

Intelligent Video Surveillance: Promises and Challenges

Technological and Commercial Intelligence Report



Valérie Gouaillier
CRIM

Aude-Emmanuelle Fleurant
Technopôle Defence and Security

March 2009
Updated April 8, 2009

Centre de recherche informatique de Montréal

550 Sherbrooke Street West, Suite 100
Montréal, Québec H3A 1B9

Technopôle Defence and Security

Building 200, Office 106
South Site - DRDC Valcartier
2459 Pie-XI North Blvd
Québec, Québec G3J 1X5

This intelligence report was made possible
with the financial support of Industry Canada



and of the Ministère du Développement économique, de
l'Innovation et de l'Exportation du Québec, main funding partner
of the CRIM



Opening Remarks

The Centre de recherche informatique de Montréal (CRIM) and Technopôle Defence and Security are proud to present this intelligence report outlining intelligent video surveillance technology for the security of individuals and places, as well as the booming market it represents.

Over the past decade, the security of individuals and property, and the security of information have become major global issues. Faced with problems such as the fight against terrorism, enhanced national security and the rapid development of cybercrime, our societies are increasingly investing in protection. This sector therefore offers great opportunities for businesses, both with respect to technological development and services. Information and communications technologies in particular provide new and sophisticated solutions for physical and IT security.

Among the solutions proposed, video surveillance is one of the oldest and most widespread security technologies. Although still mostly analogical, it is undergoing a digital revolution with the ongoing transition to videos on IP networks. Sometimes integrating hundreds of cameras, these new systems create a huge amount of video information that cannot be processed only by security agent screen surveillance. To resolve this issue, intelligent video surveillance, by video analytic, can process the information by software analysis in order to keep only the data relevant to security.

Video surveillance is now at a turning point. What does the IP shift represent and what is the full potential of video analytics? This report is directed to a non-expert public and covers the main aspects of the issue: applications, the latest technology in video analytics, user needs, development and trends in this field, and main players in the video surveillance industry, especially in Quebec.

A point of convergence for ICT research conducted by the CRIM and security research conducted by Technopôle Defence and Security, intelligent video surveillance was a major platform for an initial joint report. For Quebec businesses and researchers specialized in ICT, this emerging sector offers new technological development and services opportunities that we had to define and distribute.

TDS contacted the CRIM for the monitoring based on its video surveillance expertise. CRIM's Vision and Imaging Team in the R&D Division has actually been involved in this sector since 2003, through different multi-partner mandates, including the following projects:

- *Monitoring of Extended Premises - Tracking Pedestrians Using a Network of Loosely Coupled Cameras (MONNET project)*. Implemented by the Vision and Digital Systems Laboratory of Université Laval, the purpose of this project was to develop an intelligent

vision system for monitoring people in public places. The CRIM team contributed with the face recognition and facial expressions module. This project was funded in part by the Precarn program aimed at university-driven research (PUL) and project won the Best Demo Award at the Precarn Annual IS-2005 Conference.

- *Intelligent Pan/Tilt/Zoom Camera for Security Applications (PTZ project)*. Implemented by VideoWave Networks, the purpose of this project was to develop an intelligent Pan/Tilt/Zoom camera for video surveillance software. The CRIM team was a partner in the development and implementation of object following and recognition algorithms. PTZ was funded in part by the Precarn-CRIM Alliance Program. This project won the OCTAS 2006 Technological Innovation Award given to both VideoWave Networks and the CRIM by Fédération de l'informatique du Québec.
- *Video Scene Understanding for the VST OneTrack System (VISU project)*. This project is designed to develop an advanced version of the intelligent scene analysis module developed as part of the PTZ project. The CRIM team is responsible for, among other things, developing and testing algorithms for pedestrian counting and for detecting abnormal car tire track situations. This project is also funded in part by the Precarn-CRIM Alliance Program.

Given the explosion of activities in the video surveillance sector, CRIM had been floating around the idea of moving forward with strategic monitoring since 2007. Thanks to funding from Industry Canada, TDS and CRIM were finally able to complete this report. .

We would like to extend our sincere thanks to each person who worked on this study and to our government partners. Your judicious contributions made this project possible.

Alain Fecteau
Chairman and CEO
Technopôle Defence and Security

Jacques Ouellet
Senior Vice-President, R & D Commercialization
CRIM

TABLE OF CONTENTS

OPENING REMARKS	3
TABLE OF CONTENTS	5
EXECUTIVE SUMMARY	9
INTRODUCTION	11
ACKNOWLEDGEMENTS	12
1. DEFINITION OF THE FIELD.....	14
1.1 Security	14
1.2 Video Surveillance.....	15
1.3 Intelligent Video Surveillance	17
1.3.1 Reasons for Using Intelligent Video Surveillance	17
1.3.2 Factors Determining the Choice of an Intelligent Video Surveillance System	19
2. SECTORS OF APPLICATION.....	19
2.1 Government and Public Security.....	20
2.2 Education	21
2.3 Retail Trade	21
2.4 Transportation.....	22
2.4.1 Airports.....	23
2.4.2 Stations and public transportation	23
2.4.3 Ports	24
2.5 Bank Setting.....	24
2.6 Gaming Industry and Casinos.....	24
2.7 Other.....	25
3. TECHNOLOGY	25
3.1 Architecture of Video Surveillance Systems	25
3.1.1 Components of a Video Surveillance System	25

3.1.1.1	Acquisition	25
3.1.1.2	Transmission	26
3.1.1.3	Compression.....	27
3.1.1.4	Processing.....	27
3.1.1.5	Archiving.....	28
3.1.1.6	Display.....	29
3.1.2	Evolution of Video Surveillance Systems	29
3.1.2.1	First Generation: Analogue	30
3.1.2.2	Second Generation: The Hybrid System	30
3.1.2.3	Third Generation: IP Digital.....	32
3.1.3	IP Video Surveillance.....	32
3.1.4	Architecture of an Intelligent Video Surveillance Network.....	34
3.1.4.1	Centralized Architecture.....	35
3.1.4.2	Distributed Architecture	35
3.2	Technological Status of Video Analytics	35
3.2.1	Description of Video Analytics Techniques.....	36
3.2.1.1	Detection of Changes	37
3.2.1.2	Tracking Objects	39
3.2.1.3	Classification and Identification of Objects	40
3.2.1.4	Classification of Activities and Behaviours	41
3.2.1.5	Crowd Analysis	42
3.2.1.6	Active Video Surveillance in Multi-Camera Systems	43
3.2.2	Analytics in Commercial Systems.....	44
3.2.3	Video Analytics Needs and Challenges	46
3.3	Technological Trends for Video Surveillance.....	49
4.	DESCRIPTION OF THE SECURITY AND VIDEO SURVEILLANCE MARKET	50
4.1	Global Security Market	50
4.2	Video Surveillance Market	52
4.2.1	Video Surveillance Market Driving Forces.....	53
4.2.2	Video Surveillance Market Inhibitors	53
4.2.3	The IP and Intelligent Video Surveillance Market.....	54
4.2.4	The Players	56
4.2.5	The Impact of the Recession on the Market.....	56
4.3	IP and Intelligent Video Surveillance Supply and Demand in Quebec.....	58
4.3.1	Demand.....	58
4.3.2	Supply.....	60
4.3.3	Recommendations for the Quebec Market.....	61

5. ISSUES	64
5.1 Protection of Privacy	64
5.2 Effectiveness of Video Surveillance in Reducing Crime	65
5.3 Standards for IP Video	67
BIBLIOGRAPHY	69
APPENDIX 1 - MAJOR RESEARCH PROGRAMS IN INTELLIGENT VIDEO SURVEILLANCE	77
APPENDIX 2 - RESEARCH GROUPS (QUEBEC AND THE U.S.).....	79
APPENDIX 3 - VIDEO SURVEILLANCE COMPANIES (QUEBEC AND ELSEWHERE)	81
APPENDIX 4 - COMPANIES SPECIALIZED IN VIDEO ANALYTICS SOFTWARE DESIGN	89
APPENDIX 5 - VIDEO SURVEILLANCE RESOURCES	96

TABLE OF FIGURES

<i>Figure 1 – Surveillance Cameras</i>	15
<i>Figure 2 – Human Monitor Controlling Several Screens</i>	18
<i>Figure 3 – Evolution of Video Surveillance Equipment</i>	29
<i>Figure 4 – Object Detection and Tracking</i>	36
<i>Figure 5 – Segmentation of an Individual in Video Footage</i>	38
<i>Figure 6 – Tracking of Object Trajectories on Video Footage</i>	40
<i>Figure 7 – Object Classification (Humans vs. Vehicles)</i>	40
<i>Figure 8 – License Plate Detection</i>	41
<i>Figure 9 – Table Taken from the Report on Plans and Priorities, 2005-2006 to 2008-2009</i>	51

EXECUTIVE SUMMARY

In existence for over 50 years, monitoring using closed-circuit television (CCTV) systems has undergone vast technological progress. This technological and commercial intelligence report takes stock of the most recent advance in the field: the shift to intelligent IP video surveillance.

The emergence of the first digital records about 20 years ago began a small revolution in video surveillance. Since then, although there is still a vast array of analogue equipment, CCTV networks are increasingly integrating digital components. Moreover, video surveillance is migrating towards computer networks, transmitting video by IP protocol, in an Intranet or the Internet. Although still primarily limited to institutional sectors (governments, controlling forces, transportation systems and educational institutions), IP video surveillance has surfaced as an irreversible trend for the future. The costs, computer and network configurations required for it currently prevent it from being adopted by smaller users.

However, surveillance cameras and archival images are on the rise. Intelligent software for processing and managing all of these security videos and that analyses camera images has been developed to detect and follow objects and report suspicious events. Still quite recent and unknown, this technology, called video analytics, offers the promise of better video surveillance. In physical security, the operating paradigm is increasingly shifting from post-incident investigation to prevention. Video analytics could become a solution in detecting suspicious situations in real time for immediate intervention. It also makes it possible to save on the bandwidth by only transmitting relevant surveillance data and improve search capabilities in archived footage.

Detection of movement, detection and tracking of objects, and face and license plate recognition under controlled conditions are currently well established techniques in video analytics. However, few systems are robust enough to deal with variations and unfavourable conditions of the environment (change in outdoor lighting, rain, snow, etc.) Recognizing objects and people in loaded scenes, identifying a person based on gait, recognizing complex behaviours and conducting analytics in multi-camera systems are among the main challenges of research in this field.

In the mid-term, key factors for intelligent IP video surveillance success could be 1) drop in costs; 2) a boom in megapixel cameras using effective compression techniques (e.g., H.264); and 3) greater availability of intelligent cameras, with improved analytical processing.

According to different studies, in 2007 the global video surveillance market generated estimated revenues between 7.25 billion and 14 billion dollars (US), which could grow to 46 billion in 2013. Likewise, growth and growth forecasts in the IP video surveillance sub-

sector are quite strong. Intelligent video surveillance constitutes in itself a niche industry that is just starting out, but which to develop in coming years. New applications, such as analyzing consumer behaviours and managing a company's operations, could accelerate the boom. Concern over protecting privacy, the undemonstrated effectiveness of video technologies in reducing crime, and current efforts to establish an IP video surveillance standard are factors that may have an impact on its use.

In Quebec, video surveillance is quite widespread in security and, like elsewhere, the institutional sector is converting over to IP technologies and certain analytical applications. There are several video surveillance suppliers, particularly distributors, installers and integrators, but few video management or analytics software designers. Genetec is a Quebec company that is blooming in this field since products in the Quebec market are mostly foreign.

The Quebec IT sector should benefit from the shift to IP video surveillance to develop new markets. In order to carve out a place in the highly competitive video surveillance industry, research companies and centres could take the intelligent turn by developing products in the video analytics niche.



INTRODUCTION

The goal of this technological and commercial intelligence report is to describe the intelligent video surveillance sector for the security of individuals and places. It is an emerging, little known technology that is changing how traditional video surveillance is used and is opening up a world of opportunities, making it possible to foresee new market segments emerging in the security sector.

This document, intended for a non-expert audience, discusses the ins and outs of this technology and tries to characterize the market it represents, not only globally, but more specifically in Quebec. It contains information on video surveillance technology, its application, shift to IP networks, leading-edge video analytic techniques applicable to it, its needs, the developments and trends in this field, the issues it raises, and the supply and demand it generates.

This report was drafted following a documentation search and consultation of 14 experts in video surveillance and security in Quebec: researchers, developers, integrators, installers, users and financial backers. It is divided into five chapters:

1. Definition of the field
2. Sectors of application
3. Technology
4. Description of the security and video surveillance market
5. Issues

Appendices 2, 3 and 4 list video analytics research groups and companies selling IP and intelligent video surveillance products and services. A description of major research programs that gave rise to the intelligent video surveillance sector, as well as a list of security and video surveillance resources are also provided.

ACKNOWLEDGEMENTS

We would like to thank the following people for their valuable collaboration on this report.

Jean-François Bédard, Information Technology Adviser

Innovation and Transfer Branch

Ministère du Développement économique, de l'Innovation et de l'Exportation

René Breyel, Chair

Claridion

Alain Janelle, Chair

VideoWave Networks Inc.

Daniel Jeanson, Chair and Sales Manager

SGPTI

Martin Joncas, Industrial Development Adviser

Computer Equipment and Instrumentation

Ministère du Développement économique, de l'Innovation et de l'Exportation

Kouame Kouacou, Division Manager

Main Directorate - Métro

Société de transport de Montréal

Frédéric Landry, Product Manager, Video Surveillance Applications

ImmerVision

Danielle Lapierre, Supervisor, Call Centre

Aéroports de Montréal

Denis Laurendeau, Full Professor

Vision and Digital Systems Laboratory

Université Laval

Alain Marchildon, Vice-President, Custom Panoramic Applications

ImmerVision

Yves Messier, Vice-President, Video Surveillance Applications

ImmerVision

François Pépin, Chief Operations

Airport Patrol, Aéroports de Montréal

André Petitclerc, Director Investments

Information and Communications Technologies Group

Société générale de financement du Québec

Jean-Pierre Picard, Marketing Analyst

Genetec

Ghyslain Proulx, TCPE Senior Project Engineer

Société de transport de Montréal

Louis Richer, Associate Director
Networking and Communications Service, Voice Technologies
Université McGill

1. DEFINITION OF THE FIELD

1.1 Security

Security includes two aspects: physical and logical security. Physical security *deals with physical measures taken to keep personnel safe, prevent all unauthorized access to equipment, installations, hardware and documents, and to protect them against espionage, sabotage, deterioration and theft*¹. It therefore covers the protection of individuals, property and places.

Logical security targets the protection of an organization's IT assets and focuses on implementing a set of security measures to ensure the confidentiality and integrity of *immaterial computer property and computer operations, and to protect them against any type of accidental or human threat. The term immaterial computer property refers to software, data and networks*². With the computerization and cybercrime it leads to, software security, although quite recent, is gaining importance.

Whereas physical security is usually managed by security staff (security officers, security guards, police services, etc.), logical security belongs to information technology specialists and computer system administrators. However, at a time when physical protection and surveillance are increasingly provided by computer technologies, physical and software security tend to converge.

In its application, security may be broken down into five functions: civil protection, prevention, intervention, investigation and recovery. Since the events of September 11, 2001, in the United States, there has been a noted paradigm shift in security. The prevention of potentially catastrophic events is more important than post-incident investigation. We look for methods and technologies that will help us detect suspicious events and prevent harm to people, properly, places and data.

In Canada, although the feeling of insecurity is not as strong as in the United States, fighting crime and reinforcing national security are still government priorities. The February 2008 federal budget set aside \$630 million over two years for law and order. The government also allocated \$145 million over two years to bolster border security. A series of measures to that effect, such as the electronic passport scheduled for 2001 and the use of biometrics for issuing visas, has been put in place. The Canadian government also announced that the National Defence budget will increase to a minimum of 1.5% per year by 2010-11.

¹ Grand dictionnaire terminologique de l'Office de la langue française du Québec.

² Idem.

Quebec has also affirmed its commitment to security. In its 2006-2009 action plan arising from the Quebec International Policy, the Quebec Ministry of International Relations raises the importance to contributing to Quebec's and the North American continent's security:

It is first by protecting the citizens on its territory, by working to preserve the free flow of discussion, by securing its strategic infrastructures and by ensuring that it does not become a source of threat to its partners that the Quebec government may best contribute to international security goals.³

1.2 Video Surveillance

Video surveillance is a segment of the physical security industry, which also includes access control, fire detection and control, the technical management of buildings, systems to ensure individual safety and the detection of intrusion.

Video surveillance consists of remotely monitoring public or private places, using mostly power-operated cameras that transmit the images taken to monitoring equipment that records or reproduces the images on a screen (Figure 1)⁴. It captures images of moving people in order to monitor comings and goings, prevent theft, assault and fraud, as well as manage incidents and crowd movements.⁵



Figure 1 – Surveillance Cameras

Although first used as far back as the 1950s, monitoring using closed-circuit television (CCTV) systems truly took off in the 1970s, especially in the United Kingdom, to fight against terrorist activities. The United Kingdom is currently the “most monitored” society with an estimated number of over 4 million surveillance cameras set up on its territory.

³ Ministère des Relations internationales du Québec,
http://www.mri.gouv.qc.ca/fr/politique_internationale/securite/index.asp.

⁴ Grand dictionnaire terminologique de l'Office de la langue française du Québec.

⁵ <http://fr.wikipedia.org/wiki/Vidéosurveillance>.

Video surveillance intensified during the 1990s, but exploded following the September 2001 attacks on the United States, then those in London in 2005.

Growing fear over terrorism is not the only factor for adopting video surveillance technology. This technology appears indispensable for monitoring operations and managing security incidents in public and private places. It is also an irreplaceable investigation tool for solving crimes, misdemeanours and disputes. However, it is not yet truly proven that video surveillance prevents security incidents or lowers crime rates.

A closed-circuit television (CCTV) network⁶ is a video system that transmits images in a closed loop. Once only analogue, CCTV networks now include digital components. Access to the communication network can be gained by Internet in certain cases. Only users with access rights to the network can access the information provided by the cameras.

The following constitute the security activities of a CCTV network⁷:

- Dissuasion
- Observation
- Surveillance
- Intelligence gathering
- Assessment of and response to a possible incident
- Assessment of and response an actual incident
- Forensic analysis after an incident
- Evidentiary, analysis after an incident

There are three types of video surveillance:

- Active: surveillance of an area to assist the on-site work of security officers or during emergency response.
- Passive: an employee monitors a small number of television screens while doing other tasks.
- Recording: makes it possible to collecting information for investigation and evidence purposes. Recordings are kept for a specific period of time, depending on needs and record keeping space.

⁶ CCTV in English.

⁷ Taken from [2].

1.3 Intelligent Video Surveillance

Video analytics⁸, also called intelligent video surveillance, is a technology that uses software to automatically identify specific objects, behaviours or attitudes in video footage. It transforms the video into data to be transmitted or archived so that the video surveillance system can act accordingly. It may involve activating a mobile camera in order to obtain more specific data about the scene or simply to send a warning to surveillance personnel so that a decision may be made on the proper intervention required.

Intelligent video surveillance systems use mathematical algorithms to detect moving objects in an image and filter non-relevant movements. They create a database that records the attributes of all the objects detected and their movement properties. Decisions are made by the system or events of interest are searched in archived footage based on rules (e.g., if a person oversteps a boundary, send an alert).

1.3.1 Reasons for Using Intelligent Video Surveillance

Today, video surveillance networks have a greater number of cameras. For large infrastructures, such as a mass transit system, over a thousand surveillance cameras may be deployed. These installations represent a huge amount of video to transmit, view and archive, making it impossible for a human monitor to analyze all of these video recordings in order to detect suspicious behaviour or events. This is especially true since security control centre personnel are also required to manage other tasks, such as access control, issuance of badges/keys/permits, handling emergency calls, following up on fire alarms, radio communications control, etc.

Several studies show the limits of human surveillance (Figure 2). After only 20 minutes of looking at and analyzing video surveillance screens, the attention of most people falls below an acceptable level⁹. A monitor cannot attentively follow 9 to 12 cameras for over 15 minutes¹⁰. Certain studies report that the ratio between the number of screens and the number of cameras can be between 1:4 and 1:78 in certain video surveillance networks¹¹. The probability of reacting immediately to an event captured by a surveillance camera

⁸ In English, the term *video analytics* is used to refer to the video analysis done specifically for video surveillance. In French, no term appears to be dedicated to this field, and it is sometimes referred to as “video analytics” or “video analysis”. For this report, we have chosen to use the neologism “Video analytics”. The terms *Intelligent video surveillance* or *smart video surveillance* are also used in English to describe this technology.

⁹ US National Institute of Justice study, quoted in [5].

¹⁰ ASIS International, quoted in [5].

¹¹ Kingston University study, quoted in [8].

network is estimated at 1 out of 1,000¹². That is why, historically, video surveillance is mainly a post-event investigation tool.



Figure 2 – Human Monitor watching several screens.

In this context, video analytics has many advantages:

- It operates 24/7.
- It can trigger an alarm that will be handled by a human operator or order the movement or zooming in of a camera for a more accurate surveillance of the event, thereby providing real time instead of post-event intervention.
- It reduces the bandwidth and archiving space needed by transmitting or recording only data on relevant events.
- It relieves security personnel from continuous surveillance.
- It enables a quick search of relevant events in the archived video footage.
- It makes it possible to identify objects in a scene and follow their activity (*situation awareness*).

Nevertheless, this is still new technology with many technical limits. For example, discriminating between usual and suspicious behaviour is a difficult problem for a machine to process. How can one distinguish between a person running because he/she is late or because he/she has just committed a crime?

In artificial intelligence, there is always a compromise between the recognition rate obtained and the number of false alarms. In the case of intelligent surveillance systems, the more permissive the detection threshold, the better the chances of detecting a real security threat, but more alarms will be triggered unnecessarily. Since each alarm must be assessed by a monitor, it is essential that false alarms be kept to a minimum to prevent surveillance

¹² CCTV Today (Nov. 2005), taken from [5].

personnel loss of time and productivity. This becomes a major performance challenge when the time comes to market video analytics technology.

1.3.2 Factors Determining the Choice of an Intelligent Video Surveillance System

- Recognition rate / false alarms.
- Percentage of cameras whose images will be computer analyzed.
- Nature of the scene to be monitored: video analytics is more appropriate for scenes with few changes, that are boring for a human monitor (risk of inattention), whereas a human monitor surpasses the machine for very active scenes, with many occlusions.
- Expandability: ability to add computer-supervised cameras or increase their percentage in the network.

2. SECTORS OF APPLICATION

Video surveillance was originally used by public services (police, transportation, administration). It was then adopted by companies looking to protect strategic assets, such as refineries, nuclear power plants, dams, agri-food plants and pharmaceutical complexes. Casinos also appear as pioneers in the deployment of large video surveillance systems. Today, surveillance cameras can be found in different public and private places, such as apartment buildings, shops, parking lots, railroad/bus stations, airports, roads, mass transit, banks, etc.

Video surveillance systems are deployed on different scales. For monitoring minor crimes (e.g., assaults, vandalism, theft), video surveillance is used primarily for post-incident investigation. This level of surveillance requires simple, often analogue technologies that do not involve video intelligence. This type of system can be found at the corner store, in small shops or in a private home.

Monitoring of apartment buildings or larger shops often requires a more extensive camera system. The goal of surveillance is mainly to monitor access paths, parking lots, and in the case of stores, departments and points of sale. Video surveillance is used in these locations mainly for investigation purposes. However, these users would like to obtain surveillance systems able to generate alerts in real time for immediate intervention. Video analytics products are therefore a breakthrough in these sectors. For this clientele, return on investment is a determining factor in buying intelligent video surveillance equipment.

Large-scale video surveillance is found in cities and neighbourhoods, transportation systems, university campuses, at major events (festivals, economic summits, Olympic games, etc.), with extensive security parameters. It requires dozens, even hundreds of cameras to be deployed. These cameras must sometimes be accessible to hundreds of security responders from different government agencies, police forces or emergency

services. In these facilities, video surveillance is in addition to a plethora security and monitoring systems: access control, fires, telephony, radio communications, geomatic systems, etc. Given the number of video cameras involved and the scale of the emergency interventions, these applications are particularly conducive to the use of video analytics for the automated processing of video flow generating alarms when suspicious events are noticed. Since budgets allocated to surveillance systems in these infrastructures are often vast, adding analytical software is more easily foreseeable there.

Video surveillance has recently begun to be used in mobile units, such as patrol cars, ambulances, buses, etc.; however, wireless video signal transmission to a security control centre may pose a problem.

2.1 Government and Public Security

The different levels of government must ensure the safety of the population and of public infrastructures. On the national level, it will be used, for example, to monitor the following:

- Sensitive infrastructures
- Borders
- Government buildings and sites
- Laboratories
- Military bases
- Prisons

Locally, video surveillance is set up in several cities around the world to monitor crimes and for use as an emergency intervention tool. It also helps to ensure security during large gatherings (shows, demonstrations, sporting events, etc.). London is the city the most often cited for the number of cameras deployed in its streets. Video surveillance is also used to manage parking, especially to monitor parking permits, the application of rules, the detection of theft, vandalism or misdemeanours, and to control access.

Video surveillance is widely used by controlling forces to conduct investigations, monitor people and vehicles sought, and detect dangerous or criminal activities. It can also be found on board patrol cars to verify police interventions.

Cameras can be increasingly found along stretches of road to monitor traffic and detect incidents, dangerous behaviour or violations. Montréal has a multi-camera system and

vehicle detection stations to follow traffic conditions in real time and automatically detect incidents¹³.

Many sectors of the government require intelligent video surveillance for: identifying individuals and vehicles, counting people and monitoring crowds, recognizing suspicious or violent behaviour (fights, misdemeanours), detecting intrusions, and monitoring roads. More advanced analyses, such as computer recognition of emotions or if an individual is telling a lie, are also anticipated.

2.2 Education

Video surveillance is increasingly found in academic institutions. It is used to oversee the safety of teachers and students, as well as to protect assets from vandalism and theft. Tragic school killings, such as at Columbine, in the US, and here in Quebec at Polytechnique and Collège Dawson, have highlighted the importance of monitoring school campuses more closely. These campuses may be extensive, especially in the case of universities, and be comprised of several buildings, accesses and parking lots to monitor. In this environment, video surveillance is used in particular to:

- monitor access to the institution's perimeter, which may be extensive, such as in the case of a university campus;
- monitor equipment and data;
- detect and follow acts of vandalism, theft, misdemeanours and inappropriate behaviour;
- recognize license plates;
- support criminal investigations;
- control access.

Since educational institutions often have an IP network infrastructure, it may be beneficial for them to set up digital video surveillance systems.

2.3 Retail Trade

Retail trade is a growing market for video surveillance, which is used for both internal (store, warehouse) and external (parking lot) security. Even the smallest shops have cameras to at least keep video evidence in case of theft or an incident. In chain stores, much more sophisticated video surveillance systems are set up for centralized monitoring of different locations. For the entire sector, video surveillance is aimed primarily at:

¹³ Transports Québec, http://www.mtq.gouv.qc.ca/portal/page/portal/regions/montreal_ile/gestion_circulation.

- monitoring registers and transactions (employee theft and fraud);
- protecting material goods and infrastructures;
- monitoring inventory and wares (deliveries);
- protecting staff and clients;
- controlling access to locked areas;
- checking emergency situations (fire, alarms, etc.);
- monitoring parking lots, vehicles, entries and exits.

Given the high risk of theft and attacks to which retailers are exposed, as well as the resulting significant losses, video surveillance becomes an essential tool for ensuring the security of employees and merchandise. This market also presents a real potential for video analytics. For example, there are systems that combine video information and data from the register to check that the items taken out by clients have indeed been invoiced. This technology also makes it possible to prevent fraud involving cashiers at points of sale.

Intelligent video surveillance is also increasingly used for non-security purposes, such as managing operations and market launch. In this context, video analytics is used in particular to count clients, analyze their behaviour and in-store movements, and compile statistics on consumer habits. For example, here in Quebec, the Quebec company Organix IT set up an intelligent video surveillance system in the Couche-Tard convenience store chain that offers these possibilities¹⁴.

2.4 Transportation

The security and smooth operation of airports, railroad/bus stations, ports and mass transit systems are critical for a country's economy. A security incident can seriously upset operations and result in significant losses. Given the large flows of passengers that use transportation systems and the extent of their infrastructures, these systems face extraordinary security challenges. Terrorist acts committed in different transportation systems around the world have exacerbated these challenges.

Analytical software targets the transportation sector by offering different adapted functions: detecting an intrusion in a controlled perimeter or area, detecting people entering an exit ramp, detecting abandoned luggage, recognizing faces, counting people, recognizing license plates for monitoring access to parking lots, detecting suspicious behaviour (loitering, vandalism, graffiti), detecting people in lanes. However, the transportation sector poses major technical challenges for intelligent video surveillance systems given the number of people who pass within the camera's field, the diversity of passenger behaviours and unfavourable conditions for cameras (vibrations, dust, etc.). Moreover, for outside

¹⁴ Intelligent Security Systems, <http://www.isscctv.com/company/publicity/1645/>.

monitoring, cameras and analytical algorithms must be able to operate despite changing weather conditions (fog, snow, rain, etc.)

2.4.1 Airports

Following the events of September 11, 2001, security measures were tightened, especially at large airports, and new technologies were deployed. For airports, the priority consists in controlling access to secure areas, in particular access to airplanes, and also in ensuring the safety of passengers, personnel and the property within the perimeter (runways, parking lots, access routes, etc.)

Based on the research done for this report, intelligent video surveillance is still little used in Canadian airports. For example, at the Pierre-Elliott Trudeau Airport in Montréal, video surveillance is used above all to assist with emergency interventions. When an incident is reported, a mobile camera pivots to follow the operations live from a security control centre. Access control is provided primarily by biometric identification technologies (fingerprints, iris recognition), the use of smart cards and PINs¹⁵. Video surveillance is archived and also used as evidence in police force investigations. It is also found on board patrol cars. Currently, cameras are mostly analogue and little video analytics is used. The intelligent functions already in place consist of counting people to assess, for example, processing times at customs, as well as for license plate recognition in order to take stock of vehicles in parking lots and to detect theft. Aéroports de Montréal will soon be adding a new component to its video surveillance system that will be entirely IP and include intelligent cameras and video processing software.

2.4.2 Stations and Public Transportation

The purpose of video surveillance in railroad/bus stations and public transportation is mainly to monitor access routes, platforms, rails and tunnels, parking lots and all auxiliary service structures. It is connected to other access monitoring systems and security devices to oversee the protection of passengers, personnel and infrastructures. The video is viewed live from the security control centre, or at a later time for investigations following security incidents.

In Quebec, thanks to contributions from two levels of government, Société de transport de Montréal (STM) is pursuing the deployment of over 1,600 cameras in the infrastructures of the Montréal subway system to increase user security. Cameras can also be found on certain buses of the system as a prototype. Société de transport de Laval will also install surveillance cameras in some of its buses to discourage vandalism¹⁶. The new subway

¹⁵ Personal Identification Number.

¹⁶ Morissette, H., *Des caméras seront installées dans les autobus de Laval*, 24 heures, 3 December 2008, p. 6.

system, entirely on an IP network, is an IP video surveillance flagship project in Quebec. Controlled centrally, the video surveillance system is connected to the different monitoring and maintenance systems. The STM has begun to deploy video analytics for automated detection of people on the tracks and states that it is one of the first in Canada to use intelligent video in its mass transit. In this field, Canadian public transportation systems are behind those of European countries, such as the United Kingdom, France and Germany, which have much better video surveillance systems. In the long term, if using video analytics proves effective, the STM anticipates some other applications for it, such as detecting suspicious packages, monitoring doors and recognizing suspicious behaviour.

2.4.3 Ports

As for other transportation systems, in ports, intelligent video surveillance is used to protect passengers and personnel, to monitor comings and goings in the perimeter and to identify vehicles in this perimeter. However, ports pose a specific challenge for video analytics because they require the monitoring of the adjacent waters. Reflections on water and wave movement are environmental variations that may disrupt analytical algorithms, especially for the detection of movement.

2.5 Bank Setting

Video surveillance is widely used for bank security. The presence of cameras first acts as a deterrent to committing armed robbery and assault. Should a crime occur, archived video footage is used to investigate and identify the perpetrators.

Automated bank machines are prime targets for criminal acts. Surveillance cameras help to detect fraud, such as, for example, the installation of a device to read the magnetic information on bank cards.

In a bank setting, intelligent video surveillance can increase monitoring effectiveness. It provides for monitoring of all branches in order to detect suspicious individuals or behaviour. It also makes it possible to find, among other things, all video footage from all branches where a certain individual appears using face recognition techniques.

2.6 Gaming Industry and Casinos

Casinos and gaming centres have long used video surveillance to protect clients and premises, as well as to detect cheating, heists, cash register theft and other crimes resulting in losses. It has also been used as evidence to assess the validity of actions for damages against the gaming institution.

Since casino monitoring requires watching the behaviour of many people in a crowded environment, intelligent video surveillance is an interesting way of helping security personnel do their job. Face and gesture detection and recognition are part of the useful analytical functionalities for this environment.

2.7 Other

Video surveillance is used in many other environments, such as in stores and to monitor buildings. It is most often used to film access routes and parking lots, monitor material valuables and ensure employee and client protection.

Video surveillance can also be used in healthcare to help with interventions. It can even be found in ambulances and used in combination with other measuring instruments to monitor a patient remotely. The American company IndigoVision has developed analytical solutions installed on intelligent cameras specifically to detect the movement of helicopters landing on the site of an American hospital.

The consumer market is also developing. More and more home video surveillance systems are being sold, even in non-specialized stores. Cameras now complement the different monitoring and security devices for the residential sector.

3. TECHNOLOGY

3.1 Architecture of Video Surveillance Systems

3.1.1 Components of a Video Surveillance System

This section briefly describes the different hardware and software components of video surveillance systems. A more detailed description of the infrastructure of video surveillance systems and the principles guiding the choice of hardware can be found in numerous reference books and guides, including [1] and [20].

3.1.1.1 Acquisition

There is a whole array of camera models to meet different monitoring needs. They are analogue and digital, and can be power-operated or not. The following are, more specifically, the types of cameras found.

- **Fixed:** Pointed in a single direction, it covers a defined area (entrance, part of a parking lot, etc.). It is the traditional surveillance camera. It is an excellent choice if the goal is to have the camera and its monitoring direction be visible.
- **PTZ (Pan-Tilt-Zoom):** Power-operated, it can be manually or automatically activated for pan/tilt/zoom movements. It is used to follow objects or individuals moving along the scene or to zoom into areas of interest, such as a license plate.
- **Dome:** Covered by a hemispheric case, making it discrete and, in certain models, vandalism and weatherproof. It can be fixed or mobile. The power-operated versions cover a very vast area using 360° horizontal sweep and 180° vertical sweep. Although in guard tour mode it can replace ten fixed cameras by sweeping the area to be monitored, it only observes a single direction at a time.
- **Megapixel:** Offers a higher resolution than standard cameras, ranging from 1 to 16 megapixels¹⁷. It makes it possible to either capture a more detailed image or cover a wider visual field, reducing the number of cameras needed to cover an area to be monitored. When used with a wide angle, it has a viewing space generally ranging from 140° to 360°. It offers the possibility of zooming into the picture using the software, making it an alternative to the PTZ mechanical camera, whose parts are subject to wear. Its high resolution helps to improve the performance of the detection and recognition algorithms requiring a high level of detail, such as license plates and face recognition.
- **Infrared and thermal:** Sensitive to infrared radiation (IR), it can produce a good quality image in the dark for night monitoring. At night, it films in black and white, but can produce a colour image during the day. Some infrared cameras are equipped with their own source of IR light, which turns on when lighting levels drop below a certain threshold. Separate IR projectors (lamp or LED¹⁸) can also be used. Thermal cameras record the thermal radiation given off by objects and do not require any source of lighting.
- **Panoramic:** Special optics provide it with 360° visibility with a single camera¹⁹ and virtual PTZ in the image. The main panoramic technologies for monitoring are fisheye, mirror lens and panomorphic lens. However, the resolution of these cameras is often not enough for analyses requiring a high level of detail.

3.1.1.2 Transmission

The video captured by surveillance cameras must be sent to the recording, processing and viewing systems. This transmission can be done by cable (coaxial or fibre optic cables, stranded copper wire) or by air (infrared signals, radio transmission).

Wired video is the most predominant in video surveillance systems. It offers greater bandwidth and better reliability than wireless connections, at a lower cost. However,

¹⁷ In 2008, represented only 4% of cameras sold, but sales are increasing quickly.

¹⁸ *Light Emitting Diodes.*

¹⁹ ImmerVision and Grandeye develop two major panoramic surveillance technologies.

wireless video transmission is sometimes the best solution, for example when monitoring large perimeters where installing cables would be too costly, or when the areas to be monitored cannot be reached by cable.

Whether wired or wireless, the video signal can be analogue or digital. Most video transmissions for surveillance are currently still **analogue**. However, computer networks (LAN, WAN or Internet) are increasingly used to send video using the **IP protocol**. IP cameras can be directly connected on these networks, whereas the video flow coming from analogue cameras must first be digitized by an **encoder**, also called a **video server**, in order to pass through the IP networks.

3.1.1.3 Compression

Digitized video represents a large quantity of data to be transmitted and archived. Sending video footage may require up to 165 megabits of bandwidth, and the video of a single camera over one day may fill 7 GB of disk space. That is why surveillance video must be compressed using **codecs**²⁰, algorithms for reducing the amount of data by deleting redundancies, by image or between footage frames, as well as details that cannot be seen by a human eye.

Depending on the type of compression needed, videocoding-decoding can be fairly processor intensive. Therefore, there must be a compromise between the compression ratio and the processor resources used.

There are two major groups of international compression standards: JPEG, created by the Joint Photographic Experts Group, and MPEG, developed by the Moving Photographic Experts Group. The first group includes JPEG formats for still frames, and MJPEG for video footage. The second group includes the MPEG-1, MPEG-2, MPEG-4 and H.264 formats²¹.

Currently, MJPEG and MPEG-4 are the most widely used standards in video surveillance. However, with the improvements to quality and efficiency (compression ratio, latency, error resistance) it brings, H.264 should soon replace MPEG-4. Without affecting image quality, the H.264 encoder makes it possible to reduce image size by over 80% in relation to MJPEG, and by 50% in relation to MPEG-4 compression [15].

3.1.1.4 Processing

Video management systems process video surveillance images, such as managing different video flows, and viewing, recording, analyzing and searching recorded footage. There are four major categories of video management systems.

²⁰ Contraction of coder-decoder.

²¹ Common name for MPEG-4 Part 10 AVC/H.264.

- **Digital Video Recorder (DVR²²)**: Device with an internal hard disk for digital recording of video and built-in video processing software. It accepts only flows from analogue cameras, which it digitizes. Recent models make it possible to view the video remotely on computer. Still quite widespread, it is slowly being replaced by systems that support IP video from end to end.
- **Hybrid Digital Video Recorder (HDVR²³)**: Similar to the digital recorder, but accepts connections from both analogue and IP cameras. Several types of digital video recorders can be made hybrid by installing a software application.
- **Network Video Recorder (NVR²⁴)**: Designed for video surveillance IP network architectures, it can only process video signals from IP cameras or encoders.
- **IP video surveillance software**: Purely software-based solution for managing video on an IP network. For surveillance systems with few cameras, a Web browser may be enough to manage the video. For larger video surveillance networks, a dedicated video management software application must be used, which is installed on a PC or server. Although more complicated to install due to the required server configurations, it offers greater flexibility with respect to choice and the addition of video surveillance network parts. IP video surveillance software applications are a major trend in video management, especially in infrastructures with large numbers of cameras. Open platforms allow for easy integration of cameras and hardware components from different manufacturers.

3.1.1.5 Archiving

The video footage archiving period varies depending on surveillance needs, ranging from a few days to a few years. On average, organizations keep video evidence from 30 to 90 days. The deployment of vast networks of cameras and the use of high resolution video surveillance resulted in an explosion in demand for storage systems. Although the cost of storage media has dropped considerably in recent years, archiving is often a large part of video surveillance infrastructure expenses due to the growing amount of video data to be stored.

There are two types of storage solutions:

- **Internal**: Hard drives built into digital video recorders or servers are the most widespread type of archiving, offering up to 4 TB of space. Some IP cameras even come with a memory card or USB drive for hours, even days of video recording. Internal archiving solutions are well suited for medium size video surveillance systems comprised of up to 50 cameras.
- **Attached**: Archiving is done on devices external to the video recorders or servers. NAS (*Network Attached Storage*) or SAN (*Storage Area Network*) type systems offer shared

²² *Digital Video Recorder.*

²³ *Hybrid Digital Video Recorder.*

²⁴ *Network Video Recorder.*

storage space between different network clients. On a NAS network storage system, a file is archived on the same hard drive, whereas with the SAN storage network, a file can be saved in fragments distributed over several storage media. These attached archiving solutions are particularly well suited to large video surveillance networks with a large number of cameras²⁵. Although more expensive than internal archiving systems, these attached solutions are superior in terms of expandability, flexibility and redundancy.

3.1.1.6 Display

A large part of video captured by surveillance cameras is never viewed, but simply archived in case viewing is required following an incident. Traditionally, video surveillance has been used mainly as an investigation tool. However, in several cases, security officers view images from surveillance cameras in real time. Without necessarily watching the entire video captured, officers can periodically review different video sources.

Video surveillance can be viewed on different devices. In small facilities, the video can be viewed directly on the recorder, as the image is being recorded. Images are generally viewed remotely, on a computer, or on a mobile device such as a telephone or handheld device.

Large security operations centres that supervise hundreds of cameras often use a wall of video screens, which provide a large viewing space and allow for different video flows to be displayed.

3.1.2 Evolution of Video Surveillance Systems

Digital transition in video surveillance occurred in several steps. It began with the appearance of the digital recorder, then continued with a complete overhaul of the IP infrastructure, with video being transmitted over an intranet or Internet network from the camera to the viewing screen. Many hybrid systems took shape during this shift, integrating analogue and digital components. The figure below describes the important milestones that marked the evolution towards intelligent video surveillance on the IP network.

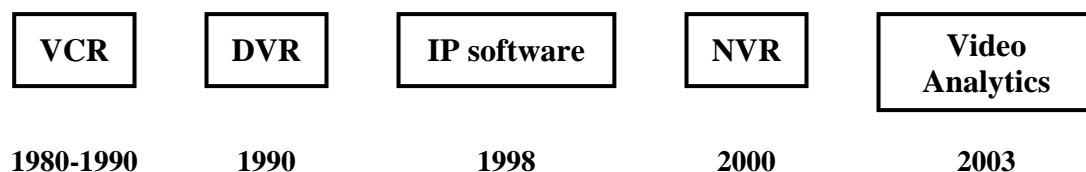


Figure 3 – Evolution of Video Surveillance Hardware

²⁵ For example, IPVideoMarket.info recommends using storage clusters for networks with over 48 analogue cameras or more than six megapixel cameras.
http://ipvideomarket.info/report/examining_the_future_of_video_surveillance_storage

3.1.2.1 First Generation: Analogue

In the traditional analogue CCTV network, analogue cameras are connected by coaxial cables (one cable per camera) to surveillance screens and, for archiving purposes, to a videotape recorder that records the video on cassette. A multiplexer may be used to group together video flows from several cameras into a single aggregate signal that is forwarded to a videotape recorder or an analogue monitor. It makes it possible to display four, nine or 16 video signals on the same screen or to record them on the same archiving system. There is no compression done for the video signals. With a videotape recorder designed for this purpose, recording at reduced frame rate helps to save space on the videotape, as required for surveillance purposes²⁶.

- Pros
 - Analogue systems are very reliable
 - Simple to use and do not require computer skills.
- Cons
 - Video quality is inferior to digital system quality.
 - The cassettes need to be changed frequently (every three days or more).
 - Requires regular cleaning and maintenance of the videotape recorders.
 - Recorded video quality deteriorates over time.
 - Cannot be viewed remotely, as on digital networks.
 - They are proprietary systems.

3.1.2.2 Second Generation: The Hybrid System

Replacing the videotape recorder with a digital recorder (DVR) was the first step in the digital transition of video surveillance. Digital recorders made their appearance in the 90s and store video on hard drives. Since they often have several video inlets, the digital recorder replaced both the multiplexer and the analogue videotape recorder.

Recent models have an Ethernet port for connection to a network and remote access to the video, either in real time or from a recording. Videos are transmitted by IP protocol from a digital recorder. They enable transmission to a hybrid video surveillance system on IP network, while maintaining the analogue cameras. The hybrid digital video recorder (HDVR) can receive video flow from both analogue and IP cameras. It is an effective solution for modernizing a video surveillance system by taking advantage of new IP cameras while keeping existing analogue cameras in place. Although it is estimated that 95% of cameras are still analogue, digital recorders and hybrid digital recorders are quite widespread technologies.

²⁶ *Time lapse mode* for recording at 15 fps (*frame per second*), 7.5 fps, 3.75 fps and 1.875 fps.

- Pros
 - No cassette to change.
 - The archived video is of better quality and does not deteriorate over time.
 - Quick search of video recordings possible.
 - Remote video surveillance and system operation from a PC.
- Cons
 - Concentration of digitization, video compression, recording and networking tasks in the same unit.
 - Digital video recorders are proprietary system, which increases maintenance and upgrading costs.
 - The number of digital recording video inputs (often a multiple of 16) limits the addition of cameras.

Video encoders, also called video servers, are used to convert signals from analogue cameras and transmit them in IP flow to a network through a switch. While retaining the analogue cameras, they enable a practically complete shift to the network infrastructure for video surveillance since the video is constantly transmitted by IP protocol through the network.

Video encoders may be used with network video recorders (NVR). These can only process and record IP video flow. They are offered on an open platform (a computer with video management software) or in dedicated proprietary equipment. In this latter form, the network video recorder is compared to a hybrid digital recorder that requires encoders to operate with analogue cameras.

- Pros
 - Use of standard network computers and hardware for video recording and management.
 - Possibility of recording outside the site to be monitored (e.g., centralization of recordings).
 - Distributed architecture that offers flexibility, scalability (one camera can be added at a time) and redundancy (in case of breakdown or failure).
- Cons
 - Take up a lot of bandwidth if the recording is done outside the site to be monitored (e.g., centralized).
 - If there is a network failure, the recording may be interrupted.
 - If centralized recording is not required, the use of network video recorders is often more costly than digital recorders.

- Require complex calculations to determine the amount of video flow that can be handled by the server, the amount of disk space needed for recording, frame rates, compression level and other factors associated with network capacity.

3.1.2.3 Third Generation: IP Digital

Strictly speaking, a video surveillance system is completely IP when all of its components are digital and all transmissions are done by IP protocol. These networks therefore have network cameras, also called IP cameras, which have their own built-in encoder. They are connected, via network switches, to servers (PCs) equipped with video management software. Recording is done on a server or on proprietary network video recorders. Processing is done on the server or in the peripheral equipment. However, many people feel that a video surveillance system whose video is transmitted by IP protocol from encoders is an IP network system. In these systems, the cameras may be analogue provided they are connected to encoders.

More information on IP video surveillance, and particularly on its pros and cons, is provided in the following section.

3.1.3 IP Video Surveillance

For the past two years, the video surveillance market has been migrating from analogue video to IP video. This boom in network video surveillance is bolstered by processor enhancements, low storage costs and improved compression algorithms.

Although this transition exists, it is merely at the beginning stages and it is difficult to predict the rate at which the move to IP will take over analogue technologies in video surveillance. Cameras continue to resist. In fact, it is estimated that 95% of the 40 million cameras installed around the world are still analogue [1]. Moreover, today only one buyer in four chooses IP cameras²⁷. However, IP cameras offer technical advantages over analogue cameras, such as better image quality, higher resolution and onboard intelligence. The high cost of IP cameras, about twice as much as analogue cameras, is the main deterrent. With the improvements made by manufacturers to video recorders and the existence of hybrid video recorders, the reign of analogue cameras could be extended by a few more years.

The last general video surveillance IP networks have the following features:

- They are completely digital: cameras, networks, recording, access.
- They can include different types of cameras: intelligent, megapixel, wireless, PTZ, panoramic, etc.

²⁷ IP Video Market Info, 2009.

- They have non-proprietary hardware.
- They operate with distributed and multiplatform servers.
- Backup is done on the network (NVR).
- Can be accessed remotely, from anywhere, at any time, either from a control centre, by Internet or a LAN or WAN network, on a cell phone or personal digital assistant, etc.
- May include video analytics.

Video surveillance in IP network offers numerous advantages. It is based on a more flexible infrastructure than analogue video, combining wired and wireless transmission. Moreover, the network infrastructure is fast and easily expandable. There is no limit to the number of cameras that may be added to it. Given that current systems can be comprised of between 400 and 500 cameras, compared to 25 to 30 four years ago, the fact that the video surveillance network can be easily expanded is very attractive when thinking about setting up a new system.

For extensive installations with vast distances between cameras and the recording systems, IP cameras are advantageous because coaxial cable costs are quite high. That is why IP cameras are used primarily for monitoring institutions, such as academic buildings, large company campuses, municipalities and military bases.

IP cameras have many technical benefits. For example, IP megapixel cameras offer undeniable advantages with respect to video surveillance. The resolution of these cameras is significantly superior to the resolution of analogue cameras and can therefore solve more crimes. Although costly, a single megapixel camera can often replace several cameras. Intelligent cameras, with built-in processors, provide technical enhancements to new generation video surveillance systems. They make it possible to distribute calculations for video analytics processing and, therefore, save on bandwidth by transmitting only security relevant data.

The open architecture of IP video surveillance networks makes it possible to use hardware from different manufacturers, and therefore to select the most adapted parts for the surveillance application. Furthermore, the IP architecture makes it easy to integrate different security systems (video, fire alarms, access control, etc.)

The configuration of these networks with redundancy, both with respect to transmission and archiving, provides for better reliability. In an entirely analogue network, a camera or recorder malfunction may mean definitive video loss. Moreover, network archiving, which is becoming increasingly less expensive, makes it possible to save years of video rather than a few days or weeks with videotape recorders or digital recorders by merely adding on hard drives to increase storage capacity.

In these networks, digital transmission of the video, from system end to end, reduces losses in quality caused by analogue to digital conversion. Moreover, intelligent software processing makes it possible to filter relevant events in the video and transmit only the

metadata describing them, thereby saving on bandwidth. These metadata are then used to index the video content for more efficient searches in the captured footage. With these networks, it is also possible to send orders to the cameras, depending on the video processed. For example, in response to a suspicious incident, the video management software may automatically activate the optical or digital zoom on a network camera for a more accurate monitoring of the situation.

There are also many drawbacks to the shift to IP video surveillance. For example, in the case of existing analogue infrastructures, rewiring the entire network may be quite costly. In this case, using encoders to digitize analogue signals will make it possible to keep the cameras in place and set up a hybrid network. Digital recorder technology has also greatly progressed in order to remain competitive. Digital recorders now offer many advantages that are comparable to IP network technologies: remote access, ability to manage a large number of cameras, integration with other systems (access control, intrusion detection, points of sale systems, etc.) and analytical ability. For small video surveillance installations, using analogue cameras with digital recorders offers excellent performance at lower costs than IP video.

Although, from a technological point of view, IP video surveillance networks offer numerous advantages, setting up these networks poses certain organizational problems. The first is with respect to installation. Most video surveillance integrators and installers work in the physical security sector. Yet, installing IP network video surveillance systems requires IT and especially networking skills. Few video surveillance integrators and installers are specialized in this field.

The second problem is with respect to managing these systems. Once installed, who in the organization is responsible for the video surveillance system? The physical security personnel or computer services? The existing uncertainty surrounding this issue in organizations often results in delays shifting to IP video surveillance.

Finally, shifting from a closed-circuit television network to a video surveillance system, whose data run through Ethernet or Internet networks, raises computer security issues. Proper security mechanisms must obviously be put in place to protect the surveillance video. Also, proper video surveillance becomes dependent on the network's reliability. In that respect, video surveillance integration on IP networks may follow that of IP telephony, which is now widespread.

3.1.4 Architecture of an Intelligent Video Surveillance Network

Intelligent video surveillance systems may be set up according to two large types of architecture: centralized or distributed. Both perform intelligent processing to extract data from video images and may, if required, order a PTZ camera to move for active monitoring.

3.1.4.1 Centralized Architecture

With centralized architecture, all intelligent processing is concentrated in the same place. In traditional systems, it is the digital recorder that collects all video flow for analyzing. For network infrastructure, it is the computer server (a PC) that will perform analytical processing.

Video analysis requires vast computing power, which monopolizes a large part of the processor's resources. Since they must also manage encoding, recording and viewing of video flow, digital recorders and servers can only carry out video analytics tasks on a limited number of cameras.

Moreover, in the case of video surveillance systems on network, transmitting all video flow to a centralized point takes up a lot of bandwidth. The computer network must be able to handle this traffic.

3.1.4.2 Distributed Architecture

As the name indicates, distributed architecture distributes intelligent processing to the different nodes of the video surveillance system. This way, the calculations required for analytics can be done on peripheral equipment, on intelligent cameras with processors, encoders or in the network switches. With this architecture, rather than sending video flow to the digital recorder or a central computer, only metadata extracted from the video are transmitted. The intelligence can also be shared between the peripheral equipment and the central processing unit.

This infrastructure helps to reduce wiring costs and the bandwidth required in the video surveillance network. It also offers better scalability, since adding cameras is not necessarily limited by the digital recorder's or the server's computing power.

3.2 Technological Status of Video Analytics

Video analytics and intelligent video surveillance are very active fields of research. Over the past ten years in particular, several conferences, special editions of magazines and articles have been dedicated to this. A few commercial products have been developed following the research done in this sector. Major projects funded by governments, such as VSAM in the United States, and PRISMATICA in Europe, have encouraged the development of object detection, tracking and recognition techniques based on video footage.

However, these are emerging technologies, and their use in large-scale applications are still recent and marginal. The cost of these technologies and their current technical limits in monitoring complex environments is an obstacle to more widespread adoption.

This section describes the technological advances made in intelligent video surveillance. It discusses the main analyses that video analytics software can perform and provides a brief description of the functionalities currently implemented in commercial systems, or that are being developed in research laboratories. A list of the main challenges these technologies are facing, as well as current and future needs anticipated by users, is also included.

A more in-depth review of the different procedures and intelligent video analysis algorithms, as well as a more extensive bibliography on the subject can be found in the scientific publications [8, 9, 10, 11, 12, 14].

3.2.1 Description of Video Analytics Techniques

Video analytics consists of computer-assisted reproduction of the analysis that a human would do looking at the video footage from the surveillance cameras. The analytics software processes video flow images to automatically detect objects (people, equipment, vehicles) and events of interest for security purposes. Once detected, the objects can be identified, monitored and located (Figure 4). Their actions and interactions are analyzed and classified in order to interpret the activity of a scene and bring it to the attention of a human operator.

Video analytics software applications are used in two modes: real and non-real time. In real time, they detect situations in the video flow that represent a security threat and trigger an alarm. In non-real time, they make it possible to quickly find video footage on an incident under investigation.

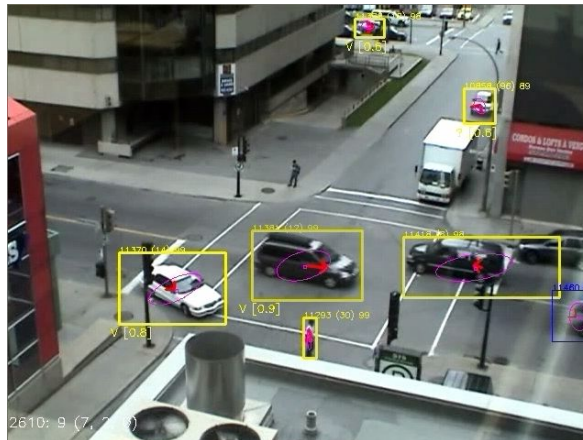


Figure 4 – Object Detection and Tracking

Real time alerts: Most alerts are defined by the intelligent video surveillance system user. They may be generic alerts, such as detecting an abandoned object or an item in the scene moving over a set speed limit. To trigger these alarms, only the properties of the object

movements are analyzed by the system. More specific alerts may be issued after the objects or their movement have been classified (e.g., discrimination between the passage of a human or animal in an outside area). Behaviour-related alerts based on conformity or non-conformity with a behaviour model entered in the system (e.g., an individual trying to open more than one car in a parking lot), constitute pre-defined alerts.

Certain real-time alerts are automatically identified. Over time, the system learns a model of activity and ends up detecting non-standard activities. For example, an analytics software may learn that vehicles drive on the street and pedestrians walk on the sidewalk. The opposite may trigger an alarm.

Video search for investigation: Analytics processing makes it possible to index video content based on characteristics such as the shape of objects, their size, appearance, trajectory, type, as well as their model of activity. Stored as metadata, this information makes it possible to conduct spatiotemporal searches such as “find all footage with a person dressed in red passing in front of a certain building between two given dates”.

The analytical functions developed for video surveillance systems have different levels of analysis. Hierarchically, they are executed at the pixel and object level to achieve the behaviour scale. They are grouped according to the following tasks:

1. Detection of changes
2. Segmentation of moving objects
3. Monitoring of objects
4. Classification and identification of objects
5. Classification of activities and behaviours

3.2.1.1 Detection of Changes

In video surveillance, detecting changes in video footage is the basis for all intelligent analysis. It may detect an activity in a scene under surveillance, in particular the movement of objects. It may also reveal the appearance or disappearance of an object (abandoned or stolen object). It is also used to automatically report accidental or intentional alterations in a camera: obstructions (dust, spider webs, moisture, paint, stickers), reorientation, blurriness.

Many techniques for detecting movements used in video analytics are based on detecting changes. However, detecting changes in video footage does not specifically target the movement of objects, but may highlight an image modulation. In order to segment²⁸ moving objects, we must be able to discriminate between fluctuations in pixel value

²⁸ Segmentation consists in separating objects from the background.

corresponding to consistent movements and fluctuations caused by environmental changes (Figure 5).



Figure 5 - Segmentation of an individual in video footage

This is a major problem in video analytics because complex environments may present many, sometimes sudden variations: change in lighting (shadows, movement of the sun, clouds, mirror reflections in glass or on water, glare caused by sources of light in the scene), non-relevant movements (flag flapping in the wind, waves on water). That is why many analytical methods work well indoors, in scenes with little movement. Algorithms that are robust enough to be applied in uncontrolled settings are much rarer.

Several movement segmentation techniques have been proposed.

Subtraction of the background: In its most primitive form, detecting changes comes down to finding, pixel by pixel, differences in colour or texture between the images of a sequence. A first category of techniques consists in comparing each frame of a sequence to a reference image, called the background, which represents the undisturbed scene. The areas of change are formed of pixels with a difference in intensity that is above a threshold. Pixel-by-pixel subtraction between two images is very sensitive to the slightest environmental change, such as changes in lighting and movements inherent to a scene (e.g., the foliage of a tree blowing in the wind). In order to offset this problem, certain techniques continually adapt the background model to intrinsic changes in the environment²⁹. The difference with the background is a method that is particularly suited to indoor environments, where lighting conditions are controlled and where there is little activity (e.g., monitoring a hallway).

Time-based difference: A second class of methods for detecting change is based on a time difference between a few consecutive frames. These frames adapt to variations in the time of the environment. On the other hand, they tend to oversee certain variations related to the movement of objects in the scene, especially if they move slowly. They often produce holes in the objects detected. These techniques therefore require smoothing treatment, with

²⁹ For example, using a Kalman filter [9].

morphological operators and filtering of holes and shapes that are too small. In order to retain only significant movements and eliminate occasional movements, certain techniques draw up a map of the regions with a high level of activity, based on a movement pattern.

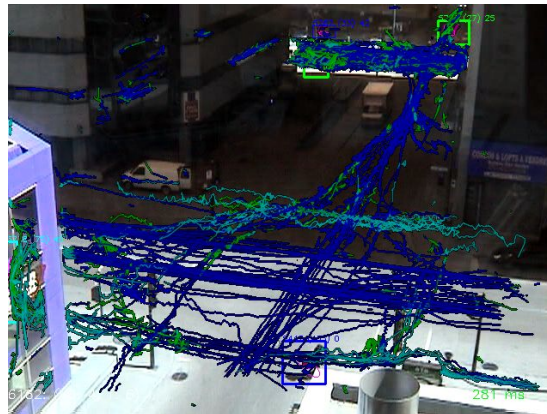
Optical Flow: Methods that analyze optical flow³⁰ help to detect consistent directions of pixel change associated with the movement of objects in the scene. However, they require complex calculations that are difficult to do in real time. Optical flow is also sensitive to the image's noise³¹.

3.2.1.2 Tracking Objects

After detecting moving objects, intelligent video surveillance systems track their movement over the video footage (Figure 6). Each task requires locating each object tracked from one image to another. This can be done in 2D with a single camera, or in 3D combining two views with known geometric relationship.

Many tracking techniques are based on mathematical methods that make it possible to predict an object's position on a frame based on its movement in the previous frames³². Tracking several objects at the same time poses many challenges. Each object detected in a frame must be associated with its corresponding object in the subsequent frame. This matching is done based on the objects' outlines, their characteristics (e.g., corners, area, ratios, etc.), or their model of appearance.

Occlusions (regions hidden by others) represent a major difficulty for tracking objects. A video surveillance system may lose track of an object if it is totally or partially obstructed over a certain period of time. It may also be difficult to separate two objects when they are very close or when one hides another.



³⁰ Optical flow is the translation vector field produced in an image by moving objects in a 3D scene.

³¹ Image defects often attributable to acquisition conditions and the camera's limits.

³² Kalman filter, specific filters, dynamic Bayesian networks, geodesic method, etc.

Figure 6 – Tracking of object trajectories in video footage

3.2.1.3 Classification and Identification of Objects

Objects detected by a video surveillance system are usually classified into different categories: human, vehicle, animal, etc. This classification may be done prior to tracking in order to retain only the trajectories of objects that are relevant for surveillance purposes.

In general, systems recognize the nature of an entity detected based on its shape attributes and movement properties. For example, a human is usually presented as a form that is taller than it is wide, whereas an automobile would be wider than it is tall (Figure 7). Human gait has specific features, in particular, a certain periodicity.

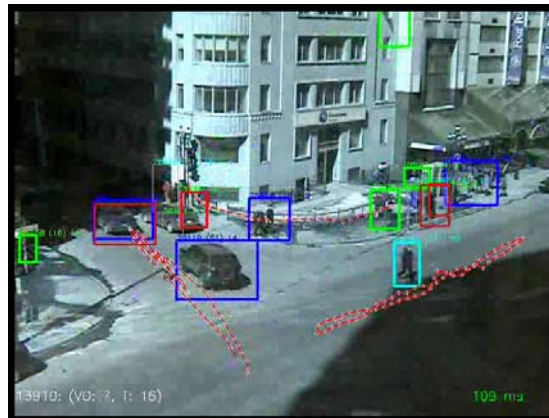


Figure 7 – Object classification (humans vs. vehicles)

Object identification pushes recognition further. After finding the class to which an object belongs, it must be identified. With surveillance, and in particular for access control or when searching for a suspect, the goal is to recognize an individual or decipher a vehicle license plate. Vast research and development efforts have been invested in recent years in these two specialized applications.

Recognizing human faces and gait are the two main biometric tools to identify people in video surveillance. Analysis of gait provides clues for the preliminary identification of an individual filmed from a distance, in a wide field.

Face recognition provides for a more accurate identification, but requires a face image with good resolution and in a proper position (facing forward as much as possible). Most systems will tolerate a face rotation of up to 45°. Many face encoding and comparison

techniques have been proposed since the early 90s³³ and are based primarily on the extraction of mathematical descriptors or topological points on the face. Initially developed based on photographs, face recognition applications have existed for a few years on video footage. Depending on the method used, recognition can be achieved by changing appearance, such as the addition of glasses or a beard, facial expressions and lighting. New 3D face recognition techniques³⁴ appear to improve identification performance and robustness in comparison to 2D techniques. However, face recognition in an uncontrolled environment, such as a crowd, continues to be a problem that has not yet been satisfactorily resolved by current video analytics systems.

Reading license plates from video surveillance is a difficult application. It requires a high-resolution image. There are many environmental interferences when analyzing an image: bad weather, headlight brightness, dirty or damaged plate. In order to read a license plate, a system must first locate the rectangle of the plate among all of the image's details (Figure 8). It must then proceed with optical character recognition³⁵. A plate filmed at an angle distorts the characters in the image and complicates the recognition process. In order to maximize the system's efficiency, plate recognition is done most often using specialized systems that concentrate on camera positioning and lighting quality.



Figure 8 – License plate detection

3.2.1.4 Classification of Activities and Behaviours

One of the goals of video surveillance is to interpret the individual behaviours of the objects in a scene and their interactions. Broadly speaking, behaviours are defined as the observable actions of agents (humans, animals, vehicles, etc.) Since behaviour recognition

³³ An overview of face recognition techniques is available at <http://www.face-rec.org/algorithms/>

³⁴ Use of A4Vision structured infrared light, or Geometrix triangulation based on multiple views.

³⁵ OCR, in English.

requires a semantic, sometimes complex analysis of what appears in the image, it is the most difficult challenge for video analytics systems.

The goal may be to detect a simple behaviour, such as “an individual has left a bag in a room.” However, the chain of interactions may quickly become complex:

Individual A leaves a bag in a room. Individual B takes the bag and leaves the room. Individual B bumps into individual A and shakes his hand. Conclusion: the bag was not stolen.

Analyzing and interpreting behaviours means recognizing movement patterns and extracting from them, at a higher level, a description of the actions and interactions. As is the case with all classification issues, a sequence of characteristics observed has to be associated with a model sequence representing a specific behaviour. The problem therefore consists of modelling typical behaviours, by learning or by definition, and finding a comparison method that tolerates slight variations.

Hidden Markov Models³⁶, neural networks and Bayesian networks are among the most used techniques for modelling normal behaviour and detecting deviant behaviour. These techniques trigger an alarm based on statistical discrepancy with the inferred model of the scene. Predefined event detection methods also exist. These are based on a system of rules, such as triggering an alarm if an object bigger than a threshold value remains stationary for a certain period of time in a given region.

3.2.1.5 Crowd Analysis

A domain of the future in video analytics research is crowd analysis and monitoring. With the quick escalation of the global population, the densification of large urban centres, and the growing issue of providing security during large gatherings, video surveillance has become an interesting avenue. Cameras are actually already set up to monitor large events (such as sporting events³⁷, political conventions, etc.), but the analytical efficiency of video systems in this context remains debatable.

Zhan et al. [14] have reviewed the research into crowd analysis. The different video analytics steps discussed in the previous sections are applied to it. However, analyzing a crowd has its own set of specific problems because crowds are made up of numerous individuals.

³⁶ In English, Hidden Markov Models (HMM).

³⁷ In 2001, the city of Tempa, Florida, used video surveillance for face recognition of members of the crowd. Taken from Barber, G, *Living on the Wrong Side of a One-Way Mirror: Face Recognition Technology and Video Surveillance*, 16 July 2001. <http://www.graysonbarber.com/pdf/WrongSide.pdf>.

Estimating density is a fundamental step in crowd monitoring and management, requiring an approximate assessment of the number of individuals. The numerous occlusions and juxtapositions make pedestrian segmentation for counting purposes difficult. Some techniques assume a proportional relationship between the number of pixels associated with the foreground, following segmentation, and the number of people. Other methods are based on image texture in order to characterize crowd density. Certain algorithms detect head contour, while others use the histograms of several characteristics to deduce the approximate number of people.

Although object tracking is one of the most popular research topics in video surveillance, most of the algorithms developed apply to a small number of people (less than ten at a time). Tracking pedestrians in crowds presents major difficulties, especially with respect to the large number of individuals to be followed from one frame to the next and the numerous occlusions present. Some methods track key features, which are less subject to being disturbed by occlusions than contours. Others model the human body or its parts. Probabilistic matching methods or specific filters are used to follow these models during video footage. Some papers exist on tracking using several cameras: M2Tracker works with synchronized cameras, and Chang et al.³⁸ use a combination of fixed and PTZ cameras.

It is important to follow a crowd's movements for security purposes. For example, the crowd's trajectory and flow will be analyzed. When modelling the crowd and its behaviours, certain researchers consider the crowd as a whole and interpret the movements of the different parts. Techniques such as optical flow and hidden Markov models are used to model movements. Some models will combine microscopic (individual) and macroscopic (crowd) analysis. In this context, two types of approaches are proposed to describe a crowd's activity: the application of physical models, such as the kinematics of gas particles and fluid dynamics, and agent-based techniques.

3.2.1.6 Active Video Surveillance in Multi-Camera Systems

Modern video surveillance systems, in particular on IP networks, may be comprised of hundreds of cameras. Sometimes, several cameras cover the same area. Some of them are power-operated and can be controlled to capture further details on an event detected in a wide field. For example, the camera can zoom in on an individual penetrating an area in order to identify him/her. In certain networks, cameras are intelligent, i.e., they have their own processing unit. They can exchange information with a central system or directly amongst themselves.

These surveillance camera networks make it possible to follow objects over extensive areas. Furthermore, multiple views may help to solve object occlusion problems. In a

³⁸ Cited in [14].

distributed architecture, analytical processing can be done in parallel, thereby accelerating the analysis and saving on bandwidth by transmitting only metadata.

However, these networks also raise specific problems that the scientific world is trying to solve:

- **Camera calibration:** Operation that consists in establishing a correspondence between the global reference mark of the scene observed and the camera coordinate system, as well as in determining the camera's intrinsic parameters, such as distortion³⁹. This precision process may be tedious for a network with many cameras. It is preferable to develop analytical functions that do not require any camera calibration or self-calibrating methods.
- **Movement detection:** For a power-operated camera, the camera's movement creates an apparent change in the image. Movement detection methods must distinguish between camera movement and independent changes.
- **Object tracking on several cameras:** In order to be able to track an object from one camera to the next, correspondence must be established between the different views in a common reference point. Camera resetting consists in calculating parameters for transforming the image from one camera to the next based on the change in reference point and the movement model. This operation uses a priori knowledge of the scene's topology. It allows for an increased 2D (2D1/2) or 3D view to be obtained of the scene. Changes in object appearance and positioning over time, as well as changes in lighting, complicate the resetting process.
- **Detection of camera tampering:** The more cameras a network has, the more difficult it is to control how they function. These systems must have built-in tools for automatic detection of camera breakdowns and alterations in order to remain functional.

Multi-camera active video surveillance systems are used above all for monitoring extensive or distributed areas, such as transportation systems, banking infrastructures, government institutions (military bases, prisons, strategic infrastructures, radar centres, hospitals), public buildings, shopping malls and parking lots.

3.2.2 Analytics in Commercial Systems

Many video analytics products to enable intelligent video surveillance have been introduced into the market since the start of the decade. A list of the main developers of video analytics software is provided in Appendix 4.

Overall, the products available offer roughly the same basic functionalities. Some software applications stand out because they offer more specialized functionalities (e.g., license plate recognition) or due to performance.

³⁹ Taken from http://wcours.gel.ulaval.ca/2008/a/19263/default/5notes/modele_camera.pdf.

The main video analytics functions on the market can be summarized as follows:

- Tracking by PTZ camera triggered by an alarm.
- Detection of camera breakdown and tampering.
- Detection of disappeared or abandoned object.
- Detection of intrusion (person or vehicle) in controlled areas or perimeters: restricted virtual limits, security zones, passage of several individuals or vehicles through access control using a single piece of ID (*tailgating*), intrusion through an exit ramp, person passing over or under a booth.
- Detection and tracking of people or vehicles: analysis of speed and direction of movement, detection of stationary person/car/object near a sensitive infrastructure.
- Counting of people or vehicles, detection of crowds or excess numbers.
- Detection of theft and fraud at points of sale.
- Behaviour recognition: detection of loitering, fights, races, falls, movement against the flow of traffic, graffiti, vandalism.
- Traffic monitoring: traffic speed/density/direction, objects on the pavement, disregard for speed limits, congestion, pedestrians, etc.
- Face detection and recognition.
- License plate recognition.
- Fire detection by image analysis.

Video analytics technologies are still young and require development. Many commercial applications work well in controlled environments, but most of them perform less well when set up at the client's location and actually used. These systems require vast adjustments and parameterization in order to operate properly for a specific application.

Basic functions, such as movement detection, image improvement and detection of camera alterations are generally robust enough to function in a wide range of applications. People counting, intrusion detection (virtual limits) and license plate recognition are fairly mature analyses. Although some parameterization is required, they are being more widely used.

In general, the research into object detection and tracking techniques has been vastly developed and some techniques are built into implemented commercial systems for simple cases of use. However, a lot of work is still needed to develop these techniques in order to achieve the performance and robustness required to operate in complex environments. Object detection and tracking in crowds or through a multi-camera network are difficult problems.

There are many commercial products specializing in image detection and recognition (see Appendix 4). Their efficiency depends largely on the application and the complexity of the environments in which they must operate. These technologies generally require that

acquisition conditions (lighting, position, etc.) be controlled in order to provide satisfactory results.

Certain behaviours are detected by the analytics software available on the market. These consist of activities that can be deduced from the properties of simple movements (speed, direction, etc.), such as a person running, loitering or falling. However, it is often difficult to determine the threat level this movement represents. For example, is a person running because they are trying to get away or because they don't want to miss their flight at the airport? Behaviour recognition remains an experimental field in analytics.

Video analytics expectations often greatly exceed the actual performance of the technologies, which are difficult to integrate and use. On this topic, Hearing et al. [11] suggest a list of desirable characteristics for a commercial video analytics system.

- **Minimizing the necessary configurations:** A commercial system should not require a vast amount of configuration, parameterization and training time. Ideally, the user should provide a minimum amount of additional information to video flow on installation.
- **Offer suitable performance:** The number of false alarms should be kept as low as possible to avoid disturbing security personnel needlessly. However, it is even more critical that the system not allow a real threat to pass. The balance to be achieved between the number of false alarms and missed detections depends on the security application.
- **No camera calibration or automation of same required:** Camera calibration makes it possible to calculate the actual size and speed of the objects in the scene. It establishes the correspondence between the geometry of the scene and that of the image.
- **Support a wide range of cameras:** Video analysis should be equally possible on images from colour, black and white, infrared, thermal or omni-directional cameras.
- **Remain as generic as possible:** Ideally, the detection of relevant events should be possible in different types of environments and cases of application. However, certain settings have very specific problems, such as areas with bodies of water. Water movement and mirror reflections disturb the algorithms that detect changes in the image on which object detection and tracking is based.
- **Offer privacy protection mechanisms:** Analytics systems should make it possible to hide details on video footage (such as faces) that are not essential for processing a security alarm.

3.2.3 Video Analytics Needs and Challenges

A few technological needs and challenges were identified for the intelligent video surveillance field following a search of the documentation and a consultation of experts and users. We have presented them in this section.

Given the explosion in the amount of video footage captured by security, the need to develop automatic methods for detecting suspicious people, objects or events so that only sequences relevant for human analysis are submitted has been widely noted. Existing techniques are promising, but few of them are currently commercially used in real case scenarios.

With respect to research, there are many algorithms applicable to video surveillance, but they are often partial solutions dealing with only part of the video surveillance problem. There are few complete experimental systems operating under near-reality conditions.

It is currently widely agreed that what works well in video analytics is movement detection, the detection of specific objects, license plate recognition done from specialized systems, and the detection of certain specific behaviours (walking, running, carrying an object).

The following needs to be developed or improved:

- Near-real-time detection and recognition, i.e., in the minutes following the incident (especially important for the security of sensitive infrastructures or during major events).
- More specifically, real-time face recognition (25 to 30 frames/sec).
- Face recognition in a crowd. This requires an image with sufficient resolution that can be accessible with the megapixel cameras now available on the market.
- People counting in crowded environments and under various angles-of-view.
- Tracking of specific objects in crowded scenes (an individual in a crowd or a vehicle in traffic).
- Tracking of hinged bodies for understanding activities.
- Recognition of more complex behaviours, relevant for security purposes.
- Segmentation of areas of colour. For example, colour information on a car may improve the performance of the plate recognition algorithm. It may also be used to recognize different pieces of an individual's clothing.
- For detection and recognition, the fusion of different video data (e.g., combining face recognition with gait recognition), or the merger of video data with those obtained by different systems (temperature sensors, biometric systems, etc.), are the methods being built on.

Many video analytics algorithms function only for fixed cameras, good resolution and with adequate and constant lighting, which is not very useful for most applications. Some frequent problems are never taken into consideration, such as sudden camera changes (spider webs, dust, moved camera). The robustness and accuracy of most of the existing detection, tracking and recognition algorithms are vital when dealing with changing environmental conditions. In order to be adopted by consumers, intelligent video surveillance systems must be strong enough to deal with different weather conditions, adjust to lighting changes (natural and artificial) of the scene and adapt to hardware and software failures.

This is a sizeable challenge in the development of intelligent video surveillance systems, i.e., performance assessments. Should systems be compared to humans? For many surveillance tasks, such as detecting abandoned objects, humans perform horribly. Yet it is difficult to compare the systems to each other since most performance tests are carried out on different sets of data.

Therefore, objective and systematic methods should be developed to evaluate and compare intelligent video surveillance system performance. This operation depends greatly on the analytical task to be evaluated. It also requires building a set of annotated data (ground truth) and choosing a distance measure to evaluate the difference between the system's responses and the ground truth.

The following are some video analytics system evaluation initiatives already in place:

- PETS (Performance Evaluation of Tracking and Surveillance)⁴⁰: Makes it possible to submit an online algorithm for evaluation. Proposes a metric.
- CREDS (Challenge for real time event detection solutions): Competition for detecting predefined events on Paris subway surveillance footage (e.g., person walking on the tracks).
- I-LIDS (Imagery Library for intelligent Detection Systems)⁴¹: Launched by Great Britain's Home Office Scientific Development Branch. Makes it possible to perform tests on video data to detect parked vehicles, abandoned luggage, intruders in controlled perimeters, and door monitoring.
- ETISEO (Évaluation du traitement de l'interprétation de séquences video – performance evaluation project for video surveillance)⁴²: By the French government, project terminated, but body of knowledge available on request for non-commercial research purposes.
- FRVT (Face Recognition Vendor Tests)⁴³: Conducts tests of different face recognition systems on several databases in order to provide an objective comparison between vendors. The results enable the American government and their security agencies to know where face recognition technologies may be deployed and to identify future research bases in this field.

Finally, analytics algorithms must adapt to the new video surveillance system architectures: heterogeneous multi-cameras (possibly power-operated), distributed intelligence, high-resolution video. Research and development will be necessary for:

- Introducing intelligence in the cameras.

⁴⁰ www.petsmetrics.net.

⁴¹ <http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/video-based-detection-systems/i-lids/ilids-datasets-pricing/>.

⁴² <http://www.sop.inria.fr/orion/ETISEO/>.

⁴³ <http://www.frvt.org>.

- Creating adaptive algorithms.
- Enabling tracking with power-operated cameras in a multi-scale approach: wide detection field, then zooming-in on an object or individual to extract greater details.
- Developing self-adapting and self-calibrating algorithms for real-time adjustment of camera parameters (zoom, focus, aperture, etc.), based on changes in the monitored scene.

3.3 Technological Trends for Video Surveillance

Many current video surveillance systems still rely on traditional technologies: analogue cameras, coaxial cables, digital recorders. However, technical progress in this field has led to changes in video surveillance system architectures, components and capacities.

The following are the main technological trends anticipated by experts in the field for the coming years.

- A shift to video surveillance on IP networks is underway. Currently mainly adopted for large infrastructures, IP video surveillance could win over smaller users if IP camera costs drop.
- Megapixel cameras are a major technical breakthrough in video surveillance, offering better resolution and wider coverage. They also improve the performance of analytical processing. They should therefore become widespread. One expert questioned for this report predicted that half of surveillance cameras will be high resolution by 2012.
- The H.264 compression standard (MPEG-4 Part 10/AVC for Advanced Video Coding) should become established in video surveillance. Its superior compression ratios in comparison to existing standards make it possible to save on bandwidth and storage space. This standard should encourage the adoption of megapixel cameras in video surveillance.
- Surveillance systems will have multiple camera networks operating in real time. In these systems, the trend is to distribute recordings and processing in different nodes (cameras and encoders) in order to decrease the quantity of data transmitted.
- There should be greater integration and better interoperability of the different security systems to enable their management under the same command and control centre. Thus, video surveillance, access control, biometric solutions, RFID, intrusion detection systems could be connected.
- Intelligent video surveillance should progress and video analytics products should become more robust and efficient for security applications. Object (people, faces, vehicles, etc.) detection, tracking and recognition in loaded crowded scenes, as well as behaviour recognition will be the most active research fields for video surveillance.

- The use of video surveillance systems will progressively extend beyond security. Applications will develop for marketing analyses, studying consumer behaviours and monitoring company operations.

4. DESCRIPTION OF THE SECURITY AND VIDEO SURVEILLANCE MARKET

4.1 Global Security Market

The security market is a vast and eclectic market that covers several industry activities (manufacturing, services, integration, distribution, etc.). Supply can also be divided into various market segments: safety of individuals, computer, network and communication security (IT security), security of infrastructures, access control, authentication, front-line services, including emergency assistance and interventions during times of crisis, the war on terrorism, transportation security (air, maritime, railway, roads), industrial security, detection of and response to a chemical, biological, radiological and nuclear attack, etc. It should be noted that numerous segments identified are primarily driven by the State, which shows the importance of this player in guiding the market, both as a legislator and as a client.

Many of the products or services offered within the aforementioned segments are overlapping, which highlights the difficulties in defining this market and what it entails. No official classification has been adopted in Canada to date to designate the field of security.

Of note in this respect is the approach taken by the Centre for Security Science (CSS), a public federal organization set up jointly by Defence Research and Development Canada and Public Safety Canada, and which includes 19 federal government agencies. The CSS's mission is primarily civil defence and public protection, and it divides its S&T activities into the following four broad areas:

- Critical Infrastructure Protection (CIP);
- Surveillance, Intelligence and Interdiction (SI²);
- Emergency Management and Systems Integration (EMSI);
- Protection against Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Agents.

In this context, analyzing the size of this market and the income it generates based on the different studies published is a complex task. The way the market is defined, i.e., what is and is not included in said definition, varies from study to study, making a comparison difficult. Despite this fact, this report sets out the main data available in order to provide an idea of the size of the security market and its growth trends.

According to a report by Homeland Security Research Corporation, the public and civil security market experienced a phase of quite significant growth (about 600%) between 2000 and 2008⁴⁴, especially following the September 2001 attacks. Of note that, in this study, the security market has been defined in very broad terms and includes, for example, certain expenses associated with homeland security activities conducted by the Departments of Defence. This market is expected to grow by 81% between 2008 and 2018. This study covers 20 key national markets that define trends in this field.

Although Canada is not a major international player in security matters, it has followed the growth trend and increased public safety expenses following the events in New York, and also in response to the administrative reorganizations of the US federal government and the creation of the Department of Homeland Security. Since being created in 2003, the Department of Public Safety and Emergency Preparedness (formerly PSEPC, now Public Safety Canada) was allocated an annual budget between \$5 billion and \$7 billion (Figure 9). A more in-depth study of the expenses incurred by this Department and its organizations⁴⁵ would be required in order to accurately determine how they are earmarked.

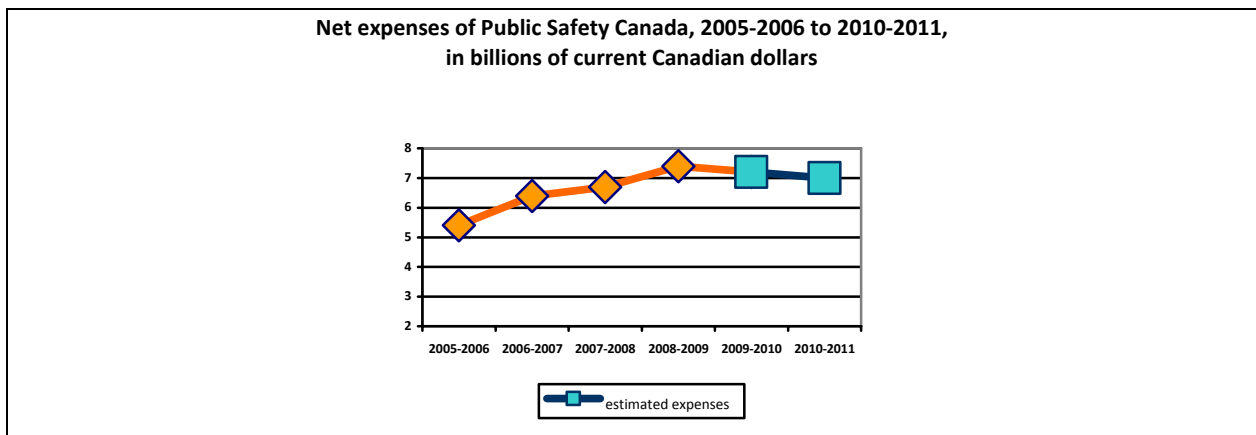


Figure 9 – Table taken from the Report on Plans and Priorities, 2005-2006 to 2008-2009

The available data tend to indicate that markets will continue to grow worldwide, but that said growth will be slower than over the past eight years.

⁴⁴ Homeland Security Research Corporation. National Security Spending Outlook in 20 countries, 2009-2018, 13 November 2008, available at: <http://www.homelandsecurityresearch.net/2008/11/13/national-security-spending-outlook-in-20-countries-2009-2018/>.

⁴⁵ Royal Canadian Mounted Police, Correctional Service Canada, Canada Border Services Agency, Canadian Security Intelligence Service, National Parole Board, Commission for Public Complaints Against the RCMP, Office of the Correctional Investigator, RCMP External Review Committee.

There are many factors to explain this phenomenon. The most important include the fact that growth in the first half of the current decade was due mainly to the vast public funds invested by the American government as part of the implementation of Homeland Security and of various programs to secure the territory. Part of these programs included major immobilization efforts. For example, the Secure Border Initiative (SBI_{net}) is aimed at securing the northern and southern borders of the United States. The portion of the program allocated to the Canadian-American border is currently at the deployment stage following the granting of contracts in 2006 to Boeing to supervise the program.

4.2 Video Surveillance Market

The video surveillance market is part of the security market and overlaps into many of the segments discussed in the previous section. For example, in 2007 in the United States, the video surveillance segment represented 34% of the national security market, valued at \$9.5 billion⁴⁶.

The Multimedia Intelligence⁴⁷ White Book identifies six key client groups for video surveillance-related products:

- Financial and banking environments.
- Transportation sector.
- Industry.
- Retailing sector.
- Public sector.
- Education sector.

Three of these sectors (transportation, education and the public sector) are heavily influenced by governments in terms of legislation and guidelines (standards, interoperability, etc.), or in terms of funding. According to this firm, the residential and small business sectors do not, therefore, appear to be a priority for video surveillance.

Most analysts consider that the global video surveillance market will also continue to grow in coming years, but opinions differ as to the expected rate of this growth.

Organizations such as ABI Research have very optimistic forecasts, estimating that the global video surveillance market should increase from US\$13.5 billion in 2006 to US\$46 billion in 2013, which represents a 34% increase per year over seven years. IMS in turn reports global revenues of about \$7.25 billion for 2007, which is below ABI Research's

⁴⁶ United States Security Market Report and Economic Impact Study, SIA, <https://siamembers.siaonline.org/eweb/upload/imr/USSMRfactsheet.pdf>.

⁴⁷ Multimedia intelligence. 2008. *The Expanding World of IP Video Surveillance*.

estimates, while the highly respected firm Freedonia talks of 6% annual growth for video surveillance⁴⁸. Given the difference in these figures, probably resulting from different market definitions, revenues may range between US\$7.25 billion and \$14 billion for 2007 using these two sources as an example.

4.2.1 Video Surveillance Market Driving Forces

The following are a few driving forces behind the video surveillance market:

- The after-effects of September 11, 2001, and the fear of new terrorist attacks (New York, London, Madrid, Bali, Mumbai, etc.)
- Events such as shootings in public places, especially in educational institutions (Columbine, Virginia-Tech, Collège Dawson, etc.)
- Hikes in local crime.
- Certain technological advances that improve the performance of systems and/or reduce costs associated with their installation or maintenance.
- Greater public consent as to the installation of video surveillance systems in public places.
- The possibility of using the images gathered for legal proceedings.
- The possibility of combining video surveillance technology with other access control technologies (such as biometrics).

4.2.2 Video Surveillance Market Inhibitors

The following are a few video surveillance market inhibitors:

- Concerns expressed with respect to protecting individual privacy.
- Doubts about the efficiency of these systems in preventing a terrorist attack or a “Virginia-Tech” type of attack.
- System reliability.
- Complex system installation and use (user-friendliness).
- Maintenance and upgrading costs.
- Absence of harmonized industry-wide standards.
- Decreased fears of a terrorist attack.
- Lack of qualified personnel.

⁴⁸ Institute of Management and Administration, Inc. Security's Director Report, Newsbrief, February https://www.ioma.com/?&IPAuth=&source=WW_200903&stype=WEB.

On a sector-based level, ABI anticipates high video surveillance growth in the transportation market, with revenues of US\$2 billion, and expects the retailing market to generate its own revenues of US\$4 billion in 2013⁴⁹.

4.2.3 The IP and Intelligent Video Surveillance Market

The video surveillance market is at a turning point in its evolution, initiating a shift towards digital applications and IP network infrastructures⁵⁰. The flexibility and expandability scalability of IP systems, the fact that most of them can operate on non-proprietary hardware, as well as technological advances in parts are making these systems more interesting for potential clients and driving down costs.

As mentioned in Multimedia Intelligence's white book paper, growth and growth expectations for the IP video surveillance market are quite robust. The IP camera sub-section in particular is experiencing strong expansion, recording a 50% jump in revenues for 2007, reaching \$500 million world-wide⁵¹. This growth is almost four times higher than for all video surveillance equipment put together. Despite this, based on revenues, IP cameras only represent 8% of the total surveillance camera market.

The high cost of IP cameras, almost twice that of analogue cameras, is the main obstacle facing consumers⁵². However, according to some experts, IP cameras should dominate the market within three to seven years, thereby giving a boom to "all IP" video surveillance. Megapixel cameras could be the driving force behind this transition to IP technologies. Technical advantages in terms of the image quality and resolution afforded by megapixel cameras in video surveillance are a real motivation for users. Axis is the largest manufacturer of IP cameras, and Mobotix is the main manufacturer of megapixel cameras.

The advent of IP video surveillance does not mean the death knell is being tolled for traditional CCTV systems using analogue cameras. The technical progress made by manufacturers to digital recorders and hybrid digital recorders, such as remote access, expandability and integration of on-board analytics, keeps them competitive with video on IP networks. Both types of technologies should be able to share the market for a few years and hybrid systems should allow for a gradual transition to network video surveillance.

⁴⁹ Video Surveillance Dollars Not Just for Security, ABI Research, 8 October 2008, <http://www.abiresearch.com/press/1257-Video+Surveillance+Dollars+Not+Just+for+Security>

⁵⁰ Russ Gazer. 2008. Special Report: Video Surveillance. SDM.

⁵¹ Multimedia Intelligence, *The Expanding World of IP Video Surveillance: Cameras, Storage, Technology and Semiconductors*, November 2008.

⁵² According to IP Videomarket Info, only one in five buyers chooses IP cameras.

According to Frost & Sullivan⁵³, the education sector should become a major IP video surveillance consumer. The large bandwidth available on academic institution networks enables them to support video transmission, thereby encouraging the replacement of analogue infrastructures with IP cameras. However, the retail business remains a leader in the deployment of IP video surveillance systems.

Intelligent video surveillance is a niche industry that is still in the early stages of development? (suggestion). As concerns the video surveillance software sector in particular, ABI Research anticipates high revenue growth, from the current level at \$245 million, to over \$900 million in 2013⁵⁴. This forecast covers all video surveillance software, from video management to analytics. Based on revenues, the two largest international players in video management software are Milestone and the Quebec company Genetec. For video analytics, iomage Ltd. and ObjectVideo are among the most renowned companies⁵⁵.

However, certain analysts have shown disappointment in this sub-sector of intelligent video surveillance. There still seem to be some barriers as to the more widespread adoption of intelligent video surveillance, in particular with respect to technical performance (e.g., the high number of false alarms), the absence of industry-wide standards, which would create confusion for potential clients, and costs associated with setting up an effective and efficient system⁵⁶.

In this perspective, intelligent video surveillance continues to be a risk for the buyer, given the confusion surrounding the real possibilities of the video analytics tools available on the market. For many applications, the capacities of video analytics systems have not yet met user expectations. Moreover, the cost of these systems is still high, confining them to an upscale market, such as the surveillance networks of large, mainly public or critical infrastructures (e.g., power stations). Even in those sectors, a market analyst estimates that the video analytics systems deployed are still at the pilot project phase⁵⁷.

Despite these difficulties, video analytics seems quite promising as a means to improve the efficiency of video surveillance and searches of archived footage. Video surveillance users have currently shown a certain interest in video analytics, but seem to be waiting for this technology to prove its worth. Now that certain types of intelligent video processing

⁵³ Frost & Sullivan, World Video Surveillance Market- Investment Analysis, June 2008, <http://www.researchandmarkets.com/reports/612498>.

⁵⁴ Strong growth for video surveillance software, Security Info Watch, 11 June 2008, <http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/15921SIW321>.

⁵⁵ John Honovich, *How U.S. IP video companies fit into the world market*, 8 March 2009, SecurityInfoWatch.com available at: <http://www.securityinfowatch.com/CCTV+%2526+Surveillance/1309661>.

⁵⁶ John Honovich, *Video Surveillance Market Size & Forecast Reference Guide*, IP Video Market Info, 24 January 2009, available at: http://ipvideomarket.info/report/video_surveillance_market_size_forecast.

⁵⁷ Simon Harris de IMS Research, cited by Geoff Kohl in SecurityInfoWatch.com, 11 March 2009, *Where video analytics is today*.

systems have begun to display satisfactory performance, it can be assumed that this market's real growth is still to come, but may take a few years to materialize.

De plus, selon plusieurs analystes, de nouvelles applications moins liées à la sécurité (gestion des opérations, protection contre les poursuites, analyses du comportement des consommateurs, etc.) sont susceptibles de créer un regain d'intérêt pour ce type de systèmes et de contribuer à la croissance globale du secteur à moyen et plus long termes.

4.2.4 The Players

Video surveillance is a very fragmented market with several players sharing the existing clientele. Some players dominate certain segments, such as Axis for IP cameras, Pelco for analogue cameras and Genetec for video management software, but many competitors seize small parts of the market. The industry is characterized by inevitable partnerships between equipment manufacturers and developers of video management and analytics software, in order to ensure compatibility between the different parts of a video surveillance system.

It has been interesting to watch players such as Cisco, IBM and EMC, more traditionally associated with IT, enter onto the video surveillance market scene⁵⁸. According to MMI, this tends to change the business environment of more "traditional" video surveillance firms such as Axis Communications. It also indicates a certain interest on the part of these firms in the video surveillance markets and the anticipated convergence between physical security and software security.

A ranking by Asmag⁵⁹ of the 50 largest security firms for 2008, based on revenues, indicates that the driving force behind 30 of them is video surveillance. It is interesting to note that only one Canadian company appears on this list, March Networks, and that it ranks 21st⁶⁰.

4.2.5 The Impact of the Recession on the Market

It is currently quite difficult to determine the impact of the financial crisis on the security and video surveillance markets as opinions are quite divided.

For many consulting firms, the security market is recession-proof since part of this market's activities is determined by public and government demand. Moreover, some people see a correlation between periods of economic crisis and increased crime, which could result in higher sales in security systems, including video surveillance. Intelligent

⁵⁸ Frost & Sullivan 2008, op. cit.

⁵⁹ Manufacturing only, therefore excluding installation, distribution and resale.

⁶⁰ Asmag.com, Security Top 50, 2009.

video surveillance systems could also represent an interesting alternative for more traditional devices since they require few personnel. This viewpoint is highlighted by an article published in the Boston Globe in February 2009⁶¹ and by most consulting firms, which continue to anticipate growth in these markets.

However, others fear that the security and video surveillance markets are not immune to a drop in revenues. The 2009 edition of SDM's Industry Forecast focusing on electronic security clearly states that, for the first time since the organization began this exercise, the people polled anticipate a drop in their total revenues to the tune of 7.8% in 2009. John Honovich of IP Video Market Info also predicts a substantial drop in growth for video surveillance between 2008 and 2009 in comparison to 2008 forecasts. He also highlights the fact that most market studies predicting considerable hikes in business volume were published prior to fourth quarter earnings reports. He therefore directs his readers to be prudent since, in the current economic context, projections can be quite hazardous.

Severin Sorensen from Sikyur LLC also tends to lean on the side of prudence, stating that if the company has disruptive technology enabling its client to save large amounts of money, then the market will work in his favour. However, for projects requiring heavy investments, the prognosis is nowhere near as good, given current economic difficulties⁶². He also cautions about public markets being "recession-proof": these markets are not only federal, but also provincial and municipal. As stated by the Center on Budget and Policy Priorities⁶³, the American states are currently experiencing a deep financial crisis that is directly related to the global economic crisis. This situation risks putting the brakes on several projects that were supposed to be started up during the year and the situation will most likely be the same at the municipal level. However, the recovery plan proposed by President Obama and adopted by Congress includes local security provisions that may result in business opportunities of about US\$4.5 billion⁶⁴, which may help to revive the situation, at least partially. It remains to be seen how these funds will be defrayed.

In Canada, the Economic Action Plan does not really mention the issue of national security⁶⁵. The only announcement made is in association with improved airport security in the country, but that's it⁶⁶. It is therefore difficult to gauge the impact of the crisis on the Canadian market since the related data are difficult to obtain and are often not recent. Since

⁶¹ Kirsner, Scott. Surveillance gest intelligent. *Security Firms see Growth as the Downturn Worsens*, 8 February 2009.

⁶² Sorensen, Severin. *Recession Impacting Security Projects*. IPVideoMarket Info, 10 February 2009, available at http://ipvideomarket.info/report/recession_impacting_security_projects.

⁶³ Center on Budget and Policy Priorities, *State Budget Troubles Worsen*, By [Elizabeth McNichol](#) and [Iris J. Lav](#), 13 March 2009, available at <http://www.cbpp.org/files/9-8-08sfp.pdf>.

⁶⁴ William Welsh, Stimulus to generate \$4.5B state and local tech spending, Washington Technology, 13 February 2009, available at: <http://www.washingtontechnology.com/Articles/2009/02/13/Stimulus-to-generate-new-state-and-local-tech-spending.aspx>.

⁶⁵ Canada, Department of Finance, Canada's Economic Action Plan. 2009 Budget, 27 January 2009.

⁶⁶ Government of Canada. 23 January 2009. Government of Canada Invests in Airport Safety Across the Country. Press Release.

in many aspects Canada and Quebec seem to be withstanding the crisis better than other national or provincial players, the budget deficits announced may put some large projects on the backburner. It should be mentioned that nothing to that effect has been announced to date.

With respect to the private sector, a tightening of security expenses by companies has already been noticed, and there has been a realignment of priorities in this field towards the maintenance and operation of existing systems instead of the installation of new systems⁶⁷.

4.3 IP and Intelligent Video Surveillance Supply and Demand in Quebec

There is little available public data on the specific video surveillance sector in Quebec, and what is available sometimes dates back a few years. Painting a picture of the IP and intelligent video surveillance sector in Quebec would require an in-depth study among the different market players and be beyond the scope of this report. We have therefore chosen only a few market representatives: developers, integrators and installers, large digital video surveillance users. They were asked questions about client needs, services offered and products available. Their comments on the current state of the Quebec video surveillance industry and opportunities for video analytics were collated.

This section describes the Quebec supply and demand trends in digital video surveillance based on the testimonies gathered, and in relation to the global video surveillance market analyses available to the public. Quebec companies and research centres offering specific expertise in digital and intelligent video surveillance are identified herein and a list of the main Quebec and international players in this market is available in Appendices 2, 3 and 4. A few recommendations on the Quebec market's position in this sector are also made.

4.3.1 Demand

According to the experts questioned, as is the case with other industrialized countries, there is high demand in Quebec for video surveillance systems, which are part of the security equipment needed. IP digital video surveillance is beginning to gain ground, especially in the upmarket. Large IP video surveillance networks are found in particular in the public and parapublic sectors, transportation systems, large retail store chains, casinos and universities. Small and medium-sized businesses delay in shifting to IP video surveillance due in particular to the high cost of equipment.

In 2003-2004, the Commission québécoise d'accès à l'information held a public consultation on the use of video surveillance by public agencies in public places⁶⁸. It was

⁶⁷ Sorensen, op.cit.

already noted at that time that most of the public and parapublic agencies of the province (including municipalities) used video surveillance systems, which, in 2003-2004, represented over 5,000 cameras. Moreover, practically all of the new public structures built in Quebec are wired for video surveillance system installation, which indicates that the use of this type of equipment has become common practice for organizations.

In the transportation sector, Aéroports de Montréal (ADM) and Société de transport de Montréal (STM) were cited as examples in section 2.4 for video surveillance use. They represent networks of several hundreds of cameras. At the STM in particular, the IP shift was carried out. The transportation sector is also integrating analytics projects, at least at the pilot project stage.

A joint study conducted by PriceWaterhouseCoopers and the Retail Council of Canada revealed that 90% of respondents to a poll on security measures taken against theft used video surveillance systems⁶⁹. It would not be surprising to find video surveillance as well in a high proportion of Quebec businesses. The case of Couche-Tard convenient stores was already cited as an example of video analytics use in section 2.3.

Quebec universities must oversee the security of large campuses, consisting of several buildings and parking lots, that are sometimes quite geographically dispersed. Video surveillance has been set up on said campuses for several years. With the need to renew broken or outdated equipment, universities are increasingly migrating towards IP video surveillance. At McGill University, for example, the video surveillance network is already a hybrid system, comprised of analogue and IP cameras, and digital recorders. Network recording solutions are now being considered.

In the final report based on the 2004 public consultation conducted by the Commission d'accès à l'information⁷⁰, the commissioner revealed that video surveillance system use by private businesses is not sufficiently documented in Quebec. According to the experts consulted for this report, this market is comprised primarily of SMEs, which have modest means to allocate to security. The video surveillance systems set up in these businesses typically consist of under 50 cameras. In most cases, this clientele is unaware of the existence of video analytics. However, it appreciates functionalities such as the automated tracking of objects with PTZ cameras.

For all the sectors, the experts consulted issued different comments to characterize Quebec demand for video surveillance. The Quebec video surveillance market is apparently less mature than the American or European markets. Business and public agencies are quite

⁶⁸ Commission d'accès à l'information du Québec. Public Consultation. *L'utilisation de caméras de surveillance par les organismes publics dans les lieux publics*. Assessment, April 2004.

⁶⁹ Canada Newswire. June 2008. *Survey shows Canadian Retailers are Taking Necessary Actions to Combat Theft : Retail Council of Canada*, PriceWaterhouseCoopers.

⁷⁰ Commission d'accès à l'information du Québec, op.cit.

often in reaction mode when it comes to security system deployment. They do not believe they are at risk until a serious event occurs.

In Quebec, clients prefer above all ready-made systems, unlike European users who have custom solutions developed more often. Proprietary systems are more popular in Quebec than open systems, which are held in much greater esteem in Europe.

Quebec users, like those in other countries, are seeking to reduce the staff assigned to surveillance. Furthermore, in several cases, they wish to shift from reactive surveillance to preventive surveillance and obtain better performing tools for video archive searches. Video analytics may provide certain solutions to these problems, but users are still somewhat ignorant about the possibilities and limits of this technology. Analytics is breaking above all into large businesses or infrastructures, but not yet into systems aimed at SMEs.

The Quebec market has specific video surveillance needs. Extreme weather conditions (heat and cold, snow, etc.) in Quebec may affect how the hardware components of video surveillance systems operate. Also, climate variations are an additional challenge for video analytics algorithms. Finally, Quebec society is the only one in North America to require video surveillance software in French.

4.3.2 Supply

The industry is divided primarily between manufacturers, distributors, resellers-installers, integrators-installers, and video or analytics management software developers. Resellers-installers sell complete solutions they buy from distributors and install them at the client's premises for a turnkey solution. Integrators-installers assemble the computers and servers themselves to provide clients with a system adapted to their needs.

The largest video surveillance product distributors in Canada and Quebec are ADI-Burtek and Tri-Ed. Most products sold on the Quebec market come from foreign manufacturers, especially American ones. Chinese and Korean cameras and video software have been entering the Canadian market over the past year. These products are currently quite basic and do not have the level of quality and the functionalities of Western products, but there is the potential for development.

There are many resellers-installers and integrators-installers in Quebec, and these are often very small businesses. Some large security and alarm companies, such as ADT and Protectron, offer video surveillance system installation services, but this is not their area of speciality. Very few integrators in Quebec are specialized in IP video surveillance. Of these, we met with Claridion and SGPTI to conduct an intelligence study. Resellers-installers and integrators-installers were not polled for this study; however, those mentioned by the experts interviewed are included in the list of companies in Appendix 3.

In the category of software designers, Genetec is a boom in the Quebec industry. It is one of the two largest video management software developers in the world. In 2008, the newspaper *Les Affaires* reported that the company's sales had increased 900% in five years⁷¹. Its most sophisticated system can manage up to 250,000 cameras on an IP network. Genetec's software has built-in video analytics functions developed by third parties.

VideoWave Networks and Organix IT are two other examples of Quebec companies developing video management software with built-in intelligent functionalities. VideoWave Networks is specialized in PTZ camera management software, and Organix IT, in partnership with ISS Technology, offers video management software on an open architecture.

In the camera sector, ImmerVision develops software applications and panomorphic optics for capturing, processing and viewing photographs and videos at 360°. The company Obzerv has launched innovative night vision system technology for surveillance.

There are, in Quebec, many suppliers in the video surveillance field, but these companies are generally fairly small (less than ten employees), and most of them offer integration and installation services. There is therefore strong competition in this sector. However, according to the experts interviewed, there is still no critical mass of specialized IP video surveillance suppliers. Traditional physical security companies do not necessarily have the IT expertise required to install systems on IP networks. Some of the experts interviewed are of the opinion that demand outweighs supply in digital video surveillance.

Product supply is mainly provided by foreign companies. Except for Genetec, there are few digital video surveillance solution developers in Quebec. Yet Quebec's expertise in the field of vision and image analysis is quite high. A few research centres, especially at the Laval, McGill, Concordia and Polytechnique universities, and at CRIM, specialize in video analytics and could transfer knowledge and technologies in this field to Quebec businesses.

4.3.3 Recommendations for the Quebec Market

The security market, and in particular the video surveillance market, is growing world-wide and offers interesting business opportunities. A company does not need to be very big to break into this already fragmented market. The shift to video surveillance on IP networks and video analytics opens up new opportunities for development.

Due to the high level of expertise in IT in Quebec, Quebec businesses and universities are well positioned to take advantage of the opportunities in technological and commercial development that the emergence of intelligence video surveillance offers.

⁷¹ *Les Affaires*, *Genetec veut consolider ses acquis*, 5 July 2008, p. 24.

We have a few recommendations in order to benefit the position of Quebec businesses in this sector.

- With the advent of IP cameras and network surveillance, the IT community should work closely with the video surveillance industry. The migration of video surveillance systems to IP networks raises several IT issues, such as:
 - optimal network use (video transmission takes up a lot of bandwidth);
 - creation of software interfaces and components for intelligent management of video surveillance on the intranet or Internet;
 - efficient search of large, possibly video databases on network;
 - automatic integration of video surveillance with geomatic systems, GPS and other security systems.
- Quebec developers should take the intelligent turn begun in video surveillance. They would benefit from getting into this niche market and taking advantage of the video analytics expertise already found in Quebec universities and research centres. New intelligent video surveillance applications, such as consumer behaviour analysis and business operations management, appear to be commercially promising sectors since they show a return on the consumer's investment.
- Users should not only rely on hardware components, but also invest in system intelligence. The management of masses of video data must be anticipated and techniques developed to detect real-time anomalies, index video content and create video summaries for post-event searches.
- For example, developers and suppliers should work together and create a consortium in order to bring together all IP video surveillance players.
- Video management software developers should pay attention to the standardization efforts being made in IP video surveillance and take part in them.
- In order to ensure sufficient IP network video surveillance supply by competent suppliers, integrators-installers must be trained so as to acquire the IT skills and physical security knowledge that this technology requires.
- Integrators-installers should also be trained on video analytics products. Also, in order to increase the adoption of these technologies, developers should make the configuration and installation of their software applications as user-friendly as possible for integrators and installers.
- There is a need for "super-integrators" capable of coordinating the development and set-up of different built-in security systems, for centralized operations control of large security installations. This would make things easier for clients required to deal with several integrators to assemble a unified surveillance system.
- Clients (in government, transportation, education, etc.) should be made aware of the pros and cons of IP video and the possibilities of video analytics, without exaggerating them.

- When dealing with large deployments or when the network infrastructure is already in place, priority should be given to choosing IP video surveillance.
- Users should invest in wide-angle or panoramic camera systems and megapixel cameras, rather than in a large number of standard cameras. The inconvenience however is that a failure with a panoramic camera has more consequences than a failure in a few cameras on a large network.
- Quebec must offer more financial aid for marketing developed products and expanding businesses, because the funds are mainly allocated to research and development. Venture capital is often too hastily removed from companies.

5. ISSUES

Despite being widely adopted, video surveillance technology raises certain issues and faces significant resistance. This section deals with three video surveillance-related issues that may have a major impact on its implementation and development.

5.1 Protection of Privacy

Vast recourse to video surveillance in public and private places raises several concerns among groups that defend the respect of privacy. With cameras pointing everywhere in the streets, parks, buildings, businesses and possibly at work, many people fear misuse of these video recordings and the personal information they contain. Video surveillance must not be used to draw up profiles of the people filmed or for futile or discriminatory purposes when in the hands of public authorities and the forces of order.

The Office of the Privacy Commissioner of Canada has drafted guidelines in order to better define and oversee the use of this surveillance tool by authorities and police forces in public places⁷², and by private sector organizations⁷³. Video surveillance is subject to the *Personal Information Protection and Electronic Documents Act (PIPECA)*. However, Criminal Code provisions regarding the recording of private communications apply to the use of cameras that capture sounds.

“The guidelines set out principles for evaluating the need for resorting to video surveillance and for ensuring that, if it is conducted, it is done in a way that minimizes the impact on privacy.”⁷⁴ In general, the need for using surveillance cameras must be justified and other means should be given priority whenever possible. For example, a store may decide to lock up highly valuable items rather than resorting to continuous video surveillance. Video surveillance must therefore be used to deal with a real, specific and important problem. Also, the space covered by cameras and surveillance time must be reduced to the bare minimum. It is understood that cameras are prohibited in places where people usually expect to have privacy (washrooms, dressing rooms, fitting rooms, showers, etc.) The public must be informed of the presence of surveillance cameras and the people filmed are entitled to access to their personal information.

⁷² Office of the Privacy Commissioner of Canada Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities, 2006, http://www.privcom.gc.ca/information/guide/vs_060301_e.asp.

⁷³ Guidelines for Overt Video Surveillance in the Private Sector, 2008, http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_e.asp.

⁷⁴ OPC Guidelines for Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities, 2006, op.cit.

In the public sector, like the private sector, organizations using video surveillance must draft a policy on its use, specifically defining the objectives of surveillance and the location of the equipment, controlling access to the video captured, protecting personal information and limiting storage time of video footage, except, of course, for footage required for investigations.

These guidelines are not intended to interfere with police authority to conduct investigations. In the private sector, they apply only to overt equipment and do not cover covert equipment that may be used, for example, for insurance company investigations.

There is still little jurisprudence to guide the practice of employer use of video surveillance in companies. This situation deals with two competing rights: the employee's right to privacy in the workplace and the employer's right to protect his company. Once again, two principles should guide the installation of cameras in the workplace: evidence of the need for video surveillance to protect the premises, personnel and facilities under the employer's responsibility and the concern for minimizing the extent of the intrusion on the employee's privacy. For example, cameras would be acceptable to control access to the building or sensitive areas, but it would seem excessive to point a camera directly at an employee's work station and film said employee during his/her shift. An employer may only film an employee if there is reasonable doubt that he/she has committed or is on the verge of committing an offence. The video surveillance system cannot, however, be used to monitor employee productivity or assess work quality. Important note: the employer's responsibility for measured use of video surveillance extends to anyone viewing the video footage from the company's surveillance cameras, even sub-contractors hired to that effect.

The video surveillance boom in public places, companies and even private residences raises the issue of protecting the personal information of the people filmed. Although people are increasingly accepting of the presence of cameras for security purposes, protecting privacy remains a concern expressed when new surveillance cameras are deployed, especially in public areas.

Some people maintain that video analytics help to protect personal data captured on video. The automatic processing of images makes it possible to hide, for example, irrelevant faces or objects on the video prior to transmission for viewing. Furthermore, computer detection of suspicious individuals or behaviours may reduce the risk of profiling, i.e., monitoring based on the colour, race, or membership group of the people filmed. However the use of intelligent video surveillance for purposes other than security, such as consumer behaviour analysis, may call into question the principle behind the need for video surveillance.

5.2 Effectiveness of Video Surveillance in Reducing Crime

Video surveillance systems are deployed in most large cities around the world. Do these systems help to reduce and solve more crimes? There have been several studies conducted

on the effectiveness of video surveillance systems and their results differ greatly. Some studies reveal major drops in crime rates, while others find that video surveillance installation has a minor impact on crime.

Measuring the impact of video surveillance systems is a complex task since many factors may explain the rise or drop in crime. All variations should be placed in context, considering the general crime trend, its possible shift to other regions and the combined effect of several security measures, such as reinforced police patrols or improved lighting in an area.

After reviewing studies published on this topic, Dee and Velastin [8] report that there really is no hard evidence that video surveillance lowers crime rates. The ACLU Technology and Liberty Program states that, in order to assess the effectiveness of video surveillance, a meta-analysis should be conducted of several studies in order to obtain statistically solid data, rather than considering a single study⁷⁵. Similar studies conducted for the British Home Office note that video surveillance has little impact on lowering crime rates^{76, 77}.

A recent study done in the United States on the San Francisco video surveillance program, in neighbourhoods with high crime rates, revealed that installing surveillance cameras did not reduce the number of homicides and violent crimes. However, it did cause a drop in misdemeanours, such as armed robbery, burglaries and vandalism. Technological and organizational failures in the video surveillance system's operation were also identified. It should be noted that, in this program, police officers can only use video images as investigative tools when a crime is committed, in order to prevent the invasion of privacy that real-time surveillance would involve. In this context, the presence of cameras does not appear to discourage violent crimes, often committed irrationally, but it does seem to be effective in dissuading petty theft. This is one of the most complete reports on public surveillance in the United States⁷⁸.

There is therefore no clear evidence that installing surveillance cameras may reduce crime. In certain cases, video surveillance systems appeared to have an impact on premeditated crimes, but not on spontaneous crimes. The presence of cameras did, however, appear to be effective in reducing car thefts in parking lots.

With respect to crime-solving, an article from L'Actualité magazine reported that in London, the city with the most surveillance cameras, only 3% of thefts are solved using the

⁷⁵ Noam Biale, ACLU Technology and Liberty Program, *What Criminologists and Others Studying Cameras Have Found*, <http://www.youarebeingwatched.us/about/182/>.

⁷⁶ Welsh, B. and Farrington, D., *Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (2002), Home Office Research, Development and Statistics Directorate. Cited in <http://www.youarebeingwatched.us/about/182/#footnote10>.

⁷⁷ Gill and Spriggs, *Assessing the Impact of CCTV*. (2005) Home Office Study. Cited in <http://www.youarebeingwatched.us/about/182/#footnote10>.

⁷⁸ Security Info Watch, *Study gives split verdict on crime cameras*, 8 March 2009, <http://www.securityinfowatch.com/root+level/1309228>.

video surveillance system⁷⁹. It would be tedious for police officers to look through hoards of archived video images for their investigations. Yet, the London video surveillance system was indeed successful in helping to identify the terrorists who tried to blow up bombs in the subway system in 2005.

The conclusions of these studies reveal a serious problem with the effectiveness of video surveillance in fighting crime. Nevertheless, they do not prove the uselessness of video surveillance systems, either. The technical limits of these systems, the conditions under which they are deployed, and the way they are used have a major influence on the results obtained. For example, in order to be effective, these systems must be included as part of the security measures and be deployed with specific operational objectives.

When used alone, cameras do not appear to effectively discourage many crimes. Passive video surveillance (post-incident) does not help to prevent offences. However, active, ongoing surveillance raises the issue of respect for privacy. It is therefore imaginable that intelligent processing algorithms capable of triggering alarms effectively could allow for acceptable real-time surveillance to help intervene when crimes are being committed. Furthermore, video analytics could help to solve more crimes if it provides effective search methods for archived video footage. Improving image quality will undoubtedly mean major progress in identifying suspects.

5.3 Standards for IP Video

Now that video surveillance on IP networks has boomed, manufacturers are working on drafting a standard to govern communication between IP cameras and video management software. Each manufacturer must currently develop interfaces enabling their cameras to connect with each other and exchange information with video management software. This activity is costly, both in time and money. Adopting a standard, while encouraging the interoperability of the different products available, will enable the IP video surveillance market to develop more quickly, while reducing costs for manufacturers and clients.

While the SIA Standards Committee⁸⁰ has been working for some time on defining an IP video surveillance standard, two groups unhappy with the slowness of the process have launched their own initiatives, namely: PSIA (Physical Security Interoperability Alliance), led by Cisco Systems, DVTel, General Electric, Honeywell, IQinVision, Panasonic, Pelco and Verint, and ONVIF (Open Network Video Interface Forum), led by Axis, Bosch and Sony⁸¹.

⁷⁹ Schaëffner, Yves, « *Big Brother* » est aveugle, L'Actualité, 15 October 2008.

⁸⁰ <http://www.siaonline.org/content.aspx?id=4580>.

⁸¹ Honovich, J., *Will ONVIF or PSIA win the IP Camera Standards Battle?*, IP Video Market Info, http://ipvideomarket.info/report/onvif_psia_ip_camera_standards.

Without admitting it, these two groups are in a race to develop and impose their own standard in order to ensure they have a competitive edge in the market. Axis, Bosch and Sony already own over 50% of the camera market share. These companies will therefore benefit little from introducing a standard since, as leaders, their products are already supported by most video management systems. They would have a greater interest in controlling or delaying the development of a standard that would facilitate their competitors' access to the market. However, the manufacturers supporting PSIA have small shares of the camera market. That is why they are in a hurry to introduce a standard that would give them better interoperability with most of the video management software applications, and thus expand their market. It is also a major issue for manufacturers of analogue cameras, such as Pelco, GE and Honeywell, which are trying in turn to enter the IP camera market.

While the standard developed by ONVIF targets video connectivity, the PSIA standard targets vaster interoperability, covering several security platforms, including IP video, DVRs, analytics, access and audio. At the design level, PSIA is built like an API, while the ONVIF specifications are based on Web services using protocols such as *Extensible Markup Language* and *Web Services Description Language*.

The future will tell who will win the standards war. Perhaps unification is the answer? Support from the Security Industry Association (SIA) may determine which standard is adopted, which is why ONVIF and PSIA are working to harmonize their standards with those currently developed by the SIA.

BIBLIOGRAPHY

BOOKS

- [1] Nilsson, F. "Intelligent Network Video: Understanding Modern Video Surveillance System". Boca Raton: CRC Press, 2009. 389 p.
- [2] Transports Canada. *Réseau de télévision en circuit fermé : manuel de référence pour l'utilisation dans des applications de sécurité*. 2008. 79 p.

PROCEEDINGS FROM CONFERENCES, SEMINARS, WORKSHOPS

- [3] Cucchiara, R. "Multimedia surveillance systems" dans Proceedings of the third ACM International Workshop on Video Surveillance & Sensor Networks, International Multimedia Conference, pp. 3-10, Singapour, 2005.
- [4] Gagnon, L., Laliberté, L., Foucher, S, Laurendeau, D., Branzan Albu, A. "A System for Tracking and Recognising Pedestrian Faces using a Network of Loosely Coupled Cameras". SPIE Defense & Security: Visual Information Processing XV (SPIE #6246), Orlando, 2006.
- [5] Hampapur, A., Brown, L., Connell, J., Pankanti, S., Senior, A., Tian, Y. "Smart Surveillance: Applications, Technologies and Implications" dans *2003 Joint Conference of the Fourth International Conference on Information, Communications & Signal Processing and Fourth Pacific-Rim Conference on Multimedia*, pp. 1133-1138, vol.2. New York, État-Unis, December 15-18, 2003.
- [6] Sedky, M.H., Moniri, M., Chibelushi, C.C. "Classification of Smart Video Surveillance systems for Commercial Applications". IEEE Conference on Advanced Video and Signal Based Surveillance, Septembre 15-16, 2005. pp. 638-648.
- [7] Xiao, Z., Poursoltanmohammadi, A., Sorell, M. "Video motion detection beyond reasonable doubt", dans *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, article no 6, Adelaide, Australie, January 21-23, 2008.

PERIODICALS, MAGAZINES

- [8] Dee, H. M., Velastin, S. A. "How close are we to solving the problem of automated visual surveillance? A review of real-world surveillance, scientific progress and evaluative mechanisms". *Machine Vision and Applications*, 19 (5-6). Septembre 2008. pp. 329-343.

- [9] Foresti, G. L., Micheloni, C., Snidaro, L. Remagnino, P., Ellis, T. « Active Video-Based Surveillance System: The low-level image and video processing techniques needed for implementation ». IEEE Signal Processing Magazine, 22 (2) March 2005. pp. 25-37.
- [10] Hampapur, A., Brown, L., Connel, J., Ekin, A., Haas, N., Lu, M., Merkl H., Pankanti, S., ASenior, A., Shu, C.-F., Tian, Y. L., « Smart Video Surveillance : Exploring the concept of multiscale spatiotemporal tracking », IEEE Signal Processing Magazine, 22 (2) March 2005. pp. 38-51.
- [11] Hearing, N., Venetianer, P. L., Lipton, A. « The evolution of video surveillance: an overview». Machine Vision and Applications, 19 (5-6) September 2008 : pp. 279-290.
- [12] Hu, W., Tieniu, T., Wang, L., Maybank, S. « A Survey on Visual Surveillance of Object Motion and Behaviors ». IEEE Transactions on systems, man, and cybernetics-Part C: Applications and reviews, 34(3), août 2004, pp. 334-352.
- [13] Kosk, N., « OnSSI Secures 2008 Political Conventions ». Video Technology & Applications, Février 2009 : pp. 6-10.
- [14] Zhan, B., Monekosso, D. N., Remagnino, P., Velastin, S. A., Xu, L.-Q. “Crowd analysis: a survey”, Machine Vision and Applications, 19 (5-6) Septembre 2008. pp. 345-357.

TECHNICAL REPORTS

- [15] Axis Communications, *H.264 video compression standard. New possibilities within video surveillance*. Document technique. 2008. 9 p.
- [16] Biale, N. *Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found*. American Civil Liberties Union. 29 mai 2008, 6 p.
- [17] Fullerton, E. *Enabling Video Analytics - The advantages of an open platform IP video surveillance management solution for enaling video analytics*. White Paper, Milestone Systems, 2008, 20 p.
- [18] Gager, R. Special Report: Video Surveillance, State of the Market, SDM, vol. 38, no 3, p. 68.
- [19] Hewitson, N. *Video Content Analysis, shat is it and why would I want it*. White Paper, Smart CCTV Limited, 2005. 3 p.
- [20] Honovich, J., *Security Manager's Guide to Video Surveillance*. Version 2.0, IPVideoMarket.info, Novembre 2008, 131 p.

- [21] Institute of Management and Administration, Inc. *Security's Director Report*, Newsbrief, Février 2009.
- [22] King, et al. *CITRIS Report: The San Francisco Community Safety Camera Program – An Evaluation of the Effectiveness of San Francisco's Community Safety Cameras*. Décembre 2008, 184 p.
- [23] Kirstein, M. *The expanding World of IP Video Surveillance: Cameras, Storage, Technology and Semiconductors*. Multimedia Intelligence, 2008. 10 p. [MMI080405WP].
- [24] McNichol, J. Lav, I. J., *State Budget Troubles Worsen*, Center on Budget and Policy Priorities, 13 mars 2009.
- [25] Senior, A., Pankanti, S., Hampapur, A., Brown, L. Tian, Y.-L., Ekin, A. *Blinkering Surveillance: Enabling Video Privacy through Computer Vision*. IBM Research Report. 28 août 2003, 14 p. [RC22886 (W0308-109)].

PRESENTATIONS

- [26] Diamant, M. *Why is Everyone Migrating to Intelligent IP Video Surveillance?* ISC East, 29 octobre 2008.
- [27] Gorodnichy, D. *Systèmes de reconnaissance vidéo, Vidéotechnologie pour la sécurité : problèmes et solutions*. Atelier sur la sécurité du transport ferroviaire et urbain, Montréal, Novembre 2007.
- [28] Moellman, D. *VACE Program Manager Video Analysis and Content Extraction (VACE) R&D Program: Overview of Phase 2*. Novembre 2003.

ELECTRONIC REFERENCES IN ADDITION TO THOSE CITED IN THE TEXT

(Note: All electronic references were on-line on March 28, 2009)

Security and Video Surveillance

Castonguay, A. *La loi, l'ordre et la sécurité restent des priorités conservatrices*, Le Devoir, 27 février 2008, <http://www.ledevoir.com/2008/02/27/177974.html>.

Ministère des Relations internationales du Québec, *Contribuer à la sécurité du Québec et du continent nord-américain*,
http://www.mri.gouv.qc.ca/fr/politique_internationale/securete/index.asp.

Siemon, *CCTV & Video Surveillance over 10G ip™*,
http://www.siemon.com/us/white_papers/03-10-29-cctv.asp.

Wasatis, *Historique*, <http://www.wasatis.com/spip/spip.php?article5>.

Kammerer, D. *Police use of public video surveillance in Germany 1956: management of traffic, repression of flows, persuasion of offenders*, *Surveillance & Society*, Vol. 6, No 1 (2009), http://www.siemon.com/us/white_papers/03-10-29-cctv.asp.

Fullerton, E., *The History of Video Surveillance*, Milestone,
http://www.milestonesys.com/files/UserFiles/Articles/History_of_Video_Surveillance.pdf.

Wikipedia. *Vidéosurveillance*. <http://fr.wikipedia.org/wiki/Vidéosurveillance>.

Wikipedia. *Video Analytics*. http://en.wikipedia.org/wiki/Video_analytics.

Office québécois de la langues française, Grand dictionnaire terminologique,
<http://www.granddictionnaire.com>.

VideoAnalytics.net, *What Is Video Analytics / Intelligent Video Surveillance*,
<http://www.videoanalytics.net/articles/whatisva.html>.

Vlahos, J. *Surveillance Society: New High-Tech Cameras Are Watching You*,
PopularMechanics, janvier 2008,
http://popularmechanics.smartmoney.com/technology/military_law/4236865.html?page=1.

Cager, Y. *Smart Video Surveillance: Digital Technology vs. Tradition Analog Systems*,
Advanced Imaging Magazine, 8 juillet 2008,
<http://www.advancedimagingpro.com/publication/article.jsp?pubId=1&id=2537&pageNum=1>.

Vision Industrielle.Org, *Qu'est-ce que la télésurveillance intelligente ?*,
<http://www.visionindustrielle.org/visionwhat-remotemonitoring.php>.

VisioWave, *Intelligent Security Applications, Image Processing And Video Content Analysis*,
<http://www.visiowave.com/index.asp?index=intelligentVideo>.

Freschi, C., *A Smart Future for Video Surveillance*, *Security Magazine*, 1^{er} janvier 2009,
http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000364844.

IP Video Market Info, *Video Analytics Overview and News*,
<http://ipvideomarket.info/topics/VideoAnalytics>.

Honovich, J., *Top 3 Problems Limiting the Use and Growth of Video Analytics*, IP Video Market Info, 19 juin 2008, http://ipvideomarket.info/report/top_3_problems_limiting_the_use_and_growth_of_video_analytics

Automated Video Systems, *Video Surveillance made simple*, <http://www.ezwatch-security-cameras.com/downloads/>

Thomas, S. *Out-of-the-box Thinking—The Transition Away from Analog CCTV and DVRs to IP Video*, LossPreventionMagazine.com, 14 octobre 2008, http://www.losspreventionmagazine.com/wparchives_view.html?id=2234.

Hu, Y. H., *Survey of Video Surveillance Technology*, www.ece.wisc.edu/~facerec/cameranet/survey2008Oct03.ppt.

Honovich, J., *Should I Use IP Cameras? Re-Assessing IP Camera's Advantages*, IP Video Market Info, 14 mai 2008, http://ipvideomarket.info/report/should_i_use_ip_cameras_reviewing_ip_camera_advantages.

Honovich, J., *Top 5 IP Camera Problems*, 26 juillet 2008, IP Video Market Info, http://ipvideomarket.info/report/top_5_ip_camera_problems.

Digital Visions Security Technologies, *Digital IP Video Surveillance*, http://www.digitalvisionsllc.com/digital_ip_video_surveillance_systems.aspx.

VideoSurveillance.com, <http://www.videosurveillance.com>.

Applications

Genetec, *Solutions innovatrices*, <http://www.genetec.com/Francais/Solutions/Pages/solutions.aspx>.

VideoSurveillance.com, www.videosurveillance.com.

IndigoVision, Whatever your business, <http://www.indigovision.com/business.php#it>.

Osborn, A., *Top 7 non-security uses for video surveillance cameras -- more than just a crime prevention tool*, Video-Surveillance-Guide.com, <http://www.video-surveillance-guide.com/video-surveillance-cameras.htm>.

Industry Solutions, VideoSurveillance.com, <http://www.videosurveillance.com/industry-solutions/>.

Salvi, D. V., *A Clear View: Megapixel cameras playing into the gaming surveillance market*, 3 mars 2009, <http://www.secprodonline.com/Articles/2009/03/03/A-Clear-View.aspx>.

Bombardier, *Intégration d'un système de sécurité dans les trains de passagers*, 7 décembre 2006, http://www.aqtr.qc.ca/documents/14_AllocutionsConferences/7_decembre_ReneMeuser.pdf.

Transports Québec, Gestion de la circulation,
http://www.mtq.gouv.qc.ca/portal/page/portal/regions/montreal_ile/gestion_circulation.

Components and Architecture of a Surveillance System

BSI Alès, *Les différents types de caméras sur réseau informatique*,
<http://www.bsi.fr/Informatique/Informatiquedentreprise/Vid%C3%A9osurveillance/tabid/73/articleType/ArticleView/articleId/6/Default.aspx>.

Honovich, J., *Examining the Future of Video Surveillance Storage*, IP Video Market Info, 6 août 2008,
http://ipvideomarket.info/report/examining_the_future_of_video_surveillance_storage.

Honovich, J., *Should You Use Video Encoders?*, IP Video Market Info, 18 mars 2009,
http://ipvideomarket.info/report/video_surveillance_analog_encoders.

Grossman, R. *The Nuances of Network Video Recorder, Security Sales & Integration*, Août 2006, http://www.securitysales.com/t_inside.aspx?action=article&StoryID=2529.

Honovich, J., *Analytics - To Lead or Not to Lead*, IP Video Market Info, 19 septembre 2008, http://ipvideomarket.info/report/analytics_to_lead_or_not_to_lead.

Mobotix AG, http://www.mobotix.com/fre_CH/content/view/full/2.

Honovich, J., *Upcoming Panoramic Megapixel Camera from Scallop*, IP Video Market Info,
http://ipvideomarket.info/report/upcoming_panoramic_megapixel_camera_from_scallop.

Research, Companies, Commercial Products and Intelligent Functionalities

Carnegie Mellon University, Robotics Institute, *Overview*, <http://www.cs.cmu.edu/~vsam/>.

Networks & Organizations, *The Intelligence Community Invests in Video*, 9 mars 2006,
<http://www.intelligenceonline.com/c/illustrations/io/pdf/INT518%208.pdf>.

IBM, *IBM Smart Surveillance System (S3)*, <http://www.research.ibm.com/peoplevision/>.

Organix IT, <http://www.organixit.com>.

YouTube, *Trends and Solutions for Video Surveillance Market*,
<http://www.youtube.com/watch?v=l031ca0j7gk>.

Home Security Blog, *Video surveillance enhancements for Airport security*, 20 août 2008, <http://www.2mcctv.net/blog/content/view/69/26/>.

Honovich, J., *Upcoming Panoramic Megapixel Camera from Scallop*, IP Video Market Info, 9 janvier 2009, http://ipvideomarket.info/report/upcoming_panoramic_megapixel_camera_from_scallop.

Industrie Canada, *Répertoire d'entreprises par secteur industriel*, <http://www.ic.gc.ca/eic/site/company-entreprises.nsf/fra/accueil>.

Industrial Embedded Systems, *Matrox Graphics Unveils IP Video Decoding Accelerator for Surveillance Systems*, 17 novembre 2008, <http://www.industrial-embedded.com/news/db/?14296>.

Honovich, J., *Wireless Video Surveillance Tutorial*, IP Video Market Info, http://ipvideomarket.info/report/wireless_video_surveillance_tutorial.

ExpertsDuRisque.com, *Les softs d'analyse d'image*, http://www.expertsdurisque.com/annuaire/site/FR/Dossiers_produits/Dossiers_Securite/Les_softs_danalyse_dimage,I2404.htm?xtor=SEC-15.

ISC-West 2009, *Exhibitor list*, http://iscwest09.mapyourshow.com/2_1/search.cfm?let=@.

Face Recognition

Osborn, A., *How biometric technology is used in video surveillance*, <http://www.video-surveillance-guide.com/biometric-technology.htm>.

Face Recognition Homepage, <http://www.face-rec.org/general-info/>.

Woodward, J. D. et al., *Biometrics: A look at Facial Recognition*, http://electronics.howstuffworks.com/framed.htm?parent=facial-recognition.htm&url=http://www.rand.org/pubs/documented_briefings/DB396/DB396.pdf.

Howstuffworks, *Face Recognition*, <http://electronics.howstuffworks.com/framed.htm?parent=facial-recognition.htm&url=http://www.epic.org/privacy/facerecognition>.

Airport International, *3D face recognition technology*, <http://www.airport-int.com/categories/3d-face-recognition-technology/3d-face-recognition-technology.asp>.

Face Recognition Vendor Test 2006, <http://www.frvt.org/FRVT2006/default.aspx>.

Bryner, J., *Computers Get Better at Face Recognition*, Live Science, 24 janvier 2008, <http://www.livescience.com/technology/080124-face-recognition.html>.

Issues

Les chroniques judiciaires de Me Alain P. Lecours, *Vidéo surveillance en milieu de travail & protection de la vie privée*, <http://www.lecourslessard.com/droit-travail-video-surveillance-en-milieu-de-travail-protection-de-la-vie-privee.html>.

Conger, C., *Do police cameras reduce crime?*, Howstuffworks, <http://electronics.howstuffworks.com/police-camera-crime.htm>.

University of Victoria, *Does Video Surveillance Prevent Crime?*, <http://socialsciences.uvic.ca/about/VideoSurveillanceandCrime.htm>.

APPENDIX 1 – Major Research Programs in Intelligent Video Surveillance

This appendix provides a list of certain research programs that have greatly contributed to the development of analytics technologies for video surveillance. These programs and projects have helped to fund research work in universities and companies, and have often lead to the marketing of video analysis technologies for security purposes.

Projet	Description
Annotated Digital Video for Surveillance and Optimised Retrieval (ADVISOR) (Communauté européenne), 2000-2003 http://www.ist-world.org/ProjectDetails.aspx?ProjectId=3c4d4b1710844de5962bc5f91f7ec5c8	L'objectif de ce projet était de développer des outils logiciels pour la vidéosurveillance intelligente dans les transports publics. Il visait le développement de techniques pour la détection de mouvement, le suivi de personnes, la reconnaissance de comportements, la surveillance d'individus et de foules.
BEHAVE (Royaume-Uni., EPSRC), 2007 http://www.secure-force.eu/index.php?option=com_content&task=view&id=155&Itemid=9	L'objectif de ce projet est de développer des technologies pour détecter les comportements suspects dans les lieux publics, à partir de la vidéo provenant d'un réseau de plusieurs caméras.
Combat Zone That See (DARPA, États-Unis), 2003 http://www.atec-tec.net/fr/its_news_det.asp?code_news=1404	Programme qui fut lancé par l'armée américaine, sous la direction de la DARPA (Defense Advanced Research Projects Agency) et qui visait la surveillance dans les zones de conflits urbains grâce à un réseau de caméras. L'objectif était de développer des logiciels permettant de traiter l'information provenant des différentes caméras pour identifier les véhicules (type, couleur, et plaque d'immatriculation), les conducteurs et les événements suspects.
Context Aware Vision using Image-based Active Recognition (CAVIAR) (Communauté européenne), 2002-2005 http://homepages.inf.ed.ac.uk/rbf/CAVIAR/caviar.htm	Financé par la Information Society Technology, ce programme visait, entre autres, la reconnaissance d'objets, de contexte et de situations pour la surveillance urbaine et les analyses marketing.
Integrated Surveillance of Crowded Areas for Public Security (ISCAPS) (Europe) (consortium de dix entreprises et institutions académiques), 2005 http://www.iscaps.reading.ac.uk/	Mené par un consortium de dix entreprises et institutions académiques, ce projet vise la surveillance de foules et des lieux achalandés. Il vise notamment le développement d'outils biométriques pour l'identification de personnes.

Projet	Description
<p>Pro-active Integrated Systems for Security Management by Technological Institutional and Communications (PRISMATICA) (Communauté européenne), terminé en 2002 http://tf1.lci.fr/infos/high-tech/2001/0..818766.00-prismatica-informatique-service-securite-transport.html</p>	<p>Initié par six transporteurs européens, ce projet vise à renforcer la sécurité dans les transports publics, en développant des outils logiciels pour l'analyse des images de surveillance. Elle touche notamment à la détection de personnes et d'objets, ainsi qu'à l'analyse de leurs comportements, pour détecter des colis suspects ou des vols, par exemple.</p>
<p>Video Analysis and Content Extraction (VACE) (DTO, Etats-Unis) – Phase 3 : 2006-2009 http://www.perceptual-vision.com/vt4ns/vace_brochure.pdf</p>	<p>Programme mené par le Disruptive Technology Office (DTO), relevant du Director of National Intelligence (DNI). Il a pour objectif de développer des technologies d'analyse et d'indexation de la vidéo provenant de différentes sources, en particulier celle captée par les caméras de surveillance. Les recherches dans ce programme portent, notamment, sur l'extraction de données significatives à partir de la vidéo, la fusion multimodale, la reconnaissance et la compréhension de comportements à partir de différentes sources vidéo, dont celles provenant de caméras de surveillance.</p>
<p>Video Surveillance and Monitoring (VSAM), 1997-2000 http://www.cs.cmu.edu/~vsam/OldVsamWeb/vsamhome.html</p>	<p>Lancé et financé par le Information Systems Office de la Defense Advanced REsearch Projects Agency (DARPA), aux États-Unis. C'était l'un des premiers projets d'analyse en temps réel de données de vidéo surveillance pour l'intervention et la prévention d'incidents. L'objectif de ce projet était de développer la vidéo automatisée et la rendre capable de comprendre et évaluer l'information reçue pour l'utilisation dans des applications militaires de surveillance des zones urbaines ou de combat. La recherche portait, entre autres, sur la surveillance de zones étendues, la détection et le suivi d'objets en temps réel, la reconnaissance d'objets, le comptage de véhicules, le contrôle actif de caméras, la reconnaissance d'activités humaines.</p>

APPENDIX 2 – Research Groups (Quebec and United States)

This appendix provides a list of research groups in Quebec working in video analysis for intelligent video surveillance. American university laboratories contributing heavily to this field are also listed herein. Most of them have taken part in the VACE research program.

Laboratory/Group	Description of Work
Québec	
Laboratoire de Vision et Systèmes Numériques, Université Laval http://vision.gel.ulaval.ca/	Reconnaissance d'activités humaines. Modélisation de démarche humaine. Détection et suivi d'objet. Réseau de caméras intelligentes. Participation au projet MONNET, sur la surveillance d'environnements complexes et le suivi de personnes à l'aide d'un réseau faiblement couplé de caméras (http://vision.gel.ulaval.ca/fr/Projects/IdEns_41/index.php)
LITIV, École Polytechnique de Montréal http://www.polymtl.ca/litiv/en/	Traitement d'images et de la vidéo, entre autres, pour des applications de vidéosurveillance.
VidPro, Université Concordia http://users.encs.concordia.ca/~vidprog/	Détection et suivi d'objets, même sous occlusions. Détection d'événements. Application à la vidéosurveillance.
Groupe Vision et imagerie, CRIM http://www.crim.ca/fr/r-d/vision_imagerie/index.html	Détection et suivi d'objet, détection et reconnaissance de visage, reconnaissance d'expressions faciales, reconnaissance de plaques d'immatriculation, reconnaissance de mouvements anormaux, indexation de banques vidéo. Le groupe a mené plusieurs projets en vidéosurveillance pour la sécurité, dont MONNET, PTZ et VISU (http://www.crim.ca/fr/r-d/vision_imagerie/projets.html).
Visual Motor Research Lab, Université McGill http://www.cim.mcgill.ca/~clark/vmrl/web-content/vmrl.html	Détection d'anomalies pour la vidéosurveillance.

États-Unis	
Computer Vision Laboratory, University of Maryland http://www.cfar.umd.edu/cvl/	Reconnaissance d'objets. Détection et suivi de véhicules et d'humains. Caractérisation de la démarche humaine et reconnaissance faciale. Détection de la taille d'un individu. Identification de personnes dans les foules. Détection d'objets abandonnés.
Computer Vision Lab, University of Central Florida http://server.cs.ucf.edu/~vision/	Détection et suivi d'objet, reconnaissance d'activités humaines, analyse de foules et suivi d'individu dans des environnements peuplés.
Face Recognition and Video Processing Lab, New Jersey Institute of Technology http://www.cs.njit.edu/liu/FRVPlab/index.html	Reconnaissance de visages.
Informedia, Carnegie Mellon University http://www.informedia.cs.cmu.edu/	Participe au programme de recherche VACE. Indexation et recherche de contenus vidéo. Détection des personnes et patrons d'activité dans des images vidéo. Méthodes de protection des informations privées sur la vidéo visionnées par plusieurs usagers.
Institute for Robotics and Intelligent Systems, University of Southern California http://iris.usc.edu/	Participe au programme VACE. Détection et suivi d'objets et d'humains pour la vidéosurveillance. Reconnaissance d'activités et d'événements.
Robotics Institute, Carnegie Mellon University http://www.ri.cmu.edu/	Différents groupes couvrent des aspects de recherche applicables à la vidéosurveillance : détection et suivi de personnes, détection et reconnaissance faciale, identification de personnes, reconnaissance de gestes et de comportements humains.
Vision Research Group, Massachusetts Institute of Technology http://groups.csail.mit.edu/vision/app/	Avait participé au programme de recherche VISAM. Techniques d'analyse vidéo dans un réseau distribué de caméras : détection, suivi et reconnaissance d'objets, classification d'activités, détection d'événements normaux et anormaux.

Appendix 3 – Video Surveillance Companies (Quebec and elsewhere)

In view of the vast number of companies offering video surveillance products and services, an exhaustive list would be impossible to provide. This appendix lists the main companies found following Web searches, expert consultations and meetings held during the ISC-West 2008 and ISC-East 2008 conferences. Specific research was conducted to list Quebec companies, as well as those from other Canadian provinces that develop intelligent digital video surveillance products. These are listed first under each category of services. However, not all video surveillance integrators, installers and distributors have been indexed.

More exhaustive lists of companies in the field of security and video surveillance can be found on the following sites:

- http://www.canasa.org/en/membership/mem_directory/index.html.
- <http://www.sourcesecurity.com/companies.html>.
- <http://www.videosurveillance.com/manufacturers/>.
- <http://ipvideomarket.info/>.
- <http://www.iscwest.com/App/homepage.cfm?appname=180&moduleID=2958&LinkID=20077&submenuheader=7>.

Company descriptions were taken or adapted from the above Web references or company Web sites.

Large manufacturers or suppliers offering video surveillance security products	
Axis Communications (Suède) www.axis.com	Axis est le leader mondial du marché de la vidéo sur IP. Société suédoise fondée en 1984, elle dispose de filiales dans plus de 20 pays et travaille en coopération avec de nombreux partenaires dans plus de 70 pays. Axis s'est spécialisée dans les solutions professionnelles de vidéo sur IP destinées à la surveillance, la télésurveillance et la diffusion. Cette gamme de produits comprend des caméras réseau, des serveurs vidéo, des décodeurs vidéo, des logiciels de gestion vidéo, ainsi qu'un ensemble complet d'accessoires.
Bosch Security Systems (Allemagne) www.boschsecurity.com	Bosch Security Systems offre différents produits de sécurité, dont des systèmes de vidéosurveillance, incluant des solutions IP.
Checkpoint Systems (États-Unis) www.checkpointsystems.com	Checkpoint Systems offre une gamme complète de produits et services en sécurité, notamment des systèmes de vidéosurveillance.

Large manufacturers or suppliers offering video surveillance security products	
Cisco (États-Unis) www.cisco.com	Cisco offre une solution complète de vidéosurveillance qui s'intègre à ses équipements de réseau. L'entreprise vend notamment des encodeurs (fournis par SyPixx) et un logiciel de gestion vidéo (développé par Broadware) qui peut fonctionner sur les routeurs de Cisco. Ce géant des TI commercialise aussi deux caméras IP.
D-Link (Taiwan) www.dlink.com/products/end-to-end-surveillance	À travers ses partenariats avec les fabricants et développeurs de composants de vidéosurveillance, D-Link offre des solutions complètes de vidéosurveillance IP.
GE Security (États-Unis) www.gesecurity.com	GE Security vend différents systèmes de sécurité, dont des outils de vidéosurveillance. L'entreprise offre même un logiciel de gestion vidéo intelligent (VisioWave Intelligent Video Platform).
Honeywell Security (États-Unis) www.honeywellvideo.com	Honeywell Security est un fournisseur et un distributeur international de systèmes électroniques de sécurité. L'entreprise commercialise Digital Video Manager, une solution de vidéosurveillance numérique en réseau basée sur une architecture ouverte.
JVC (États-Unis) www.pro.jvc.com	Géant de l'électronique, JVC vend des caméras analogiques, mais fabrique aussi une gamme de caméras et d'accessoires de surveillance IP. L'entreprise produit aussi des enregistreurs numériques réseau (NVR).
Mitsubishi (Japon) www.mitsubishi.com	À travers ses différentes divisions, Mitsubishi fabrique plusieurs produits de vidéosurveillance, dont des enregistreurs numériques, des murs d'écrans et, plus récemment, des caméras IP.
Panasonic (Japon) www.panasonic.com/business/security/home.asp	Panasonic est l'un des principaux fabricants de caméras analogiques. L'entreprise développe aussi une gamme d'enregistreurs numériques et de caméras IP pour la surveillance. Celles-ci viennent sous différentes formes : mégapixel, PTZ, dôme.
Pelco (États-Unis) www.pelco.com	Pelco est l'une des plus grandes entreprises en vidéosurveillance et le leader des fabricants de caméras analogiques. L'entreprise offre une gamme étendue de composants de vidéosurveillance, dont des solutions de gestion vidéo sur enregistreur numérique, traditionnel ou hybride, et sur enregistreur réseau. Pelco s'est lancée dans le marché des caméras IP en commercialisant quelques modèles.
Samsung GVI (États-Unis) www.gviss.com	Samsung GVI offre une suite complète de solutions de vidéosurveillance et de solutions intégrées de sécurité qui permettent la vidéosurveillance intelligente.
Toshiba (Japon) www.toshiba.com	Toshiba offre une gamme complète de produits de vidéosurveillance, incluant des caméras analogiques et IP, moniteurs, enregistreurs numériques et réseau. Ses caméras IP sont réputées pour la qualité de leur image dans des conditions de faible illumination.
Tyco International (Bermudes) www.tyco.com	Tyco International est une entreprise diversifiée offrant des produits et des services dans 60 pays. Elle commercialise une gamme étendue de technologies de contrôle d'accès et de vidéo sous ses différentes marques : Software House, American Dynamics and Kantech.

Large manufacturers or suppliers offering video surveillance security products	
Vicon (États-Unis) www.vicon-cctv.com	Vicon développe, manufacture et commercialise des solutions complètes sur réseau IP pour intégrer la vidéosurveillance avec le contrôle d'accès. L'entreprise offre des logiciels de gestion vidéo, des enregistreurs numériques et réseau, des encodeurs et décodeurs, ainsi que des caméras (IP, mégapixel, analogiques, dôme).

Video management and IP video surveillance system software	
Genetec (Québec) www.genetec.com	Genetec est l'un des plus grands développeurs de logiciel de vidéosurveillance IP. Il développe Omnicast™, une solution de vidéosurveillance sur IP. Ce logiciel intègre les technologies d'analyse vidéo de partenaires. Celles-ci permettent la détection et l'identification d'objets et d'individus, ainsi que la reconnaissance de comportements inhabituels. La solution AutoVu permet la reconnaissance automatisée de plaques d'immatriculation dans des applications fixes et mobiles.
Aimetis (Ontario) www.aimetis.com	Aimetis développe un logiciel de gestion vidéo supportant les caméras analogiques et numériques intégrant des bibliothèques de fonctions d'analytique vidéo pour des applications spécifiques. L'entreprise développe notamment des algorithmes propriétaires de détection et de suivi d'objets (voitures/personnes) fonctionnant sous des conditions changeantes d'illumination et de météo, de comptage de personnes, de détection et classification d'événements tels que les intrusions, les stationnements interdits et les fraudes au guichet automatique. Ses marchés principaux touchent aux applications de surveillance extérieure et au commerce de détail.
Impath Networks (Nouvelle-Écosse) www.impathnetworks.com	Impath offre i-Volution, une gamme de produits de vidéosurveillance sur réseau IP, ainsi que TeleVue, un logiciel de gestion d'application permettant de configurer et contrôler l'équipement vidéo en réseau.
March Networks (Ontario) www.marchnetworks.com	March Networks commercialise la gamme de produits VideoSphere pour la vidéosurveillance IP sur des réseaux filaires ou sans fil. L'entreprise offre des caméras IP, des enregistreurs numériques, des encodeurs et un logiciel de gestion vidéo. Ce dernier inclut des fonctionnalités d'analytique pour la surveillance aux points de vente. Son principal compétiteur est Verint.
AMAG Technology (Royaume-Uni) www.amag.com	AMAG Technology développe un système de gestion de la sécurité pour l'industrie et les gouvernements. Celui-ci comprend <i>Symmetry Video</i> , une plateforme ouverte de gestion vidéo pour les serveurs vidéo, les enregistreurs vidéo numériques et les caméras IP.
American Dynamics (États-Unis, une entreprise de Tyco) www.americandynamics.net	La famille de produits Intellex® offre des solutions de surveillance vidéo intégrant systèmes analogiques et IP. L'entreprise est l'un des plus gros vendeurs d'enregistreurs numériques au monde. Elle a acquis, en 2008, Intellivid, compagnie spécialisée en analytique vidéo.
Aventura Technologies (États-Unis) www.aventuratechnologies.com	Aventura Technologies développe un logiciel de gestion vidéo qui possède les fonctionnalités standards de navigation dans la vidéo. Celle-ci inclut des fonctions d'analytiques vidéo, telles que la détection de personnes basée sur la couleur et la texture de la peau, la détection et le suivi d'objet et la reconnaissance d'activités. Ces détections nécessitent un paramétrage chez le client.

Video management and IP video surveillance system software	
Exacq (États-Unis) www.exacq.com	Exacq Technologies Inc. développe un système de gestion vidéo à architecture ouverte dont la qualité est reconnue.
IBM (États-Unis) www.ibm.com	IBM offre des solutions intégrées de vidéosurveillance et de sécurité. L'entreprise mène aussi des travaux de recherche dans le domaine de l'analytique vidéo. Elle commercialise un système de vidéosurveillance intelligente basé sur une architecture ouverte.
IndigoVision (Royaume-Uni) www.indigovision.com	IndigoVision offre une solution de vidéosurveillance IP de bout en bout. Sa ligne de produit comprend des caméras IP, des encodeurs, des enregistreurs sur réseau et un logiciel de gestion vidéo. L'entreprise développe son propre CODEC. Ses produits ne supportent pas les caméras de concurrents. IndigoVision a obtenu un contrat de plusieurs millions de dollars de l'Agence des services frontaliers du Canada, pour déployer des caméras IP aux postes frontaliers entre le Canada et les États-Unis
Milestone (Danemark) www.milestonesys.com	Milestone développe la plateforme de gestion de vidéosurveillance IP ouverte Milestone XProtect™. L'interface permet d'intégrer plusieurs modules d'analytique vidéo. Cette entreprise se spécialise dans le logiciel et ne vend pas de composants matérielles. Son logiciel supporte un grand nombre de caméras et systèmes de sécurité sur le marché.
Mosaic Dynamic Solutions (États-Unis) www.mosaicdyns.com	Mosaic Dynamic Solutions offre plusieurs produits pour la surveillance et le suivi des actifs d'une organisation. L'entreprise commercialise des solutions d'analytique vidéo permettant la détection d'objet, la reconnaissance de comportements suspects, la reconnaissance de visages et de plaques d'immatriculation.
Nice Systems (Israël) www.nice.com	Nice fournit des solutions complètes de sécurité, notamment des produits de vidéosurveillance. Nice Inform capture et synchronise des données multimédia pour la surveillance (voix, vidéo, texte, etc.) pour les fins d'enquêtes.
OnSSI, On-Net Surveillance Systems Inc. (États-Unis) www.onssi.com	OnSSI développe Ocularis, un logiciel de gestion vidéo IP qui comprend une interface très sophistiquée offrant plusieurs outils de navigation et de visualisation à l'utilisateur.
Video Insight (États-Unis) www.video-insight.com	Video Insight développe une suite étendue de modules logiciels pour la gestion de la vidéosurveillance.
3VR (États-Unis) www.3vr.com	3VR commercialise un logiciel de gestion vidéo pour la surveillance permettant des recherches avancées grâce à des outils intégrés d'analytique vidéo (reconnaissance de visages, reconnaissance de plaques d'immatriculation, détection de mouvement).

Cameras	
ImmerVision (Québec) www.immervision.com	ImmerVision commercialise la technologie brevetée Panomorphe, qui comprend une lentille grand angle accompagnée d'algorithmes de gestion de la distorsion. Cette lentille offre un champ de vision oval de 360° par 180°, dont la résolution ne diminue pas en périphérie. Elle s'adapte sur une caméra ordinaire, ce qui constitue un net avantage commercial sur son principal concurrent, Grandeye. La lentille Panomorphe utilise 33 % plus de pixels que la technologie <i>fisheye</i> . Toutes les vues PTZ sont recréées numériquement. L'entreprise offre aussi une librairie logicielle gratuite permettant de gérer l'affichage des images vidéo et la navigation dans celles-ci. Cette librairie peut être intégrée aux enregistreurs numériques et réseau.
Avigilon (Colombie-Britannique) www.avigilon.com	Bien qu'elle offre des caméras IP, des encodeurs et des logiciels de gestion vidéo, Avigilon se spécialise dans les caméras mégapixel (jusqu'à 16 mégapixels) et l'optimisation de la vidéosurveillance en haute définition. Ces produits sont particulièrement bien adaptés pour les environnements extérieurs. Cette entreprise supporte peu de systèmes de tiers.
Lumenera (Ontario) www.lumenera.com	Lumenera commercialise une gamme de caméras mégapixel (jusqu'à 11 mégapixels), sensibles à de faibles éclairages. Supporte l'analytique vidéo pour leur série <i>li</i> et est partenaire de ObjectVideo.
ACTi (Taiwan) www.acti.com	ACTi offre une gamme complète de caméras IP de bonne qualité à bas prix, ainsi que des logiciels d'enregistrement sur réseau. Les caméras d'ACTi sont supportées par plusieurs fabricants d'enregistreurs numériques. Les caméras de l'entreprise constituent souvent une alternative moins coûteuse par rapport aux caméras d'Axis.
Arecont Vision (États-Unis) www.arecontvision.com	Arecont Vision offre une ligne complète de caméras mégapixel (jusqu'à 8 mégapixels), à des prix inférieurs à ses principaux concurrents, IQInVision et Lumenera. En 2008, l'entreprise a commencé à supporter la compression H.264, ce qui pourrait avoir un impact majeur sur l'industrie.
Grandeye (Royaume-Uni) http://www.grandeye.com/	GrandEye commercialise des caméras panoramiques, en versions analogiques ou IP. La version IP offre cinq mégapixels de résolution. Ses principaux concurrents sont Mobotix et ImmerVision.
IPIX Corporation (États-Unis) www.ipix.com	IPIX a développé l'un des premiers systèmes permettant de produire des images 360° par 360° (<i>fish eye</i>) dans lesquelles on peut naviguer. En sécurité, Grandeye commercialise la technologie d'IPIX sous une marque conjointe.
IQinVision (États-Unis) www.iqeye.com/	IQinVision commercialise des caméras mégapixels et intelligentes. L'entreprise est implantée dans le marché de la vidéosurveillance en haute définition depuis 1998. Elle offre des caméras jour/nuit, des caméras à dôme résistantes aux vandalisme et des caméras IP résistantes aux intempéries.
Linksys (États-Unis, une entreprise de Cisco) www.linksys.com	Linksys fournit des caméras numériques sans fil se connectant à un réseau. Les solutions offertes par Linksys visent les petites entreprises et les résidences.
Logitech (États-Unis) www.logitech.com	Logitech est une manufacture des webcams de surveillance pour le grand public.

Cameras	
Robotix (Allemagne) www.robotix.com	Robotix commercialise des caméras réseau haute résolution et des systèmes de vidéosurveillance décentralisés. L'entreprise occupe la deuxième place du secteur en Europe et la quatrième au niveau mondial. Avec une résolution de 3,1 mégapixels, les caméras ROBOTIX offrent une image 30 fois plus précise que les caméras analogiques. C'est pourquoi elles permettent de surveiller des zones plus vastes, avec une vision à 360°, réduisant ainsi le nombre de caméras requises et les coûts s'y rattachant.
Scallop Imaging (États-Unis) www.scallopimaging.com	Cette entreprise produit la caméra D7, une caméra de sept mégapixels pour la surveillance, fournissant un champ de vision de 180° sans aucune distorsion de l'image.
Theia (États-Unis) http://www.theiatech.com/	Theia produit des lentilles grand angle pour les caméras mégapixels, permettant de couvrir une très large zone de surveillance.
Vivotek (Taiwan) www.vivotek.com	Vivotek offre une vaste gamme de caméras IP économiques. Il est le plus grand fournisseur dans le segment de marché bas de gamme pour les consommateurs et les petites entreprises.

Wireless	
Réseaux Eagle (Québec) www.reseauxeagle.com	Cette entreprise se spécialise dans le déploiement, la gestion et la sécurité de réseaux sans fil, notamment pour la vidéosurveillance. Elle est spécialiste des réseaux de type 802.11.
Firetide (États-Unis) www.firetide.com	Firetide fournit des produits pour l'infrastructure et l'accès dans les réseaux à transmission sans fil. Elle offre des solutions spécialisées pour la vidéosurveillance, mais aussi pour la téléphonie et les données. Les produits de Firetide ont été implantés à Phoenix pour la surveillance du Super Bowl 2008.
Strix Systems (États-Unis) www.strixsystems.com	Strix Systems est un fournisseur d'équipements pour les réseaux sans-fil. Ses solutions permettent de déployer un réseau distribué de vidéosurveillance IP, dont les composantes (caméras, serveurs vidéo, archivage, logiciels et systèmes de visionnement) peuvent être géographiquement distribuées.
Tropos Networks (États-Unis) www.tropos.com	Tropos Networks est un chef de file dans les réseaux sans fil à large bande permettant aux clients de déployer une infrastructure IP, notamment pour la vidéosurveillance.

Other video surveillance companies	
VideoWave Networks (Québec) www.videowave.ca	VideoWave Networks Inc. est une firme canadienne basée à Saint-Laurent, spécialisée dans la conception de systèmes intelligents de vidéo surveillance visant à optimiser la sécurité des particuliers, des entreprises et agences gouvernementales. L'équipe de concepteurs de VideoWave a conçu le produit VST-OneTrack, un système de tracking avec caméra PTZ, pour lequel VideoWave s'est mérité le prix Octas 2006 dans la catégorie Innovation technologique. Outre ses produits propriétaires, VideoWave propose une gamme complète d'enregistreurs numériques, caméras et serveurs vidéo.

Other video surveillance companies	
Visio-Soft (Québec) www.visio-soft.com	Visio-soft offre des systèmes de surveillance intégrés, entièrement numériques, sur les protocoles de communications réseaux TCP/IP. L'entreprise détient son propre codec, appelé W1. Elle offre aussi des solutions pour la vidéosurveillance par cellulaire nécessitant une transmission à bas débit.
AdvancedIO (Colombie-Britannique) www.advancedio.com	AdvancedIO vend des produits de connectivité Ethernet gigabit adapté pour le transfert IP, notamment de vidéo, dans les systèmes informatiques à haute performance.
Extreme CCTV (Colombie-Britannique) www.ExtremeCCTV.com	Manufacturier de systèmes de vision nocturne active, à partir d'illumination infrarouge, Extreme CCTV vend ses produits pour la surveillance d'installations critiques, la Défense, la sécurité intérieure, les transports et les sites patrimoniaux.
Micro Video (Ontario) www.microvideo.ca	Micro Video commercialise des caméras miniatures de vidéosurveillance.
Pleora Technologies (Ontario) www.pleora.com	Pleora Technologies fournit des solutions de connectivité Ethernet gigabit pour la vidéosurveillance, la diffusion vidéo et la visionique.
Visual Defence (Ontario, avec bureau à Montréal) www.visualdefence.com	Cette entreprise intègre et installe de l'équipement de vidéosurveillance, tels que caméras, enregistreurs numériques et logiciels d'analytique vidéo.
ADI-Burtek (États-Unis, point de vente au Québec) www.adi-burtek.com	ADI-Burtek est un distributeur de produits électroniques, notamment de vidéosurveillance.
ADT (États-Unis, bureaux au Canada, entreprise de Tyco) www.adt.com	Établi à travers le monde, ADT est l'un des plus grands intégrateurs de systèmes de sécurité. ADT intègre et commercialise les produits de vidéosurveillance de Cisco.
ATEME (France, bureau au Québec) www.ateme.com	ATEME est un fabricant d'encodeurs et d'enregistreurs vidéo pour la surveillance. Il fournit des solutions de compression, notamment selon les standards MPEG-4 et H.264.
ICX Vision Systems (États-Unis) www.visionsystems.icxt.com	ICx Vision Systems (anciennement PureTech Systems, Inc., division de ICX Technologies) développe PureActiv™, un système pour la surveillance automatisée sur des sites extérieurs. Ce système permet de détecter et suivre les objets, détecter les intrusions, contrôler des caméras, pour générer des alarmes et transmettre les séquences présentant une activité suspecte.
Intransa (États-Unis) www.intransa.com	Intransa vend des solutions de stockage en grappe (<i>cluster storage</i>) offrant des centaines de téraoctets d'espace d'archivage pour les systèmes de gestion vidéo IP. Concurrent direct de Pivot3 ou de fournisseurs de solutions de stockage, tels que EMC et Dell.
Pivot3 (États-Unis) www.pivot3.com	Pivot3 vend des solutions de stockage en grappe (<i>cluster storage</i>) offrant des centaines de téraoctets d'espace d'archivage pour les systèmes de gestion vidéo IP. Concurrent direct de Intransa ou de fournisseurs de solutions de stockage, tels que EMC et Dell.

Other video surveillance companies	
Simplex Grinnell (États-Unis, bureaux au Canada) www.simplexgrinnell.com	Simplex Grinnell vend différents systèmes de sécurité, dont de vidéosurveillance, en intégrant les solutions de partenaires.
Tri-ED (États-Unis, point de vente au Québec) www.tri-ed.com	Tri-ED est un distributeur nord-américain de produits de sécurité et de domotique.

Appendix 4 – Specialized video analytics software design companies

This section lists the major video analytics software developers. These products are quite often built into the video management software of partner companies. It includes a short list of companies specialized in face recognition and license plate recognition products.

Company	Company Description / Product	Intelligent Functionalities
Organix IT (Québec) www.organixitt.com	Logiciels de vidéosurveillance SVMS qui inclut des fonctionnalités intelligentes. Intègre la technologie de ISS pour la détection et le suivi d'objets, ainsi que la reconnaissance de comportements.	<ul style="list-style-type: none"> • Détection et suivi d'humains. • Reconnaissance de comportements : bagarre, course, saut par-dessus une guérite, graffiti. • Détection d'objets abandonnés. • Détection de fraude aux points de services. • Monitoring de trafic : accidents, objets sur la chaussée, limites de vitesse enfreintes, congestion, piétons, etc. • Comptage de personnes et détection d'affluence. • Reconnaissance de visages (atteint un taux de précision de 93 %). • Reconnaissance de plaques d'immatriculation, acquisition à 60 km/h.
IntelliView Technologies (Alberta) www.intelliview.ca	Développe et commercialise un système complet d'analytique et de gestion vidéo. L'analyse vidéo est faite dans un DVR.	<ul style="list-style-type: none"> • Détection d'intrusion dans un périmètre. • Activation de PTZ pour suivi d'objet. • Reconnaissance de plaques d'immatriculation. • Filtrage des fausses alarmes causées par les variations environnementales, telles qu'ombres, reflets et neige. • Création de sommaires vidéo pour condenser les séquences à visionner.

Company	Company Description / Product	Intelligent Functionalities
Agent VI (États-Unis) www.agentvi.com	Plateforme logicielle dont l'architecture répartit les traitements entre le serveur et les équipements de périphérie (caméras et encodeurs). Déployée dans plus de 25 pays, dans les principaux secteurs d'application.	<ul style="list-style-type: none"> • Détection de voitures : stationnement illégal, circulation à contresens, passage de plusieurs voitures sous une seule identification (tailgating). • Détection d'objets suspects ou abandonnés. • Détection et suivi d'individus, détection d'attroupements. • Comportements : Détection d'intrusions, rôdeurs, entrée de deux personnes en même temps à un point de contrôle.
Cernium (États-Unis) www.cernium.com	Suite de produits d'analytique : Perceptrak® (intégré avec Milestone), Cernium Edge™, ExitSentry® (détection de déplacement à contresens dans des aires contrôlées, destiné aux aéroports) et Archerfish™ (solution domestique). Reconnue par Frost & Sullivan à titre d'entreprise nord-américaine émergente de l'année 2008.	<ul style="list-style-type: none"> • Détection de personnes, d'objets et de véhicules et de leur modèle de mouvement. • Reconnaissance de comportements. • Détection de personnes circulant à contresens.
Intelligent Security Systems (ISS) International (États-Unis) www.isscctv.com	Implantée en Amérique et en Europe, cette entreprise offre une gamme étendue de solutions pour la vidéosurveillance, incluant des modules d'analytique. Intègre les produits de tiers.	<ul style="list-style-type: none"> • Reconnaissance faciale (précision de 95 %, meilleur système selon l'évaluation du département de la Défense). • Monitoring de trafic. • Reconnaissance d'inscriptions sur les conteneurs. • Reconnaissance de plaques d'immatriculation (capture jusqu'à 150 km/h avec un taux de reconnaissance entre 60 % et 95 %). • Détection de fraudes aux points de service et systèmes de guichets automatiques. • Comptage de personnes.
Intellivid (États-Unis) www.intellivid.com	Développeur d'analytique vidéo spécialisé pour l'industrie du commerce de détail. L'entreprise a été achetée par Tyco, en 2008.	<ul style="list-style-type: none"> • Surveillance des actifs de valeur et détection de vols. • Détection d'intrusion dans une zone à accès contrôlé. • Suivi de suspects d'une caméra à l'autre. • Analyse des déplacements et comportements des consommateurs. • Monitoring de l'affluence des clients pour permettre d'adapter le service.

Company	Company Description / Product	Intelligent Functionalities
Ioimage (Israël) www.ioimage.com	Fondée en 2000, commercialise des encodeurs et des caméras intégrant des fonctions d'analytique vidéo, ainsi qu'un logiciel intelligent de gestion vidéo centralisée.	<ul style="list-style-type: none"> • Détection d'intrusions : intrusions dans une aire contrôlée, <i>tripwire</i>, violation de périmètre. • Détection d'objet abandonné ou subtilisé. • Détection de rôdeur. • Détection de véhicule stationné. • Activation de caméra PTZ pour suivi d'objet. • Détection d'altération de caméras.
Iomniscient (Australie, bureau à Toronto) www.iomniscient.com	Fondée en 2001, l'entreprise offre une gamme étendue de fonctions analytiques. Elle développe et commercialise une suite logicielle d'analytique vidéo, Genius Range, basée sur un algorithme breveté de détection d'absence de mouvement.	<ul style="list-style-type: none"> • Détection d'objet abandonné dans une foule. • Détection de vol ou de graffiti/vandalisme dans une foule. • Détection d'objet présentant un contraste très faible. • Gestion de foule et de files d'attentes. • Détection de chutes. • Comptage de personnes et véhicules. • Comportements : détection de rôdeurs, personne courant, objet se déplaçant à contresens. • Détection de course. • Protection de périmètres, détection d'intrusion. • Analyse de vitesse/détection d'excès de vitesse. • Reconnaissance de plaques d'immatriculation.

Company	Company Description / Product	Intelligent Functionalities
<p>Mate (Israël) www.mate.co.il (Israël) www.mateusa.net (États-Unis)</p>	<p>Fournit une solution complète d'analytique vidéo pour des analyses centralisées ou en périphérie, selon trois couches : protection du périmètre, protection du site et contrôle d'accès. Mate Cortex est un système de gestion d'analytique vidéo destiné à la gestion d'alarme provenant de plusieurs périphériques d'analytique vidéo, tels que :</p> <ul style="list-style-type: none"> • Behavior Watch : Système avancé d'analytique vidéo. • Trigger : Encodeur vidéo analytique permettant d'effectuer des analyses vidéo à partir de la caméra. • iSense : Appareil vidéo de comptage de personnes avec caméra intégrée. <p>Count Watch : Système de comptage de personnes ou véhicules à partir de la vidéo captée par une caméra placée en hauteur.</p>	<ul style="list-style-type: none"> • Détection de mouvement. • Détection de trajectoire. • Détection d'objet statique. • Détection de présence dans des zones définies. • Détection d'objets circulant à contresens. • Détection de déplacement ou retrait d'objet. • Analyse de la vitesse d'un objet.

Company	Company Description / Product	Intelligent Functionalities
ObjectVideo (États-Unis) www.objectvideo.com	Fondée en 1998, commercialise deux plateformes d'analytique vidéo : ObjectVideo OnBoard, pour l'analytique embarquée dans des périphériques, et ObjectVideo VEW, une application sur serveur. Offre une solution avancée de comptage de personnes (ne nécessite pas de vue de haut). Avec plus de 770 000 canaux d'analyse vidéo vendus dans le monde, ObjectVideo® est le premier fournisseur de logiciel vidéo intelligent.	<ul style="list-style-type: none"> • Détection, classification et suivi d'objets. • Détection d'intrusion. • Détection de comportements suspects, tels qu'une personne rôdant. • Détection d'objet abandonné ou subtilisé. • Comptage de personnes ou de véhicules applicable, par exemple, à la gestion de file d'attente ou le monitoring de trafic. • Activation de fonctions PTZ pour le suivi d'objet suite à une alarme. • Fonctionnalités de recherche à base de règles.
Vidient (États-Unis) www.vidient.com	Fondée en 2003, cette entreprise commercialise une technologie initialement développée chez NEC Labs. Smar'Catch, le produit d'analytique de Vidient est notamment intégré dans les systèmes d'Unisys, NEC, et Raytheon	<ul style="list-style-type: none"> • Détection d'intrusions : personne ou véhicule dans une zone interdite, violation d'un périmètre de sécurité, plusieurs personnes ou véhicules entrant avec la même carte d'accès, intrusion par une sortie, personne passant au-dessus ou au-dessous d'une guérite. • Détections de menaces : rôdeurs, voiture stationnée près d'infrastructures sensibles, objets abandonnés/subtilisés, formation d'attroupements, personnes en surnombre. • Suivi par caméra PTZ activé sur alarme.

Face Recognition

Company	Description
Animetrics (États-Unis) www.animetrics.com	Animetrics développe des algorithmes permettant de recréer un modèle 3D à partir de deux photos d'un visage. Cette technologie est commercialisée en différents produits, dont Animetric90 permettant la reconnaissance faciale robuste à des rotations de +/- 45°.
Cognitec Systems GmbH (Allemagne) www.cognitec-systems.de	Cognitec commercialise FaceVACS, un logiciel de reconnaissance faciale. L'entreprise développe sa technologie depuis 1995.
Geometrix (États-Unis) www.geometrix.com	Geometrix développe des produits d'identification biométrique combinant reconnaissance 3D et 2D du visage et des empreintes digitales. Sa technologie de reconnaissance faciale combine deux caméras ou plus pour bâtir une forme 3D par triangulation.
L-1 Identity Solutions (États-Unis) www.l1id.com	L-1 Identity Solutions offre des solutions matérielles et logicielles, ainsi que des services, pour les applications d'identification d'individu et de contrôle d'accès. L'entreprise commercialise notamment une plateforme biométrique multi-modale, incluant de la reconnaissance faciale.
Note: Other face recognition software designers can be found at:	

License Plate Recognition

Company	License Plate Recognition Product
Genetec (Québec) www.genetec.com	AutoVu : http://www.genetec.com/Francais/Products/Pages/license-plate-recognition.aspx
Adaptive Recognition Hungary (Hongrie) www.anpr.net	CARMEN®
CitySync (Royaume-Uni) www.citysync.co.uk	Développe un logiciel de reconnaissance de plaques d'immatriculation et manufacture des produits matériels reliés.
Hi-Tech Solutions (Israël) www.x.htsol.com	Ligne de produits SeeCar : www.htsol.com/Products/SeeCar.html
INEX/ZAMIR (Israël) www.inexzamor.com	Offre plusieurs produits matériels et logiciels pour différentes applications de reconnaissance de plaques.
LPREditor (France) www.lpreditor.com	Commercialise des systèmes mobiles et fixes pour la reconnaissance de plaques d'immatriculation.

Company	License Plate Recognition Product
Milestone (Danemark) www.milestonesys.com	XProtect Analytics - License Plate Recognition : http://www.milestonesys.com/products/value_add_products/video_analytics/license-plate-recognition
Optasia (Singapoure) www.singaporegateway.com/optasia/imps.html	IMPS™ : www.singaporegateway.com/optasia/imps.html
Pips Technology (Royaume-Uni) www.pipstechnology.com	Commercialise une gamme complète de produits (caméras, logiciels, accessoires) pour la reconnaissance de plaques d'immatriculation.

APPENDIX 5 – Video Surveillance-related Resources

Video Surveillance	
IP Video Market ipvideomarket.info	Site Internet rassemblant de l'information gratuite sur l'industrie et la technologie de la vidéosurveillance IP.
Video Surveillance www.videosurveillance.com	Site Web dédié à la vidéosurveillance. Présente des nouvelles, des éditoriaux, des blogues, des revues et analyses sur les produits de cette industrie.
Video analytics www.videoanalytics.org	Se positionne comme une ressource Internet neutre sur la technologie d'analytique vidéo et sur les fournisseurs de celle-ci.
Security	
Access Control and Security Systems www.securitysolutions.com	Publication destinée aux entreprises et professionnels dans le domaine de la sécurité, présentant les équipements de sécurité et leurs différentes applications.
ASIS International www.asisonline.org	Rassemblant plus de 36 000 membres à travers le monde, il s'agit de la plus grande association en sécurité. Elle offre plusieurs services à ses membres, tels que la formation, la publication d'un magazine et des services de représentation auprès des entreprises, du gouvernement et des médias.
Canadian Association of Defence and Security Industries (CADSI) www.defenceandsecurity.ca	Association sans but lucratif qui représente les entreprises canadiennes oeuvrant dans le domaine de la défense et la sécurité.
CSO www.csoonline.com	Publie des nouvelles, des analyses et des recherches sur un vaste éventail de sujets : sécurité de l'information , sécurité physique, contrôle d'accès et beaucoup plus.
HS Daily Wire www.hsdailywire.com	Site Web de nouvelles sur le marché de la sécurité intérieure, ainsi que les tendances technologiques s'y rattachant.
ISC365.com www.isc365.com	Visant à rapprocher et informer les professionnels de la sécurité, ce site présente des nouvelles quotidiennes, des formations, un répertoire de produits et des opportunités de maillage.
SDM www.submag.com	Magazine couvrant le marché des vendeurs, intégrateurs, distributeurs et installateurs de produits de sécurité.

Security (cont'd)	
Security Industry Association (SIA) www.siaonline.org	Association américaine pour les entreprises en sécurité logique et physique. Elle défend les intérêts de ses membres auprès du gouvernement américain, publie des études de marché, crée des standards favorisant l'intégration, dispense de la formation et commandite des foires commerciales.
Security Industry Buyer's Guide www.sibgonline.com	Publié par ASIS International, ce guide recense les produits et les services de l'industrie de la sécurité. Il comprend plus de 3 000 manufacturiers et fournisseurs de produits et services dans ce domaine.
Security Info Watch www.securityinfowatch.com	Site Internet présentant des nouvelles sur l'industrie et le marché de la sécurité.
SourceSecurity.com www.sourcesecurity.com	Guide en ligne pour le secteur de la sécurité.