

RELEASED UNDER THE FOI ACT 1982

CCTV Futures Report

For Australian Customs and Border Protection

Prof. Brian C. Lovell (NICTA)

Mr. Paul Donato (Lighthouse Alliance)

Dr. Abbas Bigdelli (NICTA)

Ms. Sandra Mau (NICTA)

30 June 2009

CCTV Futures Report

Table of Contents

1 Executive Summary 4

2 Introduction 6

3 Trends Summary 7

3.1 Top 10 CCTV Technology Trends 7

3.2 Top 10 CCTV System Trends 8

4 Customs Business Context 9

4.1 The role of CCTV in Customs 9

4.2 Customs Environments for CCTV Usage 9

4.3 Classification of Current Customs CCTV Systems 11

4.4 Need to Digitise Infrastructure 12

5 CCTV Technology Trends 13

5.1 CCTV Evolution: From Analog to Digital 13

5.1.1 CCTV Generations 13

5.1.2 Migration to Digital 16

5.1.3 Implications & Benefits of Going Digital 17

5.2 Data Storage 17

5.2.1 Recorders: VCR/DVR/NVR 17

5.2.2 Local vs. Remote Storage 18

5.2.3 Storage Medium 19

5.3 Data Transmissions 21

5.3.1 Data Transmission 21

5.3.2 Open Standards in Compression Technology (H264 SVC) 27

5.3.3 Bandwidth 29

5.3.4 Data Security 31

5.3.5 Open Standards in Communication and Software 32

5.3.6 Systems Ownership 33

5.4 Cameras 34

5.4.1 Megapixel Cameras 34

5.4.2 Other Special Purpose Features 38

5.4.3 Placement 40

RELEASED UNDER THE FOI ACT 1982

5.4.4 Automated Camera Checking 40
5.4.5 Sensor Fusion 41
5.5 Analytics 42
5.5.1 Integrating Video Analytics into a Monitoring Centre 42
5.5.2 Common Analytic Challenges 47
5.5.3 Mitigating Common Analytic Challenges 47
5.6 Displays 48
5.6.1 Advanced Presentation on 2D and 3D maps 48
5.6.2 16:9 Format Based on HDTV standard 50
5.6.3 Mobile Device Integration (PDA, Phone) 52
5.7 Command, Control & Coordination (C3) 53
5.8 Evaluation – Performance Metrics and ROI Measures 56
6 The CCTV Future 57

Table of Tables

Table 1 Top 10 Technologies for Future CCTV 7
Table 2 Top 10 System Trends 8
Table 3 Typical Customs environments 10
Table 4 Classification of existing Customs CCTV systems 11
Table 5 Comparison of SSD and HDD storage 20
Table 6 WIFI data transmission standards 25
Table 7 Mobile phone data transmission standards 25
Table 8 Codecs for Surveillance Applications 29
Table 9 CIF standards for standard definition digital video 34
Table 10 Standards for high definition digital video 35
Table 11 Timeframe for Visual Alarms 46

Table of Figures

Figure 1 Transition from analog to IP (digital) cameras in world video surveillance market over the period 1980 to 2010 12
Figure 2 Classification of CCTV Generations from CISCO White Paper 14
Figure 3 Typical IP-video network configuration with NVRs 16
Figure 4 24dBi 2.4GHz Square Grid/Dish Antenna 24

RELEASED UNDER THE FOI ACT 1982

Figure 5 Wireless IP camera network based on mesh networking technology 26

Figure 6 CCTV Image of London Tube Bombers 7th of July, 2005. Note the interframe prediction artifact that shows the metal railing in front of one of the bombers instead of behind him..... 28

Figure 7 Total Open IP Surveillance Software Market..... 33

Figure 8 HD resolution (left) versus SD resolution (right) 36

Figure 9 A 16 MPixel camera viewing airport departure hall..... 37

Figure 10 A 16 MPixel camera viewing city intersection..... 38

Figure 11 IP camera made up of 5 cell phone camera lenses. In the form of an Ethernet powered box, this camera provides a 180° panoramic shot..... 40

Figure 12 Rain mitigation video filter operating at the Port of Brisbane during storm. 44

Figure 13 Feature selective fusion of IR and visible light 45

Figure 14 Overlay of AIS data on 3D model of container ship at Port of Brisbane. 45

Figure 15 Surveillance video stitched in real-time at Newark Airport 48

Figure 16 Surveillance video of a real fire at the Port of Brisbane overlaid on a 3D model of the site..... 49

Figure 17 Tracking a suspect at Jacksonville airport. Suspect position is overlaid on a map of the terminal. Alternate view of suspect from another camera is made available to operator through a popup video. 49

Figure 18 HDTV widescreen 16:9 aspect ratio, compared to analog 4:3 ratio..... 50

Figure 19 UK share of sales of 16:9 with the introduction of digital..... 51

Figure 20 Forecast of 16:9 Panel Penetration in the Notebook PC (Left) and LCD Monitor Markets (Right)..... 51

Figure 21 Mobile Device Integration 52

Figure 22 Examples of virtual desktop software. Left: Spaces on Mac, Right: openSUSE 10.2's virtual desktop 54

RELEASED UNDER THE FOI ACT 1982

1 Executive Summary

CCTV is an important tool for monitoring the major air and seaport borders to safeguard Australian national interests. Currently, the CCTV industry is undergoing a technological shift as traditional analog CCTV technologies based on television technologies are being replaced with hybrid and full digital systems based on internet and computer networking technologies. section 47E(d)

There is no practical possibility of keeping analog CCTV systems alive into the near future - indeed, even the underlying analog television infrastructure is being switched-off across Australia between 2010 and 2013[1]. Thus the CCTV systems must be upgraded to digital technologies to maintain, and preferably improve, their effectiveness both in terms of performance and operational costs.

CCTV surveillance is a vast area that is changing rapidly due to the adoption of IP network technologies. It is also a very diverse field and a complete survey would require several textbooks. In an attempt to make the report accessible to several target audiences, we have extracted the top 10 technology (Table 1 on page 7) and system trends (Table 2 on page 8) for particular attention, but in no particular order, and have highlighted how they relate to Customs business areas. The report can certainly be read from cover to cover, but it would possibly be more efficient to look over the top 10s and then drill down to the relevant sections of interest.

RELEASED UNDER THE FOI ACT 1982

Top 10 Technology Trends

1. IP end-to end, Power over Ethernet
2. HDD/SSD Local Storage
3. Open Standards in Compression Technology
4. Wireless CCTV
5. Special Purpose cameras - Low Light, Wide Dynamic Range
6. Advanced Presentation on 2D and 3D maps
7. Megapixel Cameras
8. 16:9 format based on HDTV standard
9. Fast Forensic Search
10. Video Analytics -Motion, Queue length, face , etc

[1] *Digital Switchover*, Australian Government Department of Broadband, Communications and the Digital Economy, 2009.

Top 10 System Trends

1. Open Standards - Seamless access to all cameras
2. Single Desktop Control Room
3. Interoperability of Camera Networks
4. Partitioning of Infrastructure
5. Remote Monitoring
6. Data Fusion - CCTV + sensors
7. Scalable Situational Awareness
8. Automated Camera Checking
9. Mobile Device Integration
10. Performance & ROI Metrics

RELEASED UNDER
THE FOI ACT 1982

2 Introduction

In 2009, Customs engaged National Information and Communications Technology Australia (NICTA) to provide an independent assessment of the current state of the art and future trends in CCTV surveillance systems which can enhance Customs operations in the future. NICTA is a government funded company dedicated to ICT research, commercialization, and research training.

Scope

The scope of this report is a high level overview of the trends for CCTV technologies, systems and, operations with a focus on the Customs environments of airport, seaport, container examination facilities, and armouries. Other environments including post cargo, air cargo, investigation rooms, and aircraft are out of scope. This report briefly reviews the requirements for those operating environments in-scope and examines how emerging and current technologies can better meet those requirements to provide highly effective CCTV surveillance in the future. The report does not advocate any one solution in particular, nor does it examine the resource constraints for Customs to provide a strategy for migration or upgrading. Since this report is focused primarily on a future vision for CCTV surveillance, funding considerations for the migration to a future network is out of the scope.

Approach

Each Customs environment has an associated symbol which is used throughout the report to indicate strong relevance of a particular trend or technology to that environment:

Seaport	Symbol: 
Airport	Symbol: 
Container Examination Facilities (CEFS)	Symbol: 
Detained Goods and Custodial Armouries (DGCA)	Symbol: 

RELEASED UNDER THE FOI ACT 1982

The report is divided into sections comprising:

- **Top 10 Trends Summaries** - Section 3 summarizes the top 10 technology trends and top 10 system trends in terms of their business benefits to Customs and provides a quick reference to the rest of the document
- **Custom's Business Context** - Section 4 discusses Custom's activities and operational requirements
- **CCTV Surveillance Trends** - Section 5 gives an overview of trends in CCTV surveillance technologies and systems
- **A Vision for the Future** - Section 6 summarises the business benefits to Customs in embracing the emerging technology trends

3 Trends Summary

3.1 Top 10 CCTV Technology Trends

As there are many stakeholders in Australian Customs and Border Security with different issues and objectives, it may be convenient to use the following table to determine which emerging and future technologies will be most relevant to business objectives. Many of these technologies are available for purchase now, but they will no doubt improve over time. The following table lists 10 of the top CCTV technologies that are emerging.

Top 10 Technology Trends		Overall Business Benefits					
		Save $	Save Time	Save Staff	Improved Performance	Relevant Environments	Pages
1	IP end-to end Power over Ethernet	✓	✓	✓	✓✓✓		21
2	HDD/SSD Local Storage	✓			✓✓		18
3	Open Standards in Compression Technology H264 SVC	✓✓			✓✓✓		27
4	Wireless CCTV	✓✓✓	✓✓		✓✓✓		24
5	Special Purpose cameras Low Light, Wide Dynamic Range				✓✓✓		34
6	Advanced Presentation on 2D and 3D maps		✓	✓	✓✓✓		48
7	Megapixel Cameras				✓✓✓		34
8	16:9 format based on HDTV standard	✓		✓	✓✓✓		50
9	Fast Forensic Search		✓✓✓	✓	✓✓✓		45
10	Video Analytics Motion, Queue length, face , etc		✓✓	✓✓	✓✓✓		42

Table 1 Top 10 Technologies for Future CCTV (Legend: Seaport Airport CEFS DGCA)

RELEASED UNDER THE FOI ACT 1982

3.2 Top 10 CCTV System Trends

In addition to the point technologies listed in the previous section, the new technologies are promoting a complete rethink of how CCTV should be used and operated. A major disruptor is the introduction of IP (Internet Protocol) technologies from computer networks. In analog systems it was difficult and expensive to send video signals long distances on coax and dedicated fibre links. The introduction of IP means that video can be transmitted over virtually any distance and through any internet medium (wireless, phone network etc). Now it is becoming possible to build surveillance systems that span whole cities or even multiple cities. With this trend management problems are emerging that require new solutions and different priorities. For example, in small systems that are not interconnected, proprietary solutions are easier to install and convenient. However as more systems become connected there is a strong need for non-proprietary open standards that are supported by a variety of equipment. The following table lists 10 of the top CCTV System Trends that are emerging.

Top 10 System Trends	Overall Business Benefits					
	Save $	Save Time	Save Staff	Improved Performance	Relevant Environments	Pages
1 Open Standards Seamless access to all cameras	✓✓	✓	✓	✓✓✓		32
2 Single Desktop Control Room	✓✓	✓	✓✓	✓✓✓		54
3 Interoperability of Camera Networks	✓✓✓	✓	✓	✓✓✓		53
4 Partitioning of Infrastructure	✓	✓	✓	✓✓✓		33
5 Remote Monitoring	✓✓	✓✓✓	✓✓✓	✓✓✓		53
6 Data Fusion CCTV + sensors		✓✓	✓✓	✓✓✓		41
7 Scalable Situational Awareness		✓	✓	✓✓✓		54
8 Automated Camera Checking	✓✓	✓✓✓	✓✓✓	✓✓		40
9 Mobile Device Integration		✓✓	✓✓	✓✓✓		52
10 Performance & ROI Metrics	✓			✓✓✓		57

Table 2 Top 10 System Trends (Legend: Seaport Airport CEFS DGCA)

RELEASED UNDER THE FOI ACT 1982

4 Customs Business Context

4.1 The role of CCTV in Customs

Customs is responsible for Australian border management to prevent illegal movement of goods and people while facilitating legitimate trade and travel. It also contributes to wider national security by assisting other agencies in counter terrorism and law enforcement initiatives using CCTV as a tool to detect and target criminal and terrorist activity, assisting in incident response at Australian airports and seaports, and providing high quality CCTV images as evidence for law enforcement agencies when mounting prosecutions.

In day to day operations CCTV has many practical roles to play.

- Gathering performance statistics for passenger movements as a measure of quality of service at airports
- Monitoring queue lengths to ensure adequate staffing and effective passenger movements at airports
- Protecting staff by repudiating claims for damage and theft by members of the public (airports- baggage inspection)
- Gathering surveillance footage on persons of interest at the request of agencies at airports
- Determining which aircraft a passenger has arrived on for illegal immigrants who have destroyed their documents at airports.
- Monitoring staff to ensure safety as they enter and exit vessels at sea ports
- Monitoring distant sites to determine when customs officers should leave the office to inspect arriving ships at sea ports
- Monitoring visitors accessing Detained Goods Facility

RELEASED UNDER THE FOI ACT 1982

4.2 Customs Environments for CCTV Usage

Customs operates CCTV in many environments including airports, seaports, container inspection, and armouries. Each environment has special needs and the same CCTV equipment is unlikely to be suitable for all environments. The following table is a summary of typical CCTV characteristics in the main Customs Environments:

Seaport	▪ The goal of the surveillance is to detect, recognize, or identify objects in the field of view ▪ section 47E(d) ▪ section 47E(d) ▪ Areas of activity may change as ships arrive and depart from docks. Typically addressed by PTZ cameras. ▪ section 47E(d) ▪ Need recognition capability for vehicle number plates and containers ▪ Day and night video operation is needed - 24/7 monitoring requirement ▪ Low light conditions are common

		▪ Surveillance system needs to be covert in some instances (so that no visible illumination is used at night) ▪ Harsh external environment due to temperature, weather, and sea air as well as exposed infrastructure ▪ Wind causes camera and image vibration ▪ Appropriate mountings and housings are critical ▪ High cost to install – also labour intensive ▪ section 47E(d) ▪ CCTV equipment is usually obvious to those behaving in a criminal manner and thus enables them transfer activity outside the range of view or obscure view. ▪ Requirement to ensure cameras or in good working order at all times (ie. routine maintenance automated rather than manual – alarm to be triggered if a camera is not working) ▪ OH&S issues are a major operational need addressed by CCTV ▪ section 47E(d) ▪ Need for remote monitoring for some sites that are unable to be manned
	Airport	▪ The goal of the surveillance is to detect, recognize or identify objects and people in the field of view ▪ Airports internal environment is always shifting (new signs, extensions etc) - need to be able to relocate cameras at minimal cost ▪ Surveillance system needs to be covert in some instances ▪ Mix of environments both inside and outside ▪ Lighting within terminals is generally not a problem. Low light conditions occur on the tarmac (light aircraft surveillance) ▪ section 47E(d) ▪ High people traffic flows ▪ Short processing times in which to move passengers through ▪ Need to identify a face in the crowd ▪ Need to detect unauthorized access to secure areas ▪ Threats to passenger safety such as unattended luggage, persons of interest ▪ CCTV assists in OH&S issues – baggage inspection, GST refund counter ▪ Responsive systems required to monitor incidents in real time ▪ High level of need to ensure cameras or in good working order at all times (i.e., routine maintenance automated rather than manual – alarm to be triggered if a camera is not working)
	Container Examination Facilities (CEFS)	▪ The goal of the surveillance is to detect, recognize or identify objects in the field of view ▪ Night time and day time surveillance - 24/7 monitoring requirement ▪ High contrast in light between capturing images within containers and outside of containers ▪ Require good view of the unpack and repack activity ▪ Surveillance system needs to be covert in some instances (so that no visible illumination is used at night)
	Detained Goods and Custodial Armouries (DGCA)	▪ The goal of the surveillance is to detect, recognize or identify objects in the field of view ▪ Night time and day time surveillance - 24/7 monitoring requirement ▪ section 47E(d) ▪ section 47E(d) ▪ Destruction of detained goods requires close surveillance to ensure any criminal behaviour (e.g., theft) is deterred or captured on surveillance. ▪ Surveillance system needs to be covert in some instances

Table 3 Typical Customs environments

RELEASED UNDER THE FOI ACT 1982

4.3 Classification of Current Customs CCTV Systems

CCTV systems can be classed into four basic generations depending on the degree of digital processing.

- First Generation: Analog for everything - VCR for storage
- Second Generation: Analog Switching, Digital Recording - DVR for storage
- Third Generation: Analog Switching, IP Recording - NVR for storage
- Fourth Generation: IP for everything - NVR for storage

The existing Customs CCTV systems in the four Customs environments can thus be categorised as per Table 4 below. See Section 5.1.1 on page 13 for a full description of CCTV Generations. Also refer to Mike Hogben's (GHD) report for a description of the current system architecture.

	First Generation	Second Generation	Third Generation	Fourth Generation
Seaport - 32 Ports System	✓			
Seaport - 31 Ports System			✓	
Airports		✓		
Cargo Examination Facility		✓		
Detained Goods and Custodial Armouries		✓		

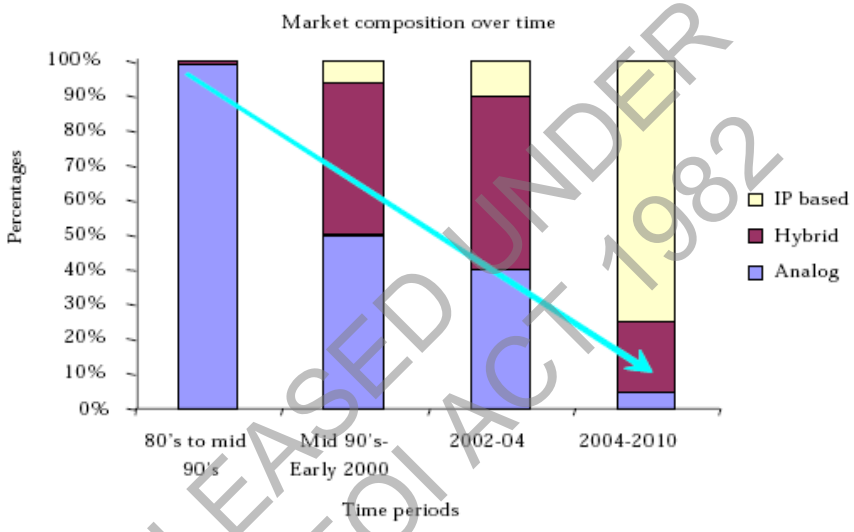
Table 4 Classification of existing Customs CCTV systems

RELEASED UNDER THE FOI ACT 1982

4.4 Need to Digitise Infrastructure

CCTV technologies have been steadily evolving from analog to digital over the past few decades and Fourth Generation IP Surveillance systems is the current industry focus. Figure 1 plots the evolution of surveillance equipment from analog to IP (digital) back in the 1980s to present. Industry analysis has found that demand for digital systems (IP and hybrids) surpassed that of analog systems back in 2002[2] and predict that analog product sales would be flat for 2009.[3] As demand evolves, supply in terms of analog equipment and replacement parts, will soon be phased out as well.

Video Surveillance Equipment Market: Market Composition of Video Surveillance Equipment (World), 1980s-2010



Source: Frost & Sullivan

Figure 1 Transition from analog to IP (digital) cameras in world video surveillance market over the period 1980 to 2010[4]

RELEASED UNDER THE FOI ACT 1982

Customs is aware of this transition towards digital and is actively reviewing the current and future CCTV Surveillance options to avoid obscelecence. They are in the process of migrating their systems to digital (most are hybrids with only the "Thirty Two" ports system still analog). This report hopes to provide an overview of current and emerging CCTV Surveillance technologies and to identify the ones most relevant to Customs operating environments.

[2] Converting an Analog CCTV System to IP-Surveillance. Axis Communications White Paper, 2002.

[3] Frost & Sullivan makes bold predictions for security, IP. Security System News, 2009.

[4] World Video surveillance market – Investment Analysis 2008. Frost and Sullivan, 2008.

5 CCTV Technology Trends

5.1 CCTV Evolution: From Analog to Digital

CCTV technologies have been steadily evolving from analog to digital over the past few decades as seen in Figure 1. The reason for this migration is that digital technology allows greater reliability, effectiveness and flexibility in surveillance operations, access to high definition images, generic hardware platforms, and video analytics.

In the past, CCTV surveillance has been characterised by analog systems that suffered from several major short-comings, including high maintenance requirements (especially with tape systems), costly retrofits for remote accessibility, and difficulties in integrating with other systems. Customs experience some of these issues daily in the "Thirty-Two" ports analog systems which have remote access at high cost, costly maintenance, storage of low quality video on VHS tapes, and no video analytic or instantaneous playback capabilities. Even the hybrid analog-digital systems currently in Customs airport and "Thirty-One" ports installations suffer from some of the legacy analog drawbacks including the use of costly fibre optics, local storage limitations, and remote access limitations.

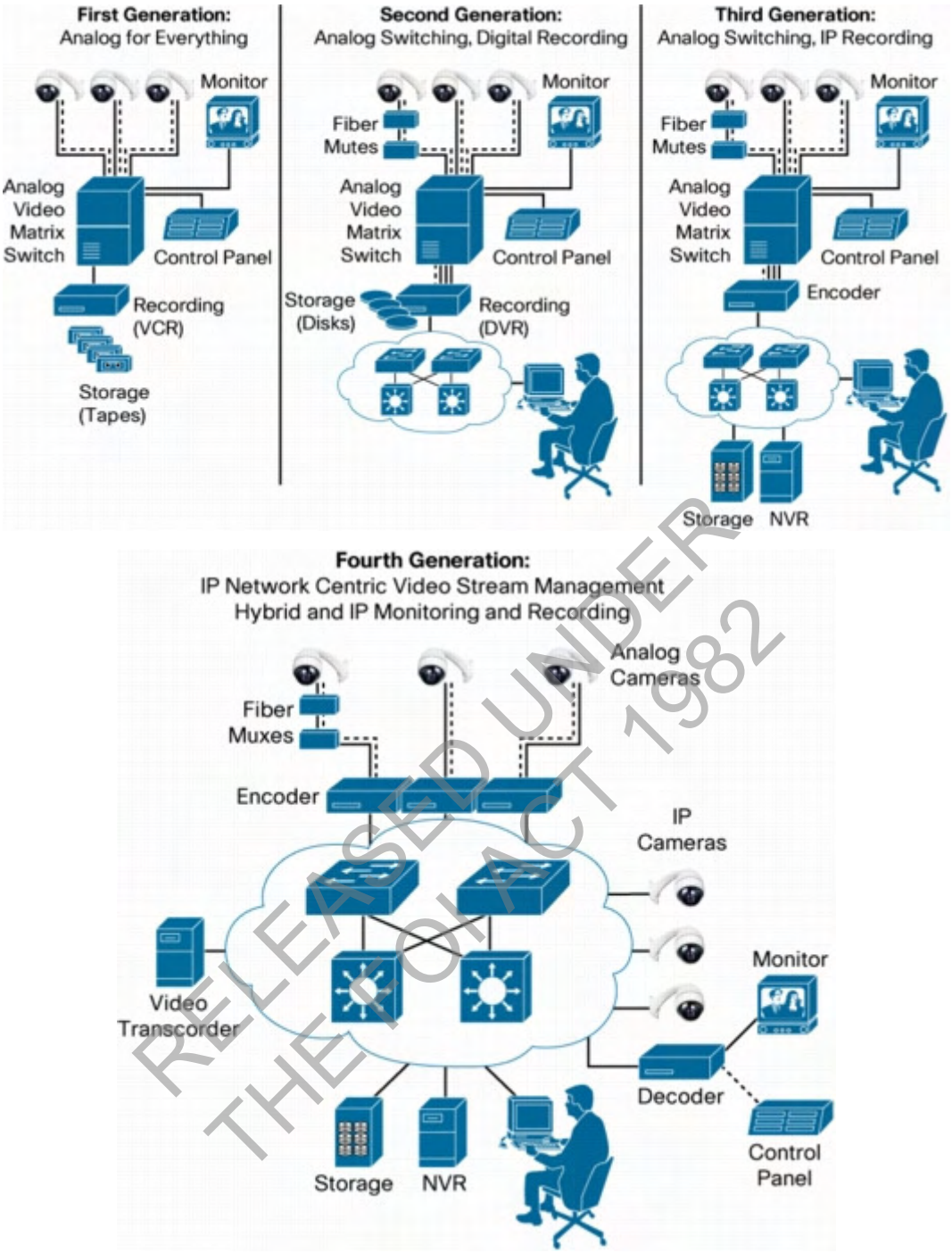
Emerging digital systems can be designed to eliminate many such issues for Customs by allowing remote access of video by multiple agencies, higher quality digital videos and storage for forensic analysis and evidence, and lower cost in maintenance and expansion. On top of that, there are other benefits including ease of use for the operators, advanced search capabilities, and shorter training periods. Digital CCTV systems also have the potential to increase safety and efficiency in operations, and assist in areas with lower staffing resources through computer analytics.

RELEASED UNDER THE FOI ACT 1982

5.1.1 CCTV Generations

CCTV systems can be classed into four basic generations depending on the degree of digital processing (illustrated in Figure 2):

- First Generation: Analog for everything - VCR for storage
- Second Generation: Analog Switching, Digital Recording - DVR for storage
- Third Generation: Analog Switching, IP Recording - NVR for storage
- Fourth Generation: IP for everything - NVR for storage



RELEASED UNDER THE FOI ACT 1982

Figure 2 Classification of CCTV Generations from CISCO White Paper[5]

First Generation (Analog System)

In analog video surveillance systems all components are analog: analog cameras, coaxial cables for transmission, analog video matrix and switch, analog TV monitors, and video cassette recorders (VCRs) using VHS cassette tapes. There are numerous drawbacks in using analog systems including no simultaneous recording and feedback, slow video search, tape

[5] Cisco Systems IP Network-Centric Video Surveillance. Cisco, 2009.

wear, tape storage, lower quality images, distance restrictions, and high maintenance costs. Moreover, analog systems are usually based on proprietary signaling and format protocols thus multi-vendor component interoperability is not an option without extensive and costly customization. Customs is well aware of these limitations and have started migrating to hybrid systems with only the Thirty-Two ports system still fully analog as of 2009.

Second and Third Generation (Hybrid Systems)

Hybrid video surveillance systems combine some analog components with digital components. Typically, the component which benefits most from digital technology is the storage – replacing VCRs with Digital Video Recorders (DVRs) in Second Generation systems or Network Video Recorders (NVRs) in Third Generation systems to store video on disk drives rather than tape.

DVRs offer the capability of real-time simultaneous recording and playback, they search through video faster, store with higher video quality and less loss, and can provide convenient storage redundancy. Display can be via analog monitors or PC client systems. DVRs still stores data locally, but can be connected to a network to provide remote access and viewing of these data. This Second Generation model is what is currently implemented by Customs in Airports, CEFS, and DGCA.

An NVR differs from a DVR in that the analog signals from the cameras are encoded to digital and switched to a network using the Internet Protocol (IP). Having an IP system facilitates remote storage, can be run on lower-cost commercial off the shelf (COTS) servers, and offers secure and convenient multi-user remote viewing and data access. Customs has implemented something similar for the Thirty-One ports system which has remote access and control capabilities.

RELEASED UNDER THE FOIA ACT 1982

Fourth Generation (Fully Digital Systems)

The biggest trend in video surveillance is a fully digital surveillance system (also known as IP-Surveillance systems). Rather than a centralized system for switching, storage, and monitoring, the IP-Surveillance system components all connect to an IP network. Cameras connect to the network either directly or through a video server and the data is stored on Network Video Recorders (NVR) which can be situated anywhere on the network. IP systems can still support analog technology (for example, analog cameras with coax transmission, or analog monitors), but those analog inputs need to be converted to IP protocol in a video server (Figure 3). As the older analog technology gets progressively phased out, it can be replaced with new IP hardware which will have a wider range of capabilities (*i.e.*, multi-megapixel cameras, sensor fusion and integration, etc.).



Figure 3 Typical IP-video network configuration with NVRs

From a Customs perspective, IP-surveillance would be a good fit as it conveniently allows multiple national agencies that rely on CCTV video data to independently access the information without interfering with other parties (*i.e.*, AFP could access a fixed airport CCTV cam and zoom into a multi-mega pixel image without other parties knowing who they are observing). IP-based systems can also use video analytics to alert operators, either locally or remotely, of any alarms (*i.e.,* motion in a secure area, identification of person on a watch list, etc.) which should lower operator resource requirements and also increase effectiveness of detection of suspicious activity.

5.1.2 Migration to Digital

Implementing a full digital system can be achieved through a step-by-step process to replace legacy technology over time. Having a migration plan with an end vision of a fully IP system by a certain time horizon can effectively evolve the infrastructure from an analog system, to a hybrid system, and finally to an IP system.

Cost-benefit and resource analysis by Customs will be required to determine which components should be migrated to digital first. For example, it can be prohibitively expensive to replace analog cameras and the coaxial cable infrastructure for an seaport to adopt it to IP due to costs associated with removal of old cables and placement of new cables with consideration for the new IP camera placements. Yet the decision to replace VCRs with DVRs, or TV monitors with a PC and PC monitor is relatively inexpensive.

Note that hybrid systems tend to suffer from high latency (video is delayed compared to real-time) due to multiple conversion of analog to digital. Due to frame interleaving of the MPEG and related digital formats, each conversion from analog to digital incurs a minimum delay of 3 frames which corresponds to a 200 ms delay. Any latency greater than 200ms causes operators great difficulty when operating PTZ cameras. A full digital solution will generally have lower latency than a hybrid system.

RELEASED UNDER THE FOI ACT 1982

5.1.3 Implications & Benefits of Going Digital

The migration to digital for any long-term system is not a matter of "if", but "when". Digital CCTV technology is an imminent trend that can be met through progressive system upgrades and advanced planning for future systems.

The following sections in this report will go into more detail regarding how digital surveillance will impact the individual component technologies, the benefits and drawbacks, and the challenges and considerations.

5.2 Data Storage

The choice of data storage medium should be made depending on the environment and cost. The choice of local or remote storage can also be impacted by the structure of the system, available bandwidth, and costs.

5.2.1 Recorders: VCR/DVR/NVR

Video Cassette Recorders (VCRs) were used to record analog video to a magnetic tape medium. It was a single copy on a VHS cassette, and not easily sharable or searchable (linear).

Digital Video Recorders (DVRs) are a digital recording (from either an analog or a digital signal) to a disk which allowed random access to the data (*i.e.,* not linear). The versatility of DVRs is much greater than VCRs, allowing digital frame grabs, computer network connectivity, and searching based on time, date, or even motion. Typically, when used with analog video cameras, DVRs incorporate proprietary devices containing analog to digital capture cards, which can be expensive. The cameras connect to the DVRs through BNC connectors.

Network Video Recorders (NVRs) allow the direct transmission of digital data between the camera and the recorder over a network. All the cameras connect to the NVR via a high speed Ethernet port. It is an internet protocol (IP) based system which can be managed, accessed, and controlled remotely allowing for greater flexibility in choice of storage and workstation location (local, remote, multiple), and is easily scalable. The newest generation of NVR hardware are on open platform systems, which means that they can run any IP recording software on the market (rather than proprietary software as with analog CCTV systems).

Digital systems applying either DVR or NVR, can offer enormous advantages over VCR including:

- No tape management, cataloguing, and failure issues, and no visits to remote locations to change tapes
- Automatic offsite backup (mainly NVR) and automatic management of storage (30 day retention) at a low cost
- Video coding and strong encryption

RELEASED UNDER THE FOI ACT 1982

- Simultaneous record and playback, and high speed search, fast forward, rewind (600x)
- Easy extraction of video and high quality still frames

There are also some potential drawbacks:

- Potential manipulation of video which can be a problem for court evidence. Need to ensure that system meets standards for forensic evidence.
- Difficult to detect tampering . Need for digital watermarking to prevent tampering.
- Need trusted operators and good policies

From a Custom's perspective, the requirement to provide Australian government agencies with forensic video evidence involves reviewing and searching the video, and providing a digital copy which is easily facilitated by both DVRs and NVRs. NVRs also offer multiple and remote access capabilities such that other federal agencies can be given remote access to the video (security issues discussed in Section 5.3.4) thus freeing Custom's agents to continue surveillance; For example, Customs locations that are low on staff can fall back on remote surveillance from the National Monitoring Centre in Melbourne (NMC). At the moment, only the Thirty-One ports system facilitates remote access by the NMC and none of the systems facilitate access by multiple agencies. 

Between NVR and DVR, the trend is heading towards a NVR solution with separate video servers which allow more flexibility in storage location (which is particularly useful for airports with space constraints) increased reliability in storage and flexibility for future expansion. With NVR, multiple control room solutions are possible (rather than the single local control rooms of the 1960's analog CCTV systems). In regards to migration, it is best to ensure that any infrastructure being upgraded should be made IP ready so that individual analog components (i.e. cameras, etc.) can be phased out bit by bit at they reach their end of life.

RELEASED UNDER THE FOI ACT 1982

5.2.2 Local vs. Remote Storage

Digital CCTV technologies and networked IP-Surveillance systems will allow storage of video at the source (i.e. camera), near the source, and/or elsewhere on the network through scalable distributed storage solutions. With a networked system, the video can be stored in multiple locations as well (whether local or remote) which can provides redundancy which shields against unexpected failure.

Note that typical hard disk drives in CCTV environments actively reading or writing 99% of the time compared to a server which may be active 40% of the time or a desktop PC which may be active just 3% of the time. This load means that disk failures are common in CCTV systems, so it is important to specify high quality disks and have a hot swap facility such as provided by RAID[6] systems.

[6] David A. Patterson, Garth Gibson, and Randy H. Katz: A Case for Redundant Arrays of Inexpensive Disks (RAID). University of California Berkley. 1988.

For remote data storage, network bandwidth is the major stumbling block, particularly if there are many cameras on the network. In such systems it makes much more sense for the recorded video to remain local to the camera network. Local storage may have to be performed in a high quality, high-bandwidth format such as MJPEG to maintain the forensic nature of the recording. Such formats use too much bandwidth for the purposes of remote viewing through leased lines where bandwidth is expensive. The trick is to realise that only the video feeds that are viewed need physical transmission to the remote site and this can be done using a compressed format such as H264. 

For example, in a large site with 1000 cameras perhaps only, say, 10 would need to be viewed at any one time. These could be compressed using H264 video compression to just 20% of the bandwidth required for MJPEG. Thus remote viewing would only require 0.2% of the bandwidth of the recording system. This can be further improved by more aggressive compression strategies especially if the display size is less than the native resolution of the video feed — which is common is single desktop surveillance displays

Although the overall surveillance system may have distributed network storage with multiple local NVRs, the overall system can be made totally seamless to the operator as there is no need to know where the video is physically stored, analogous to websites hosted on different ISPs that can be accessed through the internet.

RELEASED UNDER THE FOI ACT 1982

5.2.3 Storage Medium

With the advent of digitisation, the two major options for storage are Solid State Drives (SSD) and Hard Disk Drives (HDD). Tape is considered to be a legacy technology. Optical media such as DVD are mainly useful for providing video to external agencies for forensic examination. Table 5 compares the two storage options and further details are provided below.

	Solid State Drives (SSD)	**Hard Disk Drives (HDD)**
Features	Robust to shock, altitude, vibration, and temperature variations; low power consumption	Low cost, wide availability, and largest storage capacity
Limitations	High cost, lower storage capacity, limited number of erase cycles 10,000 – 1,000,000[7]	Lower mechanical reliability (can be mitigated by RAID configuration)
Costs[8]	Flash: US$1.50 - US$3.45/GB (c.f. DRAM: USD80.00/GB)	US$0.38/GB
Usage		

[7] Bez, R.; Camerlenghi, E.; Modelli, A.; Visconti, A. (2003), "Introduction to flash memory", *Proceedings of the IEEE* **91** (4): 489–502, 2003-04

[8] Lucas Mearian, "Solid-state disk lackluster for laptops, PCs", Published 27 Aug 2008, Retrieved on 3 Nov 2009.

	Remote, high vibration (vehicle), or harsh environments that need local storage; Portable devices.	Indoors & stationary

Table 5 Comparison of SSD and HDD storage

Solid State Drive (SSD)

Solid state storage is based on semiconductor technologies and is commonly used in flash memory or memory cards. For video storage purposes, a solid-state drive (SSD) can be used in place of a hard disk drive (HDD) using the same interfaces with PC and servers. In comparison with HDD, SSD has the advantages of:

- High mechanical reliability as there are no moving parts, which makes it robust to shock, altitude, vibration and extreme temperatures
- Faster start-up times and fast random access

There are also disadvantages in comparison to HDD, including:

- Higher cost: As of mid-2008, commercial HDD cost less than about US$0.38/GB, compared to US$1.50 - US$3.45/GB for flash SSD (lower power but slower) and over US$80.00/GB for DRAM-based SSD (higher power but faster). However, the trend is that the prices are coming down for all storage media[9].
- Limited write/erase cycles for flash SSD, though high endurance cells can endure 1-5 million write cycles.
- DRAM-based SSD require more power than HDD

Given its higher cost, lower storage capacity, and mechanical robustness, SSDs may be most suitable for local back-up storage, particularly if the camera and storage are located in remote or harsh environmental locations where regular maintenance may be an issue. Such local back-ups can add an extra redundancy to maintain video surveillance even if the network connection is experiencing issues (e.g., wireless links). It can also be used for storage that is portable or is likely to move around (i.e. commonly found in ruggedized laptops).

RELEASED UNDER THE FOI ACT 1982

Hard Disk Drive (HDD)

Hard disk storage stores digitally encoded data on rotating magnetic disks. It is currently the standard for storage in PCs and servers. Note that SSD devices are just emerging as an alternative in the notebook market. Currently, the highest capacity HDDs are 2 TB with spin

[9] Lucas Mearian, "Solid-state disk lackluster for laptops, PCs", Published 27 Aug 2008, Retrieved on 3 Nov 2009.

speeds ranging from 5,400 rpm for desktop systems to up to 15,000 rpm for enterprise systems.

A common data storage scheme is to use an array of disks for redundancy known as RAID. For CCTV applications, it is common to use RAID 1 or mirrored disks. Two disks each store exactly the same data, at the same time, and at all times. Data is not lost as long as one disk remains working. If the two mirrored disk sets are physically remote from each other, there is significant protection against fire and other threats. Note that mirroring requires twice the disk space.

The trend in HDDs over the past decade has been an exponential increase in disk space and data access speeds. They can currently provide large storage capacities for memory intensive storage such as digital video and audio recordings. HDDs are a widely adopted technology with few competitors in this sector.

Given is low cost, wide availability, and large storage capacity, HDDs is the most suitable medium for a bulk of the video data storage into the foreseeable future.

RELEASED UNDER THE FOI ACT 1982

5.3 Data Transmissions

The current trend is the progression towards a networked, IP-based surveillance system through which video can be easily routed, stored and streamed to multiple locations. This section looks at considerations for network structure, security, standards and ownership in an IP-Surveillance systems in relation to Custom's needs.

5.3.1 Data Transmission

Internet Protocol (IP) 

The term Internet Protocol (IP) is typically used to refer to communication of data through a packet-switched network using the TCP/IP (Transport Control Protocol/Internet Protocol) standard. The internet protocol was designed to allow computers running different operating systems and using different communication protocols to share their information using a ***common network communication language***.

It is illuminating to revisit the early days of the internet and the motivation behind the military project called the ARPAnet which led to today's public internet. The need for inter-networking was made obvious by the apparent waste of resources the isolated nature of computer systems caused in the 1960's.

> **"For each of these three terminals, I had three different sets of user commands. So if I was talking online with someone at S.D.C. and I wanted to talk to someone I knew at Berkeley or M.I.T. about this, I had to get up from the S.D.C. terminal, go over and log into the other terminal and get in touch with them. [...] I said, it's obvious what to do (But I don't want to do it): If you have these three terminals, there ought to be one terminal that goes anywhere you want to go where you have interactive computing. That idea is the ARPAnet."**
>
> ***—Robert W. Taylor, co-writer with Licklider of "The Computer as a Communications Device", in an interview with the New York Times***[10]

It could be argued that the advent of IP communication for CCTV today is allowing isolated CCTV systems to link with other systems in a similar manner to the early stages of the internet. Once again this is driving equipment manufacturers away from proprietary solutions and ***towards common formats and open standards***.

Communication in IP networks is typically through Ethernet connections. Within buildings this is generally carried on Category 5 (CAT 5)[11] twisted pair wiring as is currently used for both data and communications in modern structured wiring systems. CAT 5 can carry IP over Ethernet at 100Mbps over distances of up to 100m. For longer distances and between buildings[12], IP is supported on a huge number of transmission media including long-range single-mode[13] fibre, mobile (3G), and WiFi (IEEE 802.11) wireless networks.

Some of the advantages of using IP include:

- Digital transmission (IP) carries CCTV video virtually any distance with no loss or error due to the regenerative nature of digital systems coupled with error control mechanisms
- Convenient and secure transmission of CCTV through the public internet for remote viewing and maintenance
- Very high levels of transmission security using well-accepted data encryption technologies
- Cost reduction due to using COTS computer networking components from IT suppliers rather than specialist CCTV equipment

RELEASED UNDER THE FOI ACT 1982

---

[10] An Internet Pioneer Ponders the Next Revolution. New York Times, 20 December 1999.

[11] Federal Standard 1037C - August 7, 1996: Glossary of Telecommunication Terms.

[12] Fibre should be used between buildings for electrical isolation and lightning protection.

[13] Single Modem fibre is used in many applications where data is sent at multi-frequency (WDM Wave-Division-Multiplexing) so only one cable is needed to transmit many channels. Single-mode fibre supports higher transmission rates and up to 50 times more distance than multimode. For more information see http://www.arcelect.com/fibercable.htm

- Potential to use existing structured cabling infrastructure in buildings
- Power over Ethernet (PoE) technology uses CAT 5 cabling to carry both data and power
- A single CAT 5 cable provides communication both ways: carrying video data, remote camera control and maintenance, and possibly power.
- IP is easily integrated with other transmission methods, including wireless technology, single mode fibre for long haul, and legacy coaxial cables using commercially available converters
- Additional cameras can be added to the network over time through conventional routers and switches

Some potential disadvantages include:

- Requires existing or new IP cabling infrastructure
- Ethernet signals on CAT 5 cables span a similar distance to composite TV signals on coax; they have a maximum length of 100 meters – longer distances require switches, routers, and possibly fibre connections.
- High network bandwidth requirements: a typical CCTV camera with resolution of 640x480 pixels and 10 frames per second (10 frame/s) in MJPEG mode requires about 3 Mbps[14]. This problem is mitigated by emerging video compression standards such as H264 which offer very high quality at low data rates. For example, the typical CCTV camera above would require only 0.24 Mbps using H264 compression[15]. Also there is no need to transmit all the recorded video over the network; only the cameras that are being physically monitored at each instant need be transmitted.
- Some users report that IP cameras do not operate well under low light conditions or that there is noise in the image. This can happen, but is certainly not the case in well designed IP surveillance systems.
- There can be significant latency in poorly designed IP surveillance networks. The main problem occurs when operating PTZ cameras where there may be significant delays in response to camera movement commands. Such delays are mostly a result of analog to digital conversion, use of inappropriate codecs, and inappropriate use of routers (Level 3 or IP routing) rather than switches (Level 2 or ethernet switching). The problem is much worse in hybrid digital-analog systems than in true digital

RELEASED UNDER THE FOI ACT 1982

[14] Network bandwidth and video storage space calculation by JVSG, 17 January 2008

[15] H264 offers 80% reduction in bandwidth with low latency. For more information, see http://www.axis.com/products/video/about_networkvideo/compression_formats.htm

systems. Careful design can keep latency to less that 200ms which is quite acceptable in practice[16].

A positive trend which might make IP communication even more attractive is the Australian Government's commitment to improve the broadband infrastructure in Australia, setting aside $53.2 million in the 2009 budget for the National Broadband Network in 2009-10[17]. Over the next 8 years, it aims to connect 90% of all Australian homes, schools and workplaces with broadband services with speeds up to 100 Mbits/s[18]. This may facilitate (at a lower cost) communication with more remote regions which currently do not have the IP infrastructure, and also decrease potential bandwidth issues if using their infrastructure.

Wireless CCTV

Many IP CCTV cameras offer a wireless option that can be added by inserting a WiFi[19] card (IEEE 802.11) into the camera housing. This allows the camera to connect to the network over a range of a hundred metres without additional cabling or special antennae. This is very useful for nomadic and mobile cameras for covert operations and special purposes. Note that with cheap directional antennae, standard WiFi cards can span distances of many kms as long as there is clear line of sight between the transmitter and receiver. This technology can be a very easy and cost-effective way to obtain video from a remote camera.



Figure 4 24dBi 2.4GHz Square Grid/Dish Antenna

Beyond a distance of 3 km, WIFI throughput may begin to decrease due to the ACK (acknowledgement) timeout setting of the access point. The ACK timing must be optimized for longer distances - especially over links covering dozens of kilometers[20]. Rain and fog can interfere with performance but have minimal impact on shorter range links.

RELEASED UNDER THE FOI ACT 1982

---

[16] Future CCTV 2009, Invited talk, Greg Morrison, Exec Director, Technology Systems (Asia), Venetian Macau Resort Hotel

[17] BUDGET 2009: The spending mirage by Alan Kohler, 12 May 2009

[18] New National Broadband Network by Senator Stephen Conroy, 7 April 2009

[19] WiFi Alliance, 2009.

[20] Kameswari Chebrolu, Kameswari Chebrolu, and Kameswari Chebrolu, LongDistance 802.11b Links: Performance Measurements and Experience MobiCom'06, September 23–26, 2006, Los Angeles, California, USA.

Data rates for the different versions of WIFI are given in Table 6. These data rates should be compared to those available on the commercial mobile phone network given in Table 7.

Standard	Operating Frequency	Typical Throughput
802.11a	5 GHz	27 Mbps
802.11b	2.4 GHz	5 Mbps
802.11g	2.4 GHz	22 Mbps
802.11n	5 GHz and/or 2.4 GHz	144 Mbps

Table 6 WIFI data transmission standards[21]

Standard	Operating Frequency	Typical Throughput
3G (UMTS)	0.8/1.8 GHz	2.0-14.4 Mbps
HSDPA	0.8/1.8 GHz	1.8, 3.6, 7.2, 14.4 Mbps
HSPA+ (Telstra NextG)	0.8/1.8 GHz	Up to 42 Mbps

Table 7 Mobile phone data transmission standards[22]

The Hong Kong Mass Transit Railway uses short range WIFI video feeds (802.11a) to show the driver a view of the railway platform when he is at the station. This allows him to see the passengers and prevent accidents.

For longer distances a convenient option is 3G wireless transmission using IP over the standard telecommunication network. Data costs can be quite high for long term deployment, but the mobile phone network is ideal for short term surveillance operations or where line of sight is not available.

Security should always be considered in wireless links, but as both WIFI and 3G can be configured to use encryption, this should not be a major impediment to deployment.

Wireless mesh networking allows the wireless cameras to form an infrastructure less camera network by routing the video wirelessly from camera to camera as indicated in Figure 5. This could be an attractive option to extend a network — especially if altering traditional cabling is prohibitively expensive as may be the case in some privately operated sea ports.

RELEASED UNDER THE FOI ACT 1982

[21] Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure (2nd ed.). Hacker Friendly LLC. 2007. pp. 425. page 14

[22] World's first 21Mbps eHSPA/HSPA+ data "call" made in Australia, ITWire, 8 Dec 2008.

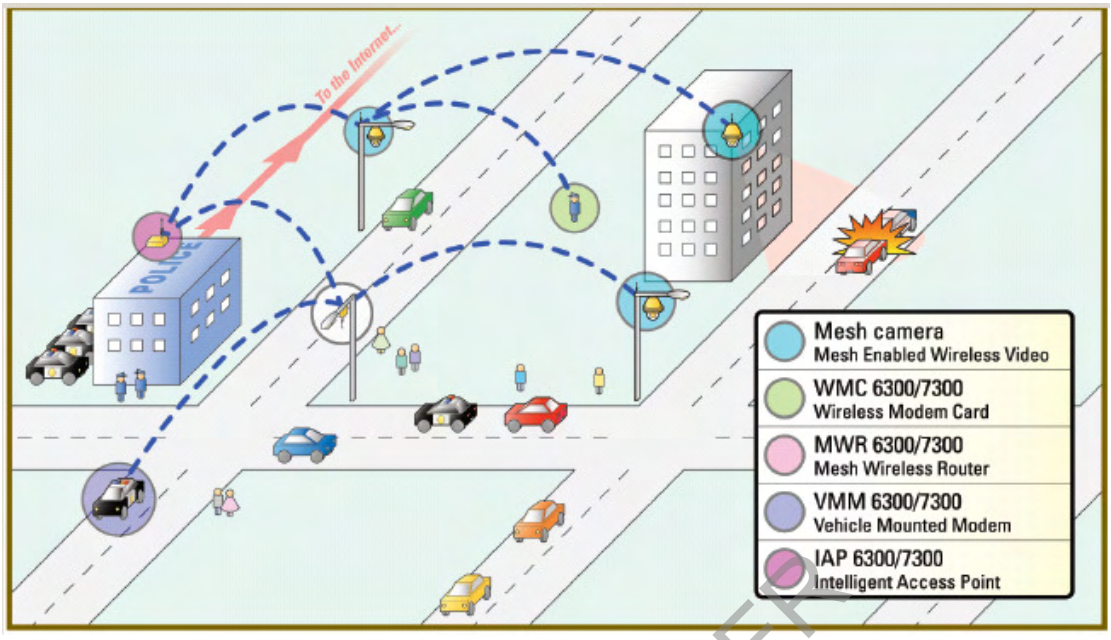


Figure 5 Wireless IP camera network based on mesh networking technology[23]

RELEASED UNDER THE FOI ACT 1982

Satellite

Fixed satellite services is available for non-military purposes and is used for broadcast feeds for television networks, as well as for telephony and data communications. This method of communication is feasible in terms of bandwidth, but is expensive. It requires the signal be routed through an earth-based transmission tower for both transmission and reception of data, which introduces latency. This method of communication may be useful for emergency situations or infrequent communication with remote cameras that are not accessible through other methods (i.e. IP infrastructure)

Fibre

Some of Australia's IP infrastructure is based on fibre optics, which allows for long distance transmissions with low signal degradation. The major disadvantage of fibre is the high cost in fibre and installation. There is typically no existing infrastructure thus cables will have to be laid. Also, due to the long-distance method of transmission, the topology of the network becomes more centralised as opposed to distributed, which often means even higher costs for laying down more cables.

Two main types of optical fibre used in fibre optic communications include multi-mode optical fibres and single-mode optical fibres. A multi-mode optical fibre has a larger core (≥ 50 micrometres), allowing less precise, cheaper transmitters and receivers to connect to it as well as cheaper connectors. However, a multi-mode fibre introduces multimode distortion, which often limits the bandwidth and length of the link (~1km). Furthermore, because of its higher dopant content, multimode fibres are usually expensive and exhibit higher

[23] Motorola Wireless Camera Spec Sheet, by Motorola Inc, 2008.

attenuation. The core of a single-mode fibre is smaller (<10 micrometres) and requires more expensive components and interconnection methods, but allows much longer, higher-performance links.

Microwave/Laser/Colour

Potential future methods of communication for wireless communication (currently not widely adopted) include microwave and lasers. Microwave is a medium range wireless method, but requires a spectrum licence to use that channel (higher cost). Lasers require line of sight, but is fast, wireless and does not require a spectrum licence.

To address the issue of supporting multiple cameras through fibre optic communication, colour wavelength multiplexing[24] can be used to increase the channels available in existing fibre optic infrastructure thus increasing bandwidth. This can thus increase the number of cameras a fibre can carry.

5.3.2 Open Standards in Compression Technology (H264 SVC)

A major difficulty with digital technology is the large bandwidth consumed by digital video. Some form of digital compression is always used to alleviate this problem even if it is only compressing the raw image frame to jpeg. These compressors are called codecs[25] A number of proprietary codecs are in use which are generally just propriatary modifications of open codec standards for the surveillance task. Recently there has been a strong trend away from proprietary systems towards open-systems so that different brands of cameras can interconnect in large IP networks.

A major initiative in this area is the new BAS camera standard being forged by Bosch, Axis, and Sony[26]. In June 2008, these manufacturers announced the very first cooperation in the security industry to establish a global open standard for the interface of network video products. This trend also extends to support of open standards for codecs — especially H264.

RELEASED UNDER THE FOI ACT 1982

[24] "Wavelength-division multiplexing", from Wikipedia. Accessed 27 June 2009.

[25] Codec stands for Compressor-Decompressor

[26] Axis, Bosch and Sony cooperate to standardise the interface of network video products, Sony press release, 19 June 2008.



Figure 6 CCTV Image of London Tube Bombers 7th of July, 2005. Note the interframe prediction artifact that shows the metal railing in front of one of the bombers instead of behind him.

RELEASED UNDER THE FOI ACT 1982

It is important to record video at the highest possible quality if it is to be used for forensic purposes (as could always be the case). Codecs such as MPEG4 and H264 use interframe prediction so that the current frame is often assembled from parts of earlier and possibly later frames. This can have unfortunate consequences as seen in the famous photograph in Figure 6 where a railing is shown in front of one of the bombers instead of behind. Such a significant error in a forensic image could have serious consequences in a court of law.

Customs currently uses MP4 codecs extensively, mainly due to the bandwidth saving and high quality of images. The Group of Pictures (GOP)[27] structure used has a key frame interval of 4 secs, which is fairly benign. Keyframes are stored independently of adjacent frames and are thus suitable for forensic purposes. Customs systems use variable bit rate encoding and is not highly compressed. These allow the codec enough processing power to reduce the risk of prediction errors, although the risk can't be dismissed altogether.

Where the above risks can't be mitigated it is recommended to record in a still frame format which uses intraframe compression only at such as JPEG, JPEG2000, or MJPEG as described in Table 8. For remote viewing and monitoring, H264 Scalable Video Codec (SVC) is rapidly becoming the codec of choice in surveillance applications.

Scalable Video Coding (SVC) is an extension of the H.264/MPEG-4 AVC video compression standard. The objective of SVC is to enable the encoding of a high-quality video bitstream in a scalable manner to accommodate viewing at many different resolutions. The subset bitstream is derived by dropping packets from the larger bitstream. This allows very high

[27] In MPEG encoding, a **group of pictures**, or **GOP**, specifies the order in which intra-frames and inter frames are arranged. See http://en.wikipedia.org/wiki/Group_of_pictures

quality video data to be viewed at much lower resolutions on a wide range of devices. The need for scalability arises from degradation of transmission rates (wireless or internet), or needs for specific spatial formats, bit rates or power. Unlike other digital codecs such as MP4, the SVC codec was specifically designed for surveillance applications.[28]

Codec	Bandwidth compared to baseline MJPEG codec	Application	Comments
JPEG	1.0	Still frame transmission,	Standard for photography
JPEG2000	0.8	Megapixel Cameras, scalable, easy to reconstruct at different resolutions.	Better than JPEG for certain images but not widely supported
MJPEG	1.0	Often used for surveillance where frame rate is low and there is large movement between frames. Good for forensic analysis. Good quality for local recording.	low processor overhead, ease of editing, no standard implementation
MPEG4	0.4	Often used for remote viewing, not so good for forensic applications due to interframe artifacts	Introduces high latency due to frame deinterleaving process
H264	0.2	Best for remote viewing, not as good for forensic applications due to interframe artifacts	Baseline implementation has low latency,
H264 SVC	0.2	Similar to H264 but designed with multimedia and surveillance applications in mind. Very easy to scale bandwidth. Codec of choice for surveillance	Baseline implementation has low latency, very easy to convert to different resolutions

RELEASED UNDER THE FOI ACT 1982

Table 8 Codecs for Surveillance Applications

5.3.3 Bandwidth

There are numerous misconceptions in the video surveillance market regarding bandwidth requirements of video surveillance running over a digital IP network infrastructure. The factors which should be considered when considering bandwidth are:

Compression and DSP technology improvements

As discussed above, rapid advancements in compressing algorithms have been helpful in reducing bandwidth requirements. For a 30 fps D1 720x480 resolution (NTSC) video camera,

[28] "Scalable Video Encoding" from Wikipedia, accessed 27 June 2009.

the old MPEG-2 format required 4 to 5 Mbps video stream, the more recently introduced MPEG-4 format cut the video stream down to approximately 3.5 Mbps with no discernable loss in quality[29]. Other compression techniques, including H.264 SVC offers to further reduce video bandwidth requirements even further.

Network bandwidth

A LAN switch is a local area networking device that prevents data packet collision, and maximizes transmission speed as well as bandwidth allocation. It can be used instead of a network hub (which does not prevent collisions and shares bandwidth) to solve problems associated with expanding networks. Most LAN infrastructure deployed in organisations in the last 10 years are using at 100 Mbps switches which have an effective throughput of 80 Mbps to support 40 streams of 2 Mbps video. Larger organisations have 1000 Mbps or 1 Gigabit LAN switches which can support 400 streams of 2 Mbps video[30]. Such corporate network infrastructure should meet the needs of even the largest Customs installations (Brisbane airport anticipates around 400 cameras after expansion).

Wide area network (WAN) for remote access

WAN connectivity from remote locations may have more limited bandwidth (due to cost/availability), and thus need to minimise consumption through measure such as on-site recording, on-demand-only remote video streaming, or alarm/analytics-based trigger for video transmission (refer to section 5.2.2 for further discussion on storage and streaming).

What kind of streaming is being used: multicast or unicast?

A single video camera produces a single "unicast" video stream. If multiple users want to view the same information, rather than sending multiple copies over the network, “multicast” technology should be used. Multicast provides a copy to users through subscription where the network infrastructure handles the replication of the video to multiple devices at the point closest to each subscriber, rather than replicating from the source, thereby minimizing bandwidth over shared links.

Although in the Customs environment it is less likely that multiple people will wish to view exactly the same video feed, this may be required in an emergency situation. A more common scenario is that the same video may need to be viewed by multiple computer agents. For example the same video feed may need to go to an NVR, face recognition system, numberplate recognition systems, and camera checking system.

RELEASED UNDER THE FOI ACT 1982

[29] “Cisco Systems IP Network-Centric Video Surveillance”, Cisco, 2009.

[30] ibid

5.3.4 Data Security

IP opens the possibility of interoperability with multiple stakeholders over the network; data is no longer localised, but rather, can be accessed from around the world. Wireless communication and networking has resulted in a need for ensuring that the data is protected and can only be accessed by certain stakeholders. An access policy will also have to be determined to give specified levels of user access privileges to these data.

Encryption

For IP-surveillance, encryption can be used to prevent the unauthorised viewing of transmitted video. While an encrypted stream may be intercepted, it has no value unless it can be decrypted. Modern best practice cryptography is very strong and is virtually impossible to break. There are numerous encryption methods, the details of which are out of scope for this document, however the major factors to consider for encryption are common; A good video encryption method should ensure that[31]:

- Everyone has a unique encryption key or code.
- The encrypted signal should be positively identified by the decoder. The decoder should recognise the encrypted signal and only attempt to decode when fully validated.
- On screen status display and identification.
- Work with any video standard.
- Not introduce unacceptable processing latency or bandwidth constraints

RELEASED UNDER THE FOI ACT 1982

Virtual Private Network

A VPN is a network constructed using public channels. VPNs rely mainly on encryption and firewalls to ensure that only authorized users can use the network and the data cannot be intercepted. Strong encryption prevents eavesdropping. Public key encryption allows authentication of wireless terminal users. Other security methods include simple user names and passwords for authentication and user server directory systems using digital certificates.[32]

[31] "Video Encryption" by Ovation Systems. Retrieved on 17 June 2009.

[32] "Security Technology-North American Trends and Developments in Video Surveillance", Frost & Sullivan Technical Insights, 2004.

The advent of VPN has significantly reduced the risks attached to network access and is the most commonly used method. However, with network access technologies emerging to displace existing communications technologies, VPN remains only slightly uncontested[33].

Access Policy

Access Policy multiplexing can be used to separate data with different levels of access control. An access policy can be set to permit or deny the use of particular resources, such as cameras recordings, by a particular entity and define acceptable methods of remotely connecting to the internal network.

5.3.5 Open Standards in Communication and Software

The increasing awareness and commitment to security are pushing countries to develop more efficient command and control centre networks for border security, especially at airports.[34] As the trend moves from analog to digital (IP) CCTV systems, it is also moving from a proprietary model where the components of the analog system including camera, codec and software were sold as a "black box", to an "open standard" or "open architecture" system where components have standardized interfaces and communication protocols (such as HTTP and RTSP) thus allowing for swappable components. In particular open IP surveillance software, which includes the software that enables digital managing and processing of video image surveillance in network server-based installations, are becoming non-proprietary in nature and offer extensive scope for customization. The trend for open standards in software has been increasing in recent years, mirroring the adaption of open architecture systems, and is forecasted to have steady growth through to 2012 as seen in Figure 7.

Airports, particularly in the US, are anticipating the introduction of updated digital technologies, and thus have implemented open architecture schemes in order to accommodate new technology as well as greater network interoperability.[35] The connection of all security initiatives to a main network and control room allows the security operators to have greater oversight over various operations and areas. Network connection throughout the airport is based on open architecture systems and typically using WAN or LAN IP communications. Wireless connectivity is becoming increasingly useful for border security, especially to communicate flexibly with emergency first responders, such as the AFP, state police and fire department.

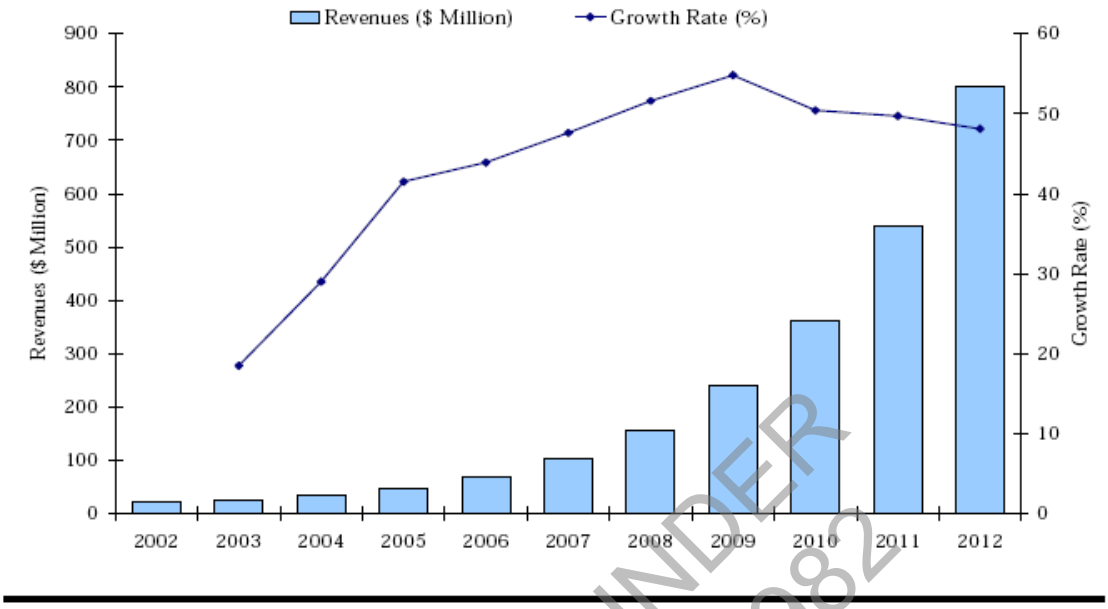
RELEASED UNDER THE FOI ACT 1982

[33] Rohan, R., "NETWORK SECURITY TACTICS: Letting telecommuters in -- Your VPN alternatives", SearchSecurity, 2005.

[34] "World Airport Perimeter Security Markets", Frost & Sullivan, 2006.

[35] Ibid.

Total Open Internet Protocol (IP) Surveillance Software Market: Revenue Forecasts (World), 2002-2012



Note: All figures are rounded; the base year is 2005. Source: Frost & Sullivan

Figure 7 Total Open IP Surveillance Software Market[36]

RELEASED UNDER THE FOI ACT 1982

5.3.6 Systems Ownership

The implications of using IP-Surveillance have an impact on Custom's business model. Currently, Customs owns everything in its surveillance systems due to proprietary technologies which are black boxes. However, with open standards being introduced for digital and networked systems, components can be individually managed and even outsourced.

section 47E(d) [redacted] However, it is not uncommon for seaport terminal operators to deploy their own CCTV systems. With the migration to Open Standards private operators are increasingly likely to adopt open video transmission protocols through IP and open video compression standards such as MP4 or H.264. Thus, there is a` potential for Customs to share or access private networks which will eliminate installation and maintenance costs for Customs (though with the draw back of less control and potentially fewer access privileges).

[36] "World Internet Protocol (IP) Surveillance Markets", Frost & Sullivan, 2006.

5.4 Cameras

The most common form factors for CCTV camera are dome, bullet and standard body cameras, which can have a variety of features incorporated. This section will discuss the latest trend of megapixel cameras in depth and give a brief overview of other available or emerging special purpose camera features. Camera placement issues, automated camera checking, and sensor fusion will also be mentioned in this section.



Standard body



Dome



Bullet[37]

5.4.1 Megapixel Cameras

Standard definition cameras have resolutions comparable to analog television. Only a few video resolutions are widely supported in the industry, mostly based on the CIF (*Common Intermediate Format*) standard used to specify the horizontal and vertical resolutions specified in pixels of video signals. It was first proposed in the H.261 standard and is commonly used in video teleconferencing systems. Table 9 gives the resolution of common CIF standards. This is quite an old standard as if was first proposed in 1990. The 4CIF standard is equivalent in resolution to standard television and is commonly supported by modern DVRs which digitize analog video feeds. While a higher resolution of 16CIF is defined, it is not supported by any analog television standard and thus is not used in practice.

RELEASED UNDER THE FOI ACT 1982

SD Format	Video Resolution	Aspect Ratio	MPixels
SQCIF	128 × 96	4:3	0.012
QCIF	176 × 144	4:3	0.025
CIF	352 × 288	4:3	0.1
4CIF	704 × 576	4:3	0.4
16CIF	1408 × 1152	4:3	1.6

Table 9 CIF standards for standard definition digital video

Good image quality and higher resolution is essential to identify objects and people as we often need to read text (licence plate or container number recognition), or to recognize faces.

In analog CCTV camera systems, the traditional approach to obtaining high resolution detail while maintaining situational awareness over a wide area is to supplement fixed wide-angle CCTV cameras with high power PTZs. The PTZ cameras can magnify the size of objects by a factor of 50 or more.

---

[37] "CCTV Security Camera Types", Camera Security Now, Accessed 13 May 2009.

The PTZ cameras alone can be used for situational awareness when they are set to wide angle view, but there is a significant risk in this approach. The problem is that when they are zoomed in to observe details, they are no longer available for situational awareness. Moreover, unless the operator returns the PTZs to a preset wide angle view, situational awareness can be lost for hours.

This is exactly the problem that occurred in Kuala Lumpur International when the terminal was robbed last year[38]. In April 2008, robbers shot and wounded six people at Malaysia's main international airport before fleeing with $1 million. Unfortunately there is no CCTV footage of the robbery because although there were many CCTV cameras, none of the PTZ cameras were actually looking in the right direction at the time. The problem was that there were no fixed CCTV cameras installed to record the overall scene. The airport is now retrofitting the airport with a mix of fixed and PTZ cameras[39].

IP surveillance systems can support resolutions much higher than the 0.4 MPixels represented by analog television standards. Such cameras are usually referred to megapixel cameras and most are based on HDTV standards as provided in Table 10. Note that these so-called megapixel cameras are all IP-based as there are no analog cameras with resolutions greater than standard definition television.

RELEASED UNDER THE FOI ACT 1982

HD Format	Video Resolutions	MPixels	Aspect Ratio	Comments
720p	1024×768, 1280×720, 1366×768	0.8, 0.9, 1.0	16:9	Often used on PC monitors
1080i	1280×1080	1.4	Approx 16:9	Non-square pixels
1080p	1920×1080	2.1	16:9	Full HD

Table 10 Standards for high definition digital video

These megapixel cameras offer about 5 times the number of pixels of standard 4CIF and about twice the linear resolution as illustrated in Figure 8. The linear resolution is defined by the number of pixels per cm for a given display size. Thus for a square image with side *n* pixels and area *nxn* pixels, the linear resolution increases as the square root of the number of pixels. This is a worthwhile gain but the resolution improvement is only a factor of 2 equating to a PTZ with a zoom of only X2 —a useful improvement but this doesn't change the need for PTZs to supplement fixed cameras to gather necessary detail.

[38] Sean Yoong, "Six injured at Kuala Lumpur airport in million-dollar robbery", The Seattle Times, 9 Apr 2008.

[39] FutureCCTV, personal communication with Datuk Kamaruddin Mohd Ismail, Malaysia Airports Holdings

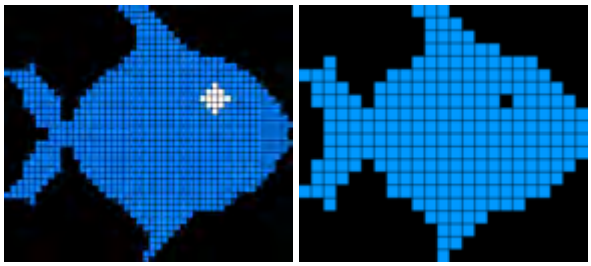


Figure 8 HD resolution (left) versus SD resolution (right)[40]

Now that analog television is being made obsolete by digital television, it is likely that 1.4 and 2.1 MPixel cameras with 16:9 aspect ratios will become the entry level formats for both fixed and PTZ formats— there will be little support for CIF standards in the future.

Super Megapixel Cameras and Virtual PTZs

There is however a game changing super megapixel camera technology emerging that may largely do away with the need for PTZ cameras for within building surveillance in, say, airport terminals. Currently these cameras record video at up to 16Mpixels at a slow frame rate of approximately 3 fps — but both frame rates and resolution are improving continually.

Figure 9 shows a super megapixel image of an airport departure check-in area. The single super megapixel camera gives a view of the whole scene and also provides "virtual" PTZ views into the main window so that faces and activities can be identified. Note that unlike a traditional PTZ, these virtual PTZ's can be zoomed in after the video is recorded. Compare this to a traditional analog PTZ which must be zoomed in on the person of interest in real-time or the capture opportunity is lost forever. The number of analog PTZs that can be used to track persons of interest is thus limited to the number of control room operators as the zooming must happen in real time.

In the super megapixel system, quality forensic evidence can be extracted well after the event has occurred. Note that these cameras provide the wide-angle situational awareness view as well as the virtual PTZ detail at zoom factors of about X7. Certainly this is not a powerful zoom capability compared to many conventional PTZs operating at X30, but it does allow detailed forensic observations to be extracted after the event has occurred. Moreover one well positioned camera can do the job of several conventional cameras. Of course, super megapixel cameras can be mounted as PTZs with powerful optical zooms, but then we come back to the problem of loss of situational awareness and the risk of having poor camera placement at the time when an unforeseen incident occurs.

RELEASED UNDER THE FOI ACT 1982

[40] High-definition Television. Retrieved from Wikipedia on 17 June 2009.

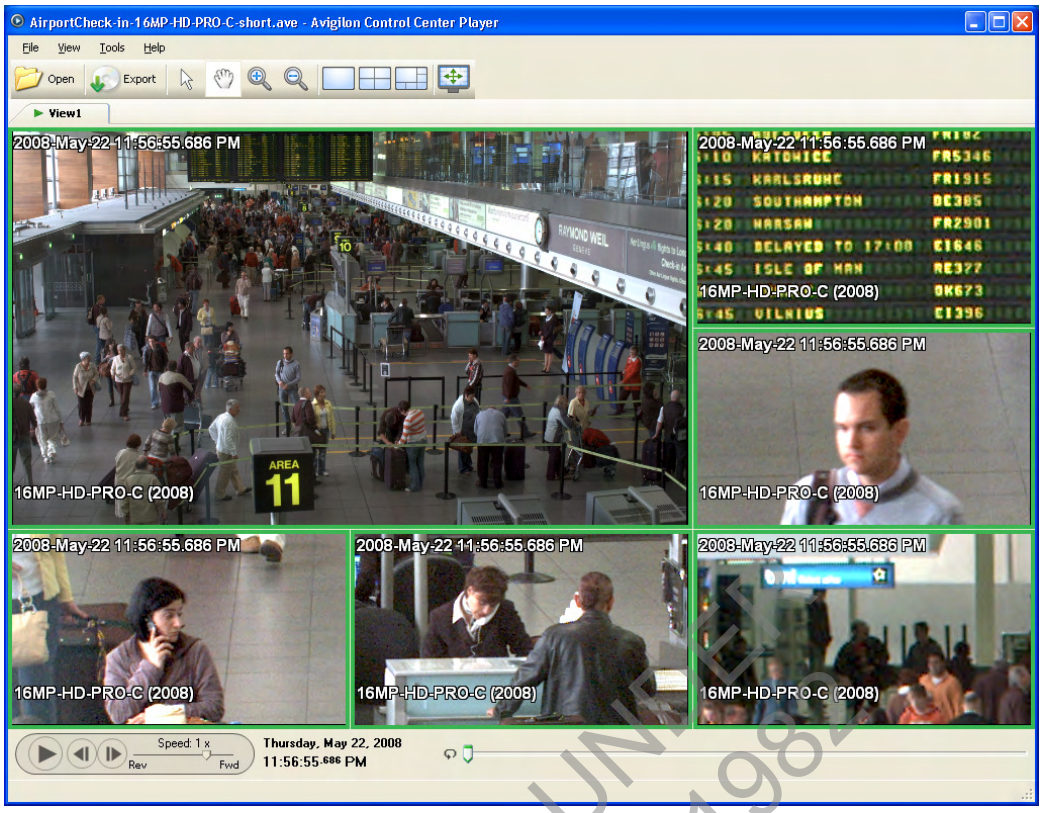


Figure 9 A 16 MPixel camera viewing airport departure hall[41]

RELEASED UNDER THE FOI ACT 1982

Figure 10 shows a super megapixel camera viewing a city intersection. Once again faces and number plates can be identified well after the event was recorded. One camera can give complete coverage of a large area with both detailed observations and situational awareness.

Another less obvious advantage of the technology over conventional PTZs is that many users can share the same camera and the virtual PTZs without revealing what each user looking at. One potential application for Customs is to enable Customs, the AFP, and airlines to all have access to the same super megapixel cameras and without one knowing what the others are interested in. At Brisbane airport, the customs officer said that they would share fixed cameras, but would not share PTZs as this would reveal their interests. It would seem that super megapixel cameras can offer a technological solution for multi-agency sharing through the use of virtual PTZs.

An immediate objection to using this technology is the data storage requirement which can be considerable. For this reason the full resolution 16MPixel images must be stored locally. Even terabyte disks are quite cheap these days (AUD200 per Tb). Moreover data can transparently be migrated to cheap offline storage and easily recovered by any user using

[41] Avigilion Corporate website. Retrieved 17 June 2009.

hierarchical storage management (HSM)[42] systems as developed for the seismic industry and now commonly deployed to manage huge corporate data and email repositories in large organizations. Such commercial HSM systems are readily adaptable to surveillance systems. It is just a matter of deciding an appropriate metric for migrating data to slow storage. Simple metrics include recording time or time of most recent access.

Remote viewing can be done anywhere as there is no need to send the full resolution super megapixel images. For example, If video is displaying remotely on a 1280x1080 PC screen, it is quite impossible to display more than 1280x1080 = 0.9 MPixels per frame, regardless of the source resolution — so all that the remote site needs is a standard video datalink to view super megapixel data. Downsampling of the datastreams to match the remote viewing resolution is handled transparently by the server software.

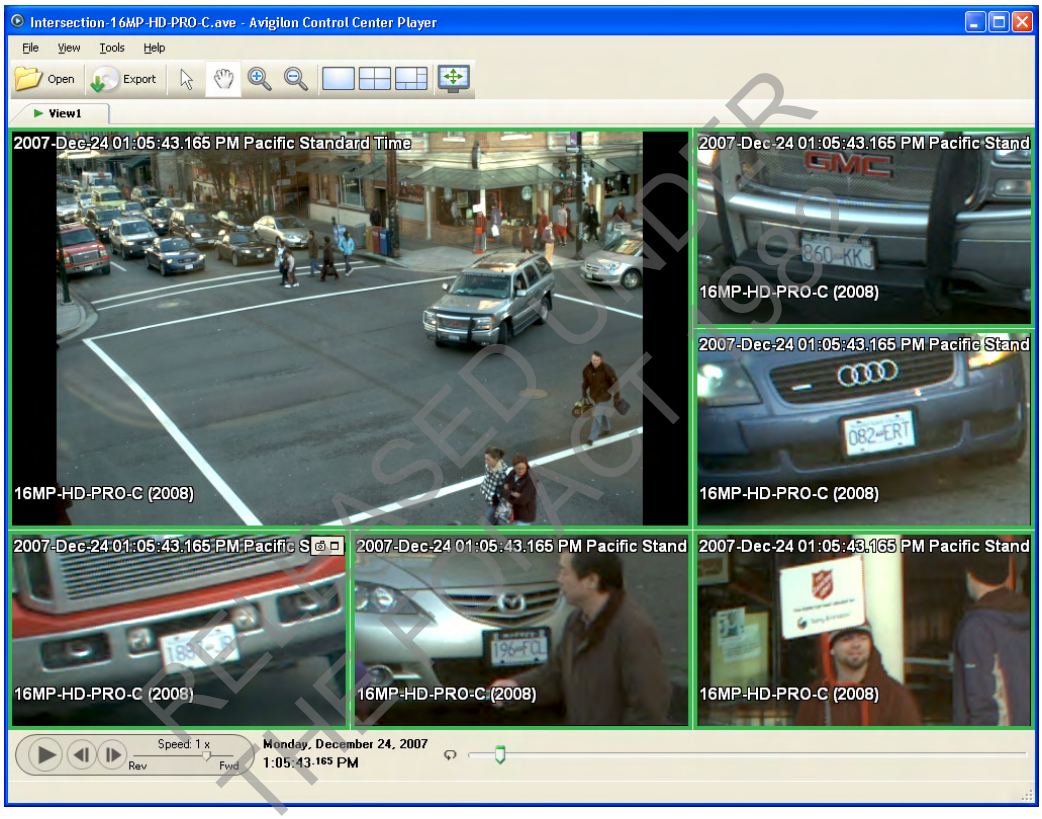


Figure 10 A 16 MPixel camera viewing city intersection[41]

5.4.2 Other Special Purpose Features

- **Low light** – Cameras are typically rated to be most suited to particular lighting conditions, presented as a specification known as lux rating or minimum illumination rating; the closer to zero the lux rating, the better the camera will perform in a low light applications. Some low-light cameras can have sensitivities as low as 0.0009

[42] **Hierarchical Storage Management** (**HSM**) is a data storage technique which automatically moves data between high-cost (flash, fast disk) and low-cost (slow disk, tape, optical) storage media. More information available from http://en.wikipedia.org/wiki/Hierarchical_storage_management

lux. Another option for low light is thermal imaging or supplementary artificial lighting (visible or infrared).

- **High Dynamic Range** - High dynamic range imaging allows for a greater dynamic range of luminance between light and dark areas of a scene than normal digital imaging techniques. This feature is useful for sporadically lit night scenes.
- **Thermal** – Cameras can operate in the infra-red range to image temperature rather than visible light. This feature is useful to provide another type of information that is not visible to the human eye, and also for low-lighting conditions.
- **180/360 degree** – Some cameras can provide hemisphere, or spherical views. Such views may be useful as overview cameras to provide more context, and thus situational awareness. The 180/360 degree cameras can be particularly useful in busy open areas that require extensive monitoring. It avoids one of the limitations of PTZ hotspot cameras in that those cameras typically have narrow field of view, thus may miss something if not pointed in the right direction (refer to the KL airport robbery story[43]). However, hotspot cameras typically can zoom into a scene whereas 180/360 cannot. Thus, they can be used in combination to get both an overview and detailed view when necessary.
- **All focus** – Emerging work is looking into cameras which synthesize an all in-focus image that is clear and sharp throughout the entire scene, as opposed to conventional cameras with blurred images of scenes not in its plane of focus. Having sharper images will improve forensic analysis capabilities such as for person identification.
- **Computational Photography** – An emerging feature is the combination of images captured from different types of lenses to computationally fuse together information about a scene. Figure 11 shows a compact wall mounted camera that fuses 5 cameras into a single panoramic view. This is an excellent alternative to expensive wide angle lenses to provide situational awareness in an indoor environment.
- **Image Stabilisation** – This feature makes the video more robust to vibrations to reduce noise the in the video. It can either be through software, or hardware.

RELEASED UNDER THE FOI ACT 1982

[43] Sean Yoong, "Six injured at Kuala Lumpur airport in million-dollar robbery", The Seattle Times, 9 Apr 2008.



Figure 11 IP camera made up of 5 cell phone camera lenses. In the form of an Ethernet powered box, this camera provides a 180° panoramic shot[44]

RELEASED UNDER THE FOI ACT 1982

5.4.3 Placement

The different features available for the above cameras will affect the camera placement. Currently placements of cameras are done manually based on experienced installers, common sense and similar reference sites. Some considerations manual installers must consider are:

- Camera placement to give both overview and also particular hotspot areas
- Cameras placed to cover too much area will typically be useless for forensic analysis
- Ensuring the placement is close enough to meet certain resolution criteria (e.g. using a test image of "E" with dimensions 160x96 mm which must be greater than 10x6 pixels on the CCTV monitor)

There is emerging software to assist with optimal camera placement, including Sarnoff Corporation's 3D camera placement tool[45] used at Superbowl 2007 which reduced the required number of cameras by 40% with improved coverage compared to manual placement[46].

5.4.4 Automated Camera Checking

At the beginning of every shift, Customs operators at Brisbane Airport manually scan every camera to ensure that they are operating correctly. With hundreds of cameras installed this task takes considerable time to perform (30 mins). In IP-based CCTV systems (or hybrid

---

[44] Scallop Imaging Corporate Site. Available at http://scallopimaging.com/product.php

[45] Praetorian: Intelligent Surveillance Solutions Corporate Site. Available at http://www.l3praetorian.com/cameraplacement/index.htm

[46] Praetorian case study

systems), software exists to automatically scan all the cameras on a regular schedule to check for correct operation. Often the current camera image is checked against a reference image ensure a good match and to detect anomalies that may need human attention.

Such a system can provide automatic alerts and reports when cameras

- are disconnected or out of focus
- have been physically moved or tampered with
- are providing poor image quality
- are unable to see well due to bad weather, variable lighting or other complex conditions.

Such tools are extremely useful to optimise performance and minimize downtime. One very useful feature is to detect when cameras are moved out of position to provide blind spots for illicit activities. Such changes are hard to detect, especially if movement is gradual over several days.

5.4.5 Sensor Fusion

With the digitization of surveillance systems, other forms of data can be relayed along the same digital channels as the video. This enables sensor fusion capabilities, which augment visible information from the camera with other environmental information such as audio, thermal, wind, GPS location, etc.

An example of such fusion in a retail situation is showing the video of checkout operators alongside the barcode reader output on the same display screen[47]. This same company has also connected the PTZ camera control to the asset protection tag readers. This means that if a person walks out of the store with a tagged asset, the alarm goes off, and the PTZ immediately positions itself to record video of the shopper and security guard. They also use analytics to count crowds at marketing promotions and sell these data to the suppliers for added cash flow. There is no permanently staffed control room and all recording is gathered automatically throughout the day.

Translating these ideas to the Customs environments, it may be worth considering combining the X-ray inspection video with CCTV or the PACE (passport) system with CCTV of persons at immigration. Customs may be able to sell crowd statistics gathered by analytics to airport operators or possibly the airlines themselves and can certainly use these internally to generate quality of service metrics.

At the seaports it would be helpful for the AIS data to be presented alongside video of the vessel. Already many advanced interfaces combine maps and video for added context — but the possibilities are endless . The open architecture IP network facilitates very easy reuse and combination of disparate data sources.

RELEASED UNDER THE FOI ACT 1982

[47] FutureCCTV, Gao Yan Hui, Asset Protection Director, Best Buy Shanghai

5.5 Analytics

With advances in computer vision analytics, there is an increasing portfolio of software for assisting and augmenting surveillance. This section provides an overview of the emerging areas of analytics, their challenges, and the mitigation of those challenges.

The motivation for analytics is the potential to generate alarms from the CCTV feeds themselves without the need for continual human monitoring. One simple analytic is motion detection where the CCTV can act like a passive infrared home alarm system that raises an alarm when movement is detected in an area under surveillance. Rather than just simple movement, alarms can be much more sophisticated than burglar alarms. For example fence climbing can be detected on perimeter fences. Alarms may be directional. For example, people can be detected travelling in one direction rather than another (entering through the exit door perhaps).

This is the promise of analytics, the reality is that many visual alarms are unreliable and generate so many false alarms that the systems are simply switched off. Indeed, some cheap home alarms have the same problem. Almost none of the current systems can cope with the simple problem of a vibrating or panning camera. However, when used correctly the very best of the current commercial systems can operate reliably and effectively. Analytics offer huge cost benefits through reducing monitoring costs and increasing effectiveness when they work properly, but developing reliable alarms is a huge technological challenge that is extremely expensive. New and improved analytics are emerging all the time and a well-designed IP surveillance system should be fairly easily upgraded to emerging technologies using open standards.

RELEASED UNDER THE FOI ACT 1982

In the words of Angus Hamilton:

"I can see in the next 20 years everything will become automated. Once the camera is sophisticated enough, it will profile people that we don't really need human beings apart from to check it out and analyse it."

"Integrated Security Management is the way it's all going to go. It's all going to multipurpose, all being analysed and put together."

— Angus Hamilton, Director of Corporate Security, Shangri-La Hotels and Resorts, Hong Kong, and former Assistant Commissioner of the Hong Kong Police [48]

5.5.1 Integrating Video Analytics into a Monitoring Centre

Visual Alarms

With the introduction of digital video, computer vision techniques can be used to analyse and infer events to augment surveillance by providing operators with visual alarms, i.e. alerting operators by highlighting areas of interest in the videos being monitored. It has been shown in the past that operators are good at confirming whether an event is a security issue but poor at watching videos for a long time (operator monotony) which can lead to missed events. There are also typically more camera views than operators available

[48] Asian Security Review, Aug, 2007

(Brisbane airport has 2-3 personnel monitoring nearly 200 cameras), thus an operator cannot be aware of all things at all times. Given the potential cost of missing an event for border security may be fatal (for example not spotting a terrorist activity), visual alarms is a crucial piece of analytics for future CCTV Surveillance systems.

Object detection, classification, recognition, and tracking

There are numerous practical applications in the area of object detection, classification, recognition and tracking. There is extensive R&D in software can detect objects (left luggage, runway debris, people, faces) or lack of objects (asset tracking). Once detected, further analytics can classify the objects to determine whether it is appropriate for the scene (luggage without an associated person, box left on platform too long, vehicle speed and type etc.) or to recognise the object from a database (nameplate recognition, face recognition, biometrics), and alert the operators upon suspicion. Another variant is motion detection, for areas with restricted access. These objects can also be tracked through the various video frames and video feeds. Below are a few examples of analytics for surveillance applications potentially of interest to Customs:

- **Automatic Number Plate Recognition (ANPR)** – Available software using optical character recognition (OCR) to extract the characters from a licence plate 
- **Container Number Recognition** – Available software using OCR to extract numbers from cargo containers (typically not a flat surface) 
- **Left luggage** – Emerging research that detects left objects without an owner nearby 
- **Portal crossing or tripwire** – Available software which alerts operators for movement in portal crossing or breaching a defined line. MAS uses this for aircraft security after servicing. 
- **Movement (no motion, no monitoring)** – Secure areas can be monitored to alert operators to movement (i.e. to ensure personel is allowed or should be there) 
- **Counter Flow** – Emerging software for person moving against an immigration route 
- **Face detection** – Detect and record face images to be reviewed later in the event of an incident. Currently used in ATM security. 
- **Face recognition** – An emerging area of research which can use images of faces detected to see if they are similar to any in a watch list, or for searching through recorded video using face images. 
- **Biometrics** – Using computer vision to verify the identity of a person. Can be used for access control or border security. 
- **Person & Multicamera tracking** – Emerging research that tracks people in videos which can help in airports to follow or retrace the movements of people being

RELEASED UNDER THE FOI ACT 1982

monitored, or people who have just arrived and thrown away their documents

Video Enhancements

Through image processing or incorporating other sensory data:

- **Rain and fog mitigation**[49] - This technology can provide an improved operator view during rain and fog as shown in Figure 12.
- **Infrared** – Near and far infrared cameras can be mixed with visible light cameras.
- **Sidescan Sonar** – Sidescan sonar can image objects underwater including the hulls of vessels.
- **Sensor Fusion** – For example, Infrared and visible cameras can be combined to form an enhanced view of low light events as shown in Figure 13.
- **Integration of Other Data Sources** (AIS, Radar, LIDAR) – Figure 14 shows AIS information overlaid on a 3D model of a container ship at Port of Brisbane.

RELEASED UNDER THE FOI ACT 1982



Figure 12 Rain mitigation video filter operating at the Port of Brisbane during storm.

[49] NICTA research prototype at Port of Brisbane



Figure 13 Feature selective fusion of IR and visible light



Figure 14 Overlay of AIS data on 3D model of container ship at Port of Brisbane.

RELEASED UNDER THE FOI ACT 1982

Fast Forensic Search

In modern CCTV systems, more and more cameras are being interconnected, image resolution is increasing, and thus data storage is growing exponentially. It is simply impossible for a human to search for the rare events of interest in such large archives. Even computers can rarely search video streams at a rate much faster than real-time.[50] This means that thoroughly searching, say, 8hrs of video for a certain event on 100 cameras could take up to 800 hours or 20 weeks for a single human operator. Time can be saved by using fast forward and rewind at speeds of up to 600x, but there is a significant risk that short duration critical events will be missed due to frame dropping.

[50] This limitation is partly because there has been little incentive for the industry to develop hardware or software to scan video at rates greater than real-time — there is simply no demand for this from the mainstream broadcast media market. Modern computer hardware is struggling to keep up with 25 fps. The traditional approach to high speed viewing is to drop frames, which is often unacceptable for forensic searches.

Some searches are much easier to conduct as we know where and approximately when the event occurred – this is the case when we have information gathered outside the CCTV environment (e.g. physical evidence, witness report). Such information means that we may know the camera number and the time frame. However there are many searches where information must be gathered by exhaustive searching of the CCTV itself. A famous example is the identification of the London Tube bombers after the attack of 7th of July 2005 where thousands of hours of video had to be examined by hundreds of police.

There is a pressing need for a Google-like tool which can instantly search for events of interest in large CCTV archives. This would require each video to be pre-labeled in real time by the computers so that the search could be performed almost instantaneously to gather all likely video candidates. Such technology is several years off, but is highly desirable and is the subject of current research.

Some attempts to label video by content are contained in the MPEG7/21 standards, but they are not aimed at the surveillance market. However one useful feature is the support for face recognition already in the standards. If customs wants to position itself to adopt these emerging technologies, it must first convert to a digital backbone using open video standards. Labelling engines will run alongside the NVRs in real-time and extract the necessary metadata for fast indexing.

There are some commercial analytics are already emerging that follow this concept. For example, there is motion detection software which analyses the image using many small motion detection subwindows. Motion detection for each tile is recorded while the video is processed. After recording, the user selects the area of interest by selecting cluster of tiles. Instantly motion in these regions of interest is retrieved without the need to rescan the video. This can be helpful in, say, a port where we wish to instantly find videos of all people entering a vessel while ignoring other movements on the wharf. Although there are a very few visual alarms that can perform motion detection from panning cameras, in general fixed cameras should be used for computer monitoring.

Much more powerful systems being researched would allow operators to instantly search for people by face, height, or colour of their clothing.

RELEASED UNDER THE FOI ACT 1982

Visual Alarm	**Estimated Timeframe** **(Available Commercially and fit for purpose)**
Motion Detection	Now
ANPR	Now
Face Detection	Now
Left Object	Now
Person Tracking	Now?
Container Number Recognition	Now?
CCTV Face Recognition	3 years
CCTV Fast Forensic Search	5 years

Table 11 Timeframe for Visual Alarms

5.5.2 Common Analytic Challenges

The biggest problem with analytics is usually false alarms rather than missed events. The danger of this is that too many nuisance alarms will result in systems being turned off or ignored. Visual analytics will vary depending on the environment and will require tuning. It is best to consult an expert on the system to get the most of it.

5.5.3 Mitigating Common Analytic Challenges

For mitigating the problem of too many false alarms, some general guidelines are:

- Ask for expert advice on what is possible and what is not
- Do not rely on sales brochures. Ask users and share information
- Consider ease of use
- Get expert to set up your system and provide remote access
- Use the right cameras and position well as retrofits to existing cameras are often unsatisfactory
- Trial the technology according to a plan agreed by stakeholders

General guidelines on mitigating other environmental issues to ensure image quality (and thus getting better analytics) include:

- Use of fixed cameras for overview and to decrease camera shake[51]
- Control lighting, image quality, and camera shake
- Camera must be appropriately positioned, focused[52] (and lenses must be clean
- High frame rates and high resolution
- Other types of cameras or sensors (e.g., infrared can be easier due to greater lighting control)

RELEASED UNDER THE FOI ACT 1982

[51] Sarnoff image stabilisation technologies can handle panning cameras

[52] Pan Focus cameras

5.6 Displays

5.6.1 Advanced Presentation on 2D and 3D maps

Brisbane Airport has a system where operators click on a map of the terminal to access the corresponding camera feed on a separate screen. This system has proved to be most useful as the operators use the map to quickly access cameras is specific parts of the terminal. Another useful trick is sensible block numbering of the camera numbers — the first few digits indicate where the camera is located in the terminal.

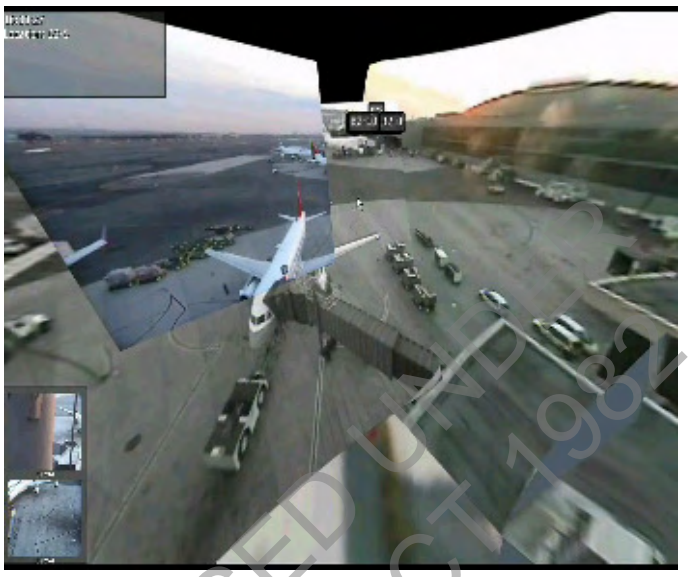


Figure 15 Surveillance video stitched in real-time at Newark Airport[53]

This concept has been taken much further in state-of-the-art presentation alternatives to traditional split screens which are commercially available. For example, Figure 15 shows an image where all the surveillance feeds from fixed and PTZ cameras covering the Newark Airport tarmac are stitched together in real-time to show an integrated view of the scene. Such a display is highly intuitive as there is now no need to memorise camera numbers at all — you just move to the area you wish to observe and zoom in as you would in a computer game. Figure 16 shows a variation of this technique where there are fewer cameras available. Here the missing camera feeds are replaced by a 3D texture mapped model of the Port of Brisbane. The fire in this image is real and the surveillance feeds comes from a camera located at Luggage Point on the other side of the Brisbane River.

RELEASED UNDER THE FOI ACT 1982



Figure 16 Surveillance video of a real fire at the Port of Brisbane overlaid on a 3D model of the site[53]

Finally Figure 17 shows a split screen presentation of the terminal at Jacksonville Airport. The surveillance system is tracking a suspect through the terminal. The current position of the suspect is shown as a moving red dot on the terminal plan in the upper part of the screen. The current camera view of the suspect is shown in the lower part of the screen as well as alternative camera views which appears as a popup video window when an alternate camera view is available. The operator can switch between the cameras by clicking on the popup. All PTZ cameras in range are automatically driven to follow the suspect without operator intervention.

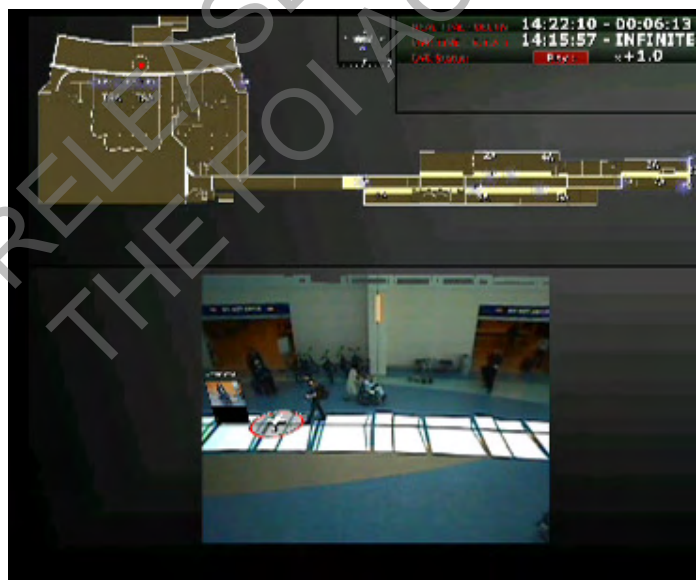


Figure 17 Tracking a suspect at Jacksonville airport. Suspect position is overlaid on a map of the terminal. Alternate view of suspect from another camera is made available to operator through a popup video.[53]

Modern IP surveillance system can present their information in many modes as these are just software modules that access video from the NVR in near real-time. There is no need to

[53] Praetorian corporate site. 2009.

RELEASED UNDER THE FOI ACT 1982

commit to a particular presentation method as multiple systems can run simultaneously. Also presentation systems can be upgraded and changed over the life of the surveillance system based on needs analysis and operator feedback.

5.6.2 16:9 Format Based on HDTV standard

Television and LCD displays are trending towards 16:9 aspect ratio, which is the standard for High Definition Television (HDTV), thus CCTV videos should conform to this aspect ratio as well to maximize screen utilization.

HDTV is an innovative set of standards for television that brings roughly twice the vertical and horizontal picture resolution of analog.[54] HDTV also has a screen ratio of 16:9 (often known as widescreen) compared with most of the traditional television sets which have a screen ratio of 4:3.

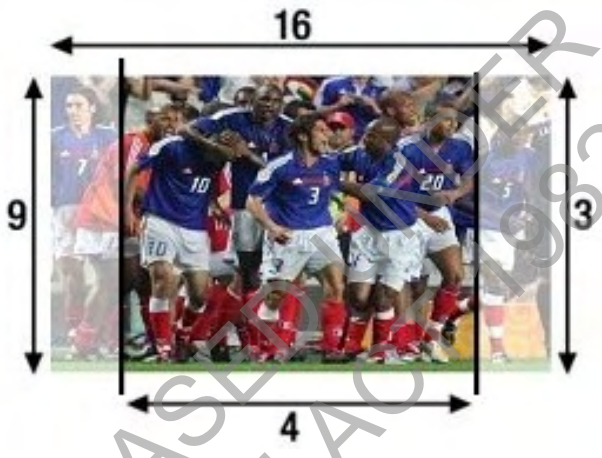


Figure 18 HDTV widescreen 16:9 aspect ratio, compared to analog 4:3 ratio

In 2008, HDTV was the trend most discussed at Australian television and broadcasting conferences and is the trend all around the world.[55] Due to the migration to digital[56] and HDTV, 16:9 transition is happening now from both the supply and demand perspectives. Digital television's role in the development of the widescreen TV market can be well illustrated by the British experience. The BBC's move to supply digital content and support the 16:9 output formats back in the 1990's has spurred the uptake of HDTV sets and clearly helped assure the consumer that widescreen is the direction, not to mention the shape, of TV's future (see Figure 19). As of 2008, 32% of homes in the UK can handle HD digital

RELEASED UNDER THE FOI ACT 1982

[54] "High Definition (HD) Technology and its Impact on Videoconferencing", by Frost & Sullivan. 17 February 2006.

[55] Peter Smart, "TV Trends in 2008", Foxtel HD: The Full Picture.

[56] Australian Government Department of Broadband, Communications and the Digital Economy (2009). *Digital Switchover*. Retrieved June 2009 from http://www.digitalready.gov.au/

content in the 16:9 format and this is projected to continue rising to 71% uptake in 2012.[57] With the rising production, the costs have also decreased to be on par with 4:3 sets[58].

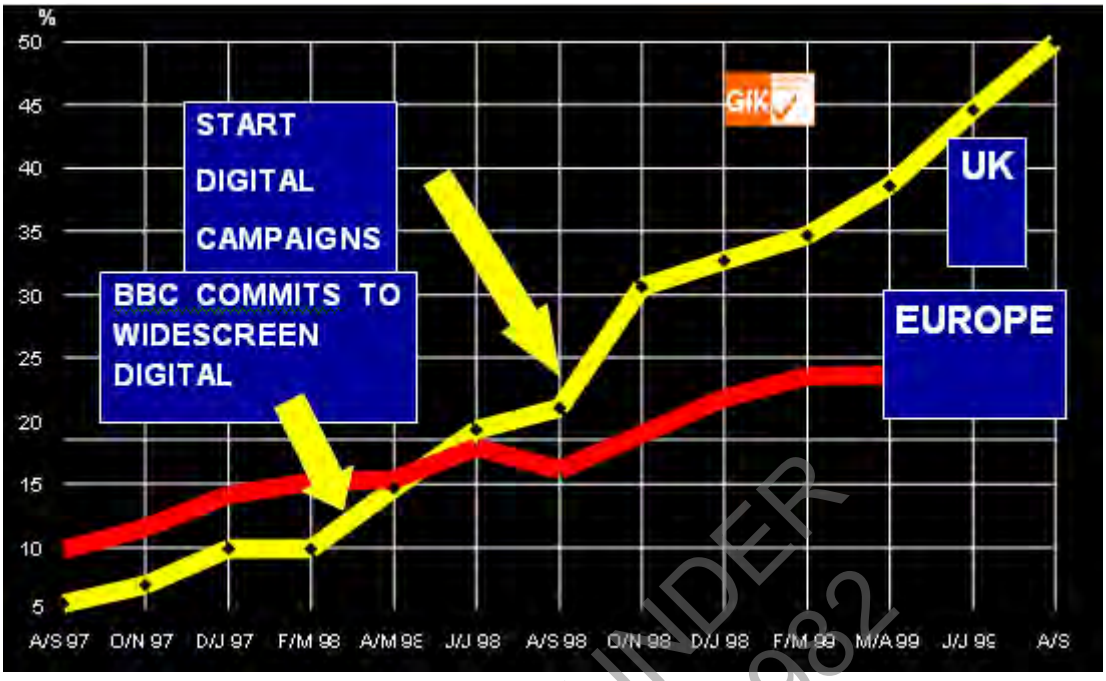


Figure 19 UK share of sales of 16:9 with the introduction of digital

Computer monitors are following a similar trend with industry analysts projecting that by 2012, 16:9 penetration will reach 90% of notebook PC panels and 67% of LCD monitor panels, as shown in Figure 20.

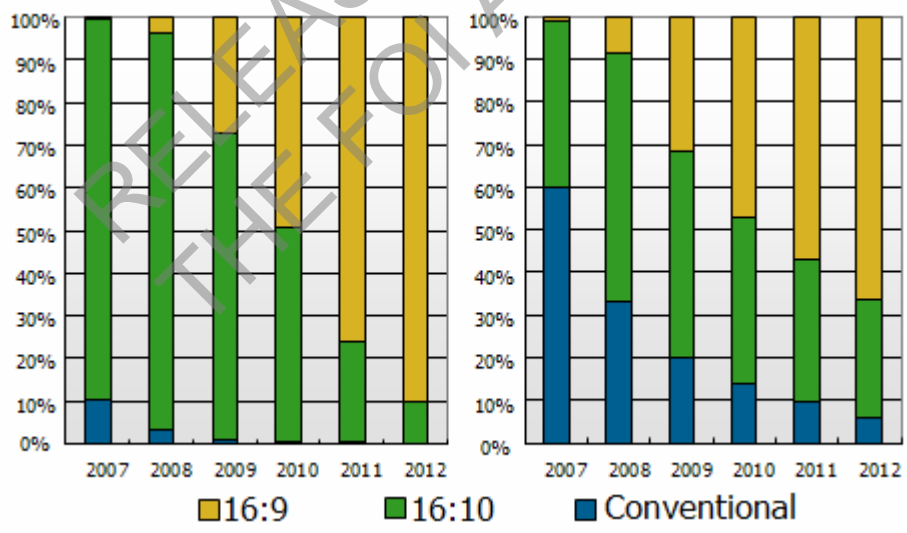


Figure 20 Forecast of 16:9 Panel Penetration in the Notebook PC (Left) and LCD Monitor Markets (Right)[59]

RELEASED UNDER THE FOI ACT 1982

[57] Jim Bottoms from specialist media analyst house, Futuresource Consulting

[58] Host Broadcast Services (HBS) "Sport and HDTV in 2006", by Francis Tellier, CEO. 17 Dec 2004.

[59] DisplaySearch *16:9 Notebook PC and LCD Monitor Analysis Report*

As the trend towards widescreen progresses, CCTV surveillance monitoring stations have started to adopt this trend. The advantage of having 16:9 aspect ratio on CCTV is that higher quality video can be observed on screen. Also, the increase in screen size also allows easy viewing of multiple camera feeds simultaneously. To maximize screen utilization and facilitate tiling, the videos should ideally be formatted to have a 16:9 aspect ratio. HDTV IP cameras which provide mega-pixel resolution, HD compatibility, and 16:9 aspect ratio, are emerging in the market to address this need. The first HDTV IP Camera on the market, the Axis Q1755, introduced by Axis Communication in 2009 delivers HDTV 1080i or 720 resolution, 16:9 aspect ratio and supports both H.264 and Motion JPEG in full frame rate.[60] This trend in HDTV IP cameras is likely to continue.

5.6.3 Mobile Device Integration (PDA, Phone)

In many IP-based surveillance products, the full surveillance capabilities can be accessed from PC or similar device connected to the internet. Thus full system capability could be accessed from a notebook, PDA, or possibly even a smart phone. This means that the CCTV operator is not tied to the control room, but is able to move about in the field. They can view and replay all cameras from anywhere they wish on a mobile platform. Effectively each guard or field operator becomes a mobile CCTV control room in their own right. There is great potential for such technology to free up staff time and improve operational effectiveness, especially in covert operations and for environments such as sea ports which may not have permanently staffed control rooms.

section 47E(c) & (d)

Mobile device integration would directly enable such covert surveillance by the officer in the field.

Moreover, visual and other alerts can be configured to send a message (SMS) to a guard when a specified event is triggered. section 47E(c) & (d)

RELEASED UNDER THE FOI ACT 1982



Figure 21 Mobile Device Integration[61]

[60] "Meet the First HDTV IP Camera - The Axis Q1755", by Wes on IP Camera Guru,

[61] iOmniscient Corporate site. 2009.

5.7 Command, Control & Coordination (C3)

There is today a worldwide trend toward a greatly extended use of information and communication technology in business, government and defense systems in order to improve operational capabilities and cost efficiency. Command, Control & Coordination (C3) technology must provide the capability to acquire, process, and disseminate information across multiple agencies; in Custom's case, to disseminate information between the AFP, APS, ASIO and State Police. This section will highlight some of the important features and benefits of C3.

Interoperability

With the use of IP networks, information can be processed through one or several, real or virtual Command, Control and Coordination Centers.

The concept is aimed to improve and extend important capabilities such as:

- Information gathering, processing and dissemination.
- Decision quality and speed of command, control and deployment.
- Collaboration between different agencies and different organizational levels.
- Flexibility in the use of a variation of emergency services and systems.

These enhanced capabilities also involve new or evolving methods for how to conduct operations and respond to events, which may require modifications to Customs operational procedure, both internally and externally (i.e. coordination with other federal agencies).

RELEASED UNDER THE FOI ACT 1982

Remote Monitoring

The same idea of interoperability can be applied internally across different geographically located hubs or business units. This can facilitate nation-wide coordination in tracking targets, but primarily, its main advantage would be to alleviate resource constraints of not having enough staff on site by reassigning monitoring tasks to remote resources. section 47E (c) & (d)

In Custom's case, remote district or national video monitoring is currently available for Seaports using a variety of transmission methods (ISDN, ATM, BDSL or Frame Relay using terrestrial or satellite telecommunication links). With an IP infrastructure and advanced scalable codecs, remote monitoring becomes less expensive with bandwidth and latency being the major considerations for network traffic. While transmission of all CCTV data to a central location is impractical, it is quite feasible to have a combination of local storage and remote streaming on request as discussed in the Bandwidth Section (5.3.3).

Single Desktop Display

In the past with analog, each camera stream was connected to a television monitor. Multiple camera streams to a single monitor required additional hardware (multiplexors) to switch between the signals. It was also impossible to display more than one camera stream on a television.

With IP, all camera streams come through the same channel. The computer which receives the video streams can display multiple feeds simultaneously in different windows on the same screen. Computer windows in a displaying video can be resized to fit more windows/video streams to an operator's preference. With the increasing size of monitors and the existence of virtual desktop software (which effectively multiplies the number of displays an operator can control Figure 22), there is an emerging trend towards having a single desktop display per operator. The shift is being adopted in casinos and hotels in Macau and across the world. [62]



Figure 22 Examples of virtual desktop software. Left: Spaces on Mac, Right: openSUSE 10.2's virtual desktop

Having a single desktop display has many benefits. It requires fewer monitors, which lowers costs and decreases space requirements; it is also more efficient for operators as they no longer have to coordinate to share consoles or search for the correct monitor to view amongst the many available; they have an individual monitor right in front of them. This arrangement makes particular sense for large control centres with many operators such as Custom's National Monitoring Centre in Melbourne.

RELEASED UNDER THE FOI ACT 1982

Scalable Situational Awareness

Situational awareness is the perception of the current situation and environmental elements, the comprehension of their meaning, and the projection of their status in the near future. Situational awareness is critical to decision makers in command and control, and emergency response. Inadequate SA has been identified as one of the primary factors in accidents attributed to human error.[63]

---

[62] Future CCTV 2009, Invited talk, Greg Morrison, Exec Director, Technology Systems (Asia), Venetian Macau Resort Hotel

[63] Hartel, C. E. J., Smith, K., & Prince, C. (1991, April). Defining aircrew coordination: Searching mishaps for meaning. Paper presented at the 6th International Symposium on Aviation Psychology, USA.

Situation awareness typically comprises of three elements:

- Perception of elements in current situation
- Comprehension of current situation
- Projection of future status

The perception of elements in the current situation is partially informed by the available CCTV and other sensory information from the site. Operators can use the cameras to observe the environment and activities in order to understand the situation. This "visual" situational awareness can be better facilitated by having the right infrastructure for example having adequate camera coverage and high enough resolution for zooming into the image, which can easily be facilitated by megapixel camera technology.

Comprehension of the current situation, currently done by individuals, can be augmented through the use of advanced displays (i.e. advanced presentation using 2D and 3D maps) to put the scene into context, and also advanced analytics to provide a potential hypothesis on the issue.

In a team situation, team situational awareness can be defined as "the degree to which every team member possesses the situational awareness required for his or her responsibilities"[64]. The success or failure of a team depends on the success or failure of each of its team members. If any one of the team members has poor situational awareness, it can lead to a critical error in performance that can undermine the success of the entire team. This is particularly applicable to Customs in an emergency response situation where Customs would have to coordinate with other State and Federal agencies to address the issue. Being able to share CCTV, sensory and analytic information through an IP network infrastructure can go a long way to establishing some common perception of the elements and comprehension of the situation to enable a faster, more coordinated and more unified response.

RELEASED UNDER THE FOI ACT 1982

[64] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32-64.

5.8 Evaluation – Performance Metrics and ROI Measures

The UK is far more advanced than Australia in the uptake and utilisation of CCTV in many areas. What is quite remarkable when discussing CCTV technologies with UK Police and the National Policing Improvement Agency (NPIA) in recent communication[65] is how well they model the costs and benefits of CCTV related activities. For example, DCC Graeme Gerrard of the Cheshire Constabulary was able to say that a basic investigation using CCTV would cost GBP1200. The Home Office was able to say that the cost of an illegal immigrant getting off a plane at Heathrow, destroying their documents, and claiming asylum status was GBP40,000 — they require a technology to rapidly determine which plane the passenger arrived on. In India, the Head of Security of Reliance Petroleum, largest private company in India, has associated costs with every security incident intercepted by CCTV and he can demonstrate to management that the investment in CCTV is actually a source of cash and not a sink. In Australia, the Port of Brisbane was able to say that since the introduction of CCTV, the cost of pilferage has reduced from AUD3 million per annum to just AUD1 million per annum.

Such statistics and facts are very persuasive when it comes to arguing for budget allocations for improved CCTV and for building the business case for change. However collecting the statistical data and reporting in general can be very time consuming using manual methods. The advent of IP surveillance system offers the opportunity to automatically log and gather such performance statistics.

Such technology has been used to great advantage by a private guarding company in Singapore[66] which looks after the security of the Mass Rapid Transit system as well as prisons. They automate the reporting of many of the security tasks. By tightly binding CCTV operation with the security guards using technologies such as visual alarms on CCTV, RFID, GPS, and direct mobile communications to security guards they have been able to reduce the number of guards and CCTV operators by 80% while achieving higher levels of effectiveness. The system automatically collects statistics and reports on incidents intercepted which helps demonstrate the effectiveness of the guarding service.

Another interesting trend to note is the privatisation of the security services for government-owned services in Singapore such as transport and prisons. This private guarding service has a central CCTV monitoring facility and monitors all remote sites via broadband internet connections.

RELEASED UNDER THE FOI ACT 1982

[65] Personal Communication, Abbas Bigdeli, May, 2009.

[66] OneBerry Corporate Site. 2009.

6 The CCTV Future

The advent of digital CCTV networks has created opportunities for an increased return on CCTV investment, both in terms of ***reduced costs and higher performance***. Gains in video quantity and quality will provide significantly more useful information; remote monitoring options will provide more flexibility and assistance for local staff; whilst economies of scale will flow from using common off-the-shelf IT equipment. Nevertheless realizing these opportunities may demand greater levels of planning and expertise than was needed in simpler systems of the past. Graphical planning tools will assist in deploying CCTV resources according to risk analysis.

Future CCTV systems will be marked by the ***'information anywhere'*** paradigm. This will see video delivered to users wherever their workplace is, such as their desktop PC or roaming mobile phone or remote monitoring centre in another city. The internet protocol (IP) which facilitates this paradigm shift is likely to dominate for years to come and promises far greater and more convenient access to both CCTV and other related information from non-CCTV systems. For example, textual, graphical or audio information from 3rd party systems can be presented to CCTV users to provide greater context thus resulting in a ***more holistic approach to business solutions***. Ethernet networks transporting IP data can easily incorporate data security and redundancy measures, providing more resilient CCTV services.

While high definition video continues to be 'data hungry' despite advances in video compression, on-demand-only video streaming with on-site storage can help alleviate bandwidth. Also, reductions in computing and telecommunication costs, helped by the National Broadband Network initiative, will further ***support flexible information delivery***. We therefore recommend that IP communications should therefore underpin all Customs CCTV design decisions.

Whilst the CCTV industry is embracing digital capture, transmission and display, there remain compatibility problems between competing manufacturers of related products. Various standards are being developed to standardize video data compression and control protocols. CCTV systems that subscribe to such standards will allow a ***greater choice of CCTV cameras*** and probably ***lower the total cost of CCTV ownership***. This shift will have a major impact on the industry that is still dominated by proprietary CCTV hardware manufacturers. It is recommended that Customs keep a 'watching brief' on this issue to take advantage of ***open standards*** as they become available.

Many organizations within Customs seaport and airport environments have a similar need for visual information and are implementing their own CCTV systems. Occasionally the needs of Customs and other CCTV operators overlap which presents opportunities to ***share services*** and ***increase returns on investment***. Technology today, namely IP communications, is capable of facilitating these shared information flow, but ongoing legislative and relationship development is needed. Consultation can occur in the interim to best position Customs for future sharing; this extends to systems and business requirements.

RELEASED UNDER THE FOI ACT 1982

Video analytics adds value to visual information and will be increasingly important feature in future CCTV systems. ***Real time alerts and correlated intelligence*** again increase the return on CCTV investment by providing a greater likelihood that useable information is being analyzed by CCTV user resources in the ***most efficient way***. Video analytical tools is an expanding industry and there is scope for Customs to trial 'off the shelf' solutions or commission made to order applications. The benefits offered by facial recognition technology are significant and will continue to drive research and development investment in this area.

Further adoption of software based CCTV 'video management systems' is expected. These systems epitomize the open standards approach where research is directed at enhancing the CCTV user interface but is hardware 'agnostic'. This gives rise to frequent design iterations that incorporate many of the features highlighted above.

In conclusion, digital CCTV surveillance systems based on IP networking infrastructure are the way of the future. Not only does the investment for system migration result in lower costs and improved performance in the long-term, it will also allow Customs to maintain its standard of operational performance on par with the rest of the world.

RELEASED UNDER
THE FOI ACT 1982