## INTRODUCTION

### Analogue CCTV System Components

- A Typical Analog CCTV System
- Cameras
- Digital Video Recorder
- Coaxial Cable
- BNC Connectors
- Power supply
- Backup Power
- Monitors

### IP CCTV System Components

- A Typical IP CCTV System
- Active Components
- Design Considerations
- Bandwidth and Storage Calculations
- Storage Options
- Advanced Features

### System Installation

- DVR/NVR Network connection setup
- Cable Preparation
- Connector Termination and Testing
- Adjusting Camera Field of View
- Adjusting Camera Parameters through OSD
- Alternate Cabling Solution
Introduction

This document is a reference guide of Best Practices for Analogue and IP CCTV installation.
The Analogue CCTV System comprises of components, such as, Cameras, Digital Video Recorder (DVR), Coaxial Cable, Coaxial Cable Connectors, Power Supply, UPS and Monitor.

A typical Analogue CCTV System is as shown below:
Analogue CCTV System Components

Cameras

Analogue Cameras
CCTV cameras come in various types, styles, and configurations. A wide range of cameras are available to select from, depending on what will work best for the application. Some of the camera types based on the shape of the camera are Dome, Box, Bullet, PTZ Speed Dome Cameras. For outdoor applications, cameras installed should be both vandal and weather proof. To capture video images in low lighting conditions, IR Cameras are used, these cameras come fitted with IR illuminators.

Dome Cameras are the most commonly used in indoor applications. The "dome" shape makes it difficult to tell the direction that these cameras are facing, and thus are ideal for deterring criminals from executing their plans. The dome cameras are easy to install and can be easily mounted on both horizontal and vertical surfaces such as walls and ceilings. Dome Cameras are also available with IR illuminators, which enable the cameras to capture video images in low lighting conditions. The dome-shaped, hardened plastic casing that covers the camera also protects it from vandalism.

Bullet Cameras have a long, cylindrical, and tapered shape, similar to that of a "rifle bullet." These cameras are ideal for outdoor use, particularly in applications that require long distance viewing. Bullet Cameras are usually installed inside protective casings, which protect against dust, dirt, rain, hail and other harmful elements. A mounting bracket enables the camera to be pointed in the desired direction. The cameras come fitted with either fixed or varifocal lens.

Box Cameras can be fitted with C or CS-mount detachable varifocal lens, they give the flexibility to use lens to suit different applications. For instance, the standard CCTV camera lens can only cover distances of between 35 and 40ft. By using Box Cameras, it is possible to use special lenses, which can cover distances beyond the 40ft.

PTZ Speed Domes are also dome shaped CCTV Cameras, but include pan, tilt and zoom capability. These cameras can be set up to follow pre-programmed routes and presets. Most applications include a joystick - keyboard, operated by surveillance personal. Speed Domes are used to monitor vast areas such as Malls, Supermarkets Aisle, Car Parks, etc. However for reliable security, fixed non-rotating CCTV Cameras, should be installed, as very often during important incidents if the Speed Dome monitored another area no evidence will be captured. All security risk areas like gates, ground floor window rows, doors and fire exits should have their own fixed non-rotating camera, zoomed in on the highest risk area.
Selecting the right DVR is an important aspect of the Security System. There are many factors which have to be taken into consideration before choosing the right DVR for the installation. The specifications to consider are:

**Frame Rate**
Frame rate refers to the number of frames a DVR can record at a given resolution each second. Real time is considered to be 30 frames per second (FPS). So in order to record real time video on 16 channels you would need a unit that can record a total of 480 frames per second (FPS). Some DVRs are able to display live video at 30 FPS on each channel, but what is truly important is the recorded video, not the live video. Also due consideration should be given to the local authorities regulations regarding the FPS, when selecting a DVR.

**Compression**
Once video is transmitted to the DVR it is compressed to conserve storage and make internet viewing without lags. The compression used can vary from nearly no compression like wavelet or MJPEG, to the higher compression methods like MPEG4 or H.264. Compression methods can vary between DVRs, there are even some that use a combination of compressions, one for recording and one for streaming over the internet. Most of the newer DVRs use H.264 which is 40% more efficient both in storage and internet streaming.

**Storage Capacity**
How much storage a DVR can hold is an important factor to consider. Based on the recording days required and the FPS, the hard drive capacity can be calculated. Most of the DVRs comes with 1, 2 or 3 HDD Bays from capacities ranging from 4TB to 12 TB.

**Audio Recording**
Audio recording is not required in most of the installations. Some DVR’s will accommodate audio recording for all channels while some DVRs will have audio recording for few channels only. Again based on the requirements and the budget allocated for the DVR, the right type of DVR should be chosen. Please check the local laws prior to using the audio recording.

**Video Output**
DVR’s will often only offer BNC video output which would require the use of a BNC to VGA converter to view the DVR on a standard VGA monitor. The higher end units will have a VGA output as well as a BNC out and also HDMI output.

**Remote View**
Most DVR’s these days are networkable and can allow an individual to log in using internet explorer to view their security cameras. The more advanced units will have a client software that allows an individual to view multiple DVR’s at the same time. This software may have features like E-mapping, camera groupings, various user levels, the ability to restrict access to individual functions and cameras for each user and more.
Analogue CCTV System Components

Digital Video Recorder

DVRs record video in different resolutions, please check the DVR to know which video resolutions are supported. The following resolutions are available based on the DVR model you are using in your installation.

**CIF** (352 x 240 or 288),
**2CIF** (704 x 240 or 288),
**4CIF** (704 x 480 or 576),
**Half D1** (720 x 240 or 288),
**D1** (720 x 480 or 576),
**960H** (960 x 480 or 576)

Please refer the next page for more details on these resolutions.
Analogue CCTV System Components

**Digital Video Recorder**

**CIF**: This is the lowest and outdated resolution-quality. Video and picture is produced at 352 X 240/288 Pixels. Proper IDENTIFICATION of suspects is unlikely and chances of success in court rather dim - unless the incident occurred very close to the recording security camera. Distant subjects and objects become very unclear. Yet even many high profile security clients keep this as their standard recording format. There are a number of reasons for this, mainly being Frame Rate FPS (frames per second) and least but certainly not last to avoid 4CIF Line Interlacing.

**2CIF or Half D1**: Semi Recording Quality / recommended only for home and small business use. Does not produce fully professional and reliable evidence in all situations. Up to 720 X 240/288 Pixels. CIF and 2CIF are sometimes preferred for frame rate advantages and in order to avoid Line Interlacing, but both video formats require close up camera positioning in order to reach chances of identification.

**4CIF or D1**: Records at up to 720 X 480/576 Pixels, which is similar to DVD Quality. In a professionally configured CCTV System even distant suspects have a chance of identification. 4CIF is not recommended for scenarios where the to be identified individuals or subjects can be expected to move swiftly. This is due to the great downside of D1 / 4CIF being Line Interlacing.

**960H**: 960H is a new standard that provides high resolution images using advanced image sensors. Security cameras that are capable of 960H resolution produce an image that is 960 horizontal and 480 vertical pixels large(960x480) Images are 34% sharper than D1 and more than 500% sharper than CIF.

**FPS**: FPS Frames Per Second is one of the most crucial DVR function specification to be considered prior to selecting the DVR. The overall Frame Rate determines how many frames (images) per second can be recorded for each connected camera individually.

**Line Interlacing at 4CIF DVRs**

Line Interlacing is the one great disadvantage of configuring a DVR to record in 4CIF Resolution. It causes a delay distortion of fast moving objects and subjects in every second horizontal video line. So it is recommended to use the Deinterlace feature in the DVR.
Analogue CCTV System Components

Coaxial Cable

Coaxial cable is a two-conductor electronic cable that is used as the transmission medium for a variety of applications such as Analog Baseband Video (CCTV — Closed Circuit Television), RF Broadband Video (CATV - Cable Television, Satellite) and for some data, radio and antenna applications. It is constructed to provide protection against outside signal interference.

CCTV operates in a lower frequency range than CATV and requires different cable constructions. Be sure that the cable used is chosen accordingly. The primary differences are based on the frequency range differences as shown below:

* Note: Skin effect is the tendency of alternating current, as its frequency increases, to travel only on the surface of a conductor. In copper-clad steel coax, the high-frequency signal travels only on the copper "skin."
Coaxial Cable

Coaxial cables are also available in different RG types. RG stands for Radio Guide, or Radio Grade and is a term that is used when sending Radio Frequency (RF) signals down a coaxial cable. 75 ohm coaxial cable comes in several sizes with the most common types being RG-179, RG-59, RG-6, and RG-11.

An RG-179 & RG-59 cables are the most commonly used coax because they are small in diameter and easy to work with. The RG-11 cable is the largest in diameter and harder to work with. The RG-6 size is between the RG59 and RG11. The difference between the RG types are not just size, but also the attenuation characteristics and therefore the transmission distance. Typically, the coax cable transmission limitations for CCTV is described in the table below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Distance (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RG-179</td>
<td>RG-179, 75 ohm, cable is generally used in CCTV head-ends and for precision analog and digital video applications such as component video. Single or bundled (multiple unit) coax construction from 23-30 AWG with either a tinned or bare solid copper conductor or a stranded conductor. Shielding is a 90–95 percent braid with a foil shield.</td>
<td>150</td>
</tr>
<tr>
<td>RG-59</td>
<td>RG-59, 75-ohm cable is used for flexibility, small size and shorter run lengths. 23 AWG solid copper conductor, 95 percent coverage bare copper braid shield.</td>
<td>150</td>
</tr>
<tr>
<td>RG-6</td>
<td>RG-6 is a high quality 75 ohm coaxial cable used generally for antenna and CATV wiring. RG-6 is a higher-grade cable than RG-59 and therefore a better choice where performance is important. It uses a larger, higher-capacity 18 AWG solid copper center conductor, larger insulating dielectric and 95 percent coverage bare copper braid shield</td>
<td>300</td>
</tr>
<tr>
<td>RG-11</td>
<td>higher cost used in long run-length, low-attenuation applications where larger size is acceptable. CCTV: 14 AWG solid copper conductor, 95 percent coverage bare copper braid shield</td>
<td>450</td>
</tr>
</tbody>
</table>

Note: This is not a complete list. It covers the most common types of 75-ohm coaxial cables. The installation methods outlined in the guide are common practice for many types of coaxial cables.
Analogue CCTV System Components

BNC Connectors

Coaxial connectors are components attached to the end of a coaxial cable that connect with an audio, video, data or other device to prevent interference and damage.

BNC Connectors are the most common connector for coaxial cables, and they are available in both 50-ohm and 75-ohm versions. Based on the geThere are different types BNC Connectors, the common types are, Compression, Crimp-on and Twist-on Type BNC Connectors.

With compression type connectors, you twist them onto the cable, then use a compression tool to squeeze a ring towards the main body of the fitting. In between the ring and the body is some fairly stiff, yet pliable plastic tubing. When you compress the ring towards the body, the plastic bends inwards towards the cable, creating a snug, watertight seal that holds the fitting in place.

Crimp-on connectors are probably the most popular type of BNC connectors on coax cable. A crimp type connection allows for quick and simple installation while still maintaining a mechanical and electrical connection fairly close to a solder type termination. Proper size connector should be used to match the coax cable used, as a tight fit on the cable is important.

Twist-on connectors are known for creating poor connections and can easily come loose, if not properly installed. When using twist-on connectors, extra care should be taken so that the cable is secured well.

It is recommended to use good quality compression or crimp-on connectors with the coaxial cables. Proper tools should also be used when creating the connections.
Analogue CCTV System Components

Power Supply

In Analogue CCTV Systems the cameras can be powered either by local power supply or central power supply. In IP CCTV Systems, the cameras are either powered through local power supply, PoE switches, Mid Span, PoE Injector.

Local Power Supply
In this system, A local regulated DC adapter is connected to the camera. This is recommended as each camera will have its own dedicated power supply.

Central Power Supply
In this system, a CCTV power supply box, also known as a power distribution box, allows surveillance system installers to easily manage the power to multiple CCTV cameras at a central point (usually at the location of the DVR). This allows the camera installation to be more structured. Instead of having 8 power supply plugs (local power supply), the cameras are plugged into a power strip / electric surge protector, all the camera power wires can neatly be run to a power supply box. The central power supply box is normally installed near your DVR.

However, when using centralized power supply, proper care has to be taken and the power at the end of the cable run has to be tested. It is known that the DC power attenuates rapidly as the distance of the cable increases. Also, this attenuation is directly proportional to the cable gauge. The higher the cable gauge, higher the attenuation. So it is recommended to use a thick gauge wire if the distance between the camera and the central power supply is more.

The Voltage and Amperage has to be tested at the camera end of the power cable and has to be checked if there is enough power to run the camera.

For example, if a 18 AWG wire is used to transmit 12V for 150m, and the camera consumes 300mA current. If the voltage is measured at the end of the cable, the voltage will be 9.6V which is not enough to power the camera. Most of the cameras are rated 12V±10%. So a minimum of 10.8V is needed near the camera end. So in order to power this camera effectively, either a thicker wire gauge must be used or the voltage at the source must be increased.
The CCTV system should not be connected directly to raw line power because of the potential problems such as voltage surges, spikes, dips, brownouts, blackouts, electrical noise etc. It requires line conditioning and filtering to provide a source of continuous uninterrupted power at all times including power failure.

For this reason, an Uninterrupted Power Supply (UPS) must be used. Numerous manufacturers have UPS designs that satisfactorily eliminate most of the problems mentioned. Most UPS systems operate over a maximum period of several minutes to several hours to maintain uninterrupted power.

The following example illustrates how to determine the size and type of UPS system to choose for an installation having 32 cameras, 2 main monitors, 2 Spot monitors and 2 DVRs and a PC. The total backup power required is 909 VA (watts). Since UPS systems are usually available in 250, 500, and 1000 VA ratings, choose the 1000 VA unit. This will provide a good margin of safety.

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Power (Watts)</th>
<th>Quantity</th>
<th>Total VA* (Volt-Ampere)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR Bullet Camera</td>
<td>6</td>
<td>16</td>
<td>96</td>
</tr>
<tr>
<td>Dome Camera</td>
<td>3</td>
<td>16</td>
<td>48</td>
</tr>
<tr>
<td>16 Channel DVR</td>
<td>80</td>
<td>2</td>
<td>160</td>
</tr>
<tr>
<td>17” LCD Spot Monitor</td>
<td>50</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>20” CRT Main Monitor</td>
<td>90</td>
<td>2</td>
<td>180</td>
</tr>
<tr>
<td>PC</td>
<td>300</td>
<td>1</td>
<td>300</td>
</tr>
<tr>
<td>Misc</td>
<td>25</td>
<td>1</td>
<td>25</td>
</tr>
</tbody>
</table>

Total VA Required: 909

* Assuming resistance load (Power factor = 1)
VA = WATTS
Analogue CCTV System Components

Monitor

A CCTV monitor is an important component of a security system, as the video captured by the Camera is viewed using the monitor. CCTV monitors come in all different sizes, types, and price options. The goal when buying the best CCTV monitor is to buy the one that has the highest resolution, and warranty. If the CCTV monitor used is not matching the resolution of the cameras, then the video displayed on the monitor is not matching that of the cameras, resulting in the performance of the entire system to be compromised.

Security Systems are designed to run 24/7/365, any downtime will be a breach of security, so while choosing the monitor, due consideration should be given to this fact. It is important to choose industrial grade monitors rather than consumer grade ones. When choosing a new CCTV monitor, do look into the following factors.

Resolution
When choosing a CCTV monitor the resolution is always the most important specification. The last thing you want to do is watch the video your cameras are capturing at a lower resolution. This is common when people decide not to use a CCTV monitor and instead use a standard computer monitor. Doing this only causes you to miss out on the finer details the cameras are capturing like identifying a face, a license plate number, or small movements of people in the areas being secured. Using a low resolution monitor just hinders the performance of the security system.

Power Consumption
Where ever possible, it is best to choose an LED rather than an LCD monitor. A LED panel uses less power, and is therefore cheaper to run than a similar sized LCD panel. LED monitors use up to 46% less power over the life of the unit.

Heat
One of the main reasons for the failure of an electrical device is the build-up of heat in the chassis. To combat this, monitor buyers should select, where possible, a monitor with an external PSU. This will greatly reduce the heat generated inside the unit and extend its longevity. LED monitors give off less heat than LCD monitors because they use less power.

Connectivity
The CCTV monitors of today also come with various connection options to support your needs. Most CCTV monitors come with VGA, DVI, and BNC connector connections. Plus some of the newer CCTV monitors are now offering HDMI. The installation of a CCTV monitor is very simple since you are just attaching it directly to your security DVR. Once your CCTV system is live you will be able to navigate your DVR software right on the monitor and view the live and recorded video right on the CCTV monitor. A CCTV monitor has the ability to sit right on a desk, mount on a rack, or mount on the wall. So you have the flexibility you need to position the CCTV monitor in the way that best supports your needs.
The IP CCTV System comprises of components, such as, Cameras, Network Video Recorder (NVR), UTP Cable, Power Supply, CMS etc.,

A typical IP CCTV System is as shown below:
IP CCTV System Components

Active Components

**POE**

- The IEEE standard for PoE requires a minimum cat5 cable. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device, such as an Ethernet switch, or can be injected into a cable run with a midspan power supply.

- The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

- The updated IEEE 802.3at-2009 PoE standard, also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power, however there are some products that state compatibility with the 802.3at standard and offer up to 65 W of power over a single cable by utilizing all four pairs in the cat5 cable.

- All PoE standards are subject to the same distance limitations for Ethernet, which means the CAT cable length must not exceed ~300 ft or ~100 meter.

**POE Powering options**

1. **Using a PoE Injector**
   In this method, the standard network is fed into an injector that adds (or injects) power to the cable and then continues to connect to the camera.

2. **Using a PoE Midspan**
   An expansion of the injector concept, where multiple devices can be connected and get PoE added onto their network connections from a single appliance.
IP CCTV System Components

Active Components

3. PoE-Enabled Switches: This is the most common appliance today and combines both the network side and the power, delivering them directly to the cameras.

The primary benefits of PoE include:
- Cost savings - PoE significantly reduces the need for electricians to install conduit, electrical wiring, and outlets throughout the enterprise.
- Flexibility - A PoE appliance or device can be located anywhere without the need for AC outlets.
- Reliability - Because PoE networks have fewer wires, there is less likelihood of an inadvertent power disruption (accidental shut off, etc). With an Uninterrupted Power Supply (UPS) power to the devices is assured during a power failure.
- Network Control - Using SNMP, network administrators can monitor and control powered devices, including resetting or shut-off. This allows increased security, as devices can be powered down when not in use, or if there is unauthorized access.
- Safety - Power mains are eliminated. Since only 48v DC is used, PoE conforms to Underwriter’s Laboratories (UL) Safety Extra Low Voltage (SELV) classification.

Practical Example:

Suppose a switch is used for an IP installation which has 24 PoE ports and the specs states that the switch can deliver 15.4W per port and 180W per switch.

Therefore, the Power on maximal load: 180W/24 ports = 7.5W

If each camera consumes power around 6.5W, then 24 cameras can be connected to the PoE Switch as the power consumed is lower than 7.5W. But if each camera consumes around 11.5W, then only 12 cameras can be connected to the PoE switch so as to maintain the maximum PoE power of the switch.
There are a number of factors to consider when setting up an IP-based surveillance system.

The key considerations are the following:

- Network Bandwidth
- Network Security
- System Scalability
- Video Storage

Putting thought into these areas before you set up your system will help to ensure that you have the right equipment and the proper game plan to fulfill your surveillance requirements.

**Network Bandwidth & Storage**

The amount of bandwidth used by network cameras and the storage required is determined by several factors, most notably:

A. Number of cameras
   The more the number of cameras. The overall bandwidth is high and the storage space need also increases.

B. Whether recording will be continuous or event-based
   Continuous recording consumes more bandwidth and needs more storage space. Using event based recording is a good way to minimize the bandwidth and cut on storage costs.

C. Number of hours per day the camera will be recording
   By Limiting the recording to a certain period of the day can save the storage and bandwidth a lot.

D. Frames per second
   Frame rate is something that can be adjusted within your IP camera, video server, or video management software. By controlling the frame rate, you can greatly reduce bandwidth usage and can eliminate unnecessary frames from traveling over the network. One common technique is to set the surveillance system to increase the frame rate only when motion is detected. Another is to send higher frame rates for local viewing, and lower frame rates over the Internet for remote viewing.

E. Image resolution
   An IP camera's resolution is determined by pixels. The higher the resolution, the higher the pixel-count, and the greater amount of detail you'll be able to capture in a video image. It's important to determine how much detail is enough to meet the requirements of your particular surveillance application. Typically, as the image quality goes up, so does the amount of bandwidth required, so it's best to find a level that meets your needs while optimizing network bandwidth.

F. Video compression type: MJPEG, MPEG-4, H.264
   Video compression is an important tool in helping to ease strain on the network. Compression technologies such as MJPEG, MPEG-4, and H.264 allow users to stream and record high-quality video without hoarding bandwidth. H.264 is the latest compression technique, dramatically reducing video file sizes while increasing overall efficiency and lowering storage costs.
IP CCTV System Components
Design Considerations

G. Scenery
Image complexity, lighting conditions and amount of motion
The more complex the scene is in terms of the motion, the lighting conditions etc., the more the bandwidth consumed is and hence more storage is required.

H. How long data must be stored
Typically, a 30 days of storage is good enough for most of the surveillance purposes. If data storage is required for more time period, then proper storage techniques has to be implemented.

Network Security
As with any video surveillance system, privacy and security are important factors to consider when setting up an IP-based video solution. Users want to be assured that no one can tap into their video feeds. Those concerns are understandable, but with IP network cameras, it’s quite easy to protect your files from unauthorized viewing and tampering. In most cases, the network camera encrypts the surveillance video before sending it over the network. This helps to ensure that only authorized viewers can access the camera feeds. Most systems also include password protection and different levels of authentication that work to prevent hacking and outside access.

Another tool for protecting network video feeds is digital watermarking. IP cameras are capable of adding encrypted watermarks into the video stream. The watermarks can include information such as time, location, and user activity, while time stamping can create a trail that shows who has accessed specific video images, and whether any edits have been made to the files.

System Scalability
One of the great advantages of IP surveillance is system scalability. With analog surveillance systems, adding new cameras often involves complicated and expensive cabling. But with an IP-based system, it’s as simple as connecting the additional cameras to your existing IP network, the same way you would any other network device. Power over Ethernet (PoE) and wireless network cameras enhance flexibility even further by allowing you to install cameras in locations without a readily available power outlet.

Since a server records and manages the video footage in an IP surveillance system, there’s no limit to the size and scope of the installation. Different types of servers can be chosen depending on how many cameras are needed and what frame rate is required.
Calculating required bandwidth

In a small surveillance system involving 8 to 10 cameras, a basic 100-megabit (Mbit) network switch can be used without having to consider bandwidth limitations. Most companies can implement a surveillance system of this size using their existing network. When implementing 10 or more cameras, the network load can be estimated using a few rules of thumb:

- A camera that is configured to deliver high-quality images at high frame rates will use approx. 2 to 3 Mbit/s of the available network bandwidth.
- With more than 12 to 15 cameras, consider using a switch with a gigabit backbone. If a gigabit-supporting switch is used, NVR should have a gigabit network adapter installed.

Calculating required storage

As mentioned earlier, the type of video compression used is one of the factors affecting storage requirements. The H.264 compression format is by far the most efficient video compression technique available today. Without compromising image quality, an H.264 encoder can reduce the size of a digital video file by more than 80% compared with the MJPEG format and as much as 50% more than with the MPEG-4 (Part 2) standard. This means much less network bandwidth and storage space are required for an H.264 video file.

Sample storage calculations for all three compression formats are provided in the tables below. Because of a number of variables that affect average bit rate levels, calculations are not so clearcut for H.264 and MPEG-4. With Motion JPEG, there is a clear formula because Motion JPEG consists of one individual file for each image. Storage requirements for Motion JPEG recordings vary depending on the frame rate, resolution and level of compression.

**H.264 calculation**

Approx. bit rate / 8(bits in a byte) x 3600s = KB per hour / 1000 = MB per hour

MB per hour x hours of operation per day / 1000 = GB per day

GB per day x requested period of storage = Storage need

<table>
<thead>
<tr>
<th>Camera</th>
<th>Resolution</th>
<th>Approx. bit rate (Kbit/s)</th>
<th>Frames per second</th>
<th>MB/hour</th>
<th>Hours of operation</th>
<th>GB/day</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. 1</td>
<td>CIF</td>
<td>110</td>
<td>5</td>
<td>49.5</td>
<td>8</td>
<td>0.4</td>
</tr>
<tr>
<td>No. 2</td>
<td>CIF</td>
<td>250</td>
<td>15</td>
<td>112.5</td>
<td>8</td>
<td>0.9</td>
</tr>
<tr>
<td>No. 3</td>
<td>4CIF</td>
<td>600</td>
<td>15</td>
<td>270</td>
<td>12</td>
<td>3.2</td>
</tr>
</tbody>
</table>

**Total for the 3 cameras and 30 days of storage = 135 GB**
IP CCTV System Components

Storage Options

NVR Based Storage
Depending on a NVR’s central processing unit (CPU), network card and internal RAM (Random Access Memory), it can handle a certain number of cameras, frames per second and size of images. Most NVRs can hold between two and four hard disks, and each disk can be up to approx. 4 Terabyte. There are also High end servers which can have more than 24 Hot swappable Hard disks for extended storage. This is called a direct-attached storage.

NAS and SAN

When the amount of stored data and management requirements exceed the limitations of a direct-attached storage, a network-attached storage (NAS) or storage area network (SAN) allows for increased storage space, flexibility and recoverability.

NAS provides a single storage device that is directly attached to a LAN and offers shared storage to all clients on the network. A NAS device is simple to install and easy to administer, providing a low-cost storage solution. However, it provides limited throughput for incoming data because it has only one network connection, which can become problematic in high-performance systems.

SANs are high-speed, special-purpose networks for storage, typically connected to one or more servers via fiber. Users can access any of the storage devices on the SAN through the servers, and the storage is scalable to hundreds of terabytes. Centralized storage reduces administration and provides a high performance, flexible storage system for use in multi-server environments. Fiber Channel technology is commonly used to provide data transfers at four gigabits per second and to allow large amounts of data to be stored with a high level of redundancy.

Redundant storage

Redundancy in a storage system allows video, or any other data, to be saved simultaneously in more than one location. This provides a backup for recovering video if a portion of the storage system becomes unreadable. Redundant Array of Independent Disks (RAID) is one of the prominent method achieving redundant storage.

RAID is a method of arranging standard, off-the-shelf hard drives such that the operating system sees them as one large hard disk. A RAID setup spans data over multiple hard disk drives with enough redundancy so that data can be recovered if one disk fails. There are different levels of RAID, ranging from practically no redundancy to a full-mirrored solution in which there is no disruption and no loss of data in the event of a hard disk failure.

Below is an overview of the most popular RAID levels:

RAID level 0 – Striping
In a RAID 0 system data are split up in blocks that get written across all the drives in the array. By using multiple disks (at least 2) at the same time, this offers superior I/O performance. This performance can be enhanced further by using multiple controllers, ideally one controller per disk.
RAID level 1 – Mirroring
Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives). If a drive fails, the controller uses either the data drive or the mirror drive for data recovery and continues operation. **You need at least 2 drives for a RAID 1 array.**

**Advantages**
- RAID 1 offers excellent read speed and a write-speed that is comparable to that of a single drive.
- In case a drive fails, data do not have to be rebuild, they just have to be copied to the replacement drive.

**Disadvantages**
- The main disadvantage is that the effective storage capacity is only half of the total drive capacity because all data get written twice.
- Software RAID 1 solutions do not always allow a hot swap of a failed drive (meaning it cannot be replaced while the server keeps running). Ideally a hardware controller is used.

**Ideal use**
RAID-1 is ideal for mission critical storage, for instance for accounting systems. It is also suitable for small servers in which only two data drives will be used.
RAID level 5
RAID 5 is the most common secure RAID level. It requires at least 3 drives but can work with up to 16. Data blocks are striped across the drives and on one drive a parity check sum of all the block data is written. The parity data are not written to a fixed drive, they are spread across all drives, as the drawing below shows. Using the parity data, the computer can recalculate the data of one of the other data blocks, should those data no longer be available. That means a RAID 5 array can withstand a single drive failure without losing data or access to data. Although RAID 5 can be achieved in software, a hardware controller is recommended. Often extra cache memory is used on these controllers to improve the write performance.

![RAID 5 diagram](image)

Advantages
- Read data transactions are very fast while write data transactions are somewhat slower (due to the parity that has to be calculated).
- If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

Disadvantages
- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. If one of the disks in an array using 4TB disks fails and is replaced, restoring the data (the rebuild time) may take a day or longer, depending on the load on the array and the speed of the controller. If another disk goes bad during that time, data are lost forever.

Ideal use
RAID 5 is a good all-round system that combines efficient storage with excellent security and decent performance. It is ideal for file and application servers that have a limited number of data drives.
An IFP CCTV System Components

Storage Options

RAID level 6 – Striping with double parity
RAID 6 is like RAID 5 but it writes the parity data to two drives. That means it **requires at least 4 drives** and can withstand 2 drives dying simultaneously. The chances that two drives break down at exactly the same moment are of course very small. However, if a drive in a RAID 5 system dies and is replaced by a new drive, it takes hours to rebuild the swapped drive. If another drive dies during that time, you still lose all of your data. With RAID 6, the RAID array will even survive that second failure.

**Advantages**
- Like with RAID 5, read data transactions are very fast.
- If two drives fail, you still have access to all data, even while the failed drives are being replaced. So RAID 6 is more secure than RAID 5.

**Disadvantages**
- Write data transactions are slowed down due to the parity that has to be calculated.
- Drive failures have an effect on throughput, although this is still acceptable.
- This is complex technology. Rebuilding an array in which one drive failed can take a long time.

**Ideal use**
RAID 6 is a good all-round system that combines efficient storage with excellent security and decent performance. It is preferable over RAID 5 in file and application servers that use many large drives for data storage.
**Dual LAN**
In a dual LAN system, there will be two Ethernet cards working independently. NVRs with dual Ethernet connections can use them to connect simultaneously with different networks. There are a number of potential applications for this.

For example, the NVR could be connected to internet to monitor over internet, and simultaneously it could be connected to a separate internal network for local monitoring. This not only improves security, it frees up all the bandwidth of the in-house network to handle the data infrastructure.

Dual gigabit Ethernet interface cards are targeted at the enterprise and other high-performance environments, and usually have a number of enhancements built in to take full advantage of the gigabit throughput. Some support the use of larger-than-normal data packets, which increase the effective throughput of the network.

**Redundant Power Supply**
A redundant power supply contains two (or more) power supply units inside it. Each power supply is capable of powering the NVR and only one runs at a time. If one fails, the other power supply starts running to keep the NVR powered up. The switch between the power supplies is seamless, so as not to interrupt the normal functioning of the NVR.

**Note**: It is always recommended to use UPS as a backup power supply.

**E-SATA**
External Serial Advanced Technology Attachment or eSATA is an external interface for SATA technologies. Unlike USB2.0, eSATA requires its own power connector. It is an excellent choice for external disk storage. It is much faster than USB and thus it can be used as a recording HDD for the NVR.

Typically, a HDD docking station which supports ESATA is needed for this purpose. Depending on the number of E-SATA ports available on the NVR and the number of HDD slots available in the docking station, the storage of the NVR can be increased.
Step 1: Find the TCP/IP settings of your network
Use a network connected computer, click Start, Run…, in the Open field, type cmd and click OK button to open the MS-DOS Command Prompt window.

From the Command Prompt window, at C:\> prompt, type ipconfig and press the Enter key The TCP/IP settings for this networked computer will look like this:
The TCP/IP settings for this networked computer will look like this:

![Network Configuration](image1)

From this screen, you can see the IP configuration of your network and this computer. Write down these numbers on a piece of paper as follows:

- IP address is 192.168.0.120
- Subnet Mask is 255.255.255.0
- Default Gateway is 192.168.0.1

**Step 2: Obtain a static IP address for the DVR.**

A typical router has DHCP function which will dynamically assign an IP address when a device requests an IP address. You should use a static IP address which is outside the DHCP assigned range so that the IP address for DVR will not change over the time.

For example, we use 192.168.0.200 as IP address for DVR. Check the IP address to make sure it has not been assigned to any device in the network. Open the MS-DOS Command Prompt window, at C:\> prompt type `ping 192.168.0.200` and press Enter to see if this address has been assigned to a device.

![Ping Command](image2)
System Installation

DVR/NVR Connection Setup

From this screen, you can tell that the IP address of 192.168.0.200 has not been assigned to any device at this time because all four responses are “Request timed out.” And therefore you can assign this address for DVR/NVR.

Step 3: Connect DVR/NVR to network
1. Use a cat-5 network cable connect to the RJ-45 port and network.
2. Set IP address, subnet mask, and default gateway for DVR as showed in the previous page.
3. Set the client port(s) and the web port. Note down the client port(s) and web ports in a sheet of paper. This information is needed in future for port forwarding.

Step 4: Install DVR/NVR Remote Viewer software and configure settings on Computer
A. Check IP network connection between DVR/NVR and computer.
   a. From the network connected computer, open a MS-DOS Command Prompt window
   b. From MS-DOS Command Prompt windows, at C:> prompt, type ping 192.168.0.200 and press Enter key.
   c. If you see 4 packets was sent and received, it means the connection is working properly.

B. Download the Remote viewer software to your computer. Refer to the Software manual for the procedure to use the software.

Step 5: Port Forwarding in the Router
Port forwarding of a router is required with the DVR/NVR system to allow user access from a remote location.

The port forwarding process is dependent on the brand and model number of the router being used. You will need to enable the ports by locating the port range forwarding screen. Please refer to the manuals of the specific routers which is being used for more information. Below is an example showing port forwarding in D-LINK router Model DI-524.

1. Open your web browser. Enter the router IP address 192.168.0.1 in the address bar, followed by pressing Enter.
2. Enter the user name (admin). Leave the password blank followed by pressing the OK button.
3. Select the Advanced tab.
4. Select the Virtual Server tab.
   • In the Name field enter a description of your DVR.
   • In the Private IP field enter the DVR IP address.
   • In the Protocol field, select Both.
   • In the Private port enter the port number you need to port forward (e.g. 80)
   • In the Public port re-enter the port number you entered in the private port field (e.g. 80)
   • Select the Schedule to Always. If more ports are required to be port forwarded, repeat the above steps. When complete, select the Apply button located at the bottom of the page to save your changes.

Port forwarding is now complete for the D-Link router!

www.infinique.com
Step 6: Check Port Forwarding
You can use any port checking website to verify that the ports which are setup are working properly. Here are some of the sites.
http://www.canyouseeme.org/
http://www.yougetsignal.com/tools/open-ports/

Enter the Port Number and Click Check.

Step 7: Setting up the DDNS Service
The next step is to set-up the DDNS service. Internet Providers work from a pool of IP addresses and those are “leased” out to you and tracked by your router. From time to time it is possible that your IP address is going to change. Tracking those changes and directing the user to the correct internet IP address is what the DDNS service does. The DVR has the built in function to “ping” the DDNS Server to let the DDNS Service know what the DVR’s Internet IP address is, so the DDNS server can be updated to the correct internet IP address. Please refer to the DVR manual to know how to set up DDNS Service.
System Installation

Cable Preparation

Note:
For IP camera cabling, Please refer to “Infinique SC Installation and Operations Manual”.

Bend Radius
Current coaxial standards do not specify bend radius; however, various manufacturers do provide guidance. Check with manufacturers for specifics. Special care should be taken when pulling a coaxial cable around bends. Using too much force or too tight of a bend can deform the dielectric and cause a drop in transmission performance.

Transmission media is the most important part of an installation. It is estimated that over 65% of failure in a CCTV system is associated with transmission media which includes the type of cable used, connectors, connections and the installation methods.

The second biggest area that account for nearly 27% of the problems are power and environment related which includes either excessive or inadequate input power, ineffective or improper grounding or an excessive temperature around the equipment. Incorrect equipment setup, improper equipment termination and improper camera installation account for about 7% of the problems directly associated with the installation personnel. Only 1% of the failures in a CCTV installation are actually caused by device failures.
The following steps will guide you through the preparation and termination process for coaxial cable with compression connectors. Following these guidelines will help make sure that you receive the optimum performance from the coaxial cable.

**Step 1**
The tools you will need:
Compression tool
Cable stripper
Compression Connectors

**Step 2**
Adjust the blades of the stripper to expose \( \frac{1}{4} \) inch of the conductor and \( \frac{1}{4} \) inch of the insulation. Insert the coax cable into the strip cartridge to the adjusted length.

**Step 3**
Holding the cable near the tool, rotate the cutter around the cable (three to five full turns) to score the jacket and cut through the insulation. Be sure the braid is cut (you can hear when the wires of the braid have all been cut). Then flex the jacket to separate and slide it off to expose the center conductor.
Installation
Connector Termination and Testing

Step 4
Flare and bend back the remaining outer braid onto the cable outer jacket. Make sure to remove any stray or loose braids. Stray or loose braids can cause shorts if they touch the center conductor. Verify that the center conductor and the insulation are not nicked or scored.
When handling cables with multiple braids, such as quad-shield, refer to the manufacturer’s literature for proper braid handling techniques.

Step 5
Insert the sleeve ferrule and BNC body onto the coaxial cable. Firmly push the cable as far as possible or until 1/8 inch of the center conductor is protruding from the connector.

Make sure the connector is fully seated and the white dielectric material is firmly pushed against the inner stop of the connector. You can see this by looking into the open end of some connectors.

Step 6
Insert the cable and connector into the crimping device, making sure that it is positioned firmly. Squeeze the crimper handle tightly. Use a ratcheting tool that does not release until the proper crimping displacement has been applied for the specific cabling and connector type. Once the tool releases after the final “click,” the crimp should be complete.
Step 7
Inspect the connection making sure that there’s no braiding exposed and that the connector is firmly attached to the cable.

Step 8
Once the cable is pulled, the cable is to be tested for resistance and proper termination in order to assure good video quality.

The following method is used to test the proper resistance in a single cable loop.

1. Remove the BNC connection from the output of the camera.
2. Short the center conductor of the cable to the shield or ground of the connector.
3. Locate the other end of the cable under test and remove it from the DVR.
4. Connect a standard ohm meter to the circuit (black test lead to the shield of the connector, red lead to the center pin of the connector).
5. Check the DC resistance value on the meter. The maximum DC resistance of the cable assembly should be between 10 to 15 ohms. This indicates the resistance loss of the cable, resistance loss due to connector used or splice points, and any breakdown of the copper components of the coaxial cable. This is the acceptable maximum resistance between the camera and monitoring location (DVR side). A lesser resistance value than stated above will result in better video quality.
Installation
Connector Termination and Testing

Step 9
Check the cable length and the termination in a single cable loop.

Step 1: Make sure one end of the cable being tested is connected to the DVR.

Step 2: Remove the BNC connection from the output of the camera.

Step 3: Connect a standard ohm meter to the BNC connector at the camera end (black test lead to the shield of the connector, red lead to the center pin of the connector).

Step 4: Check the resistance value on the meter. If the ohm meter registers 76 to 90 ohms, then it indicates proper cable length and system termination. If the reading is 36 to 52 ohms, the cable is double terminated (kinks or cuts), then cable has to changed or locate the double termination point and rectify the same.

Note: If the meter does not register any readings, this indicates that the system is not terminated correctly, check the termination at both the ends and redo the test.

Step 10
Label the cables for easy troubleshooting

Step 1: Label both ends of the cable.

Step 2: Put the label about 2-3 inches away from the cable end as putting it close to the jack makes it hard to read, especially on the back of a server in a rack.

Step 3: Consider labeling the cable in multiple places on the cable, for instance along the cable run under the raised floor or overhead ladder.
Installation

Adjusting Camera Field of View (FOV)

Place the camera at a height that allows the detection algorithms to function and yet high enough to prevent any tampering with the camera. The true sizes of objects can only be judged when viewing at an angle. The recommended height is anything between 4-8 meters (12-24 feet), the exact height is dependent on the area it has to cover, the topographic conditions, the type of intrusion to be detected, camera CCD and the lens.

Camera positioning should be such that the 'dead zone' of one camera is covered by another camera’s field of view. Ensure that there is at least one point where an intruder is detected by at least two cameras.

The position of the cameras relative to lighting is extremely important. Do not install cameras too close to lights which could attract insects, or facing into lights, windows, the sun, or in areas that have a large number of reflections or shadows.

The cameras should be aligned properly and installed as per design requirements:
- Place traffic cones or markers at the edges of the expected detection areas to provide a mechanism for initially aligning the camera for a perfect FOV.
- Alternatively have a person use a monitor and a two way radio to direct another person walking the site.
- Adjust the tilt properly so that the camera is aimed at upright people.
Installation

Adjusting Camera Field of View (FOV)

The Camera Field of View (FOV) has to be adjusted according to the standards. The following are the standards to set different FOV settings.

Detection View
Ability to detect any moving object/body on the screen and recognize the body in a view where it is displayed on 10% of the monitor screen.

Recognition View
Ability to distinguish a known individual from other known individuals in a view where his/her body is displayed on 50% of the monitor screen.

Identification View
Ability to identify any unknown individual for the first time in a view where his body is displayed on 120% of the monitor screen.

Number Plate Recognition
Ability to read clearly the numbers and letters on the license plate in a view where the license plate is displayed on 20% of the monitor screen.
Installation
Adjusting Camera Parameters through OSD

All cameras come with factory default settings, since light conditions different in each camera installation, use the OSD menu to change the default settings in the camera to optimize the video for the given scene or camera view.

The following camera parameters can be adjusted to provide optimum video for a given camera installation:

**Automatic White Balance (AWB)**
Accurate color reproduction requires that the camera compensate for the color temperature of the light source. Automatic white balance is a feature that the camera uses to do color compensation. For indoor applications incandescent, fluorescent, and quartz lighting all have different color temperatures. Outdoors there is sunlight, mercury vapor, and low pressure sodium lighting, all of which have drastically different color temperatures. In many applications the color temperature can change as lighting conditions change.

**Back Light Compensation (BLC)**
In CCTV applications it is common to have a bright light source behind the subject of interest. A person at an ATM or entering through an outside door are common examples. Without compensation, these subjects would normally appear as dark silhouettes. The aim of backlight compensation technology is to allow the camera to find the best picture conditions and automatically give the necessary light level compensation, so that users can obtain good identification of a subject in the foreground when there is a bright light source in the background. BLC works by enhancing specific zones in the picture which usually contains the subject of interest. WDR is a more effective alternative to BLC that does not depend on the subject being in a specific zone.

**Wide Dynamic Range (WDR)**
Wide Dynamic Range (WDR) technology helps to get detailed information from the dark part of the image without saturation from the bright part. There is no limitation of zone area with the WDR function and the color image is crisper than when using traditional BLC functions. It combines two fields which are high shutter speed exposure in bright areas and low shutter speed exposure in dark areas into one composite image.

**Digital Noise Reduction (DNR)**
Infinique’s cameras are equipped with 3D Digital Noise Reduction and have effective 3D noise filtering system which removes picture noise from the recorded video. These cameras give high quality video in low light conditions and by reducing the noise, they use less digital bandwidth and storage space compared to cameras without 3D-DNR.
Apart from Coaxial Cable, the CCTV video and audio signal can also be transmitted using baluns and Cat.5e or Cat.6 Twisted Pair Cable and Fiber Cable.

**Baluns and UTP Cable**
If the distance between the camera and the DVR is more then it is recommended to use Baluns. The function of the Balun is to allow the traditional 75-ohm coaxial video cable to be replaced by twisted pair cable in the CCTV security and surveillance environment, thereby allowing CCTV camera and monitoring equipment to be deployed for longer distances using structured cabling techniques. Depending on the baluns used the distances mentioned below can be achieved by using baluns:

- **Passive Baluns** - 670m
- **Active and Passive Baluns** - 1.8km
- **Active Baluns** - 2.1km

**Troubleshooting**
During the installation of the baluns various picture problems may result. It is important to know what is causing these problems and how to correct them.

**Total Absence of Signal** - is almost always due a discontinuity in the connection between the camera and the mux. Check the continuity of the twisted pair link.

**Smearing** - occurs when the edge of an image leaves trail traces similar to smudging a line of ink on a piece of paper. This may occur as the length of twisted pair cable increases. As the maximum distance specification is neared, the physical properties of the cable and baluns begin to show this effect. This is due to the effects of propagation delay and attenuation. Aside from using an active device with a built-in amplifier to correct the problem, the other possible solutions are:
- a) to shorten the length of cable or
- b) adjust the contrast and brightness of the monitor.

**Flutter** - occurs when the background fluctuates between light and dark. This symptom may be due to problems with the grounding between the CCTV equipment or the connection may be picking up some external interference from a nearby power transformer. A solution to minimize this effect is to adjust the monitor’s contrast and brightness.

**Ghosting** - is characterized by a second video image being received after the main image, resulting in a double image that is skewed in relation to the first. This is usually due to a problem with the UTP cable connection itself. Poor crimping, untwisted pairs, some of the twisted pairs may be longer than others, poor quality cable, exceptionally high crosstalk between the camera and the monitor are all some of the causes. In these cases it is best to replace the existing cable with a new one.
Alternative Cabling Solution
Transmission through CCTV Baluns—Troubleshooting

Loss of Color and Image Detail - may occur if twisted pair cable length exceeds the distance specifications. As the maximum distance specification is neared, the physical properties of the cable and baluns will begin to show this effect. This is due to the effects of propagation delay and attenuation. Other than using an active device, one can improve the image by shortening the length of twisted pair or by eliminating other contributing signal losses such as splices, cross-connects, low-grade patch cables, etc.

External EMI and RFI - The installation of the CCTV Balun should follow the cabling guidelines outlined in the TIA-568 standard for structured cabling. In regard to external EMI and RFI, it is recommended to keep the CCTV cabling away from strong sources of radio frequency or electromagnetic radiation:
- 5" from power lines of 2 kVA or less
- 12" from fluorescent lighting & power lines between 2 & 5 kVA
- 36" from power lines greater than 5 kVA
- 40" from transformers & motors

Flat untwisted cable is not recommended, even for patching with short runs since it acts as an antenna and will pick up nearby radio-frequency or electromagnetic radiation noise interference.

Ground Loop Problems - Due to the fact that the CCTV Balun features DC-continuity, one must be careful about ground loop problems. If there is a serious ground loop problem, then higher than normal current may flow between the CCTV camera and mux. This could cause the coil inside the CCTV Balun to overheat and fail. This problem can be spotted by the appearance of a pin-hole burn in the side of the balun. The balun will no longer operate after this.

One remedy is to correct the ground loop problem or replace the cable by coax, although the ground loop problem will continue to exist. Another solution is to install a ground loop blocker on the line.
Alternative Cabling Solution
Transmission over Fiber

For larger distances of CCTV Video Transmission, Fiber Transmitters and Receivers are used. Shown below is a Fiber Optic Ring Solution, which can be used for both Analogue and IP Cameras. The media converter is equipped with a built-in network management module which uses SNMP Protocol to monitor the health of the media converter remotely. With the use of fiber transmitters and receivers, the video signal from the camera can be carried to up to 80Km.