Emerging Trends in Intelligent Video Surveillance

December 2008

Why are Security Manufacturers Pushing Intelligence out to the Edge?

Larry Barfield

xpt^2, LLC

www.xpt2.com
(540) 364-2058

9687 Conde Road
Marshall. VA 20115

Leveraging Expertise, Powering Success

Why are Security Manufacturers Pushing Intelligence out to the Edge?

-- Larry Barfield

KEY DRIVERS

There are a number of reasons to suggest why the security manufacturing market is progressively moving towards distributed intelligence architecture. Technological Advances in micro-processor technologies provide increasingly robust processing power, which is required for complex and intensive machine vision tasks. This power is available at much lower prices and in a small form factor.

Additionally, security manufacturing companies are facing increasingly competitive pressure and will continue to leverage product innovation and differentiation to hold onto and gain additional market share.

As these companies deliver value to the market and demonstrate profitability, they become attractive to an active investment community. M&A activities typically fuel additional innovation in a converging industry. These are the progressive maturations where value along the business enterprise is realized vis-à-vis technological advances in a time of industry consolidation and convergence.

Drivers:

- *Technological Advances*
- *Competition/M&A*
- *Number of Devices*
- *Limitations of Network*
- *Role of IT Departments*
- *Performance*

USER ACCEPTANCE

However, these trends do not fully explain why the user community is accepting this trek to the edge. It is no longer rare to see solicitations and RFPs specify video analytics in their requirements language. In some verticals like commercial aviation and port facilities, it is now commonplace. The early adopter community makes up a small fraction of the overall decision-maker community in the security industry. Intelligent video is in its infancy. So, there must be other forces driving device intelligence to the edge in the security industry.

So, what else is driving it? - When we look at the sheer number of cameras that are installed (analog & IP) and the continued growth rate that is expected, video represents a significant percentage of the overall security device footprint. As those numbers increase, the ability to monitor, manage, and consume the available information becomes costly. I believe that we will look back in 3 – 4 years and see that we crossed a quantity threshold sometime in 2007 whereby video-based surveillance requires intelligence in order for it to be useful and not overwhelming. Intelligence whereby camera functions as well as scene monitoring is automated to relieve the requirement for human involvement. This is the promise of automation.

"I believe that we will look back in 3 – 4 years and see that we crossed a quantity threshold sometime in 2007 whereby video-based surveillance requires intelligence in order for it to be useful and not overwhelming."

IT DEPARTMENTS

Another driving factor is the limitation of the network itself and the influence from the keepers of the network. As security cameras become more ubiquitous, there is an inherent need to collect, manage and share larger amounts of data generated from the edge. IT departments saw this coming long before convergence became a buzz word and were steadfast in preventing video from causing chaos in an otherwise well-structured environment. In order to sell into a market of exponential growth in video cameras, manufacturers began to listen to IT and saw additional value in products that moved away from DVR and NVR-based camera control to those products that contained intelligence that could address the concerns voiced by IT while also delivering additional performance to remain competitive.

> *"IT Departments saw the need for convergence long before it became a buzz word and were steadfast in preventing video from causing chaos in an otherwise well-structured environment."*

EFFECTS

These key drivers have had profound positive effects for the users of the products. Device functionality has been adequately increased to gain the acceptance of IT departments in general. We now see cameras that can self-regulate the transmission of large amounts of data in multiple compression formats.

We see products that are highly specialized including thermal, megapixel, onboard storage, image stabilization, etc. We see a fairly wide market acceptance of these new products reflected in continued growth even in periods of economic downturn. We see video products behaving as good network citizens and organizations such as the Security Industry Association (SIA) and the Security Equipment Integration Working Group (SEIWG) developing industry standards around how these devices will function in the near future.

Effects:

- *Improved Functionality*
- *Specialized Products*
- *Market Acceptance*
- *Good Network Citizenry*
- *Standards Development*
- *Interoperability*

More importantly, with much of this intelligence located at the edge, we see interoperability as a natural outflow. Although video analytics is more or less along for the ride to the edge with distributed intelligence, it certainly occupies the front seat.

For example, as video analytics is pushed to camera-based or encoder-based products, manufacturers are abandoning their proprietary server-centric software applications in favor of open architectures that will allow the data and metadata to be consumed by most of the NVRs and C2 systems on the market today. Video analytics manufacturers are increasingly providing geospatial functionality to their edge systems and increasing the accuracy and range, which has plagued the industry in it's somewhat checkered past.

FUTURE ISSUES

What are the issues in front of intelligent video? First and foremost, the enormous growth projected in the data curve. Megapixel cameras present a unique concern in that the amount of data from a single camera can now easily represent an order of magnitude or more of data, just in the video data alone. Dual streaming cameras, camera installation growth, and increased information produced from the edge require specific solutions sooner rather than later. Otherwise, we will fail as an industry to deliver on the promise of automation.

Future Issues:

- *Exponential Data Growth*
- *Megapixel Cameras*
- *Sensor Correlation/Fusion*
- *Domain Awareness*
- *Excessive Automation*

Is it the right approach? We also have to be careful in our drive to place intelligence at the edge. Edge devices by their very nature are somewhat independent and disconnected from the rest of the environment in which they reside. A sophisticated and powerful smart camera has no idea what the camera mounted on the pole next to it is doing or seeing much less the radar system monitoring the same area within its field of view. There is a compelling argument to be made today that suggests the need for a higher level of intelligence that is centralized and more than just video-based in its architecture. Cross correlation of disparate sensor types, fusion of multiple video tracks to provide single target declaration and tracking, detecting temporal and spatial anomalies that are beyond the scope of any single device or system, these are the requirements of the Security Operations Centers (SOCs) that are being built today. To go beyond simple situational awareness to provide domain awareness - the effective awareness of anything associated with the enterprise domain that could impact the security, safety, economy, or environment of the enterprise itself.

I've listed **Excessive Automation** as a future issue to deal with simply because in our industry, it is a dagger. If we rely heavily upon video analytics to automate certain tasks that are best left to humans, we add risk to an equation that is inherently risk adverse. For example, take target classification.

Many video analytics manufacturers will tell you that their products can classify objects and tell you whether the object is a human or a deer; a bird or a helicopter; a Hummer or a JEEP. Although advances are being made in this area, video is still a two-dimensional plane from which the third dimension, depth, is extrapolated and thereby, somewhat unreliable. No video analytics product that I have seen can tell the difference between a bear and a human in a bear suit. However, a human can make that distinction effortlessly. We should let computers do what computers do best – highly computational, repetitive tasks; and let humans do what they do best – exercise judgment and resolve ambiguity.

> *"We should let computers do what computers do best – highly computational, repetitive tasks; and let humans do what they do best – exercise judgment and resolve ambiguity."*

BREAKTHROUGHS

I believe we are in the midst of seeing transformational technologies emerging already. Traditional security functions are moving from one-dimensional technologies to multi-dimensional technologies. As these transformational technologies emerge, the edge becomes populated with more sophisticated sensors delivering increasingly rich data.

But it's still not information. Data is merely the numbers, characters, and images that flow out of a particular device. In order to derive any meaning, data must be interpreted. For information to actionable (high value), it should be reliable, well-timed, and complete.

Edge device reliability (false positives) is only going to take the reliability factor so far. Higher level analytics will be the technology platform that delivers on the promise of automation and ultimately provides the reliability video analytics has been searching for. The same products will deliver on the domain awareness requirement.

We will also begin to see video management systems (NVRs) move from the SOC to the router level, embedded into the network. Some video analytics manufacturers are approaching the solution from a split-architecture perspective letting the edge device do what edge devices do best and subsequently taking only the necessary metadata to a sensor aggregation point and performing higher level functions such as sensor fusion and multi-user/single device operations away from the edge.

A highly sought breakthrough is the ability through the use of video analytics and other sensors, to derive intent. Much like a lie detector, video systems that combine visual and thermal imagery, eye movement, respiration, and limb movement with empirical human behavior models, can ultimately predict whether or not a person is likely to be harboring the intent to do harm. This is the Holy Grail for the commercial aviation industry, already a leader in the adoption of video analytics.

Breakthroughs:

- *False Positives*
- *Domain Awareness*
- *Embedded into Network*
- *Split Processing Architectures*
- *Derivation of intent*

GUIDELINES

So, in closing, where should integrators, specifiers, and end users look for the product breakthroughs? What video analytics products should you recommend your clients? What happens when you bid on a RFP where you know it's spec'd for a product that will most likely fail?

First of all, ask an expert before you get into a bind. Second of all, don't believe manufacturer's claims on accuracy and performance. Video clips are easy to doctor and most all manufacturers doctor clips. Reducing the false positive (or improving the accuracy) is a big challenge even to the most sophisticated video analytics manufacturer so they tend to misrepresent. Everyone claims to have the lowest false alarm and nuisance alarm levels (FAR/NAR). It is very difficult to quantify the accuracy of video analytics in an outdoor environment on this matter. Every scene is different every single second. Ask them to provide, at no cost, the equipment and software needed to prove the effectiveness in the environment most like your clients. Do this every time.

Secondly, don't depend on a single manufacturer to solve all your clients' needs. An indoor requirement for left object is not likely to be the same manufacturer for long range, outdoor intrusion detection.

Finally, make sure the smarts are where they are needed. In most cases, encoder-based products are perfectly suitable from a performance perspective as a smart camera. Most video analytics manufacturers will try to sell you on a feature list but at the end of the day, all you need is the most reliable (determined through YOUR testing and evaluation), cost-effective (cost per linear foot of coverage), and sustainable (is the company well capitalized, number of installations, etc).

Guidelines:

- *Seek expert advice*
- *Verify manufacturers claims*
- *Test in similar setting*
- *Don't rely on single source for all needs*