Livre blanc - 2015

Télévidéosurveillance

UNION DES ENTREPRISES
usp
DE SÉCURITÉ PRIVÉE
TECHNOLOGIES

Préambule

Qualification des risques

La détection

Traitement au PC

Intervention

Conclusion

Préambule

Remerciements aux contributeurs du présent ouvrage

- M. Stéphane **BIDAULT** - TEB
- M. Vincent **BONNARD** - Securitas Réponse
- M. Serge **CAILLET** - Groupe Scutum
- M. Edouard **CHÂTEAU** - Groupe ADEC
- M. Christophe **COUTURIER** - Eurofeu Technologies
- M. Philippe **DEBAYE** - Axis Communications
- M. Pascal **DEBOUT** - TEB
- M. Alain **DELCROIX** - AXA Corporate Solutions
- M. Jean-Baptiste **DUCATEZ** - Foxstream
- M. Rémi **FARGETTE** - AN2V
- M. Patrick **LAUNAY** - Groupe Scutum
- M. Garry **GOLDENBERG** - Open-IPVideo
- M. Dominique **LEGRAND** - AN2V
- M. Thibault du **MANOIR de JUAYE** - Avocat à la cour
- M. Ivan **MARCIANO** - Groupe ITQ
- M. Raphaël **MAURO** - GIP2 - EPSITRONIC
- M. Claude **NERI** - ESI
- M. Christophe **ROMAIN** - Securitas Mobile
- M. Claude **TARLET** - Président de l'USP
- M. Francis **SERRANO** - Securitas Technologie
- M. Eric **VANDER-MAELEN** - Securitas Technologie
- M. Frédéric **VIAL** - ONET Sécurité
- M. Olivier **WEBER** - Groupe Scutum

« Nous avons un devoir : réussir ! »

Cette édition 2015 du Livre Blanc de la télévidéosurveillance constitue un nouveau marqueur dans l'évolution de la profession.

Le paysage se modifie, les acteurs se rassemblent, la sécurité privée est au cœur du débat sur les équilibres de la sécurité intérieure du pays.

Tout montre une prise de conscience des enjeux.
Le développement des technologies nouvelles, l'explosion des réseaux de communication, la globalisation et la convergence des solutions ouvertes par les télécommunications et l'informatique font naître un nouveau monde qui bouleverse les esprits et les rites culturels.

Notre véritable défi est celui de l'opinion publique. Elle vit avec angoisse ces mutations car elle craint pour sa liberté. Mais elle perçoit aussi l'espoir que l'évolution de l'offre fait naître pour garantir, dans sa vie quotidienne, sa tranquillité.

Dans un environnement incertain et fragilisé par de nombreuses interrogations politiques et économiques, seule une ambition collective peut conduire au succès et à la création de valeur.

USP-TECHNOLOGIES est engagée dans cette démarche et, par sa participation active aux évolutions du marché, apporte une contribution innovante au développement de la filière rassemblée au sein de l'Alliance nationale des entreprises de sécurité privée.
Une Alliance née pour porter un message, produire des idées et créer la synergie entre les métiers. Une Alliance porteuse d'avenir et de dialogue avec la puissance publique.

C'est, aussi, dans un échange transparent avec le CNAPS, que doivent se dessiner, maintenant, les pistes de progrès pour que les objectifs soient atteints et ressentis par les opérateurs comme utiles.
Nous avons un devoir : réussir !

Claude TARLET - Président de l'USP

L'arrivée du numérique a en quelques années seulement, profondément bouleversé le monde de la sécurité des personnes, des biens et de l'information.

Le numérique impose l'ère de la multitude ; il redessine les chaînes de valeur, les limites d'intervention des acteurs. Il invente de nouveaux métiers.

Dans cet environnement où les frontières se redessinent, la profession regroupée au sein de l'USP-Technologies propose un livre blanc pour ouvrir le débat sans tabou.

En pleine mutation, elle propose les pistes nécessaires pour une maturité assumée, pour garantir sécurité et qualité aux marchés.

Les thèmes essentiels tels que compétence, technologie, convergence « privé-public », ou défense des libertés individuelles et publiques sont abordés sans tabou pour éclairer l'ensemble des acteurs et ainsi formuler des propositions pragmatiques.
Enrichie, retravaillée, cette nouvelle version délivre des propositions efficaces pour la profession.

Outil de référence en matière de télévidéosurveillance, il dessine aujourd'hui le métier de demain. Une chaîne de valeurs non pas pour des métiers isolés et juxtaposés, mais pour un métier intégré : l'intégration de sécurité.

Par son engagement au cœur de la convergence homme-technologie, l'USP-Technologies contribue activement à la professionnalisation et la reconnaissance de l'intégration des métiers technologiques de la sécurité. En s'imposant comme le lieu d'échange et de faire savoir entre les constructeurs, les intégrateurs et les utilisateurs, l'USP-Technologies vulgarise les innovations technologiques au service de la qualité de la sécurité.

Stéphane BIDAULT, Président de l'USP-Technologies,
Président de TEB vidéoprotection

Quels sont les objectifs de la télévidéosurveillance ?

Depuis son origine, la télésurveillance s'est positionnée au cœur de la chaîne de sécurité. En amont, il y a la détection des évènements, la transmission des alarmes. En aval, il y a les contacts Clients, les professionnels de l'intervention et les forces de l'ordre.

Contrairement à l'auto surveillance, la télévidéosurveillance réalisée par des professionnels de la sécurité reconnus et formés, apporte toutes les garanties qu'une action appropriée sera déployée suite aux déclenchements d'alarmes, que les systèmes seront supervisés. La réglementation et les diverses certifications métier assurent au Client une parfaite traçabilité des actions du télésurveilleur.

Deux configurations «juridiques» existent : l'installateur est télésurveilleur, ou il y a un installateur plus un télésurveilleur.

- L'installateur est télésurveilleur : sa responsabilité peut être engagée à 100% en cas de sinistre responsable,
- L'installateur et le télésurveilleur sont juridiquement dissociés : Il peut y avoir partage des responsabilités en cas de sinistre,
- Dans tous les cas, l'installateur a une obligation de conseil qui lui impose d'apporter toutes les informations nécessaires sur la réglementation en vigueur sur la nature des lieux à traiter.

Quelle est la nature des lieux traités ?

La France est l'un des pays dans lequel l'usage de la vidéoprotection est le plus réglementé. C'est aussi l'un des pays où la réglementation est la plus restrictive. L'installation de vidéoprotection n'est pas libre, et quel que soit le lieu dans lequel elle est installée, il y a des règles à respecter, y compris dans un domicile, lieu pourtant strictement privé.

La nature du lieu à traiter est le critère le plus important de notre réglementation. En effet, les règles applicables à un dispositif ne sont pas les mêmes en fonction des différents types de lieux.

Rappelons qu'il existe trois grands types de lieux :

- **La voie publique :** qui est constituée de tous les espaces publics, ceux qui appartiennent à la collectivité et dans lesquels on peut habituellement circuler librement, à n'importe quelle heure du jour et de la nuit.

- **Les lieux privés ouverts au public :** au sens de la jurisprudence des juridictions de l'ordre judiciaire, est un lieu ouvert au public « un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions » (TGI de Paris, 23 octobre 1986, Gaz. Pal. du 8 janvier 1987, confirmé par un arrêt de la Cour d'appel de Paris du 19 novembre 1986). Ce sont des lieux qui peuvent être fermés à un moment quelconque de la journée, mais qui accueillent du public durant leur ouverture. Par exemple on trouvera ici un musée, un centre commercial ou le hall d'une mairie.

- **Les lieux strictement privés :** un lieu devient privé dès lors qu'un contrôle quelconque est mis en place aux accès : contrôle d'accès automatique, accueil avec présentation de papiers d'identité, digicode, visiophone… Un domicile entre donc logiquement dans cette dernière catégorie. La différence avec un lieu ouvert au public (où un contrôle peut être effectué à l'entrée) est la fréquentation. Attention ! Pour qu'un espace extérieur puisse être considéré comme strictement privé, les tribunaux exigent que l'espace soit clôturé, avec un portillon équipé d'un dispositif de fermeture. Une maison abritant à la fois des locaux privés et des locaux à usage professionnel peut être concernée par plusieurs régimes juridiques différents. Pour un lieu de travail, si l'endroit dans lequel la vidéoprotection est déployée est occupé par des salariés, alors le droit du travail s'applique.

Le droit de la vidéoprotection

La réglementation de la vidéoprotection est assez complexe car elle repose sur plusieurs ensembles de textes et notamment :

- Les textes protégeant l'image et la vie privée : code civil, code pénal, code du travail…
- Le code de sécurité intérieure, qui regroupe aujourd'hui tous les textes réglementant la vidéoprotection sur la voie publique ou dans les lieux privés ouverts au public, et imposant une autorisation préfectorale,
- La réglementation propre aux sociétés de vidéoprotection, dont l'activité relève de celles soumises à la tutelle du CNAPS,
- Les dispositions de la loi de 1978 « Informatique et libertés », qui s'applique à certains lieux ou à certains types de dispositifs de vidéoprotection.

Pour définir quels sont les textes qui s'appliquent à l'espace qui doit être vidéo protégé, il est impératif de se poser plusieurs questions successives :

- Quelle est la nature du lieu à vidéo protéger ?
- Quelles sont les finalités du dispositif ?
- Quelle est la nature du dispositif installé ?

Le critère de la nature du lieu de l'installation

Le critère principal permettant de définir le ou les régimes juridiques s'appliquant à l'espace devant être vidéo protégé est la nature du lieu vidéo protégé. Au sens de la réglementation de la vidéoprotection, on distingue trois types de lieux :

- Les lieux publics
- Les lieux privés
- Les lieux ouverts au public

Il faut être très attentif à cette question, car une installation sans autorisation d'un système de vidéoprotection dans un espace public ou ouvert au public est un délit. On rappellera donc très sommairement comment distinguer ces trois espaces :

Lieu public

Un lieu public est un lieu où quiconque peut accéder librement à tout moment : une rue, une place…

Lieu ouvert au public

Un lieu privé ouvert au public est un lieu où l'on peut accéder librement, mais avec certaines restrictions : fermeture au public à certaines heures par exemple. C'est le cas de tous les commerces, d'une bibliothèque, de l'espace d'accueil d'un service public en général.

La circulaire du 14 septembre 2011 a défini ainsi les lieux ouverts au public :

« Constituent des lieux ouverts au public, les lieux dont l'accès est libre (plages, jardins publics, promenades publiques, commerces, etc.) ainsi que les lieux dont l'accès est possible, même sous condition, dans la mesure où toute personne qui le souhaite peut remplir cette condition (paiement d'un droit d'entrée, par exemple au cinéma) ». Les tribunaux ont posé des définitions quasi-identiques.

Il existe d'ailleurs une anecdote amusante sur Bernard Tapie, qui avait attaqué un journal qui avait publié une image de lieu le montrant dépité (on le comprend) dans sa cellule de la prison de la Santé. Le support de presse pour sa défense soutenait que la prison était un bâtiment public et donc que les photos étaient autorisées. Non sans humour la justice devait lui donner tort en expliquant qu'une prison n'était pas un lieu où l'on sort et où l'on rentre

comme on veut et que dès lors elle s'apparentait à un lieu privé.
Une autre décision de justice illustre bien cette notion de vie privée dans une pharmacie : la zone de chalandise où évoluent les clients est considérée comme un lieu public, alors que les zones de réserve sont considérées comme des lieux privés : « la ligne de démarcation » est matérialisée par le comptoir. Il existe une passerelle entre lieu public et lieu privé, puisqu'une entreprise peut filmer ses abords immédiats en cas de menace terroriste ou lorsqu'il y a un risque de délinquance majeur (Article L. 251-2 du Code de la sécurité intérieure). Mais, le visionnage des images est limité aux agents de l'autorité publique, sous peine de sanctions pénales. Par ailleurs, les caméras surveillant la voie publique ne doivent pas être interconnectées avec celles installées à l'intérieur du lieu ouvert au public de manière à ce que le responsable ou ses subordonnés ne puissent avoir accès aux images enregistrées par la ou les caméras extérieures (Décret n°2015-489 du 29 avril 2015 - art. 3).

Lieu privé

Un lieu privé est un lieu dont l'accès est filtré par des moyens humains ou technologiques : hôtesse d'accueil, contrôle d'accès… Toutefois, il peut exister un filtrage sans que pour autant l'espace situé après le contrôle soit considéré comme privé. Par exemple une salle de concert, à laquelle on accède avec un billet et après une éventuelle palpation de sécurité et/ou une inspection visuelle des sacs.

Une réglementation spécifique pour chaque type de lieu

Lieux publics, ou lieux ouverts au public :

Il résulte des articles R251-1 à R253-4 du Code de la sécurité intérieure :
Les dispositifs de vidéoprotection doivent obtenir une autorisation du préfet du lieu d'implantation, après avis d'une commission départementale présidée par un magistrat (sauf cas d'urgence). La demande d'autorisation s'effectue au moyen des formulaires cerfa n° 13806-03. L'autorisation est délivrée pour une durée de 5 ans renouvelable.
Il est possible de ne pas consulter la commission départementale, le préfet délivrant alors une autorisation limitée 4 mois :

- En cas d'exposition particulière à des risques de terrorisme ;
- En cas de manifestation ou de rassemblement de grande ampleur comportant des risques particuliers d'atteinte à la sécurité des personnes et des biens.

Lieux privés (hors domicile)

L'installation peut être libre (sous réserve de la présence de salariés auquel cas le droit du travail devra être pris en compte), ou soumise aux disposition de la de la loi du 6 janvier 1978.
Pour définir le régime applicable, il convient de se référer à la circulaire du 14 septembre 2011 (NOR : PRMX1124533C) qui a fixé deux conditions cumulatives :
Les images font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage.
Le responsable du traitement ou les agents ayant

accès aux enregistrements ou ayant vocation à y accéder sont en mesure, par les moyens dont ils disposent normalement, d'identifier les personnes filmées. L'identification des personnes est considérée comme possible dès lors que le système est mis en œuvre dans des lieux habituellement fréquentés par des personnes dont une partie significative est connue du responsable du système de vidéoprotection, ou des personnes ayant vocation à visionner les images enregistrées. »

Le domicile

La loi de 1978 ne s'appliquant pas au domicile, l'installation de vidéoprotection est libre sous réserve :

- D'informer les personnes accédant au domicile,
- De ne pas filmer les espaces publics,
- De ne pas filmer les espaces privés voisins,
- De respecter le droit du travail dans le cas d'un employé à domicile.

L'international

Par hypothèse, la captation d'images est en France. Il faut distinguer ensuite le lieu de traitement de l'image du lieu de stockage des enregistrements.

Traitement de l'image :

Le CNAPS rappelle sur son site Internet que les sociétés étrangères exerçant en France doivent requérir des autorisations identiques à celles des sociétés françaises. Mais, le traitement à l'étranger de données de source française constitue-t-il une activité exercée en France ? Aucune réponse semble-t-il n'a été apportée à cette interrogation.

Transfert des données et stockage des données :

La loi informatique et libertés n'autorise le transfert de données personnelles que vers des pays offrant un niveau de protection des données suffisant.

Pour les installations relevant du Code de sécurité intérieure, le recours à un stockage externalisé des images de type « cloud » n'est pas encore autorisé par les autorités préfectorales. Mais ces dernières ne justifient leur position par aucun texte.

Prendre en compte la qualité de la personne exploitant le dispositif

Les autorités publiques compétentes

Une autorité publique compétente, le maire d'une commune par exemple, a la faculté de déployer de la vidéoprotection sur la voie publique, sous réserve que le système déployé ait une finalité prévue par la réglementation.

Une autorité publique a l'interdiction formelle de filmer l'intérieur d'un immeuble d'habitation.

Une autorité publique ne peut pas confier l'exploitation des caméras filmant la voie publique à une personne morale de droit privé (un télésurveilleur par exemple).

Les personnes morales de droit privé

Les personnes morales de droit privé ne peuvent déployer de la vidéoprotection que dans un lieu privé ouvert au public. Elles seront alors soumises aux dispositions du code de sécurité intérieure. Les finalités de déploiement prévues par la réglementation sont moins étendues que pour les autorités publiques (prévention des atteintes aux biens et aux personnes uniquement).

Une personne morale de droit privé a l'interdiction formelle de filmer la voie publique.

Une modeste exception à ce principe : dans le cas d'un risque terroriste, une personne morale de droit privé peut surveiller les abords immédiats de son établissement, en débordant éventuellement sur la voie publique. Mais attention, les commissions départementales veillent à ce que la captation d'images de la voie publique soit la plus réduite possible.

Un employeur

Le droit du travail pose un certain nombre de règles relatives à l'installation de vidéoprotection sur le lieu de travail. Information préalable, interdiction de filmer certains lieux d'intimité…
Il ressort de la jurisprudence que la vidéoprotection d'un lieu de travail doit être motivée et qu'il est interdit, sauf cas particulier, de réaliser une surveillance permanente d'un salarié par ce biais.

Des finalités de déploiement limitées par la réglementation

La réglementation française pose un principe d'interdiction de la vidéoprotection des espaces publics et ouverts au public, sauf exception. En effet, dans ce cas la vidéoprotection n'est autorisée que pour certains usages. Il s'agit des « finalités du dispositif », limitativement énumérées notamment par le Code de sécurité intérieure.
Pour les autorités publiques : elles disposent de plusieurs finalités, comme la prévention des atteintes aux biens et aux personnes, la surveillance des flux de transport, la protection des bâtiments publics…
Pour les personnes morales de droit privé : la seule finalité est la prévention des atteintes aux biens et aux personnes.
En outre, quel que soit le cas, il faut donc motiver sa demande, en justifiant le fait que la vidéoprotection permettra de répondre à un besoin réel. Le système doit de plus être proportionné à la menace.

Les systèmes soumis par nature à la loi de 1978

Avec ou sans enregistrement, un système permettant de transporter une image d'un point A vers un point B distant est soumis à la réglementation précédemment décrite.
Certains systèmes, et quels que soient les précédents critères évoqués, relèvent systématiquement de la loi du 6 janvier 1978 : enregistrements visuels de vidéoprotection utilisés dans des traitements automatisés, ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques.
Il s'agit par exemple :

- Des systèmes couplant un système de contrôle d'accès à de la vidéoprotection : biométrie, badges…
- Des systèmes de lecture automatisée de plaques d'immatriculation.

En l'absence d'une réglementation spécifique, il existe encore des vides juridiques ou des difficultés d'application sur l'utilisation des caméras piétons style go-pro.

Un principe général d'information

Quels que soient le lieu d'implantation ou la qualité des personnes exploitant le système, une information claire et permanente doit être donnée aux personnes avant qu'elles ne pénètrent dans une zone vidéo protégée. Des panonceaux d'information doivent donc être installés. Pour les systèmes relevant du Code de sécurité intérieure, certaines mentions sont obligatoires. Cela ne signifie pas que les caméras doivent être visibles : à partir du moment où une information est donnée sur l'existence d'une vidéoprotection, il est tout à fait possible de dissimuler tout ou partie des caméras.

Des obligations complémentaires relevant de différents textes

Le Code pénal

L'enregistrement de l'image ou de la voix d'une personne à son insu dans un lieu privé est pénalement sanctionné (Code pénal, article 226-1).

La loi informatique et libertés

Le conseil d'Etat dans une décision du 24 mai 2011 considère que « le seul fait de capter les images au moyen d'une caméra et de les visionner en temps réel sans procéder à un enregistrement n'implique pas un traitement de données et n'entre donc pas dans le champ de la directive ni de la loi ».

A contrario les contraintes de la loi informatique et libertés s'appliquent dès qu'il y a enregistrement et plus encore lorsqu'il y a des logiciels d'analyse comportementale.

Dans un lieu privé ouvert au public, le traitement donne lieu à une déclaration auprès de la CNIL et doit respecter les obligations de collecte loyale, de respect de la finalité, de conservation durant un délai adapté et d'information des personnes (Articles 226-18 et suivants du Code pénal).

La cour d'appel de Paris (Cour d'appel de Paris, pôle 6 - 1ère chambre, arrêt du 24 février 2015) a ainsi condamné un célèbre restaurant parisien qui avait tenté de justifier le licenciement d'un salarié en produisant des images issues d'un système de vidéoprotection. Le restaurant avait, en définitive, renoncé à l'utilisation de ces images devant le conseil de prud'hommes de Paris.

Mais, la Cour a constaté d'abord qu'une déclaration à la CNIL avait bien été effectuée, mais que la finalité déclarée du traitement était « d'améliorer la sécurité, de dissuader toutes sortes de dégradations, et de disposer d'images en cas d'intrusion de toute personne non autorisée » et que dès lors comme l'avait écrit la CNIL au salarié concerné, les caméras ne pouvaient pas avoir pour objectif la mise sous surveillance d'un employé déterminé ou d'un groupe d'employés.

L'entreprise a donc été condamnée sur le fondement de l'article L254-1 du code de la sécurité qui prévoit que les systèmes de vidéoprotection ne peuvent être utilisés à « d'autres fins que celles pour lesquelles ils sont autorisés ».

Le droit du travail

La mise en place au sein d'une entreprise d'un système de vidéoprotection doit respecter le triptyque habituel de la surveillance des salariés :

- Informer le salarié ((article L.2323-32 du code du travail, lois n° 84-16 du 11 janvier 1984, n° 84-53 du 26 janvier 1984 et n° 86-33 du 9 janvier 1986).
- Informer et consulter le comité d'entreprise (Code du travail, art L. 2323-32)
- Etre proportionnel au but poursuivi.

L'Évolution du métier

Initialement centré sur la détection intrusion basique, ce métier est en constante évolution. Très rapidement les prestations ont été étendues à la détection d'incendie, technique, froid, à la surveillance des individus (particulièrement en Téléassistance). Il est soumis à des facteurs extérieurs qui l'influencent et le modifient inéluctablement dans le temps afin de s'adapter aux changements de notre société. Ces facteurs sont notamment :

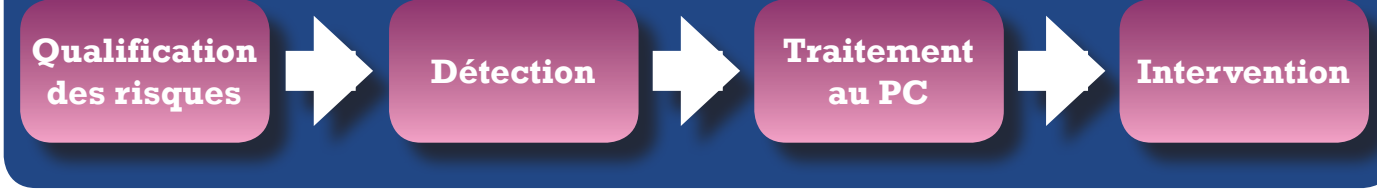
- Les technologies,
- Les infrastructures de communication
- Les lois et normes
- Les usages
- L'environnement économique
- Les événements
- Les intervenants dans le cycle de décision

La réflexion de l'USP-Technologies est de prendre en compte ces facteurs et de proposer une offre globale intégrant les prestations (y compris la prestation humaine) et la technologie afin de répondre au plus juste aux attentes de nos clients et du marché.
Cette offre globale est composée de quatre parties fonctionnelles interdépendantes :

- La qualification des risques,
- La détection,
- Le traitement au PC,
- L'intervention.

Elle peut être portée et proposée par une seule entreprise ou par plusieurs entreprises qui dans ce dernier cas, chacune d'entre elles propose une ou plusieurs parties fonctionnelles.
L'offre peut être déclinée sous forme classique où le client achète les prestations et les équipements et devient donc propriétaire de la solution, on parle dans ce cas de CAPEX*, ou alors le client souscrit un contrat de service où il paye chaque mois un « loyer », dans ce cas le client n'est pas propriétaire de la solution, on parle alors d'OPEX*.

** Les dépenses d'exploitation (souvent abrégées en OPEX) sont les coûts courants pour exploiter un produit, des entreprises, ou un système.*
** Les dépenses d'investissement de capital (souvent abrégées en CAPEX), se réfèrent aux coûts de développement ou de fourniture des pièces non-consommables pour le produit ou le système. Par exemple, l'achat d'un photocopieur est le CAPEX, et le coût annuel de papier et de toner consommé est l'OPEX. Pour de plus grands systèmes comme les entreprises, l'OPEX peut également inclure le coût des employés et des dépenses de service telles que le loyer et l'eau, le gaz, l'électricité, etc*



Qualification des risques

Nous avons préalablement défini une liste de risques, pour lesquels la télévidéosurveillance pourrait constituer un moyen de prévention ou de traitement.

L'approche tient compte assez naturellement de la différenciation entre le traitement des actes de **malveillance** (toujours avec à l'origine une action volontaire d'une ou de plusieurs personnes), et le traitement des **accidents** (sinistres provoqués sans action volontaire).

A chaque type de risque, correspondent des modes de traitement préventif, d'évitement ou d'identification de causes. Dans de nombreux cas, les moyens de télévidéosurveillance sont une alternative dans le choix de ces modes de traitement.

L'approche du traitement du risque dans la sécurité globale est donc adaptée en fonction du domaine duquel il relève :

- **La sécurité :** désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux risques techniques, physiques, chimiques et environnementaux pouvant nuire aux personnes et aux biens sans avoir un but de profit. Elle répond à de nombreuses règles établies, notamment la sécurité incendie qui est de la compétence des sapeurs-pompiers.
- **La sûreté :** concerne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux actes spontanés ou réfléchis ayant pour but de nuire, ou de porter atteinte dans un but de profit psychique ou/et financier. Elle répond à des règles distinctes de celles établies pour la sécurité, et est régie par des textes différents.

La malveillance

Les agressions verbales, les incivilités

Elles se produisent plutôt dans les lieux publics. A l'origine, des personnes dont le comportement devient agressif, suite à la non prise en compte et la résolution immédiate d'une requête, une demande.

Exemples :
- File d'attente,
- Caisse de paiement dans un commerce,
- Guichet Pôle Emploi,
- Restauration rapide,
- Banque,
- Un différend avec une autre personne.

Dans tous les cas, une insatisfaction ou une exaspération qui fait que la personne ne se contrôle plus. Il s'agit d'un comportement irréfléchi et spontané, l'action n'est pas préméditée. La prévention est compliquée à mettre en œuvre (pas de classification juridique/pénale), il faut faire appel au sens civique, au comportement social, et avertir contre le risque de dérive vers l'agression physique (contravention, délit). Tout système de vidéosurveillance peut permettre le traitement de ce type de risque : détection (analyse comportementale), dissuasion et aide à la résolution : stockage d'images avec information préalable au public, identification. Difficulté majeure : il s'agit d'un risque, qui, s'il ne dérive pas vers l'agression physique, n'expose pas l'auteur à des sanctions.

Les agressions physiques, les vols à main armée (VMA), les prises d'otages

Le risque est permanent, en tous lieux (intérieur, extérieur), où la présence de personnes est réduite. Les auteurs en sont des délinquants, des personnes en lien avec le grand banditisme, qui agissent individuellement, ou en bande organisée, avec ou sans armes : armes blanches, armes à feu…

A l'origine :
- Un différend,
- Une altercation,
- L'appât du gain,
- Une revendication idéologique,

où la contrainte exercée sur une tierce personne, ou un groupe de personnes, va permettre à l'auteur de l'agression, du braquage, de la prise d'otage, d'atteindre son but.

Les actions peuvent être préméditées ou non, préparées ou irréfléchies :
- Violence gratuite,
- Racisme,
- Homophobie,
- Vol sous la contrainte,
- Séquestration,
- Home jacking…

Pour lutter contre ce type de risque : la protection physique des locaux (domicile, lieux de travail), les alarmes (boutons agression, alarmes individuelles avec géolocalisation…), la vidéosurveillance, à l'intérieur des bâtiments, ou sur les lieux publics avec la vidéoprotection. Difficulté majeure pour les alarmes volontaires : la menace peut inhiber toute réaction pour signaler la situation d'agression.

Les intrusions, les cambriolages

Dans les locaux d'habitation, les locaux professionnels, ce risque se présente plutôt en absence partielle ou totale d'occupants.
Les auteurs potentiels d'intrusions, de cambriolage sont très divers :

- Petite délinquance (mineurs, isolés en groupes),
- Grande délinquance, banditisme,
- Bandes organisées : familles, mafias…

Les actes sont très souvent prémédités, en fonction des opportunités (absences, congés…), et c'est l'appât du gain, la revente potentielle d'objets de valeur, l'assouvissement immédiat de besoins personnels (stupéfiants) qui motive ces actes. Pour se prémunir : la protection physique des locaux, le contrôle des accès, les dispositifs d'alarme intrusion reliés en télésurveillance, les systèmes dissuasifs locaux (avertisseurs, diffuseurs de brouillard…), les agents de sécurité, et les systèmes de vidéosurveillance, permettant la dissuasion, la levée de doute, et l'exploitation des enregistrements par les enquêteurs, aux fins d'identification des circonstances, voire des auteurs.

Les vols, la démarque inconnue

Ces faits sont commis dans les lieux publics, en période d'affluence dans les commerces, dans les lieux privés, en présence ou non de tierces personnes. Les modes opératoires sont très diversifiés, ce qui rend compliquée leur détection.

Fait marquant, tout le monde peut être à l'origine d'un vol, il peut s'agir de délinquants, de personnes insérées socialement, mais en proie à une pulsion irraisonnée, d'hommes, de femmes…

Les cibles privilégiées :

- Les individus avec vol sans violence (téléphones mobiles, sac à main…),
- Les commerces,
- La grande distribution,
- Les entreprises,
- Les lieux publics, en intérieur, en extérieur…

Il peut s'agir d'actions préméditées, calculées, mais également d'actes opportunistes, qui se font avec rapidité et furtivité. Pour lutter : les marqueurs électroniques, les portiques antivols (boutiques), les codes et systèmes de protection logiques ou de blocage à distance (téléphones mobiles, ordinateurs…), le gardiennage, et la vidéosurveillance (analyse comportementale, vidéo haute définition pour l'identification). La difficulté majeure réside dans la fraude des dispositifs de protection antivol, et dans la ressource nécessaire en moyens humains pour exploiter un système de vidéosurveillance.

Les dégradations volontaires, le vandalisme

Il s'agit d'un risque permanent 24h/24, en tous lieux, en tous secteurs (urbain, rural, sites naturels…), qui peut survenir avec ou sans présence de tierces personnes. Les auteurs, comme pour les vols et la démarque inconnue, sont multiples et sans catégorisation précise.
Les motivations sont diverses :

- Actes gratuits,
- Vengeance et volonté de nuire à un tiers ou à la société,
- Altercations,
- Différends…

Les actes commis sont souvent rapides et furtifs. S'en prémunir est très difficile, sauf pour les lieux clos, où une protection physique efficace, combinée à un dispositif de détection électronique (Tags RFID dans les expositions) ou à un dispositif de gardiennage, peut dissuader les auteurs potentiels. La vidéosurveillance est un outil précieux pour anticiper (analyse comportementale) et identifier.

L'espionnage (secteur économique, industriel…)

Le risque est permanent, 24h/24, il concerne (hors secteur militaire & le Gouvernement) essentiellement le secteur économique, industriel, où des concurrents déloyaux pourraient être tentés de s'approprier toutes informations, toutes données techniques, commerciales…

Les auteurs sont difficiles à identifier, en interne ou en externe de l'entreprise victime d'espionnage. Le risque existe sur le lieu de l'entreprise, mais également dans les lieux publics, au domicile des personnes ciblées. Les actes sont toujours prémédités, savamment préparés, de manière à ce que leur exécution ne soit pas détectable par des tiers, ou par la personne directement visée. Pour se protéger : contrôle des accès, sécurité informatique, vidéosurveillance, en installations fixes ou en dispositifs temporaires (appât), en véhicules mobiles… Principale difficulté : difficile à anticipé, grande part d'aléatoire…

Le terrorisme

Le risque est directement lié aux évolutions géopolitiques, à l'émergence d'idéaux sociologiques, religieux, qui se placent en opposition avec les régimes gouvernementaux en place. Les mouvements ou groupes terroristes sont par essence non reconnus légalement et existent donc dans la clandestinité, ce qui rend leur identification et leur localisation extrêmement complexe. Les auteurs potentiels d'actes sont difficiles à identifier, cette tâche est de la responsabilité des services de l'état.

Toutefois, les observations menées par ces services de l'état, quels qu'ils soient (Ministère de l'Intérieur, Ministère de la Défense…) peuvent conduire ces mêmes services à solliciter les moyens privés de la sûreté pour compléter les investigations en cours.

Bien naturellement, les moyens de vidéosurveillance sont des outils précieux qui peuvent être utilisés pour rechercher un évènement, reconstituer son déroulé, et analyser de manière contradictoire certaines hypothèses. Plus le réseau de vidéosurveillance est dense, plus leur efficacité pour permettre la lutte contre le terrorisme est réelle.

Les actes de terrorisme peuvent être de différentes natures envers des individus, des sites critiques publics ou privés (sites industriels SEVESO et agro alimentaires, sites de télécommunication, eau, énergie, transport, OIV). En fait, tous les sites qui peuvent avoir un impact important sur l'économie d'un pays et sur sa population.

Le risque incendie, les risques naturels, les risques industriels

Les incendies

Risque permanent, en tous lieux, tous secteurs, accentué sur certaines périodes : en été pour les incendies de forêts, en hiver pour les incendies habitations. Il y a peu d'incendies « instantanés », il y a toujours une cause humaine : négligence, combinaison de facteurs déclenchant (accidents). Les incendies volontaires sont, dans ce cas, plus assimilables à un acte de dégradation volontaire, de destruction. La détection est possible dans les lieux clos en intérieur, sous certaines conditions en extérieur, avec la détection par caméras thermiques. La prévention également, avec le gardiennage, les postes de vigie locale ou à distance par vidéosurveillance. Principale difficulté : la rapidité de détection et de réactivité, opposées à la vitesse de propagation d'un incendie.

Les risques naturels

Ces risques sont essentiellement géologiques, climatologiques : tremblements de terre, tsunamis, et les conséquences sont considérables. Leur anticipation est effectuée par divers services de l'Etat : Services d'intérêt Vital, Points d'intérêt Vital. Le risque est existant 24h/24, en tous lieux, avec toutefois des zones potentiellement plus exposées que d'autres (cartographie des risques). La détection précoce est assurée par les services de l'état, par les entreprises : ERDF pour les barrages par exemple, avec de la détection sismique, du contrôle de mesures sur site, et également de la vidéosurveillance. Point majeur : le risque ne peut être éradiqué, il s'agit d'en minimiser les conséquences.

Les risques industriels

NRBC : les risques Nucléaires, Radiologiques, Biologiques, Chimiques.

Ce risque permanent, lorsqu'il est identifié, est localisé sur les lieux de production d'énergie : centrales nucléaires, centres de production d'uranium, centres de traitement des déchets nucléaires. Au niveau des entreprises, secteur de la chimie, du médical, centres de recherche…

Facteurs déclenchants : combinaison de faits concomitants, non prévus dans leur globalité, négligences, erreurs humaines. Les moyens de prévention sont nombreux, gérés industriellement, la difficulté est similaire au risque incendie : propagation rapide, jusqu'à en rendre les effets incontrôlables. La vidéo peut constituer un moyen de coordination des actions de secours.

Les risques individuels

Les moyens de protection individuelle pour les personnes isolées se sont développés avec l'évolution des moyens de communication (GSM, GPRS associés à la géolocalisation).

Les particuliers (personnes seules ou âgées, patients soignés à domicile…) peuvent bénéficier de ces moyens de protection individuelle, associés à des services de téléassistance.

Comme en télésurveillance, la difficulté et l'efficience de ces services sont proportionnels aux moyens de vérification du bien fondé du déclenchement de l'alarme ou de l'appel de détresse. Lorsque l'interphonie est inefficace, les moyens de visualisation à distance en temps réel sont un atout précieux pour gagner du temps et caractériser la situation avant sollicitation des forces de l'ordre ou des pompiers.

D'autres types de risque (risque sanitaire, risques liés à des mouvements sociaux de grande ampleur tels que manifestations, troubles à l'ordre public…) pourront être traités par le biais de la vidéo, dès lors que les moyens seront mutualisés et administrés de façon à permettre une continuité « logique et physique » de l'exploitation de ces moyens de vidéosurveillance.

Ce document couvre les applications principales, autres que ces risques spécifiques.

Synthèse

En synthèse, quels que soient les risques identifiés :

- La malveillance : les agressions, les intrusions, les vols, les dégradations,
- Le risque incendie, les risques naturels, les risques industriels.

Nous pouvons déjà, à l'énumération de ces événements, deviner et envisager l'apport que les moyens de télévidéosurveillance peuvent constituer, avec plus ou moins d'efficacité et d'efficience, suivant leur dimensionnement.

Ces moyens ne peuvent constituer à eux seuls la parade universelle et unique à tous ces risques, mais ils sont une composante incontournable dans la lutte contre ceux-ci.

Le chapitre suivant traite des moyens permettant d'identifier et déceler ces différents risques.

La détection

Suite à la qualification des risques identifiés dans le précédent chapitre, il est nécessaire de mettre en place une solution fiable permettant de les détecter et d'alerter.

Jusqu'à maintenant, les alarmes intempestives et la réglementation ont contraint d'adjoindre à la détection des moyens de levée de doute. Cela a commencé par un appel sur site, par de l'écoute grâce à des micros, de l'interphonie associant micro et haut-parleur, puis grâce à l'évolution de la technologie, notamment la qualité des images permettant une réelle identification, les capacités d'analyse et d'intelligence embarquée, des protocoles et supports de communications permettant de transmettre les informations vers le centre de gestion (Traitement au PC).

Les détecteurs

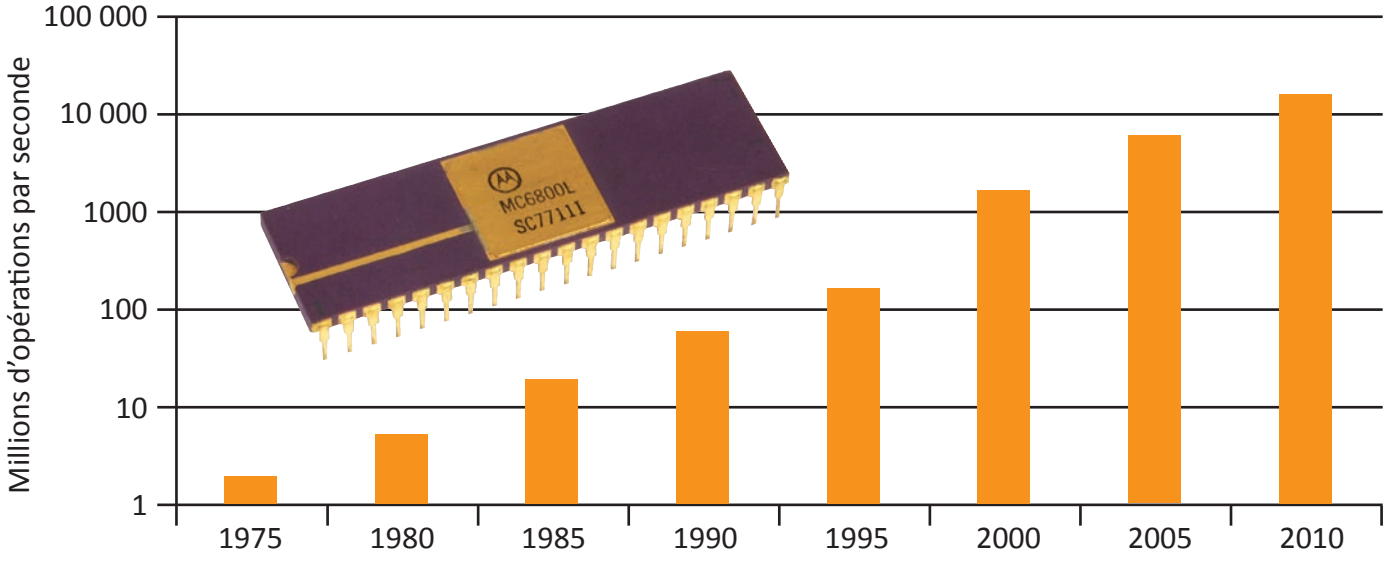
Un détecteur est un dispositif technique (instrument, substance, matière) qui change d'état en présence de l'élément ou de la situation pour lequel il a été spécifiquement conçu. Les détecteurs sont composés d'un ou plusieurs capteurs et d'une intelligence associée permettant d'analyser les informations issues du ou des capteurs et de détecter un événement suivant des critères prédéfinis.
Par exemple, dans le cas de la vidéo, le détecteur est une caméra vidéo intégrant des capacités d'analyse et de détection.

Avant de traiter de l'évolution des derniers détecteurs ayant émergé sur le marché de la vidéoprotection, il est impératif et nécessaire de comprendre que ces évolutions sont étroitement liées à celles des processeurs qui sans nul doute favorisent leur émergence. Le processeur garantit en outre une puissance et des performances de traitement renforcées, de quoi autoriser le développement d'applications de traitement et d'analyse vidéo intelligentes.

Les détecteurs vidéo

Les détecteurs vidéo, communément appelés caméras intelligentes, peuvent être de différentes formes (caméra fixe, caméra dôme, caméra discrète, caméra tube ou Bullet, caméra mobile PTZ …) intégrant différents types de technologie de capteurs du spectre de la lumière (lumière visible, lumière proche Infra rouge, lumière infra rouge ou thermique).

Evolution de la puissance des ordinateurs



Les caméras hautes résolutions dans le domaine de la lumière visible

Ces caméras sont composées d'un capteur vidéo haute résolution ou multi-mégapixel qui va permettre de délivrer des images avec un million de pixels ou plus. Cette résolution est largement supérieure à celle qu'il est possible d'obtenir avec une caméra analogique.

Une caméra mégapixel peut être utilisée de deux manières : soit pour afficher davantage de détails dans une image de plus haute résolution (ce qui peut être utile pour identifier des personnes ou des objets), soit pour couvrir une plus grande partie d'une scène si une résolution d'image identique à celle d'une caméra non mégapixel est utilisée.

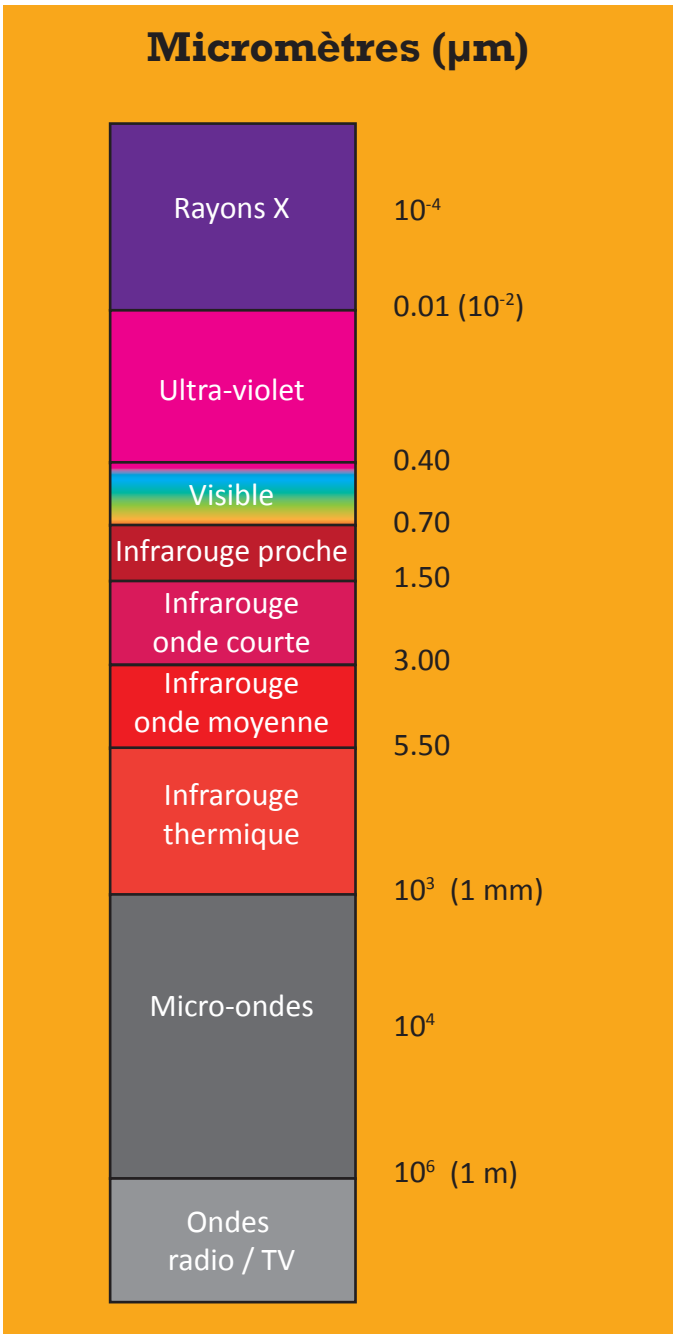
Les flux vidéo à haute résolution générés par une caméra mégapixel nécessitent en outre davantage de bande passante réseau et d'espace de stockage pour les enregistrements, bien que cet inconvénient puisse être atténué par l'utilisation de la norme de compression vidéo H.264.

Ces flux vidéo vont nécessiter l'utilisation de serveurs d'exploitation de plus en plus puissants permettant d'analyser et d'exploiter les informations délivrées.

Les caméras thermiques ou bolométriques

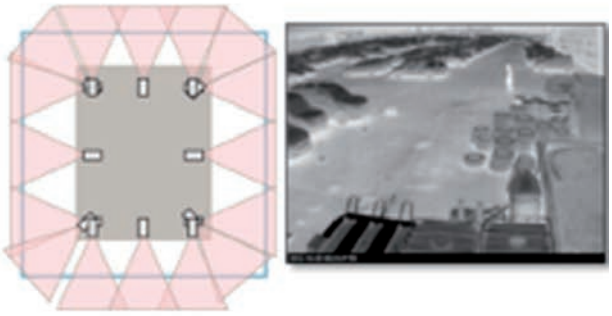
Les caméras équipées d'un capteur « bolométrique » vont reconstituer une image en fonction des différences de température des objets, véhicules ou personnes composant cette image. Ainsi, elles peuvent voir dans l'obscurité la plus totale à des distances pouvant atteindre parfois plusieurs kilomètres et transmettre des images permettant aux opérateurs de détecter les activités suspectes (individus, température anormale) et d'agir. Combinées à l'analyse vidéo intelligente, ces caméras vont permettre une prévention des risques liés à l'incendie et aux intrusions sur des sites nécessitant un niveau de sécurité accrue.

Deux types de caméras existent, les caméras thermographiques et les caméras thermiques.



**Caméras traditionnelles (images du haut)
vs cameras thermiques (images du bas)**

Installation en périmétrie



Installation sur les bâtiments

Les caméras thermographiques

Thermographie infrarouge, elle va consister à transformer une image infrarouge en une image radiométrique, qui permet la mesure de température et ainsi la détection précoce d'incendie ou de déceler des points chauds pour éviter les incendies.

Exemples d'applications :

- Appareillages de commutation, de gaz et de turbines d'eau
- Transformateurs et sous-stations électriques
- Décharges, sites de stockage ou silos
- Matières auto-allumage

Les caméras thermiques

Les caméras thermiques excellent dans la détection des personnes, objets et incidents dans l'obscurité et autres conditions difficiles (pluie, brouillard…). Elles ne fournissent en revanche aucune image permettant une identification fiable. Elles sont souvent utilisées pour des usages de protection périmétrique et la détection d'intrusion.
Autrement dit, les caméras thermiques et les caméras de surveillance classiques sont parfaitement complémentaires dans une installation de surveillance, la première pour la détection, la deuxième pour la recherche de détail (reconnaissance, identification) et le suivi (tracking) de l'intrus.

Exemples d'applications :

- Protection périmétrique
- Franchissement de ligne
- Comptage de personnes
- Détection et Levée de doute visuelle

En ce qui concerne la protection périmétrique, deux types d'installation peuvent être réalisés, tout dépend de l'infrastructure existante (électricité et réseau), les coûts de génie civil pour l'installation en périmétrie, la taille de la zone à protéger et le type de sécurité souhaitée.

Les détecteurs sonores

Les détecteurs sonores peuvent être dédiés ou intégrés directement dans les caméras de vidéoprotection. Cela a été possible grâce à la puissance de traitement des nouveaux processeurs des caméras qui permettent ainsi d'intégrer les algorithmes de détection audio en plus de la vidéo. De cette façon, les sons qui caractérisent l'agression verbale, les

coups de feu, l'alarme de voiture, le bris de verre ou le spray d'aérosols graffitis peuvent être reconnus. D'autres sons sont filtrés et ignorés.

Le fait de disposer de l'audio dans un système de vidéosurvelllance peut se révéler précieux pour la détection et l'interprétation d'évènements et de situations d'urgence. L'audio peut couvrir une zone de 360° et permet au système de vidéosurveillance d'étendre sa couverture au-delà du champ de la caméra. L'audio peut permettre d'envoyer une instruction à une caméra PTZ ou alerter un opérateur de caméra pour vérifier visuellement l'endroit où une alarme audio s'est déclenchée.

Les applications d'analyse vidéo et audio embarquées dans les détecteurs

Les algorithmes

L'évolution de la puissance de calcul des processeurs a permis le développement d'algorithmes d'analyse de plus en plus complexes faisant appel aux nouvelles sources d'information fournies par les capteurs. Ces algorithmes vont autoriser l'intégration de nouveaux paramètres comportementaux ou environnementaux qui jusqu'à alors n'étaient pas exploités par les systèmes de surveillance.

Les flux vidéo et audio numérisés deviennent une matière qui traitée par ces supercalculateurs embarqués ou distants va nous permettre d'établir des règles et d'affiner les alertes liées à des évènements. La combinaison des paramètres va donner la possibilité d'élaborer des scénarios de détection qui vont optimiser les ressources humaines et électroniques dédiées à la surveillance des sites. Nous assistons à une interconnexion des informations qui vont offrir après analyse et traitement la possibilité d'anticiper, de détecter et d'agir.

Quelques exemples d'algorithmes d'analyse vidéo et audio par type de marché :

Retail (commerces) :

- Comptage de personne
- Zones de passage chaudes et froides
- Détection Phase d'achat (mesure du temps des clients en face de chaque produit)
- Segmentation démographique (homme, femme, âge)
- Mesure de file d'attente en caisse
- Détection de démarque inconnue en caisse

Transport :

- Détection Automatique d'Incident (DAI)
- Détection de ralentissement et bouchon
- Classification véhicule
- Comptage de véhicule par voie
- Mesure de file et Gestion de carrefour
- Lecture de plaque d'immatriculation
- Détection de fumée en tunnel

Logistique :
- Scan de code barre
- Suivi de colis vidéo
- Lecture de plaque d'immatriculation en entrée de site
- Protection périmétrique (Cross line)

Parking
- Détection vidéo de Maraudage
- Détection sonore d'Alarme véhicule
- Détection sonore de bris de vitre
- Lecture de plaque d'immatriculation
- Détection sonore d'Agression verbale
- Gestion places de parking

Protection de site
- Détection d'intrusion (détection de mouvement dans une zone)
- Détection de franchissement d'une ligne (protection périmétrique)
- Suivi automatique de personne
- Lecture de plaque
- Détection extérieure de départ de feu
- Détection sonore de bris de vitre

Site critiques
- Reconnaissance faciale (exclusivement sur serveur pour l'instant)

Villes
- Détection sonore d'agression verbale
- Détection sonore de bris de vitre
- Détection sonore de coup de feu
- Détection sonore de graffiti et spray
- Gestion places de parking

Les métadonnées

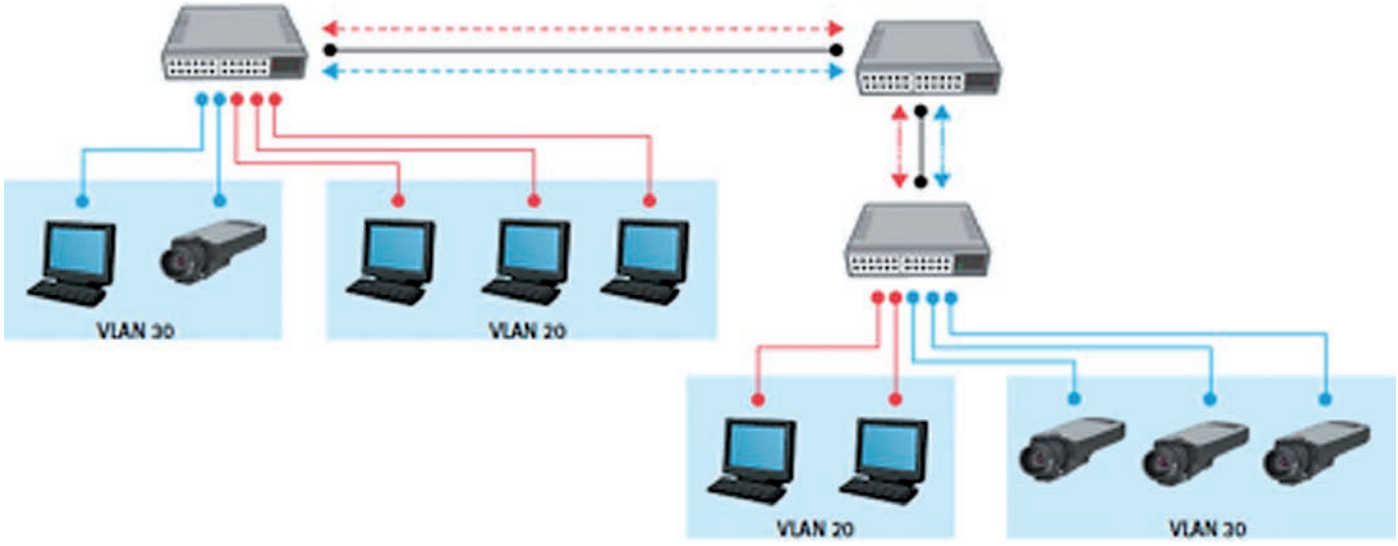
Les métadonnées vidéo sont des données de description de contenu vidéo. Ces données peuvent être aussi bien des descriptions textuelles, que des données extraites automatiquement des images représentées sous forme de descripteurs. Ces métadonnées sont renseignées par les algorithmes d'analyse vidéo.

Le moteur de métadonnées va redéfinir la gestion des données de sécurité. Les données provenant de diverses sources, comme de l'analyse vidéo, de points de vente, de la reconnaissance de plaques minéralogiques et de systèmes de contrôle d'accès, sont recueillies par le moteur de métadonnées et indexées aux séquences vidéo/audio pertinentes, permettant des requêtes intelligentes et des informations détaillées sur les événements en temps réel.

La transmission des informations vers le traitement au PC

Les réseaux

Pour transférer des données entre deux périphériques sur des réseaux locaux différents, une normalisation de la communication est nécessaire, puisque les réseaux locaux peuvent obéir à différentes technologies. C'est pourquoi on a mis au point l'adressage IP et de nombreux protocoles IP de communication sur Internet, système global de réseaux informatiques interconnectés. Avant de traiter l'adressage IP, il faut examiner tout d'abord certains éléments de base des communications In-



ternet tels que les routeurs, les pare-feu et les fournisseurs d'accès Internet.

Plusieurs types de réseaux existent :

Les réseaux locaux :

Le réseau local, souvent désigné par son acronyme anglais LAN (Local Area Network), désigne un réseau informatique local, qui relie des ordinateurs dans une zone limitée, comme une maison, école, laboratoire informatique, ou immeuble de bureaux.

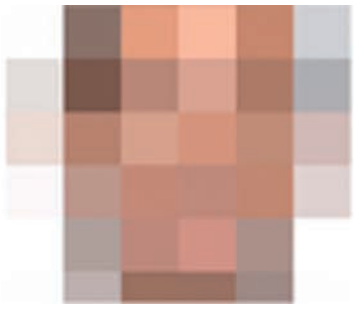
Les réseaux étendus :

Un réseau étendu, souvent désigné par son acronyme anglais WAN (Wide Area Network), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Le plus grand WAN est le réseau Internet. Les réseaux de télécommunication de types 3G, 4G LTE en font aussi partis.

Séparation des réseaux, le VLAN

Lors de la conception d'un système de vidéo sur IP, il est souvent souhaitable de séparer ce réseau des autres, pour des raisons de sécurité et de performance à la fois. Au premier abord, la meilleure solution consiste à créer un réseau distinct. Bien que cela simplifie la conception, les coûts liés à l'acquisition, à l'installation et à la maintenance de ce réseau sont bien souvent supérieurs aux coûts d'utilisation d'une technologie appelée réseau local virtuel (VLAN).

VLAN est une technologie de segmentation virtuelle des réseaux prise en charge par la plupart des commutateurs réseau. Elle répartit les utilisateurs réseau en groupes logiques. Seuls les utilisateurs d'un groupe spécifique sont capables d'échanger des données ou d'accéder à certaines ressources sur le réseau. Lorsqu'un système de vidéo sur IP est segmenté en VLAN, seuls les serveurs situés sur ce VLAN peuvent accéder aux caméras réseau. Les VLAN représentent généralement une solution plus rentable et plus performante qu'un réseau distinct. Le principal protocole utilisé lors de la configuration d'un VLAN est IEEE 802.1Q.



Les protocoles de transmission de données vidéo et audio

Les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont les deux protocoles IP utilisés pour le transfert de données. Ces protocoles de transfert jouent le rôle de « porteur » pour de nombreux autres protocoles. Ainsi, le protocole HTTP (Hyper Text Transfer Protocol), qui est utilisé pour parcourir des pages Web sur des serveurs dans le monde entier par Internet, est porté par le protocole TCP.

Le protocole TCP constitue un canal de transmission fiable, basé sur les connexions. Il garantit que les données envoyées d'un endroit à l'autre sont bien reçues. La fiabilité obtenue par retransmission peut cependant causer des latences importantes. En général, le protocole TCP s'utilise lorsque la fiabilité de la communication a priorité sur la latence de transmission.

Le protocole UDP est un protocole dit « sans connexion » qui ne garantit pas la livraison physique des données envoyées et laisse donc à l'application le soin de vérifier et de contrôler les erreurs. Ne permettant pas la transmission des données perdues, il n'introduit pas de délais supplémentaires.

Les débits nécessaires

Le débit, c'est à dire la quantité de données vidéo à transmettre sur le réseau dépend de plusieurs facteurs :

La résolution des images

- La fréquence des images
- Le type de compression (H264, MPEG4, MJPEG)
- Le type de régulation (CBR ou VBR)
- Le type de scène (paysage avec peu de mouvement, porte d'un grand magasin)
- L'environnement (lumière, pluie, neige, vent, vibration)

Le type d'utilisation de la vidéo va déterminer le débit nécessaire. Par exemple, la levée de doute vidéo nécessite une vidéo qui permet de voir uniquement ce qui se passe par conséquent la résolution, la fréquence des images, la qualité (compression importante) peuvent être réduites. A contrario, pour de l'identification et de l'investigation, la qualité de l'image doit être importante, ce qui oblige à avoir un débit plus important.

En parallèle, la bande passante disponible entre le site et le centre de télévidéosurveillance va jouer aussi un rôle dans le choix du type de service (levée de doute, analyse vidéo sur serveur distant ou de l'enregistrement à distance).

Dans ce dernier cas de figure, l'analyse vidéo et/ou l'enregistrement se font directement en local, sur le site.

En fonction de la qualité et de la durée de rétention des images, l'enregistrement pourra être réalisé directement sur la carte SD intégrée dans la caméra.

La résolution des images en fonction des usages

La résolution d'une caméra est définie par le nombre de pixels d'une image prise par le capteur. En fonction de l'objectif, la résolution permet soit de distinguer plus de détails, soit d'obtenir un champ plus large.

Le choix de la résolution est défini en fonction des objectifs de surveillance suivants :

- Vue d'ensemble, Détection et Levée de doute (densité de pixels de 10 à 20 pixels par mètre)
- Reconnaissance, lecture de plaque (densité de pixels de 150 à 200 pixels par mètre)
- Identification (densité de pixels de 300 à 400 pixels par mètre)

Les vues d'ensemble permettent de surveiller une scène en général ou le mouvement d'ensemble des personnes qui s'y trouvent.

Les images à haut niveau de détail sont importantes pour l'identification des personnes ou des objets (visages, plaques minéralogiques, surveillance de systèmes de point de vente). Le but de la surveillance détermine le champ et le positionnement de la caméra, le type de caméra et d'objectif utilisé.

Par exemple, la résolution nécessaire pour l'identification est définie dans l'arrêté d'août 2007 sur la vidéoprotection en stipulant que pour identifier un visage de 16 cm de largeur, la surface du visage dans l'image doit occuper au moins 60 pixels, ce qui donne une densité pixel par mètre de : 60 pixels / 0,16 m = 375 pixels par mètre.

C'est également la recommandation faite dans la version la plus récente de la norme européenne EN50132-7:2012 de CENELEC. Toutefois, dans des conditions difficiles, il est recommandé d'augmenter la densité pixels à 400 pixels par mètre.

En comparaison, une caméra de résolution 4CIF soit 704 pixels de large couvrira une zone de 1,87 mètres de large pour de l'identification. A contrario, une caméra Full HD de 1920 pixels de large couvrira une zone de 5,12 mètres de large.

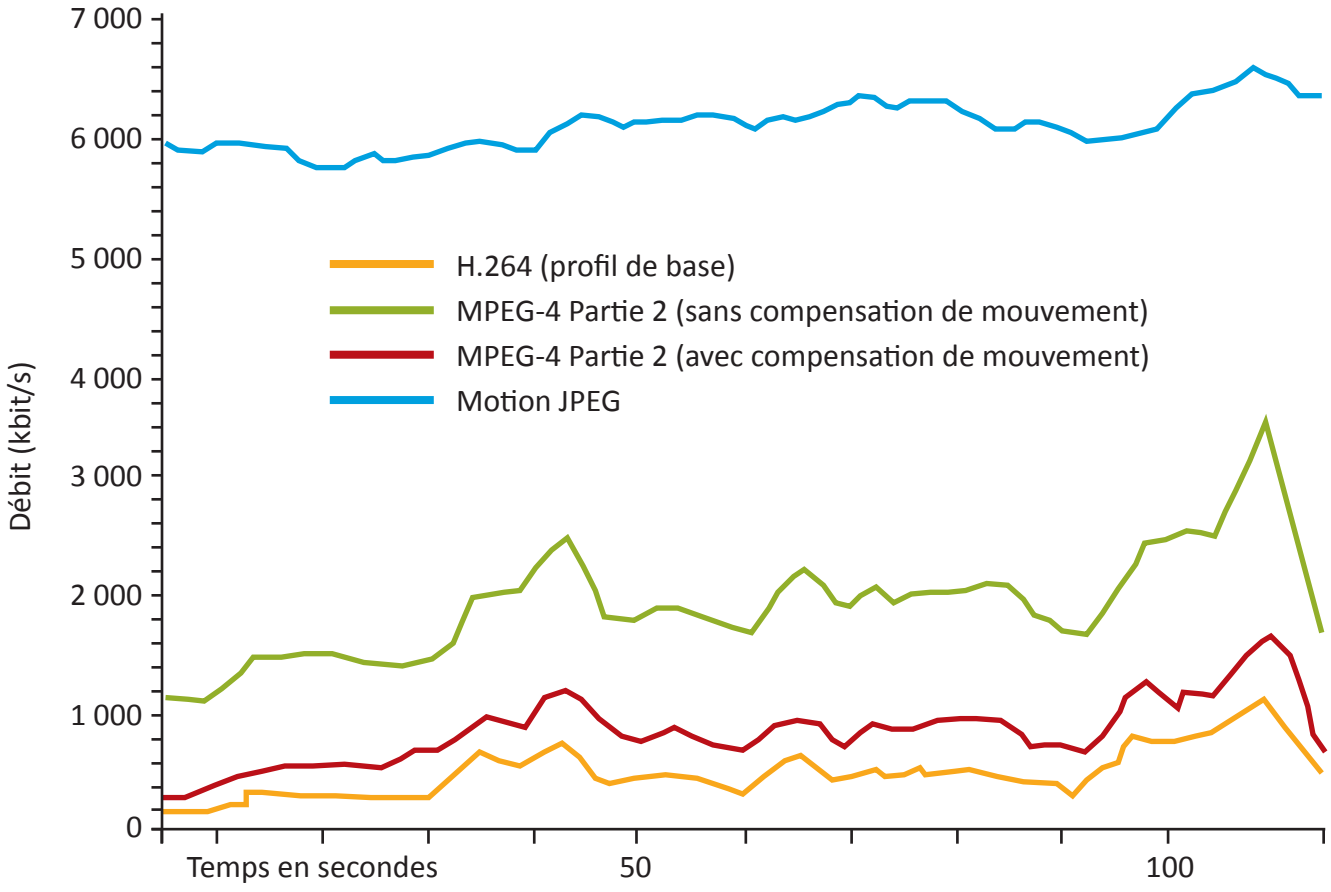
Pour les plaques d'immatriculation, il est également recommandé que le texte occupe 20 pixels en hauteur pour une plaque d'immatriculation de 52 cm de large et de 11 cm de hauteur soit 181 pixels par mètre.

En comparaison, une caméra de résolution 4CIF soit 704 pixels de large couvrira une zone de 3,88 mètres de large pour de la lecture de plaque d'immatriculation. A contrario, une caméra Full HD de 1920 pixels de large couvrira une zone de 10,6 mètres de large.

La compression vidéo

La qualité de la compression vidéo va être déterminante notamment sur le type d'utilisation souhaitée (levée de doute, reconnaissance et identification).

Lorsque l'on compare les performances des normes MPEG telles que MPEG-4 et H.264, il est important de noter que les résultats peuvent varier d'un encodeur à l'autre, même s'ils utilisent la même norme. Ceci est dû au fait que le concepteur d'un encodeur a le choix parmi un ensemble d'outils à implémenter dans le cadre d'une norme. Il est possible de conserver un flux conforme à la norme à la sortie de l'encodeur tout en utilisant des ensembles différents. Une norme MPEG ne peut donc garantir un débit binaire ou un niveau de qualité donné, et il est im-



possible d'effectuer des comparaisons fiables sans définir au préalable comment sont implémentées les normes dans l'encodeur. Contrairement à l'encodeur, le décodeur doit implémenter toutes les parties requises d'une norme pour décoder un flux binaire conforme. Une norme spécifie la façon exacte dont un algorithme de décompression doit rétablir chaque bit d'une vidéo compressée.

Le graphique suivant présente une comparaison du débit obtenu, à niveau de qualité d'image égal, entre les normes vidéo suivantes : Motion JPEG, MPEG-4 Part 2 (sans compensation de mouvement), MPEG-4 Part 2 (avec compensation de mouvement) et H.264 (profil de base BP).

Afin d'améliorer la qualité de compression à qualité d'image équivalente, certains constructeurs ont développé et intégré dans leur encodeur des algorithmes de pré traitement de l'image.
Par exemple, une première méthode consiste à définir par l'algorithme de pré traitement une région d'intérêt dynamique, les images consécutives (vidéo) sont analysées en temps réel pour déterminer les régions les plus intéressantes, soit celles qui présentent le plus de détails ou de mouvement. Ces zones sont alors traitées différemment du reste de l'image, comme décrit ci-dessous.
Une seconde méthode, basée sur le Groupe d'images dynamique où l'intervalle entre les images I (intra-images) est réglé dynamiquement en fonction de la quantité de mouvement existant dans la

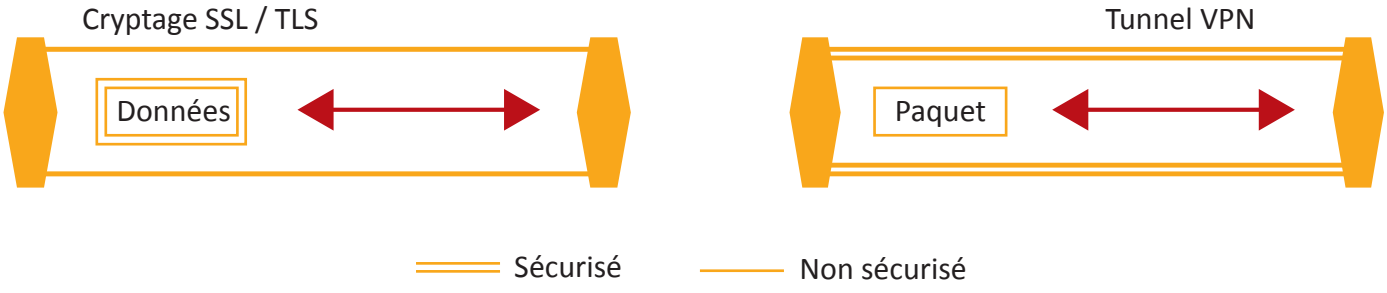
scène. Sur une période pendant laquelle il n'y a que peu de mouvement, le débit binaire est réduit en fournissant moins fréquemment des images I.
Ces deux méthodes peuvent être utilisées indépendamment l'une de l'autre ou bien ensemble, afin de diminuer le débit binaire et d'utiliser au mieux la bande passante disponible.
Alors, quel est l'intérêt de ces nouvelles technologies, c'est de faire une compression dite intelligente et par définition réduire sensiblement le débit (de 30 à 80% en fonction de la scène).
L'impact de cette réduction est économique (réduction de l'espace de stockage c'est à dire moins de disques durs ou plus de qualité et de jour d'enregistrement sur une carte SD) et aussi moins de bande passante nécessaire sur le réseau, ce qui peut modifier le mode d'utilisation de la vidéo (transmission de plus de flux, augmentation du niveau de qualité, mobilité…).

La sécurité des réseaux

De plus en plus, des articles mettant en lumière des événements de cyber attaque ou de piratage, instaurent de fait une méfiance concernant la sécurité des réseaux.
La sécurité des réseaux doit être prise en compte dans le processus de conception et de déploiement en mettant en place l'architecture et les protocoles de sécurité qui permettent de sécuriser les informations.
En ce qui concerne la sécurisation des informations transmises sur les réseaux IP, il existe différents niveaux de sécurité. Le premier est l'authentification et l'autorisation. L'utilisateur ou le périphérique s'identifie auprès du réseau et de l'extrémité distante à l'aide d'un nom d'utilisateur et d'un mot de passe, qui sont ensuite vérifiés avant que le périphérique soit autorisé à accéder au système. Un niveau de sécurité additionnel peut être obtenu en cryptant les données afin d'empêcher toute autre personne de les utiliser ou de les lire. Les méthodes les plus couramment employées sont HTTPS (également appelé SSL/TLS), VPN et WEP ou WPA sur les réseaux sans fil. Selon le type d'implémentation et de cryptage utilisé, il peut arriver que le recours au cryptage ralentisse les communications. Une autre protection telle que la norme IEEE 802.1X, empêche la connexion à des périphériques non autorisés. La norme IEEE 802.1X établit une connexion point à point ou interdit l'accès depuis le port de réseau local en cas d'échec de l'authentification. Elle empêche ce que l'on appelle le « piratage de port », c'est-à-dire les attaques par lesquelles un ordinateur non autorisé accède à un réseau en se connectant à une prise réseau située à l'intérieur ou à l'extérieur d'un bâtiment. Cette norme est utile dans les applications de vidéo sur IP, car les caméras réseau sont souvent placées dans des lieux publics, où une prise réseau accessible à tous peut représenter un risque pour la sécurité. Dans les réseaux d'entreprise actuels, la norme IEEE 802.1X est devenue une exigence de base pour tout périphérique relié à un réseau.

Raccorder les sites distants via le réseau WAN internet

Les sites des clients sont souvent distants et doivent être raccordés via le réseau WAN internet. Les deux moyens les plus répandus permettant de sécuriser la transmission des données sont le protocole HTTPS utilisé notamment pour les transactions bancaires et le réseau Privé virtuel VPN.



Protocole HTTPS ou SSL/TLS

HTTPS (Hyper Text Transfer Protocol Secure) est une méthode de communication sécurisée qui envoie du code HTTP vers une connexion SSL (Secure Socket Layer) ou TLS (Transport Layer Security). Cela signifie que le code HTTP et les données sont cryptés.

De nombreux produits de vidéo sur IP disposent d'une prise en charge intégrée du protocole HTTPS, ce qui permet de visualiser les vidéos sur un navigateur Web en toute sécurité. Un certificat numérique et un couple de clés asymétriques doivent être installés sur les caméras réseau pour qu'ils puissent utiliser le protocole HTTPS. Le couple de clés est généré par le périphérique. Le certificat peut être soit généré et signé par le périphérique, soit délivré par un organisme de certification. Avec HTTPS, le certificat est utilisé tant pour l'authentification que le cryptage. Cela signifie que le certificat permet à un navigateur Web de vérifier l'identité de la caméra ou de l'encodeur et de coder la communication à l'aide des clés générées par un processus de cryptage à clé publique.

Réseau privé virtuel (VPN)

Avec la technologie VPN, il est possible de créer un « tunnel » sécurisé entre deux périphériques, et de sécuriser ainsi la communication par Internet. Dans ce type de configuration, le paquet d'origine, à savoir les données et leur en-tête, est crypté. Il peut contenir des informations telles que les adresses source et de destination, le type d'informations envoyées, le numéro du paquet dans une séquence et la longueur du paquet. Le paquet crypté est ensuite encapsulé dans un autre paquet qui n'affiche que l'adresse IP des deux périphériques communicants (des routeurs par exemple). Cette technique protège le trafic de tout accès non autorisé et seuls les périphériques possédant la bonne « clé » seront en mesure de fonctionner sur le VPN. Les périphériques réseau entre le client et le serveur ne pourront ni accéder aux données, ni les visualiser.

La différence entre les protocoles SSL/TLS et VPN est qu'avec les premiers, seules les données d'un paquet sont cryptées. Dans le cas du VPN, l'ensemble du paquet peut être crypté et encapsulé de manière à créer un « tunnel sécurisé ». Les deux techniques peuvent être utilisées en parallèle, mais cela n'est pas recommandé car chacune augmente la charge du système et en réduit les performances.

Précautions d'installation

Lors de l'installation et le choix du type de détecteur, quelques précautions doivent être prises :

Bien définir le but de la surveillance :

Vue d'ensemble ou haut niveau de détail, détection, reconnaissance ou identification. Les vues d'en-

semble permettent de surveiller une scène en général ou le mouvement d'ensemble des personnes qui s'y trouvent.
Les images de haute résolution sont importantes pour l'identification des personnes ou des objets (visages, plaques minéralogiques, surveillance de systèmes de point de vente). Le but de la Surveillance détermine le champ et le positionnement de la caméra, le type de caméra et d'objectif utilisé.
Le positionnement de la caméra est important pour capturer des images non déformées et éviter des vues trop verticales qui rendent l'identification difficile. Il est très probable que votre sujet soit en mouvement. Vous devrez choisir une fréquence d'images et une vitesse d'obturateur adaptées à vos objectifs de surveillance.

La Zone de couverture :
Pour un lieu donné, il faut déterminer le nombre de zones d'intérêt, la part de ces zones à couvrir et savoir si ces zones sont ou non proches les unes des autres. La zone à couvrir détermine le type de caméra et le nombre de caméras nécessaires.

Les Conditions ambiantes en intérieur ou en extérieur
Sensibilité à la lumière et besoins d'éclairage :
Les caméras présentent différentes sensibilités à la lumière. Deux facteurs sont à considérer : le nombre d'ouverture (nombre f) de l'objectif, qui doit être le plus faible possible (plus le nombre est petit, plus il est sensible à la lumière), et la caractéristique en lux (la plus faible étant la meilleure).
Cette dernière combine les caractéristiques de plusieurs éléments : l'objectif, le capteur et le traitement des images (il faut garder à l'esprit que les mesures ne sont pas les mêmes selon les fabricants de caméras vidéo : il n'existe pas de normes de mesure de la sensibilité à la lumière).
Dans les environnements extérieurs, l'utilisation de caméras jour / nuit est à envisager.
Certaines caméras proposent des technologies apportant une meilleure sensibilité à la lumière et fournissent des informations de couleurs même dans des environnements sombres. De la même manière, les caméras avec LED IR intégrées ou des projecteurs IR externes améliorent la qualité des vidéos noir et blanc en conditions de faible lumière et fournissent des vidéos exploitables, même dans l'obscurité la plus complète.
S'il n'est pas possible d'utiliser une lampe normale ou un projecteur IR, il faut envisager l'emploi d'une caméra thermique pour la détection dans l'obscurité complète. Pour des scènes avec contre-jour, comme cela se produit face à une fenêtre ou une porte, ou celles où coexistent des zones très lumineuses et des zones sombres, la solution peut être de déplacer la caméra pour obtenir une meilleure qualité vidéo. Si cela s'avère impossible, il faut envisager des caméras à plage dynamique étendue (WDR). Une bonne caméra de surveillance WDR peut fournir des images avec un niveau de détail acceptable dans les deux types de zones.

Niveau d'éclairage	Condition d'éclairage
100 000 lux	Plein soleil
10 000 lux	Plein jour
500 lux	Lumière intérieure d'un bureau
100 lux	Pièce faiblement éclairée

Les Protections :

Si la caméra doit être placée en extérieur ou protégée de son environnement, il faut choisir des caméras avec des caractéristiques adaptées : un indice de protection IP51/52. L'intérieur, IP66 et NEMA 4X à l'extérieur, IK08/10 contre le vandalisme et des températures de fonctionnement correspondant aux conditions ambiantes. Il existe des boîtiers spéciaux pour l'extérieur.

Normes de protection IP

Protection contre la pénétration de solides 1er Chiffre	Protection contre la pénétration de liquides 2ème Chiffre
1 : corps solides de plus de 50 mm IP 1x	1 : chutes verticales de gouttes d'eau IP x1
2 : corps solides de plus de 12 mm IP 2x	2 : chutes de gouttes d'eau jusqu'à 15° de la verticale IP x2
3 : corps solides de plus de 2,5 mm IP 3x	3 : pluie (0 à 60°) IP x3
4 : corps solides de plus de 1 mm IP 4x	4 : arrosages dans toutes les directions IP x4
5 : poussière IP 5x	5 : jets d'eau IP x5
6 : étanche à la poussière IP 6x	6 : lance d'arrosage pression 0,3 bar à 3 m IP x6 -
	7 : immersion < 1 m IP x7
	8 : matériel submersible immersion > 1 m IP x8

Normes de protection IK

Indice	IK 01	IK 02	IK 03	IK 04	IK 05	IK 06	IK 07	IK 08	IK 09	IK 10
Energie / Joule	0,15	0,23	0,35	0,5	0,7	1	2	5	10	20
Choc / kg	0,15	0,15	0,15	0,15	0,15	0,5	0,5	0,5	1	1
h / m	0,1	0,15	0,25	0,35	0,50	0,20	0,40	1	1	2

Les évolutions technologiques

Les IOT (Internet Of Things)

L'Internet des objets (IDO) ou Internet of Things (IOT) représente l'expansion d'Internet à des choses/objets et à des lieux dans le monde physique. L'Internet des objets désigne le « mouvement de liaison » d'objets quotidiens ou de nouveaux objets à Internet.

Il n'y a pas de définition officielle pour ce terme mais voici la définition d'internet des objets que nous trouvons la plus pertinente :

« L'internet des objets est un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant. »

Source : L'Internet des objets de Pierre-Jean Benghozi, Sylvain Bureau et Françoise Massit-Folléa (Edition MSH)

En pratique : sa composition

The internet of things est composé de six types de systèmes différents :

- L'identification : Elle permet d'identifier des objets et de recueillir leurs données
- De capteurs et détecteurs : Recueillir des informations de l'environnement pour améliorer le dispositif
- Une connexion : Connecter les systèmes entre eux
- Une intégration : Intégrer les systèmes entre eux
- Le traitement des données : Stocker et analyser des données (Big Data)
- Des réseaux : Transférer ces données entre le monde physique et virtuel

Afin que ce système soit optimal sept composants sont nécessaires. Tout d'abord la présence d'une étiquette virtuelle qui permette d'identifier les objets et les lieux, un moyen de déchiffrer ces étiquettes, un dispositif mobile, un logiciel pour dispositif mobile, un réseau sans fils (2G, 3G), une information sur chaque objet lié et un affichage pour lire l'information.

Les IOT appliqués à nos métiers

Plusieurs constructeurs se sont déjà lancés dans les IOT en développant une large gamme de produits IP (capteurs et détecteurs audio/vidéo intelligents, contrôle d'accès, haut-parleurs, interphones, Interfaces Entrées/Sorties…) permettant de proposer une solution globale pour les différents marchés (transport, logistique, commerces, santé, sites critiques, industrie…).

Ces IOT vont générer différentes données qui permettront après analyse, de créer et proposer des nouveaux services en plus de la sécurité tels que des services de marketing, de mesure (comptage de personnes, mesure de niveau d'une rivière…), d'accueil à distance, suivi de colis, trafic monitoring…

Afin de déployer facilement et inter connecter en toute sécurité ces IOT, des protocoles ont été développés et mis en place afin de s'affranchir des contraintes liées aux firewalls, routeurs sans pour cela mettre place de lourds VPN.

Des solutions pour chaque risque

Détecter des actes de malveillance

Agressions verbales, incivilités

Il existe aujourd'hui des technologies matures de détection automatique d'agressions verbales.

Toutefois, des dispositifs de prévention des incivilités sont actuellement intégrés dans certains systèmes de vidéosurveillance. Ils sont basés sur :

- Une détection automatique de l'agression sonore par un détecteur sonore
- Un mode de signalisation volontaire par la personne se sentant agressée (bouton poussoir, tablette tactile…)
- Un affichage dissuasif via un écran PLV (Publicité sur le Lieu de Vente) dont le contenu va être modifié dynamiquement lorsque l'employé signale une dérive de comportement d'un client : commutation sur un film de sensibilisation aux incivilités, commutation en direct sur la caméra visionnant l'individu. L'objectif étant essentiellement de dissuader avant le passage à l'acte, la télévidéosurveillance n'est pas sollicitée à ce stade.

Signalons également que de nombreuses caméras IP disposent de micro intégré et peuvent détecter un franchissement de seuil du niveau sonore ambiant. Si ce type alarme peut constituer une alternative à l'alarme volontaire pour contrôler un affichage dynamique, les télésurveilleurs ne sont pas prompts à accepter la gestion d'alarmes sonores :

- D'une part le micro de la caméra ne fera pas la différence entre une élévation normale du niveau sonore (passage d'un camion de pompier) et une élévation sonore liée à un individu qui s'emporte, d'où de nombreuses fausses alarmes.
- D'autre part, même si la levée de doute par télévidéosurveillance est techniquement possible avec des clips audio/vidéo, il y a un problème juridique lié à l'écoute d'une personne sans son consentement puisque les images et le son sont enregistrés dans la caméra et au centre de télésurveillance…

L'Analyse Vidéo Intelligente propose également aujourd'hui la détection de signatures intéressantes dans la détection de ce type d'incivilité, les technologies étant issues de recherches sur les mouvements de foule :

- Détection sonore d'agression verbale,
- Détection sonore de coups de feu,
- Détection sonore d'alarme de voiture,
- Détection sonore de bris de verre,
- Détection sonore de spray d'aérosols graffitis,
- Détection vidéo d'attroupement (les autres personnes prennent fait et cause pour l'agresseur),
- Détection vidéo de dispersion rapide (les personnes se désolidarisent et s'éloignent de l'agresseur),
- Détection vidéo de mouvements brusques d'une personne (l'agresseur, l'agressé ou un autre client effrayé).

Plusieurs de ces techniques sont actuellement testées en vidéosurveillance urbaine et dans des PC de Sécurité de lieux publics : il en ressort généralement qu'une multitude de faits normaux produisent des signatures similaires aux faits que l'on souhaite détecter, rendant rapidement ces dispositifs peu crédibles aux yeux des agents d'exploitation.

Enfin, des études scientifiques sur l'analyse comportementale permettent aux éditeurs de logiciels spécialisés dans l'Analyse Vidéo Intelligente d'entrevoir la possibilité d'intégrer dans les caméras des algorithmes de détection de changement d'expression des visages (colère, mépris, dégoût, peur…) : couplés à une levée de doute vidéo en télévidéosurveillance, ces technologies pourront peut-être un jour se substituer à la signalisation volontaire par la personne agressée ?

Agressions physiques, vols à main armée (VMA), prises d'otages

Actuellement, plusieurs techniques de détection sont déployées :

- L'alarme agression, par composition volontaire d'un code sous contrainte, appui sur un bouton d'agression, activation d'un équipement de protection individuelle, non appui sur un bouton d'acquittement…
- L'alarme dite « comportementale », par non respect volontaire, par les employés, des procédures obligatoires (ouverture d'un coffre tout en laissant la porte du local coffre ouverte…)
- La détection automatique d'agression d'un employé à l'ouverture d'un commerce le matin ; celle-ci utilise soit l'Analyse Vidéo Intelligente pour compter le nombre de personnes pénétrant dans le commerce : si l'employé rentre seul, tout va bien, si une personne l'accompagne (alors que la procédure l'interdit), il y a suspicion d'agression ou l'analyse sonore pour détecter une agression verbale.

La télévidéosurveillance permet de lever le doute face aux erreurs de manipulations ou au non respect des consignes et d'alerter la police sur des situations critiques confirmées.

Intrusions et cambriolages

C'est dans ce domaine que la télévidéosurveillance rencontre aujourd'hui le plus de succès :
En permettant la vérification des alarmes directement par les opérateurs, elle évite d'exposer inutilement les responsables des sites ou leurs mandataires par une vérification sur site alors que des intrus opèrent
En autorisant l'alerte des forces de l'ordre lorsqu'une infraction est confirmée par les images, elle permet des arrestations en flagrant délit : encore faut-il que la police soit appelée très rapidement. Il convient donc que les clients, installateurs et télésurveilleurs,

s'entendent sur la mise en œuvre des techniques de levée de doute rapide (push, pull, Analyse Vidéo Intelligente).

Détecter une intrusion et lever le doute à l'intérieur de bâtiments

Télévidéosurveillance par Pircam

De nombreux systèmes de télévidéosurveillance utilisent des détecteurs d'intrusion intégrant des caméras dont les champs de vision recouvrent les zones de détection des capteurs de mouvements : une série de photos ou clips vidéo pris au moment des alarmes est présentée aux opérateurs conjointement à l'alarme intrusion. Ces détecteurs/caméras sont appelés couramment Pircam (Passive Infra-Red Camera). Ils ne bénéficient généralement pas des certifications produits NFA2P qui pourraient être requises pour la couverture de niveaux de risques élevés (au sens de l'assurance).

Autres systèmes de télévidéosurveillance

D'autres systèmes de télévidéosurveillance consistent à coupler les systèmes de détection d'intrusion classiques avec les systèmes de vidéoprotection des mêmes sites.

Le couplage de type « asservissement entre systèmes » (ou mode « push ») n'est pas toujours aisé à réaliser techniquement et rarement pérenne : systèmes d'alarme et systèmes de vidéosurveillance ne répondent pas aux même attentes des clients et il n'est pas rare de voir les investissements successifs diverger dans le temps entre les deux systèmes, conduisant parfois à des installateurs et mainteneurs différents pour l'alarme et pour la vidéosurveillance.

C'est pourquoi, il est souvent préféré un couplage « logique » effectué par l'informatique du centre de télésurveillance (mode « pull » dont le fonctionnement a été décrit plus haut). Ce mode de couplage permet une évolution non concertée des équipements d'alarme et de vidéosurveillance : si un couplage caméra/détecteur est possible, il permettra une levée de doute automatique par télévidéosurveillance ; si aucun couplage caméra/détecteur n'est possible ou s'il n'est plus possible pour un détecteur, la levée de doute devra s'opérer par les moyens traditionnels. A noter que l'information du télésurveilleur par le client (via ses installateurs) lorsqu'une modification intervient sur un des systèmes d'alarme ou de vidéosurveillance est indispensable au maintien des couplages logiques.

Détecter une intrusion et lever le doute à l'extérieur des bâtiments

La télévidéosurveillance à l'extérieur des bâtiments représente un enjeu important pour de nombreux sites, notamment en raison de l'accélération des vols de carburants sur les véhicules parqués, et plus généralement, des vols de matériels et équipements stockés à l'extérieur des bâtiments.

La clé du succès consiste à résoudre une équation à trois inconnues :

- Un système de détection extérieur couvrant soit les secteurs à risques (parcs véhicules, aires de stockage), soit les points d'intrusion potentiels sur le site, va permettre la transmission d'une alarme en télésurveillance ; inconnue 1 : quelle technique mettre en œuvre (barrières infrarouges, câbles détecteurs sur clôtures, lasers…)?
- La vérification par télévidéosurveillance va permettre de faire appel aux forces de l'ordre ; inconnue 2 : le système de vidéosurveillance est-il qualifiant sur tout le site et tout le temps (de jour, de

nuit, par temps de pluie, neige, brouillard, en cas de coupure d'électricité sur le site…) ?
- L'arrivée rapide des forces de l'ordre pourra conduire à des arrestations en flagrant délit ; inconnue 3 : combien de temps s'est-il écoulé entre le déclenchement de l'alarme et l'arrivée sur place des forces de l'ordre ?

Les techniques de type « Pircam » se révèlent peu efficaces en extérieur : portée de détection limitée, instabilité (fausses alarmes), faible qualité des images de levée de doute : installateurs et télésurveilleurs limitent généralement leur usage au piégeage de points de passages obligés.

Par ailleurs, associer des systèmes de détection extérieurs éprouvés (barrières infrarouges, hyperfréquences, laser, câble enterré, câble choc sur clôture…) à de la levée de doute vidéo nécessite une expertise technique importante. La difficulté essentielle consiste à fournir en télévidéosurveillance des images de levée de doute qualifiantes quelles que soient les conditions d'éclairage (jour/nuit) et d'intempéries (pluie, neige, brouillard) et quel que soit le point de pénétration sur le site : une image où un intrus ne représente que 2 ou 3 pixels à l'image parce qu'il est loin de la caméra ne permettra pas à l'opérateur de lever le doute.

Là-aussi, l'Analyse Vidéo Intelligente associée à des caméras « visibles » ou « thermiques » simplifie la conception des systèmes de détection et de levée de doute vidéo qui ne font plus qu'un seul système. L'équation à trois inconnues devient une équation à deux inconnues : détection/levée de doute, alerte/intervention des forces de l'ordre.

La contrepartie de la simplification de la conception est qu'il convient de s'assurer de la robustesse de ces systèmes, notamment leur résistance à la fraude et à la panne :
- Stabilité satisfaisante du système (trop de fausses alarmes fragilise l'exploitation)
- Autonomie de fonctionnement de plusieurs heures de la chaîne de détection, d'alerte et de levée de doute en cas de coupure secteur,
- Modes de transmission multiples des alarmes vers le télésurveilleur afin de pallier à la défaillance d'un réseau de transmission,
- Supervision de la bonne orientation des caméras et de leur non obstruction,
- Supervision du bon fonctionnement des caméras et des processus d'Analyse Vidéo Intelligente.

Des solutions de supervision automatiques existent :
- Au niveau des enregistreurs numériques : détection de masquage, floutage, dé-azimutage, défocalisation des caméras, perte de connexions ; ces alarmes sont transmises en télésurveillance,
- Directement depuis les systèmes informatiques d'exploitation des centres de télésurveillance : interrogation cycliques des équipements, vérification de bon fonctionnement des processus vitaux (comme l'analyse vidéo intelligente).

Quelle que soit la pertinence de ces processus automatiques, il peut être intéressant de programmer également des rondes vidéo régulières effectuées par les opérateurs (une fois par mois ou par semaine).

Vol et démarque inconnue

De nombreux systèmes existent pour lutter contre la démarque inconnue, les plus connus étant les étiquettes antivol associées à des portiques de détection installés aux entrées/sorties des commerces.

L'exploitation est locale et mobilise des agents de

sécurité en surface de vente et des agents de sécurité dans les PC de Sécurité. Les besoins de télévidéosurveillance actuellement exprimés par les responsables sécurité de grandes chaînes vont dans le sens d'une mutualisation de leurs PC de sécurité (un PC de sécurité régional ou national, versus un PC de sécurité par magasin). Certains ont franchi le pas et sont satisfaits.
Nous n'avons pas connaissance aujourd'hui d'expériences d'externalisation de ces missions sur un centre de télésurveillance.

Dégradations volontaires et vandalisme

Avant de privilégier telle ou telle technique de détection en vue d'une télévidéosurveillance, il convient de se poser la question suivante :
Un délai de réaction de plusieurs minutes entre la commission des faits et l'arrivée sur les lieux d'une force d'interposition (privée ou publique) est-il acceptable ?
En fonction de la réponse à cette question, il conviendra de choisir entre plusieurs solutions possibles :
Réponse négative (un tel délai n'est pas acceptable) :

- Ne rien faire (les biens sont assurés ou les investissements trop importants par rapport à la valeur des biens)
- Agent de sécurité sur place
- Moyens de vidéosurveillance avec enregistrements pour dissuasion, investigation et dépôts de plaintes éventuels

Par exemple, les musées déploient des tags RFID pour détecter le mouvement/choc/déplacement des œuvres exposées, avec des caméras de surveillance pour vérifier les alarmes et identifier les auteurs : dans la journée, ces caméras sont toujours exploitées dans un PC de Sécurité local et un agent de surveillance est souvent à proximité immédiate des œuvres.
Par contre, la nuit, le conservateur pourra accepter une solution de télévidéosurveillance, car il sait que, avant d'accéder aux œuvres, un intrus aura été détecté en amont et que sa progression sera freinée par des obstacles mécaniques (portes des salles fermées à clés, par exemple), laissant ainsi le temps aux agents de sécurité d'intervenir.

Réponse positive (délai acceptable) :

- Télévidéosurveillance avec intervention des forces de l'ordre
- Éventuellement, installation de moyens de vidéosurveillance complémentaires

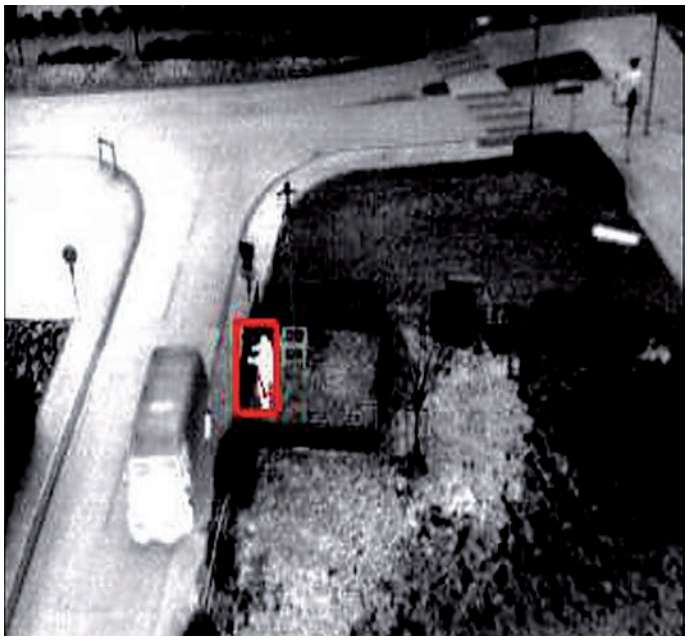
Par exemple, des caméras installées sur des mâts dans un quartier où s'opèrent des trafics de drogue peuvent provoquer deux réactions de la part des dealers :

- Réorganisation du trafic en dehors de la zone sous vidéoprotection
- Vandalisme des caméras

Nous pouvons citer un exemple concret où plusieurs mâts de vidéosurveillance sont sécurisés par télévidéosurveillance par des caméras thermiques opérant en vue plongeante depuis les toits des immeubles voisins.
Un no man's land doit être construit autour des mâts pour renforcer leur protection physique et pour éviter les déclenchements d'alarmes intempestifs par les chiens qui viendraient se soulager…
En cas de détection d'intrusion dans le no man's land, l'Analyse Vidéo Intelligente détoure l'intrus dans les images et transmet l'alarme et la vidéo au centre de télésurveillance. Après vérification, l'opérateur alerte la police municipale et la gendarmerie.

Caméra de télévidéosurveillance thermique

Intrus détecté dans le no man’s land



Élément protégé en plein jour (dispositif de vidéoprotection urbain, géré par la Ville)

Espionnage (secteur économique, industriel)
Les mesures de prévention en matière d'espionnage généralement prises par les entreprises sont :

- Le contrôle des accès (DESFire, biométrie, reconnaissance faciale avec alertes en télévidéosurveillance)
- La détection des intrusions en secteurs sensibles (salles informatiques)
- La télévidéosurveillance des locaux sensibles, par des caméras en installations fixes ou en dispositifs de vidéosurveillance temporaires (caméras cachées).

La principale difficulté pour un opérateur de télésurveillance amené à lever le doute sur une alarme intrusion dans un bâtiment, est qu'il n'est pas en capacité de faire la distinction entre un employé et un espion. Tout au plus, peut-il informer rapidement le client de la présence d'une personne dans un lieu sécurisé et lui transmettre les images sur son téléphone portable ; charge au client de consulter les images et de demander à l'opérateur soit de classer l'alarme, soit d'envoyer la police ou un intervenant privé.

Terrorisme
L'analyse vidéo intelligente permet de détecter des objets abandonnés dans un lieu public sous vidéoprotection. Cette technologie fonctionne, mais elle détecte tout ce qui n'a pas bougé depuis plus d'un certain temps dans une zone donnée, en éliminant le fond (murs et mobiliers).

En pratique, de nombreux cas non anticipés de stationnarité normale viennent polluer le fonctionnement de ces détecteurs automatiques rendant cette technologie complexe à utiliser en télévidéosurveillance privée.

De plus, suite à l'explosion d'un colis explosif réellement abandonné ayant généré une alarme qu'un opérateur aurait classé trop rapidement sans suite, on peut imaginer les conséquences en recherche de responsabilité pour la société de télésurveillance impliquée…

Détecter les risques incendie, les risques naturels, les risques industriels

Détecter et lever le doute à l'intérieur
La détection par des détecteurs automatiques d'incendie est réglementaire et normalisée. La télévidéosurveillance permet, dans certaines conditions, de lever le doute sur un déclenchement intempestif d'un détecteur automatique. Mais, dans une pièce enfumée, une caméra avec leds infrarouges produit une image inexploitable. Compte-tenu des responsabilités en cas de mauvaise interprétation, les télésurveilleurs acceptant d'assurer ce type de prestation déclinent contractuellement toute obligation de résultat.

Détecter et lever le doute en extérieur
Sous certaines conditions, une détection de départ de feu peut être réalisée en extérieur par des caméras thermographiques (caméras thermiques mesurant la température en tout point de l'image) avec :
Alarme par détection de franchissement de seuils de températures (fonctions intégrées dans les caméras)
Et alarme par une Analyse Vidéo Intelligente des images mesurant la croissance et/ou détectant la propagation d'une zone « chaude » (isotherme), si-

gnature caractéristique d'un départ de feu.

La télévidéosurveillance est toujours associée à un dispositif de signalisation locale d'incendie sur le site destiné à alerter les personnes éventuellement présentes.

Risques naturels

La détection et la vérification de risques naturels à évolution lente pourraient techniquement être gérées en télévidéosurveillance : par exemple, la détection de la montée des eaux sur les berges d'une rivière. Là encore, même si des techniques de détection et de levée de doute vidéo existent, il convient de s'interroger sur la pertinence de l'intervention d'un prestataire privé dans la chaîne de détection et d'information et de mesurer les conséquences :
d'un délai technique d'information de l'autorité responsable de plusieurs minutes après la détection des faits
de la possibilité d'une mauvaise interprétation des images par un opérateur « généraliste » par opposition à un agent d'exploitation public ou privé spécifiquement formé et sensibilisé pour ce type de risques

Risques industriels

Généralement détectées par des capteurs industriels, les alarmes liées à la prévention des risques industriels ne peuvent pas toujours être confirmées par des caméras de vidéosurveillance : par exemple, une fuite de gaz n'est pas visible, ni avec une caméra traditionnelle, ni avec une caméra thermique standard.

Il existe toutefois des caméras thermographiques disposant de capteurs spécifiques, fonction du type de gaz à détecter, permettant de visualiser les fuites de gaz : ce type de caméras peut-être relié sans problème en télévidéosurveillance.

D'une manière générale, la télévidéosurveillance peut constituer un moyen de coordination des actions de secours en permettant aux opérateurs de rétrocéder aux services d'intervention des informations utiles comme :
La localisation précise des secteurs en alarme,
L'ampleur d'un phénomène,
L'évolution d'un phénomène d'une alarme à une autre.

Risques individuels : télévidéosurveillance et vie privée

Les risques liés la personne recouvrent la détection de chute ou de malaise par PTI (équipement de Protection du Travailleur Isolé), les systèmes de téléassistance (médaillons d'appel d'urgence pour personnes âgées ou handicapées), ou encore les bracelets électroniques.

La télévidéosurveillance, lorsqu'elle est possible, permet de qualifier l'alarme, éliminer des fausses alarmes et parfois rendre compte de la gravité d'une situation.

Pour autant, on constate en pratique que la présence de caméras de levée de doute est souvent ressentie comme intrusive et policière aussi bien par les personnes concernées par la surveillance que par les intervenants amenés à travailler dans l'environnement vidéo surveillé de la personne.

Ainsi, on a vu des infirmières refusant d'intervenir auprès d'une personne âgée si les soins devaient

être dispensés devant une caméra et exiger de pouvoir couper la caméra lorsqu'elles sont présentes.

La miniaturisation et la baisse de coût des caméras thermiques peuvent révolutionner le marché de la télévidéosurveillance individuelle. Par rapport à une caméra traditionnelle ce type de caméra est non intrusif car elle ne permet pas de reconnaître une personne.

Une caméra thermique peut être installée en fixe dans une pièce, mais aussi embarquée dans un Smartphone. Les images produites peuvent parfaitement lever le doute suite à un appel volontaire, sans porter atteinte à l'intimité des personnes.

Associées à une Analyse Vidéo Intelligente, une caméra thermique peut détecter une situation anormale comme la chute d'une personne.

Synthèse

Ce groupe de travail a démontré que le choix des bonnes techniques de télévidéosurveillance conduit dans de nombreux cas à une vraie efficacité dans la prévention, la détection et le traitement des risques. L'Analyse Vidéo Intelligente prend aujourd'hui le pas sur les technologies classiques et le couple humain-technologie rencontre des succès indéniables : le nombre d'arrestations en flagrant délit par les forces de l'ordre sur appel télésurveillance après levée de doute en télévidéosurveillance en témoigne.

Comment l'exploitant en bout de chaîne, le centre de télésurveillance, vit-il cette mutation ?

Traitement au PC

La prévention, la détection et la qualification/vérification des actes de malveillance et des risques incendie, naturels et technologiques utilisent de plus en plus la télévidéosurveillance.
Deux offres de télévidéosurveillance sont disponibles sur le marché, l'une propose une infrastructure et des services gérés par des professionnels de la télésurveillance, et l'autre propose une solution gérée par des particuliers (solution d'auto vidéosurveillance).

La télé surveillance réalisée par des professionnels

Beaucoup trop de clients imaginent encore un centre de télévidéosurveillance comme un poste de gardiennage d'un grand site industriel, avec un nombre de gardiens et un nombre d'écrans beaucoup plus important, s'agissant de surveiller non pas un seul site mais plusieurs dizaines de milliers de sites : lorsqu'un site est en alarme, les caméras de ce site seraient automatiquement affichées sur un écran et un des opérateurs disponibles regarderait l'écran. Une mutualisation de moyens de gardiennage en quelque sorte, rendue possible grâce au transport de la vidéo sur les réseaux publics.

Un centre de télésurveillance est avant tout un centre de traitement d'alarmes entrantes, plusieurs milliers d'alarmes par jour, la plupart n'étant liées ou liables à aucune caméra : alarmes techniques, défaut de fonctionnement, défaut de liaison avec les sites, absence de mise sous surveillance… Ces alarmes entrantes s'empilent dans le système informatique de gestion du centre de télésurveillance et plusieurs opérateurs les dépilent en frontal devant leurs écrans de travail. Règle du jeu : respecter un délai de prise en compte réglementaire de 3 minutes maximum (Règle APSAD R31) entre l'arrivée de l'alarme et le début de traitement de cette alarme par un opérateur.

Toutes les alarmes reçues doivent être traitées. Elles font donc l'objet de consignes détaillées du traitement à réaliser par les opérateurs : appel du client ou de ses mandataires, envoi d'un intervenant sur place, suivi et compte-rendu de l'intervention…

Parmi ces milliers d'alarmes présentées aux opérateurs, quelques-unes sont notifiées comme bénéficiant d'un dispositif de levée de doute vidéo. Pour celles-ci, l'opérateur aura donc la possibilité d'analyser des images afin de qualifier ou vérifier l'alarme : à la suite de cette analyse, certaines alarmes seront classées comme fausses alarmes, d'autres alarmes entraîneront l'appel direct des forces de l'ordre.

Ainsi, à la différence de la vidéoprotection où des agents postés dans des Centres de Supervisions Urbains observent 24h/24 des écrans et pilotent des caméras, la télévidéosurveillance relève plus d'analyses ponctuelles d'images par des opérateurs dans un contexte de vérification d'une alarme entrante.

Le métier de télésurveilleur

Le métier de télésurveilleur poursuit son évolution naturelle, principalement grâce aux innovations technologiques qui sont à notre disposition et que la plupart d'entre nous utilisent déjà, la vidéosurveillance à distance par l'IP avec l'analytique en est une.
Si le rythme de transformation de certaines missions du télésurveilleur s'accélère, cette phase de développement de nos activités est logique et déjà anticipée par les professionnels de la sécurité et sûreté à distance.
Le télésurveilleur possède un véritable rôle d'intégrateur, tant par la multitude de protocoles gérés,

les réseaux, serveurs, logiciels et matériels divers… et ce avec le souci de rendre interopérable toute la chaîne pour délivrer le service au client. Le professionnel de la télésurveillance, qui en principe est soumis aux règles APSAD, est vigilant quant à la fiabilité de tous ses systèmes et ceux-ci sont testés régulièrement, aucune faille n'est permise dans ce métier à hauts risques.

Il est à noter que cette interopérabilité n'est pas une évidence, dans la mesure où il n'existe à l'heure actuelle aucune norme définissant les critères à remplir par les différents équipements ou systèmes pour leur permettre de fonctionner avec des équipements ou systèmes tiers. Des initiatives industrielles comme Onvif ou PSIA tentent de créer des spécifications techniques visant à devenir des standards, mais la conformité à ces standards ne garantit pas l'interopérabilité des équipements.

Le rôle d'intégrateur du télésurveilleur s'en trouve d'autant plus renforcé, car il lui appartient de vérifier que les différents maillons de la chaîne technologique lui permettront de délivrer le service attendu. Ceci implique une validation préalable lors de la reprise éventuelle d'un parc de vidéosurveillance appartenant à son client.

L'exigence de nos clients est croissante, tant par la qualité et rapidité du traitement des évènements, que par les « reportings » fournis et l'accès aux informations.

La télévidéosurveillance ne vient pas se substituer aux missions de prestations humaines (agents, personnel du client, etc.) mais les complète et les améliore.

La mission principale du télésurveilleur est bien de surveiller à distance des personnes et/ou des biens avec les prérequis suivants :

- Disposer de tous les moyens pour recevoir, analyser, traiter et gérer des informations en provenance de systèmes de détection et de respecter les procédures définies avec le client, en cas d'évènement, incident ou simplement sur demande.
- Mettre en place des « Processus » clairs pour le personnel exploitant, définis avec le client pour anticiper chaque incident ou évènement, permettant d'appliquer les mesures adaptées à une situation et/ou nature d'évènement (l'opérateur a une mission prioritaire qui est l'application des procédures et consignes définies au moment de la signature du contrat).
- Acteur principal lors d'un déclenchement d'alarme, il est le lien entre les différents services ou entités, susceptibles d'être sollicités pour intervenir : agent d'intervention, forces de l'ordre. Ce rôle lui assigne dans la plupart du temps le pilotage des actions engagées et les reportings.

Les technologies et matériels devenant plus fiables, performants, et s'appuyant sur des réseaux permettant le traitement en temps réel, ce n'est pas un scoop en affirmant que le couplage de systèmes de détection avec de la vidéo, est désormais incontournable, voire il devient presque inacceptable de continuer à transmettre des informations «aveugles» aux télésurveilleurs.

L'organisation humaine et matérielle des stations de télésurveillance

Les stations de télésurveillance gèrent la sécurité des biens et des personnes de leurs clients, elles sont en possession de nombreuses informations sensibles leur permettant d'appliquer les plans d'actions en cas d'alarme, en particulier des mots de passe, coordonnées de contacts, codes d'accès.
Elles doivent être en mesure d'assurer un service fiable 24h/24 365j/an quelles que soient les conditions. Les données vidéos et autres informations liées à l'évolution du métier sont autant de risques qu'il faut gérer au quotidien. Pour toutes ces raisons, les stations de télésurveillance sont pour la plupart des centres fortement protégés, tant physiquement par la protection des structures, des alimentations électriques et téléphoniques et des secours qu'électroniquement par le contrôle strict des accès aux locaux, aux données, aux vidéo et aux réseaux IP à fortiori. La traçabilité totale des actions opérateurs, les sauvegardes et l'accès à celles-ci sont une garantie de transparence pour les clients et de preuves le cas échéant. Le backup d'une station sur une station de repli est un élément majeur de la sécurité d'une station. Les opérateurs ainsi que les superviseurs sont les pièces maîtresses du fonctionnement de la station. Ils traitent les évènements d'alarmes reçus par la station. La planification pour une bonne adéquation charge/capacité est également une des clés de qualité du service produit. Grâce aux moyens informatiques, les opérateurs ne traitent en moyenne qu'environ 2% des informations reçues en station, ce qui représente néanmoins un volume important, mais seulement 0,1% de celles-ci font l'objet d'un appel des Forces de l'Ordre. L'APSAD, grâce à la règle R31 pour les stations, est actuellement l'organisme qui garantit le référentiel et le contrôle objectif de l'application des règles édictées.

Les outils du télésurveilleur

La ronde vidéo : un outil de contrôle
C'est une prestation de télévidéosurveillance ponctuelle, opérée depuis un centre de télésurveillance pour une durée limitée dans le temps, généralement de quelques minutes au plus. Elle peut être programmée aléatoirement ou à heure fixe dans le système informatique de gestion du centre de télésurveillance : c'est donc une mission qui s'insère dans la pile des alarmes entrantes du centre de télésurveillance et dont se saisit un opérateur disponible du centre de télésurveillance.

La ronde vidéo constitue un moyen de prévention des risques : elle peut permettre aux opérateurs de constater une situation anormale, caractéristique d'un fait imminent, en cours ou déjà survenu. De par son caractère non permanent, elle ne peut être considérée comme un moyen fiable de détection des risques.

Par contre, la ronde vidéo permet de vérifier la disponibilité et la qualité des images des caméras déployées sur les sites distants, caméras qui pourraient se révéler capitales pour lever le doute sur une alarme future.

La levée de doute vidéo : un outil de qualification
Sous ce vocable, on regroupe toutes les techniques permettant aux opérateurs de qualifier/vérifier par l'image, les alarmes générées sur les sites distants

par des personnes ou des équipements de surveillance automatique.

Les techniques aléatoires et chronophages de levée de doute

Beaucoup s'imaginent que la seule disponibilité d'un système de vidéosurveillance et d'une connexion Internet permet d'effectuer une levée de doute vidéo par télévidéosurveillance : ce sont évidemment deux conditions nécessaires, mais pas suffisantes.

En effet, il convient de se remettre dans le contexte du traitement d'une alarme : lorsqu'un opérateur se saisit d'une alarme dans la pile des alarmes entrantes, celle-ci date déjà de plusieurs secondes à … plusieurs minutes. Même si, grâce à des mécanismes de priorisation, la moyenne des temps de prise en compte des alarmes se situe le plus souvent au-dessous de la minute, ce décalage entre le fait générateur d'une alarme et la disponibilité d'un opérateur pour traiter cette alarme permet de comprendre le défit technique de la levée de doute vidéo.

Connexion en direct par l'opérateur sur les caméras

Cette technique est aléatoire, car plusieurs secondes après les faits, les images fournies en direct par les caméras peuvent ne rien révéler sans pour autant qu'il ne se soit rien passé : par exemple, dans le cas d'un système de détection d'intrusion extérieur, un intrus détecté au franchissement d'une clôture et visible à ce moment là par une caméra extérieure, peut déjà être hors champ de vision de toute caméra lorsque l'opérateur se connecte en direct. Si l'intrus est encore visible, tant mieux, on pourra prévenir les forces de l'ordre. Si l'opérateur ne constate rien d'anormal, il faudra le plus souvent prévenir le client et/ou envoyer un intervenant pour vérifier sur place.

Recherche d'images sur les enregistreurs vidéo des sites

Si l'opérateur dispose des moyens techniques et des droits pour consulter les enregistrements vidéo d'un site en alarme, il peut rechercher les images enregistrées au moment de l'alarme.

Cette technique est chronophage, car l'opérateur doit successivement rechercher la présence d'enregistrements sur les bonnes caméras à l'heure de l'alarme (pour faciliter les choses, la plupart du temps les enregistreurs ne sont pas à l'heure) et ensuite rapatrier ceux-ci ou les lire en streaming au travers d'un réseau ne disposant généralement pas d'une bande passante adaptée (l'ADSL privilégie les flux d'informations descendant vers le site client au détriment des vidéos qui remontent vers le centre de télésurveillance).

Il faut souvent plusieurs minutes supplémentaires pour aboutir (ou non) à une levée de doute qualifiante avec cette technique.

Les techniques de récupération automatique d'images qualifiantes

Les techniques les plus efficaces sont celles où les images qualifiantes sont automatiquement associées aux alarmes et directement soumises à l'analyse des opérateurs. Ces techniques nécessitent un couplage « caméra-détecteur » réalisé soit :

- par l'installateur des systèmes de sécurité, par réalisation d'asservissements entre les systèmes de détection et les systèmes de vidéosurveillance,
- au niveau du centre de télésurveillance, par paramétrage du système informatique de gestion du

USP Technologies Télévidéosurveillance Livre blanc

centre de télésurveillance,
- par Analyse Vidéo Intelligente, procédé consistant à transformer la caméra à la fois en détecteur et en dispositif de levée de doute vidéo.

Dans tous les cas, un mauvais couplage « caméra-détecteur » peut conduire à la production d'images hors contexte à l'opérateur qui, de bonne foi, procédera au classement d'une intrusion réelle en fausse alarme. D'où la nécessité d'une conception sans faille des systèmes et d'une forte collaboration entre l'installateur du système de surveillance et le télésurveilleur du site.

Le mode « push »

Dans ce mode, les équipements de surveillance du site sous télévidéosurveillance transmettent à la fois les alarmes et des clips vidéo ou images qualifiantes au centre de télésurveillance. L'opérateur qui se saisit du traitement de l'alarme dispose déjà des images sur son poste informatique. Sa mission est donc de qualifier les images reçues sans avoir besoin d'aller les chercher. L'efficacité du dispositif repose sur la qualité du couplage « caméra-détecteur » réalisé par l'installateur du système de télévidéosurveillance.

Le mode « pull »

Dans ce mode, c'est l'informatique de gestion du centre de télésurveillance qui, à la réception d'une alarme et avant qu'un opérateur se saisisse de celle-ci, va se connecter sur les équipements vidéo du site et requérir les images qualifiantes afin de les associer à l'alarme reçue. L'efficacité du dispositif repose également sur le couplage « caméra-détecteur » conçu par l'installateur du système de télévidéosurveillance et communiqué au centre de télésurveillance. On parle de mode « pull » ou encore parfois « d'opérateur logique ».

Le mode « détection et levée de doute vidéo par Analyse Vidéo Intelligente »

Les alarmes et pré-alarmes sont directement générées par des systèmes d'Analyse Vidéo Intelligents exploitant les images des caméras de surveillance afin d'y repérer des « signatures » caractéristiques des faits et risques que l'on souhaite détecter : intrusion d'un intrus dans une zone, départ de feu, agression potentielle d'un employé…

Dans ce mode, il n'y a plus de problème de couplage « caméra-détecteur » car la caméra est, en quelque sorte, le détecteur. De plus, avant de transmettre les images au centre de télésurveillance, le dispositif d'Analyse Vidéo Intelligente les enrichit d'informations destinées à en faciliter l'analyse par les opérateurs.

<u>Exemples :</u>
- Détourage dans les images du ou des intrus dans le cas d'une détection d'intrusion,
- Inscription des valeurs de température mesurées dans le cas de la détection d'un départ de feu,
- Détourage de l'employé et de l'agresseur dans le cas d'une détection d'agression.

La multiplicité des techniques de détection existantes et l'émergence de nouvelles techniques de détection par Analyse Vidéo Intelligente ne doivent pas faire oublier aux clients et aux installateurs que ce sont des hommes qui sont au cœur du traitement de l'information. Même si les dernières technologies autorisent des levées de doute rapides et plus sûres par les opérateurs, trop d'alarmes intempes-

tives peuvent discréditer complètement un site télévidéo surveillé aux yeux des opérateurs et affaiblir leur vigilance pour l'analyse des images de celui-ci.

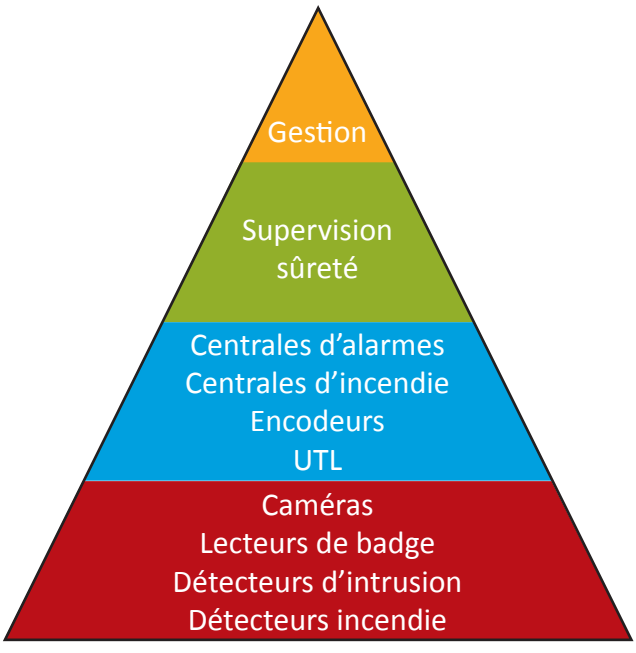
Les outils d'Hypervision

Historiquement, les systèmes de sécurité (vidéosurveillance, détection incendie, contrôle d'accès et autres) ont toujours été séparés des systèmes de surveillance de la production. Toutefois, les technologies ont fortement évolué et les performances des PC modernes rassurent, tout comme la robustesse des logiciels industriels. Désormais, piloter une machine depuis un PC est devenu courant, et les logiciels surveillent des processus toujours plus critiques.

Comme son nom l'indique, un système d'hyper vision (ou "hyperviseur") sera placé au-dessus de la supervision. Capable d'accéder à toutes les données relatives aux processus de l'entreprise, il en profite pour agréger des données provenant d'autres systèmes informatiques (sécurité, mais aussi confort des employés), de manière à proposer aux utilisateurs de nouvelles fonctions, voire de nouvelles méthodes de travail.

Grâce à l'hyper vision, les fonctions vidéo peuvent être pilotées directement depuis un hyperviseur graphique unique, commun à tous les systèmes de sécurité d'un bâtiment (contrôle d'accès, intrusion, incendie, GTB, ...).

Pour aller vers toujours plus de sécurité, l'hyperviseur pourra accélérer la prise de décision et la levée de doute. En cas d'alarme, l'exploitant pourra réagir beaucoup plus vite car le logiciel lui proposera une aide au diagnostic, un choix entre plusieurs actions à mener, et le déroulement des procédures correspondantes. C'est ce que l'on appelle l'"aide à la décision". Dans le cas d'un aéroport qui comprend des zones très sensibles (douanes, tri des bagages, etc.), il faut pouvoir prendre des mesures très rapides en cas de bris de porte ou de déclenchement d'une alarme. L'hyperviseur affichera donc des messages du type "voulez-vous afficher la vidéo en direct ?" "Faut-il prévenir les services de police ? ou encore "souhaitez-vous tracer l'itinéraire pour vous rendre sur les lieux ?". Au final, « l'hyper vision, c'est une interface unique, homogène et adaptable qui assure l'interopérabilité entre les systèmes et effectue le filtrage de toutes les données en fonction du contexte ou de l'utilisateur. »



La télévidéosurveillance réalisée par des particuliers

Qu'est ce que l'auto-vidéo-surveillance ? C'est la faculté donnée à toute personne de pouvoir à distance visualiser un site et de pouvoir ainsi le «surveiller» par ses propres moyens.

Les technologies actuelles permettent sans grande difficulté de mettre en place des caméras accessibles à distance, permettant à tout un chacun, de se connecter et de visualiser son domicile, son bureau, son magasin, ses entrepôts, etc. Une bonne liaison Internet est nécessaire, mais le très haut débit se généralise, et cette contrainte n'en est souvent plus une.

De nombreuses offres sur le marché sont apparues sur ce créneau, et de simples webcam permettent cette surveillance à distance. Et la mobilité se développant, c'est d'une simple tablette ou d'un Smartphone que l'on peut désormais voir et entendre tout ce qui se passe à son domicile ou sur son lieu de travail et ce de quasiment n'importe où. C'est une solution extrêmement pratique et de plus, séduisante par son aspect high-tech.

Chacun peut ainsi devenir son propre opérateur de télévidéosurveillance, effectuer directement la levée de doute, voir assurer le rôle d'intervenant en allant soi-même, ou par l'intermédiaire d'un tiers non professionnel (voisin, ami, membre de la famille…), sur site.

C'est la solution low cost par excellence. L'utilisateur final maîtrise, en effet, l'ensemble de la chaîne sécuritaire et réduit ainsi les coûts de fonctionnement en assurant lui-même l'ensemble des tâches.

Comme tout système low cost, celui-ci a des limites. Il y en a ici 2 importantes.

La première est la disponibilité nécessaire pour jouer ce rôle d'opérateur. Se connecter aux caméras régulièrement, ou suite à la réception d'une alarme, peut vite devenir fastidieux. Si au début, la nouveauté fait souvent se connecter l'utilisateur plusieurs fois par jour, de fait, par lassitude, le nombre de connexions se réduit rapidement, pour finir par ne se connecter que sur réception d'alarme. Ce qui là aussi peut devenir vite contraignant, voire pénible si des alarmes se déclenchent à 3 heures du matin. Les systèmes de détection ne sont pas tous 100% parfaits, surtout sur ces équipements low-cost, et des fausses alarmes existent. Qui est prêt à accepter d'être régulièrement réveillé en pleine nuit ? La tendance est alors, et c'est compréhensible, de se «débrancher».

La deuxième concerne le risque lors d'une intervention, savoir qu'un intrus se trouve dans vos bureaux est une chose, intervenir en est une autre. Il peut être extrêmement dangereux, voir inconscient, de vouloir agir seul.

L'auto-vidéo-surveillance est en plein développement et peut répondre à un premier niveau d'exi-

gence, mais seule la télésurveillance réalisée par des professionnels de la sécurité peut apporter toutes les garanties d'une action appropriée, efficace, et fiable dans la durée.

Les évolutions technologiques

Le Cloud computing

Le cloud computing en général

Le cloud computing est un modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurables (comme par exemple : des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être provisionnées et libérées avec un minimum d'administration.

Ce modèle est composé de 5 caractéristiques essentielles, de 3 modèles de services et de 4 modèles de déploiement.

Les 5 caractéristiques du cloud computing :

- Un service à la demande
- Un accès aux ressources par le réseau

- Mise en commun des ressources
- Flexibilité des ressources
- Un service mesuré

Les 3 modèles de services du cloud computing :

- SaaS (Software as a Service)
  Utilisation du logiciel de supervision, comme d'un service.
  Vous n'installez pas le logiciel que vous voulez utiliser sur votre ordinateur, mais vous l'utilisez à distance (le logiciel « tourne » sur des serveurs dans des datacenters). La plupart du temps, ces logiciels s'utilisent via un navigateur Web ou sont interfacés via une API à des frontaux de télésurveillance.
- IaaS (Infrastructure as a Service)
  Utilisation d'une infrastructure, comme d'un service.
  Vous n'avez pas besoin d'acheter un ensemble de matériel pour installer votre infrastructure. Vous vous contentez de louer ce matériel comme s'il vous appartenait. Vous installez les serveurs que vous souhaitez utiliser. Vous gérez l'ensemble des OS installés sur les serveurs que vous louez.
  Les entreprises utilisent beaucoup le IaaS car elles peuvent ainsi disposer de serveurs disponibles, de dernières génération et très rapidement disponibles.
- PaaS (Plateform as as Service)
  Utilisation d'une plateforme, comme d'un service.
  Vous louez une plateforme, c'est à dire une machine avec un OS, le tout prêt à l'emploi, c'est la virtualisation.

Les 4 modèles de déploiement :

- Cloud Privé
  L'ensemble des ressources n'est affecté qu'à une

seule organisation ou entreprise. C'est ce type cloud qui est le plus adapté à notre marché.

- Cloud Communautaire
  L'ensemble des ressources provient de plusieurs organisations ou entreprises qui se les partagent.
- Cloud Public
  Les ressources sont mises à disposition de tout le monde.
- Cloud Hybride
  Il s'agit d'un mixte entre le privé et le public.

Le cloud computing appliqué à notre métier

En choisissant une solution de vidéo hébergée dans le cloud, vous n'avez plus besoin d'aucun serveur ni d'enregistreurs sur site. Des caméras et une connexion Internet suffisent. Toutes les vidéos sont téléchargées sur le cloud et stockées par votre fournisseur de services. Il s'occupe de tout à votre place. Des applications de visualisation sur appareils portables vous permettent d'accéder à vos sites même lorsque vous êtes en déplacement.

Avec la vidéo hébergée, vous pouvez bénéficier d'autres services en plus de ceux liés à la sécurité, qui vous permettent d'améliorer le fonctionnement de votre entreprise. Dans les commerces de détail par exemple, vous pouvez surveiller les livraisons quotidiennes, l'intégration des caisses ou encore assurer la protection de l'argent en liquide.

Nous assistons d'ailleurs depuis peu avec l'évolution des moyens de communication à la mise en place de ces services de vidéoprotection hébergée. L'analyse, la détection et le stockage sont dès lors externalisées dans des Data centers qui mutualisent les ressources physiques. La sécurité à la carte fait apparition et l'utilisateur peut faire évoluer les services en

fonction de ses besoins.

Dernier point, le cloud computing et les IOT permettront d'unifier à travers une infrastructure unique les différents services. Par exemple, une ville pourra utiliser cette infrastructure pour ces propres usages mais aussi proposer des services à ses citoyens (sécurité, accès à distances aux services de la ville…). Le fait d'unifier ces services va permettre d'une part de réduire d'une façon importante les coûts de déploiement et de maintenance de l'infrastructure unique et des services (mise à jour…) et d'autre part de rendre plus efficace et rapide l'échange des données, donc par exemple une intervention plus rapide des forces de l'ordre suite à la détection d'un événement par les détecteurs et à sa qualification par le centre de télévidéosurveillance.

Le Big data

L'idée générale du big data, c'est d'enregistrer beaucoup de données (le plus possible). D'ailleurs si l'on traduit « Big Data », on obtient quelque chose comme « Grande Donnée » ou « Données importantes ».

Le stockage d'un tel volume de données a nécessité de revoir le mode d'enregistrement des données. Normalement pour stocker un volume de données important, on utilise des bases de données, mais le volume étant tellement important, cela

n'était pas possible. Il a fallu repenser le stockage. Pour ce nouveau mode de stockage on applique les règles des 3 V :

- Volume : Il faut stocker énormément d'information
- Variété : Il faut stocker beaucoup de données de toutes sortes
- Vélocité : Il faut pouvoir avoir accès rapidement à toutes ces données

Le Big Data appliqué à notre métier

L'objectif ultime de cette collecte, c'est de mieux connaître l'environnement du client et pouvoir nous proposer des outils permettant au final de proposer à nos clients des nouveaux services tels que des services de « Business Intelligence », de mesure et de reporting.

A l'aide du big data, les services proposés seront ciblés plus finement et en fonction de plus de critères que ceux généralement utilisés aujourd'hui.

Les Datacenters

Les centres de données sont les usines des temps modernes. Ils hébergent Internet : les sites web, les emails, les données et les photos des particuliers ; mais également les données des entreprises. A l'heure de la centralisation de l'informatique et du cloud computing, ils deviennent la clé de voûte de l'économie numérique. Une panne d'un datacenter, et des milliers de personnes peuvent être privées de réseau, de téléphone, d'emails ou de données.

Pour autant, on ne connaît pas bien leur sécurité. Souvent sous prétexte de confidentialité, certains exploitants de datacenters communiquent peu d'information sur leur architecture thermique, électrique, et sur les pannes rencontrées. Cette communication est plutôt faite par les utilisateurs qui ont à souffrir d'une interruption de service. Il n'existe pas de norme définissant la sécurité d'un datacenter.

La sécurité dans les Datacenters

Des critères fondés sur l'architecture des datacenters permettent à un organisme privé, l'Uptime institute, de classifier les datacenters. Ils sont catégorisés de « Tier I » à « Tier IV ».

Afin de connaître la sécurisation de son datacenter, voici quelques questions de base qu'il nous paraît utile de poser à son hébergeur :

- La sécurité thermique
- La sécurité électrique
- Les réseaux de fibres (points de raccordement bout en bout dans des locaux sécurisés)
- Les personnels (mise en production, maintenance, SAV…)
- Les accès (contrôle d'accès, vidéo…)

Proposition d'améliorations

Il apparaît clairement que le temps de réaction du centre de télésurveillance est un élément important de la chaîne de détection et d'information. Il est donc nécessaire de généraliser les techniques de levée de doute vidéo optimisant le temps de traitement par les opérateurs, notamment les techniques de « push » et « pull » et l'Analyse Vidéo Intelligente qui produit des images où les risques sont clairement détourés et identifiés dans les images.

Par ailleurs, une fois que l'on s'est assuré que ce travail de vérification/qualification et d'information est effectué dans les meilleures conditions techniques possibles par les centres de télésurveillance privés, on s'interroge alors sur la possibilité d'optimiser également l'intervention des services publics : eux-mêmes sont également dans une problématique d'appels entrants à traiter, de gestion des équipes terrain disponibles et de priorisation des interventions.

En ce sens, la profession convient qu'il serait utile de pouvoir transmettre aux Centres d'Information et de Commandements les images qualifiantes dont dispose le télésurveilleur

Synthèse

L'intégration de la technologie chez les télésurveilleurs est un incontournable depuis de nombreuses années. Elle impose de la rigueur, la mise en place de processus précis et la formation de tous les acteurs. Ces évolutions permettent aux Opérateurs de télésurveillance de réagir aux alarmes avec le plus de discernement possible.

Pour une meilleure efficacité, les constructeurs doivent intégrer les besoins des télésurveilleurs dans leurs démarches. Leurs technologies doivent être innovantes, fiables et interopérables.

L'intervention humaine sur alarme est un complément indispensable de la télévidéosurveillance.

Intervention

Situation actuelle du marché

Nombre d'interventions

Concernant le marché des interventions en France, aucune donnée officielle n'est disponible. En effet, le marché des interventions représente une composante de la surveillance humaine et seules quelques sociétés se sont spécialisées dans ce domaine d'activité.
Cependant et en recoupant les données des principaux acteurs, nous pouvons estimer que ce marché représente environ 600 000 interventions physiques par an.
A noter que ce marché est en constante baisse avec des raisons que nous évoquerons dans les chapitres suivants.

Plus de 90% des alarmes déclenchées en France sont injustifiées

La nature même du déclenchement d'une alarme entraîne automatiquement un taux d'erreurs et d'interprétations de la part de l'opérateur qui a généralement pour conséquence la demande d'un déplacement d'un agent de sécurité mobile.
De nombreuses alarmes sont en effet déclenchées par des évènements jugés sans risque tels que des erreurs d'utilisation, une méconnaissance des consignes de télésurveillance de la part du personnel ou de tiers (livreurs, ménage, services annexes…), un mauvais paramétrage du système en place ou tout simplement une porte ou une fenêtre ouverte.
La simple analyse ne permet pas de différencier rapidement et facilement les alarmes intempestives des vraies.
Par défaut, l'opérateur de télésurveillance demande donc la réalisation d'une levée de doute visuelle facturée, entraînant ainsi la plupart du temps un coût supplémentaire ainsi qu'une insatisfaction du client.

Gendarmerie Nationale / Police Nationale / Polices Municipales / Sociétés de sécurité privées

Le redéploiement récent de la police-gendarmerie a pour objectif de gagner en cohérence et en efficacité en faisant coïncider les territoires d'actions des deux forces principales. En effet, l'urbanisation redessine les bassins de délinquances et l'harmonisation des rôles est primordiale afin d'assurer l'efficacité de chacun.

En plein développement, les polices municipales ont également évolué dans leurs missions et se transforment progressivement en une force de police mutualisée au service des intercommunalités.
La coordination sur le terrain avec la police-gendarmerie est donc primordiale afin de coordonner les missions de chacun à travers l'organisation d'opérations de sécurisation conjointes.

Au même titre que les polices municipales et parce que les sociétés de sécurité privée ont acquis de la légitimité grâce à la création du CNAPS (Conseil National des Activités de Sécurité Privée : date de démarrage : 1er janvier 2012), ce secteur privé est devenu un élément incontournable de la vie quotidienne des citoyens.
A ce sujet, les 200 000 agents de sécurité privée représentent un levier considérable d'action sur lequel peuvent s'appuyer les forces publiques sans verser dans la confusion des genres, ni la dilution du

service public.
Cependant, aucune politique transversale visant à coordonner les actions de chacun n'a été entreprise à ce jour, chaque force en présence restant sur son domaine juridique « espace privé – espace public ».
La volonté des pouvoirs publics, à travers l'évolution de la loi de 1983, devrait permettre de dynamiser et d'influer une synergie positive visant à redéfinir les domaines de chacun tout en accordant à l'ensemble des acteurs un même cadre juridique.

Définition et perception par l'utilisateur

Définition de l'intervention

La définition de l'intervention physique proprement dîte fait souvent référence à une notion associée beaucoup plus imagée : la levée de doute.
En effet, l'opérateur de télésurveillance a besoin de confirmer la nature du déclenchement de l'alarme avant de prévenir les forces de l'ordre, conformément aux dispositions de l'article L.613-6 du code de la sécurité intérieure. Tout appel injustifié des forces de police ou de gendarmerie expose le télésurveilleur à une sanction pécuniaire d'un montant pouvant atteindre 450€.
Une circulaire du ministère de l'intérieur du 26 mars 2015 est venue préciser cet article :

- Dans le cas d'un crime ou délit flagrant d'atteinte aux personnes, la levée de doute n'est pas formellement prescrite (même si, en pratique, le télésurveilleur essaiera de confirmer le plus vite possible le renseignement initial),
- En cas d'atteinte aux biens mobiliers ou immobiliers, la levée de doute, obligatoire, peut être réalisée de différentes manières :
  - Images vidéo non équivoques, confortées par l'existence d'éléments inhabituels,
  - Ou, en l'absence d'images non équivoques, prise de contact avec le client. Après deux appels infructueux, vérification par aux moins deux éléments (interaction phonique, concordances entre différentes alarmes…), sinon envoi d'un agent sur place.

Définition 1 : « En cas de déclenchement de l'alarme d'un site sous surveillance électronique, un agent de sécurité mobile est immédiatement dépêché sur place à la demande de l'opérateur de télésurveillance afin d'y effectuer une levée de doute. Rendu sur place à bord de son véhicule, l'agent de sécurité mobile effectue une ronde extérieure ou intérieure. Si l'incident est avéré, la mission de l'agent de sécurité mobile est alors de contacter l'opérateur de télésurveillance qui, soit avertira les services compétents, soit avisera le client par téléphone.
L'agent de sécurité mobile ne quitte le site qu'une fois la situation sous contrôle. »

Définition 2 : « Une intervention est nécessaire pour vérifier sur place l'origine de l'alarme reçue par l'opérateur de la station de télésurveillance. C'est ce qu'on appelle communément la levée de doute. L'intervention est déclenchée et exécutée en fonction de consignes préalablement mises au point avec le client dans les délais les plus réduits possibles par des équipes motorisées et pré positionnées par secteur géographique. Arrivé sur place et après une ronde de reconnaissance, l'intervenant prend les mesures conservatoires qui s'imposent. »

Définition 3 : « La levée de doute est l'opération

consistant à vérifier la matérialité d'un évènement ayant provoqué le déclenchement d'une alarme. Préalable indispensable à l'appel des forces de l'ordre, la levée de doute est majoritairement opérée par une personne physique, dans la plupart des cas un agent de sécurité. L'agent de sécurité effectuera une ronde sur site et procédera aux vérifications idoines qui attesteront du bienfondé ou pas de l'alarme reçue ».

Rappel législatif et contraintes (véhicule non prioritaire, conditions météo…)

Les contraintes liées à un déplacement sur site d'un intervenant ne sont généralement pas prises en compte par les clients, volontairement ou pas, voire sont inconnues du grand public :

- Véhicule d'intervention non prioritaire,
- Aléas de la circulation,
- Conditions météorologiques,
- Diverses manifestations,
- Moyens mutualisés d'intervention à l'ensemble des clients sur un même secteur géographique.

Il va de soi que le délai d'intervention doit être le plus rapide possible afin de limiter les dommages sur site et dans certains cas, mettre en échec toute tentative d'effraction, mais il est utile de rappeler ici que les agents de sécurité en chargent de ces interventions n'ont en aucun cas pour mission d'interpeller les malfrats.

Le rôle de l'intervenant consiste :

- A s'assurer de la véracité des alarmes,
- Permettre à l'opérateur de la station de télésurveillance de clôturer les alarmes reçues,
- Rétablir le bon fonctionnement normal du système de détection électronique en place,
- Assurer la mise en place des mesures conservatoires en cas d'incident.

Au niveau de la responsabilité et des engagements demandés vis-à-vis de la société intervenante, il ne peut s'agir que d'une obligation de moyens et non de résultat compte tenu des éléments développés ci-dessus. C'est en ce sens que la jurisprudence se prononce régulièrement : « la société de gardiennage chargée d'assurer la prestation d'assistance est tenue d'une obligation de moyens et qu'il lui incombe à ce titre d'adapter ses moyens d'intervention aux différents engagements qu'elle a souscrits pour assurer à ses abonnés un traitement satisfaisant des demandes d'intervention qu'ils lui adressent » (arrêt du 06 mars 2007 - CA Montpellier n°06/00997).

Ceci entraîne de facto l'inassurabilité de l'obligation d'intervention de résultat.

Remise en cause

De l'utilité et de l'efficacité de l'intervention par l'utilisateur final (délai d'intervention, coût de l'intervention),

Dans le domaine de la sécurité, l'intervention est souvent assimilée à un phénomène d'urgence et prioritaire sans tenir compte de la mutualisation des forces humaines sur un même secteur géographique. Chaque client a le sentiment de disposer de moyens humains totalement dédiés à son site et qu'un intervenant attend l'ordre de l'opérateur de télésurveillance dans un endroit géographiquement proche du sien.

Ainsi, le délai d'intervention et donc, la nature même

de l'intervention, sont souvent remis en cause par l'utilisateur final, à la fois au niveau de l'efficacité mais également au niveau de la facturation.

De l'efficacité du système en place proposé,
Une fois arrivé sur place, la cause du déclenchement d'alarme est recherchée par l'intervenant dans la limite de ses moyens (mise à disposition des moyens d'accès, configuration géographique, végétation, éclairage public, superficie du site…) et de ses compétences.
Les caméras ou détecteurs installés sur site doivent être configurés afin de répondre précisément aux risques détectés lors de l'audit et la visite préventive du site lors de l'évaluation des risques. A ce titre, le système proposé et accepté par le client doit être adapté.

De la réputation de l'installateur,
Pour des sites complexes ou étendus, le matériel installé doit être configuré de telle manière à ce que l'opérateur de télésurveillance puisse guider l'intervenant sur l'origine du déclenchement d'alarme. Dans le cas contraire, l'intervention risque d'être inefficace et peut entraîner des conséquences néfastes dans la compréhension de l'incident.

De l'organisation de la société intervenante.
Tous ces éléments sont donc une source d'insatisfaction et sont susceptibles de remettre en cause la nature même de l'intervention humaine.
Les conditions économiques avec une baisse constante constatée sur le prix facturé de l'intervention ont entraîné la disparition de plusieurs centaines de sociétés de sécurité privée, accentuée avec la mise en place des contrôles CNAPS.

Intervention humaine

Secteur d'activités	Type d'interventions		
	Humaine		
	Avantages	Limites	Commentaires
Particulier urbain	Délai	Accès et embouteillage	Hormis les VIP, intervention humaine appelée à disparaitre compte tenu de l'évolution du prix à la baisse
Particulier rural	Sauvegarde immédiate des lieux. Analyse et prise de décision adaptées	Délai et repérage	Coût d'intervention non répercuté sur le prix de vente
Particulier résidence secondaire	Sauvegarde immédiate des lieux	Délai et repérage	Hormis les VIP, intervention humaine appelée à disparaitre compte tenu de l'évolution du prix à la baisse et les coûts de fonctionnement à la hausse
Particulier SAP	Délai	Responsabilité engagée en cas de dommages corporels	Notion de responsabilités juridiques en cas de décès ou d'invalidité due à la notion de délai d'intervention
Artisan Commerce de proximité	Sauvegarde immédiate des lieux	Zone de couverture	Concurrence de l'intervention réalisée par le personnel interne
Chaîne de magasins	Sauvegarde immédiate des lieux	Zone de couverture	Intervention low-cost souvent en extérieur
PME - PMI	Sauvegarde immédiate des lieux	Zone de couverture	Intervention utile compte tenu de la spécificité de chaque site. Réelle valeur ajoutée
Site industriel de production	Sauvegarde immédiate des lieux	Zone de couverture	Souvent proposer des rondes aléatoires avec et/ou sans contrainte horaire
Site sensible et/ou Seveso	Idem. Application des mesures de sécurité	Zone de couverture	Souvent proposer des rondes aléatoires avec et/ou sans contrainte horaire
Transport et logistique	Sauvegarde immédiate des lieux	Zone de couverture	Intervention low-cost compte tenu de l'activité du client
Zone d'activité industrielle	Mise en place rapide. Efficace car visible	Le coût	Intervention utile et économiquement viable dans le cadre d'une mutualisation
Commune Collectivité	Bon alternatif à la police municipale. Très dissuasif	Voie publique et mission	Intervention utile et économiquement viable dans le cadre d'une mutualisation. Attention au rôle dédié à la PM

Intervention vidéo

Secteur d'activités	Type d'interventions		
	Vidéo		
	Avantages	Limites	Commentaires
Particulier urbain	Immédiat	Le budget	La meilleure solution !
Particulier rural	Immédiat	Couverture de transmission	Sous réserve d'une couverture réseau fiable, la meilleure solution avec intervention directe des forces de l'ordre
Particulier résidence secondaire	Immédiat	Couverture de transmission	Sous réserve d'une couverture réseau fiable, la meilleure solution avec intervention directe des forces de l'ordre
Particulier SAP	Immédiat	Respect de la vie privée	Législation concernant l'utilisation des images pas adaptée
Artisan Commerce de proximité	Immédiat	Pas sur place	Solution à terme avec un équipement par branche d'activité
Chaîne de magasins	Immédiat	Pas sur place	La meilleure solution à travers un équipement fiable et standardisé
PME - PMI	Immédiat	Pas sur place	Complément vidéo approprié dans le cadre de certains secteurs d'activité ou certaines zones sensibles
Site industriel de production	Immédiat	Pas sur place	Opportunité de nouvelles technologies type drone
Site sensible et/ou Seveso	Immédiat	Pas sur place	Opportunité de nouvelles technologies type drone
Transport et logistique	Immédiat	Idem - La superficie à vidéo surveiller et le définition des caméras	Complément vidéo approprié dans le cadre de certains secteurs d'activité ou certaines zones sensibles (carburant)
Zone d'activité industrielle	Le coût	Voie publique	Opportunité de nouvelles technologies type drone sur zones privatives
Commune Collectivité	Le coût	Voie publique	Investissement lourd mais en pleine expansion

Intervention humaine et vidéo

Secteur d'activités	Type d'interventions		
	Humaine et vidéo		
	Avantages	Limites	Commentaires
Particulier urbain	Sauvegarde des lieux	Le coût	Economiquement et compte tenu de l'évolution des technologies B to C, le particulier urbain se transforme en opérateur de TLS et en intervenant
Particulier rural	Sauvegarde des lieux	Le coût	Economiquement, difficile à commercialiser
Particulier résidence secondaire	Sauvegarde des lieux	Le délai d'intervention	Prestations humaines plutôt consacrées à la mise en place d'un agent de surveillance en cas de dégradations
Particulier SAP	Solution idéale sur le papier	Le coût	Economiquement non viable sauf client VIP
Artisan Commerce de proximité	Sauvegarde sur place. Levée de doute immédiate	Le coût	Economiquement difficile à proposer
Chaîne de magasins	Sauvegarde sur place. Levée de doute immédiate	Le coût	Offre standardisée et de masse afin d'être économiquement intéressante
PME - PMI	Sauvegarde sur place. Levée de doute immédiate	Le coût	Offre à établir avec optimisation nécessaire
Site industriel de production	Sauvegarde sur place. Levée de doute immédiate	Le coût	Association de vidéo ciblée et de rondes techniques ou de contrôle
Site sensible et/ou Seveso	Sauvegarde sur place. Levée de doute immédiate	Le coût	Association de vidéo performante et de rondes techniques. Investissement lourd mais nécessaire
Transport et logistique	Sauvegarde sur place. Levée de doute immédiate	Le coût	Compromis économiquement viable
Zone d'activité industrielle	Efficace si report véhicule zone	Le coût	Mix efficace. Démarche commerciale compliquée
Commune Collectivité	Bon alternatif à la police municipale. Très dissuasif	Voie publique	Efficace sous condition d'une bonne coordination entre privé et public

Evolution du marché

Contraintes financières (augmentation du carburant, baisse du prix moyen de l'intervention, augmentation des charges, pénalités de + en + appliquées)

Le marché de l'intervention humaine en France est en régression depuis plusieurs années. Ce phénomène a été accentué par plusieurs évènements :

- Augmentation du prix du carburant (+57% entre janvier 2004 et juin 2014 source INSEE).
- Augmentation des frais de carrosserie et plus globalement des frais de réparation des véhicules.
- Baisse du prix de l'intervention facturée (environ -30% environ en 10 ans).
- Mise en place de plus en plus fréquente de délais d'intervention imposés, voire de pénalités en cas de non respect.
- Politique urbaine des municipalités visant à restreindre ou exclure les véhicules des centres villes entraînant des surcoûts difficilement répercutés chez le client et des délais d'intervention allongés (frais de parkings, changement de véhicule une fois arrivé sur le secteur de l'intervention – 2 roues - vélo électrique, véhicule électrique avec frais de garage).

Contraintes géographiques (répartition nationale des sociétés de sécurité privée, apparition de zones « blanches »)

Les sociétés de sécurité privée, et plus particulièrement celles qui possèdent plusieurs activités, sont confrontées depuis plusieurs années à une stagnation du marché de la surveillance avec des marges bénéficiaires en baisse constante.

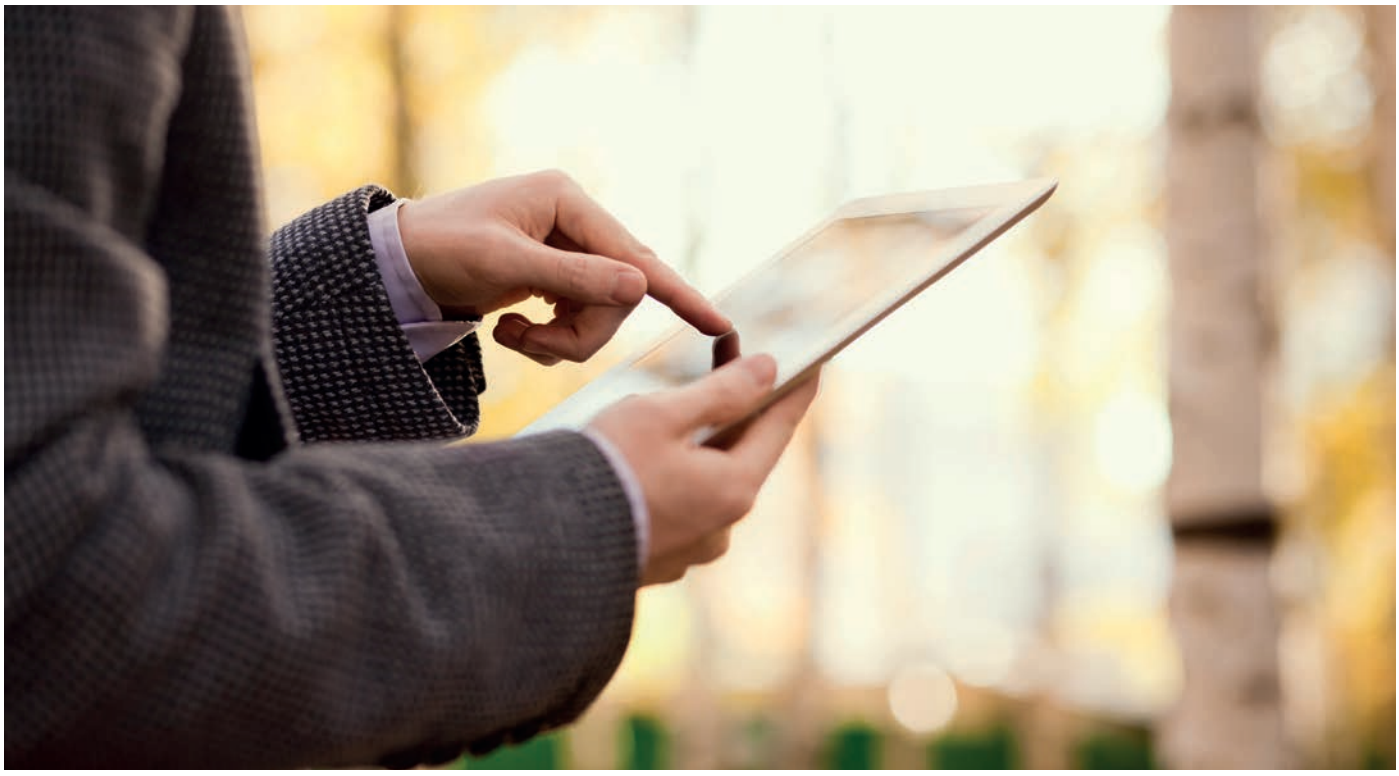
L'activité la plus touchée par les restructurations est l'intervention sur alarme et ce, pour plusieurs raisons :

- Facturation aléatoire et hypothétique de cette activité (facturation à l'unité au « coup par coup » avec de plus en plus de contraintes des donneurs d'ordre telles que des pénalités appliquées en cas de dépassement de délai).
- Activité à risques entraînant des coûts de fonctionnement importants (entretien général du véhicule d'intervention, accidentologie forte, assurances, environnement à risque pour l'intervenant…)
- Recherche en responsabilité de plus en plus fréquente de la part du donneur d'ordre entraînant une obligation pour la société de sécurité privée à faire appel à des cabinets juridiques spécialisés ou à une organisation interne qui entraîne des coûts de fonctionnement le plus souvent à fond perdu.

Ceci entraîne inexorablement un abandon de cette activité au profit de domaines plus rentables comme l'installation de matériel ou la télésurveillance.

Certaines zones géographiques deviennent donc des « zones blanches » sur lesquelles plus aucune société de sécurité privée n'effectue les missions d'intervention avec des délais raisonnables.
Le marché de l'intervention s'oriente donc naturellement vers des solutions gérables à distance et dans cette perspective, les moyens déportés de détection et d'analyse qui servent à vérifier le bien-fondé des alarmes reçues sont en plein développement.

Evolution technologique



Outils pour l'intervention

Drones et robots

Les nouveaux « outils » du futur pressentis sur le marché des interventions levées de doute sont le drone et le robot.

Le robot est utilisé pour des missions en intérieur comme les rondes dans le domaine des entrepôts de logistique.

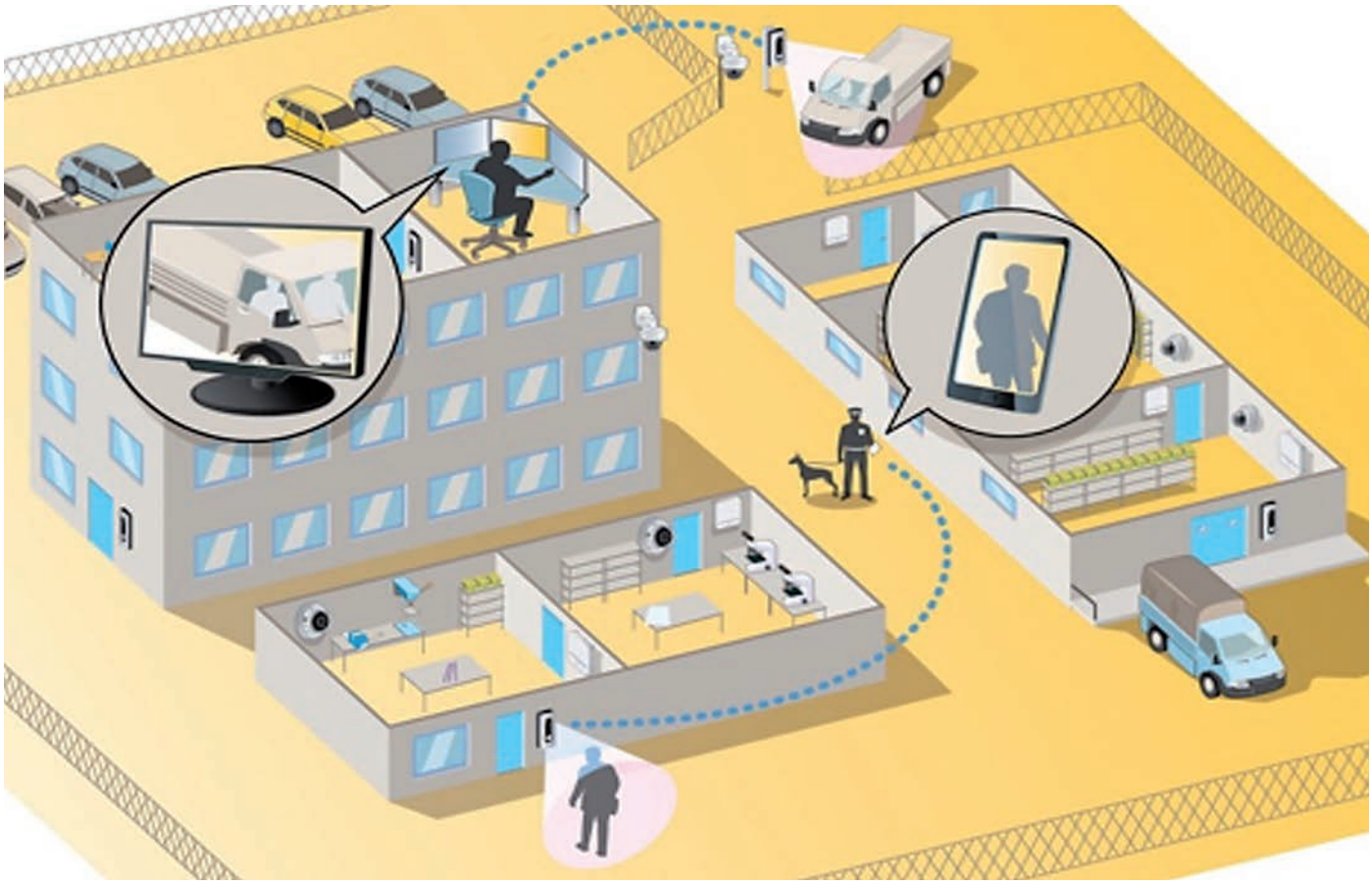
Le drone est à la mode et envahit l'audiovisuel public en créant un nouvel angle de vue enrichissant.

Cette nouvelle technique est issue de l'usage militaire et les applications civiles tendent à se développer. La surveillance préventive et les missions liées à la sécurité privée semblent être à court terme la prochaine cible de ce marché en pleine construction.

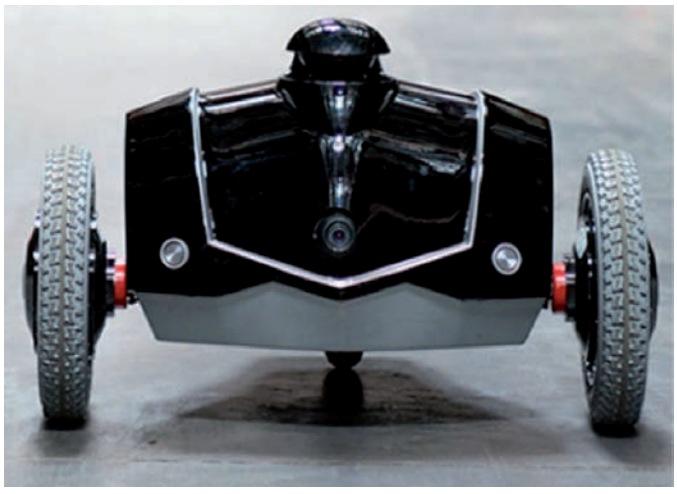
Les constructeurs et utilisateurs de drones s'organisent à travers la création d'une fédération nationale, la FPDC (Fédération Professionnelle du Drone Civil).

Le seul bémol demeure l'adaptation de la législation française et européenne à ce nouvel outil qui se heurte pour l'instant au cadre réglementaire de l'aviation civile (DGAC) mais également dans la formation et la qualification des « télé pilotes » en charge de l'utilisation du drone.

Quel statut pour cette nouvelle profession en charge de la détection à distance de toute tentative d'effraction sur un site ?



Le télé pilote sera-t-il intégré dans la station de télésurveillance au même titre qu'un opérateur de télévidéosurveillance ?



En fonction de l'évolution de la réglementation, les professionnels de la sécurité privée devront également intégrer cette nouvelle technologie qui sera, soit complémentaire à un système existant avec intervention humaine possible sur le lieu même du déclenchement d'alarme (agent de surveillance en poste sur une zone d'activité ou industrielle avec intervention rapide en équipe avec le télé pilote qui le guidera à distance), soit permettant de prévenir directement les forces de l'ordre pour constater un flagrant délit.

Les objets communicants

Les agents disposent sur le terrain de fonctions informatique et de communication telles que des ta-

blettes ou des smart phones. A travers ces outils, l'agent accède aux informations et aux vidéos du site et peut transmettre en retour des vidéos ou photos via sa tablette vers le centre de supervision.
D'autres missions, autres que des missions de sécurité, peuvent aussi être menées par l'agent, par exemple la vérification des extincteurs ce qui augmente la valeur de l'agent.

Services à distance

Pour les clients

A travers ces nouvelles technologies (Cloud computing, IOT, Big data, réseaux…), les clients peuvent accéder à distance à de nouveaux services notamment les données marketing sous forme de rapports, la sécurité (vidéo, alertes) et d'autres.
Ces services sont en plein essor et permettent d'envisager une modification profonde de nos métiers.

Pour le télésurveilleur

L'audio à distance

Les haut-parleurs IP sont faciles à installer pour une communication claire à longue distance dans des applications de vidéosurveillance. Dans les situations de surveillance avec vidéo en direct, ces haut-parleurs permettent de s'adresser à des personnes à distance et de les décourager de mal agir.
Le haut-parleur peut également diffuser un fichier

audio préenregistré, déclenché manuellement ou automatiquement sur alarme.

L'ouverture et la gestion des accès

A travers les produits d'interphonie et de contrôle d'accès IP, le centre de télévidéosurveillance peut gérer à distance la communication bidirectionnelle, l'identification et le contrôle d'accès à distance. Ces nouvelles solutions vous offrent de nouvelles possibilités de sécuriser votre activité et complète parfaitement toute installation de surveillance.

Les systèmes de marquage par ADN synthétique

Le Spray ADN synthétique est un nouveau dispositif dans la dissuasion et la lutte contre les cambriolages et les attaques à main armée dans les locaux commerciaux. Contenant de l'ADN synthétique, il lie les intrus à la scène de crime et s'avère être une façon hautement efficace dans la prévention.

Une fois activé, le Spray ADN vaporise un liquide forensic de haute technologie sur les criminels. La solution contient un traceur UV et un code ADN unique, liant irréfutablement le voleur à la scène de crime. Les traces d'ADN peuvent être prélevées de la peau, des cheveux et des vêtements afin de les analyser par un laboratoire médico-légal et de prouver la présence d'un suspect dans un lieu particulier au moment des faits. Bien qu'invisibles et inoffensifs, les traces adhèrent pendant des semaines - s'accrochant aux fibres et dans les plis de la peau.

Lors d'interpellations et gardes-à-vue la police peut détecter les traces moyennant une lumière UV et ainsi confondre des suspects et obtenir des preuves permettant une condamnation. Souvent, la police a des doutes sur les auteurs de crimes, mais ne détient aucune preuve substantielle les accusant formellement ; le fournisseur de spray peut fournir cette évidence.

Exemple d'application :

Le couplage de ce dispositif avec un détecteur d'agression sonore intégré dans une caméra et d'un raccordement à un centre de télésurveillance permet de répondre efficacement aux problématiques des vols à main armée avec violence dans les points de vente. Ce dispositif évite ainsi que le personnel soit impliqué dans le processus d'alerte et apporte un faisceau de preuve indéniable par le marquage.

Synthèse

Intervenir physiquement sur un déclenchement d'alarme à la demande du télésurveilleur semblait jusqu'à présent la solution majoritairement et historiquement la plus répandue sur le marché de la sécurité.

Les évolutions, liées notamment à l'environnement défavorable des contraintes imposées par les acteurs de ce marché, ont rendu ce secteur extrêmement fragile financièrement.

En conséquence, les sociétés de surveillance se désengagent massivement d'un marché devenu à risques et de moins en moins rentable.

Parallèlement, l'émergence de la télévidéosurveillance oriente le marché de l'intervention vers la levée de doute à distance.

Est-ce une tendance lourde et irrémédiable ?

Les prescripteurs seront-ils prêts à en accepter les conséquences, notamment financières en terme d'investissement ?

Les solutions technologiques répondront-elles exhaustivement aux attentes du client final ?

Quel est l'avenir à moyen terme des sociétés d'interventions avec cette orientation technologique ?

Comment gérer l'abandon des clients qui continueront à solliciter les interventions humaines ?

Les années à venir nous le diront très rapidement.

Conclusion

Dans un monde futur et forcément idéal, la levée de doute par télévidéosurveillance permettra à un opérateur déporté :

- De prendre connaissance, en temps réel et sans déperdition, de la situation sur place grâce à des détecteurs audio, vidéos, sensoriels…
- D'analyser rapidement la situation grâce à la transmission d'images qui seront analysées préalablement par le logiciel intégré à la caméra et qui ne transmettra les images paramétrées qu'en fonction de l'environnement immédiat et spécifique.
- D'agir immédiatement en entrant en communication directe avec les personnes suspectes sur place.
- De transmettre en temps réel les images aux Forces de L'ordre et/ou à des équipes de sécurité privée qui pourront intervenir rapidement et conjointement directement sur place.
- De guider à distance les forces de l'ordre et/ou les sociétés de sécurité privée afin de prévenir tout risque d'aggravation ou de constater le flagrant délit.
- De suivre à distance les personnes suspectes grâce à l'accès aux caméras de surveillance présentes sur les lieux publics (communes, réseaux routiers, gares, aéroports, parkings, etc.) ainsi que les drones de surveillance.

Pour cela, plusieurs améliorations devront intervenir dans les années futures tant sur le plan technique que juridique :

- L'évolution de la qualité des images : jour/nuit, contrejour, résolution, nombre d'images par seconde,
- L'évolution des techniques de transmissions d'images au niveau des flux et du réseau garantissant la rapidité et la sécurité des données transmises,
- L'évolution de la législation en permettant l'accès du domaine public aux entreprises de sécurité privée,
- L'évolution vers un consensus dans les systèmes de transmission et d'analyse d'images à l'ensemble des intervenants privés et publics afin d'inter-réagir efficacement sur le lieu choisi.

L'agent d'intervention évoluera quant à lui vers un rôle beaucoup plus centré sur la dissuasion et la connaissance personnalisée de son secteur géographique permettant ainsi d'anticiper tout acte de malveillance grâce à sa présence sur le terrain et à l'accès en temps réel des images analysées préalablement par l'opérateur de télévidéosurveillance.

Il ne sera plus l'acteur low-cost par défaut qui constate le délit ou la tentative d'effraction mais un maillon essentiel de la chaîne de prévention sécuritaire en liaison permanente avec les installateurs de systèmes de protection et les forces de l'ordre de son secteur géographique.
Il sera financé en amont par l'ensemble des clients adhérents grâce à des subventions locales, régionales (région, département communauté de communes ou agglomérations urbaines…) ou privées à travers des collectivités publiques ou des associations privées (zones d'activités ou industrielles, chambres de commerce et d'industrie, associations de commerçants, zones pavillonnaires ou résidentielles…).
Sa valeur ajoutée sera donc essentiellement axée sur la proximité et la prévention.

En cas de nécessité, l'intervention physique ne représentera plus un coût supplémentaire vis-à-vis du client mais un complément de prestation inclus dans la prestation de sécurité globale.
L'intervention ne sera plus vécue comme une action servant à constater le sinistre mais comme une présence rassurante en attendant l'arrivée du client.

24, rue Firmin Gillot
75015 Paris