

Votre projet de vidéo protection Guide Méthodologique



P R E A M B U L E

Comité de Pilotage Stratégique pour le
développement de la vidéo protection

Introduction

Nous savons maintenant que, combinée avec d'autres solutions, la vidéo protection constitue un outil très utile pour la sécurité de nos concitoyens. C'est, bien sûr, pourquoi ceux-ci y sont aussi favorables.

Nous savons également, beaucoup mieux maintenant, à quelles conditions et dans quelles limites.

C'est pourquoi les ministres concernés (ministre de l'intérieur, bien sûr, mais aussi ministres en charge des transports, du logement et de la ville) ont voulu que ce guide méthodologique soit mis à la disposition des nombreux décideurs, collectivités territoriales, entreprises industrielles ou commerciales, transporteurs publics, organismes de logement, particuliers, afin que, ayant défini leur besoin, ils décident et mettent en œuvre, dans le cadre de la loi et le respect des règles déontologiques, les dispositifs humains et techniques qu'ils jugeront les plus appropriés.

Ce guide a été conçu avec l'aide d'un cabinet spécialisé, par des professionnels et soumis ensuite des utilisateurs sous l'égide du Comité de pilotage stratégique pour le développement de la vidéo protection. Il tente d'apporter des réponses à des situations diverses : un système de vidéo protection de plusieurs centaines de caméras sur la voie publique est par définition plus complexe à concevoir que celui d'un commerçant de détail. Il comprend donc des développements utiles à certains, inutiles à d'autres. Il tente surtout d'accompagner une réflexion puis des choix :

- Quel est mon besoin ?
- Quelle contribution la vidéo protection peut-elle apporter à la réponse ?
- Quels choix techniques, humains, organisationnels?
- A quel prix et avec quel financement ?

Tel qu'il est, ce guide est maintenant le vôtre. Aidez-nous à l'améliorer et à l'adapter à l'évolution des problématiques et des technologies.

Philippe MELCHIOR.

Président du comité de pilotage stratégique

Pour le développement de la vidéo protection

Sommaire

1 PREAMBULE.....	7
1.1 A QUI CE GUIDE EST-IL DESTINE ? COMMENT EST-IL ORGANISE ? COMMENT LIRE CE GUIDE ?	7
1.2. VIDEOSURVEILLANCE OU VIDEO PROTECTION ?	14
1.3. UN PRE REQUIS : LA VOLONTE DU DECIDEUR	14
1.4. LE MESSAGE ESSENTIEL A RETENIR DE CE PREAMBULE	15
2 UL 1 : LE DIAGNOSTIC DE SECURITE.....	17
2.1. COMMENT DEFINIR LE BESOIN DE SECURITE ?	17
2.1.1. <i>La protection d'un commerce</i>	17
2.1.2. <i>La protection d'un commerce dans sa rue</i>	18
2.1.3. <i>La rue dans la ville</i>	19
2.2. LE DIAGNOSTIC DE SECURITE.....	20
2.3. ENGAGER UN DIAGNOSTIC DANS UN CADRE PARTENARIAL	21
2.4. IDENTIFIER ET QUANTIFIER LES DIFFICULTES DE TERRAIN ET LA TYPOLOGIE DE LA DELINQUANCE	22
2.4.1. <i>Définir le périmètre à prendre en compte dans les milieux ouverts</i>	22
2.4.2. <i>Les outils du diagnostic</i>	23
2.4.3. <i>Comment utiliser Les données recueillies</i>	24
2.5. REALISER UN ETAT DES MOYENS EXISTANTS	25
2.6. DEFINIR UNE STRATEGIE GENERALE DE SURETE	26
2.7. SYNTHESE UL 1 : LES MESSAGES ESSENTIELS	27
3. UL 2 : LES FONCTIONNALITES PROPRES A LA VIDEOPROTECTION.....	28
3.1. A QUOI PEUT SERVIR LA VIDEO PROTECTION ?	28
3.2. COMMENT FONCTIONNE L'OUTIL ?	30
3.3. J'ADAPTE L'OUTIL A MES BESOINS DE SECURITE	31
3.3.1. <i>Les prealables</i>	31
3.3.2. <i>Le besoin détermine la qualité d'image</i>	32
3.3.3. <i>le besoin détermine le choix du reseau</i>	33
3.3.4. <i>Le besoin détermine le choix du mode d'exploitation</i>	33
3.3.5. <i>le besoin détermine les modalités du stockage</i>	35
3.4. SYNTHESE UL 2 : LES MESSAGES ESSENTIELS.....	36
4. UL 3 LA PROTECTION DES LIBERTES PUBLIQUES.....	37
4.1. LE REGIME JURIDIQUE DE LA VIDEO PROTECTION EN FRANCE ORGANISE QUATRE CAS DE FIGURE.....	37
4.2. LA VIDEO PROTECTION DE LA VOIE PUBLIQUE, D'UN LIEU OU D'UN ETABLISSEMENT OUVERT AU PUBLIC	37
4.2.1. <i>Pour quels systèmes faut-il une autorisation?</i>	38
4.2.2. <i>La compétence de la CNIL :</i>	39
4.2.3. <i>Dans quels lieux l'autorisation préfectorale est-elle nécessaire?</i>	39
4.2.4. <i>Qu'est ce qu'un lieu privé?</i>	41
4.2.5. <i>Dans quels cas les préfets peuvent-ils prescrire?</i>	42
4.2.6. <i>Dans quel cas la vidéo protection est-elle obligatoire?</i>	42

4.2.7.	Dans quel but peut-on installer de la vidéo protection ?	42
4.2.8.	Qui demande, qui visionne, qui a accès aux données?	44
4.2.9.	Quelle est la procédure d'instruction des demandes d'autorisation ?	46
4.2.10.	Quelles garanties apporte la procédure d'instruction des demandes d'autorisation ?	47
4.3.	L'ETHIQUE ET L'ACCEPTABILITE	50
4.3.1.	Crainces relatives à la vidéo protection de lieux publics et privés ouverts au public	50
4.3.2.	Crainces relatives à la vidéo protection de lieux privés	50
4.3.3.	une organisation visible de la protection des libertes	51
4.4.	SYNTHESE UL3 : LES MESSAGES ESSENTIELS	51
5.	UL4 : OPTIMISER LE COUT DU SYSTEME DE VIDEO PROTECTION	52
5.1.	QUELLE EST LA STRUCTURE DE COUT ?	52
5.1.1.	Les coûts d'investissements immobiliers et mobiliers	52
5.1.2.	Les coûts de fonctionnement	54
5.2.	COMMENT LES REDUIRE ?	54
5.2.1.	la mutualisation : Une Piste essentielle de réduction des coûts	54
5.2.2.	Le retour sur investissement global (ROI)	55
5.3.	COMMENT LES FINANCER ?	56
5.4.	SYNTHESE UL 4: LES MESSAGES ESSENTIELS	59
6.	UL5 : L'ORGANISATION HUMAINE DU PROJET	60
6.1.	LA PERSONNE RESPONSABLE DU SYSTEME	60
6.2.	LA GESTION DU PROJET : AVANT L'INSTALLATION	61
6.3.	LA GESTION DU QUOTIDIEN : APRES L'INSTALLATION	62
6.3.1.	Les relations avec les partenaires externes	62
6.3.2.	L'accès aux images enregistrées	63
6.3.3.	Les documents à prévoir	63
6.4.	ORGANISATION SPECIFIQUE AUX SYSTEMES SUPERVISES	65
6.4.1.	Les relations avec les services de securite interieure	65
6.4.2.	La gestion ou le suivi des GRANDS EVENEMENTS	66
6.4.3.	Les opérateurs du système de vidéo protection	67
6.5.	SYNTHESE UL 5 : LES MESSAGES ESSENTIELS	69
7.	UL6 : DE L'ARCHITECTURE TECHNIQUE A LA LIVRAISON	70
7.1.	LES CHOIX TECHNIQUES	70
7.2.	LA STRUCTURE D'UN SYSTEME DE VIDEOPROTECTION	70
7.2.1.	Bloc 1 : L'acquisition	72
7.2.2.	Cas particulier du bloc d'encodage et de compression des images	77
7.2.3.	Bloc 2 : Transport	79
7.2.4.	Bloc 3 : L'exploitation des images	85
7.2.5.	bloc 4 : L'enregistrement, le stockage	89
7.2.6.	L'administration du système	91
7.3.	SYNTHESE UL 6 : LES MESSAGES ESSENTIELS	93
8.	UL7 : L'APPEL D'OFFRES, LE DEPLOIEMENT ET LA VALIDATION	95
8.1.	LES QUESTIONS-CLES AVANT DE LANCER L'APPEL D'OFFRES	95

8.2.	L'APPEL D'OFFRES.....	96
8.3.	DEPLOIEMENT.....	97
8.4.1	<i>Méthodologie et organisation</i>	97
8.3.1.	<i>Phase de préparation</i>	98
8.3.2.	<i>Prototype</i>	98
8.3.3.	<i>Pilote</i>	98
8.3.4.	<i>Formation du personnel</i>	98
8.3.5.	<i>Déploiement généralisé</i>	99
8.3.6.	<i>Validation</i>	99
8.3.7.	<i>La réception provisoire (vérification d'aptitude)</i>	99
8.3.8.	<i>La réception définitive (vérification de service régulier)</i>	99
8.3.9.	<i>Dossier d'interventions ultérieures sur les ouvrages (DIUO)</i>	100
8.3.10.	<i>Phase d'évaluation du dispositif en mode opérationnel</i>	101
8.4.	LES POINTS CLES A VERIFIER AVANT DE SIGNER LA RECETTE.....	101
8.5.	SYNTHESE UL 7 : LES MESSAGES ESSENTIELS.....	103
9.	UL8 : MAINTENANCE ET EVOLUTION TECHNIQUE.....	105
9.1.	LA SURVEILLANCE QUOTIDIENNE NECESSAIRE AU BON FONCTIONNEMENT DU SYSTEME	105
9.2.	LA MAINTENANCE	105
9.2.1.	<i>la Maintenance préventive</i>	108
9.2.2.	<i>la Maintenance curative</i>	108
9.2.3.	<i>Evolution du système</i>	109
9.3.	SYNTHESE UL 8 : LES MESSAGES ESSENTIELS.....	110
10.	GLOSSAIRE.....	111
11.	POUR ALLER PLUS LOIN.....	115

1 PREAMBULE

1.1 A QUI CE GUIDE EST-IL DESTINE ? COMMENT EST-IL ORGANISE ? COMMENT LIRE CE GUIDE ?

I. Si vous le voulez bien, commençons par une histoire de la vie courante.

Un propriétaire de jardinerie examine la porte fracturée du dépôt et l'endroit où se trouvaient les tondeuses, la veille, lorsqu'il avait fait le tour des locaux et tout fermé. C'est la deuxième fois en un an.

Cette fois, ça suffit, il se dit qu'il lui faut de la vidéosurveillance. Cependant, il hésite encore. Les notices techniques d'équipements et de caméras le laissent pantois. Tout cela lui paraît compliqué et cher. De plus, un collègue lui a parlé de dossier à déposer en préfecture et la paperasse lui donne la migraine.

Comment m'y prendre ? Comment définir mon besoin ? Qu'est ce que je dois commander ? Combien cela va-t-il me coûter ? Ai-je le droit ? Est-ce que cela va gêner mes clients ?

II. Le but du guide

C'est tout simplement de répondre aux questions ci-dessus et de décrire en détail la démarche méthodologique dans les différents domaines où la vidéo protection est utile.

III A qui ce guide est-il destiné?

Ce guide méthodologique a pour ambition de s'adresser à tout responsable ayant à piloter pour la première fois un projet de vidéo protection, ayant l'intention de le faire ou souhaitant développer ou améliorer un dispositif existant, et qui ne dispose pas des compétences adaptées dans son service. Il veut donc apporter un éclairage global et atteindre un très vaste public, du commerçant évoqué dans l'exemple initial au directeur général des services d'une commune importante, en passant par un directeur d'une entreprise de transports publics ou un responsable d'organisme HLM.

Il vise principalement les projets déployés dans les lieux où la vidéo protection est soumise au régime juridique de la loi du 21 janvier 1995, qui est le texte de référence pour la vidéosurveillance des espaces publics ou privés ouverts au public. Il abordera également les cas dans lesquels cette loi ne s'applique pas : zones de stockage non accessibles au public des commerces, dépôts de bus, zones de tri bagages des aéroports, etc.

Il se veut également compréhensible par un large public.

IV Comment est-il organisé?

Le guide comprend trois parties :

1. Présentation de la démarche méthodologique ;
2. Etudes de cas : pour chaque type d'application (commerces, bailleurs sociaux, transporteurs, communes, ZAC)

3. Fiches détaillées : pour « zoomer » sur les points pour lesquels le lecteur souhaite plus d'informations.

Il comprend en outre un glossaire et une rubrique « pour aller plus loin » présentant la bibliographie et les sites internet dignes d'intérêt.

Compte tenu de l'évolution rapide de la matière, il est découpé en unités de lecture, dont la mise à jour sera régulière et d'une taille permettant le téléchargement. La version papier sera diffusée en classeur.

Cette démarche s'articule en quatre phases. Pour faciliter la lecture, chaque phase est identifiée par un idéogramme spécifique et une couleur.

Chaque phase comprend une ou plusieurs unités de lecture, suivant le schéma ci-après.

Une unité de lecture comprend une dizaine de pages. Le but est de pouvoir les mettre à jour facilement en fonction de l'évolution de la matière et de les télécharger sans difficulté.

V. La démarche méthodologique

La démarche méthodologique, objet de la première partie, est, dans son principe, applicable par tous : collectivités, bailleurs sociaux, centres commerciaux... Elle est organisée en 4 étapes successives, essentielles à la réussite d'un projet :



Le diagramme illustre les quatre étapes de la démarche méthodologique, chacune avec un pictogramme et une liste d'unités de lecture (UL) associées :

- Analyse des besoins** (rouge) :
 - UL 1 : Le diagnostic sécurité
 - UL 2 : Les fonctionnalités propres à la vidéoprotection
- L'organisation humaine du projet** (vert) :
 - UL 3 : La protection des libertés publiques
 - UL 4 : Optimiser le coût du système de vidéoprotection
 - UL 5 : L'organisation humaine du projet
- La définition de l'architecture technique du système** (violet) :
 - UL 6 : De l'architecture technique à la livraison
 - UL 7 : L'appel d'offres, le déploiement et la validation
- La maintenance et l'évolution du système** (bleu) :
 - UL 8 : Maintenance et évolution technique

- Etape 1 : L'analyse des besoins,
- Etape 2 : L'organisation humaine du projet de vidéo protection,
- Etape 3 : La définition de l'architecture technique du système,
- Etape 4 : La maintenance et l'évolution du système.

Nous avons tous fait des choix de solutions avant d'avoir analysé correctement nos besoins. La technique est trop souvent privilégiée (« Je veux installer 20 caméras ») au détriment de l'étude de besoin (« De la vidéo, pour quoi faire ? ») et de l'organisation (« Quelle organisation mettre en place pour déployer, exploiter, entretenir mon système ? »).

L'analyse des besoins permettra la mise en place d'une organisation qui, à son tour, favorisera le bon fonctionnement du système. C'est donc le premier point à étudier dès le démarrage d'un projet et avant toute étude technique.

VI Etudes de cas

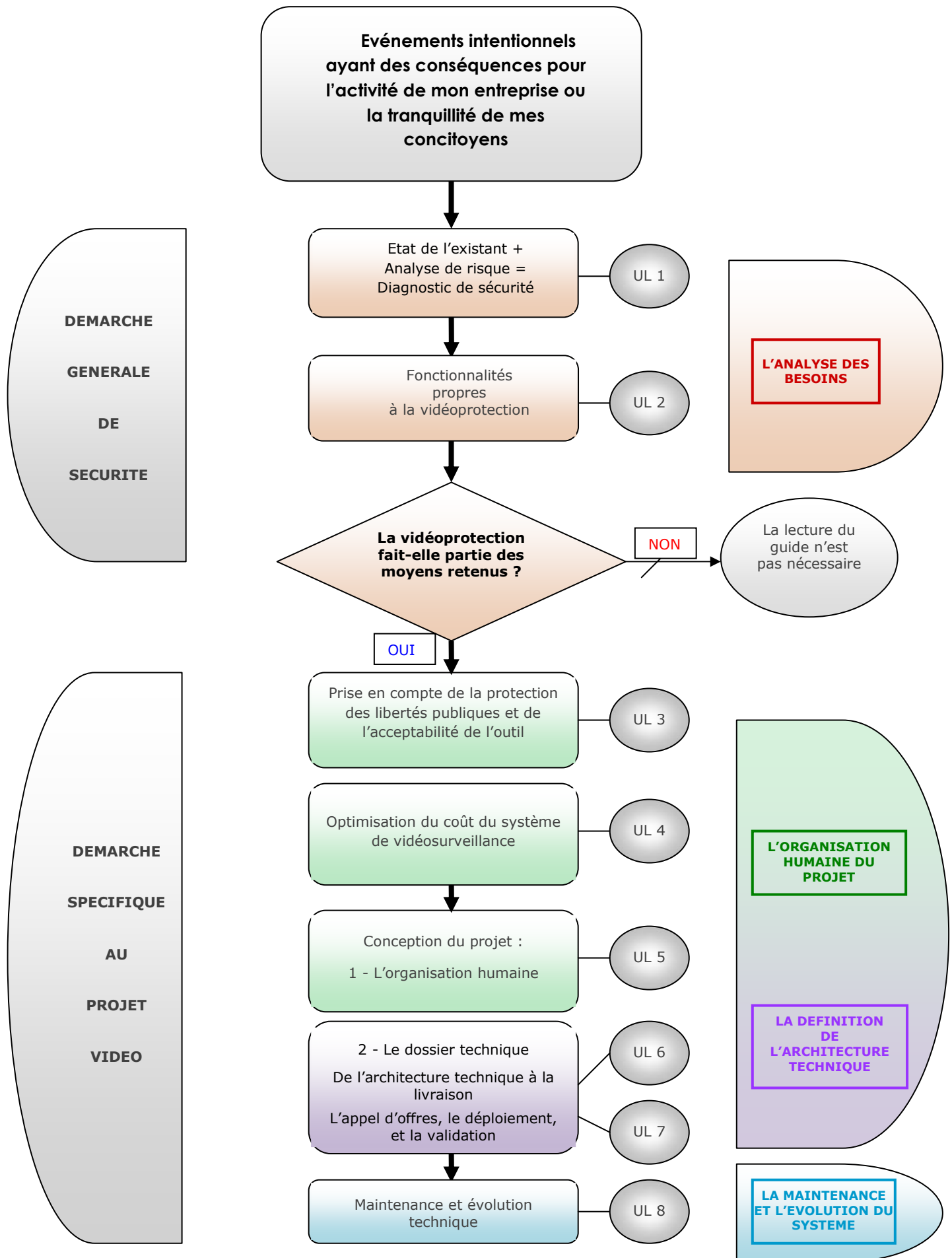
La seconde partie du guide présente les spécificités de la démarche de projet pour cinq cas types de déploiement de vidéo protection :

- Communes petites et moyennes,
- Bailleurs sociaux,
- Transporteurs,
- Centres commerciaux,
- Zones artisanales.

Le guide détaille les points spécifiques à chaque cas : besoin, organisation, aspect technique, cadre juridique... Chaque étape est illustrée par des cas réels.

VII Fiches thématiques

Cette troisième partie est composée de 16 fiches thématiques permettant d'approfondir certains aspects particulièrement importants ou complexes d'un projet.



VIII Comment lire ce guide?

Si la lecture des études de cas (partie 2) et des fiches thématiques (partie 3) est « à la carte » en fonction de l'activité exercée par le lecteur et de ses centres d'intérêt, l'appropriation de la première partie reste essentielle, même si le processus de prise de décision peut-être allégé et adapté à la complexité de chaque situation.

Nous vous suggérons :



- de lire au minimum les passages ayant en marge un logo à liseré vert, si votre système est simple (cas d'un petit établissement ou d'une protection bâtementaire de faible ampleur) ;



- de lire en outre les passages ayant en marge un logo à liseré rouge, si votre système est de taille intermédiaire (par exemple, centre commercial important),



- enfin, de lire tout le texte, incluant les passages ayant en marge un logo à liseré noir dans le cas des systèmes de vidéoprotection urbaine supervisés

A la fin de chaque unité de lecture, les « messages essentiels » permettent de synthétiser l'information à retenir.

Trois listes de questions devraient retenir l'attention :

- 20 questions à se poser avant de lancer le projet (fiche thématique N° 1);
- les questions-clés avant de lancer l'appel d'offres (au début de l'UL 7) ;
- les points-clés à vérifier avant de signer la recette (à la fin de l'UL 7) et 20 tests à réaliser à la réception du système (fiche thématique N°13 :)

Enfin, le tableau ci-après indique les thèmes indispensables que le lecteur pressé devrait avoir en mémoire suivant que le système de vidéo protection est destiné :

- à un petit établissement (moins de huit caméras) ;
- une entreprise disposant d'un PC de sécurité (pas d'opérateur dédié);
- une collectivité territoriale moyenne ou importante (présence d'opérateurs dédiés à la vidéo protection)

Taille de votre système	Description	Ce que nous vous suggérons de lire
<p>Petit établissement</p> <p>Ou</p> <p>Protection bâtementaire</p>	<p>1 à 2 caméras avec observation aléatoire des images par le commerçant</p> <p>Quelques caméras. Seules des images préalablement enregistrées sont regardées après événement.</p>	<p>-La première partie de l'UL 1 (le diagnostic de sécurité) et en particulier le tableau des questions essentielles à se poser avant d'envisager d'installer de la vidéo protection</p> <p>-Les fonctions de l'outil vidéo protection : ce que je peux en attendre (UL 2)</p> <p>-Les libertés publiques (UL3): ce que j'ai le droit de faire, les démarches à réaliser auprès de la commission départementale</p> <p>-L'exploitation (UL5): comment faire en sorte que mon outil soit efficace au quotidien ;</p>
<p>«de taille intermédiaire à gestion interne »</p>	<p>(nombre moyen de caméras avec personnel exploitant des images en temps réel en réalisant simultanément d'autres tâches (exemple: cas d'un PC sécurité dans une entreprise ou un centre commercial)</p>	<p>En complément des suggestions de lecture pour le petit établissement :</p> <p>-L'analyse de besoin des lieux ouverts au public (UL 1)</p> <p>-Les libertés publiques (reste de l'UL 3)</p> <p>-L'environnement humain et l'organisation (UL 5)</p> <p>-L'architecture, les choix techniques, l'appel d'offres et la validation (UL 6 et UL 7)</p> <p>-L'exploitation</p>
<p>Gros systèmes de voie publique</p>	<p>Nombre de caméras important et gestion en direct par un centre s'appuyant sur un partenariat portant sur le diagnostic local et la mutualisation de l'exploitation</p>	<p>Toute la partie démarche de projet, incluant l' UL 4 (le coût du système de VP)</p>

1.2. VIDEOSURVEILLANCE OU VIDEO PROTECTION ?

Le glissement sémantique accompagne l'évolution de l'opinion publique qui juge aujourd'hui cet outil protecteur à plus de 70%, alors qu'en 1995, la représentation nationale ressentait la nécessité de s'en protéger.

La prochaine loi d'orientation et de programmation pour la performance de la sécurité intérieure en tire les conséquences. Le terme vidéosurveillance sera remplacé par celui de vidéo protection dans l'ensemble des textes juridiques.

1.3. UN PRE REQUIS : LA VOLONTE DU DECIDEUR

La volonté du décideur est indispensable pour renforcer ou mettre en place tout système de sûreté. Cette volonté se traduit par la recherche de la cohérence opérationnelle des moyens de vidéo protection dans le système global de sécurité.

Cette volonté permettra d'obtenir des financements et de mobiliser les acteurs concernés. Un projet de vidéo protection ne doit pas être bâclé ou être un simple outil de communication. Son efficacité et sa crédibilité seraient fortement compromises.

1.4. LE MESSAGE ESSENTIEL A RETENIR DE CE PREAMBULE

La vidéo protection est l'application à la sécurité, des techniques de création et d'exploitation à distance d'images appelée vidéosurveillance. Elle apporte des fonctions essentielles à tout dispositif de sécurité.

La vidéo protection consiste à placer des caméras de surveillance dans un lieu public ou privé pour prévenir tout acte de malveillance (intrusion, vol, agression, violence, dégradation, destruction,...).

Elle permet, en temps réel ou différé, de :

- Surveiller l'espace en vision large ou concentrée ;
- Apprécier les situations ;
- Dissuader par la présence d'une surveillance visible et permanente;
- Détecter tout événement ou comportement anormal ;
- Identifier un individu, un véhicule, un objet...

Néanmoins :

- Elle ne permet pas de remplacer en toute circonstance la présence humaine.
- Elle doit s'inscrire dans un plan d'ensemble de sécurité dont elle n'est qu'un des éléments.
- Elle doit répondre à des conditions strictes d'emploi.

Un dispositif de vidéo protection produit des images qui sont transmises en vue d'une exploitation en temps réel sur un écran ainsi que leur enregistrement, aussi appelé stockage. Le moyen de stockage permet une exploitation en temps différé.

L'architecture du dispositif est modulable en fonction des objectifs recherchés : veut-on simplement surveiller la fluidité du trafic ou lire les chiffres et les lettres de plaque d'immatriculation ?

Les fonctions production des images (caméra), transmission, exploitation (visualisation des images) et stockage sont à la base de tout dispositif de vidéo protection. La combinaison de ces fonctions et le niveau d'exigences associé à chacune d'elles définissent l'architecture.

Les contraintes budgétaires (aussi bien en matière d'investissement que de fonctionnement) sont déterminantes pour déterminer les choix architecturaux.

L'étude technique détaillée permet ensuite de définir précisément le système et son coût.

Votre projet de vidéo protection

Guide Méthodologique



La démarche projet

Comité de Pilotage Stratégique
pour le développement
de la vidéo protection



2 UL 1 : LE DIAGNOSTIC DE SECURITE



Analyse des besoins

- UL 1 : Le diagnostic sécurité
- UL 2 : Les fonctionnalités propres à la vidéoprotection

2.1. COMMENT DEFINIR LE BESOIN DE SECURITE ?

Nous vous proposons d'entamer la démarche par des illustrations de la vie courante dans un ordre de difficultés croissantes.

2.1.1. LA PROTECTION D'UN COMMERCE

Revenons à l'exemple de la jardinerie vu dans le préambule. Avec l'aide d'un installateur recommandé par son assureur, le propriétaire de la jardinerie va réaliser un état de l'existant, qui consiste en :

- visiter l'ensemble des locaux,
- examiner les portes, l'issue de secours, les fenêtres, la vitrine, ainsi que les autres points de vulnérabilité (toit...),
- vérifier la qualité des dispositifs mécaniques de fermeture (serrures, rideau de fer...),
- prendre en compte l'environnement, (éclairage de nuit, disposition du parking par rapport à la rue...).

Ensuite, il procède à une analyse de risque :

- circonstances des cambriolages subis,
- obtention auprès d'une organisation professionnelle des scénarios les plus souvent rencontrés,
- réflexion sur les cheminements les plus probables des auteurs de délits.

Tout ce qui précède constitue la phase diagnostic de sécurité.

En fonction de l'objectif de sécurité du commerçant qui est de retarder la commission des vols et de faire intervenir une société de sécurité sur alerte confirmée, le spécialiste et le commerçant établissent une liste de préconisations :

- renforcement des serrures et du rideau de fer de la vitrine,
- amélioration de l'alarme,
- aménagement du magasin de manière à visualiser les zones à risques, les entrées et sorties (livraisons, personnels, clients),
- aménager l'espace intérieur de manière à être vu de l'extérieur et de voir l'extérieur,

Analyse des besoins

UL 1

Le diagnostic de sécurité



- mettre en place des règles de bon sens telles que de ne pas placer les marchandises de valeur près des portes mais plutôt près de la caisse, placer la caisse de manière à avoir une vision d'ensemble du magasin et des zones de passage, supprimer les angles morts,
- mettre en place un dispositif de vidéo protection ayant pour objectif de prévenir les cambriolages dans le magasin et les réserves, ainsi que visualiser la caisse, les issues de secours, l'entrée du magasin, les clients, le personnel.

A partir de là, et en fonction de la manière dont le propriétaire du magasin veut exploiter son système au quotidien et de son budget, les éléments du système de vidéo protection seront choisis sur catalogue. Auparavant, les précautions nécessaires à la protection des libertés publiques seront prises en s'assurant du respect des lois et en préparant le dossier de demande d'autorisation. Après, il ne restera plus qu'à installer le système et à l'exploiter.

Tout ce processus indispensable a pris une demi-journée.

Dans le cas de la jardinerie, les difficultés à traiter sont internes au magasin, le diagnostic de sécurité est simple à produire, les partenariats à nouer sont réduits, la mutualisation des moyens inexistante. Le projet de vidéo protection est implanté rapidement

2.1.2. LA PROTECTION D'UN COMMERCE DANS SA RUE

Prenons ensuite l'exemple de la pizzeria voisine. Elle se trouve dans une situation difficile, avec des répercussions économiques du fait du rassemblement intempestif et récurrent de jeunes dans la rue devant son établissement. Le diagnostic doit prendre en compte l'analyse de la situation qui gêne cette démarche commerciale. Il convient donc de connaître les raisons de ces regroupements.

En fonction de la situation, les réponses à apporter seront différenciées, concerneront directement ou pas le commerçant et pourront intégrer ou pas un dispositif de vidéo protection.

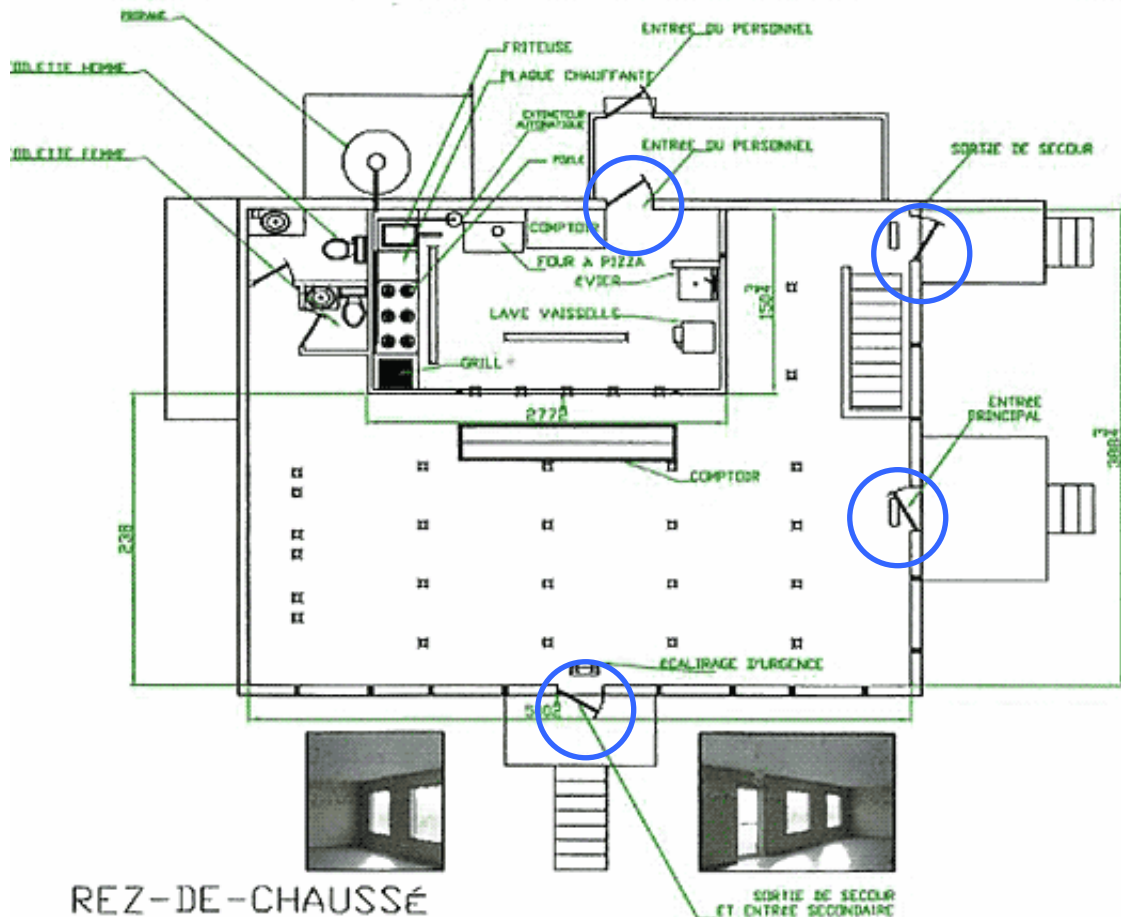
Ce commerçant doit prendre l'attache, par l'intermédiaire de l'association locale des commerçants, de la mairie et des référents police ou gendarmerie, afin de s'informer de l'état de la délinquance dans le quartier et de connaître les dispositifs mis en place pour pallier cette insécurité : dispositif de médiation incluant une équipe de prévention spécialisée, système de vidéo protection... Il convient également de s'informer sur les causes de ces phénomènes sociaux.

Pour illustrer le propos, considérons le problème du rassemblement de jeunes aux abords du commerce, et examinons les solutions qu'il peut mettre en œuvre.

Préconisations pour la sécurisation des abords du commerce :

Il faut voir avec la collectivité la possibilité d'aménager ou de supprimer aux abords du commerce le mobilier urbain favorisant le regroupement de personnes. Par exemple, suppression des bancs, surélévation des murets, mise en place de buissons évitant ainsi de s'adosser aux murs, s'assurer de la suffisance de l'éclairage public à la nuit tombée, supprimer une végétation trop dense pouvant servir d'échelle naturelle favorisant une pénétration dans les locaux par le toit, etc.

En complément de ces aménagements matériels ou techniques, d'autres solutions partenariales peuvent être proposées (par exemple un service de médiation, le recours à des agents de sécurité, le développement de patrouilles de la police...).



Cette phase du diagnostic doit permettre également de constater l'existant c'est-à-dire l'ensemble des dispositifs, qu'ils soient techniques, humains, matériels ou organisationnels présents sur le territoire et contribuant concomitamment à la réduction de la délinquance et à la prévention des actes de malveillance.

Après ces étapes, il convient de faire figurer dans le diagnostic les préconisations les plus adéquates aux problèmes à résoudre (voir UL 2) et ce n'est qu'à ce stade que l'on juge de l'opportunité ou non de mettre en place un système de vidéo protection. L'emplacement des caméras doit tenir compte des phénomènes d'insécurité et de délinquance. Celles-ci doivent donc être placées judicieusement pour favoriser la pertinence de cette action générale de sécurité.

Les difficultés à traiter sont extérieures à l'établissement commercial : le diagnostic est plus complexe à réaliser que dans le cas précédent. Il est recommandé de nouer des contacts avec les autorités locales. Les questions techniques restent simples mais du fait de l'impact des relations humaines, il faudra un peu plus de temps pour réaliser le projet. Ceci est également vrai dans une galerie commerciale.

2.1.3.LA RUE DANS LA VILLE

On identifie les partenaires avec qui travailler:



- On examine les difficultés du terrain et la typologie de la délinquance ;
- On étudie les différents moyens et dispositifs de prévention et sécurité déjà mis en œuvre sur le territoire concerné ;
- On définit enfin une stratégie générale de sécurité

Dans ce cas, c'est la collectivité territoriale, maître d'ouvrage, (commune, intercommunalité,...) qui va animer la réalisation du diagnostic de sécurité. Le nombre d'acteurs est plus important, l'identification des difficultés prend un peu plus de temps pour aboutir à une stratégie générale de sécurité qui doit rester fondée sur quelques principes simples.

Pour les dispositifs simples (enceinte fermée), il n'est pas nécessaire de lire en détail les développements des paragraphes qui suivent. Cependant, même dans ce cas, et pour bien comprendre l'objectif poursuivi et les résultats auxquels on veut arriver, il est recommandé de lire le paragraphe « définir une stratégie générale de sécurité » (paragraphe 2.6)

2.2. LE DIAGNOSTIC DE SECURITE

Commencer par décider d'affecter un budget à un nombre de caméras à déployer sur un territoire donné (Exemple : « j'ai un budget de 200 000 € ce qui correspond à 10 caméras, que je vais répartir sur le territoire à sécuriser »), est une démarche à proscrire quel que soit le type de projet. L'approche budgétaire ne doit être effectuée qu'après avoir recensé et qualifié les problèmes à régler.

L'analyse des besoins est la première étape d'un projet de sécurisation. C'est aussi la plus importante car sa pertinence conditionne l'efficacité des moyens déployés. Elle comporte deux phases successives :

La réalisation d'un diagnostic de sécurité.

Ce diagnostic permettra d'analyser l'historique des événements, leur typologie, les moyens engagés et d'effectuer la visite des lieux afin d'étudier le contexte général dans lequel la situation s'inscrit.

Le but du diagnostic est triple :

- Evaluer les difficultés rencontrées dans le périmètre concerné, ce qui suppose une connaissance du terrain, du contexte social et urbain
- Produire un état des moyens et dispositifs déjà mis en œuvre pour répondre à ces difficultés
- Elaborer une stratégie de sécurisation incluant des préconisations hiérarchisées (voir UL2)

Bien entendu, les formes que doit prendre ce diagnostic doivent être adaptées à la nature et à l'ampleur des problèmes rencontrés, ainsi qu'à la qualité de l'espace concerné et du maître d'ouvrage.

Ainsi, la mise en place d'un dispositif de vidéo protection sur la voie publique à l'échelle d'une commune nécessitera l'élaboration d'une démarche de diagnostic préalable plus complète que dans le cas d'un simple équipement ou commerce de proximité (cf. le cas d'une commune moyenne dans la partie relative aux études de cas

La formalisation des préconisations



Cette phase permettra de déterminer les dispositifs de sécurité et la mobilisation des ressources nécessaires dans le temps.

On verra que souvent la vidéo protection est associée à des moyens physiques de retardement (clés, clôtures, grilles...) ou électroniques (barrières infrarouges) permettant la détection de l'intrusion, des moyens humains et de supervision (gardiennage).

Cette partie ne sera pas développée car elle ne relève pas de l'objet spécifique de ce guide.

2.3. ENGAGER UN DIAGNOSTIC DANS UN CADRE PARTENARIAL

Dans le cas d'un dispositif de vidéo protection sur la voie publique, et afin de commencer correctement un diagnostic de sécurité, il faut prendre des dispositions pratiques et cibler la démarche dans un environnement partenarial. Il convient donc de savoir qui va réaliser le diagnostic et prendre les dispositions les plus précises pour faire interagir les différents partenaires dans ce domaine afin de lutter conjointement contre la délinquance et le sentiment d'insécurité persistant dans ces commerces.

A qui confier la réalisation du diagnostic ?

Le diagnostic peut être réalisé en interne mais il est également possible de faire appel à un prestataire extérieur (voir la Fiche 8). Dans ce cas, l'implication du maître d'ouvrage reste nécessaire et celle des services de sécurité intérieure est fortement conseillée. L'activité sous-traitée à un cabinet privé devra faire l'objet d'un suivi particulièrement attentif.

Réaliser un diagnostic partagé : associer les partenaires locaux

Il est nécessaire d'inscrire cette démarche de sécurité dans un partenariat et s'informer sur les dispositifs mis en place par les autres organismes pour agir en complémentarité. Par exemple, pour les commerces, il semble important de faire figurer l'association des commerçants dans le CLSPD afin d'agir en unité sur les problématiques touchant l'ensemble de cette profession.

Sur les sites dotés d'un CLSPD et/ou d'un CLS, il est recommandé de restituer cette démarche dans le cadre de ces instances et de s'appuyer sur les données quantitatives et qualitatives disponibles ainsi que sur les analyses et l'expertise des principaux partenaires, au premier rang desquels le coordonnateur du CLSPD et le référent des services de sécurité intérieure. Dans certains cas, il peut également être utile de faire appel à un prestataire extérieur, en sollicitant le cas échéant un soutien financier du FIPD (dans les conditions précisées à l'UL 4).

Associer les services de sécurité intérieure

La fiabilité d'un diagnostic de sûreté, qu'il soit réalisé en interne ou par un prestataire extérieur, et d'une façon générale d'un projet de vidéo protection, dépendra en grande partie de l'association de ces services, particulièrement pour les projets importants.

o **Les services locaux de sécurité**

La réalisation d'un diagnostic de sécurité suppose le recueil de données statistiques dont disposent les services de police et de gendarmerie. Les policiers et gendarmes connaissent bien leur territoire et les difficultés spécifiques de chaque secteur. De plus, en cas de commission d'infractions, les services de sécurité seront bénéficiaires des images obtenues. Il convient donc d'associer les services locaux de police ou de gendarmerie dans la démarche de projet, pour qu'ils puissent exprimer leurs besoins.

Il existe par ailleurs au sein de la police et de la gendarmerie des référents sûreté qui peuvent apporter leurs conseils dans l'élaboration d'un projet de vidéo protection, dès la phase de diagnostic, que celui-ci soit réalisé en interne ou par un prestataire extérieur.



- **Qu'est-ce qu'un référent sûreté?**

Depuis 2007, la direction générale de la police nationale et la direction générale de la gendarmerie nationale ont lancé une formation commune pour professionnaliser des policiers ou des gendarmes en matière de conseil en sécurité urbaine. Ces personnels de terrain expérimentés, connaissent particulièrement les modes opératoires et les lieux privilégiant la délinquance. La formation les spécialise notamment dans les domaines de la sûreté bâtiminaire et de la vidéo protection. Ces effectifs sont placés auprès des directeurs départementaux de la sécurité publique ou des commandants de groupement de la gendarmerie nationale.

- **Le rôle du référent sûreté :**

Le rôle du référent sûreté comprend deux aspects :

Expertise réglementaire et obligatoire dans le cadre de l'évaluation des études de sûreté et de sécurité publique (ESSP) au sein de la sous-commission pour la sécurité publique.

Les opérations importantes d'aménagement et de rénovation urbaine, doivent être précédées d'une étude de sûreté et de sécurité publique (cf. article L 111-3-1 du code de l'urbanisme). Cette ESSP fait l'objet d'un examen par une commission départementale où l'avis du policier et du gendarme est primordial. Ce sont les référents sûreté qui participent en qualité de rapporteur à cette commission.

Expertise réalisée dans le cadre de diagnostics au profit des personnes publiques ou d'établissements privés.

Les référents sûreté peuvent être sollicités pour évaluer un dispositif de sûreté existant ou pour préconiser une stratégie de sécurisation d'un site. En matière de vidéo protection, ils peuvent intervenir pour évaluer les besoins, présenter de façon objective les avantages et inconvénients de la vidéo protection, expliquer la réglementation applicable, indiquer les éventuelles aides financières possibles et donner un avis sur les lieux d'implantation et sur les types de matériels les plus adaptés à la situation. Toutefois, le référent sûreté n'étant pas un technicien mais plutôt un « stratège » en matière de vidéo protection, son intervention ne permet pas de se passer d'une étude de faisabilité.

- **Quand faire intervenir le référent sûreté dans un projet ?**

Le référent sûreté doit être impliqué le plus tôt possible dans un projet. De cette façon, il pourra vous conseiller afin que vous disposiez d'un dispositif optimum de vidéo protection sans être contraint par des choix techniques ou stratégiques précédemment effectués.

Le référent sûreté peut vous aider, il dispose d'un réseau d'experts juridiques, techniques, financiers. N'hésitez pas à le solliciter.

Il convient de se renseigner sur l'ensemble des systèmes préalablement mis en place et d'évaluer leurs actions et leurs effets sur la situation actuelle afin de s'inspirer des bonnes pratiques et d'améliorer la coordination de l'ensemble des dispositifs luttant contre la délinquance. Cette étape vise également à déceler les vulnérabilités du site à vidéoprotéger.

2.4. IDENTIFIER ET QUANTIFIER LES DIFFICULTÉS DE TERRAIN ET LA TYPOLOGIE DE LA DELINQUANCE

Réaliser un diagnostic de sécurité nécessite de recenser et de territorialiser les faits de délinquance contre lesquels on souhaite lutter, en faisant appel à toutes les données disponibles en interne mais également auprès des partenaires locaux.

2.4.1. DÉFINIR LE PÉRIMÈTRE À PRENDRE EN COMPTE DANS LES MILIEUX OUVERTS



La question du périmètre ne se pose pas dans les milieux fermés (centre commercial, entrepôt). Il en va différemment dans les espaces ouverts comme une zone urbaine. Il convient de déterminer dans quel périmètre l'action de sécurisation va être menée.

Le périmètre retenu doit permettre de traiter les problèmes rencontrés et dans la mesure du possible de ne pas les déplacer vers un espace vulnérable.

Il est à noter que la vidéo protection se révélera plus efficace sur un périmètre restreint permettant d'avoir un bon maillage de caméras, que sur une zone plus importante avec un éparpillement des caméras. Il en résulte qu'il sera peut être nécessaire d'établir une hiérarchisation des différents secteurs à équiper, pour avoir une véritable efficacité du système de vidéo protection. Cette démarche est souvent incontournable pour des raisons budgétaires.

Dans un cadre urbain, l'intercommunalité est à privilégier. Elle permet notamment de limiter les coûts d'un dispositif en mutualisant les charges d'exploitation, voire d'investissement. L'intercommunalité minimise également le risque de migration des délinquants d'un territoire vers un autre dans une zone urbaine homogène. D'autres formes de mutualisation peuvent être encouragées, s'agissant notamment des bailleurs sociaux.



2.4.2. LES OUTILS DU DIAGNOSTIC

Un certain nombre d'outils peuvent être utilisés pour réaliser un diagnostic de sécurité. Certains d'entre eux ne sont pas indispensables pour tous les types de projet (exemple : enquêtes de victimation) mais peuvent être utilement employés dans le cadre d'un projet urbain.

Les principaux outils de diagnostic sont les suivants :

Les données statistiques

o **Les statistiques des services de sécurité :**

Le service de police ou de gendarmerie dont vous dépendez pourra vous fournir, le cas échéant, des données statistiques pour vous permettre d'évaluer le niveau de délinquance de votre quartier ou de votre commune. L'existence d'un dispositif local de concertation dans le champ de la prévention et de la sécurité (CLSPD) ou d'un contrat local de sécurité (CLS) facilite l'échange de données. Quand elle existe, c'est à cette structure qu'il conviendra de s'adresser pour obtenir communication des statistiques. Le répertoire des infractions devra être préalablement analysé, car tous les comportements ne sont pas impactés par l'outil.

o **Les statistiques des exploitants :**

Les exploitants publics ou privés d'un espace ou d'un équipement recensent souvent les faits de délinquance ou d'incivilités dont ils sont victimes. Ce recueil peut être indirect (coût de la maintenance d'un site) ou directement utilisable (sinistralité, statistiques sûreté).

Les entretiens

Les entretiens sont utiles dans le cadre des diagnostics de sécurité, car ils permettent de compléter les données statistiques ou d'obtenir un état des lieux, lorsque ces dernières sont insuffisantes. Il convient, en premier lieu, d'identifier les personnes clés à interroger (responsable des questions de prévention / sécurité / sûreté, des services techniques, de la gestion et de l'entretien...), puis d'élaborer une grille d'entretien qui permette d'aborder l'ensemble de la problématique. L'avantage de l'entretien est qu'il est interactif et réactif. Il peut vous permettre de révéler une thématique importante à laquelle vous n'aviez pas songé de prime abord.

Pour être productif, l'entretien implique de pouvoir créer un climat de confiance avec votre interlocuteur.



Les questionnaires

Les questionnaires reposent sur le même principe que les entretiens. Ils sont utilisés quand le nombre de personnes à consulter est trop important ou les délais trop courts pour pouvoir être réalisé par entretien. Ils peuvent également servir à confirmer les éléments obtenus au cours des entretiens.

Les enquêtes de victimation

Réalisées par voie de questionnaires ou d'entretiens, les enquêtes de victimation ont pour objet de compléter les statistiques ou d'obtenir des données non recensées par les statistiques existantes. L'enquête de victimation permet d'interroger un panel représentatif et de connaître dans le détail les faits dont ces personnes ont été victimes, durant une période et dans un espace donné. Cet outil suppose la mise en place d'une méthodologie assez rigoureuse. L'enquête peut utilement s'accompagner d'une étude sur le sentiment d'insécurité éventuellement ressenti par les personnes interrogées. Quel que soit leur intérêt, ces enquêtes longues et lourdes n'ont de sens que pour des dispositifs très importants.

Les visites sur site

L'organisation de visite(s) de terrain et la réalisation de clichés photographiques des lieux ou zones problématiques est une étape primordiale afin de connaître et de comprendre le territoire étudié et ses spécificités. Cette visite permet de saisir une ambiance, de révéler des difficultés techniques potentielles, des obstacles d'origine naturelle (recoins insécures...) ou humaine, des dysfonctionnements en matière d'entretien ou de maintenance d'un espace public ou d'un équipement qui impacteront directement l'efficacité du dispositif de vidéo protection.

Cette visite consiste à établir un diagnostic physique portant sur la périphérie du site, sa périmétrie ainsi que sur l'analyse des flux internes. Elle permettra de concevoir la zonalisation du site ainsi que l'amélioration du contrôle des accès.

Il est important de porter une attention toute particulière à l'état de l'éclairage qui devra souvent être revu ou complété.

2.4.3. COMMENT UTILISER LES DONNÉES RECUEILLIES

○ **Effectuer un premier tri :**

Il conviendra premièrement de trier ces données hétéroclites (nature, périodes ou périmètres différents). Enfin, toutes les données n'ont pas la même valeur. Il pourra donc être nécessaire d'évaluer les informations obtenues et écarter tout ce qui ne paraîtrait pas fiable ou représentatif ou ne concernant pas le périmètre étudié.

○ **Classer les informations par catégories :**

- Atteintes aux biens : dégradations, vols ...
- Atteintes aux personnes : agressions, insultes...
- Informations relatives aux victimes
- Informations relatives aux auteurs : âge, sexe...
- Informations relatives au mode opératoire : individus seuls, en groupe, de jour, de nuit...
- Origine de la délinquance :



- Endogène : une délinquance est endogène lorsque les auteurs des faits constatés vivent à proximité du lieu de commission.
- Exogène : un moyen de transport quelconque est utilisé par les auteurs des faits.

Cette notion est importante car les moyens de prévention sont très différents dans les deux cas. Dans le cas d'une délinquance endogène, on privilégiera la prévention sociale, dans le cas contraire, on mettra l'accent en priorité sur des dispositifs de prévention situationnelle. Cette approche est bien évidemment à nuancer selon la nature des sites traités.

- Fréquence : mensuelle, hebdomadaire, quotidienne,
- Répartition spatio-temporelle des faits
- Intensité / gravité :

Sur le plan pénal : crime, délit, contravention, incivilité,

Sur une échelle interne : faible, moyenne, importante, majeure (au regard de : conséquence sur l'activité, dégâts, image et notoriété...).

2.5. REALISER UN ETAT DES MOYENS EXISTANTS

Il s'agit de recenser et d'évaluer tous les moyens déjà déployés pour rendre le passage à l'acte plus pénible, plus risqué, moins avantageux, moins banal... Il s'agit des dispositifs techniques tels que la détection d'intrusion, le contrôle d'accès. Il faut également prendre en compte les moyens humains, c'est-à-dire le personnel en charge de la surveillance de l'espace concerné. Il peut s'agir du personnel directement dédié à la sécurité d'un site mais également tout le personnel chargé de l'accueil et de l'orientation des visiteurs.

o **Etablir des tableaux de suivi dans l'espace et le temps**

Ces outils de pilotage seront nécessaires pour évaluer la performance des systèmes de prévention (y compris la vidéo protection), afin d'envisager des évolutions ultérieures.

o **Un recensement des dispositifs existants**

Ce recensement doit s'accompagner d'une évaluation permettant de déceler les failles du dispositif en place : éclairage insuffisant, dysfonctionnement ou vulnérabilité d'un système de contrôle d'accès ...

o **Un bilan de l'organisation interne et du respect des procédures.**

Fréquemment, des problèmes de sécurité perdurent alors que l'exploitant d'un site a déployé des moyens importants de sécurisation, techniques ou humains. Un examen attentif de la situation permet le plus souvent de mettre en cause un déficit d'organisation interne : définition et respect des procédures.

Un diagnostic de sécurité doit comprendre un bilan détaillé de l'organisation mise en place dans le cadre d'un dispositif de sécurité.

Ce bilan peut par exemple s'appuyer :

Sur des mises en situation : simulation de situations critiques et étude du comportement du personnel, notamment celui en charge de la sécurité.

Sur une visite de terrain qui permettra d'identifier les mauvaises habitudes : portes laissées ouvertes, serrures neutralisées, obstacles devant des détecteurs d'intrusion...



2.6. DEFINIR UNE STRATEGIE GENERALE DE SURETE

A l'issue du diagnostic, il est possible de construire une démarche de sécurité fondée sur des préconisations. Celles-ci concernent tous les aspects de sécurité et sûreté. Par exemple :

Faits constatés	Préconisations	Effets
Tags	Mettre en place un service de nettoyage supprimant en temps réel tous les tags.	Lassitude des jeunes de voir leurs tags effacés.
Sentiment d'insécurité	Améliorer l'éclairage, mettre en place un service de médiation, supprimer des zones abandonnées, se réapproprié l'espace, favoriser la visibilité des passants	Augmentation de la fréquentation des commerces par une amélioration des conditions de bien être.
Dégradation de vitrine, vol avec effraction dans les boutiques	Mettre en place une protection métallique pour la sécurisation des vitrines, un service de gardiennage privé, d'alarme, une ronde de la police, mettre en place un système de vidéo protection	Abandon d'appropriation de la place par les délinquants, réduction du nombre des délits commis, possibilité d'identification des auteurs.
Rassemblements intempestifs de jeunes	Installer un dispositif de médiation favorisant le dialogue avec les jeunes. mettre à disposition un local adéquat à leur réunion, supprimer tout mobilier urbain favorisant un lieu de squat, mobiliser une équipe d'éducateurs de rue	Réaménagement urbain permettant le déplacement de population gênant le développement du commerce.

Lister les priorités, les objectifs de sécurité, à la fois dans le temps et dans l'espace, afin de mettre en place un dispositif pertinent répondant aux attentes, de tenir compte des ressources humaines et budgétaires et de prendre en compte les développements techniques.

Ce n'est qu'à cette étape que l'on va juger de l'opportunité de mettre en place un dispositif de vidéo protection après avoir envisagé les différentes possibilités pour répondre aux problèmes.

A ce stade, il est également nécessaire d'envisager une mutualisation de l'action, si nous nous trouvons dans une situation le permettant (par exemple une rue commerçante). Cette mutualisation se fait avec l'ensemble des commerçants, mais également avec la collectivité locale lorsque l'on peut agir sur le domaine public.



2.7. SYNTHÈSE UL 1 : LES MESSAGES ESSENTIELS

Le diagnostic de sécurité est la première étape d'un projet de vidéo protection, quelle que soit la nature du site concerné. C'est une étape essentielle d'un projet de sécurisation. Le diagnostic permet de connaître les problèmes d'insécurité rencontrés sur un site, de les qualifier (atteintes aux biens, aux personnes...), de les quantifier, de les hiérarchiser, de comprendre leur origine. Le diagnostic apporte une vision objective de la situation auquel le gestionnaire d'un site est confronté.

Lorsque le périmètre pris en compte concerne la voie publique, on utilisera le terme de diagnostic local de sécurité. Celui-ci doit impérativement s'inscrire dans une démarche partenariale. La démarche de diagnostic doit, dans ce cas, s'appuyer sur l'expertise des référents sûreté de la police et de la gendarmerie nationale. Il doit aussi prendre en compte les dispositifs locaux de prévention et de concertation, présents dans toutes les communes de plus de 10 000 habitants et ouverts à tous les acteurs publics ou privés confrontés à des problèmes de délinquance (conseils locaux de sécurité et de prévention de la délinquance). Dans tous les autres cas, l'expertise des services de sécurité intérieure pourra également être utile pour sécuriser des espaces privés.

Le diagnostic de sécurité doit être l'occasion de réaliser un bilan de l'existant. Il s'agit des moyens de protection humains ou techniques déjà déployés, mais aussi des procédures, de la politique de sécurité mise en place. Il ne s'agit pas uniquement de collecter des données statistiques. Une visite approfondie d'un site, des tests réalisés sur les systèmes, des mises en situation sont autant de moyens de détecter des failles dans un dispositif de sécurité.

Le diagnostic de sécurité doit aboutir à la réalisation d'une synthèse cohérente des actions de sécurisation. Il s'agit en premier lieu d'identifier des « fragilités » dans le site étudié (exemple : désaffectation d'un parking liée à la présence de squatters) qui permettront de fixer des solutions de sécurité pour y remédier. Ensuite, ces fragilités devront être traitées dans le cadre d'une stratégie générale de sécurisation organisée (ex : contrôler les accès d'un parking). La stratégie doit également définir le périmètre à prendre en compte, notamment en milieu ouvert. La vidéo protection nécessitant en général un maillage serré de caméras pour être réellement efficace, il sera peut être utile de prioriser les zones à équiper.

Cette stratégie ayant été élaborée, il faut ensuite définir des préconisations propres à la vidéo protection (voir UL2)

**Analyse des
besoins**

UL 1

**Le diagnostic
de sécurité**



3. UL 2 : LES FONCTIONNALITES PROPRES A LA VIDEOPROTECTION

Pour mémoire, le diagnostic de sécurité préalablement établi conduit à la réalisation d'une synthèse globale des risques encourus. Il permet de fixer des objectifs concrets et précis de prévention des faits de délinquance et de réduction des risques. Certaines des préconisations impliquent spontanément l'idée d'utiliser des images.

Toutefois, avant de décider si la vidéo protection peut être envisagée pour répondre à un objectif, il est nécessaire d'avoir identifié les capacités fonctionnelles de l'outil et de comprendre son fonctionnement général et ses contraintes. Le but de la présente unité de lecture est d'examiner les objectifs opérationnels pour lesquels la vidéo protection peut être préconisée, puis, pour chacun d'entre eux, de présenter les caractéristiques des moyens qu'il faudra sélectionner.

Par exemple, pour surveiller en permanence un espace et en même temps contrôler l'accès à une zone particulière de cet espace, il faudra des caméras dites dômes qui pivotent sur 360° et des caméras fixes.

3.1. A QUOI PEUT SERVIR LA VIDEO PROTECTION ?

Les systèmes de vidéo protection font l'objet d'une autorisation administrative préalable, comme nous le verrons dans l'unité de lecture suivante. Toutefois, de nombreux opérateurs exploitent les dispositifs techniques pour des usages complémentaires, tout en respectant la déontologie et le droit.

L'expérience des opérateurs de milieux très différents, aussi bien en milieu urbain ouvert que dans le commerce ou les transports, permet de constater les usages suivants :

Dissuasion et contribution à la prévention de la délinquance

La certitude de la sanction est un facteur dissuasif fort. Certaines personnes, les auteurs mineurs notamment, ne réalisent le risque pénal que très tardivement. Ils adoptent un comportement désinhibé et passent à l'acte facilement.

Le fait de savoir que l'on est vu modifie certains comportements. Bien entendu, la dissuasion est meilleure si les personnes concernées ont connaissance de cas élucidés grâce à la vidéo protection.

Il n'est pas possible de disposer d'une réelle étude **générale** d'impact de l'outil, en France comme à l'étranger. Cela nécessiterait par exemple de disposer de deux villes tests et de ses habitants, protégées de toutes modifications internes ou d'interactions externes nouvelles, pour une durée qui ne saurait être inférieure à plusieurs mois, ce qui est irréalisable. Cependant, de nombreuses recherches menées depuis plus de 20 ans, permettent de décrire quelques conditions impératives pour rendre l'outil efficace.

La vidéo protection est très efficace pour prévenir de nombreuses infractions telles que les vols, les dégradations. Elle permet aussi de réduire les atteintes aux personnes telles que les vols avec violence. L'outil est particulièrement efficace dans les endroits clos qui ont fait l'objet d'un traitement complet de sécurisation. On mentionne souvent l'exemple du parking souterrain, public ou privé, qui est repeint et éclairé, dont les accès sont placés sous contrôle, en direct, grâce à la vidéo protection. On estime dans ce cas que la baisse des faits de délinquance peut atteindre 90% !

Ce qui relève d'un acte terroriste effectué par un individu qui accepte sa propre mort ou d'un acte commis sous l'empire de la colère n'est évidemment pas dissuadé par la vidéo protection. L'outil n'en demeure pas moins efficace pour autant. Parce que les images recueillies permettent de savoir ce qui s'est réellement passé et d'identifier rapidement le terroriste, l'effet souhaité visant à déstabiliser la société est fortement diminué.





Quelques études montrent que certaines infractions sont en hausse du fait de l'utilisation de la vidéo protection. C'est le cas des usages de produits stupéfiants, des atteintes à la tranquillité publique ou encore des infractions à la circulation routière. Il s'agit d'infractions « révélées par l'activité des services de sécurité », en l'absence de plaintes.

Aide à l'intervention

Il faut souligner que l'efficacité d'un système lors de la commission d'une infraction flagrante suppose qu'un opérateur détecte en direct l'infraction, parvienne à visualiser de façon satisfaisante l'espace contrôlé pour identifier l'auteur, tout en alertant les services de sécurité qui procèdent alors à son interpellation. Cela suppose une formation et une organisation adaptée. Cela impose de réfléchir lors de la conception du projet aux objectifs assignés au système de vidéo protection et notamment à la fonction de chacune de ses caméras.

Outil d'investigation

La vidéo protection est un outil apprécié par les forces de sécurité intérieure, car elle leur apporte souvent des éléments d'information décisifs dans une enquête judiciaire ou administrative, qui n'auraient pas pu être recueillis par d'autres moyens. L'efficacité d'un système peut varier sensiblement selon plusieurs critères.

Prenons l'exemple hypothétique d'un système dont l'objectif opérationnel est de reconnaître toutes les personnes circulant dans un couloir : son efficacité pourra varier selon de nombreux critères. On peut citer quelques exemples :

- Affluence : reconnaître une personne circulant dans une foule est plus difficile que reconnaître un individu isolé et statique,
- Qualité du système : certains systèmes apporteront une meilleure qualité d'images que d'autres,
- Stratégie d'évitement : quelqu'un qui ne veut pas être reconnu pourra être tenté de recourir à des stratégies permettant de neutraliser les possibilités de la vidéo : cagoule, lunettes, tête baissée...Néanmoins, cette attitude alertera l'opérateur et la tenue ou le comportement de l'individu peuvent servir d'éléments d'enquête, à défaut d'identification formelle.
- Conditions d'éclairage et climatiques : dans un lieu fermé, elles sont stables. Ce n'est pas le cas en extérieur.

En fonction des besoins, on s'orientera vers un système de vidéo protection dit passif ou un système supervisé, c'est-à-dire doté d'opérateurs surveillant les images. Un système passif peut tout à fait répondre à un objectif ne nécessitant pas une réactivité face à un événement donné. Exemple : enregistrer les plaques de tous les véhicules entrant dans un parking. C'est la définition des besoins opérationnels qui détermine le système et l'organisation adaptés.

La lecture des enregistrements des images permet très souvent l'identification a posteriori de l'auteur d'une infraction.

Moyen de gérer les événements d'ordre public

Par événements d'ordre public, il faut entendre tous les troubles occasionnés dans l'espace public (voie, place, lieux privés ouverts au public, etc.).

Il peut s'agir :

- de rassemblements festifs ou revendicatifs,
- de protection des déplacements d'autorités gouvernementales ou de régulation de la circulation au quotidien,



- de levée de doute faisant suite à une demande d'intervention des forces de l'ordre ou des secours,

Les opérateurs privés disposent de la même facilité pour effectuer les levées de doute lors d'un déclenchement d'une alarme-intrusion et de la même capacité à exercer des contrôles de l'activité interne à leur entreprise.

Outil de gestion des incidents

Les opérateurs publics et privés se servent de la vidéo protection en complément pour assurer une veille opérationnelle de leurs dispositifs techniques. A titre d'illustration non exhaustive, on peut mentionner les usages suivants :

- gestion du risque tel qu'un passager coincé lors de la commande de fermeture des portes d'un train ou d'un métro ;
- surveillance des flux de personnes circulant sur un escalier mécanique ;
- surveillance de l'écoulement des bagages sur un tapis bagages ;
- surveillance de la manœuvre d'une écluse pour éviter tout accident ;
- surveillance de l'absence de personnes dans la zone de manœuvre d'un engin à faible visibilité (passerelle d'avion,...)

3.2. COMMENT FONCTIONNE L'OUTIL ?

La lecture des chapitres 6 et 7 donnera quelques clés de compréhension de l'outil vidéo, aujourd'hui d'une technicité complexe. En effet, on est passé de l'ère de l'analogique au tout numérique qui offre des possibilités quasi-infinies de traitement des espaces.

Néanmoins, la démarche projet nécessite que l'on se pose quelques questions préalables simples afin de comprendre les limites et les contraintes de l'outil.

Le système vidéo est composé d'un moyen de capture des images (la caméra), d'un moyen de transport de l'image (du courant faible à la fibre optique, d'un faisceau hertzien à la diffusion Wifi locale), d'un moyen de visualiser et de piloter les images (un écran et un clavier) et enfin d'un moyen d'enregistrer (enregistreur). On peut enregistrer sur la caméra comme à distance. On peut visualiser et piloter sur les lieux de la capture des images comme à quelques centaines de kilomètres de distance.

L'œil humain reste très supérieur à l'outil technique. Concevoir un projet vidéo nécessite de connaître les capacités de l'outil, notamment dans un environnement où la luminosité est faible. C'est encore plus vrai avec la technologie numérique car les images capturées, de très belle qualité, sont trop volumineuses pour être transportées dans leur état initial et donc visualisées à distance dans leur état initial, trop volumineuses pour être stockées dans leur état initial sur un support économiquement accessible. Les images sont alors compressées pour en réduire le volume. Or, il n'existe pas aujourd'hui de moyens pour retrouver la qualité initiale depuis les images transportées ou enregistrées. C'est un handicap que l'on contourne en trouvant le bon équilibre entre le besoin à satisfaire et l'architecture technique à mettre en œuvre.

L'Etat a tiré les conséquences de cette difficulté technique en considérant que les dispositifs de vidéo protection autorisés devaient respecter des normes techniques minimales de manière à leur conserver une efficacité.

DES SPECIFICATIONS TECHNIQUES FIXEES PAR ARRETE

Les spécifications techniques minimales des images des systèmes de vidéo protection sont définies par un **arrêté interministériel du 3 août 2007, complété par une annexe**



technique parue le 21 août 2007. Ces spécifications doivent être respectées par tout nouveau système. Pour les systèmes plus anciens, la mise en conformité est obligatoire à compter du 22 août 2009.

Le but de ces règles techniques est d'assurer une bonne qualité des images en visualisation directe ou après transmission afin qu'elles permettent les identifications nécessaires et qu'elles servent effectivement à lutter contre la délinquance.

Au-delà de ces spécifications, l'image fournie par le système dépendra de nombreux facteurs : capteur, positionnement, angle de vue. Ces éléments techniques sont secondaires car il faut, dans un premier temps, choisir le type d'image dont on a besoin pour répondre à l'usage fixé.

3.3. J'ADAPTE L'OUTIL A MES BESOINS DE SECURITE

L'efficacité des dispositifs de vidéo protection tient à l'articulation entre l'outil et l'humain. Il n'existe pas de politique de sécurité sérieuse reposant uniquement sur l'outil technique quel qu'il soit sans prendre en compte l'action humaine. La caméra elle-même, nécessite l'intervention humaine pour la rendre performante.

Les capacités techniques de l'outil doivent s'adapter à son environnement naturel comme aux objectifs de sécurité qu'on lui assigne.

3.3.1. LES PREALABLES

Quelque soit la taille des projets, un certain nombre de réflexions préalables doivent être menées.

IL FAUT RETENIR QUE L'ENVIRONNEMENT DOIT ETRE PRIS EN COMPTE

La qualité d'image fournie par une caméra donnée est fonction des conditions d'éclairage, de stabilité (une image « tremblée » est illisible), de température, de chocs physiques, de propreté, de l'environnement végétal etc.

IL FAUT RETENIR QU'UNE CAMERA DOIT ETRE DEDIEE A UN USAGE

Les systèmes sont peu polyvalents, une caméra doit le plus souvent être dédiée à un usage précis.

Exemple : une caméra prévue pour lire une plaque d'immatriculation dans toutes les conditions (jour, nuit, pluie, soleil) ne répondra qu'à cet objectif. Elle ne sera pas adaptée par exemple pour voir le visage du passager arrière du véhicule.

IL FAUT RETENIR QUE LE MODE D'EXPLOITATION DEPEND DU BESOIN

L'objectif principal assigné au système détermine les modalités d'exploitation des images :

Images enregistrées :

Les images sont consultées en cas de besoin, en temps différé. Certaines applications ne nécessitent pas une supervision et une architecture simple, sans poste de supervision, peut être déployée.

Exploitation en temps réel des images :



Les images sont renvoyées en temps réel vers un centre de surveillance vidéo, où un opérateur est chargé de les exploiter. Cette architecture permet la réactivité du système.

Nota : La réactivité peut, dans certains cas, être assurée par une « intelligence » du système (Voir également fiche n° 12 : les traitements intelligents)

IL FAUT ETRE SUR DE SON OBJECTIF

Imaginons qu'il soit décidé de surveiller en permanence toute une place en centre ville, en milieu urbain, lieu de regroupements et de trafics.

La première idée est d'utiliser une caméra dôme. Mais cette caméra ne correspond pas au besoin exprimé, car elle ne surveille pas 360° **en permanence**, mais un angle de vue limité que l'on peut faire défiler. La seule solution est alors d'installer un réseau de caméras que l'on fige, assurant un quadrillage permettant de répondre au besoin. Les caméras restent mobiles pour permettre de zoomer un endroit précis en fonction des circonstances.

Cet exemple montre, une fois de plus, l'importance de l'étude du juste besoin. A-t-on vraiment besoin de surveiller toute la place en permanence ? Si oui, il faudra dimensionner le système en conséquence.

IL FAUT HIERARCHISER LES BESOINS

Dans la plupart des projets, les contraintes budgétaires imposent de faire des choix. Il convient donc de s'y préparer en hiérarchisant les besoins en vidéo protection.

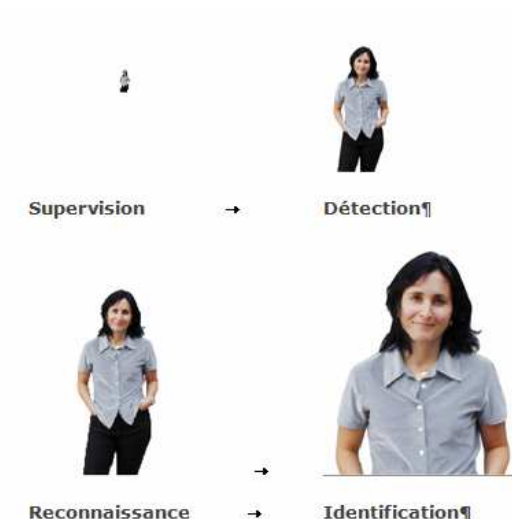
Quelques critères de hiérarchisation :

- Donner la priorité aux sites qui ne peuvent pas être traités efficacement par d'autres moyens techniques ou humains,
- Eviter le saupoudrage : il vaut mieux bien couvrir un secteur limité mais stratégique, par un maillage étroit, que de disperser des capteurs sur un large territoire,
- Planifier le déploiement : un projet peut souvent être déployé par étapes, dans le temps.

Prendre en compte les opportunités du territoire : réseau existant chez un partenaire, travaux de génie civil effectué par une autre entreprise, mise en réseau des alarmes techniques, de la téléphonie, des données, etc.

3.3.2. LE BESOIN DÉTERMINE LA QUALITÉ D'IMAGE

Chaque application nécessite une qualité particulière d'image :



Il est donc logique de bien définir le résultat attendu avant de choisir un matériel.

Exemple : pour réaliser un contrôle d'accès avec reconnaissance de visage, il faudra un système dédié avec des images de très bonne qualité, centrées sur le visage.

QUEL TYPE DE CAMERA POUR QUEL BESOIN ?

Il existe plusieurs types de caméras. Certaines caméras permettront d'obtenir un plan fixe de bonne qualité, d'autres offriront la possibilité de changer de champs de vision, d'agir à distance sur ce champ. Le choix entre ces différents matériels dépend complètement du besoin spécifique correspondant au rôle donné au système. Un projet pourra faire appel à plusieurs types de matériels.

Exemple : caméra fixe dans le cas de la surveillance d'une porte, caméra mobile pour la surveillance d'un vaste espace...

La fiche thématique 10 présente les caractéristiques principales des caméras permettant de comprendre une notice technique constructeur.

3.3.3. LE BESOIN DETERMINE LE CHOIX DU RESEAU

Les modalités de transport de la vidéo protection sont très diverses. Les réseaux doivent être choisis en fonction de critères de besoins.

La fiche thématique 10, paragraphe 2 présente les caractéristiques principales d'un réseau.

3.3.4. LE BESOIN DÉTERMINE LE CHOIX DU MODE D'EXPLOITATION

Différentes architectures de systèmes vidéo protection sont mises en œuvre en fonction de l'objectif retenu.



SI L'ON A BESOIN D'UN OUTIL D'INVESTIGATION A POSTERIORI

Il peut suffire d'acquérir des images, de les enregistrer pour ensuite les visualiser en temps différé. L'ensemble des moyens peut être localisé au même endroit.

C'est le système le plus simple, que l'on rencontre classiquement pour les besoins de commerces indépendants ou de petites supérettes. Il comprend quelques caméras, un système d'enregistrement, un écran de visualisation et quelques câbles reliant le tout.

Il répondra souvent à un deuxième objectif de levée de doute sur alerte, de jour comme de nuit. Si quelqu'un entre dans le magasin, cela déclenche la sonnerie ce qui incite à jeter un coup d'œil sur l'écran. Ce deuxième emploi est en « temps réel ». La nuit, l'alarme déclenche l'enregistrement, ce qui nécessite une caméra sensible ou un éclairage complémentaire (projecteur infrarouge).

Le coût d'installation d'un tel système est très faible et son coût d'exploitation est nul.

Exemple d'un système non opéré : les images sont enregistrées directement. Les enregistrements ne sont consultés qu'après événement (station service, petit établissement).

SI L'ON A BESOIN D'UN SYSTEME PERMANENT DE SUIVI DES ALERTES

Un centre commercial important dispose d'un service de sécurité, chargé de régler les multiples soucis de la vie courante, de l'incident de circulation dans le parking à la surveillance d'une bande et la prévention du vol en passant par la gestion du système de sécurité incendie. Ce service dispose d'un PC sécurité-sûreté. Dans ce PC, les images sont regardées en temps réel, mais par des personnes qui ne sont pas dédiées à cette seule tâche. L'alerte viendra souvent d'un appel radio des rondiers.

La différence d'architecture par rapport au cas précédent est liée à l'existence de ce PC et à la taille de la zone à vidéosurveiller. Les images sont déportées sur des distances parfois importantes. Le moyen de transmission devient un composant du système méritant un examen attentif.

Le coût d'installation d'un tel système est proportionnel à sa taille et la partie transmission en représente une part non négligeable. Le coût d'exploitation est faible, puisque la vidéosurveillance ne représente qu'une des tâches du personnel de sécurité.

SI L'ON A BESOIN DE DETECTER EN TEMPS REEL UNE SITUATION ANORMALE

Cette détection suppose une surveillance constante. Il faudra alors disposer de personnel dédié à l'observation des images car c'est à partir de cet examen qu'est déclenchée l'alerte. Un tel système est dit opéré.

Le coût d'exploitation d'un tel système est important.

Exemple de système supervisé : les images d'une caméra sont renvoyées vers un centre de surveillance vidéo où elles sont visionnées par un opérateur. Celui-ci alerte les services concernés lorsqu'un événement survient (centre de surveillance vidéo d'une commune ou d'un grand centre commercial).

DANS CERTAINS CAS, LA SURVEILLANCE PERMANENTE SERA FONDEE SUR DES DISPOSITIFS AUTOMATIQUES

Par exemple la surveillance d'un accès en voiture à une zone sensible pourra être basée sur l'identification automatique d'un véhicule par sa



plaque d'immatriculation. Le coût d'exploitation d'un tel système est nul ou très faible.

La vidéo protection peut être utilisée à titre principal pour répondre à un objectif de sécurité. Elle peut aussi être utilisée en complément de systèmes de protection, tels que la détection d'intrusion. Dans ce cas, la vidéo permet de réaliser une « levée de doute » suite à un déclenchement d'alarme. Elle évite ainsi l'envoi d'une équipe sur le terrain et permet de réaliser des économies significatives.

LA POSSIBILITE DE « PILOTER » LES CAMERAS A DISTANCE

La capacité offerte par un système de piloter les caméras à distance n'est pas systématique. Certains systèmes n'utilisent que des caméras fixes, l'image transmise étant un plan fixe. Dans d'autres systèmes, l'opérateur a la possibilité d'agir sur le système en pilotant les caméras : zoom avant et arrière, rotation haut/ bas, rotation droite/gauche. La spécification de cette caractéristique peut avoir des conséquences importantes sur l'organisation humaine. Il y aura, à un moment donné, un seul pilote de la caméra qu'il faudra désigner.

QUELLE CONTINUITÉ DE SERVICE ?

Comme tout équipement, un système de vidéo protection est susceptible de connaître des pannes, quelle que soit la qualité du matériel ou de l'entretien. Ces pannes peuvent conduire à des interruptions de service. Il est donc souhaitable que tout système soit doté d'une capacité d'auto test de ses divers constituants et d'alarme en cas de défaillance, un contrat de maintenance garantissant un rapide retour à la pleine capacité du dispositif.

Dans certains cas, notamment pour les applications très sécuritaires, une interruption de service n'est pas acceptable. Le système doit, dans ce cas, être défini en fonction de cette contrainte particulière : doublement des capteurs et des réseaux, enregistrement redondant, équipe d'intervention d'astreinte...

BESOINS DU PROJET DE VIDEO PROTECTION MUTUALISE AVEC D'AUTRES APPLICATIONS.

Exemple : profiter du déploiement d'un système de vidéosurveillance pour relier tous les bâtiments municipaux en informatique et en téléphonie.

3.3.5. LE BESOIN DETERMINE LES MODALITES DU STOCKAGE

Le stockage des images est un élément important d'un projet. Certaines spécifications techniques sont prévues dans l'arrêté du 3 août 2007, mais là encore il s'agit de spécifications minimales. Certaines applications peuvent nécessiter des conditions d'enregistrement supérieures. Le résultat attendu détermine la qualité des images enregistrées (taux et format de compression...), le nombre d'images par seconde enregistrées, la durée minimum et maximum d'enregistrement. La loi limite à un mois la durée maximale de conservation des images. La police judiciaire recommande une durée minimale de conservation des images de 7 à 10 jours.

La saisie peut nécessiter l'exportation d'un volume important d'images et cette contrainte doit être prise en compte au moment du choix du matériel à déployer. De même, il est important, pour l'exercice de la police judiciaire, que les images soient indexées (date, heure, lieu) pour faciliter l'exploitation des enregistrements.



3.4. SYNTHÈSE UL 2 : LES MESSAGES ESSENTIELS

Le diagnostic de sécurité a permis d'identifier des fragilités. En réponse à ces constats, une stratégie globale de sécurisation a été élaborée. Parmi les solutions possibles, la prévention par la vidéo protection peut être intégrée dans la démarche en tenant compte de ses spécificités.

Il faudra définir la meilleure synergie de complémentarité entre la vidéo protection et les autres solutions. Pour y parvenir, il est nécessaire de connaître les possibilités et les limites de la vidéo protection.

Le principe de fonctionnement de la vidéo protection est relativement simple : une caméra permet de surveiller de façon permanente ou non un espace donné. Les images peuvent être renvoyées vers un centre de surveillance vidéo où elles sont exploitées par un opérateur et enregistrées. Dans d'autres cas les images sont enregistrées directement et ne sont exploitées qu'en relecture, a posteriori.

La définition des besoins en vidéo protection est indispensable à l'efficacité d'un système. Cette définition des besoins doit être réalisée poste par poste : quelle caméra pour quel besoin ? Quel réseau pour quel besoin ?

Chacune de ces architectures possède des avantages et des inconvénients. Ce qui est primordial, c'est que le système réponde à l'objectif qui lui a été donné. Lorsque la réactivité est nécessaire, le choix d'un système supervisé s'impose.

La vidéo protection représente un investissement parfois modeste, mais dans certains cas importants, elle implique un engagement dans la durée : il faut hiérarchiser les besoins en définissant un territoire à traiter, puis des priorités et des objectifs ciblés au sein de ce territoire. Il faut profiter des opportunités du territoire.

La vidéo protection peut être utilisée à titre principal pour répondre à un objectif opérationnel de sécurité ou comme moyen complémentaire (exemple : outil de levée de doute en appui d'un dispositif de détection d'intrusion).



Analyse des besoins

UL 2

Les fonctionnalités propres à la Vidéoprotection



4. UL 3 LA PROTECTION DES LIBERTES PUBLIQUES



L'organisation humaine du projet

- UL 3 : La protection des libertés publiques
- UL 4 : Optimiser le coût du système de vidéoprotection
- UL 5 : L'organisation humaine du projet

4.1. LE REGIME JURIDIQUE DE LA VIDEO PROTECTION EN FRANCE ORGANISE QUATRE CAS DE FIGURE

1-Le lieu vidéosurveillé est privé

Il s'agit de locaux d'habitation, de loisirs ou professionnels. Sauf à respecter les règles du code civil et, pour les locaux professionnels, de droit du travail, l'installation est libre et ne demande ni autorisation ni déclaration.

2-la vidéo protection porte sur la voie publique, un lieu ou un établissement ouvert au public.

Dans ce cas, l'installation doit être autorisée par le préfet de département.

3-par exception aux cas précédents

Si le dispositif de vidéo protection conduit à des enregistrements inclus dans des fichiers structurés ou des traitements automatisés permettant l'identification des personnes, la compétence est exclusivement celle de la CNIL.

4-Il y a un risque particulier au regard du terrorisme

Le lieu concerné présente un risque particulier au regard du terrorisme et le Préfet peut non seulement autoriser mais prescrire. Il s'agit notamment des transports et des installations d'importance vitale.

En conclusion, le premier cas n'appelle pas d'intervention administrative. Le troisième est manifestement exceptionnel et le dernier relève de l'initiative préfectorale. C'est évidemment le deuxième cas qui sera le plus largement développé ci-après.

4.2. LA VIDEO PROTECTION DE LA VOIE PUBLIQUE, D'UN LIEU OU D'UN ETABLISSEMENT OUVERT AU PUBLIC

Les fondements du régime juridique de la vidéo protection sont posés par la loi. L'intervention du législateur résulte de l'article 34 de la Constitution : la loi fixe les règles permettant de garantir le respect des libertés publiques. Or, les systèmes de vidéo protection, dans le souci de concrétiser la sûreté en sécurisant la liberté d'aller et de venir, risquent, si les précautions ne sont pas prises, de porter une atteinte excessive au respect de la vie privée.

La loi traduit un équilibre entre soucis contradictoires et cet équilibre évolue. Cela explique des élargissements significatifs déjà apportés par la loi du 23 janvier 2006 dite

L'organisation humaine du projet de vidéoprotection

UL 3

La protection des libertés publiques





antiterroriste au premier texte (loi n°95-73 du 21 janvier 1995) et ceux que prévoira - probablement - la future loi de programmation et de performance de la sécurité intérieure.

Il demeure - et il demeurera - que la décision d'autoriser la mise en place d'un dispositif de vidéo protection résulte d'une appréciation de la proportionnalité entre la réduction de l'insécurité et l'augmentation du risque d'atteinte à la vie privée résultant de chaque dispositif.

Cette décision devra donc être précédée d'un examen concret.

- Des risques d'insécurité du lieu concerné et de la capacité du système de vidéo protection à les réduire.
- Des risques d'atteintes à la vie privée présentés par le système et, en conséquence, des précautions techniques et organisationnelles déployées pour les éviter.

C'est de la nécessité de cet examen concret, au cas par cas, que découle l'organisation - elle-même évolutive- de la procédure d'instruction.

Et c'est cet examen, après avis d'une commission départementale présidée par un magistrat judiciaire, qui permettra au Préfet de département de se déterminer et de donner, ou non, l'autorisation ou, dans certains cas, de prescrire.

Les textes réglementaires déterminent la composition du dossier joint à la demande, afin qu'il permette cette approche concrète.

Tout récemment, un décret modificatif en tire encore plus profondément les conséquences en prévoyant la constitution d'un dossier d'autant plus simple que le risque d'atteinte aux libertés créé par le type de situation pour laquelle la demande est faite, est moins grand.

On trouvera ci-après les réponses aux questions suivantes présentées

1 Pour quels systèmes faut-il une autorisation ?

2 Pour quels lieux faut-il une autorisation ?

3 Dans quels cas les Préfets peuvent-ils prescrire ?

4 Dans quels buts peut-on installer de la vidéo protection ?

5 Qui peut demander, gérer et qui peut avoir accès aux données ?

6 Quel est le mécanisme d'instruction des demandes ?

7 Quelles sont les garanties des libertés individuelles ?

La fiche thématique 7 précise quelle est la composition du dossier et les intervenants.

4.2.1. POUR QUELS SYSTÈMES FAUT-IL UNE AUTORISATION?

La loi s'applique à tous les systèmes de vidéo protection installés sur la voie publique ou dans les lieux ou établissements recevant du public.



- Que le dispositif technique fasse appel aux techniques analogiques ou numériques,
- Quand il y a simple visionnage d'images transmises à un poste central, sans dispositif d'enregistrement,
- Quand il y a transmission et enregistrement des images, mais seulement dans le cas où les images ne sont pas utilisées pour alimenter un fichier nominatif.

Un système qui n'enregistre ni ne transmet des images n'est pas un système de vidéo protection.

Il y a système de vidéo protection lorsqu'il y a 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, visionnées, en temps réel ou en différé, sur place ou dans un lieu distant, sur un écran type télévision ou sur un écran d'ordinateur.

Ainsi, un système ne prenant que des photographies ne sera jamais considéré comme un système de vidéo protection, quelque soit le support utilisé (appareil numérique). Par contre, un dispositif dans lequel des images sont enregistrées à l'occasion d'une intrusion ayant déclenché le fonctionnement de caméras et transmises à un poste de contrôle, correspond bien à la définition de la vidéo protection. Dans ce cas, ce dispositif participe des activités dites de télésurveillance régies par la loi n°83-629 du 12 juillet 1983.

4.2.2. LA COMPÉTENCE DE LA CNIL :

Lorsqu'il y a compétence de la CNIL, c'est-à-dire lorsque les enregistrements sont utilisés ou contenus dans des traitements permettant d'identifier, directement ou indirectement des personnes physiques, la loi de 1995 sur la vidéo protection ne s'applique pas et il n'y a pas lieu à demander une autorisation préfectorale.

Il convient dans ce cas de saisir la CNIL. Si le préfet est saisi à tort, il en informe le pétitionnaire et la CNIL.

Cette disposition appelle deux précisions :

La technologie utilisée pour la vidéo protection – numérique ou analogique- est indifférente. S'il n'y a pas connexion ou inclusion dans un fichier permettant l'identification, le préfet est seul compétent, que les caméras soient analogiques ou numériques.

Si en revanche, par utilisation d'un système dit intelligent il y a identification possible, le Préfet devient incompétent et la CNIL sera saisie.

Les deux autorités ne peuvent donc être compétentes en même temps ; c'est l'une ou l'autre.

4.2.3. DANS QUELS LIEUX L'AUTORISATION PREFERATORALE EST-ELLE NECESSAIRE?

L'autorisation préfectorale est nécessaire pour les installations visionnant la voie publique ou l'intérieur des établissements ouverts au public.

1° par voie publique il convient d'entendre certes les routes, mais aussi les voies d'eau.



2° le concept d'établissement ouvert au public mérite un développement un peu plus long.

Il n'existe pas de définition « technique » du « lieu » ou « de l'établissement ouvert au public ». Des éléments de doctrine et de jurisprudence développés ci-dessous, on peut conclure qu'est considéré comme un lieu ou établissement ouvert au public celui dans lequel chacun est susceptible de se rendre pour une raison autre que l'exercice de sa profession.

Définition jurisprudentielle de la notion de « lieu ouvert au public »

Il résulte de la jurisprudence de l'ordre judiciaire (par exemple, jugement du TGI de Paris du 23 octobre 1986 confirmé par l'arrêt de la Cour d'appel de Paris du 19 novembre 1986), qu'un lieu ouvert au public est un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions.

Définition jurisprudentielle de la notion « d'établissement ouvert au public »

Il résulte de la jurisprudence de l'ordre administratif, que ne sont considérés comme un établissement ouvert au public ni les locaux d'une caisse primaire d'assurance maladie non accessible au public (TA Lille 7/12/2007 : Caisse Primaire d'assurance maladie de Boulogne sur Mer), ni les locaux d'une université (TA Lille, 19/10/2004 : M.Simon Grysole n°0301944)

Sont considérés comme des établissements ouverts au public :

- Tous les services publics, dans les parties accessibles au public,
- Les établissements privés accueillant du public derrière guichet (mais non des locaux exclusivement réservés au personnel), par exemple les agences bancaires
- Les commerces de détail, (hors réserve)
- Les centres commerciaux,
- Les débits de boisson et les restaurants, (hors parties privatives)
- Les parties accessibles au public des établissements de soins ou maisons de retraite (parking et hall d'accueil par exemple) à l'exclusion des parties accessibles sous code, des circulations desservant les chambres et les chambres elles-mêmes.

Ne sont pas considérés comme des établissements ouverts au public :

- Les domiciles,
- La plupart des locaux d'entreprise,
- Les établissements scolaires, publics ou privés.



4.2.4. QU'EST CE QU'UN LIEU PRIVÉ?

La loi de 1995 sur la vidéo protection ne s'applique qu'à la voie publique et aux établissements recevant du public. Pas aux lieux privés.

La mise en place éventuelle de caméras doit cependant s'effectuer dans le respect de la vie privée. Il ne saurait être envisagé d'installer des caméras relatives à l'intimité de la vie privée sans le consentement des personnes concernées.

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 (articles L.120, L.121.8 et L.432-2-1, d'ailleurs visés dans la loi du 21 janvier 1995), 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 et qui n'y aurait pas consenti.

Locaux professionnels.

Les dispositions du **code du travail** applicables en cas de vidéo protection sur le lieu de travail :

3^{ème} alinéa de l'article L.2323-32 : « (...) Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. » Le comité d'entreprise doit être informé et consulté préalablement à la décision de mise en œuvre des caméras dans la mesure où elles permettent un contrôle de l'activité des salariés.

Articles L.1221-9 et L.1222-4 : « aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collecté par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi ». L'employeur ne peut mettre en œuvre un tel système de contrôle du salarié sans l'en informer préalablement. Dans le cas contraire, l'employeur serait en situation irrégulière.

Locaux d'habitation

Le système installé par un particulier à l'entrée de son domicile ne doit pas filmer la voie publique. Il ne demande pas d'autorisation.

Un hall d'immeuble constituera un lieu privé – ne demandant pas d'autorisation – s'il dispose d'un dispositif de fermeture ou de contrôle d'accès. Le fait que la serrure soit dégradée importe peu. Il s'agit d'une obligation de moyen et non de résultat. En revanche, un porche ou un passage constituent des lieux ouverts au public.

De même, un parking couvert ou non soumis à contrôle d'accès constitue un lieu privé non soumis à autorisation.

En ce qui concerne les aires de jeu, il est rare qu'elles soient soumises à contrôle d'accès; y installer un dispositif de vidéo protection **nécessitera** donc le plus souvent une autorisation.



Toutefois, le choix a été fait de ne pas faire entrer dans le champ d'application de la loi tous les systèmes relevant de la catégorie des « vidéo-portiers », considérant que leur mode d'utilisation ne répond pas aux critères de la loi et qu'en particulier, ils sont installés à l'entrée des locaux strictement privés et c'est la personne qui demande un accès à ces locaux qui actionne leur mise en fonctionnement : il s'établit un lien direct et immédiat entre le visiteur et son hôte, et ce qui se passe autour du visiteur, notamment la portion de trottoir ou de voie publique qui se trouve derrière lui n'entre pas dans le champ de vision de la caméra, ou s'il y entre, c'est dans des conditions telles qu'il est impossible de distinguer quoi que ce soit.

Quant aux systèmes de vidéo protection installée pour assurer la surveillance à distance de malades placés en soins intensifs, les lieux où ils sont installés ne sont pas considérés comme ouverts au public.

4.2.5. DANS QUELS CAS LES PRÉFETS PEUVENT-ILS PRESCRIRE?

Pour la prévention du terrorisme, les Préfets peuvent prescrire l'installation ou le renforcement d'un dispositif de vidéo protection :

- Pour les établissements qui, mentionnés au code de la défense – articles L1332-1 et L1332-2 – présentent une sensibilité particulière pour la capacité de la nation : par exemple centrales nucléaires, usines SEVESO, château d'eau, etc.
- Pour les infrastructures et moyens de transports collectifs,
- Les aéroports ouverts au trafic international.

La procédure d'instruction du dossier suit le cours normal après la décision de prescription prise par le préfet.

4.2.6. DANS QUEL CAS LA VIDÉO PROTECTION EST-ELLE OBLIGATOIRE?

L'exercice de certaines professions nécessite l'usage de la vidéo protection de manière obligatoire. Il en est ainsi par exemple dans les casinos, l'inspection-filtrage des passagers dans les aéroports et dans les transports de fonds.

L'article 12 de la loi 95-73 du 21 janvier 1995 impose une obligation de gardiennage ou de surveillance qui peut être satisfaite par l'utilisation de la vidéosurveillance. Il en est ainsi dans les parkings de plus de 200 places.

4.2.7. DANS QUEL BUT PEUT-ON INSTALLER DE LA VIDÉO PROTECTION ?

Le terme juridique utilisé est celui de finalité. Il appartient au demandeur d'indiquer et de démontrer – par le dossier constitué – que le système envisagé répond à cette ou ces finalités.

Présentation des différentes finalités



Sur la voie publique, les finalités possibles sont plus nombreuses que dans les lieux ou établissements ouverts au public.

Finalités qui peuvent être invoquées par les autorités publiques pour visionner sur la voie publique :

- 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 les lieux particulièrement exposés à des risques d'agression ou de vol ou à des actes de terrorisme.

Finalité qui peut être invoquée par des personnes privées pour visionner la voie publique :

Prévention des abords immédiats des bâtiments et installations relevant de personnes morales de droit privé situés dans des lieux susceptibles d'être exposés à des actes de terrorisme.

Sont concernés les établissements constituant une cible potentielle en cas d'attentat.

Finalités qui peuvent être invoquées par des autorités publiques ou des personnes privées (morales ou physiques) pour visionner un lieu ou un établissement ouvert au public :

- Assurer la protection des personnes et des biens contre les risques d'agression ou de vol dans un lieu ou établissement particulièrement exposé à ces risques,
- Assurer la protection des personnes et des biens contre les actes de terrorisme dans des lieux ou établissements susceptibles d'être exposés à des actes de terrorisme.

Il n'existe pas à proprement parler de jurisprudence permettant de définir la notion de « lieu particulièrement exposé à des risques d'agression ou de vol », seulement des décisions de justice, généralement de premier niveau, assez contradictoires et confirmatives des décisions préfectorales.

Deux recommandations peuvent être soumises à l'appréciation des maîtres d'ouvrage :



- Motiver sérieusement leur dossier par une description précise du risque,
- Pour cela prendre contact avec les services de police ou de gendarmerie, et notamment avec le référent sûreté spécialement formé à ce sujet.

Les autres usages de la vidéo protection

La vidéo protection ne répond pas seulement à une logique de sécurité. Dans une entreprise elle peut être, et est souvent, d'abord une logique d'exploitation de l'entreprise.

C'est seulement parce qu'il s'agit d'un établissement ouvert au public ou d'une autorité publique et donc d'un système « autorisé » que se pose la question suivante :

Puis-je utiliser dans un but complémentaire la vidéo protection autorisée pour une finalité prévue par la loi ?

Si l'usage supplémentaire est interne à la vie de l'organisme concerné la réponse est positive dès lors que les règles – par exemple le droit du travail – sont respectées.

A cet égard, la vidéo protection sur la voie publique pose un problème particulier aux collectivités territoriales qui sont des sortes « d'entreprises » certes particulières et dont la gestion des tâches s'exerce en partie sur la voie publique. En effet, actuellement, la gestion des risques industriels, naturels ou accidentels ne figure pas dans la liste des finalités. Et pourtant on ne peut pas imaginer qu'un service municipal visionnant un incendie qui se déclare ou une personne atteinte d'un malaise ne déclenche pas une intervention des pompiers ou du SAMU. Il apparaît donc légitime qu'une autorité publique ayant obtenu l'autorisation d'installer un dispositif de vidéo protection pour une finalité prévue par la loi, l'utilise aussi dans le cadre de ses compétences dès lors qu'elle le fait dans des conditions légales, en respectant en particulier le droit à la vie privée.

4.2.8. QUI DEMANDE, QUI VISIONNE, QUI A ACCÈS AUX DONNÉES?

Qui demande ?

En fait, deux questions sont posées :

1) Quel type d'organisme peut présenter une demande et plus concrètement quel type d'organisme peut visionner la voie publique ?

A cette question, la loi (alinéa 3 du II de l'article 10) répond : « l'autorité publique compétente » ce qui est plus large que l'autorité investie d'un pouvoir de police. Il en résulte que la demande pourra émaner :



- d'une collectivité territoriale sur son territoire,
- d'un groupement de collectivités ayant reçu compétence,
- d'une collectivité pour une autre par voie de convention,
- de responsables d'établissements publics (SNCF, RATP) ou de services publics (établissements pénitentiaires).
- De concessionnaires, éventuellement privés, affectataires d'une part du domaine public, et d'autre part, bénéficiaires d'une autorisation de voirie et chargés de l'entretien d'installations publiques.

2) Quand la demande est présentée par une personne morale, quelle personne physique présente la demande ?

La personne habilitée pour demander et prendre la responsabilité du fonctionnement du dispositif.

Qui gère et notamment qui visionne ?

S'agissant d'un dispositif concernant un établissement recevant du public ; ce seront ses personnels ou l'organisme qu'il mandate.

S'agissant de la voie publique, ce visionnage sera assuré par des employés de la personne publique agissant sous son contrôle. Le présent guide insiste d'ailleurs (cf. UL5 relative à l'organisation du projet et la fiche thématique n° 9 portant sur la formation) sur l'importance d'une bonne formation technique et déontologique.

Les personnes publiques ne peuvent déléguer à un organisme privé le visionnage, dès lors qu'il s'effectue sur la voie publique.

Elles peuvent en revanche coopérer entre elles et, en particulier, l'intérêt de la coopération intercommunale parfaitement possible doit être souligné – non seulement en termes financiers, mais aussi en termes de sécurité puisque cela permet d'assurer une certaine continuité territoriale du visionnage-.

Qui a accès aux données ?

Pour les employés du demandeur, le dossier de demande le précise et l'autorisation préfectorale l'indique finalement.

Mais il est d'intérêt commun que les services de police et de gendarmerie puissent également avoir cet accès.

Cela est possible non seulement en cas de procédure judiciaire par la voie de la réquisition mais également, dans le cadre de la police administrative, dès lors que l'autorisation préfectorale désigne les services habilités ou que le chef du service de police ou le commandant de gendarmerie procède à cette désignation sous la forme d'une habilitation individuelle.



C'est d'ailleurs pour que ce droit d'accès des services de police et de gendarmerie ait une portée concrète que des normes techniques imposent une qualité minimum des images. Cette disposition, résultant de l'arrêté du 3 août 2007, s'applique pour les systèmes déjà autorisés à partir du 22 août 2009 et immédiatement pour les nouvelles déclarations

4.2.9. QUELLE EST LA PROCÉDURE D'INSTRUCTION DES DEMANDES D'AUTORISATION ?

La composition du dossier et le processus d'instruction fait l'objet de la fiche thématique n° 7

Les règles, récemment modifiées du décret 96-926 du 17 octobre 1996, répondent aux principes généraux suivants :

1) le contenu du dossier de demande d'autorisation doit permettre au Préfet d'apprécier si le dispositif répond à une finalité prévue par la loi, et respecte les obligations légales comportant garanties des libertés et le principe de proportionnalité.

2) A cette fin le Préfet bénéficie d'un avis - qu'il suivra ou ne suivra pas - mais qui éclairera sa décision. Cet avis est donné par une commission composée d'un maire, d'un représentant de chambre de commerce, d'une personnalité qualifiée. Elle est présidée par un magistrat judiciaire du siège ou honoraire, afin d'insister sur la nécessaire attention au respect des garanties des libertés.

3) le Préfet dispose d'un délai de 4 mois pour se prononcer, délai au-delà duquel sa décision est réputée négative. Toutefois, cela ne lui interdit pas de prendre sa décision au-delà de ce délai.

4) l'autorisation est donnée pour 5 ans.

Le décret modifié 96-926 du 17 octobre 1996 apporte d'importantes modifications au dispositif réglementaire antérieur, notamment :

- En simplifiant la composition du dossier pour les établissements recevant du public, pour les petits dispositifs (moins de 8 caméras) ;
- En précisant que les informations à fournir ont un caractère limitatif,
- En créant la notion de périmètre vidéosurveillé à l'intérieur duquel le bénéficiaire de l'autorisation est libre du nombre et de l'emplacement des caméras, sauf à en informer, après installation, l'autorité préfectorale,
- En limitant à trois mois, qui peuvent être prolongés d'un mois à sa demande, le délai donné à la commission pour rendre son avis,
- En prévoyant que la commission doit entendre un fonctionnaire de police ou un militaire de la gendarmerie avant de donner son avis, ce qui lui permettra de mieux apprécier l'intérêt de l'installation projetée en termes de sécurité.

5) Le Préfet doit être informé des modifications relatives aux informations fournies dans le dossier initial. Si ces modifications sont substantielles, elles conduiront à un nouvel examen, se traduisant par une nouvelle autorisation ou par un refus.



Cette modification substantielle peut concerner :

- Le risque d'insécurité auquel le système veut remédier par exemple en cas de changement d'activité professionnelle d'un établissement recevant du public.
- Les caractéristiques techniques du système pour répondre aux risques d'insécurité, par exemple remplacement de caméras fixes par des caméras orientables donc qui changent le champ de vision.

6) En cas d'urgence et d'exposition particulière à un risque terroriste, le Préfet peut donner une autorisation temporaire de 4 mois. Il ne recueille pas l'avis préalable de la Commission départementale mais en informe son Président qui réunit la Commission durant cette période de 4 mois, afin qu'elle donne l'avis permettant la décision préfectorale applicable pour une durée de 5 ans.

4.2.10. QUELLES GARANTIES APPORTE LA PROCÉDURE D'INSTRUCTION DES DEMANDES D'AUTORISATION ?

La composition de la commission départementale, et notamment sa présidence par un magistrat judiciaire du siège ou honoraire, constitue une garantie importante.

D'autres garanties résultent :

- De l'installation autorisée,
- Des droits d'accès et d'information.

Garanties relatives à l'installation

La conciliation du souci de sécurité avec le devoir d'assurer le respect de la vie privée impose certaines limites aux systèmes de vidéo protection :

a. Entrées et intérieurs des immeubles d'habitation non visualisés

Articles 10 II 4^{ème} alinéa de la loi n°95-73 du 21 janvier 1995

« Les opérations de vidéo protection de la voie publique sont réalisées de telle sorte qu'elles ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées. »

b. Durée de conservation des images

Le préfet fixe, dans son autorisation, une durée maximale de conservation des images qui en application de la loi ne peut excéder un mois. En revanche, aucune disposition

législative ne permet à ce jour au préfet d'imposer à l'exploitant une durée minimale de conservation des images.

c. Pouvoir de contrôle de la Commission départementale

La commission départementale peut procéder à tout contrôle sur place pour vérifier que l'installation effectuée est bien conforme à l'autorisation.



Garanties pour le public

L'information du public

« Le public doit être informé de manière claire et permanente de l'existence du système de vidéo protection et de l'autorité ou de la personne responsable. »

Cette information se fait de la façon suivante.

Pour la voie publique :

« I. L'information sur l'existence d'un système fixe de vidéo protection est apportée au moyen de panneaux comportant un pictogramme représentant une caméra »

Pour les lieux et établissements ouverts au public :

« II. L'information est apportée au moyen d'affiches ou de panneaux.

Ces affiches ou panneaux indiquent le nom ou la qualité et le numéro de téléphone du responsable auprès duquel toute personne intéressée peut s'adresser pour faire valoir son droit d'accès, lorsque l'importance des lieux et établissements concernés et la multiplicité des intervenants rendent difficile l'identification de ce responsable ».

Le droit d'accès aux enregistrements

Le bénéficiaire de l'autorisation est « propriétaire » de ses images. Il doit garantir leur confidentialité sous réserve d'un droit d'accès.

« Toute personne intéressée peut s'adresser au responsable d'un système de vidéo protection 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 ».

La seule obligation posée à la personne faisant valoir son droit d'accès est qu'il doit s'agir d'une « personne intéressée », c'est-à-dire la personne qui a été filmée par les caméras.

Toutefois, le droit d'accès est limité dès lors qu'il fait obstacle aux droits d'un tiers. C'est pourquoi le responsable du système doit visualiser préalablement les images, afin de déterminer si le droit d'accès est possible.

De même, la visualisation des images enregistrées ne peut s'effectuer dans le local d'exploitation du système afin d'interdire au demandeur la vue des images en direct.

Afin d'assurer l'efficacité de ce droit d'accès, et sauf en matière de défense nationale la Commission départementale peut, en cas de refus, procéder à tout examen sur pièce et sur place.



4.3. L'ETHIQUE ET L'ACCEPTABILITE

La première partie de cette UL nous a montré que de nombreuses protections sont prévues par la loi pour garantir le respect des libertés individuelles.

Pourtant, le déploiement d'un dispositif de vidéo protection suscite toujours des craintes chez certains. Outre les garanties légales, les règles déontologiques et procédures mises en œuvre pour garantir le respect de la vie privée par l'opérateur sont donc un élément important dans un projet. L'expérience montre en effet qu'un certain nombre de mesures simples, spécifiques au type de lieu vidéoprotégé, sont de nature à rassurer le public concerné par un projet de vidéo protection

Même si ces freins sont à nuancer et si la vidéo protection fait rarement l'objet de réelles contestations et qu'il faut relativiser le risque de voir un projet menacé par une opposition massive de la part des administrés, ce risque sera d'autant moins grand que des mesures de communication auront été prises dès le démarrage du projet et que les règles déontologiques auront fait l'objet d'un consensus après débat.

4.3.1. CRAINTES RELATIVES À LA VIDÉO PROTECTION DE LIEUX PUBLICS ET PRIVÉS OUVERTS AU PUBLIC

La vidéo protection est généralement acceptée sans aucune difficulté dans les établissements ouverts au public (centres commerciaux, musées) ou dans des lieux de grand passage (gares routières ou ferroviaires). La vidéo protection sur la voie publique reste un sujet plus sensible.

La vidéo protection s'applique aux usagers des lieux, c'est-à-dire les clients, les visiteurs et les employés. Il est de bonne pratique que des actions de communication interne et externe facilitent l'acceptabilité du projet. On peut envisager par exemple une visite du PC ou la distribution d'une plaquette explicative.

Comme l'ont anticipé certaines collectivités (Lyon, Clichy la Garenne, Paris,...), la mise en place d'une charte d'éthique améliore l'acceptabilité du système de vidéo protection dont le rôle et les limites sont ainsi mieux comprises. Une action de communication doit favoriser la participation du plus grand nombre aux débats de production de cette charte. Cette communication doit également expliquer, de la façon la plus transparente, les motivations, les objectifs et les mesures de protections liées à la vidéo protection.

Exemples : Journal municipal, réunions publiques, conseil municipal, site web de la Ville, forum...

4.3.2. CRAINTES RELATIVES À LA VIDÉO PROTECTION DE LIEUX PRIVÉS

La vidéo protection mise en œuvre dans un lieu privé nécessite l'accord préalable des personnes concernées. Dans le cas de lieux de travail, cet accord n'est pas a priori acquis car la vidéo protection peut être perçue comme un moyen de surveiller le personnel.

Une action de communication et de négociation des règles d'exploitation et d'enregistrement est donc à mener en amont du projet avec les représentants du personnel :

- Présenter clairement les finalités du projet pour démontrer que la vidéo protection est justifiée et qu'elle n'aura pas d'autre fonction que d'assurer la protection des biens et des personnels ;



- Présenter les conditions restrictives d'utilisation des images. Il est important que les règles d'exploitation des images soient clairement précisées : qui accède aux images ? Dans quels cas ?

4.3.3. UNE ORGANISATION VISIBLE DE LA PROTECTION DES LIBERTES

Charte de déontologie et comité d'éthique

L'instruction de la demande d'autorisation par la Préfecture porte évidemment sur les mesures prises pour limiter au maximum le risque d'atteinte à la vie privée. En tout état de cause, les obligations légales doivent être remplies.

Mais au-delà, en particulier pour les grands systèmes de vidéo protection notamment sur la voie publique et dans les transports, le maître d'ouvrage verra son projet d'autant mieux accepté d'abord par le Préfet mais aussi et surtout par la population qu'il aura pris des précautions non légalement obligatoires mais complémentaires et qu'il les aura fait connaître par une communication appropriée et préalable.

Dans cet esprit, plusieurs communes ont adopté une charte déontologique et mis en place un comité d'éthique.

La charte déontologique va rappeler l'ensemble des mesures, légalement obligatoires que prend le maître d'ouvrage pour assurer que les images seront utilisées dans le seul but d'intérêt public poursuivi.

Par exemple, elle précise les conditions d'accès aux images, d'entrée dans les locaux, d'exercice pratique du droit à l'information. Elle prévoit le plus souvent un règlement intérieur de centre de supervision.

Enfin, elle peut instituer un comité d'éthique qui veillera à son application ou pourra faire toutes suggestions et être saisi par la population concernée. Elle déterminera sa composition...

Charte déontologique, règlement intérieur, comité d'éthique se sont pas des obligations légales mais pour les systèmes de vidéo protection sur la voie publique ou les transports publics, ils constituent des éléments utiles de la démarche globale de sécurité, utiles sur le fond pour veiller à l'absence de dérapages, utiles psychologiquement pour rassurer la partie de la population qui serait préoccupée au départ.

Dans cet esprit, on retrouve sur la fiche technique n° 15 deux exemples de villes ayant décidé de procéder ainsi.



4.4. SYNTHÈSE UL3 : LES MESSAGES ESSENTIELS

La vidéoprotection des lieux publics et ouverts au public est soumise à autorisation préfectorale.

Quand, par exception, les images contiennent un fichier nominatif, elles relèvent de la CNIL.

Le dispositif doit avoir pour but la sécurité des personnes et des biens.

L'instruction de la demande va vérifier ce but ainsi que les précautions prises pour ne pas porter atteinte à la vie privée.

Tout récemment, un décret a simplifié la composition du dossier de l'autorisation.



5. UL4 : OPTIMISER LE COUT DU SYSTEME DE VIDEO PROTECTION

Le coût d'un système de vidéo protection est très variable.

Très modeste quand il ne comporte pas transmission et visualisation en temps réel, ou quand il y est procédé par une organisation technique et humaine préexistante. Il va devenir important quand il cumule les facteurs de complexité et quand on part de rien.

On tentera ici de répondre à trois questions :

- Quelle est la structure de coût ?
- Comment les réduire ?
- Comment les financer ?

On précisera que ce développement concerne surtout les projets relativement importants.

5.1. QUELLE EST LA STRUCTURE DE COUT ?

Quatre types de coûts sont à appréhender :

	A la mise en route	Annuel
Matériel	Investissement mobilier et immobilier	Maintenance préventive et curative
Humain	Recrutement, formation initiale	Frais de personnel Formation continue

5.1.1. LES COÛTS D'INVESTISSEMENTS IMMOBILIERS ET MOBILIERS

La liste des coûts d'investissement présentée ici ne peut être exhaustive. On peut toutefois proposer quelques exemples, en distinguant les investissements immobiliers et mobiliers.

Investissements immobiliers :

Pour les projets complexes, nécessitant en particulier l'aménagement d'un centre spécifique pour la supervision, on trouvera des coûts incompressibles liés à la mise en place d'une salle technique : faux plancher, faux plafond, climatisation, alimentation secourue et régulée, éclairage... Ces frais de mise en place sont élevés (entre 50 et 100 000 euros, parfois plus) et sensiblement identiques quel que soit le nombre de caméras du système. Il





est donc préférable d'éviter, pour les petits systèmes, la création ex-nihilo de telle structure et de chercher plutôt des solutions d'exploitation mutualisée auprès d'un centre existant lorsque c'est techniquement et réglementairement possible.

Le poste budgétaire considéré comme le plus lourd pour les projets de vidéosurveillance urbaine est certainement celui lié aux travaux de génie civil correspondant au déploiement d'un réseau adapté (réseau fibre optique, lorsque ce média de transmission est retenu). La mise en œuvre complète d'un nouveau réseau de fibre optique peut atteindre 50% du coût total du projet. Il est fortement conseillé alors d'envisager au maximum les solutions de contournement qui sont nombreuses : technologies sans fil, location de fibre noire ou location de bande passante, mutualisation des infrastructures avec d'autres partenaires ou d'autres services que la vidéo, acquisition d'une prestation de service de fourniture d'image...

Les coûts liés au transport de l'image sont néanmoins en **décroissance rapide** : le haut débit coûte de moins en moins cher, particulièrement lorsque le dossier global est envisagé de manière astucieuse et en optimisant au mieux les complémentarités entre les liens filaires, aériens et opérés.

Il est très important que ces alternatives soient envisagées de façon très ouverte en début de projet, afin d'éviter les orientations par défaut vers un schéma, simple, mais extrêmement pénalisant sur le plan financier, qui consiste à réaliser systématiquement une infrastructure dédiée pour le transport des images.

Cette problématique vaut également pour les systèmes plus simple, à l'intérieur d'un bâtiment par exemple ou sur un site restreint, pour lesquels la mise en place de systèmes de transmission innovants, sans fil du type Wi-Fi ou WI-Max ou sur support de courants porteurs (utilisation des lignes électriques existantes) peut occasionner des économies d'investissement tout à fait significatives.

Investissements mobiliers :

Ce volet concerne l'ensemble des éléments qui constituent la chaîne d'un système de vidéo protection, depuis l'acquisition jusqu'à la restitution des images. Elle comporte donc en particulier : les équipements d'acquisition (caméras) et leurs supports physiques (dômes, tourelles, fixe...), les alimentations électriques (EDF, solaire, éolien...), les équipements de stockage des images, les équipements de conversion et de transmission, les logiciels, les équipements liés à l'exploitation des images (postes de travail des opérateurs), l'aménagement des salles techniques, d'exploitation et de relecture (climatisation & sécurisation). Ces dépenses comportent la particularité d'être proportionnelles au nombre de caméras et elles ont tendance à baisser de manière significative avec l'apparition de nouvelles technologies dites à bas coûts. Aux deux extrémités de la chaîne, on note la même tendance à la baisse avec, d'un côté, la chute du prix des caméras numériques de qualité et, de l'autre, la chute du coût des enregistreurs liée à celle des média de stockage.

Assez souvent, les projets ne profitent pas pleinement de cet effet de baisse des composants de système de vidéo protection, du fait d'une mauvaise évaluation fonctionnelle du système cible. La chute des coûts s'accompagne, en effet, d'une augmentation constante des capacités, des performances et des possibilités fonctionnelles qui maintient les prix par le renouvellement extrêmement rapide des générations technologiques. Il faudra donc rester vigilant à sélectionner le système le plus approprié aux besoins recensés plutôt que le système au plus proche de l'état de l'art, cher et mal adapté à une problématique qui ne nécessite pas la technologie la plus élaborée. En tout état de cause, pour bâtir un système pérenne, il vaudra mieux définir un système évolutif - donc ouvert - plutôt qu'un système évolué, voire en rupture technologique, mais fermé.

Il convient également de noter que les caméras actuelles permettent le plus souvent de profiter d'une alimentation électrique directement apportée par le réseau de données (norme POE), ce qui permet de s'affranchir de la mise en place d'un système d'alimentation spécifique pour chacune des caméras. Ces nouvelles technologies permettent ainsi de réaliser des économies substantielles sur la mise en place des points de collecte de l'image.



Pour les projets d'une certaine complexité, il est conseillé de prévoir une partie étude / accompagnement, parfois appelée « Assistance à Maîtrise d'Ouvrage » expérimentée, indispensable pour définir les choix structurants du projet.

5.1.2. LES COÛTS DE FONCTIONNEMENT

L'évaluation et surtout la prise en compte des coûts de fonctionnement sont un des critères majeurs de bon dimensionnement du budget et donc de la réussite du projet. Parmi ces coûts, on citera notamment :

Les coûts liés au personnel d'exploitation

La rémunération du personnel en charge de l'administration et de l'exploitation du système peut constituer le poste le plus important, notamment dans le cas d'une exploitation 24/24.

Il conviendra, bien entendu, de ne pas sous estimer les coûts des formations initiale et continue du personnel.

Les coûts liés à la maintenance

Il faut évaluer le coût annuel moyen en maintenance préventive, auquel s'ajoute le coût annuel moyen en maintenance curative, avec un délai courant d'intervention.

5.2. COMMENT LES REDUIRE ?

5.2.1. LA MUTUALISATION : UNE PISTE ESSENTIELLE DE RÉDUCTION DES COÛTS

La structure des coûts définie plus haut permet d'envisager deux facteurs importants de réduction de coûts, applicables dans de nombreux projets : l'un est relatif à la mutualisation des centres de supervision, il permet la réduction des frais d'infrastructure et de personnel, l'autre concerne principalement la mutualisation des infrastructures de transport des images, il limite considérablement les frais de mise en place d'infrastructures de communication et, par la suite, minimise les redevances associées.

Mutualisation de la supervision : centre partagé de surveillance vidéo

Dans ce cas, il est crucial d'établir toutes les conventions nécessaires pour ce partage, en respectant scrupuleusement les textes de lois s'appliquant à chaque partie vidéoprotégée. Il peut être nécessaire dans certains cas de monter des structures dédiées (association regroupant les commerçants par exemple).

- Intercommunalité,
- Inter bailleurs,
- Inter transporteurs,
- Centre commercial,

Pour les collectivités territoriales qui exercent un pouvoir de police, cette mutualisation n'est possible qu'entre elles. Mais, dans ce cadre, elle est vivement recommandée. : Le



coût global d'un centre de supervision s'élève rapidement à 400 000€ par an et n'est pas proportionnel au nombre de caméras. La coopération est donc très rentable.

Les collectivités territoriales peuvent, dans leur centre de supervision, accueillir d'autres personnes publiques et, sous certaines conditions, des personnes privées.

Enfin, la mutualisation de la supervision entre personnes privées est libre.

Mutualisation des réseaux

Force est de constater que les cas de réseaux mutualisés à ce jour dans le domaine de la vidéo protection sont encore limités.

La mutualisation dans le transport de l'image peut pourtant s'appliquer à plusieurs niveaux, sans blocage formel réglementaire ou technique :

Les passages physiques :

Les égouts, les conduites d'eaux pluviales, les fourreaux d'éclairage public, une ancienne conduite de gaz désaffectée... peuvent être partagés.

Deux exemples réels :

- réutilisation de fourreaux destinés à l'origine à l'arrosage public,
- enfouissement à 20cm dans une micro tranchée recouverte de ciment, dans le lit bétonné d'une rivière traversant toute la ville.

Les câbles optiques :

Il est parfois très peu coûteux de solliciter le propriétaire d'un câble optique existant : rares sont les cas où toutes les fibres sont utilisées, et ce propriétaire sera souvent ravi de pouvoir vendre, ou louer, quelques paires de fibre...

Le réseau IP :

Le réseau de transmission est souvent dédié à la vidéo protection, alors que, par nature, le réseau IP est construit pour véhiculer plusieurs flux simultanés, en respectant les contraintes de qualité de transmission de chaque flux, appelées "Qualité de Services" ou QS (un flux de données ne possède pas les mêmes caractéristiques qu'un flux de téléphonie, ou de vidéo protection...).

Dans ce partage de réseau, il est souvent rétorqué qu'il réside un risque sur la confidentialité, le brouillage, l'écoute, la saturation etc. A ce jour, des mécanismes normalisés existent et permettent d'étanchéifier les réseaux (réseaux virtuels ou VLAN) et de lever facilement ces objections.

Les techniques sont prêtes, normalisées et disponibles. Les freins sont peut-être plus dans nos esprits.

5.2.2. LE RETOUR SUR INVESTISSEMENT GLOBAL (ROI)

La décision de mise en œuvre d'un projet de vidéo protection passe souvent par une phase de conviction, des élus, des managers ou des financiers, s'appuyant sur une prévision



de retour sur investissement (ROI) de la solution proposée. Les éléments ci dessous permettent d'éclairer cette question rendue complexe par la nature de la vidéo protection.

Quels sont les retours sur investissement à attendre ?

-Il peut d'abord s'agir d'économies :

- Sur les primes d'assurance. Une commune qui avait développé, depuis 6 ans, un dispositif significatif de vidéo protection (environ une caméra pour mille habitants) a vu ses primes d'assurance divisées par 10.
- Sur les personnels de garde. Une communauté urbaine qui affectait 14 policiers municipaux à la garde de son garage des bus et tramways l'a placé sous vidéo protection et réduit le personnel à 2.
- Sur la non-destruction de bâtiments publics. En 2007, une commune a pu éviter qu'un incendie se développe dans une salle de sport parce que le dispositif de vidéo protection l'a immédiatement décelé.

-Il peut s'agir d'une augmentation de clientèle. C'est notamment le cas pour certains parkings où des places restaient vides et donc non louées du fait de l'insécurité ; la même observation a été faite pour des moyens de transport (bus).

-il est en revanche plus difficile de chiffrer l'effet financier de la diminution de la délinquance. Si les Britanniques disposent de modèles comparant au coût de la vidéo protection de voie publique l'économie résultant des délits évités, ce type d'études n'a pas été conduit en France. C'est alors à une appréciation plus globale que se livreront les décideurs.

5.3. COMMENT LES FINANCER ?

LES AIDES POTENTIELLES

Le panorama des sources possibles de financement, ou d'aide, est disponible dans la fiche thématique n°5: « sources et moyens de financement pour les différents types d'opérateurs »

Les aides d'Etat

Le principal vecteur des aides d'Etat est le Fonds interministériel de Prévention de la Délinquance (FIPD) qui peut, sous certaines conditions, financer études et réalisation de projets vidéoprotection sur la voie publique au profit des actions conduites principalement par des collectivités territoriales.

De manière plus secondaire, il convient de signaler :

- Que la vidéo protection ouvre droit au fonds de compensation pour la taxe sur la valeur ajoutée (FCTVA) ;
- Que la dotation globale d'équipement des petites communes peut financer de la vidéo protection ;

Enfin, et pour l'habitat social, la vidéo protection peut figurer au compte d'exploitation des opérations d'aménagement et de résidentialisation financées par l'Agence Nationale pour la rénovation urbaine (ANRU)

Les aides régionales et départementales



Au delà des équipements qui relèvent d'eux (en particulier collèges ou lycées), de nombreux départements ou régions ont mis en place des mécanismes de subvention, parfois à taux élevé, pour les investissements publics de vidéo protection.

Au delà des aides, la forme du financement d'un projet de vidéo protection peut permettre de lisser, ou de mieux maîtriser, les dépenses engagées. Le partenariat public privé constitue une forme de financement qui se développe, en particulierité pour les collectivités territoriales. De même, les contrats de location peuvent constituer une alternative intéressante à la création d'une infrastructure dédiée et propriétaire de vidéo protection.

LE PARTENARIAT PUBLIC – PRIVE (PPP)

- 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 services 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 exerçant 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 recours au Contrat de Partenariat est limité aux cas, soit d'urgence, soit de complexité du projet (ce qui sera toujours le cas pour la vidéo protection). 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.
- L'intérêt du PPP tient à ce que le partenaire privé pourra rechercher des clients –il sait le faire- pour ce qui est mutualisable, en fait le système de transmission. Le maître d'ouvrage public du système de vidéo protection n'aura donc pas à payer un loyer correspondant à l'intégralité de l'investissement.
- En outre, un maître d'ouvrage mettant en place un système complexe peut trouver avantage à avoir un interlocuteur unique.
- Voir également la fiche n°5 : sources et moyens de financement pour les différents types d'opérateurs.

LA LOCATION

Les avantages d'un contrat de location :

- Une solution flexible :

En cours de contrat, le locataire peut décider de faire des adjonctions de matériels ou de services, en se calant sur la durée initiale, ou en allant au-delà de cette durée. Le locataire peut ainsi profiter des évolutions technologiques.

- Une souplesse budgétaire :



Les loyers sont comptabilisés en charge d'exploitation. Pas d'incidence sur la trésorerie et la capacité d'endettement du locataire. Plus grande souplesse aussi dans sa durée. Une sécurité budgétaire :

L'intégration des services dans la location élimine les risques de coûts cachés : pas d'indexation de la maintenance, coût de la maintenance fixe pour la durée de la location.

- Un renfort dans la garantie du projet :

Le maître d'ouvrage n'a qu'un seul interlocuteur pour un projet global (produits, maintenance, télésurveillance et le financement du projet).



5.4. SYNTHÈSE UL 4: LES MESSAGES ESSENTIELS

Le principal frein au développement des systèmes complexes de vidéo protection est leur coût actuel. Il faut distinguer, d'une part les coûts d'investissement liés à l'installation du système et, d'autre part, les coûts de fonctionnement liés à l'exploitation : opérateurs supervisant le système, maintenances préventive et curative.

Il convient, dans un premier temps, de rechercher le système le plus adapté à son besoin opérationnel ; profiter de la chute des prix sans participer à la course aux solutions les plus technologiquement avancées,

Il faut, dans la mesure du possible, mutualiser son installation avec d'autres partenaires ou avec d'autres usages pour le même maître d'ouvrage. Cette mutualisation peut ne concerner que certaines « parties » d'un système : exploitation, réseau... Cette mutualisation peut susciter des économies considérables, elle nécessite toutefois une remise en question parfois forte des organisations en place.

Après avoir pris en compte les économies rendues possibles par le projet de vidéo protection, il convient de solliciter toutes les aides financières proposées et envisager les montages financiers possibles. L'Agence Nationale pour la Rénovation Urbaine (ANRU), le FIPD... offrent par exemple chaque année des possibilités de financement.



**L'organisation
humaine du
projet de
vidéoprotection**

UL 4

**Optimiser le coût
du système de
vidéoprotection**



6. UL5 : L'ORGANISATION HUMAINE DU PROJET

Un programme d'accompagnement est très généralement associé à la mise en place d'un nouveau programme, quel qu'il soit. Il faut, en effet, mettre en place une organisation particulière permettant d'assurer d'une part le bon déroulement du projet, puis de permettre le bon fonctionnement du système. Il s'agit, avant tout, de définir une répartition claire des rôles et des responsabilités des différents intervenants dans le cycle de vie du système.

6.1. LA PERSONNE RESPONSABLE DU SYSTEME

Qu'il s'agisse de systèmes de vidéo protection de taille très réduite (commerce, banque...) ou de systèmes de grande ampleur (commune, centre commercial...), et ce, indépendamment du contexte d'usage public ou privé des caméras, il est toujours conseillé de nommer une personne dite « responsable du système ». Cette personne sera en charge de répondre à toute demande relative au système, de s'assurer de son fonctionnement, de contacter les partenaires extérieurs et, dans le cas où une assistance à maîtrise d'ouvrage a été prise, d'être l'interface entre celle-ci et les ressources internes.

Pour résumer, **la personne responsable du système est la garante du fonctionnement du système et l'interface avec l'extérieur**, elle est la personne à contacter en premier lieu pour toutes questions relatives au système. Elle est également force de proposition pour faire évoluer celui-ci.

En général, la personne responsable du projet est celle qui sera désignée comme le responsable juridique du système autorisé.

Lorsque le système relève de la loi du 21 janvier 1995, il peut être distingué entre la personne titulaire de l'autorisation préfectorale et la, ou les, personnes responsables. L'article 1^{er} du décret modifié n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance prescrit que la demande d'autorisation préalable à l'installation d'un système de vidéosurveillance doit comprendre « la désignation de la personne ou du service responsable du système et, s'il s'agit d'une personne ou d'un service différent, la désignation du responsable de sa maintenance ».

Pour les personnes publiques, la personne responsable n'est donc pas nécessairement son représentant ou l'exécutif. Il peut s'agir d'un élu ayant délégation, ou un chef de service. La désignation doit concerner tant l'exploitation que la maintenance du système.

Pour les propriétés privées ouvertes au public, la personne responsable visée dans l'autorisation peut être un responsable sécurité ou un chef de centre qui assure le suivi quotidien du système.

Si le système relève de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un « responsable du traitement » devra également être désigné dans le cadre de la déclaration ou de la demande d'autorisation adressée à la CNIL

Néanmoins, dans les gros systèmes, il faudra porter une attention particulière au choix de la personne responsable du projet.

Un projet de vidéo protection est composé de trois domaines différents : la sécurité proprement dite, le juridique et la technique. Pour les projets importants, il est parfois nécessaire que chaque domaine soit traité par une personne compétente, sous la direction du responsable du système. Il s'agit le plus souvent d'une responsabilité fonctionnelle, l'expert juridique ou le spécialiste technique n'étant pas affecté à 100% sur le projet de vidéo protection. Même dans ce cas, il est utile que la personne responsable du système soit en mesure de comprendre et de suivre les trois composantes d'un projet de vidéo





protection. Pour des systèmes de taille plus réduite, la personne responsable du système devra souvent être en mesure d'assurer le suivi de ces trois domaines.

Si une personne a été désignée en interne pour assurer le diagnostic de sécurité, cette personne peut constituer un bon choix pour assurer cette fonction, puisqu'elle est déjà sensibilisée aux différents problèmes rencontrés et également aux composantes sécuritaire et technique du projet. Il est important de bien comprendre que le responsable désigné doit accepter de prendre en compte des aspects qui ne sont pas habituellement dans son champ de compétence. C'est pourquoi on peut envisager de désigner un tiers neutre qui ne connaît rien à la problématique et qui dispose d'une forte capacité de manager des techniciens.

Les tâches du responsable du projet sont différentes avant et après l'installation du système de vidéo protection. Des compétences de suivi de projet sont requises dans la phase amont, alors que des compétences relationnelles et d'encadrement sont plutôt requises lors de la phase de fonctionnement. Il n'est donc pas exclu que la personne responsable du projet puisse changer entre les deux phases, tout en veillant à ce que le transfert des connaissances soit bien assuré.



6.2. LA GESTION DU PROJET : AVANT L'INSTALLATION

Lors de la phase en amont de la mise en place et de l'exploitation du système, la personne responsable du système sera chargée de veiller au bon déroulement des différentes étapes du projet, d'en assister les acteurs, d'être le point d'entrée entre les acteurs internes au projet (juristes, techniciens, opérationnels, décideurs...) et les acteurs extérieurs (forces de police et de gendarmerie, titulaire du marché, cabinet conseil, commission départementale, .).

Par exemple, si le système relève de la **loi du 21 Janvier 1995**, cette personne pourra assurer la réalisation du dossier de demande d'autorisation en préfecture en s'appuyant sur les personnes compétentes en interne, Elle pourra également assurer la liaison entre l'entreprise qui réalise les travaux d'installation du système et les interlocuteurs en interne.

La personne responsable du projet sera par ailleurs en charge de veiller à ce que tous les axes de mutualisation mis en valeur lors du diagnostic de sécurité soient mis en œuvre et optimisés.

Comme nous l'avons vu dans l'unité de lecture concernant le diagnostic de sécurité, même pour les petites installations il est conseillé d'aviser les acteurs locaux de sécurité intérieure, de se renseigner sur l'existence d'un dispositif territorial de sécurité tel qu'un conseil local de sécurité et de prévention de la délinquance (CLSPD), afin de réaliser toutes les synergies nécessaires

La circulaire du ministre de l'intérieur du 26 mai 2008 précise que les projets de vidéo urbaine doivent s'appuyer sur un comité de pilotage intégré au CLSPD. Le recours systématique aux référents sûreté (police ou gendarmerie), dès l'origine du projet, doit être fortement encouragé. C'est la phase de l'analyse de besoins qui doit être menée avec soin. C'est aussi l'occasion de réfléchir en amont sur les questions essentielles suivantes :

- Système supervisé ou non, 24h/24 ou non et, dans ce cas, sur quelles plages horaires,
- Centre de gestion des images, mais aussi des alarmes incendie ou intrusion, de renvoi du standard, etc.
- Renvoi des images ou non vers la police ou gendarmerie,
- Rédaction d'un protocole d'intervention entre les vidéosurveilleurs, la police municipale et les forces de sécurité intérieure,
- Localisation des caméras en fonction des besoins de sécurité,



- Lieu de stockage et modalités d'accès si le système n'est pas supervisé.

Pour un petit système (commerce), cette personne pourra être responsable de :

- Assurer le lien avec les forces de police et de gendarmerie, la société de gardiennage, la société mère, les sociétés d'assurance... pour cibler les besoins, les gains et les limites dans l'installation du dispositif,
- Réaliser les démarches juridiques associées à l'installation d'un système de vidéosurveillance (constitution, dépôt et suivi des dossiers),
- Vérifier le bon déroulement des travaux conformément à la commande.

Pour un système plus important, la personne responsable du système s'appuiera sur :

- un responsable sécurité, s'il y en a, (police municipale, gardien, agents de sécurité...), pour aider à la définition des besoins,
- un responsable juridique, pour constituer le dossier de demande d'autorisation, qui sera l'interface entre la commission départementale et les ressources internes pour répondre aux différentes questions,
- Le responsable technique et l'entreprise réalisant les travaux ou le cabinet retenu pour l'assistance à maîtrise d'ouvrage.

Rappel : il n'est pas toujours nécessaire de nommer ces responsables à temps plein. Mais leur disponibilité doit être adaptée à la taille du projet et, dans tous les cas, suffisante pour être efficace.

6.3. LA GESTION DU QUOTIDIEN : APRES L'INSTALLATION

La personne responsable du système est la garante de l'efficacité du système. Elle sait qui contacter lorsque le système tombe en panne. Elle sait où sont placés les enregistreurs et les différents éléments du système de vidéosurveillance. Elle est force de proposition pour faire évoluer le système et mettre à jour les composants défectueux ou obsolètes. Elle est en mesure d'aider les forces de police et de gendarmerie lorsqu'un accès aux images est requis. Elle est également en mesure de répondre aux personnes faisant valoir leur droit d'accès aux images (Cf. fiche N°6). Elle en maîtrise les protocoles d'exploitation et d'exportation. Le cas échéant, elle assure la gestion des opérateurs dans le cas de systèmes supervisés.

6.3.1. LES RELATIONS AVEC LES PARTENAIRES EXTERIEURS

Comme évoqué dans l'UL1, il est fondamental d'associer ou de consulter les partenaires extérieurs lorsque l'on décide de mettre en place un système de vidéo protection, d'abord pour augmenter l'efficacité du dispositif, mais également pour tenter de réduire les coûts associés. Cette démarche est également valable tout au long de la vie du système, pour résoudre des problèmes ou envisager des évolutions. La personne responsable du système est la meilleure personne pour assurer le lien entre le système de vidéo protection et les partenaires extérieurs.

Exemple : Un commerce installé dans une rue piétonne ou dans un centre commercial dispose d'un système propre de vidéo protection. Il est judicieux que le responsable du système soit la personne en charge des relations avec les autres magasins de la zone ou avec le gérant du centre commercial sur les questions de sécurité.



6.3.2. L'ACCES AUX IMAGES ENREGISTREES

L'intérêt d'un système de vidéo protection réside le plus souvent dans les images qu'il enregistre. Ce postulat simple et apparemment anodin est cependant souvent battu en brèche par un manque d'organisation. Cette organisation est formalisée par la procédure d'accès aux images enregistrées.

Exemple : Un système de vidéo protection dans un établissement fermé le week-end enregistre les images pendant sept jours. Une démarque inconnue est constatée six jours après la date probable de l'événement et le responsable de l'accès aux images est absent. L'accès aux images est rendu impossible si un minimum d'organisation préalable n'a pas été pensé par l'établissement.

Il est donc important de prévoir une organisation solide autour de l'accès aux images, pour autoriser ou non l'accès des opérateurs aux enregistrements. La prise en compte des deux points suivants est fortement recommandée :

- Prévoir un numéro de téléphone (celui qui est inscrit sur le pictogramme) et les modalités pour l'accès aux images pour les services de sécurité « en dehors des heures de bureau » et ne pas hésiter à prévoir une personne remplaçante en cas d'absence prolongée du responsable du système. Le responsable du système peut ne pas être la seule personne à réaliser les exportations, cependant, les autres personnes doivent être clairement identifiées et habilitées.
- Prévoir des protections simples pour éviter que tous les membres du personnel ou que des « visiteurs » puissent librement y accéder (local fermé à clef, protection mécanique autour du système d'enregistrement, système de mot de passe et de login pour les systèmes numériques...). En effet, l'accès aux images et surtout aux images enregistrées est réglementé et leur liberté d'accès ne peut être confiée à tous les employés ou à tous les opérateurs de vidéosurveillance.



6.3.3. LES DOCUMENTS À PRÉVOIR

Dans toute structure ou organisation, un minimum de documents de gestion doit être prévu. Ces documents sont souvent un critère de bon fonctionnement du système, ils permettent de mettre en exergue les manques de sécurité, les manques opérationnels, et les atouts du système ; ils peuvent s'avérer tout aussi important que le système lui-même.

LE REGISTRE DES ENREGISTREMENTS

D'un point de vue opérationnel, ce registre est très fortement conseillé, car il permet de retracer les opérations de sortie des images du système. Dans les systèmes soumis au régime juridique de la loi du 21 Janvier 1995, le **décret modifié n°96-926 du 17 octobre 1996** impose que le titulaire de l'autorisation tienne un registre mentionnant les enregistrements réalisés, la date de destruction des images et, le cas échéant, la date de leur transmission au parquet. L'**arrêté du 3 août 2007** impose également que ce registre soit informatisé pour les systèmes numériques de huit caméras ou plus et qu'il mentionne les opérations d'exportation des images (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), la suppression de l'image.

Sont mentionnés dans ce document:

- Toutes les exportations d'images réalisées à la demande des services de police et unités de gendarmerie, en police judiciaire ou administrative,



- Toutes les relectures réalisées par ou pour les services de police,
- Les relectures effectuées par les personnes ayant fait valoir leur droit à l'image,
- Les enregistrements effectués et la date de leur destruction.

Cette procédure permet d'éviter que des images soient sorties du système et utilisées à l'insu de personnes filmées.

LE REGISTRE DES ACCES AUX INSTALLATIONS

Ce document porte la mention de tous les accès aux installations liées à la vidéo protection par des personnes étrangères au service qui en a la charge:

- Locaux techniques,
- Centre de surveillance vidéo.

Ce document peut être sous format papier ou informatisé. Par exemple, ce peut être le journal des accès badgés lorsqu'un tel système est disponible.

Il portera la mention des personnels de police et de gendarmerie spécialement habilités et nominativement désignés pour avoir le droit d'accéder aux installations, dans le mode administratif.

LA MAIN COURANTE DE L'ACTIVITE ET DES EVENEMENTS

La main courante concernant les événements visualisés par les opérateurs et les prises de poste, est utile pour la gestion du centre de supervision. Certains communes ont créé un logiciel permettant un partage d'informations opérationnelles et statistiques avec les forces de sécurité intérieure (cartographie de la délinquance, des interventions, etc.). C'est aussi l'occasion de créer des outils mesurant la performance des caméras.

Souvent mal appréhendée dans la réflexion qui précède l'installation d'un système de vidéosurveillance, la partie concernant le fonctionnement administratif se révèle très lourde pour les chefs de centre. C'est la face immergée de l'iceberg, elle est génératrice de beaucoup de perte de temps, cependant c'est elle qui va présider à l'efficacité du système.

La main courante, dans sa formule papier, a montré aujourd'hui ses limites et c'est vers les mains courantes électroniques, outil d'analyse, qu'il est conseillé de s'orienter pour optimiser la lisibilité et la traçabilité des événements, ainsi que la mise en évidence des problèmes de sécurité ou de sûreté.

Journal de bord du chef de centre, mémoire vive et passive du service, la main courante est à même de collecter, enregistrer, tracer et diffuser l'activité du service dans son intégralité et dans ses moindres détails. Outil de communication, il est préconisé d'y intégrer la transmission automatique de l'information en direction des services intéressés.

De préférence professionnelle et spécifiquement dédiée à la vidéosurveillance, la simplicité est à rechercher dans son utilisation qui pourra être formatrice pour le personnel. Sa conception devra la rendre réductrice des tâches administratives, et performante dans la gestion des ressources humaines qu'elle devra prendre en considération dans sa globalité. Elle devra faciliter la rédaction des rapports et automatiser la production des statistiques dans des formules unies ou multicritères.

Il est fortement conseillé de respecter, dans la rédaction des critères de qualification des infractions ainsi que dans les critères de signalement des individus, le langage commun à l'ensemble des services de sécurité. Il est également recommandé que la main courante soit



couplée au système de vidéo protection, afin de remonter de manière automatique aux événements filmés et aux enregistrements par le système afin de faciliter leur exploitation.

Les enregistrements devront être conservés dans leur originalité et aucune modification ne devra pouvoir leur être apportée. Toutes les informations, communications ou diffusions devront être saisies et horodatées.

LE REGLEMENT INTERIEUR

Le règlement intérieur est un document auquel les chartes d'éthique font référence et qui établit les règles d'hygiène et de sécurité au travail. Dans ce document, peuvent ainsi être fixées les conditions d'exploitation du système de vidéo protection, de nature à rassurer l'utilisateur, le client ou le citoyen et donc à rendre l'outil acceptable. Il peut également lister les personnes en charge du système et précise les conditions d'accès aux installations.

6.4. ORGANISATION SPECIFIQUE AUX SYSTEMES SUPERVISES

L'utilisation en temps réel du système est la différence essentielle entre les systèmes supervisés et les autres. Si une organisation spécifique a été mise en place, l'utilisation en temps réel permet d'augmenter très fortement l'efficacité du système de vidéo protection.

6.4.1. LES RELATIONS AVEC LES SERVICES DE SECURITE INTERIEURE

Sur les systèmes supervisés, le fait de pouvoir proposer des images en temps réel en plus des images enregistrées peut renforcer l'intérêt des forces de police et de gendarmerie pour le système de vidéo protection mis en place, car il peut devenir un outil supplémentaire au maintien de l'ordre et de la sécurité publique.

LA CONVENTION DE PARTENARIAT

Il est très fortement conseillé de passer une convention de partenariat avec les services de sécurité intérieure locaux pour définir les conditions d'accès aux images par les services territorialement compétents.

Ce sera aussi l'occasion de revisiter la convention de coordination qui existe entre la police municipale et les forces de sécurité intérieure.

Cette convention abordera notamment :

- Les modalités de saisine et d'intervention des forces locales, pour garantir l'efficacité du système de vidéo protection,
- Les conditions d'accès aux images en temps réel : supervision conjointe service de sécurité / opérateur titulaire dans le cadre d'opérations ponctuelles de police,
- Les conditions d'accès aux enregistrements : relecture et saisie éventuelle des images en cas d'infraction. Il faut notamment prévoir quelle est la personne qui doit être jointe en cas de besoin par les services de police et quelle est l'astreinte mise en place (week-ends, nuit, jours fériés),



- Les moyens de communication éventuellement mis en œuvre entre les opérateurs et les services de sécurité,
- Les modalités de report d'images du centre superviseur vers les services de sécurité,
- Les conditions de fourniture d'informations par les services de sécurité relevant de l'Etat et notamment les statistiques.

LE RENVOI D'IMAGES VERS LA POLICE OU LA GENDARMERIE

En fonction des échanges avec la police et la gendarmerie, il est vivement recommandé de prévoir un renvoi des images du centre superviseur vers les locaux des services de sécurité les plus proches. Il s'agit de renvoyer tout ou partie des images, avec ou sans la possibilité pour le destinataire des images d'agir sur le système (pilotage d'un dôme par exemple).

Dans la plupart des cas, le renvoi est simple : une image est renvoyée sur un écran standard à la demande de la police ou de la gendarmerie. Une liaison téléphonique ou radio permet à la police ou à la gendarmerie de demander à l'opérateur le renvoi de l'image de telle ou telle caméra.

Dans tous les cas, il est très important de formaliser les conditions du partenariat mis en place avec les services de sécurité par une convention.

Il est fortement recommandé d'associer les services concernés dès le démarrage du projet, afin de préciser quel type de renvoi est le plus à même de répondre à leurs besoins.

Il faut retenir que des aides financières peuvent être accordées aux communes mettant en place un tel renvoi (voir le financement par le FIPD).

6.4.2. LA GESTION OU LE SUIVI DES GRANDS EVENEMENTS

La possibilité de visualiser en temps réel apporte un nouvel outil de gestion urbaine en cas de grands événements à l'occasion de :

- Violences urbaines,
- Visite officielle de haute personnalité,
- Manifestation sportive,
- Rassemblement revendicatif,
- Catastrophe naturelle telle qu'une inondation, conditions climatiques extrêmes,
- Accident ou sinistre de toute nature.

Selon leur nature et leur importance, ces grands événements appelleront une intervention différente des autorités municipales. Celles-ci trouveront toujours un intérêt à l'exploitation des images soit pour suivre soit pour gérer. Une bonne gestion nécessite la définition, la validation et la mise en œuvre de procédures prédéfinies. Il est rare que le centre de supervision prévoit dès l'origine sa transformation en salle de gestion d'événements exceptionnels.

Dans ces conditions, il sera opportun de disposer d'une salle proche dotée des moyens de transmission permettant de rassembler les partenaires utiles.



6.4.3. LES OPÉRATEURS DU SYSTÈME DE VIDÉO PROTECTION

(Voir également la fiche thématique n°9 : recrutement et formation des opérateurs)

Les opérateurs du système de vidéo protection exploitent quotidiennement le système de vidéo protection supervisé. Leurs missions principales sont

- Observer les espaces sous couverture vidéo,
- Rendre compte des événements constatés,
- Exécuter les consignes de télésurveillance.

Toutefois, afin de rendre plus efficient le centre de gestion, les opérateurs peuvent être polyvalents et prendre en compte le renvoi d'un standard, la gestion des alarmes techniques, intrusion ou incendie.

Le recrutement des opérateurs est donc une phase cruciale dans un projet de système de vidéo protection supervisé, car il conditionne la réussite du projet. Ce paragraphe a pour objet d'aider les responsables de projets de vidéo protection à effectuer les bons choix en termes de personnel.

Le recrutement des opérateurs sera abordé sous trois aspects successifs :

- Déterminer le statut des personnes pouvant être recrutés,
- Déterminer le profil des agents à rechercher,
- Elaborer une procédure de recrutement.

UN STATUT VARIABLE SELON LES PROJETS

La nature de l'autorité autorisée à gérer le système conditionne les modalités d'exploitation des images.

L'exploitation des images par des prestataires extérieurs.

Rappelons que l'exploitation des images par des personnes extérieures est possible, sauf pour les collectivités territoriales agissant pour la surveillance de la voie publique. Un tel mode d'exploitation est souvent un facteur de réduction de coût, dans le domaine de la surveillance ou du gardiennage de biens meubles ou immeubles, ainsi que de la sécurité des personnes se trouvant dans ces immeubles, conformément la loi n°83-629 du 12 juillet 1983 réglementant les activités privées de sécurité.

S'agissant des collectivités territoriales, l'interdiction formulée par le Conseil d'Etat s'oppose donc à ce que le personnel d'une entreprise de sécurité privée se voit confier, même sans délégation de service public, une mission comportant accès aux images d'un système de vidéosurveillance établi par une autorité publique dans le but de surveiller la voie publique.

L'exploitation des images par des agents de l'exploitant du système.

Le principe de l'exploitation des images par des agents de l'exploitant ne connaît aucune exception lorsque les images sont prises sur la voie publique, ou pour l'exercice d'une mission de police.

Lorsque le système relève de l'autorisation préfectorale de la loi du 21 janvier 1995, le dossier de demande doit comporter « toute indication sur la qualité des personnes chargées de l'exploitation du système et susceptibles de visionner les images » (8° de l'article 1^{er} du décret modifié n°96-926 du 17 octobre 1996 relatif à la vidéosurveillance). Cela concerne



les personnes qui seront seules habilitées à accéder aux images soit lors de leur captation, soit après enregistrement pour satisfaire aux demandes d'accès des citoyens et des autorités judiciaires.

Pour les systèmes des autorités publiques, les agents peuvent être soit des titulaires, soit des agents contractuels, dès lors que le recours à cette catégorie d'agents est autorisé.

LE PROFIL A RECHERCHER

Quel que soit le site protégé, on recherchera en priorité des personnes acceptant des contraintes fortes. Le métier est soumis à des contraintes de sécurité (contrôle d'accès, bonne moralité...), à des contraintes horaires (travail de nuit, les jours fériés...). Enfin, la tâche de supervision est par elle-même difficile : visualiser quotidiennement des images peut devenir fastidieux. Il faudra donc rechercher en priorité des personnes ayant une expérience de la vidéosurveillance, de la télésurveillance et des métiers de la sécurité en général. L'exigence de formation des personnels est forte car ils doivent appréhender les nombreux contextes de sécurité et de sûreté.

IL FAUT RETENIR QUE ce travail statique peut convenir à certaines personnes à mobilité réduite sous réserve, bien entendu, d'un aménagement spécifique du poste de travail.

LA PROCEDURE DE RECRUTEMENT

Une fiche thématique spécifique détaille ces éléments (voir fiche 9). Il est important de bien exposer au candidat les spécificités du métier et ses contraintes, et d'organiser l'évolution et la carrière de l'agent.



6.5. SYNTHÈSE UL 5 : LES MESSAGES ESSENTIELS

La seconde étape du projet de vidéo protection concerne l'organisation humaine. On rappelle que la première est l'analyse des besoins en vidéo protection.

La désignation d'une personne responsable du projet est fortement conseillée. Cette personne aura en charge tout le suivi du projet en amont (relation avec les partenaires extérieurs, constitution des dossiers juridiques, relation avec l'installateur) et également la gestion de la vie du système (relation avec les partenaires extérieurs, suivi de la maintenance, accès aux images). Cette personne sera l'interface entre le système et l'extérieur. On peut imaginer que le responsable du projet soit différent de celui qui sera ensuite chargé de l'exploitation.

Il faut distinguer deux grands types de systèmes : ceux dont les images sont visualisées en temps réel par des opérateurs et ceux dont les images sont enregistrées et consultées a posteriori. Une partie des règles d'organisation d'un système est commune à ces deux architectures (exemples: définition des accès aux images, définition des astreintes, ...). Le principal point à régler est l'accès aux images, qu'elles soient en temps réel ou enregistrées. Les enregistrements doivent bénéficier d'une protection particulière et il est impératif de séparer physiquement l'enregistrement des images en temps réel. Dans la pratique, il est conseillé que la consultation des images se fasse dans une salle spécifique.

Les systèmes supervisés présentent des contraintes spécifiques liées aux opérateurs. Le statut des opérateurs varie selon le type de lieu vidéoprotégé : voie publique ou lieu privé. Actuellement, il n'est pas possible de confier la surveillance de la voie publique à un personnel mis à disposition par une entreprise privée ou de renvoyer pour exploitation des images de la voie publique à une entreprise privée. Cela est en revanche possible pour les espaces privés. De fait, les collectivités (communes, établissements publics de coopération intercommunale) doivent soit prévoir le recrutement d'agents municipaux spécifiques, soit confier cette exploitation à des agents déjà en poste (policiers municipaux, ASVP...).

La coordination avec les services de police ou de gendarmerie est un élément fondamental de l'organisation. Le partenariat à mettre en place avec les services de sécurité comprend quatre aspects :

- 1 - les modalités de saisine et d'intervention des services de sécurité intérieure et de la police municipale,
- 2 - la consultation et la saisie des images enregistrées,
- 3 - dans certains cas, le renvoi d'images vers le poste de police ou la brigade de gendarmerie les plus proches,
- 4 - les échanges concernant les évaluations d'impact des systèmes de vidéo protection sur la délinquance.

Le métier d'opérateur vidéo est relativement nouveau et reste encore peu structuré : pas de formation spécifique reconnue, pas de statut. De plus, la pénibilité spécifique à ce métier engendre une forte rotation de personnel mais qui peut être limitée par une bonne organisation.





7. UL6 : DE L'ARCHITECTURE TECHNIQUE A LA LIVRAISON



La définition de l'architecture technique du système

- UL 6 : De l'architecture technique à la livraison
- UL 7 : L'appel d'offres, le déploiement et la validation

7.1. LES CHOIX TECHNIQUES

Par opposition aux petits systèmes localisés, les réseaux de vidéosurveillance sont des systèmes complexes en ce sens qu'ils sollicitent un spectre de compétences très étendu, allant potentiellement de la réalisation de travaux de génie civil au développement d'applications informatiques.

Les choix techniques découlent directement des besoins fonctionnels exprimés, des objectifs en termes d'évolution et des contraintes d'environnement, dans le respect de la réglementation en vigueur.

Les solutions mises en œuvre représentent des compromis sur le plan technique lorsque l'on considère la chaîne de liaison dans sa globalité : **acquisition, transport**, (incluant la commutation et la compression), **visualisation** (incluant le pilotage), **enregistrement**. Tout l'enjeu consiste à résoudre l'équation technique qui aboutit aux résultats escomptés et à l'efficacité attendue du dispositif.

En termes de technologie, la tendance est à la numérisation des signaux de l'acquisition des images à leur visualisation. Toutefois, le marché n'est pas encore arrivé à maturité et la majorité des systèmes déployés continuent à tirer parti des technologies analogique et numérique, en les mêlant de manière pertinente et opportuniste.

Les solutions analogiques restent plus simples à déployer mais demeurent isolées et moins évolutives. Le numérique a pour ambition de positionner la vidéosurveillance au sein du Système d'Information de l'établissement concerné en privilégiant la mutualisation des moyens (équipements et ressources) et en facilitant le couplage avec des applications métiers. En outre, il permet de s'affranchir des contraintes géographiques (distances, localisation des ressources centrales) et garantit l'évolutivité du système sur les plans architecturaux et applicatifs.

La suite du chapitre correspond à des architectures classiques, qui sont de loin, les plus utilisées, et qui correspondent à des installations dans lesquelles le maître d'ouvrage souhaite visualiser les images de façon assez régulière et en temps réel, notamment en vue de contrer un acte malveillant en cours. On se reportera pour des systèmes avancés à la fiche N0 12 « traitements intelligents ».

7.2. LA STRUCTURE D'UN SYSTEME DE VIDEOPROTECTION

L'architecture d'un système de vidéosurveillance peut être modélisée sur le plan fonctionnel selon les 4 blocs suivants :

L'œil du système - L'**acquisition** des images vidéos (issues des caméras fixes ou mobiles), d'alarmes de toute nature (contact, vidéos, ...), et, le cas échéant, de flux audios (écoute),

Le système nerveux - Le **transport** bidirectionnel des flux vidéos, audios et de

La définition de
l'architecture
technique du
système

UL 6

De l'architecture
technique à la
livraison



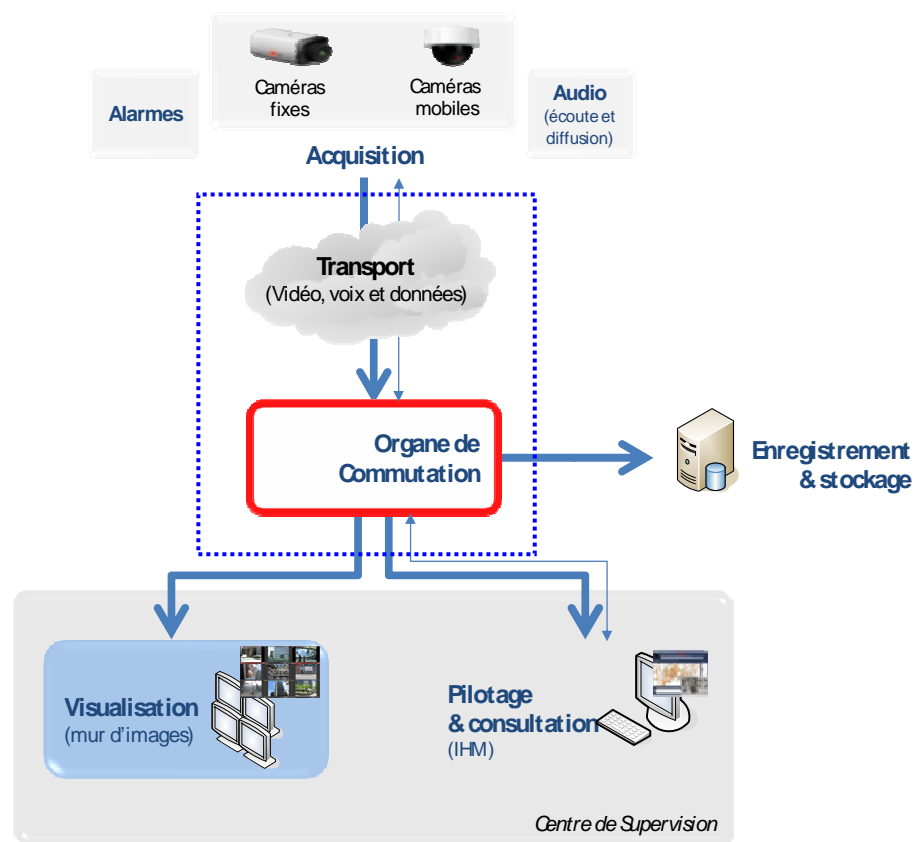
données, et leur **commutation** vers les ressources concernées (enregistreurs, moniteurs de visualisation, postes de pilotage),

Le cerveau - Le **pilotage** des caméras, la **visualisation** des images en temps réel sur un dispositif spécifique (mur d'écrans, multivision sur écran unique, ...), puis la **consultation** des images enregistrées à partir d'une interface ergonomique (IHM – Interface Homme-Machine),

La mémoire - L'**enregistrement** des images qui aujourd'hui est réalisé exclusivement en numérique.

Un dernier maillon est la numérisation du signal vidéo, dont le positionnement dans la chaîne ci après est variable suivant les systèmes. Pour être en phase avec les systèmes les plus modernes, on l'évoquera juste après l'acquisition.

Schématiquement, un dispositif global peut être représenté comme suit. Les briques techniques d'administration et de supervision du système ne sont pas représentées.



Nota : Dans le cas de systèmes numériques, les fonctions de transport et de commutation sont imbriquées puisque les organes de commutation sont des routeurs.

Ces différents éléments d'architectures, fortement interdépendants, doivent être interopérables et former un ensemble cohérent. Les choix techniques et technologiques sont, d'une manière générale, des compromis à obtenir en considérant la chaîne de liaison dans sa globalité.

En termes de marché, deux tendances se dessinent nettement :

- Les systèmes ouverts, mettant en œuvre des constituants de différents constructeurs en s'appuyant, en termes d'interopérabilité, sur des normes mais nécessitant souvent des développements logiciels spécifiques et des accords commerciaux bilatéraux entre les différents constructeurs (sur la base de kit de développement – SDK),



- Les systèmes intégrés et propriétaires ne mettant en œuvre que des constituants provenant du même constructeur.

Les systèmes de grande envergure, déployés en plusieurs phases et nécessitant des fonctionnalités particulières, favoriseront la mise en place de systèmes ouverts. Les réseaux de plus petite taille peuvent s'orienter vers des solutions intégrées, packagées, qui demeurent plus simples à mettre en œuvre.

7.2.1. BLOC 1 : L'ACQUISITION



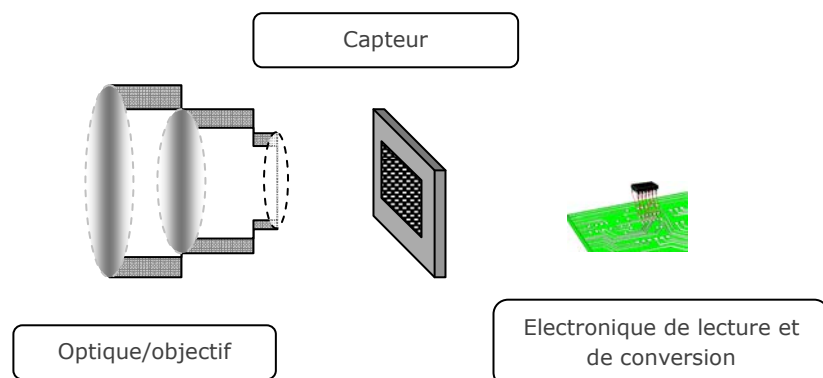
Les caméras constituent la réponse au besoin initial de base de surveillance d'une zone. Leur positionnement et les choix techniques associés sont très importants pour l'atteinte des objectifs fixés et résultats attendus.

Une bonne qualité d'image, dès son acquisition, est primordiale car elle impacte la chaîne de liaison globale vers la restitution (visualisation en temps réel et enregistrements). La qualité initiale de prise de vue détermine la qualité maximale de l'ensemble de la chaîne.

PRINCIPE SIMPLIFIE D'UNE CAMERA

Une caméra est composée de 3 blocs indépendants:

- L'optique
- Le capteur
- L'électronique de lecture, de conversion du signal



L'optique

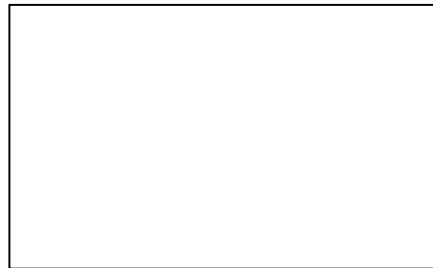
L'optique est la partie du système qui permet de reprendre la scène observée et de l'imager sur la surface du capteur. L'optique peut disposer d'une focale fixe, ou d'une focale variable, les zooms optiques sont des optiques dont la focale est variable et sur lesquels il n'est pas nécessaire de mettre au point l'image lors d'un changement de focale. Le choix de l'optique influe directement sur la taille de la scène que la caméra va permettre d'observer. La focale fixe la taille des objets dans l'image et fixe également la scène que l'on est capable d'observer. Même si ce qui suit peut varier en fonction de la prise de vue spécifique (couloir, hall...), on peut généralement considérer que :

- Un objectif à **grande focale** permet d'obtenir une taille plus grande des objets ou personnes dans le champ, mais avec un champ d'observation réduit. → **Vision plan étroit.**
- Un objectif à **courte focale (grand angle)** permet d'obtenir un champ d'observation large, cependant, les objets de la scène sont réduits sur l'image. → **Vision plan large.**



Par exemple, on ne peut pas sur la même caméra avoir une vue d'ensemble d'un carrefour, tout en lisant les plaques d'immatriculation des voitures qui passent.

Ces notions sont toutefois aujourd'hui tempérées par l'arrivée des caméras mégapixels qui permettent, grâce à leur haute résolution, de réaliser des zooms numériques utiles, et donc de pouvoir combiner la vision plan large et la vision plan étroit. Pour illustrer, avec une optique (objectif) de focale identique, sur une caméra standard 640 X 480, on peut considérer que si on est capable d'identifier une personne à 5 mètres, alors on est capable d'identifier avec une caméra mégapixel de résolution 1280 x 1024, une personne à 10 mètres (2 fois plus de résolution en hauteur et en largeur).



Images avec des optiques de différentes focales

Le capteur

La capture de l'image par les caméras constitue un traitement numérique du signal (capteur CCD ou capteur CMOS), les différents éléments de la scène sont transcrits en courant électrique de valeur plus ou moins importante selon la quantité de lumière qu'ils réfléchissent. Les caractéristiques électroniques du capteur définissent la sensibilité de la caméra. A configuration comparable, une caméra noir et blanc est généralement plus sensible qu'une caméra couleur. Le passage en noir et blanc est souvent appliqué pour la surveillance des scènes de nuit. La sensibilité d'une caméra se mesure en lux (unité qui correspond à une quantité de lumière reçue par une surface (éclairage) pondérée par la sensibilité de l'œil humain). Cette notion de sensibilité est très importante car elle fixe la capacité du capteur à visualiser des scènes peu éclairées.

Le capteur est composé de cellules photosensibles ou photosites (sensibles à la lumière) que l'on assimile plus communément à des pixels (pour reconstituer la couleur, sur certains capteurs plusieurs photosites correspondent à un seul pixel). À un niveau d'éclairage sur le pixel, une tension électrique correspond en sortie, chaque pixel génère un signal électrique qui est fonction de la lumière reçue. La taille, ainsi que le nombre de pixel du capteur définissent sa résolution. Avec la miniaturisation des technologies et l'augmentation de la fréquence des électroniques, le nombre de pixels dans un capteur dépasse le Million, ces types de capteurs sont dénommés capteur Megapixels.

Il existe des capteurs de taille 1/4", 1/3", 1/2", 2/3". Ces valeurs ne correspondent pas à une dimension réelle en pouces, il n'est donc pas possible de les relier à une taille en cm en effectuant un simple calcul de conversion.

Électronique de lecture et de conditionnement

L'électronique de lecture et de conversion permet de reconditionner le signal issu du capteur pour le rendre visualisable par d'autres composants électroniques. Aujourd'hui les électroniques de lecture et de conversion sont généralement confondues sur une même



carte électronique, voire intégrées au capteur lui-même grâce à la miniaturisation des technologies.

Une caméra est dite **analogique** lorsqu'elle dispose d'une sortie analogique. Le signal, de faible amplitude, est très sensible aux parasites. La connectique est généralement de type BNC pour transport sur câble cuivre coaxial. Certaines caméras intègrent un convertisseur cuivre-optique et présentent directement une connectique fibre optique qui présente les avantages de l'immunité aux perturbations électromagnétiques et d'une distance de propagation bien supérieure. Un convertisseur extérieur peut également être utilisé (cas très fréquent). A noter que le flux de télémétrie nécessaire au pilotage des caméras mobiles est transporté soit à l'aide d'un câble cuivre dédié (multipaire, FTP) soit dans une fréquence adjacente directement dans le câble coaxial ou la fibre optique (solution propriétaire).

Une caméra est **numérique** lorsqu'elle embarque directement un encodeur et offre une sortie numérique. L'intérêt est de disposer en sortie de caméra d'un signal modélisé, facile à régénérer après déformations subies dans le transport et interprétable par les équipements d'extrémité. L'encodeur et par symétrie le décodeur, ont une influence très significative sur la qualité de l'image restituée (temps réel et enregistrée) (cf. 7.2.2). Ces capacités de calcul embarquées dans les caméras occasionnent en revanche un surcoût en matière de consommation électrique qui peut se révéler non négligeable pour des installations importantes.

Actuellement, les caméras numériques utilisent en majorité le protocole **IP**. L'encodeur intégré assure la transformation du signal vidéo en trame IP permettant le transport du flux vidéo sur un réseau de données, multiservices, banalisé : Ethernet dans les réseaux locaux et métropolitains (LAN, MAN) et MPLS, ou WAN sur les réseaux longue distance.

LES DIFFERENTS TYPES DE CAMERAS

Les caméras analogiques ou numériques installées dans le cadre de dispositif de vidéosurveillance prennent différentes formes selon les supports dans lesquels elles sont intégrées :

Caméras fixes, avec ou sans zoom optique motorisé,

7.3. Surveille une scène unique, selon un plan plus ou moins large (si zoom optique motorisé),

7.4. Un éventuel zoom optique motorisé nécessite une liaison de télémétrie.



Caméras mobiles PTZ (tourelles, à ne pas confondre avec des caméras embarquées)

7.5. Vitesse de déplacement compris entre 1 et 100° par seconde,

7.6. Grande stabilité permet l'utilisation de zooms optiques pour des observations à des longues distances.

7.7. Ses caractéristiques lui permettent la surveillance d'une zone très étendue.



Caméras dômes fixes (minidômes):

7.8. Surveille une scène unique, selon un plan défini

7.9. Discrétion et installation facile

7.10. Cas particulier des **dômes fixes 360°**: visibilité globale de la scène en permanence sur des distances réduites.



Caméras dômes mobiles:

7.11. Vitesse de déplacement pouvant aller jusqu'à 400° par seconde,

7.12. Ses caractéristiques lui offre une grande réactivité et lui permettent notamment de suivre un sujet en déplacement (tracking).





Les caméras mégapixels peuvent entrer dans presque chacune des catégories précédentes. La fonctionnalité étant reliée au capteur, celui peut être intégré dans différents types de supports. (Il est tout de même plus courant de trouver des capteurs mégapixels, dans des supports fixes ou dômes fixes)

Les caractéristiques des caméras (sensibilité, zooms optiques) doivent être adaptées aux conditions d'utilisation : niveau d'éclairage (notamment de nuit), distance maximum entre la caméra et le sujet surveillé (niveau de détail visible attendu). A noter que la plupart des caméras intègrent une commutation automatique en noir et blanc dès lors que la luminosité ambiante devient insuffisante (mode jour/nuit). Il est toutefois conseillé lorsque le système doit fonctionner de nuit de prévoir des éclairages d'appoint en infrarouge lorsque l'éclairage ambiant n'est pas suffisant.

Le support utilisé doit être adapté aux conditions environnement et d'utilisation, notamment en extérieur :

- Conditions de température, d'hygrométrie, de pression, de vent,
- Niveau d'étanchéité nécessaire (indice de protection IP norme NF EN 60529)
- Niveau de résistance aux chocs (indice de protection IK norme NF EN 50102)
- Prise en compte des risques relatifs à des atmosphères explosives (classification du site et réglementation ATEX).

LA RESOLUTION DES CAMERAS

La résolution des caméras (nombre de lignes et de colonnes) est un point important qui conditionne la qualité de l'image et le traitement qui peut en être fait.

L'arrêté de normes techniques du 3 août 2007 fixe 2 niveaux de résolution minimale pour les systèmes soumis à la loi du 21 Janvier 1995 :

- une résolution 1 CIF (352 x 288 pixels) pour les caméras à plan large destinées à visualiser une scène sans chercher à en analyser les détails.
- une résolution 4 CIF (704 x 576 pixels) pour les caméras à plan étroit destinées à analyser les détails de la scène - identifier les individus.

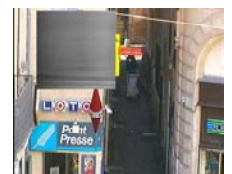
La résolution obtenue avec des caméras numériques, notamment les caméras mégapixels (>1280 x 1024 pixels) dépasse aujourd'hui celle qu'on peut atteindre avec des caméras analogiques.

Une liste non exhaustive des résolutions standard est précisée dans la fiche technique N°10

PRINCIPALES FONCTIONNALITES DES CAMERAS UTILISEES EN VIDEOSURVEILLANCE

Ce paragraphe concerne essentiellement les caméras mobiles. Les principales fonctionnalités utilisées dans le cadre de dispositif de vidéosurveillance sont les suivantes :

Masquage dynamique (toutes caméras) : cette fonctionnalité, très utile pour les caméras de voie publique, permet de masquer les champs de vision non autorisés d'une caméra, dynamiquement, c'est-à-dire en tenant compte de la position des axes de prise de vue et de la valeur de la focale du zoom optique à chaque instant.



Prépositions et cycle de prépositions (caméra mobiles): pour une caméra considérée, il est possible de définir les points d'intérêt à surveiller lorsque celle-ci n'est pas pilotée par un opérateur. Ces points d'intérêts constituent des



prépositions que la caméra balaye en cycle avec une temporisation définie pour chacune des prépositions.

Mémorisation d'un cadrage (caméra mobiles): lorsqu'un opérateur pilote une caméra, il peut mémoriser un point d'intérêt (cadrage) de manière à pouvoir y revenir, par une manœuvre simple, à sa convenance après avoir manipulé cette même caméra ou après son redémarrage en cycle,

Caméra figée (caméra mobiles): cette fonction permet de figer, par une manœuvre volontaire, une caméra sur une scène particulière. La caméra ne sera libérée que par une nouvelle action volontaire de l'opérateur.

PRECONISATIONS POUR LE POSITIONNEMENT DES CAMERAS

Le positionnement des caméras est un point primordial pour l'efficacité du dispositif. Ce point est même plus important que la technologie de la caméra utilisée, une caméra haute technologie mal positionnée sera bien moins efficace qu'une caméra standard positionnée correctement.

Il doit être étudié selon l'usage initialement défini pour chacune des caméras tout en conservant à l'esprit que les objectifs fixés peuvent évoluer.

Par ailleurs, le choix de positionnement des caméras peut avoir un impact direct sur le coût de la réalisation des travaux. En effet, une caméra isolée, très éloignée de toute artère de communication ou de toute source d'alimentation, peut s'avérer très onéreuse au vue des missions qui lui seront subordonnées. Des compromis seront donc à nouveau à trouver pour atteindre les objectifs globaux dans le respect de budgets raisonnables.

Le positionnement des caméras requiert donc une attention toute particulière et doit tenir compte également des points suivants :

La **luminosité** ambiante de jour et le niveau d'éclairage de nuit: la luminosité insuffisante constitue de loin la première source d'images inexploitable par les services de police, Il est ainsi parfois nécessaire d'adjoindre à la caméra un dispositif d'éclairage d'appoint visible (toutes caméras) ou infrarouge (caméras noir et blanc ou jour/nuit uniquement)

La **hauteur** à laquelle sera positionnée la caméra :

Positionnée trop haut, elle souffrira d'un mauvais angle de vue à son pied et d'un déficit du niveau de détail du à l'éloignement de la caméra par rapport au sujet filmé,

Positionnée trop bas, elle sera exposée au vandalisme et inefficace pour des prises de vues distantes (prise de vues rasantes),

Les **activités événementielles** : drapeaux et banderoles des festivités, stores de terrasse des commerçants par beau temps, décorations de Noël, ...

La **saisonnalité** : arbres à feuilles au printemps et l'été, hauteur du soleil,

L'éblouissement : soleil bas (matin et soir notamment), contre-jours, lampadaires à proximité, phares de véhicules,

Les **intempéries** : brouillard, neige, pluie d'orage, vent,

La **propreté** de la caméra : un nettoyage régulier est à prévoir,

Les **zones privées** qui obligeraient, in fine, à positionner un nombre de masques numériques démesuré et nuisible à l'efficacité de la caméra,

Le positionnement des caméras les unes par rapport aux autres de manière à :

- o assurer une couverture cohérente d'une zone sensible,
- o assurer une surveillance des caméras entre elles pour éviter leur dégradation.

La réalisation de prises de vues en position réelle, c'est-à-dire en lieu et place des caméras envisagées, est fortement suggérée. Les moyens techniques simples existent et l'utilisation de nacelles permettra par

exemple de réaliser des simulations très proches de la réalité et constitueront des outils d'aide à la décision efficaces pour les décideurs.



L'ALIMENTATION ELECTRIQUE DES CAMERAS

Une caméra (ainsi que les éventuelles interfaces à proximité telles que les convertisseurs cuivre/optique) doit dans tous les cas être alimentée électriquement. Ce point n'est, sur les plans techniques et financiers, absolument pas négligeable et doit être appréhendé à sa juste dimension.

A noter qu'une simple coupure d'alimentation (volontaire ou non) rend une caméra complètement inopérante. Un raisonnement sécuritaire doit donc être apporté concernant le niveau de continuité de service acceptable.

Les différentes solutions envisageables sont les suivantes :

Alimentation locale à partir d'un compteur spécifique implanté à proximité (dans la rue ou dans un bâtiment proche dont l'accès est facile à toute heure du jour et de la nuit),

Alimentation « à distance » :

- Alimentation en courant basse tension (12V, 24V, 48V) à partir du local technique le plus proche, par un câble dédié ou par des conducteurs intégrés dans la gaine des câbles coaxiaux),
- Concernant les caméras IP raccordées en Ethernet, celles-ci peuvent être téléalimentées directement par les commutateurs Ethernet (sous réserve que ces derniers soient POE (*power Over Ethernet*) selon la norme 802.3af. Cette dernière est en cours d'évolution et devrait permettre la téléalimentation d'équipements IP dont la puissance nécessaire est supérieure 15W, limite actuelle de la norme).

7.2.2. CAS PARTICULIER DU BLOC D'ENCODAGE ET DE COMPRESSION DES IMAGES

Sur un système dont le réseau central ou bien l'enregistrement sont numériques, les images doivent être numérisées à un endroit ou un autre de la chaîne. La numérisation est toujours associée à une compression car la numérisation brute correspondrait à un débit de transmission bien trop élevé qu'il serait difficile de transmettre avec les moyens techniques disponibles.

Le transport numérique des flux bidirectionnels (vidéo et télémétrie) relatifs à une caméra analogique, nécessite la mise en place d'un **encodeur** vidéo qui transforme les signaux analogiques en signaux numériques selon le protocole IP. Par symétrie, la restitution en analogique nécessite le **décodage** du signal (pour un affichage sur un écran analogique par exemple). Encodeur et décodeur doivent être strictement interopérables : dans la pratique, et même si une normalisation est en cours au sein de l'AFNOR (à échéance 2011) il est hautement préférable que les équipements proviennent du même constructeur. Le décodage du signal est toutefois de plus en plus intégré aux briques logicielles (décodage logiciel) des Interfaces Homme-Machine des postes de visionnages (il faudra donc veiller à ce que l'IHM soit compatible avec les méthodes d'encodage, sous peine de devoir acquérir un décodeur spécifique (décodage matériel)).

Toutefois, ce bloc a tendance à se confondre soit dans le Bloc 1 : L'acquisition, soit dans le bloc transport. En effet, d'une part, les caméras numériques l'intègrent directement sur



l'électronique de lecture et de conversion (les caméras jouent donc le rôle de caméra et d'encodeur), et d'autre part les systèmes d'enregistrement numériques pour caméras analogiques, encodent les flux analogiques et les compressent ensuite, pour pouvoir enregistrer les images sur support informatique et les envoyer si nécessaire sur un réseau informatique (les enregistreurs analogiques/numériques jouent donc le rôle d'enregistreur et d'encodeur).

La fiche technique n°11 détaille les différentes normes de compression mais il est utile de savoir que pour des caméras de résolution 4CIF, les normes de type (MJPEG, MPEG 2) nécessitent un débit de 5 Mbit/s environ, que les premières implémentations du MPEG4 nécessitent environ 2 à 3 Mbit/s environ, tandis que la norme la plus récente (qui sera utilisée pour la TV HD Grand public en France), le H264 (MPEG4-AVC, MPEG4 Part 10 ou H264 sont la même norme de compression) permet de transmettre un signal de qualité DVD avec un débit inférieur à 1 Mbit/s.



[MPEG4 vs MPEG4 H264 – MPEG4 AVC.](#)

Il est important de noter que les caméras, encodeurs ou enregistreurs proposant une compression MPEG4 uniquement et non spécifiquement labellisée H264 ou MPEG4 AVC dans la documentation technique, ne compressent les vidéos qu'avec les anciennes implémentations de la norme MPEG4.

La compression des images impose une attention particulière, en effet, le taux de compression choisi impacte directement la qualité des images, et ce indépendamment de la caméra et de l'optique choisie. Il est important de ne pas trop compresser les images sous peine de rendre les images inutilisables. A titre d'exemple, une vidéo provenant d'une caméra Mégapixel fortement compressée proposera une qualité et une quantité d'information bien inférieure à celle d'une caméra standard peu compressée. Il est ainsi important de toujours vérifier que la compression effectuée sur les images enregistrées et sur les images temps réel permet toujours de remplir les objectifs opérationnels qui ont conditionnés l'installation de la caméra. Il convient de regarder le résultat sur les images temps réel **et** sur les images enregistrées, les enregistreurs et les caméras proposant souvent deux modes de compression distincts pour les flux temps réels et les enregistrements.

Les images enregistrées et exportées après compression seront celles fournies aux forces de l'ordre lors des enquêtes judiciaires. Pour un système de vidéoprotection non supervisé, la qualité de la compression des images est, l'un des critères les plus importants, si ce n'est le plus important. En effet, une mauvaise compression dégrade les images du système, qui perd ainsi beaucoup de son efficacité. Un système avec une mauvaise compression ou une compression trop forte des images, est un système très peu utile, voir inefficace dans le cadre d'une utilisation a posteriori des images, les exemples suivant le prouvent aisément.



Images pour sensibiliser à la compression



En fonction de la technologie utilisée pour le transport des images, un débit sera disponible. C'est ce débit disponible qui fixera le taux de compression des images. Il faut donc toujours songer que le critère de qualité des images (compression) est également lié à la qualité du réseau choisi.

7.2.3. BLOC 2 : TRANSPORT

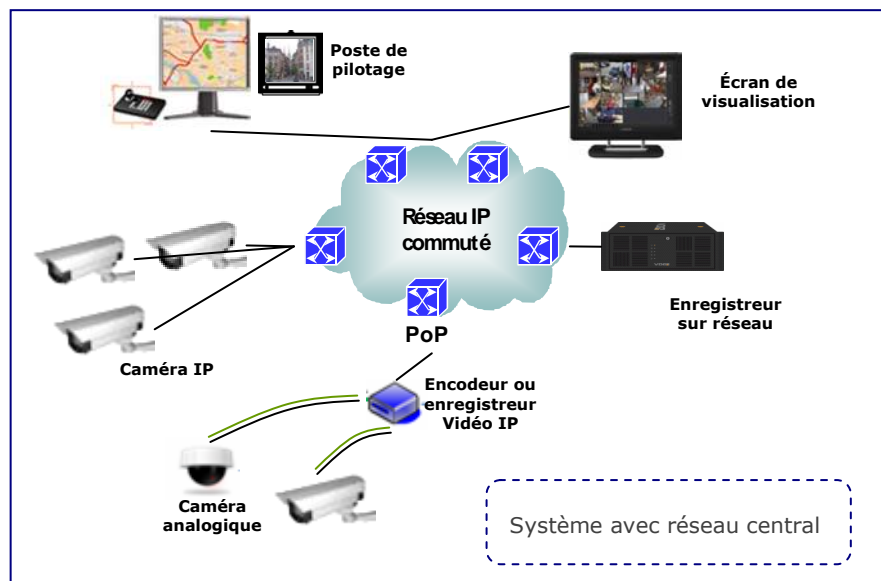


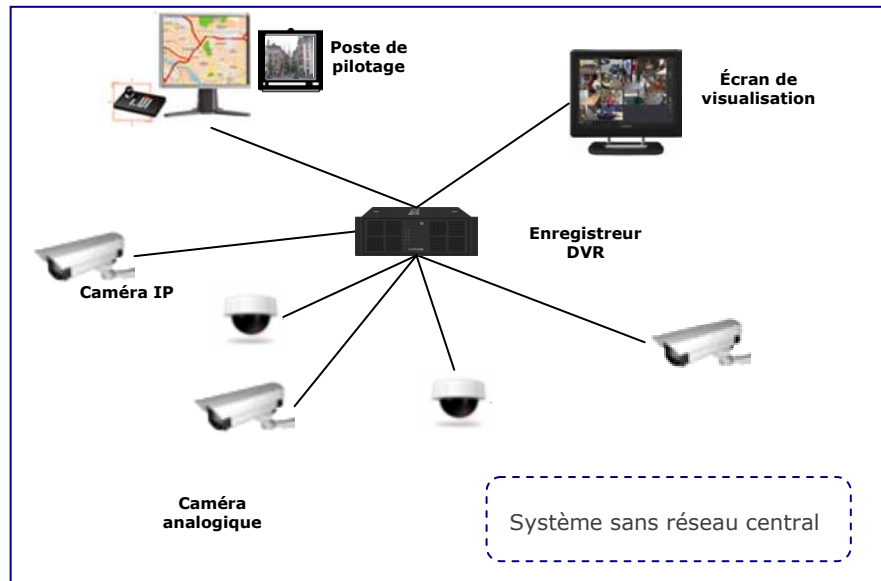
Deux cas sont à considérer : soit la transmission d'un signal analogique, soit celle d'une information codée en numérique. Le transport peut-être réalisé par câble ou fibre optique (transport filaire) ou par ondes radio, incluant la liaison satellite.

Il existe plusieurs architectures réseaux types pour les systèmes de vidéoprotection qui sont souvent déterminées par le nombre de caméras à installer, la reprise de l'existant, le budget, les fonctionnalités temps réel...

LE RESEAU CENTRAL, CŒUR DE RESEAU OU BACKBONE

Le réseau central permet de relier tous les éléments du système, souvent situés à des endroits distants, comme les caméras, le stockage et les écrans de visualisation. Cette notion n'apparaît pas dans le cas par exemple d'un système de vidéosurveillance non supervisé déployé sur un site unique, où les caméras sont reliées directement vers l'enregistreur et ce de manière individuelle. Sur un système sans réseau central, l'enregistreur « digital video recorder » (DVR) joue souvent le rôle d'élément central (pilotage, enregistrement, relecture...). Toutefois, dès lors que plusieurs caméras utilisent le même câble réseau, on peut considérer qu'un réseau central est présent car des notions de disponibilité, de gestion des priorités (...) apparaissent.





Le réseau est composé d'un (ou plusieurs) organe de commutation (ou de routage) qui a en charge l'affectation des flux vidéos et data (téléométrie) entre les différentes briques fonctionnelles du système et de dispositifs de transport des informations (filaire, sans fil, satellite...) qui permettent d'acheminer les informations routées par l'organe de commutation.

Ci-après sont présentés les 2 types de réseaux centraux utilisant technologie analogique puis numérique. Il est important de préciser que les réseaux centraux analogiques sont de plus en plus rares, et plutôt condamnés à disparaître.

LE CAS D'UN RESEAU ANALOGIQUE

Dans les réseaux entièrement analogiques, la partie transport est restreinte à chaque segment terminal (cf. le paragraphe segment terminal pour plus de précision sur les technologies utilisées) chaque caméra (téléométrie et vidéo) est reliée directement à l'organe de commutation le plus proche (en général en analogique, une fibre ou un câble transporte l'information concernant une caméra et une seule). Du point de vue de la fiabilité du système, seuls les fourreaux de câbles peuvent constituer une forme rudimentaire de réseau central.

Dans un réseau analogique, la commutation est assurée par une matrice analogique qui se caractérise notamment par un nombre de ports en entrée et en sortie. La commutation analogique disparaît rapidement du marché, car même si nombre de caméras sont encore analogiques, les flux issus des caméras sont rapidement numérisés dans la chaîne de transport.

La matrice de commutation raccorde notamment, en analogique, les équipements suivants :

- Les caméras (prise d'image et téléométrie)
- Les postes de pilotage (affichage - *moniteurs vidéo* et téléométrie - *pupitre*)
- Le serveur vidéo (enregistrement et gestion de la téléométrie)

La matrice est également capable de centraliser des alarmes et de les commuter vers un système connexe.

Une attention particulière doit être portée sur le dimensionnement de la matrice. Il est, en effet, nécessaire de prévoir les interfaces nécessaires dès le départ (capacité équipée), à



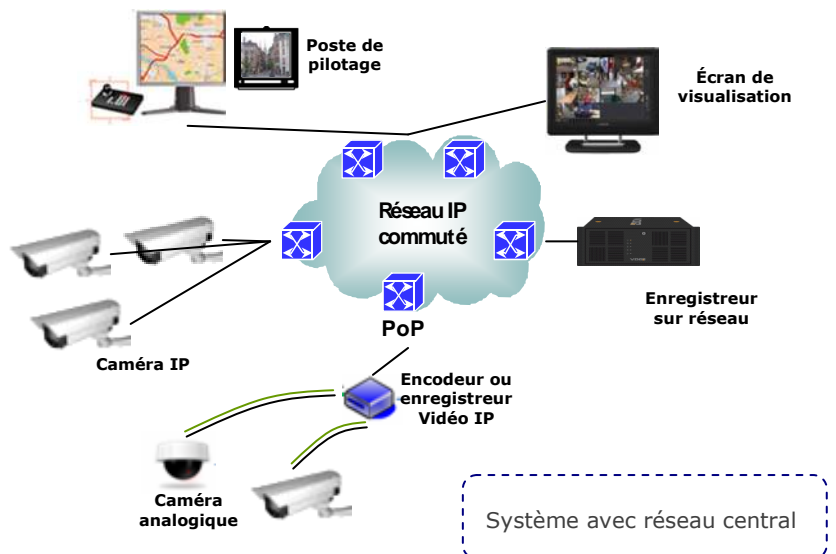
l'extension du système, par simple adjonction de cartes d'équipements (capacité câblée), et d'anticiper une croissance forte du dispositif sans remise en question des investissements initiaux (capacité extensible).

Bien que peu pérenne, l'utilisation d'une matrice analogique peut éventuellement être envisagée dans un réseau de taille réduite avec un centre de surveillance vidéo unique. Toutefois il faut dès le début prévoir les coûts de maintenance et de remplacement qui peuvent être très élevés à cause de la raréfaction de cette technologie.

CAS D'UN RESEAU NUMERIQUE

Le réseau numérique est la technologie déployée dans la grande majorité des systèmes nécessitant un réseau central. Dans un réseau numérique, la notion de commutation n'est plus réellement existante, on parle plutôt de routage car elle est directement assurée par le réseau de données (composants actifs du système comme les routeurs et le serveur) qui peut assurer souvent le transport des flux voix et data. En ce sens, il constitue le cœur du système et doit donc présenter un très haut niveau de disponibilité.

Ce réseau utilise de plus en plus fréquemment le protocole IP transporté sur Ethernet, qui a tendance à se généraliser. Le réseau peut être mono-site (cas, par exemple, de réseaux locaux utilisant des caméras IP) ou distribué dans différents locaux techniques distants créant ainsi des points de présence du réseau (PoP – Point of Presence) assurant la desserte de caméras dans une ou plusieurs zones élargies. Un point de présence peut être assimilé au point d'entrée sur le réseau central (switch, hub, routeur, encodeur, serveur analogique numérique...). Le protocole IP ne conditionne toutefois pas le matériel et le lien physique : un réseau IP peut aussi bien utilisé un support filaire que du sans-fil.



Cas des liaisons sans fil

Pour des raisons de confidentialité, mais surtout de garantie de disponibilité du réseau, l'usage de technologies sans fil doit être limité aux segments de réseau terminaux ou impropres aux technologies filaires.

Ainsi, pour certaines parties du réseau non primordiales (caméras ne nécessitant pas constamment un visionnage temps réel), il peut être envisagé d'utiliser des solutions radio pour diminuer les coûts. Dans ce cas il est fortement recommandé de mettre en place un stockage local avant la liaison sans fil, car sans cela, une perte de service signifierait immédiatement une perte de la vidéo temps réel et en enregistrement. Ces solutions peuvent être couplées à un système MESH (chaque élément du réseau joue le rôle de routeur) pour proposer un maillage d'un site et donc disposer de points de redondances



multiples sur le réseau (il est toutefois fortement recommandé, de s'appuyer sur un réseau central filaire).

Il est dans tous les cas indispensable de réaliser sur terrain des tests préalables pour bien vérifier que la technologie de liaison choisie est compatible de la transmission des signaux (signaux vidéo et télémétrie si supervisé).

Une attention particulière doit également être apportée aux débits disponibles (montants et descendants) et à la confidentialité et l'intégrité des données. Pour les dispositifs mobiles, l'alimentation électrique des équipements ne doit pas être omise dans la réflexion.

Le réseau central doit être dimensionné en fonction du nombre de flux vidéos simultanés à transporter (visualisation en temps réel, flux vers les enregistreurs) qui constituent l'essentiel du volume et apte à véhiculer, en toute sécurité, des flux de natures différentes selon le choix de mutualiser le réseau avec d'autres applications (vidéo, télémétrie, alarme, voix). Il est également conseillé de prévoir les possibles évolutions du système en terme de capacité de transmission (Adjonction de caméras, intégration d'une autre application dans le flux de données), le coût d'un réseau légèrement surdimensionné et le redéploiement d'un réseau, car l'ajout d'une ou deux caméras n'a pas été prévue initialement, est sans commune mesure.

Pour les petites entités avec quelques caméras, il est préférable de disposer d'un réseau IP dédié à la vidéoprotection. Pour les entreprises, la synergie avec le réseau interne de l'entreprise peut engendrer des gains financiers appréciables, et le câblage existant est souvent réutilisé. La transmission des flux de vidéoprotection sur le réseau doit alors obéir à quelques règles de sécurité pour isoler le flux vidéo des autres flux, en général l'utilisation de VLAN.

SEGMENT TERMINAL

Dans la présente sous partie, le transport est assimilé, de manière volontairement réductrice, au segment du réseau situé, en point à point, entre la caméra et l'organe de commutation (matrice), ou son point de présence (Pop) le plus proche lorsqu'il s'agit d'un réseau de données. Pour un système à réseau central numérique, les segments terminaux peuvent être en technologie analogique ou en technologie numérique, selon la technologie des caméras.

ANALOGIQUE

En analogique, nous parlerons d'un transport en **bande de base**, en ce sens que le signal est transmis tel qu'il est disponible en sortie de caméra.

Pour des courtes distances (inférieures à 600 mètres) et dans un environnement peu perturbé sur le plan électromagnétique, les **câbles en cuivre coaxiaux** peuvent être utilisés. Il s'agit du cas le plus simple puisque les équipements d'extrémités (caméras, matrices vidéos, encodeurs) disposent généralement, en standard, d'une connectique adaptée (BNC, 75 ohms).

Concernant les caméras mobiles, un lien de télémétrie doit également être établi entre la caméra et les organes de contrôle. Cette liaison de données peut être assurée de différentes manières :

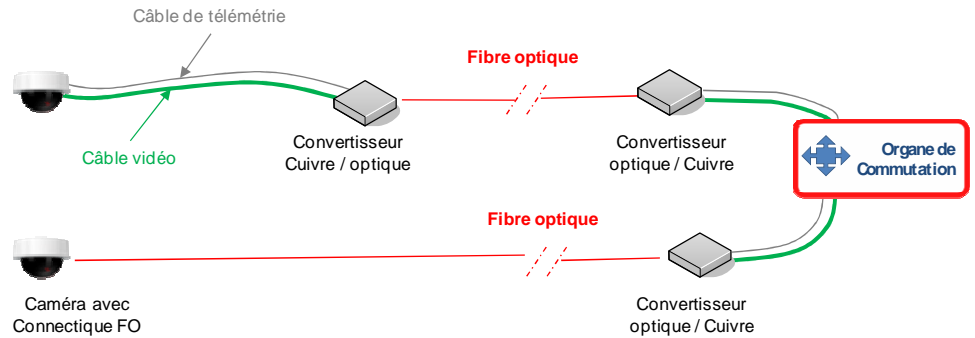
- Modulation de fréquence dans le câble coaxial (solutions propriétaires),
- Mise en place, en parallèle, d'un câble cuivre à paires torsadées. Il peut s'agir d'un câble supplémentaire, indépendant, ou de paires torsadées intégrées dans la gaine du câble coaxial (des câbles d'alimentation basse tension peuvent également être intégrés).





Au-delà de ces distances, l'utilisation de **fibres optiques** est préconisée : fibre optique multimode (MM) jusqu'à 3 km et monomode (SM) jusqu'à 10 kilomètres environ. Un bilan de liaison doit être systématiquement réalisé pour déterminer précisément la distance maximum acceptable en fonction de l'atténuation constatée sur la liaison optique (fiche de recette), des niveaux de puissances fournis en entrée et requis en sortie.

L'utilisation de la fibre optique implique la mise en place de convertisseurs cuivre/optique à chaque extrémité de la liaison. A noter que certaines caméras intègrent directement ce type d'équipement.



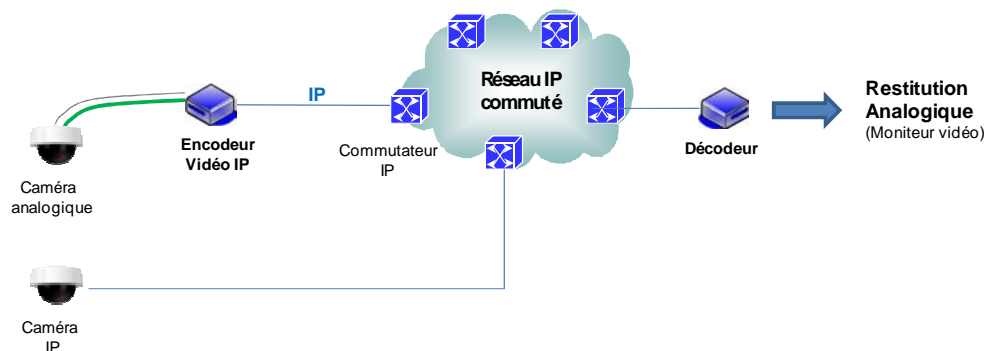
Des solutions de transmission hertzienne sont également disponibles. Toutefois, il faut bien s'assurer du cryptage des transmissions, la capture d'un signal analogique vidéo étant beaucoup plus aisée que la capture d'un signal numérique.

TRANSPORT NUMERIQUE (IP)

Pour la desserte des caméras, les technologies numériques sont utilisées dans les cas suivants :

- En prolongation d'un cœur de réseau numérique,
- En point-à-point pour le raccordement d'une caméra dont l'emplacement géographique justifie le choix de technologies sans fil ou le recours à une offre de services d'un opérateur de télécommunications.

Comme évoqué précédemment (cf. 7.2.2) lorsque des caméras analogiques sont utilisées, il est nécessaire de numériser les signaux vidéo et de télémétrie avant de les intégrer dans le réseau central, soit via un encodeur (ou serveur vidéo) ou un enregistreur de type DVR.



Le choix du support IP entre la caméra (ou l'encodeur IP) et le point de raccordement au réseau est large. Il est fonction de la faisabilité technique de la technologie choisie et des principaux avantages de chacune d'elle :

Solutions privatives



Ces liaisons nécessitent que le matériel soit acheté et installé au préalable. La gestion du réseau et la maintenance des matériels ne sont toutefois pas garantis, il faut donc le prendre en compte dans la maintenance du système (contrat de maintenance). Il faut donc s'assurer de bien disposer des ressources et des connaissances nécessaires, surtout dans le cas où aucun contrat de maintenance n'a été souscrit. Il n'est ici généralement pas nécessaire de s'acquitter d'un loyer pour l'utilisation de ces technologies.

Solutions privées filaires :

- Réseau Ethernet sur cuivre (4 paires FTP) : distance maxi 90m (1 km maxi avec des commutateurs LRE – Long Reach Ethernet),
- Réseau Ethernet sur fibre optique : distance cible 550 m en multimode et 5 km en monomode.
Note : dans ce cas, l'encodeur est souvent positionné à proximité du commutateur IP.

Solutions privées sans fil :

- Liaison de type pré-wimax (matériels ne nécessitant pas de licences d'utilisation)
- Faisceau Hertzien, (distance très variable selon les conditions météorologiques, l'environnement urbain ou rural, portée de 50m à 1km)
- Liaison laser (nécessité de vision directe, le passage d'un objet devant le trajet du laser rend la liaison inefficace)

Dans ce cas comme évoqué au paragraphe « Cas d'un réseau numérique », il faut bien vérifier la compatibilité entre la technologie choisie et l'objectif fixé (confidentialité, débit, garantie de service...). Les solutions WIFI ne sont pas nommées expressément car aucune garantie de service n'est proposée actuellement, et que l'explosion de ces solutions sur des produits grand public peut selon les sites provoquer des saturations réseau.

Solutions opérées

Un opérateur de service (comme les opérateurs de téléphonie mobile pour la téléphonie), en contrepartie d'un loyer et parfois d'un coût d'acquisition (dépendant du débit nécessaire ou de la quantité de données transmises sur une période donnée), met à disposition, à proximité de la caméra, une interface et un débit associé. Il garantit selon le contrat le transport des flux en tenant compte de leurs caractéristiques (flux temps réels, priorisation). Les liaisons fournies par les opérateurs peuvent être de type filaires ou sans fil. Ces solutions sont généralement plus chères que les solutions privées, toutefois, elles possèdent un avantage majeur car la maintenance et le remplacement du matériel défectueux est souvent réalisé par l'opérateur (y penser lors de la signature du contrat d'opérateur, en intégrant par exemple la période d'indisponibilité maximale).

Solutions opérées filaires :

Les deux solutions suivantes sont des offres sur lesquelles la qualité de service et la sécurité sont généralement garanties.

- de type fibre optique : le débit est alors élevé, souvent supérieur au besoin
- de type xDSL sur paires de cuivre : cette solution permet des débits de plusieurs Mb/s en général suffisants si le codage est performant. Bien vérifier avec l'opérateur le débit montant de la liaison.



Il peut arriver que le réseau de transport soit Internet. La qualité de service n'est alors pas garantie, mais le coût est moindre. Il faut alors



particulièrement veiller à l'aspect sécurité : l'usage d'un login/ mot de passe associé à un chiffrement SSL (https) est indispensable, l'authentification par certificat est préférable

Solutions opérées sans fil :

- Liaison de type Wimax (dans les zones couvertes),
- Services de données sur les réseaux GSM (3G, 3G+, UMTS).

Dans ce cas comme évoqué précédemment il faut bien vérifier avec l'opérateur que la technologie choisie permet de remplir l'objectif fixé, en terme de confidentialité, de sécurité, et de débit ; des tests terrain sont toujours le meilleur moyen de vérifier la compatibilité. La remarque concernant les réseaux sans fil (§Cas d'un réseau numérique) est ici également toujours valable.

7.2.4. BLOC 3 : L'EXPLOITATION DES IMAGES



Les paragraphes « Le pilotage des caméras » et « La visualisation » concernent exclusivement les systèmes supervisés. Le paragraphe « La consultation » concerne aussi bien les systèmes non supervisés que les systèmes supervisés.

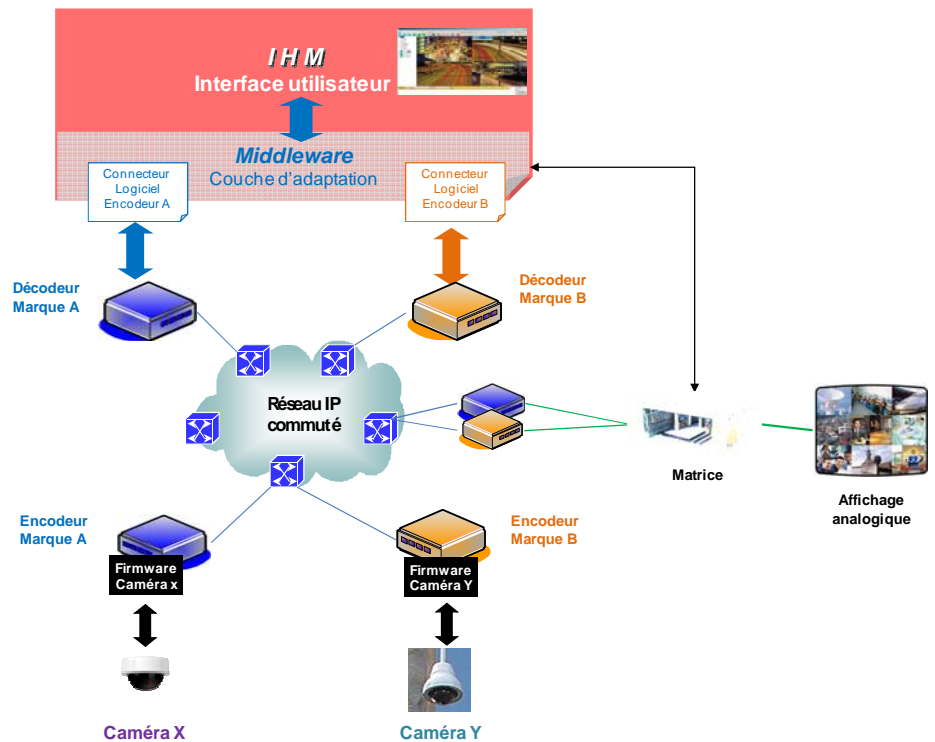
Les organes de pilotage et de contrôle revêtent une importance prépondérante dans l'efficacité d'un dispositif de vidéosurveillance. Il s'agit, en effet, d'exploiter, en temps réel, un système complexe sur le plan technique, avec des contraintes fortes sur les plans temporel et géographique.

Les environnements informatiques graphiques permettent désormais de répondre de manière efficace à la problématique et proposent des **I**nterface **H**omme-**M**achine (IHM) performantes et ergonomiques.

L'IHM communique donc avec l'ensemble des constituants de l'architecture technique (caméras, encodeurs/décodeurs, enregistreurs, système d'affichage, matrice vidéo, ...). Le dialogue est bidirectionnel.

En fonction des objectifs à atteindre, de la dimension du projet et du phasage de son déploiement dans le temps, une attention particulière doit être portée sur la capacité de l'IHM à être interopérable avec le plus grand nombre d'équipementiers du marché :

- une IHM « propriétaire » dialoguera parfaitement avec les équipements du même constructeur (systèmes globaux packagés) mais proposera une interopérabilité limitée ou des pertes de fonctionnalités avec d'autres fabricants.
- une IHM ouverte permettra l'intégration d'éléments d'architecture provenant de différents fabricants, ouvrant ainsi le spectre du choix des équipements et favorisant la concurrence.



LE PILOTAGE DES CAMERAS

L'ARCHITECTURE LOGICIELLE

Plusieurs opérateurs regardant les images, l'application est souvent en multipostes, et s'appuie sur une architecture classique de type client / serveur ou Ntiers, afin de pouvoir gérer facilement les surcharges réseaux et l'utilisation des caméras par de multiples utilisateurs.

La notion de disponibilité de l'application est un point très important. Ainsi, les serveurs mis en place bénéficient souvent d'un niveau de redondance adapté (actif/standby, partage de charge, ...).

Principales fonctionnalités de l'IHM :

Une IHM bien pensée doit permettre à un opérateur de se concentrer sur ses objectifs et missions en s'affranchissant complètement des aspects techniques. Les principales fonctionnalités courantes sont les suivantes :

Gestion de la cartographie : la base de travail est constituée usuellement par un fond de plan couvrant la zone à surveiller, avec fonction de zoom avant et arrière et hiérarchisation. Ce fond de plan peut être une simple image (cartographie statique) ou une source issue d'un système d'information géographique (SIG). Cette dernière approche constitue une tendance forte du marché.

Pilotage des caméras : toutes les caméras raccordées doivent pouvoir être pilotées à partir de l'interface graphique de l'IHM. La sélection et le pilotage des caméras pourront s'effectuer à partir du clavier du poste de travail, de la souris et/ou d'un Joystick.

Gestion de l'affichage : affectation des caméras à visualiser depuis la carte ou une liste hiérarchisées des caméras (tree-view) vers le système d'affichage.

Gestion d'une arborescence (tree view) : regroupement de caméras par zone géographique sous une forme arborescente (ville, rives, quartier, secteur, rue, etc...) de manière à ce que l'opérateur puisse accéder rapidement à l'ensemble



des caméras correspondant à la zone géographique choisie,

Gestion des cycles et prépositions : lorsqu'une caméra n'est pas pilotée par un opérateur, elle décrit, en cycle, un ensemble de cadrages prédéfinis ou prépositions.

Caméra postée : possibilité, pour les opérateurs, de désactiver les cycles d'une caméra et de la figer volontairement sur un cadrage.

Mode « poursuite » : lorsque le mode poursuite est enclenché, les caméras les plus proches de celle en cours de pilotage (5 au maximum), s'affichent sur le mur d'images et se positionnent en fonction de l'angle de vision de la caméra pilotée.

Relecture d'images enregistrées : potentiellement, le module relecture peut être intégré à l'IHM. Les images sont alors affichées sur le poste de travail de l'opérateur ou sur un moniteur externe. A noter que la relecture peut également être disponible sur une application dédiée (cf. §La consultation).

LE POSTE DE TRAVAIL

Le poste de travail destiné à l'opérateur doit lui permettre d'atteindre ses objectifs et de réaliser les missions qui lui sont confiées.



L'ergonomie des postes de travail est primordiale pour une efficacité optimum des opérateurs.

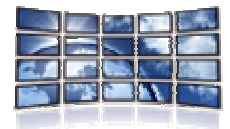
Les conditions de travail doivent être les plus agréables possibles :

Le poste de travail en lui-même est équipé :

- D'un PC équipé de l'Interface Homme Machine,
- De deux écrans :
 - Un écran pour l'interface graphique,
 - Un écran pour la visualisation des images,
- D'un joystick de pilotage,
- Des moyens de communications nécessaires pour contacter les services de police (radio, téléphone, ...).

LA VISUALISATION

MUR D'IMAGES



Pour les systèmes supervisés, la présence d'un mur d'images est souvent appréciée pour donner une vue d'ensemble du périmètre vidéosurveillé, et pouvoir gérer des situations de crise et de grands événements. Le mur d'images est utilisé pour la visualisation en temps réel des images issues des caméras.

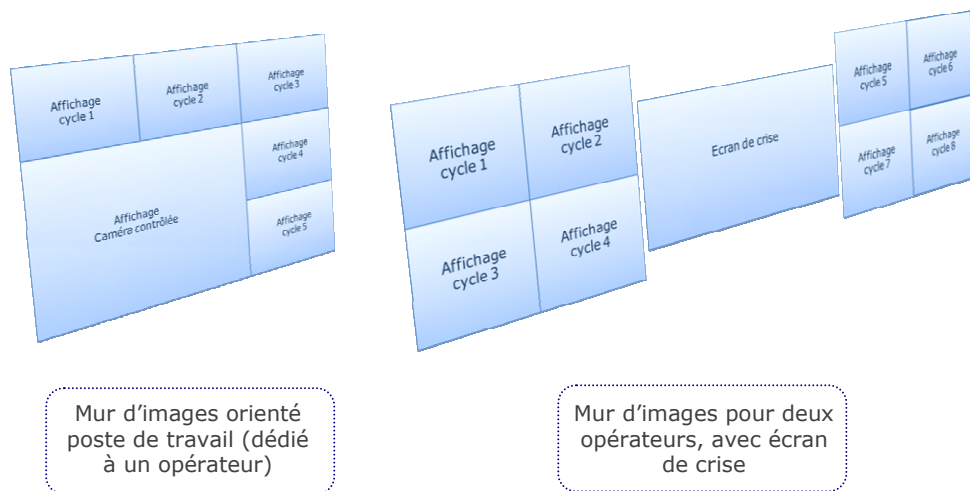
La disposition d'un mur d'images est fonction :

- Des objectifs attendus,
- Des missions affectées aux opérateurs : travail individuel ou en équipe,
- Du nombre de moniteurs qui le composent,
- Des scénarii d'affichages envisagés,
- Des fonctions dédiées à certaines zones du mur d'images.

Le mur d'images doit être suffisamment éloigné pour avoir une vue d'ensemble des écrans (au minimum à 2m de l'opérateur).



Un mur d'images peut être segmenté par opérateur pour un travail individuel ou, par opposition, mutualiser entre différents opérateurs de manière à favoriser un travail en équipe.



Le nombre de moniteurs composant un mur d'images est variable en fonction de la finalité du dispositif de vidéosurveillance. Il n'est pas directement lié au nombre de caméras. Les critères déterminants sont généralement les suivants :

- Nombre d'opérateurs visualisant le mur d'images : le nombre de moniteurs maximum pouvant être supervisé par un opérateur est estimé entre cinq et huit,
- Nombre de moniteurs dédiés à une fonction.

Sur chacun des moniteurs (ou équivalent en multivision), il est généralement apprécié de générer des cycles d'affichage de caméras (jusqu'à six caméras par moniteur) qui globalement composent les scénarii de visualisation en temps réel (rondes virtuelles...).

VISUALISATION DE CRISE

En cas de crise, le système de vidéosurveillance prévoit un dispositif spécifique de visualisation. Ce dispositif peut :

- Etre intégré au mur d'images, l'écran, souvent de grande dimension, est alors, en fonctionnement nominal, éteint,
- Etre installé dans une salle de crise spécifique et faire parti d'un dispositif de crise plus global. Cette tendance tend à se généraliser.

LA CONSULTATION

Sur les systèmes non opérés l'interface avec le système est réduite à l'exploitation des images enregistrées et aux opérations d'exports. Sur les systèmes opérés, cette opération est tout de même l'un des principaux gages d'efficacité du système.

Le logiciel ou l'interface utilisés doivent être simples d'utilisation, doivent permettre de remonter facilement à des vidéos en fonction de la date, l'heure, ou l'identifiant de la caméra. Des fonctions de recherche sur les trois critères précédents doivent être permises. Il est conseillé que le logiciel permettant l'exploitation des images enregistrées propose une lecture accélérée, image par image, zoom numérique dans l'image, impression d'un arrêt sur image en pleine qualité, exportation de séquences sélectionnées...

L'enregistrement et la consultation des images sont des fonctions qui doivent pouvoir se dérouler simultanément. La recherche des images mémorisées doit être multicritères.



Les critères principaux sont les suivants :

- Plage de date et d'heure de mémorisation,
- Zone géographique dans laquelle les images ont été enregistrées. Il est souhaitable que la zone à considérer puisse être définie de manière graphique.

Avec des systèmes plus évolués, il est également possible d'associer des critères d'analyse d'image, à la recherche, pour n'afficher par exemple que les séquences contenant un mouvement. Il est conseillé d'inclure des fonctions de recherche s'appuyant sur des traitements intelligents selon l'objectif du système de vidéoprotection pour réduire la durée de la recherche. (cf. la fiche 12 « traitements intelligents »).

En effet, l'utilisation de traitements intelligents et de critères de recherche efficace et simple d'emploi peut permettre de d'économiser du temps lors des opérations de consultation et d'exports des images. Une recherche d'événements sur un système peut devenir très complexe selon le nombre de caméras déployées et la zone géographique et temporelle couverte.

L'exportation des images sélectionnées est traitée spécifiquement dans la fiche N°6 En synthèse, on peut rappeler que ces exportations, surtout pour les systèmes soumis au régime juridique de la loi du 21 janvier 1995, doivent être réalisées sans perte afin que les images exportées soient bien les mêmes que celles enregistrées sur le système: Il serait aberrant qu'après exportation on ne puisse plus reconnaître l'auteur d'un crime sur la vidéo exportée, personne qu'il était aisé d'identifier sur le système. Toutes les informations sur les opérations d'exportation (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) sur le système doivent être fidèlement conservées de manière automatique ou manuelle selon la taille du système.

7.2.5. BLOC 4 : L'ENREGISTREMENT, LE STOCKAGE.

Les systèmes d'enregistrement sont désormais systématiquement numériques. Leurs structures matérielles se basent sur des équipements informatiques spécifiques ou banalisés.

Ainsi, la politique de stockage est de nature à s'intégrer, de plus en plus, dans le schéma global d'organisation du système d'information d'un établissement, mutualisant ainsi, des équipements partagés par différentes applications (solution de stockage SAN et NAS).

Le stockage des vidéos peut être envisagé de manière décentralisée (caméra enregistrée par groupes locaux) ou centralisé enregistrement de toutes les caméras en un ou deux points uniques. Il n'est pas question ici de trancher sur les avantages d'une ou de l'autre solution, toutefois, il faut voir que le choix de l'une ou l'autre solutions peut apporter des facilités en termes de maintenance et d'évolution, ou en termes de coûts selon l'ampleur et le délai de rentabilité souhaité. Il est conseillé de s'appuyer sur le résultat de l'étude de cas pour motiver son choix, car il est fortement dimensionnant pour les évolutions futures du système de vidéoprotection.

LA NOTION DE DVR

Les DVR (Digital Video Recorder) sont des équipements destinés à l'enregistrement numérique des flux vidéo et le stockage des données. Ces équipements sont utilisés pour la numérisation/compression des flux provenant des caméras analogiques afin de les enregistrer et également de les rendre accessible via un réseau informatique (les équipements qui numérisent et compressent les flux vidéo analogiques pour les diffuser sur le réseau sans les enregistrer sont uniquement des encodeurs).

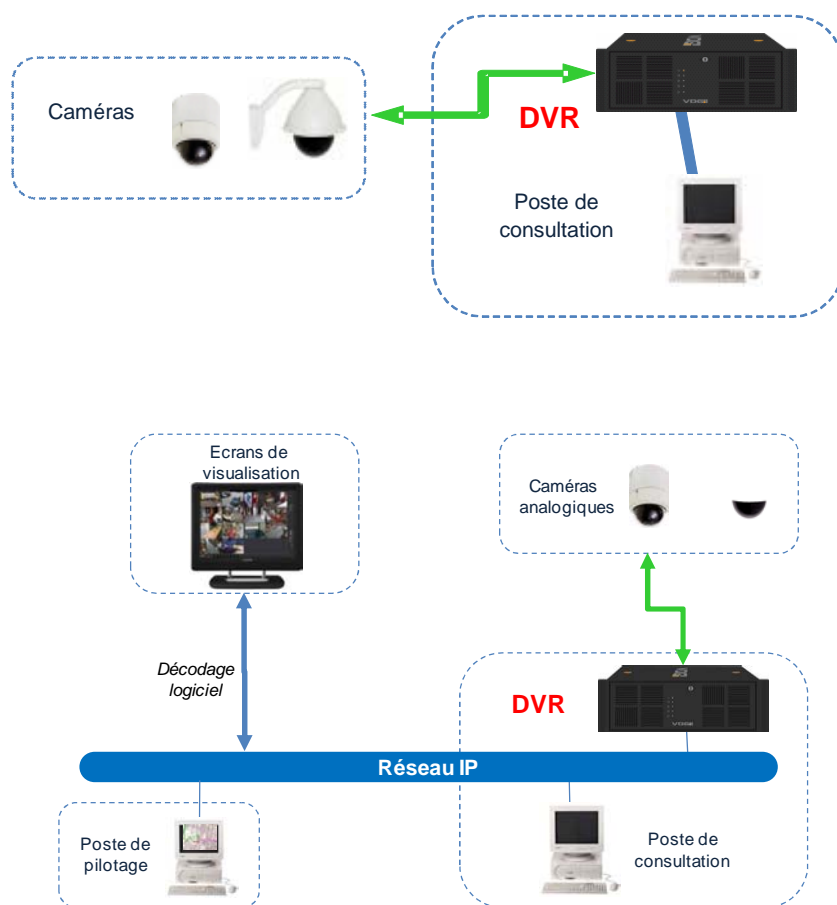


Pour ce faire, ils sont équipés de cartes d'acquisition permettant de numériser les flux vidéos analogique (encodage), de capacités de stockage (disque dur) et disposent d'une connectivité au réseau IP au travers duquel est réalisée la consultation des images enregistrées à partir de postes clients.

En termes d'architecture, les caméras analogiques sont raccordées directement sur l'équipement (connecteurs BNC ou S-Vidéo généralement). Certains boîtiers « tout-en-un » assurent également les fonctions de commutation, pilotage (IHM) et restitution, positionnant ainsi le DVR au cœur d'un dispositif de vidéosurveillance. Il conviendrait d'ailleurs dans ce cas de rebaptiser le DVR compte tenu de ses fonctions étendues.

Ce type de solution, propriétaire, est très adaptée à la surveillance de périmètres de faible envergure. Même si la nécessité d'accéder aux images enregistrées par le réseau n'a pas été relevée par l'étude fonctionnelle, ces systèmes représentent la nouvelle génération des enregistreurs analogique à bandes (VHS...).

Il est très important toutefois de vérifier dans le cas où des caméras mobiles ou avec zoom optique sont utilisées, que le DVR est compatible avec les fonctions de télémétrie de cette caméra (ces fonctions étant généralement spécifiques).



LA NOTION DE NVR

Présent au sein des grands systèmes numériques, le NVR (Network Video Recorder) est un équipement dont le rôle est d'enregistrer les images provenant du réseau (IP) et d'en assurer le stockage. Ce matériel est donc adapté aux systèmes utilisant des caméras IP ou des caméras analogiques avec encodeurs. Les fonctions de commutation et d'encodage sont, pour leur part, réalisées, en amont, par d'autres équipements.



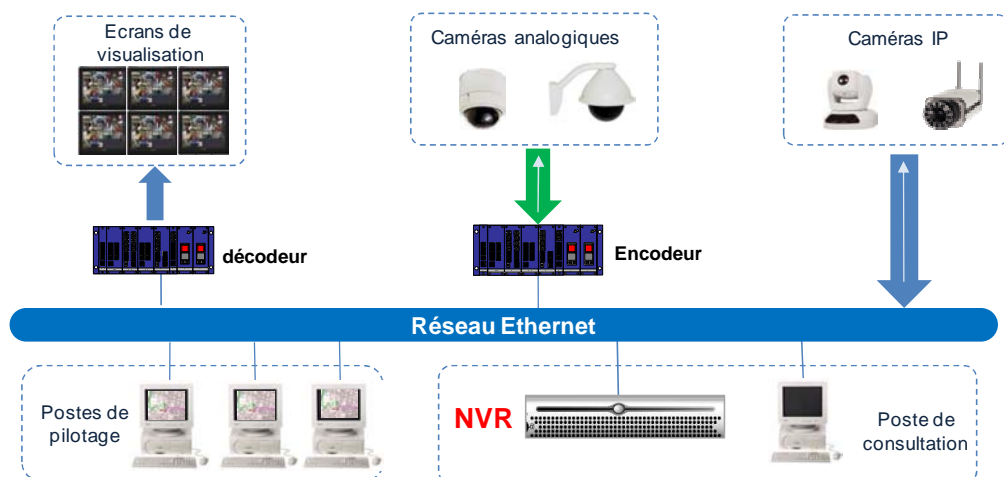
Sur le plan matériel, il s'agit généralement de serveurs informatiques banalisés associés à une grande capacité de stockage (interne ou externe). L'architecture logicielle est généralement de type client-serveur.

Le recours à ce type de solutions permet assurément de bénéficier de tous les avantages capitalisés au sein du système d'information dont la tendance est à l'urbanisation : le NVR représente ainsi un îlot du système d'information, banalisé, communicant et sécurisé, mutualisant des ressources techniques et humaines souvent existantes. (Architecture, ressources humaines, ...). Il n'est pas conseillé de stocker sur les mêmes disques physiques les données provenant du système de vidéoprotection et des données tierces (voix, données de l'entreprise...), toutefois, il est possible de s'appuyer sur des architectures similaires et de profiter des ressources humaines compétentes. Les NVR ne sont que des systèmes de stockage informatique un peu plus performant en capacité d'entrée/sortie que les disques réseau traditionnels.

Les principaux avantages sont les suivants :

- Utilisation de plates-formes matérielles non propriétaires,
- Fortes capacités d'évolution et d'extension (scalabilité),
- Mutualisation de ressources existantes :
 - techniques : stockage NAS/SAN, sécurité physique et logique, ...
 - humaines : profils et compétences des intervenants,
- Solution de sécurisation physique et logicielle maîtrisée (redondance, clusterisation de serveurs, ...),
- Par voie de conséquence, la maîtrise des coûts d'investissement et d'exploitation.

Les NVR se positionnent dans les architectures de systèmes de grande envergure, car ils nécessitent une certaine connaissance en administration de systèmes informatiques.



7.2.6. L'ADMINISTRATION DU SYSTÈME

Un système complexe doit disposer d'un ensemble d'outils performants permettant son administration technique.

Dans un système homogène dont les constituants sont issus d'un seul constructeur, ces différents outils sont fédérés sous une application unique.



Dans un système ouvert mettant en œuvre des constituants provenant de différents constructeurs et éditeurs, les outils d'administration sont souvent propres à chaque élément d'architecture. Ces différents outils peuvent alors être fédérés au travers de l'IHM (au moins en termes d'accès).

Des opérations de maintenance peuvent également être proposées, et sont fortement recommandées (vérification du bon fonctionnement des caméras, vérification du bon positionnement des caméras...). La supervision de la maintenance doit être gérée de la même manière que l'administration. Il est très fortement conseillé d'utiliser à ce titre des traitements intelligents pour faciliter et réduire le temps et le coût de la maintenance. (Gestion du masquage, du floutage, de la défaillance d'une caméra...cf. fiche 12 « traitements intelligents »)

Contrairement à la notion de stockage, celui-ci pouvant être centralisé ou décentralisé, il est très important voire indispensable de prévoir une administration centralisée du système, c'est-à-dire que celle-ci peut s'effectuer sur tout le système depuis un point unique (souvent la salle ou un poste d'exploitation dédié de préférence)

L'administration concerne notamment :

Au niveau des caméras :

Gestion technique et paramétrage,
Programmation des prépositions et cycles,
Masquage dynamique,

Au niveau des équipements d'interfaces (encodeurs, convertisseurs,...),

Gestion technique et paramétrage,
Remontée d'alarmes.

Au niveau de l'organe de commutation (matrice ou réseau IP),

Gestion technique et paramétrage,
Remontée d'alarmes.

Au niveau enregistrement :

Gestion technique et paramétrage,
Remontée d'alarmes.

Au niveau IHM :

Gestion technique et paramétrage,
Statistiques et traçabilité,
Gestion des profils et droits utilisateurs,
Sécurisation du poste de travail,
Gestion des événements,
Remontée d'alarmes.



7.3. SYNTHÈSE UL 6 : LES MESSAGES ESSENTIELS

L'architecture d'un système de vidéosurveillance peut être modélisée selon quatre grandes briques suivantes :

L'acquisition et donc la qualité initiale de prise de vue détermine la qualité max de l'ensemble de la chaîne.

- L'optique (sa focale) permettra de définir si la visualisation est en plan étroit ou en plan large, et de définir la taille maximale des objets
- La sensibilité du capteur permettra de s'adapter à un environnement plus ou moins lumineux.
- Le positionnement de la caméra est plus important que la technologie utilisée: même avec une meilleure technologie, une caméra mal positionnée (trop loin, dans une zone mal éclairée) sera moins efficace.

La chaîne **de transport** des images est un poste de dépense important qui déterminera les possibles évolutions du système.

De plus, la capacité du réseau fixera la compression et donc la qualité des images transmises. (Il faudra veiller également à la différence de compression entre les vidéos temps réel et enregistrées en vérifiant que ces dernières remplissent toujours les objectifs du système)

Pour **le pilotage, la visualisation et la consultation** (IHM), il faut veiller à faciliter l'accès aux images, et en particulier aux images enregistrées, en associant des critères simples de recherche.

Pour **l'enregistrement**, il est important de restituer fidèlement les images enregistrées pour que les images enregistrées permettent toujours de remplir les objectifs du système de vidéoprotection, et que l'export des images n'entraîne pas d'arrêt de l'enregistrement.

Aucune de ces briques ne doit être négligée lors de la conception du système pour éviter tout maillon faible dans le traitement des images.

La technique et la technologie sont mises au service des besoins exprimés et des objectifs en termes de résultats :

- Les choix techniques et d'architecture se déclinent à partir des besoins fonctionnels et organisationnels exprimés et tiennent comptes de l'environnement, des contraintes opérationnelles et financières,
- Les technologies d'aujourd'hui sont aptes à s'adapter et à répondre à toutes les attentes, et les contraintes imposées.

Les choix techniques, ainsi que l'offre de produits et services, sont très étendus. Pour répondre à un besoin exprimé, plusieurs solutions sont souvent envisageables. Aussi, l'enjeu consiste à trouver le meilleur compromis qui, à la fois, réponde au cahier des charges formalisé et respecte les budgets alloués en investissement et fonctionnement. Il s'agit en particulier :

- De tirer parti des avantages des différentes technologies disponibles en les adaptant de manière pertinente au contexte,
- D'évaluer, en amont, l'évolution et l'évolutivité du système mis en place,
- De se prémunir d'une certaine captivité par rapport aux équipementiers et éditeurs choisis lors des premières phases de déploiement.

La mutualisation des infrastructures, des ressources techniques et humaines doit, par ailleurs, rester une préoccupation permanente. Cette attitude est garante d'une rationalisation des coûts en investissement et en exploitation.



**La définition de
l'architecture
technique du
système**

UL 6

**De l'architecture
technique à la
livraison**



Globalement, le volet technique n'est pas un frein mais peut, au contraire, constituer un moteur au développement de la vidéoprotection et faciliter le déploiement d'autres services qui partageront les mêmes supports.

Ce tableau doit permettre de faciliter la compréhension et le choix des technologies existantes concernant les blocs fonctionnels.

ACQUISITION		Types	Fixe	Mobile (sur tourelle ou dôme)
		Champs d'application	Plan étroit (rue, couloir, ...). Scène unique (entrée, barrière, ...)	Grande zone à couvrir, sur 360°. Tracking. Zoom nécessaire.
		Particularités	Utile pour réaliser de l'analyse d'image. Peut être équipé d'un zoom.	Grande vitesse de rotation. Zoom important.
TRANSPORT		Types	Analogique	IP
		Champs d'application	Architecture composée d'un seul point de raccordement, dans un périmètre géographique restreint	Architecture basée sur plusieurs points de connexion en réseau. Liaison sans-fil ou opérée.
		Particularités	Bonne qualité des images en temps réel	Fort potentiel de mutualisation des infrastructures
COMMUTATION		Types	Analogique	Numérique (réseau commuté IP)
		Champs d'application	Reprise d'un système existant. Système de taille réduite.	Tout type de projet. Incontournable dans les architecture basée sur plusieurs points de connexion en réseau.
		Particularités	Equipement dédié à la vidéo.	Peut utiliser un réseau existant.
PILOTAGE		Types	IHM propriétaire	IHM Ouverte
		Champs d'application	Système de dimension limitée. Fonctionnalités standards.	Réutilisation de matériels existants. Architecture évolutive en termes de fonctionnalités et de matériels utilisés.
		Particularités	Le maître d'ouvrage s'adapte au système et non le contraire.	Des développements spécifiques peuvent être nécessaires pour intégrer un constructeur non référencé (sur la base d'un SDK)
VISUALISATION		Types	Moniteurs vidéo	Mur d'images modulaire
		Champs d'application	Poste de travail. Mur d'images classique	Affichage de données et de cartes en plus des vidéos. Affichage de vidéos sur de grandes surfaces.
		Particularités	Tendance : Evolution des moniteurs vidéo vers des écrans informatiques	L'affichage constitue à lui seul une solution à part entière
ENREGISTREMENT		Types	DVR	NVR
		Champs d'application	Système de faible envergure.	Système numérique de grande envergure.
		Particularités	Les caméras sont raccordées directement sur le DVR.	Equipement banalisé (serveur informatique).



8. UL7 : L'APPEL D'OFFRES, LE DEPLOIEMENT ET LA VALIDATION

8.1. LES QUESTIONS-CLES AVANT DE LANCER L'APPEL D'OFFRES

Est-ce que la maître d'ouvrage :

- a des objectifs de sécurité précis?
- dispose d'un diagnostic de sécurité représentatif, fiable et complet ?
- est en mesure d'exprimer clairement ses besoins, et ses contraintes de manière à les formaliser dans un dossier de consultation ? Les approches suivantes peuvent être envisagées :
 - Réalisation d'un programme fonctionnel et dialogue avec les candidats jusqu'à l'élaboration de la solution finale,
 - Rédaction de spécifications techniques précises (Cahier des Clauses Techniques particulières).
- bénéficie d'un retour d'expérience acquis auprès d'entités ayant mené un projet similaire ?
- a évalué les limites que la réglementation en vigueur impose à son projet?
- dispose des compétences et des ressources internes pour mener à bien le projet technique ou estime-t-il que le recours à une assistance externe (Assistance à Maîtrise d'Ouvrage ou Maître d'œuvre) est nécessaire ?
- a mesuré l'impact de l'architecture du système en termes de coûts d'investissement et d'exploitation relatifs au système à mettre en œuvre ?
- a, en conséquence, une idée précise du mode d'exploitation qu'il souhaite mettre en œuvre
- a, le cas échéant, un projet d'organisation des relations avec les entités opérationnelles d'intervention ?
- a exploré toutes les opportunités de mutualisation d'infrastructures et ressources avec ses partenaires potentiels, et, en fonction de la taille de l'entreprise, ses différents services internes?
- a prévu d'accompagner la mise en œuvre de sa vidéo protection par une campagne de communication adaptée à destination des usagers des zones à surveiller, de manière à prendre en compte leurs craintes éventuelles et à faciliter l'acceptation ?



**La définition de
l'architecture
technique du
système**

UL 7

**L'appel d'offres,
le déploiement et
la validation**



8.2. L'APPEL D'OFFRES

L'appel d'offres est une phase qui formalise les besoins exprimés, les contraintes opérationnelles et environnementales et qui constitue un processus d'achats.

L'un des objectifs à atteindre sur le plan contractuel est de garantir au Maître d'Ouvrage un cadre d'achats exhaustif sur la durée du marché prenant en compte notamment :

Les investissements initiaux (prestations forfaitaires),

Les éventuelles extensions (prestations à prix unitaires),

Les coûts de maintenance associés.

Le Dossier de consultation des entreprises (DCE) doit satisfaire aux impératifs suivants :

être strictement ouvert à toutes les entreprises compétentes du marché, intéressées par le projet, sans discrimination ou orientation technique,

présenter un niveau de précision et d'exigence suffisant pour ne laisser place à aucune interprétation de la part des soumissionnaires,

suyant l'importance du projet, proposer un découpage en lots permettant une réelle mise en concurrence des acteurs dans les domaines identifiés dans lesquels la concurrence existe.

En effet, comme tout appel d'offres, un marché de vidéo protection peut être décomposé en plusieurs lots.

Les infrastructures « passives » comme la pose de fourreaux ou de câbles ou des travaux tels que l'aménagement de locaux (peinture, climatisation, ...) peuvent faire l'objet de lots indépendants.

En revanche, en ce qui concerne les équipements « actifs » (caméras, équipements de réseaux, écrans, postes de travail, enregistreurs, IHM, ...), il est préconisé de les regrouper dans un même lot afin de maîtriser l'ensemble de la chaîne de liaison (de l'acquisition à la restitution).

Sauf contrainte particulière, le DCE devra être assez ouvert de manière à permettre :

Différents types de réponse :

Les systèmes ouverts (plusieurs constructeurs),

Les systèmes intégrés et propriétaires (un seul constructeur).

Différents types d'architecture :

Système mixte analogique/numérique,

Système entièrement numérique.

Dans cette philosophie et compte tenu de la complexité potentielle des propositions, la phase d'analyse des offres revêt une dimension très importante et requiert un travail important. La tendance aujourd'hui va clairement vers les procédures permettant un dialogue ouvert avec les candidats.



8.3. DEPLOIEMENT

8.4.1 MÉTHODOLOGIE ET ORGANISATION

Un projet, tel que la mise en œuvre d'un système de vidéo protection, reste unique, avec ses spécificités, un certain degré d'incertitude et des risques à identifier et maîtriser. La méthodologie de déploiement à appliquer doit donc être éprouvée.

Il apparaît donc indispensable de découper le projet en plusieurs phases, afin de mieux maîtriser et contrôler leur déroulement et leur enchaînement.

Le passage d'une phase à la suivante est validé par un livrable qui représente un moyen tangible d'apprécier les résultats intermédiaires ou finaux. Chaque phase laisse néanmoins la possibilité d'un repli sur la phase précédente et sécurise ainsi la démarche globale.

Lors du déploiement, le découpage du projet en phase est défini dans le cadre de l'établissement d'un Plan de Projet, en collaboration avec l'entreprise en charge de la réalisation (intégrateur et/ou opérateur).

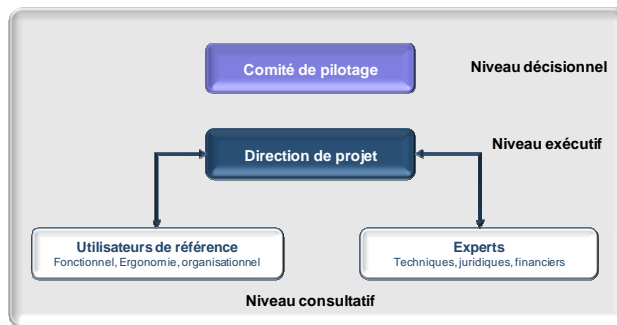
Cette démarche doit être adaptée aux ressources humaines disponibles côté Maître d'Ouvrage.

En résumé, le déploiement s'intègre dans une démarche de Conduite de Projet dont la finalité est de maîtriser à tout moment le cadre technique, les délais, les coûts et la qualité.

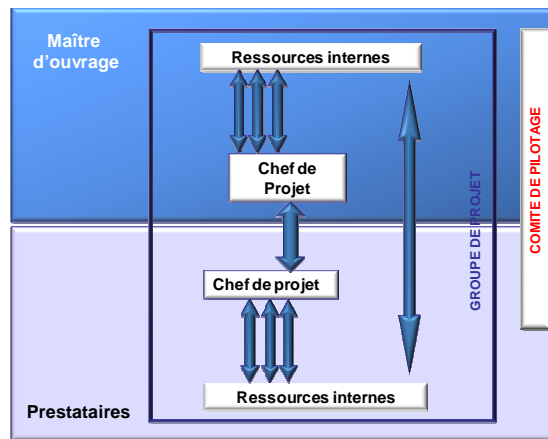
Compte tenu de la dimension stratégique et politique des projets de vidéo protection, un pilotage à 2 niveaux est préconisé :

Niveau de pilotage stratégique : il garantit la pertinence du projet et décide d'adapter ou non la cible à atteindre par le projet en fonction des évolutions externes, voire internes, du projet.

Niveau de pilotage opérationnel : il garantit l'atteinte de la cible du projet, et décide d'adapter ou non le déroulement du projet pour atteindre la cible.



En termes d'organisation, il est indispensable que le maître d'ouvrage et le titulaire du marché désignent un chef de projet, chargé de coordonner les différentes équipes ou sous-traitants intervenant sur le système.



8.3.1. PHASE DE PRÉPARATION

La phase de déploiement est précédée d'une phase de préparation dont l'objectif est de :

- finaliser le calendrier détaillé des travaux,
- réaliser la collecte des données nécessaire à la configuration des équipements,
- élaborer les dossiers d'exécution (plans d'installation, descriptifs techniques et fonctionnels détaillés, ...),
- prendre en compte les délais d'approvisionnement,
- finaliser le dossier de demande d'autorisation préfectorale.

8.3.2. PROTOTYPE

En fonction de l'importance du projet, une phase de prototype (maquette) est à prévoir avant déploiement concernant :

- l'architecture de la solution,
- les services packagés,
- les services nécessitant le développement d'un interfaçage spécifique.

Cette phase sera préalable au déploiement de la solution en phase pilote et aboutira au VISA de mise en œuvre de la part du Maître d'Ouvrage.

8.3.3. PILOTE

En fonction de l'importance du projet, les premiers sites et services qui seront déployés pourront servir de Pilote avant un déploiement généralisé.

Une batterie de tests sera alors réalisée, identiques à ceux prévus en phase de vérification d'aptitude.

8.3.4. FORMATION DU PERSONNEL

L'accompagnement des personnels en charge de l'exploitation du système est un volet essentiel dans le déroulement du déploiement. De celle-ci dépend la bonne appropriation des outils par les opérateurs et la maîtrise technique du système par les techniciens et donc, au final, l'efficacité du dispositif.



Concernant les opérateurs, deux types de formation sont nécessaires :

Formation, en amont, au métier d'opérateur de vidéosurveillance, proposée par des organismes référencés auprès de l'autorité,

Formation à l'utilisation des outils mis en place, assurée par le prestataire en charge du déploiement (titulaire du marché).

S'agissant des personnels techniques, les formations nécessaires à l'exploitation technique du système seront également assurées par le prestataire.

Une session de formation est systématiquement ponctuée par une évaluation qui valide sa portée et sa qualité.

8.3.5. DÉPLOIEMENT GÉNÉRALISÉ

Dès lors que les phases de prototype et pilote sont validées, le maître d'ouvrage peut ordonner le déploiement généralisé de la solution.

La gestion de l'avancement, le suivi et la coordination des différents prestataires nécessite, de la part du maître d'ouvrage, une présence forte sur le terrain. Des réunions d'avancement doivent être animées régulièrement, typiquement chaque semaine, pour la bonne maîtrise du projet et le traitement des aléas de chantier.

8.3.6. VALIDATION

La validation du bon fonctionnement du système passe par deux étapes :

une réception provisoire, qui constitue la Vérification d'Aptitude,

une réception définitive, qui permet la Vérification du Service Régulier.

Ces phases de réception seront précédées d'une Mise en Ordre de Marche (MOM) qui permet notamment de vérifier la livraison exhaustive des matériels et qui constitue une première base de travail pour la mise au point opérationnelle de la solution.

8.3.7. LA RÉCEPTION PROVISOIRE (VÉRIFICATION D'APTITUDE)

La réception provisoire, qui se déroule un mois après la MOM (Mise en Ordre de Marche), a pour objet de vérifier le bon fonctionnement de la totalité des matériels installés. Elle a lieu en présence du Maître d'Ouvrage.

Le Titulaire aura réalisé au préalable tous les tests sur la totalité des matériels afin d'avoir déjà localisé d'éventuels problèmes d'installation et en fournira la liste.

Un cahier de recette général est fourni à l'issue de cette réception. Ce document comprend :

le plan d'implantation du matériel,

les tests,

la nomenclature et documentation de tout matériel mis en œuvre.

8.3.8. LA RÉCEPTION DÉFINITIVE (VÉRIFICATION DE SERVICE RÉGULIER)



La réception définitive a pour objet de valider le bon fonctionnement des matériels suite à une exploitation proche de la configuration définitive, avec des liens en production. A titre indicatif, la recette définitive a lieu **2 mois** après l'acceptation de la recette provisoire si aucun défaut n'a été constaté.

8.3.9. DOSSIER D'INTERVENTIONS ULTÉRIEURES SUR LES OUVRAGES (DIUO)

Les documents à fournir par le titulaire du marché seront déclinés de la manière suivante :

Dossier d'installation :

Le dossier d'installation permet de réinstaller tout ou partie des équipements et logiciels mis en œuvre dans le cas, par exemple, d'un problème majeur ou d'une reconfiguration d'un serveur ou tout autre poste de travail.

Il comprendra au minimum les documents suivants :

la documentation technique complète de chacun des matériels installés, destinée aux exploitants des systèmes,

les procédures d'installation et de configuration des différents matériels et logiciels,

les plans de recollement relatifs aux travaux exécutés.

Dossier d'exploitation :

Le dossier d'exploitation est utilisé quotidiennement par les exploitants ou utilisateurs pour le bon fonctionnement de la plate-forme.

Il sera composé au minimum notamment des éléments suivants :

la documentation technique d'exploitation des organes centraux (matériels et logiciels),

les recueils de procédures d'exploitation.

Dossier de secours :

Le dossier de secours est le document de référence à utiliser en cas de dysfonctionnement, même mineur ; il doit permettre de rétablir le service dans les meilleurs délais, éventuellement en mode dégradé.

Il est pour sa part composé de toute procédure à mettre en œuvre immédiatement après le constat d'un incident.

La clarté du document est un point essentiel en cas d'urgence. Sa structure permet d'identifier instantanément les points suivants :

Identification de l'alarme :

Comment reconnaître une alarme,

Comment l'interpréter.

Diagnostic du problème :

En fonction du message, faire les tests permettant d'identifier l'élément ou le fonctionnement défectueux,

Déterminer de manière précise l'intervention à prévoir.

Procédures de résolution du problème :



Résolution définitive,

Mode dégradé.

8.3.10. PHASE D'ÉVALUATION DU DISPOSITIF EN MODE OPÉRATIONNEL

Après la mise en service officielle du dispositif, il est préconisé la mise en place d'un comité de suivi, dont le rôle sera notamment :

La vérification de la bonne exécution des règles déontologiques

Visualisation d'échantillons d'images enregistrées (caméras pilotées) et identification des opérateurs auteurs d'éventuels écarts,

Vérification de la stabilité des dispositifs techniques visant à respecter la vie privée (masquages dynamiques, ...),

Mise en place des actions correctives.

Le bilan de l'adéquation moyens / besoins

Mise à jour régulier de l'état de l'art fourni dans le cadre de la présente prestation (veille technologique),

Evaluation de l'évolution des besoins, exprimés dans le cadre du groupe de travail,

Evaluation de la pertinence du dispositif et de son adéquation aux besoins :

Positionnement des caméras,

Stratégie de visualisation des images,

Stratégie d'enregistrement,

Qualité des images,

Prise en compte des contraintes éventuelles formulées par les forces de l'ordre (force de terrain, police scientifique, ...),

Evaluation de la nécessité de développement du système,

Prise en compte des points d'amélioration identifiés par les exploitants,

Mise en œuvre des éventuelles actions correctives.

8.4. LES POINTS CLES A VERIFIER AVANT DE SIGNER LA RECETTE

Sur le plan fonctionnel, vérifier si les objectifs initiaux sont atteints :

Valider le périmètre couvert, la pertinence du positionnement des caméras au final,

Simuler l'ensemble des tâches en mode opérationnel : pilotage actif et réactif, affichage, analyse d'enregistrements, export de données, ...

Valider la qualité des images de jour et de nuit, en temps réel et au niveau de l'enregistrement.

Sur le plan organisationnel :

Valider les procédures internes : rôle de chacun,



Valider les procédures externes : relations avec les services de police, d'urgence, ...

Valider la traçabilité des actions et interventions.

Sur le plan humain :

Valider le niveau de formation des opérateurs et leur bonne appropriation du dispositif,

Valider l'adéquation des conditions de travail, de jour et de nuit, si possible par un ergonomiste,

Valider l'encadrement apporté aux opérateurs.

Sur le plan opérationnel :

Valider les procédures de maintenance et les conditions d'interventions, soit globalement les garanties du maintien en conditions opérationnelles,

Valider la sécurité des accès dans les CSV et les locaux techniques,

Identifier les éventuels points névralgiques du dispositif.

Sur le plan réglementaire :

Valider la conformité de la signalétique mise en place dans les zones surveillées,

Valider la stabilité du masquage appliqué aux caméras,

Valider les conditions et la sécurité d'accès aux informations (images),

Valider l'habilitation des différents intervenants.



8.5. SYNTHÈSE UL 7 : LES MESSAGES ESSENTIELS

La mise en œuvre de systèmes complexes tels que ceux destinés à la vidéosurveillance implique de nombreux acteurs et nécessite une gestion de projet rigoureuse. Un pilotage à deux niveaux, stratégique et opérationnel, est le plus souvent nécessaire.

Le processus d'achats s'appuie sur des procédures classiques de consultation (formalisation des besoins et contraintes) et d'analyse des offres. Compte tenu de la diversité et de la complexité des propositions, la tendance va clairement vers les procédures favorisant le dialogue et la négociation avec les entreprises, sur la base de besoins fonctionnels exprimés par le maître d'ouvrage.

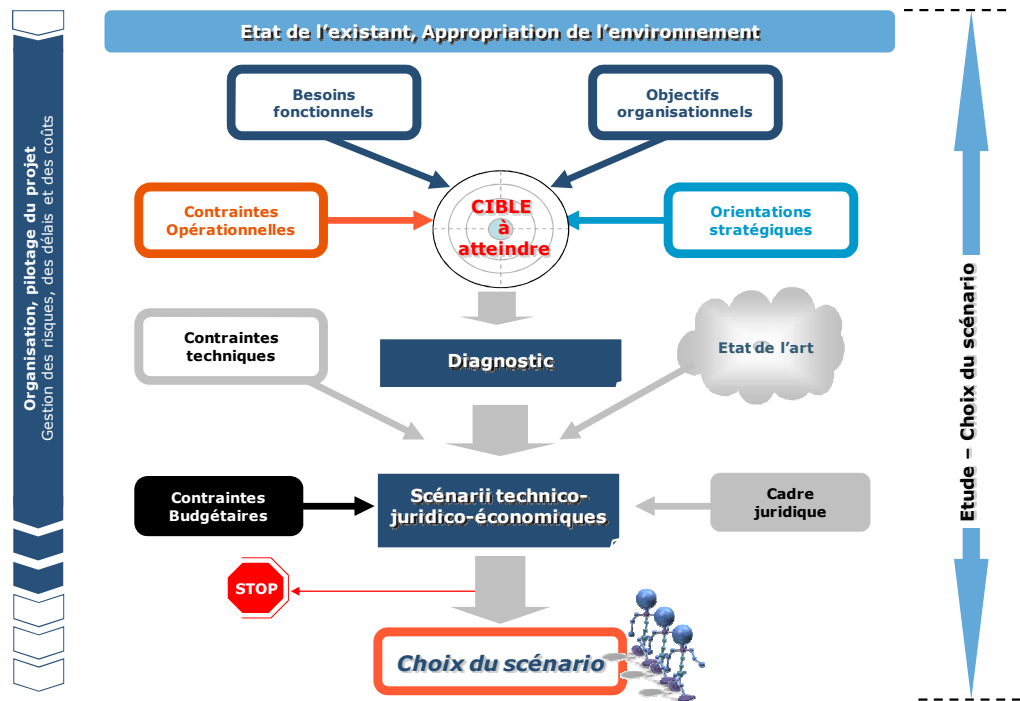
Il est primordial que le cadre d'achats retenu garantisse les investissements initiaux, les extensions sur la durée de vie du système et la maintenance associée.

S'agissant du déploiement, la méthodologie appliquée doit être éprouvée et apte à se porter garante du résultat, à savoir, la maîtrise complète du cadre technique, des délais, des coûts et de la qualité.

Au préalable, les opérateurs et les exploitants techniques du système auront été formés avec pour objectifs une appropriation complète des outils et la performance requise dans leur utilisation.

À l'issue des phases de réception, à partir de la mise en marche opérationnelle du système, une évaluation périodique du système est nécessaire pour mesurer et prendre en compte les éventuels ajustements aptes à améliorer l'efficacité du dispositif et vérifier que l'utilisation du système est assurée dans le respect des règles déontologiques.

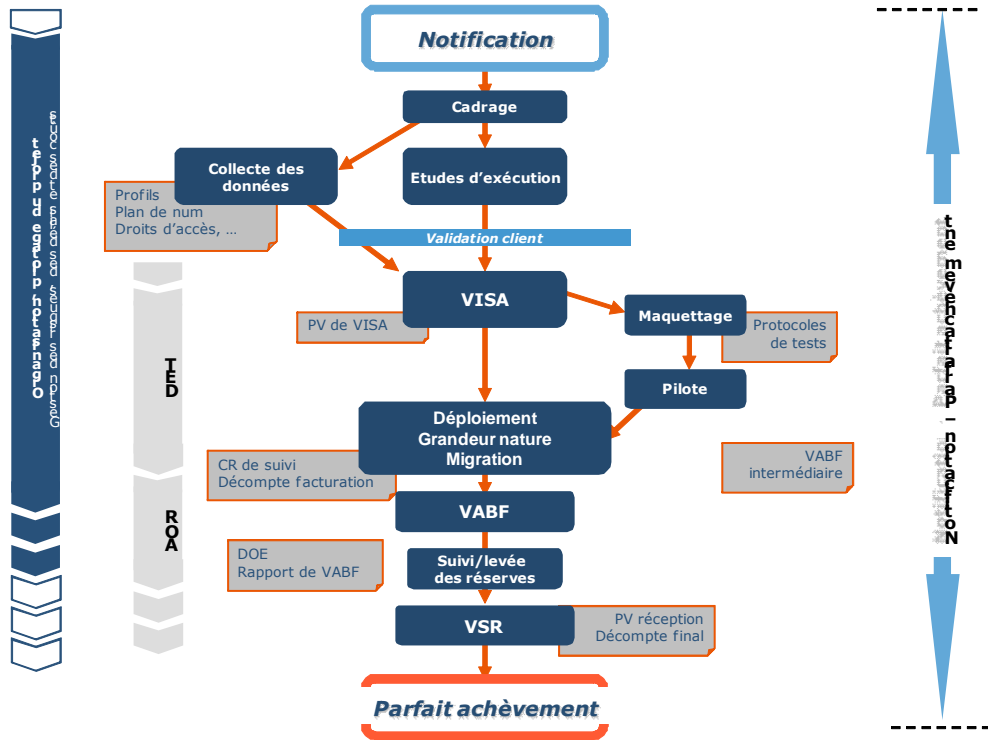
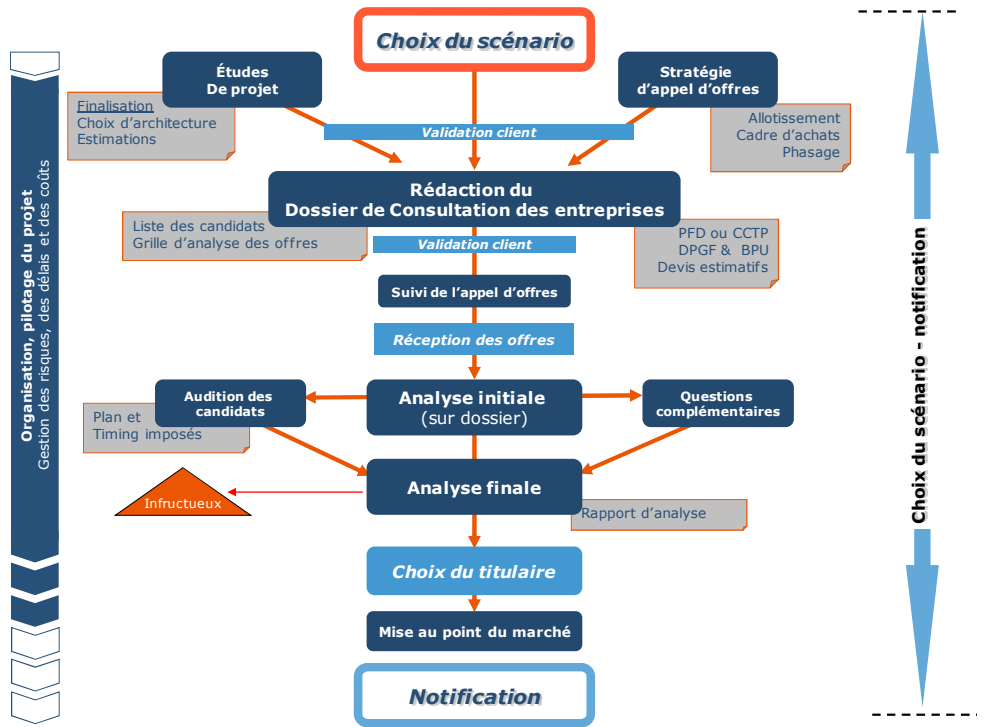
Les différentes étapes à appliquer peuvent être synthétisées par les schémas ci-dessous.

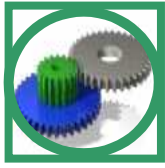


La définition de l'architecture technique du système

UL 7

L'appel d'offres, le déploiement et la validation





9. UL8 : MAINTENANCE ET EVOLUTION TECHNIQUE



La maintenance et l'évolution du système

• UL 8 : Maintenance et évolution technique

La gestion technique d'un système comporte deux aspects :

La surveillance au quotidien du bon fonctionnement du système,

La maintenance préventive et corrective.

9.1. LA SURVEILLANCE QUOTIDIENNE NECESSAIRE AU BON FONCTIONNEMENT DU SYSTEME

Il est important d'effectuer une surveillance quotidienne du système afin de détecter au plus tôt les éventuels dysfonctionnements. En effet, les fonctions interagissent entre elles. Le dysfonctionnement de l'un des équipements entraîne la coupure de la chaîne acquisition-transport-commutation-enregistrement.

Les points névralgiques à vérifier lors de la prise de service de l'opérateur sont les suivants :

Le réseau,

Les enregistreurs,

Les postes de travail,

Les caméras.

L'objectif est de ne pas découvrir que l'installation n'est pas opérationnelle au moment où on en a besoin (Exemple : constater qu'un enregistreur est en panne depuis deux jours au moment de réaliser une relecture avec les services de sécurité.)

9.2. LA MAINTENANCE

Un système qui n'est pas entretenu régulièrement aura une durée de vie limitée et perdra rapidement sa capacité opérationnelle.

L'élément essentiel au bon entretien des équipements est de disposer d'un contrat de maintenance qui couvrira les opérations préventives et correctives. Seules seront exclues de ce contrat les remises en état suite à des dégradations ou des actes de vandalisme qui feront l'objet de commandes spécifiques.

Il est très difficile pour un utilisateur de définir par avance le contenu exact du contrat pour des matériels pour lesquels il n'a aucun retour d'expérience; aussi il est conseillé dans le marché de réalisation de fixer des clauses qui intègrent en plus de la garantie classique les modalités de réalisation de celle-ci pendant une durée suffisamment longue, trois ans conseillés, qui lui assureront le retour suffisant pour préparer son marché de maintenance.

Quelques points importants dans le marché de base au titre de la garantie :

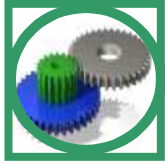
Exiger une garantie totale **sur site** pièces, main d'œuvre et déplacements compris.

La maintenance
et l'évolution du
système

UL 8

Maintenance et
évolution
technique

Les matériels échangés pendant cette période bénéficient d'une extension de garantie minimale de six mois.



Imposer des délais d'intervention et des délais de remise en état de l'installation; attention à bien faire la différence entre ces deux points, l'intervention consiste à faire un diagnostic du dysfonctionnement et la remise en état à corriger le dysfonctionnement.

A titre d'exemple, pour une caméra dôme implantée sur mat, le technicien d'intervention vient constater le dysfonctionnement, vérifie éventuellement les alimentations et câblages, mais n'a pas obligatoirement les outillages nécessaire pour un contrôle du dôme ni une nacelle pour intervenir; le résultat, l'intervention a été faite dans les délais mais le problème de l'installation persiste. Cela nécessitera une nouvelle intervention ultérieure mais quand (si le délai n'est pas imposé)? Que fait-on si c'est l'unité de gestion dont la maintenance est souvent exécutée par le fabricant ? D'où l'importance du délai de remise en état.

Si nous continuons notre exemple, la dépose est effectuée trois jours plus tard, le matériel renvoyé chez le distributeur qui le renvoie chez le fabricant et le dôme est réinstallé dans les trois mois voire plus. Pendant toute cette période, la zone concernée est restée sans surveillance.

Le critère de maintenabilité des équipements doit être pris en compte dès le marché de réalisation de l'installation.

- Les points essentiels d'un contrat de maintenance :

La liste détaillée des matériels concernés.

Un bordereau de prix unitaire de tous les ensembles et sous ensembles constituant l'installation.

Un bordereau de prix de déplacement et de main d'œuvre avec les taux horaires détaillés.

Le nombre de techniciens intervenant pour chaque type de dysfonctionnement.

Le coût global et forfaitaire pour chaque type d'intervention et de remise en état pour chacun des ensembles et sous ensembles de l'installation.

Les limites de prestation en particulier au niveau des interfaces de câblage.

La durée de la garantie des éléments échangés.

Les conditions de déclenchement d'une intervention.

Le délai d'intervention.

Le délai de remise en état.

Les conditions d'accès aux équipements.

La périodicité des visites préventives et le type de travaux qui seront effectués.

La mise à jour gratuite et systématique des logiciels pendant une durée de sept ans.

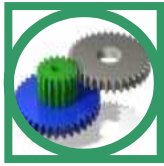
Les rapports à fournir à l'issue de chacune des interventions.

Les pénalités applicables.

Les modalités de règlement des prestations.

Tous les points précédents permettent la rédaction d'un contrat de maintenance clair, évitant tout litige et permettant un choix de prestataire compétent.

Le coût global de la maintenance d'un système de vidéo protection est estimé entre 7 et 10% du montant de l'installation.



9.2.1. LA MAINTENANCE PRÉVENTIVE

Les opérations à réaliser lors de la maintenance préventive touchent différents aspects du système :

Les caméras : qualité de l'image, vérification de l'orientation et de l'azimut et nettoyage complet.

Les moniteurs : réglage, étalonnage des moniteurs et nettoyage des écrans.

Le réseau : vérification de la transmission et de la commutation.

L'enregistrement : vérifier que l'enregistrement et le stockage se fassent correctement.

Les onduleurs : vérification du fonctionnement.

L'IHM : vérification du masquage dynamique et des cycles de préposition.

Ces contrôles pourront être répertoriés dans un registre qui aura la forme suivante :

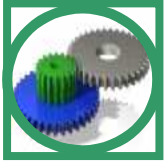
Liste des équipements testés	Observations
Vérification des caméras	
Caméra N°1	
Caméra N°2	
Caméra N°3	
Caméra N°x	
Vérification des écrans	
Ecran N°1	
Ecran N°2	
Ecran N°3	
Ecran N°x	
Vérification des postes de contrôle	
Poste N°1	
Poste N°x	
Vérification des enregistreurs	
Enregistrements (qualité, sélection, exportation)	
Vérification du matériel d'impression	
Fonctionnement des imprimantes	
Vérification du réseau	
Vérification de la transmission	
Vérification onduleur	
<i>Nom de la personne ayant procédé aux contrôles</i>	<i>Date : Signature</i>

9.2.2. LA MAINTENANCE CURATIVE

La maintenance curative s'applique lors d'un dysfonctionnement du système. L'exploitant doit pouvoir agir rapidement pour déclencher une intervention du mainteneur.

Il est important de prévoir, dans le contrat de maintenance :

Un numéro d'appel unique pour joindre le service de maintenance,



La fourniture d'un lot de maintenance permettant de remplacer le matériel défectueux rapidement,

Une garantie de temps d'intervention (GTI),

Une garantie de temps de rétablissement (GTR).

9.2.3. EVOLUTION DU SYSTÈME

EVOLUTION LOGICIELLE

Les équipements et logiciels utilisés sont régulièrement mis à jour par leur constructeur pour améliorer leurs performances ou corriger des défauts.

L'évolution du système doit donc comprendre :

La mise à niveau des logiciels d'exploitation vidéo et système d'exploitation,

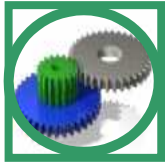
La mise à jour des firmwares de tous les équipements.

MISE A JOUR DES DOCUMENTS

Lors des interventions de maintenance ou de l'évolution du système, certains matériels seront remplacés ou amenés à évoluer, il est par conséquent impératif :

De mettre à jour la documentation du système (DIUO - Dossier d'interventions ultérieures sur les ouvrages),

D'obtenir les documentations techniques correspondant aux nouveaux matériels.



9.3. SYNTHÈSE UL 8 : LES MESSAGES ESSENTIELS

La disponibilité opérationnelle du système dépend de sa gestion technique. Une surveillance et un entretien constant des installations est à prévoir (réglage, nettoyage, ...).

Les opérateurs doivent effectuer une vérification des éléments du système, de manière quotidienne, pour détecter au plus vite, tout dysfonctionnement.

La maintenance de niveau 1 doit être intégrée dans la formation des opérateurs.

Une garantie étendue intégrée au marché de réalisation permet de préparer efficacement son contrat de maintenance.

Le contrat signé avec le mainteneur doit inclure une GTI (Garantie de Temps d'Intervention) et une GTR (Garantie de Temps de Rétablissement).

Il est indispensable de disposer d'un lot de maintenance sur place.

Ne pas oublier de prévoir un budget pour les équipements dégradés qui ne sont pas pris en charge au titre de la garantie ou du contrat de maintenance.



10. GLOSSAIRE

Page

A

Affichage obligatoire

les personnes susceptibles d'être filmées par un système de vidéo protection, que ce soit dans un lieu public ou privé doivent avoir été préalablement informées par un affichage adapté. Dans le cas de lieux publics les panneaux doivent comporter certaines mentions obligatoires

32

Autorisation administrative

Dans le cadre de la vidéo protection il s'agit de l'autorisation accordée par le préfet de déployer un système. Cette autorisation prend la forme d'un arrêté préfectoral, décision administrative susceptible de recours.

8

C

Capteur CCD

le CCD (Charge-Coupled Device, ou dispositif à transfert de charge) est le plus simple à fabriquer, a une bonne sensibilité, mais, du fait de son principe, le transfert de charge, est relativement lent. Mis au point par les Laboratoires Bell en 1969, il a rapidement été adopté pour des applications de pointe (imagerie astronomique) puis popularisé sur les caméras et appareils photo.

57

Capteur CMOS

les capteurs CMOS (Complementary metal oxide semi-conductor) sont apparus dans les années 1980. Ils sont plus complexes à fabriquer que les CCD mais sont produits selon des techniques classiques de micro-électroniques et de ce fait peuvent avoir des dimensions importantes

57

Commission départementale des systèmes de vidéosurveillance

commission administrative instituée dans chaque département. Elle est chargée de rendre un avis sur les demandes d'autorisation des systèmes soumis à la loi de 1995 et d'assurer une mission de contrôle des installations autorisées.

12

Commission nationale informatique et libertés (CNIL)

Autorité de contrôle française en matière de protection des données personnelles instituée par la loi du 6 janvier 1978.

9

Conseils locaux de sécurité et de prévention de la délinquance

Au terme des décret et circulaire du 17 juillet 2002, le Conseil local de sécurité et de prévention de la délinquance constitue la seule instance de pilotage des politiques locales de sécurité. Le CLSPD est présidé par le Maire. Le Préfet et le Procureur de la République en sont membres de droit.

18

D

Délégation de service public

contrats par lesquels une personne morale de droit public confie la gestion d'un service public dont elle a la responsabilité à un délégataire public ou privé dont la rémunération est substantiellement liée au résultat d'exploitation du service.

14

Déontologie

ensemble des règles morales qui régissent l'exercice d'une profession ou les rapports sociaux de ses membres.

31

Diagnostic de sécurité

Démarche engagée au début d'un projet de sécurisation d'un espace, elle vise à recenser, analyser et synthétiser les faiblesses éventuelles. Dans le cas d'un diagnostic réalisé sur le territoire d'une commune on parle de diagnostic local de sécurité.	16
Dispositif local de prévention et de concertation	
il s'agit des instances de concertation organisées localement (département, commune, intercommunalité) pour définir, déployer et suivre les politiques locales de prévention et de sécurité	
conseils locaux de sécurité et de prévention de la délinquance, conseils départementaux.	17
Droit d'accès aux images	
toute personne susceptible d'avoir été filmée dispose d'un droit d'accès aux images la concernant. L'exercice de ce droit est limité (droit des tiers par exemple).	33
DVR	
Les DVR (Digital Video Recorder) sont des équipements destinés à l'enregistrement numérique des flux vidéos et le stockage des données.	89
Les NVR (Network Video Recorder) sont des équipements dont le rôle est d'enregistrer les images provenant du réseau (IP) et d'en assurer le stockage	67
E	
Enregistrement	
stockage de données sur un support permettant leur conservation.	9
Etablissement public de coopération intercommunale	
structure administrative française régie par les dispositions de la cinquième partie du Code général des collectivités territoriales, regroupant des communes ayant choisi de développer un certain nombre d'aspects en commun, comme par exemple les transports en commun	47
Ethique	
science qui traite des principes régulateurs de l'action et de la conduite morale	31
Etudes de sûreté et de sécurité publique (ESSP)	
depuis le 1er octobre 2007 et l'entrée en vigueur du nouveau régime des permis de construire, les opérations urbaines de grande envergure doivent faire l'objet d'une étude de sûreté et de sécurité publique (ESSP), qui impose au maître d'ouvrage de prendre en compte la malveillance et le sentiment d'insécurité dans son projet	17
F	
Firmwares	
Un micrologiciel, également désigné sous l'anglicisme firmware, ou parfois logiciel interne, embarqué ou d'exploitation, est un logiciel (software en anglais) qui est intégré dans un composant matériel (hardware en anglais).	89
G	
GTI	
Garantie de temps d'intervention.	89
GTR	
Garantie de temps de rétablissement.	89
I	
Interface Homme-Machine	
Logiciel permettant le pilotage du système vidéo.	55
IP	
Internet Protocol	

protocole de communication de niveau 3 utilisé pour l'Internet.	57
L	
Lieux et établissements ouverts au public	
lieux accessibles à tous sans autorisation préalable de quiconque, que l'accès en soit permanent ou inconditionnel ou subordonné à certaines conditions, heures ou causes déterminées.	11
LAN	
Local Area Network, en français réseau local, désignant un réseau informatique d'échelle géographique restreint.	57
M	
MAN	
Les MAN (Metropolitan Area Network, réseaux métropolitains) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Ainsi, un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.	57
MPLS	
MultiProtocol Label Switching - est un mécanisme de transport de données, opérant sur la couche de liaison de données du modèle OSI.	57
O	
Obligation d'information préalable	
Obligation d'information par une signalétique adaptée de l'existence d'un dispositif de vidéo protection. Les modalités de cette information varie selon la nature du lieu.	10
P	
Parties privatives	
les parties privatives sont les zones privées qui n'ont pas vocation à être filmées par un système soumis à la loi de 1995. Il s'agit des fenêtres, entrées d'immeubles, parkings, jardins... Il appartient au responsable du système de prévoir les mesures nécessaires pour éviter que ces zones puissent être filmées.	33
prévention situationnelle	
Théorie criminologique visant à décourager le délinquant en rendant le passage à l'acte plus risqué, moins profitable, moins tentant... Cela se traduisant par une analyse des comportements et le déploiement de moyens humains et techniques adaptés.	20
Prévention situationnelle	
Théorie criminologique visant à décourager le délinquant en rendant le passage à l'acte plus risqué, moins profitable, moins tentant... Cela se traduisant par une analyse des comportements et le déploiement de moyens humains et techniques adaptés.	5
R	
Référent sûreté	
expert en sûreté mis en place dans chaque département, auprès de la direction départementale de la sécurité publique ou du groupement de gendarmerie départementale. Le référent intervient dans le cadre des ESSP et des projets touchant à la sécurité.	17
S	
SDK	
T	
titulaire	
Entreprise titulaire du marché chargé de réaliser les prestations.	75
V	
Vidéosurveillance intelligente (VSI)	

Définition proposée par l'AN2V

Voie publique

la voie publique est le périmètre d'exercice des pouvoirs de police municipal du maire en application du 1° de l'article L.2212-2 du Code Général de Collectivités Territoriales. Elle comprend l'ensemble des voiries du domaine public routier tel que défini par le code de la voirie routière et délimité conformément aux articles L.112-1 et L.112-2 du même code.

11

W

WAN

Wide area network (réseau étendu).

57

watermarked

Signifie tatouage numérique. Il s'agit d'une technique permettant d'ajouter des informations de copyright ou d'autres messages à un fichier ou signal audio, vidéo, une image ou un autre document numérique.

39

11. POUR ALLER PLUS LOIN

Un certain nombre de documents sont accessibles sur internet. La liste proposée ne se veut pas exhaustive.

Article rédigé par Eric Heilmann dans la revue *Criminologie*, vol.36, n°1, 2003, p. 89-102. <http://id.erudit.org/iderudit/006554ar>