

The Future of Video Analytics

Reduction and Management of False Alarms as the Key to Success

A year ago, the video analytics issue has been only discussed between experts and the broad market was only aware of basic motion detection that has already been commodity in most IP cameras and DVRs. But markets proceed, and recently there has been some important developments going forward both on the technical side as well as on positioning that now allow a reliable prediction about future developments.

An Inconvenient Truth: False Alarms Will Remain

I would like to start with one of the biggest taboos in the industry: No intruder detection or high end "lost objects"-detection, no algorithm nor any other solution will be 100% reliable. There will always be false alarms! Consequently, the biggest challenge is not to create a reliable alarm. The biggest challenge in real life applications is to reduce false alarm rates and to handle those false alarms in a way that the whole solution is not rendered null and void.

The Importance of Video Management Systems

No matter from which perspective you look to a state-of-the-art CCTV installation, there is no denial that the Video Management System (VMS) is the central component, that makes the complete solutions intelligent – or not! The VMS is the only component that has access to all information available in the system. It defines the screen that the user or guard sees. It steers the workflow of alerts, alarms and events and last but not least, the VMS allows the user and installer to configure a complex setup – including analytics – under a unified user interface.

Sounds too good? Well, that is true – but it can be real in the near future if all manufacturers of the respective components do their homework and work on real IP video network standards and interfaces. And according to analytics, the most important duty is the consequent handling of Meta Data.

The Importance of Meta Data

Currently most VMS simply accept a pure alarm trigger signal from an analytical sensor channel – for instance a Axis or IQInvision camera, enhanced and enabled with video analytics. The intelligent "sensor" is treated like a thumb photo-electric guard or a glass breakage detector.



False Alarm caused by rain and heavy wind. Due to the detection frame the guard is able to close the file of false alarm in seconds. Without he has to scan the complete picture with the naked eye.

That simple ON or Off signal is only a fraction what video analytics can provide. For instance, in the application of intruder detection or perimeter protection, even the smallest and cheapest full-featured solution – the viasys edge client – is able to provide information like the size of the movement, which allows a discrimination e.g. if it's a person or a vehicle, the coordinates of the upper left and lower right corner of the movement (to draw the red alarm box around the detected object) and date, time, sequence number and of course the picture itself, together with a sequence of pre- and post alarm pictures. As solutions get more complex, providers like Agent VI or Vidient add to the above list more meta data like "object falling, running or lying" or directional information of several objects.

Meta Data Makes False Alarms Manageable

What is that good for? Is it not enough to have the right camera pop up on the screen when an alarm is triggered, but if the alarm is a real alarm and the object that caused the event can be clearly identified a bounding box around the object enhanced with some more information like size or direction may be regarded upon as a nice-to-have feature. But in case of a false alarm without any object information or any information which area caused the alarm its simply impossible for a human to handle that "alarm" quickly and efficiently. Theoretically, the guard have to scan the whole picture with the

naked eye to make sure that this alarm can be ignored.

And last but not least, meta data becomes essential when scenes and sequences should be found in archived video data. In well structured meta data, a search over a year like "show all cars that drove in that section from left to right without a stop" may take only some seconds search in a database whereas uncompressing the video streams with H.264 can easily take days and block the server that is computing such a search.

Consequences

The above insights have already initiated first reactions from the market. Many leading camera manufacturers, for example Axis, Bosch and Sony, realized that there is a need for standardization if they want to push VoIP further into the mass market. They initiated the Open Network Video Interface Forum (ONVIF) and 18 other manufacturers like Panasonic and HIKvision already followed. Even in the first version of the specifications, ONVIF reserves a special chapter exclusively for video analytics and how to handle events and meta data.

The leading VMS developer Milestone Systems has recently released their Xprotect analytical server which exactly solves the above issues: Alarm triggers from various sources can be managed under a unified platform. Meta data is accepted and stored in conjunction with the respective video stream and processed, e.g. for the

above mentioned alarm box around intruders. But also from the general concept, the approach from the market leader for VMS looks like a big hit: Their framework handles server-based, edge-based and even library based video content analysis. That covers everything that will be available in the future – and it will be a milestone in the IP Networked Video segment that other VMS vendors will have to match up with. And they surely will!

Server Based vs. Edge Analytics

The above approaches, especially the analytical server framework pose the question about the advantages and disadvantages of the respective way to host the analytical algorithms – but also responds to that question in a clear way that will be outlined at the end of this section. First let's have a closer look to the two – or more exactly - three ways to host analytics:

Server Based Analytics

The oldest and currently widest spread way to host video content analysis is to put it centralized on dedicated server. That was necessary because most of the algorithms consumed huge amount of resources both in CPU usage and RAM. Even on those dual or quad core machines, barely more than a dozen camera channels can be analyzed. To implement a larger complex intelligent CCTV network can easily end up in building a heavy and expensive data processing center – or, in like in many projects, it will cause the customer to step back from analytics and handle things in the old fashioned way.

The second serious disadvantage is the fact, that all video streams from all cameras have to be sent continuously 24 hours a day from the edge of the network (cameras, video encoders) all the way to the centralized server(s) – even if most of time nothing relevant happens. In doing so, terabytes of data block jam-pack the valuable network bandwidth – another serious reason for consumers stepping back from analytics or even choose analog cameras and wiring instead.

Those server based solutions have the advantage, that the above discussed handling of meta data is solved – naturally in a way that fits best with the underlying algorithms. After all it's the analytics vendor itself that designed the user interface. But even in that case the analytics has been a separate program, outside from the VMS that may not have been able to handle meta data. That may be a reason why some analytics vendors dare to step away from their core business and try to provide a full video management system with integrated analytics – aimetis is an example for such a positioning. In that case, the consumer has to abandon the option for a best-of-breed approach and may miss features on the VMS side. Another vendor did a move in the opposite direction: IOimage is now a manufacturer of cameras and encoders with embedded analytics. It will be interesting how those companies

will handle the channel conflicts involved into such a positioning and how they can convince their clients of buying their closed proprietary solutions and not the open standard solutions of the many other manufacturers like Axis, Milestone and viasys.

Library Based Analytics:

This is the latest development in server based technology: Encapsulated algorithms with standardized interfaces can be loaded and run on the same machine that hosts the VMS. The advantages are clear: less hardware is needed and the complete solution can be configured and handled under one unified user interface. A standard for meta data allows a deep integration of analytics so that the user is no longer aware that different manufacturers are involved.

Edge Based Analytics:

This is the consequent way to avoid the most serious problems of both server based approaches: Need for heavy CPU/memory resources and extensive network bandwidth consumption. In this case "edge" means the edge or end of the network, so not only cameras but also video encoders as the first device between analog signals and IP belong to the class of edge devices. If analytics is able to run on those devices itself the network traffic is simply zero as long as nothing relevant happens. Not until an alarm is triggered there need to be sent short IP signals with meta information to the VMS. This will then – in any desired frame rate and resolution – connect to the camera and monitor the event. The viasys solution for instance is also able to send in a push mode a complete alarm sequence including pre- and postalarm pictures via network to any receiver. The bandwidth consumption is so low, that even ISDN or UMTS connections are sufficient.

If VMS now start to accept and integrate the provided meta data, the effect for the user is the same as in server based analytics. A red alert box around the intruder, additional information displayed together with the video stream under one unified interface.

Edge Analytics – the Ultimate Solution?

Looks like the ultimate solution? There is no expert in the market that will deny – but only on the long run. The big "disadvantage" of edge analytics is the simple fact, that there are only very few algorithms worldwide that can run and will run for the next years on standard IP cameras. Of course you can pack a "server" in the camera, and some high end models have such a DSP (digital signal processing) chip and tons of RAM already integrated in the device – but that price level is far beyond mass market needs. In fact, such solutions are much more expensive than a centralized server park.

On the other hand, there are some few solutions available that feature small and smart al-

gorithms for the "bread and butter" needs in video analytics. For people counting there is a solution for a few selected Axis cameras available from a Cognimatics, same with some basic algorithms from server based manufacturers for one or two camera models.

The widest spectrum of supported cameras and hardware is available from viasys: Intrusion detection, perimeter protection and alarming can be handled reliable with features like "directional detection" or "trip wire" even outdoors. A pure piece of software (the Plug-In) runs fully at the edge on all Axis cameras and video servers as well as on all IQeye Megapixel Pro Line cameras. No additional hardware or DSP chip is needed, which brings the TCO for the customer to a minimum. Users of the above solutions do not have to make compromises in the quality of detection or false alarm rate, as long as they accepts that advanced behaviour recognition like "slip & fall", "lost objects" or "face recognition" can not be upgraded on those cameras at the moment.

Conclusion

In the new integrated video world that handles meta data, there will be no conflict between the different hosting forms of analytics. Customers may choose between server and edge analytics according to their needs – and why not combine an affordable edge analytics for intrusion detection on the majority of cameras with enterprise class behaviour recognition on a server from another vendor? All algorithms will anyhow be available and configurable under the unified user interface of the VMS.

And with the increasing CPU power of the standard IP-cameras there will be more features available at the edge. But smart vendors of edge analytics will also provide in the near future server based and library based algorithms. If their solution is able to run on a standard Axis camera, it naturally can run on any PC or as a library embedded into any VMS – and the advantage of small and fast algorithms is still a big advantage. When an analytical channel does consume less than 1% of CPU load, why not run a dozen analytical channels on a Milestone server or hundreds of channels on a single dedicated server.

And last but not least, customers can expect to find analytics on devices that they have not thought such an application to be possible. In Q1 2009 for instance American Fibertec – a manufacturer of high end network infrastructure – will release a network switch with embedded video analytics from the leading edge analytics company. The suspense continues...

▶ CONTACT

Dirk Owerfeldt

viasys Intelligent Video GmbH,
Neu Isenburg, Germany

Tel.: +49 0 6102 364668 · Fax: +49 0 6102 364680
owerfeldt@viasys-iv.com · www.viasys-iv.com