Czech University of Life Sciences Prague

Faculty of Economics and Management
Informatics
Department of Information Technologies

Diploma Thesis

Network video surveillance system for a company

Author: Sergey Golovunin
Supervisor: Ing. Miloš Ulman, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Department of Information Technologies

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Golovunin Sergey

Informatics

Thesis title

Network video surveillance system for a company

Objectives of thesis

The goal of this project is to design an implementation of network security system for a company.
Partial goals are:
- to analyse current state of video surveillance systems,
- to compare possible technical solutions, and
- to identify obstacles and propose solutions for network security systems.

Methodology

Security is a top priority for many companies and organizations. Secondary research of the thesis is based on study and analysis of specialized information resources. Own research is based on application of network hardware and software tools and resources to successfully deploy IP video surveillance on complex networks. On the basis of theoretical knowledge and analysis of information resources, conclusions and recommendations of the thesis will be formulated.

Schedule for processing

1) Preparation and study of specialized information resources, refinement of partial goals and selection of work process: 8/2012
2) Processing of literature overview according to information resources: 9/2012-10/2012
3) Elaboration of the analytical, discussion and evaluation of results: 11/2012- 12/2012
4) Creation of the final document of the diploma thesis: 12/2012- 2/2013
5) Submission of thesis and abstract: 3/2013

The proposed extent of the thesis

60-80 pages

Keywords

Network video surveillance, Cisco, security system, IP camera.

Recommended information sources

A.S., Tanenbaum. 2010. Computer Networks. Fifth Edition. New Jersey 07458 : Pearson Education, Inc. Publishing as Prentice Hall PTR Upper Saddle River, 2010.

Luigi Di Stefano, Carlo Regazzoni, and Dan Schonfeld. 2011. Advanced Video-Based Surveillance. s.l. : Hindawi Publishing Corporation, 2011.

Robert T. Collins, Alan J. Lipton, Takeo Kanade, Hironobu Fujiyoshi, David Duggins, Yanghai Tsin, David Tolliver, Nobuyoshi Enomoto, Osamu Hasegawa, Peter Burt1 and Lambert Wixson1. 2000. A System for Video Surveillance and Monitoring. s.l. : Carnegie Mellon University, 2000.

Wei Niu, Jiao Long, Dan Han, and Yuan-Fang Wang. Human Activity Detection and Recognition for Video Surveillance. Santa Barbara, CA 93106 : Department of Computer Science University of California.

The Diploma Thesis Supervisor

Ulman Miloš, Ing., Ph.D.

Last date for the submission

March 2013

doc. Ing. Zdeněk Havlíček, CSc.
Head of the Department

prof. Ing. Jan Hron, DrSc., dr.h.c.
Dean

Prague January 15, 2013

Declaration

I declare that I have worked on my diploma thesis, titled “Network video surveillance system for a company" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any third person.

In Prague on _____________ ____________________

Sergey Golovunin

Acknowledgement

I would like to express my gratitude to Ing Miloš Ulman, Ph.D. for his constructive advices, supervision of this diploma thesis, and actual proposal of its name, which eventually turned out to be much more fitting than I had been able to imagine one year ago.

Many thanks also deserve my entire family, for creating supportive environment, which is the crucial determinant of any successful work.

Network video surveillance system
for a company

Síťový kamerový systém
ve firmé

Summary

Nowadays, security is a top priority for many companies and organizations. One of important components of security is video surveillance system. The properly chosen solution can increase the security of the company and to prevent unwanted threats.

The goals of the diploma thesis are the choice efficiently solution and the implementation of design of the network video surveillance security system for a company. In literature review will be summarized information about parts and principles solutions for video surveillance. In practical part author compares possible technical solutions and approaches from different companies in design video surveillance. The solution for the company will be evaluated based on Multiple Criteria Analysis. Scheme of video surveillance system will be implemented on video surveillance solution from Cisco. Conclusion will contain identification of obstacles and proposition effective solutions for network security systems.

Key words

Network video surveillance, Cisco, security system, IP camera.

Shrnuti

V současné době je bezpečnost nejvyšší prioritou pro mnoho firem a organizací. Jedním z důležitých prvků bezpečnosti je kamerový systém. Řádně zvolené řešení může zvýšit bezpečnost společnosti a aby se zabránilo nežádoucím hrozbám.

Cíle diplomové práce jsou výběr efektivního řešení a realizace návrhu sítě sledovacího video bezpečnostního systému pro společnost. V přehledu literatury budou shrnuty informace o částech a principy řešení pro video sledování. V praktické části autor srovnává možná technická řešení a přístupy z různých společností z pohledu návrhu video sledování. Řešení pro společnost budou hodnoceny na základě více kriteriální analýzy. Schéma kamerového systému bude realizováno na základě řešení kamerového dohledu od společnosti Cisco. Závěr bude obsahovat identifikace překážek a propozice účinných řešení pro systémy týkající se zabezpečení sítě.

Klíčová slova

Síťové video dohled, Cisco, bezpečnostní systém, IP kamera.

Contents

1. Introduction

Video surveillance is a rapidly growing industry. Driven by low-hardware cost, heightened security fears and increased capabilities; video surveillance equipment is being deployed ever more widely, and with ever greater storage and ability for recall. (1) In nowadays, video surveillance is a key component of the safety and security of many organizations, providing real-time monitoring of the environment, people and assets, and providing recording for investigation purposes. Modern public video surveillance systems consist of networks of linked cameras spread over vast portions of public space (2). They can be installed anywhere and everywhere like banks, casinos, offices, airports, government buildings and other locations which need vital protection. These cameras can be equipped with technologies like high resolution, motion detection, infrared vision, and biometric identification. Surveillance video is used in two key modes, watching for known threats in real-time and searching for events of interest after the fact.

IP video surveillance is a term for a security system that gives users the ability to monitor and record video and/or audio over an IP (Internet Protocol-based) computer network such as a local area network (LAN) or the Internet. In broad terms, advanced video-based surveillance could be described as intelligent video processing designed to assist security personnel by providing reliable real-time alerts and to support efficient video analysis for forensics investigations (3). Every video surveillance system consists of cameras, video management software, servers, and storage. The time between 2007 and 2010 represents a market transition in the industry where sales of IP-based components began out-selling analog-based systems. While analog systems have a cost advantage in small deployments (sixteen cameras or less), for larger number of cameras are deployed, IP-based systems may be more cost-effective initially and have a lower ongoing total cost of ownership. IP-based video surveillance systems, especially the end-node (the IP camera), have several operational and technological advantages (4). There are essential differences between the digital video surveillance and the analog video surveillance at the aspects of signal transmission, control and storage. Digital video surveillance is an innovation in the security field, and it exceeds the analog video surveillance at the aspects of long distance transmission engineering wiring operation maintenance and flexible application (5).

Many of the advantages of implementing IP video surveillance are similar to those of VoIP adoption. The reason of using the IP for voice and data transmission is the cost saving. By using existing IP network for video surveillance the separate cables for video and voice can be eliminated. Also can be eliminated the cabling for electrical power by using PoE. While power to some camera deployments continue to be a requirement (PTZ—Pan-Tilt-Zoom housings, wireless cameras and cameras that require fiber connectivity due to distance), PoE is a significant cost savings. IP video surveillance cameras, once connected to the network, may be remotely managed and configured. The technicians who install the camera must have a laptop to focus the lens and adjust the viewpoint of the one, but following this initial installation, the camera configuration may be completed by a technician in a central, rather than local, facility.

2. Thesis objective and methodology

2.1 Objectives

This diploma thesis is focused on analyze approaches and choices components and solutions for video surveillance system. There are two objectives of this thesis. The first one is to present the state of the video surveillance system. This part will be contains the basic information and definitions of important terms about types and components of video surveillance system. Video surveillance system is part of security and has to be described in security policy of each company. Meaning and content of security policy company will be briefly describes in first part of diploma thesis.

The objective of second part, the part of author's own research, is compare video surveillance solutions from different companies. The author has chosen companies that offer a complex solution in video surveillance. Different solutions will be considered from point of requirement the company that has a need to integrate three independent surveillance locations into reliable network within existing corporative network. And next objective is to present common principle of implementation and possible solution video surveillance system for a company based on Cisco solution.

Partial goals diploma thesis are:

- Analyze of current state and market of video surveillance system,
- Comparison and evaluation of possible technical solutions and approaches different companies in design video surveillance,
- Identification of obstacles and proposition effective solutions for network security systems.

2.2 Methodology

All information and data in diploma thesis are from literature, magazines and internet resources. Methodology of the thesis is based on analysis of available information resources and knowledge bases.

Own research is based on application of network hardware and software tools and resources to successfully deploy IP video surveillance on complex networks. First step was to find up all the possible information about components of video surveillance system and principles designing such systems. Next step was to gathering information about companies that offer IP video surveillance solution and analyzing approaches of deploying video surveillance. Optimal solution for company was found by using Multiple Criteria Analysis. Design IP video surveillance system for the company based on Cisco solution is shown at the end of diploma thesis. The recommendation will be given to solve issues and restrictions for selected solution.

3 Literature review

3.1 Security policy

Each company faces the threats and vulnerabilities. That is why company must consider what has to be done to improve the physical and IT security of organization. For this aim should be created security policy. It is a document that provides high level and specific guidelines on how company carry out protection, but will not specify exactly how that is to be accomplished. Security policy is considered as “living document”. It means that the document is never finished and has to be continuously updated as employee requirements and technology change. A security policy is independent from vendor and technology. Company can implement the policy in any manner that accomplishes the special goals.

A security policy has to be written in manner that its content could be understood by target audience which should be clearly identified in the document. A security policy should not have the place for misunderstanding.

Video surveillance policy has to be part of security policy of company. The Video Surveillance Policy has to provide detailed direction concerning the context, procedures and protocols within which the company installs and operates surveillance cameras. Goal of this document is to ensure that the company balances the security, safety and other benefits derived from the use of video surveillance with the privacy rights of the individual. The Video Surveillance Policy provides detailed direction concerning the context, procedures and protocols within which the company installs and operates surveillance cameras.

Text below is a template of Video surveillance policy based on Brock University Video Surveillance and Recording for Safety and Security Policy (original document’s link: *http://brocku.ca/webfm_send/14790*).

Video Surveillance and Recording for Safety and Security Policy

Category:
Responsibility:
Approval:
Approval Date:
Issue Date:
Next Review:

1. INTRODUCTION

This policy is to provide guidance in the responsible use of video surveillance and recording on company premises for the purpose of safety and security of the *"COMPANY NAME"* and its visitors. *"COMPANY NAME"* is committed to enhancing the company quality of life by integrating the best practices of safety and security with the responsible use of technology.

2. OBJECTIVES

The principal objectives of video surveillance and recording include:

- Video surveillance and recording coverage twenty-four hours a day each day of the year throughout the interior and exterior of the company in several public and key areas.
- Enhancing safety and security.
- Preventing/deterring crime and public disorder.
- Reducing and removing the fear of crime.
- Identifying criminal activity.
- Identifying suspects.
- Gathering evidence.

- Reducing the cost and impact of crime to the university community.

- Endeavoring to use the least intrusive video surveillance and recording which will still fulfill this policy’s requirements.

- Improving the allocation and deployment of Company Security Services’ enforcement assets.

3. APPLICATION

This Video Surveillance and Recording for Safety and Security Policy applies to video surveillance and recordings administered by Company Security Services. It does not apply to video recordings gathered in other circumstances, for example, as part of recordings for an approved research initiative. To ensure such other collections are performed in compliance with applicable privacy law, reference should be made to the “Related Policies” at the end of this document.

4. ROLES AND RESPONSIBILITIES OF COMPANY SECURITY SERVICES:

- Responsible for video surveillance and recording for safety and security purposes.

- May disclose information, including any surveillance camera recordings with domestic law enforcement agencies within country (e.g., municipal, regional, provincial or federal police) as required for the purposes of the investigation of an offence. The exchange will be facilitated through Company Security Services to ensure continuity in the event the recording becomes evidence in a judicial proceeding.

- In conjunction with Telecommunications and Network Services, will be responsible for recording all monitored activity and the secure storage of data recordings.

• Will be responsible for ensuring appropriate signage about the existence of video surveillance and recording cameras at *“COMPANY NAME”*.

• Will conduct an operational audit yearly to assess compliance with these guidelines, including an ongoing assessment of the involvement and support of the university community.

5. PROCEDURES:

A) Confidentiality:

1. Video surveillance and recordings of university premises shall be conducted in a professional, ethical and legal manner, in accordance with the Freedom of Information and Protection of Privacy Act, and any other relevant legislation.

2. Collection of video data must be accompanied by signage placed at accessible locations which provides faculty, staff, students and members of the public with advance notice that their images may be collected. This may include facility or public space entrances. Notices should provide as follows: This area is being video recorded for safety and security purposes. The personal information is collected under the authority of the *“COMPANY NAME” Act*.

3. Video surveillance and recording for the purpose of monitoring work areas and social areas should only occur in special circumstances, and this surveillance and recording will further the policy’s principle objectives, which include the prevention/deterrence of illegal activity and the enhancement of safety.

4. Video surveillance and recording cameras shall not be directed through windows of a residential dwelling (including a university residence), or any non-university location where an individual has a reasonable expectation of privacy.

5. Only personnel authorized by Company Security Services can view video surveillance recordings, either “real time” or recorded.

6. Copies of recordings shall only be made for investigative and/or evidence purposes and shall be controlled by Company Security Services.

B) Security:

1. Information obtained through video surveillance or recording shall be used exclusively for security and law enforcement purposes, and only be released in accordance with this policy.

2. Video recordings shall be maintained in a secure environment.

3. No attempt shall be made to alter any part of a recording.

4. When a recording is seized as evidence, the name of the investigating officer, date, and time of seizure shall be recorded and retained in a log book within Company Security Services.

C) Retention of Recordings:

1. Recordings that are not viewed will be retained for a period not in excess of 180 days. Recordings viewed for any purpose will be retained for a minimum period of one year from completion of use. In the case of use in court or tribunal proceedings, recordings will be kept for a minimum one year following final disposition of the matter including any court reviews and appeals.

6. APPROVAL:

The installation of video surveillance and recording cameras requires the approval of the Director of Company Security Services in consultation with Information Technology

Services in order to ensure the installation of the camera meets the objectives of this policy and ensure its compatibility with existing systems falls within legal boundaries.

7. REPORT:

The Annual Company Security Services Report will include information regarding the installation of video surveillance and recording cameras. This Report will be published on the Company Security Services Web Site.

RELATED POLICIES:

- Access to Information and Protection of Privacy Policy
- Procedure: Handling Personal Information

3.2 Introduction to an IP surveillance system

Video surveillance has two main baseline functions: live viewing and real-time monitoring of video feeds, and retrieval and viewing of video as a post-event investigation (4). An enterprise video surveillance system may have functions of live viewing and/or recording.

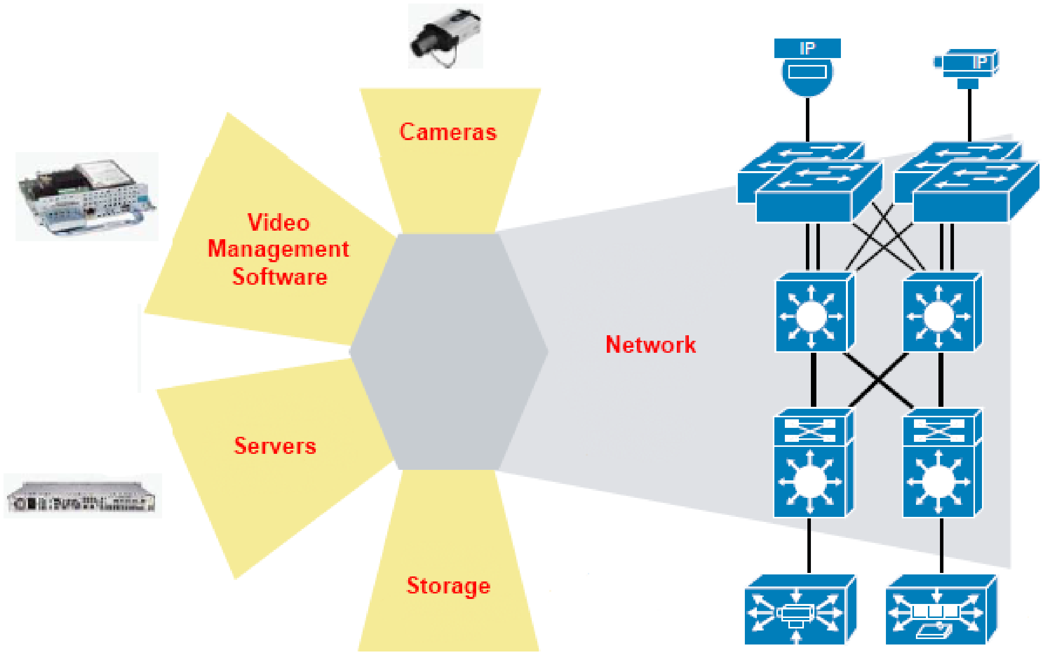
The video surveillance functions are:

- *Capture* — getting and encoding video feeds for network transport
- *Move* — camera feeds are moved from camera to one or more servers
- *Manage* — control of cameras, setting up archives, configuring operator views, etc.
- *Archive* — storing real-time camera feeds to server for later retrieval
- *View* — viewing either live or archived feeds

3.3 IP Video Surveillance Components

Every video surveillance system includes cameras, video management software, servers and storages. The IP network is backbone that ties all components into a converged network infrastructure. The relationship is shown in Figure 1

Figure 1: Components of IP Video Surveillance Deployments [source: Cisco, 2009]



Designing of a video surveillance solutions requires consider several aspects that are influenced on design system:

- Cameras
- Connection
- Video Management System
- Storage
- Record Video
- Video Analytics

- Viewing Video
- Integration Video Surveillance with Others System

3.3.1 Cameras

Cameras are crucial element of any video surveillance system. It should be installed in critical areas and view either checkpoint (like doorway or driveway) or cover the certain area (like parking spot or lobbies). There are a few characteristics of cameras which must be considered what type of camera we should use on the certain location.

- IP or Analog

  All cameras' video is digitized to view and record on computers. For digitize video from analog camera we have to use an encoder or DVR, while IP cameras digitize the video inside the camera. IP camera has advantages: it can be directly connected to IP network and supports megapixel high-res definition while analog does not.
- PTZ (or Panoramic) or Fixed camera

  Fixed camera can look only at one specific view. The view can be changed only mechanically. On the other hand PZT camera lets us to view more widely area using remote moving left and right, up and down, close and farther away. Panoramic camera can view 360^0 angle. The main reason to use fixed cameras is that they cheaper than other one.
- Standard Definition or Hi-Res Definition

  Modern video surveillance cameras can provide hi-definition resolution (such as 720p, 1080p HD, 3MP, 5MP, etc.). From a performance standpoint, there is no reason to use standard definition cameras today.
- Color or Infrared or Thermal

There are color or black and white cameras for video surveillance. Black and white cameras are used when lighting is very low (at night time). Infrared and thermal cameras produce black and white images in those conditions. Infrared cameras require infrared illuminators and produce clear video in low light conditions. There is no needs special lightning for thermal cameras but they produce only silhouettes of objects. Both of those types of cameras are very expensive. Color cameras are the obvious choice for lighted places or day time.

3.3.2 Connection

In video surveillance system, cameras have to be connected to VMS (Video Management System) for recording, managing and viewing purposes. There are two types of connections: wired or wireless. Video from a camera can be transmitted either by cables or through the air. The first one is generally the cheapest and more reliable way for transmitting video. But wireless connection has advantage in places where cables installation can be very hard task and cost-prohibitive (3).

3.3.3 Video Management System

Video Management System is the core of video surveillance solution that receives feed from cameras, store it and distribute video for viewers. There are four options in Video Management System:

- DVR — Digital Video Recorder can record only analog video feeds

- HDVR — Hybrid Digital Video Recorder support both analog and IP cameras
- NVR — Network Digital Video Recorder support only IP cameras
- VMS (Video Management Software)

All types of Video Recorders are computers that combine hardware, software and video storage all in one. DVRs are very easy to install, but they limit expansion of a system and hardware changes. HDVRs are more attractive to use because support both analog and IP cameras. In despite of NVR support only IP cameras, analog cameras can be connected to NVR by using encoder.

Video Management Software is a software application that does not related with certain hardware or storage. It provides more flexibility and lower cost solution compare to using DVR/NVR, but can be more complexity and the time required to set up and optimize the system.

3.3.4 Storage

Surveillance video has to be stored for later retrieval and review. Despite the fact that storage is always becoming cheaper, video surveillance demands more and more an amount of storage. Storage duration is depended on the length of time required to investigations of issues. There are four types of storages for video surveillance:

- Internal Storage — hard drives are built into DVR, NVR or server.
- Directly Attached Storage (DAS) — hard drives are not built into DVR, NVR or server, but connected directly to device without to use a network.
- Network Storage (NAS, SAN) — is based on IP network connection to storing video from many numbers of cameras, DVR, NVR or servers to these storage cluster.
- Onboard Camera Storage — is embedded storage by SD card or hard drive.

3.3.5 Record Video

Surveillance video can be recorded depending on the video resolution, the frame rate and continuously or based on motion recording. Video resolution is depended on type camera is used. Usually, users record at highest resolution the camera can capture. Continuously video means what video is recorded all the time but wastes storage space. Motion based recording saves significantly the space storage but increase the risk that important video will be missing. Frame rate is also important the parameter to save a storage space. In case using 1 fps we get slide show or 30 fps like TV. Statistics on frame rate usage show that 6-10 fps is most common (6).

3.3.6 Video Analytics

Video Analytics software can be used for two general purposes. First, it is used for optimization of the storage by examines video feeds to identify changes in motion. The Video Management System could decide either record video at a lower frame rate (resolution) or nor record video at all. Motion video analytics can help to significant reduce storage consumption. Second, Video Analytics software can identify threatening or interesting events. For example: perimeter violation, license plate recognition or people counting.

3.3.7 Viewing Video

From this side viewing of surveillance video can be divided by:

- Local Viewing — is viewing directly from DVR, NVR or server. This approach allows do not use computer for viewing video and thus, save money.
- Remote PC Viewing — is the most popular means of viewing surveillance video. PC is used to view live or recorded video. It can be done by using special software application or a web browser.
- Remote Mobile Viewing — is viewing on mobile devices (like iPhone, iPad and Android based devices). This approach allows immediately check surveillance video wherever you are.
- Video Wall Viewing — is viewing many cameras at one moment on large screens. This is ideal solution for large security operation center that have hundreds or thousands of cameras under control. Video wall have abilities to switch between cameras and automatically display feeds from locations of alarm.

3.3.8 Integration Video Surveillance with Other Systems

Video surveillance system can be used by itself, just for watching recorded or live video for security purpose. In other hand, video surveillance system can be a part of common security system and can be integrated with a physical security system like electronic access control system. Video surveillance system can send a control signal after recognizing an image to the security access system to allow or denied access. Also Video Surveillance system can response on a security sensor by automatic switching operation layout to view the emergency zone.

4 Practical part

The goal of the practical part is to implement the video surveillance system for a company. Author will compare different solutions for video surveillance for the company to find optimal solution. It will be done using Multiple Criteria Analysis (MCA).

The company "HiTECH-Net" is a not real (fictional) company. It does services and consulting in IT and has own data servers. Company has two branches in different cities and headquarters office. The number of employees is 200. Existing company's corporative network is based on Cisco products. Network includes servers, routers, switches and other equipment by Cisco. Also company uses VoiP (IP Telephony/Voice over IP) on Cisco Unified Communications Manager (CallManager). The video surveillance system that will be implemented has to provide security and monitoring outside (parking slots, entrances, perimeter) and inside (data center, entrances, elevators, corridors, storages, working places) of office buildings. Each branch will has 25 IP cameras and headquarters will has 40 IP cameras.

4.1 Comparing different solutions

There are many companies on the video surveillance market that offers different complex solutions. It can be big integrators, companies that offer different part of video surveillance equipment (cameras, DVR, HDVR, NVR, and Video Manager Software) and an end to end video surveillance solution. Only companies that provide end to end surveillance solution will be compared. In research will be considering an end to end video surveillance solution from these companies:

Panasonic Corporation is one of the largest electronic product manufacturers in the world. Panasonic provides the finest end-to-end imaging, performance for IP, analog and hybrid systems. Company offers integrated solutions with third party partners that cover a wide variety of applications. *Web site: http://www.panasonic.net/*

3VR was founded in 2002. 3VR offers HDVR and NVR appliances with built-in video analytics software. The company primarily targets banking, retail and government applications. *Web site: http://www.3vr.com/*

American Dynamics offers full line products for video surveillance products. Company is providing an end to end IP video solution. They have DVR, HDVR, and NVR with build-in video analytics. Products of American Dynamics are sold into a variety of markets but their main market is retail. *Web site: http://www.americandymanics.net*

Axis was founded in 1984. Company offer IP video solutions for professional installations. It is one of the largest manufacturers of video surveillance globally. Axis focuses primarily on cameras, with an extremely broad array of offerings; Axis is also developing management systems including a hosted video solution (AVHS) and a decentralized VMS in addition to their traditional VMS. *Web site: www.axis.com*

Avigilon offers IP cameras, encoders and VMS software. The company is best known for super high resolution cameras (up to 29MP) and for optimizing the display and retrieval of such cameras. *Web site: http://avigilon.com*

Cisco offers an end to end video surveillance solution that strongly integrates with Cisco's networking equipment. Video surveillance solution from Cisco includes IP cameras, encoders and video management software. *Web site: http://www.cisco.com*

Verint is one of the leaders on video surveillance market. Company provides wide range of cameras, encoders, wireless, and analytics and IP video management software. Nextiva platform is the center of offer which provides tight integration with analytics and advanced command and control functionality. *Web site: http://verint.com*

IndigoVision offers an end to end IP video surveillance solution. IndigoVision's product line consists of IP cameras, encoders, NVR appliances and IP video surveillance software. *Web site: http://www.indigovision.com*

DVTel offers products center around their own line of IP cameras, encoders and IP video surveillance software. There is video analytic software which designed to automatically detect threats and distribute intelligent alerts to the right personnel in real time. *Web site: http://www.dvtel.com*

March Networks offers HDVRs, analytics, encoders, IP and Analog cameras and IP video surveillance software. *Web site: http://www.marchnetworks.com*

Summary of video surveillance components are in following tables (Table 1 and Table 2).

Table 1: Comparison of Video surveillance components of the chosen companies [author]

COMPANY COMPONENT	3VR	Panasonic	American Dynamic	Axis	Cisco
Cameras	Third-party	IP and Analog, Fixed, Fixed Dome, PTZ	IP and Analog, Fixed, Fixed Dome, PTZ	IP: Fixed, Fixed Dome, PTZ, Thermal	IP: Fixed, Fixed Dome, PTZ, third party support
Resolution	None	IP- High resolution, Analog- Standard resolution	IP- High resolution, Analog- Standard resolution	High resolution, Standard resolution	High resolution, Standard resolution
Codec	None	H.264, JPEG, MPEG-4	MJPEG, H.264, MPEG-4	MJPEG, H.264, MPEG-4	MJPEG, H.264, MPEG-4
Connections	None	cable	cable	cable, wireless	cable, wireless
VMS	HDVR, NVR	DVR, NVR	DVR, HDVR, NVR	NVR	Media Server Software
Storage	Internal Storage	Internal Storage	Internal Storage	Internal Storage, Onboard Camera Storage	DAS, NAS, SAN
Video Analytics	Demographics, Facial Surveillance , License Plate Recognition, Advanced Object Tracking, DWELL TIME, Queue Line Analysis, People Counting	build-in camera face detection, video motion detection. "People counting", "Face matching, Age & Gender Estimation"	build-in camera face detection, video motion detection, blur detection	build-in camera video motion detection, audio detection, tampering alarm	build-in camera video motion detection
Viewing Video	PC View	PC View	PC View, Video Wall	PC View, Cloud based View	PC View, Video Wall
Integrations	Access Control, Alarm or ATM & Teller	no information	Real-time alarms	available	Access control, Incident Response

Table 2: Comparison of Video surveillance components of the chosen companies (Continue) [author]

COMPANY COMPONENT	Avigilon	Verint	IndigoVision	DVTel	March Networks
Cameras	IP: Fixed, Dome, PTZ, Panoramic, LPR(License Plate Recognition), third party support	IP: Fixed, Fixed Dome, PTZ	IP: Fixed, Fixed Dome, PTZ, third party	IP: Fixed, PTZ	IP: Fixed, PTZ Analog: Fixed, Fixed Dome, PTZ
Resolution	High resolution	High resolution, Standard resolution	High resolution, Standard resolution	High resolution	High resolution
Codec	MJPEG, H.264, MPEG-4, JPEG2000	MJPEG, H.264, MPEG-4	H.264, MPEG-4	H.264, MPEG-4	MJPEG, H.264, MPEG-4
Connections	cable	cable, wireless	cable	cable	cable
VMS	NVR	HDVR, NVR	NVR, Windows NVR	None	HDVR
Storage	Internal Storage	Internal Storage, Onboard Camera Storage	Internal Storage, DAS, SAN, NAS	None	Internal Storage
Video Analytics	third party	Scene Scan captures, Camera Tampering Detection, Perimeter Intrusion Detection, Secure Area Monitoring, Wrong Direction, Equipment Removal Detection	Congestion Detection, Motion detection, Abandoned Object Detection, Virtual tripwire, Theft Detection, Counter Flow, Hooded Camera Detection	available	Fall Detection, Loitering Detection, Speed Monitoring, Wrong Way Detection
Viewing Video	PC View, Video Wall	PC View, Video Wall, Mobile	PC View, Mobile	PC View	PC View
Integrations	Access Control and Intercom Systems	available	available	no information	no information

Companies offer a different design of video surveillance system that consists from different types of components. Thus, the scheme of the system will be different depends of supplier company. Many companies provide price list only by demand (call). That is why it is very difficult to compare solutions by price.

4.2 Multiple Criteria Decision Making

Choice of a solution will be done based on Table 1 and Table 2. Our problem of choice has multiple attributes. Decision will be made by using the Multiple Criteria Decision-Making (MCDM), in particular, one of parts of MCDM, Multiple Attribute Decision Making (MADM). There are a limited number of predetermined alternatives (variants) (Table 3).

Table 3: Criterion

	Criterion
1	Support own & third part cameras
2	Connection (wired or wireless)
3	Support distributed video surveillance location
4	Ability to integrate new VSS into exist network based on Cisco equipment
5	Video Analytics
6	Support video wall
7	Integration

First step: Assessing weights by score method requires first assignment of certain number of points to each criterion (Table 4). Minimum is 1, maximum 5 in our example. The weights are than counted as:

$$vj = \frac{pj}{\sum_{j=1}^{n} pj}$$

Table 4: Weights of criterions

Criterion	1	2	3	4	5	6	7	SUM
Number of points, pj	1	2	5	4	3	5	4	24
Weights, vj	0,0417	0,0833	0,2083	0,1667	0,1250	0,2083	0,1667	1

The weight of criteria was obtained mainly based on specified requirements by the company. Also, IT experts were interviewed about the significance of each criteria respect to IT infrastructure of the company.

Second step: The MADM problem can be expressed in a matrix containing criteria in columns and variants in lines (7). Evaluate and assign for each variant and criterion number of points from 1 to 5 (higher is better) (Table 5).

Table 5: Variant - Criterion

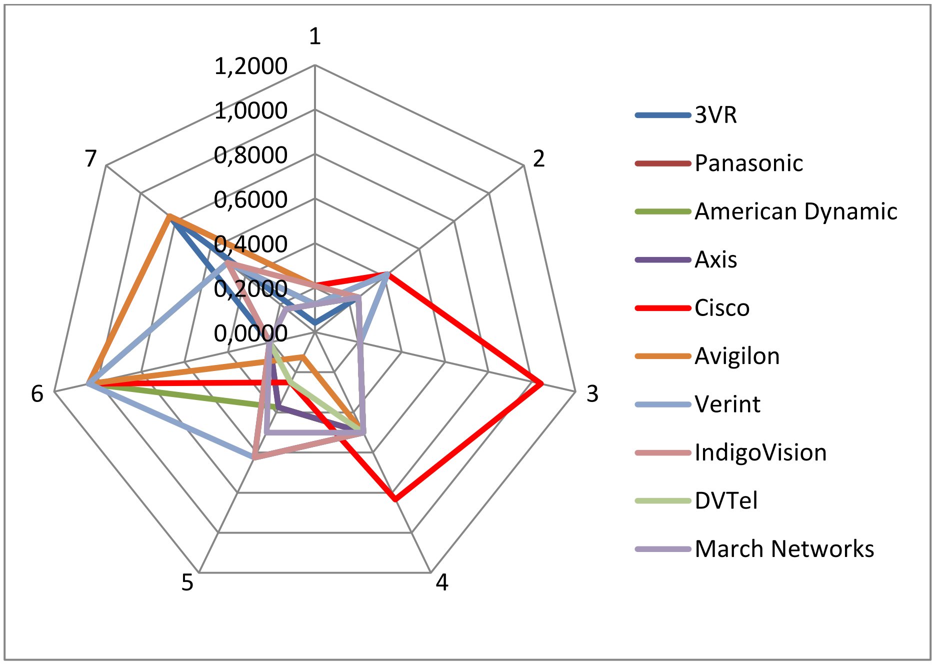
		Criterion						
Variant		1	2	3	4	5	6	7
1	3VR	1	3	1	3	5	1	5
2	Panasonic	3	3	1	3	3	1	1
3	American Dynamic	3	3	1	3	3	5	3
4	Axis	3	5	1	3	3	1	3
5	Cisco	5	5	5	5	2	5	5
6	Avigilon	5	3	1	3	1	5	5
7	Verint	3	5	1	3	5	5	3
8	IndigoVision	5	3	1	3	5	1	3
9	DVTel	3	3	1	3	2	1	1
10	March Networks	3	3	1	3	4	1	1

Third step: Apply weights of criterion to each sell of Table 6.

Table 6

		Criterion							
Variant		1	2	3	4	5	6	7	SUM
1	3VR	0,0417	0,2500	0,2083	0,5000	0,6250	0,2083	0,8333	2,6667
2	Panasonic	0,1250	0,2500	0,2083	0,5000	0,3750	0,2083	0,1667	1,8333
3	American Dynamic	0,1250	0,2500	0,2083	0,5000	0,3750	1,0417	0,5000	3,0000
4	Axis	0,1250	0,4167	0,2083	0,5000	0,3750	0,2083	0,5000	2,3333
5	Cisco	0,2083	0,4167	1,0417	0,8333	0,2500	1,0417	0,8333	4,6250
6	Avigilon	0,2083	0,2500	0,2083	0,5000	0,1250	1,0417	0,8333	3,1667
7	Verint	0,1250	0,4167	0,2083	0,5000	0,6250	1,0417	0,5000	3,4167
8	IndigoVision	0,2083	0,2500	0,2083	0,5000	0,6250	0,2083	0,5000	2,5000
9	DVTel	0,1250	0,2500	0,2083	0,5000	0,2500	0,2083	0,1667	1,7083
10	March Networks	0,1250	0,2500	0,2083	0,5000	0,5000	0,2083	0,1667	1,9583

Figure 2: Radar Chart



The variant which has a maximum value in column “SUM” is the best choice. In our case it is the video surveillance solution from Cisco.

4.3 The Cisco Video Surveillance solution components

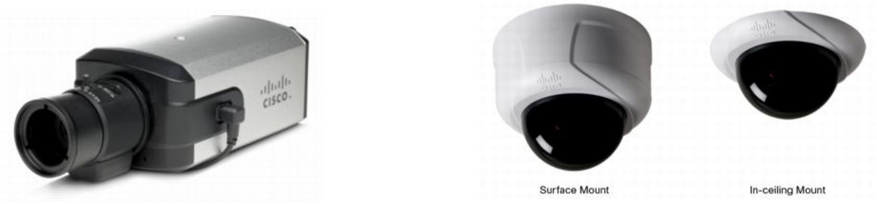
The Cisco Video Surveillance solution is based on an IP network to connect all components together. Cisco offers an approach that allows joining different proprietary systems to a common IP backbone.

4.3.1 Camera

Type of cameras will be considered respect to types of CODECs, resolutions and bit/frame rates that will be needed for choosing equipment and the technical solution. Aspects of physical placement (camera's angle of view, coverage of the observation zone, etc.) and installation are beyond the scope of the practical part of the diploma thesis and will not be considered.

Cisco 4000 Series fixed IP cameras and Cisco 5010/5011 Indoor Fixed Dome (PTZ) IP cameras [Figure 3] with a resolution of 1080p (1920 x 1080) are satisfy our requirements for video quality. Those cameras use H.264 CODEC for video coding and can be configured for a constant bit rate in increments of 2, 4, 6, 8, 10, 12, and 15 Mbps [Table 7].

Figure 3: Cisco 4000 Series and Cisco 5010/5011IP cameras [source: Cisco]



In viewing live video streams, a configured rate of 4Mbps will provide acceptable video quality.

Table 7: Camera Network Bandwidth Estimates

Camera	CODEC	Resolution	Estimated Bitrate
Cisco 4000 Series	H.264	1920 x 1080 (2.1 MP) (1080p) HD	4 Mbps
Cisco 5010/5011	H.264	1920 x 1080 (2.1 MP) (1080p) HD	4 Mbps

Each IP camera uses Power-over-Ethernet (PoE) for easy installation. Camera has to be attached to the access switch at 100Mbps.

4.3.2 Switch

Choosing of switch to deploy have to be based on these three factors: number of cameras, bit rate, support PoE.

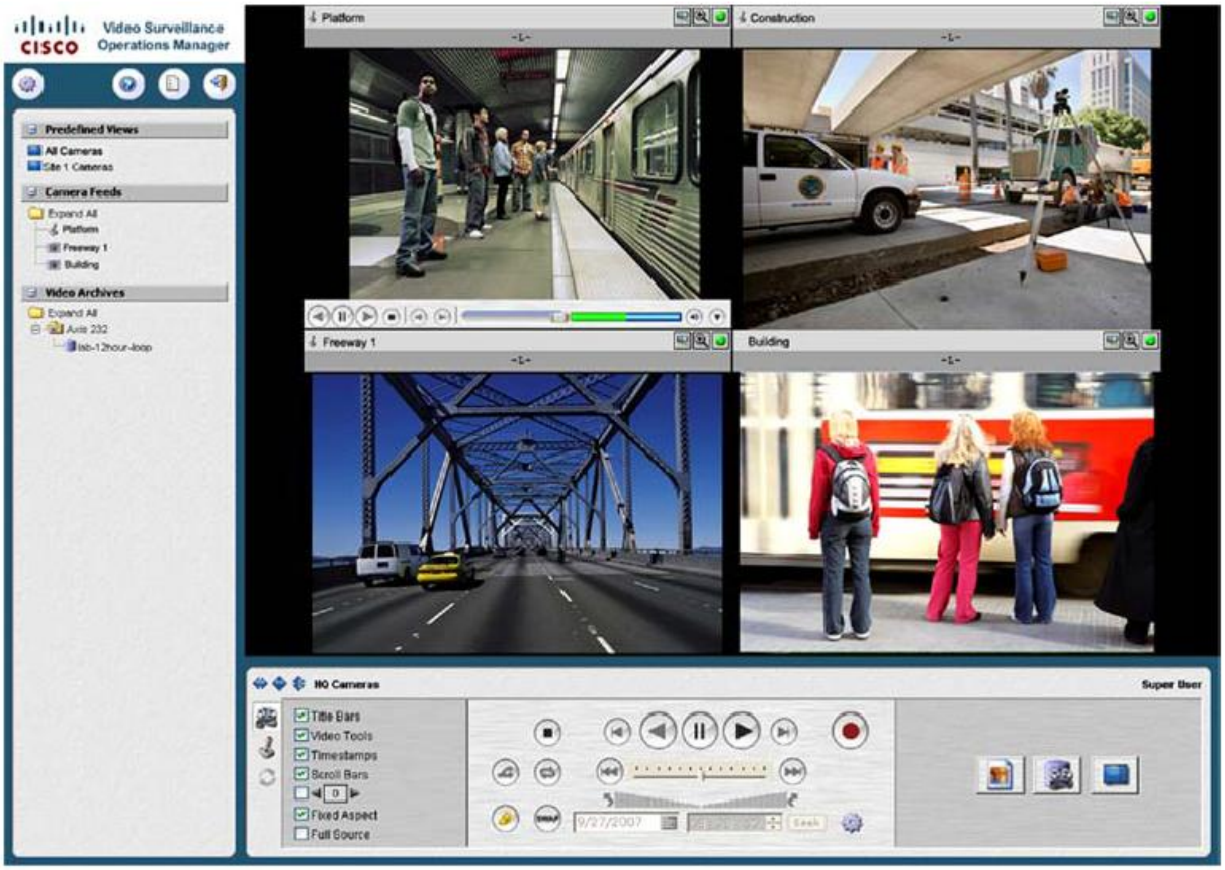
Target constant bit-rate is 4Mbps. Therefore a 24-port switch at 4Mbps per port, is 96 Mbps of offered load and a 48 port switch offers 192 Mbps. Based on this value, a switch with 48 ports, 32Gbps backplane, and 1Gbps uplinks will service these requirements. One of switches that meet the requirement is the Cisco Catalyst 3560G-48PS [Figure 4]: 48 Eth 10/100/1000 ports with PoE and 4 SFP GigE ports.

Figure 4: Cisco Catalyst 3560G-48PS [source: Cisco]

4.3.3 Operations Manager

Operations Manager provides a web-based browser console to authentication, configuration, and manages access to video feeds at the branch location. It is administration tool for management of Media Servers, Virtual Matrixes, cameras, encoders, and viewers—and for viewing network-based video. The responsibility of the Operations Manager is delivering a list of resource definitions. It could be camera feed, archived video, and predefined view to the viewer. Once this information is provided to the viewer, the viewer communicates directly with the appropriate Media Server to request and receive video streams. Figure 5 the Operations Manager main screen, which is accessed via a web browser.

Figure 5: Video Surveillance Operations Manager [source: Cisco, 2009]



The Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing:

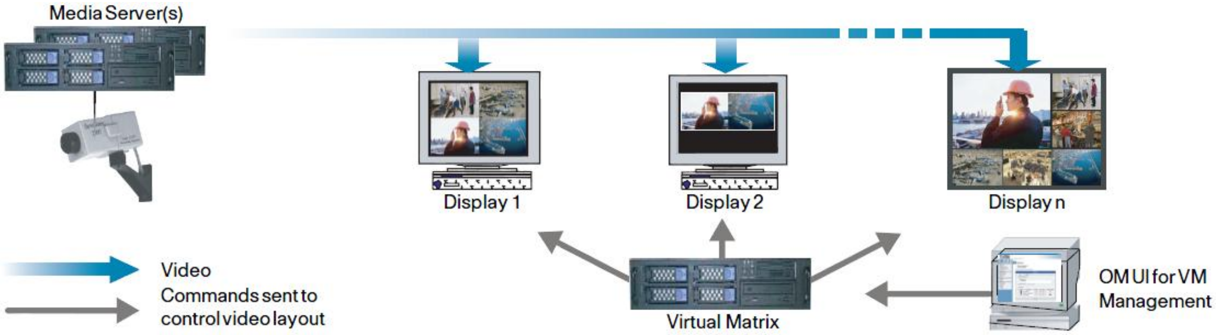
- Multiple Web-based consoles to configure, manage, display, and control video throughout a customer’s IP network
- The ability to manage a large number of Cisco Video Surveillance Media Servers, Cisco Video Surveillance Virtual Matrixes, cameras and users
- Customizable interface, ideal for branded application delivery
- Encoder and camera administration
- Scheduled and event-based video recording
- Interface to Media Server and Virtual Matrix software for pushing predefined views to multiple monitors
- User and role management
- Secure login
- Live and archived video views
- Friendly user interface for PTZ controls and presets, digital zoom, and instant replay
- Event setup and event notifications
- “Record Now” feature while viewing live video
- Archive review and clipping (4)

4.3.4 Virtual Matrix

The Virtual Matrix is responsible for live or recorded video in command center. It allows operators to provide detailed monitor layout to the Virtual Matrix monitors and the position of each camera feed on multiple local and remote monitors. One Virtual Matrix server is able to manage a large number of Virtual Matrix monitors because the communication between the monitors and the server is required only during the initialization procedure or when a new view is being added to the monitor.

Figure 6 demonstrates the scheme how operators can make choice from available cameras to be displayed on any system monitors within any custom video display patterns. The Virtual Matrix can be also integrated with other security systems that have user-defined event triggers to automatically displaying actual video in to response to trigger. For example these triggers can be access control, fire alarm system in buildings, or motion sensors.

Figure 6: Virtual Matrix Switch [source: Cisco, 2009]



4.3.5 Media Server

Media Server is used for manages, stores, and delivers surveillance video from IP cameras to viewers or other media servers. It can be single physical server or distributed across the network, scaling to handle thousands of cameras and users. Media Server runs on Linux-based servers.

Video Surveillance Media Server provides the following functions:

- Collection and routing of video from a wide range of cameras and encoders over an IP network

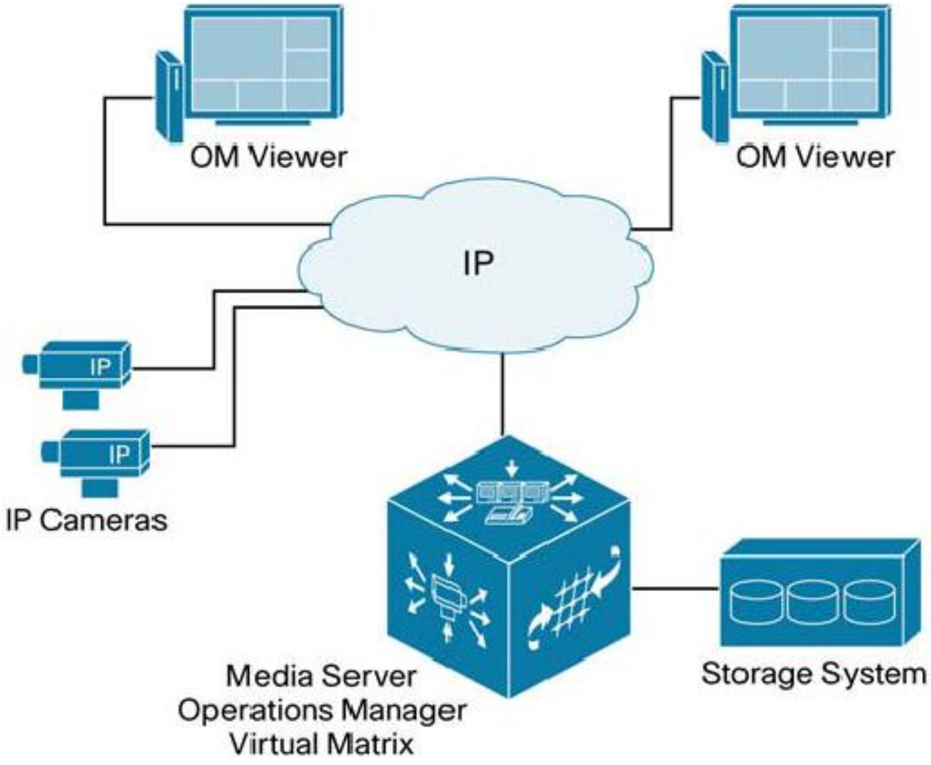
- Secure local, remote, and redundant video archive capabilities
- Event tagging for review and archival purposes
- Bandwidth management for both live distribution and historical recording (4)

4.3.6 Storage

Media Server's internal storage can be combined with direct-attached storage (DAS) and storage area networks (SANs). Video surveillance video can be stored in system in loops or as event clips triggered or as one-time archives.

Figure 7 shows a single server that operate as a Media Server, Operations Manager and Virtual Matrix that is also connected to an external storage system.

Figure 7: VS Storage System [source: Cisco, 2009]



Features of Storage System:

- Media Server maintains internal storage up to 24 TB
- DAS arrays support up to 42 TB per array, 420 TB per rack
- Support for 3rd party SANS
- RAID 5 configuration available (4)

Calculation the need capacity of storage:

The following formula is used to calculate the bandwidth requirements for H.264 streams:

H.264 storage = Bit rate (kbps) x duration

The target bit rate is configured on the camera and is already expressed in bits per second. In our case bitrate equals to 4 Mbps.

Mbps / 8 bits/s = 0,5 MB / second x 3600 = 1800 MB / hour = 1,8 Gb/hour

*24 cameras = 1,8 Gb/hour * 24 = 43,2 Gb/hour (for each branch)*

*40 cameras = 1,8 Gb/hour * 40 = 72 Gb/hour (for headquarters)*

Hard Disk Drive in Media Server has capacity 2 Tb.

Total time for recording (for each branch) = 2000 Gb / 43,2Gb/hour = 46 hour

Total time for recording (for headquarters) = 2000 Gb / 72Gb/hour = 27 hour

Thus, surveillance video has to be archived to archive server in headquarters for branches each 1.5 days and for headquarters each day.

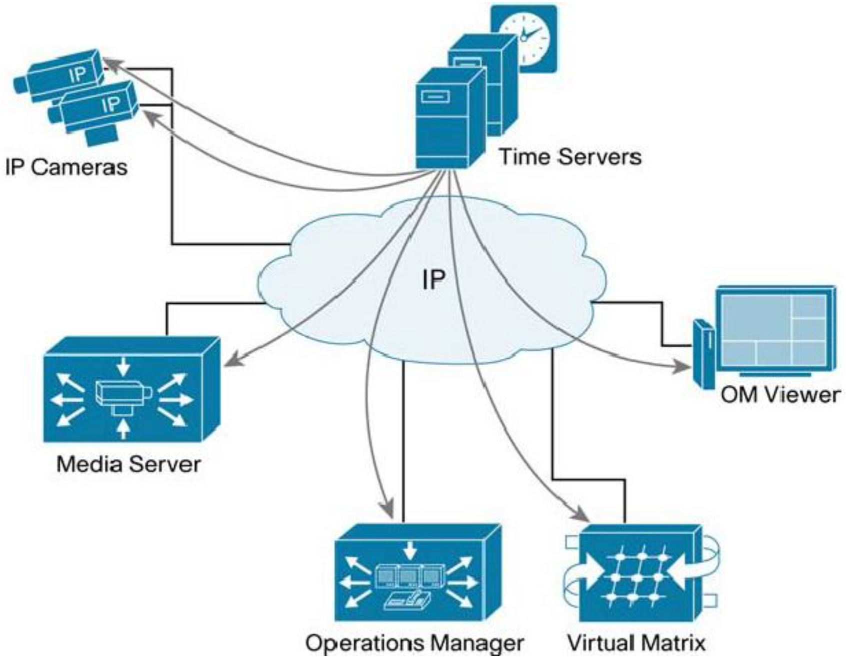
To archive surveillance video we will use iSCSI server with capacity 48 Tb. It lets record on server 303 hours surveillance video.

4.4 Application Requirements to Network protocols

The Cisco Video Surveillance Media Manager application requires several network protocols to operate efficiently.

Time Synchronization — The Network Time Protocol (NTP) is used to synchronize clocks of network elements with a reliable time source. Clock synchronization is important when retrieving recorded video streams. Figure 8 shows how the NTP server distributes the current time to IP cameras, viewers and servers.

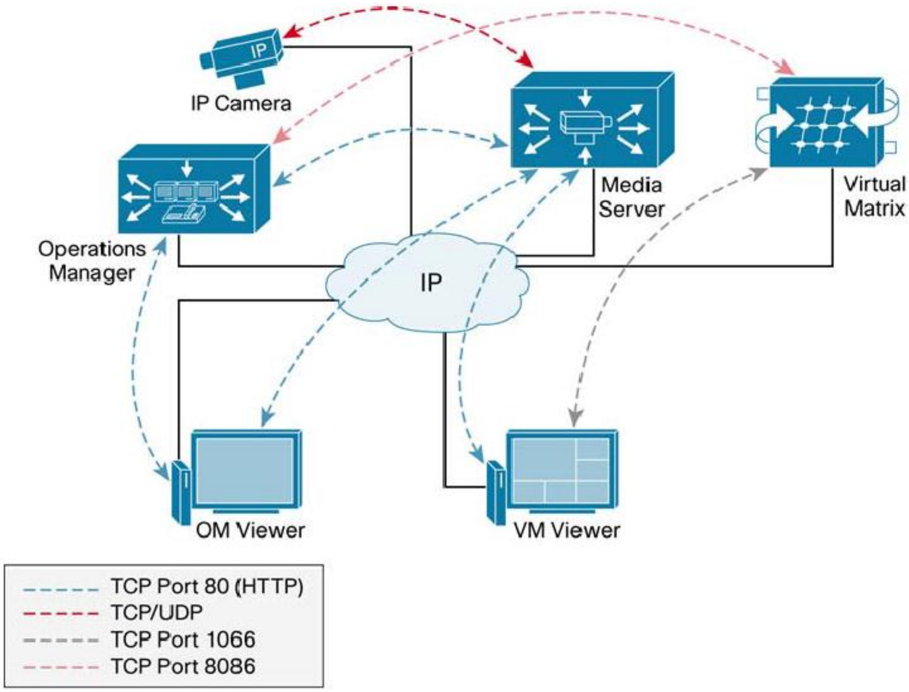
Figure 8: Network Time Protocol (NTP) [source: Cisco, 2009]



TCP/UDP Transport — IP cameras and encoders can transport video and audio to and get command from the Media Server in different ways that depends on the manufacturer. Some devices may support only MJPEG over TCP (Transmission Control Protocol), while others may also support MPEG-4/H.264 over UDP (User Datagram Protocol).

Required TCP/UDP Ports — the communication between the Media Server and viewers relies on TCP port 80 (HTTP) is shown in Figure 9. The communication between edge devices and the Media Server may use vary TCP ports (Virtual Matrix Server - VM Monitor — TCP port 1066, Virtual Matrix Server - Operations Manager — TCP port 8086).

Figure 9: TCP/UDP Ports [source: Cisco, 2009]



Quaity of Service (QoS) — serves to manage network congestion during time where bandwidth is constrained. However, problem with bandwidth constraints cannot be solved by QoS. It just provides the control to access for competitive applications to the bandwidth by set up priority one application over another.

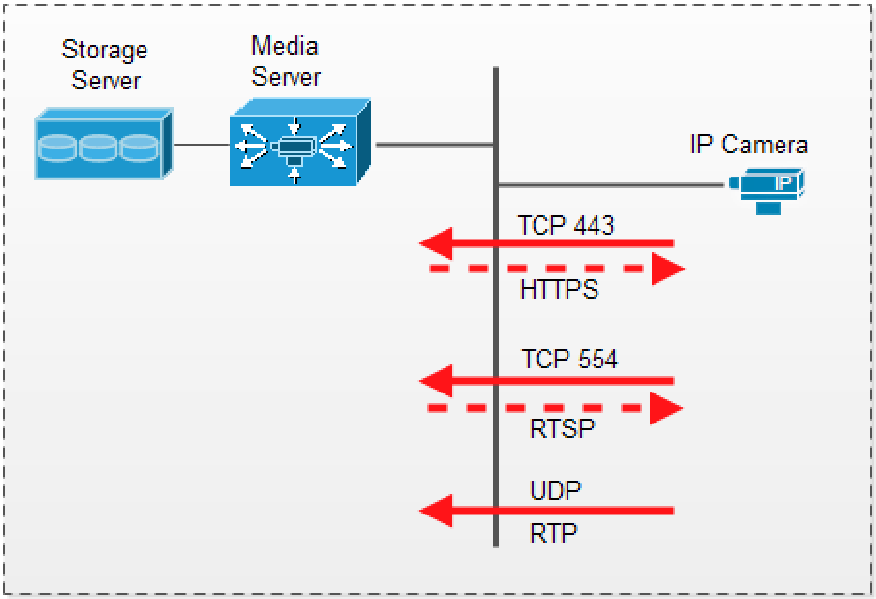
QoS is critical in a converged environment where voice, video, and data traverse the same network infrastructure. Video surveillance traffic is sensitive to packet loss, delay, and delay variation (jitter) in the network. Cisco switches and routers provide the QoS features that are required to protect critical network applications from these effects.

4.5 Traffic Flow between IP Camera and Media Server

Video from an IP camera can be viewed directly. It can be doing by a webserver client connecting to the camera API—Application Programming Interface.

Traffic flow between IP camera and Media Server is shown on Figure 10. When there is a need to archive or live feed from an IP camera, Media Server initiates a HTTPS session with the IP camera for authentication and control plane and RTSP session with the IP camera for description, initiation or termination of the media feeds. The IP camera transmits media feed as UDP/RTP session on port negotiated in the RTSP exchange.

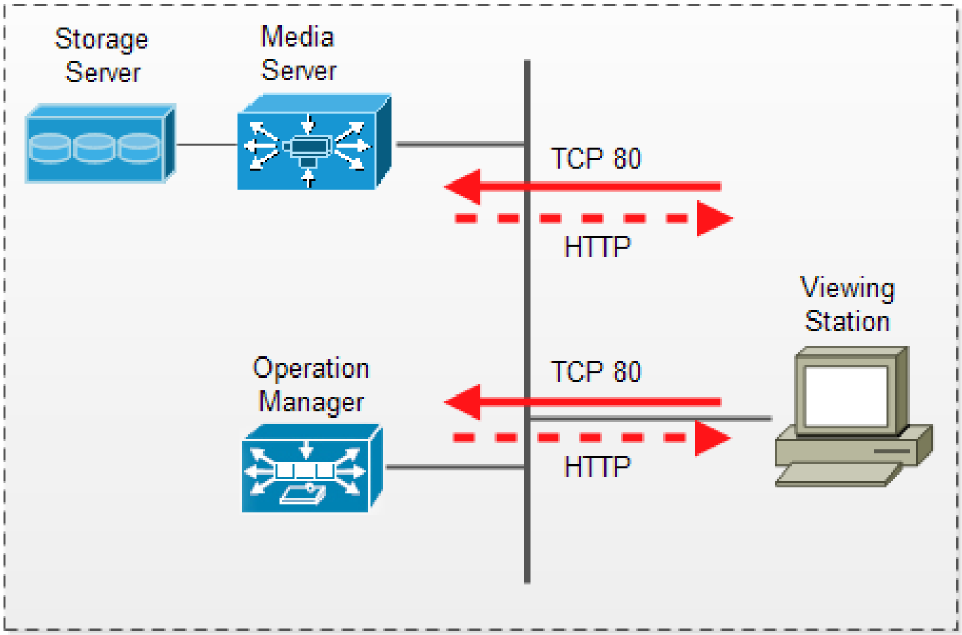
Figure 10: Traffic Flow IP Camera and Media Server [source: Cisco, 2009]



4.6 Traffic Flow Viewing Station and Media Server

Traffic flow between IP camera and Media Server is shown on Figure 11. Viewing station initiates TCP connection to IP address of Operation Manager and issue HTTP GETs to the appropriate IP address of Media Server to initiate the video stream.

Figure 11: Traffic Flow Viewing Station and Media Server [source: Cisco, 2009]



4.7 Design Network for Video Surveillance System

In the scheme, Media Servers will be distributed on branches. Figure 12 shows a deployment two remote sites, each with a local Media Server acting as the direct proxy and archive for local IP cameras. The surveillance video is recorded at the remote branches and live video streams are viewed by OM Viewers and VM monitors on video walls at the headquarters. The Media Server at the headquarters requests the remote surveillance video only when it required. Also surveillance video feeds are viewed at branches by local security personals.

Figure 12: Distributed Media Servers [author]

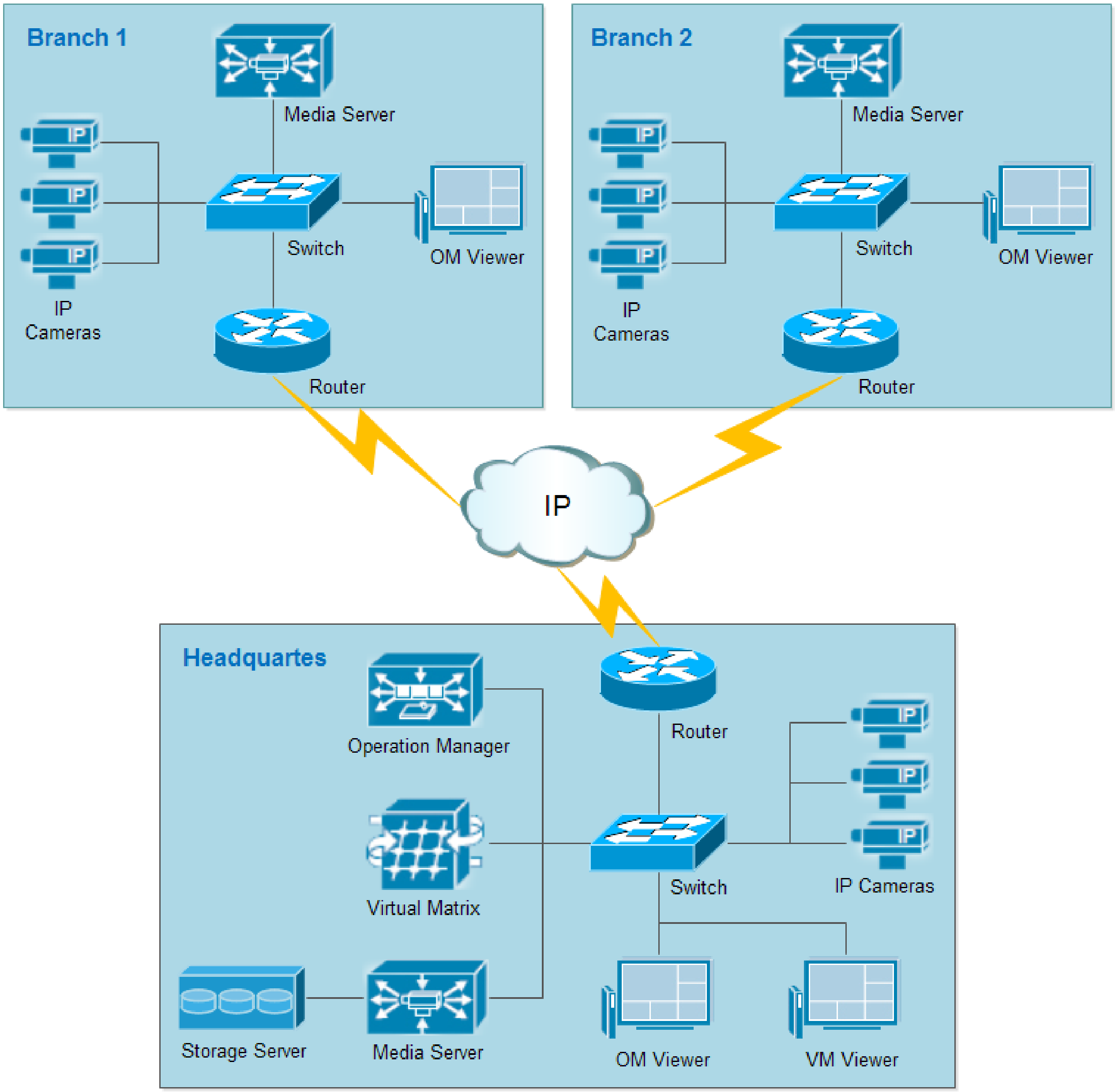
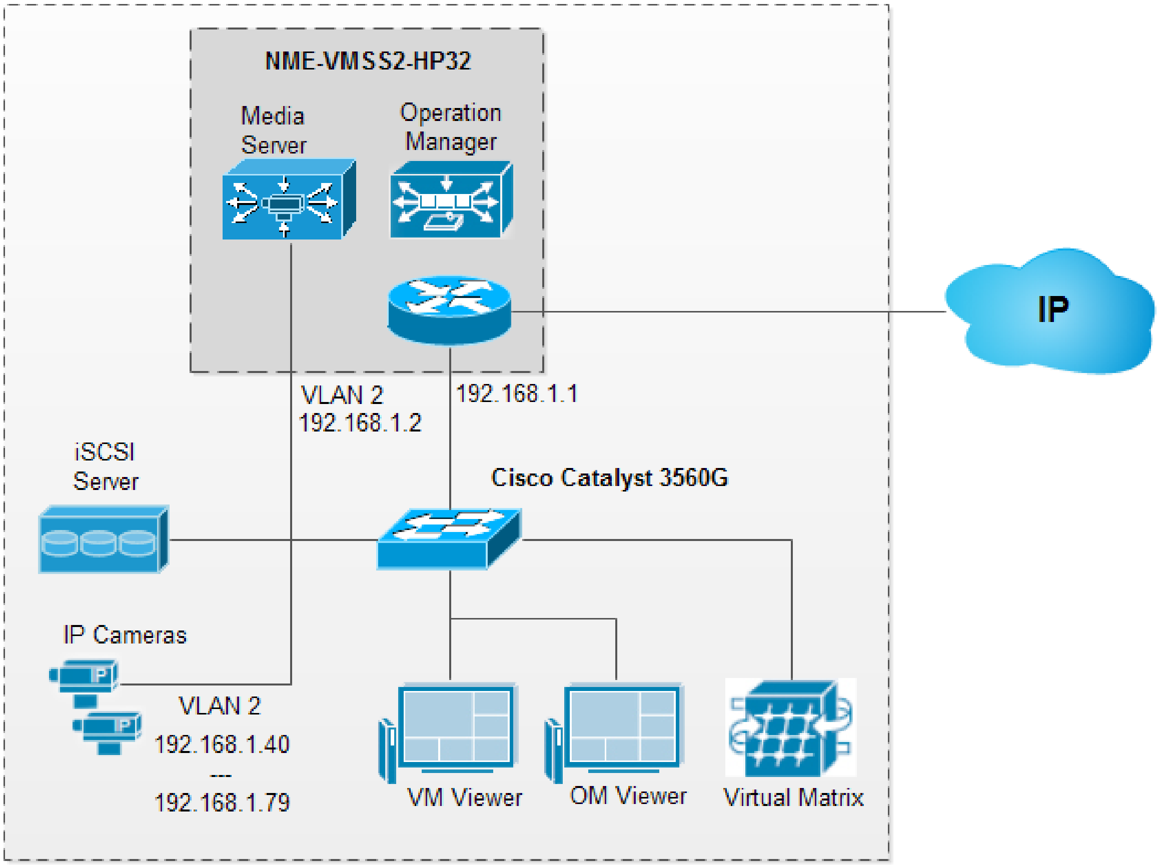


Figure 13 depict the topology of the headquarters router deployment. Existing ISR Cisco 3825 is equipped an operational Cisco VMSS Network Module (NME-VMSS2-HP32). A Layer-2 switch Cisco Catalyst 3560G capable of providing Power-over-Ethernet (or an external power injector, or power supply is available) and a FastEthernet network connection on a VLAN dedicated to the cameras at the headquarters.

Figure 13: Headquarter Router Deployment Topology [author]



Topology of branches is similar to Figure 13 except iSCSI server, VM viewer and Virtual Matrix.

4.6 Financial analysis

Financial plan is approximate and do not include cabling, installation, setting up and supporting costs. All price information was found on vendor's web sites and provides the estimated values of components.

Table 8: Cost of video surveillance components

Description	Qty	Unit price	Total price
Fixed camera Cisco 4300E Series	15	17 400,00 CZK	261 000,00 CZK
PTZ camera Cisco 5011	65	26 000,00 CZK	1 690 000,00 CZK
Switch Cisco Catalyst 3560G-48PS	3	118 000,00 CZK	354 000,00 CZK
Cisco Video Management and Storage System NME-VMSS2-HP32 HDD 2Tb	3	62 000,00 CZK	186 000,00 CZK
iSCSI Server + 48 Tb	1	143 000,00 CZK	143 000,00 CZK
3x3 Video Wall using 9 Samsung UE46A 46" LED Screens (138" Diagonal screen size)	1	656 400,00 CZK	656 400,00 CZK
Viewer PC HP Pro 3500 MicroTower + 27" ASUS VE278N	4	18 300,00 CZK	54 900,00 CZK
		TOTAL:	**3 202 300,00 CZK**

Total estimated cost of video surveillance deployment is 3.202.300 CZK

5 Evaluation of results and recommendations

Based on result Multiple Criteria Analysis (Table 6) solution from Cisco had been chosen. In case other conditions, solution from Cisco will not be optimal because the higher price. In our case, company has the network infrastructure based on Cisco products and parts of this equipment are used for video surveillance system and help reduce total cost of system implementation.

The Cisco Video Surveillance solution is optimized for distributing video using advanced network features and functions. Users can get the access to video surveillance at any time from any place. Cisco solution has advantage in the live video monitoring. The virtual matrix provides the distribution of live video from many locations to many monitoring location.

To solve issues with bandwidth constraints, proxy processes are used to adjust resolution and frame rate to make video. This allows remote users to view video without overloading the network. For maximizing video surveillance performance there are two of the most significant means: Quality of service (QoS) and multicasting. When many viewers are watching the same video stream multicasting has ability to reduce load of bandwidth. QoS can help ensure that resources and bandwidth are available for video. In other hand such kinds of optimization require Cisco routers and other devices that support these features and expert configuration.

6 Conclusion

Video surveillance system based on Cisco products is very expensive but it could be used in case there are big numbers of cameras, a need for live video surveillance and distributed surveillance locations.

Restriction with bandwidth can be more efficiently solved by video analytics. It reduces flow of data through network. Cisco tries to solve this restriction not efficiently by optimizing live video. From security point of view monitoring live video from many cameras does not address the critical issue in security: how do you assess and identify threats? Often security stuff cannot make meaningful decisions based on it.

At the same time, the fundamental issue of live video can be solved by video analytics. Of course, this does not mean that live video monitoring will be eliminated at all. Rather analytics will decrease the need to watch as much a live video. Competitor of Cisco much more intensity use video analytics to reduce the importance of the network. Strengths of Cisco are routing and IP telephony because it is very advantageous for customers to use a single supplier for both solutions. Also Cisco provides features beyond the standards. If you decide to use them you could have issues with integration 3rd party products. While Cisco offers strong solutions in network devices and IP telephony make sense to buy whole solution from Cisco.

7 References

1. **Senior, Andrew.** *Protecting Privacy in Video Surveillance.* London : Springer-Verlag London Limited, 2009.

2. **Sloan, Virginia E. and Messinger, Scott I.** *GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE.* Constitution Project, Washington : 2007.

3. **Luigi Di Stefano, Carlo Regazzoni, and Dan Schonfeld.** *Advanced Video-Based Surveillance.* s.l. : Hindawi Publishing Corporation, 2011.

4. **King, Joel W.** *Cisco IP Video Surveillance Design Guide.* s.l. : Cisco Systems, 2009.

5. **Sun, Tong , Xia, Yongquan and Gan, Yong .** Discussion on Integration of Urban Video Surveillance System. China : Zhengzhou University of Light Industry.

6. **Honovich, John.** Average Frame Rate Used for Recording. *IP Video Market Info.* [Online] 04 11, 2011. [Cited: 2 10, 2013.] http://ipvm.com/updates/1100.

7. Multiple Criteria Decision Making /Finite Number of Alternatives. *http://orms.pef.czu.cz.* [Online] [Cited: March 03, 2013.] http://orms.pef.czu.cz/text/Multicriteria/MCfirstLevel.html.

8. **Tanenbaum, A.S.** *Computer Networks. Fifth Edition.* New Jersey 07458 : Pearson Education, Inc.Publishing as Prentice Hall PTR Upper Saddle River, 2010.

9. **Wei Niu, Jiao Long, Dan Han, and Yuan-Fang Wang.** *Human Activity Detection and Recognition for Video Surveillance.* Santa Barbara, CA 93106 : Department of Computer Science University of California, 2004.

10. Bussiness Video. *http://www.cisco.com/go/businessvideo.* [Online]

11. Physical Security and Building System. *http://www.cisco.com/go/physicalsecurity.* [Online]

12. **Foresti G.L., Mahonen P. and Regazzoni C.S.** *Multimedia Video-Based Surveillance Systems: from User Requirements to Research Solutions.* s.l. : Kluwer Academic Publishers, 2000.

13. **Regazzoni C., Fabri G., and Vernazzza G.** *Advanced Video-based Surveillance System.* USA : Kluwer Academic Publishers, 2002.

14. **Robert T. Collins, Alan J. Lipton, Takeo Kanade, Hironobu Fujiyoshi, David Duggins, Yanghai Tsin, David Tolliver, Nobuyoshi Enomoto, Osamu Hasegawa, Peter Burt1 and Lambert Wixson1.** *A System for Video Surveillance and Monitoring.* s.l. : Carnegie Mellon University, 2000.

15. **Dean, Tamara.** *Network+ Guide to Networks, Fifth Edition.* USA : Course Technology, Cengage Learning, 2010.

16. **Romero, Carlos and Rehman, Tahir.** *Multiple Criteria Analysis for Agricultural Decisions, Second Edition.* Amsterdam : ELSEVIER, 2003.

17. **Figueira, José , Greco, Salvatore and Ehrgott, Matthias.** *Multiple Criteria Decision Analysis: State of the Art Surveys.* USA : Springer Science+Business Media, Inc., 2005.

18. **Peltier, Thomas R.** *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition.* New-York : Business & Economics, 2004.

19. **Johnson, Robert .** *Security Policies and Implementation Issues.* USA : Jones & Bartlett Publishers, 2011.

20. **R. Webster, C. William, et al., et al.** *Video Surveillance: Practices and Policies in Europe.* USA : IOS Press, 2012.

21. **Caputo, Anthony C. .** *Digital Video Surveillance and Security.* USA : ELSEVIER, 2010.

22. **Dufour, Jean-Yves.** *Intelligent Video Surveillance Systems (ISTE).* USA : Wiley-ISTE, 2012.

8 List of abbreviation

9 Tables

10 Figures