



Honeywell's recent purchase of ActiveEye analytics in the USA has greatly improved our presence in this market. By acquiring a strong US analytics company with a proven track record of installations, we can ensure support for our partners in the implementation of strong analytics solutions without getting caught up in overselling. We have already integrated the successful ActiveEye products, now known as Honeywell ActiveAlert, into our best selling Fusion DVR, giving us both server- and DVR-based analytics solutions. The big advantage of the Fusion-based solution is that it allows installers to fit a DVR knowing that if their customer later wants to add analytics capability, they can easily upgrade the Fusion without needing to move to a completely different machine or technology. It is another way to future-proof your installations.

Analytics is going to be an increasing part of video solutions over the next three years and will be as ubiquitous as video motion detection within five years. If you would like any guidance on the application of analytics, Honeywell Security would be delighted to help you.

Contact Jeremy Kimber at jeremy.kimber@honeywell.com. You can also consult our website at www.honeywell.com/security/uk or email us at systemsenquiries@honeywell.com



More Information:

Honeywell is a \$38 billion global diversified technology and manufacturing leader. Over \$9 billion of the company's revenue is generated by its businesses in the Europe, Middle East and Africa region. Honeywell opened its first office outside of the US in The Netherlands in 1934. Honeywell operates in over 35 countries in the EMEA region and employs more than 30,000 people. Honeywell's presence has grown and continues to expand through acquisitions and by building on its great position in good industries, offering innovations to our customers worldwide. Each of our businesses - Aerospace, Automation and Control Solutions, Transportation Systems and Specialty Materials – are engaged in manufacturing, sales and services across the region to serve global customers. Honeywell also invests in R&D across the region with global engineering and innovation centers in Romania and the Czech Republic.

For additional information,

please visit www.honeywell.com/security/uk

Honeywell Security & Data Collection

Honeywell Systems Group
 Aston Fields Road
 Whitehouse Industrial Estate
 Runcorn
 Cheshire
 WA7 3DL

Tel: 08448 000 235
 Fax: 01928 701 063
www.honeywell.com

Video Analytics – the new magic solution?

Jeremy Kimber, EMEA Marketing Leader – Video and Access Control, Honeywell Systems Group

Like the pharmaceutical industry, CCTV is always unveiling a new wonder cure. Given the rapid pace of technology development, it is inevitable that new solutions are constantly being brought to market. However, in many cases these new solutions are no better than previous, proven approaches and can even be solutions to problems that do not really exist.

Video analytics is the latest application that is generating huge amounts of interest in the industry. Respected industry analysts such as IMS are predicting that the market for analytics software alone will be worth hundreds of millions of dollars within the next 2-3 years.

There is a strong rationale to support the need for such a new solution. You don't need to be a part of the security industry to be aware of the huge number of surveillance cameras now in use in the UK – it is a fact constantly discussed in the media. At present, there are over 4.2 million cameras – one for every 14 people in the population - and the number is still growing. Generally there is still strong acceptance of the value of CCTV cameras in Britain. However, given the huge numbers, there is inevitably increasing concern from the public over privacy and the potential risks of intrusion into people's private lives.

Currently, the main benefits of CCTV cameras are seen to be an element of deterrence (due to the perception that anyone engaged in illegal activity is being watched so may think twice), and a proven capability to support the identification and prosecution of criminals

after the event. The rapid responses to the 21/7 terrorist plots and the more recent abortive airport and nightclub incidents are good examples of this latter point. However, there is a growing desire to see if CCTV can be turned into a more proactive tool. This is typified by the public address systems linked to cameras in Middlesbrough, for example, which allow operators to reprimand individuals via loudspeaker, helping reduce minor misdemeanours and prevent bigger problems.

Video analytics potentially helps address these concerns and is one reason why the technology is seen as such an exciting new development. Users of video are looking to find more effective ways to manage the vast mass of undifferentiated data that they are currently receiving from cameras and turn it into useful information. They are also looking to find ways to turn their cameras into predictive tools that will allow them to spot problems brewing and prevent incidents in a more proactive manner, rather than just filming the events for later investigative use. By supporting these changes in the use of CCTV, analytics will help address the public concerns over invasion of privacy. Cameras will increasingly be able to be used for the identification and prevention of real incidents - rather than just being surveillance for surveillance sake, sweeping up the good with the bad and everything in between. As video becomes increasingly used for targeting real criminal incidents, then in turn, the public should become more willing to accept further increases in the use and number of cameras without a major backlash on privacy grounds.

In broad terms, video analytics uses a variety of rules, which can be specifically tailored both to the scene and the objects being observed, in order to intelligently identify potentially suspicious behaviours. These rules cover everything from adjusting for major environmental factors, (not raising an alarm despite heavy snow or high winds), differentiating between people and vehicles (only raising the alarm if a car moves into a restricted area rather than pedestrians), to identifying if movement is in the wrong direction (across fence lines, up



one way streets, people entering exit only doors). Multiple rules can be used together and these can also be user-defined, allowing analytics systems to be fine-tuned to identify only the behaviours that are suspicious to the particular end-user who owns the system, based on their deep knowledge of their own security issues and site concerns.

By using multiple tailored rules and algorithms that will screen out adverse weather, the effects of changing lighting conditions, and non-critical movement activity, analytics systems let security staff focus on real incidents rather than getting bogged down with hundreds of false alarms. One misconception about analytics is that it is just advanced motion detection. The intelligence in analytics systems in practice means they are able to offer massive reductions in false alarm generations compared to standard motion detection.

Humans have an amazing capacity for decision making but are notoriously poor at maintaining concentration levels. A variety of studies have shown that after 20 minutes of watching, up to 90% of the information being shown on monitors will be missed as observers lose concentration. When this is multiplied across banks of monitors in a control room and across hundreds of false

alarms, it is no wonder that responsiveness to real incidents can drop significantly. In analytics systems, the application does the mind-numbing job of monitoring, using the rules and algorithms to screen out unwarranted alarms. Only suspicious behaviours then trigger the alarms, allowing the security staff to focus on using their decision-making capabilities to identify if it really is a threat and warrants further action or is still a false alarm – potentially leading to a retuning of the analytics rules to continuously improve the effectiveness of the system.

There are a number of video analytics packages available in the market. Typical applications include:

- perimeter protection
- monitored area of interest
- left baggage
- marketing analysis
- forensics

Perimeter protection systems provide back-up to fences, external pirs, seismic systems etc., allowing the user to identify specific areas where intruders will be identified. Potentially this includes virtual 'fence' lines that will trigger when an intruder climbs over it (rather than when a guard patrols along it), tripwires that trigger when crossed in specific directions and alert areas, such as nearby roads, which will

trigger if a car sized object dwells in them for too long – i.e. if a car stops on the road or pulls over near the perimeter being monitored. Combining these rules ensures only suspicious behaviours trigger the alarms and not the local rabbit population.

Monitored area of interest applications allow parking lots, one way streets, doorways and other specific areas to be monitored to avoid cars being left in no parking bays, to identify vehicles or people moving in the wrong direction (up one way roads, up exit only gangways at airports) and to highlight excessive loitering (via dwell time analytics).

Left baggage systems allow the identification of objects that have been left behind or left stationary for too long, particularly for transport locations although this may not be fully effective in very crowded environments. Some analytics systems, however, may even identify when the scene is getting too crowded and that they are no longer able to function effectively and need to transfer monitoring back to the security team.

A lot of the analytics information may also be valuable for marketing teams in companies as well as the security teams. Many analytics solutions have marketing packages that provide people counting,

car counting and dwell time functions (to identify if customers stop by key displays). Whilst potentially very useful for the client, a bigger question may be whether you as security installers have the right contacts and capabilities to reach and effectively promote these solutions to end-user marketing teams.

The power of the new analytics platforms also offers a significant improvement in forensic analysis capability. Recorded video can be fed through the systems, post incident, using the tailored rules to allow faster and more effective identification of participants or events involved in or related to the incident.

In summary, analytics offers the ability for security teams to become both more effective by proactively addressing suspicious activity prior to incidents occurring, and more efficient through improved monitoring performance and speeding up post event forensic analysis.

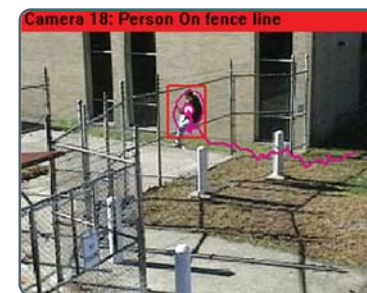
As well as the range of analytics applications, there are also a number of different architectures that support analytics. There is a lot of debate about the theoretical advantages and disadvantages of analytics at the centre (on servers or DVRs at the on-site control room or central

monitoring station), at the 'edge' (built into cameras or streamers on site) or with hybrid systems. In practice, the different architectures will be relevant for different clients with different needs. End user companies with existing infrastructures who want to upgrade by adding analytics onto some of their existing cameras may find that integrating analytics systems in their control rooms is the most cost effective and flexible solution. Customers with limited bandwidth on their networks may want to put IP cameras with built-in analytics on site so that only information on suspicious incidents is being sent through the network. Since the data will have been converted into 'metadata' by the in-camera analytics, it will also be even less of a drain on the network than normal video. As an installer, your best approach is to keep an open mind and look for manufacturers who can offer a range of analytics architectures allowing you to offer the best solutions for the individual requirements of your different clients.

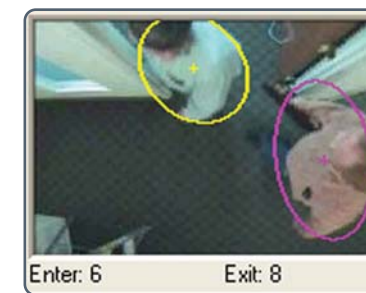
The other major caution for installers and system integrators is to be aware of overselling by manufacturers. Analytics is still in its early days of real use. There are only relatively few real sites using analytics in earnest in the UK – and there are even fewer where the client has actually paid for the system rather than using it on a trial or pilot site basis. And whilst the systems offer real potential, there is also a major risk that end users get an exaggerated impression of what the systems can offer. A number of systems also need a lot of initial set up work and on-going fine tuning. The last thing any installer or integrator wants is to sell a system and then lose all their profit on the project due to the requirements for extensive commissioning, and as a result of continually being called back to refine a system by an end user who is still not happy with it as a result of over-expectations generated in the initial selling process.

Whilst it may not be a magic solution, video analytics could be the smart bet of the security world, moving the industry away from indiscriminate saturation CCTV coverage to a more public friendly approach based on precision targeting.

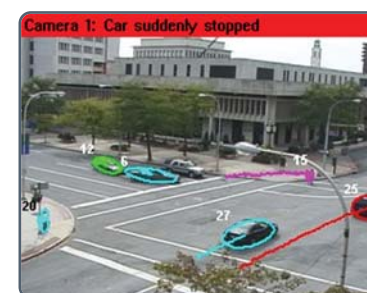
Sample applications:



Sterile Zone Surveillance



Person Counting



Vehicle Monitoring



Abandoned Baggage