République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme master profissionnel en Informatique

Option

Administration & sécurité des réseaux

Thème

Instalation d'un systeme de vidéosurveillance sur IP

Pésenté par :

Mr BEZHOUH Saadi.

Devant le jury composé de :

Président : **MrAloui Abdelouhab.**
Encadreur : **Mr HAMOUMA Moumen.**
Examinatrice : **Mr SAADI Mustapha.**

Année universitaire 2014.

Remerciements

Je remerci, avant tout, Dieu le tout puissant qui m'a donné la force, la volonté et la patience qui m'a permet d'accomplir ce modeste travail.

Je remerci chaleureusement Mr Hamouma d'avoir encadré ce travail, avec beaucoup de compétences. Merci pour votre optimisme, et la confiance que vous m'avez accordée au cours de cette année.

Merci a mes parents pour qui me portons les plus nobles sentiments et les plus profondes estimes.

Aussi aux membres de jury qui ont bien voulu m'honorer, assister à ma soutenance et évaluer mon travail.

Mes remerciements vont bien entendu a mes proches qui m'ont soutenu et encouragé.

Je tiens à remercier toutes les personnes qui m'ont aidées de près ou de loin.

Saadi.

Dédicaces

Je dédie ce modeste travail à la femme la plus adorable au monde, à la femme que j'aime 'ma chère Maman' à qui grâce à elle je suis ce que je suis aujourd'hui.

A l'homme que j'aime, mon chère pére qui ma aidé et encouragé.

A mes fréres et soeurs, et plus particulièrement mon frére Idris, qui ma aidé et soutenu durant tout l'année.

Saadi.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

CCTV Closed circuit television .
DVR Digital Video Recorder.
NVR Network Video Recorder.
IP Internet Protocol.
FTP file transfer protocol.
SMTP Simple mail transport protocol.
HTTP Hyper Text transfer Protocol.
IRA Irish Republican Army.
PC Personal computer.
Rj45 Registred Jack 45.
RTP Real time protocol.
HTTPS Hypertex Transfer protocol Secure .
TCP Transport control protocol.
RTCP Real time control protocol.
RTSP Real time Streaming protocol.
VPN virtual personal network.
SSL Secure Sockets Layer.
TLS Transport Layer Security.
WEP Wireless Equivalent Prevent .
ISO International Standard Organisation.
WPA wifi Protected Access.
PDA Personal Digital Assistan.
GSM Global System for mobile Communication .
GPRS General Packet Radio Service .
MJPEG Motion joint Photograph Expert Group .
JPEG joint Photograph Expert Group.
LAN Local area netxork.
WLAN Wireless local area network .
WAN Wide area network .
CPL courans porteur en ligne .
AES Advanced encryption Standard .
DAS Direct Attached Storage .
NAS Network Attached Storage.
MPEG Moving Pictures Expert Group .
IEC International Electrotechnical Commission .

Introduction générale

De nos jours, le monde est de plus en plus complexe dans ses infrastructures et ses interactions, ce qui a pour effet d'augmenter le nombre d'événements tragiques de natureaccidentelle ou intentionnelle.

En contrepartie, les sociétés sont aussi plus exigeantes en termes de sécurité et de prévention et exploitent les avancées technologiques afin de répondre à ces besoins de la meilleure façon possible.

C'est ainsi que l'on assiste de nos jours à la prolifération des systèmes de vidéosurveillance conçus et installés dans des lieux résidentiels, publics ou de travail (banques, centres commerciaux, usines, aéroports, écoles, gares routières...). Ces systèmes sont pour la plupart utilisés dans le but d'assister les gardiens de sécurité dans leur travail.

Dans leur forme de base, ces systèmes analogiques ou numériques ont des fonctions qui se limitent à la capture, la transmission, le stockage et l'affichage de données visuelles au niveau des postes de surveillance. Ainsi les opérateurs humains peuvent effectuer des surveillances tout en minimisant leurs déplacements.

Le but de notre travail consiste à étudier et mise en place d'un système de vidéosurveillance IP au sein de la boite informatique CTIB, ce projet comporte trois chapitres comme suite :

Le premier chapitre intitulé "Introduction à la vidéosurveillance" s'appuis sur les aspects de base de la vidéosurveillance. Dans le deuxième chapitre nous décrivons "La vidéosurveillance sur IP" et sa gestion. "L'étude et réalisation" fait objet de troisième chapitre, dont le quel nous avons étudier et réaliser un système de videosurveillance sur IP, ainsi nous avons illustré l'équipement utilisé et quelques interfaces de configuration de ce dernier.

1

Introduction à la vidéosurveillacne

1.1 Introduction

Le sentiment de l'insécurité issu de la hausse des actes de vandalisme, criminalité et bien d'autre activités malveillante ; les particuliers et les pouvoirs publiques optent pour les systèmes de vidéosurveillance non seulement pour leurseefficacité et leurs multiples avantages, mais aussi pour leur simplicité de mise en œuvre et de maintenance.

C'est ce que nous allons aborder dans ce premier chapitre ainsi quelques généralités sur les systèmes de vidéosurveillance et leurs fonctionnement, comme nous allons énumérer les différents types de ces systèmes et leurs multiples avantages et performances.

1.2 Présentation

La vidéosurveillance, parfois désignée par le sigle anglais CCTV pour "Closed Circuit Television" consiste à placer des caméras de surveillance dans un lieu public ou privé pour le surveiller. Les images obtenues avec ce système peuvent êtretraitées automatiquement et/ou visualiser puis archiver ou détruites en un endroit centralisé.

La vidéosurveillance a souvent un rôle dissuasif mais aussi préventif puisque elle permet de surveiller les allées et venues des personnes dans les lieux publiques, prévenir les vols, agressions, fraudes et gérer les incidents et mouvements de foule, et grâce à l'enregistrement des images captées, elle permet d'identifier plus facilement les agresseurs ou voleurs après un délit. Ces images sont des éléments primordiaux dans le cadre d'une enquête judiciaire.[1]

1.3 Son apparition

Les premières caméras de vidéosurveillance ont été implantées dans les années 1950 en-Grande Bretagne, à une échelle très réduite et expérimentale.Dans les années 1970, lessystèmes apparaissent dans les banques et commerces deluxe pour lutter contre les attaques ;et sur les réseaux routiers pour assister la régulation du trafic.L'utilisation de l'outil segénéralise dans les années 1980, de la lutte contre lesattaques à mains armées et autresbraquages, à la protection des personnes et desbiens ; de banques et établissements de luxe,aux commerces, aux transports et auxbâtiments publics. La technique vidéo progresse, ellepermet d'envisager la miniaturisationet l'extension des systèmes, l'accroissement descapacités de transmission et de stockage,la recherche d'une meilleure définition de l'image.Ces progrès technologiques, la relative efficacité de l'outil en milieu clos dans la luttecontreles divers délinquances, le contexte politique et social dans lequel s'impose le thèmede l'insécurité en référence à la sécurité entendue comme sûreté des personnes etdes biens,et l'émergence des menaces terroristesentraînent, dans les années 1990,son extension àl'espace public et aux rues de certaines villes.
C'est également dans cesannées là que l'on voitapparaître les premiers textes législatifs encadrant et légitimant la vidéosurveillance. Notredécennie a consacré la vidéosurveillance comme partie intégrante du quotidienurbain, allantjusqu'à l'inclure spontanément au mobilier urbain.L'exemple exubérant de la capitalebritannique est fréquemment cité. On estime

qu'unLondonien est filmé en moyenne trois centfois par jour.

L'insécurité, qui est désormais considérée comme un état de fait, repris, déformé etamplifié par les pouvoirs politiques et médiatiques, et la nouvelle forme de menaceterroristeintroduite par les attentats du 11 septembre 2001, ont donné une forte impulsionàla vidéosurveillance, L'outil se positionne au sein d'un ensemble de procédésavec lesquels il s'articule, croise des données. L'ère numérique et les progrès de l'optiquerendent les systèmes plus performants, ouvrant ainsi d'autres possibilités d'exploitation.Les quatre phases historiques de ce développement peuvent être regardées àla lumière des quatre étapes du processus de généralisation de la vidéosurveillance.[2]

1.4 Fonctions et objectifs

1.4.1 Les fonctions

la vidéosurveillance a deux fonctions principales :

- **La dissuasion** :généralement les cameras de surveillance sont visibles de tous (vision nocturne, vision 360°,...), c'est une manière efficace de dissuader les personnes avec des intentions malveillantes pour reculer de leurs actions et éviter toutes sortes d'intrusion, agressions, etc.

- **La surveillance** : elle englobe la fonction de dissuasion, dans ces systèmes les cameras peuvent être apparentes ou discret pour ne pas faire fuir les clients par exemple, le résultat recherché dans les deux cas est le même c'est-à-dire surveiller une zone où le risque et la menace sont présents.

1.4.2 Les objectifs

selon la nature du cite à surveiller et les besoins d'installation d'un système de videosurveillance on peut avoir plusieurs objectifs que nous citons ci-dessous :

- Mettre sous surveillance électronique une zone sensible d'un établissement (les entries, parkings, cours, salles d'attente, ...).
- Protection de propriétés privées.
- Visualiser à distance les zones concernées dés qu'une présence est détectée.
- Déclenchement d'enregistrement automatiquement par les différents capteursinstallés (détecteur de mouvement, présence, etc.).
- Visualiser une scène particulière sur une camera.
- Déclenchement d'activités extérieurs comme l'envoie d'emails, sereine, gyrophare, ouverture ou fermeture d'une porte et bien d'autre précautions.

1.5 Domaines d'applications

Ces dernières années, les systèmes de vidéosurveillance ont connu un développement considérable notamment grâce à l'utilisation de réseau internet pour la surveillance à distance. De nous jours la vidéosurveillance est intégrée dans plusieurs domaines que nous citons ci-dessous :

1.5.1 Domaine privé :

: la télésurveillance offre la possibilité aux particuliers de rester en contact visuel avec leurs domiciles et leurs biens, soit sur place ou à distance, c'est un moyen efficace de bien protéger leurs familles et les personnes présentes dans leurs foyers comme avoir un œil sur les enfants et éviter plusieurs incidents qui peuvent s'engendrer intentionnellement ou accidentellement.

1.5.2 Domaine public :

[2] plusieurs milieux publics s'équipent de système de vidéosurveillance afin d'améliorer leurs conditions et la sécurité des usagés, on y trouve :

1. **Sur routes et autoroutes :**
   - Gestion de trafic par la surveillance des zones dangereuse, etc.
   - Etude de comportement des automobilistes pour modifications éventuelles des voies de circulation et d'équipement (accidentologie).
2. **Dans les transports :**
   - Assurer la sécurité des passagers dans, les bus, les trains et les aéroports par la supervision de ces derniers.
   - Surveillance des bagages et les parkings.
   - Récemment ces systèmes sont équipés de reconnaissance faciale qui s'avère utile pour la lutte contre le terrorisme.
3. **Amélioration des interventions :** avec une vision sur les lieux des incidents les groupes d'intervention come les agents de police et protection civile peuvent améliorer leurs stratégies et d'y mettre les moyens nécessaires pour une intervention efficace.

1.5.3 Domaine industriel

Sur unechaîne de production on peut, par exemple, largementoptimiser les contrôles par l'utilisation d'unœil virtuel sur les points critiques de la chaîned'assemblage et favoriser la mobilité et doncl'efficacité du personnel chargé de surveiller laqualité de la production. Là où l'arrêt ou la misehors fonction d'une machine-outil provoquedes coûts d'exploitation (ou plutôt de non exploitation)importants, la vidéosurveillance peutoffrir une aide visuelle précieuse permettant de prévenir oude localiser et de résoudrerapidement des problèmes, voir même d'anticiper leur réapparitionultérieure.

1.5.4 Domaine commercial :

La vidéosurveillance y trouve à nouveau sa place et permet deréaliser des économies en étantcapable de centraliser la surveillance des points de ventes. Lesystème fournit de précieu-

sesinformations sur le niveau de fréquentationsjournalières, lesheures d'activité et permet de prévenirles risques d'agression pour la sécurité des employés etdes clients. Les responsables des magasins espèrent augmenter le niveaudes servicesofferts à la clientèle et garantir la rentabilité des points de vente en gérant aumieux le personnelen fonction du niveau de fréquentation aux différentes heures.

1.6 Concept de la vidéosurveillance

1.6.1 Schéma de principe :

Une installation de videosurveillance comporte toujours trois fonctions interdépendantes soit la prise de vue, la gestion et la visualisation comme le montre la figure figure-1.

FIGURE 1.1 – Le schema de principe de la vidéosurveillance.

1.6.2 La prise de vue :

permet l'acquisition des images à l'aide de cameras qui sont l'élément fondamental du système de videosurveillance, elles peuvent être fixes ou motorisées, voyantes ou dissimulés et avec ou sans caisson de protection ou dôme. En fonction de l'environnement à surveiller et les besoins de l'utilisateur il conviendra de choisir dans une gamme pléthorique le matériel adéquat. Nous présentons ci-dessous les deux types de cameras : les cameras analogiques et les cameras réseaux :

– Cameras analogiques : les images sont transmises par un signal analogique via un câble coaxial, même avec l'arrivé des cameras réseaux, les cameras analogique représentent 96

FIGURE 1.2 – Camera analogique.

– Cameras réseaux : A ne pas confondre avec une Webcam, une caméra réseau est une caméra qui se connecte directement au réseauet non pas à un PC. La caméra réseau réunit les fonctions optiques d'une caméra et la capacité d'un petit ordinateur équipé d'un serveur web interne. Une caméra réseau possède donc une prise RJ45 pour connexion directe sur un hub ou Switch. Elle diffuse ses images à tout poste qui en fait la demande

via un navigateur sur le réseau IP.

FIGURE 1.3 – Camera réseau.

1.6.3 La gestion :

cette fonction permet le dispatching des signaux envoyés par les caméras à la fonction de visualisation et les enregistrer en cas de besoin, elle permet aussi d'effectuer des traitements sur les images (luminosité, contraste, transcodage...), aussi ajouter d'autres entrés de donnée comme toutes sortes de détecteurs (mouvement, présence, thermique...), comme on peut ajouter des actions en sortie (déclenchement d'enregistrement, fermeture/ouverture de portes, déclenchement des sereines/gyrophare...). Les équipements de gestion sont multiples selon le système de vidéosurveillance à installer, on trouve :

- Quad/multiplexeur.
- Matrice.
- Magnétoscope traditionnel.
- Enregistreur numérique (DVR).
- Enregistreur numérique réseau (NVR).
- Serveur de caméra (encodeur vidéo).

1.6.4 La visualisation :

cette fonction est souvent agrégée au post de garde, un ou plusieurs moniteurs permettent la visualisation des images de vidéosurveillance, les moniteurs se diffèrent par leur taille d'écrans, le type d'entrée (analogique, numérique), le type de sortie (couleur, noire et blanc, simple affichage, plusieurs camera sur un même écran), etc.

1.7 Les types des systèmes de vidéosurveillance

[3]

1.7.1 Système classique :

Le réseau est basé sur un système analogique, avec dans la plupart des cas unenregistrement limité dans la durée. Il s'agit là d'une des méthodes les plus anciennes doncégalement des plus répandues dans un grand nombre d'établissement. Cependant, cessystèmes nerépondent plus, à de très rares exceptions près, aux nouvelles exigencestechniques de la vidéosurveillance.

1.7.2 Système numérique sur IP :

Ce système relie un réseau de caméras IP, qui peut compter denombreuses unités, à unsystème d'enregistrement numérique. D'une part, cela permet de pouvoir stocker une quantitéimportante d'images, sans perte de qualité, tout en pouvant les consulter rapidement grâce à deslogiciels de traitement. D'autre part, le fait d'informatiser un système de surveillance permet deprofiter des technologies de communication comme Internet. Ainsi, les caméras sont visibles et gérables depuis n'importe où dans le monde. L'évolution des téléphones mobiles a créé la"vidéosurveillance mobile" avec l'accès aux vidéos via Internet mobile sur PDA ou via GSM/GPRS sur téléphone GSM doté de Java. Cette technologie permet également d'économiser et demutualiser les câbles réseaux qui sont généralement disponibles dans les bâtiments récents.

1.7.3 Système hybride :

Les systèmes hybrides intègrent les systèmes classiques de vidéosurveillance basés sur lescaméras analogiques et les caméras en réseau. Il permet d'intégrer aisément les deux types desystèmes en place sur un seul serveur ou de faciliter l'évolution d'un système de vidéosurveillanceanalogique vers le numérique, sans remettre en cause l'existant, et introduire de nouvellesfonctions comme la détection de disparition / apparition d'objet et le comptage d'objets ou depersonnes.

1.8 L'évolution des systèmes de vidéosurveillance :

[4] Depuis l'apparition des systèmes de vidéosurveillance dans les années 1950, ils n'ont pas cessé de s'évoluer. Entièrement analogiques à leur début, ils ont évolué progressivement vers la technologienumérique. Les systèmes actuels ne ressemblentguère aux anciennes caméraanalogiques branchées sur des magnétoscopes traditionnels. Aujourd'hui, ils utilisentles caméras réseaux et les serveurs informatiques pour l'enregistrement vidéo dans unsystème entièrement numérique. Entre les systèmes entièrement analogiques et lessystèmes entièrement numériques, il existe encore néanmoins toute une série desolutions partiellement numériques incluant une quantité variable de composantsnumériques et analogiques.

1.8.1 Système de vidéosurveillance classique :

appelé aussi CCTV en anglais pour Closed Circuit Television, ou en français circuit fermé de télévision, est un système utilisant des cameras analogiques reliées directement aux moniteurs. Un operateur doit être toujours présent devant les moniteurs pour le contrôle et l'intervention dans les situations anormales.

Les aventage

- Installation très simple et non professionnelle.
- Manipulation des données assez simple et disponible à n'importe quelle personne.

Les inconvénients :

- Fonctionnement très limité.

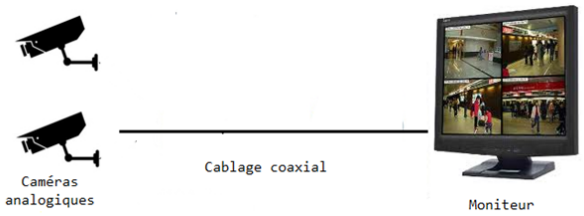

FIGURE 1.4 – Systeme de vidéosurveillance classique.

– Il faut réserver un operateur pour le contrôle.
– Pas d'enregistrement ni de déclenchement de surveillance.

1.8.2 Système de vidéosurveillance analogique avec magnétoscope traditionnel :

Un système de vidéosurveillance analogique utilisant un magnétoscopetraditionnel (VCR) est un système entièrement analogique dans lequel les camérasanalogiques avec sorties coaxiales sont reliées au magnétoscope pourl'enregistrement. Les bandes utilisées sont identiques à celles utilisées par lesparticuliers. Les séquences vidéo ne sont pas compressées, dans le cas d'unenregistrement à vitesse maximale, une cassette a une durée maximale de 8 heures.Dans les systèmes de plus grande envergure, un quadravision ou multiplexeur peutêtre connecté entre la caméra et le magnétoscope. Le quad/multiplexeur permetalors d'enregistrer le contenu de plusieurs caméras sur un même magnétoscope, maisselon une fréquence d'image cependant inférieure. La surveillance vidéo nécessite unmoniteur analogique.

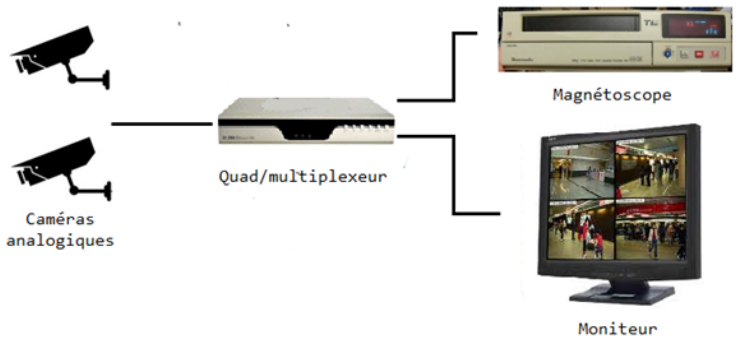

FIGURE 1.5 – Systeme de videosurveillance classique avec magnitoscope traditionnel.

Multiplexeur : c'est un appareil ajouté au système classique de vidéosurveillance pour permettre l'enregistrement de plusieurs flux de cameras analogiques sur une même bande magnétique, et il assure aussi les deux fonctions suivantes :

– Fournir aux moniteurs des images multiples selon le type (4,8 ou 16).
– Envoyer des images encodées au magnétoscope.

Quad : il permet l'affichage de quatre images en même temps ou à tour de rôles, comme il permet une priorité à une camera, il existe des modèles avec option alarme.

FIGURE 1.6 – Multiplixeur.

FIGURE 1.7 – Quadravision.

Matrice : le sélecteur matriciel est un commutateur programmable qui résout les problèmes de distribution d'affichage sur plusieurs postes de travail et moniteurs.Les systèmes matriciels offrentune diversification plus étendue tant qu'à la distribution des images incluant une hiérarchie dans le contrôle.

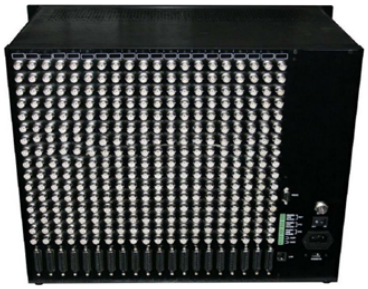

FIGURE 1.8 – Matrice.

les aventage

- Pas besoin d'avoir un operateur présent tout le temps devant les moniteurs.
- Possibilité de déclencher l'enregistrement juste en cas de besoin pour optimiser l'espace de stockage des vidéos.

Les inconvénients :

- Capacité des bondes d'enregistrement faible donc changement de casette permanant.

1.8.3 Système de vidéosurveillance analogique avec enregistreur numérique :

est un système utilisant un DVR qui permet l'enregistrement numérique des données, dans ce type de systèmes, l'enregistrement vidéo ne se fait plus surbandes magnétiques mais sur des disques durs où les séquences sont numérisées etcompressées de manière à emmagasiner chaque jour un maximum d'images. Toutefois lespremiers enregistreurs numériques disposaient d'un espace disque limité, la duréedes enregistrements était donc assez restreinte, à moins de réduire la fréquenced'images. Grâce aux progrès récents dans ce domaine, l'espace disque ne pose plusréellement problème. La plupart des enregistreurs numériques disposent en outre de plusieurs entrées vidéo, ce qui leur permet d'intégrer les fonctionnalités du quad ou des multiplexeurs.

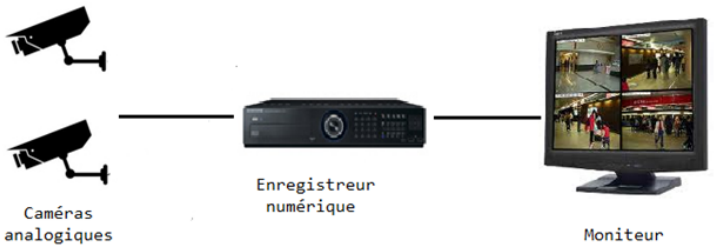

FIGURE 1.9 – SVS classique avec enregistreur numerique.

L'enregistreur numérique :est un équipement d'enregistrement qui reçoit en entrée un ou plusieurs signaux analogiques selon le model. L'enregistreur numérique converti ces signaux en signaux numériques, qui compresse sous différents formats, les plus utilisés on y trouve JPEG pour les images et MJPEG, H264, MPEG-1 et MPEG-2 pour les vidéos. Parmi ces fonctions, il classe les images de chaque camera dans un dossier dont chaque fichier représente une journée ou une plage d'horaires selon la configuration.

FIGURE 1.10 – Enregistreur numerique.

Aventage

- Pas besoin de changer à chaque fois de cassettes.
- Qualité d'image améliorée et constante.
- Paramétrage des plages horaires d'enregistrement et déclenchement sur alarme.

1.8.4 Système de vidéosurveillance avec enregistreur numérique réseau :

système de vidéosurveillance analogique passant par un enregistreurnumérique réseau (NVR) est un système en partie numérique comprenant unenregistreur numérique réseau connecté via un port Ethernet. La vidéo étantnumérisée et compressée sur l'enregistreur numérique, les images peuvent êtretransportées sur un réseau informatique à des fins de surveillance sur PC distants.Certains systèmes permettent à la fois la visualisation des séquences en direct et desséquences enregistrées, d'autres se limitent aux images enregistrées. Sur certainssystèmes, la surveillance vidéo requiert en outre un client Windows spécifique,tandis que d'autres nécessitent un simple navigateur web standard, plus flexiblepour une visualisation à distance.

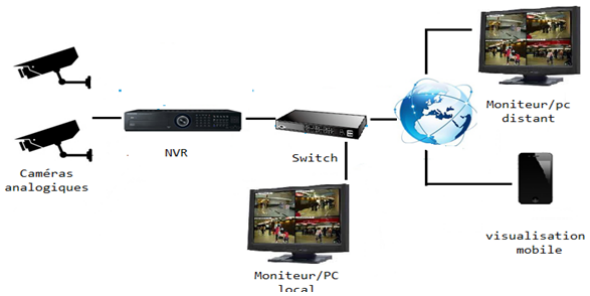

FIGURE 1.11 – SVS avec enregistreur numérique réseau.

L'enregistreur numérique réseau : c'est un enregistreur numérique doté d'une sortie Ethernet généralement une fiche RJ-45 relié au réseau local existant sur les lieux, on entend par la, ce système nécessite pas un nouveau câblage, il intègre directement les anciennes installations du réseau IP. La visualisation dans ce système se fait sur n'importe quel ordinateur de même réseau local, ou sur n'importe quel ordinateur connecté sur Internet ou que ce soit dans le monde.

FIGURE 1.12 – Enregistreur numérique réseau.

Les aventages

- Visualisation videos sur PC à distance.
- Contrôle de système à distance.

1.8.5 Système de vidéosurveillance IP avec serveur vidéo :

Un système de vidéo sur IP associé à un serveur vidéo comprend un serveurvidéo, un commutateur réseau et un PC équipé d'outils de gestion vidéo. La caméraanalogique est branchée sur le serveur vidéo, lequel assure la numérisation et lacompression des séquences vidéo. De son côté, le serveur vidéo est connecté sur leréseau qui transporte la vidéo vers un PC ou serveur d'enregistrement via un commutateur réseau. Lavidéo est alors enregistrée sur le disque dur.Il s'agit alors d'un véritablesystème de vidéo sur IP.

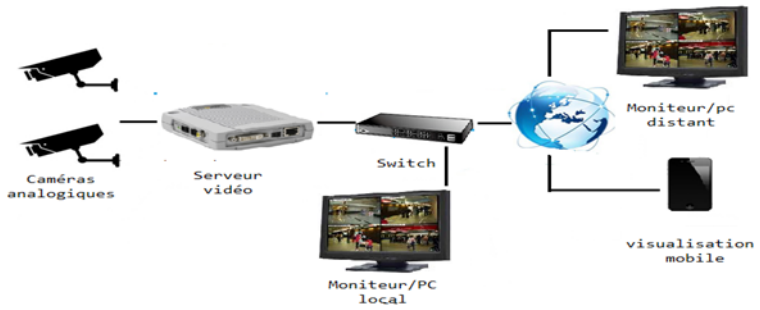

FIGURE 1.13 – SVS IP avec un serveur vidéo.

Serveur vidéo : Le serveur vidéo s'intègre facilement dans un système existant devidéosurveillance analogique CCTV (télévision en circuit fermé) et permet de migrer vers un système sur IP. Un serveur vidéonumérise les signaux vidéo analogiques et distribue des images numériquesdirectement sur un réseau IP (par exemple, un réseau local LAN/intranet/Internet),en transformant les caméras analogiques en caméras réseau et en permettant auxutilisateurs de visualiser des images en direct à partir d'un navigateur web depuistout ordinateur du réseau, en tout lieu et à tout moment.

FIGURE 1.14 – Serveur vidéo.

Les aventages

– Recours à un réseau standard et serveur informatique standard pour l'enregistrement et le traitement vidéo.

– Faible coût totale de possession grâce à l'utilisation de l'infrastructure réseau et équipements existants et évolution future garante.
– Accès distant aux imagesen direct, à tout moment, en tout lieu, à partir de tout ordinateur agréé et autorisé muni d'un navigateur web.
– Facilité de stockage des vidéos sur des supports informatiques avec possibilité d'enregistrement hors site.
– Large gamme de logiciels d'applications généralement propriétaires mais on y trouve pas mal de logiciels gratuits et fiables.

Décodeur vidéo : Dans certains cas, il est nécessaire de pouvoir surveiller les flux vidéo et audio IPsur un équipement analogique existant. Un décodeur vidéo IP permet dans ce cas detransformer les flux vidéo et audio du réseau en signaux analogiques qui serontinterprétés par les écrans de télévision classiques, les moniteurs analogiques et lescommutateurs vidéo. Un encodeur/décodeur est un moyen très économique detransmettre de la vidéo analogique sur de grandes distances (analogique -numérique- analogique)

FIGURE 1.15 – Décodeur vidéo.

Grâce au décodeur vidéo, les moniteurs analogiques peuvent recevoir desinformations vidéo et audio distantes en provenance de caméras ou de systèmes analogiquescomme s'ils étaient installés en local auprès de l'opérateur, alors qu'en réalité ils setrouvent par exemple dans une autre ville.

1.8.6 Système de vidéosurveillance IP avec caméras réseaux :

Une caméra réseau associe une caméra et un ordinateur intégré. Permettant lanumérisation et la compression vidéo, elle est en outre équipée d'un connecteurréseau. La vidéo est acheminée par réseau IP via les commutateurs réseau, pour être enregistrée sur un PC ou serveur standards à l'aide d'outils de gestion vidéo. Il s'agitd'un système de vidéo sur IP à part entière, doublé d'un système entièrementnumérique n'utilisant aucun composant analogique.

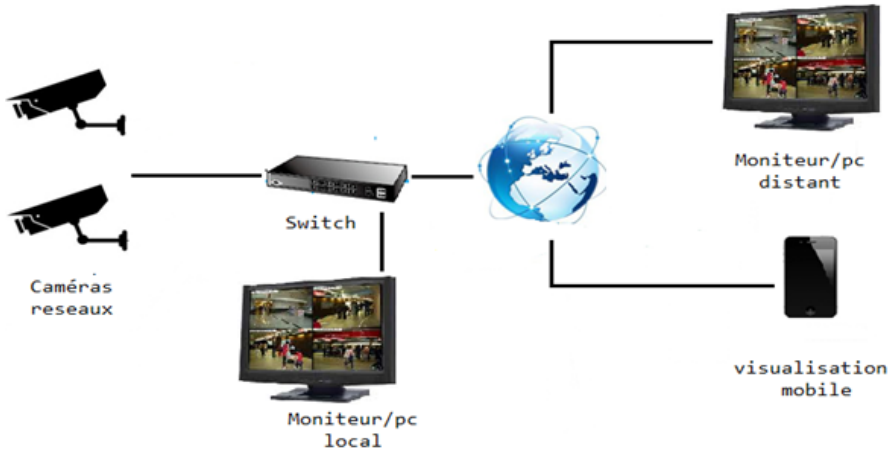

FIGURE 1.16 – SVS IP avec caméra résea.

Les aventages Les systèmes de vidéo sur IP reposant sur l'utilisation de caméras réseau présententles avantages suivants :

- Caméras haute résolution (méga pixels).
- Qualité constante de l'image.
- Fonction d'alimentation par câble Ethernet (Power over Ethernet) et réseausans fil.
- Fonctions panoramique/inclinaison/zoom, audio, entrées et sortiesnumériques sur IP.
- Grandes flexibilité et évolutivité.

1.8.7 Système de vidéosurveillanceIP sans fils :

Même si les réseaux filaires prévalent actuellement dans la plupart des bâtiments, une solution sans fil peut s'avérer intéressante pour l'utilisateur, tant financièrementque sur le plan fonctionnel.Songeons par exemple à certains bâtiments classés, où l'installation d'un câblageendommagerait inévitablement l'intérieur, ou à certains sites (commerces parexemple) pour lesquels la caméra doit être régulièrement déplacée et où l'on nesouhaite pas devoir tirer chaque fois de nouveaux câbles.Une autre utilisation courante de la technologie sans fil concerne les bâtiments ou lessites que l'on souhaite relier sans pour autant devoir entreprendre de lourds etcoûteux travaux au sol.

La technologie sans fil s'applique à la fois aux systèmes de vidéo sur IP et auxsystèmes analogiques.Elle dépasse donc le périmètre strict des réseaux. La transmission sans fil se divise endeux catégories principales :

- LAN sans fil (Wireless LAN, ou WLAN) :qui définit un réseau local, c'est-à-dire sur de courtes distances et en principe àl'intérieur.Les normes LAN sont aujourd'hui bien définies et les périphériques de marquesdifférentes sont généralement compatibles entre eux.
- Ponts sans fil :Lorsque certains bâtiments ou sites doivent être reliés par une liaison rapide, uneliaison point à point longue distance et à grande vitesse est nécessaire. Lestechnologies micro-ondes et laser sont couramment utilisées.

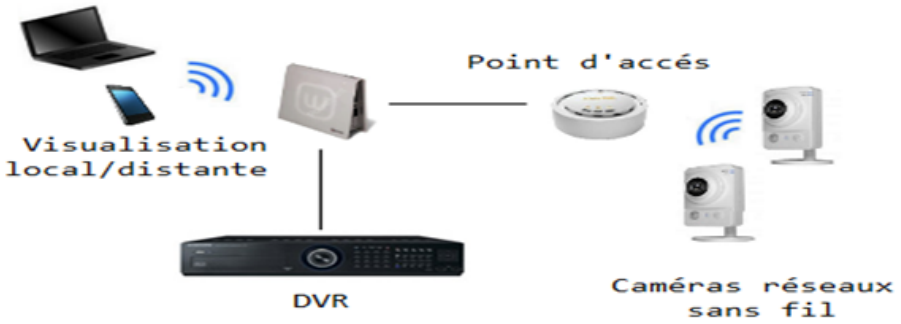

FIGURE 1.17 – SVS IP sans fil.

1.9 Conclusion

Comme nous avons vu dans ce chapitre qui a été axé sur le principe de la vidéosurveillance, les différents types de système et les avantages ainsi que les inconvénients de chaque système. La vidéosurveillance est un moyen efficace de protéger des personnes ou des biens matériels. La vidéosurveillance peut aussi être vue comme une base de données pour les domaines sociologiques, commerciales et marketing.

2

Vidéosurveillance sur IP

2.1 Introduction

La tendance de l'économie mondiale actuelle exige aux entreprises d'être réactive devant les demandes de plus en plus gourmandes de moyen de connectivite et infrastructure de communication et de marketing, la technologie de la vidéo sur réseau IP redynamise les applications de vidéosurveillance par de nombreuses fonctionnalités comme le contrôle à distance et la vidéo en temps réel.Ce qui rend plusieurs secteurs d'activités interactifs.

2.2 La vidéosurveillance IP

[2]
La videosurveillance IP (Internet Protocole) est venue compléter la vidéosurveillance analogique, qui équipe encore la majorité des installations. Elle fonctionne avec les mêmes composants (caméras, moniteur, enregistreur, câbles) et permet de visualiser et d'enregistrer des images vidéo via un réseau informatique disponible aussi bien chez un particulier que dans les grandes entreprises.

À la différence des systèmes de vidéosurveillance analogique, la vidéo sur IP utilise le réseau informatique plutôt qu'un système de câblage dédié (câble coaxial) pour transmettre les informations.

2.3 Les atouts de la vidéosurveillance IP

[16]

2.3.1 A l'installation :

- Possibilité d'utiliser le réseau informatique existant.
- Possibilité d'utiliser des caméras sur courant porteur (CPL) ou sans fil (Wifi).
- Le câble réseau transmet l'image et le son, et même l'alimentation.
- Pas d'affaiblissement du signal avec la longueur du câble.
- L'ordinateur fait office d'enregistreur numérique.
- Pas besoin de moniteurs spécifiques, l'écran informatique suffit.
- Coûts d'installation et de maintenance extrêmement limités.
- Technologie accessible aussi bien aux particuliers qu'aux entreprises et commerces.

2.3.2 A l'utilisation :

- Accès distant aux images via un simple navigateur Internet ou un téléphone mobile.
- Facilité de distribution et d'échange des images avec d'autres applications.
- Valider visuellement (à distance) une alarme qui se déclenche.
- Pour les parents, surveiller ce que font les enfants au domicile.
- Diminuer les vols dans les commerces et entreprises.
- Gérer et visualiser d'un poste fixe, plusieurs magasins, commerces ou entreprises.
- Haute et fixe qualité des images numériques visualisées et enregistrées.

– Caméras "intelligentes" capables d'envoyer des informations suite à une détection de mouvement.
– Évolutivité du système et faible besoin de maintenance des éléments.
– Coût réduit par rapport à un système traditionnel de vidéosurveillance analogique.

2.4 La production d'images

[8] La qualité de l'image représente indéniablement l'un des éléments les plus importants d'une caméra. Ceci est particulièrement vrai dans les domaines de lasurveillance, de la sécurité et du contrôle distant, où des vies et des biens peuvent être en jeu. La qualité de l'image peut varier considérablement, elle dépend d'un ensemble de facteurs tels que le choix de l'optique et du capteur d'images, les capacités de traitement et le niveau de complexité des algorithmes de numérisation et de compression. Cette dernière peut suivre deux approches différentes : sansperte ou avec perte.

Dans le cas d'une compression sans perte, chaquepixel est maintenu intact et l'image obtenue après compression est donc identique à l'originale. Cependant, il est très limité en terme de réduction des données. L'un des formats de compressionsans perte le bien connu est le format GIF, son faible taux de compression, ilne convient guère aux solutions de vidéo sur IP nécessitant l'archivage et la transmission de quantitésimportantes d'images. Voilà pourquoi plusieurs méthodes et normes de compression dites "avec pertes" ont été développées. Le principe fondamental est de réduire les éléments invisibles à l'œil humain et d'accroître ainsi considérablement le taux de compression.

Les méthodes de compression avec pertes suivent également deux approches différentes par rapport aux normes decompression : compression des images fixes et compression vidéo.

2.4.1 pression des images fixes :

Toutes les normes de compression des images fixes ont la particularité de se concentrer sur une seule image à la fois. Les normes les plus utiliséessont JPEG et JPEG2000.

JPEG :(Joint Photographic Experts Group) a été normalisé au milieu des années 1980, et grâceà ce format, il est possible de décompresser et de visualiserdes images à l'aide d'un navigateur web standard. JPEG permet d'obtenir le degré de compressionsouhaité (le taux de compression est paramétrable).La compression sélectionnée est directement liée à la qualité de l'image voulue. Outre le degré decompression, l'image elle-même influence également le taux de compression obtenu. Par exemple,un mur blanc peut produire un fichier image de taille relativement petite et un taux de compressionélevé, tandis que le même degré de compression appliqué à une scène complexe et chargée produiraun fichier de plus grande taille, avec un taux de compression plus faible.

JPEG2000 : est une autre norme utilisée pour la compression d'images fixes. Elle a été mise au pointpar le comité à l'origine de la norme JPEG. La norme JPEG2000 s'adresse principalement aux applicationsmédicales et au monde de la photographie fixe. À des taux de compression

peu élevés, la qualitéJPEG2000 est similaire à la qualité JPEG. En revanche, quand on passe à des taux beaucoup plus élevés,JPEG2000 s'avère légèrement supérieur à JPEG. Seulement que JPEG2000 reste fortpeu supporté par les navigateurs web et les applications d'affichage ou de traitement d'image.

2.4.2 Compression des vidéos :

plusieurs formats de compression sont utilisés dans la vidéosurveillance, nous citons ci-dessous les formats les plus répondues.

M-JPEG ou (Motion JPEG) : Vidéo obtenue par une suite d'images JPEGest la norme la plus répandue parmi les systèmes de vidéo sur IP. Une caméra réseau, toutcomme un appareil numérique permettant la capture d'images immobiles, saisit des images individuelles,et les compresse au format JPEG. Une caméra réseau peut ainsi capturer et compresser, parexemple, 30 images individuelles par seconde puis les envoyer sur réseau sous forme de flux continupouvant être lu sur un poste de visualisation à une fréquence de l'ordre de 16 images par seconde ouplus, l'utilisateur perçoit une vidéo en mouvement. Chaque image individuelle étant totalement compressée en JPEG, une qualité identiqueest assurée pour toutes les images, en fonction du taux de compression sélectionné pour la caméraréseau ou le serveur vidéo.

MPEG :fondée par le Moving Picture Experts Group à la fin des années 1980.Le principe de base du MPEG consiste à comparer deux images compressées destinées à êtretransmises sur le réseau. La première des deux images servira de trame de référence. Sur les imagessuivantes, seuls seront envoyées les zones qui diffèrent de la référence. L'encodeur réseau reconstruitalors toutes les images en fonction de l'image de référence et de la plage de différence.Bien que plus complexe que la technique Motion JPEG, la compression vidéo MPEG produit de pluspetits volumes de données à transmettre via le réseau.Cette méthode implique bien souvent destechniques ou des outils supplémentaires permettant de gérer certains paramètres tels que la prédiction dumouvement dans une scène ou l'identification des objets. Il existe aussi différentes normes MPEG :

- **MPEG-1 :** lancée en 1993 et destinée à l'archivage des données vidéo numériques sur CD. Elle met surtout l'accent sur le maintien d'un débit relativement constant, au détriment de la qualité d'image, laquelle est variable. En MPEG-1, la fréquence d'image est plafonnée à 25/30images par seconde.
- **MPEG-2 :** approuvée en 1994, était destiné à la vidéo numérique de qualité supérieure, Le format MPEG-2 visait à accroître la technique de compression de la norme MPEG-1 afin de couvrir des images plus grandes et de meilleure qualité, mais aux dépens d'un taux de compression plus faible et d'un débit d'images plus rapide. La fréquence est plafonnée à 25/30 images par seconde, tout comme en MPEG-1.
- **MPEG-4 :** représente une évolution substantielle par rapport au format MPEG-2. Les outils permettant de réduire le débit d'images de manière à atteindre une certaine qualité pour une application ou une scène déterminée sont beaucoup plus nombreux en MPEG-4. En outre, la fréquence n'est plus limitée à 25/30 images par seconde. Cependant la plupart des outils actuels permettant de réduire le débit ne concernent que les applications en temps réel. Ceci est dû au fait que ces outils requièrent des capacités telles que les durées

d'encodage et de décodage qui les rendent quasiment impossibles à utiliser. En réalité, la majorité des outils MPEG-4 destinés aux applications en temps réel sont les mêmes que ceux qui existent pour les formats MPEG-1 et MPEG-2.

- **H.264 :**également appelée MPEG-4 Partie 10/AVC - AVC pour "Advanced Video Coding" signifiant codage vidéo avancé. H264 est le fruit d'un projet commun entre le Groupe d'experts en codage vidéo (VCEG) de l'InternationalTelecommunications Union qui assure la coordination des normes de télécommunicationset le Groupe d'experts en images animées (MPEG) de l'ISO/IEC.L'ISO est l'Organisation internationale de normalisation. De son côté, l'IEC (Commissionélectrotechnique internationale) assure la surveillance de toutes les technologies électroniques,électriques et afférentes.
- H.264 : est une norme ouverte et sous licence compatible avec la plupart des techniques de compressiondisponibles aujourd'hui. Un encodeur H.264 peut réduire la taille d'un fichier vidéo numérique deplus de 80
  Conçue pour remédier à plusieurs faiblesses des normes de compression vidéo précédentes, la normeH.264 offre les avantages suivants :

  - qualité vidéo équivalente, réduction moyenne du débit de 50
  - Tolérance d'erreurs, ce qui signifie que les erreurs de transmission sur différents réseaux sont tolérées.
  - Latence réduite et meilleure qualité en cas de latence supérieure.
  - Spécification de syntaxe simple facilitant l'implémentation.
  - Décodage correspondant exactement à la source et définissant de façon exacte les numérisations quidoivent être effectuées par un encodeur et un décodeur pour éviter l'accumulation d'erreurs.

2.5 La transmission

[2] La vidéosurveillance sur IP se base principalement sur les technologies du réseau informatique pour l'acheminement des flux vidéos jusqu' aux supports de stockage ou vers des postes de visualisation local ou à distance. Dans ce qui suit, nous citons les méthodes de transmission et les protocoles réseaux les plus utilisés dans la vidéosurveillance IP.

2.5.1 Les méthodes de transmission :

- **Diffusion individuelle ou Unicast :** Une liaison point à point est établis entre un émetteur et un récepteur pour communiquer entre eux. Dans cette méthode de transmission les paquets de données sont adressés à un seul récepteur et aucun autre ordinateur du réseau ne traite ces informations.
- **Multidiffusion ou Multicast :** la communication se fait entre un seul émetteur et plusieurs récepteurs. Lorsque plusieurs récepteurs souhaitent visualiser une même source en même temps. Un seul flux d'information peut ainsi être envoyé à des centaines de récepteurs, ce qui permet de réduire le trafic sur le réseau. La différence majeure par rapport à la diffusion individuelle est que le flux vidéo ne doit être envoyé qu'une seule fois. La multidiffusion est fréquemment utilisée en conjonction avec les transmissions à base de protocole RTP.

– **Radiodiffusion ou Broadcast :** Dans ce type de transmission les données sont transmises de un à plusieurs. Sur un réseau LAN, la radiodiffusion est en principe limitée à certains segments spécifiques et ne s'applique pas en pratique aux transmissions vidéo sur IP.

2.5.2 Les protocoles de transport

Les images et les vidéos sont numérisées et compressées puis ordonner sous forme de paquets, chaque paquet est alors expédié indépendamment des autres. Lors de son envoie chaque paquet essaie de prendre le plus court chemin vers la destination et cela à l'aide d'un nombre important de protocoles qui gèrent le réseau informatique. Les protocoles les plus courants dans le cadre de la transmission des flux vidéo sur IP et leurs numérosde ports correspondants sont :

Le protocole	Protocole qui le transporte	Numéro de port	Utilisation en vidéo sur IP
FTP	TCP	21	Transfert d'images/vidéos de la caméra réseau/serveur vidéo vers un serveur de ficher ou une application
SMTP	TCP	25	Une caméra réseau/serveur vidéo peut envoyer des images ou notifications d'alarme grâce au client mail intégré
HTTP	TCP	80	Pour l'accès aux vidéos via interface web
HTTPS	TCP	443	Même chose avec http mais avec une transmission sécurisée
RTP	UDP/TCP	Non défini	Transmission des flux vidéos sur IP MPEG en temps réel peut être en unicast ou multicast
RTCP	TCP	Non défini	contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service
RTSP	TCP	554	Configuration et contrôle de sessions multimédia par RTP

TABLE 2.1 – protocoles de transmission utilisés dans la vidéosurveillance.

2.5.3 La bande passante :

c'est la quantité d'information maximale en bit par seconde (bit/s) qui peut être transmise sur un canal de transmission. Les équipements de la vidéosurveillance sur IP utilisent la bande passante en fonction de leur configuration et son usage dépend de plusieurs facteurs :

- La taille de l'image.
- Le taux de compression.
- La fréquence d'images (nombre d'images par seconde).
- La complexité de la scène.

Il existe de nombreuses manières de tirer pleinement parti d'un système de vidéosurveillance sur IPet degérer au mieux la consommation de la bande passante. Voici les techniques employées :

- **Réseaux commutés :** Grâce au Switching qui est une méthode très répandue aujourd'hui, le même réseau physique (ordinateurs et système de vidéo sur IP) peut être séparé en deux réseaux autonomes. Même en restant physiquement le même, cette méthode le divise de manière logique en deux réseaux virtuels et indépendants.
- **Bande passante élargie :** Le prix des commutateurs Gigabits et des routeurs baissant continuellement, les réseaux de grande capacité sont de plus en plus abordables. En augmentant la bande passante, la tendance est aux réseaux plus rapides et les systèmes de surveillance à distance sontdonc de plus en plus attrayants et rentables.
- **Fréquence évolutive :** La configuration de 25 images par seconde enregistrées en permanence pour toutes les caméras offre un niveau de qualité bien supérieur à ce que la plupart des applications ont besoin. Grâce aux capacités de configuration et à l'intelligence intégrée dans la caméra réseau ou le serveur vidéo, la fréquence peut être diminuée en conditions normales jusqu'à 5 ou 6 images/sec voire même une seule image par seconde. La consommation de la bande passante est ainsi réduite. En cas d'alarme, déclenchée par exemple par le détecteur de mouvements, la fréquence d'enregistrement peut adopter automatiquement un niveau supérieur.

  Dans la plupart des cas, la caméra envoie uniquement les images vidéo dont l'enregistrement présenteun intérêt, ce qui représente environ 10

2.5.4 La sécurisation des transmissions

Il existe plusieurs façons de sécuriser un réseau ainsi queles communications entre différents réseaux et clients.En réalité, tout peut être contrôlé et sécurisé depuis lesdonnées envoyées jusqu'aleur utilisation. La sécurité est portée sur le réseau lui-même et son accessibilité.

2.5.5 Les solutions de sécurité

La sécurisation des communications se déroule en trois étapes distinctes :

- **L'authentification :**Cette première étape doit permettre à l'utilisateur ou au périphérique de s'identifier sur le réseau ou l'hôte distant. Pour ce faire, certaines données d'identité sont communiquées au réseau ou au système, comme par exemple un code d'utilisateur et un mot de passe.
- **L'autorisation :** L'étape suivante consiste à autoriser et à accepter l'authentification, c'est-à-dire à vérifier si la machine est bien celle qu'elle prétend être. On vérifie à cet effet l'identité donnée par rapport aux informations contenues dans la base de données ou dans une liste d'identités réputées correctes et approuvées. Au terme de l'autorisation, la machine est totalement connectée et opérationnelle dans le système.
- **Confidentialité :** La dernière étape consiste à appliquer le degré de confidentialité souhaité. Pour ce faire, la communication est cryptée afin que les données ne puissent être utilisées ou lues par personne d'autre. Selon le type de déploiement et de chiffrement utilisé, il peut arriver que le recours au cryptage nuise assez fortement aux performances. La confidentialité peut être assurée de plusieurs façons. Les méthodes VPN et SSL/TLS (ou HTTPS) sont parmi les plus utilisées :

  VPN(Virtual Private Network) : Un VPN, ou réseau privé virtuel, crée un tunnel sécurisé entre les différents points du réseau.Seules sont autorisées à opérer sur le réseau VPN, les machines possédant la clé correcte. Lespériphériques réseau entre le client et le serveur ne peuvent ni accéder aux données, ni les consulter.Un réseau VPN permet à différents sites de se connecter sur Internet d'une manière sûre etsécurisée.

  SSL/TLS : Une autre façon d'assurer la sécurité est d'appliquer le cryptage aux données elles-mêmes. Dansce cas, il n'y a pas de tunnel sécurisé comme dans la solution VPN, mais les données proprementdites sont sécurisées à l'envoi.Parla méthode SSL, aussi appelée HTTPS, le périphérique ou l'ordinateur installe un certificat dansl'unité. Les certificats peuvent être émis localement par l'utilisateur ou par un organisme de confiance tiers.

2.5.6 La sécurité dans les communications wifi :

communication sans fil implique que toute personne munie d'un équipementsans fil et se trouvant dans la zone couverte par le réseau soit à même d'intervenir sur le réseau etd'utiliser les services partagés. D'où la nécessité de sécuriser le système. Il existe plusieurs techniques dont nous citons les plus adaptées pour les réseaux sans fil :

WEP : La norme WEP (Wireless Equivalent Privacy) renforce la communication par le chiffrement continu RC4RSA, évitant ainsi que quiconque n'accède au réseau s'il ne possède pas la clé adéquate.Le problème de la norme WEP est qu'elle présente plusieurs faiblesses la rendant vulnérable aux attaques,et qu'elle ne permet pas d'assurer les niveaux de sécurité essentiels. Les principaux points faibles du WEPsont sa clé de chiffrement statique et son court vecteur d'initialisation. Du fait de la facilité d'attaquecontre le WEP par des équipements peu coûteux, il est déconseillé d'y recourir sur les réseaux sans fil.

WPA : La norme WPA (WiFi Protected Access) permet de résoudre les principaux points faibles du WEP.Avec WPA, la clé est adaptée à chaque image transmise, via le protocole TKIP (Temporal Key IntegrityProtocol). Le vecteur d'initialisation passe de 24 à 48

bits. La norme WPA est considérée comme le niveaude sécurité de base pour les réseaux sans fil.

Lorsque davantage de sécurité s'impose, on envisage le WPA2, qui fait quant à lui appel à la normeAES (Advanced Encryption Standard) plutôt qu'au protocole TKIP. L'AES s'avère la meilleure méthode dechiffrement disponible actuellement pour les réseaux sans fil, et elle intègre également l'authentification.

2.6 Le stockage :

[11] L'émergence des systèmes de vidéo sur IP implique une utilisation de plus en plus importante d'espacedisque. Ceci pose un certain nombre de questions, et notamment celle de savoir quel espacedisque sera nécessaire et comment assurer un stockage sûr. Les facteurs à prendre en compte dans la détermination des besoins de stockage sont :

- Nombre de caméras.
- Nombre d'heures d'enregistrement quotidien par la caméra.
- Durée de conservation souhaitée des données.
- Détection des mouvements (événements) uniquement, ou enregistrement continu.
- Autres paramètres, comme par exemple la fréquence, la compression, la qualité d'image et la complexité demandées.

2.6.1 Solution utilisant un serveur PC :

Les solutions utilisant une plate-forme avec serveur PC fonctionnent sur un matériel standard,dont les composants physiques ont été sélectionnés avec soin, de manière à offrir des performancesoptimales. Avec ce type de solution, il est possible d'optimiser les composants standard, notammenten augmentant les capacités de stockage, en ajoutant de l'espace externe ou des postes de traitementsupplémentaires, ou en exécutant des logiciels supplémentaires en parallèle à l'application vidéo, telsque des outils pare-feu ou antivirus.

Dans ce genre de solution dont le stockage se fait principalement sur disque dure, deux approches sont possibles : l'une consiste à confier lestockage au serveur exploitant l'application ; l'autre est une solution indépendante, dans laquelle lestockage est déporté.

- **Stockage embarqué (DAS - Direct Attached Storage) :** Le stockage embarqué est la solution de stockage sur disque dur la plus fréquemment utilisée dans les installations de petite à moyenne envergure. Le disque dur se trouve sur le PC exploitant l'application de gestion vidéo. L'espace disponible est en fonction du PC et du nombre de disques durs qu'il contient. La plupart des PC accueillent deux disques durs, certains vont jusqu'à 4. Chaque disque dur peut contenir jusqu'à environ 300 Go, soit une capacité totale d'environ 1,2 To (téraoctets).
- **Stockage déporté NAS ou SAN :** Dans les applications où la quantité d'informations stockées et les contraintes globales dépassent les limites d'un système de stockage embarqué (DAS), un système de stockage séparé est mis en œuvre :NAS (Network Attached Storage) et SAN (Storage Area Network)

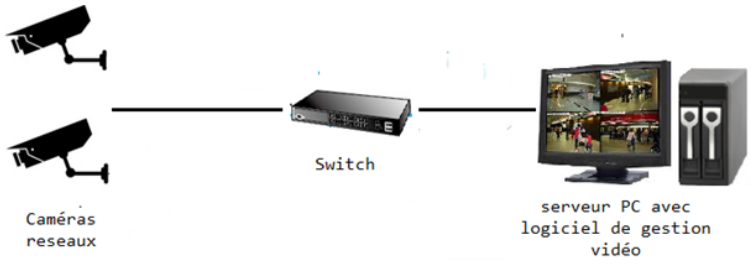

FIGURE 2.1 – Stockage en DAS.

1. **NAS :** Dans le cas d'un système NAS, un même dispositif de stockage directement rattaché à un LAN propose un stockage partagé à tous les clients du réseau. Facile à installer et à administrer, un dispositif de type NAS constitue une solution de stockage bon marché. La capacité de traitement des données entrantes est cependant limitée.
2. **SAN :** Une solution SAN propose une plate-forme de stockage polyvalente à grande vitesse, reliée par fibres optiques à un ou plusieurs serveurs. Les utilisateurs peuvent accéder à tous les dispositifs de stockage du SAN via les serveurs. La capacité de stockage est configurable jusqu'aux centaines de téraoctets.

   Le stockage centralisé des données réduit les contraintes administratives tout en offrant une mise en commun à la fois très performante et très souple des capacités de stockage au service des environnements multiserveurs.

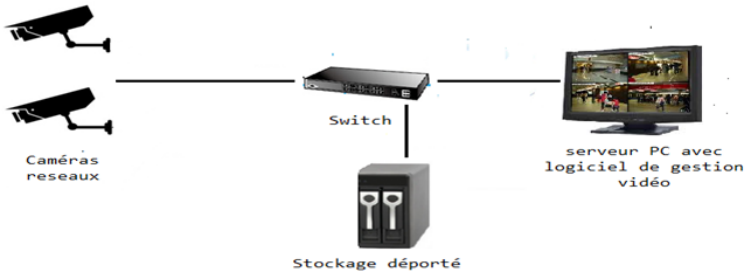

FIGURE 2.2 – Stockage déporté.

La différence entre les deux solutions est que la plate-forme NAS permet de stocker un fichier entier sur unseul disque dur, tandis que le SAN propose un stockage par blocs sur différents disques durs. Ce typede configuration de disque permet d'exploiter des solutions de taille adaptée, autorisant le stockaged'importantes quantités de données, pour un niveau de redondance élevé. Les deux types de solutionsexistent pour les logiciels de gestion vidéo.

2.6.2 Solution utilisant les enregistreurs vidéo sur IP (NVR) :

Les enregistreurs vidéo sur IP présentent certaines similitudes avec les enregistreurs numériques (DVR)en termes d'enregistrement et de lecture. Mais alors que l'enregistreur numérique

est en réalité unsystème hybride, capable de prendre en charge les caméras analogiques et de stocker les images vidéodans un format numérique sur disque dur, l'enregistreur vidéo sur IP, en revanche, est un système 100

Un enregistreur vidéo sur IP est conçu pour offrir des performances optimales pour une ou plusieurscaméras, mais ses capacités d'extension sont inférieures à celles des plates-formes utilisant un serveurPC. L'enregistreur vidéo sur IP convient donc pour les environnements de plus petite taille, lorsque lenombre de caméras reste dans les limites des capacités de l'enregistreur. Un avantage, en revanche,est que les plates-formes utilisant un enregistreur vidéo sur IP sont moins difficiles à installer queles plates-formes avec serveur PC.

2.6.3 Architecture de stockage :

[8] Il existe communément deux approches différentes pour stocker des données dans un système devidéosurveillance sur IP. Une architecture centralisée utilise une base de données principale situéedans la salle de contrôle centrale ou au siège de l'entreprise. Une architecture distribuée diffuse les données dans le système de Gestion de Sécurité, les conservant en général tout près de l'endroit oùelles sont produites ou utiles. Les données stockées peuvent être classées selon deux types : Configuration et Live.

- Les données Configuration sont des informations qui spécifient la conception et l'élaboration du système de Gestion de Sécurité. Parmi les exemples de données de configuration, on trouve les listesde caméras, les listes d'utilisateurs, les droits d'utilisateurs, les structures de sites, les cartesreprésentant la disposition du système et les informations sur les licences. Après l'installation initiale et le paramétrage du système de Gestion de Sécurité, les données de configuration n'ont pas besoind'être changées de manière très souvent. Les opérateurs y ont pourtant accès régulièrement, lorsqu'ils se connectent au système par exemple.
- Les données Live (en temps réel) correspondent typiquement aux enregistrements vidéo et aux informations des alarmes. Les dispositifs d'enregistrement des données ainsi que les opérateurs peuvent accéder aux données en temps réel de manière continue lors des opérations habituelles de gestion de sécurité.

2.6.4 1. Architecture centralisée :

Les données Configuration sont habituellement conservées dans une base de données appelée laBase de données Site. Les utilisateurs peuvent ainsi effectuer et gérer plus facilement les modifications, mais cela pose aussi un problème. Lorsqu'un administrateur effectue une modification dela Base de données Site, comment les utilisateurs, dispersés à travers le système de Gestion de Sécurité, obtiennent la modification.

La solution la plus évidente et la plus facile est de positionner la Base de données Site sur un serveurde base de données principal et de donner l'accès à ce serveur principal à tous les utilisateurs par leréseau. C'est ce que l'on appelle une architecture centralisée qui est utilisée par beaucoup de systèmes de vidéosurveillance pour stocker plus que de simples données de configuration mais aussi pour stocker des données en temps réel telles que desenregistrements

v idéo ou des données d'alarmes.

La Figure II.3représente un système de Gestion de Sécurité avec un ou plusieurs sites, chacun avec sonpropre réseau d'entreprise local connecté au bureau central. Le serveur de fichiers central qui héberge la base de données Site, est situé au bureau central. De même pour les enregistreurs vidéo sur IP pour enregistrer les vidéos et lesdonnées d'alarmes.

Toutes les caméras et les postes de travail de chaque bureau distant doivent régulièrement, et danscertains cas continuellement, communiquer avec le bureau central afin de vérifier les modifications et mises à jour de la base de données Site. Ceci inclut les vérifications pour la validité des licences, ou le stockage des enregistrements vidéos et des données d'alarmes.

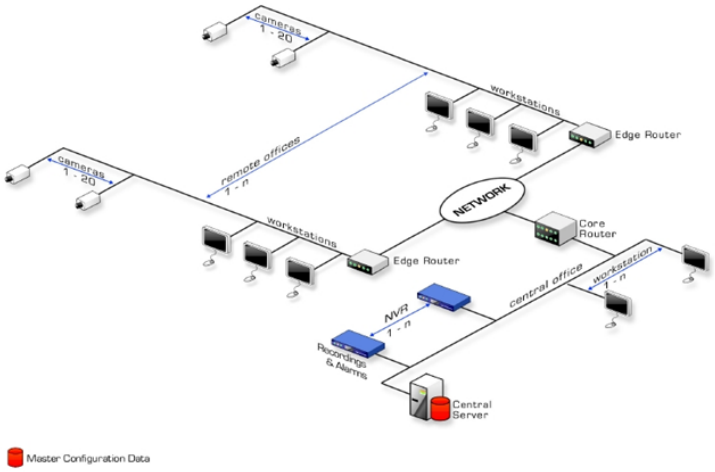

FIGURE 2.3 – Architecture centralisée.

Cependant cette architecture pose quatre problèmes majeurs :

1. **Le coût :** Tous les utilisateurs communiquent continuellement avec le bureau central sur un réseau d'entreprise local, cela revient à acheter des commutateurs haut de gammecouteux, et sur un réseau d'entreprise étendu (WAN), cela impliqued'utiliser une bande passante couteuse.
2. **Fiabilité et Résistance :** si un commutateur du réseau WAN ou du noyau LAN s'arrête, Les utilisateurs les plus éloignés peuvent se retrouver sans accès aux vidéos des camérassituées localement sur un réseau LAN qui sont parfaitement fonctionnel.
3. **Point de défaillance unique :** dans le cas ou le serveur qui héberge la base de données site rencontre une erreur, tous les utilisateurs du système dépendant de l'accès à cette base par exemple, pour obtenir la vérification des droits d'utilisateurs ou despermissions de licence seront bloqués et le systèmede Gestion de sécurité entier s'effondre.
4. **Evolutivité :** Au fur et à mesure que l'on ajoute des caméras et des utilisateurs àchaquebureau distant et que plus de bureaux distants sont ajoutés au réseau, tout commence às'encombrer. Les réseaux LAN, les liens WAN et le serveur central s'encombrent tous rencontrant des niveaux de trafic de plus en plus élevés pour chaque vérification demodi-

fications de la base site, de validité des licences et pour le stockage desenregistrements et alarmes.

2.6.5 2. Architecture distribuée :

Distribution des données Configuration : Pour distribuer des données configuration, chaque poste de travail distant garde un cache local de la bade de données site. Les données Configuration ne changent pas très fréquemment. Cela implique que l'information peut être synchronisée entre le serveur centrale et les postes de travail distants, de façon régulière, ou sur demande lorsqu'une modification est faite.

- **Distribution des données de licences :** Plutôt que de stocker les informations des licences sur le serveur central, les composants individuels du système de gestion de sécurité peuvent posséder leurs propres licences. Par exemple, les caméras peuvent garder des informations dans leur mémoire embarquée concernant les résolutions autorisées en enregistrement et en visualisation, ou les taux d'images par seconde autorisés. Elles peuvent aussi garder les informations sur les caractéristiques activées.

  Dans cette architecture où les sources des données utiles (les caméras et lesenregistreurs) contiennent leurs propres licences, signifie que ces dernières n'ont pas besoin de communiquer avec le serveur central, puisqueelles possèdent leurs propres licences distribuées. Les opérateurs ne peuvent pas visionner une vidéo donnée, sila caméra ou l'enregistreur ne le leur permet pas, Cela signifie qu'aucun des postes de travail n'a besoin de vérifier les informations de licences avec le serveur central.
- **Distribution des données Live :** Plutôt que de faire circuler un flux d'enregistrement et de données d'alarmes continu depuis les sites distants vers le site central via le réseau WAN, il est beaucoup plus avantageux de garder les données localement dans le réseau local. Les enregistreur vidéo IP sur chaque site éloigné réduirait le trafic sur le WAN et permettrait aux utilisateurs des sites distantsd'accéder aux enregistrements et alarmes même lorsque le WAN n'est pas disponible. Comme le bureau central se trouve souvent là où la gestion des alarmes est effectuée à travers tout le système, les utilisateurs situés dans le bureau central peuvent ainsiaccéder aux NVR distants dans le cas d'une investigation d'alarme ou d'incidents. La Figure II.4 présente une architecture centralisée.

Ainsi l'architecture distribuée résolve les problèmes de l'architecture centralisée et cela comme suite :

1. **Le coût :** dans le cas d'un incident de sécurité, seule la vidéo endirect ou juste certaines portions de vidéos désirées sont exportées à travers le réseau WAN ou le réseau LAN étendu, et pas besoin d'accéder aux enregistrements entiers. La bande passante n'est pas gâchée et des Switch rentables peuvent gérer les charges réseau réduites.
2. **Fiabilité et Résistance :** Le réseau WAN est une source potentielle de défaillance du réseaude gestion de sécurité, donc le budget de maintenance peut être dédié à augmenter la fiabilité des connexionsWAN mais il est beaucoup plus efficace de distribuer les données de façon à ce que lesutilisateurs aient toujours un systèmequi marche même lorsque lesconnexions WAN sont inopérantes.
3. **Point de défaillance unique :** Dans le cas où le serveur central, un Switch LAN ou WAN ou un enregistreur numérique est défaillant, lesutilisateurs peuvent continuer de

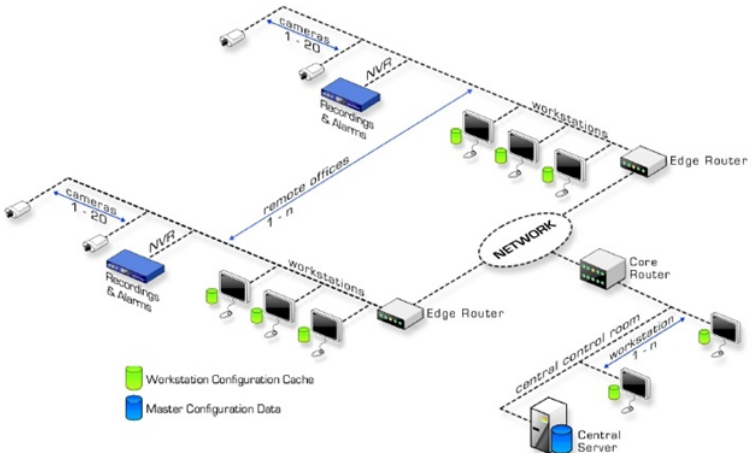

FIGURE 2.4 – Architecture déstribuée.

travailler en utilisant leur base de données site répliquée localement sur leur poste de travail. Ici encore les budgets peuvent être redirigés pour augmenter la fiabilité de ces machines.

4. **Evolutivité :** Avec une architecture distribuée, les caméras et les utilisateurssupplémentaires peuvent être ajoutés à un bureau local avec une augmentation minimale du trafic WAN, le flux de vidéo circule et est enregistré localement. De la même manière, si un autre bureau distantest ajouté, il s'agit simplement d'une duplication des bureaux existants avec un réseau local et un stockage local. Pour des systèmes de plus grande envergure, on peut distribuer et synchroniser plusieurs serveurs centraux en ajoutant encore une autrecouche dedistribution et de résistance.

2.6.6 La sécurisation de stockage

Afin de pouvoir utiliser les données visuelles collectées par un système de vidéosurveillance comme support d'investigation, il est important d'avoir une preuve sur l'authenticité et l'origine de ces données. Les méthodes de traitement numériques sont tellement disponibles et faciles d'utilisation qu'il est rendu aisé de falsifier et de manipuler les séquences vidéo. Il est donc nécessaire d'incorporer des procédées qui sécurisent les données contre toutes sortes de manipulation. Ces procédées doivent répondre aux point suivants :

- L'authentification de contenu visuel contre toute sorte de manipulation.
- La divulgation de l'origine des données en termes de temps, du lieu d'acquisition et de l'équipement utilisé.
- Les données de sécurisation doivent avoir un volume minimal.
- Détection et distinction des manipulations usuelles et innocentes (changement de format, protection des données privées, etc.) qui doivent être définies au préalable.
- Les données originales doivent être retrouvées suite à une manipulation et cette dernière doit être figurée sur les images des séquences vidéo.

2.6.7 1. La cryptographie :

son utilisation à base de clés secrètes peut se faire de plusieurs façon nous citons les cas suivant :

- Crypter chaque image et seuls les détenteurs de la bonne clé peuvent décrypter les données visuelles.
- Générer une signature de l'image et la crypter, l'authentification requiert la régénération de la même signature de l'image et de comparer son crypté avec la signature crypté fournie. Ici le cryptage des deux signatures ce fait avec la même clé.
- Générer une signature différente pour chaque localisation des images, dans ce cas des informations de localisation de régions sont fournies.

L'inconvénient avec cette approche est que le surplus de données générées est considérable, et la sécurité est restreinte à la vérification de l'intégrité des données que contenu visuel. De plus, toute visualisation ou traitement des données visuelles requiert leurs décryptage ce qui influence sur le temps de traitement des données visuelles.

2.6.8 2. Le marquage numérique :

il consiste à insérer une marque invisible dans l'image dont sa détection ou son extraction suivie d'une analyse renseigne d'une manière précise sur l'origine des données, leur authentification et toute falsification subie. Ayant une connaissance de ce qui ce fait, nous pouvons citer quelques caractéristiques et avantages de cette approche :

- Du fait que la marque est insérée dans l'image, le surplus d'informations à gérer se limite généralement aux clés requises pour l'insertion et/ou détection ou extraction de la marque.
- La nature imperceptible de la marque rend l'altération des données de l'image pas vraiment grave sur l'analyse et l'interprétation de contenu des séquences vidéo comme la reconnaissance des personnes ou suivis des véhicules. La contrainte de réversibilité de marquage n'est pas requise dans le domaine de la vidéosurveillance.

L'inconvénient avec le marquage numérique est que lors de compression des séquences vidéo qui peut être requis pour des fins de transport sur IP ou d'optimisation d'enregistrement, et que les formats de compression les plus adaptés dans ce domaine sont les formats avec pertes, les données de marquage peuvent être perdu lors de la compression. Cependant certaines méthodes d'authentifications s'appliquent sur les images compressées dans leurs formats (MPEG, JPEG, ...), comme il existe aussi des méthodes dites semi fragile qui s'appliquent avant la compression des données, et qu'elles sont conçues pour tolérer les effets de la compression. Avec ces méthodes ces manipulations sont perçues comme usuelles et innocentes.

2.7 La gestion vidéo :

[9] La gestion vidéo d'un système de vidéosurveillance sur IP englobe des activités de visualisation, gérées à l'aided'un navigateur web ou d'un logiciel de gestion vidéo spécifique, ainsi que des activités d'enregistrementvidéo pouvant être menées à l'aide d'un logiciel de gestion vidéo installé sur PC ou à l'aided'un enregistreur vidéo sur IP.

2.7.1 La visualisation :

la visualisation des vidéos se fait par deux moyens : via logiciel de gestion vidéo ou par interface WEB.

2.7.2 1. La visualisation via l'interface web :

Dans un système de vidéosurveillance sur IP, la vidéo peut être visualisée en tout point du réseau et n' importe où dans le monde à conditiond'avoir accès à internet et à un navigateur web. Les caméras réseaux et les NVRs intègrent un serveur web disposant d'une adresseIP. Pour visualiser les images sur PC, il suffit donc d'ouvrir le navigateur web et de saisir l'adresse IPdans la zone d'adresse.Une fois que l'ordinateur a établi la connexion, une page d'accueil s'afficheautomatiquement dans le navigateur web. Cette page de démarrage affichera la vidéo en direct ainsique les liens hypertexte permettant de changer les paramètres de la caméra ou du NVR, tels que la résolution, etles paramètres réseau et e-mail, à moins que l'accès ne soit limité par mot de passe par exemple.

FIGURE 2.5 – Visualisation via interface web.

2.7.3 2. La visualisation via logiciel de gestion vidéo :

Un logiciel de gestion vidéo fonctionnant sur un serveur Windows ou Unix/Linux est un outil qui permet de gérer les images vidéo, de les analyser et de les enregistrer. Bien que la vidéo puisse être visualisée directement sur un navigateur web standard, un logiciel degestion vidéo peut aussi être installé si l'on souhaite bénéficier d'options d'affichage plus spécifiques ousi l'on souhaite pouvoir archiver et gérer les enregistrements vidéo. Il existe sur le marché une multitudede solutions applicatives, allant des solutions indépendantes pour un seul PC aux logiciels client/serveuravancés, fonctionnant en mode multiutilisateurs.Ces différentes solutions proposent en général desoptions de vidéosurveillance, les versions élaborées de ces logiciels sont capable d'offrir les options suivantes :

- Affichage et enregistrement simultané des séquences directes en provenance de plusieurs caméras.
- Différents modes d'enregistrement : continu, planifie ?, détection des alarmes et des mouvements.
- Prise en charge de fréquences d'image élevées et de données en grandes quantités.
- Fonctions de recherche multiples des séquences enregistrées.
- Contrôle des cameras PTZ et dôme.
- Fonctions de gestion des alarmes (alarmes sonores, affichage de messages ou envoie par e-mail).
- Support audio duplex en temps réel.
- Intelligence vidéo.

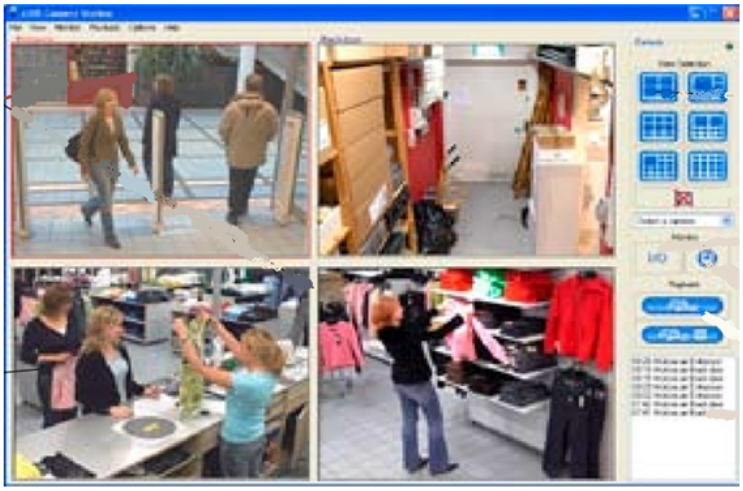

FIGURE 2.6 – Visualisation via Application de gestion.

2.7.4 L'enregistrement :

les méthodes d'enregistrement dans la vidéosurveillance sont multiples, comme nous avons vu à travers ce chapitre, la méthode choisie est souvent liée aux modèles de matériel, l'ampleur de cite à surveiller et aux exigences de client. Pour les opérations simples, les options proposées sur les caméras réseauxou les enregistreur numérique réseaux sont suffisantes pour enregistrer les images ou la vidéo enfonction d'événements programmés ou dès qu'ils surviennent. Les images sont ensuite chargées surun serveur FTP ou sur le disque dur d'un ordinateur. Pour les installations avec des caméras analogiques, un enregistreur vidéo sur IP est utilisé pour rassembler les flux d'images en provenance de ces caméras.

Dans les systèmes à grande ampleur dont plusieurs caméras sont installées et un nombre très important de flux sont à enregistrer, les installations peuvent bénéficier de contrôle de fréquence d'enregistrement que nous présentons ci-dessous :

Le contrôle de la fréquence :La vidéo sur IP permet le contrôle de la fréquence, contrairement à la vidéo analogique où toute lavidéo est envoyée en continu à partir de la caméra. Le contrôle de la fréquence des systèmes vidéosur IP signifie que la caméra réseau ou le serveur vidéo n'envoie les images qu'à la fréquence déterminée, aucune vidéo inutile n'est donc transmise sur le réseau. Un logiciel de gestion de la caméraréseau ou du serveur vidéo peut être configuré de manière à augmenter cette fréquence, par exemplelorsqu'une activité est détectée.Il est aussi possible d'envoyer des flux vidéo à des fréquences différentes en fonction du destinataire,ce qui peut être particulièrement intéressant en cas de liaison à faible bande passante vers des sitesdistants.

2.8 Conclusion

Les systèmes de vidéosurveillance sont en voie de devenir des équipements de sécurité courants au même titre que les systèmes d'alarme domestiques. Ils complètent efficacement ces derniers en offrant la possibilité de vérifier le bienfondé des alertes et peuvent également rendre de nombreux services, que ce soit pour un usage privé ou professionnel. La technologie et les prix de la vidéosurveillance ont fortement évolué dans le bon sens et permettent aujourd'hui de s'équiper d'un système complet à moindre coût et sans forcément réaliser de gros travaux d'installation.

Ce chapitre a été porté sur les caractéristiques fondamentales de la vidéosurveillance sur IP, à savoir les avantages et les atouts de cette solution, les différentes méthodes de transmissions et les protocoles utilisés, ainsi que les multiples solutions de stockage et de sécurisation des données visuelles.

3

Etude et réalisation

3.1 Analyse du besoin

3.1.1 Présentation de CTIB

En plein centre ville de Bejaia, à l'extrémité de quartier Sghire, l'un des quartiers les plus branchés de Bejaia, se situe l'immeuble de la boite informatique CTIB.

Crée en l'an 2000, CTIB pour Centre Télécommunication Informatique Bejaia se trouve au rez-de-chaussée d'un immeuble de deux étages, avec deux portes d'accès, une porte d'entrée qui donne sur le boulevard principale, et une porte derrière qui donne sur une petite ruelle utilisée par les habitants des maisons et immeubles voisins A cause de certains incidents récemment survenus aux bureaux de CTIB, le propriétaire des lieux souhaite renforcer les mesures de sécurité déjà pressentes dans les lieux, par un système de vidéosurveillance pour mieux gérer les situations déplaisantes et avoir un contacte visuel sur les incidents afin d'assurer une sécurité maximale des employés, et pour mieux servir la clientèle de cette boite qui exerce ses activités dans le domaine informatique à savoir la réparation des équipement informatique, création de sites web, étude et installation des réseaux informatique et système de sécurité.

3.1.2 Objective de l'intervention

L'objectif premier vise est l'implémentation d'une solution technique et le moins onéreuse possible afin d'augmenter le niveau de sécurité au sain de CTIB.

3.1.3 Cahier de charges

Lors de notre stage au sain de CTIB la direction nous a soumis un cahier de charges qui comporte les exigences techniques de futur système de vidéosurveillance à installer comme suite :

- La possibilité de visualiser en temps réel sur touts les postes disponibles sur les lieux.
- Mettre en place un système discret et pas très couteux.
- Donner des nivaux d'accès hiérarchiques.
- Avoir un système sécurisé par couple mot de passe/login.
- Enregistrement sur déclenchement.

3.2 Solution proposé

Lors de notre stage à CTIB nous avons proposé une solution de vidéosurveillance avec huit caméras analogiques et un enregistreur numérique réseau.

3.2.1 Présentation de l'équipement

DVR 16CH-H264 caractéristiques

- Compression H.264.
- Affichage a 480 images/sec max partage entre les cameras Enregistrement a 240 images/sec partage entre les cameras Différents modes d'enregistrements.
- Support pour souris USB.
- 4 Entrées Audio / 1 Sortie Audio.

FIGURE 3.1 – DVR 16CH-H264.

– Capacité de stockage variable selon le disque dure installé.

Caméra analogique IPB-331

FIGURE 3.2 – Caméra analogique PB-331.

caractéristiques

– Résolution 480 TVL (Couleur) 720 TVL (N/B) Rayon Maximal 15 Mètres.

3.3 Installation et configuration

3.3.1 Déploiement des caméras

figure du deploiement des cameras Pour le déploiement des caméras nous avons procédé à une étude des lieux, ainsi nous avons pu constater les zones a risque potentiel, ce qui montré en rouge sur la figure III-3, et en bleu les zonez intérieurs notamment le risque d'incidents est moins important que dans les zones extérieurs.

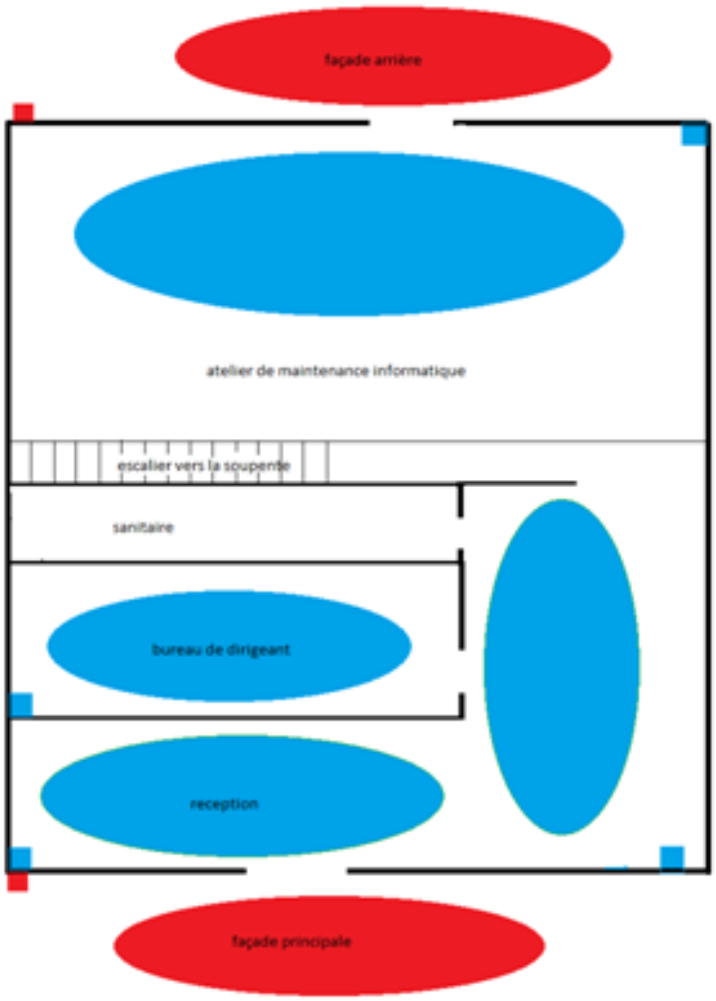

FIGURE 3.3 – Le deploiememt des caméras.

3.3.2 Configuration

Pour bien opérer le DVR afin qu'il soit pleinement fonctionnel, il y'a des paramètres debase qui doivent être définis :

1. La section Réseau : Elle regroupe plusieurs fonctionnalités tel que
   – L'adressage réseau : Il est d'ordinaire en DHCP mais peut également avoir une adresse statique sur le réseau.

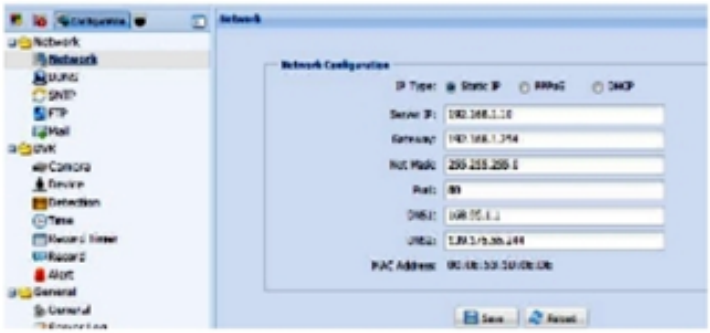

FIGURE 3.4 – La configuration réseau du DVR.

– La configuration FTP : Il est essentiel car outre son disque dur le DVR est capable d'effectuer des sauvegardes à distances. Ici on entre l'adresse du serveur FTP ainsi que les informationsde connexion.

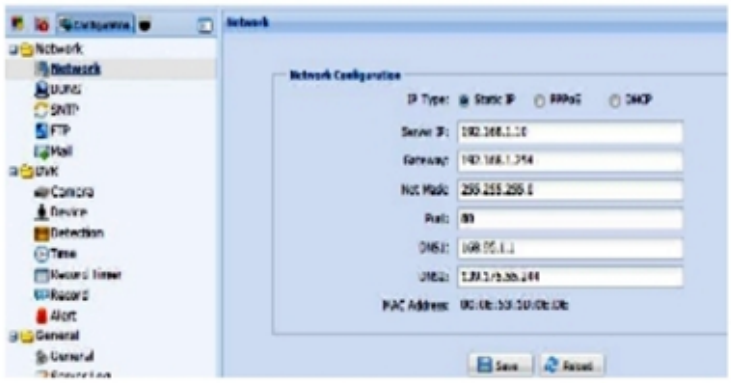

FIGURE 3.5 – La configuration FTP du DVR.

– La configuration Mail : Elle est utilisée lorsque le système doit envoyer d'alertes par mail à l'administrateur. Ici on entre les infos de connexion et le nom du serveur de messagerie.

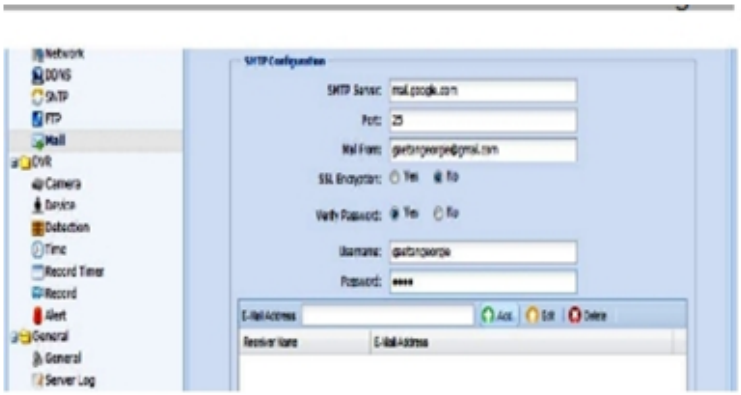

FIGURE 3.6 – La configuration mail du DVR.

2. la section utilisateur : Elle permet de créer et/ou de modifier des comptes d'utilisateurs pour se connecter au DVR. Chacun de ces comptes disposant d'un niveau de privilèges.

FIGURE 3.7 – la section utilisateur du DVR.

3.3.3 La Visualisation

Pour la visualisation on dispose de deuxmodes selon l'équipement utilisé :

– Le logiciel de visualisation VideoViewer de EagleEyes : Le logiciel VideoViewer est un logiciel gratuit distribue par EagleEyes, qui permet de visualiser les flux provenant d'un DVR sur le réseau et aussi d'enregistrer ces flux sur le disque dur de la machine locale. Pour pouvoir accéder au DVR à partir de VideoViewer il faut au préalable disposer d'un couple nom d'user/mot de passe existant sur le DVR. Ce logiciel peut s'installer aussi bien sur une machine Windows, une machine Unix, une machine MacOs, que sur un téléphone portable équipé de l'OS Symbian, Apple iOS, Androïd ou BlackBerry.

FIGURE 3.8 – La visualisation via une application de gestion vidéo.

– L'interface Web Pour pouvoir se connecter à l'interface Web comme avec VideoViewer, on doit disposer d'un compte utilisateur. Et comme pour VideoViewer l'interface varie selon le niveau de privilège de l'utilisateur.

FIGURE 3.9 – la visualisation via une interface web .

3.4 Enregistrement

Par défaut, l'enregistrement de tous les flux, venant de toutes les caméras, à toute heurede la journée, est fait directement sur le disque dur du DVR. Cependant, le DVR peut être configure pour ne faire des enregistrements sur son disque dur qu'a des moments cruciaux de la journée. Chaque utilisateur disposant du logiciel de gestion vidéo VideoViewer peut choisir de faire des enregistrements sur son disque dur à lui.

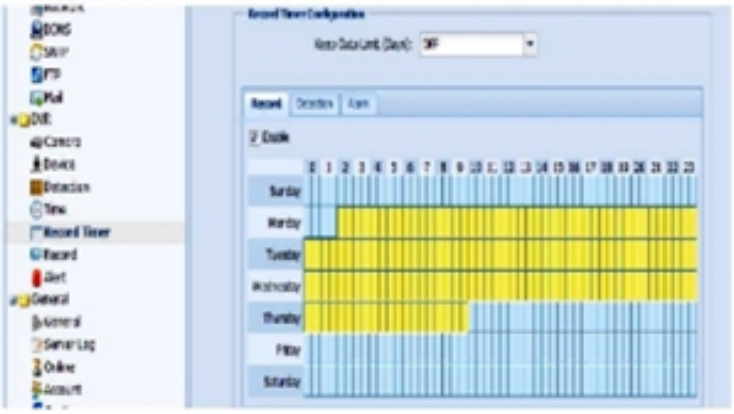

FIGURE 3.10 – la section d'enregistrement.

3.5 Conclusion

A l'issu de ce chapitre nous avons vu la démarche qui nous a permet de cerner le problème de sécurité chez CTIB, ainsi nous avons proposé une solution et nous avons procédé à l'ensemble des configurations afin d'opérer le mieux possible notre solution.

Nous déplorons le fait de n'avoir pas pu réaliser un système un peu plus évolué que celui que nous avons expérimenté en fin de projet ; Cela a cause d'une difficulté d'acquisition du matériel nécessaire et du fait que nous voulions plus axé notre projet sur une étude des systèmes de vidéosurveillance en général et de tous les paramètres qui interviennent.

Conclusion générale

La vidéosurveillance ne date pas d'aujourd'hui. Analogique à ses débuts, elle est de nos jours de plus en plus numérisée. L'avènement des réseaux IP à haut débit et la numérisation des images ouvrent la voie à une quantité d'applications innovantes et très performantes. L'industrie de la vidéosurveillance englobe aujourd'hui toute une variété de systèmes et d'équipements.

Nous tirons globalement de ce projet un bilan enrichissant, bien que nous ayons eu à faire face à certaines difficultés, alors que notre capacité à les résoudre et les méthodologies que nous avons employées pour les résoudre sont finalement du motif de satisfaction. De plus, la réalisation de ce projet nous a énormément aidés à acquérir l'esprit du travail en groupe et mettre en pratique quelques connaissances que nous avons acquises durant la formation théorique reçue durant notre parcours universitaire, qui s'est révélée adaptée aux compétences souhaitées.Vous avez donc pu constater qu'il est possible de réaliser un système de vidéosurveillance à distance sans forcément investir de grosses sommes d'argents dans du matériel onéreux comme des camera IP.

Toutefois, nous avons atteint notre objectif de réaliser un système de vidéosurveillance à distance, avec un mode d'utilisation simplifié pour l'utilisateur, cependant quelques améliorations restent possibles comme l'intégration des nouvelles technologies (logicielles et matérielle) qui vont augmente d'une part l'assistance à l'opérateur humain et en contre partie diminuer l'intervention de cedernier.Le système de vidéo surveillance doit évoluer de sa forme traditionnelle vers denouvelles formes qui intègrent des fonctionnalités additionnelles de traitement dedonnées, d'analyse et de décision.

Enfin nous souhaitons que ce travail ait une utilité quelconque pour les formateurs ou tout autre lecteur qui y trouveront certains renseignements qui pourront servir dans l'implémentation des systèmes de vidéosurveillance.

Bibliographie

[1] Kihm C. (2004), Vidéosurveillance, regard et identité : les modalités de la présence, pp.27-31.

[2] M. SERIAI Abdelhak-Djamel, Vidéo Surveillance à Distance..

[3] www.diapason-audiovisuel.com.

[4] Philippe MELCHIOR Président du Comité de pilotage stratégique du plan de développement de la vidéosurveillance page 79.

[5]http ://www.cnil.fr/dossiers/deplacements-transports/fiches-pratiques/article/videosurveillance-quelledeclaration- 3/.

[6] http ://www.cnil.fr/dossiers/videosurveillance/.

[7] Guide de la vidéosurveillance 2010 bosch.

[8] Alex Swanson, Head of Engineering IndigoVision Group plc The Edinburgh Technopole Bush Loan Edinburgh EH26 0PJ.

[9] www.indigovision.com.

[10] Le Goff T., Loudier-Malgouyres C.,Lavocat Ch., Dautheville M.,La vidéosurveillance dans les lycées en Île-de-France. Usages et impacts,Iaurif, août 2007.

[11] Projet transverse Groupe 100,Conception d'un système de vidéosurveillance intelligente pour l'IMT .

[12] http ://www.iau-idf.fr.

[13] Philippe Melchior (sous la dir.), La vidéosurveillance et la lutte contre le terrorisme, Note de synthèse,IGA, octobre 2005..

[14] Clive Norris et Garry Armstrong., The maximum surveillance society, The Rise of CCTV,1999.

[15] www.axis.com/request.

[16] http ://www.axis.com/fr/solutions/system/newold-network.htm.

[17]http ://www.axis.com/fr/solutions/system/ipsurveillance.htm.

Résumé

La vidéosurveillance ne date pas d'aujourdhuit mais elle existe depuis les années 40 ; elle est utilisée par la grande bretagne apres les ataque qu'elle a subi par des terroristes , afin d'observer tous acte non legitime..

La vidéosurveillance est une activité d'observation qui consiste à évaluer l'état opérationnel et fonctionnel d'un lieu. Elle permet de déminuer la problemes et le évenements malveillants.

Plusieurs approches de surveillance on été développées pour assurer le bon fonctionnement de cette derniere et offrire une meilleure utilisation meme a distance en utilisant la technologie IP .

Mots clés : *CCTV, IP.*