IP Surveillance Starter Guide

version 1.0

TABLE OF CONTENTS

Introduction

Every video surveillance guide lists cameras as the first thing that should be considered when designing a system. However this advice is *completely wrong!* This Starter Guide addresses key areas that almost every guide overlooks. There are several qualifying questions that need to be considered *before* you can determine what types of cameras are going to best suit your application.

Only *after* you have carefully considered the following questions, will you be ready to start comparing and evaluating cameras and recording software.

Here are the **TOP 7 QUESTIONS** you should review when planning your video surveillance system:

What Are Your Objectives?

Companies buy solutions to save money, increase profit or protect against potential loss or catastrophe. When planning your surveillance system, it's vital that you define all of your objectives. For example, if you focus only on loss prevention during the planning phase, then that's all you will end up with - a loss prevention system. It's good to keep in mind that IP-based surveillance systems provide many additional services that can increase profit and productivity in your business and potentially save you both time and money. To get the most out your surveillance system, the best place to start is within your business. Look around and identify areas that you may want to improve in terms of workflow and management. Where are you wanting to reduce costs or increase productivity? It's likely that some of these areas can be greatly assisted if you invest in the right video surveillance system.

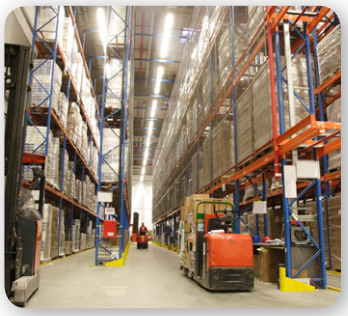
Here's three examples:

A **supermarket** chain needed to reduce shrinkage and speed up the checkout queuing times. By carefully positioning a few megapixel IP cameras, they can record store activity and monitor the aisles for congestion. When the lines start to fill up, a new check out is opened.

A **car dealership** was looking to invest in a surveillance system to protect their vehicles from out of hours damage. At the same time, they were also seeking a PA (paging) system so that they could communicate instantly with sales reps and mechanics from the office. The forward thinking business owner, began searching for a surveillance ➥

What are your objectives? *continued*

system that could provide both services. He ended up buying IP cameras equipped with VoIP functionality providing 2-way communication. This saved his company $12,000 up front, through not having to install a separate PA system. The showroom cameras are also streaming live to the dealer's website, being used as a marketing tool to attract new customers.



A **logistics company** wanted video surveillance to protect assets and monitor OH&S. At the same time they were investigating light management systems to save energy costs. Through careful planning they found an IP camera system that could manage the warehouse lighting via the surveillance systems motion detection function. The up-front cost saving was over $20,000.

Find a security company that understands your business

If you are an end user, you will at some stage engage security companies to provide quotes and professional advice. We recommend you seek out installers who have had the most experience in your particular industry - they are more likely to have a handle on common issues and solutions specific to your business needs.

Question to consider:

- What other areas of my business would I like the surveillance system to reduce cost or increase productivity? ■

Centralized or Decentralized VMS?

> video tutorial

Did you know that video management software (VMS) can be centralized or decentralized? It's important to be aware of the differences and options for each platform.

What is VMS?

VMS provides 3 core services:

• Alarm manager • Storage manager • Recording database

VMS (Video Management Software) brings intelligence and decision making ability to a surveillance system. Without VMS the system would be inefficient and difficult to manage. It is both technically and commercially viable to install only one type of VMS, so it's imperative you *choose well*.

Centralized VMS

The VMS is installed on a *central* recording device which is most commonly referred to as an NVR or DVR. Over 90% of video surveillance systems are centralized. The more you pay in terms of licensing, the more features you get.

Cost: Centralized VMS is sold under license and costs apply according to the number of cameras and recording devices connected to the system. Major upgrades fees apply.

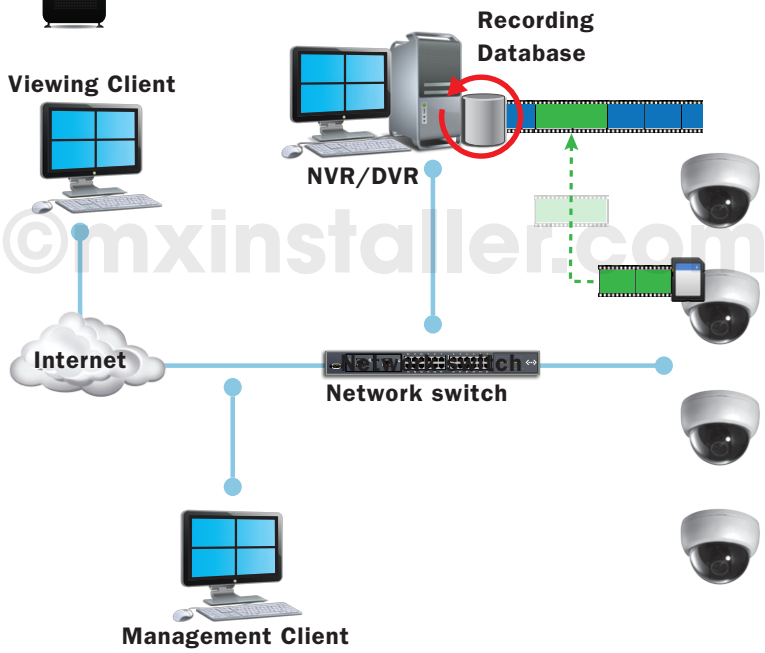
Decentralized VMS

The VMS is installed in the camera, which means each camera on the system has NVR functionality. Decentralized VMS is the very latest in surveillance technology. In 2013, less than 10% of cameras on the market are VMS-enabled.

Cost: Decentralized VMS is not sold under licensing as the software and feature upgrades are free. There are no manufacturer's licensing contracts or annual fees. ➥

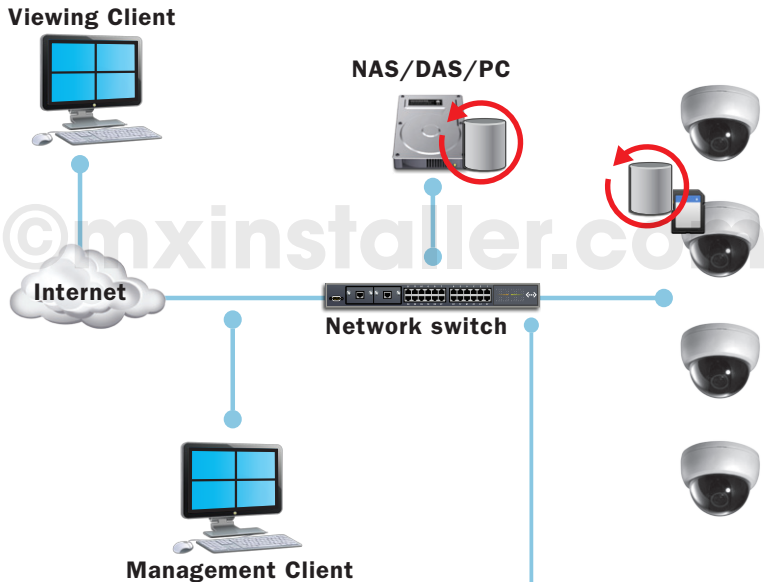
Centralized or Decentralized VMS? *continued*

CENTRALIZED VMS



In a centralized system, the cameras rely on an NVR or DVR where a central recording database resides, to complete the video management process. Because of this, recorded footage stored at the edge, must be transferred to the recording database located in the recording computer, for final processing and synchronization. Should the central recording computer fail, the system management fails and access to recorded footage is lost.

DECENTRALIZED VMS

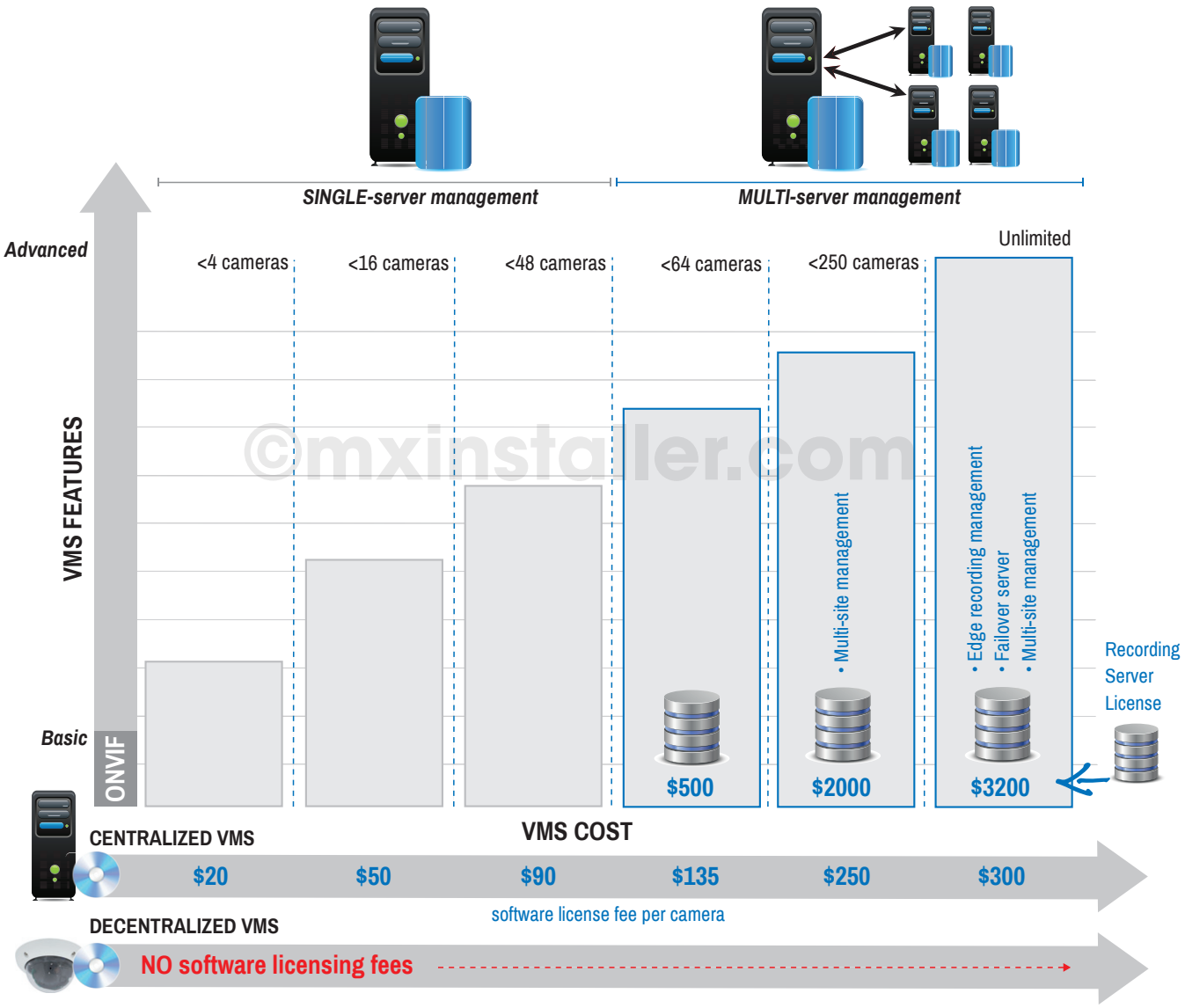


In a decentralized system, the VMS-enabled cameras can write video in a recording database directly to the storage device, allowing direct-to-storage recording. Any number of recording databases located in multiple storage devices can be simultaneously accessed and managed directly via a free of charge viewing client. Transfer of edge recordings to a central recording database (NVR) is not required.

Decentralized VMS allows each camera to write its own recording database directly to standard storage media - no NVR or additional VMS required.

Centralized or Decentralized VMS? *continued*

If you need centralized management service for several recording servers, then you should consider VMS that provides multi-server management. This allows users instant to access and administrate many recording servers and connected cameras simultaneously, speeding up the management and workflow process. By default Decentralized VMS offers multi-server management. Centralized VMS also can, but pricing for Centralized VMS with multi-server management starts at *around* $150 per camera license plus a fee for the recording server licensing. Pricing for server management over multiple sites costs even more. ➥



VMS features and pricing are as follows:

SINGLE SERVER

Decentralized: 

- *$nil - no charge*

Centralized: 

- $20 to $100 per camera

Management: Single server, single-site. Management of devices and access to recordings from only one recording server at a time from the client. VMS feature-set level is determined by price, as is the level of camera function-to-VMS integration. Not recommended for sites with 3 or more NVRs. NOTE: NAS-based VMS is the cheapest option, but these recording solutions are low-end and dont provide multi-server management.

MULTI-SERVER

Decentralized: 

- $nil - *no charge*

Centralized: 

- $150 to $300 per camera

Management: Multi server. Full management of multiple recording devices and access to multiple recording databases from a single viewing client. Pricing is charged according to the number of cameras - plus a server licensing fee. NOTE: *Only* Decentralized VMS offers multi-server recording management with NAS devices. ➥

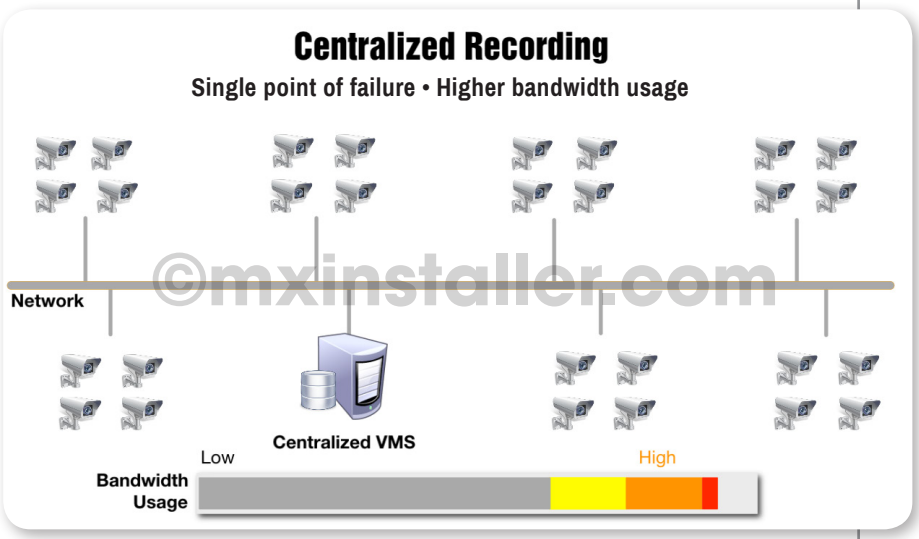
System redundancy

Redundancy is about ensuring the recording system can continue to write video data should an unexpected failure occur.

Centralized VMS

Here the recording hard drive/s are located on the same computer as the video management software. Generally a level of RAID is setup to ensure the system can still record in the event of a drive failure.

However the central recording server is a single point of failure. While RAID is important, it only protects against failed hard drive/s, but recording failure can be caused by many other factors other such as - power (PSU) failure, hardware conflicts caused by software upgrades, faulty memory, dust, viruses.



The two main options for redundancy are:

- Failover Servers

  If the loss of recorded video is not acceptable then a failover recording ➥

server can be setup. This provides data replication, so if the main recording server fails, the secondary computer will take over the system recording and management. Only the more expensive VMS solutions, offer failover services.

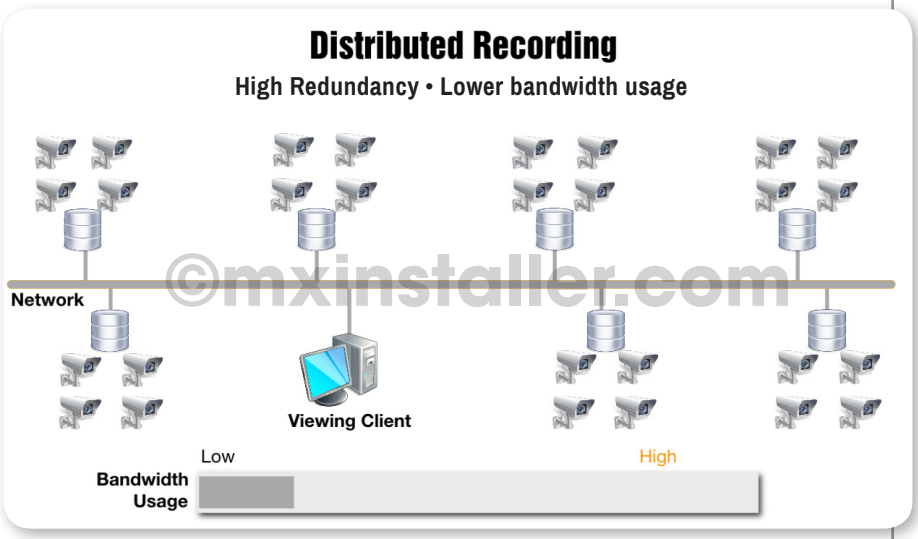
Cost example: Milestone XProtect Corporate is an enterprise solution that offers failover management, but costs around *$3200 for the base server software license. High cost is the barrier peventing most sites from implementing failover servers. *(*typical pricing USD obtained from online stores.)*

- Distributed Recording

  This is where storage devices are deployed at the edge of the network and cameras are split into smaller groups, with each group recording to its own storage device.

  This method is very effective as it can drastically reduce bandwidth load on the main network and spreads the risk of recording failure across multiple servers. If one server fails then only that smaller group of cameras have temporarily lost the ability to write video. ➥

> video tutorial



Distributed Recording can be achieved using centralized and decentralized VMS. The centralized platform requires licensed VMS deployed in servers located at the edge of the network. Decentralized platform requires only standard digital storage media.- SD, NAS, DAS, PC - no licensed VMS required.

Centralized or Decentralized VMS? continued

Cost example: VMS such as Milestone XProtect Professional would allow management of up to 5 recording servers within a single site. However licensing for say a 45 camera system @ 9 cameras per server would cost around *$6500. Of course purchasing 5 recording servers would also need to be factored in to the total cost.

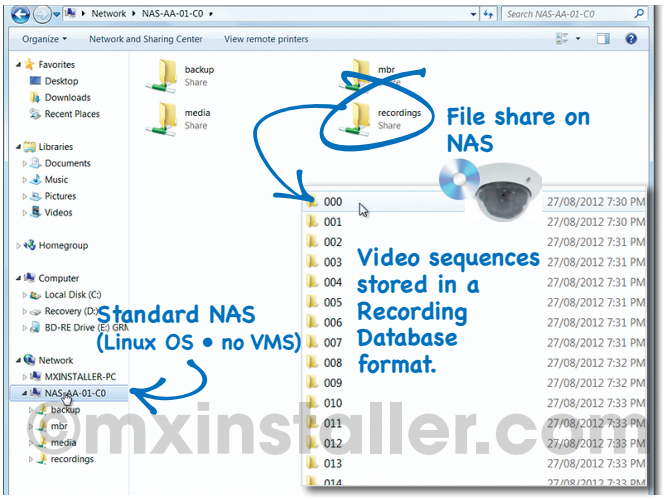
A lower cost VMS could be installed, but would not provide multi-server management. If the servers were installed across two or more sites, then a multi-site VMS such as XProtect Enterprise could be a recommended option, costing around *$13,500 for 45 cameras. *(*typical pricing USD obtained from online stores.)*

Decentralized VMS

Here the cameras on the system are VMS-enabled, which means they can write video in a *recording database format* direct to storage. The recordings and devices can be accessed and managed using a web or free-license viewing client - no VMS, no NVRs. This presents the customer with many options that are both simple and flexible. For example, distributed architecture can be implemented using inexpensive storage devices such as SD or NAS. Additionally, most storage vendors provide data replication software for free. ■

VMS-enabled cameras can write video to <u>any</u> digital media in a Recording Database format, allowing intelligent search and playback directly from the storage device - *no licensed VMS, no NVR.*

90% of IP cameras cannot do this!



Screenshot of MOBOTIX M24 sequences recorded to standard Linux NAS

Which Video Codec Is Best?

> video tutorial

In still photography, there are three main factors which impact image quality: pixel count • pixel density • file format

Other factors such as compression level, image processing, exposure etc, all play a part in determining the final image quality.

For capturing video, those factors are also very important.

In video surveillance sequences are recorded for evidentiary purposes, so capturing *movement in high quality* is absolutely critical, and sits above frame rate and resolution (pixel count), in terms of importance.

The quality of motion captured within the recorded sequence determines whether or not the video can be used to accurately identify people and objects.

In 2013, H.264 is the most prevalent codec in the surveillance industry. For example, the encoder used in all HDTV IP cameras is H.264. Let's examine if it is suitable for surveillance applications.

Why is H.264 so popular?

What's so compelling about H.264 is that it's efficient at *appearing* to stream video in higher quality than previous MPEG codecs and at lower bitrates.

A key feature is the codec's ability to discard huge amounts of detail from ➥

within each frame in such a way, that as the images flick across the screen at the right frame rate, the loss of detail goes unnoticed by the human eye. The brain is easily fooled using this clever technique. This positions H.264 as king for real-time streaming applications such as online movies and the evergrowing range of mobile applications.

Quality versus data rate

With MPEG-based codecs such as H.264, the appearance of high quality only works while the video is streaming and then only to a point. When frames rates and data rates fall below a certain level, the degradation in quality immediately becomes noticeable.

This is the reason why the video quality in a HD Blu-ray (DVD) movie is far superior to an equivalent online movie. For example, at 1080p resolution a Blu-ray movie is a much bigger data file, streaming at around 40mbps, whereas an on-demand movie at less than 7mbps. The difference in image quality between the two is enormous.

Which of the following two statements do you believe is most accurate?
1. “HD video delivers high quality video at lower bit rates”
2. “HD video delivers high resolution video at lower bit rates”

Statement no. 2 is most accurate, because picture quality is not determined by resolution alone. ➥

"H.264 standardizes only the decoder, this means there can be no guarantee of image quality, as vendors can apply their own techniques for encoding video. This is why H.264 video quality varies so significantly between camera brands."

➥ While resolution selection is an important consideration, resolution is only an assurance of the number of pixels in the image, but does not in any way guarantee image quality.

For example, H.264 video captured @ HD 1080p resolution can be recorded in low quality.

Be aware that many proponents of H.264, state categorically that both the HDTV standard and H.264 guarantee high image quality.

But is this claim factual? No it's not. The image quality produced by HDTV cameras varies significantly between brands. A visual comparison of HDTV IP cameras on display at any security show proves that HDTV standards do not guarantee anything but resolution size.

Another common claim is this one…*"without compromising image quality, an H.264 encoder can reduce the size of a video file by more than 80% compared with the Motion JPEG format…"*

It's interesting to note that this claim is found within the marketing material produced by almost every major IP camera vendor. ➥

It's certainly an extraordinary claim, but is it true?

In this excellent article, Here's what fake HD video looks like, engineer George Ou writes, (quote), *"Granted the usage of higher-end codecs like H.264/MPEG4-AVC can lessen the losses in quality, but no compression technology in the world can handle fast changing video with low bit-rates without severe degradation."*

While manufacturers of H.264/HDTV IP cameras will have you believe otherwise, the fact remains that as the bitrate is reduced, the video quality also is reduced.

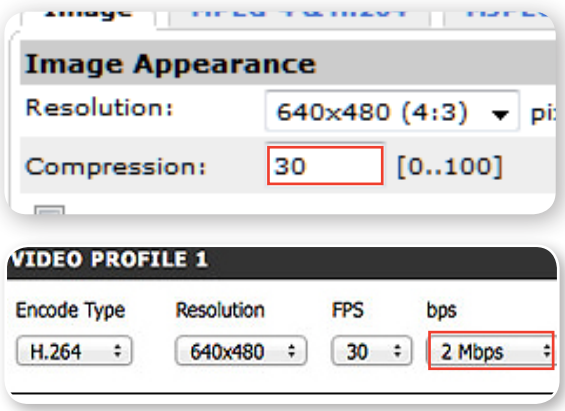
The above quoted article, also highlights one of the most fundamental but little known issues concerning H.264 – it cannot capture movement frame-by-frame in high quality at low bit rates.

Thus, the higher the video quality the more bandwidth and storage is consumed. This fact is not unique to H.264, it applies to *all codecs*! It's important to understand that the specific requirements of the site must determine the codec selection. Do not assume that H.264 is flexible enough to be used in every installation. ➥

IMPORTANT NOTE: Some proponents of H.264 may argue that comparing the use of H.264 in IP video surveillance with online TV broadcasting is not in the same context, as broadcasters stream video at fixed bit rates (CBR – constant bit rate) encoding, while with IP surveillance applications, fixed quality (VBR – variable bit rate) is most commonly used. However all H.264 cameras on the market are equipped with the ability to encode using CBR, as H.264 can be volatile. The VBR settings often have to be capped at a maximum bit rate to prevent bit rate spikes during peak times where sudden changes and movement may occur. Therefore using CBR in surveillance systems is no way, an "exception to the rule". Furthermore, the reference we've used with online broadcasting highlights the simple fact, that in the real world, the quality of HD (H.264) video *is* compromised at lower bit rates, just like any other codec.

For surveillance applications, we would only recommend H.264 for installations where:

- low bitrates are more important than capturing movement in every frame at the highest quality.
- potential network spikes during high activity periods are acceptable
- high resolution, high frame rate capture is more important than high quality frame-for-frame playback



FACT: As you lower the compression setting in an IP camera stream, it increases the camera's data bitrate output. This in turn increases the image quality - the result being that it will consume more storage and bandwidth.

H.264 is not one codec

MPEG codecs have profile level definitions so that it's easy to identify which are compatible with certain applications. For example, Baseline profile is mainly used for web applications and a HD (1080p) Blu-ray movie is coded using the High profile.

There are 17 profiles within H.264, each one having different capabilities - ➥

H.264 comes in many flavors - *17* in fact!

These are the 3 most commonly used profiles in IP video. Baseline is the most commonly used profile in IP cameras, but delivers the lowest video quality of all H.264 profiles.

See image comparisons between Baseline and Main profiles here

➥ thus they are not all equal. The H.264 profile selected and the way it has been implemented by the manufacturer will determine video quality.

Baseline is mainly utilized for mobile device streaming, producing the lowest image quality of all 17 profiles and surprisingly is most commonly implemented into IP cameras.

H.264 standardizes only the decoder, this means there is no "definite assurance" of image quality, as vendors can apply their own techniques for encoding ➥

"Within a surveillance system, video streaming is required but it's not what's most important. The system's ability to capture movement in high quality should be given highest priority."

➥ video. This is why H.264 video quality varies so significantly between camera brands. The reality is, a poorly implemented H.264 profile will negatively impact many factors, including video quality.

Price is generally the determining factor of image quality, for this reason be wary of low cost IP cameras.

In regards to the viability of using H.264 in video surveillance, this independent whitepaper, JPEG2000, MJPEG, MPEG and H.264 in the security environment, quotes the MPEG group as stating that it is an *"unsafe policy"* to use MPEG-based codecs (such as H.264) for surveillance applications, (for more information, please refer to page 5 of the document).

So, what about the bandwidth advantages of H.264?

As already mentioned, it's often stated by vendors that H.264 utilizes 80% less bandwidth than an equivalent MJPEG stream. This comparison is ridiculous in ➥

the context of recorded footage. When set at such a high level of compression, the H.264 video may suffice for live streaming, but not for playback, as the image quality in each individual frame would be insufficient, and would in no way compete with M-JPEG in the quality stakes.

This is why IP camera vendors touting compliance with the HDTV standards set by SMPTE, (Society of Motion Picture and Television Engineers), is superficial in relation to IP surveillance systems. SMPTE is about creating standards for *streaming* applications such as motion picture and television. The SMPTE specification does little to cater for the key requirements of video surveillance.

Here's what's far more important than compliance with television streaming standards…

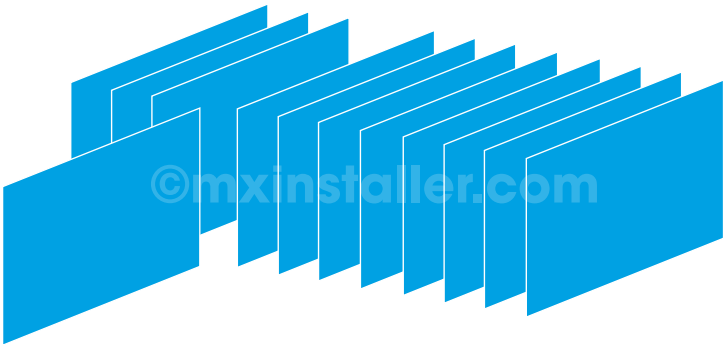
Within a surveillance system, video streaming is required, but it's not what's most important. The system's ability to capture movement in high quality should be given highest priority.

What a surveillance codec should deliver

As already covered, the codec should capture movement in high quality.

It needs to be flexible enough to allow users to slow down the recorded video, move back and forth frame-by-frame to find a high quality still image at any point within the stream and allow for digital zooming within the selected image. ➥

That's precisely where H.264 falls down – especially in frames where movement is captured. The digital zoom properties within individual frames are mostly inadequate.



A codec used for surveillance applications should allow users to extract still images, from anywhere within the recorded sequence and provide sufficient detail for digital zooming.

While proponents of H.264 will tell you that you can have it both ways – low bit rate and high image quality, the reality is you can't.

So the statement, *"H.264 delivers high quality video at low bit rates"* is an over generalization to say the least. In itself H.264 is not a guarantee of high quality video. As already highlighted, the video quality depends on many factors including bit rate and the profile implemented.

CBR vs. VBR

With compression formats you can select the data rate (bit rate) used over the network.

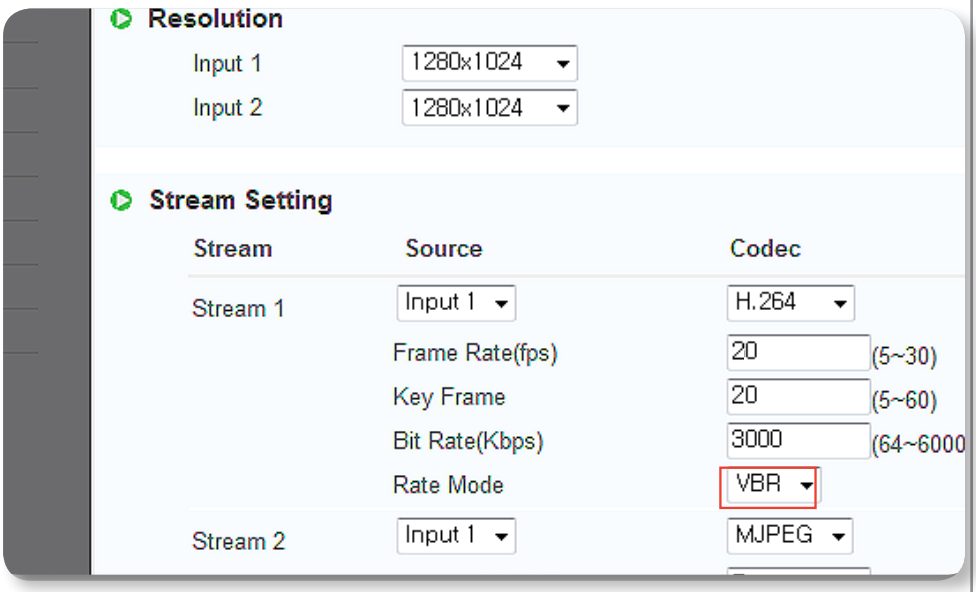
The two choices are CBR (constant bit rate) and VBR (variable bit rate).

Encode with CBR and motion will be captured in lower quality, ensuring the maximum data rate set is not exceeded. Capture movement encoded with VBR ➥

Which Video Codec Is Best? *continued*

and the bit rate goes up to ensure the preferred quality is achieved and movement is captured in higher quality.

When VBR is used, the bit rate advantage of H.264 is not realized where there is a lot of movement or changes in the camera's field of view.



Most IP cameras provide an option to encode video using VBR or CBR. While CBR may be ok for streaming, we strongly recommend selecting VBR only for recording, and select the lowest compression (highest bit rate) that is viable for your installation. This will ensure best possible quality recording.

In fact, multiple high resolution H.264 streams encoded using VBR, can bring a network to it's knees during busy periods where there's been high motion activity.

On the other hand, M-JPEG will not compromise image quality in frames where motion occurs, nor does it generate sudden spikes over the network.

What gives M-JPEG the advantage is that each frame is individually compressed and movement is captured in much higher quality, every frame is a key frame (I-frame), which is mainly why it produces a higher bit rate. ➥

H.264 applies compression to a GOP (group of pictures), in which the majority of the individual frames are missing a lot of detail, and by default capture movement in low quality.

When encoding in VBR the H.264 camera can be set to increase the number of key frames, however this completely negates the often quoted “80% savings” in bit rate advantage over M-JPEG.

As mentioned earlier, the more compression applied, the lower the bit rate which in turn lowers bandwidth and storage consumption – but also lowers the video quality.

Despite what IP camera vendors would have us believe, this simple fact also applies to H.264. There are absolutely no exceptions to this regardless of how advanced the compression implementations are.

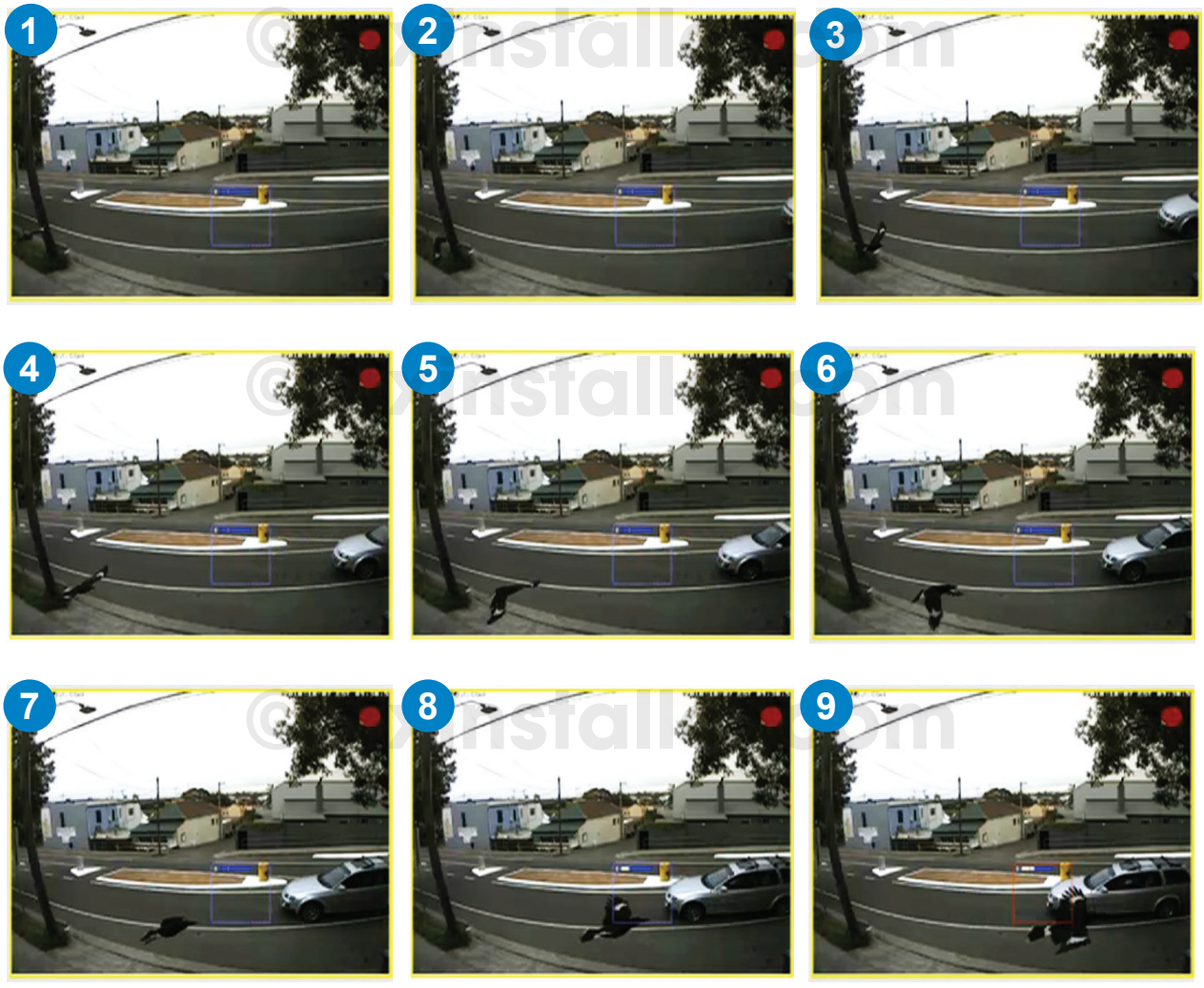
As a side note - one of the main contributors to bandwidth overload is not cause by codecs, but rather a poorly configured camera. When the camera’s event triggers have been setup correctly, this alone can dramatically reduce data rates.

The problem has been that none of these “off-the-shelf codecs” - M-JPEG, MPEG-4 or H.264, were ever designed for surveillance applications.

While we’ve been extolling the virtues of M-JPEG, by nature it can be a storage hog and deemed unsuitable for some applications. ➥

The only codec made for video surveillance

The only video codec that has been specifically designed for surveillance applications is MxPEG. To show the power of MxPEG, take a look at the following stills extracted from a recorded MxPEG sequence. Here a bird is captured travelling at around 9m/29ft in less than 0.5 seconds, - no blurring and no loss of detail.



You can view the recorded MxPEG sequence here. In a nutshell MxPEG captures movement within each frame in “jpeg-like quality”. MxPEG offers all the benefits of M-JPEG, at lower bitrates, consuming up to 70%+ less bandwidth. ➥

Frame Rates

H.264 is CPU intensive especially when there's a lot of movement or changes occurring within the scene.

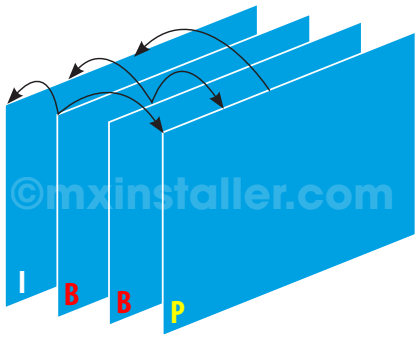
However, H.264 is also bitrate efficient thanks to the way it references the key frames (aka I-frames) containing the entire image, whenever changes occur within a group of pictures (sequence).

It's for this reason H.264 performs better at 25fps than it would at 12fps. At 30fps there are fewer changes between I-frames that have to be referenced within the video sequence.

Conversely, when the frame rate is slowed down from 30fps to 12fps, there will be many more changes to be referenced. Thus as the frame rate decreases, H.264 become less efficient.

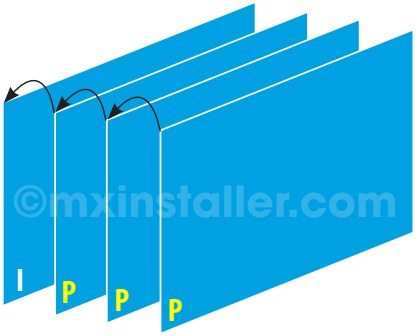
As an exercise, if you lower the frame rate of a H.264 camera, you will notice the bitrate is not nearly as efficient as when you increase the frame rate. In fact H.264 bitrate efficiency over M-JPEG is not so impressive at low frame rates. Of course, the variance in efficiency will depend on the actual implementation of H.264. ➥

H.264 MAIN/HIGH PROFILE



Higher video quality than Baseline. CABAC coding, includes B-Frames. Higher latency, more complexity and higher CPU cost.

H.264 BASELINE PROFILE



Lowest video quality, lowest latency and CPU complexity of all the profiles. Made for mobile device streaming and video conferencing.

There are of course exceptions to this, but very few sites require recording at high frame rates.

The reality is, the vast majority of security systems are configured to record at less than 10 frames per second (fps). It's at these lower frame rates, M-JPEG easily beats H.264 for image quality. Security professionals who understand highest quality image capture is more important than high recording frame rates, have long appreciated M-JPEG's viability in surveillance applications.

Unfortunately, because of the varied profiles and implementations used by the manufacturers of H.264 IP video, there is a huge difference in the final results.

For example, a three second incident captured at 25fps, may look great on the live monitor but be compromised during the recording process due to low bitrate compression. Thus high resolution streaming in no way ensures the ability to playback the event in detail, frame by frame. This is why choosing the right codec is so critical to the overall success of the system. By combining the strengths of both M-JPEG and MPEG-based codecs, MxPEG is extremely viable in both high and low frame rate environments.

Conclusion

The important question to consider when choosing a video codec is - do you want lowest bitrates or best image quality? As already shown, you can't have both.

If capturing video for the purpose of positively identifying a person or object ➥

"Unfortunately, because of the varied profiles and implementations used by the manufacturers of H.264 IP video, there is a huge difference in the final results."

➥ is your aim - then invest in a system that supports a codec that will achieve those results. If you have already installed MPEG-based (H.264) IP cameras, our recommendation is to set them up for dual streaming. Configure the live stream to be encoded with H.264 and the recorded stream using M-JPEG. This will absolutely ensure the recorded video is at the highest possible quality. Like M-JPEG, MxPEG will allow you to safely predict the bitrate consumption, in turn allows for more predictable bandwidth and storage.

H.264 is not as predictable, unless you cap the bitrate. MxPEG also allows users to extract high quality stills from within the recorded sequence for evidentiary purposes. MxPEG holds an added advantage over M-JPEG as its bitrate consumption is up to two thirds less.

Notes...

Here we briefly explain why certain comparisons were used in this section...

• Why use online movies as a comparison - aren't the applications and environments for IP cameras and online movies very different?

A consumer primarily relates HDTV to television and movies. This comparison was used to highlight the fact that a video that is streaming in ➥

"High Definition" can be low quality. It also debunks the statement, *"H.264 delivers high quality video at low bit rates"* – the comparison shows that the quality of H.264 is directly affected by low bit rates. In the same way, HD video streams from a security camera system, both IP and DVR, are often streamed at low bit rates thus recording in low quality.

And informed buyer is one who understands that HDTV is just a marketing label - rather than a guarantee of quality.

- But aren't online movies encoded in CBR not VBR?

Some may argue the fact that IP cameras are more commonly setup to stream at VBR (variable bit rate), whereas online movies stream at a CBR (constant bit rate), so it's an unfair comparison. However consider this…

It is certainly true, CBR will apply higher compression to a video stream so movement is captured in lower quality than a VBR stream. VBR ensures the quality is preserved while streaming which also means the bit rate fluctuates according to movement.

Thus the more movement or changes in the scene the higher the bit rate spike.

It's ironic when you consider that bit rate efficiency is a major USP being spruiked about H.264, yet simultaneous H.264 VBR encoded streams triggered by motion can quickly cause serious bandwidth issues on a network. ➥

Many do not understand this, measuring a camera's bandwidth usage while there is little to no movement.

When encoding H.264 as VBR an initial test should be conducted to prepare for worst-case scenarios. Test recordings should be done during peak periods where there will be the maximum amount of movement. Otherwise your network could be in jeopardy.

• Why the comparison between H.264 and M-JPEG?
To debunk a common myth that H.264 delivers better image quality than M-JPEG. As we have shown this is simply not true.

It's important to understand that while H.264 is best for streaming, M-JPEG excels in capturing, recording and frame for frame playback. M-JPEG is a predictable codec, so there are no sudden bit-rate spikes. Unlike H.264, both M-JPEG and MxPEG are very resilient in varying light levels.

However, the problem with M-JPEG is that it constantly captures everything – changed or not – in every image, which is an absolute waste of data. What is needed is the best of both worlds. This where MxPEG excels. ■

Which storage technology will you use?

For the majority of installations, storage is *very* easy to calculate and select, once you understand a few basic principles.

What you are looking for is one or more storage devices that will cater to the needs of the system in terms of price, robustness and performance. This may seem obvious, but too often the wrong type of storage is specified for a system.

A combination of the following two factors must be considered:

- storage system requirements (data throughput, capacity etc)
- expectations of the customer.

While keeping costs down is obviously going to be important to a customer, it's even more important that the buyer fully understands what the difference will be if recording to low cost storage as compared with quality storage.

Here are some qualifying questions that should be discussed prior to purchasing storage:

- what is an acceptable level of recording downtime (in hours/days)?
- how would the business be impacted if loss of recordings did occur?
- what level of redundancy is required (UPS, RAID, offsite archiving etc)?
- will a HDD swap out service need to be scheduled to prevent drive failure? ➥

This consultative approach will protect both the installer and the customer and ensure the right storage solution is selected.

Types of storage


NVR

NVR (network video recording) - is the most traditional form of IP video storage. This is comprised of a Windows PC/Server with VMS (video management software) installed. Traditionally an NVR was purchased as an all in one hardware/software solution. Today most VMS is bought separately and customers source their own recording hardware.
If you use decentralized VMS then you can direct record to any standard digital storage media - this means you can bypass NVRs and VMS licensing costs.


SD

SD flash allows in-camera recording, for edge recording to 64GB and beyond, reducing bandwidth. Only the more expensive centralized VMS packages allow for multi-site management of SD recordings, with the cost starting at around $250 per camera license. Thus SD recording is not often used in centralized systems. SD card recording and management is more commonly used with decentralized VMS because it doesn't cost any extra.


DAS

DAS (direct attached storage) - in a decentralized VMS system, you can attached Ethernet hard disks directly to the cameras. This is a viable option for low-end low-budget installations only.
Note: in a centralized VMS system, DAS has a different meaning - it always refers to storage that is attached externally to the NVR. ➥

Which storage technology will you use? *continued*

RAID storage - this is a storage device with two or more hard drives. In a system with decentralized VMS, the camera can direct record to any NAS or PC/Server, that has only the operating system installed (Win/Linux). The wide range of options, brands and reasonable pricing makes NAS a very popular storage choice for decentralized systems. Some manufacturers claim their IP cameras can record direct to NAS, but this usually means the video is not stored as a recording database thus cannot be managed.

NAS with VMS installed is classified as an NVR.

Choosing which storage device is bested suited to the needs of your installation will come down to 3 main factors:

- recording data rate (mbps)
- storage capacity (GB/TB)
- redundancy

Most IP camera and VMS vendors provide online calculators that will help you work out your system storage requirements.

Note: be aware that there will be noticeable discrepancies in the bitrate estimations between IP camera vendor's online storage calculators, even when identical data has been entered.
Much of the discrepancy is caused by the huge variance in H.264 profiles and methods of encoding implementation. ➥

Which storage technology will you use? *continued*

The following 5 areas need to be calculated to work out the recording data rate and storage capacity requirements:

- frame rate
- recording *(snapshot, continuous or event based)*
- resolution *(pixel count)*
- image quality *(low/high compression)*
- image complexity *(expected scene changes, movement and color)*

Recording data rate - is the total recording bitrate that the storage device will need to handle when writing data to disk. Knowing what this figure is will help you determine the write speed requirements of the storage device.

Calculating write speed

Why is measuring write speed important?

If you purchase a storage device that has a maximum write speed of 40MB/s, but your total recording bitrate ends up at 45MB/s then the storage device will not be able to handle the incoming traffic, resulting in recording issues. One solution for this would be to purchase a second recording device and split the camera recording data between the two.

On the other hand, if you have estimated that the total data throughput will be 100MB/s, it would be inadvisable to buy a device that can handle 105MB/s, unless its a professional video storage device, as the life expectancy of the device ➥

will be considerably shortened due to the wear and tear caused by constant data writing.
A commercially viable option would be to split the cameras so they are recording to two devices - halving the recording data rate to each storage device. If you will be recording to several recording devices, please refer back to the section on multi-server management.

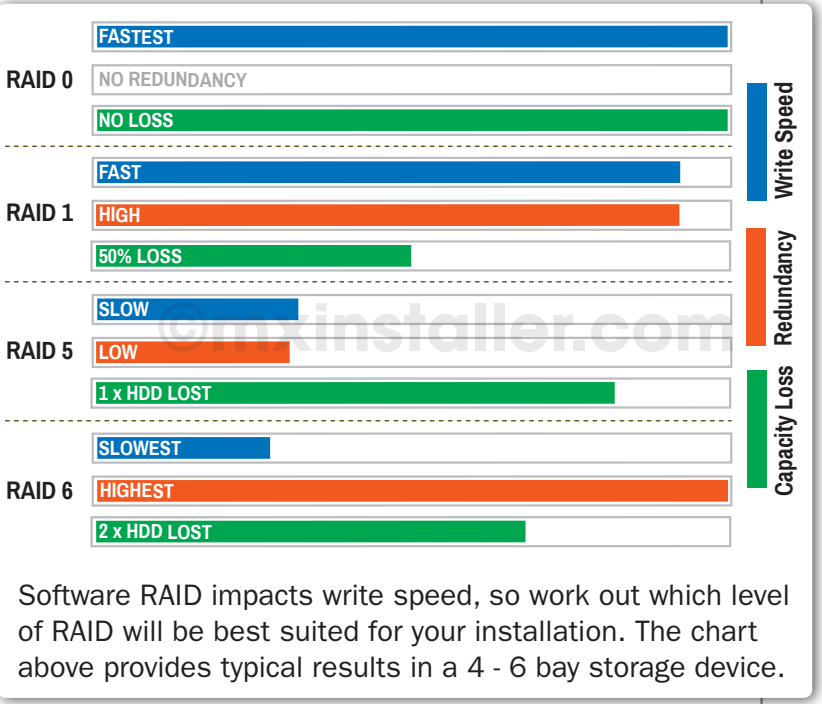
The write speed of a storage device can be impacted by 3 areas:
• Variable Bit Rate • RAID • Disk capacity.
All three must be factored in, otherwise you will run into recording errors.

1. Variable Bit Rate (VBR)
When recording video for evidentiary purposes, encode using VBR to ensure the movement and changes in the scene are captured in the highest possible quality. However keep in mind that VBR will cause fluctuations in the recording bit rate. This means that you need to plan your storage around the times when the bitrate will be at its highest peak.

If for example, the manufacturer's bandwidth and storage calculator estimates the recording bitrate from your cameras be 40MB/sec, this will not be a constant bit rate. When the cameras are encoding video in VBR, the bit rate will fluctuate above and below the estimation of 40MB/sec.
So you need to find a storage device that will handle the bitrate at the *highest bit rate* periods. Otherwise, at times, the storage device will not handle the data throughput, and cause recording errors. ➥

2. RAID

Storage devices with software RAID controllers are much less expensive than those with hardware controllers. However the write speed of a software RAID controller is directly affected by the class of CPU installed in the NAS. For example, RAID levels 5 and 6 are processor intensive so will deliver a slower write speed than RAID 1.



Software RAID impacts write speed, so work out which level of RAID will be best suited for your installation. The chart above provides typical results in a 4 - 6 bay storage device.

Once you have decided upon which level of RAID is best for your application, find out the write speeds of the storage devices when configured to that level of RAID. Seek out storage devices fitted with Intel Dual Core CPUs, as these will deliver better RAID performance. Avoid using low end devices fitted with CPUs (e.g. Marvell) - these generally lack the required write performance.

3. Disk capacity

A 25% buffer of free space, should always be factored in and allocated to the storage device.

To put it another way, the stored video on the device should not exceed 75% of the total hard drive capacity. ➥

Allocate 25% free space to maintain consistent recording performance. If the recordings exceed 75% of the total storage capacity, the HDD write speed begins to slow down.

When hard drives fill up beyond 75% capacity, the write speed of the drive will start to slow down *exponentially*. Hard drives that have less than 25% free space left, should be considered over-full, as this is a common cause of recording errors, due to a physical limitation in the way hard disk drives write data.

Calculating storage capacity

Find out what the Total Estimated Recordings are. Once you have calculated how much storage the cameras will consume, apply the following formula. Note: if you are using a vendor supplied storage calculator, be aware that the estimations vary between vendors.

Total Estimated Recordings + RAID + 25% buffer

So for example, let's assume the IP camera storage calculator has estimated that your IP camera system will consume a total of 2500GB of storage, and you have decided on a RAID 5 configuration. Then a NAS with 5000GB of RAW storage capacity is needed. ➥

Here's how the calculation would look for 4-bay storage device:

Recordings		2500GB
+ RAID 5	25%	1250GB
+ Buffer	25%	1250GB

So in this case a storage device with **5000GB** is required.

Enterprise hard drives

> video tutorial

Enterprise class hard drives should be used to record surveillance footage. They are designed to run 24/7/365. Desktop drives are not. Enterprise class drives are designed to withstand continuous writing of data. Desktop drives are not.
Enterprise-Class drives are purposely designed for RAID environments so can handle the vibrations caused by multiple disks spinning in close proximity. Desktop class drives are not.

Enterprise class drives use error detection at every stage of data transmission within the system. They proactively repair defective sectors on the platters within seconds to prevent potential read/write failure and performance degradation.

These attributes are not only important, but critical for surveillance applications. (See our Seagate interview - Which hard drive is best for video surveillance?).
Note: according to Seagate, Enterprise class SATA hard drives are suitable for the majority of video surveillance applications. ➥

Low Cost Storage

If you are going to opt for low-cost storage devices, do it with both eyes open and be honest about the results you're expecting. In other words, when recording multiple high resolution streams to a low-grade storage solution, don't expect seamless, trouble-free recording.

What makes a storage device "low-grade" in terms of recording video footage? Usually devices built with Marvell CPUs and desktop-class drives are an indicator. These for the most part, lack all the necessary functions, such as consistent write speed particularly in RAID.

Most lack the ability reconnect to the cameras on power loss or reboot. Thus a UPS is generally recommended if choosing to use one of these devices, which really negates the low cost benefits.

If you're an installer, be open with the customer about the differences between cheap storage vs. quality storage.

Based on feedback from installers in the surveillance community, and our own lab tests, 1 and 2-bay NAS devices are unsuitable for most security applications.

Low-cost devices *can* be a viable option in non-critical applications where there is very low recording activity. But again consult with the customer, to ensure if fits with their expectations in terms of recording reliability and redundancy. ■

Do you want to integrate with existing systems?

A retailer wants to integrate the video surveillance with an existing POS system. Local municipalities want to enable license plate recognition and a university wants to overlay weather station information onto the video captured by a local camera. A chocolate factory would like to use IP cameras to count the candy bars as they are moving along the conveyor. A warehouse facility is seeking a way to integrate management of their lighting system via the camera's analytics.

All of the integration examples mentioned have been successfully created and are being used to protect assets, improve public services, increase productivity and save time. Before buying a surveillance system, look around your business and think about what other systems you would like to integrate - lighting, alarm system, electronic gates, serial devices, GPS tracking, RS-232 data capture, asset management, mobile monitoring etc. The ways in which you can leverage an IP-based surveillance system is practically unlimited.

Whatever you are wanting to integrate, it's *highly* probable there is an existing solution already. So, before you even consider obtaining an Application Programming Interface (API) and start programming, your first point of call should be to find out who else has already done what you are trying to do.

Forums provide you with instant access to solutions providers located all over the world, so they're a very good place to research if your required solution exists. Forums will certainly increase the likelihood of finding a solution. ■

Should the system be “ONVIF Compliant”?

> video tutorial

Many IP video manufacturers make the following claim...

“Our products support ONVIF, which is a plug-and-play standard...”

Here we examine what ONVIF is, and whether or not it really is a “plug and play standard”.

ONVIF is about developing a universal device enabler, so that any “ONVIF compliant device” will seamlessly connect to any “ONVIF compliant software”.

While the ONVIF committee talk about future possibilities in terms of seamless integration, many IP video manufacturers are claiming their ONVIF compliant products are future proof and offer out-of-the-box plug and play integration.
But does ONVIF compliance really deliver this? What are the facts?

Proposed specifications in any industry, must first pass qualifying processes to prove viability in the real-world, before being elevated to “standards” status. ONVIF is no exception.
The ONVIF committee has confirmed this in their document entitled - About Standardization, where it states, *“The specification developed by ONVIF is not a standard in itself.”* Which then begs the question - why is it that most of the companies sponsoring the ONVIF initiative are claiming their products are compliant with the “ONVIF standard”? ➥

Should the system be "ONVIF Compliant"? *continued*

Since forming in 2008, ONVIF has stated that the ultimate goal is to bring seamless integration, openness and greater interoperability. However, four years on ONVIF has still not reached this objective.

There have been plenty of panel discussions, press releases and meetings but the main goal have proved illusive. It's actually brought with it a whole new set of problems. Ironically most of them have to do with lack of interoperability. Systems installers working with so called ONVIF compliant products, are finding integration to be chaotic, rather than seamless.

One problem is, some vendors have been applying their own interpretation of the ONVIF specification, thus the implementations vary. This in turn causes confusion in relation to device compliance. For example, the device testing tool provided by ONVIF may confirm a camera's compliance, but there can still be integration issues with some of the compliant VMS (recording software). Manufacturers are required to constantly release updates for their ONVIF compliant products so they can integrate with the differing VMS applications - some are doing this others are not.

Not keeping up to date with the latest ONVIF specification is causing incompatibility issues. Unfortunately, there is no means to effectively govern this. To the annoyance of the installer, cameras often have to be software downgraded, to an older version of the specification, so that the device can connect to the "compliant VMS". The process of integration has been so common place, that industry experts are recommending integrators first verify camera-to-VMS interoperability ➥

in a test setup prior to installation. Which when you think about it, undermines the logic of buying ONVIF compliant products in the first place.
Profile S was released as a guide to help installers navigate the specification but this has not resolved the deeper, causal issues. For these reasons, end users should be advised that ONVIF-compliant products are not "standards compliant" in terms of guaranteed interoperability and plug-and-play is far from being a reality.

The reason a proposed "universal enabler" such as ONVIF is such good news to the security industry, is that 90% of the IP video devices on the market today, are not self managing and thus require third party VMS. Integration is thus required so that the hardware can integrate with the software.

But the success of any installation is the end result of creating a seamless end to end solution. How powerful the overall solution will be is always determined by both the level of compatibility and depth of integration. If and when a global plug-and-play standard is ever be achieved, this will still be limiting if the integration remains at a basic level.

Remember, ONVIF is about integrating only the basic functions. Even more importantly, the camera-to-software integration or future-proofing under the specification is not and cannot be guaranteed. As the specification stands today, users cannot expect immediate plug-and-play integration when purchasing ONVIF compliant devices. While standards are important, they are a guideline only, thus standards compliance is not an assurance of quality. ■

Will the system be future proof?

We all know what water-proof, sound-proof, fire-proof and bullet-proof mean. Manufacturers that label their products as such have both a moral and legal obligation to deliver on the promise of "proofing" against the thing specified.

Should manufacturers also carry the same sort of responsibility when claiming their products are future proof?

Is future proof just another marketing term or are there tangible benefits being offered to the customer?

According to dictionary.com, the definition of "future-proof" is - -adj, (of a system, computer, program, etc) guaranteed not to be superseded by future versions, developments, etc"

If we're to believe everything vendors tell us, then all IP video devices and VMS applications on the market are future proof - but is that the case, and what does future proof mean in real terms?

Here's what many believe makes a system future proof:

- *"easy to expand and adapt to the future system."*
- *"a truly future-proof solution is one that enables some part of video analytics at both points – server and edge."*
- *"...can be easily integrated with other digital devices..."* ➥

Is it actually future-proof or something else?

How can a consumer determine what's fact or fiction when a vendor lays claim to having "future-proof" technology?

There are 3 main areas that IP video product vendors are saying prove they have 'future proof' products" - let's examine them...

1. IP devices are future proof

An IP device, does not mean the product is future proof. There are varied approaches to the design of IP cameras, and there have been an alarming number which were not 100% digital. The low price tag is often an indicator.

A trick often used to keep the cost of production down, is the approach of cobbling together a cheap analog camera with a hardware digitizer, placing this into an outer casing and on-selling the device as an "IP camera" and "future-proof".

While the device is IP enabled, it can only produce low analog-quality resolution. Within a relatively short time of being installed, these very same "future proof" cameras have been thrown onto the junk pile and replaced with newer technologies, because the image quality is deemed comparatively inadequate.

The point is, just because an IP camera is a "network device", does not in anyway ensure the device will be relevant in the short term. ➥

Will the system be future proof? *continued*

Technology becomes obsolete when it no longers caters to the user's needs, or when something more advanced comes along that allows users to do more. This also applies to video surveillance, highlighting the importance of careful planning and not buying into the future proof myth. Your system requirements will eventually change, so try to plan for those future changes as best you can, today.

2. 'Open platform' VMS

It's not just the camera manufacturers who are furiously waving the future proof banner. With hand on heart sincerity the VMS vendors are also claiming 'future proofing' under the banner of an 'open platform'.

The upside to many VMS applications is that the software will support multiple brands of cameras and is thus "open platform" camera-side.

The downside is, the solution is "closed-platform" server-side because the customer must commit to and invest in a single vendor's brand of software.

The limiting factor part from cost, is that not all of the camera's core functionality and advanced features are included into the VMS application - unless you invest in the enterprise range of VMS applications, but even that's no gaurantee.

While the strength of VMS solutions is that they support a large number of cameras models, in most cases the level of camera functionality integration with the software application is quite basic, not leveraging the full capabilities of the cameras the customer has purchased. ➥

Will the system be future proof? *continued*

One simple example is edge recording. A growing number of IP cameras have been able to record at the edge (at the camera), to HDD or SD card since 2007/2008. Today in 2013, seamless management of in-camera storage remains unsupported by most VMS applications. 90% of camera systems can only deliver centralized management of SD recordings over multiple sites, with expensive enterprise level VMS.

The main point being that if newer, better camera technologies are released, these advanced functions may or may not be implemented into the VMS by the vendor. So it's more about "future possibilities" than "future proofing".

3. Global standards

As mentioned earlier in this guide, ONVIF has been promising future proofing of devices with plug and play integration. However since its first release 4 years ago, it's still a pipedream, rather than a reality.

The IT industry has had global standards in place for many years, but even so, future proofing is viewed as nothing more than crystal ball gazing. Tech experts quickly criticize IT vendors when claims of future proofing are made, because technology is changing too quickly, making it increasingly difficult to predict what new platform or solution the market will demand next. With the pace of technological advancement accelerating, the changes over the next ten years will be even more dramatic than the previous. In short, the statement 'future proof' cannot and is not a guarantee on your investment.

Thus predicting developments in technology is about making reasonable guesses as to what's just around the corner, in the next year or two, but try doing it ➥

Will the system be future proof? *continued*

long term into the future and you're setting yourself up for failure.

What to look for

To ensure the best return on investment, consumers should first ignore the promise of future proofing and look for IP cameras with the following important attributes:

• 100% Digital

The ability to stream, record *and scale* in high-resolution video. Camera features and quality increase with price. Determine how important resolution and image quality for your installation. Compare the codecs (H.264, MxPEG and M-JPEG) during live view and also playback.

• Recording Platform

Give serious consideration to where you want the system recording functionality and intelligence to reside - in a server (centralized VMS) or the camera (decentralized VMS). The cost and ability to scale for each platform is vastly different

• Software upgrades

Centralized VMS upgrades are installed at the server and generally charged for. Decentralized upgrades are installed at the camera at no cost - we are not just talking about general firmware upgrades, but real VMS functions and improvements. Upgrades often include - new types of analytics, recording options, storage management and other latest tech are made available free of charge. ➥

Will the system be future proof? *continued*

It's an unfortunate fact that over 90% of the cameras purported to be future-proof on the market would need to be replaced to take advantage of any of the previously mentioned function updates. Why? Because they are hardware chipset- based not software-based. Thus major tech updates require camera replacement and also time for the VMS vendor to integrate the new tech into their software - if and when it ever happens.

• Scalable in Hi-Res

Most IP camera systems aren't setup to record in high resolution, particularly in megapixel. Because of the way VMS applications handle incoming video streams, a central server has to carry all of the load, and perform most of the video processing.

To handle this, the server spec required is usually beyond the budgets of many users. Customers wanting a highly scalable megapixel IP video system should invest in IP cameras that individually handle the video processing load (i.e. write video in a recording database format), not just encoding the video.

If each camera on the system is individually handling the load, the system can scale in size efficiently and cost effectively in high resolution, without having to sacrifice image quality or frame rates. This is important, as the video recording should be in the highest possible quality, with enough footage and detail to allow digital zoom for identification. This combination of these in-camera features means the system will have the longest life cycle, be the most flexible and open to future developments. ■

Video tutorials

NOTE: to access these tutorials you need to be registered and logged in @ www.mxinstaller.com

IP Camera Buyers Guide

Choosing a recording platform

How IP cameras record to NAS

VMS Buyer's Guide

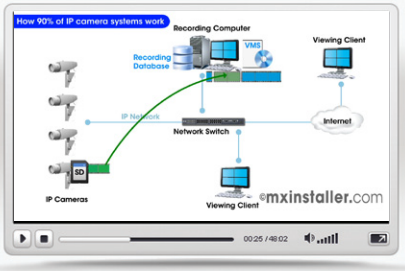
Alarm vs. Video monitoring

Hemispheric is disruptive technology

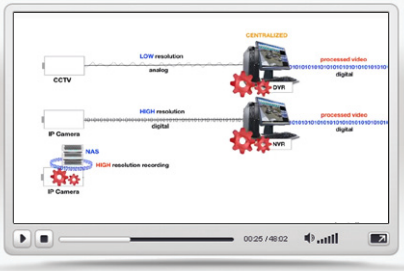
Which HDD is best for surveillance

ONVIF compliance: plug-n-play?

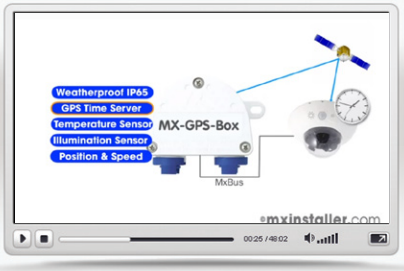
Is VMS licensing too expensive?



Cameras that record direct to storage



How an IP camera system works



How to GPS enable a camera