A Surveillance Director’s Guide to Digital Video

By Conrad Steffen & Donald Cogswell
# Table of Content

About the Authors .......................................................................................................................... 6 - 6 -
Introduction ..................................................................................................................................... 7 -
A Brief History of the DVR .............................................................................................................. 10 -
Common DVR Myths ......................................................................................................................... 12 -
What is a Security DVR ..................................................................................................................... 14 -
PC-Based Vs. Non-PC-Based ........................................................................................................... 15 -
Fault Tolerance ................................................................................................................................. 17 -
All DVR’s and Solutions are not Alike ............................................................................................ 27 -
DVR Card Differences ....................................................................................................................... 29 -
Bottlenecking ................................................................................................................................... 30 -
Shared Resources ............................................................................................................................... 31 -
Frames / Images Per Second ............................................................................................................... 32 -
Image Resolution ............................................................................................................................... 34 -
Bitrate ............................................................................................................................................. 36 -
Storage ............................................................................................................................................ 40 -
Video Quality Vis-à-vis Frames-Per-Second .................................................................................... 41 -
Size Matters ..................................................................................................................................... 42 -
Codec Algorithms .............................................................................................................................. 45 -
Compression Technology .................................................................................................................. 50 -
Compression Technology Challenges ............................................................................................... 51 -
Why is Everyone So Slow to Adapt ................................................................................................. 53 -
Obsolescence ................................................................................................................................. 55 -
The DVR Software ............................................................................................................................. 57 -
The Hardware Components ................................................................................................................. 60 -
Peripheral Software ............................................................................................................................ 61 -
The Heartbeat of your DVR ............................................................................................................... 62 -
References ........................................................................................................................................ 63 -
Welcome To The Future ..................................................................................................................... 64 -
Buyer’s Checklist ............................................................................................................................... 66 -

www.aventuratechnologies.com/casinos
About the Authors

Conrad Steffen

Conrad is the Director of Gaming Operations for Aventura Technologies, Inc., a pioneer in intelligent next-generation digital video solutions. Conrad has a 15 year history in video surveillance with some of the most preeminent names in gaming. Conrad began his gaming career in the 90’s, working with the likes of Mirage and Bellagio. Later in his tenure he moved over to Mandalay Bay and Circus where he was the Director of Surveillance. Prior to his career in video surveillance, Conrad spent 15 years in the military, with stints at Fort Knox and Fort Huachuca, home to the US Army Intelligence Center.

Donald Cogswell

Donnie is the Chief Technology Officer of Aventura Technologies, Inc., a pioneer in intelligent next-generation digital video solutions. Donnie is one of the originators and developers of voice-and-video over network protocols for video surveillance, dating back to the 1990’s. Prior to his co-founding Aventura Technologies, Donnie designed some of the communications industry’s first residential Voice-Over-Internet-Protocol (VoIP) solutions for International Bell Networks. Before his migration over to the video platform, as a Senior Analyst/Developer Donnie created security software solutions for banking. Donnie is a seasoned programmer and networking expert, certified in various skill sets.
Introduction

by Conrad Steffen

The surveillance industry has come a long way, since the days of the catwalks and two-way mirrors. As late as 1990, most surveillance departments were still writing incident reports by hand on yellow legal pads. Although the personal computer was around, many of those relegated to the surveillance department “old timers,” didn’t know how to work them.

Since well before my time, surveillance directors have struggled to define their department’s job description beyond “protecting the corporate assets.” Company executives knew very little about gaming, and even less about surveillance. Each surveillance director I’ve either worked with, or known, runs their department their own way.

Although some so-called experts have written books on how to run a surveillance department, the fact is that running a surveillance department is a little like raising a child. There is no single right way to do it. However, certain aspects of rearing a child and a surveillance department are a must. For the surveillance industry, some of those “musts” have included: the need to know the games you were watching, how to spot a cheat, what “rubber-necking” meant, making sure you don’t accidentally tape over your evidence, and getting tape-change done on time.

The musts in parenting have changed very little in the last twenty years, the musts for surveillance departments however will be like night and day. Technology and the dissemination of information will be the cause of this radical change. Computers with word processors, databases, and the Internet, have already had a profound effect on society and the way we live our lives and do business. It is a foregone conclusion, by the end of the decade, the replacement of VCRs with DVR’s, full-view 360° cameras, and video analytics, or smart video, will complete the metamorphosis.

Most surveillance directors are forty-something+, and they have never had formal training in the areas of, video compression science, networking, and information technology, as a whole. These forces are behind what will shape the next generation of surveillance departments. Corporate execs lack the specific knowledge to make informed decisions and rely on their surveillance people to provide the answers. The surveillance directors are deluged with information from a myriad of vendors and left to decipher the fact from the fiction.

As one who has been a surveillance director, I feel for those struggling to come up with the miracle cure. We have written this book with that in mind. It is well beyond my individual area of expertise to draft this alone, so I want to thank all those who contributed to this book, each in their core competence, which made this undertaking possible.

While this book won’t tell you who and where to buy from, it is a great source of information to assist you in the selection process and making informed decisions. It will educate you to ask all the necessary questions and be able to sift through the smoke and mirrors.
Introduction

by Donald Cogswell

I have grown up in an era where I remember my first Christmas’ under the tree were not bicycles or building blocks, but video games and a personal computer. My dad used to tell me the joke of “when I was your age and we were punished our parents made us come in the house, these days when y’all get punished we send you outside the house.”

As a kid I looked forward to the summers, so I could work on making my own video games and learning about the latest hacks. I had a mouse in my hand instead of a baseball, but I loved every minute of it. Sometimes my colleagues chastise me and say, “speak English damn it, stop speaking in acronyms!” I guess they hate when I speak “IT,” and I forget it’s not a spoken language to all.

I have been fortunate enough to start my career around some of the country’s finest programmers in the banking industry before moving over to data security, networking and communications. The visionaries I surrounded myself with cautioned me, that while we are moving into the age of the Jetsons, we can’t forget we are still living with the Flintstones. So we have to remember that whatever we design, Fred, Barney, Wilma and Betty are the ones going to be using it. My mentors would say, “technology is a wonderful tool, but not if the masses can’t use it.”

I watched product after product that were incredible in what their capabilities were, fall flat on their face because the users got frustrated and gave up. It was designed by software engineers for engineers. Too often, software and hardware developers cannot empathize with the masses. They assume everybody has a PhD in technology.

When I was introduced to the security industry in the 90’s, what I encountered was puzzling to me. I guess I watched too much TV and thought this was the place for cutting edge technology; to my surprise what I found was an industry in the dark ages. Why, because the industry icons were not schooled in Information Technology and the customers they were selling too knew less then they did. It was the blind leading the blind.

In talking to surveillance directors the frustration was evident. They were being called upon by management to be the guru of this coming age of digital technology and had about as much knowledge in that skill set as they do in nuclear physics. Whatever education they were able to find was usually skewed to one side to facilitate a manufacturer’s products, even though it may have been so far off the mark.

In writing this book, we have tried to take the mystery out of digital video. There is no black magic and the underlying technologies are well known and developed. There are endless research papers developed by the world’s leading companies on the subject. We have tried to translate the information into layman’s terms. I can only say do your homework and ask the right questions and don’t take anything for granted, the cost of a poor decision, well could result in your early retirement!
Chapter 1

A Brief History of the DVR

Whether you are new to digital video surveillance or experienced; this guide will provide you with valuable and comprehensive information on DVR technology and digital video surveillance systems. You will quickly learn that all DVR’s and surveillance solutions are not alike. Quality, performance and reliability vary widely. It’s not what the manufacturers and integrators do tell you, rather what they omit. The object of this guide is to make sure the products and solutions you specify and approve are suitable for gaming and meet the required specifications and overall objectives.

DVR technology for security began in the early-to-mid 90’s with mechanical-type devices. They typically were operated by remote controllers and buttons or dials on the DVR box itself. Easy to operate, their functions and keys were similar to a device users were already familiar with; the VCR. Unfortunately, due to technological limitations, early DVR’s were not reliable, had limited features, offered poor quality video recording and were not powerful enough or designed properly to provide solutions that could address managing 100’s or 1,000’s of channels of video.

Casinos and regulators required more capable and reliable systems, which resulted in the introduction of PC-based DVR’s and hardware only, encoders and decoders.

The PC-based DVR brought enhanced features and were programmable, but the early models were plagued by inherent reliability problems and still did not have the requisite robustness in order to manage anything of substantial size.

Along came hardware boxes which would “split” up all the resources required of the system to address the problems of how do we create an enterprise solution? It consisted of: “hardware encoders,” which would solely compress the video, “hardware decoders,” which would only be responsible for displaying and playing back video, storage servers to archive the video and PC’s and software to monitor and manage all the equipment.
Earlier versions of this componentized methodology were cumbersome, had too many potential points of failure, required massive amounts of space to deploy; in addition to substantial build outs and power and cooling modifications. After all that, the underlying technology still had extensive limitations.

Today, both PC based and non-PC based DVR’s and related solutions are much improved over their early predecessors. Considerable advances in digital video technology and equipment have opened as many doors to users as they present challenges and quality issues for manufacturers.
Chapter 2

Common DVR Myths

Many people have the misconception that a PC-Based DVR is merely a PC with video capture (encoder) cards, display (decoder) cards and some off-the-shelf software. This explains the presence of hundreds of DVR and security companies that have literally sprung up overnight.

While these companies may hold themselves out to be “manufacturers” and security specialists - beware - few can deliver what they promise. In later chapters, we will discuss some of the “sleight of hands” to throw the unknowing off the track- in the quest of anything to make a sale.

At a recent security industry trade show we attended there were hundreds of exhibitor booths with DVR's on display. In fact, it was difficult to find a booth without one. Many possessed attractive literature and some phenomenal marketing claims. However, many were unable to provide a live demonstration of their equipment and just limited it to a “canned” and “controlled” demonstration. Others, when trying to show the features listed in their sales brochures upon specific request, experienced problems.

A true DVR, meant for gaming surveillance, is a sophisticated system composed of specialized hardware, software and sub-assemblies with built-in checks and balances. It all must work in unison to create a robust and reliable solution. There is no margin for error. Down-time costs money.

Building a DVR surveillance system requires a dedicated team of software and hardware engineers, programmers and system designers, plus support personnel. They take years to develop and go through extensive testing.

The fact is the majority of the household names in security are ill equipped to manage the task. The obvious question is what seems to be the problem?

The obstacle for security companies is the mere fact that digital surveillance is an “IT” business. Information Technology is a world away from the culture that has been
developed by these security companies, over decades. It is no longer analog cameras, run across a coax cable, plugged into a matrix switch, quads, multiplexers and VCR’s. Rather, it’s IP, networking, fiber infrastructure, data management, encryption, security, firewalls, routers, bandwidth issues, etc.

It’s a completely different business and architecture that not in any way resembles the legacy analog technology. It requires different personnel, different skill sets, different cultures, etc. It’s the Flintstones trying to operate in the Jetsons age.

This may account for why 90% of the product peddled by the major security companies is nothing but private label solutions, to some extent, using third party technology. This explains the myriad of installation debacles prevalent over the last few years. When a problem arises, the reliance to resolve issues goes back to the true suppliers, which in many cases are half a world away in a foreign language.

This conundrum holds true on both sides of the fence. The surveillance director is ill equipped to understand the nuances and what expectations they should have. They are relying on the manufacturers to provide them with the appropriate information. Unfortunately, if the information is incorrect, how is the director supposed to know? Some gaming organizations formed committees which meet frequently meet and attentively try to sift through this quagmire.

Even regulators are confused as to what is and is not possible; what is and is not acceptable; what is coming down the road; and what technologies accomplish the goals required, so they may do their job properly. Regulators regulate, surveillance directors monitor and secure, casino management look at numbers. The point is they are not IT people. A case can also be made that IT people are not security people, so from that regard they are lacking.

The amusing thing is sales people, integrators and others from the old school are used to half day courses on learning a security product and often figure… ok, I will take a half day course in networking and PC’s and learn this stuff. It is much to their chagrin when they find out people attend school for years, just to learn the basics of IT.

When people approach us and ask can you teach me the basics in a morning session, my response is usually no problem and in the afternoon we can follow that up with a half day session on performing brain surgery.
Chapter 3

What is a Security DVR

Unlike a VCR, the DVR has many advanced features and can also be operated and viewed remotely via local network (or even an Internet connection, which most regulators prohibit.) A Digital Video Recorder differs from a VCR in several important ways, some more obvious than others.

Instead of recording video and audio data to a tape, the DVR records to a computer’s hard drive or removable media such as a CD or DVD.

Computer hard drives:

- Are more reliable (no tape jamming, degaussing or signal loss)
- Can store far more recorded material (weeks, months, years)
- Offer better video quality (tape wear causes signal loss)
- Are automated (no need to worry someone forgot to push the record button or change tapes)
- Protect data effectively
- Are automated (no need to worry someone forgot to push the record button or change tapes)

Cassette tapes:

- Are bulky
- Are vulnerable to loss of data
- Have to be replaced frequently to maintain good quality
- Can easily be tampered with and data manipulated

There really isn’t much more of a choice any more, as the primary manufacturers of VCR’s have ceased production as of the end of 2005. Even videocassettes are becoming harder to locate.

Video and audio stored on a DVR can be:

- Accessed quickly and efficiently
- Viewed or retrieved locally or remotely
- Viewed simultaneously by multiple users
- Tied to alarm systems
- Authenticated for court admissibility

www.aventuratechnologies.com/casinos
Chapter 4

PC-Based Vs. Non-PC-Based

There are two major categories of DVR solutions. One is PC-based and the other, non-PC based. In many cases, manufacturers will use multiple pieces of hardware to accomplish a single task. Both offer similar functions and both can be accessed locally, across a network or over the Internet, if cabled accordingly.

One of the most frequently asked questions about DVR's is: Which is better a PC-Based or Non PC-Based DVR solution?

There isn't much that a non-PC based DVR solution cannot do today, which a PC-Based DVR can. The difference has more to do with the "footprint." Non-PC-Based solutions in a gaming environment consist of 3 or more separate pieces of equipment; to accomplish the task (more potential assets to fail); as opposed to a single piece in the PC environment. Also PC interfaces tend to be more user-friendly and less "mechanical."

In a Non-PC environment for gaming, there are hardware “encoders” to record the video, hardware “decoders” to view and playback the video, and “RAID servers” to record and store the video, in addition to workstations and management servers. On the casino side of the equation, this means more real estate, which is precious in a casino environment.

The joke is always told, video surveillance in a casino is looked at by casino owners as the unwanted bastard child. It has to be there but it’s unwanted. It doesn’t generate revenues so therefore, they put up with it, but spend as little money as possible and the accommodations are usually cramped and minimal.

When using a Non-PC solution, it no longer becomes a swap out of DVR for VCR, but added space, power and air-conditioning requirements, extensive build outs and more devices to monitor and manage. This is usually accompanied by an increased overall hardware cost and resulting monthly utility increases. Additionally, there are the potential increased maintenance requirements.

PC-Based DVR’s tend to be more flexible and easier to manage. PC-Based solutions also tend to allow for upgrades of compression technology, which can be vital to the end user. Remember, in the IT world, you blink and they are onto the next technology.
Non-PC-based solutions tend to use “ASIC” (Application Specific Integrated Circuits) technology, which does not allow for upgrading of a technology platform, similar to your microwave oven. ASIC, is a chip that is custom designed for a specific application rather than a general-purpose, such as a microprocessor. ASIC, unlike an FPGA, has fixed functionality and is not reprogrammable.

In the PC environment, the latest technology utilizes DSP’s (digital signal processors). A DSP is a specialized digital microprocessor used to efficiently and rapidly perform calculations on digitized signals that were originally analog in form, such as audio and video. The big advantage of DSP lies in the programmability of the processor, allowing parameters to be easily changed.

In the Non-PC-Based architecture, another concern is the only item which is “fault tolerant” is the storage servers. Hardware encoders and decoders have no ability for fault tolerance.

The flip side is a PC-Based solution has a single point of concentration for failure. PC’s also run operating systems such as Windows or Linux and may be subject to operating system failures or reboots. Regardless, in either scenario you still have to record to storage servers, which virtually all jurisdictions require to be fault tolerant and redundant. Either way, you have to have a PC as part of your equation. The real question is why would you want to have the added equipment that a Non-PC system introduces?

So why do companies offer Non-PC solutions? Because this is the platform that either they developed or in most cases being that its third party product, this is what their supplier developed. Switching to another platform is not so easy.
Chapter 5

Fault Tolerance

DVR’s in the gaming environment are mission critical applications and there is no margin for error. Regulations in virtually all jurisdictions globally state, if recording and monitoring stops in gaming areas, play is to cease, immediately.

As a regulator or surveillance director, the only concern is gaming compliance. From the casino operator’s side, if the games stop, it means lost revenues. As such, both gaming control and the casino operator are concerned, there are no interruptions.

Therefore, to prevent such an occurrence, a video surveillance solution must be designed as “fault tolerant,” with a monitoring solution to automatically and audibly or visually notify, in the event of a failure. Fault tolerance has been described differently from jurisdiction to jurisdiction.

As a layman’s definition, fault tolerant means: if there is a failure of a system or component, which could potentially cause the interruption of recording or monitoring, there shall be a redundant component, system or method to function in its place automatically, quickly and seamlessly.

Some jurisdictions look at fault tolerance at the first point of concentration, which has its own definition and others look at it, at the point of viewing and recording.

When it comes to fault tolerance the big question becomes: fault tolerant at what level and to what extent? As we mentioned, in the Non-PC-Based environment, there are several different stages to the solution; encoder, decoder, storage, monitoring and workstation.

More modern PC-based solutions use but one piece of equipment to perform encoding, decoding and storage, while older more outdated PC solutions use PC’s to replicate the architecture of the non-PC solutions by having separate devices for encoding, separate devices for decoding and yet others for storage.

Before we go on further discussing fault tolerance it would be good to understand different system configurations in order to make an educated decision on what level of fault tolerance to require.

Prior to the inception of digital video, casinos had employed some basic architecture for viewing and recording video. The majority of “existing” casinos utilizes one of the three following scenarios as discussed below and identified in the accompanying diagrams:
1. A camera’s video outputs are plugged into a matrix switcher’s video inputs; and from the matrix switcher’s video outputs into the video input of the VCR. For non-gaming cameras, between the matrix switcher and the VCR might be a quad or multiplexer to save on the number of VCR’s required.

2. A camera’s video outputs are plugged into a distribution amplifier’s video inputs. From the distribution amplifier’s video outputs one output is to the matrix switcher’s video inputs, while another is to the VCR’s video inputs.
3. A camera’s video outputs are plugged into a matrix switcher’s video inputs; and from the matrix switcher’s video outputs into the distribution amplifier’s video input. From the distribution amplifier’s video outputs to the VCR’s. For non-gaming cameras, between the distribution amplifier and the VCR might be a quad or multiplexer to save on the number of VCR’s required.

In each case there is a different “first point of concentration.” The first point of concentration refers to the first point after the camera, where the video may fail for purposes of viewing. When using a matrix switcher, the matrix switcher is the first point of concentration; when using a distribution amplifier; the distribution amplifier is the first point of concentration. Some regulators consider the first point of concentration, the initial point after the matrix switcher.

In general, matrix switchers and distribution amplifiers over the past couple of decades have proven incredibly reliable. Unfortunately, neither the matrix switchers, nor distribution amplifiers have any fault tolerance.

The difference is, if the matrix switcher ever failed the entire video surveillance system is down and effectively closes gaming at the casino. In the case of a distribution amplifier, a failure would only result in the loss of the cameras plugged into the individual distribution amplifier, which typically max’s out at 16 channels. The distribution amplifier can be quickly replaced or the video re-routed, while the matrix switcher outage can become a more complex issue.

Therefore, the implementation of a distribution amplifier, whether or not using a digital or analog system is a more practical alternative in terms of a redundancy at the first point of concentration depending upon again how the regulators perceive it. The cost of a distribution amplifier is typically in the $35 - $50 per channel range; a small price to pay considering the potential downside to a casino. Consider it an insurance policy.
Let’s first address the Non-PC-Based solutions, which consist of encoders, decoders and storage servers. Since the encoders and decoders are typically ASIC “hardware boxes” and not PC’s, there is no methodology for these components to be fault tolerant; they are no different then the distribution amplifier or matrix switcher in that regard. They are different in that the distribution amplifier and matrix switcher have a proven history over decades, while the encoders and decoders are yet to be proven in a gaming environment, due to their youth.

Many manufacturers have lobbied around gaming control boards to find a compromise to the issue of fault tolerance, with respect to the non-PC-based methodology. The compromise, right or wrong, seems to be: the encoder or decoder should not have more than a specified number of channels attached to it. So in the event of a failure, the loss is minimized to a specified number of channels.

In the Non-PC-Based solution the video still needs to be recorded to a PC Server for a specified period of time, with specific characteristics, which vary from jurisdiction to jurisdiction. Storage servers in the majority of jurisdictions though, are required to be “fault tolerant.”

In the PC environment, fault tolerant has a variety of meanings. Video is stored on hard drives on the storage servers. A fault tolerant system for gaming requires the video stored on the hard drives on the servers, have a redundant solution.

In case of a hard drive failure, there shall be a duplicate copy of the video stored on another hard drive somewhere else on the server or elsewhere. This is known as a “RAID.” A RAID is a Redundant Array of Independent Disks. RAID technology has been around for decades and is well proven.

RAID is a subsystem storage concept designed for the purpose of offering higher levels of protection from data loss that can occur from any down time caused by malfunctions compared to the protection offered by conventional disk drives. RAID arrays composed of conventional discs can function for decades or even a century without losing data because of a disk failure. In addition, RAID can also improve input/output performance, make servicing easier and faster and allow users to fine-tune the drive system to match the needs of specific applications.

First conceived in 1987 by a group of Berkeley researchers, five levels of RAID were defined and three of which (Levels 1, 3 and 5) have been found to be commercially viable.

Each level offers a different way of distributing data across an array of disks so that the failure of a single disc does not cause data loss. There is also a variant of RAID known as level 0 (see Striping). RAID 5 is a striping as well. The difference is in RAID 0 there is no fault tolerance. This is used just to increase the performance, since it doesn’t have the overhead associated with the parity information.
RAID Level 1 uses the techniques of mirroring to achieve data redundancy. Mirroring takes the data on one disk and duplicates it onto another and offers excellent reliability and slightly improves I/O throughput. However, this technique is relatively inefficient in its use of total disk capacity.

RAID Level 3 and Level 5 combine the striping technique with parity codes, enabling the recovery of data if a disk fails. Both of these levels utilize total disk capacity more efficiently than RAID Level 1.

Besides redundancy, RAID contributes to automatic load balancing by avoiding hot disks where 80 percent of the I/O requests target 20 percent of the total disk capacity. By choosing the suitable RAID level, data transfers can be sped up or handle more I/O requests per second. RAID Level 5 arrays can handle large numbers of I/O requests simultaneously, so they are a good match for applications that make many small requests such as video surveillance applications. RAID Level 3 drives transfer data from all disks in parallel, which shortens the transfer times for applications that are read in large, sequential files.

In a PC or server you might have at the office, you might have multiple hard drives. Unless, the system is configured as a RAID, there is no fault tolerance, as the drives become “logical.” It doesn’t matter if there are 2, 3 or 4 hard drives; the PC sees the hard drives as one logical drive, unless it is configured as a RAID. So if any of the drives fail the entire data is lost on all drives, unless it is set as a RAID. A RAID has additional components not found in a standard PC, in order to control the RAID. Most jurisdictions require a RAID5 configuration for compliance.

The most common RAID level in terms of mission critical applications is RAID level 5. In layman’s terms, RAID5, as it is known, has fault tolerance built-in, where the failure of any single hard drive, would not result in the loss of the data as the information is being written to other drives in the “array” in case of such a failure.
A minimum of 3 hard drives is required for a RAID5 configuration. Most common, is a configuration whereby, an array of 5 hard drives are utilized. You “net” 4 usable hard drives of recorded video, as theoretically the 5th is lost for purposes of fault tolerance, known as “parity.” Technically speaking, a certain percentage of each of the drives has information of other drives, so it’s really a percentage, but the net effect is you lose 1 drive capacity out of 5.

While we have addressed the concern of what happens if a hard drive fails, another concern is how does it get replaced without any interruption? There are two types of hard drive bays; internal and external hot swappable.

If the hard drive is “fixed” internally, with no external access, then to replace the hard drive would require shutting the server down and opening up the server. The data has not been lost but it does cease to record, while being repaired. This obviously becomes a regulatory issue. The “hot swappable,” “removable” drive is accessible, while the system is live. Servers with hot swappable drive bays, allow for easy removal of the hard drives on-the-fly, so there is no interruption of recording.

There is still the issue of after the hard drive fails it must be replaced in time before another drive fails within the same array. After all, the drive array relied upon the 5 drives total to have fault tolerance and redundancy. In many cases, you don’t want surveillance operators who are not “IT” savvy, touching the storage servers for obvious reasons. But if the drive fails on a weekend or the middle of the night, who knows how long before someone comes in to address the problem. This is also why you need a monitoring system to automatically and preferably audibly notify you of a drive failure.
To manage this situation, a drive on the server, exclusive of the RAID array, is dedicated to rebuilding the data automatically, in the event of a drive failure. This drive is known as a “global spare.” The global spare drive, automatically steps into the place of the failed drive in the affected disk array. As such when performing storage calculations, not only do we have to consider the RAID but the global spare. Therefore, in a 16-drive array (which is the most common) 1 of each 5 drives is lost to the RAID, and 1 additional to the global spare.

The logical question is what happens if 2 hard drives in the array fail at the same time. For such situations, a RAID level 6 is implemented, which can sustain multiple simultaneous drive failures. RAID6 is an extension of RAID5 with the added security, but makes it much costlier. The likelihood of a simultaneous drive failure under normal operating conditions is quite remote.

What we need to understand is, the redundancy we have described relates solely to the hard drives.

A server has numerous components and logically any one of those components can also fail. The server consists of at minimum a power supply, motherboard, memory, video card, processor and RAID controller.

Power supplies in a server can be made redundant and fault tolerant. Some servers are dual redundant, while others are even triple redundant. Power supplies are also available in hot swappable configurations. Servers can continue to operate with a failed power supply, (as long as there is a redundant source). If the power supply is not hot swappable, at some point the server will need to be shut off to repair.

Power supplies are typically reliable and not prone to failure. As such, where a hot swappable hard drive is critical, since it needs to be addressed quickly for purposes of data storage, a failed power supply can be replaced at the casino’s convenience.
One of the misconceptions is if a server has a dual processor, or 2 or more sticks of memory, then it is fault tolerant. Sometimes there is confusion between “redundant” and fault tolerant. Redundant means there is a secondary system; it does not necessarily automatically become fault tolerant.

With respect to dual processors and multiple sticks of memory those have more to do with system “performance” not fault tolerance. Even then, a dual processor “may” but not always increase the system performance. Multiple sticks of memory also, “may” distribute the load and enhance system performance. In either case, the failure of system memory or processor would be considered a catastrophic failure. Catastrophic in the sense, that there is no method for the server to fix itself. Similarly, the failure of the motherboard or controller would result in a similar situation. The likelihood of a motherboard, memory or processor failure is minimal.

As a general, but not absolute rule of thumb, component failure will result within the first few weeks or will not happen for an extended period of time. There are a number of reasons for a failure but most make their presence known almost immediately. Once it is functioning, non-moving parts are not likely to fail anytime soon. It would not be any different then the likelihood of the distribution amplifier or matrix switcher failing.

If there are failures it is usually the result of some other external problems, such as unclean power, dusty or hot environments.

Hard drives at some point in time will fail. The reason you have eventual hard drive failures is because there are moving parts. A hard drive when it is storing data writes the information to a “platter.” Similar to a CD or DVD it is writing to the disk spinning at thousands of RPM’s. The disk has a specified MTBF. MTBF refers to the mean time between failures. It is the reliability rating indicating the expected failure rate of a product in power on hours. By knowing the anticipated MTBF, a scheduled
A Surveillance Director’s Guide To Digital Video

maintenance program can cycle out the old drives with new ones before a failure occurs, without system interruption. What exacerbates the situation is hard drives were never originally designed to be writing 24 hours a day, 7 days a week.

Think about the way you normally use your PC either on the personal or corporate level. It is highly unlikely that the drive is writing all the time. It is only when data is stored, backed up, etc.

Whether performing accounting functions or business functions, the drives on storage servers are typically idle the majority of the time rather than spinning. Since in the casino environment we are recording 24/7 the drives never stop spinning. Think of running your car 24/7 without stopping, at some point the moving parts will fail after a certain amount of mileage. What that mileage barrier is, can only be a best guess.

As a result of new demanding applications, some hard drive manufacturers have moved toward offering more industrial drives with longer life cycles. They have not discontinued the earlier drives; rather offer industrial ones at increased costs, with warranties of up to 5 years. The MTBF of today’s industrial drives can be anywhere from 300,000 to over 1,000,000 hours. Considering there are only 8,760 hours in a year that is a fair amount of reliability and a long time till potential failure (34 – 115 years).

Similarly other components in servers have MTBF ratings in the hundreds of thousands, which ostensibly means the system will become obsolete long before its failure potentially decades to a century from now.

What it all comes down to is a solution has to be fault tolerant not just a component. The diagram on the following page is indicative of a layout that takes into consideration all aspects of redundancies and fault tolerance.
Any video surveillance solution will need a monitoring and management system that oversees and can address all hardware and software. For purposes of redundancy and fault tolerance there should be 2 servers that monitor and manage all hardware and software, each looking at each other in case of a failure.

The DVR’s themselves should have a RAID5 configuration, which provides a level of fault tolerance and redundancy. In the event of a catastrophic failure, a RAID system regardless of the level will stop functioning. Accordingly, a backup solution is required. One of the methodologies is to have the monitoring and management system communicate with the matrix switcher, which should be outfitted with spare video outputs. Upon recognizing the failure, the monitoring and management system can reprogram the spare outputs of the matrix switcher to a “hot spare” DVR seamlessly.

If your system does not have the capability for matrix communication with third party software, (as some are proprietary) then an operator should be able to manually accomplish the same task.

In the event of a failure of a distribution amplifier, a spare already tied into the rack should be available for a quick manual cutover.

In the event of a failure of the matrix switcher, a temporary cutover can be done using the distribution amplifiers fed into the output monitors.

Herein lies the problem with having separate encoders and decoders, as opposed to one piece of equipment since there is little to no ability to create a fault tolerant scenario for the encoders and decoders on an automated basis. The most practical would be to have hot spares in a rack and perform a manual cutover once notified of a problem by the central management system.
Chapter 6

All DVR’s and Solutions are not Alike

DVR's are not all alike. In fact, many are as dislike as automobiles. In the world of DVR's you can find the equivalent of a $10,000 Kia and a $100,000 Mercedes Benz plus everything in between. Both may be capable of getting you from point “A” to point “B” but that's where the similarities often end.

Using the vehicle analogy, if you buy a light weight truck it may be a fine vehicle for hauling small loads. But, if you load it up with 10,000 pounds of cargo and drive up and down hills all day you shouldn't expect a very long useful life out of the transmission or engine. It's not that it's a poor product, rather that's not what it was designed to do. Not unlike exotic and sophisticated foreign cars, many DVR's can be just as complex and temperamental.

Every ounce of computing power is critical. Digital video recording is a process intensive, multi-tasking application which can tax even the most robust systems. Along with processing power, a good DVR depends on equally robust related parts and assemblies. The famous saying in information technology is “you are only as fast and efficient as your slowest and weakest component.” If your system is not beefed up from end-to-end, from hardware to software, it will be underpowered, will under perform and it's going to break. Even worse, it simply will not deliver any reasonable quality or cause instability from the outset and probably never meet gaming requirements. I would not want to be the one that approved the purchase of a system that was just installed to only find out gaming has rejected it.

Unfortunately, there's no official consumer's guide to DVR's. It's difficult at best for most buyers to evaluate products on a fair comparison, or to even know; what are reasonable expectations.

Hobby and consumer class products often parade as commercial and business grade. Don't be fooled. You can buy a blender for your home for $25.00 but it is not the same as the $500.00 model at your local bar which may be responsible for making hundreds of perfect daiquiris and Margaritas every night, day-after-day.
Remember, surveillance you are either monitoring or recording 24/7 so that $25 blender equivalent won't do the job for very long, if at all.

Components become even more of an issue as you get into the large casino systems. Caveat emptor – let the buyer beware – all DVR's are not alike.

For buyers who do not have a lot of experience with DVR's, separating the quality from junk can be a daunting task. Often salesmen and brochures will conveniently fail to mention the things that their system won't do. Often the buyer doesn't realize it until:

- The quality of the recorded video is poor under normal operating conditions.
- There is no ability to playback video in slow motion without distortion and choppiness.
- When you move the PTZ, the recorded video is blurry or blocky.
- You never looked at the video remotely over the network before you bought it and now you realize the remote video quality is sub-par at best.
- The recording and display speeds are not as promised.
- The number of days of storage is far less than specified.
- When you blow-up the video to full screen, the image is fuzzy.
- When you playback recorded video and freeze frames you see 2 balls on the roulette wheel, or 4 dice on the craps table.
- You can't make out the pits on the cards.
- The DVR overheats itself as well as the room.
- The noise created by the system is deafening.
- The DVR's are unstable and continue to reboot or shut down unexpectedly.
- You just decided to expand and purchased additional systems from the same company and they don't work with the old ones because the software or hardware is not compatible since they have no longer use the same supplier or technology platform.
- You can't practically control the DVR remotely from a workstation, as the way you thought it would operate.
- There is no way to burn disks of multiple cameras from different DVR's on a single disk.
- There is no way to synchronize playback video from multiple DVR's on a workstation.
- The networked video at the workstation is not real-time because its bandwidth intensive.
- Certain functions only work under limited or ideal conditions and render other features inoperable.
- There is no one – (at least locally) - to support the product that is technical.
Chapter 7

DVR Card Differences

At the heart of any DVR solution is the video capture card, also known as a DVR board or encoder. This component, more than any other, will determine the effectiveness and quality of the DVR system. The encoder is the “engine” which powers the vehicle. This video capture card contains, a hardware or software based Codec, which performs the vital operation of capturing, compressing and decompressing packets of video data. Codec, which stands for “compression-decompression,” will be discussed in greater detail later in this guide.

There are consumer quality, economy cards and components and industrial/commercial grade ones too. There are some with the current technology and others with decade old technology.

Most video capture board and encoder “manufacturers” do just that, manufacture the “board” - that green thing with a bunch of neat looking colorful soldered components.

In reality, these companies are just assembly plants. This is common throughout much of the consumer electronics industry where nearly all companies create products assembled from other companies' components, including all the household names you are familiar with.

So what is it then that makes the difference between, a top notch product and an average to sub-standard one?

We mentioned earlier that the video must be compressed and decompressed. This function requires “processing.” Processing is performed by a processor. The processors for decoders are similar in nature to a PC and come in various speeds and abilities. Just as in an Intel processor for a PC you have a Celeron and a P4, etc. Then within those architecture categories are different levels of processing power, such as 1.4MHz to 3+MHz; different bus rates; etc., so goes processors for encoders and decoders. For the gaming environment, the most powerful processors are required to meet acceptable regulatory standards.

In many cases there are multiple processors on a single encoder card in order to maximize performance. Some will have one processor for each channel of video; the more efficient ones are capable of encoding multiple channels of video on a single processor. Once you have the power of the encoding processors, you then require a powerful and efficient compression algorithm to perform the function.
Chapter 8

Bottlenecking

Perhaps the most pressing challenge relating to DVR card performance is bottlenecking.

What is bottlenecking?

Say you have 100 garden hoses connected to each other, 99 of which can pump water at 3 gallons per minute, and one hose somewhere along the line, which can only pump water at 1 gallon per minute. In spite of all your 3 gallon-per-minute hoses, the entire system of hoses will only allow 1 gallon of water per minute to pass through.

The same is true in processing video data. “You’re only as fast as your slowest component.” Put a bunch of good high-performance components on a DVR encoder board and one component is not matched or as fast as the others, and you have a slow, underperforming system.

This brings us to a critical understanding with respect to performance. Many times manufacturers will provide a demonstration and show a limited number of channels of video performing at a certain level. Since the bottleneck will cause the solution to hit a wall at some point they limit the demonstration to stop before that critical point, where system degradation can be observed. So one needs to be careful to see what happens when you use the full capacity of the system.

Bottlenecking is but a single of multiple aspects of where the system may max out before its “alleged” capacity.
Chapter 9

Shared Resources

Shared resources refer to the condition that occurs when one component is asked to perform multiple tasks simultaneously. Each task a particular component performs drains a portion of that part's total resource and this is why we mentioned that quite often multiple processors or other components are used so that resources are not drained when trying to operate the DVR system at its maximum capacity. In some instances, regardless of how many components are used, the underlying technology is just not powerful enough to drive that many components on a single board or the technologies are not compatible and do not function properly. As an analogy, you can buy the latest Intel processor but only the newer motherboards are capable of handling its architecture. If you try to run the processor it may not function or only function at the maximum capacity of the older architecture. All the pieces have to be compatible.

Beware; manufacturers will quote a specification for their equipment at its “maximum” performance level, under ideal conditions.

The quoted specification usually assumes the components are doing nothing else at the same time, but rather a single, simple function and not sharing resources. Manufacturers will merely show you functions or features as a single task and not demonstrate the same across multiple channels, knowing that the quality or stability is not otherwise possible. Welcome to sleight of hand 101.

DVR’s, encoders, decoders and servers are more often than not called upon to multitask. The problem is that not all hardware architectures and components are up to the task. The logical question would be why doesn’t everyone just use the best and most powerful components? The answer comes back to what we stated above; the underlying architecture might be quite outdated and not compatible with the latest components. Some components don’t work well with others even though each might be the best in their respective category.

What you may ask is the result of shared resources on the DVR? The answer is the same whether it’s shared resources or bottlenecking, the most common problems are “dropped frames,” choppy, robotic and poor quality recorded images. Which in some cases leads to significant instability and eventual failure as the system is running at 100% of capacity and still not keeping up.
Chapter 10

Frames / Images Per Second

Let's give you a quick lesson in translation and calculation of video “speed” or “frame rates.”

Some manufacturers use different expressions when identifying the speed capabilities of their product. It will become increasingly apparent why this is misleading.

- Thirty (30) “frames-per-second” (abbreviated as “fps”) is “real-time,” “real-motion” video in the NTSC (North America) video standard.

- Twenty-five (25) “frames-per-second” (abbreviated as “fps”) is “real-time,” “real-motion” video in the PAL (International) standard.

This is not to be confused with “fields-per-second” (also abbreviated as “fps”). Unfortunately, two (2) fields equal one (1) frame. So when a manufacturer states “30 fps” on their literature are they talking fields or frames? Are they talking about each channel of video or total capacity of the system? Are they talking about the system limitation or the operating capability?

Another acronym used by manufacturers is “ips” (images-per-second). Similar to fields-per-second, there are two (2) images-per-second to each frame-per-second; so two (2) images or two (2) fields equal one (1) frame. Therefore, in order to obtain a real-time, real-motion image you require sixty (60) fields or images per second, per camera.

When comparing a DVR’s fields (FPS), images (IPS) or frames-per-second (FPS); display, recording or playback performance claims; be careful to take into consideration all the factors that will apply to your particular application. Once again, manufacturers’ claims may be based on “optimal” conditions and have little to do with reality and what you are trying to achieve. So always check to see if the total number of FPS/IPS quoted is for the entire DVR capture card or is it on a per channel basis. Is it for display and record? You simply have to test it anyway, as claims are just that; claims. Besides if you don’t the regulators will.

- 32 -

www.aventuratechnologies.com/casinos
It’s kind of like the MPG sticker on a new car. Do you know anyone that ever got that kind of mileage? Not unless they were going downhill, in neutral, with a strong tail-wind!

Remember also what you are viewing live has nothing to do with the recorded quality, they are separate and distinct. So watching a live picture has little value, although if the live video is poor you are already in trouble.
Chapter 11

Image Resolution

Image resolution describes the detail an image holds. The term applies equally to digital images, film images, and other types of images. Higher resolution means more image detail.

Image resolution can be measured in various ways. Resolution quantifies how close lines can be to each other and still be visibly resolved. Resolution units can be tied to physical sizes (e.g. lines per mm, lines per inch) or to the overall size of a picture (lines per picture height, also known simply as lines, or TV lines).

A television or raster image display with 525 scan lines makes a picture with somewhat less than 525 TV lines of resolution.

The term resolution is often used as a pixel count in digital imaging. But when the pixel counts are referred to as resolution, the convention is to describe the pixel resolution with the set of two positive integer numbers, where the first number is the number of pixel columns (width) and the second is the number of pixel rows (height), for example as 640 by 480.

Another popular convention is to cite resolution as the total number of pixels in the image, typically given as number of megapixels, which can be calculated by multiplying pixel columns by pixel rows and dividing by one million. Other conventions include describing pixels per length unit or pixels per area unit, such as pixels per inch or per square inch.

NONE OF THESE PIXEL RESOLUTIONS SUCH AS 704 x 480 OR 640 x 480 ARE RESOLUTIONS THAT DEFINE QUALITY, EVEN THOUGH THEY ARE WIDELY REFERRED TO AS SUCH; THEY MERELY SERVE AS UPPER BOUNDS ON IMAGE RESOLUTION.

A pixel (short for picture element, using the common abbreviation "pix" for "picture") is one of the many tiny dots that make up the representation of a picture in a computer's memory. Each such information element is not really a dot, nor a square, but an abstract sample. Pixels in an image can be reproduced at any size without the appearance of visible dots or squares; but in many contexts, they are reproduced as dots or squares and can be visibly distinct when not fine enough.

A pixel is not a little square. A pixel is generally thought of as the smallest complete sample of an image. The definition is highly context sensitive; for example, we can speak of printed pixels in a page, or pixels carried by electronic signals, or represented by digital values, or pixels on a display device, or pixels in a digital camera (photosensor elements). This list is not exhaustive, and depending on context there are several synonyms that are accurate in particular contexts. We can also speak of pixels in the abstract, or as a unit of measure, in

www.aventuratechnologies.com/casinos
particular when using pixels as a measure of resolution, e.g. 2400 pixels per inch, 640 pixels per line, or spaced 10 pixels apart.

The more pixels used to represent an image, the closer the result can resemble the original. The number of pixels in an image is sometimes called the resolution, though resolution has a more specific definition.

Confused and wondering why go through all this explanation. Well be prepared it only gets more confusing.
Chapter 12

Bitrate

Many regulators specify a standard for video quality, which in fact specifies no quality at all. Huh??? Ever heard the terms CIF, 2CIF, 4CIF or D1?

CIF *(Common Intermediate Format)* is used to standardize the horizontal and vertical resolutions in pixels of YCbCr sequences in video signals. A CIF is commonly defined as one-quarter of the 'full' resolution of the video system it is intended for (listed below as 4CIF). Note that this full resolution does not match what is currently referred to as D1 video (based upon Sony’s D1 format).

<table>
<thead>
<tr>
<th>Video resolutions (in pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
</tr>
<tr>
<td>CIF</td>
</tr>
<tr>
<td>4CIF</td>
</tr>
<tr>
<td>D1</td>
</tr>
</tbody>
</table>

NTSC is the video system or standard used in North America and most of South America. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines.

PAL is the predominant video system or standard mostly used overseas. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines.

So what? Well, many regulators write the standard for gaming cameras as 4CIF (704 x 480) at 30 frames per second and non-gaming cameras are either at the same “resolution” 4CIF with a lower frame rate or a lower resolution such as CIF (352 x 240).

The problem with this standard is that these “resolutions” speak nothing of the quality of the video. 4CIF simply means that in the NTSC format there are 704 pixels that will be filled with some amount of data across each of 480 lines. CIF means, there are 352 pixels which will be filled with some amount of data across each of 240 lines. How much data has yet to be determined, which is the bitrate.

- 36 -

www.aventuratechnologies.com/casinos
While a 4CIF image “can” produce a better quality image than a CIF image because the more pixels used to represent an image, the closer the result can resemble the original; it does not necessarily have to be the case. 4CIF does not mention the amount or quality of the data to be displayed in the pixels. These are “empty” pixels. Pixels need to be filled with data. Data is referred to in terms of “bits.” Accordingly, a CIF image filled with more bits then a 4CIF image can produce better visual and audible results.

In telecommunications and computing, bitrate (sometimes written bit rate, or as a variable R_bit) is the number of bits that are conveyed or processed per unit of time. In digital multimedia, bitrate is the number of bits used per unit of time to represent a continuous medium such as audio or video. It is quantified using the bit per second (bit/s) unit or some derivative such as Mbit/s.

While often referred to as "speed", bitrate does not measure distance/time but quantity/time, and thus should be distinguished from the "propagation speed" (which depends on the transmission medium and has the usual physical meaning).

In digital video, bitrate represents the amount of information, or detail, which is stored per unit of time of a recording. The bitrate depends on several factors:

- the original material may be sampled at different frequencies
- the samples may use different numbers of bits
- the data may be encoded by different schemes
- the information may be digitally compressed by different algorithms or to different degrees
Generally, choices are made about the above factors in order to achieve the desired trade-off between minimizing the bitrate and maximizing the quality of the material when it is recorded or played.

In digital video to reduce the bitrate a “lossy” compression is utilized. A lossy compression is a compression method that discards some of the information or data to make a video or audio program occupy less storage space or less transmission bandwidth.

If lossy data compression is used on audio or visual data, differences from the original signal will be introduced since data has been discarded. If the compression is substantial, or lossy data is decompressed and recompressed, this may become noticeable in the form of compression artifacts, which appear in the form of blocky mosaic images. Whether, these affect the perceived quality, and, if so how much; depend on the compression scheme, encoder power, and the characteristics of the input data, the viewer’s perceptions, and the viewer's familiarity with artifacts.

Ostensibly what we are saying is quoting a specification as 4CIF doesn’t mean a thing. Further, even quoting a specified bitrate at a particular resolution, also means nothing, because of the amount of variables as described above.

Many times the encoding power or compression scheme is insufficient regardless of the bitrate to generate “usable” video, because of it being applied with outdated technology.

So what is a regulator or surveillance director to do? We will discuss some overall general rules of thumb and concepts; but, they are by no means the Holy Grail.

In order to view good quality 4CIF recorded video the following bitrate estimates may apply using the specified codecs:

- H.264AVC: 1 – 2 Mbps
- MPEG4 (Part 2): 2 – 4 Mbps
- MPEG2: 3 – 6 Mbps
Just because you use the above bitrates does not necessarily mean you will have acceptable quality video. These are general numbers for the particular codec and do not account for all the other potential issues we have discussed in this guide.

The higher the bitrate the more storage it requires and the slower the download and transmission time. This comes back to the truck that needs to pull 10,000 pounds. The bigger file sizes created by the high bitrates require a lot more resources to move them along.

What does this mean in terms of how much hard drive space is required? Again, it’s an estimate based upon our evaluation and testing of various systems in the marketplace and speaking with surveillance directors who have also tested the same equipment. There could be significant variations depending upon multiple factors, but this is a good rule of thumb.

H.264AVC: \( \frac{1}{2} \text{ – 1 GB per hour} \)

MPEG4 (Part 2): \( 1 \text{ – 2 GB per hour} \)

MPEG2: \( 1.5 \text{ – 3 GB per hour} \)

This is assuming the bitrates mentioned above, with “acceptable” video quality at 25/30 frames per second (PAL/NTSC).

There are several other things that would skew in the favor of the newer codecs and make them even more attractive. H.264AVC uses what is known as a Variable bit-rate (VBR). VBR allows a codec to change its bit-rate dynamically to adapt to the “difficulty” of the audio and video being encoded. In the example of a swinging PTZ or other rapid movement, a higher bit-rate to achieve good quality is required, while less active scenes can be coded adequately with fewer bits. For this reason, VBR can achieve lower bit-rate for the same quality, or a better quality for a certain bit-rate. Hard drive capacity can be substantially increased. The older codecs use a Constant bit-rate (CBR). Therefore, there are no efficiencies regardless of the scene activity; the bitrate is constant to whatever it has been set to in the firmware.

In the end, it is going to come down to, either some scientific or mathematical standard expressed in terms of signal-to-noise ratio or more likely a visual observation of the video under some specified conditions and scenarios, taking into account real world casino environments. As we said before recorded video may look ok until you start moving PTZ’s or try to slow down the video.

As we cover all these topics it becomes more evident why the move to digital surveillance has been slow. Fact is, it’s not so easy to comprehend, plus the underlying technology required to provide video to a high standard was just not there until the last couple of years. It was a combination of the lack of powerful enough components and efficient compression technology.
Chapter 13

Storage

So why do we need to understand bitrate and compression?

Ultimately, in order to accurately determine how much hard drive space you will need with your DVR you need to take into consideration the codec technology being implemented, image resolution size, the bit-rate/compression ratio, the amount of video activity, is the bitrate variable or constant, and if motion detection (setting the DVR to only record activity when the camera detects motion in its field of view) is being utilized. Next, calculate the number of cameras and how many frames per second you want to record on each.

Advanced DVR systems, will allow you to independently control each channel for:

- Image resolution
- Bit rate (constant/variable)
- Display frame rate
- Record frame rate
- Motion detection

Part of the problem will occur when the amount of hard drive storage required is so expansive that it cannot fit inside the current physical machine and space. At that point, construction costs could become significant.

Even if you do have enough space for all the additional equipment, more equipment means increased heat and power. Increased heat means additions to the air conditioning system and most likely to the HVAC.

When evaluating storage requirements remember to evaluate the quality of the video based upon the most intense circumstances. Bitrates can be reduced significantly, if there is minimal motion, but when it comes time to moving the PTZ’s, the image can be distorted.

If you have already installed the system and now find yourself in the position that you need to increase storage and you don’t have the physical space or power, you are **** out of luck

Oh yea, we may have forgot to mention the amount of noise the equipment creates. That much equipment in one area can become a significant annoyance and most gaming control boards require the equipment must be in the control room.

- 40 -

www.aventuratechnologies.com/casinos
Chapter 14

Video Quality Vis-à-vis Frames-Per-Second

The number of frames per second has nothing to do with the image quality. While 30 frames per second is real time in NTSC, it is made up of 30 individual snapshots of sort. So while a video recorded at 5 frames-per-second has $\frac{1}{6}$th the number of images, it does not have $\frac{1}{6}$th the quality; it merely has fewer snapshots (that is of course if everything else is equal – such as bitrate, resolution, etc.) Remember, it is nothing but a succession of still images.

So why is there a need to record in real time? After all human beings don’t move that quickly, or do they? We are not recording speeding cars. One answer is from a prosecutorial standpoint, what happened in between, if you are not looking at the whole picture. If you are recording in real-time, there is no room for hypotheccations by the defense lawyers. Further, a more detailed picture can make it easier to identify sleight-of-hand movements. You are also going to find that older technologies have trouble with slow motion and smooth playback under those conditions, so higher frame rates tend to compensate for some of the shortfalls, but not all.

A still shot from a recording at 30 FPS will look the same as one at 5 FPS
Chapter 15

Size Matters

A file is a collection of data. File size refers to how much data is contained in this single unit of measure. The larger the file size, the more bandwidth (the amount of data that can be transmitted in a fixed amount of time) and computer resources are required, to display, record and transfer a file.

Conversely, a smaller file, of the same amount of data, will use fewer computing resources, display and record more effectively and will transfer across networks more efficiently.

The size of a file of video data can be affected by image size (resolution), bitrate, motion, compression and various other factors, as previously discussed. Ultimately this can affect the amount of video you will be able to store on the DVR's hard drive and overall performance when viewing and recording multiple cameras simultaneously. As cautioned previously, beware of performance claims; they are usually referring to results achieved under the most optimal conditions.

As a rule, the higher the compression ratio, the smaller the file size. The smaller the file, the less sharp the image, the quicker the transmission speed, the less storage space and processing power required. Conversely, a lower compression ratio results in a larger file size, sharper image with a slower transmission speed and more storage space and processing power required.

A good way to understand compression is to think of the printer attached to your computer. If you print with a higher resolution the quality is better but it takes longer to print because:

- there is more processing power required
- more memory to buffer
- more dots per inch to process
- more ink (data) to lay down

Using a lower resolution which generates lower quality is faster because:

- there are fewer dots to process
- less memory to buffer
- less ink to lay down
This reverts back to a previous issue of speed claims. When they say your printer prints 20 pages per minute, it's usually not based on the highest resolution or with full pages of ink coverage, but the maximum possible on low resolution with the manufacturer's definition of “normal” print coverage. Again, like the MPG ratings!

The fact is, older compression technologies produce larger file sizes, since they are not as efficient as the newer technologies. Accordingly, they require more processing power, which begs the question; can it generate enough power to provide a working solution with such large file sizes? The answer in most cases is a resounding, no. This is why many manufacturers will use multiple pieces of hardware with fewer channels of video to try to compensate for the shortfalls.

Newer compression technologies can compress video more efficiently and therefore result in less power required across the board. This is why in many cases older technologies are more expensive then the latest; because the storage requirements can be as much as 3x greater, as well as the amount of equipment.

Large file sizes bring several interesting challenges for your DVR solution. One primary concern is the majority of DVR users want to be able to watch video from their workstation. Remember, the DVR’s are sitting in a rack away from the operator. So the video must be transmitted across a network. As such, bandwidth becomes a major concern and in some cases a mathematical improbability for older technologies.

We return to the garden hose analogy. If the garden hose can only accommodate one gallon of water per minute (e.g. your network connection) and you are trying to pump water from a source (e.g. the video data stream) which requires 3 gallons per minute we have ourselves a physics problem.

The water (video data) backs up (latency). Now let's add to the conundrum, what if you wanted to receive water from another source at the same time (video data from multiple DVR’s simultaneously) – the result is the throughput has been further cut. In terms of video what you end up with is chopped up and sometimes frozen images.

www.aventuratechnologies.com/casinos
The bit rates below are for uncompressed color frames at 30 frames per second NTSC:

CIF  36.5 Mbps

2CIF  73.0 Mbps

4CIF  146.0 Mbps

What do these numbers mean? A single 4CIF uncompressed image is 146Mbps. Typical network cards can only accommodate a maximum of 100Mbps. Therefore, a single camera would ostensibly surpass the capacity of the network. So what happens when you have to transmit multiple cameras? The answer is, it cannot handle it. While there have been improvements in network cards which now approach Gigabit speeds (1000Mbps), there is still the issue of the capacity of the encoding and decoding cards. They simply cannot handle the task. The processing power is too great. Therefore, in order to transmit camera images compression technology is utilized.

This is why most importantly; when you are given a demonstration of a DVR remember, that is not what you will actually be seeing in the control room. You need to see what the video will look like across the network. Ask to view and playback multiple simultaneous cameras on a workstation being fed by the DVR across a network to replicate the real world environment. Also ask to see the images on a full screen, not the size of postage stamps.
Chapter 16

Codec Algorithms

Raw uncompressed video as you see uses a tremendous amount of data. In the gaming environment we want to transmit and store, many simultaneous camera images on as few a servers as possible. In order to accomplish this task practically and efficiently the data requires compression before it can be transmitted or recorded.

Compression is performed when an input video stream is analyzed and information that is indiscernible to the viewer is discarded. Each event is then assigned a code – commonly occurring events are assigned a few bits and rare events will have more bits. These steps are commonly called signal analysis, quantization and variable length encoding.

The more the images are compressed, (meaning more information has been discarded), the lesser the quality. The challenge becomes to have the maximum amount of compression yet retain a certain standard of quality. Obviously, at some point if the video is compressed too much you end up with unusable video.

Older technologies, which use “simple” codecs, cannot do this efficiently. The newer codecs are “complex” and can intricately analyze an image resulting in better video transmission, smaller file sizes and superior image quality. Newer codecs can efficiently compress video more than 100x.
<table>
<thead>
<tr>
<th>Codec</th>
<th>Goal</th>
<th>Quality / Bit rates</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPEG-1 International Standard</td>
<td>Achieving plausible video and audio recording and transmission at approx. 1.5Mbps for VideoCD at CIF standard.</td>
<td>VHS quality at 1.5Mbps. Typical resolution CIF.</td>
<td>Nearly every computer supports MPEG-1 files. Typically used for lower resolution video, but can be used for any resolution. Progressive only.</td>
</tr>
<tr>
<td>MPEG-2 International Standard</td>
<td>High bit rate and broader generic applications, including TV, Broadcast, VOD, consumer electronics, including coding of interlaced video and HDTV.</td>
<td>High quality, typically full D1 resolution (MPEG-2 is used for Broadcasting and DVD) at 6-8 Mbps.</td>
<td>Application: Digital TV, HDTV, DVD, digital cable, satellite and terrestrial broadcast.</td>
</tr>
<tr>
<td>MPEG-4 Part 2 Visual H.263</td>
<td>Covers very low bit-rate applications. In addition to video coding, includes generic multimedia framework for animation, textures, 3D meshes.</td>
<td>DVD quality at 4 Mbps. VCR quality at 2 Mbps Provides 1.5 times better compression as compared to MPEG-2 standard, given the similar video quality level.</td>
<td>Application: Digital television; Interactive graphics applications (synthetic content); Interactive multimedia (World Wide Web, distribution of and access to content).</td>
</tr>
<tr>
<td>MPEG-4 Part 10/AVC H.264</td>
<td>All video requirements from High quality HDTV to low bit rate for cellular networks and a myriad of solutions from security to IPTV.</td>
<td>DVD quality at 2-3 Mbps. VCR quality at 1-1.5 Mbps Provides 2.5-4 times better compression as compared to MPEG-2 standard, given the similar video quality level.</td>
<td>The most advanced standard with fidelity extension ranges approved in April 2004 as the new High Definition TV Standard. New extensions allow for advanced broadcasting and video editing. Open standard adopted by all major industry participants (Intel, Microsoft, Apple, Cisco, Motorola, IBM...)</td>
</tr>
</tbody>
</table>

There are 2 types of compression; hardware and software. It is actually a case of compression and decompression.

When using hardware compression there are minimal loss of efficiencies, as all the work is being done on the DVR capture card by hardware components designed for that specific function. That is of course if you have all the right components.
Software compression utilizes software to instruct the computer's processor and memory to perform specific operations. As encoding and decoding functions are very intense, the processor and memory are taxed to their limits and beyond. It becomes further exacerbated when the computer is asked to perform multiple tasks simultaneously and there is just not sufficient power to perform. As the processor is being stressed it generates heat and accompanying noise. This leads to concerns of overheating and instability.

This is why we talk time and again about the system being designed to perform the function it is being asked to do; which explains why many DVR's are only capable of performing certain minimal tasks. Meaning, trying to record and display high quality real time images on multiple cameras simultaneously is not going to happen on low-end DVR's running software compression.

Codec Comparison

The Codec, which stands for compression- decoding, is a program or algorithm that lies at the heart of the DVR/video capture encoder card. The quality of the codec being run on your video capture card can make or break your system's visual and overall performance.
Not unlike computer processors and other digital technology, codecs have evolved rapidly over a relatively short period of time and continue to evolve and improve as we write these words.

The algorithm underlying the older codecs such as MPEG4, MPEG2 and wavelet is the Huffman Algorithm, which dates back to the 1950’s. The more current H.264 codec uses both the old Huffman algorithm and the new Arithmetic technology.

One of the headaches legacy security companies have is, they are accustomed building a black box that they can sell for years. Not so the case in IT. It is a continuous process that requires constant updating and modification to stay current; which is why many leave it to the IT savvy companies to produce, while they merely market.

In the information technology (“IT”) world we often speak of 180 days as one lifetime. Think about when you buy a PC - how long is it before the next greatest model is on the market? Every Christmas there is something new and usually at some point in between there are other advancements. So think about using an algorithm that dates back 50 years. Processing speeds of DSP's have increased almost 50% in the last year alone.

**MJPEG**

One of the oldest Codecs still in use. MJPEG (Motion JPEG) is usually found in the least expensive and lowest performance DVR’s. While capable of providing decent image quality, MJPEG is inefficient, resource intensive and requires massive amounts of storage space. It hogs bandwidth, which impedes network transmission. It has little use in an enterprise environment.

**MPEG2**

MPEG2 is a very common codec and has been in widespread use for more then a decade. It has a good reputation as a stable codec and, up until a few years ago, was the choice of most broadcast professionals. While smaller in file size then MJPEG it is still larger and more difficult to transmit across networks then newer codecs. MPEG2 dates back to the mid 1990’s.

**MPEG-4**

MPEG-4 (Part 2) is an object-based compression. In MPEG4, individual objects – rather than a scene of objects - are tracked separately and compressed together to create a data packet. This results in more efficient compression than MPEG2 or MJPEG and it is scalable, from low bit rates to very high. MPEG4 is approximately twice as efficient as MPEG2. MPEG4 dates back to the late 1990’s.
H.264

Most recently H.264AVC, also known as MPEG-4 Part 10 (Advanced Video Coding), has emerged as the leading codec for commercial video compression technology. Offering still significantly greater compression than its predecessors, H.264 provides up to 25% better compression than the current MPEG-4 ASP (Advanced Simple Profile). It also has the best image quality, smallest packet size, provides DVD-quality video and transmits video more efficiently over networks than any of the previous technologies. Unlike the previous codecs it is able to negotiate rapid complex images and provide razor sharp quality. H.264AVC is the first of what is known as a complex codec. The following chapter compares the different compression technologies.

Be very skeptical of people who say they have a proprietary codec and that it's not MPEG or whatever. Codecs are incredibly complicated to develop and are created by consortiums of some of the world's leading companies. The amount of years it takes to develop these applications with the number of people and companies involved make it highly unlikely anyone can develop a proprietary codec.

Where this is misleading is, each DVR manufacturer needs to modify the standard codec slightly in order to secure the data, so it may not be easily manipulated. This is important with respect to court admissibility. So technically speaking, each manufacturer’s solution is in a way proprietary but based on the standard codec.
Chapter 17

Compression Technology

Compared to prior generations of MPEG4 and MPEG2 technologies, H.264AVC video quality and performance is significantly better. Even with its higher quality video the H.264AVC file packet size is at least 25% smaller than MPEG4 and 50% smaller than MPEG2, requires significantly less bandwidth and offers rapid download times. Unlike the earlier MPEG technologies, H.264AVC is capable of stabilizing images.

<table>
<thead>
<tr>
<th>Efficiency</th>
<th>File Size</th>
<th>Download Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth (Mbps)</td>
<td>Storage (MB)</td>
<td>Download time (min)</td>
</tr>
<tr>
<td>MPEG-2</td>
<td>MPEG-4 (ASP)</td>
<td>H.264</td>
</tr>
<tr>
<td>2x more efficient than MPEG-4 Part 2 (natural video) encoding</td>
<td>3x smaller file size than comparable MPEG-2 encoders</td>
<td>Faster download time</td>
</tr>
</tbody>
</table>

- Higher Quality
- No Motion Blurring
- Capability

In contrast with 11-year-old MPEG2 and 7-year-old MPEG4 standards which were developed for TV and entertainment, the H.264 codec was designed with commercial security as one of its applications in mind.

H.264AVC is the standard for HDTV and runs everything from your mobile phone to Playstation, Quicktime and has been adopted by everyone from Microsoft and Apple to Intel and Motorola.

www.aventuratechnologies.com/casinos
Chapter 18

Compression Technology Challenges

One of the problems of the older MPEG formats is their inability to properly record fast moving objects. When objects are moving quickly DVR’s with older “simple” Codecs have a tendency to record blurred or distorted images, including mosaic patterns as you may observe sometimes on digital television broadcasts using similar technology.

While a scene or image is being processed, the next scene follows in sequence. As a result, there is latency, even if in milliseconds, due to time required to compress and decompress the images. Accordingly, when it can’t keep up there are voids.

Fast moving objects present formidable recording challenges in situations such as:

- A moving PTZ –
- A spinning roulette wheel –
- Rolling dice –
- A spinning wheel –
In order to efficiently negotiate a transition from one frame to the next; the codec needs a way to identify and predict what is happening in the coming scene. “Simple” codecs do not have the best of abilities to compensate or predict; resulting in potentially blurred or blocky images.

So beware. When evaluating a DVR solution for video quality, it’s not the images with minimal motion that are of as much concern as the ones containing rapid motion. In older compression technologies, to minimize the “blockiness”, the bitrate is boosted to a high level. This introduces the other concerns previously discussed of necessary resources to drive the escalated bitrate.

Can it still record 30 frames per second, without dropping frames and can it perform across multiple channels simultaneously? Is it going to overheat? Is it going to crash?

Also, by boosting the bitrate, which means larger file sizes, the storage requirements become massive. In the end, there is no fix for fast moving images using older codecs, the best that can be hoped for is a reduced amount of mosaic images with large storage requirements.

Part of the problem is older compression technologies were never designed for security or the new digital era. The first concern was simply how to compress video from a tape to a CD or DVD. So the variables and environment were somewhat controlled.

We have watched in casino environments where a number of things happen that frustrate the security people. They are unable to distinguish:

- the pips on a card
- the denomination of a bill
- spots on a dice

Then they attempt to playback video and in slow motion get blurred or skipping images.

Freezing a frame brings further challenges as they appear to have 2 balls instead of one on the roulette wheel or 3 or 4 dice instead of 2. This phenomenon is not unique to the casino industry.
Chapter 19

Why is Everyone So Slow to Adapt

Why haven't the old well-known names in security moved over to the newer technology?

First, it's important to understand that only a few years ago the CCTV business was strictly analog. It was simply connect a camera to a monitor, VCR or switch. These companies were ill equipped to deal in the information technology age. A transformation had to occur. These old time companies were accustomed to bringing to market a product in two-plus years, and running with it forever. Between the old methods and the lack of understanding of the newest technologies they have been slow to adapt but are now rapidly coming up to speed.

Part of the problem was 9/11 created an impetus to have an immediate solution even though the technology of the time was just not ready. Therefore, the foundation and building blocks for a solution were flawed from the start. The troubles were compounded by further development on the deficient platform instead of waiting for proficient technology. Why didn’t they change? How do you tell a customer that all the equipment you’ve been selling him for the past 5 years won’t work, and it’s not compatible with anything new that actually might work?

As previously discussed, many manufacturers rely on third parties, so they are at the mercy of their suppliers.

So when manufacturers eventually move to the new platform will they be on even par with everyone else?

Not necessarily. H.264AVC is not a magic pill. It is a core standard and platform on which applications have to be developed. As in all technologies there are processes and learning curves. In many cases, there are some MPEG4 solutions we are sure look just as good as H.264 solutions. Either because the underlying components are better or the solution is more stable then someone new working with H.264 for a relatively short period of time.

Understand that H.264AVC is just the “general” codec platform. Underneath this general platform many different “profiles” are being developed for different applications. HDTV will not have the same requirements as a video conferencing system. A Sony Playstation will not have the same requirements as a cell phone. So application specific profiles have been developed and advancements continue all the time.
Profiles

The H.264 standard includes many sets of capabilities, the following sets are an example of some popular profiles and how they differ. They are referred to as profiles, as they are targeting specific classes of applications:

- **Baseline Profile (BP):** Primarily for lower-cost applications demanding less computing resources, this profile is used widely in videoconferencing and mobile applications.
- **Main Profile (MP):** Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High profile was developed for those applications.
- **Extended Profile (XP):** Intended as the streaming video profile, this profile has relatively high compression capability and some extra tricks for robustness to data losses and server stream switching.

Similarly, other codecs also have a variety of profiles.

Some DVR manufacturers are onto third, fourth and fifth generations of the latest H.264 profiles, while others are first experimenting. With each generation come further enhancements, efficiencies and quality. Juxtaposed with the compression technology advances are digital processor advancements. Always remember it’s a moving target and its never perfect, as new matches of components to hardware and software introduce new challenges.

Think about Microsoft, with billions of dollars – their operating systems are never perfect and are a constant evolution.

One thing to note, all the money in the world cannot buy the time necessary for product development, as DVR solution development is “linear.” Linear meaning, the next person in line must wait for the prior one to finish their programming or development, before they can continue. Therefore, many aspects of development cannot occur simultaneously.

More and more the newest entrants into the DVR business have been the IT companies such as IBM, Cisco and Motorola, who are well equipped from a technical perspective. They too though shall go through the same painful process as their predecessors but are more qualified to solve the problems in a more expeditious and efficient manner. These entities are also participants in the consortiums that develop the compression standards such as the Motion Picture Experts Group (MPEG) and the International Telecommunications Union (ITU).
Chapter 20

Obsolescence

One of the more frustrating things about technology is how quickly it becomes obsolete. Buy something today and before it’s up and running the next improved model is out. The VCR dating back to the 1980’s never changed significantly. So gaming regulators set a policy and it stuck. Now regulators have to deal with moving targets, which change at the blink of an eye and are complex in nature and difficult for a layman to understand.

This becomes more frustrating to the casino who is spending millions of dollars to find out that by the time the installation is complete, its’ technology is old news and devalued. Some casinos want to standardize across all their properties and lock into a single solution. The problem arises that logistically by the time the casino gets to outfitting the last property, it may be several generations old. So they are going to pay yesterday’s prices today for old technology. Hardware costs universally go down in price not up. Whether it's HDTV’s, digital cameras, etc. gravity always takes hold in electronics.

Would you want a purchasing program where you are locking in today’s prices with today’s technology, for installations which will be completed over the next few years? The philosophy doesn’t work. From the technological side the issues are quite apparent. Financially, all you are doing is locking in higher prices. Technically, you are locking in older technology.

When manufacturers produce DVR’s they often “flash” (install) their compression technology to the processors in the DVR card, which stores the compression technology data. These programs are either temporarily or permanently stored on the processors.

The permanent solution is Application Specific Integration Circuits (ASIC). It is specific to that particular application and cannot be changed.

The use of re-programmable DSP’s (digital signal processors) has become all the rage. What is so special about re-programmable DSP’s is you can upgrade the codec to the chip. Products no longer have to become obsolete in order to be upgraded with newer technology.

Don’t confuse companies who say you may be able to “upgrade” software. It is still running on the same old platform and codec and what is being upgraded is a software interface or function, not the underlying quality produced by the codec.

www.aventuratechnologies.com/casinos
Therefore, if a casino buys a DVR today which uses an ASIC with last generation codecs and new technology comes out, the system becomes even further obsolete then it already is. Even more frustrating, if they bought many systems and then want to expand the security initiative, they may find out the new equipment is no longer compatible with the old and the components are no longer available. Some manufacturers say they will sell you their present solution which can seamlessly transition to the newer codecs, which is impossible. Fact is, ASIC cannot be upgraded regardless of what a sales person tells you.
Chapter 21

The DVR Software

In order to efficiently control, monitor, search, view and replay video and audio recorded over multiple channels and comprising, perhaps, hundreds or thousands of events and containing millions of images, you're going to need one heck of a software program.

- How does the software facilitate storage of the images?
- What happens when multiple users simultaneously access the DVR?
- How does it prioritize tasks?
- What happens when you have to search through millions of images or conduct queries?
- How long do requests take?

To the novice, the software's graphical user interface (GUI – the main screens) may look like a million bucks, but tells you little about its core features or performance of the DVR.

We are often asked who made the first DVR software, because many seem to “look-alike.” Again, the graphics of some systems may look alike, but that is where similarities end. You can buy a Rolex watch or Prada handbag, which cost $1,000's and last a lifetime or you can buy “knock-offs” on Canal Street in Manhattan for $25 bucks. They both look identical but that is where it ends. Usually within a short period of time the buttons fall off, the strap breaks and it stops working; but it looked great the day you saw it.

Much of the software in the market place today is based upon adaptations of entry-level type basic video capture software from earlier generations. As technology progressed, many manufacturers continued to build on top of old programs that were outdated.

The key concern of the software is the quality of the underlying source code. While the database structure is very important to DVR stability, the quality of the written software is just as important. A simple incorrect string of data can cause memory leaks similar to problems encountered with Windows of years past and the system will gradually slow down and eventually freeze, reboot or crash completely. So understand that a simple successful
product demonstration, speaks nothing of the product longevity. Software problems may not arise for days, weeks or months.

We recommend when testing a DVR solution, test it to its full capacity for an extended period of time, before committing to mass deployment. Why spend millions to find out weeks or months later, that it is not a workable solution or something better just came out.

Getting back to the software solution, there are multiple functions. Storing the video on a server and retrieving the data is but one software function. The operators after all have to review incidents, burn disks and fill out reports.

The server software is separate and distinct from the workstation software. Remember an operator is not going over to a room full of servers each time they need something from a DVR. So the workstation is just as if not more important than the server.

- How is this workstation software going to monitor hundreds or thousands of cameras?
- How is the video from different DVR’s pulled together at the workstation?
- How does the workstation software burn incidents which cover multiple cameras attached to different storage servers?
- Can the operator review video while still monitoring live images?
- How easy is it to use or does it require a PhD?
- How secure is it?
- How quickly can video be retrieved?
- How many images can be simultaneously displayed for live viewing or playback?
- When viewing or playing back, what is the display speed?
- Can the software interface with a matrix switcher so it can control PTZ's?
- Can the software interface with third party software?
- What is the quality of the remote video?

You have to think of the practical use of the system. The two main issues always are quality of the recorded video and usability of the system. A pretty graphical interface doesn’t mean it is practical, nor does a cool feature mean this is a great product. It comes back to can I use the video for an incident and how easy is it to operate the system on a “real-world” basis for all personnel, not just advanced users.

What about the management software that has to monitor all the other hardware and software? Some sort of centralized management software system is required to notify you of problems with other hardware and software systems.
The management system must provide a method to alarm in the event of a failed:

- Camera
- Hard Drive
- Server
- Encoder
- Decoder
- Matrix Switcher
- Operating System
- Software Program
- Power Backup System

Beyond alarming in such an event, what is the system capable of doing? Merely alarming doesn’t solve the problem but just advises. Technology is advanced enough today to the point where hard drive data can be rebuilt on-the-fly, failed hardware can automatically be re-routed to spare equipment. There are solutions to the problem, so don’t accept the answer that this is just the way it is and there is no solution. Or again, we emphasize, it’s not what you are told, but what they don’t tell you, because they don’t have an answer for their solution.

This is why we come back to; product demonstrations are typically scripted and you have to think beyond what you are being shown. Whether it’s at a trade show, in a control room or in a lab, real world functioning and product reliability and longevity are a concern.

We have all heard the horror stories of digital video systems, where manufacturers are camped out inside casino control rooms because they can’t keep their equipment up and running. These are not isolated incidents, rather very common place.
Chapter 22

The Hardware Components

We started out by saying some people consider a DVR, a PC with a video capture card and some special software.

There are PC’s that cost a few hundred dollars, and there are enterprise grade computer servers that cost $10’s of thousands. This is the one place you need horsepower in the form of motherboard, controllers, processors, memory, etc. Like any other product there are inexpensive solutions with questionable reliability and there is best-of-breed where quality and stability are a given.

Being deficient in any one area brings us back to bottlenecking - once again, you are only as fast as your slowest component.

Another concern is not only having the best and the fastest components but ones that are well matched. Remember, the company that manufactures the RAID controller is not the same as the one who makes the motherboard or the system memory. So while you may have the best of the best, it does not necessarily mean they are the best solution together. Many times when certain combinations are put together they are unstable or do not work at all.

When we talked earlier about RAID systems and we said that it is unusual to encounter hardware component failures, this still does not address the issue of compatibility. So while a component may not fail, the combination of components may conflict and cause problems that may surface initially or at a later date.

Manufactures can usually settle on a set of compatible hardware. The problem is its short lifespan. Next year, components are obsolete and you have to try to match new components and plan for backwards and forwards compatibility. The process is an ever moving target. Some manufacturers will just stockpile a set of components and 3 years from now you are buying 6 generation old technology.
Chapter 23

Peripheral Software

In addition to the main DVR server software and client workstations software, there are also a number of additional software programs that need to run in the background to give the system its reliability and stability.

The fact remains, DVR's are part of a very young technology where the bar is being pushed higher everyday. With constant demand for new features, a powerful foundation is required. But new features mean new unknown variables and accompanying problems.

Running diagnostic software, which constantly monitors several different functions of the hardware and software of both the DVR and server are essential. If the diagnostic detects any deviations from the established baseline criteria, it should automatically attempt to correct the problem and notify the system administrator it has detected a problem.

Diagnostic software is required onboard the DVR to monitor the operating system as well as the DVR program. From the hardware perspective, diagnostic software should monitor all devices, which are attached.

Central management servers with their software should monitor the DVR’s for their health. Optimally for fault tolerance a management server should monitor another management server. Each should monitor each other, which in turn monitors all the hardware and software throughout the entire platform.
Chapter 24

The Heartbeat of your DVR

We like to think of a DVR as a living, breathing being which deserves the quality care and attention of any beloved.

As such, your DVR should have some sort of “heartbeat” or health monitor program that constantly transmits data to let you know that it's alive and well. In the event that your DVR became ill or could no longer perform its duties, you probably want to be immediately notified.

Often, DVR manufacturers will tout a “hardware watchdog” feature. This function detects problems in your machine and tries to reboot the DVR to correct itself. When the DVR fails, the system is supposed to notify you. However, that may not be possible in certain circumstances.

What if your DVR failed and was unable to restart itself? How could it possibly notify you?

The answer is, you need some sort of third-party notification program that transmits an emergency message when it stops communicating with your DVR. This software must be located on an external machine, as opposed to the disabled DVR which cannot help itself and transmit. This is what we previously referred to as central management system.

Many gaming control boards require a central notification system, whereby when any component fails, whether it be a camera, DVR or peripheral an audible alarm sounds and continues until it is addressed.
Although Digital Video Recorders are relatively new to gaming there is already a well-defined customer base and it's growing daily. Like anything else-success stories travel quickly. Prudent business suggests that looking at who's using the product is usually a good indication of the level of quality.

Just because a company or an integrator was capable with analog products does not translate to digital solutions. Just because a company is a household name doesn't mean they are a safe bet. Remember, many of the products in the marketplace are not manufactured by the companies that peddle them.

Most recently, a couple of the most popular companies in our business were sourcing product from a company in Asia. That overseas company got into financial trouble and there was a ripple effect. Unfortunately, for the people who bought solutions based on that architecture, good luck in the future getting support.

Similarly, another major industry participant was buying product from a third party, and that company was recently purchased by a competitor. So what is the likelihood that the product will receive continued support. So ask the right questions and know what you are buying and understand that buying a big name doesn’t necessarily buy you job security.
Welcome to the Future

Casinos have made significant investments in their video surveillance infrastructure consisting of hundreds of cameras, recorders, storage devices, and video monitors. Yet, with all this state of the art infrastructure, analysis of real-time or recorded video is bounded to the limitations of humans who are often required to monitor multiple monitors to detect security threats.

No matter how highly trained or how dedicated a human observer, it is impossible to provide full attention to more than one or two things at a time; and even then, only for a few minutes at a time. A Harvard University study concluded that humans are surprisingly unaware of the details of their environment, and often do not detect large changes to objects or scenes (‘change blindness’). Furthermore, without attention, humans may not even perceive objects (‘unintentional blindness’). The Harvard experiment results showed that 50% of people counting the passes made between two basketball teams will not notice a gorilla walk into the middle of the viewing area, beat its chest, and walk out. In another study, military experiments demonstrated that after 12 minutes of continuous viewing of 2 or more sequencing monitors, an operator will miss up to 45% of all scene activity. After approximately 22 minutes, an operator will miss up to 95% of scene activity. The conclusion is clear - humans do not reliably detect security threats, whether watching live video or reviewing archived data, resulting in false conclusions that nothing occurred when, in fact, something did (referred to as ‘false negatives’).

Prior to the technological advancements that have made computer vision based solutions commercially viable, many manufacturers of cameras and digital video recorders introduced Video Motion Detection (VMD). VMD technology essentially looks for pixels that are different than the current background model in the same region of the scene. Unfortunately, these systems end up causing high number of false alarms in environments where there is a lot of irrelevant motion – such as weather, clouds, shadows, changes in lighting, etc. In fact, this caused so many false alarms (referred to as ‘false positives’) that distracted the monitoring process, and the end user simply turned off the VMD feature.

This is a compelling reason why casino management continues to look at video surveillance as a necessary evil, which does not generate revenues or save money, but just takes up space. So why spend the money? Things though have changed.

Today incredible improvements have been made in the burgeoning field of “intelligent video.” It’s no longer a matter of detecting motion or a basic smart search to locate a missing item. Advanced analytical software offers some significant features:
Unattended Baggage and Object Detection
Exit Lane and Wrong Direction Monitoring
Perimeter Intrusion Detection
Loitering
Vehicle Detection and Parking Violations
Anti-Tailgating and Piggybacking
People Counting and Crowd Detection
Secure Area Monitoring
License Plate Recognition
Slip and Fall Protections
Unusual Behavior Analysis
Card Counting Identification
Advantaged Play Detection
Facial Recognition

There is even the capability to identify objects, vehicles or humans by height, clothing worn, etc.

In addition to software analytics, intelligent cameras have arrived on the scene. These cameras can monitor and record in 360° and replace multiple area cameras. They also have the feature of being a “time machine.” After the fact, you can pan, tilt, and zoom, in all directions optically. Remember, a PTZ even at 26x zoom is only a 1x zoom after it has been recorded and only plays back where it was pointed.

So when the finance and management department say, it’s not a profit center, you can let them know, nothing could be further from the truth. Not only is intelligent video for surveillance, but it additionally has tools for marketing.

- How many people entered the casino at specified times
- Which direction people enter and exit the casino
- How many people approached a specific gaming table or slot machine
- Identify VIP’s
- Demographical studies

The potential list of uses is extensive. Surveillance is entering a new era. Training on the newest technologies is going to be a daunting task. If anything it’s a transitional period that will require re-training and the appointment of personnel that have a cross section of skill sets encompassing IT, surveillance, etc.

While it’s a little intimidating and overwhelming I hope we have taken out a little of the mystery of digital video and provided an insight into what it can do for you.
Chapter 27

Buyer’s Checklist

Demonstrations are just that and are usually “prepared” and “controlled.” For purposes of even the most basic evaluation you have to simulate real conditions. You need to control the environment, not the salesperson. Remember, they are not going to highlight their weaknesses.

Use the checklist below to note the results of your testing. One thing to consider, if you are going to compare manufacturers, test them on an equal footing. The best way to accomplish this is use the same feeds from your matrix switch to the test equipment. If possible, try to conduct the tests simultaneously, as then you can make a true apples-to-apples comparison. Otherwise, there may be other mitigating factors that may skew the evaluation.

In order to have a complete demonstration you really need to have a complete end-to-end system. If the components don’t all together meet gaming control specifications you are wasting your time. This should include:

<table>
<thead>
<tr>
<th>Non-PC-Based System</th>
<th>PC-Based System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encoder</td>
<td></td>
</tr>
<tr>
<td>Decoder</td>
<td>X</td>
</tr>
<tr>
<td>Workstation</td>
<td></td>
</tr>
<tr>
<td>Management Server</td>
<td>Management Server</td>
</tr>
<tr>
<td>Storage Server</td>
<td>Storage Server</td>
</tr>
</tbody>
</table>

1. Record each of the different games for an extended period of time. Make sure to record video where there is “significant motion.”

2. Take PTZ gaming cameras and swing them around at varying speeds, tracking individuals moving through your casino *(Remember very little motion may not be indicative of video quality, storage requirements, DVR stability)*

---

www.aventuratechnologies.com/casinos
3. Record the video on all channels simultaneously to demonstrate that you will not have a resource, bottlenecking or stability issue.

4. Check the recorded file for size. *(you can then multiply it out to get some approximate gauge of how much storage is required—but remember you still have to account for the RAID which will cost you at least 20% additional space)*

5. Playback video frame-by-frame. *(note the time and date stamp)(perform this test on the DVR Server/Decoder and the client workstation and compare the two)* Count the frames to make sure that there are 30 frames per second by the time and date reference.

6. Check the visual quality of the still images throughout the playback. Look for any pixilation, artifacts or in the case of specific games—appearance of 2 balls instead of 1 on roulette, 4 dice instead of 2, etc. *(perform this on both DVR Server/Decoder and client workstation)*

7. Playback should be done at full screen mode *(salespeople will tend to show you small images so they can hide abnormalities and poor video quality)*
8. Playback the video in real-time in full screen mode. Verify that the quality of the video is going to meet whatever published standard gaming control specifies. *(perform this on both DVR Server/Decoder and client workstation)*

9. In all playback modes note the time required to retrieve a specific amount of video from an individual or multiple files and make sure it is reasonable and practical.

10. Playback multiple cameras simultaneously. *(Note if there is any drop off in the speed or quality and check to see if you can synchronize the videos) (perform this on both DVR Server/Decoder and client workstation) (how many cameras can you retrieve remotely to the client workstation—remember the operators work at the workstation not the DVR)*

11. Check to see how do you playback video from a client workstation if the incident occurs on cameras that were plugged into different DVR Server/Decoders.

12. Burn a CD/DVD from the client workstation. *(check that the date and time are superimposed) (if the demo does not have the client workstation, make sure that a CD/DVD can be burned from the client workstation)*
13. Check that the burned CD/DVD can play in any PC.

14. After having burned a CD/DVD check to see that the encryption (watermark) is authentic. (if you have the ability attempt to “alter” the video or in the alternative find out if gaming control has approved that particular watermark)(there still may be issues as to how gaming control wants to see the watermark and where)

15. Since many incidents obviously occur using multiple cameras, which may be on different DVR’s, let them show you or explain to you how to burn a CD/DVD with video from cameras that are attached to different DVR’s. (if this is just a demo then usually it will only have a single DVR, so this must be marked as an open item)

16. Unplug a camera and verify the audible alarm and notification method. (note the time to alarm as gaming control usually has a maximum time to alarm)(if a central management server is not available for the demo then note this as an outstanding item)(the local machine alarm is of little use)

17. Verify what information is available from the central management system. Is it just audible alarms or does it have specific diagnostic information that could be useful. (remember we have to look into how practical the entire solution is)
18. Remove a hard drive from the RAID. (verify the time to alarm and check the recorded video to see that none has been lost)(many times the demos are not RAID systems, so this may not be available and noted as an outstanding item)

19. Remove the power from the DVR/RAID/Encoder/Decoder. (note the time to alarm as gaming control usually has a maximum time to alarm)(if a central management server is not available for the demo then note this as an outstanding item)

20. After removing the power from the DVR/RAID/Encoder/Decoder verify the state the equipment is restored to should be where it was just previous from it losing power.

21. When you are recording/playback video on all the channels simultaneously note the amount of noise of the equipment understanding this may be noise x 100 when the full installation is complete.

22. Put your hand on the equipment to see how much heat is being generated by the devices. (At some point, you will need to calculate the BTU output of each of the devices in addition to power to plan out HVAC and electrical requirements)
23. An important question comes in which is, what happens in the event of a catastrophic failure? What is the Mean-Time-To-Repair? Is there a catastrophic recovery plan so gaming does not have to be shut down?

24. When the complete system is installed you will need to worry about router configurations, firewalls, password protection and accessibility. (determine the level of password protection—is it by user, function, feature and camera)(is there an audit trail of the system so in the event of an incident you can ascertain what the operator did or did not do)

25. As gaming control boards seem to differ in opinion even within the same agencies you need to confirm what their definitions are as to specific standards such as: “point of concentration,” “fault tolerance,” “acceptable image quality,” etc.

26. When installing a system, be sure there is a practical approach. If you are using the same racks to house the equipment, where now sits VCR’s how are you going to perform the exchange without any down time? In our opinion run side-by-side a single rack of equipment not only until gaming certifies it but give it at least a month to confirm stability.

27. Contact Gaming Control and see if the particular system you are evaluating has a history in the jurisdiction whether good, bad or indifferent. So while the salesperson may be able to demonstrate everything to your liking if Gaming Control says that the system is not acceptable then it's merely an exercise in futility.
Before even getting to the point of ordering equipment certain pressing questions should be answered:

28. How long has the hardware and software proposed to be installed been in use?

29. Is the person selling the solution the integrator, manufacturer, reseller?

30. What IT qualifications and experience does the firm have?

31. If it’s an integrator, how long have they been selling and installing that product? *(also, as important are they an authorized reseller and trained)*

32. Who “actually” manufactures the hardware and software and who is using it?

33. Where is the actual manufacturer located, and what is their ability to support you?
34. If you are buying from an integrator, what happens if that integrator no longer supports that manufacturer?

35. If the manufacturer is not the source of the hardware and software, what happens if they no longer support the product?

36. How long do the manufacturers and integrators intend to support this particular platform? (you need to know if an expansion comes you don’t have to scrap the entire installation)

37. How long is the warranty and what parts are covered?

38. Are there Service Level Agreements and how much does it cost?

39. What technology is the product using and is the “core” technology upgradeable?