# MODULE 1: DESIGN AND APPLICATION OF IP-BASED VIDEO SURVEILLANCE SYSTEM

# FUNDAMENTALS OF IP-BASED VIDEO SURVEILLANCE SYSTEMS


BY: LENNOX BENNETT

# REVIEW OF VIDEO SURVEILLANCE SYSTEM

## Modern Application of VSS

- Automated video surveillance is a complex technology combining recent developments in computer vision, hardware (cameras, video storage), and networking and data bases.
- It is applied to protect various types of objects: state borders, industrial infrastructure, public areas, buildings, bank operations, airport, hospitals, offices, malls and parking lots.
- Automated systems gradually displace installations using solely human observers, as they are considered costly and ineffective.
- Typical video analysis components include such functions as background maintenance, object detection, classification, object tracking and activity (event) recognition.

# PUBLIC USE OF VIDEO SURVEILLANCE

## Rationale and Justification

- The word ‘surveillance’ means to observe a specific area or to monitor the activities of individual or a group.
- It is very useful to the law enforcement to maintain social control, monitor and recognize threats, and investigate criminal activity.

- **Manual Surveillance**
  - Impractical
  - Very Costly
  - Lack of Attention
  - Needs Situational Awareness

# PURPOSE OF IP VIDEO SURVEILLANCE

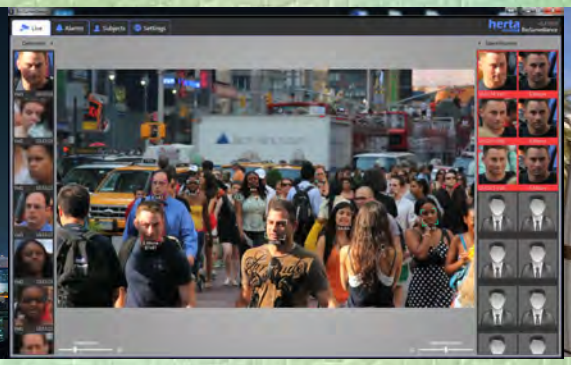
- Prevent crime or vandalism before it happens.
- Create a physical presence at the protected site.
- Observe all locations continuously
- Protect outdoor grounds and assets easily.
- Monitor and control or reduce security threats, risk and vulnerability.
- Used for traffic monitoring.

- Focus of Training
  - Correct use of System
  - Safety
  - Legal Consideration

# OVERVIEW OF VIDEO SURVEILLANCE

## Introduction

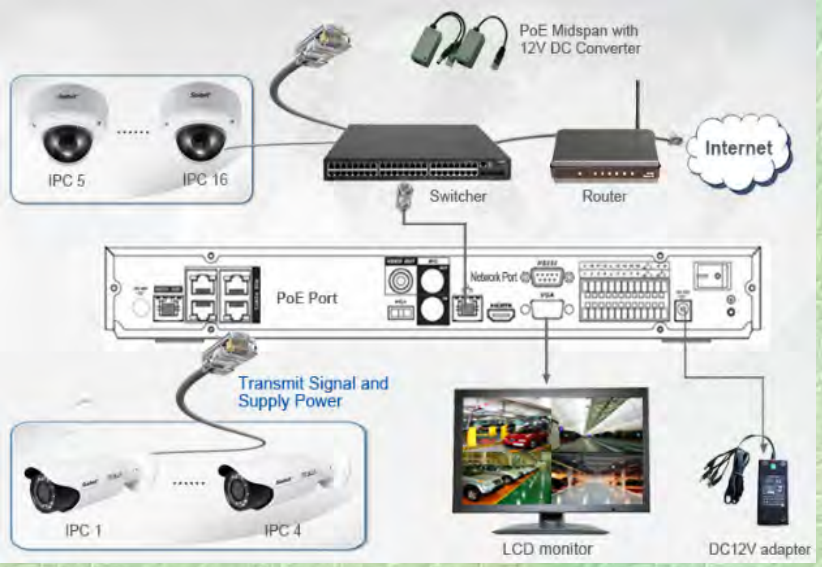
- Video surveillance systems currently are undergoing a transition where more and more traditional analog solutions are being replaced by digital ones.
- Compared with the traditional analog video surveillance system, a digital video surveillance offers much better flexibility in video content processing and transmission.
- At the same time, it, also, can easily implement advanced features such as motion detection, facial recognition and object tracking.



# DISTINGUISHING BETWEEN TYPES OF SECURITY

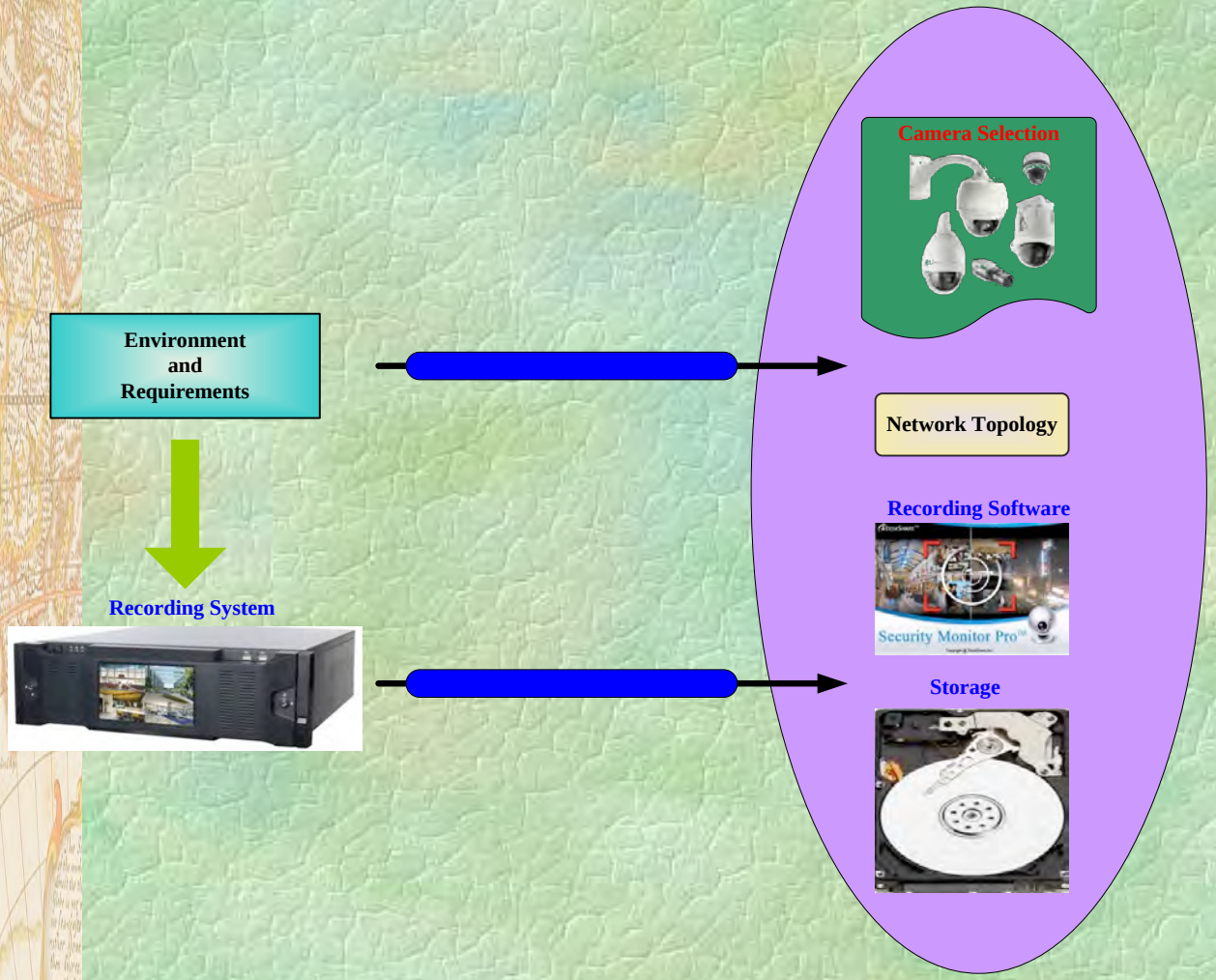
## Types of Video Security

- Crime Detection
- Loss Prevention
- Vandalism Deterrence
- Product Reliability (QA)
- Mass Casualty Response
- Insurance and False Claims
- Regulatory Agency Requirement
- Guest | Patron | Employee Safety
- Integration with IOT [Doors and Card Readers]



# SYSTEM DESIGN CONSIDERATION

**Figure 1-1:** System Consideration



# RELEVANCE OF SYSTEM FUNCTION

**Figure 1-2:** Video Surveillance System Functions


Monitor

Investigate

Alarm

Export

# IMPLEMENT FOR DIFFERENT PURPOSE

## Purpose of the Observation

**How much detail do you need in the picture?**

**Consider which of the five 'levels of detail' described in section 3.1 is most appropriate to your requirement.**

**You may wish to:**

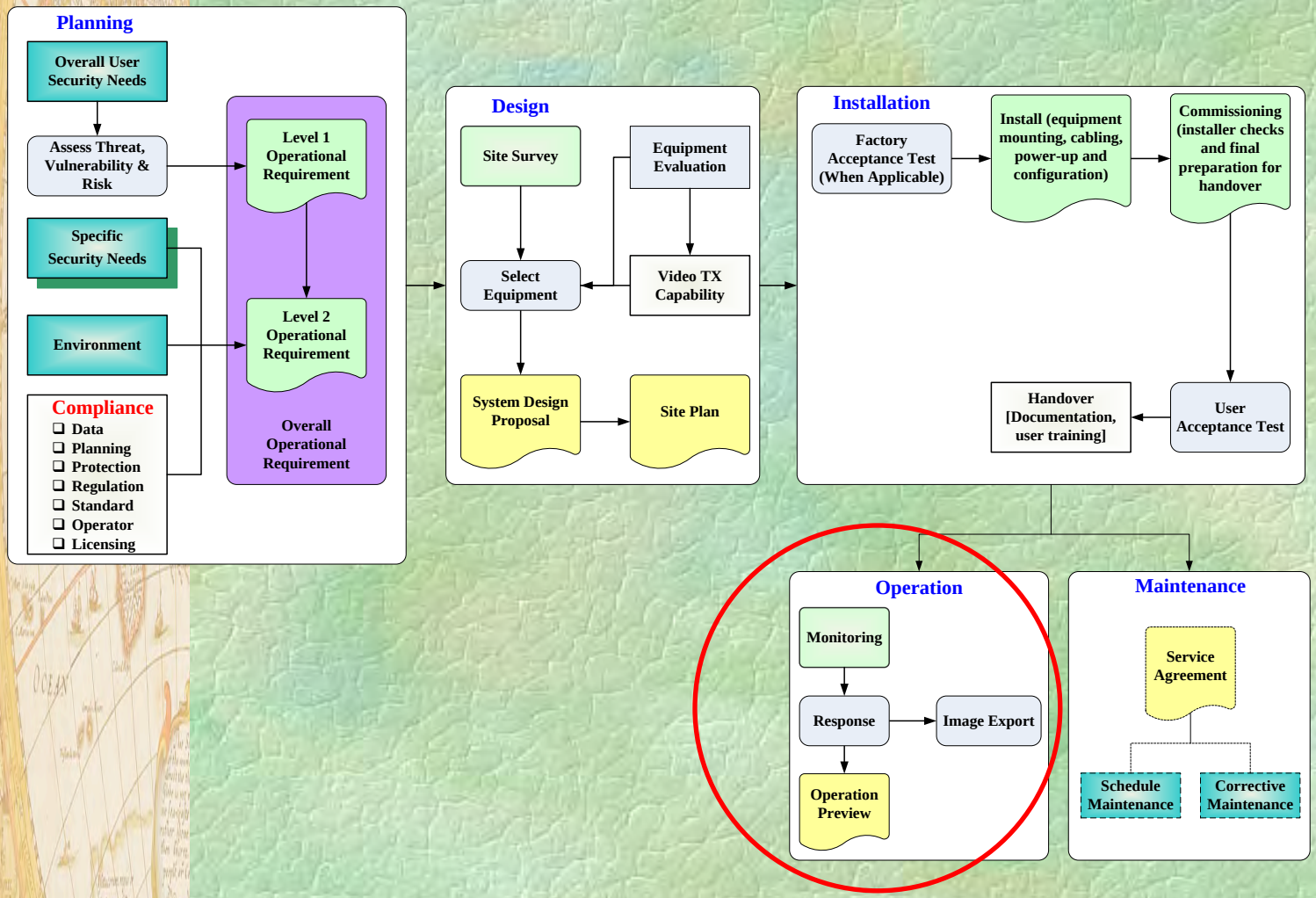
- **Monitor a large area**
- **Detect individuals approaching a building**
- **Observe the actions of a group**
- **Recognize known individuals at an entrance**
- **Obtain images that would enable you (or the police) to identify an unfamiliar individual.**

**A typical fixed camera can be specified to cover a narrow field of view with a high level of detail (for recognition / identification purposes), or a wide field of view at a lower level of detail (for monitoring / detection), but generally not both.**

**Thus it is important to consider carefully which of these requirements is the more appropriate for each location.**

# LIFE CYCLE OF SURVEILLANCE SYSTEM

**Figure 1-3:** Overall Process Flow for Video Surveillance System



# DESIGN OF VSS FOR VIDEO QUALITY

## Video Surveillance Use Cases

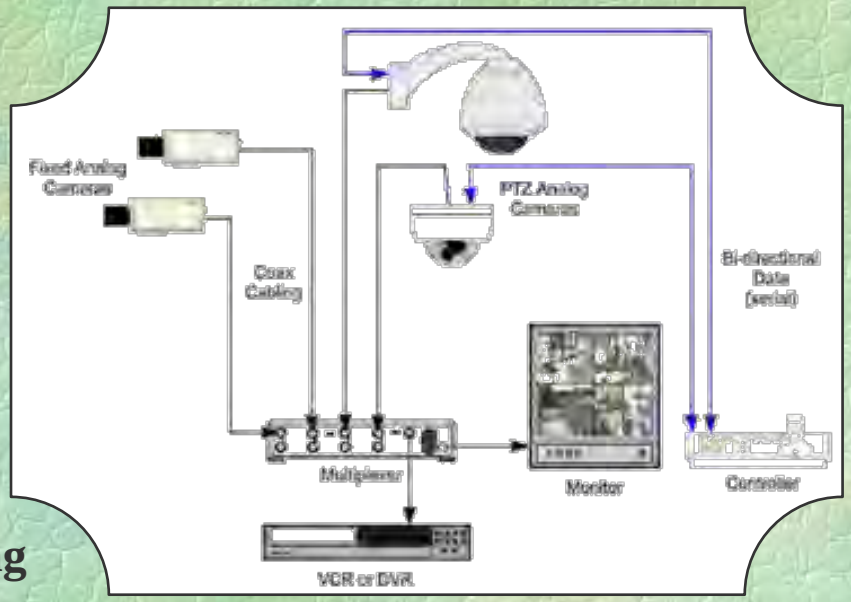
The following is a summary of the most common use cases, followed by the most common function:

**Table 1-1:** Use and Functions of Video Surveillance System

| Use Case | Function |
|---|---|
| First Responders | □ Provide enhanced video mobility through DMC delivered directly to mobile appliances and matched to the display and appliance capability and resources.<br>□ Establish interoperability and convergence between public safety and stakeholders to share information. |
| Urban Surveillance | □ Provide low-light capability for all outdoor public video surveillance devices.<br>□ Provide cameras capable of producing high-resolution video images and adding a video analytics subsystem when required.<br>□ Provide compatibility with fiber optic or wireless transport systems. |
| In-car and Transit Video Surveillance | □ Provide the most usable wide view surveillance products for identification.<br>□ Provide ruggedized, removable digital media for video storage. |
| Public Arenas | □ Provide cameras capable of producing high-resolution video images and adding a video analytics subsystem when required.<br>□ Provide low-light and infrared (IR)-compatible cameras where re- |

# INTRODUCTION CCTV TECHOLOGY APPLICATION

## The Three CCTV Technologies




- **Analogue**
  - 480 – 700TVL Recording
  - Simple to Run and Economical
  - Limited Control and Settings
- **HD-SDI**
  - 1080p
  - Dependent on Cable Quality
  - Easy Upgrade Using Analogue Cabling
  - More Limited Operations in Camera and Recorders
- **IP**
  - Typically 720p to 1080p Recording
  - Unique Camera Options
  - Runs Over Data Networks with Easy Wireless Options
  - Smarter but More Complicated to get the Setup Right
  - High Bandwidth can Give Trouble with Existing Networks

# IP VIDEO SUREVILLANCE COMPONENTS

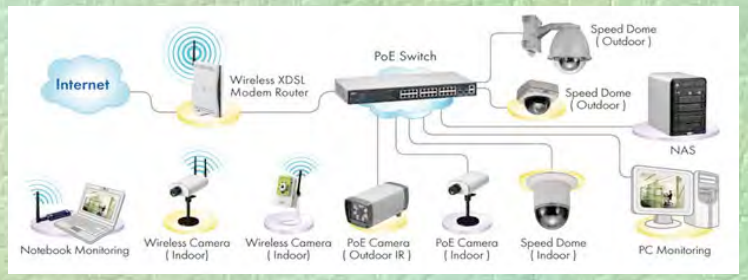
## Network (IP) Video Systems Overview Continued

**Five essential components of IP-based video surveillance solution. These are as follows:**

- **Cameras:** This is the device that capture and image then transmit to a recording device through a network.
- **Video Management Software:** This is a dedicated software required for viewing and monitoring multiple cameras at once. Typically runs one or more standalone servers or on a Video Management and Storage System network module.
- **Servers:** These are devices generally used for supporting or facilitating network digital recording and playback.
- **Storage:** This is used for for archiving and storage of video feeds generated from the IP Surveillance camera.
- **Network:** This component is the system network. The IP Video Surveillance component of the Media Ready Network is integrated within the system architecture to ensure transmission of image captured is delivered to receiving device.

# Design of Video Surveillance Systems for Video Quality

## Figure 1-4: Representative Operational Requirements for System




Input Devices

**Camera**
- No. Camera
- No. Video Stream

**Network Infrastructure**
- LAN Bandwidth 1000 Mbps to 10 Gbps
- Video Feed Running over a Dedicated Connection
- Utilize Multicast Streaming

**Video Management Software**

Should have

**Functionality**
- Video Monitoring
- Recording Setting
- Actual Recording
- Data Service Policies
- Remote Camera Management
- Migration and Replication Capabilities
- Overall Video Surveillance Management
- Menu have online, offline Media Management

**Data Recording**
- Record and Store for Future References and Analysis
- Long Term Retention Needs

**Multi-tiered Storage**

**Output of Reviewing Device**

**Computer | Laptop**
- Appropriate Software Installed
- Communicate with various storage management nodes to facilitate remote monitoring and playback

# DESIGN FOR WIRELESS CONNECTIVITY

## System Architecture Web Based Approach

- Initially the video is captured through the surveillance camera. This video is thus stored in video server.
- In the video server the videos undergo with the video streaming process. The streamed video is then compressed. Then the streamed and the compressed video is stored in the master database.
- All this methods are carried out in the application server. Now at the client side, the user sends the HTTP Request to the application server.
- The application server respond to the client server in the HTTP format that is the videos which are stored in the master database.
- This video is then viewed on the android mobile with the help of an android application.

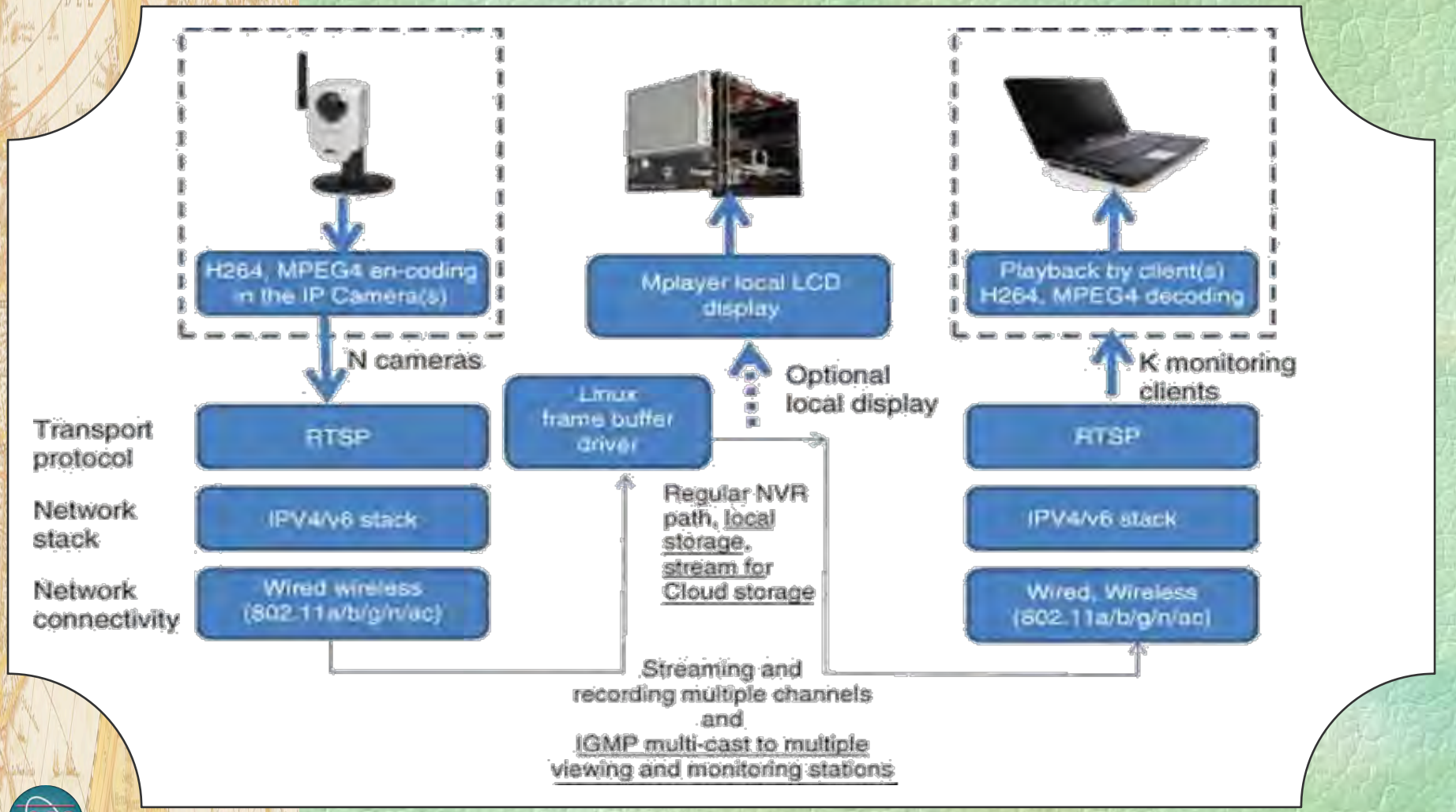
# VIDEO SUREVILLANCE CLASSIFICATION

## Video Surveillance System – Functional Aspects

- Classify Video System by type:
  - Video Surveillance (Monitoring Function)
  - Forensic (Recording Function)
  - Video Analytics
  - Perimeter Security
  - Access Control
- Classify Camera by Function
  - Monitor basic activity (subject is not less than 5% of picture height)
  - Detection (not less than 10% of the picture height)
  - Recognition (Human, Animal or Vehicle) - (50% of screen height)
  - Identification (120% of screen height)

# Design of Video Surveillance Systems for Video Quality

**Figure 1-5:** Video Surveillance and Network Video Recording (NVR) Architecture



# Video Surveillance Procedures & Policies

## Mandatory Requirements Continued

5. Recorded images will be stored in a secure location with access by authorized personnel only.
    - The definition of a "secure" location for purposes of these Guidelines is a room or closet that is always locked with authorized access only by key or, preferably, a card reader.
6. Recorded images will be stored no less than 32 days (90 is recommended) and no more than 365 days, unless retained as part of a criminal investigation or court proceeding (criminal or civil), or other use as approved by the Chief of Police or designee.
7. Quality of the video frame rate, camera placement, type, lighting, lenses, focus, view, and configuration should be designed to provide images of sufficient clarity and resolution to make an identification of individual faces and physical descriptions.

# Video Surveillance Procedures & Policies

## Value and Expectations

- Security systems, including Video Surveillance Systems, are intended to assist in mitigating risk to people, property (including buildings and building assets), and the safety and security of people in the city.
- The systems can provide the following security and safety features:
  - Video Surveillance Systems may serve as a crime deterrent.
  - Once a crime has been committed, the systems may assist in the identification of the responsible parties.
  - Video surveillance of approved locations can provide a date and time stamped video record of the presence of specific people at specific locations, including those who have entered or exited a location.

# Video Surveillance Procedures & Policies

## Respectful Uses of Video Surveillance Systems

- Video Surveillance Systems should not intrude unduly or unreasonably on the privacy interests of individuals.
  - General video surveillance is not permitted unless otherwise detailed in these Guidelines.
    - Covert video surveillance should be used only in rare circumstances for a specific security purpose, such as an investigation or protection of a particular area or activity.
    - In most situations approval is required for any covert video surveillance application.
  - JCF does not use Video Surveillance Systems for the purposes of workplace or workforce monitoring.
  - Do not install Video Surveillance Systems where privacy interests exceed the security value.
  - Do not record sound or speech as part of authorized Video Surveillance Systems.

# Governing Policies

# Video Surveillance Procedures & Policies

## Mandatory Requirements

- **Information obtained through Video Surveillance Systems will be used primarily for security, safety, and law enforcement purposes.**
- **However, JCF reserves the right to use the information for other judicial purposes including but not limited to support of administrative or in a civil suit against person(s) whose activities are shown on the recording and are the basis for the suit.**

1. **Video monitoring and recording for security purposes will be conducted in a professional, ethical, and legal manner.**
    - **Violations of the procedures for video monitoring referenced in this policy will result in disciplinary action consistent with the rules and regulations governing JDF superintendents.**

# Video Surveillance Procedures & Policies

## Mandatory Requirements

2. **Managers of Video Surveillance Systems will identify a Video Surveillance System administrator who will monitor and record based on suspicious activity or behavior and not individual characteristics.**
   - **Video Surveillance System administrators will monitor and record in a manner consistent with all JCF policies, including the Non-Discrimination Policy, the Sexual Harassment Policy, and other relevant policies.**
   - **Camera control operators will not monitor and record individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by JCF Non-Discrimination Policies.**

# Video Surveillance Procedures & Policies

## Mandatory Requirements

3. Camera control operators such as administrators, managers, and/or other individuals with authorization to operate Video Surveillance Systems will not seek out or continuously view or record people being intimate in public areas.
4. Cameras may be permanently mounted or operated from a remote location or by an automated device.

   The following signage is required at locations where cameras are in use and must be conspicuous.

   - Cameras in Use – Not a Guarantee of Safety or Security
   - Cameras In Use
   - Cameras In Use On These Premises

# Video Surveillance Procedures & Policies

## Mandatory Requirements Continued

5. Recorded images will be stored in a secure location with access by authorized personnel only.
    - The definition of a "secure" location for purposes of these Guidelines is a room or closet that is always locked with authorized access only by key or, preferably, a card reader.
6. Recorded images will be stored no less than 32 days (90 is recommended) and no more than 365 days, unless retained as part of a criminal investigation or court proceeding (criminal or civil), or other use as approved by the Chief of Police or designee.
7. Quality of the video frame rate, camera placement, type, lighting, lenses, focus, view, and configuration should be designed to provide images of sufficient clarity and resolution to make an identification of individual faces and physical descriptions.

# Video Surveillance Procedures & Policies

## Mandatory Requirements Continued

8. Installation of Video Surveillance Systems is the financial responsibility of the Ministry of Security and/or authorized individuals.
9. This responsibility includes, but is not limited to, the cost of the system design, consultant fees, labor, installation, procurement of and connection to service, repairs, and maintenance.
10. Fees are subject to approval by the JCF recharge process.

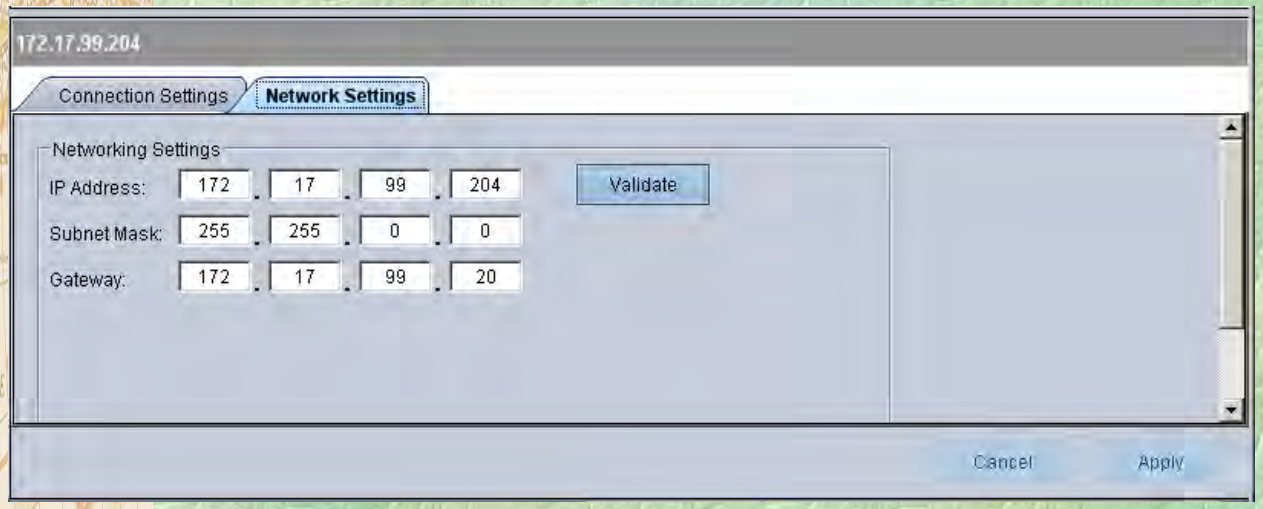
# VIDEO SURVEILLANCE ADMINISTRATION

## Specifying Network Settings

The fields displayed on the Network Settings tab vary according to whether you select a single device or multiple devices in the Device Discovery browser.

▸ **To view and configure the parameters on the Network Settings tab:**

1. In Nextiva Control Center, click **Device Discovery**.
2. Select one or more devices in the Device Discovery Browser.
3. Select the **Network Settings** tab.




If a single device is selected in the Device Discovery Browser, the Network Settings tab displays network settings and device specific properties.

4. Do one of the following:

■ If a single device is selected, edit the IP address, Subnet Mask, Gateway, and Host Name, as required. ■ If multiple devices are selected, enter an IP address range, Subnet Mask, and Gateway, as required.

5. Click **Validate** to ensure that the settings are valid.
6. Click **Apply**.

# PROVISIONING FOR REQUIREMENTS

## Planning to Meet Needs

When planning for VSS the designer must plan for the delegation and administration tasks and consider how he/she wants to define, implement and verify operational requirements.

- Provisioning provides initial specification and details required to ensure operational requirements can be met following installation, configuration, and commissioning.
- Provisioning is the process of determining the range and depth of repair parts that will be needed for the video surveillance system.
- This process ensures smart planning, accurate identification of provisioning item consistent with relevant user maintenance tasks, selected item, taking accounts of deadlines and provisions of consumed or failed items.

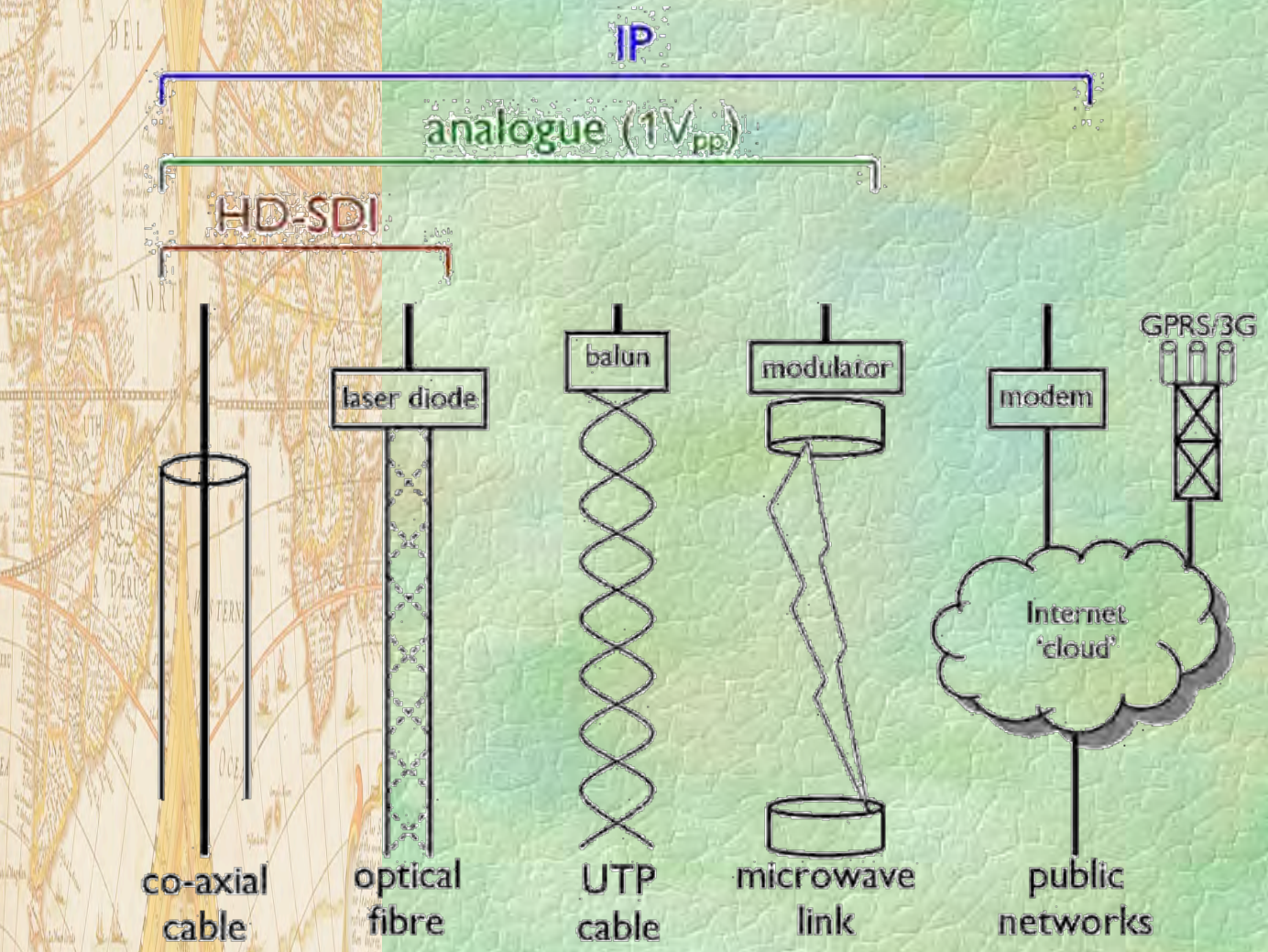
# SUREVILLANCE VIDEO TRANSMISSION

## Key Facts About Transmission

- The technology used for transmitting the video signal from one location to another is a key component of any IP Video Surveillance system.
- There is an increasing array of options available, moving away from the traditional standard analog coaxial cable solution, and so more thought now needs to be given to the choice of transmission method.
- The most significant advance in recent years has been the development of IP based transmission.
- This is an approach for transmitting any digitized data in a robust and manageable way over a variety of link types.
- Its use in the IP Video Surveillance field has grown and often results in new approaches to solving problems.
- As with any system design it is important that the system designer understands the implications of choosing one method over another.

# SUREVILLANCE VIDEO TRANSMISSION

**Figure 1-6:** CCTV Transmission Options




**Send pictures to their destination: or 'Signal Transmission'**

**Video output from the camera could be:**

- **Composite analog signal (1 volt peak-to-peak, CCIR, PAL)**
- **IP video (Internet Protocol) as TCP/IP or UDP multicast**
- **HD-SDI, High Definition – Serial Digital Interface.**

# SUREVILLANCE VIDEO TRANSMISSION

## Video Signal Type

- Video can be transmitted and consumed either as an analog or digital feed.
- Each video type can be converted to the other; however any conversions should be kept down to an absolute minimum to preserve video quality throughout the whole system.
- The benefits of using analog transmission are primarily that the technology was previously widely understood and widely deployed.
- As each video link has its own physical connection, fault finding is relatively simple.
- This video signal is mono-directional (simplex). This is a broadcasted approach, meaning that the video source is unaware of the status of any connected equipment.

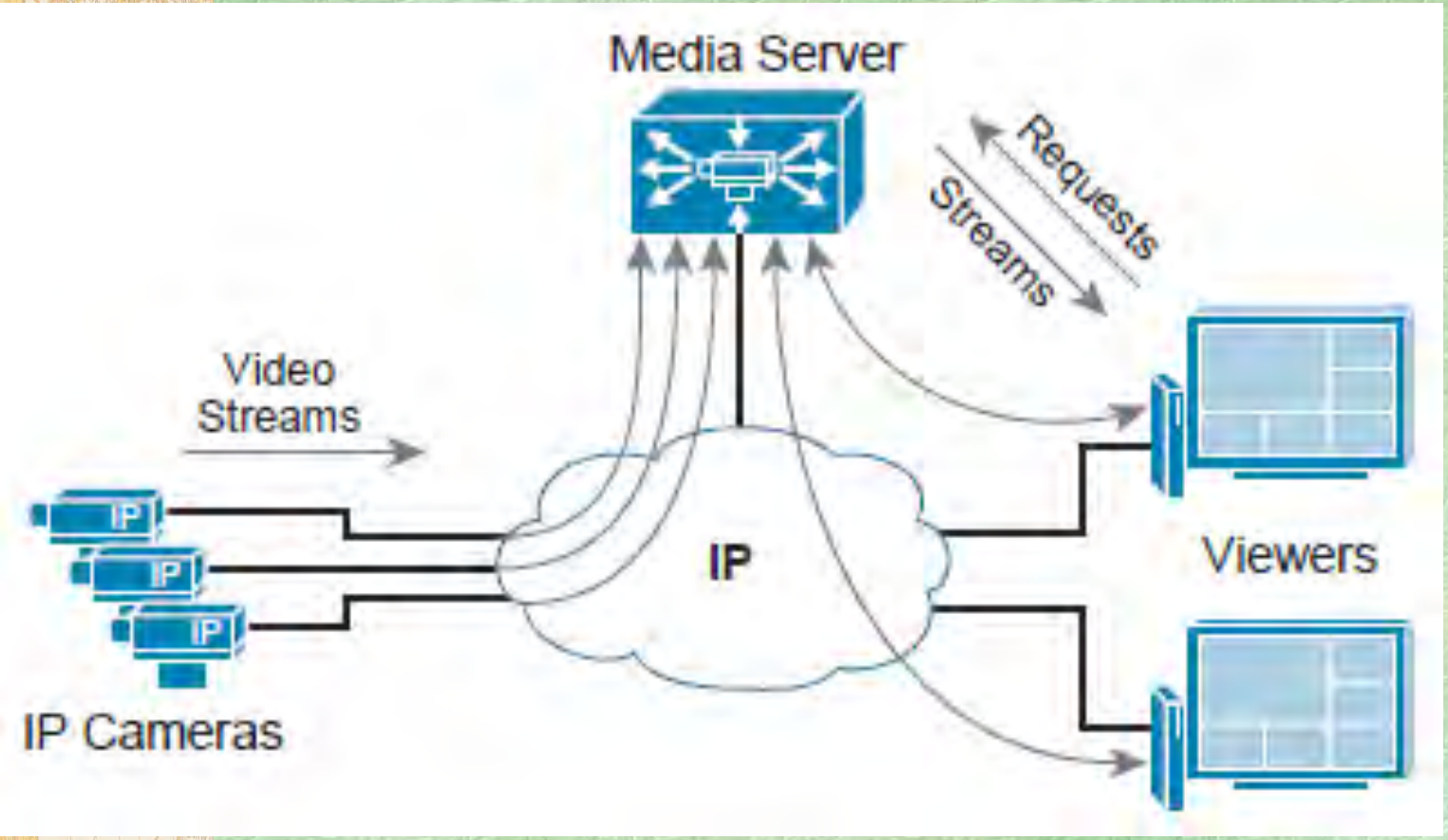
# SUREVILLANCE VIDEO TRANSMISSION

## Transmission Issues

- Wireless technology increasingly offers a more cost effective solution and should be seen as an alternative to other transmission links in suitable circumstances rather than a full replacement of another (e.g. fibre optics).
- There are technical issues that can affect performance necessary to meet the operational requirement of a camera.
- To aid understanding, a simple and brief explanation of these issues is outlined below:
- **Wireless Transmission**
  - Uses a transmitter and receiver principle. Any break in the transmission path or medium leads to an immediate loss of signal and image.
  - Most wireless devices operate on the free, un-licensed 2.4 GHz frequency band. This open band is shared with many other systems.
  - This can cause ‘congested interference in densely populated areas. Licensed frequencies cost but limit ‘congestion’ to the control of the owner.

# VIDEO SUREVILLANCE principle of Operation

**Figure 1-7:** Media Server Application




For archive viewing, the Media Server receives video from the IP camera or encoder continuously (as configured per the archive settings) and only sends video streams to the viewer when requested.

# SYSTEM DESIGNER'S RESPONSIBILITIES

**Table 1-2:** Representative Design Check List

| Design Checklist |
|---|
| Estimate the number of IP cameras required at each location. |
| Using a floor plan or exterior survey, determine cameras that can be powered by PoE and those requiring power supplies. |
| Survey existing IP or analog cameras and determine if these cameras are to be replace or migrated. |
| Estimate the CODEC, resolution, and frame rate or bit rate requirements for cameras at each location |
| Determine the retention period requirements for cameras at each location |
| Survey existing LAN switches for necessary features and available capacity |
| Based on the number of cameras per location, determine server requirements. |
| Using the *Campus Implementation Case Study* in the following section, determine what if any LAN infrastructure upgrades are required. |
| Using the estimate on the number of servers required, calculate the storage requirements for video archives based on the retention period analysis |

**This design checklist in Table 1-2 facilitates pre-implementation planning and the decision process.**

# SUVEILLANCE VIDEO MANAGEMENT

## Video Management System

- Video management systems are the hub of video surveillance solutions, accepting video from cameras, storing the video and managing distribution of video to viewers.
- There are *4 fundamental options* in video management systems. Most organizations choose 1 of the 4
- DVRs are purpose built computers that combine software, hardware and video storage all in one. By definition, they only accept analog camera feeds. Almost all DVRs today support remote viewing over the Internet.
- HDVRs or hybrid DVRs are DVRs that support IP cameras. They have all the functionality of a DVR listed above plus they add support for IP and megapixel cameras. Most DVRs can be software upgraded to become HDVRs.

# SUVEILLANCE VIDEO MANAGEMENT

## Video Management System

### NVRs

- These are like DVRs in all ways except for camera support. Whereas a DVR only supports analog cameras, an NVR only supports IP cameras.
- To support analog cameras with an NVR, an encoder must be used.

### Video Management Software (VMS)

- This is a software application, like Word or Excel. Unlike DVRs or NVRs, VMS Software does not come with any hardware or storage.
- The user must load and set up the PC/Server for the software. This provides much greater freedom and potentially lower cost than using DVR/NVR appliances.
- However, it comes with more complexity and time to set up and optimize the system.

# SUVEILLANCE VIDEO MANAGEMENT

## Video Management System and Software Explained

- An effective video management system is, essentially, the efficient combination of video software and server hardware.
- There are some important factors to consider when selecting video/security management software.
  - Architecture — An NVR solution, with a number of computer workstations, requires standalone software at each station.
    - Typically, there is a separate configuration between the NVR and each workstation.
    - Modern video management systems use server-client architecture that constantly communicates, which leads to greater flexibility and scalability, and simpler configuration.

# POTENTIAL IP SURVEILLANCE SYSTEM COSTS

**The initial cost is high, including high cost hardware/software, and installation.**

**The ongoing costs typically include: an annual maintenance fee and costs associated with times in table 1-3.**

**Table 1-3: Maintenance Costs that Could be Incurred**

| Item | Ongoing System Operating Costs | | |
|---|---|---|---|
| 1 | Space | System Configuration | Multi-site integration |
| 2 | Power | OS security patches | Central management |
| 3 | Redundancy | Tampering repairs | PC client SW install/upgrades |
| 4 | IT staff time | Router configuration | Training staff for retrieval |
| 5 | Mobile apps | Remote network access | Operating System backup |
| 6 | Video backup | SW update installation | Cyber security expertise & support |

# BEST PERFORMANCE REQUIRES MANAGEMENT

## Video Asset Management

- An IP-based network infrastructure for a video surveillance system has the following advantages:
  - High reliability
  - High system availability
  - Multi-vendor best-in-class solution support
  - Guaranteed Quality of Service (QoS)
  - Secured transmissions
  - Secure mobility
  - Ease of management
  - Reduced operation costs

- Proper network configuration and tuning has cost considerations that must be accounted for.
- Working with static or dynamic IP addresses, VPNs, firewall rules, and other network management tools add to the cost of implementation and, to a degree, on-going maintenance.

# IP Camera

# Camera Selection for Surveillance System

**You cannot just judge a camera by its looks!**

**All you need to know to select camera:**

- ❑ Lens – Fixed or Varifocal
- ❑ Resolution and Compression
- ❑ WDR – Wide Dynamic Range
- ❑ Day/Night and Indoor/Outdoor

# Camera Selection for Surveillance System

## IP Camera Features and Design Consideration

### Imaging

- ❑ WDR
- ❑ Lenses
- ❑ Exposure
- ❑ Resolution
- ❑ Lux Rating
- ❑ Frame Rate
- ❑ Field of View
- ❑ Day | Night | IR

### IP Camera Environment

- ❑ Form Factors
- ❑ Weather Proofing
- ❑ Temperature Range
- ❑ Cable Management
- ❑ Weatherproof Rating

# Camera Selection for Surveillance System

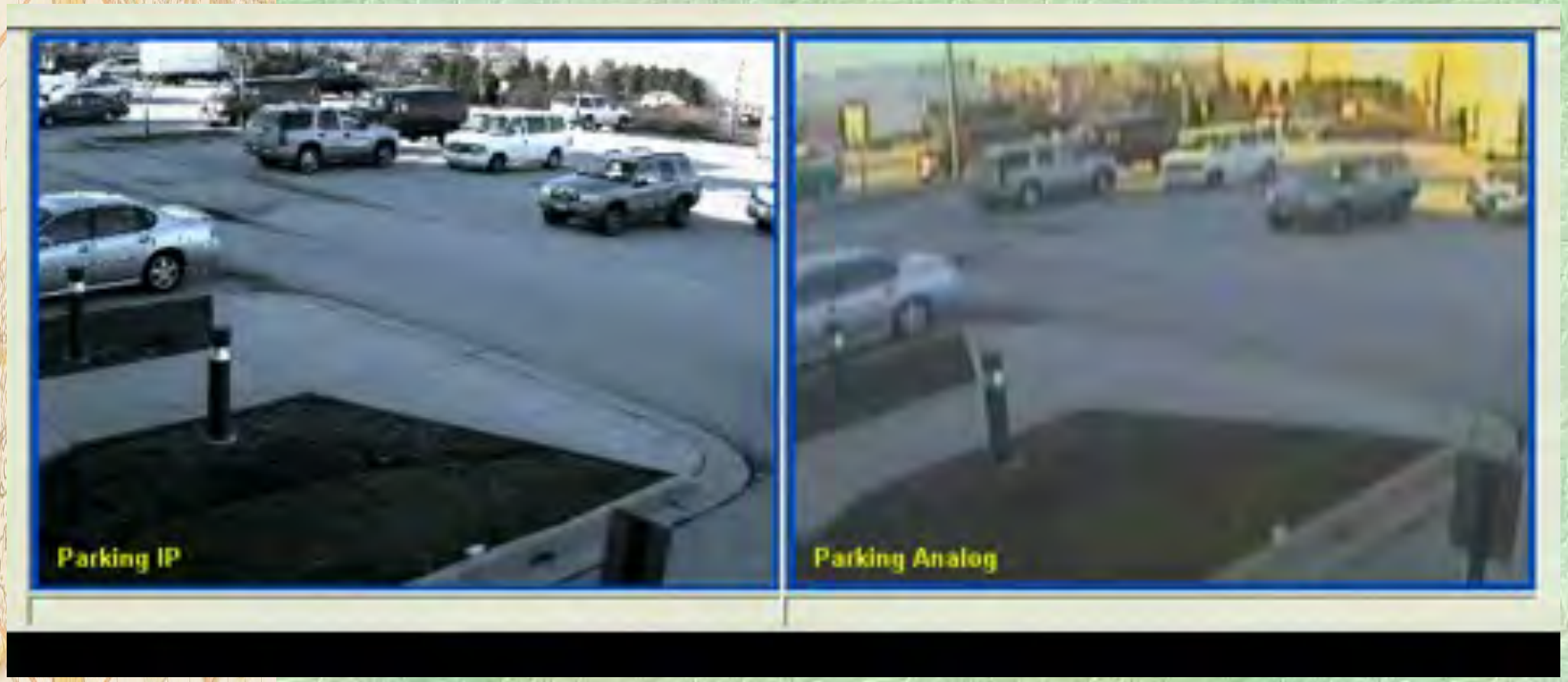
## Which Should I Choose?

**Table 1-4:** Factors to Consider When Deciding to Install Camera

| Important Questions | Solution | Rationale for Choice |
|---|---|---|
| Do You Have Coax? | Analogue | ✓ Cheapest |
|  | AHD | ✓ Economy 1080P |
| | HD-SDI | ✓ Best Image Quality |
| | HD-CVI | ✓ HMM…… |
| | HD-TVI | ✓ Wide Adoption, Many Manufactures |
| | | |
| Do You Have Data Cabling? | IP | ✓ Most Options |

# Camera Selection for Surveillance System

**Figure 1-8:** Comparing Image Quality - Analogue vs. IP - Differences



# CAMERA DESIGN CONSIDERATION

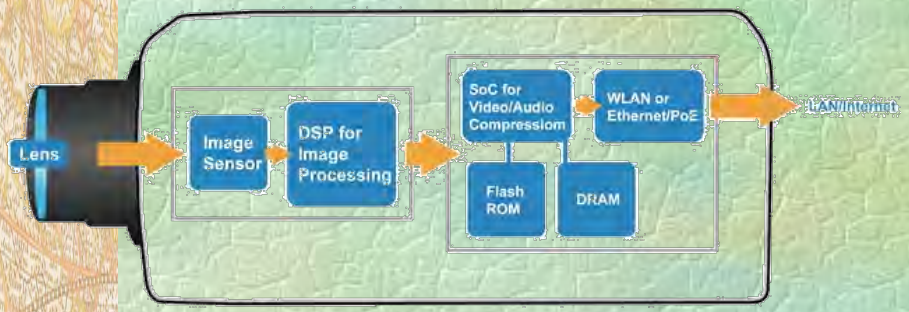
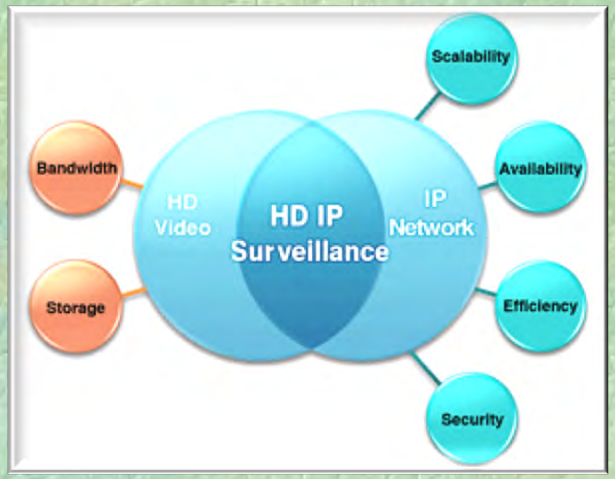



**Table1-5:** Camera Design Considerations

| Wiring | Design | Night Applications |
|---|---|---|
| PoE Switch |  | Distance |
| Cat5 for IP or Balun System | | Reflected Light |
| Coax [RG59] and 2 Conductors |  | |
| Wireless (requires power at the camera) | | What is the available Light?<br>❑ Total Darkness = 0 Lux required with IR illuminators |

# CAMERA DESIGN CONSIDERATION

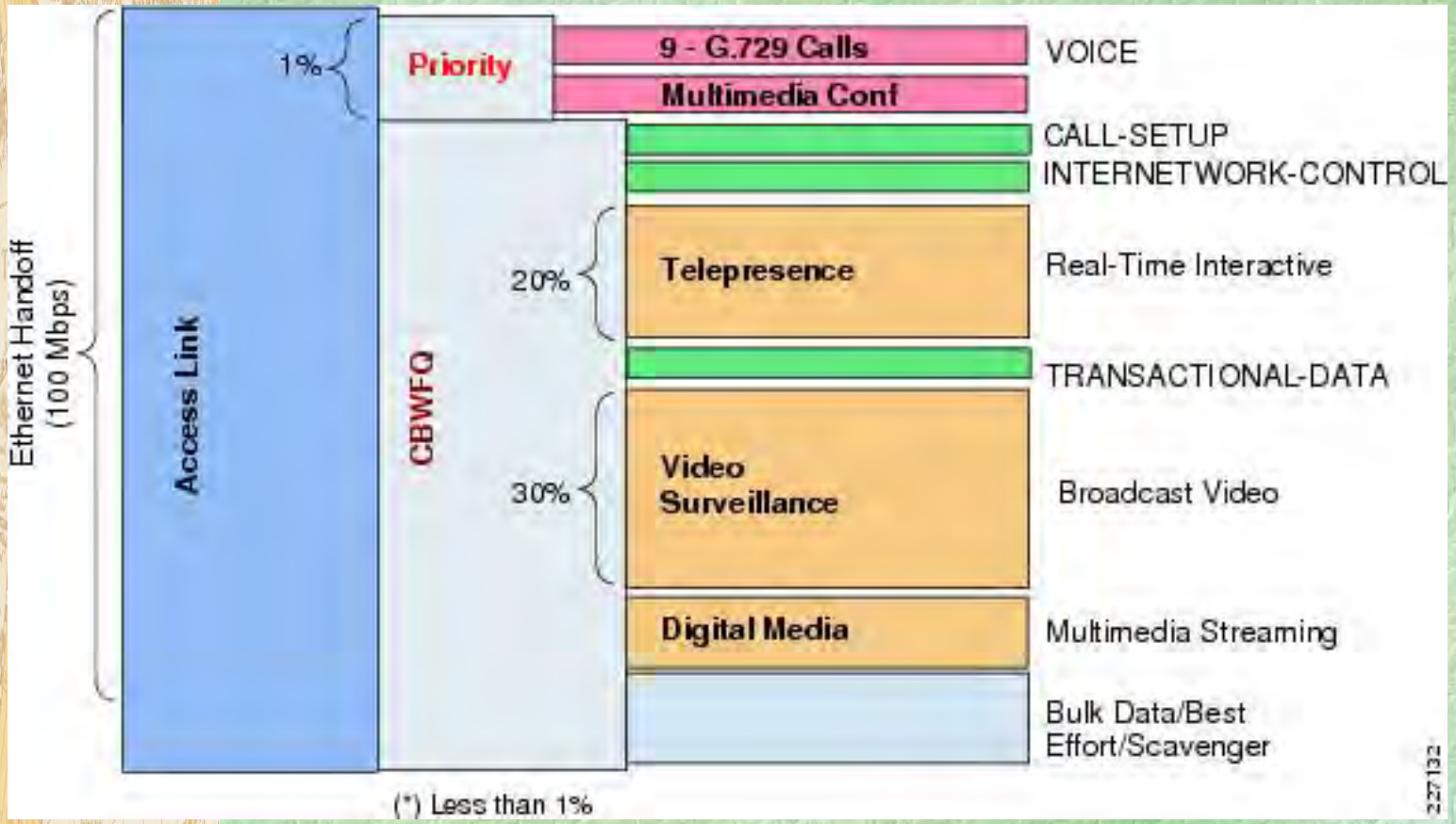
## Network Bandwidth




- The amount of bandwidth used by a network camera is determined by several factors:
  - Resolution
  - Frame Rate
  - Compression

# CAMERA DESIGN CONSIDERATION

**Figure 1-9:** Bandwidth Allocation to Provision Various Videos - 009




**Source: Cisco IP Surveillance Design Guide**

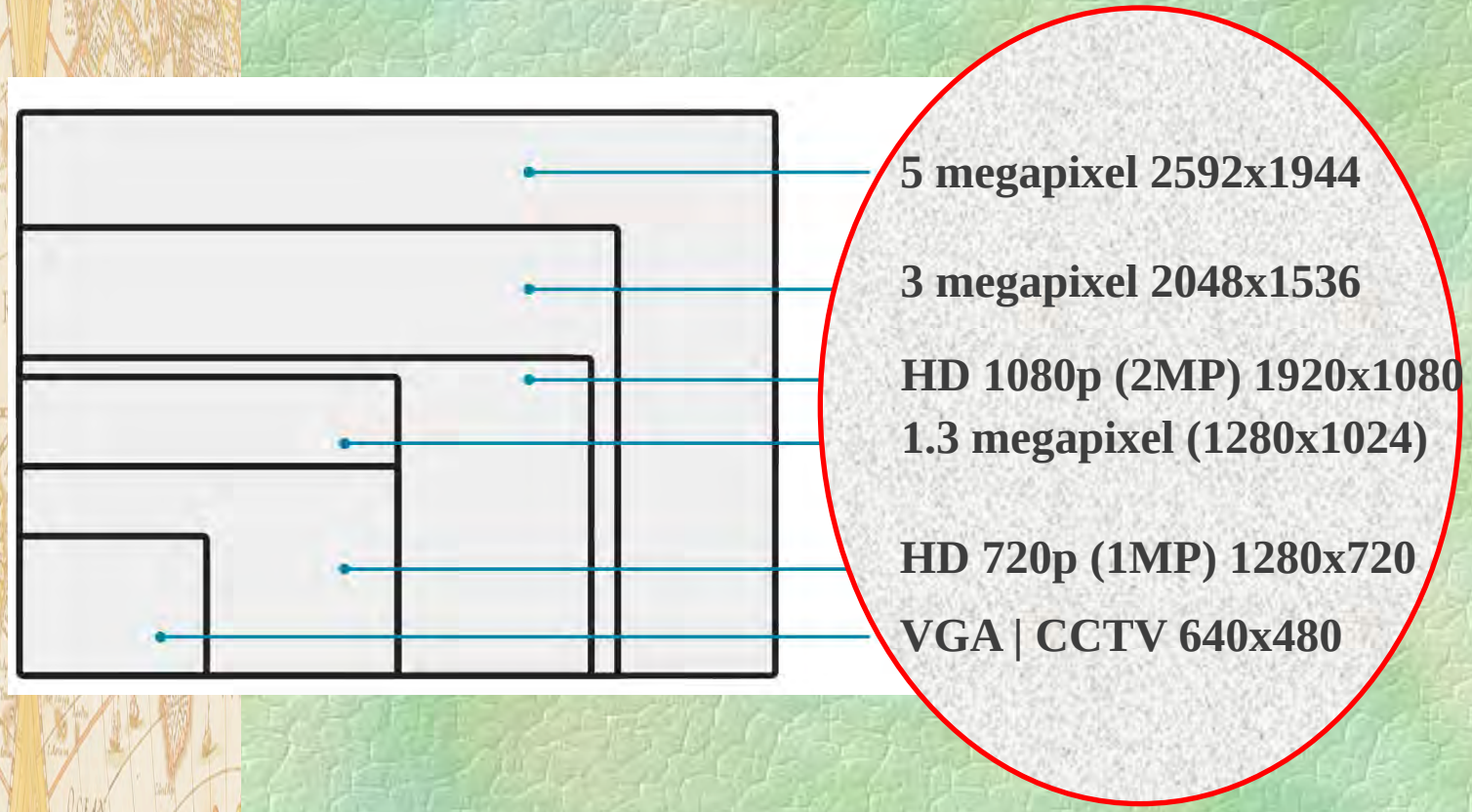
# CAMERA SPECIFICATION - RESOLUTION

## What is Resolution?

**A camera's resolution is the number of pixels on the image sensor, measured horizontally by vertically.**

# CAMERA SPECIFICATION - RESOLUTION

**Figure 1-10:** Pixel Resolution




**A Full HD 2-Megapixel camera has a resolution of 1920 pixels wide by 1080 pixels high. If you multiply 1920 x 1080, the result is the image resolution, in this case, 2,073,600 pixels or 2 megapixels.**

# LENS USED WITH DIFFERENT CAMERAS

**Figure 1-11:** Imaging | Types of Lenses


**Lens Types: Fixed and variable focal length, manual and motorized zoom.**

# FACTORS INFLUENCING CAMERA IMAGE

## What can the camera see?

- **Depends on:**
  - **Lighting conditions**
  - **Resolution of CCD**
  - **Settings and features of the camera**
  - **Distance to and size of the objects you want to see.**

# COMPARING CAMERA SPECIFICATIONS

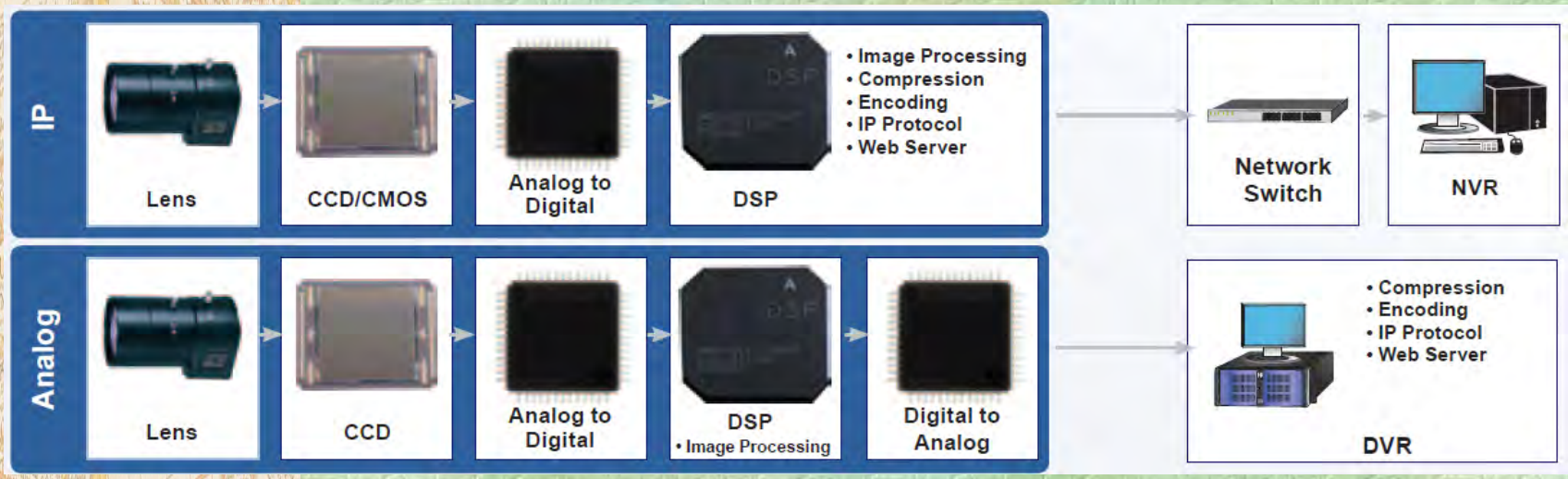
## Table 1-6: Specifications for Three Cameras



| No. | Specifications | AXIS P3354 | AXIS P5624-E Mk ll | AXIS D55 3 MP |
|---|---|---|---|---|
| 1 | Lens | 6 mm: 3.5 – 6 mm/F1.2 | 6 mm: 4.3 – 98.9 mm/F1.6 – F4.7 | 3.6 mm Fixed |
| 2 | Sensor Size | 1/3” progressive scan CMOS | 1/2.8” progressive scan CMOS | 1/3.2” progressive scan CMOS |
| 3 | Day \| Night | Automatic | Automatic | Yes |
| 4 | Resolution [pixels] | 1280 x 960 [1.3 MP] | 1280 x 720 [HDTV 720] | 1080 TVL |
| 5 | Frames per second | 30 [1280 x 960] | 50/60 fps in all resolutions | 30 fps |
| 6 | WDR | Yes | Yes | No |
| 7 | Indoor - Outdoor | Indoor | Outdoor Ready | Indoor |
| 8 | Security | Multi-level password \| HTTPS encryption | Multi-level password \| HTTPS encryption | – |
| 9 | Video Compression | Motion JPEG, H.264 | Motion JPEG, H.264 | Motion MJPEG, H.264 |
| 10 | Pan \| Tilt \| Zoom | No | Yes | No |
| 11 | Intelligent Video | Motion Detection | Motion Detection | Motion Detection |
| 12 | Power | PoE IEEE 802.3af Class 2 | PoE + IEEE 802.3af Class 2 | PoE IEEE 802.3af Class 2 |

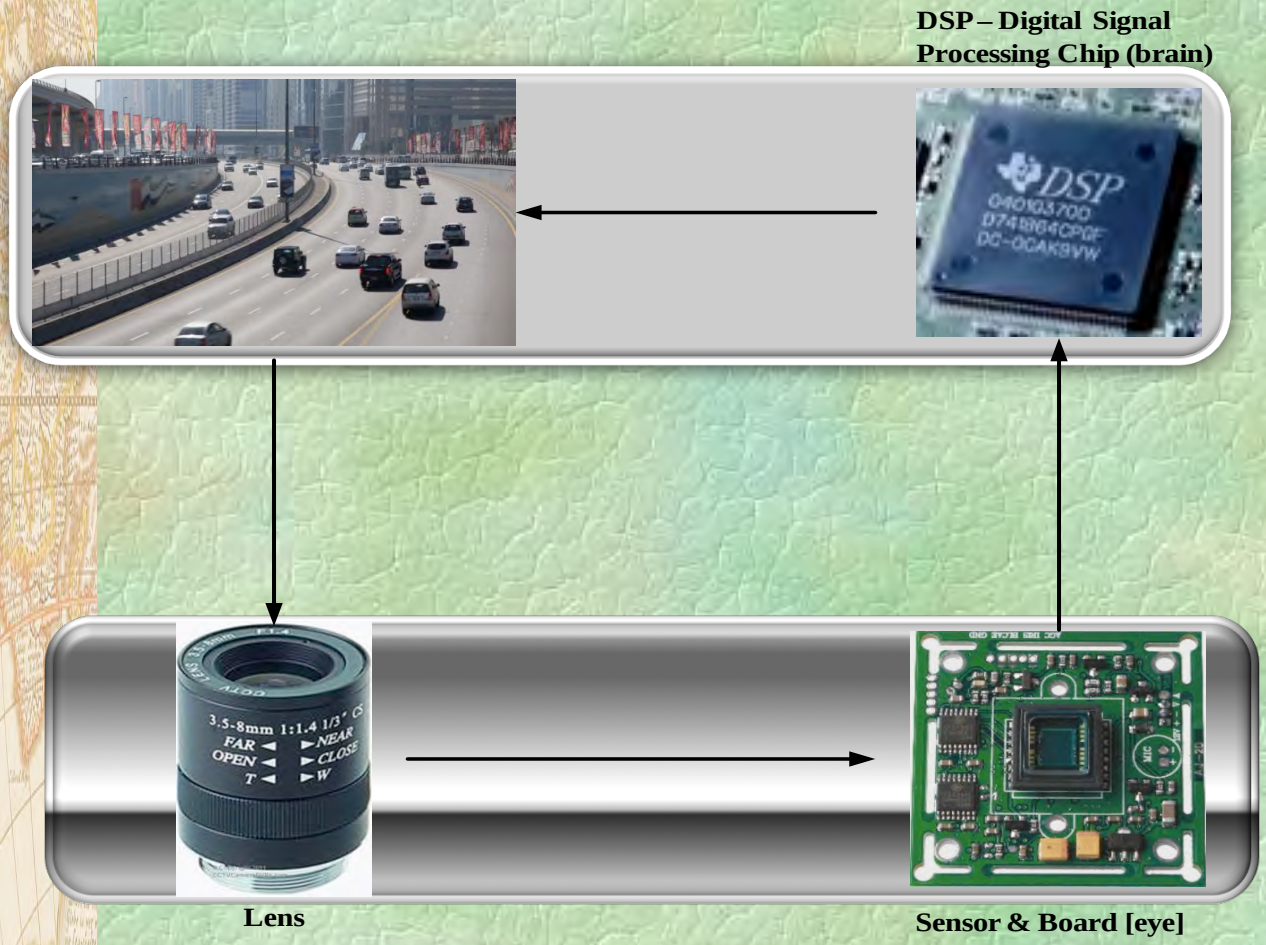
# HOW THE CAMERA WORKS

**Figure 1-12:** Comparing Camera Functionality



# CONSTITUENTS OF A CAMERA

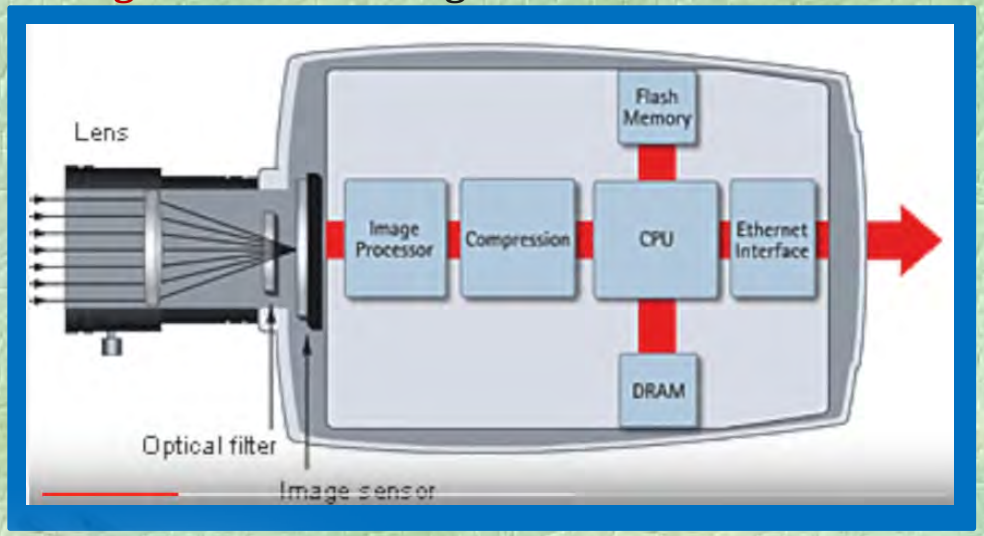
**Figure 1-13:** Camera's Internal Organs



# Digital Signal Processor [Brain]

- Features can include:
  - Motion detection
  - Analysis of footage
  - Controls and menus
  - Wide Dynamic Range (WDR)
  - Compression and video conversion
  - And many more capabilities…..

**Figure 1-14:** Building Blocks of an IP Camera




# COMPARING IMAGE QUALITY

**Figure 1-15:** CCD and CMOS Camera Lens Comparison


# Defining Camera Field of View

## Field of View (FoV)

- Also referred to as the angle of view or angle of coverage, the FoV is the amount of a given scene captured by the camera.
- Three elements decide the FoV; the lens and sensor element within the camera and where this unit is positioned in relation to the scene.
- Note that a large FoV generally results in any target object being relatively small in comparison to that shown by a camera with a small FoV.
- When determining the FoV required of a camera avoid problem areas such as shadows and blind spots, and care should also be taken not to record areas outside the remit of the installation.

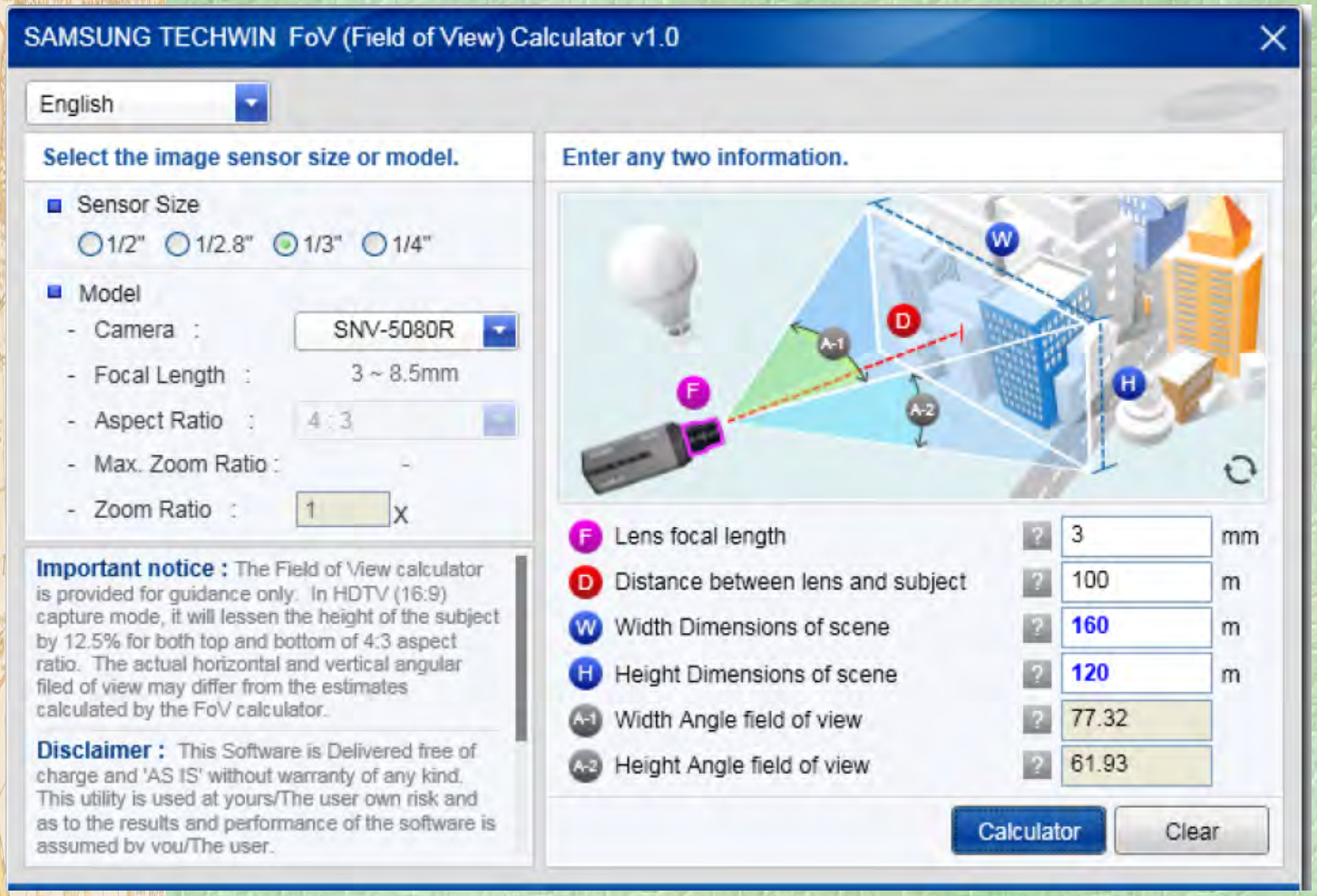
# SENSOR USED IN VIDEO CAMERA

## Sensor

- The sensor is the device that actually ‘records’ the scene view, with current cameras having either CCD (charge coupled device) or CMOS (complimentary metal-oxide-semiconductor) sensors.
- Sensors have both different sizes, which can change the field of view, and different pixel densities which affect the resolution.
- The lens in *combination with the camera sensor* dictates the field of view produced by the system which ranges from wide angle to telephoto.
- In Varifocal: lens size can be changed during the installation process and Zoom in and Zoom out is possible.
- Common sizes available are:
  - 2.5mm~8mm
  - 3.0mm~12mm
  - 5.0mm~50mm

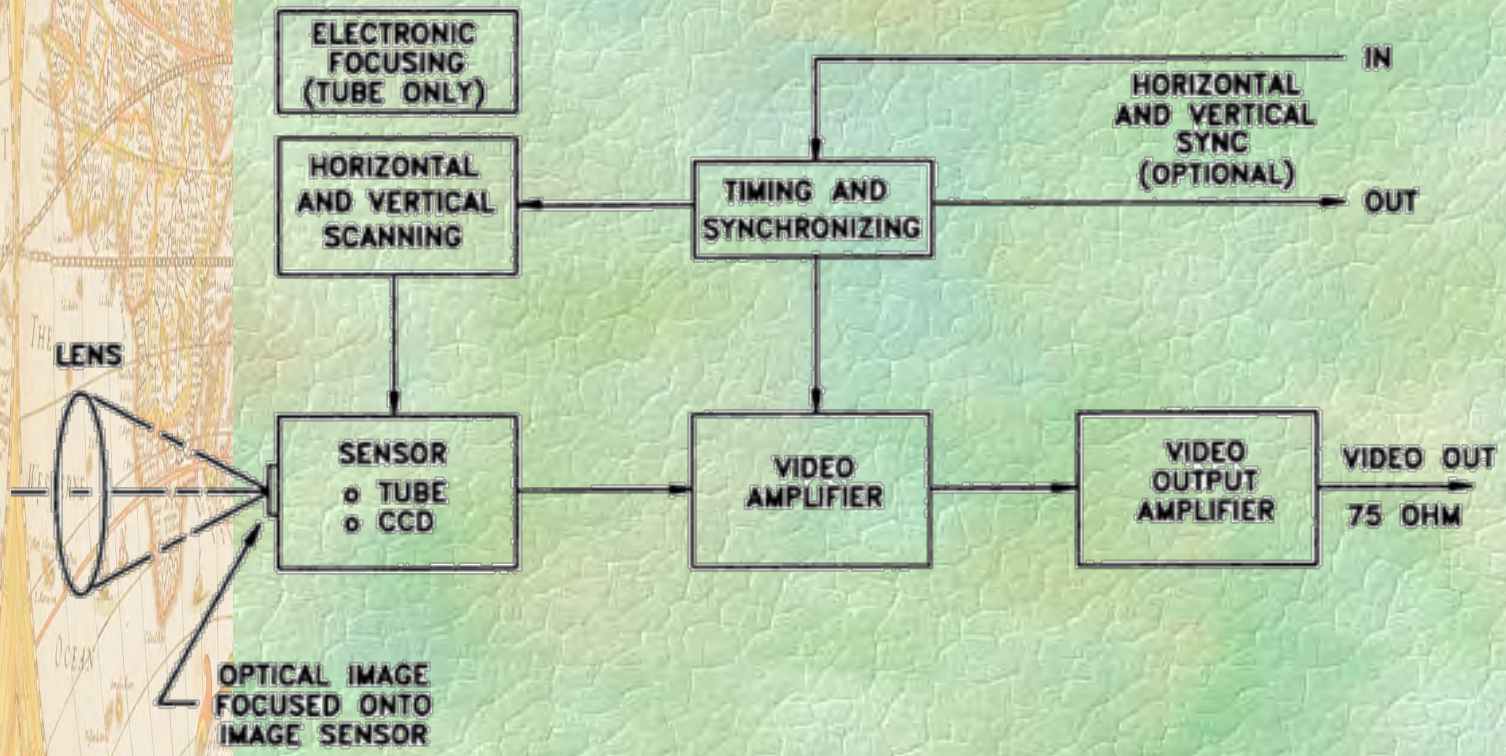
# IMAGING | Lens | field of view

**Figure 1-16:** Samsung Field of View Calculator



# EARLIER REPRESENTATION OF CAMERA

**Figure1-17:** CCTV Camera Block Diagram



# Environment | Weathering Rating

- Outdoor cameras should be rated for water and dust ingression.
- Generally outdoor cameras should have at least and IP66 rating.

# IP CAMERA INFRASTRUCTURE CONNECTIVITY

**Figure 1-18:** Methods of Connecting an IP Camera

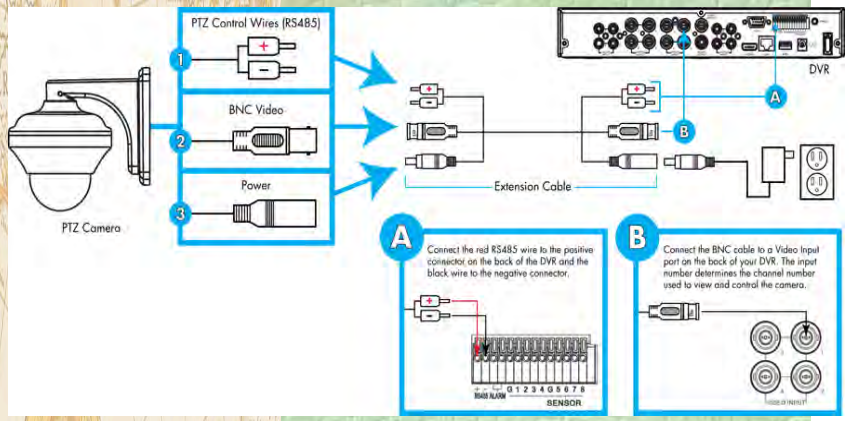
# METHODS OF INTEGRATING IP CAMERA

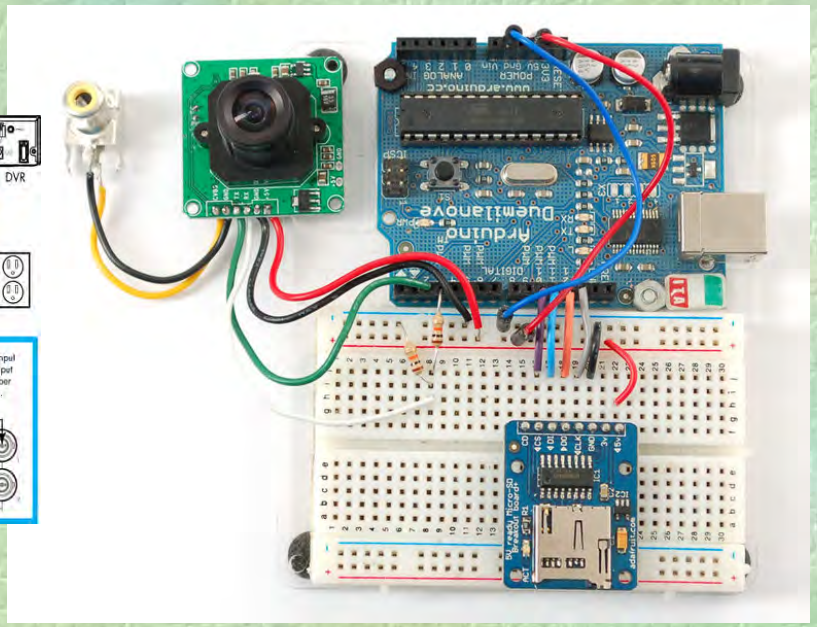
## 3 Ways to Integrate IP Camera

- Drivers.
- R.T.S.P.
- MJPEG.
- T.A.B

### Drivers.

- Specific communication protocol for specific platforms can be written by the manufacturer or installer designed to perform specific functions.

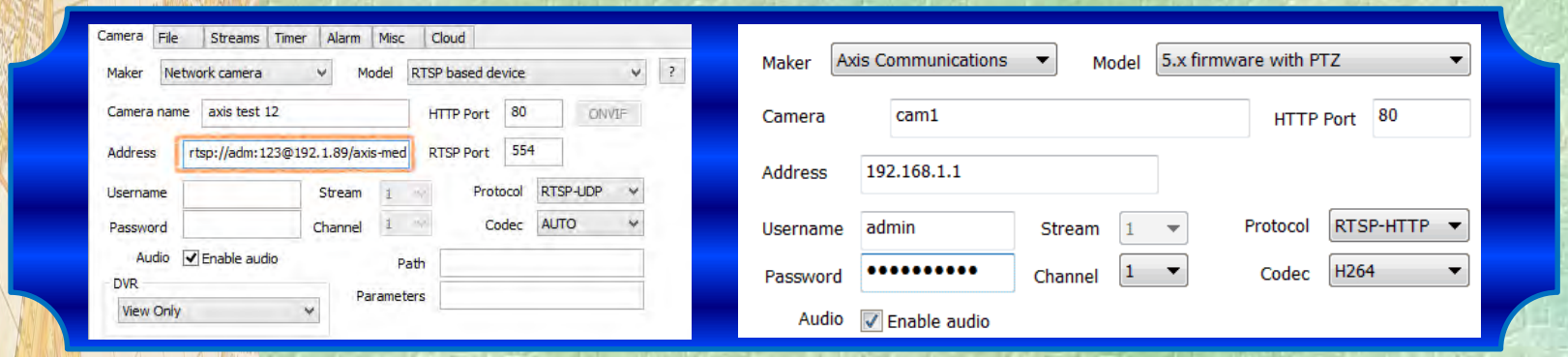


# REAL TIME STREAMING PROTOCOL

## RTSP Stream

***RTSP*** **uses a combination of reliable transmission over** ***TCP*** **(used for control) and best-efforts delivery over** ***UDP*** **(used for content) to stream content to users.**



# IMAGING | LUX RATING

- Sunny Day: 10,000+ Lux
- Overcast Day: 1000 Lux
- Office Lighting: 50 – 400 Lux
- Home Lighting: 25 – 100 Lux
- Parking Lot at Night: 0.5 – 10 Lux
- Full Moon: 0.25 – 1 Lux

# Assessing Image Quality

# Characteristics of Image Quality

## Image Quality

- Human visual perception of an image is hard to quantify, but there are some simple measures that can be taken to ensure that the image quality is optimized for whatever activity is being monitored.
- Consider four areas when determining the required image quality:
  - **Clarity** – Is the picture sharp enough, and is there any lens distortion? Ensure that the lens or lens / camera combination is of sufficient quality for the task in hand.
  - **Detail** – Is there enough to identify objects? Check that image quality is not compromised by trying to achieve a large FoV at the cost of image detail, and that lighting levels permit a useable depth of focus. If necessary break the scene into smaller sections.
  - **Color** – Is it natural? Is it necessary? If accurate color reproduction is important then ensure the lighting is of sufficient quality and quantity to allow the cameras to achieve this.
  - **Artefacts** – Are there elements in the image that should not be there? And if so are they obtrusive? If this is the case then depending on the artefact, either the amount of compression needs to reduced or the camera/lighting placement needs to be addressed.

# Fundamentals of Video Quality

**Figure 1-19:** Use Case

# VIDEO IMAGE QUALITY

## Poor Image Quality

- **The primary causes of poor image quality in most digital video surveillance systems are:**
  - **Low Resolution:** Only 25% of the resolution of a CCTV camera image is recorded.
  - **Excessive Quantization:** Each frame recorded is compressed too much, losing clarity.
  - **Low Frame Rate:** Only 25% or less of the frames per second from each camera are recorded, reducing the chance to detect even the face of human whether there is a man or a woman.

**Figure 1-20: Effects of Pixels-on-Target on Image Quality**

8 Pixels 64 Pixels

# WIDE DYNAMIC RANGE IMAGE REPRESENTATION

**Figure 1-21:** Illustration of Imaging | WDR Application

# WIDE DYNAMIC RANGE IMAGE REPRESENTATION

**Figure 22 Representation of Imaging | WDR Application**

# CAMERA NETWORK SECURITY - 1

## Network Security

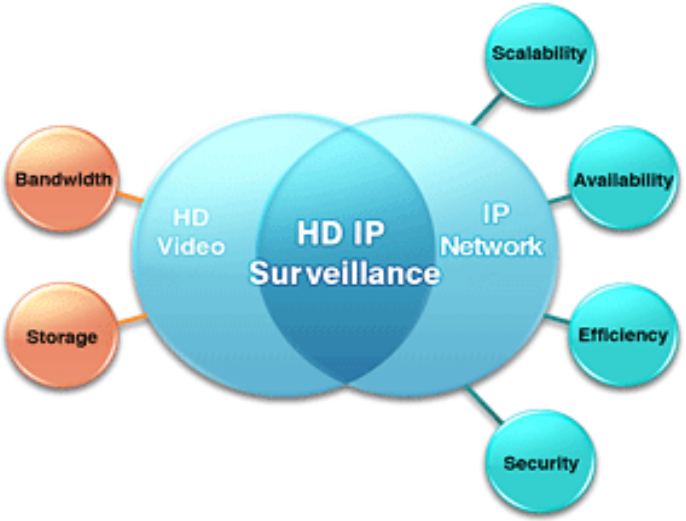
- Various security devices are employed by network surveillance system for secure data transfer between devises.
- Network security and authentication methods provided by some (Samsung) Network Cameras are described below:

### HTTPS (SSL) Login Authentication

- This communication protocol works the same as HTTP, added with SSL (Secure Socket Layer) data encoding.
- Applying SSL data encryption to all video data transferred slows down data transfer rate and causes delayed playback with a drop in frame rates due to the encryption / decryption process.
- To avoid such drawbacks, some Network Cameras apply HTTPS (SSL) data transfer only for logging in authentication challenge with account name and password but not to the subsequent video data transfer.

# Recommendations for IP Surveillance Networks

- The USDHS video handbook contains recommendations, requirements, and best practices for digital video surveillance systems (VSS).
- Different suppliers provides comprehensive line of IP surveillance network solutions that includes products that meet or exceed the following USDHS recommendations for design, selection, and deployment of digital VSS.



# Recommendations for IP Surveillance Networks

## Table 1-7: VSS Network Design Recommendations

| Item | Video Surveillance Network Recommendations | |
|---|---|---|
| 1 | High recoverability for power and network connections (redundancy) | ✓ |
| 2 | IEEE 802.3af/at compliance for PoE applications | ✓ |
| 3 | Cyber security (802.1x port-based authentication) | ✓ |
| 4 | Wide operating temperature range | ✓ |
| 5 | QoS for packet/port prioritization | ✓ |
| 6 | VLAN for isolation and added security | ✓ |
| | **Additional Considerations for edge devices (cameras and NVRs)** | |
| 7 | ONVIF for interoperability | ✓ |
| 8 | IP66 for ingress protection | ✓ |
| 9 | SDK for IVA embedded applications | ✓ |
| 10 | H.264 and MPEG-4 compression | ✓ |
| 11 | Imager viewing options for day/night, color, and black/white | ✓ |
| 12 | Wide focal length range for maximum magnification (zoom) | ✓ |
| 13 | HDTV conformance | ✓ |
| 14 | Internal memory recording (SD storage) | ✓ |

# Digital Storage And Retrieval

# Key Decision that Impacts Storage

## Considerations for Video Storage

- What level of image quality is required?
- How many surveillance cameras will be operating on the system?
- How long will the video footage be stored on the hard disk?
- Will the IP cameras be set to record only when motion is detected?
- Will the cameras be operating continuously or only at a certain hours of the day?

# TYPES OF AVAILABLE VIDEO STORAGE

## Storage Types Continued

- **Directly Attached storage** is when hard drives are located outside of the DVR, NVR or server but are 'directly' connected without having to use an IP network.
  - Examples of this include USB and eSATA. This is an inexpensive way to add dedicated storage to a single 'box' typically at low cost and with a simple setup.
- **Networked Storage**, such as NAS or SAN, are IP based 'pools' of storage specialized in storing video from large numbers of cameras.
  - Multiple DVRs, NVRs or servers can stream video to these storage clusters.
  - They provide efficient, flexible and scalable storage for very large camera counts but generally at higher cost and complexity.

# STORAGE OPTIMIZATION FUNCTIONS

## How to Optimize NVR / DVR Storage

**How Do I Optimize Storage?**

**Eight [8] commonly available storage optimization functions available on mainstream NVR /DVR systems includes.**

**Here is the list:**

- **Basic Motion Analytics**
- **Advanced Video Analytics**
- **Motion Exclusion Zones**
- **Data Aging**
- **Recording Schedule**
- **CODEC Selection**
- **Dual Streaming**
- **Storage Clusters**

**Understanding what options and measures are available is becoming increasingly important to selecting NVRs/DVRs and designing IP video systems.**

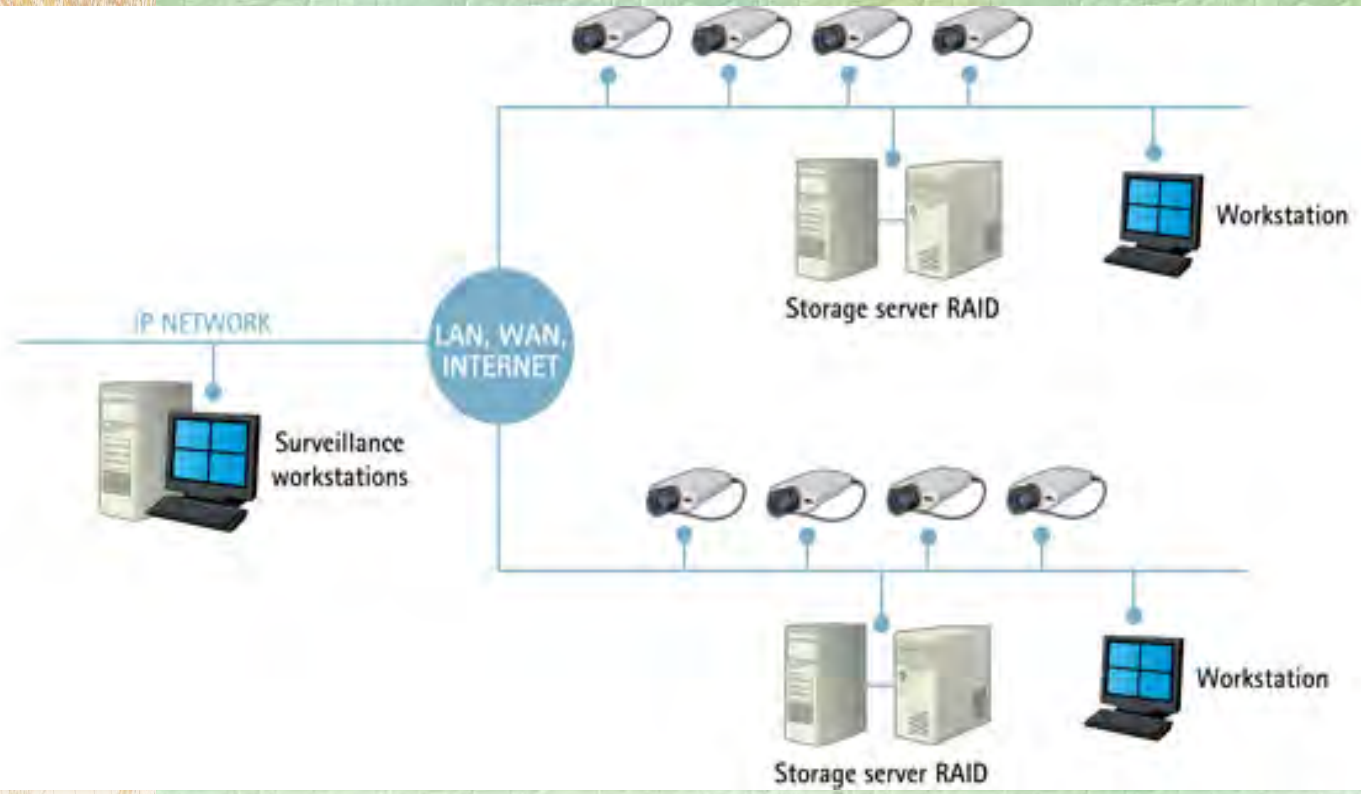
# NETWORK VIDEO RECORDER STORAGE

## Network Video Recorder

- A Network Video Recorder [or NVR] is a DVR for IP cameras.
- It combines video management software into a purpose-built desktop or rack-mount PC.
- Typically between 4 and 64 cameras can be supported per NVR.
- CMS or Central Management Software is used to manage multiple NVRs.

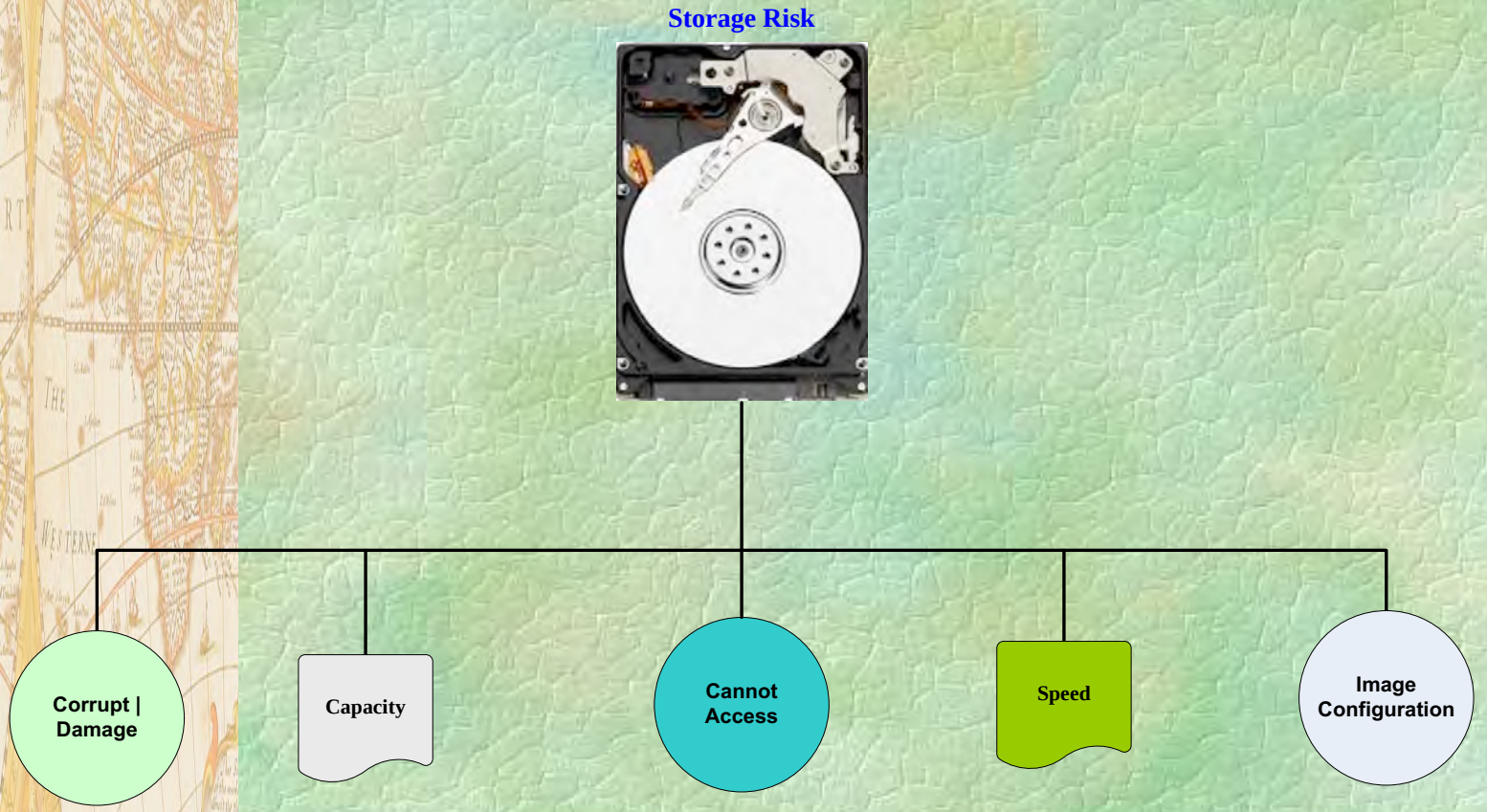
# Storage Application and Servers

**Figure 1-23:** Storage Application in Network



# Vulnerability of Video Storage

**Figure 1-24:** Risk Associated with Storage Device



# Network Basic

# Network Application for Video Surveillance

## Overview Network (IP) Video Systems

- Video over IP is best defined as the deployment of video information over a network that conforms to the Open Systems Interconnection (OSI) layer model, a standards communications model produced by the International Organization for Standardization (ISO).
- This includes support of cameras and encoders that transmit using standard network protocols like transmission control protocol TCP/ internal protocol (IP), user datagram protocol UDP, and file transfer protocol FTP.
- Devices that “stream” video over IP networks transmit frames and packets of video data to a single location or multiple locations for different purposes.
- A device like a network video camera or multi channel video encoder can send a video stream to a single network video recorder (NVR) or video decoder location or to multiple locations of the same type of equipment.

# Network Application for Video Surveillance

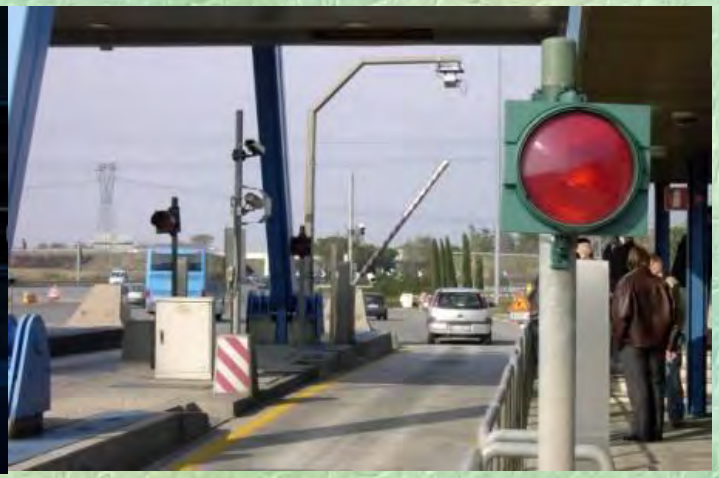
**Table 1-8:** Estimating Bandwidth Requirements For Modern Surveillance Systems

| Factor | Description | Examples |
|---|---|---|
| **Video compression method** | Typically temporal or spatial compression | MPEG-4, M-JPEG, Wavelet, and MPEG-2 |
| **Frame rate** | Images per second | 1-30 IPS |
| **Image resolution** | The number of horizontal and vertical pixels | QCIF, CIF, 2CIF, 4CIF (also known as full D1) |
| **Scene activity level** | The amount of activity in the camera's field of view | Low, medium, and high |
| **Quiet time** | The fraction of time where there is no movement (important for temporal compression algorithms like MPEG-4 because neglibible bandwidth is consumed during quiet time) | 8:00 pm - 6:00 am Monday - Friday, all day Saturday and Sunday, equates to about 50% quiet time |

# Network Application for Video Surveillance

**If you run out of bandwidth on your network, you will start to experience the following:**

- Video artifacts (e.g., blocks in MPEG and M-JPEG, and increased fuzziness in Wavelet)
- Frames may get dropped, making the video appear choppy
- The video resolution may drop from 4CIF to 2 CIF or even CIF, making the picture less clear
- The video may freeze entirely and lose the connection temporarily.



# Network Application for Video Surveillance

| Name | Also known as | Bandwidth |
|---|---|---|
| 10Base-T | Standard Ethernet | 10 Mbps (Megabits per second) |
| 100Base-T | Fast Ethernet | 100 Mbps |
| 1000Base-T | Gigabit Ethernet | 1,000 Mbps or 1 Gbps |

# DEFINE AND CONFIGURE NETWORK IP-ADDRESS

## IP Address Classes

- There are four different address formats or classes, of which only three are significant in a corporate setting.
- Each class provides for different networks and avail- able hosts, according to their size:
  - Class A: Large networks with many devices
  - Class B: Medium-sized networks
  - Class C: Small networks (less than 254 devices)

# Network Application for Video Surveillance

**Table 1-9:** IP Address Bits and Bytes

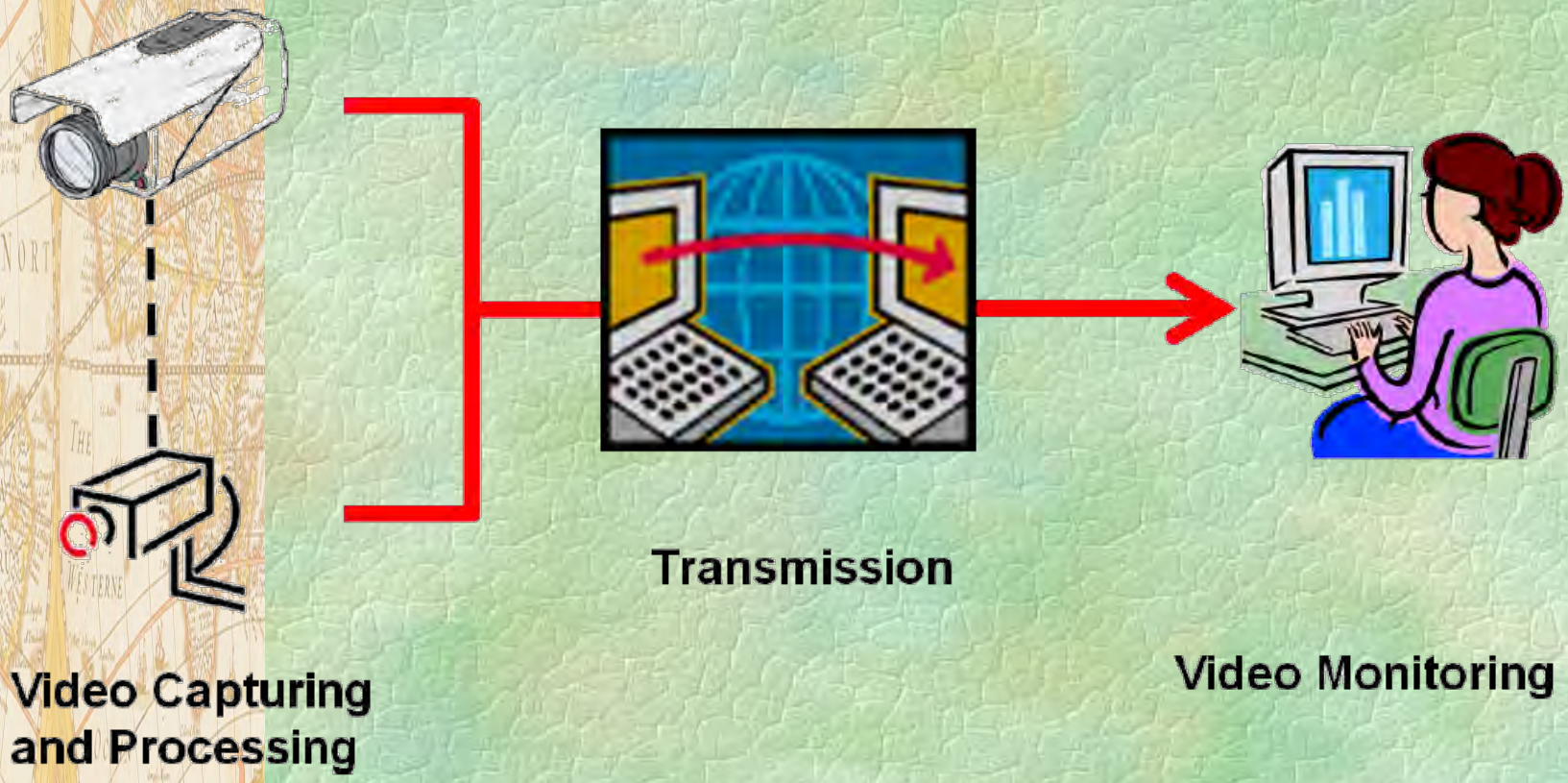
| Class | Initial Bytes [First Octet] | First Bit | Network Bits | Host Bits | Multicast Bits | Number of Networks | Maximum Number of Hosts |
|---|---|---|---|---|---|---|---|
| Class A | 0 – 127 | 0 | 7 | 24 | N \| A | 126 (0 and 127 are reserved) | 16,777,214 |
| Class B | 128 – 191 | 10 | 14 | 16 | N \| A | 16,384 | 65,532 |
| Class C | 192 – 223 | 110 | 21 | 8 | N \| A | 2,097,152 | 254 |
| Class D | 224 – 247 | 1110 | N \| A | N \| A | 128 | | |

**Table 1-10:** IP Address Class Identifiers

| Class | IP Address | Network ID | Host ID |
|---|---|---|---|
| A | a.b.c.d | a | b.c.d |
| B | a.b.c.d | a.b | c.d |
| C | a.b.c.d | a.b.c | d |

# IP VIDEO SURVEILLANCE DESIGN ELEMENTS

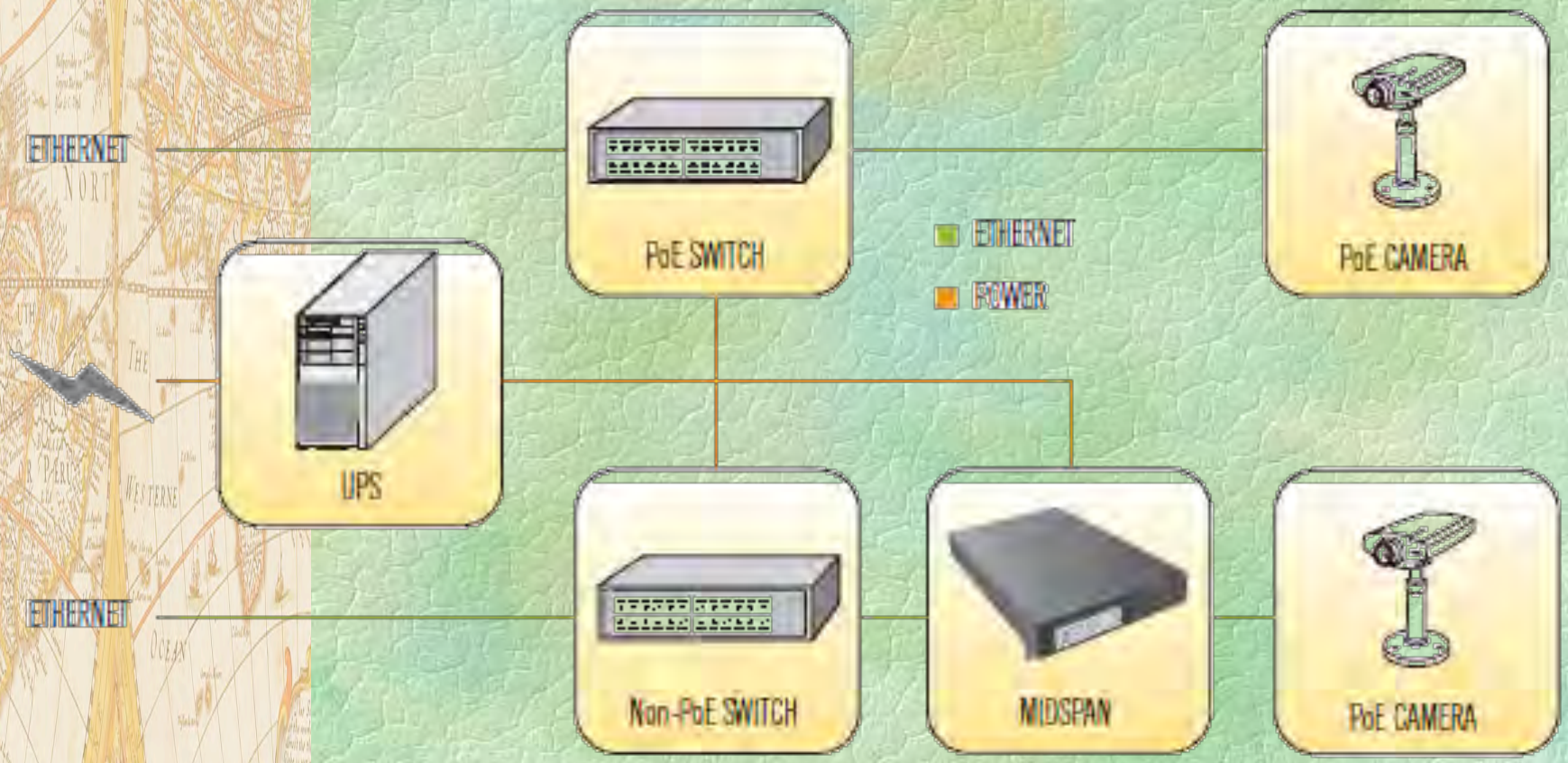
**Figure 1-25:** Three Key Elements of Network




There are many ways to implement an IP network, and there is no single best way design a perfect IP network.

# Video Surveillance PoE SYSTEM DESIGN

**Figure 1-26:** Power Option for IP Cameras



# NETWORK PERFORMANCE MONITOR

**Network outages and performance CAN BE IMPROVED with advanced network monitoring software.**

https://go.solarwinds.com/NA/NPM/Network-Management-Software-V4?CMP=KNC-TAD-MSN-SW_NA_X_PP_CPC_LD_EN_PRODB_DWA-NPM-X_X_X_X-X&kwid=aIENPW6a

**Figure 1-27:** Screen-shot of Software for Monitoring Network Performance

# Configuring Equipment for Operating VS System

# CONFIGURATION OF DEVICE SETTINGS

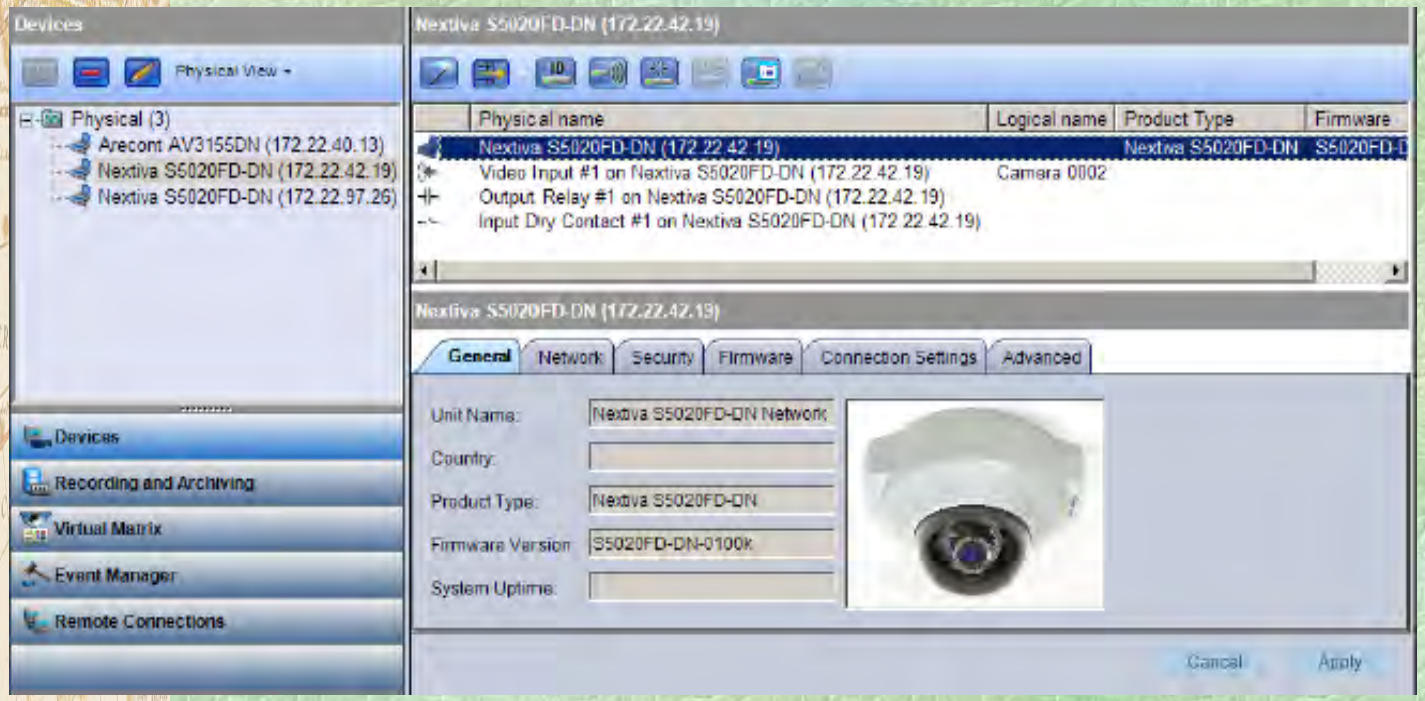
## Viewing and Configuring Physical Device Settings

### Viewing General Properties of a Device

The General page displays settings that are defined in the Nextiva edge device using SConfigurator. For details about configuring a Nextiva device, refer to the *Verint SConfigurator User Guide*.

▸ **To view general properties:**

1. From the Devices pane of System Components workspace, select **Physical View**.



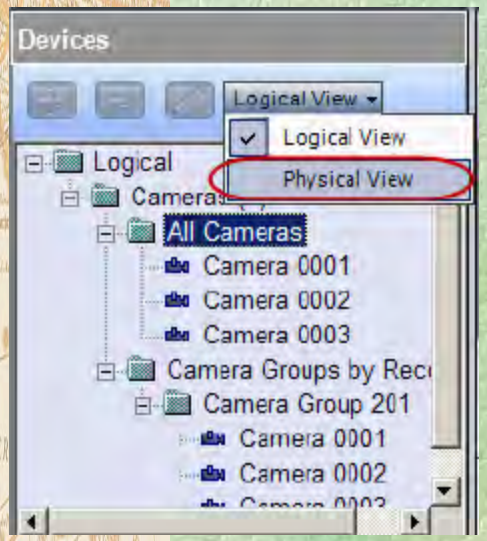
# CONFIGURATION OF DEVICE SETTINGS

## Viewing Network Settings of a Device

The **Network** tab displays the IP address, subnet mask, and gateway configured on the Nextiva edge device. These settings are provided for informational purposes only. They cannot be modified from Nextiva Control Center.

▸ **To view Network settings:**

1. Click **System Components** > **Devices** > **Physical View**.




2. Expand the group where the device is located and select the device.
3. In the Nextiva device editor, click the **Network** tab. The following settings are displayed:
   - **DHCP**: This field is set to **Disabled**. Dynamic Host Configuration Protocol (DHCP) is not supported for Nextiva edge devices or third-party hardware components.
   - **IP Address**: This field displays the IP address of the device.
   - **Subnet Mask**: This field displays the subnet mask configured on the device.
   - **Gateway**: This field displays the gateway configured on the device.

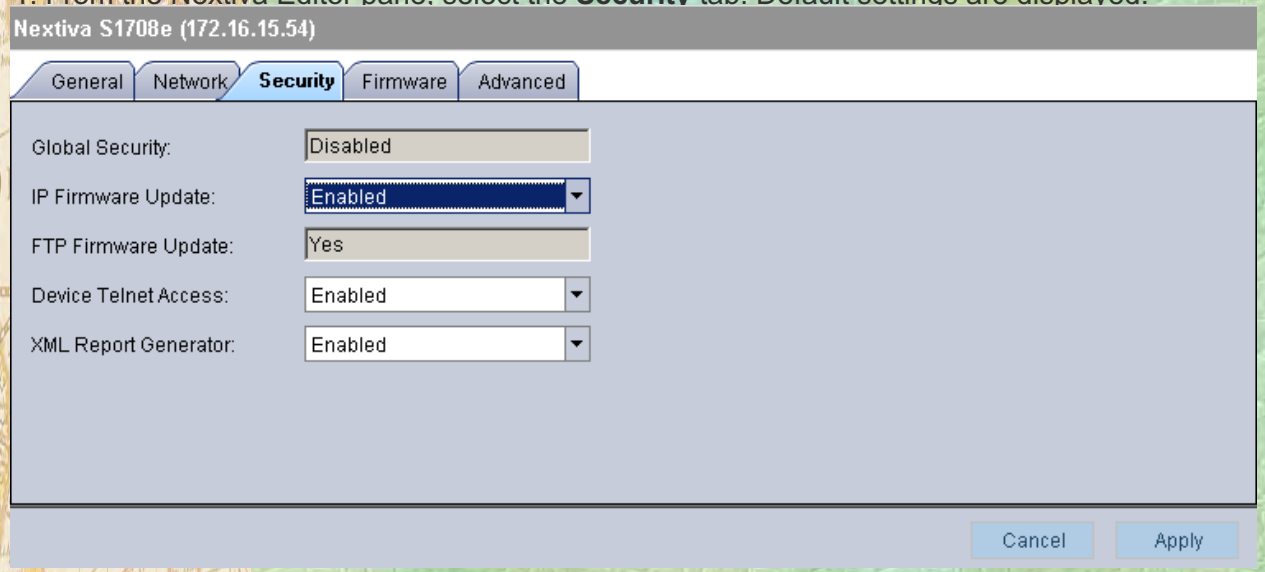
# CONFIGURATION OF SECURITY OPTIONS

## Defining Security Options for a Device

Specify some security settings for Nextiva edge devices. Settings defined in Nextiva override those defined on the edge device.

▸ **To define security options:**

1. From the Nextiva Editor pane, select the **Security** tab. Default settings are displayed.




2. Specify security parameters for the selected device:
   - **Global Security**: The Global Security profile is a security option supported by Nextiva intelligent edge devices. However, it is not supported by Nextiva VMS. Ensure that the option is disabled on all Nextiva devices by using, depending on the device type, the Web interface, Command Line Interface (CLI), or by Telneting into the device. Refer to the user guide for the specific Nextiva edge device for details.
   - **IP Firmware Update**: Select **Enabled** to enable firmware updates for the selected device on the Logical View Firmware tab. Otherwise, select Disabled. The default is enabled. For details, see "Updating the Firmware of a Device" on page 136.
   - **FTP Firmware Update**: This option enables users to update the firmware of Nextiva devices from an FTP site. By default, this option is disabled.
   - **Device Telnet Access**: Telnet refers to a terminal emulation protocol for TCP/IP networks such as the Internet. This protocol enables telnet clients to connect to devices on the network. You can then enter commands through the command line interface as if you were connected directly to the devices. By default, this option is enabled for Nextiva intelligent edge devices (except S1800e series).

# MODULE 2: DESIGN AND APPLICATION OF IP-BASED VIDEO SURVEILLANCE SYSTEM

# IP-VIDEO SURVEILLANCE SYSTEMS DESIGN AND OPERATIONS


BY: LENNOX BENNETT

# IP-Based VSS Design

# IP VIDEO SURVEILLANCE DESIGN

## SETTING UP AN IP-Based VIDEO SURVEILLANCE SYSTEM - QUICK CHECKLIST

### DEFINE YOUR SURVEILLANCE NEEDS

- Draw a plan of your installation
- Select points of interest to view (area of coverage)
- Position each camera — define what you want to be able to capture with each camera
- Consider environment — light conditions
- Consider cabling to cameras
- Position the recording server.

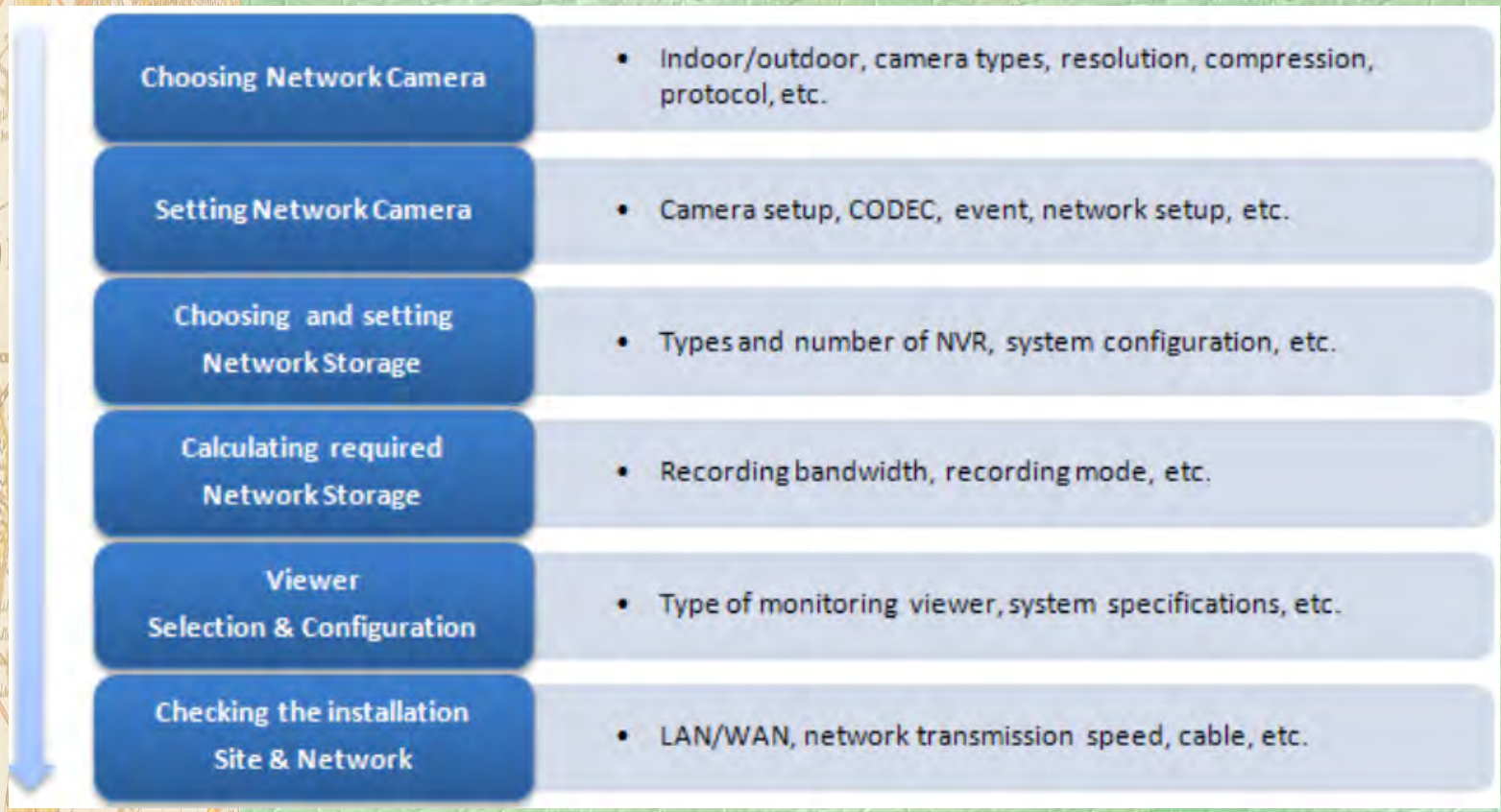
# VIDEO SYSTEM TECHNICAL SPECIFICATION

## Video Surveillance Application Software

1. The software shall operate on open architecture for integration with perimeter safety, access control, PA and fire / safety systems based on open standards.
2. Digital video surveillance control software should be capable to display and manage the entire surveillance system. It should be capable of supporting variety of devices such as cameras, video encoders, video decoders, PTZ controller, NVR, NAS boxes/Raid backup device etc.
3. The software should have inbuilt facility to store configuration of encoders / decoders and cameras.
4. The software should Support flexible 1/2/4 Windows Split screen display mode or scroll mode on the PC monitor or on preview monitor as per site requirement.
5. The software should be able to control all cameras i.e. PTZ control, Iris control, auto / manual focus, and color balance of camera, Selection of presets, Video tour selection etc.
6. There must be a single encoder for each camera.
7. The software is required to generate reports of stored device configuration. The control software is required to provide alarm and alarm log. The log shall be able to be achieved, printed and displayed using a device filter, a device group filter and/or a time window.

# Design of Video Surveillance Systems for Video Quality

**Figure 2-1:** Design Flow of Network Monitoring System




**When installing a networked surveillance system the relationship and functionality between the network environment and surveillance components should considered.**

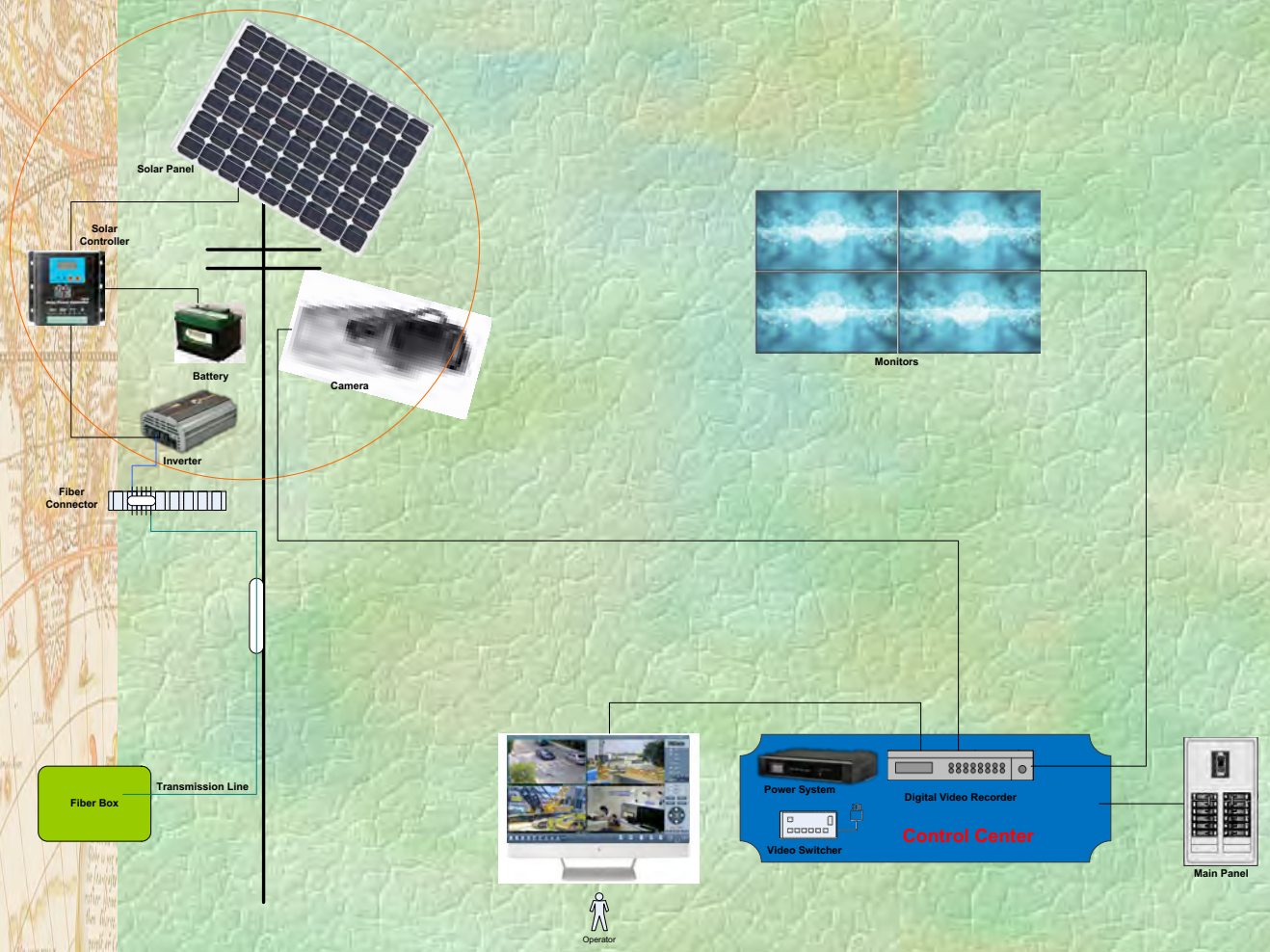
# Design of Video Surveillance Systems for Video Quality

## Component/Device Categories

- When designing a system to achieve desired video quality, consideration must be given to the following three steps:
  - Categorize components;
  - Select the highest-performing devices, infrastructure or services for the given budget; and
  - Assure/verify interoperability, compatibility and delivery of the Digital Multimedia Content [DMC] per the user's requirement.
- For example, take a small recording solution for a standalone facility, such as a small data center that requires no remote access.
- DMC recording must be of the highest quality but with retention of events only; those events are, triggered by an external source.

# Design of Video Surveillance Systems for Video Quality

**Figure 2-2:** Simplified Video Surveillance System Infrastructure



# Operating Surveillance System

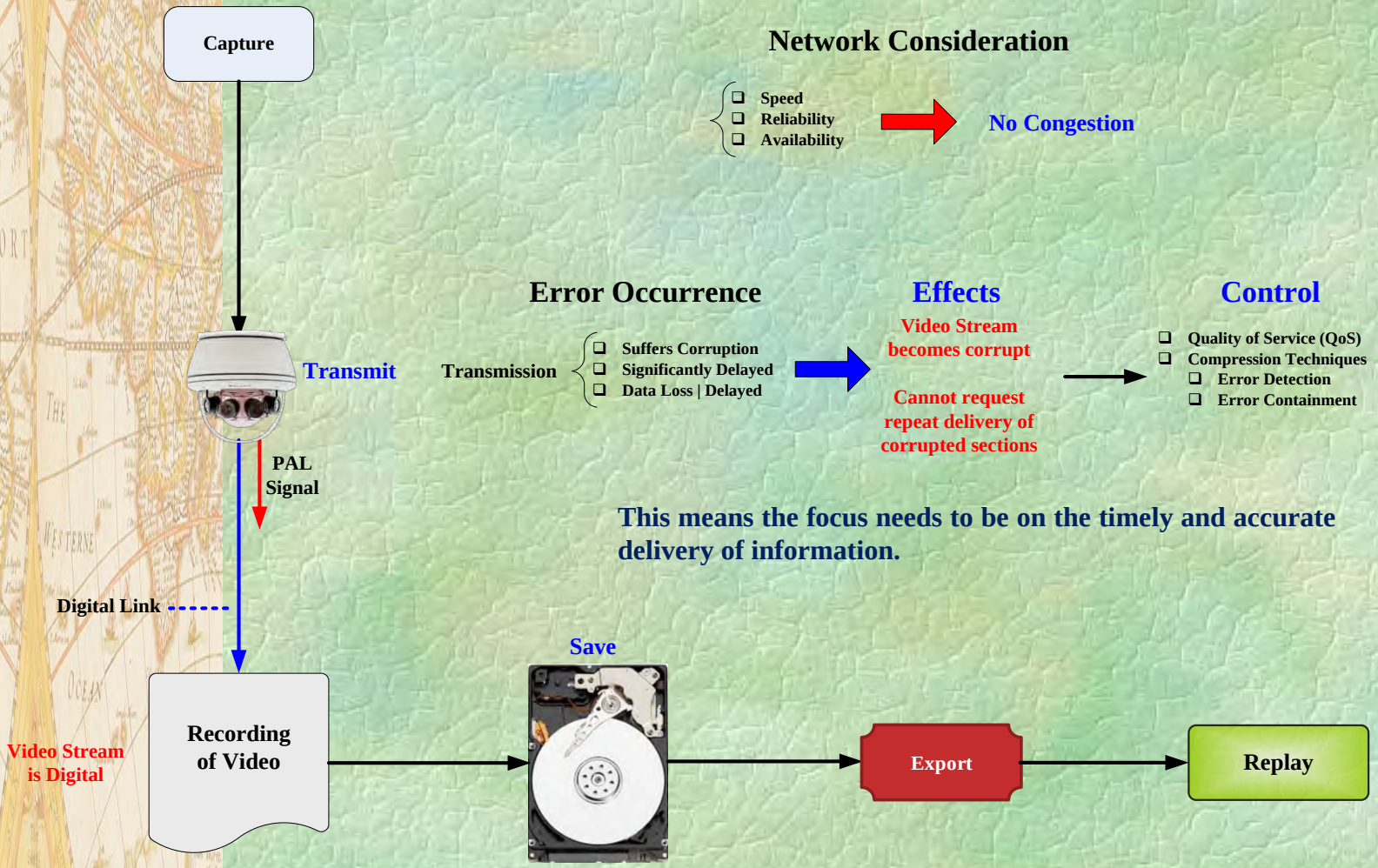
# OPERATING VIDEO SURVEILLANCE SYSTEM

## How to Operate System

- An operational manual should be developed for the Video surveillance system operations.
- The operators manual shall fully explain all procedures and instructions for the operation of the system including:
  - Computers and peripherals
  - Systems startup and shut down procedures
  - Use of system, command, and applications software
  - Recovery and restart procedures
  - Graphic alarm presentation
  - Use of report generator and generation of reports
  - Data entry
  - Operator commands
  - Alarm messages and reprinting formats
  - System permissions functions and requirements

# OPERATING VIDEO SURVEILLANCE SYSTEM

## Figure 2-3: Transfer Digital Signal in Terms of File | Video Stream



# OPERATING VIDEO SURVEILLANCE SYSTEM

- **Data Protection.**
- **Familiarity of guidelines (Data Protection Act of 1998)**
- **Special Attention to the preventing of video surveillance footage to anyone other than authorized individuals**
- **The Directive and the DPA cover two common categories of information:**
  - **Information processed, or intended to be processed, wholly or partly by automatic means (e.g. on computer); and**
  - **Information processed otherwise than by automatic means which form part of, or are intended to form part of, a 'relevant filing system' (i.e. manual information in a filing system).**

# OPERATING SURVEILLANCE SYSTEM

**What type of information is protected by the Data Protection Act?**

**The Act regulates the use of "personal data". To understand what personal data means, Let's first look at how the Act defines the word "data".**

**Data means information which:**

**A. Is being processed by means of equipment operating automatically in response to instructions given for that purpose,**

**B. Is recorded with the intention that it should be processed by means of such equipment,**

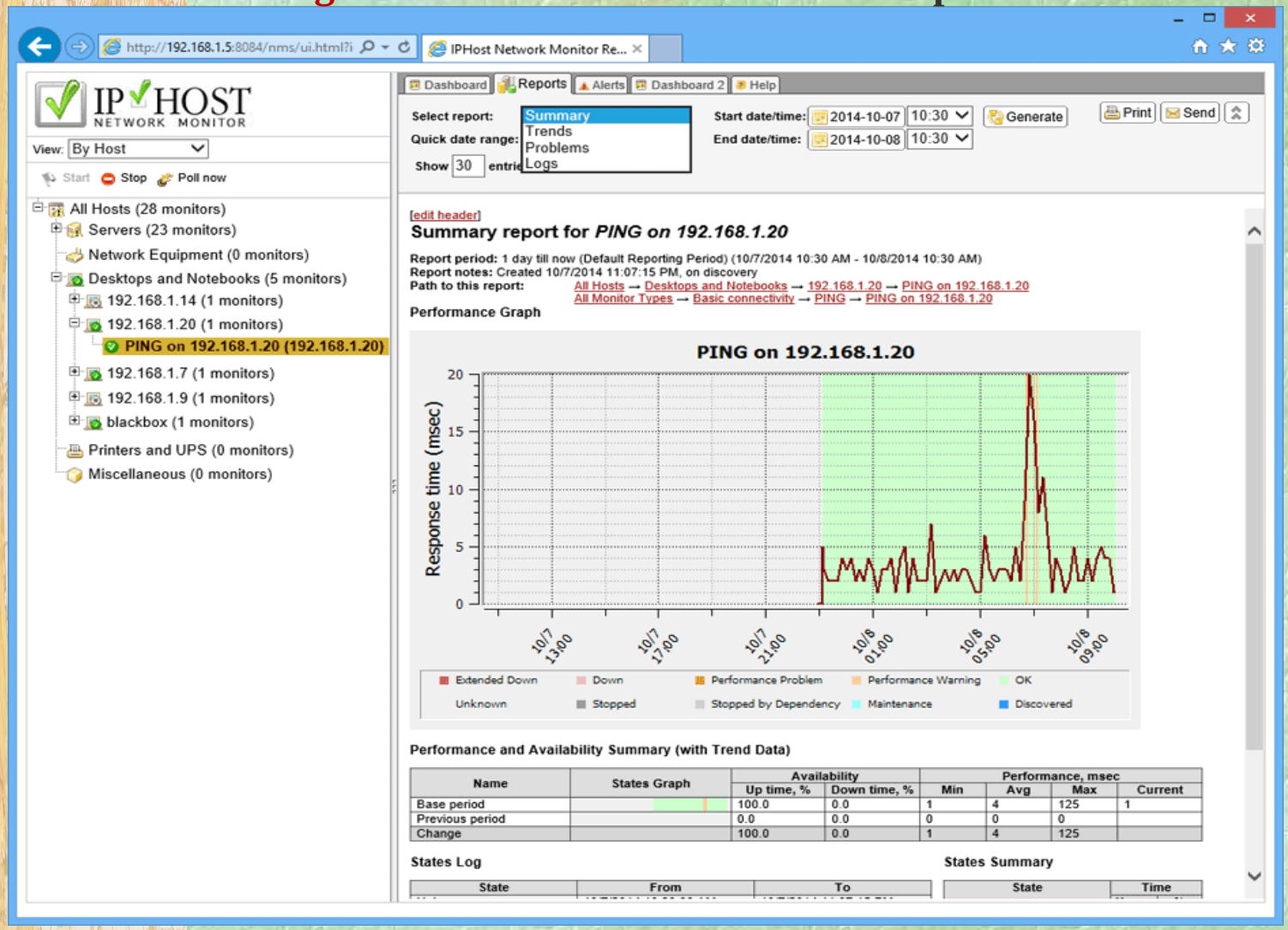
**C. Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,**

**D. Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or**

**E. Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).**

# GENERATING PERFORMANCE REPORTS

**Figure 2-4:** Network Performance Report



# Video Recording

# RECORDING SURVEILLANCE VIDEO

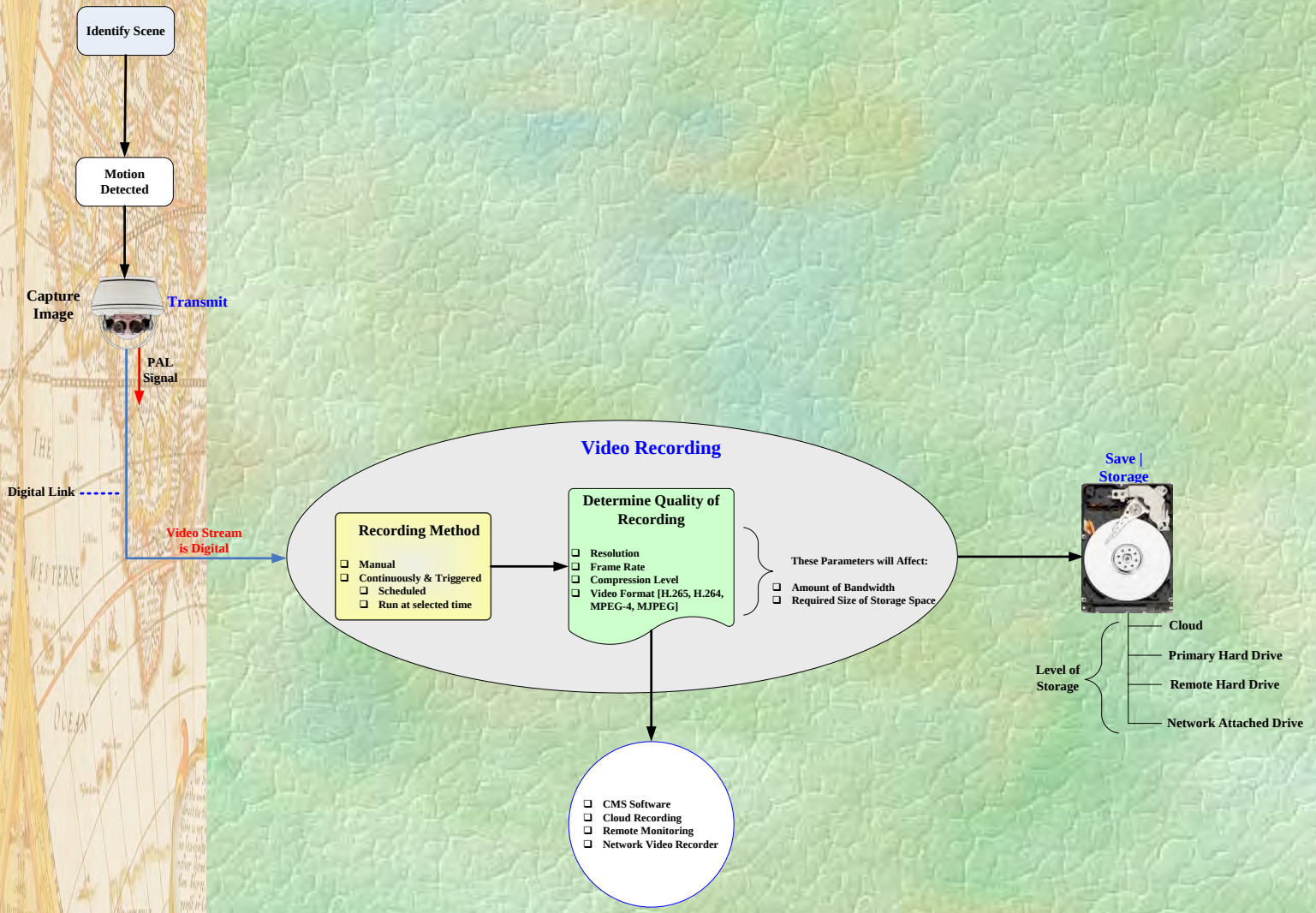
## Key Considerations for Recording

**Recording**

- How long is the video retained on the system before being overwritten?
- What image quality is required on the recorded image compared with the live image?
- What frame rate is required for the recorded video?
- What metadata (additional information) should be recorded with the video?

# VIDEO RECORDING PROCESS

## Figure 2-5: Simple Process for Recording a Video



# VIDEO RECORDING OPTIONS

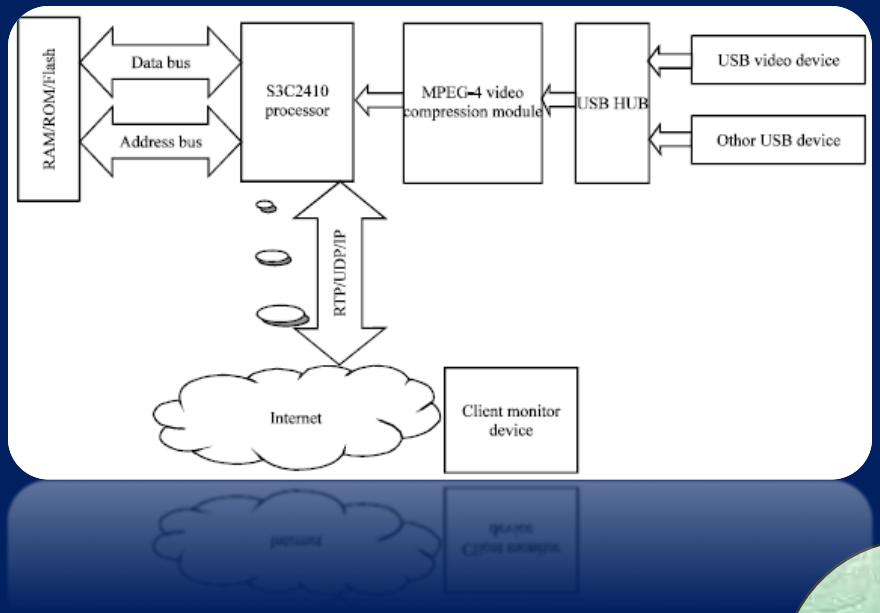
- **Recording Options: Rules and Policies Advancing technology has prompted renewed best practices in dealing with overarching recording options for cameras within an organization's video surveillance system.**
- **The ability to retain full-motion, 30fps, highest resolution video feeds creates the necessity to properly plan out long-term retention policies for an organization's video surveillance solution.**
- **By incorporating specific VLM rules and policies, an organization can create an infrastructure that will allow it to keep months and years of video feeds under management and available for fast and easy retrieval and playback.**
- **Data migration and replication rules and policies need to take into account the organization's available storage resources, such as NAS, DAS, SAN, IP-SAN, Blu-ray, and digital computer data tape, such as LTO.**
- **Best practices dictate a mix of online, near-line, and offline storage resources for optimal long-term retention periods and best utilization of those storage resources.**

# OPTIONS FOR VIDEO RECORDING

## System Integration

- CMS Software.
- Cloud Recording.
- Remote Monitoring.
- Network Video Recorder

**Figure 2-6:** Overall Framework of Remote Monitoring



# STORAGE BASED ON RECORDING MODE

## Event Recording

- **Pre-event / Post-event Recording**
  - Since the NVR has to keep video data of a certain time period to provide such a buffer, setting pre-event time to a long period is not possible.
  - Post-event recording sets how long the NVR will record video after the event time.
  - When an event occurs and saves an event recording, its total length is the sum of [Pre-event + Post-event].

## Manual Recording

- **You can record and save the video by manually pressing the record button of NVR.**
  - The required storage capacity for manual recording can be calculated with the recording time.
  - For example, assuming that the total network bandwidth is 48 Mbps and records for 10 minutes manually, the required storage capacity for this manual recording will be:
    - Required capacity for 10 minutes = 6MB (48 Mbit)/sec X 600 seconds = 3.6 GB

# TYPICAL FRAME RATES FOR RECORDING

## Recording: Frame Rates

- With *PAL cameras 25 frames* (images) per second are captured, which gives the appearance of smoothly flowing motion and is more than adequate for most scenarios.
- Broadcast quality video is recorded at 30 frames per second (fps) in NTSC standard, but for CCTV recorded in time-lapse mode, frame rates of 6-12 fps are more common, although rates as low as 1 fps are used.
- One method of reducing the storage overhead is to use an archiving strategy that allows the frame rate to be adjusted either 'on the fly' or automatically within the archive.

# Creating a New Recording Profile

You can create several recording profiles to be used with different cameras, or with the same cameras. If you assign a camera to two or more recording profiles, and the coverage period overlaps (in other words, two or more recording profiles are scheduled to run at the same time), video will not be recorded during the overlapping period.

## ▸Perform the following steps:

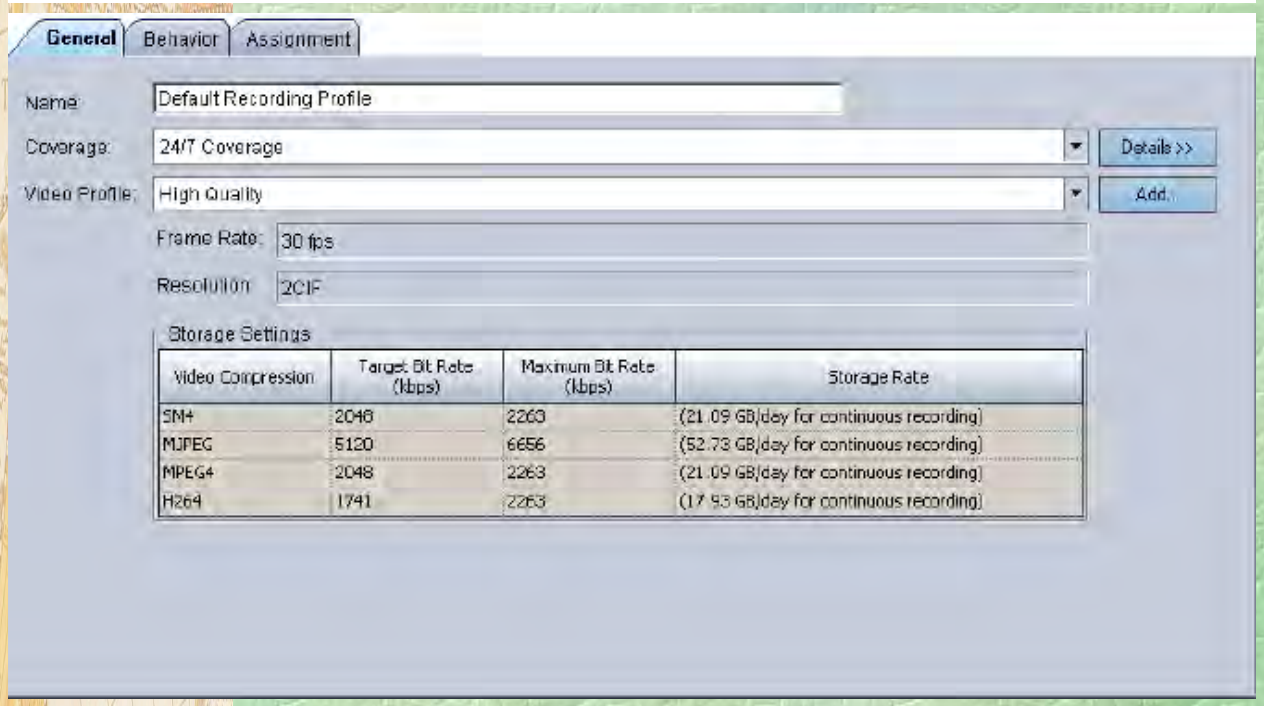
1. Click **System Components** > **Recording and Archiving** > **Recording** > **Recording Profiles**.
2. Select an existing Recording Profile to use as a template.
3. On the **General** tab, click (Add Recording Profile).
4. In the **Name** box, type a meaningful name to facilitate the management of your Recording Profiles.
5. Click **Apply**.

# CONFIGURATION OF SYSTEM EQUIPMENT

## Choosing the Coverage Schedule for a Recording Profile

When you create or modify a recording profile, you must select a coverage profile. The coverage profile defines the schedule when the Recording Profile is enabled. The coverage profiles are configured in the Global Settings workspace.

**NOTE:** You can change an existing coverage profile or create new one from the Global Settings workspace.




4. In the **Coverage** drop-down list, select a schedule.
5. To see the days and times that the coverage profile is scheduled for, click the **Details** button.
6. To save the settings, click **Apply**

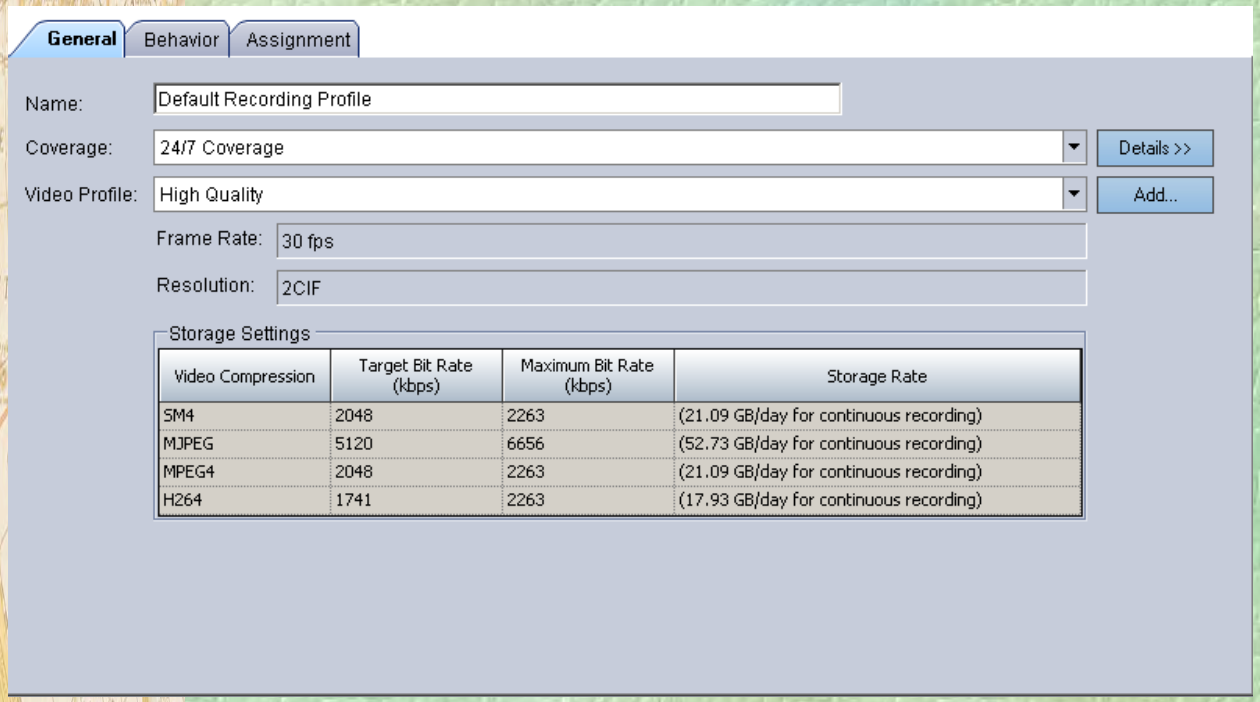
# CONFIGURATION OF SYSTEM EQUIPMENT

## Choosing the Video Quality of a Recording Profile

When you create or modify a recording profile, you must choose a video profile to define the quality of the video images.
When you expect the assigned cameras to capture lots of motion, or need to see lots of detail in the video, choose a high quality profile.
However, the higher the quality of the video, the bigger the files are, which means the video files use more storage capacity. The video profiles are configured in the Global Settings workspace.

### ▸ Perform the following steps:

1. Click **System Components** > **Recording and Archiving** > **Recording** > **Recording Profiles**.
2. Click the **General** tab.



# Exporting Video Files

# EXPORTING VIDEO FOOTAGE

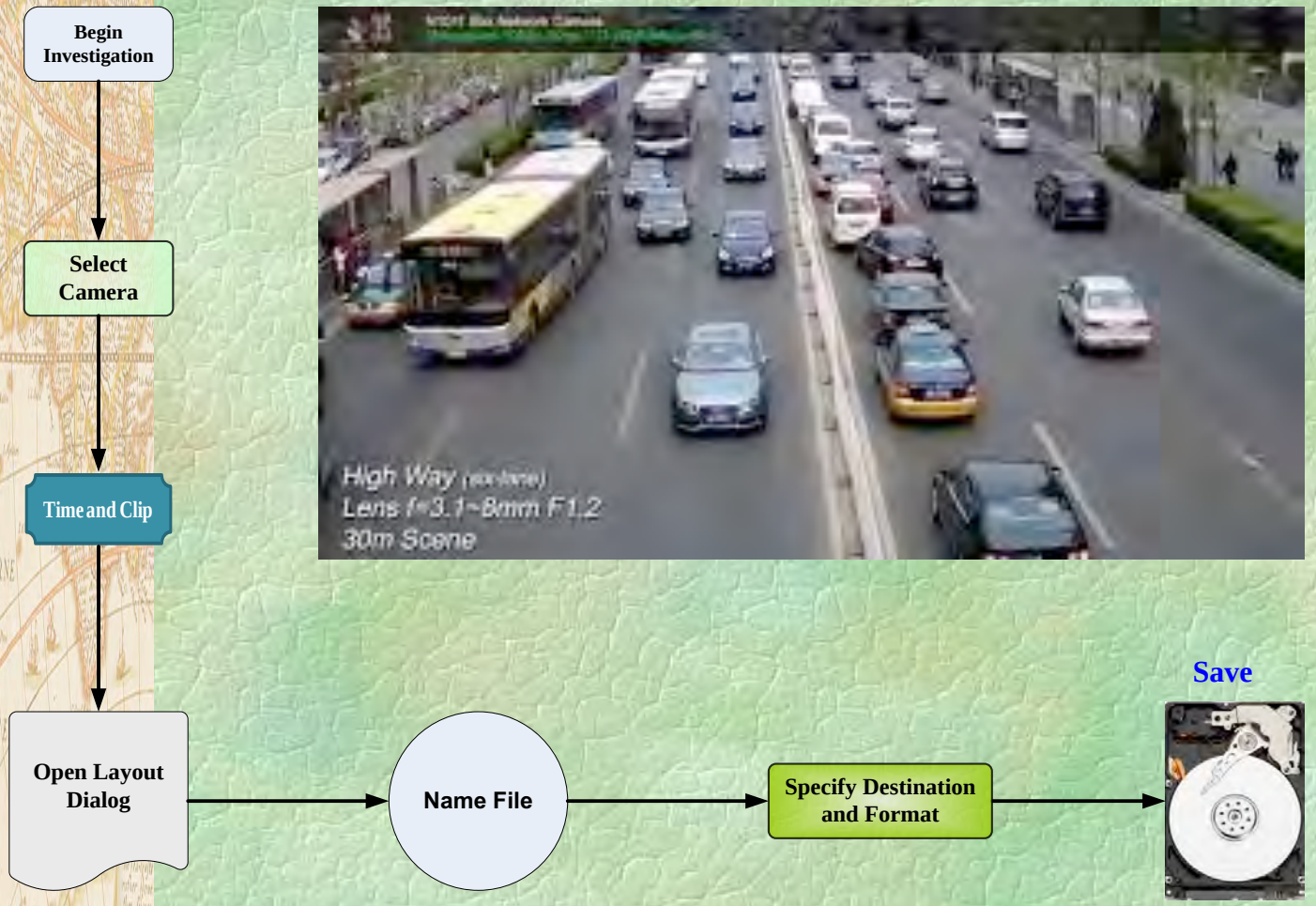
## Pertinent Information Relating to Export | Archive

### Export / Archive

- How will you export data from the system to create a permanent record?
- Who will require access to the data (e.g. police etc.)?
- How will they replay the video (e.g. is special software required)?
- For a digital recorder the incident must be copied from the internal hard drive to a permanent storage medium such as a CD/DVD, before it is overwritten.
- For exporting longer video clips and for large scale archiving, the system should provide one of the following:
  - The ability to export video to an external 'plug and play' hard drive via a USB or Firewire connection
  - Network port
  - Removable hard drive

# EXPORTING VIDEO FILES

**Figure 2-7:** Process for Exporting Still Images or Video Clips



# Code of Practice Management of CCTV

# LEGAL ISSUES RELATING TO SYSTEM USE

## Understand the Legal Ramification Before Use

**Legal issues**

- **What laws apply to the storage of and access to information?**
- **The Data Protection Act (1998) is designed to prevent the misuse of personal information. Legal obligations are placed on anybody who handles this type of information.**
- **The Freedom of Information Act (2000) provides a right of access to any recorded information held by public authorities. Legal obligations are placed on public authorities to follow certain procedures when responding to requests for information.**
- **CCTV operators and system managers should be aware of the requirements placed on them by these laws and should have procedures in place to enable them to comply.**

# Code of Practice for Management of CCTV

## CCTV Evidence Records

A high-quality code of practice for the management of CCTV evidence records should consider the following:

| Issue | Comment |
|---|---|
| Scope of responsibilities | Clearly state who is responsible for overseeing the management, security and preservation of CCTV data for use in criminal and civil proceedings.<br><br>Identify staff or positions that are responsible for operation, extraction, viewing, storage and analysis of the data. |
| The principles | Clearly state the principles adopted in relation to management of the CCTV system and commitments to:<br>• Confidentiality<br>• Appropriate use of CCTV equipment<br>• Maintaining a secure CCTV work area<br>• Management of media enquiries<br>• Appropriate storage and disposal of CCTV data<br>• Avoid the inappropriate release of data<br>• regular monitoring and review of the use and management of the CCTV system. |
| Work procedures of staff | Clearly set out the procedures for those responsible for the operation of the CCTV equipment, including procedures for:<br>• Visitors to the work area<br>• Logging of incidents<br>• The processing of CCTV data requests from police, stakeholders and FOI applicants<br>• Viewing and copying CCTV data<br>• Storage and disposal of CCTV data<br>• Maintaining records of requests, and the process by which complaints may be lodged and how they will be managed<br>• Dealing with any breach of privacy, or breach of the standard operating procedures or the code of practice. |

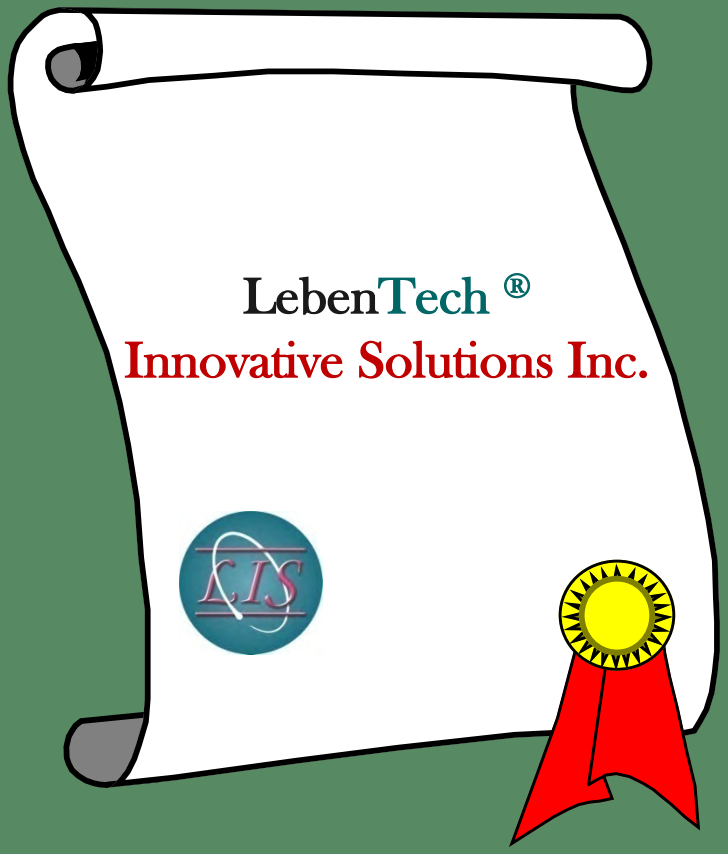
# SURVEILLANCE ETHITICAL CHALLENGES

## Privacy Concerns

- Chilling effect of free speech and association.
- Threats of privacy and potential for abuse.
- Racial disparities impact in targeting.
- Improper release of video by employee (lack of regulation)
- Pervasive camera technology jeopardizes fundamental rights.
- Individual have a constitutional right to be free from unreasonable searches.
- Specific risk of harassment surveillance pose to individual wearing skirt and blouses.

# MODULE 3: DESIGN AND APPLICATION OF IP-BASED VIDEO SURVEILLANCE SYSTEM

# BASIC ELEMENTS OF IP VIDEO SURVEILLANCE INSTALLATION

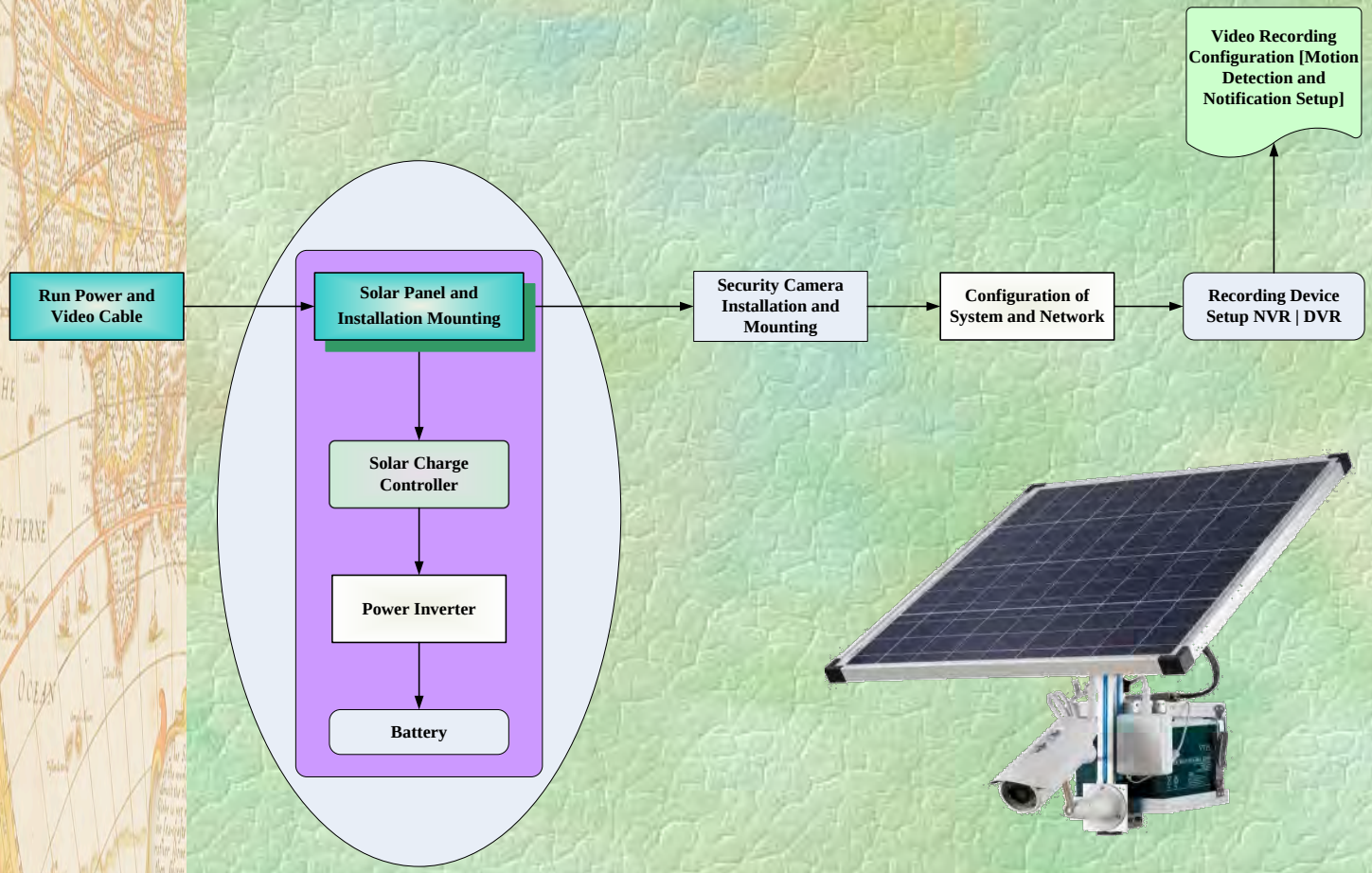



BY: LENNOX BENNETT

# Basic Elements of IP Video Installation

# INSTALLATION of Video Surveillance Systems

**Figure 3-1:** Surveillance System Installation Process



# ITEMS REQUIRED FOR INSTALLATION

## System Drawing

2. A system drawing for each applicable security system shall:
   a. Identify how all equipment within the system, from main panel to device, shall be laid out and connected.
   b. Provide full detail of all system components wiring from point-to-point.
   c. Identify wire types utilized for connection, interconnection with associate security subsystems.
   d. Show device locations that correspond to the floor plans.
   e. All general and drawing specific notes shall be included with the system drawings.

# ITEMS REQUIRED FOR INSTALLATION

## Proof of Compliance

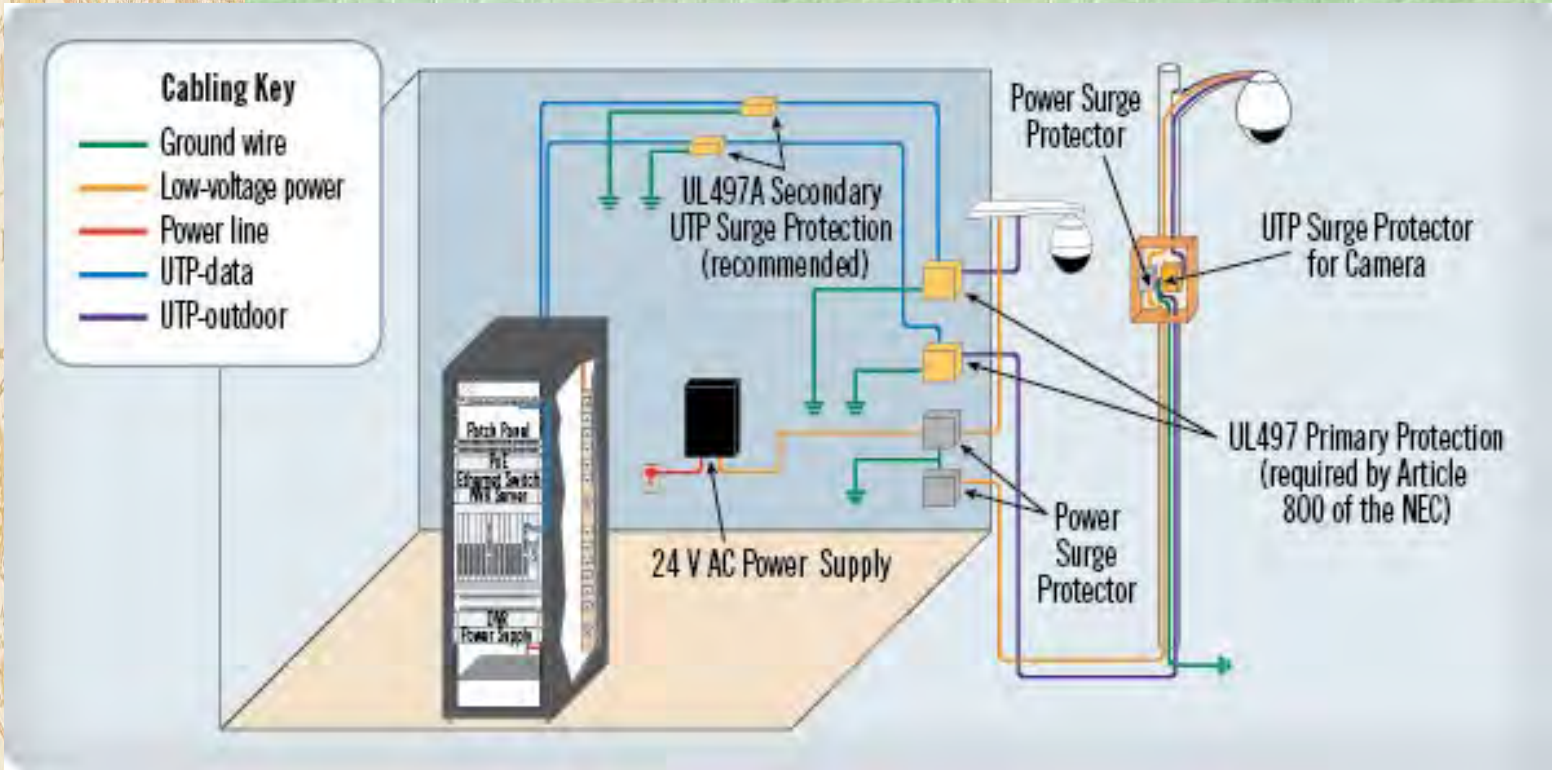
4. **Submit manufacture's certification of Underwriters Laboratories, Inc. (UL) listing as specified.**

   - **Provide all maintenance and operating manuals per the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.**

5. **Submit completed System Readiness Checklists provided by the Commissioning Agent and completed by the contractor, signed by a qualified technician and dated on the date of completion, in accordance with the requirements of Section 28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.**

# INSTALLATION of Video Surveillance Systems

**Figure 3-2:** Best Practices for Safeguarding Network Equipment



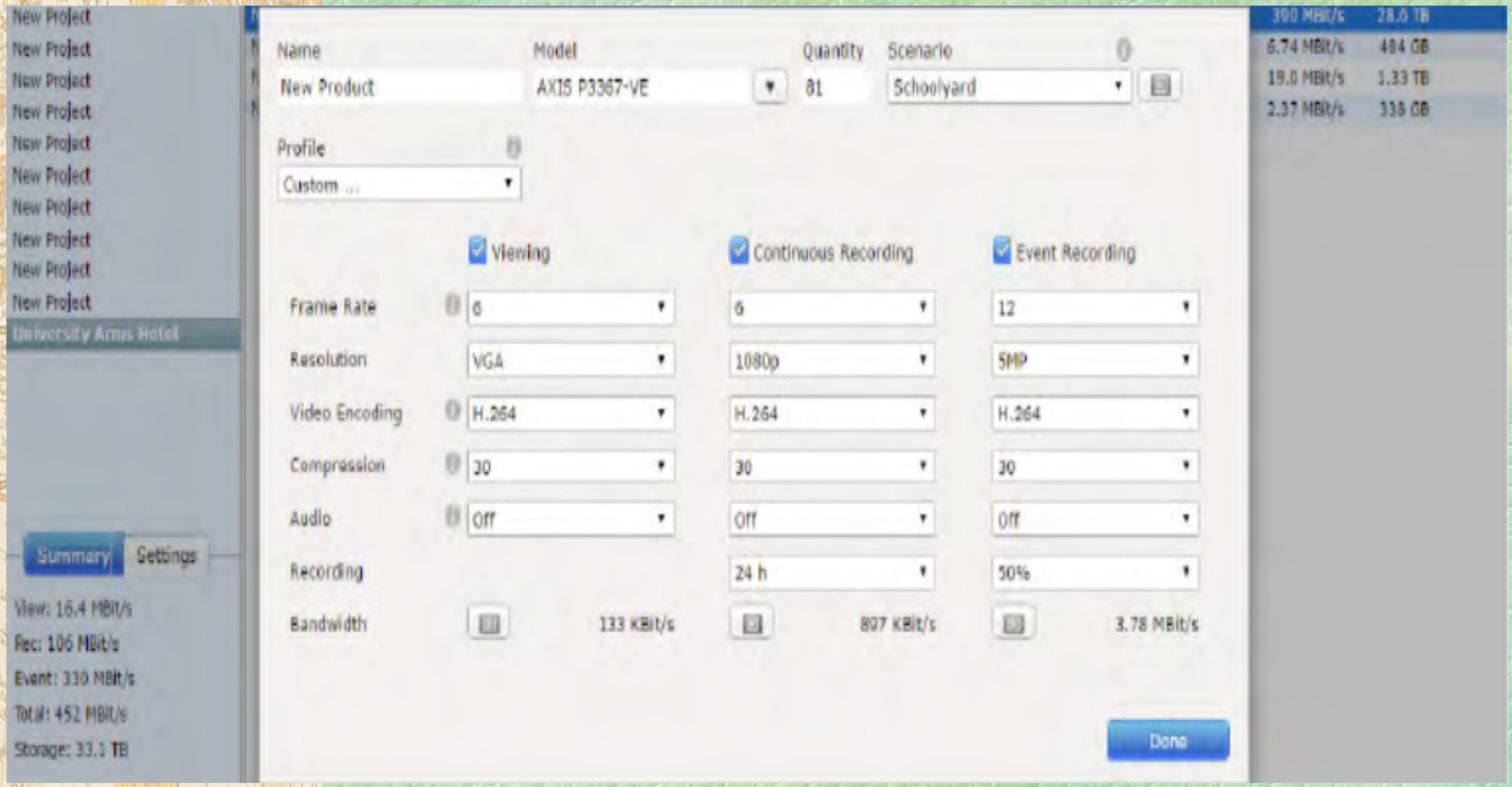

**It is important to follow best practices to effectively safeguard networking equipment against any potential damage from high-voltage electrical surges.**

# Storage Calculations and Servers

- Storage requirements, the accessibility and retrieval of images and related information including scalability, redundancy and performance, are all important to a network solution.
- The ability to use open storage solutions is one of the main benefits with IP surveillance and there are two main ways to achieve this.
  - The most common is to have the storage attached to the server running the application, as in a Network Video Recorder (NVR).
  - The other is a storage solution where the storage is separate from the server running the application, called network attached storage (NAS) or storage area networks (SANs).
- SAN systems enable the designer to build redundancy into the storage devices so video data can be saved simultaneously in more than one location.
- This configuration can include a Redundant Array of Independent Disks (RAID) set up which also enables failover where two servers work with the same storage device (clustering) to reduce system downtime.

# Storage Calculations and Servers

**Figure 3-3:** Screen Shot of Storage Calculator



# Storage Calculations and Servers

## Example 1

- An IP-Based video system is being specified for a custody suite that is required to capture high quality images of 20 kB per frame.
- 12 fps per camera are being generated and there are 8 cameras in the system.
- Each camera is recorded for 24 hours per day, and the OR has stipulated a retention period of 31 days. The storage capacity is given by:

$$\left(\frac{20 \times 12 \times 8 \times 24 \times 3{,}600}{1{,}000{,}000}\right) \times 31 = 5142\,(\text{GB})$$

# Storage Calculations and Servers

## Example 1 Continued

- As can be seen this represents a large amount of data, and another strategy might need to be considered to ensure the amount of data being collected is manageable.
- In this case it might be considered that the amount of data being generated is necessary, in which case the storage provisions should be made.
- However it might be deemed more appropriate to reduce the image size/quality on half of the cameras, or to reduce the frame rate on some of the cameras.
- Another approach might be to use IR triggers or motion detection to trigger the image recording.

# CALCULATING STORAGE REQUIREMENTS

## Manual Calculation Continued

### MJPEG

**Example 1: For an 8-hour archive of a CIF video stream with 50 percent quality and 15 frames per** second, the following is the calculation:

4 KB x 15fps x 3600s = 216,000 KB/ hour

= 216MB /hour x 8 hours

= 1.728 GB

**Example 2: For a 24-hour archive of a 4CIF video stream with 100 percent quality and 5 frames per** second, the following is the calculation:

320 KB x 5fps x 3600s = 5,760,000 KB /hour

= 5,760MB /hour = 5.76GB /hour x 24 hours

= 138.24 GB

# Commissioning of Electronic Surveillance

## Verification Test

- Integrator | System Installer shall be responsible for performing the following tests prior to final acceptance of the Video Surveillance System.
- These tests shall perform at a time mutually agreeable to both a General Contractor representative (if applicable) and the System Designer:

1. Verify the following for each Camera

a. Camera produces a clear picture and is aimed per site requirements.

b. Camera maintains a clear picture and automatically compensates for changing light conditions including day/night change.

c. Camera has wide dynamic range installed where specified and operate to prevent camera blinding.

# Commissioning of Electronic Surveillance

## Verification Test Continued

1. **Verify the following for each Camera**

   d. **Camera provides complete and correct coverage of the area specified.**

   e. **Cameras are fitted with anti-tamper/ anti-vandalism devices where specified.**

   f. **Simulated tamper alarm is transmitted to the operator workstation.**

   g. **Functioning of Alarms Input(s)/Output(s) and/or connections to other systems as specified.**

   h. **Camera resolution and encoding settings are configured per minimum requirements (28 23 13) and/or as specified per project documents.**

# IP SURVEILLANCE SYSTEM MAINTENANCE

## System Maintenance

**Maintenance are actions required for preserving system function or returning system to operational state after a failure.**

- **What regular maintenance is required?**
- **Who is responsible for ongoing maintenance tasks?**
- **If cameras are placed in awkward or inaccessible locations, then maintenance could be more difficult.**
- **Health and safety regulations may also need to be consulted when carrying out maintenance operations.**
- **Thought should also be given to how often the maintenance tasks should be performed.**

**Effective and regular maintenance of a CCTV surveillance system is essential to ensure that the system remains reliable at all times. Regular maintenance by a service company, and effective failure reporting by the user, will enable potential problems to be identified at an early stage so that appropriate action can be taken**

# Safety Considerations

# System Safety Considerations

## Safe Use of System is a Must!

- Safety is a vital consideration with the deployment of all VSS components and systems; future versions of the SIA Digital Video Quality Handbook will incorporate safety guidance.
- It is recommended that DMC source devices for exterior applications be sealed from environmental impact and incorporate a minimum Ingress Protection (IP66) rating.
- Verification of temperature range, change of temperature with time, condensation, vibration, effects of wind, and other external influences must be considered in the achievement of video quality.

# System Safety Considerations

**Electromagnetic Compatibility Directive (EMC; 2004/108/EC)**

**In addition to proving compliance with other EMC performance standards noted in Section III, manufacturers must also declare conformity with the EMC Directive, as applicable.**

**A Presumption of Conformity under the EMC Directive may be achieved by demonstrating compliance with one or more of the following additional EMC harmonized standards:**

**EN 61000-6-3:2007 Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments**

**Low Voltage Directive (LVD; 2006/95/EC)**

**For video surveillance system components utilizing hazardous voltages, manufacturers must also declare conformity with the Low Voltage Directive (LVD).**

**Harmonized standards providing a Presumption of Conformity under the LVD include the following:**

# System Safety Considerations

## Application of the UL 60950-1 Standard

**Application of the UL 60950-1 standard is intended to reduce the risk of injury or damage due to the following conditions:**

- **Electric shock**
- **Energy related hazards**
- **Acoustic shock at communication receivers**
- **Fire**
- **Heat related hazards**
- **Mechanical hazards**
- **Radiation**
- **Chemical hazards**

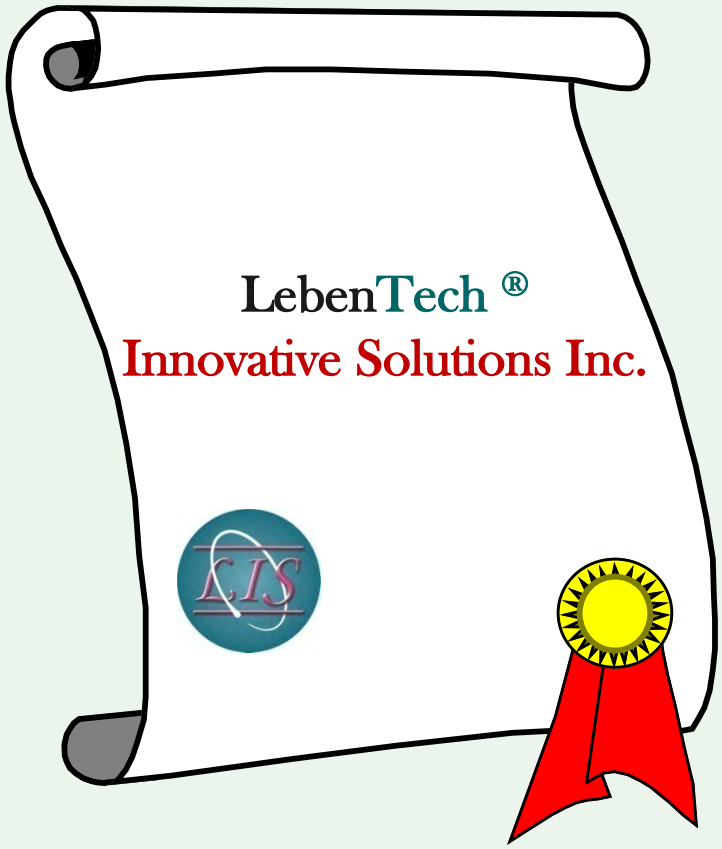
# System Safety Considerations

## Circuit Definitions

| | |
|---|---|
| Hazardous Voltage | *Any voltage exceeding 42.2 Vac peak or 60 Vdc without a limited current circuit.* |
| Extra-Low Voltage (ELV) | *A voltage in a secondary circuit not exceeding 42.4 Vac peak or 60 Vdc, the circuit being separated from hazardous voltage by at least basic insulation.* |
| Safety Extra-Low Voltage (SELV) Circuit | *A secondary circuit that cannot reach a hazardous voltage between any two accessible parts or an accessible part and protective earth under normal operation or while experiencing a single fault. In the event of a single fault condition (insulation or component failure) the voltage in accessible parts of SELV circuits shall not exceed 42.4 Vac peak or 60 Vdc for longer than 200 ms. An absolute limit of 71 Vac peak or 120 Vdc must not be exceeded.*<br><br>*SELV circuits must be separated from hazardous voltages, e.g. primary circuits, by two levels of protection, which may be double insulation, or basic insulation combined with an earthed conductive barrier.*<br><br>*SELV secondaries are considered safe for operator access. Circuits fed by SELV power supply outputs do not require extensive safety testing or creepage and clearance evaluations.* |
| Limited Current Circuits | *These circuits may be accessible even though voltages are in excess of SELV requirements. A limited current circuit is designed to ensure that under a fault condition, the current that can be drawn is not hazardous. Limits are detailed as follows:*<br><br>• *For frequencies < 1 kHz the steady state current drawn shall not exceed 0.7 mA peak ac or 2 mA dc. For frequencies above 1 kHz the limit of 0.7 mA is multiplied by the frequency in kHz but shall not exceed 70 mA.*<br><br>• *For accessible parts not exceeding 450 Vac peak or 450 Vdc, the maximum circuit capacitance allowed is 0.1 µF.*<br><br>• *For accessible parts not exceeding 1500 Vac peak or 1500 Vdc the maximum stored charge allowed is 45 µC and the available energy shall not be above 350 mJ.*<br><br>*To qualify for limited current status the circuit must also have the same segregation rules as SELV circuits.* |

# MODULE 4: DESIGN AND APPLICATION OF IP-BASED VIDEO SURVEILLANCE SYSTEM

# BASIC IP VIDEO SURVEILLANCE TROUBLESHOOTING




BY: LENNOX BENNETT

# IP Surveillance System Diagnostics

# VIDEO SURVEILLANCE DIAGNOSTICS

## Video Symptoms and Solutions

- **Faint or blurry picture with little or no color:** This symptom most often indicates loss of signal strength.
  - Check for excessive wire distance, incorrect equalization of adjustable UTP transmitter or receiver, improper camera adjustment or output level, the use of shielded wire or water damage to wire.
  - Testing for possible water in the line involves measuring the capacitance between the conductors that have been disconnected from other equipment. Cat2 or 3 wires should read 19 pf per foot or wire; Cat5 is 16pf per foot. (Example: 1000ft of Cat5 should read 16 nf or .016 µf).
- **Extremely faint picture with only shadows of an image:** There is likely a wiring problem such as an open conductor or short between conductors.
  - Verify using an ohmmeter.

# VIDEO SURVEILLANCE DIAGNOSTICS

## Video Symptoms and Solutions

**Camera is Properly Adjusted:** Set focus, iris and shutter speed using a portable monitor

**Camera is adequately Powered**

Verify the camera's input voltage is within manufacturer's tolerances under load conditions (including heaters, blowers, etc.)

With the camera connected and operating, measure the input voltage at the camera's power input terminals.

Typically, it should be higher than 21 Volts AC for a 24VAC camera, and 11.5 VDC for a 12VDC camera.

# VIDEO SURVEILLANCE DIAGNOSTICS

## Video Symptoms and Solutions

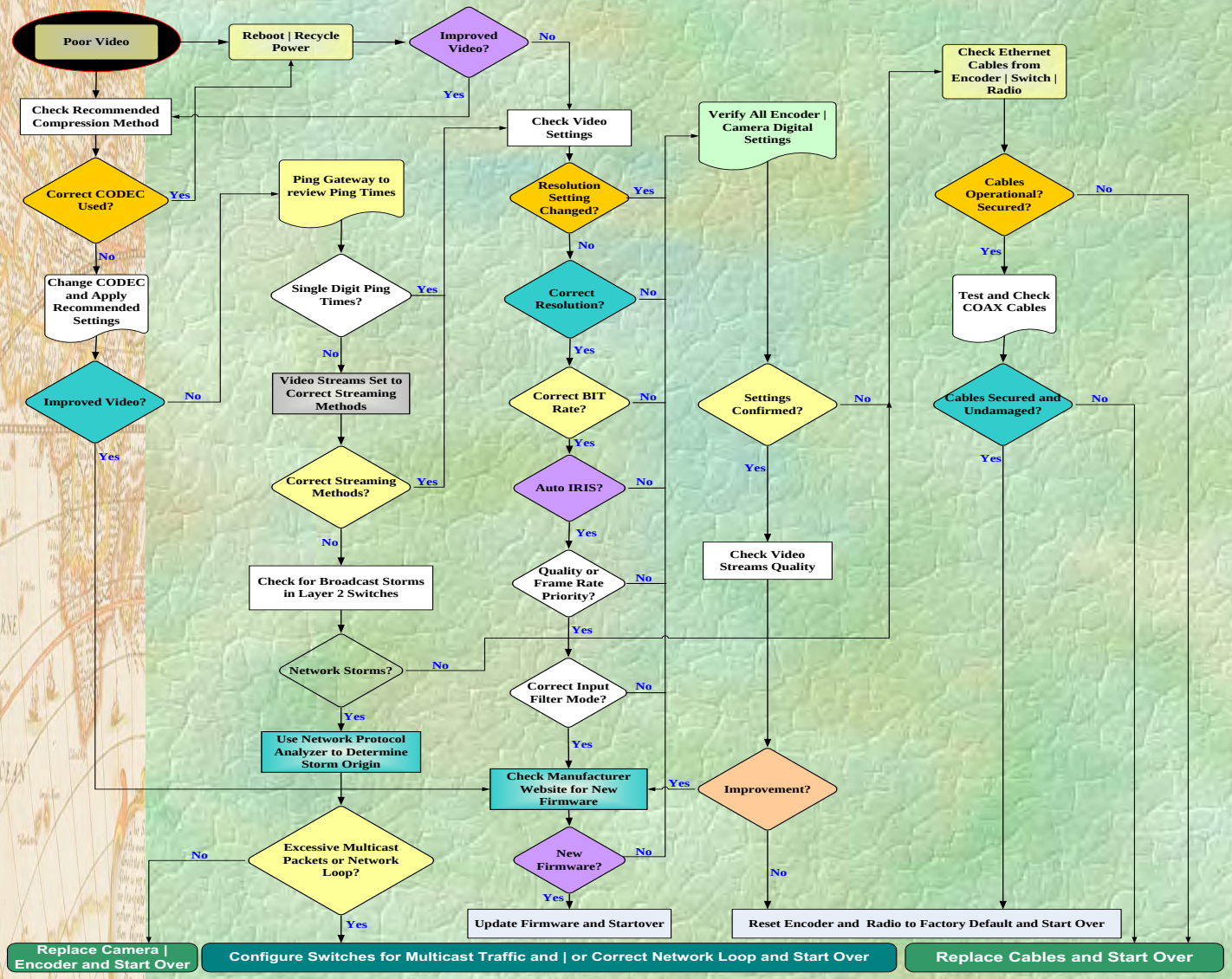
- **Random lines, noisy image or faint shadows from the image of another camera:** Crosstalk is the most likely culprit.
- **Ghosting** — faint shadows of original image shifted to the right:
  - This is an indication of an impedance mismatch, most often the result of a bridge tap — an extraneous length of dangling, un-terminated cable connected to the transmission line.
  - Locate and remove bridge taps, and check for extra conductors at punch-down connections. Ghosting can also indicate improper termination.

This image is the result of a ground loop issue

This image is the result of an interference issue

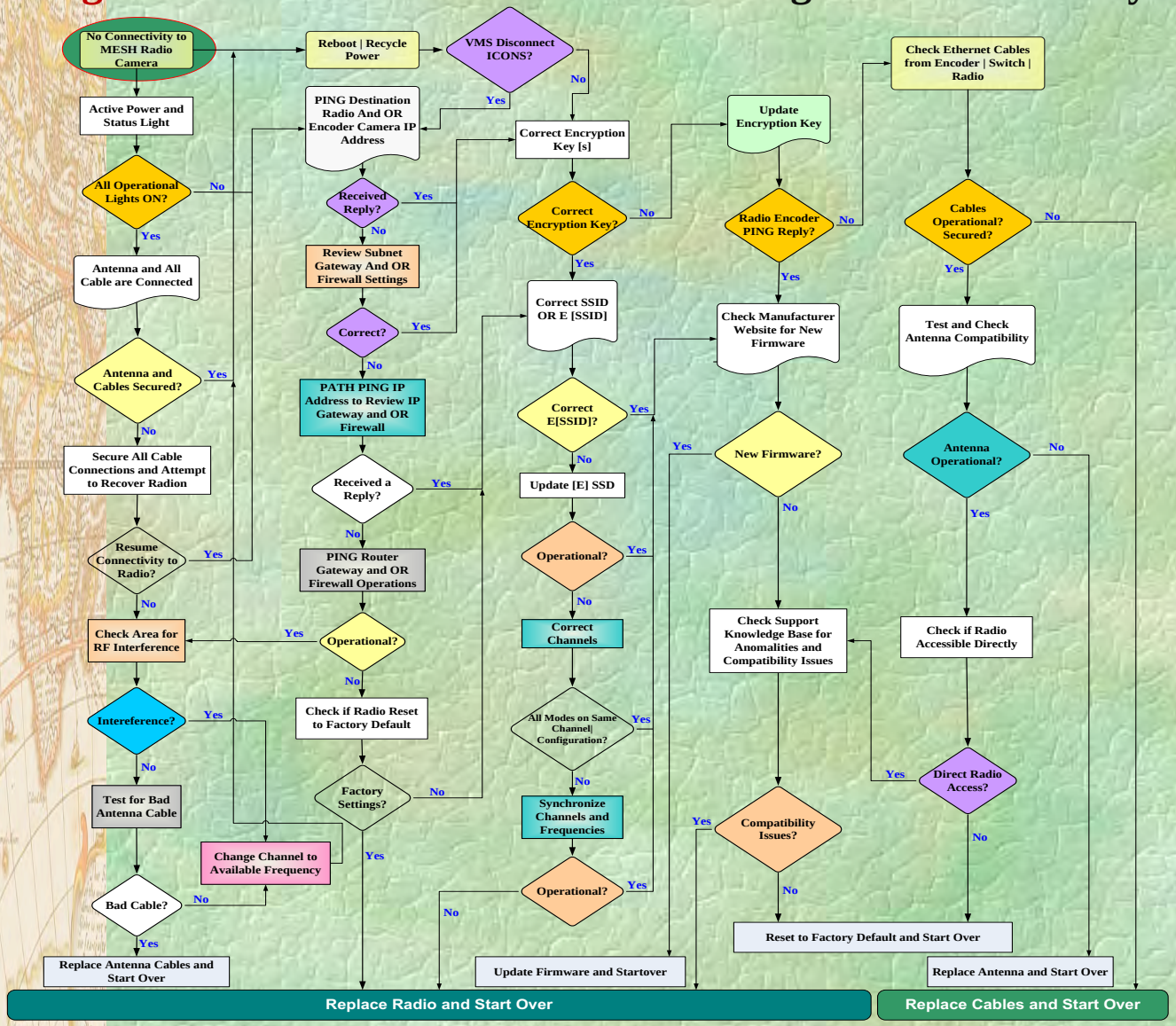
# General Problem and Solution for IP Camera

## Figure 4-1: DVS Troubleshooting – Poor Video



# General Problem and Solution for IP Camera

## Figure 4-2: Wireless DVS Troubleshooting – No Connectivity



# IP SURVEILLANCE TROUBLESHOOTING?

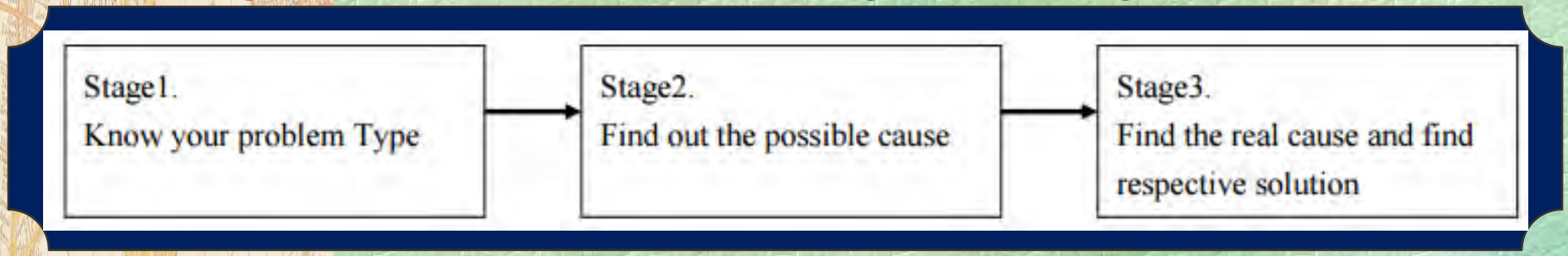
## Troubleshooting Approach

**Begin with "Define your problem type" to know what kind of problem it is and define the problem type.**

**Then follow the problem type then determine the possible causes of this type of problem.**

**After that, you can clarify what is the actual cause of the problem for a specific issue and how to solve It.**

**Figure 4-3: Process of Troubleshooting and Resolving Video Issues**



# Find your Problem Type

**Figure 4-1:** Identification and Description of Security Vulnerabilities

| IP Surveillance Solution Problem Type Table | | |
|---|---|---|
| No. | Problem Type | Description |
| 1 | Video Server/ IP camera Login | You have the IP camera / Video Server powered up but you fail to login the web-configurator to setup |
| 2 | Monitor | You can't view live images from the IP camera / Video Server |
| 3 | PTZ control | You can't control the Pan/Tilt/Zoom of the IP camera or the PTZ device connected to a video server |
| 4 | Video Quality | You don't like the quality of the video; it could be wrong color rendering, image blur, mosaic and anything about video quality. |
| 5 | Latency | You feel a lot of latency "Time difference" between the actual event and the video displayed on the monitor |
| 6 | Video Jitter | You feel the video displayed on the monitor is jumping, not smooth. |
| 7 | DIO event | 1. You can't receive DI (Digital Input) signal from sensors<br>2. You can't trigger DO device via DO. |
| 8 | MD event | 1. You can't trigger event upon Motion Event |
| 9 | Recording & Playback | 1. You can't record manually, on schedule, by motion or by event.<br>2. The recording is okay, but you can't find the recorded file. |
| 10 | NVR login (formal version) | 1. You fail to login the NVR |

# Find Out The Possible Cause

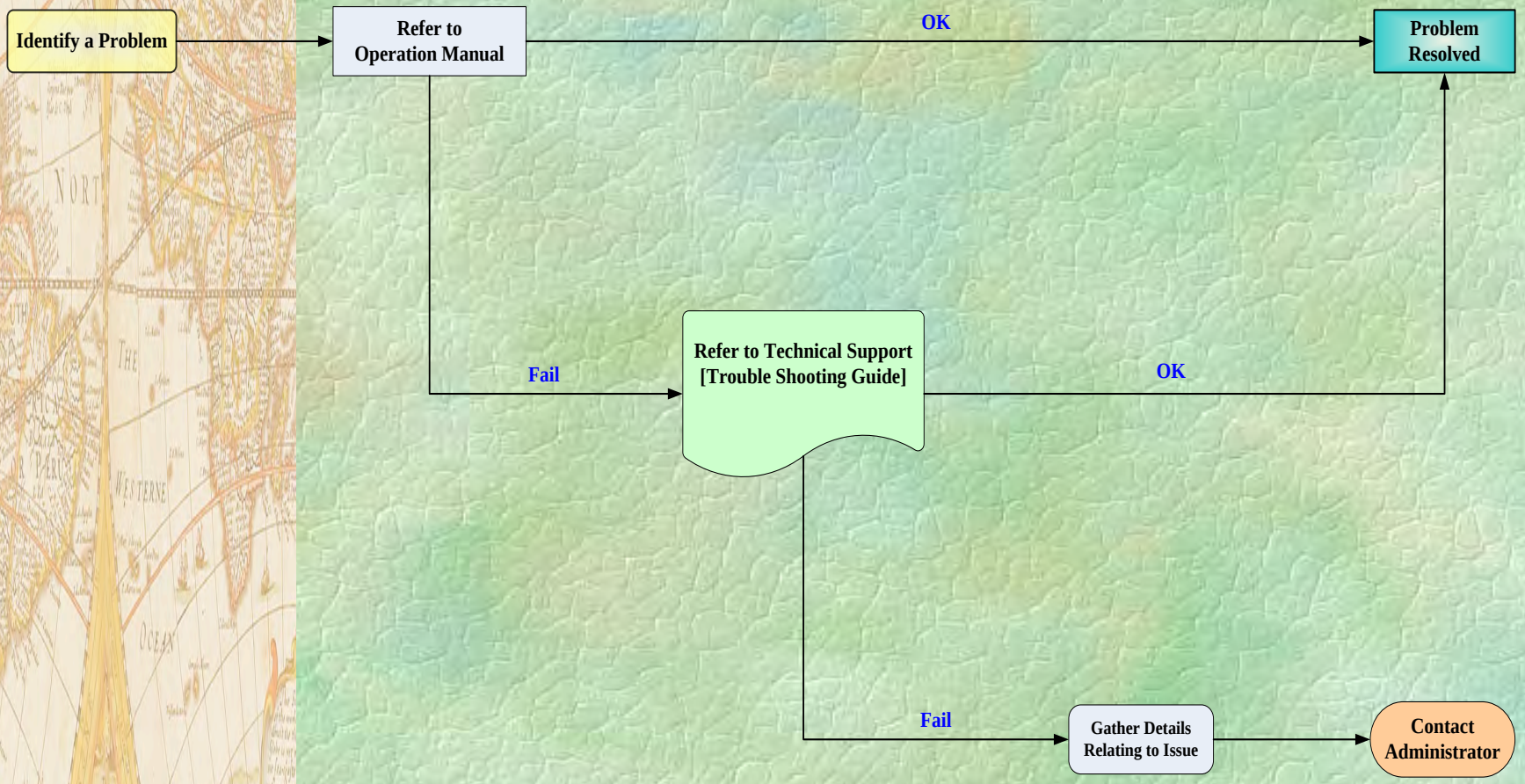
**The problem is that you can't login the Video server**

**Determine Possible Causes**

| | Check Item | Remark |
|---|---|---|
| Step1 | Check the Control Device | |
| Step2 | Connect the PC directly to the Video server/Transcoder then via cross-over cable. Then input the Video server/Transcoder to see if you can connect? | Please connect to LAN or WAN you used to connect previously |
| Step3 | Refer to the section of each problem type to do root cause clarification and find respective solutions. | |

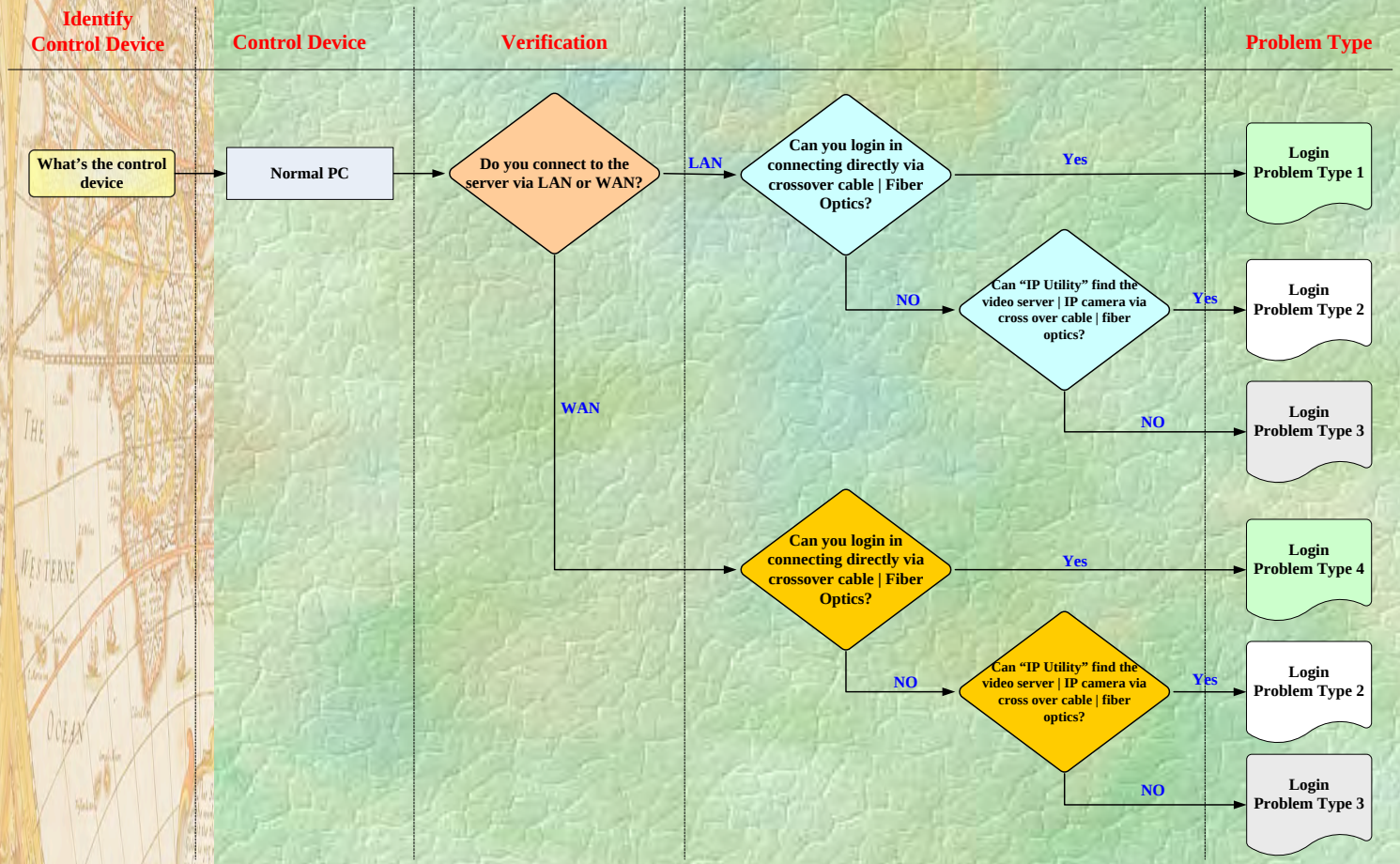
# Create a Support Ticket

**Figure 4-4:** Technical Support Work Flow



# Surveillance System Diagnostic Flow

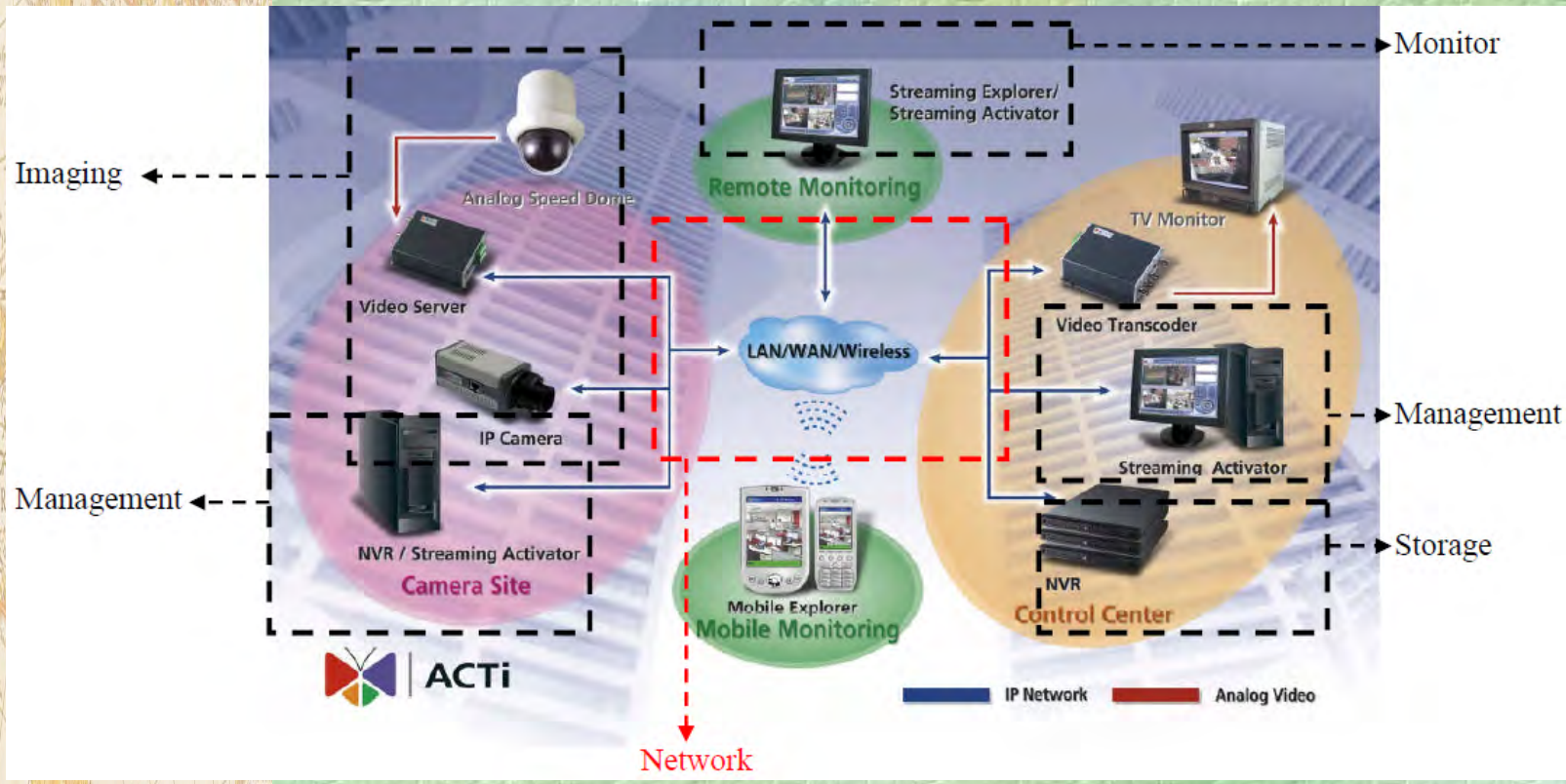
## Figure 4-5: Diagnostic Flow for Login Problems




Consult reference 6 for additional details

# Surveillance System Diagnostic Flow

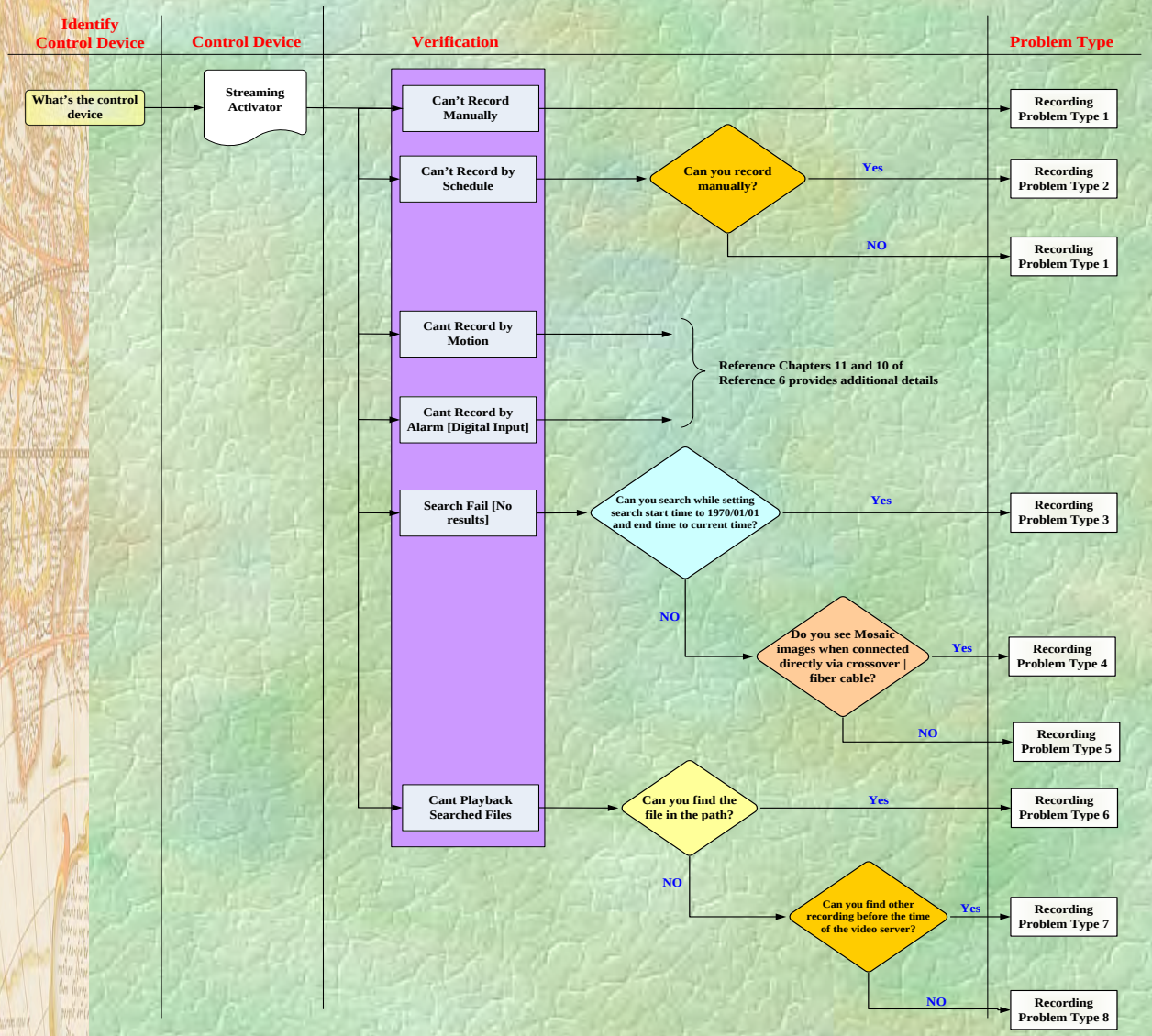
**Figure 4-6:** Potential Problem Area Identified in System Design




Source: Reference 6

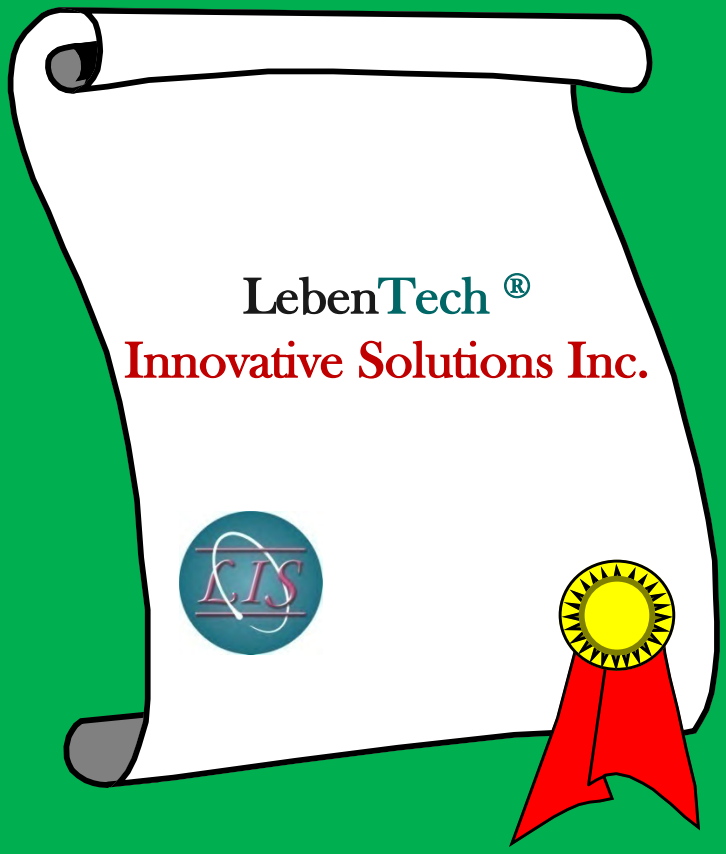
# Surveillance System Diagnostic Flow

## Figure 4-7: Diagnostic Flow for Recording Problems



# MODULE 5: DESIGN AND APPLICATION OF IP-BASED VIDEO SURVEILLANCE SYSTEM

# ADVANCEMENT IN VIDEO SURVEILLANCE TECHNOLOGIES




BY: LENNOX BENNETT

# MEGAPIXEL AND HD TECHNOLOGY

## Megapixel Camera

- **This is a general term used for any camera that has *over 1 million pixels* in the sensor.**
  - **There are many cameras that have over 1 megapixel resolution. For example, there are 2.0, 3.0, 5, 8, 10 and higher megapixel cameras.**
  - **The pixels are organized in a matrix of *horizontal and vertical* pixels. The relationship between the horizontal and vertical pixels is called the aspect ratio.**
  - **The aspect ratio (vertical to horizontal ratio) is usually 4:3 or 9:16 (wide).**
  - **For example a 1.2 Megapixel sensor on the Sony SNC-EM600 camera has 1280 horizontal pixels and 1024 vertical pixels.**
  - **The aspect ratio is 1280/1024 which is 1.24 or close to the 4/3 ratio (1.3). The 2 megapixel Samsung SND-6084 (dome camera has 1920 x 1080 pixels, and the aspect ratio is closer to 16:9.**

# NETWORK VIDEO COMPRESSION TECHNIQUES

## VIDEO COMPRESSION

- Video compression refers to reducing the quantity of data used to represent video content without excessively reducing the quality of the picture.
- It also reduces the number of bits required to store and/or transmit digital media.
- Compressed video can be transmitted more economically over a smaller carrier.

**Table 5-1:** Current and Emerging Video Compression Standards

| Video coding standards | Year developed | Publisher | Primary Intended Applications | Bit rate |
|---|---|---|---|---|
| H.261 | 1990 | ITU | Video telephony and teleconferencing over ISDN | $p \times 64$ kb $sec^{-1}$ |
| MPEG-1 | 1991 | ISO/IEC | Video on digital storage media (CDROM) | 1.5 Mb $sec^{-1}$ |
| MPEG-2 | 1994 | ISO/IEC | Digital television | 2-20 Mb $sec^{-1}$ |
| H.263 | 1996 | ITU | Video telephony over PSTN | 33.6 kb $sec^{-1}$ and up |
| MPEG-4 | 1998 | ISO/IEC | Object-based coding, synthetic content, interactivity, video streaming | Variable |
| MPEG-7 | 2001 | ISO/IEC | Real-time and non-real time applications, to tag the contents and events of video streams for more intelligent processing in video management software or video analytics applications | Variable |
| H.264/AVC | 2003 | ITU-T/ ISO/IEC | Improved video compression | 10's to 100's of kb $sec^{-1}$ |

# APPLICATION OF VIDEO COMPRESSION

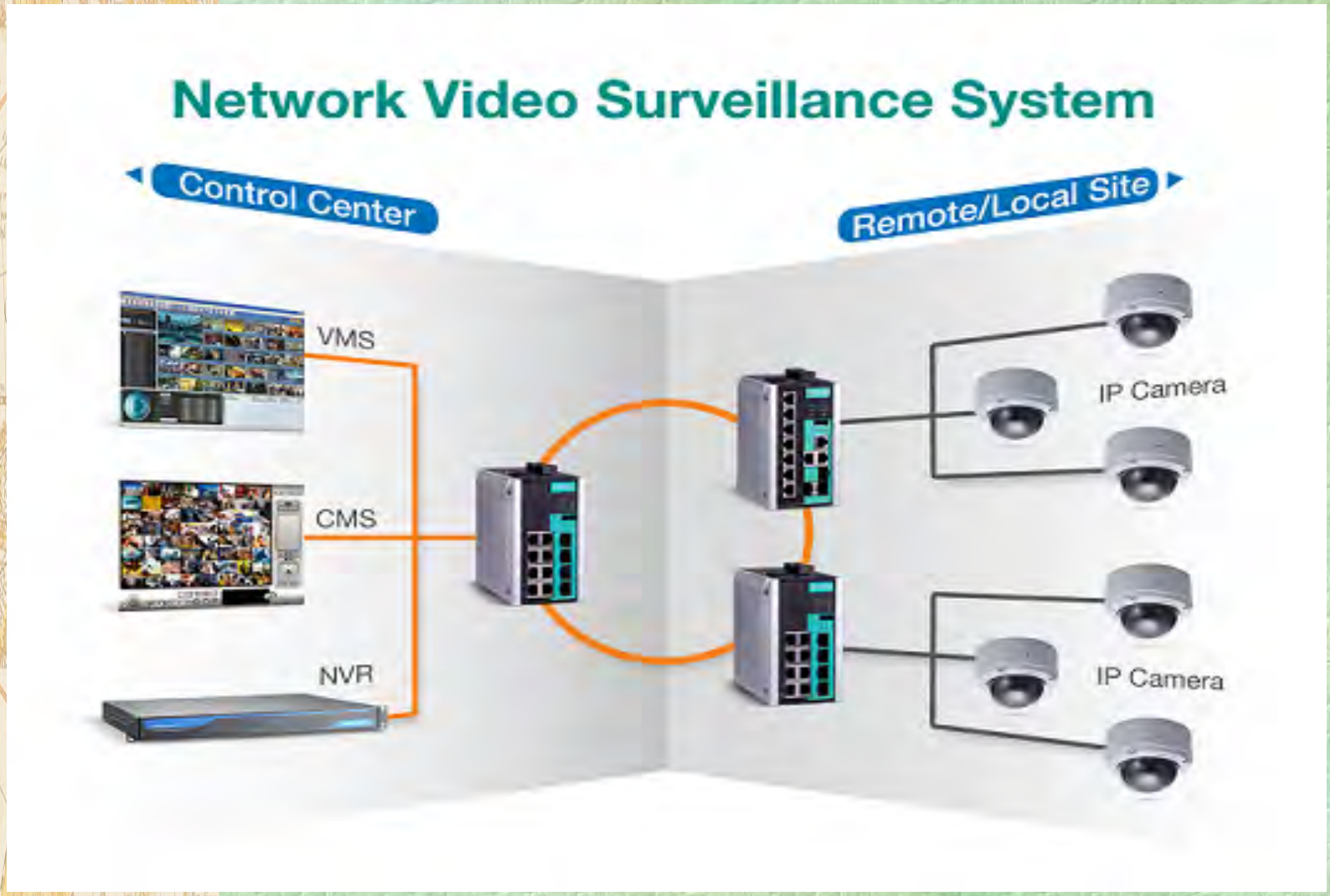
**Table 5-2: Compression Technology Selection by Application**

| Application | Resolution | Image Rate | Compression Technology |
|---|---|---|---|
| Parking Lot | 16 MP | 3 | JPEG2000 |
| Cafeteria | 5 MP | 7 | JPEG2000 |
| Lobby | 3 MP | 7 | JPEG2000 |
| Doorway | 2 MP | 15 | H.264 |
| Hallway | 1 MP | 15 | H.264 |
| Casino | 1 MP | 30 | H.264 |

**Image and video compression techniques reduce high bit rates and large file sizes associated with digital video, allowing efficient transmission and storage of video data. Compressed files are easier to transmit over a network and easier to store.**

# VMS Software

# USE OF VIDEO Management SOFTWARE



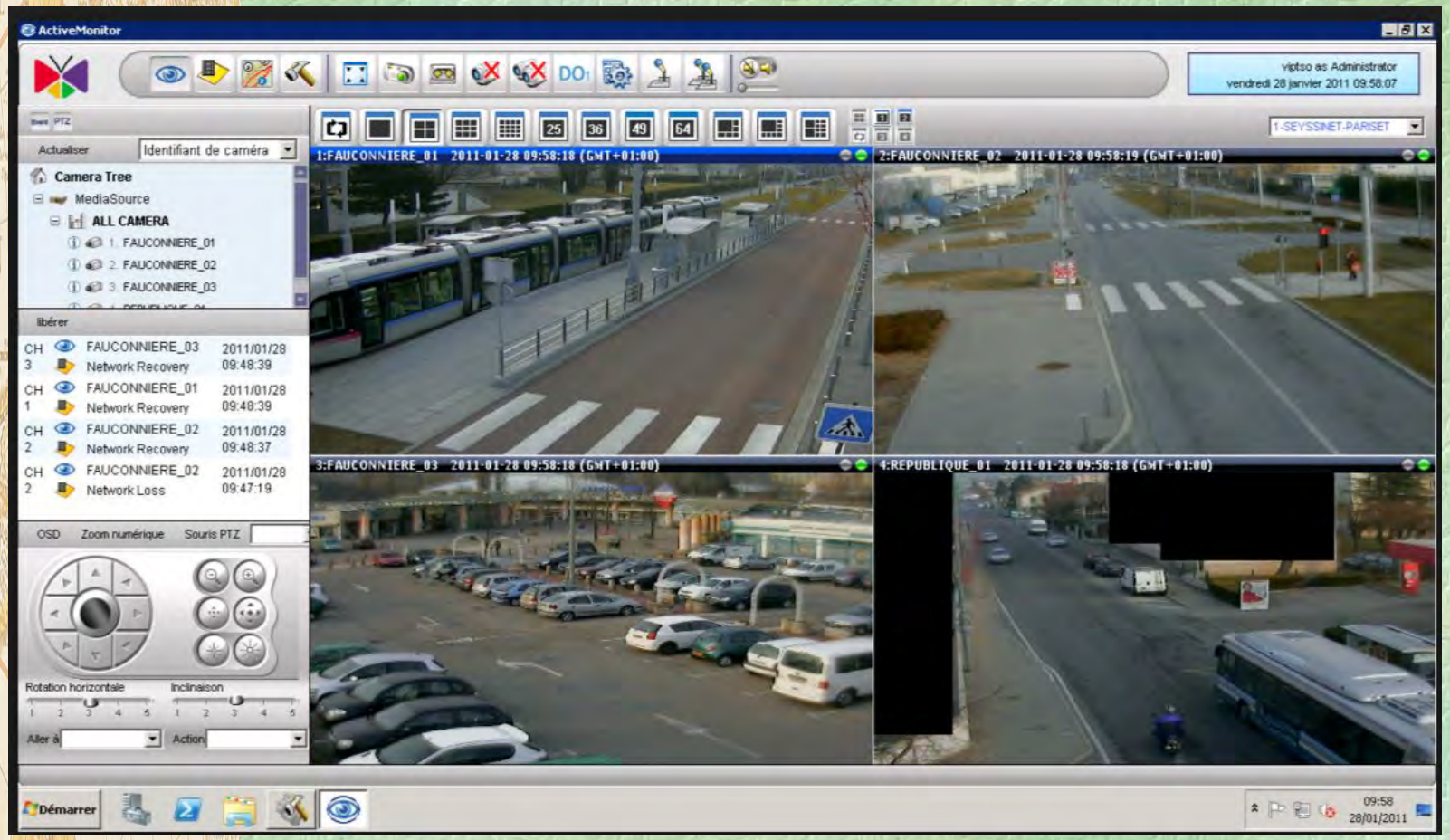
# VIDEO Management SOFTWARE - VMS

## Video Management Software

- Video Management Software products record video stream data from networked cameras and encoders and route that video data to the appropriate storage resource and video playback monitors.
- They also provide camera and user administration. The products display live video in graphical user interfaces (GUIs), provide various camera control functions such as pan/tilt/zoom (PTZ) and enable searching for recorded video.
- Product differentiators include scalability, network management, fault tolerance, operating system, client software support, and the use of standard conventions and protocols.

# VIDEO Management SOFTWARE - VMS

**Figure 5-1:** Screen Shot of a CMS Software Application



# VIDEO Management SOFTWARE Functions

## Primary VMS Functions

- Camera Video.
  - Record
  - Export
  - Playback
- Camera Management.
- Motion Detection | Alerts

## Optional VMS Functions

- Video Analytics.
- License Plate and | or Facial Recognition.


- Integration with Access Control and | or POS

**Select surveillance video management software with the quickest, easiest-to-use, most relevant search and retrieval utilities.**

# Video Analytics

# FUNDAMENTALS OF VIDEO ANALYTICS

## Intelligent Video Analysis

- By using Intelligent Video Analysis, the user can detect targeted moment from a video sequence.
- Video analysis types provided by Samsung Network Cameras are described below:
  - Motion Detection

    Most of cameras provide this feature; detects motion on the video.
  - Audio Detection

    Detects audio on the video
  - Face Detection

    Detects human face on the video
  - Tampering
- Detects tampering attempts, such as sudden change of camera's viewing direction, blocked lens and other overall change to the scenes on the video.

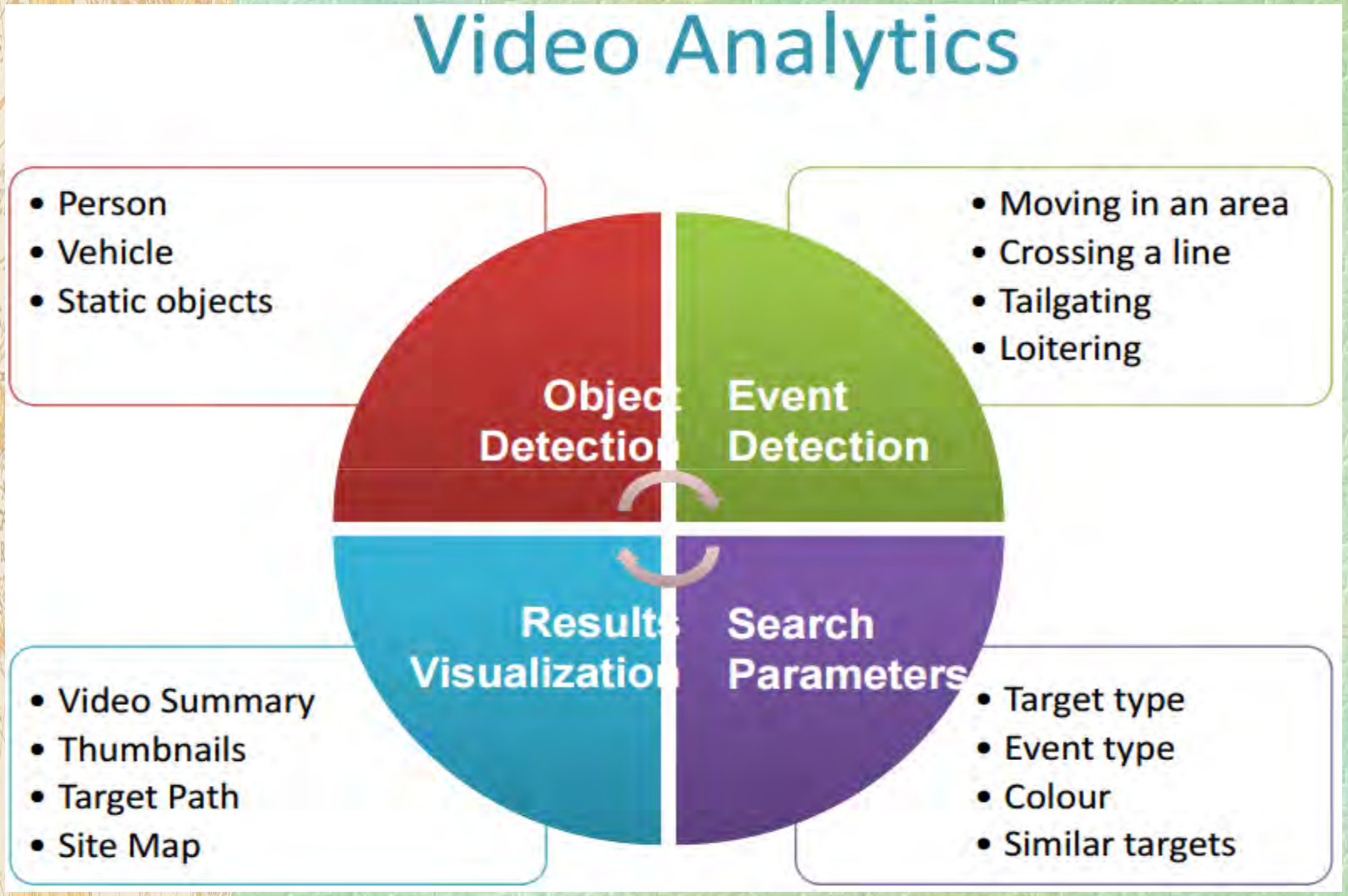
# FUNDAMENTALS OF VIDEO ANALYTICS

## Overview

- Enhancing a digital video management system with analytics enables an organization to cost efficiently and proactively monitor large video surveillance installations.
- Rather than relying on the operator to look at the right camera view precisely when an event is occurring, an analytics enabled system can deliver the event—or a series of events—in progress for assessment and action.
- Visual, audible, and messaged alerts can bring potential threats to the attention of the appropriate personnel very quickly.
- An assessment of the situation and the type of response needed can be initiated accordingly. Digital files of the alerts may be displayed and then stored for future search and retrieval.

# FEATURES OF VIDEO ANALYTICS

**Figure 5-2:** Capabilities of Video Analytics Application



# APPLICATIONS OF VIDEO ANALYTICS

## Detection And Recognition Functions

- Applications that use video analytics can perform complex repetitive functions like object detection and recognition on many channels of video simultaneously.
- A very popular video recognition solution that runs either as an embedded network camera application or in the VMS is Fixed License Plate Capture and Recognition (LPR/LPC).
- This specialized app captures license plate information for immediate processing by License Plate Recognition (LPR) software.
- The software may run in a rapid acquisition mode and compare plates later against an approved list or perform the recognition sequentially, as the vehicles pass within the camera field of view.
- In either case, LPR is a mature application embraced by law enforcement, electronic toll collection and parking management applications.
- Embedding this function reduces cost and allows for greater flexibility

# License Plate Recognition

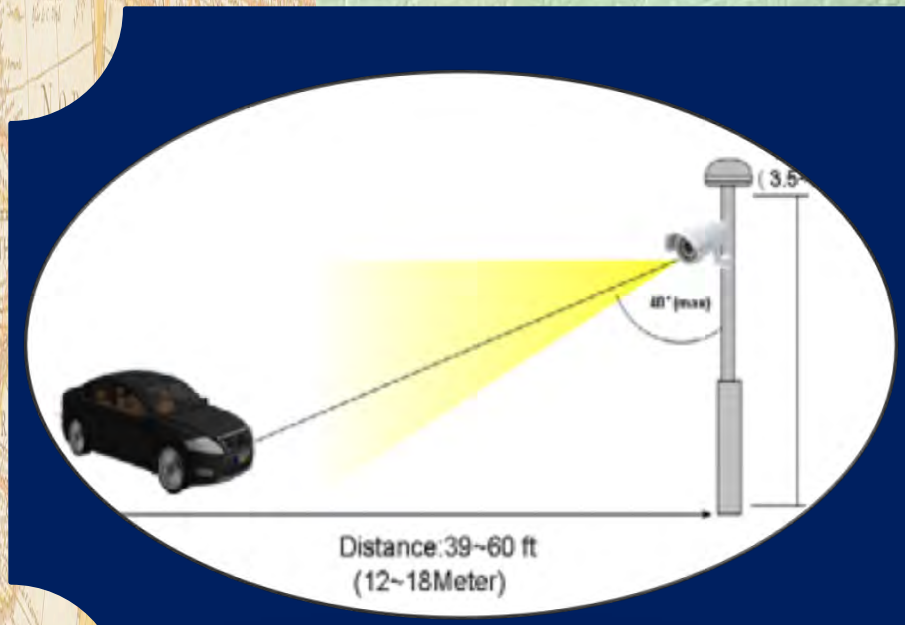
# License Plate Recognition Application

## What is License Plate Recognition?

- License plate capture cameras, also known as license plate recognition / LPR cameras, are a specialized IP/CCTV camera that has built in software to help identify and record license plates on still or moving vehicles.
- When considering a License Plate Recognition Camera or LPR, there are some very important key points that must be considered prior to purchasing CCTV Camera Pros LPR cameras.
- To increase recognition accuracy, there are certain criteria that need to be considered, such as distance, vehicle speed, plate size, lighting condition and camera angle.
- Intelligent traffic modes built into specialized license plate recognition cameras allows the camera to compensate for speed, weather, and headlight issues which all make it challenging to capture a usable video that identifies license plate.
- Used primarily in traffic monitoring in parking lots and gated security entrances, this allows the camera to capture a license plate number which is then compared to a database.

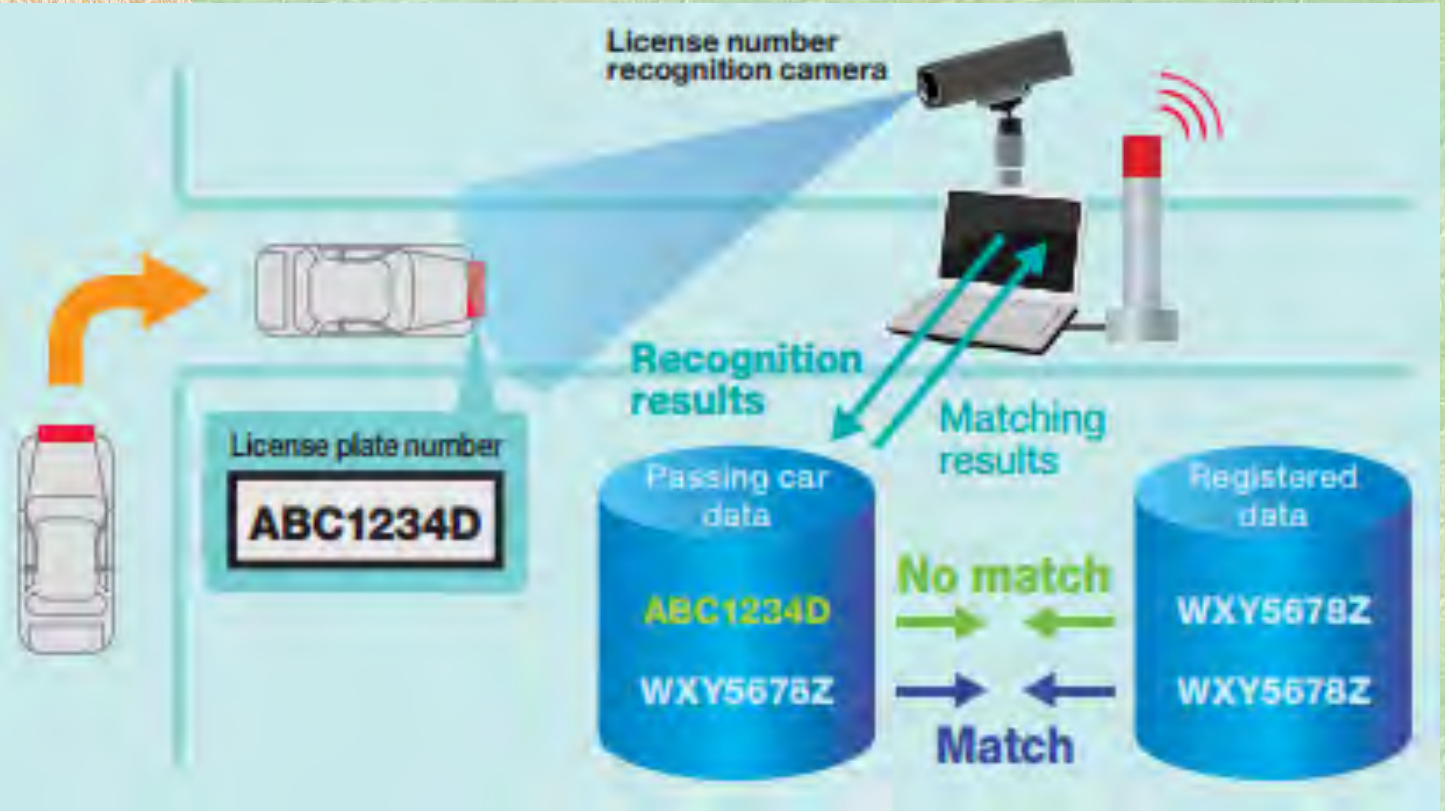
# License Plate Recognition Application


**Figure 5-3:** Principle of License Plate Recognition




# License Plate Recognition Application

**Figure 5-4:** How License Plate Recognition System Works




Source: NEC Corporation – Automatic Number Plate Recognition Solution: Cat. No. C01-12030006E [Used only for illustration]

# License Plate Recognition Application

**Figure 5-5:** Police on Patrol Utilized ALPR from Police Car


https://youtu.be/DKXp5FXVBDA

# License Plate Recognition Application

**Figure 5-6:** Application of ALPR for Traffic Management

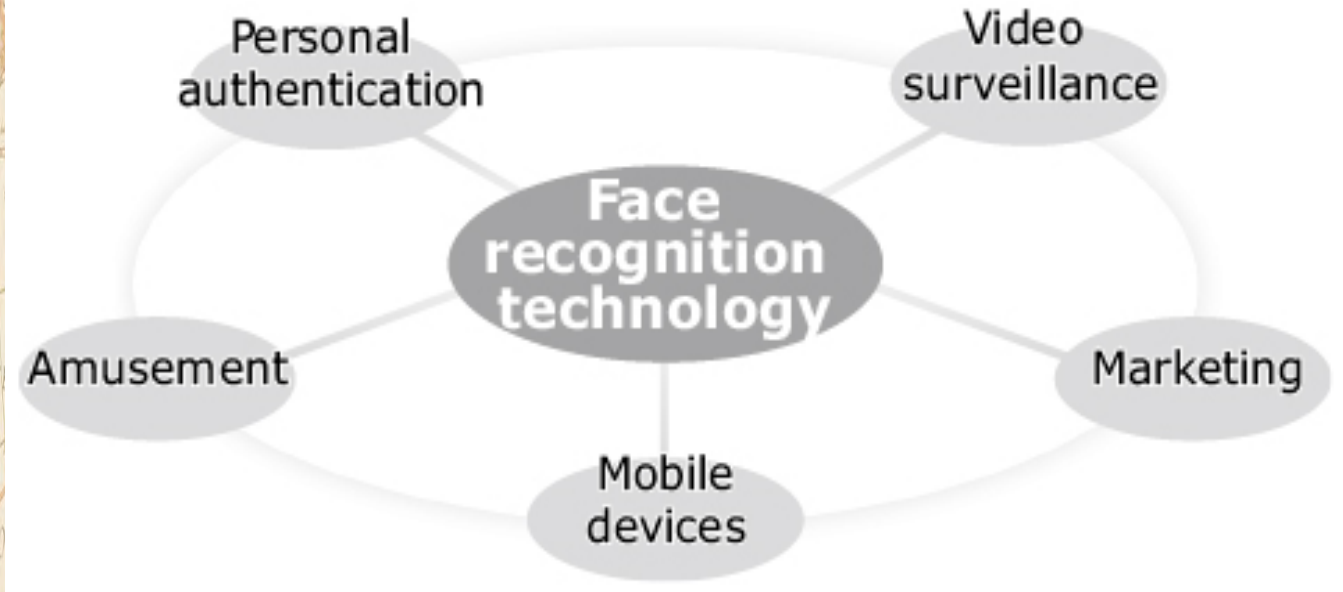

https://youtu.be/CnVwqPTwO8k

# USE OF FACE RECOGNITION TECHNOLOGY

## Introduction

- A sharp increase in crime on a worldwide scale has increased the opportunities for using the face recognition technology.

**Figure 5-7:** Wide Applications of Face Recognition Technology.



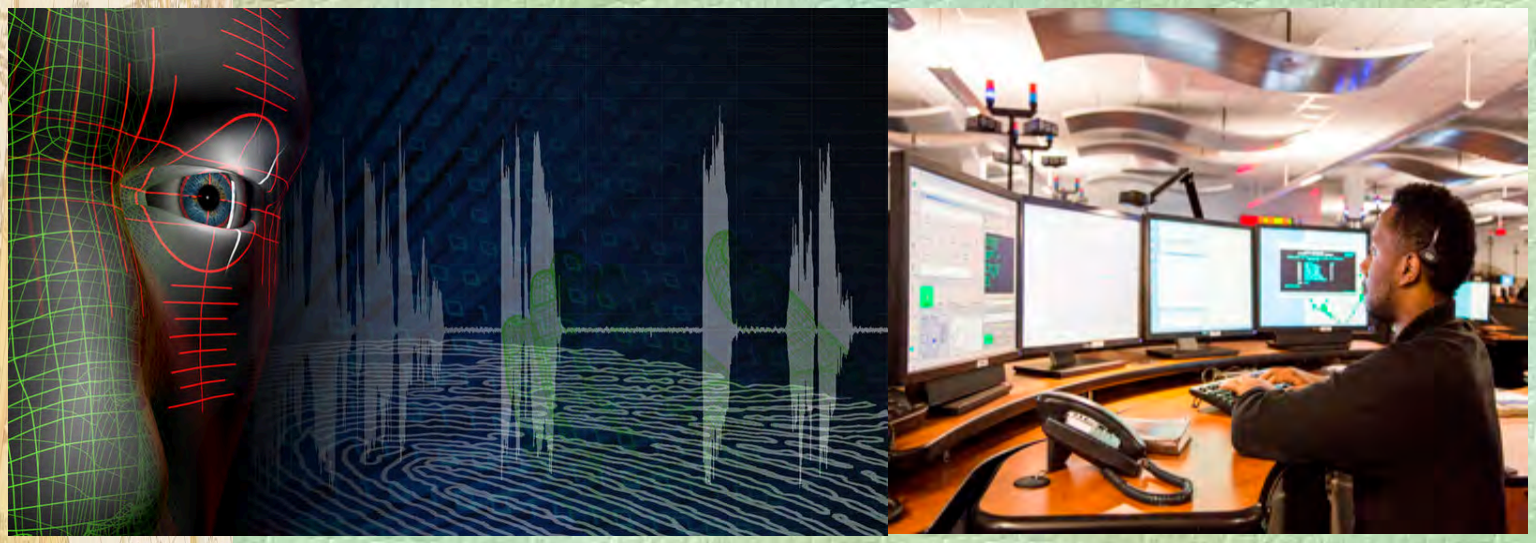

- Figure 5-6 shows typical scenarios of face recognition systems for surveillance purposes.

# USE OF FACE RECOGNITION TECHNOLOGY

## Introduction Continued

- This technology makes it possible to find each person registered in the system in video images shot in various situations including in a passageway, elevator and staircase.
- The wide variety of usages for which it can be applied include scenarios such as crime investigation, the straying of children and dementia patients.

**Figure 5-8:** Video Surveillance Monitoring



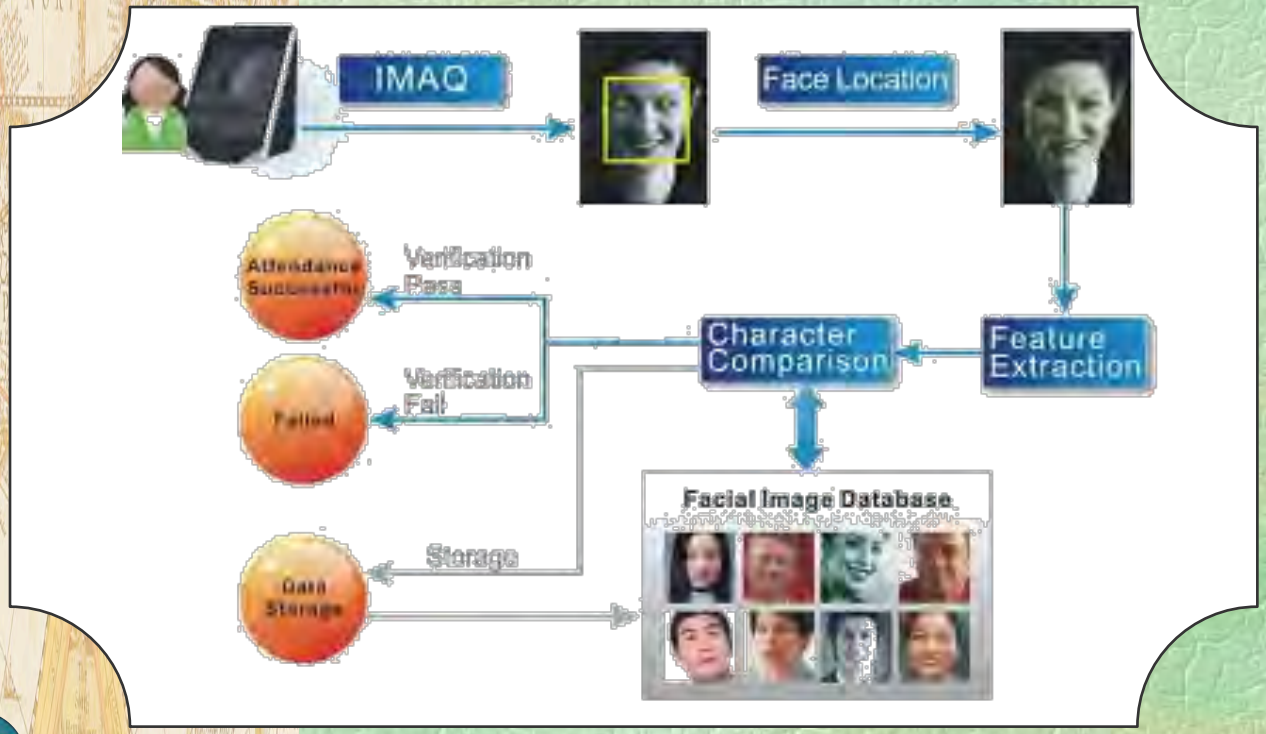
# Results of Face Technology Application

**Figure 5-9:** Illustration of Facial Recognition Match

# USE OF FACE RECOGNITION TECHNOLOGY

## Working Principle

- The face recognition is a biological recognition technology which uses a video camera or camera to capture images or video streams with faces.
- And then these faces are detected and tracked via relative technologies in terms of image acquisition (IMAQ), face location, face identification preprocess, storage and comparison to verify a variety of identities




# Facial Recognition Technology Application

**Figure 5-10:** Facial Recognition System Functions and Capabilities


# RISK CATEGORIZATION OF POLICE USE

## A Risk Framework For Law Enforcement FR

- In this section, we categorize police uses of face recognition according to the risks that they create for privacy, civil liberties, and civil rights.
- Some uses of the technology create new and sensitive risks that may undermine longstanding, legally recognized rights.
- Other uses are far less controversial and are directly comparable to longstanding police practices. Any regulatory scheme should account for those differences.

# RISK CATEGORIZATION OF POLICE USE

**Table 5-3:** Risk Framework for Law Enforcement Face Recognition

| DEPLOYMENT | | LESS RISK | MORE RISK |
|---|---|---|---|
| MODERATE RISK | **Stop and Identifty** (Mug shot Database) | • Targeted Search<br>• Targeted Database<br>• Transparent | • Real-Time<br>• Novel Use |
| | **Arrest and Identify** (Mug shot Database) | • Targeted Search<br>• Targeted Database<br>• Established Use | • Invisible |
| | **Investigate and Identify** (Mug shot Database) | • Targeted Search<br>• Targeted Database<br>• After-the-Fact<br>• Established Use | • Invisible |
| HIGH RISK | **Stop and Identify** (License Database) | • Targeted Search<br>• Transparent | • Dragnet Database<br>• Real-Time<br>• Novel Use |
| | **Arrest and Identify** (License Database) | • Targeted Search | • Dragnet Database<br>• Invisible<br>• Novel Use |
| | **Investigate and Identify** (License Database) | • Targeted Search<br>• After-the-Fact | • Dragnet Database<br>• Invisible<br>• Novel Use |
| VERY HIGH RISK | **Real-Time Video** Surveillance | • Targeted Database | • Dragnet Search<br>• Invisible<br>• Real-Time<br>• Novel Use |
| | **Historical Video** Surveillance | • Targeted Database<br>• After-the-Fact | • Dragnet Search<br>• Invisible<br>• Novel Use |

# RISK CATEGORIZATION OF POLICE USE

## High Risk Deployments

- High risk deployments are quite similar to moderate risk deployments except for the databases that they employ.
- When police or the FBI run face recognition searches against the photos of every driver in a state, they create a virtual line-up of millions of law-abiding Americans and cross a line that American law enforcement has generally avoided.

# NYPD USE OF FACIAL TECHNOLOGY

**Figure 5-11:** Police Officer Illustrating use of FR Technology

NYPD Det. Roger Rodriguez shows how a simple photo from a security camera was enhanced with facial recognition software to rotate and create a straight-on image. It then matched with a person in the database. In this case from 2013, the man was eventually sentenced on burglary charges.

# NYPD USE OF FACIAL TECHNOLOGY

**Figure 5-12:** Screens show the NYPD facial recognition unit's active cases in New York and along the East Coast

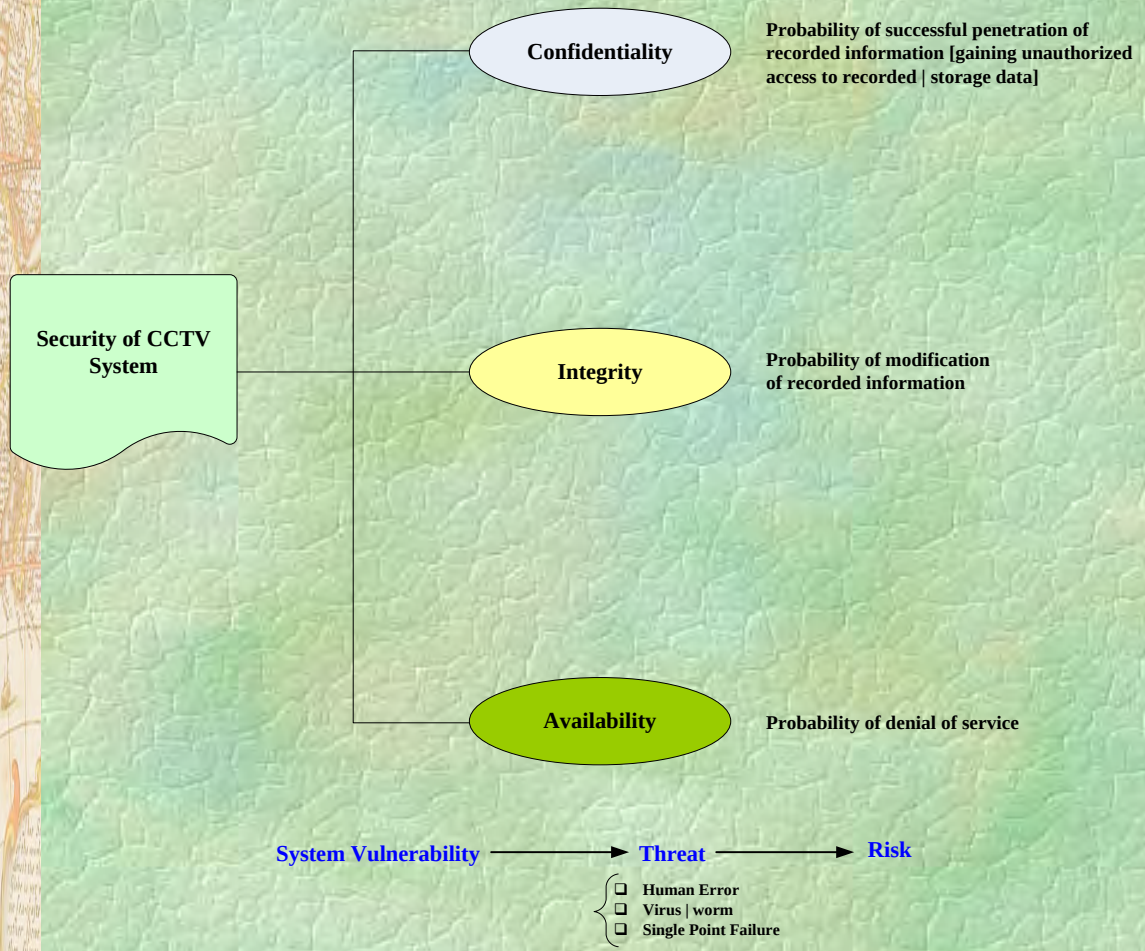
# NYPD USE OF FACIAL TECHNOLOGY

**Figure 5-13:** The NYPD posts signs when an entire area is under video surveillance, such as the base of the Brooklyn Bridge.

# Reliability Analysis

# Reliability Analysis of Video Surveillance System

**Figure 5-14:** Metrics for Security Attributes Analysis



# Reliability Analysis of Video Surveillance System

## Introduction

- Whilst it is important to continually review an IP Video Surveillance system to ensure it continues to function correctly and that the relevant sites outcomes continue to be met.
- It is also equally important to maintain the IP Video Surveillance system to ensure its ongoing reliability.

# Reliability Analysis of Video Surveillance System

## Characteristics of the CCTV Systems

- The IP-Closed Circuit Television (CCTV) is used as a surveillance system in selected districts in the country.
- It is a set of technical and program measures designed for observing, detecting, recording, and signaling conditions indicating the existence of danger.
- Given that the elements of system are responsible for safety, they should keep their usability.
- Therefore, the reliability and maintenance analysis of these systems/components are important.

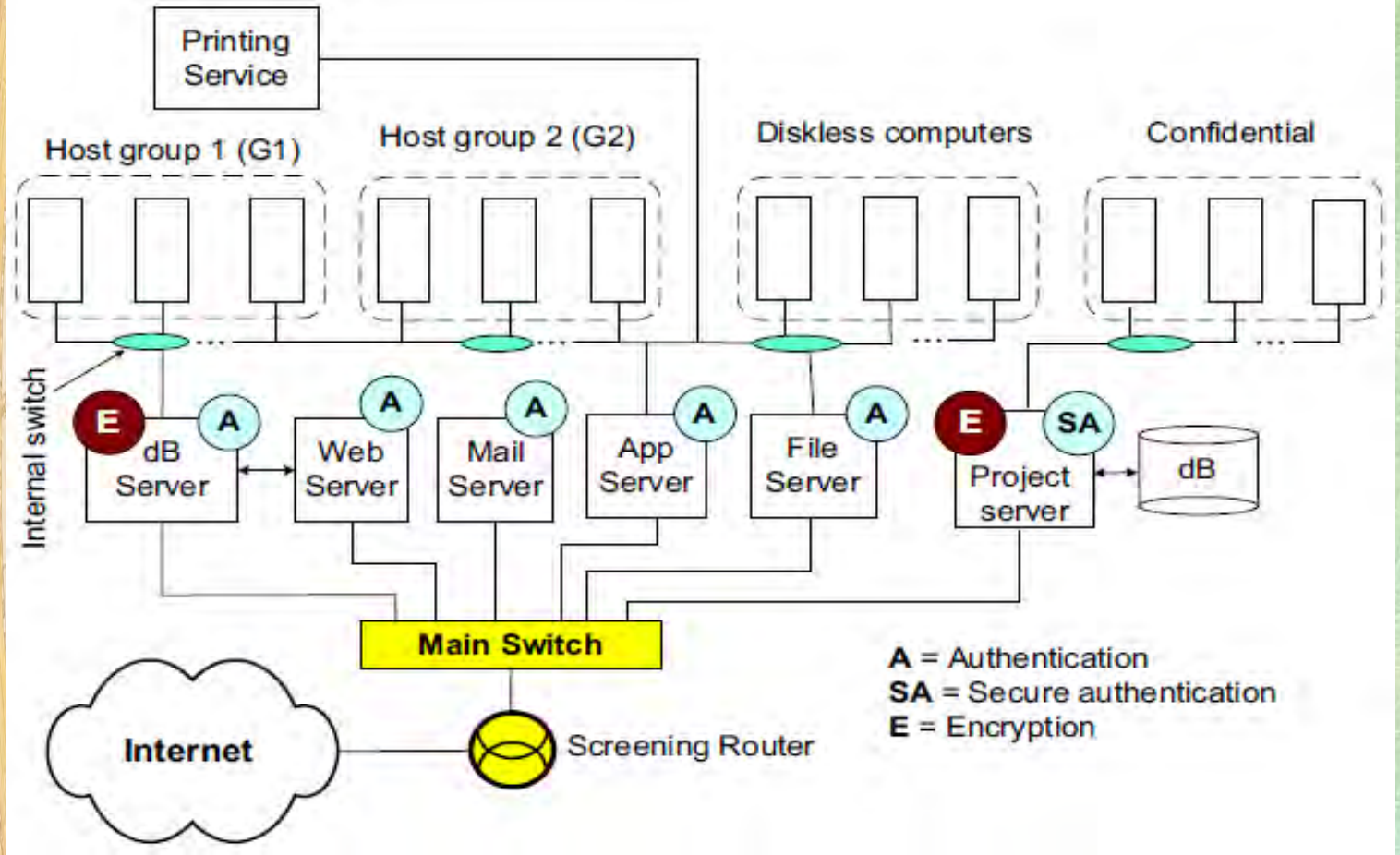
# SYSTEM RELIABILITY DEFINITION

## How Reliable is your Video Surveillance System?

- Reliability is defined as the probability that a given system operates properly for a specified period of time.
- As a companion definition to reliability, availability of a system or its users is defined as the relative frequency that the system works.
- Here, the percentage of the successful uptimes of a system is considered as a measure of the system reliability.
- From another perspective, unavailability is a probabilistic measure defined to be the probability that a system fails during a specified period of time.

# Network Assessment Perspective

**Figure 5-15:** A Topological Diagram of a Network under Reliability Analysis




As can be seen in Fig. 1, some components are tagged with A, SA, and E. These specify the protection type for the tagged component. Attacks to confidentiality and integrity of information systems are far difficult to employ but nevertheless important. Confidentiality and integrity measures are mostly implemented to ensure the security of mission critical systems, and require rather different approaches to analyze them.

# SYSTEM PERFORMANCE ASSESSMENT

## Example Application

- An IP-CCTV video surveillance system was installed for a time period of 6 months | 4380 operating hours.
- An analyst documented the failures that occurred during this time period. These are shown in table 5-3.
- Operational requirements specify 95% reliability @ 90% confidence over 10 years.
- The operational requirements also specifies at lest 99.5% availability over 10 years.
- Using the information provided determine the VS System reliability and availability based on performance over the 6 months it is in service.

# SYSTEM PERFORMANCE ASSESSMENT

## Table 5-4: Hypothetical Failure Data for VSS

| No | Incident | Time in Service (Hrs) | Failure Category | | Repair Time (Hr) |
|---|---|---|---|---|---|
| | | | Component | System | |
| 1 | Battery failure | 3840 | √ | | 12 |
| 2 | Network Issue | 310 | | √ | 1.5 |
| 3 | Channel Image Disappear | 543 | | √ | 0.5 |
| 4 | Image keeps flickering or disappearing | 180 | | √ | 1 |
| 5 | Only ¼ cameras display image | 12 | √ | | 0.5 |
| 6 | Battery failure | 3790 | √ | | 13 |
| 7 | Optical fiber transceiver | 10 | √ | | 0.5 |
| 8 | Power cable connection | 336 | √ | | 2.5 |
| 9 | Extremely faint picture with only shadows of an image | 1250 | √ | √ | 1 |
| 10 | NVR cant find or discover New IP Camera | 72 | | √ | 0.5 |
| 11 | Connection time-out error | 432 | √ | | 2 |
| 12 | Cant find IP camera when operator use search software | 2 | | √ | 1.25 |
| 13 | Solar controller failure | 4000 | √ | | 10 |
| 14 | PoE IP camera cant see at night | 24 | | √ | 0.75 |
| 15 | Cant visit IP camera from internet | 6 | | √ | 3 |

# SYSTEM AVAILABILITY ANALYSIS

## Basic Definition of Availability

- Availability is defined herein as the probability that the system is available when needed [i.e., it is already operating or is ready to operate when needed].
- System Operational Availability is calculated using equation below:

$$A_o = \frac{MTBM}{MTBM + MDT} \times 100\%$$

- Where:
  - $A_o$ – Operational Availability
  - MDT – Mean Downtime
  - MTBM – Mean Time Between Maintenance

# SYSTEM AVAILABILITY ANALYSIS

## Basic Definition of Availability

- Uptime is defined as the time that the system is in the customer's possession and works.
- Downtime is the total number of hours the system is not operable or usable.
- It should be noted that is the system is installed at the customer's selected location but does not work, or is awaiting repair/fix then it is not available.
- Alternatively system availability can be determined using equation below:

$$A_o = \frac{\text{Total System Uptime}}{\text{Total System Uptime} + \text{Total Downtime}} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \times 100\%$$

# SYSTEM AVAILABILITY ANALYSIS

## Determine Operational Availability

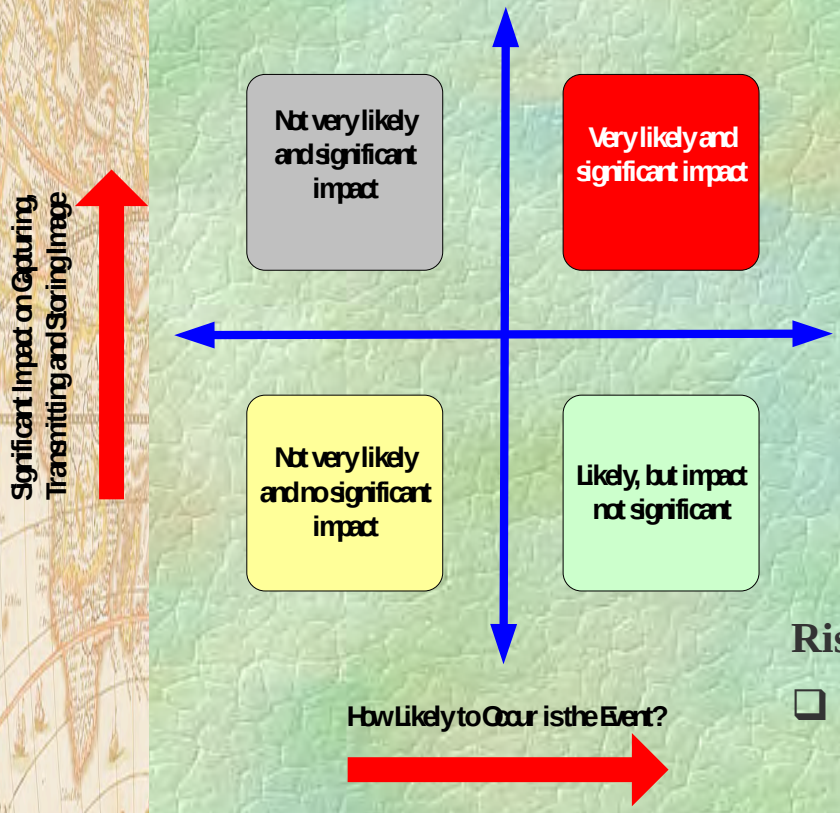
- The VS System has been installed for 6 Months | 4380 Hours. This is the system uptime.
- There were 15 failure incidents requiring 50 hours of diagnostics and repair. Reference table 5-3.
- Six [6] hours were associated with delay/waiting time for obtaining batteries and solar controller.
- Substituting respective values in equation system availability can be determined:

$$A_o = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \times 100\% = \frac{4380}{4380 + (50 + 6)} \text{ x } 100\% = 98.74\%$$

- Let's say the system operational availability requirement is 10 years with 99.5% availability. Not a good start here!

# Reliability Analysis of Video Surveillance System

**Figure 5-16:** Severity | Probability Risk Matrix




Consider each possible risk associated with observe, detected, identify or recognize a target and design a video surveillance system directed to reducing their impact and severity

## Risk Assessment

- ***What is the realistic likelihood of the activity happening?***
  - Low / medium / high
- ***What would be the consequences if the activity was not monitored and/or recorded?***
  - Minor / moderate / severe

# High Performance Industrial Network to Ensure

## Uninterrupted IP Surveillance

- **Availability** - Network availability directly affects the bottom line, and needs to be a primary requirement in any network design. For non-stop operation and minimize system downtime, it is recommend using millisecond-level network redundancy for both wired and wireless Ethernet devices.
- **Infrastructure** - A layered edge-to-core architecture (edge, distribution, and core) will enhance network flexibility, scalability, and manageability, which allow operators to easily plan for storage, bandwidth, and redundancy requirements to quickly deploy future surveillance network expansions.
- **Security** - Cyber security is a requirement for any network infrastructure. In addition to using secure routers to provide firewall/VPN to deny unauthorized access, 802.1x or port-based authentication can be applied to IP surveillance applications with high security requirements.
- **Efficiency** - To increase network efficiency, the following network features are recommended:

# Risk Assessment of Video Surveillance System

## Risk Analysis

- The security risk assessment should be structured in such a way that it provides sufficient information from development to operation and management of the video surveillance system.
- The designer needs to consider the security requirements of the VSS in the initial design phase of the project and imbed as many security features as possible into the original design concepts, prior to installation.
- The risk assessment process evaluates all external and internal factors and the standard approach is to assess the risk in a systematic manner, from the hardware and software interface to the security risks.
- The risk assessment needs to take into account the various operational requirements of the network video surveillance system and must be performed with the appropriate personnel with relevant experience.

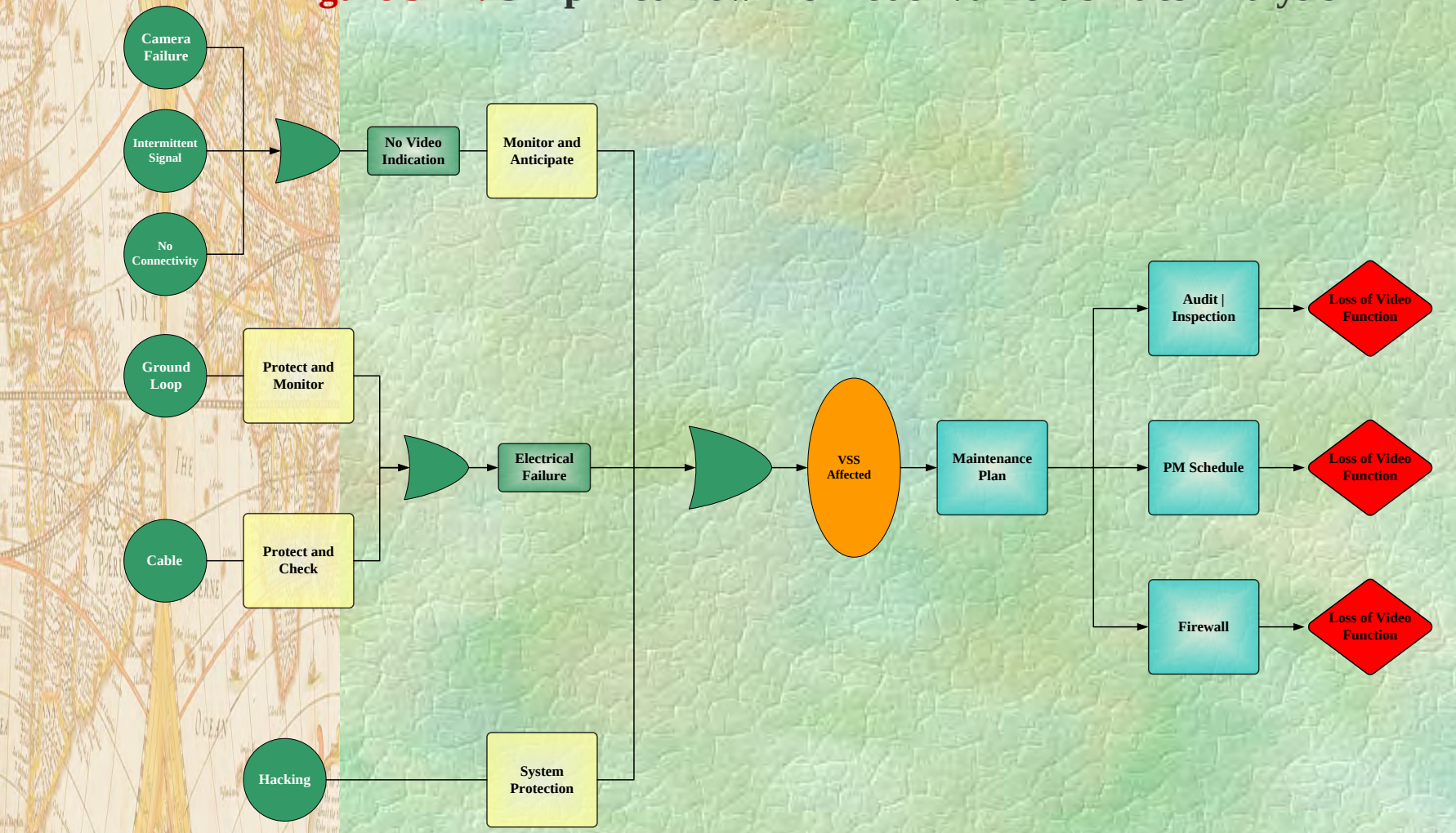
# SURVEILLANCE SYSTEM SECURITY VULNERABILITIES

**Table 5-5: Identification and Description of Security Vulnerabilities**

| No | Security Vulnerabilities | Explanation | | No | Security Vulnerabilities | Explanation |
|---|---|---|---|---|---|---|
| 1 | Camera Password | Hack into camera via web GUI to guess password | | 7 | System Password | NVR – Unauthorized access to security camera (Both VSS and Network) |
| 2 | Port Forwarding | Exposing NVR to internet (remote access) | | 8 | Connection Encryption | NVR use connection that is not encrypted with SSL or equivalent |
| 3 | Firewalls | Needed especially if you are going to expose NVR to internet | | 9 | Video Encryption | |
| 4 | Network Topology | Mixing camera on standard network without separation is a recipe for disaster | | 10 | Mobile Access | Password account deletion and encryption vulnerabilities |
| 5 | Operating System | All have vulnerabilities | | 11 | Physical Access to Equipment and Storage | |
| 6 | Operating System Password | Weak system password can create an opportunity for cyber attacks on system | | 12 | Video Recording Software | Supporting software not up to date including patches |
| | | | | | | |

# SURVEILLANCE SYSTEM SECURITY VULNERABILITIES

## Figure 5-17: Simplified Bow Tie Model Vulnerabilities Analysis



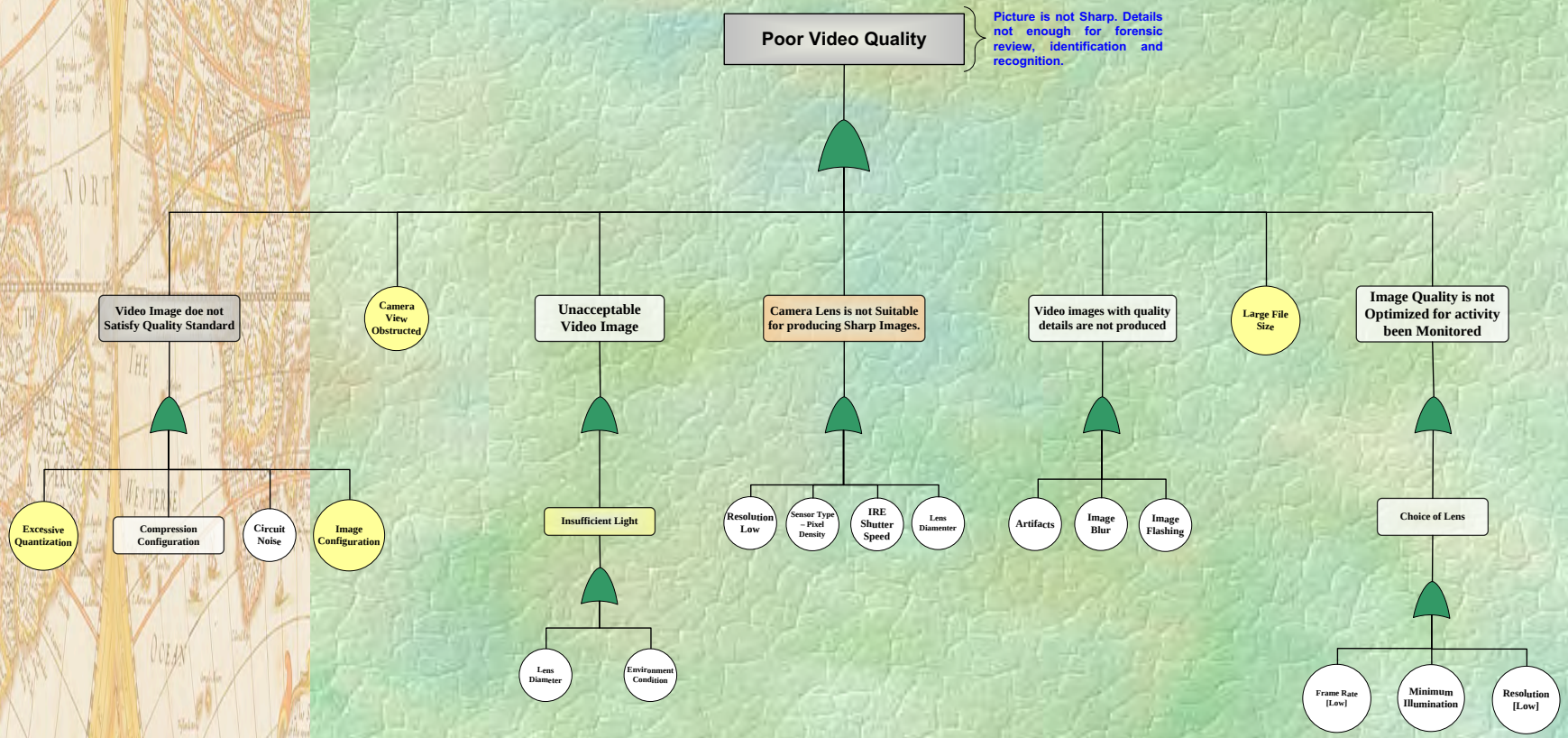
# Risk Assessment of Video Surveillance System

**Figure 5-6:** Design Failure Mode and Effect Analysis for Video Surveillance System

| LEBENTECH | | Potential Effects of Failure | | | | Current Design Control | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Product Function | Potential Failure Mode | | SEV | Potential cause of failure | OCC | Prevention | Detection | DET | RPN | Action | SEV | OCC | DET | RPN |
| Activity recognition and behavior detection of object in scene | No Motion Detected | No Video to Review therefore forensic evident will not be available if crime committed | 5 | 1 – Poor Lighting Level<br>2 – IP Camera Issue | 2 | System Audit | System Verification Testing | 2 | 20 | Risk Analysis | 5 | 1 | 2 | 10 |
| Capture Image from scene for Recording | Unable to Capture Image | Loss of video streaming capability [No video] | 5 | 1 – Camera Failure<br>2 – Camera not Discovered<br>3 – Power Failure | 2 | 1 - Operational Requirements<br>2 – Purchase Reliable Camera | Final System Testing | 3 | 30 | Root Cause Failure Analysis | 5 | 2 | 1 | 10 |
| Reliable transmit video stream/ data at a specific speed | Error occurs as Data Cross Network | 1 – Video streaming become corrupt<br>2 – Cannot request repeat delivery of corrupted section<br>3 – Video Signal Cannot be Captured | 5 | 1 – Virus<br>2 – Software conflict | 2 | 1 – QoS<br>2 – Compression Technique [Error detection/error containment] | Commissioning | 4 | 40 | Design Evaluation | 5 | 2 | 2 | 20 |
| Recording of quality video image | Poor Image Quality of Video Recorded | Cannot be used for forensic purpose | 4 | 1 - Resolution<br>2 – Frame Rate<br>3 – Compression Level<br>4 – Video Format | 4 | System Commissioning | Verification Testing | 2 | 32 | Vulnerability and Performance Assessment | 2 | 2 | 1 | 4 |
| Store or Save Video of X size | Unable to save (Medium capacity) | No video available for replay and to facilitate investigation | 5 | 1 – Operator Training<br>2 – Design Specification | 2 | 1 – Storage Calculations<br>2 – System Validation | Verification Testing | 1 | 10 | Review Specification | 5 | 1 | 1 | 5 |
| Exporting Files to Client | Unable to Export Video File | File not available for review or investigation purpose | 5 | 1 – File Corrupt<br>2 – Size \| Format | 2 | Verification Testing | System Audit | 2 | 20 | Root Cause Analysis | 5 | 1 | 2 | 10 |

# Risk Assessment of Video Surveillance System

## Figure 5-18: Fault Tree Analysis for Poor Video Quality



# MANAGEMENT OF VIDEO SURVEILLANCE SYSTEM

## What needs to be managed?

- **Management of System Performance**
- **Management of System Upgrades and**
- **Management of Video Content**

A **video management system**, also known as **video management** software or a **video management** server, is a component of a security camera **system** that in general: Collects **video** from cameras and other sources. Records / stores that **video** to a storage device.

# SUMMARY OF KEY POINTS

1. Understanding the specifications, allows you to select the right camera for your IP camera system.
2. Before reviewing the specifications, make sure you know your application and objectives. Sometimes the specs are confusing, so always check with us if you have questions.
3. Camera specifications such as resolution, low light sensitivity and the lens are some of the important factors to consider when selecting your camera.
4. Data compression can be the biggest cause of image quality loss with digital video recordings, especially when used to excess.
5. The IP network must be very reliable, providing sufficient bandwidth and redundancy. Network recovery time must be below 50ms should there be any network device failures or broken links.
6. For any video surveillance system, a set of cameras are used to monitor a scenario. The captured videos can be transmitted to the central office over internet protocol (IP). Usually, multi-video channels are supported in the video capture module.
7. The effectiveness of a surveillance camera system will be dependent upon its capability to capture images and information at a quality which is suitable for its intended purpose.

# THE END