

10 TIPS FOR SUCCESS WITH VIDEO ANALYTICS

WHITEPAPER

By Doug Marman
CTO and VP Products
VideolQ, Inc.

Video analytics are bringing new levels of intelligence to the security world. Breakthrough technologies that extract information from video and automatically trigger responses are having a wide ranging impact. Starting with improved protection at the most critical infrastructure sites and high-risk facilities, video content analysis is now making its way into the broader commercial markets. It shows signs of transforming many aspects of the industry. However, when it comes to choosing architecture, vendor, and products to implement an analytic video surveillance system, there are key considerations to keep in mind. This paper outlines the essential tips to help you make the best choices for your application, and begin successfully employing intelligent video systems today.

1: FOCUS ON A REAL RETURN ON INVESTMENT

Leading industry experts considered 2006 the watershed year that proved this new technology. This means we have passed the first stages of the new technology curve and are now seeing positive gains. There are many effective and productive ways to start using video content analysis. However, the key to success with video analytics is to:

Focus on the applications that produce a real return on investment.

Where are the **most** compelling exploits of video analytics today?

- Perimeter detection
- Protection of outdoor assets
- Guard enhancement

Customers focusing on these applications are seeing guard service savings of 75% or more, while significantly improving security protection at the same time. These are impressive results. In most of these cases, video analytics are acting as the front line for guards, multiplying the power of existing guard forces. There are simply too many cameras to monitor, and video analysis does a much better job of constantly watching them all, than guards.

Moreover, the technology has been so effective that it is creating a whole new solution for protection: **Remote Guarding**, which reduces costs even further, improves security coverage and is far more scalable than traditional on-site manpower approaches.

So, it is easy to see where the excitement is coming from. But along with these striking improvements, there is also a lot of hype. So, be wary.

You will hear about quite a few promising uses for video content analysis, such as:

- Baggage left-behind
- Missing object detection
- Graffiti warnings



- Loitering alerts
- Crowd monitoring
- Tailgating alarms

Some of these applications work well. However, even to the best of these can fall short of producing benefits large enough to justify expensive new systems for these uses alone. In other words, they make nice additions, but do not always generate a significant payback by themselves. In many cases, long hours of testing and designing systems have ended in lukewarm returns on investment. That is why the above applications represent probably less than 10% of the successful intelligent video systems deployed. The suggestion here:

Check out the ROI first.

Some of these applications might fit your needs perfectly. If they do, then they are worth pursuing. Keep an eye on the future, since returns will change dramatically as costs come down and new features are added. However, the best place to discover the power of video analytics today is where they can save you money and improve your security protection at the same time.

2: CLEAR GOALS AND OBJECTIVES

Make sure you have a clear view of what your system needs to do. Here are some questions to ask:

- What are the analytics being asked to do?
- What does the system need to detect, to report, and how does it need to trigger an alarm or notify others?
- Does the video evidence need to be presented in court? If so, be sure the video is watermarked and you have instituted procedures for handling the chain of evidence.
- Is the environment going to change significantly or will the cameras ever be moved? If so, be aware that many systems will require recalibration.
- Do you need remote access for monitoring, configuration or upgrading the system? If so, what are the IT requirements and how will it integrate with your existing networks?

Part of the challenge with new technology is that it can sound so futuristic that some people imagine it can do almost anything. However:

- Don't expect video analytics to see in the dark. If a guard can't see intruders on their screen, then video content analysis probably won't see them either. Make sure there is adequate lighting.
- Don't expect video analytics to act like an alarm sensor accurate enough to directly summon the police, such as a door contact. Video analytic alerts need to be reviewed by a person first. Therefore, critical elements in any analytics system should be intuitive and clear alarm verification video clips. Done right, verifying a clearly highlighted video clip takes less than 10 seconds.
- Don't expect video analysis to be able to count the number of people in a car. Some systems can count the number of cars, and some can count people walking through a doorway one-by-one fairly accurately. However, since the people in a car are moving as one unit, no systems today are smart enough to see them as separate objects.



Sometimes the realistic capabilities of new technology are hard to estimate unless you understand them well. For example, detecting a bag left behind in the middle of an empty hallway is not difficult and can be done reliably by many systems. But how many terrorists are going to leave a bag out in the open like this? Will this really provide the benefits you need?

If you want to detect a bag as soon as it is put down in a high traffic area, are you willing to tolerate hundreds of false alerts created when people just set their bag down for a minute? If you limit alarms to only when no one is standing nearby the bag, will the number of false alarms still be too high, as people walk a few feet away to throw some garbage in the trash? Will any of this stop the terrorist who covertly puts his bag in the trashcan or behind a planter, hiding it from the view of any camera? These are the kinds of questions that need to be considered.

Ask your analytics provider to explain in detail how the application will work and what its limitations will be.

Some applications, like outdoor perimeter detection, have years of proven track-records. However, if you are trying something new, ask your analytics provider for a trial. Most are more than willing.

The best way to know if it is going to work is to test it first.

3: MATCH THE VIDEO ANALYTICS TO THE APPLICATION

There are substantial differences in performance between video analytics systems:

- Not all work well in highly dynamic outdoor environments, such as trees blowing in the wind, sudden lighting changes, headlights at night, animals, harsh weather, etc.
- Some technologies do not work well indoors.
- If you are going to use Day/Night cameras, make sure the technology can adapt automatically when the cameras switch from day to night. Many cannot.
- If you want long range detection, such as perimeter applications, choose a system that uses VGA or D1 resolution analysis. Many process only CIF or 1/4th of a VGA image. You will lose half your detection distance with these low resolution systems.
- If you are using thermal infrared cameras, be sure the analytics have been proven with these technologies. Most systems work fairly well with most cameras, but it is best to check ahead of time.
- If you are using infrared lighting that turns on suddenly at night, verify that the video analytics can adapt to this change in lighting without creating false alarms.

In other words, make sure you choose systems designed for your applications.

Some products are designed for specific tasks, such as people-counting or baggage left behind. These systems have been tuned for these purposes. This can help save you installation and set-up time. However, in some cases these technologies are packaged like this because they are not able to work well without calibration. Here is something to keep in mind:

Any system that requires calibration will need to be recalibrated if the environment changes significantly or whenever the camera is moved.

Some systems need recalibration when the seasons change. If you are going to use these solutions, make sure your staff is trained to make these adjustments, and ask your technology provider to explain how you will know when you need to recalibrate. Will the system alert you automatically?



The better solution is:

Choose a video analytics technology that automatically self-calibrates and adapts to any changes. This assures that it is always working, and saves in significant installation and maintenance costs.

There are many good video analytic providers. The best ones have years of proven experience in real world applications. Their first few years taught them the challenges of working reliably outside the laboratory. This is worth considering.

A proven track record will save you from going through the learning curve that all new providers go through.

4: DETECTION ACCURACY REQUIREMENTS

- How important is probability of detection (POD) with your application?
- How tolerant can you be with the false alarm rate (FAR)?

These are two questions you should consider before choosing your solution.

There are no systems with 100% accuracy. However, high quality video analytics solutions will have a **POD of 99% or better, with a FAR of 1-2 false alarms per week per camera or less**. These results are even possible in outdoor settings with highly dynamic backgrounds, provided you choose the right technology. This is where results clearly separate one solution from another.

The most important thing to know here:

All video analytics technologies are not created equal.

That's why you should be careful to match the solution to your application.

The biggest mistake being made in the industry today is confusing video motion detection (VMD) systems with video analytics.

Many companies are trying to ride on the coattails of the latest breakthroughs. Don't be fooled. They might show demos that look the same, but they aren't even close.

The most sophisticated VMD systems might include: Localized pixel change detection, recognition based on object sizes, vertical versus horizontal shapes, movement patterns. In other words, they have added some improvements to traditional video motion detection technology by looking at groups of pixel changes and how these blobs move.

However, real video analytics are much more intelligent. Far more sophisticated processing power is required to achieve these results. For example, real video analytics will first extract foreground objects, which are the objects of interest, from the dynamically changing background. This is a complex process. Secondly, real video analytics provide true object recognition. In other words they can recognize what type of object it is by its shape and movement. This is why they can filter out:

- Sudden lighting changes from clouds or headlights
- Tree branches and leaves blowing in the wind
- Reflections off water, and the continuous movement in fields
- Rain, snow, hail or fog
- Animals or birds



The results speak louder than words: The most advanced VMD systems reach at best about a 90% POD with a FAR of 28 false alarms per week per camera, in outdoor applications. At worst, these systems have less than a 70% POD with hundreds of false alarms per day.¹

In other words, at their best, VMD systems are 10X worse at detection and 10X worse at generating false alarms. At their worst, they are 100X-300X worse.

It is true they have made improvements to traditional VMD, but they are a long way from equaling the performance of true video analytics. If your system is going to be installed indoors away from any windows, VMD might work fine. Otherwise, don't confuse VMD – no matter what they call it – from real video content analysis.

Another Warning: Watch out for companies that say you need to send them video from your site ahead of time. Sometimes this request can help save you time. But often this is a mask for systems that require customization of their algorithms to make the technology work. Expect a larger learning curve when customization of algorithms is required.

Where you want customization is in setting up your action and notification rules, not with the algorithms.

5: CENTRALIZED VERSUS DISTRIBUTED SYSTEMS

There are raging debates over the differences between video analytics systems that are based on distributed systems versus centralized systems. There are pros and cons for both. In most cases you can make either type of system work for your application. But there might be advantages, so it is worth considering which way to plan your job.

Here is a summary of the main differences:

Centralized Analytic Systems

- Are generally easier to integrate with legacy video equipment.
- Require more physical space in the central office.
- Are more dependent upon the network when IP video is used. In other words, the system will fail if the streams of video cannot reach the centralized processor. If you use analog video cabling instead, then your system will not depend upon network performance.
- Enable the use of the widest possible variety of camera types

Distributed Analytic Systems

- Can put data at risk, since storage is located at the edge. You can solve this problem by immediately replicating critical events in central storage.
- Place much less demand on network bandwidth. However, this is not true if the system:
 - Needs to continuously record video elsewhere on the network, or
 - Part of the analytic processing must be completed in a server elsewhere in the system. Not all technologies work this way, but some do.
- Have a higher cost per camera. However, the total installed costs of larger systems may be lower.

¹ VTD White Paper - IOImage



6: CHOOSING THE RIGHT CAMERAS AND LIGHTING

Choosing the right cameras will assure that you have the best performance with your video analytics system. Here are some things to consider:

- Day/Night cameras are best for outdoor applications. Color will give you the best video information during the day, and B&W will give you the best quality images at night. However, be sure the analytics solution you use can automatically adapt when the camera switches between day and night modes.
- Thermal cameras or infrared cameras with infrared illumination can help when lighting at night is inadequate. But sure your analytics solutions are designed to work with these images, and they can handle the sudden change in illumination when infrared lights turn on or off.
- IP Cameras require decoders to work with systems that need analog video inputs. Note, however, that there are IP Cameras with both network and analog video outputs. These should work fine.
- Most video analytics systems will not work well if the camera is in motion. This means that PTZ cameras can create problems for most systems. Some technologies can work in what is called “Stop & Stare” mode, meaning that when the camera goes on its preset tour, it can detect video when the scene is stopped, but does not try to detect when in motion. However, if the technology requires calibrating the cameras, then you will have to calibrate a different setting for each preset location.
- If detection range is important, then choose a technology that analyzes VGA or D1 resolution video. With these systems, high resolution cameras will improve performance. 540 vertical TV lines are best.
- Wide Dynamic Range cameras provide better video information for video analytics to see what is going on in the scene, especially in most outdoor applications where the brightest and darkest areas are often present at the same time. However, CCD based WDR cameras can product artifacts that aren’t visible to the eye. CMOS based WDR cameras perform better with analytics.

Another popular application for video analytics is to use “spotter” cameras that watch a large area and then tell a PTZ camera where to look. There are a few systems that can do this today. However, be careful about expecting too much. Most systems can track one object well, but can become confused with multiple objects moving in the scene. Check with your supplier and understand how well it will work for your needs.

7: VIDEO TRANSMISSION QUALITY

High quality, low noise video is important for getting the best performance with video analytics. Choose the best quality transmission possible. Here are some recommendations:

- **Coax and Fiber Optics** are almost always reliable for delivering high quality analog video.
- **UTP – Twisted Pair** wiring can produce good quality video if the wire runs aren’t too long. Be sure the installers know not to push the limits when using UTP with video analytics.
- **IP Video** – Make sure the network will deliver good quality of service (QOS) and will not drop frames, or this could cause problems for analytics.



- **Analog Wireless** – Use only high quality transceivers, and keep transmission distances well within their rated limits. Also, check to see the area is free from interference problems.
- **Digital Wireless** – Can provide better quality video transmission than analog, but the output may need to be converted to analog video before feeding into the video analytics equipment.
- **Satellite** – Has been used successfully when high quality and adequate bandwidth is available. Satellite links are generally digital, so you may need to convert the signal to analog before feeding into the video analysis product.

When IP video, or wireless, or satellite transmission is needed: Consider installing video analytics at the edge of the network next to the camera, so it can process the video before transmission. This will assure the best quality video is being analyzed, and can reduce bandwidth requirements. This is one case where distributed analytic systems work best.

8: THE FIELD OF VIEW

Selecting the right field of view can make a big difference in performance. Here are some suggestions to achieve optimized detection:

- Looking down a fence line or border makes it easier to detect intrusion, since it is easy to see when an intruder has crossed into the protected zone. However, this can also make the system more expensive if you have to trench wires to mount cameras at the perimeter, and being at the perimeter makes the cameras more vulnerable to being attacked or compromised.
- Watching a fence or border from inside the protected zone also works effectively for many video analytic systems, provided there is a clear, unobstructed view of the perimeter. Most products let you set up Regions of Interest to define the detection zones. This approach is more secure and can save significant costs in installation, if digging trenches for wires can be avoided.
- Some technologies have the ability to ignore foot traffic or vehicles passing in front of a Region of Interest because their ROIs work in three dimensions. The Region of Interest acts like a virtual rug, covering the ground-plane area that needs protection. People walking by in front of the ROI will be ignored, even if part of their upper body crosses into the ROI, because the technology recognizes where on the ground-plane they are walking. Check with your video analytic provider to see if they have this capability.
- The camera's angle of view can make a big difference for most video analytics technologies. Some systems won't detect well when looking up at people (where the camera is mounted below the tops of people's heads.) Looking straight down on people may also cause problems, although some people-counting applications are designed for this point of view. Check with your video analysis company to see what they recommend.
- When trying to detect people entering or leaving through doorways, remember to make the Region of Interest large enough to include the ground-plane near the doorway, and include some space on either side of the doorway. Video analysis needs several frames to detect and classify an object, so allow extra space around doorways.
- The size of objects in a scene is important. Most technologies need to be able to see the full person or vehicle in the field of view to recognize them, and the objects also need to be large enough to be seen clearly. Some video analytics systems can recognize smaller size



objects than others, but don't be fooled by these specifications. The question is not how small of an object they can detect. The question to ask is: What size objects will they detect reliably?

9: RECORDING AND STREAMING OPTIONS

Perhaps the most important value of video analytics is its ability to automatically alert a person to important events. Just as essential is how quickly and easily it is to understand the evidence that it captured. Therefore, it is important to plan for the delivery and storage of video. The following are some thoughts to keep in mind for recording and streaming video:

1. **Alarm Event Recording and Communication:** In most cases, you will want to send a video clip of an intrusion to someone for review. This takes advantage of the proactive power of video analytics. Today, over 95% of video cameras are not monitored. They are simply recording video. This doesn't stop the crime. It only helps show what happened after the fact. With video analytics, your cameras become digital guards. You can now be notified immediately, or have a Remote Guarding service notified. There are two things to look for here:
 - **First**, you need the system to capture and send the video clips. If the video analytics system doesn't do this, then you will need to add a DVR or another video capture device that can.
 - **Second**, it is much better if the clip includes a colored highlight around the object detected. Without a marker, you will find yourself spending a long time studying video clips over and over again trying to find out what triggered the detection.
2. **Continuous Recording:** If you only want to capture the important events with your video analysis system, you may need nothing more. However, most security professionals prefer to also include continuous recording, just in case they want to go back and review video not captured in the alarm event clips. If your video analytics equipment can't provide this, you will need to make sure it can integrate with a DVR or NVR in your system. Here are two suggestions:
 - Program the DVR to log the event whenever the video analytics system detects an alarm. This makes it easier to search for that video later.
 - The best solution triggers the DVR into higher quality and faster rate recording whenever the video analytics detect a threat.
3. **Live Viewing:** In cases where a local or remote guard reviews the alarm clips, they will also want to see live video immediately so they can track the intruder. If the video analytics system cannot provide this, then you will need to add a DVR, NVR or other streaming video solution. However, some products are better than others at streaming video over the Internet to a remote site. If remote live viewing is needed, you should choose a DVR with high resolution MPEG-4 or H.264 compression designed for fast streaming.



10: SYSTEM INTEGRATION

Integration with the rest of your security system maximizes the benefits of video analytics. You might want your video analysis system to:

- Connect to a video matrix switcher, so that the monitors immediately switch to the camera seeing the intrusion.
- Trigger a DVR to record at the highest quality and fastest recording speeds during a critical event.
- Alert an access control system if more than one person or one vehicle has entered through a door or gateway.
- Interface with a POS system so that you can recognize if a customer is present when a cash register drawer is opened.
- Email a message to an operator if a car is parked too long, or a car has pulled over to the side of the road.

Here are a few thoughts to remember with system integration:

- Make sure your integrator has been trained, especially if highly customized calibration and set-up is required.
- Control room staff should be instructed on how to use the equipment to its best advantage – particularly in the use of video verification clips to review alarms for potential intervention.
- If you can't remotely tune and make adjustments to the system (such as changing the regions of interest and detection rules), then be prepared to spend more time at the site, if you want to optimize performance.
- Don't let your video management software provider dictate which video analytics technology to use. They will often try selling you their own, but none of the good software vendors have technology that is anywhere near as good as the best video analytics companies. Remember, these software companies specialize in integration, so they should be able to integrate the best systems available. Just ask.
- If you are going down the road of developing a new, customized solution, remember that when you are picking your partners: There is a big difference between the underlying video analytics algorithms that do the detection, and the software that bundles that detection data into an easy to use application. You can find the best application software writers in the world, but their data won't be any better than the algorithms that extract the information from the video. Look first for the companies with the best underlying detection capabilities. Then, if they haven't got the application you need, work with them to customize what you want. You will end up with a much more reliable solution.

