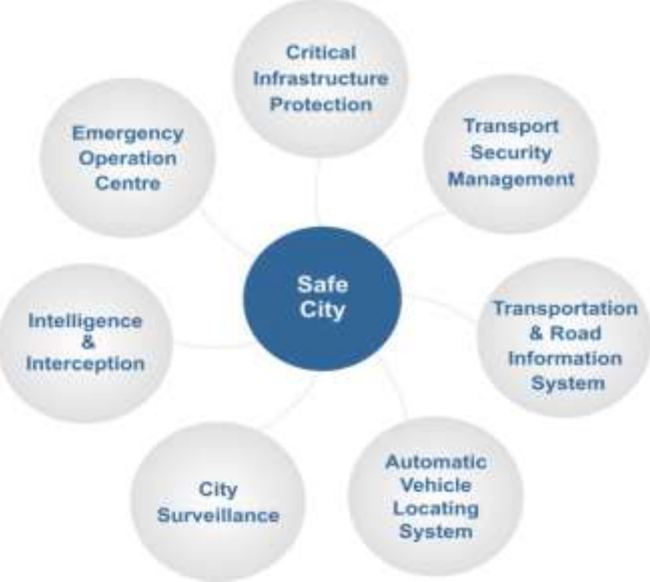
2015

Safe City Video Surveillance Technologies


Critical Infrastructure Protection
Emergency Operation Centre
Transport Security Management
Safe City
Intelligence & Interception
Transportation & Road Information System
City Surveillance
Automatic Vehicle Locating System

Homeland Security Research Corp.

Safe City Video Surveillance Technologies

August 2015

***Homeland Security Research Corp. (HSRC)** is an international market and technology research firm specializing in the Homeland Security (HLS) & Public Safety (PS) Industry. HSRC provides premium market reports on present and emerging technologies and industry expertise, enabling global clients to gain time-critical insight into business opportunities. HSRC's clients include U.S. Congress, DHS, U.S. Army, U.S. Navy, NATO, DOD, DOT, GAO, and EU, among others; as well as HLS & PS government agencies in Japan, Korea, Taiwan, Israel, Canada, UK, Germany, Australia, Sweden, Finland, Singapore. With over 750 private sector clients (72% repeat customers), including major defense and security contractors, and Fortune 500 companies. HSRC earned the reputation as the industry's Gold Standard for HLS & PS market reports.*

Washington D.C. 20004, 601 Pennsylvania Ave., NW Suite 900,
Tel: 202-455-0966, info@hsrc.biz, www.homelandsecurityresearch.com

Table of Contents

List of Figures

1 Safe City Video Surveillance Technologies

1.1 Introduction

Safe cities, law enforcement and private enterprises are all utilizing Video Surveillance Technologies to conduct security, commercial and transportation related tasks. Their greatest cost and limitation in taking fuller advantage of the wealth of captured images is the manpower required to decipher what is significant or of interest out of terabytes of images.

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

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

Video Surveillance technology appears indispensable for monitoring operations and managing security incidents in a safe city environment. It is also an irreplaceable investigation tool for solving crimes, misdemeanors and disputes. However, it is not yet truly proven that video surveillance prevents security incidents or lowers crime rates.

A Video Surveillance network is a video system that transmits images in a closed loop. Once only analogue, CCTV networks now include digital Video Surveillance Cameras and support components. Access to the communication network can be gained by internet in certain cases. Only users with access rights to the network can access the information provided by the cameras.

The following constitutes the security activities of safe city Video Surveillance Cameras network:

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

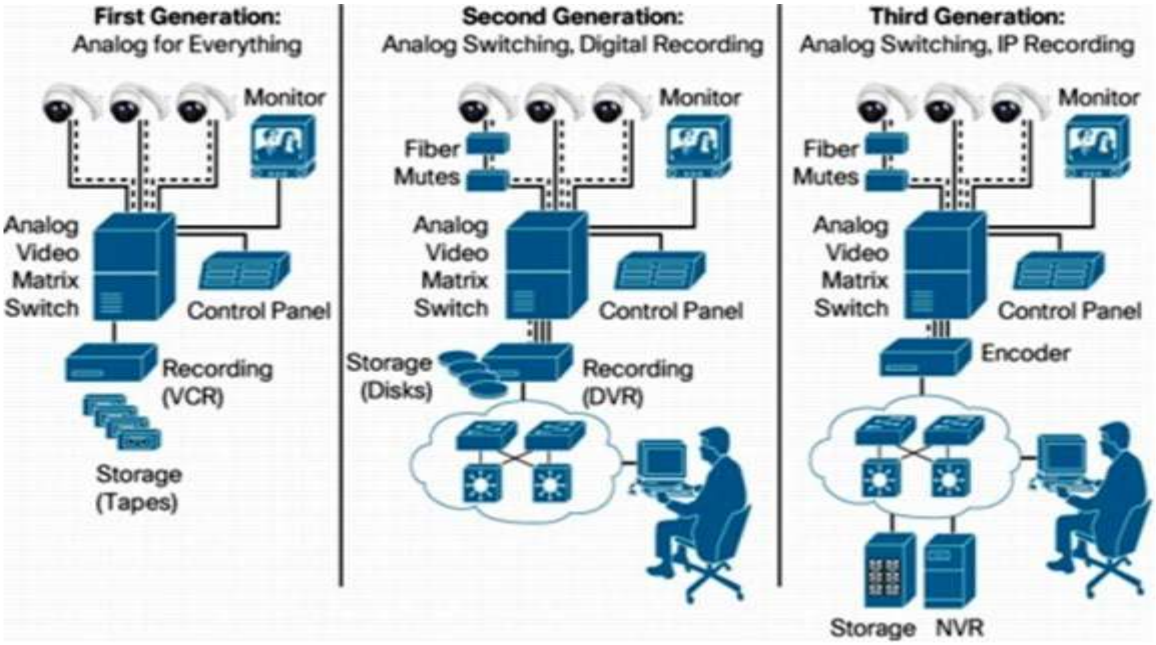
There are three types of video surveillance:

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

1.2 Video Surveillance Evolution

Various video technologies have been so compelling in their ability to solve significant video surveillance user challenges such that this field has begun to evolve, catching up with many other systems and applications.

Figure 1 - Video Surveillance Evolution

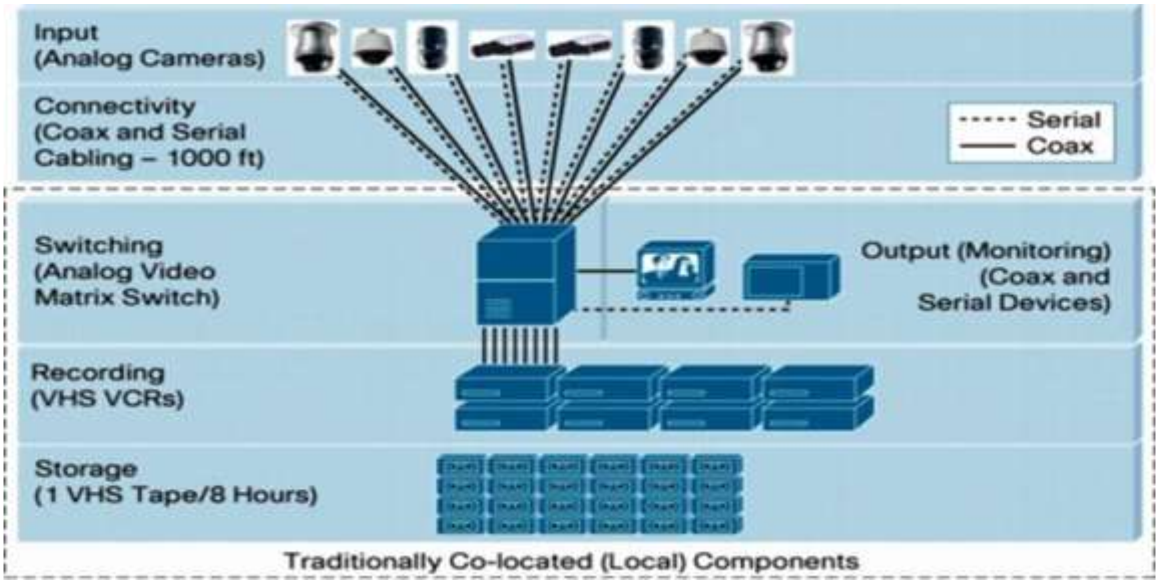


(**Source:** Cisco)

1.2.1 Analog Video Surveillance

Analog video surveillance cameras are controlled and transmitted video in an analog format. These video streams are aggregated, switched, and dispersed to monitoring displays using analog matrix switching technology. The matrix switch also provides the video stream to analog VCRs for recording purposes.

Figure 2 - Analog Video Surveillance System



(**Source:** Cisco)

While these analog devices provide basic monitoring and recording capabilities, they do have several operational drawbacks. VCR-based recording does not facilitate simultaneous recording and playback of video; separate record and playback (review) components are required in order to record video during the investigation process. Moreover, the recording process is prone to human error: replacing blank media or ensuring that recording was activated, for example. From a reliability and system availability perspective, any failure of the recording system can go undetected for an extended period.

Storage and access are also other issues. Because videos can be required for future investigation, tapes must be manually stored and indexed unless used in a jukebox type VCR device. These consume a significant amount of size and power, and generate quite a bit of heat.

The viewing of live or recorded video is limited to specific operations and investigation centers. To review recorded video from a remote location requires the appropriate tape to be located and sent to the investigation center. In virtually all cases, video surveillance system operations are based on proprietary signaling and format protocols; best-in-class multi-vendor component interoperability is not an option for video surveillance customers without extensive and costly customization.

Analog Video Surveillance System is characterized by:

- Monitoring: Viewing live video. Operators select the desired video feed and specify where the video is to be displayed. For larger installations, a special-purpose keyboard controls which camera video feed is displayed over a RS-232 connection that sends vendor- specific or proprietary commands to the matrix switch. The requested video stream is delivered to the monitor over a coaxial connection that supports the analog (NTSC/PAL) video signal. Unlike a typical PC keyboard, the layout and operation of the video surveillance keyboard is specific to the video surveillance market. This special-purpose keyboard references cameras by simple numbering schemes (01 = camera 1, 104 = camera 104, etc.). In some installations, PCs can be used instead of special-purpose keyboards and displays but many operators prefer the special purpose monitoring stations and keyboard/joystick controls.
- Recording: Independent from monitoring functions, recording has been historically accomplished using videocassette recorders (VCRs) or more recently, digital video recorders (DVRs).
- Storage: Based upon regulatory and other organization requirements, recorded video may be archived for a few days, weeks, or months. This facilitates the investigation of events that may have occurred or need to be correlated with other events.

Most manufacturers of cameras, fiber-optic transmission equipment, matrix switches, and monitoring keyboards have their own proprietary communications protocols and languages to interconnect these systems. This approach has locked the customer into a single-vendor solution, increasing equipment costs and decreasing the customer's ability to pick best-in-class solutions.

1.2.2 Second-Generation Analog Video Surveillance

Second-generation Video Surveillance systems are also based on analog camera (input), fiber or coaxial connectivity, with video switching provided by an analog video matrix switch. However, recording functions are enhanced.

Second-generation systems primarily focus on addressing recording and storage problems. DVRs replace analog VCRs. DVRs convert the analog video feeds into a digital format and save the resulting digitized video on internal hard disk drives or on locally direct attached storage (for example, digital tapes, disk drives, or DVDs). Thus, many manual efforts associated with VCRs are eliminated or reduced in frequency. Additionally, the DVR's internal database reduces video retrieval time during investigations.

While DVRs offer longer operation life than VCRs, they can pose recording system availability problems. In the event of a DVR failure, the DVR has to be replaced, generally resulting in a loss of video unless an N+1 redundancy system was offered. Some DVRs use personal computer operating systems which can be subject to tampering and virus propagation; thus, DVRs should be included in a prophylactic maintenance program with regular virus protection and security mechanism configuration. Moreover, since many DVRs tie the software-based video stream/storage management value into a hardware specific platform, a generic server/storage device with a considerably lower price may not be available.

Frequently, the DVR software is accessed and controlled by a vendor-specific user interface often running as a set of administrator and operator applications on a personal computer (PC). As such, second-generation DVRs frequently require a PC viewing client. The use of client software offers some trade-offs; it can limit access to recorded video on a local basis which may be desirable, but it also can impose problems in emergency situations where remote viewing over an IP network may be helpful.

Some DVRs can be accessed via a network-connected PC to further reduce the time associated with video archiving and retrieval. On-demand access to archived video accelerates evidence review and improves evidence control. It also saves time and effort; investigators do not have to travel to other facilities to perform investigations. To preserve remote-location WAN bandwidth, the video can be pulled over the network on an on-demand basis.

1.2.3 Third-Generation Video Surveillance

As with first- and second-generation video surveillance deployments, third-generation deployments are primarily based on analog cameras, fiber or coaxial connectivity, and video switching is provided by an analog video matrix switch. However, accessibility of live and recorded video is enhanced.

As observed, second-generation DVRs typically require video to be viewed by PC which affects video surveillance operator efficiency. Some vendors offer IP-to-analog video gateway decoders (IP gateway decoders) as part of a third-generation video surveillance solution that allows operators to view recorded video from their analog monitoring stations. By using familiar video surveillance PTZ joystick controls, operators can select the video associated with a specific camera, rewind the video, and review it over analog monitors. This enables faster response and investigation of events, eliminating the need for a PC and the associated delay. Moreover, in multi-display environments, the operator can continue to monitor other camera videos while investigating a recorded event.

Many third-generation systems frequently unbundle the DVR; discrete encoders or high-density, rack-mountable, chassis-based encoders provide the conversion from analog to digital and use the network to a greater extent. Thus, recording becomes a separate function from video digital encoding.

Encoders serve as analog-to-IP gateways and as a connection point to the network. The IP network transports the video streams to monitoring and recording locations. Encoders digitize analog video; typically, they compress the digital video using various compression algorithms, including the same ones used for production-quality motion picture DVDs, and transmit the compressed digital video over a frame-based (Ethernet) or packet-based (IP) network.

Some encoders provide additional features that allow them to operate with a wide variety of analog cameras. This gives video surveillance operators more control over their analog vendor camera selection process by offering a greater degree of multi-vendor keyboard/camera interoperability. This aspect becomes even more important when PTZ cameras are used, many of which have proprietary camera control signaling.

Encoders can also be differentiated by the latency induced by the digitization and compression algorithm implementation. The lowest-latency, high-video-quality encoders generally have less than 0.2 Sec. of latency. A lag of more than 0.2 Sec can be problematic for video surveillance operators using PTZ cameras-they commonly overshoot the intended item to monitor (zoom in too far or pass the given object).

Another benefit from unbundling the DVR and using encoders is that the recording (stream and storage management) function, sometimes referred to as a network video recorder (NVR), can be fully independent of storage. The NVR can be located anywhere on the network, often in the data center with other server systems. Moreover, the NVR software can run on lower-cost, commercially off the shelf (COTS) servers.

In first- and second-generation deployments, surveillance cameras must be within 1000 feet of the recording device when connecting over coaxial, or require fiber connections for longer distances. Now that encoding occurs in a separate device, the NVR can be located anywhere on the network-at an organization's headquarters for example, or using servers in two data centers-to simplify management and increase availability. Physically separating the encoding device from the server has another advantage as well: the server no longer needs to devote compute cycles to managing video cards and compression.

Many organizations have resorted to maintaining a separate database for each remote DVR. However, when using NVRs that can be deployed anywhere on the network, it is possible to centralize the closed circuit television or CCTV database into fewer distinct geographic database environments that can be replicated back to the organization's central safety and security operations center. This partitioning and semi-centralization of databases further simplifies video surveillance system management and reduces equipment costs.

This partitioning of system functions also helps improve operational efficiency. An organization's IT group can be tasked with the responsibility of maintaining the video surveillance servers and storage as well as protecting them along with other mission-critical servers. This allows security personnel to focus on security issues and not maintenance of storage devices. As a result, it is possible to reduce not only redundant capital infrastructure investment by using the network for transport and access of the video, but also optimize operational roles and responsibilities.

It should be recognized that this model of separate but complementary functional responsibilities is quite common in most organizations today. For example, human resources are responsible for personnel issues, yet use the power and flexibility of the IT-supported network to run networked human resource applications. The same is true of other mission-critical and business-sensitive applications including finance, engineering development, and sales. The organization's IT group ensures that edge devices are properly connected to the network, servers are properly maintained (including virus protection), and provides constant monitoring of these networked assets. Moreover, IT works with these user groups to ensure appropriate security policies are in place to provide appropriate access to restricted resources.

NVR deployments offer several other advantages compared to second-generation deployments using DVRs. Recording and storage component availability is further increased-the failure of a storage device can be almost instantly remedied by having the NVR direct the video stream to another network-connected server or storage device. The use of superior long life (higher MTBF) storage devices also helps increase video surveillance system availability.

As mentioned, NVRs offer both video stream management and video stream storage management. Storage management can be an important factor for users with high 24-hour "record everything" storage requirements. NVRs that can prune stored video based on motion or other criteria (i.e. first in first out) can further minimize regular maintenance tasks and potentially reduce the amount of storage needed to meet long-term retention requirements.

The ability for the NVR to ingest IP video also enables IP camera video to be recorded in addition to the video coming from analog video encoders. It should be recognized that IP cameras offer several advantages to analog cameras / and analog encoders. These benefits include:

- Compact, single video capture form factor (as compared to an analog camera plus an encoder)
- No separate power source required when Power over Ethernet is provided by the IP network switch, which in many cases has battery back-up in the event of a power failure
- Ease of deployment using wireless LAN technology

- Lower cost deployment using Category 5 structured cabling

One cautionary note: many current video surveillance component and system vendor "network-connected" products tunnel their proprietary communications over Ethernet to maintain a strong, single vendor-lock on customer deployments. These components cannot harness the intelligence or true interoperability of the standards-based IP network infrastructure.

Collapsing video switching functions onto an existing Ethernet switched environment further reduces the complexity and lowers the cost of deploying video surveillance. It also provides video surveillance system owners with the flexibility to design solutions tailored to their unique requirements. Furthermore, as part of an open network, operators can create policies allowing the inherent value of the video as a source of information to be used by other safety and security applications, as well as other non-traditional business applications.

1.2.4 Digital Video Surveillance

- ❑ Safe cities digital Video Surveillance is based to-date on digital CMOS cameras. These cameras do not require a video capture card because they work using a digital signal which can be saved directly to computers. The signal of digital surveillance cameras is compressed.
- ❑ Multi-megapixel IP-CCTV digital cameras are coming on the market. Though quite expensive, they can capture video images at resolutions of 1, 2, 3, 5 or up to 16 Mega pixels. Unlike analog cameras, details such as number plates are easily readable. At 11 Mega pixels, forensic quality images are made where each hand on a person can be distinguished. Because of the much higher resolutions available with these types of cameras, they can be set up to cover a wide area where normally several analog cameras would have been needed.

1.2.5 IP Surveillance Cameras

- ❑ IP cameras are so called network cameras because rather than using an analog cable to send the video down; they function with a network cable as well. This saves installation money and time.
- ❑ IP cameras can just use existing cable infrastructure. Wireless IP cameras make it easier to install surveillance security equipment.
- ❑ Most IP cameras offer a very high quality of the images due to the mega pixel resolutions; therefore, they can produce video resolutions in a HD quality. Compared to regular video surveillance security equipment, the quality of the images is highly increased. By using the Power over Ethernet (PoE) recent technology, a network camera can easily be remotely powered, making the installation simpler and faster. Recording the video from an IP camera is done using a network video recorder

(NVR). There are plenty available on the market. Some network cameras though come with their own software.

- ❑ IP Network Centric Video Surveillance systems provide additional benefits and advantages over preceding generations (See figure below) It expands and extends the capability of video surveillance gateways (enhanced encoders and decoders) and the NVR, which allows the matrix switch to be replaced by standard and typically lower-cost Ethernet switching platforms.

- ❑ When used with PCs for monitoring and reviewing video, some NVRs offer matrix switch-like functions, allowing the matrix switch to be eliminated. The switching is provided by the network infrastructure with the video stream management provided by the NVR. Without the matrix switch, encoders can be either centralized in multiport configurations to support home-run cabling schemes or located closer to the camera. By situating the encoder closer to the camera, the encoder can use the pervasive IP network cabling infrastructure, further reducing the cost of redundant cabling infrastructures.

1.2.6 IP-Based Video Surveillance Systems

- ❑ IP-Based video surveillance systems is a type of digital video surveillance system which unlike analog closed circuit television (CCTV) cameras can send and receive data via a computer network and the internet. The term "IP camera" or "netcam" is usually applied only to those used for surveillance.

- ❑ There are two kinds of IP cameras:
  - ▪ Centralized IP cameras, which require a central Network Video Recorder (NVR) to handle the recording, video and alarm management.
  - ▪ Decentralized IP cameras, which do not require a central Network Video Recorder (NVR), as the cameras have recording functionality built-in and can thus record directly to digital storage media, such as flash drives, hard disk drives or network attached storage.

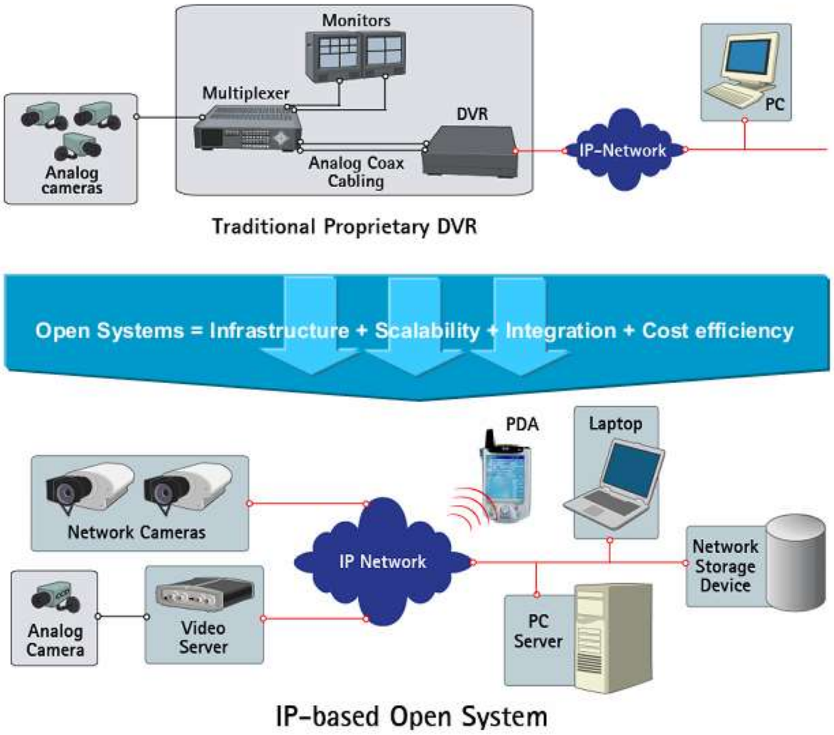
- ❑ IP cameras are available in resolutions from 0.3 (i.e. VGA) to 20 megapixels. As in the consumer TV business, in the early 21st century, there has been a shift towards high-definition video resolutions.

- ❑ In order to address issues of standardization of IP video surveillance, two industry groups have been formed, the Open Network Video Interface Forum and the Physical Security Interoperability Alliance (PSIA). While the PSIA was founded by 20 member companies including Honeywell, GE Security and Cisco, ONVIF was founded by Axis Communications, Bosch and Sony. Each group now has numerous member companies.

❑ Advantages of IP-Based video surveillance systems include the following:

- Higher image resolution: IP cameras have a resolution of at least 640x480 and can provide multi-megapixel resolution and HDTV image quality at 30 frames per second.
- Flexibility: IP cameras can be moved around anywhere on an IP network (including wireless).
- Distributed intelligence: with IP cameras, video analytics can be placed in the camera itself allowing scalability in analytics solutions.
- Transmission of commands for PTZ cameras via a single network cable.
- Encryption & authentication: IP cameras offer secure data transmission through encryption and authentication methods such as WEP, WPA, WPA2, TKIP, AES.
- Remote accessibility: live video from selected cameras can be viewed from any computer anywhere, and also from many mobile smartphones and other devices.
- IP cameras are able to function on a wireless network. Initial configuration has to be done through a router. After the IP camera is installed, it can then be used on the wireless network. These cameras are used for navigation purposes by defense forces.
- PoE - Power over Ethernet. Modern IP cameras have the ability to operate without an additional power supply. They can work with the PoE-protocol which gives power via the Ethernet-cable.

Figure 3 - Traditional vs. IP-Based Video Surveillance Systems



More information can be found at:

Global Safe City: Industry, Technologies & Market – 2015-2020