sécurisation périmétrique ne fait pas tout et que les approches *Zero trust*[38] prennent une part croissante dans les architectures de sécurité, il faut créer un cloisonnement strict entre les différents réseaux : les réseaux terrain[39], le réseau fédérateur, les réseaux métiers du centre d'exploitation, le réseau bureautique et bien sûr Internet. Des pare-feux ne doivent laisser passer que les flux préalablement définis pour des utilisateurs identifiés. Seront exclus tous les flux entrants conduisant à une prise en main à distance qui ne passeraient pas par des machines de rebond spécifiques.

### Principe de filtrage

Outre les pare-feux interconnectant des réseaux, les fonctions de pare-feu (*netfilter* par exemple pour Linux, mais aussi le pare-feu de Windows) doivent également être activées sur tout équipement actif ; cela permet notamment de réduire la propagation des vers et virus.

Sur tous les pare-feux, la politique par défaut doit être l'abandon des paquets (*drop*).

Pour faciliter l'administration, l'écho ICMP[40] (commande « *ping* ») doit être honoré par tous les équipements :

- sur leur interface physique vers le centre de gestion (port RJ45), si on est sur un réseau privé ;
- ou seulement sur une interface virtuelle si la communication est matérialisée par un tunnel VPN.

Les autres ports et protocoles ne peuvent être ouverts qu'après validation du besoin. Le fabricant doit proposer la matrice des flux à ouvrir pour le bon fonctionnement du projet, et décrire le contenu des protocoles et leur dynamique. La matrice des flux doit être discutée avec la maîtrise d'œuvre et le RSSI de l'exploitant. Dans tous les cas, il faut exclure les protocoles non sécurisés ou présentant de potentielles vulnérabilités. Les protocoles d'administration et de supervision ne peuvent être ouverts que s'ils sont utilisés par l'exploitant, et uniquement avec des machines identifiées situées sur des réseaux internes du centre d'exploitation.

## F.2.4 Supervision

Pour connaître la disponibilité du système de DAI et de ses systèmes de support (alimentation et transmission), on gagne à les intégrer à une supervision. Tous les équipements de transmission peuvent être surveillés par le biais des protocoles SNMPv3[41] et ICMP. Tous les équipements de transmission doivent avoir la capacité de remonter les journaux d'activité (logs) vers un serveur de journalisation (exemple : syslog[42]) maîtrisé par l'exploitant et sur une zone réseau isolée (DMZ) attachée au pare-feu externe.

## F.2.5 Machines informatiques

### Serveurs

Sur les serveurs qui échangent des fichiers avec l'extérieur, au minimum un antivirus doit être installé. Pour élever le niveau de sécurité, l'ajout d'un logiciel de type *Endpoint Detection and Response* (EDR) est un atout non négligeable. Il permet un niveau de détection et de protection bien plus élevé que les antivirus « classiques » (il est aussi considéré comme un antivirus « 2.0 »).

### Postes opérateur

Sur tous les postes opérateur, un antivirus ou un EDR, ou même l'un et l'autre, sera installé.

Du point de vue de la cybersécurité, il est préférable que les postes permettant de réaliser les fonctions d'extraction et d'exploitation des données soient distincts du poste opérateur diffusant les alarmes de DAI en temps réel en salle opérationnelle.

Ces fonctions d'extraction et exploitation des données ne doivent être accessibles que localement, avec une identification sur des comptes dédiés à cet usage. La session doit se verrouiller automatiquement après un délai d'inactivité de l'opérateur.

De manière générale et même pour l'extraction de données, aucun périphérique ni accessoire (usb, cdrom…) fourni par un tiers ne doit être branché sur le poste de travail sans avoir été contrôlé par un antivirus externe (poste dédié ayant accès aux mises à jour, mais hors des réseaux d'exploitation).

### Droits d'accès aux équipements

L'administration directe des équipements à distance doit être interdite (pas de connexion *Secure SHell* – SSH en compte *root*[43] par exemple). Pour cette administration, plusieurs comptes utilisateurs spécifiques doivent être créés et auront eux seuls les droits d'escalade de privilège.

Tous les serveurs et postes doivent être pleinement maîtrisés par l'exploitant qui doit être le seul à en posséder les accès de super administrateur (*root*). Si d'autres personnes identifiées (installateur pendant la phase de VABF, mainteneur tiers…) doivent obtenir des accès privilégiés, des comptes dédiés leur sont attribués, mais l'exploitant doit conserver la maîtrise totale des machines : il doit en particulier pouvoir à tout moment en auditer la configuration. Il est recommandé de faire ces vérifications de conformité de configuration au moins à la mise en service puis périodiquement. On demandera également à l'éditeur de la solution de DAI les éléments de configurations relatif à la sécurité dans ses suites logicielles, pour pouvoir les vérifier.

38. Architecture *Zero trust* : stratégie considérant qu'aucune personne ou terminal n'est considéré comme fiable ou sécurisé dans un réseau informatique sans une vérification rigoureuse.
39. Cf. chapitre 7 – Cybersécurité et sûreté de fonctionnement.
40. *Internet Control Message Protocol*, protocole réseau permettant de requérir ou donner de l'information sur l'accessibilité d'une machine.
41. *Simple Network Management Protocol*, protocole de supervision réseau permettant de surveiller l'état de fonctionnement de tout élément actif d'un réseau informatique.
42. Protocole offrant un service de journalisation d'incidents sur un réseau informatique.
43. Utilisateur ayant tous les privilèges sur un système d'exploitation Linux, il en est donc l'administrateur du système.

G

# ANNEXE G
# MAINTENANCE

## G.1 LOT DE MAINTENANCE

La maintenance corrective intervient lorsqu'un équipement devient inopinément défectueux.

Afin de pouvoir pallier rapidement l'indisponibilité du système de DAI, un lot de pièces de rechange doit être prévu et disponible dès la mise en service.

Le contenu de ce lot et le nombre d'équipements est à adapter :

- à l'architecture du système de DAI ;
- aux éventuelles conditions minimales d'exploitation liées à la DAI.

Ce lot doit comprendre au moins :

- des caméras complètes (y compris optique) ;
- des caissons ;
- des supports pour caisson ;
- un lot de petit matériel de connexion (convertisseur de média, connectiques, alimentation *Power Over Ethernet* – POE…) ;
- …

Il faut prévoir une sauvegarde des configurations du logiciel de supervision et d'analyse lors de la mise en service pour permettre une réinstallation rapide en cas de problème serveur.

## G.2 EXEMPLE D'UN PROGRAMME DE MAINTENANCE

Un exemple de programme de maintenance préventive est donné ci-dessous. Le contenu et la fréquence des tâches à mener est à adapter en fonction des spécificités de l'ouvrage et des conditions d'exploitation.

| Type | Tâches | Lieu | Fréquence |
|---|---|---|---|
| **Entretien courant / contrôle continu** | Connexion sur les serveurs DAI | Depuis le PCC ou le local technique, sans fermeture de l'ouvrage | Quotidienne / hebdomadaire |
| | Vérification de la charge des processeurs, de la mémoire utilisée, des espaces disque restants… | | |
| | Contrôle du flux et de la qualité des images | | |
| | Test de détection d'arrêt dans les garages | Dans l'ouvrage sans fermeture | |
| **Entretien courant / contrôle continu** | Vérification du niveau d'encrassement des vitres des caméras | Depuis le PCC ou le local technique, sans fermeture de l'ouvrage | Mensuelle / trimestrielle |
| | Vérification de la cohérence des masques de détection dans l'image (obligatoire après chaque lavage des caméras) | | |
| **Essais programmés « sommaires »** | Test de détection d'arrêt devant les niches / les issues | Dans l'ouvrage avec fermeture ou neutralisation de voie | |
| **Entretien courant** | Nettoyage du système de prise de vue (caisson, vitres…) | Dans l'ouvrage avec fermeture ou neutralisation de voie | Trimestrielle / semestrielle / annuelle |
| **Audit de performance** | Qualification des alarmes sur une période de x jours continus | Depuis le PCC ou le local technique, sans fermeture de l'ouvrage | Semestrielle / annuelle |
| | Analyse des logs techniques sur une période de x jours continus | | |
| | Comparaison du journal des alarmes DAI à des données de source externe à la DAI | | |
| | Suivi comparatif entre années | | |
| **Vérifications programmées « exhaustives »** | Campagne de tests de détection « exhaustive » | Dans l'ouvrage sous fermeture et depuis le PCC | Annuelle |
| **Inspection détaillée** | Examen de l'état des équipements | Dans l'ouvrage sous fermeture et depuis le PCC | Tous les 6 ans |
| | Tests de détection *in situ* | | |

Pour rappel, il convient de garder à l'esprit que :

- un système de DAI est un équipement sensible qui « dérive » dans le temps ;
- il faut privilégier des actions légères mais régulières ;
- il est possible de mutualiser les tests avec d'autres opérations de maintenance ou événements d'exploitation (y compris en phase chantier) ;
- il est important de mettre en place une traçabilité des résultats des opérations de maintenance mises en place.

## G.3 EXEMPLE D'UNE FICHE DE RÉSULTATS DE TESTS D'UNE CAMPAGNE « EXHAUSTIVE »

jeu. 28 octobre 2021

OK NOK

| STOP En fluide | CAM-2 | CAM-1 | CAM-3 | CAM-4 | CAM-5 | CAM-6 | CAM-7 | CAM-8 | CAM-9 | CAM-10 | CAM-11 | CAM-12 | CAM-13 | CAM-14 | CAM-15 | CAM-16 | CAM-17 | CAM-18 | CAM-19 | CAM-20 | 100 % | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VL Pied Champ | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 0 | 0 |
| VL Fond Champ | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | 20 | 0 |
| VR Pied Champ | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | 20 | 0 |
| VR Fond Champ | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 0 | 0 |

| Débris / Objet sur chaussée | CAM-2 | CAM-1 | CAM-3 | CAM-4 | CAM-5 | CAM-6 | CAM-7 | CAM-8 | CAM-9 | CAM-10 | CAM-11 | CAM-12 | CAM-13 | CAM-14 | CAM-15 | CAM-16 | CAM-17 | CAM-18 | CAM-19 | CAM-20 | 75 % | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Voie rapide | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 0 | 0 |
| VL sous éclairage Jour+Nuit+Nuit réduit | NOK | OK | OK | OK | Veh lent | Veh lent | NOK | NOK | Veh lent | OK | OK | Veh lent | OK | OK | OK | OK | OK | OK | NOK | OK | 12 | 4 |
| VL sous éclairage Nuit réduit | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 0 | 0 |

| Contre-sens | CAM-2 | CAM-1 | CAM-3 | CAM-4 | CAM-5 | CAM-6 | CAM-7 | CAM-8 | CAM-9 | CAM-10 | CAM-11 | CAM-12 | CAM-13 | CAM-14 | CAM-15 | CAM-16 | CAM-17 | CAM-18 | CAM-19 | CAM-20 | 55 % | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Voie rapide à 70 km/h | NOK | OK | NOK | OK | NOK | NOK | OK | OK | OK | OK | NOK | NOK | NOK | NOK | OK | OK | OK | NOK | NOK | OK | 10 | 10 |
| Voie lente à 70 km/h | NOK | OK | OK | OK | OK | OK | OK | NOK | OK | OK | OK | OK | NOK | NOK | OK | NOK | OK | NOK | NOK | NOK | 12 | 8 |

| Piéton | CAM-2 | CAM-1 | CAM-3 | CAM-4 | CAM-5 | CAM-6 | CAM-7 | CAM-8 | CAM-9 | CAM-10 | CAM-11 | CAM-12 | CAM-13 | CAM-14 | CAM-15 | CAM-16 | CAM-17 | CAM-18 | CAM-19 | CAM-20 | 80 % | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| à droite côté VL | OK | OK | OK | NOK | NOK | OK | OK | NOK | OK | OK | NOK | OK | NOK | NOK | OK | OK | OK | OK | OK | OK | 14 | 6 |
| à gauche côté VR | OK | OK | OK | OK | OK | OK | OK | NOK | OK | OK | OK | OK | OK | OK | NOK | OK | OK | OK | OK | OK | 18 | 2 |

| Visibilité | CAM-2 | CAM-1 | CAM-3 | CAM-4 | CAM-5 | CAM-6 | CAM-7 | CAM-8 | CAM-9 | CAM-10 | CAM-11 | CAM-12 | CAM-13 | CAM-14 | CAM-15 | CAM-16 | CAM-17 | CAM-18 | CAM-19 | CAM-20 | 89 % | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Visibil désact | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | OK | NOK | Visibil désact | NOK | 16 | 2 |

* VL : Voie Lente VR : Voie Rapide

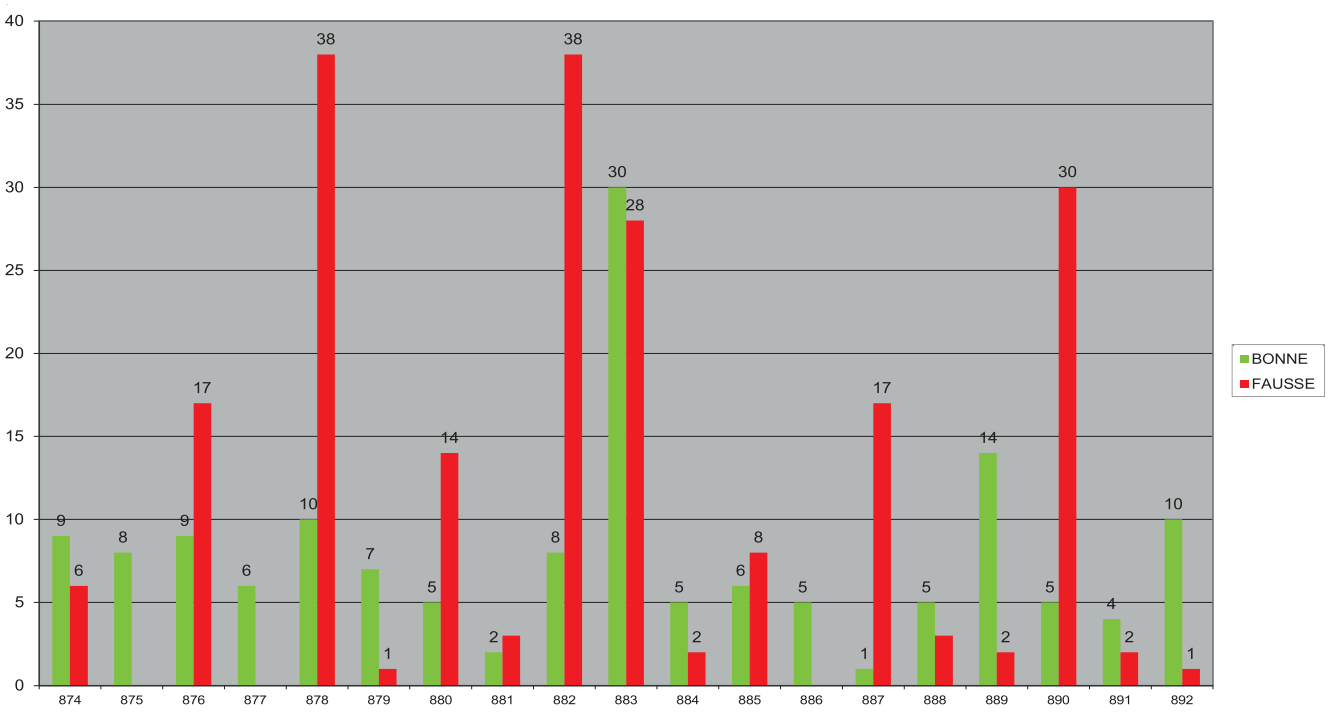
Illustration : © DIR centre-est

Le tableau ci-dessus trace les résultats obtenus lors d'une campagne annuelle de tests « exhaustifs ».
Dans cet exemple, un test a été réalisé pour chaque type d'incident à détecter, sur chaque caméra et dans chaque zone d'intérêt (voie lente, voie rapide, trottoirs, BAU…). Les alarmes mal qualifiées ont été comptabilisées comme des vraies alarmes.

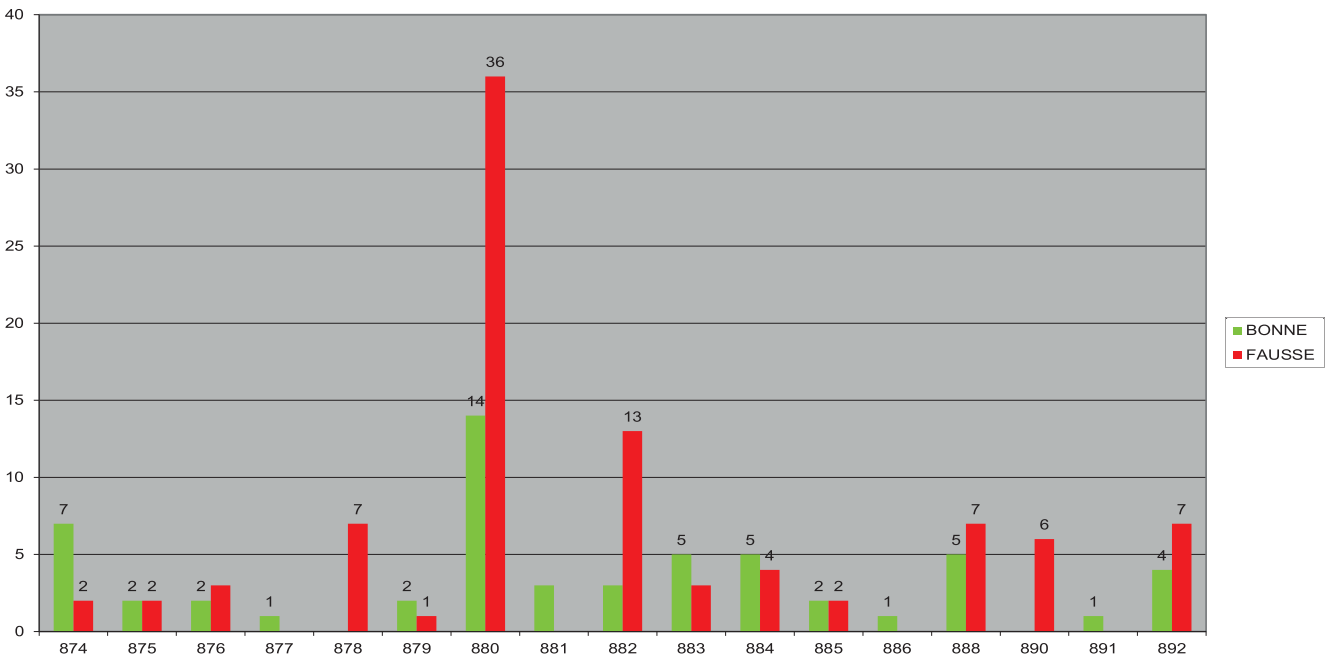
La dernière colonne indique le taux de détection déterminé par type d'incident à détecter.

Suite à cette campagne, les résultats obtenus ont été transmis au fabricant afin d'engager des actions correctives.

## G.4 EXEMPLE D'UNE FICHE DE SUIVI COMPARATIF




*Qualification des alarmes – année n-1 (© AREA)*




*Qualification des alarmes – année n (© AREA)*

Les diagrammes ci-dessus illustrent l'analyse par caméra des vraies et fausses alarmes collectées sur une période donnée. Plusieurs analyses peuvent être menées pour constater des dysfonctionnements ou dérives : ratio fausse / bonne alarme, dérive globale entre deux périodes, dysfonctionnement d'une caméra particulière en comparaison aux autres…

**GROUPE DE RÉDACTION**

Christophe BANOS (CETU), Séverine BESSON (CETU), Jérémie BOSSU (Cerema), Christophe CARNISI (CETU), Éric CHARLES (CETU), Florian FRANDIDIER (Cerema), Pierre-Yves TANNIOU (Cerema).

**REMERCIEMENTS**

Sont remerciés pour leur relecture les exploitants (DiRIF, Vinci Autoroutes, ASFA), fournisseurs (Sprinx Ai, Cyclope Ai, Citilog, Flir) et bureaux d'études (Setec, Egis).

Crédits photos : couverture Arnaud BOUISSOU (Terra), intérieur CETU - Rédaction et coordination : collaborateurs CETU - Réalisation : PAO Concept - Impression : VASSEL GRAPHIQUE

**Centre d'Études des Tunnels**

25 avenue François Mitterrand
69500 BRON - FRANCE
Tél. +33 (0)1 40 81 30 30
cetu@developpement-durable.gouv.fr

MINISTÈRE
DES TRANSPORTS
*Liberté*
*Égalité*
*Fraternité*

CETU

*www.cetu.developpement-durable.gouv.fr*