Guide de la vidéosurveillance 2010

ffpp
Fédération Française des Ports de Plaisance

BOSCH
Des technologies pour la vie

Sommaire

I Introduction

Ce guide est à destination des personnes responsables de la gestion et de la sécurité des ports de plaisance. Il constitue un recueil de plusieurs documents sur la réglementation en vigueur, les formalités administratives et les différents aspects techniques concernant la vidéosurveillance/la vidéo-protection.

Ce document a pour but d'aider à la compréhension des technologies et des formalités administratives. Il est destiné à fournir une base pour la réalisation de cahiers des charges dans le cadre d'un projet vidéosurveillance/vidéo-protection au sein d'une infrastructure portuaire.

Tout d'abord, nous présenterons une vue d'ensemble des différents points à considérer lors de la réalisation d'un projet de vidéosurveillance.

A. Approche simplifiée des formalités administratives

Nous présentons une approche simplifiée de la demande d'autorisation auprès de la préfecture et auprès de la CNIL. Vous retrouverez une explication détaillée de la réglementation en vigueur dans la partie **Réglementation en vigueur**.

1. Autorisation préfectorale – interprétation de l'arrêté du 3 Août 2007

<table>
<tr><th colspan="2">Système de vidéosurveillance installé sur un lieu ou un établissement ouvert au public ou dont les caméras sont susceptibles de visualiser la voie publique</th><th>Système de vidéosurveillance installé sur un lieu privatif ou un local à usage exclusivement professionnel qui n'accueille pas de public (entreprises, sites industriels, etc. ...)</th></tr>
<tr><td colspan="2">Le système de vidéosurveillance est soumis :
à l'article 10 de la loi n°95-73 du 21 janvier 1995 modifiée (décret d'application n°96-926 du 17 octobre 1996 modifié)
aux normes techniques décrites dans l'arrêté du 3 aout 2007</td><td>Le système de vidéosurveillance est soumis :
aux dispositions générales du code civil sur le droit à l'image (article 9)
aux articles L.1222-4, L.1221-9 et 3ème alinéa de l'article L. 2223-32 du code du travail</td></tr>
<tr><td colspan="2">Documents à transmettre à la préfecture
(Se reporter à la notice d'information CERFA n° 51336#01 et à l'arrêté du 3 Aout 2007 portant définition des normes techniques des systèmes de vidéosurveillance - rectificatif)</td><td>Pas de document à transmettre à la préfecture
L'existence d'un système de vidéosurveillance doit être porté à la connaissance des salariés</td></tr>
<tr><td>< 8 caméras</td><td>Demande d'autorisation CERFA n° 13806*01
Annexe 1 de la notice d'information n° 51336#01 (questionnaire/attestation de conformité)
Exemplaire de l'affiche d'information au public</td><td rowspan="2"></td></tr>
<tr><td>> 8 caméras</td><td>Demande d'autorisation CERFA n° 13806*01
Annexe 1 de la notice d'information n° 51336#01 (questionnaire/attestation de conformité)
Exemplaire de l'affiche d'information au public
Le rapport de présentation (description du système)
Le plan de masse et/ou plan de détail (Bâtiments, Nbre de caméras, position des caméras, champs de vision, zones couvertes)
Un plan du périmètre (uniquement dans le cas d'une surveillance d'un périmètre)</td></tr>
</table>

Tableau 1 – Récapitulatif des documents à fournir

	Champs de visualisation de la caméra		
	Plan large	Plan étroit	
		Déplacement standard de l'objet	Déplacement rapide de l'objet
	Voie publique en agglomération, quai de gare, route ou autoroute, rayon d'un magasin etc…	DAB, véhicule de transport public, pompe à essence, caisse enregistreuse, comptoir ou guichet, contrôle d'accès, issue de secours, péage routier	Entrée ou sortie d'un commerce/musée/agence bancaire, plateforme de transporteurs de fonds
Résolution et vitesse d'enregistrement minimum	**6IPS@CIF**	**6IPS@4CIF**	**12IPS@4CIF**
		6IPS@2CIF avec visualisation d'un visage avec une résolution minimum de 90x60 pixels Voir tableau des focales	**12IPS@2CIF** avec visualisation d'un visage avec une résolution minimum de 90x60 pixels Voir tableau des focales
		6IPS@CIF avec visualisation d'un visage avec une résolution minimum de 90x60 pixels Voir tableau des focales	**12IPS@CIF** avec visualisation d'un visage avec une résolution minimum de 90x60 pixels Voir tableau des focales

Tableau 2 – Contraintes sur les qualités et vitesses d'enregistrement en fonction du champ de visualisation

		Valeur de focale maximum garantissant la visualisation d'un visage avec une résolution minimum de 90x60 pixels						
		Distance par rapport à la cible						
		2m	5m	10m	20m	30m	40m	50m
Résolution	CIF	6mm	15mm	30mm	60mm	90mm	120mm	-
	2CIF	5mm	12mm	24mm	48mm	72mm	96mm	120mm

Tableau 3 – Contraintes de focale en fonction de la résolution

2. CNIL

	Lieu public (ouvert au public)	Lieu privé (non ouvert au public)
Sans enregistrement d'images numériques	Autorisation préfectorale	Aucune déclaration
Avec enregistrement d'images numériques	Autorisation préfectorale	Déclaration normale auprès de la CNIL
Avec alimentation d'un fichier	Déclaration normale ou demande d'avis auprès de la CNIL	Déclaration normale ou demande d'avis auprès de la CNIL
Avec constitution d'un fichier d'infractions	Autorisation ou demande d'avis auprès de la CNIL	Autorisation ou demande d'avis auprès de la CNIL
Avec reconnaissance faciale ou analyse comportementale	Autorisation CNIL ou demande d'avis auprès de la CNIL	Autorisation CNIL ou demande d'avis auprès de la CNIL

Tableau 4 – Récapitulatif des formalités accomplir avant de mettre en place un système de vidéosurveillance

B. Différentes étapes d'un projet de vidéosurveillance/vidéo-protection

Avant de mettre en place son système de vidéosurveillance/vidéo-protection, le responsable de projet devra établir un cahier des charges exprimant ses besoins et le type d'architecture souhaité.

Pour réaliser ce cahier des charges, il pourra se faire assister d'un bureau d'étude ou de l'installateur ou du référent sécurité de la ville / de la préfecture / de la gendarmerie. Le responsable devra aborder les points suivants :

- **La stratégie** – Les objectifs du système de vidéosurveillance/vidéo-protection, la validation de ces objectifs par l'ensemble des acteurs, les aspects juridiques et administratifs et la mutualisation ou les échanges avec d'autres projets…
- **L'organisation** – Le site du projet et son périmètre, les besoins d'exploitation (visualisation, …), les personnes exploitant les images, les besoins de personnel pour exploiter et administrer le système, le financement, le coût du projet et le calcul du retour sur investissement…

- **La technique** – Les technologies et les produits nécessaires à la réalisation des objectifs opérationnels, l'architecture du système, l'évolutivité du système, l'ouverture du système ou système propriétaire et les normes techniques à respecter…

Le cahier des charges devra également prévoir une partie organisation des travaux et déploiement du système de vidéosurveillance/vidéo-protection. Ce cahier des charges servira de document principal pour l'appel d'offre public ou privé.

Suite à l'appel d'offre public ou privé, le responsable de projet analysera les offres reçues. Pour faciliter cette analyse, il pourra être mis en place une grille d'évaluation des offres. Cette grille devra intégrer tous les paramètres clés du dispositif déployé.

La réalisation du projet s'accompagnera du suivi des travaux qui permettra de prendre toutes les dispositions nécessaires au bon déroulement des travaux de réalisation. Il sera prévu le cas échéant des réunions de suivi des travaux.

La réception est une étape clé dans la réalisation de votre projet de vidéosurveillance/vidéo-protection. Elle consistera dans un premier temps à vérifier la conformité du système déployé avec le cahier des charges. Ainsi, l'ensemble du système devra être testé, essais techniques et fonctionnels. L'ensemble de la réception devra être consigné dans un compte-rendu. Les réserves éventuelles devront être levées dans des délais consignés dans le compte-rendu.

Dans un deuxième temps, un dossier complet de réception devra être mis en place. Ce dossier a pour but de fournir l'ensemble des informations sur le système déployé. Ces informations pourront servir aux évolutions futures du site, dans le cadre du changement du prestataire effectuant la maintenance, … mais surtout à garder une trace complète du projet. Vous trouverez ci-dessous une liste non exhaustive des documents à inclure dans ce dossier :

- Le cahier des charges du projet de vidéosurveillance/vidéo-protection
- L'offre retenue et les différents éléments associés
- Les comptes-rendus des réunions de suivi de travaux et de la réception
- Les dossiers d'autorisation préfectorale et CNIL le cas échéant ainsi que les autorisations
- Les procédures d'exploitation du système
- Synoptique et descriptif de l'architecture du système
- Les données techniques – Configuration du système (Nombre d'images par seconde, Planning d'enregistrement,…) / Prises de vue
- Les documentations techniques, les fiches techniques et les manuels d'utilisation, de l'ensemble des produits composant le système
- Les procédures d'entretien et de maintenance s'il n'y a pas de contrat de maintenance

C. Présentation de différents types d'architecture

1. Application de 1 à 4 caméras

Les applications de 1 à 4 caméras peuvent être traitées avec des produits analogiques ou IP. Les capacités d'investissement détermineront le choix de la technologie.

Dans le cadre d'une **application analogique**, l'emploi d'un enregistreur numérique pour l'enregistrement et la visualisation sera recommandé. Les liaisons avec les caméras se feront via des câbles coaxiaux sur des distances inférieures à 600 m ou de la fibre optique pour des distances supérieures.

Dans le cadre d'une **application IP**, Il est recommandé d'utiliser l'enregistrement à la source et un ordinateur de visualisation pour des questions de coût. Il est toutefois possible d'utiliser des enregistreurs vidéo sur réseau (NVR) ou un enregistreur numérique IP pour l'enregistrement des vidéos sur le long terme (besoin de capacité de stockage). Un réseau local dédié à la vidéosurveillance sera utilisé pour la transmission des données. Attention, la distance maximale entre la caméra IP et le Switch (commutateur réseau) avec du câble réseau (Cat5 par exemple) est de 100 m. Pour des distances supérieures, l'utilisation de la fibre optique sera requise. Le coût des équipements réseaux utilisant de la fibre optique est assez élevé par rapport à un réseau classique. Une solution palliative est l'utilisation de caméras analogiques et d'encodeurs permettant une liaison de 600 m maximum entre la caméra et l'encodeur et de 100 m entre l'encodeur et le Switch.

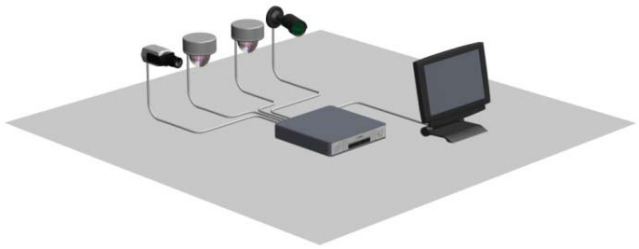


Figure 1 - Exemple de système de vidéosurveillance analogique

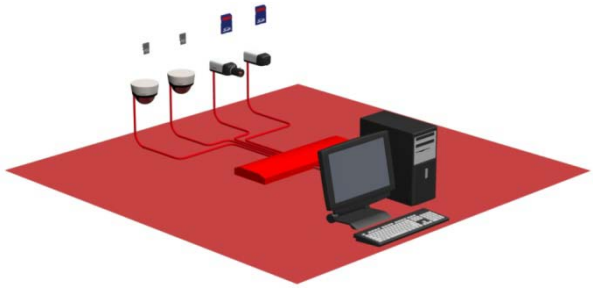


Figure 2 - Exemple de système de vidéosurveillance IP

2. Application de 5 à 16 caméras

Les applications de 5 à 16 caméras peuvent être traitées de trois manières avec des produits analogiques, hybrides ou IP. Le choix de la technologie sera pris en fonction du site et de l'investissement souhaité.

- Architecture analogique – Architecture analogique existante, souhait de réutiliser le câblage coaxial existant
- Architecture IP – Nouveau projet ou réseau local existant pouvant être dédié à la vidéosurveillance
- Architecture hybride – Souhait de passer sur un système IP avec des caméras analogiques à reprendre

Dans le cadre d'une **application analogique**, l'emploi d'un enregistreur numérique pour l'enregistrement et la visualisation sera recommandé. Les liaisons avec les caméras se feront via des câbles coaxiaux sur des distances inférieures à 600 m ou de la fibre optique pour des distances supérieures.

Dans le cadre d'une **application IP**, au vu du nombre de caméras, il sera judicieux d'opter pour une solution avec une grande capacité de stockage. Ainsi, le choix d'enregistreurs vidéo sur réseau (NVR) ou un enregistreur numérique IP sera à privilégier. Un réseau local dédié à la vidéosurveillance sera utilisé pour la transmission des données. Attention, la distance maximale entre la caméra IP et le Switch (commutateur réseau) avec du câble réseau (Cat5 par exemple) est de 100 m. Pour des distances supérieures, l'utilisation de la fibre optique sera requise. Le coût des équipements réseaux utilisant de la fibre optique est assez élevé par rapport à un réseau classique. Une solution palliative est l'utilisation de caméras analogiques et

d'encodeurs permettant une liaison de 600 m maximum entre la caméra et l'encodeur et de 100 m entre l'encodeur et le Switch.

Dans le cadre d'une **application hybride**, la solution la moins onéreuse sera d'utiliser un enregistreur numérique hybride acceptant des caméras analogiques et IP. Le choix d'un système IP pourra être envisagé en utilisant des encodeurs pour reprendre les caméras analogiques.

Dans tous les cas, si un opérateur visualise les caméras et peut en prendre le contrôle, l'utilisation de deux moniteurs s'avère souhaitable :

- un moniteur pour la visualisation de l'ensemble des caméras
- un moniteur pour la visualisation et le contrôle d'une caméra spécifique en plein écran

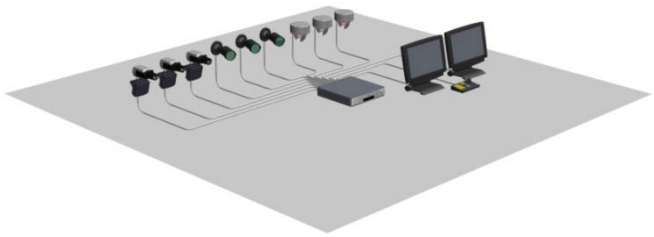


Figure 3 - Exemple de système de vidéosurveillance analogique

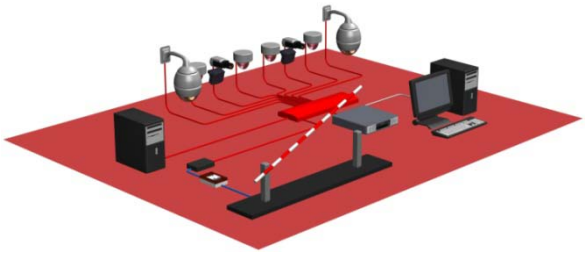


Figure 4 - Exemple de système de vidéosurveillance IP

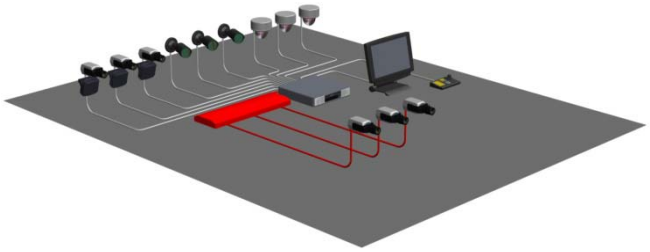


Figure 5 - Exemple de système de vidéosurveillance hybride

3. Application de 8 à 64 caméras

Les applications de 8 à 64 caméras peuvent être traitées de trois manières avec des produits analogiques, hybrides ou IP. Le choix de la technologie sera pris en fonction du site et de l'investissement souhaité.

- Architecture analogique – Architecture analogique existante, souhait de réutiliser le câblage coaxial existant
- Architecture IP – Nouveau projet ou réseau local existant pouvant être dédié à la vidéosurveillance, besoin d'un logiciel de gestion vidéo
- Architecture hybride - Souhait de passer sur un système IP avec des caméras analogiques à reprendre, besoin d'un logiciel de gestion vidéo

Dans le cadre d'une **application analogique**, nous utiliserons plusieurs enregistreurs numériques mis en cascade. Un clavier de télécommande permettra de prendre le contrôle de l'ensemble des caméras et des différents enregistreurs. Les liaisons avec les caméras se feront via des câbles coaxiaux sur des distances inférieures à 600 m ou de la fibre optique pour des distances supérieures.

Dans le cadre d'une **application IP**, nous utiliserons des solutions de stockage tel que des enregistreurs vidéo sur le réseau (NVR) ou des systèmes de stockage virtualisé (VRM) avec des unités iSCSI. L'ensemble du système sera contrôlé par un système de gestion vidéo. Un réseau local dédié à la vidéosurveillance sera utilisé pour la transmission des données. Attention, la distance maximale entre la caméra IP et le Switch (commutateur réseau) avec du câble réseau (Cat5 par exemple) est de 100 m. Pour des distances

supérieures, l'utilisation de la fibre optique sera requise. Le coût des équipements réseaux utilisant de la fibre optique est assez élevé par rapport à un réseau classique. Une solution palliative est l'utilisation de caméras analogiques et d'encodeurs, permettant une liaison de 600 m maximum entre la caméra et l'encodeur, et de 100 m entre l'encodeur et le Switch.

Dans le cadre d'une **application hybride**, nous utiliserons plusieurs enregistreurs numériques hybrides acceptant des caméras analogiques et IP. Les enregistreurs seront reliés au réseau local dédié à la vidéosurveillance. L'ensemble du système sera contrôlé via le réseau avec un logiciel. Ce logiciel permettra de visualiser et de contrôler les caméras mais également de configurer les enregistreurs.

Dans tous les cas, le nombre de moniteurs sera à prendre en compte pour une gestion optimal du système. Il faudra utiliser des moniteurs pour la multivision des caméras et un moniteur pour la prise en main d'une caméra spécifique.

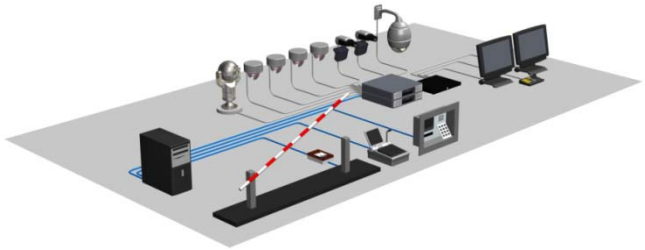


Figure 6 - Exemple de système de vidéosurveillance analogique

Figure 7 - Exemple de système de vidéosurveillance IP

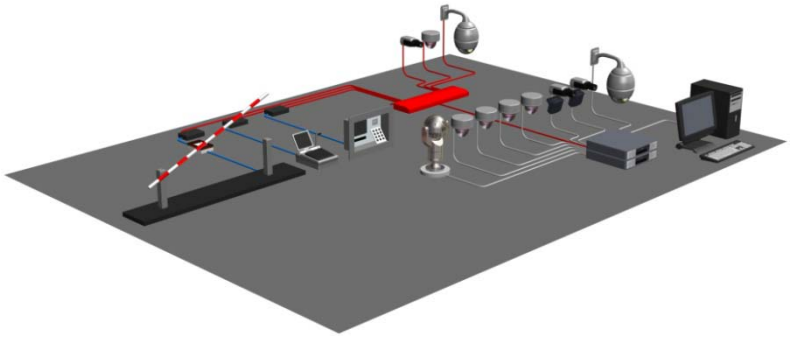


Figure 8 - Exemple de système de vidéosurveillance hybride

4. Application de 64 à 500 caméras

Pour les applications de 64 à 500 caméras, nous recommandons l'utilisation de solution de vidéosurveillance IP. Si des caméras analogiques doivent être reprises, l'utilisation d'encodeurs sera envisagée.

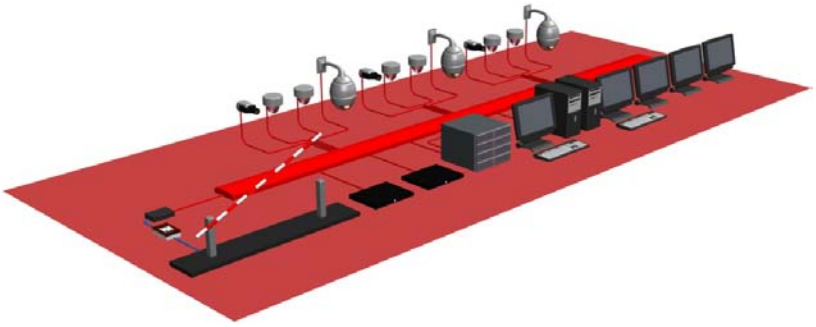


Figure 9 - Exemple de système de vidéosurveillance IP

Les solutions de stockage les plus adaptées seront les systèmes de stockage virtualisé (VRM) avec des unités iSCSI ou les enregistreurs vidéo sur le réseau (NVR). Deux stratégies de stockage peuvent être envisagées :

- Système d'enregistrement distribué
- Système d'enregistrement centralisé

La première solution permet de répartir les enregistrements sur plusieurs points. Par exemple, un système d'enregistrement par bâtiment. La deuxième solution centralisera les enregistrements en seul point. Par exemple, tous les enregistrements sont stockés à la capitainerie d'un port.

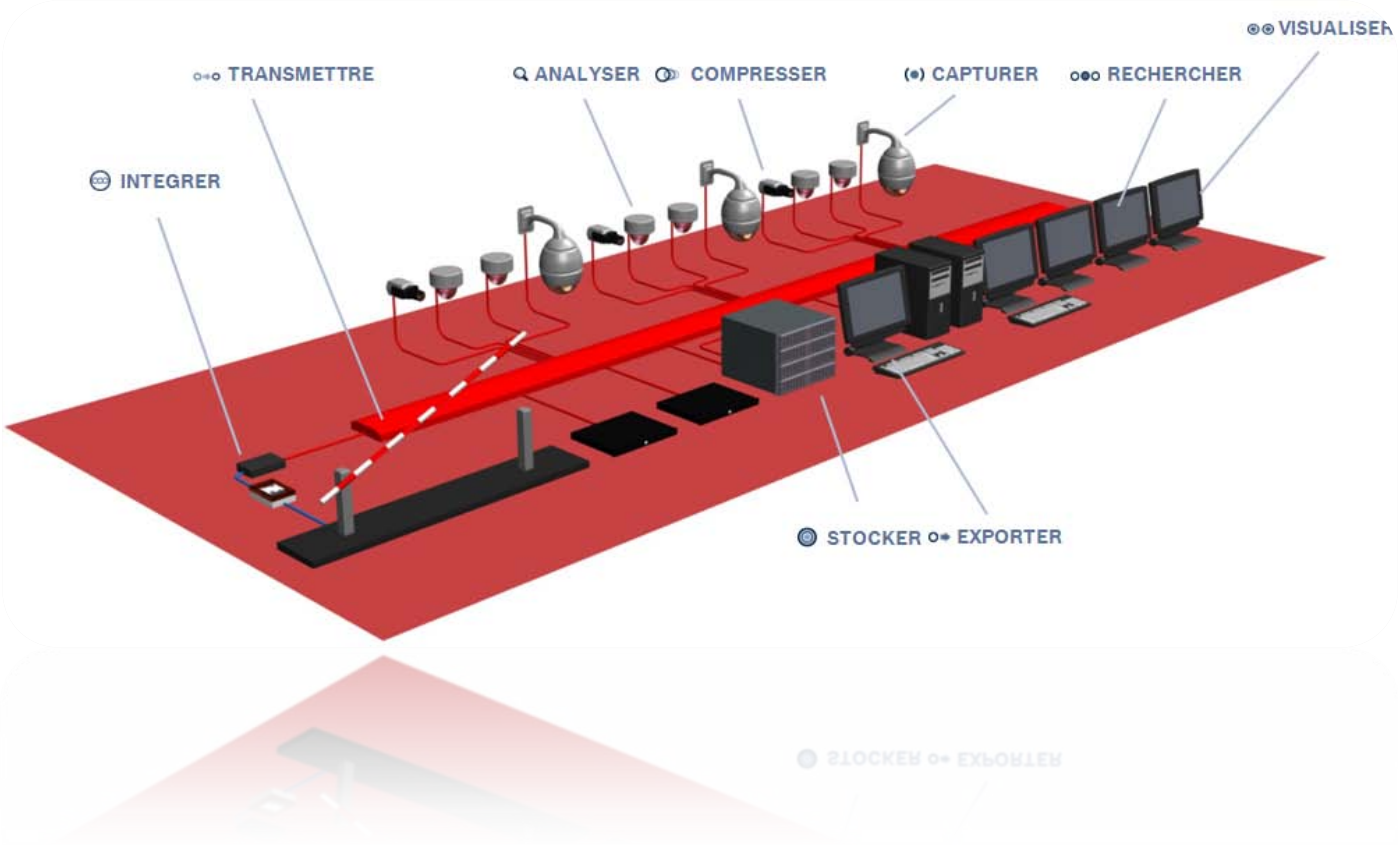
L'ensemble du système devra superviser par un système de gestion vidéo. Pour ce type d'application, vous pouvez vous reporter à la partie IIIB.5.b) L'interface homme-machine (IHM) qui présente les fonctions principales d'un système de gestion.

Un réseau local dédié à la vidéosurveillance sera utilisé pour la transmission des données. Attention, la distance maximale entre la caméra IP et le Switch (commutateur réseau) avec du câble réseau (Cat5 par exemple) est de 100 m. Pour des distances supérieures, l'utilisation de la fibre optique sera requise. Le coût des équipements réseaux utilisant de la fibre optique est assez élevé par rapport à un réseau classique. Une solution palliative est l'utilisation de caméras analogiques et d'encodeurs, permettant une liaison de 600 m maximum entre la caméra et l'encodeur, et de 100 m entre l'encodeur et le Switch.

D. Les composants d'un système de vidéosurveillance/vidéo-protection

Un système de vidéosurveillance/de vidéo-protection peut être décomposé en 9 parties. Vous devrez prendre en compte chaque partie lors de la conception de votre système.

- La capture - Les caméras
- L'analyse – Les systèmes intelligents embarqués (détection de mouvements, analyse d'image,...)
- La compression – Compression vidéo MPEG-4 / H.264...
- La transmission – Les communications tels que les réseaux locaux, les réseaux sans fil...
- La visualisation – Les écrans, l'interface homme machine du logiciel...
- Le stockage – Les enregistreurs, les unités de stockage, le logiciel d'enregistrement ...
- La recherche – La puissance, la rapidité et les fonctionnalités du système de recherche des images
- L'exportation – La simplicité d'exportation mais aussi l'intégration de système de protection et d'authentification de vos sauvegarde
- L'intégration – L'ouverture vers d'autres produits ou systèmes par exemple le contrôle d'accès



II Réglementation en vigueur

A. Liste des textes de référence en vigueur

1. Lois

- Article 10 et 10-1 de la loi n°95-73 modifiée du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.
- Article 5 de la loi 2006-784 du 5 juillet 2006 relative à la prévention des violences lors des manifestations sportives.
- Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, qui a créé l'article L5211-60 du Code général des collectivités territoriales.

2. Décrets

- Décret n°96-926 modifié du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.
- Décret n°97-46 du 15 janvier 1997 relatif aux obligations de surveillance ou de gardiennage incombant à certains propriétaires, exploitants ou affectataires de locaux professionnels ou commerciaux (article 4-II).
- Décret n° 97-47 du 15 janvier 1997 relatif aux obligations de surveillance incombant à certains propriétaires ou exploitants de garages ou de parcs de stationnement (article 1-III).
- Décret n° 2000-1234 du 18 décembre 2000 déterminant les aménagements des locaux desservis par les personnes physiques ou morales exerçant l'activité de transports de fonds.
- Décret 2004-296 du 29 mars 2004 modifiant le décret n° 2000-134 du 18 décembre 2000 déterminant les aménagements des locaux desservis par les personnes physique ou morales exerçant l'activité de transports de fonds.
- Décret n° 2006-665 du 7 juin 2006 relatif à la réduction du nombre et à la simplification de la composition de diverses commissions administratives.
- Décret n° 2006-672 du 8 juin 2006 relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif.
- Décret n° 2007-916 du 15 mai 2007 portant création de la Commission Nationale de la vidéosurveillance

3. Arrêtés

- Arrêtés des 3 et 21 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.
- Arrêté du 6 mars 2009 fixant les conditions de certification des installateurs de vidéosurveillance.

4. Circulaires

- Circulaire NOR INT D9600124C du 22 octobre 1996 relative à l'application de l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité
- Circulaire NOR INT D9700078C du 28 avril 1997 précisant le dossier de vidéosurveillance pour les stations services indépendantes
- Circulaire ministre NOR INT D0600096C du 26 octobre 2006 exposant les modifications apportées à la réglementation sur la vidéosurveillance à la suite de l'entrée en vigueur de la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, de son décret d'application n°2006-929 du 28 juillet 2006 relatif à la vidéosurveillance et modifiant le décret n°96-926 du 17 octobre 1996, ainsi que du décret n°2006-672 du 8 juin 2006 relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif.
- Circulaire ministre NOR INT K0800110C du 26 mai 2008 relative aux raccordements des centres de supervision urbaine aux services de police et de gendarmerie et conditions d'attribution du Fonds Interministériel de Prévention de la Délinquance en matière de vidéoprotection.
- Circulaire NOR INT K0900017C du 23 janvier 2009 du secrétaire général du CIPD relative aux orientations du FIPD pour l'année 2009
- Circulaire NOR INT D0900057C du 12 mars 2009 relative aux conditions de déploiement des systèmes de vidéoprotection.

5. Code du travail

- Article L 1221-9, aucune information concernant personnellement un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.
- Article L 1222-4, aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.
- Article L 2313-2, si un délégué du personnel constate, notamment par l'intermédiaire d'un salarié, qu'il existe une atteinte aux droits des personnes, à leur santé physique et mentale ou aux libertés individuelles dans l'entreprise qui ne serait pas justifiée par la nature de la tâche à accomplir, ni proportionnée au but recherché, il en saisit immédiatement l'employeur [...]
- Article L 2323-13, le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail [...]
- Article L2323-32, Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci [...]

6. Code civil

- Article 9, le droit à la vie privée.

7. Code pénal

- Article 226-1, qui réprime les atteintes à la vie privée.

B. Les normes techniques – Arrêté du 3 Août 2007

1. Arrêté du 3 Août 2007

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance

2. Arrêté du 3 Août 2007 – Annexes techniques

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance (rectificatif)

ANNEXE TECHNIQUE 1

3. Arrêté du 3 Août 2007 – Notice explicative

Note explicative de l'arrêté du 3 août portant définition des normes techniques en matière de vidéosurveillance

C. Dossier de demande d'autorisation pour un système de vidéosurveillance

La demande d'autorisation préfectorale ne doit être sollicitée que pour les dispositifs visionnant la voie publique et les lieux ou établissement recevant du public et qui ne conduisent pas à des fichiers structurés avec données nominatives pour l'identification des personnes.

Par ailleurs, il est également possible d'effectuer cette démarche via une télé-procédure en vous connectant au site internet http://www.videoprotection.interieur.gouv.fr/index/teleprocedure/ .

Le dossier à constituer sera différent selon que l'on se trouve dans le cadre d'une des quatre situations suivantes :

- Le dispositif de vidéosurveillance/de vidéo-protection visionne la voie publique
- Le dispositif visionne un lieu ou établissement recevant du public et comporte huit caméras ou plus
- Le dispositif visionne un lieu ou établissement recevant du public et comporte moins de huit caméras
- La demande porte sur la création d'un périmètre vidéosurveillé

1. Le dispositif de vidéosurveillance/de vidéo-protection visionne la voie publique

C'est le cas où le dossier est le plus complexe. Il va comporter :

- Le CERFA n°13806*01 qui rassemble les informations essentielles
- Un rapport de présentation dont le but principal est d'exposer les finalités, c'est-à-dire les raisons justifiant la mise en œuvre du dispositif (le niveau de risque, par exemple de délinquance de proximité dans la zone concernée, et les moyens techniques qui doivent respecter les normes de l'arrêté du 3 août 2007).

  Les caractéristique générales du système qu'il s'agisse des moyens d'acquisition (caméras fixes ou mobiles, nombre de caméras), de transmission des images puis de visualisation et de stockage.
- Le plan de masse :

  Ce plan doit permettre de vérifier la non visualisation de l'intérieur des immeubles d'habitation par les caméras visualisant la voie publique.

  Il doit indiquer : les bâtiments du pétitionnaire et les bâtiments appartenant à des tiers qui se trouveraient dans le champ de vision des caméras avec l'indication de leur accès et de leurs ouvertures.

  Ce plan doit bien sûr être lisible et clair. Il est important de faire figurer sur ce plan une représentation des masquages qui seront programmés dans les caméras pour empêcher la surveillance des parties privées.
- Le plan de détail

  Ce plan à l'échelle suffisante doit indiquer :
  - Nombre et l'emplacement des caméras
  - Les zones couvertes par celles-ci

  Il s'agit de vérifier que le champ de vision des caméras ne porte pas atteinte à l'intimité de la vie privée.
- La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images
  - Description des moyens d'enregistrement
  - Description des réseaux de transmission : fibre, cuivre, hertzien…,
  - Description des modalités d'exploitation des images : modalités de renvoi et d'exploitation des images en temps réels et différé :
    - Stockage local, avec ou sans possibilité de consultation à distance,
    - Centralisation vers un local technique.

Si certaines de ces informations peuvent être renseignées dans la rubrique 4.5. et 7 du CERFA, concernant les dispositifs de voie publique, un document de description plus élaboré est recommandé.

- La description des mesures de sécurité qui seront prises pour la sauvegarde et la protection des images éventuellement enregistrées.

  Moyens techniques dédiés à la sécurisation des installations : portes blindés, vidéo, alarmes (anti feu, anti-intrusion).

  - Procédures de sécurité dédiées à la sécurisation des installations

  Un document spécifique n'est pas à priori nécessaire, ces informations devant figurer dans le CERFA à la rubrique 8 mais, s'agissant d'un dispositif de voie publique, un document plus complet est toutefois recommandé.

- Les modalités de l'information du public :

  Le but est de faire en sorte que toute personne susceptible d'être filmée en soit prévenue. Le dossier doit donc contenir :

  - Un modèle de l'affiche ou panonceau. Concernant la voie publique le panonceau qui sera utilisé doit contenir un pictogramme représentant une caméra.
  - Une description des modalités : nombre d'affiches ou panonceaux, l'emplacement prévu de leur implantation. Cette description est prévue à la rubrique 9 du CERFA et le renseignement de cette rubrique suffit mais en cas de multiples implantations pour les dispositifs importants, un document décrivant de façon détaillée ce type d'information peut être apprécié.

- Le délai de conservation des images avec s'il y a lieu les justificatifs nécessaires

  - Le délai maximum est d'un mois. Il n'y a pas de délai minimum mais si un dispositif apparaît justifié par le niveau de délinquance de proximité, il n'aurait guère de sens si les images n'étaient pas conservées le temps minimum pour s'assurer de l'ouverture d'une procédure judiciaire. (Celle-ci permettra de conserver ensuite les images le temps nécessaire). Les services de sécurité estime en général à 7 jours le délai de sécurité.

  Cette information figurant dans le CERFA à la rubrique 5 qu'il faut obligatoirement compléter, aucun document sur ce point n'a besoin d'être joint au dossier.

- La désignation du personnel concerné par l'installation

  - Désignation de la personne ou du service responsable du système,
  - Désignation de la personne responsable de la maintenance,
  - Indication sur la qualité des personnes chargées de l'exploitation du système et susceptibles de visionner les images.

  L'ensemble de ces informations doit être renseigné dans le CERFA en complétant les rubriques 2, 6, 10 et, le cas échéant 7. Il n'y a par conséquent aucun document à fournir. S'agissant de la voie publique une information complémentaire concernant les opérateurs (recrutement, formation…) sera bien sûr appréciée. (Une note explicative peut suffire).

- Les consignes générales données aux personnels d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images.

  Si les indications principales figurent déjà dans le CERFA, s'agissant de la voie publique, il est recommandé de fournir une note d'information complémentaire répondant aux points suivants :

  - Règlement intérieur ou notes internes :
    - Personnel habilité à accéder aux images,
    - Conditions d'accès du personnel chargé de la maintenance,
    - Conditions d'accès des visiteurs.
  - Horaires de fonctionnement
  - Conditions d'accès des services en situation normale et en cas d'urgence

- Les modalités du droit d'accès des personnes intéressées

  L'information figure dans le CERFA. S'agissant de la voie publique, une information sur les règles internes mises en place pour permettre aux personnes intéressées d'accéder aux images enregistrées les concernant peut être appréciée, dans ce cas elle pourra faire l'objet d'une note complémentaire.

- La justification de la conformité du système de vidéosurveillance aux normes techniques de l'arrêté du 3 août 2007 :

  Deux situations se présentent :

  - L'installateur est certifié dans les conditions fixées par arrêté du ministre de l'Intérieur

  Dans ce cas, le CERFA mentionne l'identité de l'installateur et son numéro de certification. L'installateur doit remettre au maître d'ouvrage une attestation de conformité ; elle suffit à en justifier et, dans ce cas, un rapport technique n'est pas requis.

  - L'installateur n'est pas certifié

  Le maître d'ouvrage joint au dossier le questionnaire rempli par l'utilisateur. Les services préfectoraux et la commission départementale apprécient si ces indications sont suffisantes dans le cas concerné.

2. Le dispositif visionne un lieu recevant du public et comporte huit caméras ou plus

Le dossier comprendra les mêmes pièces et informations que ci-dessus sauf le plan de masse (ce dernier est en effet justifié parce qu'il permet de savoir quelles zones privatives d'immeubles le dispositif pourrait visionner, il n'a donc de sens que si le dispositif visionne la voie publique où peuvent se trouver de tels immeubles).

Précision : Les modalités d'information du public sur l'existence du dispositif seront plus précises et comportement la description du panneau d'information et de son ou de ses emplacements.

En ce qui concerne l'emplacement, chacun comprend qu'un panneau informatif devra être situé à l'entrée du lieu et le, cas échéant, du parking associé afin que les tiers choisissent en toute connaissance de cause d'y entrer ou non.

3. Le dispositif visionne un lieu recevant du public et comporte moins de huit caméras

Dans ce cas, qui, à la fois, présente a priori le moins de risques d'atteinte à la vie privée et correspond au plus grand nombre de demandes, le dossier sera simplifié.

Il ne comportera pas :

- Le rapport de présentation, l'exposé succinct des finalités, indications des risques et caractéristiques du système figurent déjà sur le CERFA,

- Le plan de masse exigé pour la seule voie publique,

- Le plan de détail indiquant nombre, implantation des caméras et zones couvertes par celles-ci. Le nombre de caméras et zones couvertes par celles-ci. Le nombre de caméras est indiqué dans le CERFA.

Il est par conséquent recommandé de renseigner attentivement toutes les rubriques du CERFA et de joindre simplement le modèle d'affiche d'information du public ainsi que le questionnaire de conformité du système si l'installateur n'est pas certifié. S'il est certifié, l'indication dans le CERFA doit suffire mais l'attestation remise de conformité de l'installateur doit pouvoir être produite à tout moment.

4. La demande porte sur la création d'un périmètre vidéosurveillé

Lorsque le système de vidéosurveillance porte sur un ensemble immobilier ou foncier de grande dimension ou complexe, il peut être demandé la création d'un périmètre vidéosurveillé.

Cette possibilité nouvelle ouverte par le décret modifié n° 96.926 concerne des types de situations différentes :

A titres d'exemples :

- Sur la voie publique, il pourra s'agir d'une place centrale avec les rues qui y conduisent ou un centre piétonnier comportant de s traverses ou de nombreuses petites rues,
- Dans un programme immobilier ce pourra être le fait d'un vaste projet devant comporter étude de sûreté ou d'un centre commercial comportant de nombreuses enseignes.

Dans ces cas, le nombre et l'implantation des caméras peuvent en effet être sujets à évolution.

Le dossier sera alors profondément différent.

- Le rapport de présentation devra établir non seulement les finalités et les risques que l'on devra réduire mais aussi, en fonction du site, l'intérêt de pouvoir adapter le nombre et l'implantation des caméras.
- Sera fourni un plan portant simple délimitation du périmètre ce document se substitue en fait aux plans de masse et de détail prévus pour les dispositifs de voie publique et/ou pour ceux de huit caméras ou plus.
- Le CERFA ne comportera pas d'indication sur le nombre de caméras, ni sur leur emplacement, c'est la rubrique 4.2 qu'il faut renseigner.

Les autres informations : description du dispositif, mesures de sécurité pour la sauvegarde des images, modalités d'information du public, délai de conservation des images, désignation du personnel, consignes d'exploitation, modalités du droit d'accès, seront évidemment fournis.

D. Documents

1. CERFA n°13806*01

DEMANDE D'AUTORISATION
D'UN SYSTÈME DE VIDÉOSURVEILLANCE

Loi n° 95-73 du 21 janvier 1995 - Article 10 - Décret n° 96-926 du 17 octobre 1996

N° 13806*01

MINISTÈRE DE L'INTÉRIEUR

Veuillez indiquer dans la case ci après le numéro du département de la préfecture compétente (il s'agit du département dans lequel vous souhaitez installer votre système de vidéosurveillance sauf s'il s'agit d'un système en réseau couvrant plusieurs départements auquel cas vous devez saisir la préfecture du département où est installé le siège social).

PARTIE RESERVEE A L'ADMINISTRATION

1 - NATURE DE LA DEMANDE

- ☐ Demande d'autorisation d'un nouveau système
- ☐ Modification d'un système autorisé — N° de dossier
- ☐ Demande de renouvellement d'un système autorisé — N° de dossier

DATE D'ARRIVEE :
RECEPISSE DELIVRE LE :
DATE DE LA DECISION :

2 - IDENTITE DU DECLARANT

Nom de naissance :
Prénom :
Dénomination de la collectivité territoriale ou la raison sociale de l'établissement ou de l'entreprise :
Éventuellement nom usuel ou sigle (si différent de la raison sociale) :
Activité :
Adresse : Numéro de voie | Extension (bis, ter...) | Type de voie (rue, av...) | Nom de la voie
Code postal : | Commune :
Téléphone : | Télécopie :
Adresse électronique du déclarant ou le cas échéant de la société, de l'établissement ou de la collectivité :

3 - INFORMATIONS GENERALES ET FINALITE DU SYSTÈME DE VIDEOSURVEILLANCE

a) Informations générales
Horaires d'ouverture (pour les établissements ouverts au public) :
A préciser le cas échéant, (descriptions des éventuelles agressions survenues ou risques à prendre en compte) :

b) Finalité du système : (veuillez cocher la ou les cases correspondantes)

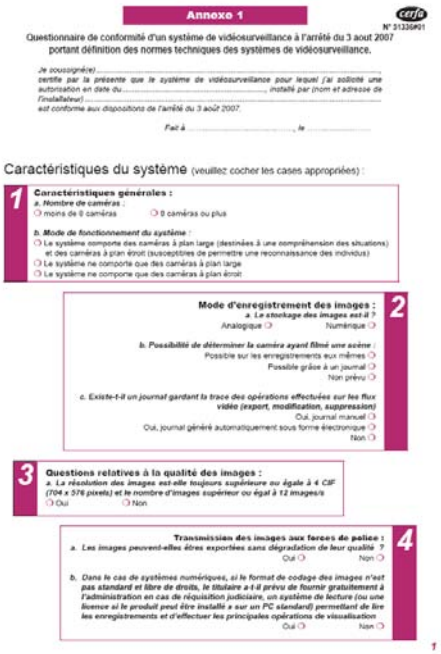
- ☐ Sécurité des personnes
- ☐ Protection incendie/Accidents
- ☐ Défense nationale
- ☐ Prévention des atteintes aux biens
- ☐ Protection des bâtiments publics
- ☐ Régulation du trafic routier
- ☐ Lutte contre la démarque inconnue
- ☐ Autres (préciser) :

4 - LOCALISATION DU SYSTÈME DE VIDEOSURVEILLANCE (Veuillez renseigner uniquement une des deux rubriques ci-dessous)

4-1) LIEU D'INSTALLATION ET NOMBRE DE CAMERAS (cette rubrique n'est pas à renseigner pour les demandes portant sur un périmètre vidéo-surveillé, dans ce cas vous ne devez renseigner que la rubrique 4-2)
Adresse : Numéro de voie | Extension (bis, ter...) | Type de voie (rue, av...) | Nom de la voie | Code postal | Commune
Nombre de caméras intérieures installées : ..... (*joindre le cas échéant le plan de détail et plan de masse (cf notice)*)
Nombre de caméras extérieures installées : ..... (*joindre le cas échéant le plan de détail et plan de masse (cf notice)*)
Pour les systèmes de moins de 8 caméras installées à l'intérieur d'un établissement ouvert au public, veuillez indiquer si après la superficie de l'établissement : m2

4-2) DEMANDE PORTANT SUR UN PERIMETRE VIDEOSURVEILLE (cette rubrique ne doit être renseignée que si vous souhaitez avoir recours à la notion de périmètre vidéosurveillé)
Si au moins une des caméras que vous souhaitez installer doit visualiser la voie publique, veuillez cocher la case ci-après ☐
Délimitation du périmètre : pour délimiter ce périmètre, veuillez indiquer ci-après les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre :
Adresse : Numéro de voie | Extension (bis, ter...) | Type de voie (rue, av...) | Nom de la voie | Code postal | Commune

2. Notice d'information



Annexe 1

N° 51336#01

Questionnaire de conformité d'un système de vidéosurveillance à l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

Je soussigné(e) .....
certifie par la présente que le système de vidéosurveillance pour lequel j'ai sollicité une autorisation en date du ..... installé par (nom et adresse de l'installateur) .....
est conforme aux dispositions de l'arrêté du 3 août 2007.

Fait à ..... le .....

Caractéristiques du système (veuillez cocher les cases appropriées) :

1 Caractéristiques générales :
a. Nombre de caméras :
○ moins de 8 caméras ○ 8 caméras ou plus
b. Mode de fonctionnement du système :
○ Le système comporte des caméras à plan large (destinées à une compréhension des situations) et des caméras à plan étroit (susceptibles de permettre une reconnaissance des individus)
○ Le système ne comporte que des caméras à plan large
○ Le système ne comporte que des caméras à plan étroit

2 Mode d'enregistrement des images :
a. Le stockage des images est-il ?
Analogique ○ Numérique ○
b. Possibilité de déterminer la caméra ayant filmé une scène :
Possible sur les enregistrements eux mêmes ○
Possible grâce à un journal ○
Non prévu ○
c. Existe-t-il un journal gardant la trace des opérations effectuées sur les flux vidéo (export, modification, suppression)
Oui, journal manuel ○
Oui, journal généré automatiquement sous forme électronique ○
Non ○

3 Questions relatives à la qualité des images :
a. La résolution des images est-elle toujours supérieure ou égale à 4 CIF (704 x 576 pixels) et le nombre d'images supérieur ou égal à 12 images/s
○ Oui ○ Non

4 Transmission des images aux forces de police :
a. Les images peuvent-elles être exportées sans dégradation de leur qualité ?
Oui ○ Non ○
b. Dans le cas de systèmes numériques, si le format de codage des images n'est pas standard et libre de droits, le titulaire a-t-il prévu de fournir gratuitement à l'administration en cas de réquisition judiciaire, un système de lecture (ou une licence si le produit peut être installé s sur un PC standard) permettant de lire les enregistrements et d'effectuer les principales opérations de visualisation
Oui ○ Non ○

1

E. Informations complémentaires

Pour toutes informations supplémentaires sur les démarches et la mise en application de la réglementation en vigueur, le ministère de l'intérieur met à disposition son site web : http://www.videoprotection.interieur.gouv.fr.

F. La CNIL et la Vidéosurveillance

1. Quelles formalités accomplir avant de mettre en place un système de vidéosurveillance ?

	Lieu public (ouvert au public)	Lieu privé (non ouvert au public)
Sans enregistrement d'images numériques	Autorisation préfectorale	Aucune déclaration
Avec enregistrement d'images numériques	Autorisation préfectorale	Déclaration normale auprès de la CNIL
Avec alimentation d'un fichier	Déclaration normale ou demande d'avis auprès de la CNIL	Déclaration normale ou demande d'avis auprès de la CNIL
Avec constitution d'un fichier d'infractions	Autorisation ou demande d'avis auprès de la CNIL	Autorisation ou demande d'avis auprès de la CNIL
Avec reconnaissance faciale ou analyse comportementale	Autorisation CNIL ou demande d'avis auprès de la CNIL	Autorisation CNIL ou demande d'avis auprès de la CNIL

Tableau 5 – Récapitulatif des formalités accomplir avant de mettre en place un système de vidéosurveillance

N.B : la demande d'avis concerne les traitements mis en œuvre pour le compte de l'État, aux termes de l'article 26 de la loi informatique et libertés modifiée

Dans tous les cas :

- Information des personnes par un panneau d'information situé à l'entrée de l'établissement
- Information préalable des instances représentatives du personnel
- Respect de l'intimité des personnes (interdiction de filmer les toilettes, les vestiaires, l'intérieur d'un appartement)
- Une durée de conservation limitée à un mois

2. Informations complémentaires

Pour toutes informations supplémentaires sur les démarches et la télé-déclaration, la CNIL met à disposition un dossier sur son site web : http://www.cnil.fr/dossiers/videosurveillance/

III Systèmes de vidéosurveillance/ de vidéo-protection

A. Pourquoi utiliser de la vidéosurveillance/la vidéo-protection ?

La vidéosurveillance/la vidéo-protection a pour but de :

- Protéger les personnes, les biens, les habitations, les entreprises…
- Dissuader et rassurer – Aspect dissuasif
- Aider à la gestion – Visualisation des places libres dans un port, des voitures mal garées, ou assistance aux plaisanciers…
- Informer – Utilisation touristique (météo, visualisation du port sur site internet)…

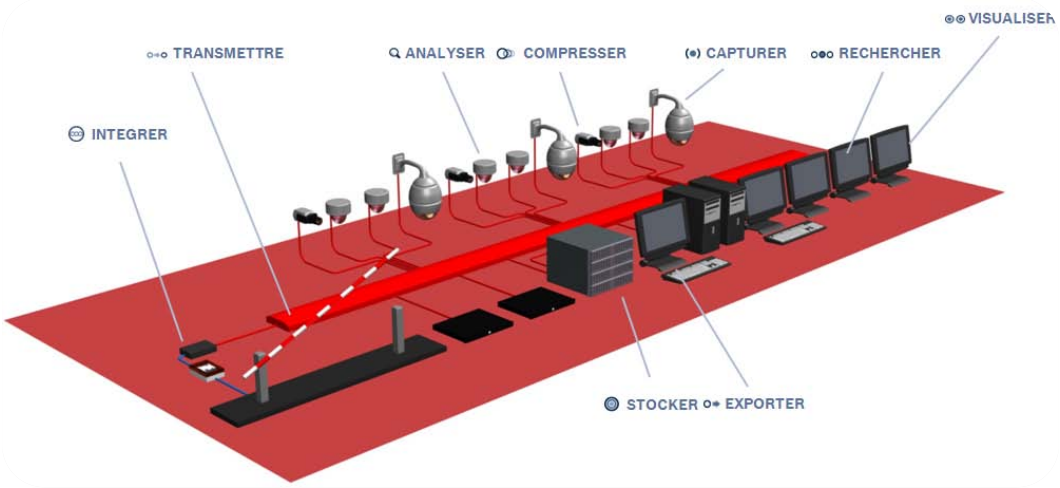
Cette liste est non exhaustive mais permet d'appréhender la multitude d'applications liées à l'utilisation d'un système de vidéosurveillance/de vidéo-protection.

En outre, le but principal de la vidéosurveillance/la vidéo-protection reste l'obtention d'une image utilisable quelque soit les conditions et surtout à n'importe quel moment.

B. Les composants d'un système de vidéosurveillance

Un système de vidéosurveillance/de vidéo-protection peut être décomposé en 9 parties :

- La capture
- L'analyse
- La compression
- La transmission
- La visualisation
- Le stockage
- La recherche
- L'exportation
- L'intégration



1. La capture

La capture est l'un des éléments clés d'un système de vidéosurveillance car il va permettre de fournir les données vidéo à l'ensemble de la chaîne. Les éléments essentiels pour réaliser une capture de qualité sont :

- La caméra
- L'objectif
- L'éclairage

a) La caméra

Les caméras peuvent être classées en deux catégories :

- Les caméras fixes
- Les caméras mobiles, orientation (pan), inclinaison (tilt) et zoom (zoom) dites aussi caméras PTZ

Les caméras fixes permettent d'observer une zone prédéterminée lors de l'installation de celles-ci. En général elles sont installées pour surveiller des passages obligés, des périmètres, ou pour détecter la réalité d'une menace (surveillance d'un couloir, d'une porte, d'une entrée).

Les caméras mobiles ont l'avantage de permettre à l'opérateur de pouvoir observer une région de 360° autour de la caméra. Les caméras mobiles sont davantage utilisées pour suivre une menace mobile ou pour être opérées manuellement (rondes ou patrouilles vidéo par exemple), elles nécessitent logiquement un mode d'opération plus exigeant (grande place, grand parking, surveillance périmétrique). Ces caméras bien que très utiles pour la gestion temps réel ou sur événement sont souvent moins efficaces pour une analyse à posteriori puisqu'elles peuvent être mal orientées au moment où l'événement est apparu.

Le choix dépend donc de la nature de la menace mobile ou non, de l'existence de passages obligés, et des moyens associés à l'exploitation de la vidéo-protection.

Plusieurs types de caméras existent parmi ces deux catégories :

- Les caméras couleurs permettent d'apporter beaucoup plus d'informations qu'une image monochrome et est donc plus efficace en termes d'identification.

  A titre d'exemple, si des personnes habilitées à pénétrer dans une zone sécurisée doivent être vêtues d'une blouse orange, il est impossible, sur une image monochrome, de les discerner d'individus habillés d'une blouse bleue. Le rendu des gris est identique.

  En revanche, les caméras couleurs sont moins sensibles à la lumière que les caméras noir et blanc.

- Les caméras noir et blanc sont ainsi plus souvent utilisées, pour des applications en éclairement faible.
- Pour couvrir les 2 précédentes applications, des caméras Jour/Nuit avec filtre infrarouge spécifique ont été conçues. Lorsque l'éclairement est satisfaisant, l'image est transmise en couleurs, s'il est insuffisant, l'image est transmise en noir et blanc, la bascule peut être automatique ou manuelle. Sur un site de grande taille avec des éclairages différents, il peut être utile de basculer simultanément toutes les caméras en mode N/B pour éviter l'hétérogénéité des affichages.

Lorsque les conditions d'éclairage ne sont pas suffisantes il est possible de coupler un dispositif d'éclairage infrarouge (directement intégré à la caméra ou dans un module complémentaire), permettant d'éclairer la scène avec une lumière invisible à l'œil nu, mais visible par la caméra. Ce type d'éclairage, selon la puissance utilisée, peut permettre une bonne observation de nuit. Les caméras doivent alors avoir une bonne sensibilité spectrale dans la gamme des infrarouges.

Des caméras thermiques peuvent être utilisées également pour des besoins spécifiques. Leurs coûts et leurs capacités les réservaient à des besoins de type quasi-militaires. Le marché de ce type de caméra est cependant en plein développement et les prix deviennent très abordables. Cependant les images issues de ces caméras ne permettent pas d'identifier, mais seulement de détecter une intrusion, et sont exclusivement réservées à un usage nocturne.

Figure 10- Exemple d'image thermique

Nota: Les caméras dites caméras thermiques restituent une image en fonction de la température de la scène observée (l'image en sortie est constituée de points chauds et de zone froide). Les caméras infrarouges évoquées précédemment restituent elles une image en fonction de la lumière émise ou réfléchie par les éléments de la scène (l'image en sortie est assez proche de ce que produit une caméra noir et blanc).

Une caméra se décompose en deux parties :

- Le capteur
- Le processeur assurant le traitement d'image

i. Le capteur de la caméra

1) Les technologies

En vidéosurveillance, il existe différentes technologie de capteurs :

- Technologie CCD (Charge Coupled Device)
- Technologie CMOS (Complementary Metal Oxyde Semiconductor)

Le **capteur CCD**, le capteur à transfert de charges, ou capteur CCD (Charge Coupled Device), fait appel à la technologie des semi-conducteurs et se présente sous forme de rangée ou plus souvent de matrice de capteurs individuels microscopiques qui assureront chacun la génération d'un pixel. Chacun de ces capteurs transforme en effet la lumière qu'il reçoit en signaux électriques qui sont ensuite numérisés par un convertisseur analogique- numérique.

Capteur CCD - Points forts :

- Haute résolution : qualité d'image et sensibilité
- Niveau de bruit très faible
- Uniformité de l'image
- Rendu des couleurs

Capteur CCD - Points faibles :

- Dynamique trop faible dans des situations d'images contrastées
- Sensibilité à l'éblouissement (blooming)
- Sensibilité à l'effet de traînée verticale (smearing)

Le **capteur CMOS** (Complementary Metal Oxide Semiconductors) est un nouveau type de détecteur semi-conducteur à oxyde de métal complémentaire. Ce sont de minuscules circuits et dispositifs gravés sur des puces de silicium. La fabrication de capteurs d'image CMOS selon le même procédé que pour les puces d'ordinateur se traduit par une baisse spectaculaire des coûts. Le coût de fabrication d'une plaquette CMOS est le tiers de celui d'une plaquette équivalente avec des dispositifs à couplage de charge.

Comme pour les capteurs CCD, la cible comporte des cellules élémentaires, le plus souvent organisées en ligne et en colonnes. Chaque cellule élémentaire peut être équipée d'un amplificateur intégré. La sortie des amplificateurs composant une ligne est validée séquentiellement par l'intermédiaire d'une ligne d'adressage. La technologie CMOS permet l'intégration des opérateurs analogiques (amplificateurs) ou numériques (adressage) sur la même puce de semi-conducteur.

Capteur CMOS - Points forts :

- Une bonne dynamique face aux contrastes.
- Fréquence d'image élevée.
- Possibilité de traiter une partie de l'image (ROI : Region Of Interest) autorisant une plus grande cadence.
- Électronique moins complexe.
- Faible consommation d'énergie.
- Compacité.
- Meilleure intégration de fonctions de traitement au plus près du capteur.

Capteur CMOS - Points faibles :

- Sensibilité insuffisante aux faibles luminosités

2) Taille de capteur

Les capteurs peuvent être de tailles différentes. En matière de vidéosurveillance, on recense quatre tailles couramment utilisées selon le type de capteur.

Capteur	Taille	Diagonale (en mm)	Hauteur (en mm)	Largeur (en mm)
CCD	1/4”	4	3.6	2.7
	1/3”	6	4.8	3.6
	1/2”	8	6.4	4.8
CMOS	2/3”	11	8.8	6.6

Tableau 6 - Différentes tailles de capteurs

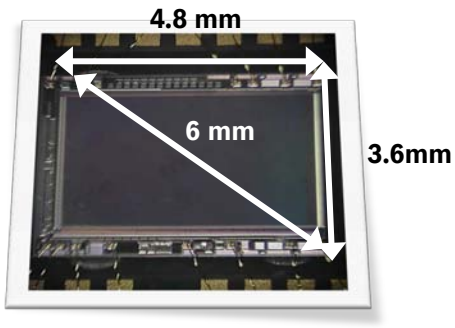


Figure 11 – Capteur 1/3“

3) La HD

Actuellement, le marché grand public draine les développements technologiques sur la compression H264, les capteurs HD et l’enregistrement. De plus, les progrès technologiques permettent d’améliorer la qualité d’image de façon constante

Alors, pourquoi la haute définition ?

L’approche traditionnelle consiste à argumenter sur le fait qu’une caméra HD peut remplacer plusieurs caméras SD (standard définition). La valeur ajoutée de la HD est de fournir une image plus détaillée afin d’identifier plus facilement les personnes ou les situations. Une définition plus importante permet une détection plus fiable de l’intelligence embarquée. L’efficacité des technologies d'analyse d'image se trouve renforcée

L'élément clé est que les solutions ainsi que le marché sont prêts à accueillir cette nouvelle technologie.

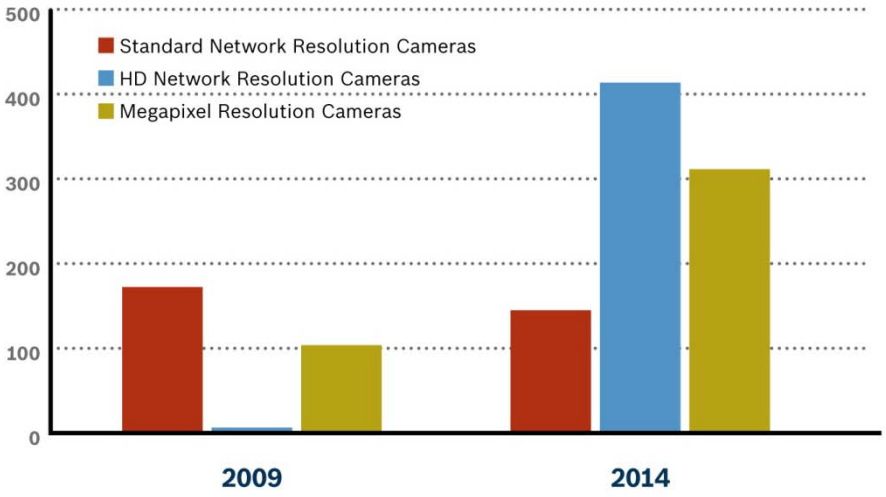


Figure 12 - Evolution du marché Européen par resolution

Standard Network Resolution Cameras – Caméras réseaux en résolution standard
HD Network Resolution Cameras – Caméras réseaux en résolution HD
MegaPixel Resolution Cameras – Caméras réseaux MegaPixel

Les résolutions :

La résolution maximum en SD est le 4 CIF soit 640x480 pixels. Lorsque l'on aborde la HD, on parlera de deux résolutions

- 720p soit 1280 x **720**
- 1080p soit 1920 x **1080.**

HD ou MegaPixel ?

Les caméras HD sont des caméras MegaPixel. Les caméras MP suivent surtout l'industrie des appareils photo

	HD	MP
Définition max du capteur	2.1 MP	16 MP
Résolution	1280 x **720** 1920 x **1080**	Nombreuses combinaisons
Format	16:9	4:3, 5:4
Taux de raffraichissement	(Elevé) 30	(Faible) 3 – 15
Norme	Standard reconnu	Aucune, dépend du nombre de pixels

ii. Le traitement d'image

Cette partie constitue l'intelligence de la caméra c'est-à-dire toutes les fonctions permettant d'exploiter au mieux l'image fournir par le capteur.

Le traitement d'images des caméras est réalisé par une puce appelée DSP (Digital Signal Processing). Il est possible qu'une caméra soit équipée de plusieurs DSP afin de pouvoir réaliser le traitement d'image et l'analyse du contenu de l'image par exemple.

La puissance du DSP s'évalue par le nombre de bits. Toutefois, une caméra s'évalue également par les fonctions de traitement d'image proposées par la caméra.

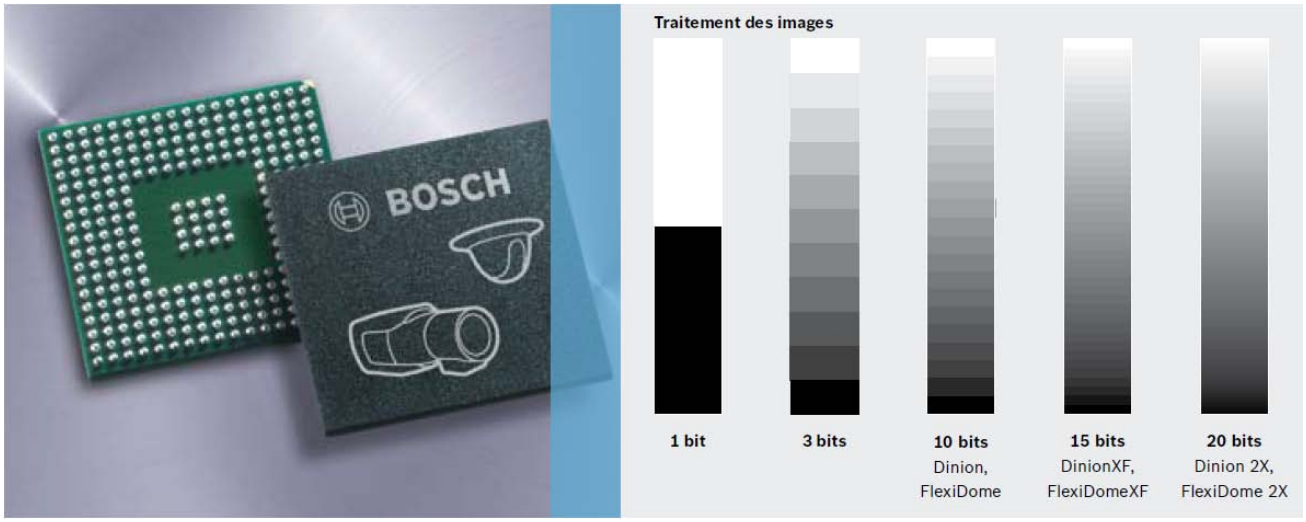


Figure 13 - Traitement des couleurs en fonction du nombre de bits – Exemple sur du Noir & Blanc

Exemples de fonctions de traitement d'image :

- Compensation de contre-jour

Avec compensation   Sans compensation

- La compensation Noir Auto (Auto Black) est une technique permettant de renforcer le niveau de signal vidéo afin de produire un signal à amplitude totale, même lorsque le contraste de la scène est inférieur à la pleine gamme. La portion la plus sombre du signal est définie en noir et la portion la plus claire en blanc, ce qui augmente le contraste.
- Le shutter intelligent optimise automatiquement la vitesse d'obturation. Quand la luminosité est normale, l'obturation rapide permet d'éviter les flous, tandis que la vitesse normale garantit une sensibilité optimale quand il fait plus sombre
- Compensation de câble
- Balance des blancs automatique - Fonction permettant à une caméra couleur de régler automatiquement sa couleur de sortie, afin de restituer des couleurs naturelles indépendamment de l'éclairage utilisé.
- Réduction automatique du bruit (DNR) - Traitement vidéo numérique mesurant le bruit de l'image et le réduisant automatiquement.

a) L’objectif

i. Qu’est ce qu’un objectif ?

L’objectif est l’élément qui va définir la qualité finale de votre image. L’objectif est un ensemble optique qui capture l’image en focalisant la lumière sur le capteur.

L’objectif est couplé à l’iris (diaphragme) qui permet de réguler la quantité de lumière qui passe.

La longueur des objectifs est mesurée en millimètres et indique la distance entre le centre de la lentille de l’objectif et le capteur. Cette mesure définie si l'angle de vision est large ou étroit. Cette caractéristique est aussi appelée focale et définie le grossissement de l'image. Plus cette longueur est petite plus l'angle de vision est large. Donc avec une caméra, objectif de 8 mm, l'angle de vision sera plus large qu'une caméra 12mm ou à l'inverse, plus on augmente la focale plus on diminue l'angle.

En conséquence, plusieurs éléments vont avoir leur importance :

- Sa focale (fixe ou variable)
- Son angle de champ de vision
- Son ouverture c’est-à-dire la quantité maximale de lumière captée par l’objectif
- Sa distance minimale de mise au point

ii. Types d’objectifs

Il existe 3 types d’objectif :

- Focale fixe
  - Sans iris
  - Iris manuel
  - Auto-iris
- Focal variable
  - Iris manuel
  - Auto-iris
- Zoom
  - Auto-iris

Pour choisir un objectif, il faut prendre en compte plusieurs paramètres comme :

- La monture C ou CS
- Le format du capteur CCD ou CMOS (cf i.2) Taille de capteurIIIB.1.a)i.2)
- La focale
- L'iris

iii. La monture C ou CS

Les montures sont définies suivant la distance entre le capteur et l'objectif. Ainsi, pour une monture CS, la distance entre le capteur et l'objectif doit être de 12.5mm. Pour une monture C, la distance entre le capteur et l'objectif doit être de 17.5mm.

Pour passer du montage C en montage CS, vous devez utiliser une bague de 5 mm.

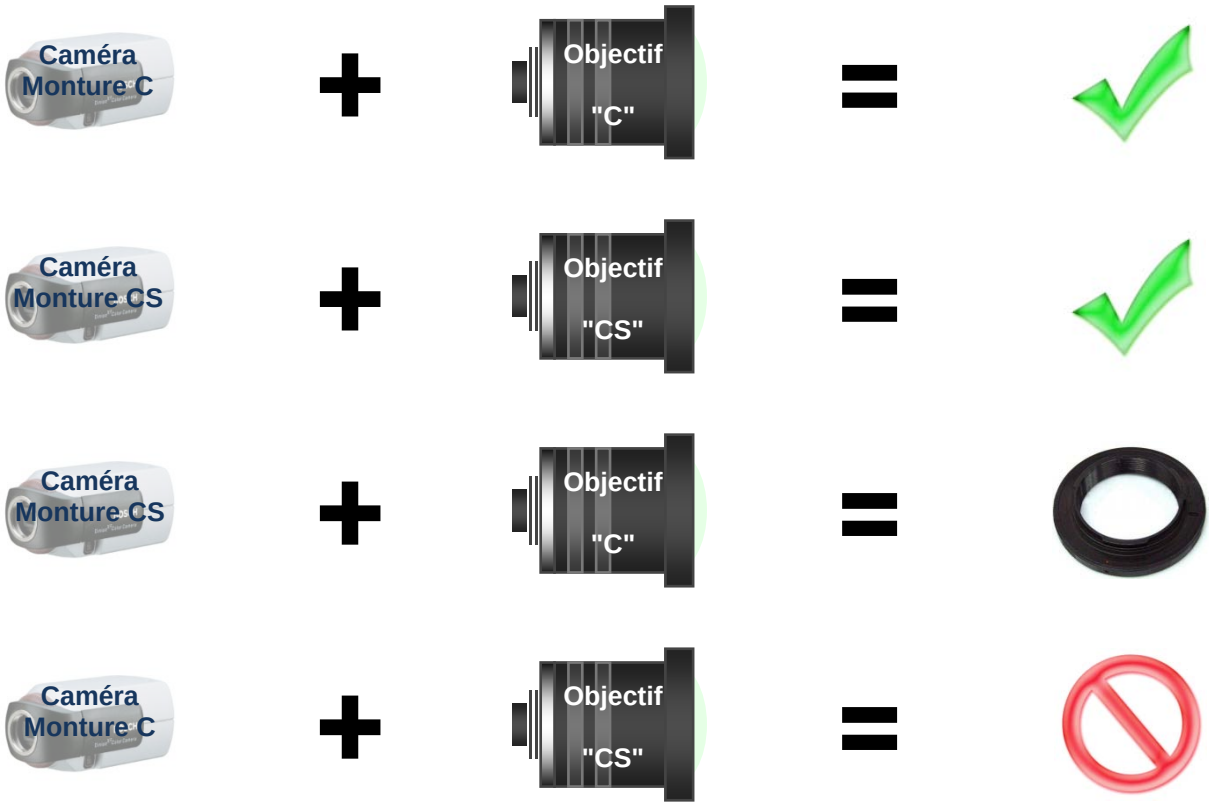


Tableau 7 – Tableau des combinaisons caméra et objectif

iv. La focale

La distance focale représente la distance en millimètres qui sépare le capteur du centre optique de l'objectif (assimilé au point nodal, c'est-à-dire le point où les rayons commencent à converger), lorsque la mise au point est faite sur l'infini.

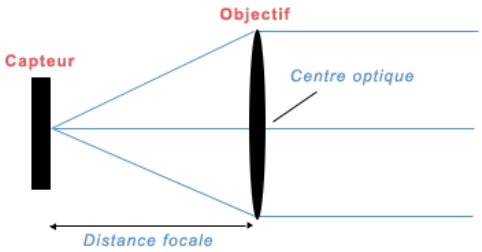


Figure 14 – Schéma de principe

Elle est exprimée en mm, cette valeur détermine directement l'angle de vue.

Plus elle est élevée, plus l'objectif « grossit » et plus l'angle de champ de vision est faible et inversement.

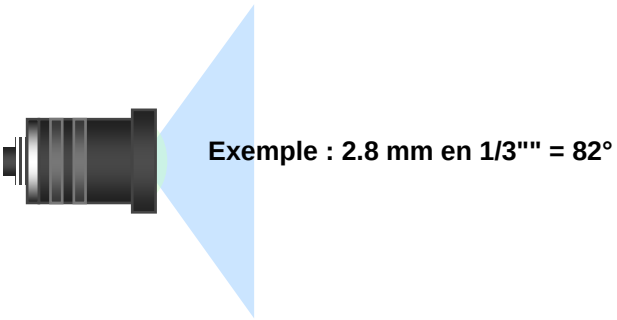


Figure 15 – Objectif 2.8 mm dit « grand angle »

Figure 16 – Objectif 50 mm dit « téléobjectif »

Figure 17 - Un même objet photographié à travers diverses focales depuis un même point (le photographe ne se déplace pas)

Pour déterminer la focale d'un objectif, vous utiliserez la formule mathématique suivante :

$$\textbf{Focale} = \textbf{Distance} \times \frac{\textbf{Largeur du capteur}}{\textbf{Largeur de la scène}}$$

Figure 18 – Calcul de la distance focale

v. L'iris

L'iris permet le réglage de la quantité de lumière qui atteint la surface sensible du capteur. La valeur est indiquée par la lettre F puis un nombre. Plus ce nombre est grand, moins il laisse passer la lumière

Les valeurs retenues sont les suivantes d'un iris ouvert vers un iris fermé :

1 - 1,4 - 2 - 2,8 - 4 - 5,6 - 8 - 11 - 16 - 22 – 32

La valeur F d'un objectif (ouverture de l'iris) exprime le rapport entre la distance focale et le diamètre efficace de l'iris. Elle détermine la quantité d'énergie lumineuse admise au niveau du capteur et joue un rôle important dans le résultat final. Plus la valeur F est grande, moins la lumière parvient au capteur. Moins la valeur F est élevée, plus la lumière arrive au capteur et meilleure est la qualité de l'image obtenue dans des situations de faible exposition.

- Iris à contrôle manuel : Dans ce cas, l'iris est en général réglé lors de l'installation de la caméra, de manière à l'adapter aux conditions de luminosité ambiantes. Ces objectifs ne pouvant réagir aux changements d'exposition, on règlera l'iris sur « moyen » pour des conditions de luminosité variable.

- Iris à contrôle automatique **:** Dans les conditions d'extérieur ou quand l'exposition varie constamment, il est préférable d'utiliser un objectif équipé d'un diaphragme à contrôle automatique. L'ouverture de l'iris est alors commandée par la caméra et adaptée en permanence de manière à garder un niveau de luminosité optimal pour le capteur d'images.

    - Iris DC : L'iris connecté à la sortie de la caméra est contrôlé par le processeur de la caméra.

    - Iris par contrôle vidéo : contrôlé par le signal vidéo.

  Les objectifs auto-iris sont recommandés pour les applications en extérieur. L'iris ajuste automatiquement la quantité de lumière qui parvient à la caméra. Le résultat est optimal et le capteur d'images est protégé contre les risques de surexposition.

Un iris de faible diamètre permet de réduire la lumière pour une meilleure profondeur de champ (mise au point sur une distance plus grande). Un iris plus large offre quant à lui une meilleure qualité d'image en cas de faible luminosité.

vi. Le tirage optique

Le choix de l'objectif est critique dans une application de vidéosurveillance mais le réglage de l'ensemble caméra/objectif l'est aussi.

Le tirage optique d'un objectif est une opération, qu'il est indispensable d'exécuter à chaque changement, ou montage d'un objectif, afin d'obtenir une image parfaitement focalisée quelque soit les conditions d'éclairage.

En effet, une caméra, dont le tirage optique n'a pas été effectué, fournira des images floues à l'aube et au crépuscule.

La procédure de réglage du tirage optique dépend du produit utilisé. Généralement, cette procédure ne s'applique qu'aux caméras fixes non prêtes à l'emploi (sur les caméras prêtes à l'emploi, le tirage optique est réalisé en usine).

b) L’éclairage

i. Définitions

1) Spectre électromagnétique

Les concepts de lumière et de vision sont tellement liés entre eux dans l'usage courant que l'idée de "lumière invisible" semble à première vue contradictoire. Pourtant la lumière visible n'est qu'une petite partie de ce qu'on appelle aujourd'hui le spectre électromagnétique.

Le spectre électromagnétique est la décomposition du rayonnement électromagnétique selon ses différentes composantes en terme de fréquence, d'énergie des photons ou encore de longueur d'onde associée, les trois grandeurs v (fréquence), E (énergie) et λ (longueur d'onde) étant liées deux à deux par la constante de Planck h et la vitesse de la lumière c , selon les formules :

$$\begin{matrix} E = h\nu \\ c = \lambda\nu \end{matrix}$$

d'où aussi :

$$E = \frac{hc}{\lambda}$$

Pour les ondes radio et la lumière, on utilise habituellement la longueur d'onde. À partir des rayons X, les longueurs d'ondes sont rarement utilisées : comme on a affaire à des particules très énergétiques, l'énergie correspondant au photon X ou γ détecté est plus utile. Cette énergie est exprimée en électronvolt (eV), soit l'énergie d'1 électron accéléré par un potentiel de 1 volt.

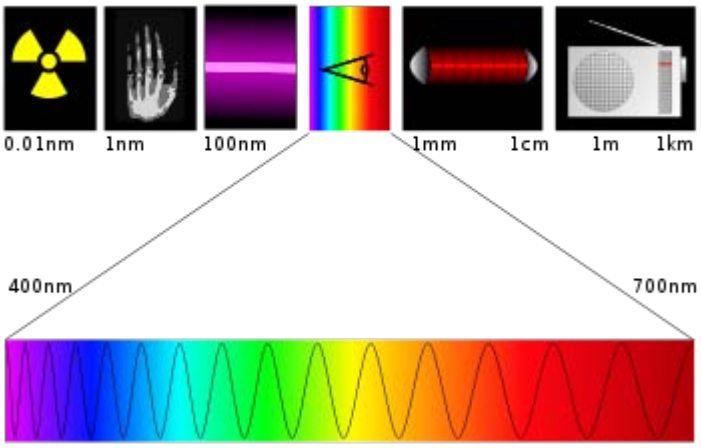


Figure 19 - Le domaine visible du spectre électromagnétique

2) Infrarouge

Le rayonnement infrarouge (IR) est un rayonnement électromagnétique d'une longueur d'onde supérieure à celle de la lumière visible mais plus courte que celle des micro-ondes.

Le nom signifie « en-deçà du rouge » (du latin infra : « en-deçà de »), le rouge étant la couleur de longueur d'onde la plus longue de la lumière visible. Cette longueur d'onde est comprise entre 700 nm et 1 mm.

Les infrarouges sont souvent subdivisés en IR proches (0,7-5 µm), IR moyens (5-30 µm) et IR lointains (30-1 000 µm). Toutefois cette classification n'est pas précise, chaque domaine d'utilisation ayant sa propre idée de la frontière entre les différents types.

Les infrarouges sont souvent associés à la chaleur car, à température normale, les objets émettent spontanément des radiations dans le domaine des infrarouges ; par ailleurs, le rayonnement infrarouge met

en vibration les atomes du corps qui les absorbe et donc élève sa température (transfert de chaleur par rayonnement).

Les infrarouges sont utilisés dans les équipements de vision de nuit quand la quantité de lumière visible est insuffisante pour voir les objets. Le rayonnement est détecté puis affiché sur un écran, les objets les plus chauds devenant aussi les plus lumineux. Il faut également ajouter comme utilisation, en plus de la vision de nuit, tout le domaine de la thermographie infrarouge permettant de mesurer à distance et sans contact la température d'objets cible. Il existe d'autres applications mais qui ne touchent pas le domaine de la vidéosurveillance.

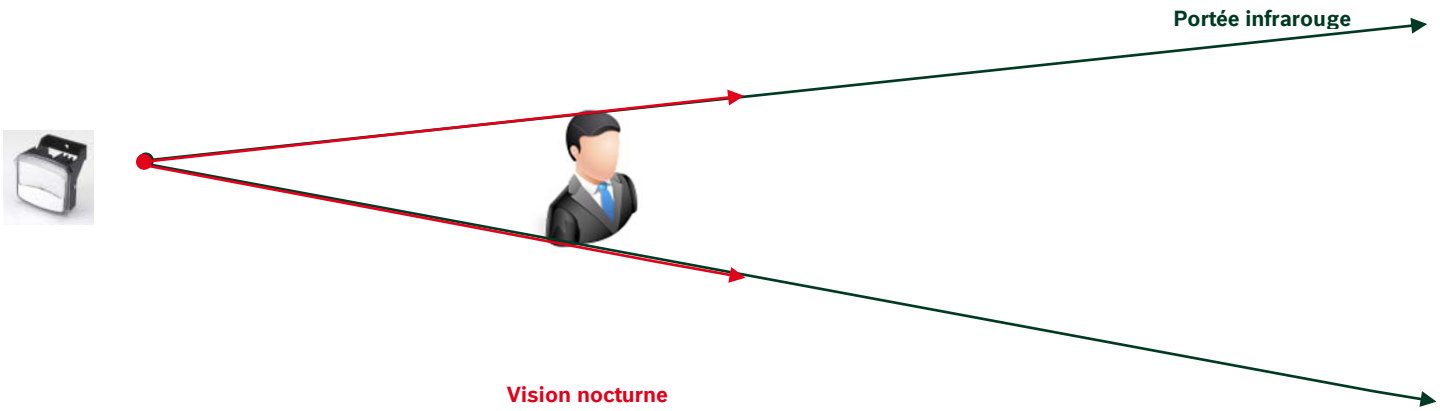
3) Notions de portée et de vision nocturne

Il ne faut pas confondre les termes « portée » et « vision nocturne » lorsque l'on parle de vidéosurveillance.

La portée d'un éclairage correspond à la distance maximale pouvant être atteinte par la lumière infrarouge ou visible.

La vision nocturne correspond à la distance maximale de visualisation et dépend de l'ensemble caméra/objectif utilisé.

En matière de vidéosurveillance, il est important de connaître la distance de vision nocturne et le matériel utilisé pour faire les tests ayant permis de fournir cette distance. Ainsi, il vous sera plus simple de choisir votre éclairage en fonction de l'ensemble caméra/objectif utilisé.



ii. Applications à la vidéosurveillance

4) L'éclairage pour la vidéosurveillance

Depuis quelques années, l'éclairage est devenu un élément critique de la surveillance 24h/24. En effet, la plupart des méfaits ont lieu la nuit et l'éclairage permet d'obtenir des images exploitables pour les forces de l'ordre.

Dans les applications de vidéosurveillance/de vidéo-protection, il est utilisé deux sortes d'éclairage :

- Eclairage en lumière blanche ou visible (éclairage urbain, éclairage à LED dédié à la vidéosurveillance ...)

  La lumière visible est une reproduction la plus fidèle possible de la lumière du jour par un éclairage. Dans le cadre d'une application couleur de nuit, on utilisera ce type de lumière, optimisée pour la vidéosurveillance. Cet éclairage apporte également un effet dissuasif.

- Eclairage infrarouge – Deux longueurs d'onde sont principalement utilisées en vidéosurveillance/vidéo-protection

  - 830-850 nm – Cette longueur d'onde produit un faible rayonnement rouge visible uniquement lorsqu'on le regarde dans l'axe de l'éclairage. Cet éclairage est aussi défini comme semi-furtif.

    Il reste le plus utilisé dans le milieu de la sécurité dès qu'un éclairage infrarouge est nécessaire. Il a l'avantage de proposer des distances de vision nocturne plus importantes que le 940-950 nm ou la lumière visible

  - 940-950nm – Cette longueur d'onde est plus connue sous le nom de lumière noire. Cet éclairage est aussi défini comme furtif. Ce type d'infrarouge ne produit aucun rayonnement rouge pouvant être vu par un œil humain. Il doit être utilisé avec des caméras ayant une sensibilité très élevée.

  Nous avons également constaté un accroissement de l'utilisation des éclairages infrarouges permettant de limiter la pollution lumineuse.

Figure 20 - Type d'éclairage utilisé en vidéosurveillance/vidéo-protection

L'utilisation d'éclairage a également un effet sur le stockage des images notamment avec l'utilisation des nouvelles technologies de compression vidéo.

D'une part, il est généralement constaté que des conditions de très faible luminosité entraînent du bruit et une qualité basse de la vidéo.

D'autre part, les nouveaux algorithmes de compression vidéo telle que le MPEG-4 ou le H.264 se base sur les parties immobiles de la scène pour réduire le débit de données. Le bruit est interprété par ces algorithmes comme du mouvement, qui par définition est sensé être une information utile. Le résultat ? Un débit de données élevé.

Un éclairage uniforme sur l'ensemble de la scène et adapté à la vidéosurveillance résout cette problématique en réduisant le bruit et permet de fournir des images exceptionnelles même de nuit. Le résultat ? Un débit de données bas donc une bande passante préservée et un espace de stockage optimisé

Pas de bruit dans la vidéo grâce à un éclairage Bosch adapté

Bonne compression

Débit de données bas

=	=
Réseau optimisé	**Réduction de l'espace de stockage Jusqu'à 70 % de nuit**

Enfin, l'éclairage permettra une analyse de vidéo plus performante.

5) Eclairage à LED

Dans le cas de la lumière visible ou infrarouge, la technologie d'éclairage à LED s'impose pour les applications de vidéosurveillance/de vidéo-protection. Tout d'abord, nous pouvons réaliser un comparatif sur l'efficacité énergétique des différentes solutions d'éclairage dans le domaine de la vidéosurveillance.

Efficacité	0%	15%	40%	60%	90%	100%
	**Lampes incandescentes (halogènes inclus)** Efficacité énergétique quasi nulle, les lampes halogènes dissipent 85% de leur énergie en chaleur (90 % pour les lampes normales), durée de vie courte (~5 mois), beaucoup de coût de maintenance					
	**Lampes fluorescentes** Efficacité énergétique réduite, les lampes fluorescentes dissipent 60% de leur énergie en chaleur, durée de vie longue (>5 ans), Utilisation faible du à l'effet de scintillement provoqué par ces dernières					
	**Lampes HID (High Density Discharge)** Efficacité énergétique correcte, les lampes HID dissipent entre 20-40% de leur énergie en chaleur, durée de vie longue (~4 ans), Utilisation faible du à leur lenteur d'allumage (~2-3 min) et l'impossibilité de les éteindre tout de suite					
	**Eclairage à LED** Efficacité énergétique reconnu, les éclairages à LED ne dissipe que seulement 10% de leur énergie en chaleur, durée de vie longue (jusqu'à 10 ans), peu de coût de maintenance					

Tableau 8 – Comparatif sur l'efficacité énergétique

Enfin, nous analyserons les coûts engendrés par les différentes solutions d'éclairages.

	Lampe halogène	Lampes HID	Eclairage LED Bosch
			
Efficacité Energie réellement utilisé pour l'éclairage	15 % de l'énergie consommée	20-40 % de l'énergie consommée	90 % de l'énergie consommée
Consommation électrique	500 W	250 W	45 W max.
Coût électrique*	264 €	132 €	24 €
Durée de vie de la lampe / des LED	5.5 mois	24 mois	120 mois (10 ans)
Remplacement de lampe / an	2	0.5	0
Prix de la lampe	10 €	25 €	N/A
Coût des lampes / an	20 €	12.5 €	0 €
Coût de la maintenance / an**	50 €	12.5 €	0 €
Coût total / an	**334 €**	**157 €**	**24 €**

* Basé sur utilisation de 4 400 heures / an à 0.12 € du kW/h
** Calculé avec un coût de 25 € par changement de lampe

Tableau 9 – Comparatif des coûts d'exploitation

Par exemple, 10 éclairages à LED fonctionnant durant 5 ans permettront une économie de :

- 15 500 € par rapport à un éclairage halogène avec 100 changements de lampes
- 6 650 € par rapport à un éclairage HID avec 25 changements de lampes

Ces différents comparatifs démontrent que les solutions d'éclairage à LED sont beaucoup plus économiques et respectueuses de l'environnement.

Technologies appliquées aux éclairages à LED améliorant la capture

Certaines technologies améliorent la qualité d'image en procurant un éclairage adapté. Nous allons nous intéresser tout particulièrement à deux d'entre elles afin de comprendre quels avantages elles apportent aux applications de vidéosurveillance/de vidéo-protection.

- La diffusion 3D : Cette technologie de lentilles micro-réfractives permet de réfracter et de modeler la lumière afin d'étendre la portée et les angles de couverture pour des images de surveillance nocturne avec un éclairage homogène
- L'éclairage constant : Cette technologie d'éclairage permet de compenser les variations de température et la dégradation des LED pour une surveillance nocturne de qualité

La diffusion 3D

L'éclairage traditionnel génère une surexposition de l'avant-plan et une sous-exposition de l'arrière-plan. Ce type d'éclairage peut également provoquer des effets de zones blanches au centre du champ de vision de la caméra.

La technologie de diffusion 3D permet un éclairage réparti sur l'ensemble du champ de visualisation de la caméra. Elle élimine entièrement les zones sous-exposées et surexposées du champ de vision. Elle améliore ainsi le niveau d'éclairage de l'arrière-plan et permet de fournir une image de qualité supérieure.

Figure 21 - Eclairages standards

Figure 22 - Eclairages avec technologie de diffusion 3D

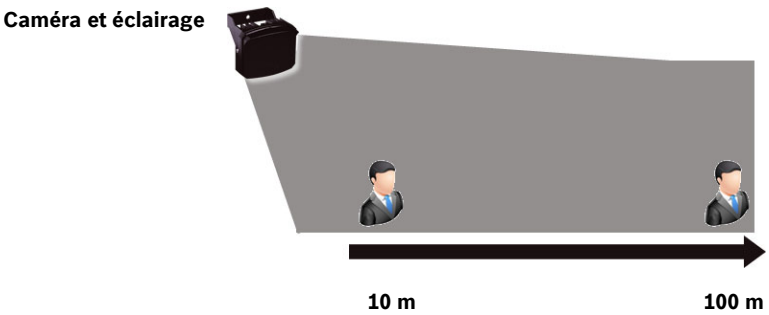


Figure 23 - Principe de la diffusion 3D

L'éclairage constant

Un phénomène bien connu ... Les LED traditionnelles se dégradent avec le temps. Les images produites par un éclairage traditionnel au premier jour ne sont pas les mêmes après 6 mois d'utilisation. La dégradation des LED entraine une faible puissance d'éclairage, réduit la portée et la qualité d'image.

La technologie d'éclairage constant contrôle la sortie et ajuste dynamiquement le courant du panneau de LED pour assurer un niveau constant d'éclairage. Elle permet également d'améliorer la durée de vie du produit. La faible consommation d'énergie, tout le long de la vie du produit, permet de réduire les coûts sur votre facture d'électricité.

Figure 24 - Eclairage standard après six mois

Figure 25 - Eclairage avec la technologie d'éclairage constant après six mois

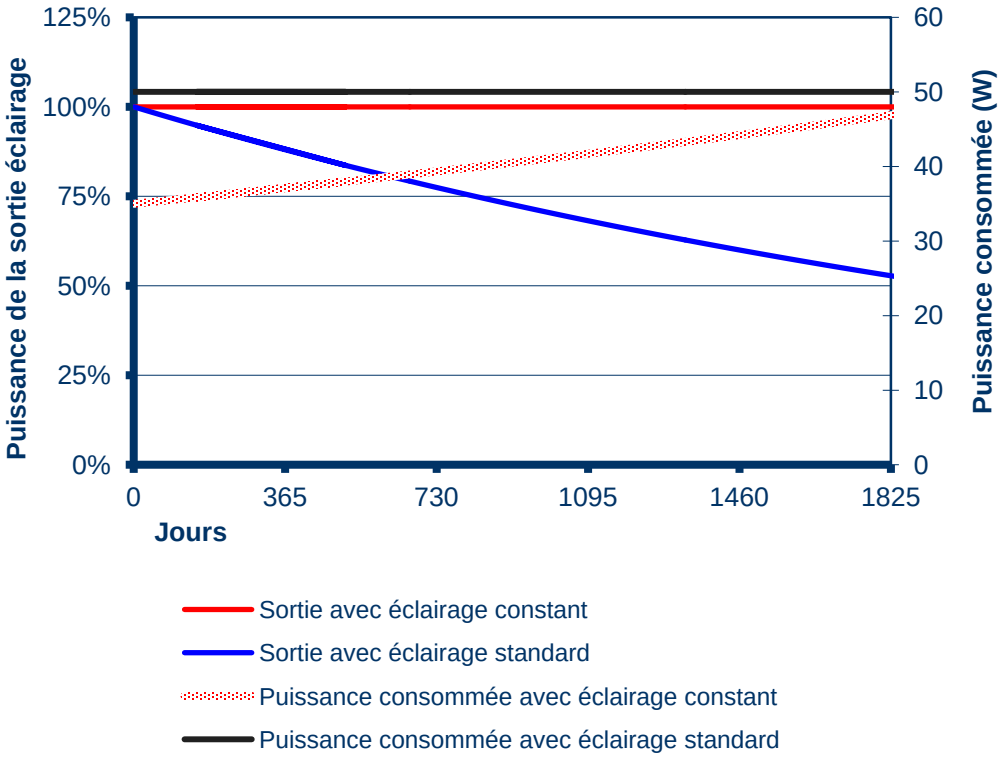


Figure 26 – Comparaison des puissances consommées et des puissances de la sortie éclairage

La puissance nécessaire aux LED pour fournir un niveau constant d'éclairage varie également en fonction de la température. Le graphique suivant montre l'intérêt de réguler la puissance électrique nécessaire pour obtenir un niveau constant d'éclairage.

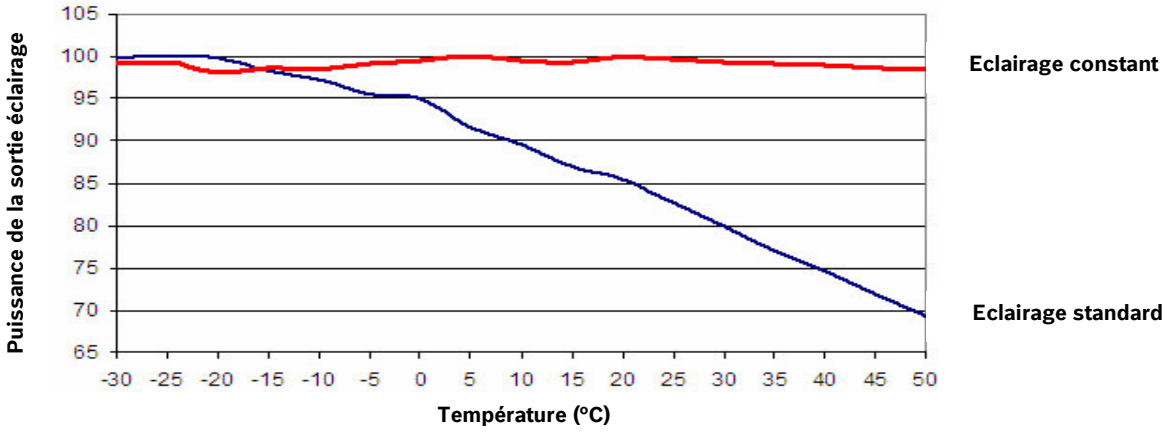


Figure 27 – Variation de la sortie éclairage en fonction de la température

c) Les objets à visualiser - Critères DCRI

Les critères DCRI permettent de définir la pertinence d'un système de vidéosurveillance. Ces critères sont basés sur un standard développé par John Johnson dans ses travaux au sein du laboratoire de vision nocturne de l'armée américaine. Conformément aux travaux de Johnson, il est possible de définir une distance maximale de visualisation pour chaque critère permettant une action spécifique.

Les critères DCRI se décomposent comme suit :

- Détection,
- Classification,
- Reconnaissance,
- Identification

Les définitions des différents critères, données ci-dessous, sont basées sur un test standard réalisé avec une cible de 1.6 m de hauteur.

<table>
<tr>
<td> 
5% – DÉTECTION
Le sujet ne doit pas représenté moins de 5% de la hauteur de l'écran</td>
<td> 
10% – CLASSIFICATION
Le sujet ne doit pas représenté moins de 10% de la hauteur de l'écran</td>
</tr>
<tr>
<td> 
50% – RECONNAISSANCE
Le sujet ne doit pas représenté moins de 50% de la hauteur de l'écran</td>
<td> 
120% – IDENTIFICATION
Le sujet ne doit pas représenté moins de 120% de la hauteur de l'écran</td>
</tr>
</table>

2. L'analyse

L'ajout du numérique dans la vidéosurveillance/vidéo-protection a permis le développement de systèmes intelligents d'analyse. Ces systèmes apportent une aide décisionnelle ou tout simplement alertent directement l'opérateur qui peut ainsi détecter un problème plus rapidement.

Ces technologies permettent une exploitation plus efficace des images en temps réel afin de prévenir un incident ou en temps différé en accélérant les recherches.

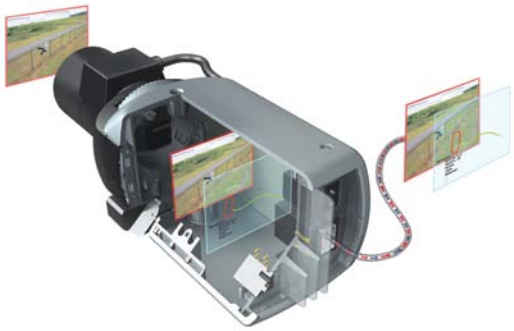


Figure 28 – Exemple d'analyse directement dans la caméra

A ce jour, tout n'est pas envisageable en matière de systèmes intelligents d'analyse. Les applications actuellement considérées comme mature sont les suivantes (liste non exhaustive) :

- La détection d'activité
- La détection d'intrusion
- La lecture automatique de plaques d'immatriculation
- La détection automatique d'incidents sur la voie publique (arrêt sur bande d'urgence, contre sens, ...)
- Vérification de fonctionnement des caméras (perte vidéo, détection d'éblouissement et de masquage, ...)
- Détection de comportements anormaux (flânerie...)
- Suivi automatique d'individu

L'intelligence que l'on peut ainsi donner à un système de vidéosurveillance/de vidéo-protection permettra à terme de réduire les infrastructures notamment en utilisant des caméras intelligentes qui n'émettront des flux vidéo pertinents qu'en cas d'alertes.

Toutefois, les sources de fausses alarmes en analyse du contenu de l'image peuvent être multiples (liste non exhaustive) :

- Mauvaise image,
- Prise de vue non adaptée,
- Réflexion importante/réverbération,
- Mouvement important des arbres,
- Réflexions sur plan d'eau, bitume surchauffé,
- Changement violent de luminosité,
- Effet de chevauchement dans les scènes encombrées.

Il est aussi possible de coupler les capteurs vidéo avec des capteurs sonores, de détection de présence ou d'ouverture de portes pour que les caméras ne soient en fonctionnement que lorsque cela est utile. De plus l'utilisation sur des systèmes conséquents d'outils de vérification de maintenance automatique afin de vérifier que telle ou telle caméra fonctionne toujours et dans les conditions d'origine permet un gain non négligeable en terme de coût de maintenance (sur des systèmes de plusieurs centaines de caméras la maintenance est très complexe et coûteuse) et donc d'efficacité du système.

3. La compression

La compression des images et des données vidéo peut suivre deux approches différentes :

- la compression spatiale
- la compression temporelle

a) La compression spatiale

La norme de compression la plus connue et répandue de ce type est le M-JPEG.

Le JPEG a été normalisé au milieu des années 1980, à l'initiative du Joint Photographic Experts Group. Le JPEG permet d'obtenir le degré de compression souhaité : le taux de compression est paramétrable.

La compression sélectionnée est directement liée à la qualité de l'image voulue. Outre le degré de compression, l'image elle-même influence également le taux de compression obtenu. Par exemple, un mur blanc peut produire un fichier image de taille relativement petit (et un taux de compression élevé), tandis que le même degré de compression appliqué à une scène complexe et chargée produira un fichier de plus grande taille, avec un taux de compression plus faible.

Un système d'acquisition (caméra) saisit des images individuelles, et les compresse au format JPEG. Une caméra peut ainsi capturer et compresser (par exemple 25 fois par seconde) puis les envoyer pour lecture ou enregistrement. Lors de la lecture l'utilisateur percevra une vidéo en mouvement. C'est cette méthode que l'on appelle Motion JPEG ou M-JPEG. Chaque image individuelle étant compressée en JPEG, en fonction du taux de compression sélectionné par le système d'acquisition ou/et l'enregistreur.

Figure 29 – Compression M-JPEG

b) La compression temporelle

La norme MPEG (fondée par le Motion Picture Experts Group à la fin des années 1980) est la plus connue des techniques de transmission directe en vidéo.

Le principe de base du MPEG consiste à comparer entre elles deux images compressées destinées à être transmises sur le réseau. La première des deux images servira de trame de référence. Sur les images suivantes, seules seront envoyées les zones qui diffèrent de la référence. L'encodeur reconstruit alors toutes les images en fonction de l'image de référence.

Bien que plus complexe que la technique Motion JPEG, la compression vidéo MPEG produit de plus petits volumes de données à transmettre sur un réseau.

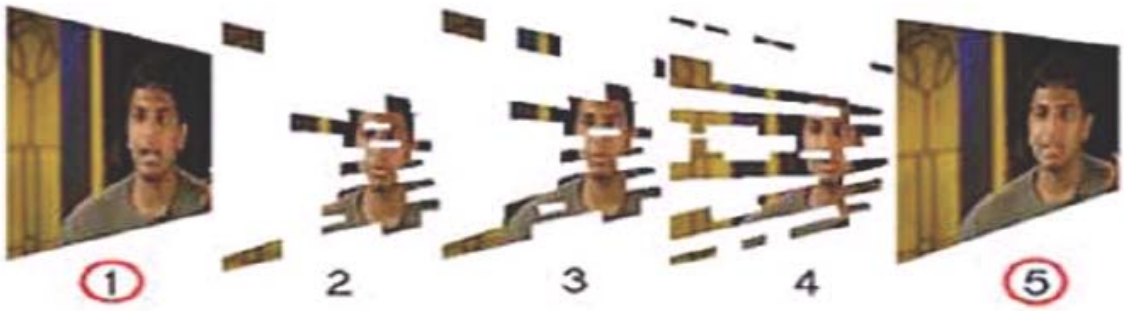


Figure 30 – Compression MPEG

Il est a noté qu'il existe différentes normes MPEG. Nous présentons ci-dessous les plus récentes :

- MPEG-4

Le MPEG-4 représente une évolution substantielle par rapport au format MPEG-2 (format des DVD).

Les possibilités permettant de réduire le débit d'images de manière à atteindre une certaine qualité pour une application ou une scène déterminée sont beaucoup plus nombreuses en MPEG-4. Le débit par caméra varie entre 1 et 5 Mbit/s.

En outre, la fréquence n'est plus limitée à 25 ou 30 images par seconde. Il est notamment très efficace sur des taux de rafraîchissement important (>8IPS) et sur des scènes moyennement et faiblement animées.

Il offre aussi des temps de latence très faible ce qui s'avère très utile lorsque l'on souhaite piloter une caméra mobile à distance.

- H.264

La toute dernière norme de compression vidéo H.264, est appelée à devenir la norme de vidéo de référence. Elle est parfaitement intégrée dans le secteur de la vidéosurveillance. Le H.264 offre de nouvelles possibilités en termes de réduction des frais de transport, de stockage et de renforcement de l'efficacité globale.

Le H.264 est le fruit d'un projet commun entre le groupe d'experts en codage vidéo (VCEG) de l'International Telecommunications Union et le groupe d'expert en images animées (MPEG) de l'ISO/IEC. L'ISO est l'organisation internationale de normalisation et l'IEC est une organisation de surveillance des normes électroniques et électriques. Le H.264 est le nom employé par l'ITU-T, l'ISO/IEC préférant pour sa part opter pour l'appellation MPEG-4 Partie 10/AVC, la norme étant présentée comme un nouvel élément de sa série de normes MPEG-4.

Le H.264 est une norme ouverte sous licence, compatible avec les techniques de compression vidéo les plus efficaces d'aujourd'hui. Un encodeur H.264 peut réduire la taille d'un fichier vidéo numérique de plus de 80% par rapport à la norme M-JPEG et de 50% par rapport à la norme traditionnelle MPEG-4, sans que la qualité d'image ne soit compromise. L'importance de ces gains rend le H.264 très intéressant pour des applications de vidéosurveillance. Le débit par caméra varie entre 1 et 4 Mbit/s.

Le H.264 devrait accélérer l'adoption des caméras mégapixel dans le secteur de la surveillance. Un des inconvénients actuels des caméras mégapixel est la taille importante des fichiers de données vidéo obtenus. Comme indiqué, le H.264 réduit la taille des fichiers, sans compromettre la qualité des images. Il est probable que cette technologie de compression hautement efficace trouve rapidement sa place dans des applications mégapixels où les utilisateurs exigent à la fois une haute résolution et des fréquences d'images élevées, comme pour la vidéo-protection de certains lieux spécifiques.

4. La transmission

a) Le media de transmission

Le transport des informations (images, son ...) est réalisé par la liaison entre la caméra et le local technique (ou point de concentration). Le type de liaison dépendra de la distance entre ces deux points, de la faisabilité technique et des coûts associés. Ils peuvent être résumés en cinq catégories différentes :

- Câble cuivre coaxial,
- Fibre optique,
- Câble cuivre multi-paires,
- Les courants porteurs en ligne (CPL),
- Liaison radio ou sans fil

i. Câble cuivre coaxial,

Pour une distance inférieure à 300 m, des câbles coaxiaux de type KX6 seront utilisés. Pour une distance inférieure à 600 m, des câbles coaxiaux de type KX8 seront utilisés.

Caratéristiques	KX6	KX8
Normes et directives de référence		
Caractéristiques	UTE C93550	
Environnement (directives européennes)	ROHS et CEEE	
Caractéristiques techniques		
Impédance caractéristique	75 Ω	
Diamètre brut (± 5%)	6 mm	10 mm
Bande passante	1,5 Ghz	
Connectique	BNC, RG58	BNC, RG59
Distance d'utilisation	300 m	600 m

Figure 31 - Caractéristiques des câbles coaxiaux

Remarque : Aucune interface spécifique n'est nécessaire dans le cas d'une caméra raccordée en coaxial. Côté points de concentration, ces câbles seront raccordés sur les équipements vidéo (matrice analogique ou encodeur), côté caméra, ils seront raccordés directement.

ii. Fibre optique

Pour une distance maximale de 4 km en analogique de base ou 2 km en numérique, la fibre optique multi-mode est préconisée. Pour une distance plus élevée (typiquement, jusqu'à 10 km), la fibre optique monomode s'impose. Les principales caractéristiques sont les suivantes :

Caratéristiques	Multimode 50/ 125 OM3	Monomode 9/ 125 OSI
Normes de référence		
Caractéristiques	ITU-T G651	ITU-T G652
Caractéristiques géométriques		
Diamètre du cœur (µm)	50 ±3	9,3 ±0,5
Diamètre de la gaine (µm)	125 ±3	125 ±1
Diamètre du revêtement primaire (µm)	250 ±10	245 ±10
Valeur de l'ouverture numérique	0,275 ±0,02	0,12 ±0,01
Excentricité du coeur (%)	< 6	< 6
Excentricité de la gaine (%)	< 2	< 2
Excentricité entre la gaine et le cœur (µm)	< 1.5	< 0,8
Caractéristiques de transmission		
Atténuation linéique assurée (dB/km)		
	< 3.2 à 850 nm	< 0,5 à 1310 nm
	< 1.0 à 1300 nm	< 0,4 à 1550 nm
Bande passante modale (Mhz.km)		
	> 200 à 850 nm	> 2 000 à 1310 nm
	> 500 à 1300 nm	> 5 000 à 1550 nm

Figure 32 - Caractéristiques des fibres optiques

Remarque : Il faut utiliser une interface coaxial/fibre optique dans le cas de matériel analogique et 10BaseTX/100BaseFx (RJ45/Fibre optique) dans le cadre de matériel IP.

iii. Câble cuivre multi-paires

Pour une liaison de moins de 90 m entre le point de concentration et une caméra IP, un câble 4 paires de catégorie 6 sera utilisé. Un câble de ce type peut également être utilisé pour la liaison de télémétrie d'une caméra analogique raccordée avec un câble coaxial vidéo (kx6, kx8).

Remarque : Aucune interface spécifique n'est nécessaire : Côté points de concentration, ces câbles seront raccordés sur des équipements réseaux, coté caméra (IP), ils seront raccordés directement.

iv. Les courants porteurs en ligne (CPL)

La technologie des courants porteurs en ligne (CPL) permet de transférer de l'information numérique sur le réseau électrique basse tension. Une caméra vidéo ayant besoin d'une source d'énergie, il est envisageable d'utiliser le réseau électrique pour transmettre les flux vidéo depuis une caméra sur une distance inférieure au km.

Néanmoins, cette technologie ne permet pas encore de transmettre autant de données qu'avec un réseau Ethernet traditionnel puisqu'elle est limitée actuellement à un débit théorique de 200 Mbit/s, limite repoussée régulièrement avec l'évolution de cette technologie. De plus, le débit réel varie fortement en fonction des perturbations présentes sur le réseau électrique.

v. Radio ou sans fil

Ces types de liaisons sont utilisés lorsque les distances sont relativement importantes et que les coûts en géni civil sont trop élevés.

Les liaisons radio utilisent des bandes de fréquences de 5.4Ghz ou 5.8Ghz.

Bien qu'il soit possible d'utiliser, d'un point de vue technique, des liaisons sans fil dédiées à la transmission de données telles que le WIFI ou le WIMAX, pour les réseaux informatiques ou le DVB-T employé en télévision numérique terrestre, l'utilisation de ces technologies doit faire l'objet d'une étude préalable attentive.

Il s'agit d'un type de liaison qui peut être très facilement intercepté ou brouillé. Il faut donc porter une attention toute particulière à la sécurisation des données (cryptage des données, contrôle d'association basé sur des adresses MAC, adresses IP autorisées, ...) pour être sûr qu'une personne non autorisée ne puisse décoder les images transmises. Les réseaux sans fil présentent actuellement un débit de données limité et se heurtent, parfois, à des difficultés de propagation en milieu urbain. Ainsi un test préalable de transmission est à envisager.

5. La visualisation

La visualisation comprend deux aspects :

- La visualisation via des moniteurs ou mur d'images
- L'interface homme-machine (IHM)

a) La visualisation via des moniteurs ou mur d'images

Il faut distinguer le(s) moniteur(s) associé(s) au poste de contrôle et les moniteurs du mur d'image dont la dimension est fonction de la distance entre l'opérateur et les écrans.

Poste de travail de l'opérateur

Concernant le poste de travail, il est préconisé d'avoir deux écrans par opérateur : Un écran avec la cartographie des différents zones vidéosurveillées et un écran visualisant la caméra souhaitée.

Dans les petites applications, un écran visualisant la caméra souhaitée et un écran présentant une multivision pourront être installés.

Mur d'image

Le mur d'image peut être composé de plusieurs moniteurs affichant chacun une caméra ou de quelques moniteurs affichant une multivision.

b) L'interface homme-machine (IHM)

L'IHM permet certes de visualiser votre système mais aussi de l'exploiter en temps réel.

L'IHM va prendre en compte les contraintes géographique et technique de votre site afin de vous assister dans la gestion de votre site.

Figure 33 - Exemple d'IHM

Lors du choix de l'IHM, les points suivants devront être étudiés :

i. La cartographie

La cartographie peut s'avérer nécessaire pour la gestion de site étendu ou de multi-sites afin de repérer géographiquement l'ensemble des prises de vues du système. Le logiciel proposant cette fonction devra gérer une arborescence de plans utilisant un format couramment utilisé (.dxf, .dwd, ...). Ces plans pourront être enrichis de différents champs (icône, texte, ...) afin d'améliorer la convivialité du système.

ii. Mémorisation de préposition

Lors d'une opération de surveillance, en pilotant sa caméra, l'opérateur peut repérer une zone à surveiller ponctuellement, de manière spécifique (ex : accident ou incident, événement divers). Le système doit donc permettre la mémorisation simple, du cadrage de la scène (position caméra + zoom) concernée.

iii. Automatisation

Afin de faciliter et automatiser des séquences d'exploitation (visualisation et/ou mémorisation), ces dernières seront gérées par le logiciel. Ces scénarii vidéo seront ceux préalablement paramétrés par le responsable d'exploitation. Ceux-ci pourront être déclenchés de la manière suivante :

- Sélection de boutons spécifiques,
- Apparition d'un événement d'alarme,
- Heure de déclenchement planifiée, dans un agenda journalier et hebdomadaire intégrant les jours fériés et des jours ou heures particulières.

Les séquences possibles dans un scénario seront au minimum les suivantes :

- Affichage d'une ou de plusieurs caméra(s) sur un ou plusieurs moniteur(s) ou dans l'IHM,
- Positionnement automatique d'une caméra et de son zoom,
- Durée d'affichage ou de mise en position pour chaque instruction ou événements,
- Mémorisation des images d'une ou plusieurs caméras,
- Choix de la vitesse et la durée de l'enregistrement,
- Affichage d'un plan,
- Affichage de messages consigne,

iv. Exemple de fonctions proposées dans une IHM

L'exemple suivant permet d'appréhender les fonctions incluses dans un logiciel de gestion vidéo (IHM).

Déploiement

- Mises à jour automatiques du logiciel

Configuration

- Détection automatique des périphériques IP
- Affectation automatique de l'adresse IP des périphériques IP

- Mises à jour par lots du firmware des périphériques IP
- Arborescence Logique configurable
- Séquences de caméra prédéfinies
- « Séquences automatiques » créées par sélection multiple et glisser/déposer vers les volets d'images (caméos)
- Minimum de quatre boutons configurables par l'utilisateur

Interface utilisateur

- Plans de site avec liens, périphériques, séquences et scripts de commande
- Les plans de site au format DWF sont utilisés.
- Jusqu'à 4 moniteurs PC pris en charge par station de travail
- Prise en charge de clavier (pupitre de télécommande) connecté à une station de travail ou à un décodeur IP
- Volets flexibles d'images (caméos) permettant de faire varier la taille et la disposition des fenêtres vidéo
- Volets d'images (caméos) de visualisation en temps réel pouvant tous passer en mode de lecture instantanée
- Affichage de plusieurs volets d'images (caméos) en mode lecture instantanée
- Fenêtres de visualisation pouvant afficher des vidéos en temps réel, des vidéos en mode de lecture instantanée, des documents texte, des cartes ou des pages Web
- Icônes fournissant des informations sur l'état des périphériques, y compris les pertes de connexion réseau, les pertes vidéo et le déréglage de la caméra
- Configuration individuelle, utilisateur par utilisateur, de l'arborescence des favoris
- Possibilité d'inclure, dans l'arborescence des favoris, des vues complètes avec les mises en page des volets d'images (caméos) et les affectations des caméras
- Sélection de caméra par double-clic ou à l'aide de la fonction glisser/déposer depuis les plans de site, l'arborescence logique ou l'arborescence des favoris
- Organisation des décodeurs en murs de moniteurs analogiques
- Contrôle des moniteurs analogiques connectés aux décodeurs à l'aide de la fonction glisser/déposer
- Lecture synchronisée de caméras
- Barre chronologique sophistiquée avec prise en charge de plusieurs caméras permettant une recherche graphique simple dans les vidéos stockées
- Couleurs de la barre chronologique indiquant l'état des enregistrements : enregistrement normal, enregistrement sur alarme, enregistrement protégé, enregistrement audio
- Sélection facile des clips en faisant glisser le repère sur la barre chronologique
- Possibilité d'exporter les clips sélectionnés vers des DVD, des lecteurs réseau ou des clés USB en seulement quelques clics de souris
- Recherche flexible sur tous les NVR et les enregistreurs numériques (DVR) connectés au système
- Recherche de mouvements après enregistrement permettant de repérer aisément les modifications apportées aux zones sélectionnées de l'image
- Fonction de recherche contextuelle (Forensic Search) permettant d'utiliser des algorithmes d'analyse intelligente de la vidéo (IVA, Intelligent Video Analysis) sur la vidéo enregistrée

- Deux options d'écoute audio : uniquement un canal sélectionné ou plusieurs canaux simultanément
- Fonction intercom audio

Planification

- Jusqu'à 10 profils d'enregistrements avec vacances et jours d'exception
- Planifications de tâches avec prise en charge des vacances, des jours d'exception et des planifications de tâches récurrentes
- Paramétrage des temps d'enregistrement maximum et minimum par caméra
- Cadence d'images par caméra et par enregistrement, paramètres de qualité pour les enregistrements en temps réel, normaux, sur activité et sur alarmes

Traitement des événements

- Liste d'événements avec les événements concernant les périphériques (par exemple, les pertes de signal vidéo), les événements système (par exemple, disque saturé), les traps SNMP à partir de périphériques réseau (par exemple, trafic réseau trop important), les événements sous-système, les événements utilisateur (par exemple, échec de la connexion), les événements de planification (par exemple, tous les mardis à 10h15), etc.
- Événements combinés (combinaison des événements avec les opérateurs logiques booléens)
- Duplication d'événements permettant une gestion séparée
- Affectation d'événements à des groupes d'utilisateurs
- Génération d'alarmes selon les planifications
- Journalisation des événements selon les planifications
- Invocation de scripts de commande générés par événement selon les planifications

Gestion d'alarme

- Alarmes permettant de déclencher des enregistrements en mode alarme pour toutes les caméras
- 100 niveaux de priorité d'alarme
- Apparition automatique de fenêtre vidéo en cas d'alarme
- Alarmes affichées dans des fenêtres d'alarmes distinctes
- Jusqu'à 5 volets d'images (caméos) par alarme, avec affichage des vidéos en temps réel ou enregistrées, cartes de site, documents ou pages Web, disposés en colonne, les alarmes prioritaires s'affichant sur la ligne du haut
- Fichier audio par alarme
- Flux de travail avec instructions d'utilisation et commentaires utilisateur, avec l'option « Forcer le flux de travail » avant effacement de l'alarme
- Notification par e-mail ou SMS en cas d'alarme
- Affichage des alarmes sur les murs de moniteurs analogiques
- Options d'effacement automatique des alarmes basées sur le temps ou sur l'état

Gestion des utilisateurs

- Compatible LDAP pour intégration aux systèmes de gestion des utilisateurs des entreprises tels que Microsoft Active Directory
- Accès aux ressources système contrôlé individuellement par groupe d'utilisateurs
- Arborescence Logique personnalisable par groupe d'utilisateurs (seuls les périphériques auxquels les utilisateurs ont accès s'affichent)
- Droits de protection, de suppression, d'exportation et d'impression des enregistrements vidéo par groupe d'utilisateurs

- Droits d'accès au Journal des Connexions par groupe d'utilisateurs
- Affectation de niveaux de priorité par groupe d'utilisateurs pour l'accès aux commandes des caméras mobiles
- Droits d'accès individuels par caméra attribuables par groupe d'utilisateurs pour l'accès au temps réel, à la lecture instantanée, à l'audio, à l'affichage des métadonnées et à la commande de caméras mobiles
- Connexion avec double autorisation permettant l'activation de droits spéciaux et de priorités lorsque deux utilisateurs se connectent simultanément

Surveillance du système

- Surveillance de l'état d'un système, y compris les caméras, les ordinateurs, les logiciels et l'équipement réseau
- Équipement réseau et autres périphériques tiers contrôlés par SNMP

Personnalisation et interface

- Scripts de commande personnalisés permettant de contrôler l'ensemble des fonctions système
- Éditeur de Script de commande intégré prenant en charge les environnements C# et Visual Basic .Net
- Logiciel externe pouvant déclencher des événements et envoyer des métadonnées par les « Entrées virtuelles »
- Possibilité d'utiliser tous les langages de programmation de type .Net (C#, JScript, etc.) ou COM (C++, Visual Basic, etc.) pour déclencher des entrées virtuelles

6. Le stockage

La fonction enregistrement a en charge le stockage des images fournis par les caméras. Il doit également permettre une recherche multicritères sur les données enregistrées (date, heure, identification caméra, événement déclenchant, zone géographique, ...). L'enregistreur doit pouvoir être piloté depuis une IHM.

Les capacités de stockage des enregistreurs dépendent :

- Du nombre de caméras à enregistrer,
- Du nombre de jours d'enregistrement,
- Du temps d'enregistrement par jour (heure),
- Du nombre d'images par seconde,
- De la qualité de l'image,

a) Type d'enregistreur

Il existe 3 sortes d'enregistreurs :

- Les enregistreurs numériques – DVR

  Les DVR (Digital Video Recorder) sont des équipements permettant de numériser et de stocker les vidéos. Les caméras analogiques sont donc raccordées directement sur l'équipement. Il est à noter qu'il existe des enregistreurs numériques hybrides permettant d'enregistrer à la fois des caméras analogiques et des caméras IP.

Figure 34 - Enregistreur numérique

- Les enregistreurs numériques réseaux – NVR

  Les NVR (Network Video Recorder) sont des équipements dont le rôle est d'enregistrer les images provenant du réseau. Ce matériel est donc adapté aux systèmes utilisant des caméras IP ou des caméras analogiques avec encodeurs. Il s'agit généralement d'un serveur équipé d'une grande capacité de stockage. Ce type de matériel est adapté aux systèmes de grandes envergures du fait de sa grande capacité d'extension.

- Les enregistreurs numériques virtualisés – VRM

  Le Video Recording Manager (VRM) est une solution de gestion des enregistrements vidéo via le réseau. Il gère de manière centralisée les enregistrements sur des périphériques iSCSI provenant de caméras et d'encodeurs IP. Le VRM constitue la technologie de deuxième génération d'enregistreurs vidéo via le réseau, qui remplace les serveurs NVR (Network Video Recorders ou enregistreurs réseau) de première génération. Le VRM rend inutile la multiplication des serveurs NVR, de leurs systèmes d'exploitation, des logiciels NVR et antivirus, facilitant ainsi les tâches de maintenance de l'équipe informatique. Les systèmes utilisant les enregistrements sur des périphériques iSCSI avec le VRM présentent un retour sur investissement particulièrement intéressant, en réduisant les frais de maintenance et d'exploitation.

  Le VRM regroupe tous les unités iSCSI disponibles et alloue automatiquement les espaces de stockage à la demande des périphériques IP, facilitant ainsi la configuration de l'espace de stockage par l'installateur. Pour agrandir l'espace de stockage, il suffit d'ajouter une nouvelle unité iSCSI sur le réseau. Le logiciel VRM joue le rôle d'un « chef d'orchestre » qui répartit les vidéos sur les différents périphériques de stockage. Il offre ainsi une grande fiabilité en terme, de redondance en cas de défaillance et de meilleures performances, grâce à l'équilibrage des charges.

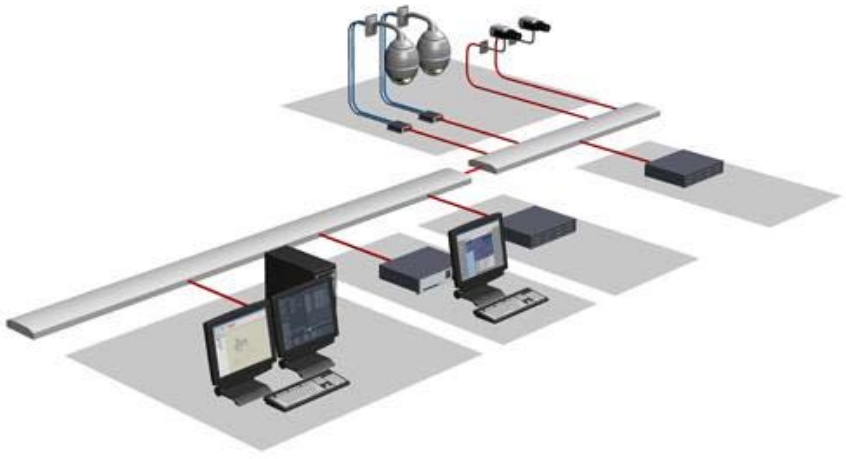


Figure 35 - Exemple d'application avec enregistrement virtualisé

b) La sécurisation des enregistrements

La sécurisation des données peut être réalisée à plusieurs niveaux :

i. Alimentation de l'enregistreur

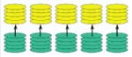
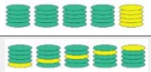
Les alimentations des enregistreurs doivent être fiable et voir redondantes dans certaine applications critiques (utilisation de serveur ou unité iSCSI avec des Téraoctets de données…).

Les alimentations doivent être conformes à la norme « EN50130-5 :1999 Alarm systems part 5, Class I fixed equipment » de « l'Internationnal Alarm Standard » afin de garantir l'intégrité des enregistrements en cas de coupure secteur de moins de 100 ms.

ii. Système RAID

Le terme RAID (Redundant Array of Independent Disks) désigne les techniques permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit la tolérance aux pannes, soit la sécurité, soit les performances de l'ensemble, ou une répartition de tout cela.

Il existe différents types de RAID. Le tableau ci-dessous résume les caractéristiques des principaux types de RAID utilisés en vidéosurveillance, le RAID 4 et le RAID 5 étant les plus utilisés.

RAID	Impact sur la capacité	Protection des données	Performance		Description
			Écriture	Lecture	
RAID 0	Aucun	Aucune	Très bonne	Très bonne	
RAID 1	50 %	Bonne	Moyenne	Moyenne	
RAID 4	n-1	Bonne	Très bonne*	Très bonne	
RAID 5	n-1	Bonne	Bonne	Très bonne	
RAID DP	n-2	Très bonne	Très bonne	Très bonne	

*Via des technologies logicielles

Tableau 10 – Différents types de RAID

Il est à noter que si on est en RAID4, il n'y aura pas de perte de donnée si 1 disque dur est en panne et en RAID DP, il n'y aura pas de perte de donnée si 2 disques durs sont en panne. Le RAID DP présente donc le plus de sécurisation pour les enregistrements mais il présente un coût d'achat plus important.

Un des avantages principaux des systèmes RAID reste la possibilité de remplacer les disques à chaud c'est-à-dire sans couper l'alimentation du système d'enregistrement et donc sans perturber l'enregistrement.

Attention, Le RAID apporte un sentiment de sécurité mais il a des Limites. Le RAID ne dispense pas d'effectuer des sauvegardes régulières. En effet, des défaillances à plusieurs disques sont plus fréquentes que l'on ne le croit. De plus, des erreurs humaines (effacement/corruption de fichiers) finissent toujours par se produire.

- Ce que peut faire le RAID
  - réduire les risques de pertes de données en cas de défaillance d'une unité de stockage
  - améliorer les performances
- Ce que ne peut pas faire le RAID
  - Protéger totalement des défaillances matérielles (éventualité de pannes successives de plusieurs disques ou du système RAID lui-même).
  - Protéger les données des erreurs humaines (suppression accidentelle de fichiers).

- Protéger l'utilisateur des risques extérieurs au système (surcharge électrique qui grillerait l'ensemble des disques, incendie, vol, inondation, vandalisme).
- Protéger les données des virus et des spywares qui pourraient corrompre les données.

o Comment le RAID peut vous trahir

Le RAID a tendance à rendre les utilisateurs trop confiants. Cet excès de confiance en une technologie très robuste et très fiable en apparence a entraîné de nombreux désastres. Multiplier le nombre de disques multiplie les risques de panne. De plus, les disques utilisés par une grappe RAID sont souvent de même type et de même âge. Ils auront donc une durée de vie similaire. La complexité du système RAID ajoute des risques technologiques (bug du contrôleur RAID ou du logiciel). Un disque défectueux peut aussi perturber le fonctionnement du contrôleur, logiquement ou électriquement ; ce qui causera la perte de plusieurs unités ; ce qui, enfin, dans le cas d'une grappe RAID 5, causera la perte totale de la grappe.

Le RAID n'apporte aucune protection contre les défaillances du système d'exploitation (intrinsèques ou dues à un problème de configuration ou d'un conflit de composants), d'une destruction de données par dysfonctionnement d'un logiciel, virus ou malveillance. En outre, les systèmes RAID sont vulnérables à tous les risques physiques classiques (feu, inondation, vol, foudre et surtensions externes, surtensions internes à la machine, etc.), excepté pour les très onéreux miroirs distants (remote mirroring).

Ne faites donc jamais totalement confiance à un système de stockage de données quel qu'il soit. Effectuez toujours des sauvegardes régulières et rappelez-vous que la seule façon sûre de préserver votre banque de données du vol ou de l'incendie, c'est d'en stocker une copie dans un autre endroit sécurisé.

7. La recherche / L’exportation

Tout système de vidéosurveillance/vidéo-protection qui enregistre des images possède un système de recherche et d'exportation. Généralement, ce système est basé sur une recherche chronologique. Cette méthode prend du temps car elle nécessite la visualisation de l'ensemble des enregistrements vidéo.

Pour optimiser la recherche, certain logiciel propose une recherche basée sur la détection de mouvement à postériori ou une recherche contextuelle basée sur les métadonnées d'analyse de la vidéo. La recherche basée sur la détection de mouvement permet de diminuer le temps de recherche mais reste limitée au mouvement dans l'image. La recherche contextuelle est bien plus précise car elle permet de rechercher les objets de type véhicule et de couleur rouge garés devant la capitainerie ou le véhicule qui va à contre-sens par exemple.

L'exportation des séquences vidéo s'effectue sur un DVD. Les séquences vidéo sont en format natif du fabricant pour pouvoir authentifier ces dernières à l'aide d'un logiciel. Ainsi, les séquences vidéo ne peuvent être modifiées.

8. L’intégration et l'ouverture d'un système de Vidéosurveillance

a) Intégration

Un système de vidéosurveillance peut être intégré dans un système plus complexe. Pour réaliser ce genre d'infrastructure, il est nécessaire de développer une passerelle entre les différents systèmes autour d'un kit de développement logiciel généralement fourni par les fabricants. Ces kits de développement sont appelés SDK.

Par exemple, on pourra développer un lien entre un système de vidéosurveillance et un système de contrôle d'accès.

b) Ouverture du système

Un système de Vidéosurveillance peut être ouvert à des produits de différentes marques. Généralement, il s'agit de systèmes compatibles entre eux via une norme ou un protocole. En matière de vidéosurveillance analogique, le standard PAL assure cette compatibilité entre les caméras de différentes marques et les

enregistreurs. En matière de vidéosurveillance IP, les spécifications fournies par l'organisation ONVIF permettent une intégration plus aisée.

http://www.onvif.org/

C. Spécificités des secteurs maritimes et portuaires

1. La résistance environnementale

a) Les indices de protection IP et IK

L'indice de protection IP détermine le degré de protection du matériel contre la pénétration des corps solides (1er chiffre, de 0 à 6) et des liquides (2ème chiffre, de 0 à 8).
Il peut également être complété par une Lettre additionnelle (option) qui détermine la protection des personnes contre les accès aux parties dangereuses (A, B, C, D) et une Lettre supplémentaire (option) qui fournit une information spécifique (H, M, S, W).
Exemple : IP45CH

Remarque : S'il n'est pas exigé de spécifier un chiffre caractéristique, celui-ci doit être remplacé par la lettre « X » (ou « XX » si les deux chiffres sont omis). Les lettres additionnelles et ou les lettres supplémentaires peuvent être omises sans remplacement.

PREMIER CHIFFRE PROTECTION CONTRE LES OBJETS SOLIDES			SECOND CHIFFRE PROTECTION CONTRE LES LIQUIDES		
IP		TEST	IP		TEST
0		Pas de protection	0		Pas de protection
1		Protection contre les objets solides de plus de 50 mm, par ex. contact accidentel des mains.	1		Protection contre les gouttes d'eau tombant à la verticale.
2		Protection contre les objets solides de plus de 12 mm, par ex.doigts.	2		Protection contre les projections directes d'eau jusqu'à 15° de la verticale.
3		Protection contre les objets solides de plus de 2,5 mm (outils + petits fils).	3		Protection contre les projections d'eau jusqu'à 60° de la verticale.
4		Protection contre les objets solides de plus de 1 mm (outils, petits fils).	4		Protection contre les projections d'eau dans toutes les directions-admission limitée permise.

5		Protection contre la poussière-admission limitée permise (pas de dépôts nocifs).	**5**		Protection contre les jets d'eau de faible pression de toutes les directions-admission limitée permise.
6		Protection totale contre la poussière.	**6**		Protection contre les jets d'eau forts, par ex. utilisation sur les ponts de navires-admission limitée permise.
			7		Protection contre les effets de l'immersion entre 15 cm et 1 m.
			8		Protection contre les longues périodes d'immersion sous pression.

Tableau 11 –Tableau des indices IP

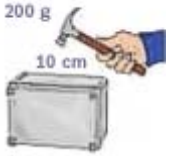
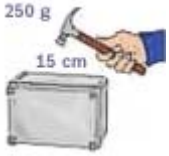
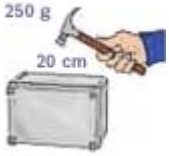
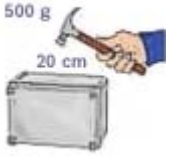
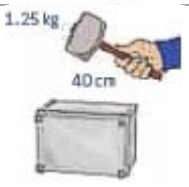
Lettre additionnelle	
A	Protégé contre l'accès du dos de la main
B	Protégé contre l'accès du doigt
C	Protégé contre l'accès d'un outil – Ø 2.5 mm
D	Protégé contre l'accès d'un outil – Ø 1 mm

Tableau 12 – Correspondance lettre additionnelle

Lettre supplémentaire	
H	Matériel à haute tension
M	Mouvement pendant l'essai à l'eau
S	Stationnaire pendant l'essai à l'eau
W	Intempéries

Tableau 13 – Correspondance lettre supplémentaire

L'indice IK fournit le degré de protection du matériel contre les chocs d'origine mécanique.

CODE IK PROTECTION CONTRE LES CHOCS MECANIQUES		
IK		**TEST**
00		Pas de protection
01		choc de 0.15 joules
02		choc de 0.20 joules
03		choc de 0.37 joule
04		choc de 0.50 joule
05		choc de 0.70 joule
06		choc de 1 joule
07		choc de 2 joules
08		choc de 5 joules

09		choc de 10 joules
10		choc de 20 joules

Tableau 14 – Tableau des indices IK

b) La résistance à la corrosion

Les phénomènes de corrosion des métaux sont surtout de nature électrochimique. En présence d'une solution de type électrolyte, le potentiel métal-solution varie selon les points de la surface et de ce fait, des courants électriques apparaissent et provoquent l'endommagement du métal.

La résistance à la corrosion dépend de la valeur de ces potentiels et surtout de leur répartition sur les surfaces. Toutes les hétérogénéités donnent naissance à des couples électriques, à commencer par celles qui résultent des différences de structure et de composition des microcristaux qui constituent le matériau lui-même. D'autres hétérogénéités sont dues à la présence de soudures, de rivets, de façonnages locaux entraînant un écrouissage (dans les tôles pliées par exemple), mais aussi au frottement contre des pièces antagonistes ou même à de simples rayures.

À chaud, la diffusion des agents corrosifs dans l'épaisseur du métal peut compliquer encore le problème.

La lutte contre la corrosion est une préoccupation constante dans beaucoup de domaines industriels et maritimes. Une solution relativement simple consiste à recouvrir la surface à protéger par un matériau insensible au milieu agressif, matériau qui peut être métallique ou non. Les peintures, les vernis, certains traitements de surface, les revêtements métalliques de plomb, de zinc, de nickel, de chrome, etc. peuvent être souvent utilisés avec succès. Il est possible également de remplacer les métaux par d'autres matériaux de plus grande inertie chimique comme le graphite, la céramique, le verre, les matières plastiques, etc.

Pour la vidéosurveillance/vidéo-protection, trois protections peuvent être utilisées :

- Utilisation de plastiques résistant au sel marin tels que le plastique ABS par exemple. Le principal défaut de ces matériaux est leur résistance aux chocs.

- Utilisation de revêtement anticorrosion tel que l'Alochrom 1200. L'Alochrom 1200 est un revêtement d'aluminium de conversion au chromate, utilisé dans les secteurs de l'aérospatiale et de la défense lorsqu'une couche de protection est nécessaire pour améliorer la résistance à la corrosion.

- Utilisation d'INOX marin avec un traitement appelé l'électro-polissage. L'INOX marin appelé 316L ou A4 est en réalité un Z3 CND 17-11 (un chrome16% à18% / nickel 11 à 13% / molybdène 2%). Le reste étant constitué de fer et de carbone (définition de l'acier...). La résistance à la corrosion de l'acier inoxydable est due à la couche d'oxyde "passive", riche en chrome qui se forme naturellement à la surface de l'acier. Toutefois, afin de renforcer cette protection qui peut être altérée en milieu marin, il est nécessaire de réaliser un traitement de protection appelé l'électro-polissage.

L'électro-polissage apporte :

- La suppression des micro-fissures de surface
- La disparition des angles vifs
- Une surface de qualité "poli brillant"
- Une passivation complète
- L'enlèvement des oxydes et ternissures
- Une mise en conformité qui répond aux exigences d'hygiène des industries chimiques, pharmaceutiques, alimentaires et nucléaires
- Facilite la décontamination des pièces exposées à la radioactivité.

2. Les spécificités produits

a) L'essuie-glace

Lorsque les caméras sont placées en bord de mer et soumis aux embruns, la visualisation de certaines scènes peut s'avérer difficile voire impossible après quelques semaines d'utilisation. La cause est le dépôt de sel et autres particules sur les bulles des caméras mobiles ou les vitres des caissons pour caméras fixes.

Il est fortement recommandé dans ce cas là d'utiliser des essuie-glaces pour les caméras les plus exposées.

Figure 36 - Exemples de caméras mobiles avec un essuie-glace

IV Financement

Ce document n'a pas pour objet de présenter les modes classiques de financement utilisés pour l'acquisition de matériel ou de construction d'une infrastructure de réseaux (emprunt, crédit-bail, location financière).

Il s'agit de recenser les pratiques permettant un transfert ou un partage des coûts supportés par des personnes publiques ou des personnes privées lors de la création, la rénovation et l'exploitation d'un réseau de vidéosurveillance/de vidéo-protection.

Plusieurs départements et régions ont mis en place un dispositif de financement de la vidéosurveillance/de la vidéo-protection. Pour pouvoir en bénéficier, les maîtres d'ouvrages peuvent se renseigner auprès de ces collectivités. Le développement qui suit ne concerne que le financement par l'état.

A. Aide publique spécifique par l'état

1. Le fond interministériel de prévention de la délinquance

La loi du 5 mars 2007 dans son article 5 crée, au sein de l'agence nationale pour la cohésion sociale et l'égalité des chances (l'Ascé), un fond interministériel de prévention de la délinquance (FIPD).

Le FIPD est destiné à financer la réalisation d'actions de prévention de la délinquance mises en œuvre dans un cadre partenarial (CLS, plan d'action d'un CLSPD, CUCS, plan départemental de prévention de délinquance). Ces actions ne doivent pas être incompatibles avec le plan de prévention de la délinquance arrêté par le représentant de l'état, leurs groupements, les associations et les organismes publics ou privés. Le FIPD peut également financer des actions de prévention conduites par les services de l'état (études, actions de communication, formation…) à la condition que celui-ci n'intervienne pas en substitution des crédits de droit commun de chaque ministère s'agissant en particulier du fonctionnement de leurs services.

Le comité interministériel de prévention de la délinquance (CIPD) fixe les orientations et coordonne l'utilisation des crédits de ce fond. En application de ces orientations, le conseil d'administration de l'Ascé, quant à lui, approuve les programmes d'intervention correspondants et répartit les crédits ente les départements. L'Ascé est chargée du suivi et de l'évaluation de l'utilisation de ces crédits. Le préfet de département est le délégué territorial et l'ordonnateur secondaire de l'agence et chargé à ce titre d'organiser les appels à projets.

En référence au plan national de développement de la vidéosurveillance/la vidéo-protection sur la voie publique, le FIPD a été mobilisé dès 2007 pour financer 309 projets de vidéosurveillance/de vidéo-protection pour un montant de 13.4 millions d'euros. En 2008, 304 projets ont été financés pour un montant de 10.3 millions d'euros, ce qui représente environ 27% des crédits engagés sur le FIPD.

Ce fond est constitué d'un montant prélevé sur le produit des amendes forfaitaires de la police de la circulation ainsi que d'éventuels reliquats de crédits des années précédentes.

- Les projets de vidéosurveillance/de vidéo-protection sur la voie publique, au profit des actions conduites principalement par des collectivités locales, sont éligibles au FIPD à la triple condition suivante :
- Réalisation d'une étude préalable, associant obligatoirement la direction départementale de la sécurité publique ou le groupement de gendarmerie ainsi que le SZSIC territorialement compétents ;
- Qualité technique de l'installation permettant un raccordement du centre de supervision urbain (CSU-CSV) aux services de sécurité publique dans les conditions de fonctionnement opérationnelles et conformes aux dispositions de l'arrêté du 3 Août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

Comme pour les études préalables faisant appel à un prestataire extérieur, la participation de l'état via le FIPD aux frais d'installation ou d'extension des systèmes de vidéoprotection ne pourra excéder un taux de 50%. Les dépenses de fonctionnement et de maintenance restent à la charge du propriétaire du dispositif.

Pour leur part, les projets de raccordement des centres de supervision urbaine (CSU-CSV) des communes aux services de police ou de gendarmerie (dépôts d'images) peuvent être financés à hauteur de 100% sur les crédits déconcentrés du FIPD. Ces dépenses incluent les travaux liés au raccordement, l'acquisition du matériel informatique nécessaire au déport d'images ainsi que la location de la ligne assurant la liaison, celle-ci étant financé la première année par le FIPD, puis par les services de police ou de la gendarmerie compétents au cours des années suivantes.

En tout état de cause, il appartient aux préfets de département de valider les projets qui pourront bénéficier d'un soutien du FIPD, compte tenu des orientations fixées par le CIPD et déclinées dans le plan départemental de prévention de la délinquance.

B. Financement privé des systèmes publics

1. La délégation de service public

La délégation de service public, et plus particulièrement la concession, permet à une personne publique de confier à une autre personne publique ou privée, la construction d'installations destinées à un service public dont cette dernière assure l'exploitation contre la rémunération substantiellement liée aux résultats de l'exploitation du service.

En matière d'exercice de pouvoirs de police, notamment sur la voie publique, la jurisprudence du Conseil d'Etat a fixé un principe d'interdiction des délégations.

Ainsi, à chaque fois que la vidéosurveillance/la vidéo-protection est mise en œuvre pour une activité de police sur la voie publique, elle doit être gérée directement par l'autorité compétente qui peut seule obtenir l'autorisation préfectorale requise par l'article 10 de la loi du 21 janvier 1995.

De plus, les entreprises privées habilitées par arrêté préfectorale à exercer des prestations de vidéosurveillance/de vidéo-protection ne peuvent remplir leur mission exclusivement dans un but de sécurité ou de gardiennage de biens meubles ou immeubles ainsi que pour la sécurité des personnes se trouvant dans ces immeubles.

Les personnes publiques ne peuvent donc recourir à une réalisation et l'exploitation de leur système par la voie d'une délégation de service public qu'à la double condition que le système :

- N'est pas institué pour l'exercice de pouvoir de police,
- Ne sert qu'à la sécurité ou au gardiennage de biens meubles ou immeubles ainsi que pour la sécurité des personnes se trouvant dans ces immeubles.

2. L'offre de concours

L'offre de concours est un contrat en vertu duquel une personne qui a intérêt à la réalisation de certains travaux publics met, à la disposition de la personne publique, des moyens (financiers, immobiliers) facilitant, voire permettant, la réalisation des travaux.

Ce contrat peut être conclu lorsque, par exemple, pour des zones excentrées, il est sollicité des citoyens ou des entreprises l'établissement d'installation pour la vidéosurveillance/la vidéo-protection sur les voies publiques ou des lieux ouverts au public.

L'offre de concours est un acte volontaire de la part de la personne participant à la réalisation du système. Il ne s'agit ni d'une taxe, ni d'une rémunération pour service rendu. Elle ne peut être conclue que pour les frais d'investissement.

Au risque d'être qualifié de participation indue, l'offre de concours ne peut être obtenue dans le cadre de l'instruction d'une autorisation d'urbanisme de la part d'un pétitionnaire.

3. Contrat de partenariat (Partenariat Public Privé)

Le contrat de partenariat est un contrat par lequel une personne publique confie à un tiers, pour une période déterminée en fonction de la durée d'amortissement des investissements ou des modalités de financement retenues, une mission globale relative au financement d'investissements immatériels, d'ouvrages ou d'équipements nécessaires au service public, à la construction ou transformation des ouvrages ou équipements, ainsi qu'à leur entretien, leur maintenance, leur exploitation ou leur gestion, et, le cas échéant, à d'autres prestations de service concourant à l'exercice, par la personne publique, de la mission de service public dont elle est chargée.

L'équipement ainsi créé et entretenu est la propriété du partenaire privé qui le loue à la personne publique qui exerce directement sa mission de service public ou d'intérêt général. En fin de contrat, il peut être contractuellement prévu un droit d'acquisition de tout ou partie de l'équipement.

Le contrat de partenariat prévoit une analyse de la performance de la prestation fournie par le contractant de l'administration et permet de moduler l'étendue de sa rémunération ou d'adapter l'équipement au besoin.

Le recours au contrat de partenariat est limité au cas soit d'urgence soit de complexité du projet. Dans les deux cas, il convient que le contrat de partenariat présente un avantage économique pour la personne publique par rapport aux autres formes de contrats possibles de réalisation et de financement.

C. La mutualisation

1. Mutualisation de tout ou partie des systèmes

Pour les personnes privées, la possibilité de mutualisation des moyens de protection a été consacrée par le décret n° 97-46 relatif aux obligations de surveillance ou de gardiennage incombant à certains propriétaires, exploitants ou affectataires de locaux professionnels ou commerciaux. Les systèmes de vidéosurveillance/ de vidéo-protection font partie de ces moyens et la mutualisation de réseau, de centre de supervision et des personnels est souvent pratiquée dans les ensembles commerciaux.

Pour les collectivités territoriales, outre le recours aux établissements publics de coopération intercommunale dans les conditions de l'article L.5211-60 du code général des collectivités territoriales, la mutualisation de moyens et de personnels peut être opérée dans le cadre de convention ou d'entente.

2. Mutualisation des usages

Une installation de vidéosurveillance/ de vidéo-protection repose nécessairement sur un réseau de collecte et de transmission. Ce réseau privé peut être construit à partir d'infrastructures telles que fourreaux ou fibres d'un réseau existant de communications électroniques.

Dans les zones d'activité, les infrastructures établies pour l'accueil des réseaux d'opérateur de téléphonie peuvent être mises à la disposition des structures crées entre les propriétaires ou exploitant des sites privés ou sur les voieries tertiaires gérées par des personnes privées.

Pour les collectivités locales qui mettent en place un des réseaux d'initiative publique une réflexion sur un tracé adapté aux besoins en matière de vidéosurveillance/ de vidéo-protection peut précéder le déploiement.

Il est à noter que si les installations de vidéosurveillance/ de vidéo-protection ne sont pas éligibles au bénéfice de subventions européennes, en revanche l'établissement de réseaux de communications électroniques d'initiative publique peut bénéficier de fonds structurels européens et également d'éventuelles aides spécifiques votées au niveau régional et départemental.

V Etude de cas

A. Port de Beaulieu

1. Introduction

Le port de Beaulieu propose environ 750 places et est entouré par une galerie commerciale.

Le système de vidéosurveillance, installé en 2009, comprend 9 caméras dont 7 caméras mobiles, un enregistreur numérique et 2 claviers de télécommande.

2. But

Le but de ce système est double. En effet, il constitue à la fois un outil de sécurité et un outil de gestion. Il permet de visualiser les mouvements dans la passe, de contrôler et de surveiller l'ensemble des activités du port. Il apporte également une aide aux équipes du port dans leur gestion quotidienne.

3. Installation

Ce système de vidéosurveillance a été mis en place suite à un appel d'offres privé (3 à 4 devis). Le critère du choix de l'installateur a été basé sur l'offre offrant le plus de garantie et de maintenance. Dans le cas du port de Beaulieu, ce sont les installateurs qui ont proposé leur solution de vidéosurveillance. La partie documentations administratives liée à la réglementation en vigueur (document à remettre à la préfecture) a été pris en charge par l'installateur. Après l'installation, une formation d'aide à la prise en main d'environ 2h a été réalisée.

4. Contrat maintenance

Le port de Beaulieu a souhaité souscrire un contrat de maintenance. Ce contrat prévoit une visite trimestrielle pour le nettoyage des caméras et le cas échéant une maintenance corrective.

5. Utilisation du système

Le port a mis en place une procédure d'utilisation de ce système de vidéosurveillance. Cette procédure est disponible dans la partie Annexes. Elle limite notamment l'accès aux enregistrements vidéo, aux responsables du port et à la gendarmerie.

Le port de Beaulieu a fait le choix d'avoir un opérateur pour utiliser ce système. La journée, il s'agit d'un membre de l'équipe du port qui va aider les équipes sur le terrain. La nuit, un veilleur prend le relais et assure une fonction de surveillance.

Dans le cas d'un problème lié à la sécurité détecté grâce à la vidéosurveillance, le port de Beaulieu fait appel à la gendarmerie seul habilitée à intervenir.

6. Coûts

Le coût d'investissement est de 60 k€ et le contrat de maintenance s'élève à 3 600 €/an.

7. Conclusion

Selon l'équipe du port, le résultat est satisfaisant et présente un accueil favorable auprès des plaisanciers. Il s'agit d'un outil innovant permettant une aide à la gestion.

Dans le futur, le port de Beaulieu souhaiterait l'installation de nouvelles caméras pour le site web, caméras avec une résolution plus importante, et un système de contrôle d'accès vidéo pour l'accès au parking du port.

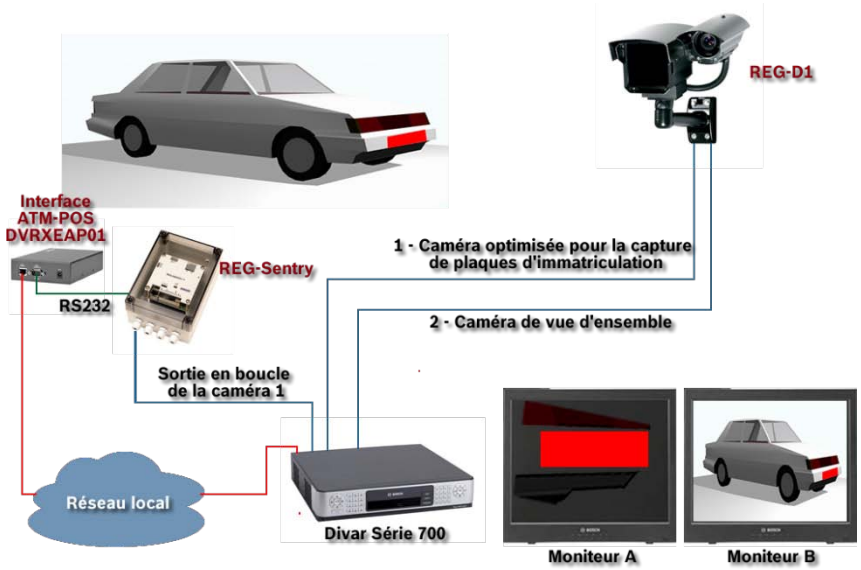


Figure 37 - Exemple de solution de contrôle des accès couplé à la vidéo – Utilisation de caméra optimisée pour la capture de plaques d'immatriculation

A la suite de cette visite, nous avons constaté que lors du choix de la solution de vidéosurveillance, il faut notamment porter son attention sur certains éléments tel que :

- Le choix de la caméra fixe ou mobile
- Le zoom de la caméra, le cas échéant
- Les conditions d'entretien, éventuellement prévoir un essuie-glace sur la caméra
- Le type de mât sur lequel les caméras sont installées - il faut penser à la stabilisation de l'image vidéo lorsqu'il y a beaucoup de vent

B. Port de Leucate

1. Introduction

Le port Leucate est composé de plusieurs bassins enchâssés au cœur des habitations, entre mer et étang. Bordé d'une immense plage, le port dispose de 1350 anneaux abonnés à l'année. Le "Port à sec" vient compléter les équipements et permet le stationnement de 250 bateaux de moins de 7m.

Le système de vidéosurveillance, installé en 2009, comprend 18 caméras (dont 5 caméras dômes) réparties sur 2 bassins du port. L'architecture système retenue est une architecture avec 2 sous-systèmes (une par bassin) comportant chacune des caméras et un système d'enregistrement des images. Cette architecture s'intègre parfaitement dans le système de vidéosurveillance/vidéo-protection équipant la ville de Leucate et comportant lui même plusieurs sous-systèmes. Les sous-systèmes sont consultables via un réseau local.

Cette architecture a été retenu en raison de son aptitude à accroitre de manière importante le nombre de caméras et aux distantes importantes séparant les différentes entités de la commune.

2. But

La particularité du port est le nombre de bassins et son étendue. Un système de vidéosurveillance/vidéo-protection pour l'exploitation d'un tel port devient nécessaire afin d'en optimiser la sécurité.

Le but de ce système est double. En effet, il constitue à la fois un outil de sécurité et un outil de gestion. Les caméras mobiles sont notamment utilisée pour la visualisation en direct par le personnel de la Capitainerie des entrées et des sorties des bassins.

Les images sont enregistrées dans le strict respect de la législation en vigueur.

3. Installation

Le cahier des charges de la solution de vidéosurveillance a été réalisé en collaboration avec le responsable sécurité de la ville et le référent sécurité de la gendarmerie. Un installateur a été choisi suite à un appel d'offres.

4. Maintenance

La maintenance de 1er niveau est assurée par l'équipe Informatique de la ville qui ne fait appel à l'installateur qu'en cas de panne grave. Il a été nécessaire de bien spécifier les livrables attendus en terme de documentation technique à fournir par l'installateur, afin de permettre cette prise en compte de la maintenance par le client.

5. Utilisation du système et retour d’expérience

Le port a mis en place une procédure d'utilisation de ce système de vidéosurveillance. Elle limite notamment l'accès aux enregistrements vidéo, conformément à la législation en vigueur.

La Ville et le Port de Leucate ont fait le choix de ne pas mettre de surveillant derrière les écrans vidéo du système pour le moment. Toutefois, le responsable du port reconnaît l'utilité d'un opérateur surtout lors de tempête (intervention plus rapide de l'équipe portuaire) ou la nuit pour la sécurité.

Le retour d’expérience est convaincant. Le nombre de plaintes déposées en Gendarmerie est passé d’une moyenne de 30 par an à 2. L’effet dissuasif est à développer par la mise en place de panneaux signalant correctement la vidéosurveillance/vidéo-protection du port.

6. Coûts

Le coût d'investissement est de 100 k€.

7. Conclusion

Selon le responsable du port, le résultat est satisfaisant et présente un accueil favorable auprès des plaisanciers.

Dans le futur, le port de Port Leucate souhaite installer de nouvelles caméras notamment à l'entrée du port et une caméra de lecture de plaque d'immatriculation à l'entrée du parking afin de remplacer les badges d’ouverture des barrières des parking..

A la suite de cette visite, nous avons constaté la nécessité d'essuie-glace sur les caméras soumis aux vents et aux embruns. Sur des ports étendus, il faut bien étudier la répartition des caméras et les solutions de communication car la partie génie civil peut s'avérer très couteuse.

VI Remerciements

Nous remercions :

- M. Richard Bonin et Mme Catherine Martin ainsi que l'équipe du port de Beaulieu pour leur accueil et leur participation à l'étude de cas
- M. René Corbefin et M. Bruno Troqueraud ainsi que l'équipe du port de Port Leucate pour leur accueil et leur participation à l'étude de cas

VII Sources

Acier inoxydable [En ligne] / aut. Wikipedia // Wikipedia. - 2010. - Novembre 2010. - http://fr.wikipedia.org/wiki/Acier_inoxydable.

Comment choisir son objectif ? [En ligne] / aut. Créations Absolut // Absolut photo. - Mai 2010. - http://www.absolut-photo.com/cours/objectif/focale.php.

Distance focale [En ligne] / aut. Wikipedia // Wikipedia. - 15 Juin 2010. - 26 Juin 2010. - http://fr.wikipedia.org/wiki/Focale.

Fiche description technique des composants d'un système de vidéo-protection [En ligne] / aut. Ministère de l'intérieur de l'outre mer et des collectivités territoriales // Vidéo Protection. - Mai 2010. - http://www.videoprotection.interieur.gouv.fr.

Les capteurs silicium CCD et CMOS [En ligne] / aut. Couderc Christian // Voilelec. - 10 Juillet 2009. - Mai 2010. - http://www.voilelec.com/pages/ccd.php.

Liste des textes de référence en vigueur [En ligne] / aut. Ministère de l'intérieur de l'outre mer et des collectivités territoriales // Video Protection. - Mai 2010. - http://www.videoprotection.interieur.gouv.fr.

RAID (informatique) [En ligne] / aut. Wikipedia // Wikipedia. - 23 Juin 2010. - 25 Juin 2010. - http://fr.wikipedia.org/wiki/RAID_%28informatique%29.

Vidéosurveillance : quelle déclaration ? [En ligne] / aut. CNIL // CNIL. - 01 Septembre 2010. - Septembre 2010. - http://www.cnil.fr/dossiers/deplacements-transports/fiches-pratiques/article/videosurveillance-quelle-declaration-3/.

Votre projet de vidéo-protection – Guide Méthodologique [En ligne] / aut. Ministère de l'intérieur de l'outre mer et des collectivités territoriales // Vidéo Protection. - 2009. - Mai 2010. - http://www.videoprotection.interieur.gouv.fr.

VIII Liste des figures

IX Liste des tableaux

X Annexes

Les normes techniques – Arrêté du 3 Août 2007

- Arrêté du 3 Août 2007
- Arrêté du 3 Août 2007 – Annexes techniques
- Arrêté du 3 Août 2007 – Notice explicative

Document CERFA n°13806*01

- CERFA n°13806*01
- Notice d'information

Procédure d'utilisation du système de vidéosurveillance du port de Beaulieu

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance

NOR : *IOCD0762353A*

La ministre de l'intérieur, de l'outre-mer et des collectivités territoriales,

Vu la loi nº 95-73 du 21 janvier 1995 d'orientation et de programmation modifiée relative à la sécurité ;

Vu le décret nº 96-926 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application de l'article 10 de la loi nº 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, modifié par le décret nº 2002-814 du 3 mai 2002 pris pour l'application de l'article 21 de la loi nº 2000-321 du 12 avril 2000 et relatif aux délais faisant naître une décision implicite de rejet et par le décret nº 2006-665 du 7 juin 2006 relatif à la réduction du nombre et à la simplification de la composition de diverses commissions administratives,

Arrête :

Art. 1er. – Les caméras sont réglées, équipées et connectées au système de visualisation et, le cas échéant, au système de stockage, de façon que les images restituées lors de la visualisation en temps réel ou en temps différé permettent de répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé.

Les caméras présentent les caractéristiques techniques adaptées aux conditions d'illumination du lieu vidéosurveillé.

Les réseaux sur lesquels transitent les flux vidéo offrent une bande passante compatible avec les débits nécessaires à la transmission d'images de qualité suffisante pour répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé.

Les réseaux sur lesquels transitent les flux vidéo prennent en compte la sécurité de ces derniers, garantissant leur disponibilité, leur confidentialité et leur intégrité.

Art. 2. – Le stockage des flux vidéo est réalisé sur support numérique pour les systèmes de vidéosurveillance comportant huit caméras ou plus. Ce stockage peut également être réalisé sur un autre type de support. Le stockage des flux vidéo est réalisé sur support analogique ou numérique pour les systèmes de vidéosurveillance comportant moins de huit caméras.

Tout flux vidéo enregistré numériquement est stocké avec des informations permettant de déterminer à tout moment de la séquence vidéo sa date, son heure et l'emplacement de la caméra.

Pour les systèmes à enregistrement analogique des flux vidéo, un dispositif permet de déterminer à tout moment la date, l'heure et l'emplacement de la caméra correspondant aux images enregistrées.

L'enregistrement numérique garantit l'intégrité des flux vidéo et des données associées relatives à la date, à l'heure et à l'emplacement de la caméra.

Les flux vidéo stockés issus des caméras, qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit, à l'exclusion de celles de régulation du trafic routier, ont un format d'image supérieur ou égal à 704 × 576 pixels. Ce format pourra être inférieur si le système permet l'extraction de vignettes de visage d'une résolution minimum de 90 × 60 pixels.

Les autres flux vidéo stockés ont un format d'image supérieur ou égal à 352 × 288 pixels.

Une fréquence minimale de douze images par seconde est requise pour l'enregistrement des flux vidéo issus de caméras installées pour une des finalités mentionnées au II de l'article 10 de la loi du 21 janvier 1995 susvisée, à l'exclusion de celles de régulation du trafic routier, et qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit et filment principalement des flux d'individus en déplacement rapide.

Pour l'enregistrement des autres flux vidéo, une fréquence minimale de six images par seconde est requise.

Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo.

Texte précédent Page suivante Texte suivant

Pour les systèmes numériques, ce journal est généré automatiquement sous forme électronique.

Art. 3. – Les flux vidéo sont exportés sans dégradation de la qualité.

Pour les systèmes de vidéosurveillance utilisant la technologie analogique, un dispositif détermine la liste des flux exportés indiquant la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation.

Pour les systèmes de vidéosurveillance utilisant la technologie numérique, un journal électronique des exportations, comportant les informations citées à l'alinéa précédent, est généré automatiquement.

Le système d'enregistrement reste en fonctionnement lors de ces opérations d'exportation.

Le support physique d'exportation est un support numérique non réinscriptible et à accès direct, compatible avec le volume de données à exporter. Dans le cas de volumes importants de données à exporter, des disques durs utilisant une connectique standard pourront être utilisés. Pour les systèmes numériques de vidéosurveillance, un logiciel permettant l'exploitation des images est fourni sur support numérique, disjoint du support des données.

Le logiciel permet :

1° La lecture des flux vidéo sans dégradation de la qualité de l'image ;

2° La lecture des flux vidéo en accéléré, en arrière, au ralenti ;

3° La lecture image par image des flux vidéo, l'arrêt sur une image, la sauvegarde d'une image et d'une séquence, dans un format standard sans perte d'information ;

4° L'affichage sur l'écran de l'identifiant de la caméra, de la date et de l'heure de l'enregistrement ;

5° La recherche par caméra, date et heure.

Art. 4. – Le présent arrêté est complété de trois annexes techniques.

Art. 5. – L'arrêté du 26 septembre 2006 portant définition des normes techniques des systèmes de vidéosurveillance est abrogé.

Art. 6. – Le directeur général de la police nationale, le directeur général de la gendarmerie nationale et le directeur des libertés publiques et des affaires juridiques sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 3 août 2007.

MICHÈLE ALLIOT-MARIE

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance (rectificatif)

NOR : *IOCD0762353Z*

Rectificatif au *Journal officiel* du 21 août 2007, édition électronique, texte n° 4, et édition papier, page 13889, après la signature, ajouter les annexes suivantes :

ANNEXE TECHNIQUE 1

L'arrêté fixe des normes techniques qui portent, d'une part, sur les caméras et sur les systèmes de transmission et de stockage (articles 1er et 2), d'autre part, sur l'interopérabilité des systèmes de stockage et d'exportation des données vers les forces de police et de gendarmerie (article 3).

Afin de faciliter l'utilisation de la présente circulaire, les prescriptions de l'arrêté qu'elle commente sont reprises en italique.

1. **Les caméras**

« Les caméras sont réglées, équipées et connectées au système de visualisation et, le cas échéant, au système de stockage, de façon que les images restituées lors de la visualisation en temps réel ou en temps différé permettent de répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé. »

1.1. Les caractéristiques techniques du système de vidéosurveillance doivent permettre d'atteindre les objectifs de sécurité ayant présidé à son installation.

La première implication est que les objectifs du système et de chaque caméra, en termes de sécurité, doivent être clairement énoncés. Ces objectifs concernent le système global (taux d'indisponibilité accepté, caractéristiques du système de stockage...) ainsi que les caméras proprement dites, dont les rôles doivent être définis. A titre d'exemple, tel groupe de caméras pourra avoir comme rôle principal de permettre la levée de doute avant une ouverture de porte, alors que tel autre groupe de caméras aura comme objectif principal de permettre l'analyse de l'image en temps réel comme, par exemple, la reconnaissance d'individus ayant accédé à une zone donnée.

1.2. La qualité des images.

La seconde implication, fondamentale, est que les caractéristiques techniques du système doivent être cohérentes avec les objectifs énoncés. Ce point est essentiel car, si la diversité des situations interdit de définir de manière absolue ce que doivent être les caractéristiques techniques d'un système pour obtenir un certain résultat, il est toujours possible en revanche de vérifier la cohérence d'un système avec les objectifs qui lui sont assignés. L'arrêté précise que cette vérification ne doit pas se faire exclusivement sur les différents éléments du système (qualité des caméras, qualité des liaisons de données, qualité de la compression des images...) mais sur la qualité des images restituées.

Cette mise en cohérence impose à l'opérateur d'adapter les éléments déficients ou mal dimensionnés du système lorsque la qualité des images restituées est incompatible avec les objectifs de celui-ci.

Le contrôle de cette cohérence lors de l'examen de la demande d'autorisation préalable à l'installation, donc « sur dossier », peut s'avérer difficile. Une annexe technique fournit néanmoins quelques repères dont les services des préfectures pourront s'inspirer lors de l'examen des dossiers.

Il convient toutefois d'attirer l'attention sur le fait que cette première prescription présente un intérêt certain dans l'hypothèse d'un contrôle *a posteriori* du système, lors de la demande de renouvellement de l'autorisation par exemple.

« Les caméras présentent les caractéristiques techniques adaptées aux conditions d'illumination du lieu vidéosurveillé ».

Il s'agit de vérifier simplement que l'opérateur a pris en compte les spécificités liées à l'illumination des scènes à vidéosurveiller lors du choix des caméras. En effet, s'il s'agit de pouvoir enregistrer des images de

qualité en vision nocturne, alors il conviendra soit d'utiliser des caméras à haute sensibilité soit de prévoir un éclairage d'appoint, infrarouge par exemple. Ces éléments doivent aller de pair avec les conditions particulières d'éclairage des scènes filmées, qui devront être également précisées (un éclairage intense peut en effet, en intérieur notamment, autoriser l'usage d'une caméra moins sensible).

2. **La transmission des images**

« Les réseaux sur lesquels transitent les flux vidéo offrent une bande passante compatible avec les débits nécessaires à la transmission d'images de qualité suffisante pour répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé. »

Les images issues des caméras, pour être transmises sur les réseaux, doivent être codées et généralement compressées pour pouvoir être communiquées en temps réel au travers des artères de transmission. Le débit maximum de ces voies de transmission, appelé bande passante, conditionne donc directement la qualité des images réceptionnées. Ainsi, une bande passante insuffisante entraînera automatiquement une perte de qualité (compression des images trop importante induisant une perte préjudiciable d'information) ou de performance (diminution du nombre d'images par seconde ou choix de ne pas transmettre tous les flux).

La diversité des cas d'utilisation (image fixe ou avec beaucoup de mouvement par exemple) et des dispositifs techniques (compression MPEG 2, MPEG 4, JPEG, JPEG 2000...) ne permet pas de définir à l'avance la bande passante minimum nécessaire à la transmission numérique d'une image de qualité, cette qualité dépendant également de l'objectif de sécurité fixé. Il est rappelé pour mémoire, que le poids moyen d'une image d'excellente qualité est de 45 Ko. En revanche, le tableau ci-dessous donne un aperçu de l'ordre de grandeur de la bande passante utilisée pour transmettre des images avec certaines caractéristiques pour les différentes classes de compression de données.

TYPE DE MÉCANISME DE COMPRESSION	DÉBIT THÉORIQUE MOYEN pour disposer d'images au format 4 CIF à 12 images par seconde
JPEG	5 Mbits/s
JPEG 2000	3 Mbits/s
MPEG 2	2 Mbits/s
MPEG 4	1 Mbits/s
MPEG 4 (H 264)	0,5 Mbits/s

Ainsi, si un opérateur déclare faire transiter 8 flux simultanés d'images, au format 4 CIF à 12 images par seconde comprimées au format MPEG 2 (2 Mbits × 8 = 16 Mbits de débit théorique nécessaire à la transmission de ces flux), sur un système disposant d'une bande passante de 4Mbits, il conviendra de s'interroger sur la pertinence de ce choix.

« Les réseaux sur lesquels transitent les flux vidéo prennent en compte la sécurité de ces derniers, garantissant leur disponibilité, leur confidentialité et leur intégrité. »

Les données restituées par les systèmes de vidéosurveillance doivent présenter trois types de caractéristiques essentielles :

– elles doivent être conformes aux images originelles. Ces dernières ne doivent donc pas avoir été corrompues ou modifiées durant leur transfert. Le système de transmission doit offrir une garantie d'intégrité des données communiquées ;
– elles doivent être accessibles en cas de sollicitation. Pour cela, il faut en premier lieu que le système de transmission soit robuste aux dysfonctionnements comme aux éventuelles agressions externes. Il doit offrir une garantie de disponibilité des données communiquées ;
– elles ne doivent être accessibles qu'aux personnes habilitées à en disposer. Cela implique que des dispositifs spécifiques doivent être mis en œuvre pour empêcher l'interception et la lecture des données transmises. Le système de transmission doit donc offrir une garantie de confidentialité des données échangées, le plus souvent par le biais de fonctions de chiffrement adaptées.

Il ne s'agit pas ici de se livrer à une expertise de sécurité exhaustive garantissant ces trois critères, ni même de solliciter l'opérateur pour un certificat formel de sécurité. En revanche, il convient de s'assurer que ces critères ont été pris en compte et que les solutions mises en œuvre adressent ces trois sujets.

Le cas des transmissions numériques sans fil (technologies dites Wi-Fi ou Wi-Max par exemple) méritent assurément une attention particulière. En effet, l'interception des flux est par nature aisée ainsi que, dans une moindre mesure, le « déni de service ». Il convient donc que, d'une part, l'opérateur garantisse la confidentialité des données par l'utilisation d'un chiffrement adapté et fiable et que, d'autre part, il limite l'usage de ces technologies aux segments de réseau terminaux ou impropres aux technologies filaires.

3. **Le stockage**

« Le stockage des flux vidéo est réalisé sur support numérique pour les systèmes de vidéosurveillance comportant huit caméras ou plus. Ce stockage peut également être réalisé sur un autre type de support. Le stockage des flux vidéo est réalisé sur support analogique ou numérique pour les systèmes de vidéosurveillance comportant moins de huit caméras. »

Lorsqu'une installation de vidéosurveillance devient importante, il n'est pas concevable, dans un objectif de qualité de service, d'utiliser un stockage de type analogique. Le stockage numérique est donc impératif. Il convient de noter que cette contrainte ne porte que sur le module d'enregistrement des images, ce qui implique notamment que rien n'interdit d'utiliser des caméras analogiques dont les flux seront numérisés par la suite. Il est toutefois précisé que le stockage peut également être réalisé sur un autre type de support afin de permettre aux opérateurs de conserver leur système d'enregistrement analogique (type cassettes VHS), en plus du système d'enregistrement numérique qu'ils seront tenus de mettre en place.

Pour limiter le coût d'installation de petits systèmes de vidéosurveillance, il est possible d'utiliser un support de stockage analogique apportant une plus grande facilité d'installation et d'utilisation. Les systèmes visés ici, qui comportent sept caméras ou moins, doivent être compris comme ceux destinés à sécuriser une entité géographique autonome. A titre d'exemple, une entreprise qui dépose une demande d'autorisation pour des systèmes de vidéosurveillance dans chacune de ses agences (donc indépendants et autonomes) peut concevoir ces systèmes comme autonomes pour chacune d'elles. Dans ce cas, toutes les agences de sept caméras ou moins sont autorisées à conserver un système de stockage de type analogique. Néanmoins, il faut bien préciser que ces systèmes ne sont considérés comme autonomes que si le stockage et/ou la visualisation s'effectue(nt) dans chacune des agences. Si les vidéos des agences sont rapatriées sur un ou plusieurs sites communs, alors les systèmes de chaque agence ne peuvent plus être considérés comme indépendants.

« Tout flux vidéo enregistré numériquement est stocké avec des informations permettant de déterminer à tout moment de la séquence vidéo sa date, son heure et l'emplacement de la caméra. »

Dans l'objectif de pouvoir utiliser les images vidéo stockées dans des procédures judiciaires, il est nécessaire de pouvoir certifier les informations spatiales et temporelles associées aux images. L'article 2, deuxième alinéa, de l'arrêté du 26 septembre 2006 ne vise explicitement que la capacité du système d'enregistrement à associer aux images ces trois données. Son esprit est toutefois de permettre à un service enquêteur d'utiliser efficacement les données numériques transmises, ce qui a une double implication :

– les paramètres de date et de localisation doivent être accessibles à l'enquêteur avec le système de visualisation dont il dispose ;
– les paramètres doivent être exacts.

Il conviendra donc de s'assurer, dans la mesure du possible, que ces deux contraintes ont été prises en compte.

Il existe une méthode simple qui consiste à marquer ces informations directement sur l'image vidéo. Néanmoins, cette méthode a le désavantage de masquer des parties de l'image. Une autre méthode consiste à associer les informations avec le flux vidéo, puis de créer une liaison logicielle entre les images et le fichier d'information associé. Dans ce cas particulier, les lecteurs fournis aux services d'enquête devront disposer d'une capacité spécifique pour réassocier les données et les images lors de leur exploitation.

L'opérateur du système de vidéosurveillance devra par ailleurs préciser comment il s'assure de la fiabilité du référentiel temporel qui sera associé aux images.

« Pour les systèmes à enregistrement analogique des flux vidéo, un dispositif permet de déterminer à tout moment la date, l'heure et l'emplacement de la caméra correspondant aux images enregistrées. »

Le besoin des forces de police est identique quelle que soit la nature du système, seul le mécanisme de stockage des informations associées aux images sera différent. Dans le cas d'enregistrement analogique (du type cassettes VHS), les informations doivent exister mais leur format (fichier papier ou numérique) n'est pas précisé. Il conviendra néanmoins de s'assurer que les enquêteurs pourront disposer de ces informations lors de l'analyse des images. Les données associées aux supports analogiques doivent donc pouvoir leur être communiquées avec les cassettes vidéo.

« L'enregistrement numérique garantit l'intégrité des flux vidéo et des données associées relatives à la date, à l'heure et à l'emplacement de la caméra. ».

Les moyens à mettre en œuvre pour garantir l'intégrité des flux vidéo et des données associées relatives à la date, à l'heure et à l'emplacement de la caméra ne sont pas spécifiés. En particulier, il n'est pas exigé ici que les systèmes intègrent des dispositifs de marquage électronique des images (parfois appelé *watermarking* ou *filigranage*), même si ces dispositifs sont les bienvenus et doivent être encouragés. En effet, un système numérique robuste quant aux traces enregistrées (toute intervention de nature à modifier les données est immanquablement enregistrée) et à l'environnement d'exploitation (qui garantit notamment l'intégrité du système de traces) est susceptible d'atteindre les objectifs d'intégrité.

« Les flux vidéo stockés issus des caméras qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit, à l'exclusion de celles de régulation du trafic routier, ont un format d'image supérieur ou égal à 704 × 576 pixels. Ce format pourra être inférieur si le système permet l'extraction de vignettes de visage d'une résolution minimum de 90 × 60 pixels. »

L'objet de l'article 2, cinquième alinéa, est de favoriser l'existence d'images d'une précision satisfaisante pour le travail des enquêteurs. Il pose donc le principe d'un niveau de qualité minimum des images stockées lorsqu'elles sont issues de caméras fonctionnant en plan étroit.

L'équilibre recherché ici consiste à garantir un bon niveau de qualité des images seulement lorsque c'est nécessaire pour les forces de police et de gendarmerie, sans faire peser des contraintes techniques trop importantes sur les parties du dispositif qui concernent moins directement le travail d'investigation.

Pour cela, on distingue deux grands types de caméras de vidéosurveillance, celles dont la fonction principale est d'analyser les informations sur les individus ou les objets présents dans le champ des caméras (qui sont dites fonctionner en plan étroit) et celles dont la fonction principale est de fournir une vue globale de la situation (qui sont dites fonctionner en plan large).

Cette classification appelle deux remarques et mérite d'être illustrée par quelques exemples.

Tout d'abord, il est entendu que les caméras qui constituent un dispositif de vidéosurveillance ont le plus souvent des missions multiples. Ceci est d'autant plus vrai que certaines caméras sont dotées de fonctions de zoom et d'orientation rapide qui leur permettent d'offrir un plan global et de passer l'instant suivant en plan rapproché. Néanmoins, il reste qu'à chaque caméra est le plus souvent assigné un objectif principal d'exploitation : levée de doute, gestion d'une file d'attente, surveillance d'un objectif sensible, contrôle des flux...

Il est nécessaire que ces objectifs principaux soient précisés pour chaque caméra dans les dossiers transmis par les opérateurs. Le plus souvent ils doivent permettre de statuer sur la classification des caméras à plan large ou à plan étroit.

Ensuite, il est légitime de s'interroger sur la corrélation éventuelle entre les caractéristiques techniques en termes de focale ou de zoom des caméras et leur usage en plan large ou plan étroit (telles que ces notions ont été définies ci-dessus). Compte tenu de la diversité des usages de la vidéosurveillance, ce lien ne semble pas être pertinent. En effet, une caméra destinée à garantir la sécurité d'un distributeur automatique de billets ou à sécuriser les entrées-sorties dans un bus peut, du fait de la faible distance à la cible, fonctionner avec une ouverture angulaire importante, alors qu'au sens de l'arrêté du 26 septembre 2006 il s'agit bien, compte tenu de la précision attendue de l'image, d'un fonctionnement en plan étroit. De la même manière, certaines caméras destinées à sécuriser des voies ferrées peuvent fonctionner avec une petite ouverture angulaire mais en plan large au sens de l'arrêté, si elles sont destinées à la régulation du trafic ferroviaire.

La résolution de 704 × 576 correspond au format dit 4 CIF, normalisé dans le domaine de la vidéo, compatible avec les performances de la majorité des caméras installées et constituant la norme haute en matière de définition d'image en attendant la généralisation des caméras dites à haute définition. La définition visée dans cet article concerne les images stockées sur le système d'enregistrement. Ceci implique que toute la chaîne vidéo doit afficher des caractéristiques compatibles avec ces formats d'enregistrement : la résolution des capteurs (caractéristiques techniques des caméras), le format d'image en sortie de caméra, le taux de compression des images lors du transfert et du stockage. Une autre conséquence est que les espaces de stockage doivent être compatibles avec les caractéristiques globales du système. Il est donc important que les spécifications techniques (définition, taux de compression, nombre d'images par seconde, durée de conservation des données, nombre de flux stockés) du système soient précisées ainsi que le calcul menant au dimensionnement des espaces de stockage.

Dans certains cas, il n'est pas nécessaire de disposer d'une image de 704 × 576 pixels pour offrir une résolution satisfaisante des sujets filmés. Les opérateurs ont donc toute latitude pour retenir un format inférieur pour peu que celui-ci propose, dans la zone nominale de prise de vue, une résolution permettant l'identification d'un visage. En particulier, des caméras numériques au format VGA (640 × 480 pixels) qui permettraient l'extraction sur les vidéos enregistrées de vignettes de visage de 90 × 60 pixels conviennent.

Il est certain que la diversité des situations occasionnera inévitablement des cas litigieux ou ambigus pour lesquels la proposition de classification *plan large/plan étroit* du soumissionnaire pourra apparaître discutable. Pour déterminer de façon pratique les caractéristiques minimales des images stockées, le tableau d'exemples proposé en annexe I doit permettre le plus souvent d'assimiler ces situations à un cas d'usage approchant déjà traité.

« Les autres flux vidéo stockés ont un format d'image supérieur ou égal à 352 × 288 pixels ».

Tous les autres flux vidéo issus des systèmes de vidéosurveillance visés par la loi du 21 janvier 1995, modifiée par la loi du 23 janvier 2006, doivent au minimum être stockés avec une résolution de 352 × 288 pixels, aussi appelé format CIF. C'est notamment le cas des images issues d'un dispositif de régulation du trafic routier.

« Une fréquence minimale de douze images par seconde est requise pour l'enregistrement des flux vidéo issus de caméras installées pour une des finalités mentionnées au II de l'article 10 de la loi du 21 janvier 1995 susvisée, à l'exclusion de celles de régulation du trafic routier, et qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit et filment principalement des flux d'individus en déplacement rapide. »

Le nombre d'images par seconde constitue également un paramètre important lorsqu'il s'agit de chercher des éléments précis dans une scène vidéo en mouvement. Il convient pourtant de moduler les exigences en fonction des besoins opérationnels véritables pour ne pas surdimensionner le système de vidéosurveillance inutilement. C'est pourquoi l'exigence de disposer de 12 images enregistrées par seconde ne s'applique qu'aux caméras fonctionnant principalement en plan étroit (cf. article 2, alinéa 5) et parmi celles-ci exclusivement à celles destinées à surveiller des flux de personnes en « déplacement rapide ».

Cette notion fait explicitement référence à des situations où les individus filmés sont, sauf circonstances particulières, en train de marcher sans rencontrer d'obstacle lorsqu'ils traversent la zone de prise de vue. Il est question en particulier *de déplacement* rapide pour les caméras destinées à filmer un espace de transit dans les

lieux publics (couloir de métro, hall d'aéroport, trottoir urbain...). En revanche ne sont pas considérées comme des déplacements rapides les images d'individus en train de franchir une porte ou un tourniquet de métro, ou stationnant dans un hall destiné à l'attente ou au recueil de bagages.

Les cas de figure les plus typiques ou susceptibles de poser problèmes sont évoqués en annexe 2.

« Pour l'enregistrement des autres flux vidéo, une fréquence minimale de six images par seconde est requise. »

Toutes les autres images visées par la loi du 21 janvier 1995 doivent au minimum être enregistrées à une cadence réelle de 6 images par seconde à partir d'une caméra dont bien entendu la fréquence d'acquisition des images sera d'au minimum 6 images par seconde. Ainsi, il ne serait donc être question de reconstruire artificiellement un flux à 6 images par seconde à partir par exemple d'une séquence initiale à 3 images par seconde. Il en est de même pour un enregistrement à 12 images par seconde.

« Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo. »

La traçabilité des actions effectuées sur le système est primordiale pour vérifier qu'aucun abus et qu'aucune action de malveillance n'ont été commis. Dans le cas des systèmes d'enregistrement analogique ou des systèmes de vidéosurveillance numériques de moins de huit caméras, un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux (export, modification, suppression...) peut être tenu à la main.

« Pour les systèmes numériques, ce journal est généré automatiquement sous forme électronique. »

Pour simplifier l'opération de journalisation, qui peut être fastidieuse pour de gros systèmes, il faut que, pour les systèmes numériques, cette opération soit automatisée. Il conviendra donc de s'assurer que le système proposé intègre cette fonction et que l'opérateur prévoie dans son plan d'exploitation de la mettre en œuvre.

4. **Les contraintes d'interopérabilité**

L'arrêté du 26 septembre 2006 a pour objectif que les techniques de la vidéosurveillance puissent mettre en œuvre de façon concrète les dispositions que la loi du 21 janvier 1995 modifiée a édictées.

Les dispositions de l'article 3 de l'arrêté précité ont pour but de faciliter concrètement l'exploitation des systèmes par les services de police et de gendarmerie.

« Les flux vidéo sont exportés sans dégradation de la qualité. »

La transmission des films vidéo aux forces de police et de gendarmerie nécessite une opération dite « d'exportation ». Il est nécessaire que la qualité des images exportées soit maximale, ce qui implique que le système doit être en mesure d'exporter ses données sans perte de qualité.

Si, lors de l'opération d'exportation, il s'avère nécessaire de modifier le format ou le type de compression des flux vidéo, il conviendra alors de s'assurer que la compression des vidéos exportées ne dégrade pas leur qualité.

Il est donc important de connaître la méthode d'exportation des flux vidéo et, dans le cas où il ne s'agit pas d'une simple copie des données, les caractéristiques de la compression utilisée pour le stockage et l'exportation.

« Pour les systèmes de vidéosurveillance utilisant la technologie analogique, un dispositif détermine la liste des flux exportés, indiquant la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation. »

Il est important de conserver une traçabilité des exportations pour assurer qu'aucun abus ne soit commis. La difficulté de cette mesure pour un système de vidéosurveillance analogique, et dans une moindre mesure pour les systèmes numériques de moins huit caméras, est parfois le manque d'automatisation du système. Il est alors nécessaire d'intégrer dans la procédure d'exportation de flux vidéo la constitution manuelle d'un journal des différentes opérations effectuées sur le système. Cette action de constitution d'un journal doit en particulier permettre de pouvoir identifier la ou les personnes qui ont exporté les flux vidéo.

« Pour les systèmes de vidéosurveillance utilisant la technologie numérique, un journal électronique des exportations, comportant les informations citées à l'alinéa précédent, est généré automatiquement. »

De même que pour les systèmes analogiques, la traçabilité des exportations est, pour les systèmes numériques, primordiale. L'avantage d'un système numérique est la possibilité d'automatiser des actions. Ainsi, pour assurer l'exactitude des informations contenues dans la liste des flux exportés, il suffit de créer un « journal » électronique constitué automatiquement par le système.

« Le système d'enregistrement reste en fonctionnement lors de ces opérations d'exportation. »

L'exportation de données ne doit en aucun cas diminuer les capacités d'un système de vidéosurveillance. En effet, il serait fortement dommageable que, lors de l'exportation d'images vidéo, un événement grave se produise et qu'il soit impossible d'enregistrer les flux vidéo y afférents. Le fait que le système d'enregistrement reste en fonctionnement lors des opérations d'exportation vise en particulier à interdire l'extraction des unités de stockage du système durant les phases d'investigation si cette action interdit la poursuite du fonctionnement normal du système. Il est donc important de vérifier que la procédure d'exportation soit conforme à cette exigence. Une méthode simple consiste à prévoir des supports de stockage supplémentaires afin de remplacer ceux qui seraient temporairement extraits du système.

« Le support physique d'exportation est un support numérique non réinscriptible et à accès direct, compatible avec le volume de données à exporter. Dans le cas de volumes importants de données à exporter, des disques

durs utilisant une connectique standard pourront être utilisés. Pour les systèmes numériques de vidéosurveillance, un logiciel permettant l'exploitation des images est fourni sur support numérique, disjoint du support des données. »

Le système de stockage des enregistrements vidéo doit être doté de la capacité à exporter des films et des photos vers un support non réinscriptible, qui, en l'état actuel, sera le plus souvent du type graveur de CD ou de DVD. Tous les systèmes doivent donc disposer de cette fonctionnalité. Ceci implique notamment que les clés USB (qui constituent un support réinscriptible) ne peuvent être le seul support d'exportation sur un tel système.

Le support doit de plus être à *accès direct*, c'est-à-dire que les informations doivent être accessibles sans avoir à parcourir séquentiellement l'ensemble du support. En particulier, les cassettes DAT ne peuvent constituer un support d'exportation valable.

Toutefois, il est parfois nécessaire d'exporter une quantité importante de données. Dans ce cas exclusivement, il est autorisé d'utiliser des disques durs, qui permettent une plus grande capacité de stockage. Cette possibilité vient s'ajouter à la capacité d'export sur des supports non réinscriptibles, qui constituent dans tous les cas le moyen par défaut de transmission des données vers les forces de sécurité.

« Le logiciel permet :

« 1° La lecture des flux vidéo sans dégradation de la qualité de l'image ;

« 2° La lecture des flux vidéo en accéléré, en arrière, au ralenti ;

« 3° La lecture image par image des flux vidéo, l'arrêt sur une image, la sauvegarde d'une image et d'une séquence, dans un format standard sans perte d'information ;

« 4° L'affichage sur l'écran de l'identifiant de la caméra, de la date et de l'heure de l'enregistrement ;

« 5° La recherche par caméra, date et heure. »

Les flux vidéo sont exportés pour être traités par les services de police ou de gendarmerie. Les caractéristiques mentionnées doivent donc être intégrées dans le logiciel de lecture, fourni sur un support numérique séparé distinct de celui des images, par l'opérateur aux services enquêteurs en même temps que les images.

ANNEXE TECHNIQUE 2

Exemples caractéristiques, illustrant les notions de « fonctionnement en plan étroit » et de « flux d'individus en déplacement rapide » :

SITUATION	RÉSOLUTION minimum de l'image stockée	NOMBRE D'IMAGES par seconde au minimum	COMMENTAIRES classification plan étroit/plan large
Caméra de surveillance de la voie publique en agglomération aux abords d'un site sensible.	CIF	6	Plan large.
Caméra de surveillance d'un monument sur la voie publique	CIF	6	Plan large.
Caméra de surveillance d'un automate (DAB...).	4 CIF*	6	Plan étroit.
Caméra de surveillance à l'intérieur d'un véhicule de transport public.	4 CIF*	6	Plan étroit.
Caméra de surveillance sur un quai de gare.	CIF	6	Plan large.
Caméra de surveillance en entrée ou sortie d'un commerce, d'un musée, d'une agence bancaire, d'un lieu ouvert au public.	4 CIF*	12 *ou 6*	Plan étroit *6 si un dispositif de filtrage des flux de personnes est présent (sas, tourniquet...).*
Caméra de régulation du trafic routier	CIF	6	Plan large.
Caméra de surveillance d'un comptoir ou d'un guichet.	4 CIF	6	Plan large.
Caméra de surveillance de rayons d'un magasin.	CIF	6	Plan large.
Caméra de surveillance d'une pompe de carburant.	4 CIF*	6	Plan étroit.
Caméra de surveillance d'une caisse ou d'un terminal de paiement.	4 CIF*	6	Plan étroit.

SITUATION	RÉSOLUTION minimum de l'image stockée	NOMBRE D'IMAGES par seconde au minimum	COMMENTAIRES classification plan étroit/plan large
Caméra de surveillance de voie sur route ou autoroute.	CIF	6	Plan large.
Caméra de surveillance aux abords d'un péage routier.	4 CIF*	6	Plan étroit.
Caméra de surveillance sur une issue de secours.	4 CIF*	6	Plan étroit.
Caméra de lutte contre la démarque inconnue.	4 CIF*	6	Plan étroit.
Caméra de vérification et de contrôle d'accès (filmant dans la zone ouverte au public).	4 CIF*	6	Plan étroit.
Visualisation d'un lieu de distribution de fonds transportés.	4 CIF*	6 *ou 12*	Plan étroit.
(*) Ou résolution permettant l'extraction de vignettes de visages de 90 x 60 pixels.			

Ces exemples permettent de couvrir un grand nombre de cas d'implantations de caméras. Ce tableau est présenté à titre indicatif pour permettre aux commissions départementales de statuer plus facilement sur la classification plan large, plan étroit.

Cependant, il est bien entendu qu'il peut exister certains cas particuliers où ce tableau n'est pas applicable :

– des caméras dont l'objectif est de faciliter le contrôle des flux sont des caméras fonctionnant habituellement en plan large. Néanmoins, dès qu'il est précisé que ce contrôle doit permettre de savoir quelles sont les personnes sur les vidéos, ces caméras seront considérées comme fonctionnant en plan étroit ;

– de même, une caméra surveillant une entrée de parking dont l'objectif est de contrôler quelle personne et/ou quel véhicule accède au parking devra fonctionner en 4 CIF et en 6 images par seconde ou 12 images par seconde (flux en déplacement rapide) selon l'entrée régulée ou non des véhicules et personnes ;

– toute caméra dont l'objectif est d'analyser des informations sur les individus ou les objets dans la scène devra être considérée comme fonctionnant en plan étroit, et ce quelles que soient sa situation et son implantation ;

– toute caméra dont l'objectif est d'analyser des informations sur des individus ou des objets en déplacement rapide présents dans la scène devra fonctionner en 12 images par seconde (personnes sur tapis roulant, entrée dans un magasin sans dispositif de filtrage...).

ANNEXE TECHNIQUE 3

Glossaire

Définition de quelques termes techniques utilisés fréquemment en matière de vidéosurveillance

Accès direct (stockage à) : cette notion réfère à la capacité d'un système de stockage à pouvoir accéder directement à une information enregistrée, sans parcourir l'enregistrement. Le système de stockage à accès direct le plus courant est le disque dur. Ces systèmes sont à opposer aux systèmes de stockage à accès séquentiel.

Accès séquentiel (stockage à) : stockage où la lecture et l'enregistrement s'effectuent selon un ordre prédéfini. Par exemple, les cassettes VHS, K7, DV, DAT, où, pour accéder à la troisième minute de l'enregistrement, il est nécessaire de parcourir les trois premières minutes, sont des systèmes de stockage à accès séquentiel.

Bande passante (réseau) : dans le domaine de l'informatique, le terme bande passante désigne un débit d'informations, plus précisément la quantité d'informations que peut transmettre un réseau (système informatique). Cette bande passante ce mesure généralement en octets par seconde ou en bits par seconde.

Cassettes VHS : support d'enregistrement analogique à accès séquentiel utilisant la norme VHS.

Champ (optique) : en optique, la notion de champ réfère à la portion d'espace visible à travers l'objectif de la caméra.

Compression : réduction de l'espace nécessaire au stockage et à la transmission de données (vidéos, images...). Cette compression peut être réalisée avec ou sans perte d'information sur ces données.

DAT : *Digital Audio Tape* est à la base un support d'enregistrement audionumérique. Ce support est aujourd'hui également utilisé pour stocker des vidéos, de l'audio ou des données informatiques. Ce type de stockage est à accès séquentiel.

Déni de service : en sécurité informatique, « l'attaque par déni de service » est une tentative de rendre une application, un système ou une ressource informatique indisponible à ses utilisateurs autorisés. Si un système informatique (serveur par exemple) n'est plus capable de traiter les requêtes de ses clients pour des raisons volontairement provoquées par un tiers, il y a « déni de service ». Le type d'attaque le plus répandu est de rendre un serveur inopérant en lui adressant de trop nombreuses requêtes. Les conséquences d'un tel acte peuvent se traduire dans le cas d'un système réseau de vidéosurveillance par :

– un réseau inhabituellement ralenti (difficulté pour communiquer en continu avec une caméra par exemple) ;
– impossibilité d'accéder à une caméra particulière ;
– impossibilité d'accéder à n'importe quelle caméra ;
– augmentation du nombre de messages reçus via le réseau (mail, message de contrôle, message d'erreur...).

Disque dur : système de stockage à accès direct et à mémoire non volatile s'appuyant sur le principe de mémoire magnétique. Développé dans un premier temps pour une utilisation sur ordinateur, il a peu à peu remplacé tous les autres systèmes de stockage vidéo et audio par l'évolution rapide de sa capacité de stockage et de la facilité d'accès aux données sauvegardées.

Exportation (de données) : opération consistant à copier ou à extraire du système de stockage des informations ciblées.

Flux : en informatique, ensemble de données élémentaires issues d'un système informatique.

Focale (distance) : la distance focale d'un système optique est l'une des grandeurs qui définit entièrement un système optique. On peut l'assimiler dans la plupart des cas à la distance entre l'objectif et le capteur de la caméra.

Format CIF (4 CIF) : *Common Intermediate Format*. Le format CIF est un format numérique d'images de 352 × 288 pixels. Le format 4 CIF évoqué dans cette circulaire est le format d'image standard de 704 × 576 pixels.

Format d'image : taille de l'image définie en terme de pixels ou de lignes et de colonnes.

Liaison logicielle : liaison assurée par un logiciel informatique de manière automatique entre plusieurs données ou opérateurs.

Ouverture angulaire (optique) : cette grandeur représente la portion d'espace en terme d'angle visible à travers l'objectif de la caméra.

Pixel *(Picture Element)* : structure élémentaire d'une image numérique. C'est le plus petit point discernable sur une image. Le pixel peut être une forme géométrique quelconque, même si le carré est sa structure la plus répandue. Chaque pixel contient des informations de couleur (image couleur) ou de niveau de gris (noir et blanc)

Résolution : *cf.* format d'image.

Stockage (analogique/numérique) : entreposage, sauvegarde des données (dans ce cas vidéo) sur un support de type analogique (cassette VHS...) ou numérique (disque dur, DVD...).

Système numérique : la notion de système numérique, dans le contexte de l'arrêté, s'applique exclusivement aux modules de stockage. Ainsi un système composé de caméras analogiques, mais avec un module de stockage numérique, sera considéré comme un système numérique de vidéosurveillance.

Système analogique : la notion de système analogique, dans le contexte de l'arrêté, s'applique exclusivement aux modules de stockage. Sur une installation de vidéosurveillance, si le module de stockage est analogique, alors le système de vidéosurveillance sera donc considéré comme analogique. On étendra cette catégorie aux systèmes de vidéosurveillance de moins de huit caméras équipés de modules de stockage numérique, mais dont les fonctionnalités se limitent à celles d'un module de stockage analogique.

Visage : on entendra par dimensions du visage les distances entre le bas du menton et le haut des cheveux ou du crâne et entre les deux oreilles. Selon les exigences présentes dans l'arrêté, les dimensions d'un visage sur une caméra de format inférieur au 4 CIF, fonctionnant en plan étroit, devront donc être d'au moins 60 pixels pour la distance entre les deux oreilles et 90 pixels pour la distance entre le bas du menton et le haut des cheveux ou du crâne.

Watermarking/filigranage : technique permettant d'ajouter des informations destinées à sécuriser une image, une vidéo ou tout autre type de documents numériques, en les intégrant dans le fichier sans le modifier ni le détériorer

Wi-Fi : technologie de réseau informatique sans fil fonctionnant sur une courte distance (d'une dizaine à une centaine de mètres dans des conditions usuelles d'utilisation).

Wi-Max : famille de norme pour les réseaux informatiques sans fil utilisant des technologies hertziennes.

Zoom (optique) : objectif sur lequel la distance focale est modifiable en continu. Une caméra équipée d'un zoom permet de restreindre ou d'augmenter le champ (optique) visible sur la vidéo enregistrée sans modifier la résolution de la vidéo.

Paris, le 1 er juillet 2008

L'arrêté du 3 août 2007 relatif aux normes applicables et son annexe technique aux projets de vidéosurveillance à partir du 21 août 2009, ont paru à certains interlocuteurs de l'Administrations – installateurs ou organismes qui veulent installer de la vidéo – poser problème de clarté.

Un groupe de travail composé de représentants des services techniques et de ces professionnels a donc préparé une notice explicative qui a été soumise au Comité de pilotage de la vidéosurveillance.

Vous en trouverez le texte ci-après. Nous pensons qu'elle est de nature à faciliter la compréhension tant des demandeurs que des services techniques instructeurs et donc à calmer de légitimes inquiétudes et vous pouvez bien sûr vous y référer.

Si vous aviez des observations à formuler nous vous en serions reconnaissants de bien vouloir le faire dans la rubrique de questions réponses du présent site.

Merci.

Philippe MELCHIOR
Président du Comité de pilotage
stratégique du plan de développement de
la vidéosurveillance

Note explicative de l'arrêté du 3 août portant définition des normes techniques en matière de vidéosurveillance

La présente note a pour objet de préciser le domaine d'application de l'arrêté du 3 août 2007 publié au JO du 21 août 2007 ainsi que ses objectifs, et d'en expliciter les quelques termes qui posent une difficulté d'interprétation.
Ces précisions viennent en complément des annexes techniques publiées au JO le 25 août 2007 qui permettent d'interpréter l'ensemble des points abordés dans l'arrêté.

1. Champ d'application et objectifs de l'arrêté.

1.1. Les systèmes concernés.

Il y a lieu de tenir compte du régime juridique auquel sont soumis les dispositifs de vidéosurveillance et de leur date d'installation.

1.1.1. La vidéosurveillance soumise au régime juridique de la loi du 21 janvier 1995.

Les normes techniques définies par l'arrêté du 3 août 2007 s'appliquent aux systèmes de vidéosurveillance installés dans le cadre des articles 10 et 10-1 de la loi du 21 janvier 1995. Sont donc concernés les caméras et dispositifs d'enregistrement mis en œuvre :

- sur la voie publique,
  - par une autorité publique compétente, pour l'une des **6 finalités** prévues par la loi (**protection** des bâtiments et installations publics et de leurs abords, **sauvegarde** des installations utiles à la défense nationale, **régulation** du trafic routier, **constatation** des infractions aux règles de la circulation, **prévention** des atteintes à la sécurité des personnes et des biens dans des

lieux particulièrement exposés à des risques d'agression et de vol, **prévention** d'actes de terrorisme dans des lieux susceptibles d'être exposés),

- par une personne morale, pour la protection des abords immédiats de ses bâtiments, dans les lieux susceptibles d'être exposés à des actes de terrorisme

- par une autorité publique compétente mais aussi par une personne physique ou une personne morale de droit privé, dans les lieux ouverts au public particulièrement exposés aux risques d'agression et de vol, ou lorsqu'ils sont susceptibles d'êtres exposés à un risque terroriste.

1.1.2. Une mise en conformité dans un délai de deux ans.

Aux termes de l'article 10 modifié de la loi du 21 janvier 1995, les systèmes installés devront être conformes aux prescriptions de l'arrêté portant normes techniques dans un délai de deux ans après sa publication. Celle-ci étant intervenue dans le Journal Officiel du 21 et du 25 août 2007, les dispositifs devront être mis en conformité au plus tard le 26 août 2009. Ceci signifie que ceux qui sont actuellement installés devront évoluer dans cet intervalle, alors que ceux qui font l'objet d'une demande d'autorisation doivent d'ores et déjà se soumettre à cette réglementation. Néanmoins, il convient de préciser que la mise en conformité s'appréciera différemment selon qu'il s'agisse d'un complément de caméras sur une installation existante, d'un complément du système de gestion et de stockage ou d'un nouveau système complet de vidéos intégrés. Lorsque la demande porte sur un complément de caméras la conformité aux normes de l'arrêté du 3 août n'est exigible que pour ce complément dans le cadre de cette demande, tandis que le reste du dispositif déjà en place devra être mis en conformité au plus tard le 26 août 2009.

1.2. Les objectifs de l'arrêté.

Si le législateur a souhaité encourager le développement de la vidéosurveillance dans la lutte contre le terrorisme, il lui est apparu qu'il fallait dans le même temps veiller à la qualité des installations afin de permettre aux forces de sécurité intérieure de les exploiter dans de bonnes conditions. En effet, il n'est pas rare, lorsque les policiers ou les gendarmes souhaitent visualiser les images dans le cadre de leurs enquêtes, que les dispositifs soient obsolètes, que la qualité des images soit médiocre voire inexistante. Cela peut s'expliquer par la mauvaise qualité des dispositifs, le fait qu'ils soient devenus obsolètes, par le manque d'entretien régulier ou le fait que la conservation des images soit faite dans de très mauvaises conditions ou encore que leur exportation soit irréalisable.

L'arrêté du 3 août 2007 détermine un certain nombre de contraintes minimales auxquelles doivent désormais obéir les systèmes installés afin de fournir aux services de police et de gendarmerie :

- des caméras proposant des images ayant une qualité suffisante et nécessaire pour l'exercice de leurs attributions,

- des conditions d'exploitation des images aisées.

C'est ainsi que les normes qui ont été définies portent sur

- La prise d'image (qui doit être adaptée à l'environnement)
- La transmission (qui doit permettre l'acheminement des images depuis la caméra vers l'unité de stockage et/ou de visualisation)
- L'enregistrement des images (qui doit garantir une qualité minimale des images enregistrées et la traçabilité de certaines actions)

- L'exportation aux services de sécurité (qui doit permettre aux services de relire les vidéos sans dégradation de qualité)
- La cohérence globale (Le système de vidéosurveillance doit permettre de répondre aux finalités pour lesquelles il a été mis en place)

Il s'agit de contraintes minimales. L'exploitant devra s'assurer que les exigences minimales de l'arrêté soient satisfaites durant toute la durée de service de l'installation. Il n'est donc pas interdit à un exploitant d'un dispositif de vidéosurveillance d'installer des matériels qui ont des caractéristiques supérieures à celles définies dans le règlement.

1.3. Sécurité des réseaux

Les réseaux visés par les exigences sont ceux par lesquels transitent les flux vidéo numérisés.

L'arrêté pose des principes sur la prise en compte des critères d'intégrité, de confidentialité et de disponibilité que la sécurité des réseaux doit apporter aux flux vidéo transportés mais il n'impose pas de certificats formels ni de chiffrement systématique du flux. La locution "garantie d'intégrité" ne doit donc pas être comprise comme "absolue garantie d'intégrité, …", notion qui dans certains contextes n'a pas de sens puisqu'elle ne peut être mise en œuvre. L'arrêté ne fixe donc pas un niveau de sécurité générique pour ces trois critères.

Ces solutions peuvent aller d'une simple protection du cheminement des câbles dédiés avec protection mécanique des tronçons vulnérables dans des réseaux non accessibles au public; à la mise en œuvre de mécanisme de chiffrement, de contrôle d'accès sur des réseaux publics, privés mutualisés, utilisant des technologies sans fil (RLAN), de type CPL, opérant sur un réseau "ouvert"; à la mise en œuvre de techniques de type Réseau Privé Virtuel sur des réseaux publics ou réseaux privés mutualisés, à l'utilisation de réseaux d'opérateurs garantissant intégrité et confidentialité des données (VPN, MPLS…)…

Les solutions techniques qui permettent d'adresser le niveau d'exigence pour ces 3 critères dépendent du système et du contexte d'installation : ainsi, dans les établissements ouverts au public, lorsque les liaisons entre les caméras et les systèmes d'enregistrement sont dédiées et protégées mécaniquement sur les tronçons vulnérables (notamment les tronçons terminaux), la simple sécurisation des matériels d'enregistrement dans des locaux fermés à clés peut être considérée comme suffisante. Si un renvoi d'images à distance (hors site) est effectué pour l'exploitation, il faudra également prendre en compte ces 3 critères pour cette transmission hors site.

La disponibilité pourra être assurée par exemple par un temps de rétablissement compatible avec les objectifs fixés, par des tests réguliers de la capacité de transmission des flux vidéo...

D'une manière générale, il convient que le dossier de demande d'autorisation permette de s'assurer que les critères d'intégrité, de confidentialité et de disponibilité des flux vidéo transportés ont été pris en compte et que les solutions mises en œuvre adressent ces trois sujets dans le contexte spécifique de la demande.

1.4.Paramètres de localisation des vidéos et garantie de ces paramètres et des vidéos

Il est précisé dans l'arrêté que les paramètres de date et de localisation doivent être "accessibles"… et que ces paramètres "doivent être exacts". Cette notion implique que le système doit faire l'objet d'une procédure automatique ou manuelle, régulière (hebdomadaire, mensuel…) qui permettent de vérifier que les paramètres sont exacts. (Vérification de la date par un opérateur, ou par une mise à jour automatique de l'horloge, vérification de la position des caméras sur le système/dispositif par rapport à la position réelle des caméras…)

Dans l'arrêté il est précisé que la mise en place de mécanisme de "marquage numérique" n'est pas obligatoire et que des mesures plus simples peuvent être envisagées. En particulier, la sauvegarde de la traçabilité des actions réalisées sur le système dans un fichier, ou via un protocole bien sécurisé peut être considérée comme une mesure suffisante.

Ceci ne préjuge pas de la valeur probante que pourront avoir les images en cas d'enquête judiciaire. Il appartiendra au juge de décider si les images peuvent être utilisées dans le cadre d'une telle procédure.

1.5. Traçabilité des actions réalisées sur les flux vidéo et les images enregistrées

L'arrêté pose les principes permettant le contrôle à postériori des actions effectuées sur les images.

Pour cela, il doit être possible de consulter un journal des principales actions effectuées contenant au minimum l'historique des opérations de modifications, suppressions et d'exportations d'enregistrements. Pour les opérations d'exportation, il est rappelé que le journal doit impérativement déterminer et indiquer la liste des fichiers exportés, ainsi que la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation.

Le journal devra être sous forme électronique pour les systèmes numériques et pourra être tenu à la main pour les systèmes de vidéosurveillance de moins de huit caméras (que les enregistreurs soient analogiques ou numériques).

Cette notion rejoint et complète celle de la nécessaire tenue d'un registre mentionnant les enregistrements réalisés, la date de destruction des images et le cas échéant, la date de leur transmission au parquet mentionné dans l'article 13 du décret N°96-926 du 17 octobre 1996. La tenue manuelle d'un tel registre n'est plus nécessaire en cas de journal électronique reprenant les mêmes informations.

1.6. Support d'extraction des données

L'arrêté exige que le système d'enregistrement puisse au minimum[1] exporter les données sur un support non réinscriptible, le plus souvent de type CDROM ou DVDROM et prévoit, dans les cas de volumes important de données à exporter, la possibilité d'utiliser des disques durs utilisant une connectique « standard ».

Il convient de préciser que cette possibilité n'est pas une obligation et qu'actuellement, les connectiques de type USB, IEE 1394A ou IEE 1394 B, RJ45 peuvent être considérées comme *standard* dans la mesure ou elles équipent par défaut la majorité des ordinateurs du marché. La connectique série (RS 232) qui fut standard dans les années 90, ne peut en revanche plus être considérée comme telle de nos jours. Cet élément est donc laissé à l'appréciation de l'expertise et doit avant tout permettre de s'affranchir des connectiques qui seraient trop rares. Cette notion de « standard » pourra donc évoluer avec les technologies.

Dans le même esprit, pour la compression, certaines implémentations des normes MJPEG, MPEG 2, ou MPEG 4 peuvent être considérées comme standard dans la mesure où elles sont largement diffusées sur Internet et libres de droits. Celles-ci ne nécessitent donc pas la fourniture par le déclarant d'un logiciel de lecture. A contrario, pour un système de type ondelettes propriétaire ou d'implémentation propriétaire ou peu diffusée, il convient que le déclarant prévoit la fourniture d'un logiciel au profit de la police pour que les données puissent être exploitées. A titre d'illustration, les fichiers qui peuvent êtres visionnés par des logiciels libres de droits et largement diffusés de type "VLC", "Média Player Classic" et autres n'ont pas besoin d'être fournis avec un logiciel de lecture spécifique.

[1] Il n'est donc pas interdit de réaliser des exportations sur clés USB, cependant ce support ne peut être le seul support d'exportation disponible.

1.7.Annexe 2: Tableau d'exemples

Il est important de rappeler que le tableau de l'annexe 2 de l'arrêté du 3 aout 2007 n'est qu'un tableau reprenant quelques exemples caractéristiques de situation et non pas universels. Ce tableau n'a pas pour objectif de définir la spécification technique pour chaque cas bien précis. Il est bien entendu que les exemples évoqués dans le tableau ne sont que des exemples, et non des règles, et que certains cas opérationnels peuvent donc aller à l'encontre du tableau. Il faut toujours rappeler que la classification plan large/plan étroit dépend de l'objectif fixé à la caméra et ceci indépendamment de son lieu d'implantation.

1.8.Erreur de frappe dans les annexes techniques de l’arrêté du 3 août 2007.

Les termes "circulaires" apparaissent à tort à la première page de l’annexe technique 1 et dernière page de l’annexe technique 3.

Les termes "arrêté du 26 septembre 2006" apparaissent aux pages 3 (3.le stockage), 4, 5 (4.Les contraintes d’interopérabilité). Il s’agit bien de l’arrêté du 3 août 2007.

Erreur de frappe dans l’annexe technique 2 "caméra de surveillance d’un comptoir ou d’un guichet" :

Il est écrit :

Caméra de surveillance d’un comptoir ou d’un guichet	4 CIF	6	Plan large

Il faut lire

Caméra de surveillance d’un comptoir ou d’un guichet	4 CIF*	6	Plan étroit

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR

cerfa
N° 13806*01

DEMANDE D'AUTORISATION D'UN SYSTÈME DE VIDÉOSURVEILLANCE

Loi n° 95-73 du 21 janvier 1995 - Article 10 - Décret n° 96-926 du 17 octobre 1996

Veuillez indiquer dans la case ci après le numéro du département de la préfecture compétente (il s'agit du département dans lequel vous souhaitez installer votre système de vidéosurveillance sauf s'il s'agit d'un système en réseau couvrant plusieurs départements auquel cas vous devez saisir la préfecture du département où est installé le siège social).

PARTIE RESERVEE A L'ADMINISTRATION

DATE D'ARRIVEE :
RECEPISSE DELIVRE LE :
DATE DE LA DECISION :

1 - NATURE DE LA DEMANDE

☐ Demande d'autorisation d'un nouveau système

☐ Modification d'un système autorisé — **N° de dossier**

☐ Demande de renouvellement d'un système autorisé — **N° de dossier**

2 - IDENTITE DU DECLARANT

Nom de naissance :.....
Prénom :.....
Dénomination de la collectivité territoriale ou la raison sociale de l'établissement ou de l'entreprise :.....
Eventuellement nom usuel ou sigle (si différent de la raison sociale).....
Activité :.....
.....
Adresse : Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie
....
Code postal :..... Commune :.....
Téléphone :..... Télécopie :.....
Adresse électronique du déclarant ou le cas échéant de la société, de l'établissement ou de la collectivité :
.....

3 - INFORMATIONS GENERALES ET FINALITE DU SYSTÈME DE VIDEOSURVEILLANCE

a) Informations générales

Horaires d'ouverture (pour les établissements ouverts au public) : .....

A préciser le cas échéant, (descriptions des éventuelles agressions survenues ou risques à prendre en compte) :
.....

b) Finalité du système : (veuillez cocher la ou les cases correspondantes)

☐ Sécurité des personnes
☐ Protection Incendie/Accidents
☐ Défense nationale
☐ Prévention des atteintes aux biens
☐ Protection des bâtiments publics
☐ Régulation du trafic routier
☐ Lutte contre la démarque inconnue
☐ Autres (préciser).....
.....

4 - LOCALISATION DU SYSTÈME DE VIDEOSURVEILLANCE (Veuillez renseigner uniquement une des deux rubriques ci-dessous)

4-1) LIEU D'INSTALLATION ET NOMBRE DE CAMERAS (cette rubrique n'est pas à renseigner pour les demandes portant sur un périmètre vidéo-surveillé, dans ce cas vous ne devez renseigner que la rubrique 4-2)

Adresse : Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie Code postal Commune
....

Nombre de caméras intérieures installées :.....
joindre le cas échéant le plan de détail et plan de masse (cf notice)

Nombre de caméras extérieures installées :.....
joindre le cas échéant le plan de détail et plan de masse (cf notice)

Pour les systèmes de moins de 8 caméras installées à l'intérieur d'un établissement ouvert au public, veuillez indiquer ci après la superficie de l'établissement : m2

4-2) DEMANDE PORTANT SUR UN PERIMETRE VIDEOSURVEILLE (cette rubrique ne doit être renseignée que si vous souhaitez avoir recours à la notion de périmètre vidéosurveillé)

Si au moins une des caméras que vous souhaitez installer doit visualiser la voie publique, veuillez cocher la case ci-après ☐

Délimitation du périmètre : pour délimiter ce périmètre, veuillez indiquer ci-après les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre

Adresse : Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie Code postal Commune
....
....
....
....
....
....
....
....

5 - CARACTERISTIQUES DU SYSTÈME

Délai de conservation des images (exprimé en jours) : ☐☐ ***(Indiquez un nombre compris entre 0 et 30)***
(la durée maximale est de 30 jours)

Existence d'un système de retransmission des images : ☐ oui ☐ non
si oui, veuillez cocher la case correspondante ci-dessous
Retransmission en temps réel : ☐
Retransmission en temps différé : ☐

Le système de vidéoprotection est-il mis en place par un installateur certifié ? ☐ oui ☐ non
si oui, veuillez indiquer ci-dessous le nom de cet installateur ou de cette société d'installation ainsi que son numéro de certification.

Nom de l'installateur ou de la société : …… Numéro de certification……..
Cet installateur vous a-t-il remis une attestation de conformité aux normes techniques définies par l'arrêté du 3 août 2007 ? ☐ oui ☐ non

Si l'installateur n'est pas certifié, veuillez joindre un questionnaire précisant les caractéristiques techniques du dispositif et sa conformité aux normes techniques définies par l'arrêté du 3 août 2007***(cf notice).***

6 - PERSONNES HABILITEES A ACCEDER AUX IMAGES :

NOM : ..... prénom : ..... Fonctions : .....
NOM : ..... prénom : ..... Fonctions : .....
NOM : ..... prénom : ..... Fonctions : .....
NOM : ..... prénom : ..... Fonctions : .....
si plus de quatre personnes, vous pouvez adresser (par courrier ou sous forme électronique) une liste complémentaire.

7 - TRAITEMENT DES IMAGES (cette rubrique n'est à renseigner que si les images font l'objet d'un traitement dans un lieu différent de celui de l'implantation du système et/ou par une personne autre que le responsable du système)

Adresse du lieu de traitement à renseigner ci-après :

Numéro de voie	Extension (bis, ter...)	Type de voie (rue, av...)	Nom de la voie	Code postal	Commune
.....	.....	.....	.....	.....	.....

Si ce traitement est effectué par un service, veuillez indiquer ci après le nom du service : .....
Si ce traitement est effectué par une personne, veuillez indiquer ci-après ses noms et prénoms : .....

8 - SECURITE ET CONFIDENTIALITE
(nous vous remercions de décrire ci-dessous les mesures adoptées pour assurer la confidentialité des images)

Mesures prises pour contrôler l'accès au poste central de surveillance (par exemple code d'accès, porte blindée, accès contrôlé...) :
.....

Si existence d'un système d'enregistrement :

Mesures pour la sauvegarde et la protection de ces enregistrements : .....
.....

Modalités de destructions des enregistrements : .....
.....

9 - MODALITES D'INFORMATION DU PUBLIC

Veuillez indiquer ci après le nombre d'affiches ou de pannonceaux d'information (cf notice) : .....
Précisez la (ou les) localisation(s) de cet affichage : .....

10 - SERVICE (OU PERSONNE) AUPRES DUQUEL S'EXERCE LE DROIT D'ACCES

Nom : ..... Prénom : ..... Fonction de cette personne : .....

ou service responsable : .....
Veuillez renseigner ci-après l'adresse de cette personne ou de ce service :

Numéro de voie	Extension (bis, ter...)	Type de voie (rue, av...)	Nom de la voie	Code postal	Commune
.....	.....	.....	.....	.....	.....

Fonction habilitant le déclarant à signer : .....
Le signataire s'engage à se conformer aux dispositions de l'article 10 de la loi n°95-73 du 21 janvier 1995 relatives à la vidéosurveillance.

SIGNATURE ET CACHET : Date : .....

Conformément aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le demandeur est informé que les renseignements qu'il doit fournir pour satisfaire sa demande font l'objet d'un traitement automatisé par la préfecture du lieu de dépôt de son dossier. Le droit d'accès et de rectification s'exercera auprès de cette préfecture.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR

cerfa
N° 51336#01

NOTICE D'INFORMATION

relative au formulaire CERFA n° 13806*01 de

Demande d'autorisation d'un système de vidéosurveillance

A) Informations générales

A-1) L'encadrement juridique :

L'usage de la vidéosurveillance est régi par **l'article 10 de la loi n° 95-73 du 21 janvier 1995 modifiée,** et par son décret d'application **n° 96-926 du 17 octobre 1996 modifié.** Les conditions d'application de ces textes sont explicitées par les circulaires : **INTD9600124C du 22 octobre 1996, INTD0600096C du 26 octobre 2006 et INTK0930018J du 2 février 2009.**

Dans les lieux privatifs ou les locaux à usage exclusivement professionnel qui n'accueillent pas de public au sens de la loi, la réglementation de la vidéosurveillance mentionnée ci-dessus n'est pas applicable. La mise en place éventuelle de caméras doit cependant s'effectuer dans le respect de la vie privée et sans visionner la voie publique.

Ce sont alors les règles générales du code civil sur le droit à l'image (article 9) ou des réglementations particulières, telle que celle du code du travail **(3ème alinéa de l'article L. 2223-32 et articles L. 1222-4 et L.1221-9)** qui s'appliquent.

L'article 226-1 du code pénal punit d'un an d'emprisonnement et de 45 000 € d'amende toute personne ayant volontairement porté atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant l'image d'une personne se trouvant dans un lieu privé, c'est-à-dire, selon la jurisprudence, un lieu qui n'est ouvert à personne sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire.

Dans les cas très rares où le système de vidéosurveillance est relié à un traitement de données automatisées (fichier de données à caractère personnel), c'est la loi « informatique et libertés » n°78-17 du 6 janvier 1978 qui est applicable. Dans ce cas précis, vous devez adresser une déclaration spécifique à la CNIL. (En cas de doute n'hésitez pas à poser votre question à l'adresse ci-après, une réponse vous sera adressée en retour dans les 10 jours : videoprotection@interieur.gouv.fr. Vous pouvez également prendre contact avec l'accueil de la préfecture qui instruira votre demande).

A-2) Dans quels cas devez vous déposer une demande d'autorisation ?

➢ *DANS LE CAS D'UN SYSTÈME VISÉ PAR LA LOI INSTALLÉ EN VOIE PUBLIQUE OU DANS UN LIEU OU UN ÉTABLISSEMENT OUVERT AU PUBLIC :*

1) Quel système est visé par la loi ?

Il y a vidéosurveillance toutes les fois que sont mis en œuvre au moins une caméra et un moniteur, c'est-à-dire un écran permettant la visualisation des images, même s'ils ne sont pas situés dans le même local, et lorsque les caméras, fixes ou mobiles, fonctionnent de manière permanente ou non, prennent des images, éventuellement de manière séquentielle ou aléatoire, qui peuvent être visionnées, en temps réel ou en différé, sur place ou dans un lieu distant, sur un écran de type télévision ou sur un écran d'ordinateur.

Ainsi, la prise de photographies n'est pas un système de vidéosurveillance et ce, quelque soit la technique utilisée (appareil numérique). Par contre, un dispositif dans lequel des images sont enregistrées à l'occasion d'une intrusion ayant déclenché le fonctionnement de caméras, dans un poste de contrôle éloigné, correspond bien à la définition de la vidéosurveillance. Dans ce cas, le dispositif participe en outre des activités dites de télésurveillance régies par la loi n°83-629 du 12 juillet 1983.

La loi ne se prononce pas sur la technologie utilisée. Elle définit seulement les principales modalités de fonctionnement des systèmes et fixe des normes techniques (par arrêté du 3 août 2007- annexes techniques publiées au JO du 25 août 2007). Cette absence de détermination précise des caractéristiques des dispositifs de vidéosurveillance a permis d'accompagner le développement des nouvelles technologies et d'appliquer la réglementation à des cas auxquels le législateur ne pouvait penser en 1995 (ex : utilisation des webcam).

Ainsi, les systèmes de vidéosurveillance numériques dont les images sont transmises par internet et consultées, à distance, par les personnes responsables du système entrent dans le champ de la loi du 21 janvier 1995. Le procédé numérique doit permettre le respect des garanties imposées par la loi.

Par contre, la diffusion sur internet d'images issues de webcams ne constituent pas un dispositif de vidéosurveillance car il n'y a pas visionnage des images sur un écran appartenant au propriétaire de la webcam mais transmission directe sur internet.

2) Les lieux visés par la Loi :

L'article 10 de la loi du 21 janvier 1995 détermine les lieux dans lesquels un dispositif de vidéosurveillance peut être installé. Il s'agit de :

- L'intérieur des **lieux et établissements ouverts au public ;**
- La **voie publique** limitée géographiquement :
- Aux abords des bâtiments et installations publics ;
- Aux abords immédiats des bâtiments et installations appartenant à des personnes physiques ou morales de droit privé en cas de risque d'attentat terroriste ;
- Aux voies de circulation routière.

Concernant la voie publique, la vidéosurveillance peut être mise en œuvre :

- Par une personne publique pour assurer soit la protection des bâtiments et installations publics et leurs abords, soit la sauvegarde des installations utiles à la défense nationale, soit la régulation du trafic routier et la constatation des infractions aux règles de la circulation, soit la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agressions ou de vols, soit la prévention d'actes de terrorisme (alinéas 1 et 2 du II de l'article 10) ;

- Par une personne physique ou morale de droit privé pour visionner les abords immédiats de ses bâtiments ou installations (alinéa 2 du II de l'article 10) au titre de la finalité de prévention d'actes de terrorisme ;

- Dans certains lieux revêtant une dimension ou une complexité particulières, le préfet peut autoriser qu'un périmètre de voie publique ou compris dans un établissement ou un lieu ouvert au public puisse être vidéosurveillé, dans les limites et le cadre des finalités imposées par la loi. Cette notion répond à une nécessité opérationnelle d'adaptation de la vidéosurveillance puisqu'elle recouvre l'espace susceptible d'être situé dans le champ d'une ou plusieurs caméras.

Sont visées par la notion d'ensemble immobilier ou foncier complexe les lieux ouverts au public dans des zones à forte concentration urbaine ou touristique ou dont la configuration géographique et architecturale rend difficile l'intervention des services de sécurité ou de secours mais également dans des zones utilisées dans le cadre de manifestations exceptionnelles. Pourraient entrer dans ce champ, à titre d'exemple : la place de la Concorde, une cité composée de plusieurs immeubles à usage d'habitation, une zone rurale utilisée dans le cadre d'une manifestation d'une ampleur exceptionnelle, comme une rave-party.

A-3) Quels documents devez-vous joindre à votre demande et dans quels cas ?

1) Les documents constitutifs d'une demande d'autorisation :

*L'ensemble des documents décrits ci-dessous ne sont pas exigibles dans tous les cas. Veuillez vous reporter au **2**) afin d'identifier précisément la nature de votre demande.*

- Le formulaire CERFA n° 13806*01 complété ;

- Le rapport de présentation : il s'agit d'un rapport spécial expliquant les finalités du projet au regard des objectifs définis par la loi et les techniques mises en œuvre, eu égard à la nature de l'activité exercée, aux risques d'agression ou de vol présentés par le lieu ou l'établissement à protéger ;

- Le plan de masse : Il s'agit d'un plan des lieux montrant les bâtiments du demandeur et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures ;

- Le plan de détail : Il s'agit d'un plan à une échelle suffisante montrant le nombre, le positionnement des caméras ainsi que les zones couvertes par celles-ci ;

- Un plan du périmètre : Il s'agit d'un document qui peut se substituer au plan de détails et au plan de masse, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras dans le cas d'une demande portant sur un périmètre à vidéosurveiller ;

- La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images : théoriquement ces informations sont indiquées dans les parties 5,7 et 8 du formulaire mais en cas de dispositif élaboré notamment en cas de traitement par une société extérieure, un document expliquant le fonctionnement du système peut-être demandé.

- La désignation des personnes susceptibles d'accéder aux images (rubrique 6 du formulaire) : il s'agit de toute personne habilitée par le responsable à accéder aux images et donc susceptible de les visionner (il peut s'agir bien sûr du responsable lui-même mais aussi du technicien de maintenance par exemple). **Ce n'est que dans l'hypothèse où plus de 4 personnes sont habilitées à accéder aux images qu'il convient de joindre une liste complémentaire au formulaire de demande.**

- Modèle de l'affiche ou du panonceau d'information du public : les panonceaux destinés à informer d'un système sur la voie publique doivent comporter un pictogramme (dessin) représentant une caméra. Si les affiches ou panonceaux sont placés dans les lieux et établissements ouverts au public, le nom ou la qualité, ainsi que le numéro de téléphone du responsable auprès duquel toute personne intéressée peut s'adresser pour exercer son droit d'accès doivent y figurer.

Attestation de la conformité du système aux normes techniques définies par l'arrêté du 3 août 2007 : deux cas de figure se présentent. En fonction de l'installateur auquel vous aurez recouru vous devrez produire un des documents prévus à cet effet :

1) Si vous avez fait appel à un installateur certifié : une attestation de conformité établie par ce dernier suffit.

2) Si votre installateur n'est pas certifié : il vous faut produire un questionnaire précisant les caractéristiques techniques du dispositif et sa conformité aux normes techniques (voir modèle joint en Annexe 1).

2) Les documents à fournir en fonction des différents cas suivants :

Vidéosurveillance de la voie publique avec désignation du nombre de caméras : vous devez joindre à votre dossier tous les documents énumérés en **1**) (sauf le plan du périmètre qui ne concerne que les cas de vidéosurveillance d'un périmètre).

Vidéosurveillance d'un périmètre (en voie publique ou dans un lieu ouvert au public) : le formulaire CERFA n° 13806*01 complété, le rapport de présentation, le modèle d'affiche et/ou de panonceau d'information du public, le plan du périmètre, le justificatif de la conformité aux normes techniques (attestation de conformité par un installateur certifié ou questionnaire dans l'autre cas), description du dispositif (dans ce cas de figure ce descriptif sera limité aux techniques employées et aux modes de visionnage et d'exploitation des images **le nombre de caméras et leur emplacement n'auront pas à être indiqués)**. Eventuellement la liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéosurveillance dans un lieu ou un établissement ouvert au public et 7 caméras maximum : le dossier dans ce cas est très simplifié : le formulaire CERFA n° 13806*01 complété, l'affiche d'information et le justificatif de conformité si l'installateur n'est pas certifié (si vous avez fait appel à un installateur certifié, vous devez pouvoir produire son attestation en cas de contrôle mais n'êtes pas obligé de la transmettre dans le cas où vous effectuez votre déclaration par téléprocédure), éventuellement liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéosurveillance dans un lieu ou un établissement ouvert au public et 8 caméras minimum : le formulaire CERFA n° 13806*01 complété, le rapport de présentation, le plan de détail, l'affiche d'information du public et le justificatif de conformité, éventuellement la liste complémentaire des personnes habilitées à accéder aux images si la rubrique 6 du formulaire ne suffit pas.

A-4) A qui devez-vous adresser votre dossier ?

A la préfecture du département dans lequel vous souhaitez installer le dispositif (par exemple pour une société dont le déclarant est à Paris mais qui veut installer un dispositif dans une de ses succursales située en Gironde, il faut adresser votre déclaration à la préfecture de Bordeaux). Dans le cas d'un dispositif qui concernerait plusieurs départements (exemple : réseau autoroutier), le dossier doit être déposé à la préfecture du siège de l'établissement demandeur.

Ce dossier peut être transmis soit sous forme papier par voie postale ou déposé à l'accueil de la préfecture compétente, soit par téléprocédure disponible sur le site «videoprotection.interieur.gouv.fr» qui propose par ailleurs un ensemble d'informations ou d'actualités sur le sujet de la vidéo protection.

B) Comment remplir le formulaire de demande d'autorisation ?

Vous devez indiquer le numéro du département où se trouve la préfecture compétente en complétant par trois chiffres la case prévue à cet effet en haut du formulaire CERFA. (par exemple pour PARIS renseigner 075, pour Marseille indiquer 013.).

Rubrique 1 - Nature de la demande

Veuillez cocher obligatoirement une des trois cases proposées correspondant à la nature de votre demande (par exemple s'il s'agit d'une première demande vous cocherez «demande initiale»).

En cas de demande de modification d'un dispositif existant ou de demande de renouvellement, préciser le numéro de dossier sous lequel il a été enregistré dans la partie prévue à cet effet.

La modification peut concerner par exemple l'augmentation du nombre de caméras ou la localisation de celles-ci, sauf si l'autorisation obtenue portait sur un périmètre vidéosurveillé, Dans ce dernier cas vous devez simplement déclarer au préfet compétent soit par courrier soit par téléprocédure (sur le site «vidéoprotection.interieur.gouv.fr» à la rubrique «TELE-VIDEOPROTECTION» dans le menu «déclaration de mise en service») le nouveau positionnement de vos caméras. Si vous souhaitez, en revanche, modifier la définition du périmètre (changement de l'environnement de celui-ci), vous devez adresser une demande de modification complétée des documents nécessaires.

Rubriques 2 et 10 Identité et fonction du déclarant

L'autorisation de mise en œuvre d'un système de vidéosurveillance est délivrée à la personne responsable du système, c'est-à-dire à celle qui, ayant la capacité juridique pour ce faire, estime nécessaire de recourir à la vidéosurveillance. L'obligation de déclaration des systèmes entrant dans le champ d'application de la loi du 21 janvier 1995 incombe à l'exploitant des lieux où sont installées les caméras, qu'il soit ou non le propriétaire des lieux et même lorsque le système de vidéosurveillance n'est installé que pour une durée limitée. Le responsable n'est donc pas l'installateur.

Vous devez par conséquent impérativement compléter les informations relatives au nom, prénom et fonction du déclarant (la fonction se trouve à la rubrique 10 en fin de formulaire). **(Si par la suite, le responsable du système change, par exemple suite à une mutation ou un départ à la retraite, il faudra en aviser la préfecture, dans certains cas ce changement peut nécessiter une nouvelle demande d'autorisation, la préfecture vous le précisera).**

Vous devez ensuite renseigner la dénomination (il peut s'agir d'une collectivité exemple : commune de XXX, d'une entreprise exemple : – SARL XXX- , d'un établissement privé ou public exemple : bibliothèque municipale de XXX ; ou institut XXX)

S'il existe un nom usuel différent de ce que vous avez indiqué, il est recommandé de l'indiquer à la ligne suivante qui reste une information facultative.

Concernant l'activité, elle doit être impérativement renseignée si la demande concerne une entreprise ou un lieu ouvert au public (exemple : musée, commerce de vêtements…).

Vous complèterez ensuite l'adresse de la collectivité, de l'établissement ou de l'entreprise (vous devez renseigner le plus précisément possible cette adresse en complétant toutes les rubriques proposées).

L'adresse électronique reste facultative, il est conseillé toutefois de la mentionner afin de faciliter les échanges le cas échéant, entre l'administration et le demandeur.

Rubrique 3 - Informations générales et finalité(s) du système de vidéosurveillance

a) les informations générales :

Dans cette rubrique, vous devez compléter la partie relative aux horaires d'ouverture **sauf en cas de vidéosurveillance sur la voie publique.** (par exemple Si vous déposez un dossier pour un commerce cette information peut vous être réclamée en complément si vous ne la renseignez pas dès le départ).

De même, vous êtes invité à signaler les éventuelles agressions déjà survenues sur le lieu que vous souhaitez protéger ou les risques particuliers auxquels vous l'estimez exposé (délinquance de proximité, commerce recevant beaucoup de liquidités).

b) la ou les finalité(s) du système

Vous devez obligatoirement cocher au moins une des cases proposées et vous pouvez en cocher plusieurs, la finalité n'étant pas nécessairement unique. Si vous cochez la case «autre», vous devez préciser sur la ligne suivante le but que vous recherchez en installant un système de vidéosurveillance.

Rubrique 4 - Localisation du système de vidéosurveillance

Vous devez compléter soit la rubrique 4-1, soit la rubrique 4-2. En aucun cas vous ne pouvez compléter les deux rubriques en même temps (la rubrique 4-2 concerne uniquement les ensembles immobiliers ou fonciers de dimension importante ou complexes).

4-1 Lieu d'installation et nombre de caméras

Vous devez compléter le plus précisément possible l'adresse du lieu d'installation du dispositif (en cas d'installation sur la voie publique de plusieurs caméras réparties sur une certaine distance, veuillez indiquer au moins le nom de la voie).

Pour les dispositifs de 7 caméras maximum installées à l'intérieur d'un établissement, vous préciserez impérativement la superficie de cet espace intérieur.

4-2 Demande portant sur un périmètre

Il est possible, lorsque l'installation de vidéosurveillance est prévue sur un ensemble foncier ou immobilier de dimension importante ou complexe, de recourir à la notion de périmètre vidéo surveillé.

Cette formule présente l'avantage de vous dispenser du dépôt de demande de modification pour déplacer les caméras ou en augmenter le nombre à l'intérieur du périmètre.

Si vous souhaitez obtenir une autorisation au titre d'un périmètre vidéo surveillé, vous devez préciser les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre (par exemple si vous souhaitez une autorisation pour protéger une gare, vous préciserez à la rubrique 2 l'activité « gare » et indiquerez toutes les adresses permettant de délimiter le périmètre géographique dans lequel se trouve située cette gare).

Dans cette hypothèse c'est au moment où vous informerez le préfet de la mise en service des caméras que vous lui en préciserez la localisation.

Rubrique 5 - Caractéristiques du système

Vous devez préciser impérativement le nombre de jours pendant lesquels seront conservées les images. Ce chiffre (de 00 à 30 jours, délai de conservation maximum autorisé par la loi) sera reporté dans la case correspondante.

Vous devez répondre ensuite à la question «existence d'un système de retransmission». Si vous cochez non, vous pouvez passer à la question relative à l'installateur. Si vous répondez oui, vous devrez cocher obligatoirement une des deux cases suivantes : retransmission en temps réel ou retransmission en temps différé.

Vous devrez ensuite préciser en cochant la case correspondante si l'installateur auquel vous avez fait appel est certifié.

Si vous avez coché la case «oui» et que cet installateur est certifié par l'AFNOR-CNPP ou par un mécanisme de certification équivalent, Il faut mentionner le nom de cet installateur (ou de cette société d'installation) et son numéro de certification. Vous devez également répondre à la question suivante en cochant «oui» ou «non». Si l'installateur vous a remis une attestation, vous n'êtes pas obligé de la joindre à votre dossier (pour les dispositifs importants de plus de 7 caméras ou en voie publique, il est toutefois conseillé de la joindre ; pour les petits dispositifs hors voie publique de 7 caméras maximum, vous n'êtes pas obligé de joindre au dossier cette attestation mais elle peut vous être réclamée en cas de contrôle à posteriori).

Si l'installateur n'est pas certifié, vous joindrez au dossier le questionnaire (dont le modèle figure en annexe1) précisant les caractéristiques du système.

Rubrique 6 - Personnes habilitées à accéder aux images

Il s'agit de mentionner le nom et prénoms des personnes qui seront en charge de visionner les images ou qui peuvent y accéder (s'il s'agit du responsable-déclarant de la demande d'autorisation lui-même il convient de le préciser en réécrivant ses nom, prénoms et fonction qui devront dans ce cas correspondre aux informations contenues à la rubrique 2 et 10. De même, le ou les techniciens susceptibles d'intervenir sur le système au titre de la maintenance doivent être mentionnés dans cette liste. S'il y a plus de quatre personnes, il faut joindre une liste complémentaire).

En cas de modification de la liste des personnes habilitées, le signataire informera l'autorité préfectorale (soit par courrier, soit par «téléprocédure»).

Rubrique 7 - Traitement des images

Cette rubrique doit être renseignée dans le cas où les images font l'objet d'un traitement dans un lieu différent de celui de l'implantation des caméras et/ou par une personne autre que les responsables du système. Si ce n'est pas le cas, vous devez passer à la rubrique 8.

Rubrique 8 - Sécurité et confidentialité

La première ligne de cette rubrique doit impérativement être renseignée, il s'agit de décrire les mesures prises pour contrôler l'accès au poste central (code d'accès, porte blindée, badge d'accès, accès contrôlé).

Si vous avez coché la réponse «oui» à la question «existence d'un système d'enregistrement» en rubrique 5, vous devez répondre aux deux questions suivantes en décrivant 1) les mesures pour la sauvegarde et la protection des enregistrements (par exemple : armoire blindée) et 2) les modalités de destruction de ces enregistrements (par exemple : écrasement).

Rubrique 9 - Modalités d'information du public

Les textes en vigueur prévoyant l'obligation d'informer le public susceptible d'être filmé, vous préciserez les mesures prévues à cet effet.

Vous devez par conséquent compléter les deux lignes prévues dans cette rubrique.

Par ailleurs l'information sur l'existence d'un système de vidéosurveillance devant être apportée au moyen de panonceaux comportant un pictogramme représentant une caméra (dans les cas de vidéosurveillance sur la voie publique) et au moyen d'affiches ou de panonceaux (au choix en cas de vidéosurveillance dans un lieu ou établissement recevant du public), n'oubliez pas de joindre à votre dossier le modèle d'affiche ou de panonceau.

Rubrique 10 - Service (ou personne) auprès duquel s'exerce le droit d'accès

L'article 10 V (1er alinéa) de la loi n° 95-73 du 21 janvier 1995 modifiée dispose :

«Toute personne intéressée peut s'adresser au responsable d'un système de vidéosurveillance afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit. Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers.»

Il s'agit de préciser auprès de quelle personne ou de quel service doit s'adresser une personne ayant été filmée par le dispositif que vous souhaitez installer pour vérifier les images.

Il vous appartient par conséquent de renseigner cette rubrique en indiquant soit le nom, prénom et fonction de la personne auprès de laquelle s'exerce ce droit d'accès aux images, soit le nom du service.

Vous pouvez compléter éventuellement ces quatre informations (nom, prénom, fonction, service auquel appartient cette personne).

Vous indiquerez ensuite l'adresse de cette personne et/ou de ce service (cela peut être la même personne que le déclarant-responsable du système).

La signature du formulaire

Veuillez, une fois les rubriques complétées, indiquer la fonction du signataire-déclarant (rubrique 2 du formulaire, page 4 de la présente notice), dater votre document et le signer en apposant, le cas échéant le cachet de la collectivité, de l'établissement ou de l'entreprise.

Si vous effectuez votre déclaration par téléprocédure, vous compléterez simplement la mention relative à la fonction du déclarant.

Annexe 1

cerfa
N° 51336#01

Questionnaire de conformité d'un système de vidéosurveillance à l'arrêté du 3 aout 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

Je soussigné(e).....,
certifie par la présente que le système de vidéosurveillance pour lequel j'ai sollicité une autorisation en date du....., installé par (nom et adresse de l'installateur).....
est conforme aux dispositions de l'arrêté du 3 août 2007.

Fait à ……, le …….

Caractéristiques du système (veuillez cocher les cases appropriées) :

1 Caractéristiques générales :

a. Nombre de caméras :

❍ moins de 8 caméras ❍ 8 caméras ou plus

b. Mode de fonctionnement du système :

❍ Le système comporte des caméras à plan large (destinées à une compréhension des situations) et des caméras à plan étroit (susceptibles de permettre une reconnaissance des individus)
❍ Le système ne comporte que des caméras à plan large
❍ Le système ne comporte que des caméras à plan étroit

2 Mode d'enregistrement des images :

a. Le stockage des images est-il ?

Analogique ❍ Numérique ❍

b. Possibilité de déterminer la caméra ayant filmé une scène :

Possible sur les enregistrements eux mêmes ❍
Possible grâce à un journal ❍
Non prévu ❍

c. Existe-t-il un journal gardant la trace des opérations effectuées sur les flux vidéo (export, modification, suppression)

Oui, journal manuel ❍
Oui, journal généré automatiquement sous forme électronique ❍
Non ❍

3 Questions relatives à la qualité des images :

a. La résolution des images est-elle toujours supérieure ou égale à 4 CIF (704 x 576 pixels) et le nombre d'images supérieur ou égal à 12 images/s

❍ Oui ❍ Non

4 Transmission des images aux forces de police :

a. Les images peuvent-elles êtres exportées sans dégradation de leur qualité ?

Oui ❍ Non ❍

b. Dans le cas de systèmes numériques, si le format de codage des images n'est pas standard et libre de droits, le titulaire a-t-il prévu de fournir gratuitement à l'administration en cas de réquisition judiciaire, un système de lecture (ou une licence si le produit peut être installé « sur un PC standard) permettant de lire les enregistrements et d'effectuer les principales opérations de visualisation

Oui ❍ Non ❍

PR-51: Videoprotection

Moyens et données d'entrée	Technique : Réseau de 7 caméras « dôme » et 2 caméras fixes. 2 PC de surveillance.
Déclenchement	Surveillance des infrastructures portuaires 24h/24 et 7j/7.
Exécutants	Maîtres de port, agents portuaires, agents de sécurité.
Finalité	Aide à la gestion portuaire et sécurisation du site.
Contrôle	Maîtres de port. Accès aux images contrôlé. Autorisation préfectorale.

Matériel:

Le port est couvert par 9 caméras dont :

- 2 caméras A et B fixes, avec objectif grand angle et iris automatique sur un champ de vision de 4m sur 20m pour contrôler l'entrée principale du port et la capitainerie.
- 7 caméras « dôme » C1 à C6 pivotant à 380° avec objectif site azimut en une seconde, sur un champ de vision de 80m à 100m avec le masquage des zones non autorisées.

Les 9 caméras sont branchées sur un enregistreur numérique. 9 entrées vidéos sont reliés à un Joystick et 2 moniteurs à la capitainerie pour le personnel exploitation.
Un Joystick et 2 moniteurs au PC sécurité, au 2ème étage pour le personnel de sécurité la nuit.

Utilisation:

- Le système vidéo installé à l'entrée principale de la Capitainerie du port n'est accessible qu'aux agents portuaires, maîtres de port, agents de sécurité et Direction du port.
- Il est interdit d'utiliser les images à des fins personnelles et de divulguer la vision à toute autre personne.
- Le système fonctionne avec enregistrement des images autorisées et conservées avec un délai maximum de 26 jours (arrêté préfectoral du 30 juin 2009).
- La lecture des images antérieures est accessible avec un code d'accès que seuls le PDG et le Sous Directeur connaissent. La lecture et l'impression d'image antérieures ne peut se faire que suite à une requête de la gendarmerie ou de la police municipale.
- Des affichettes sont apposées aux principales entrées du port signalant que celui-ci est sous vidéo-protection.
- Une affichette par caméra est aussi apposée à proximité immédiate du support.

Gérez et sécurisez vos ports de plaisance avec les solutions Bosch

Vidéosurveillance

Contrôle d'accès

Sonorisation

Intrusion

Vos interlocuteurs

FRANCE

Christophe RAIX

christophe.raix@fr.bosch.com

0 825 12 8000

0.15 € TTC/min depuis un poste fixe

NORD

Roland TOURNOIS

roland.tournois@fr.bosch.com

06 11 18 79 75

NORMANDIE

Mathias DROUIN

mathias.drouin@fr.bosch.com

06 13 40 45 85

GRAND OUEST

Frederic AGLAOR

frederic.aglaor@fr.bosch.com

06 07 61 46 56

SUD-OUEST

Laurent GOURNIER

laurent.gournier@fr.bosch.com

06 07 61 39 25

SUD

Jean-claude ROSSAT

jean-claude.rossat@fr.bosch.com

06 07 61 46 48

www.boschsecurity.fr

BOSCH

Des technologies pour la vie