VIDEO SECURITY FOR TRANSPORT

Lucas Young *discusses how cloud analytics, edge computing and AI is changing the way video surveillance is used across the transport sector*

Operators in the transport industry have a responsibility to ensure that members of the public who use their services do so feeling confident that all appropriate steps have been taken to ensure their safety and that security is not open to compromise. Whether it's at the bus depot, rail station or travelling by air, the technologies to protect passengers are in a state of continuous evolution.

Modern video surveillance coupled with cloud-based analytics is emerging as one of the most powerful, versatile and cost-effective tools available for transport operators to meet their responsibility in all areas of passenger safety and can deliver extra benefits for the business as a whole. This is boosted by the emergence of edge-based computing that allows video data to be processed closer to the point of creation. This lessens the burden on data transfer to the cloud, minimises the tasks required by video content analytics (VCAs) and massively reduces the cost of such services.

Video surveillance is a key beneficiary of the 'fourth industrial revolution' and emerging technologies. Over the last few years, the digitalisation of video data has given us the ability to apply new analytics applications to help shift the paradigm from forensic review to identify and track suspects or incidents in real time. Up until now, most of these cutting-edge features have only been available through expensive, on-site server applications.

Today's network cameras with edge computing capabilities transfer smaller data packets to agents for faster analysis, and when combined with data from other sources provide valuable business insights. We're already starting to see a fusion between camera vision, which is no longer just a lens, and deep learning technologies – which are enabling video analytics to become more accurate in extracting, classifying and cataloguing metadata, smarter at tracking patterns and trending demographics, identifying hot spots and transforming video into actionable intelligence.

The digitalisation of video data has given us the ability to identify and track suspects or incidents in real time

MOTION DETECTION ALGORITHMS CAN WORK WITH PERIMETER ALARMS TO DETECT INTRUSIONS

The aim is to combine the power of computers and their increasing ability to learn and understand with the unique decision-making abilities of human beings. Algorithms are proving to be a powerful tool and the more they're used the better they will become at differentiating between 'normal' and suspicious behaviour. We will see smarter cameras, more able to effectively analyse situations through AI, delivering the most relevant information to operators upon which they can make accurate, rapid and effective decisions regarding the appropriate response.

And the cameras themselves are continuously being upgraded to improve their ability to capture high-resolution, colour-rich images, even in poor lighting conditions. This means that those engaged in remote monitoring are able to get a better idea of what's happening on the ground, giving them better information to make decisions about incidents and engage in an appropriate course of action.

High-speed mobile broadband means that internet-connected cameras can also be deployed anywhere. 5G is already being rolled out across many cities and the communications network is only set to improve in the coming months and years. This is, of course, greatly beneficial to the transport sector. Whether it's at a bus stop or onboard a train, existing coverage can be extended at minimal cost and with little time spent on configuration. So long as there is access to power and IP connectivity, a camera network can be expanded on demand to provide cover where it is needed.

Significant parts of the rail network across Europe are relatively unmonitored, and inevitably these areas are more vulnerable to vandalism. Abuse of passengers and staff and acts of criminal behaviour remain a concern. The majority of journeys that take place are either essential commutes or freight, making the industry a key player in critical national infrastructure. However, delays and cancellations caused by maintenance issues or human interference, such as trespassing on the tracks and suicide, can have a profound impact on the network, its staff and the wider economy.

Video surveillance platforms which are capable of real-time identification of suspicious behaviour that might be a precursor to violence can also offer predictive maintenance capabilities, triggering alerts for events ranging from damage to infrastructure, tools left on train tracks or even overgrown and overhanging shrubbery that requires cutting back. By drawing an agent's eye to a developing situation before it occurs, security staff can be alerted before an incident escalates.

Bus travel security can also be greatly improved by using appropriate surveillance and data analysis tools. From time to time, driver errors have devastating consequences. To combat this, mobile surveillance systems that couple with accelerometers can record every time hard braking is sensed and combine this with other data to determine whether braking is due to bad driving or traffic congestion on the route. It is also a powerful aid in post-accident investigation, with cloud-based video providing instantly accessible footage for appropriate authorities. Investigators can quickly determine whether any failures were caused by driver behaviour or circumstances outside their control.

Similarly, onboard cameras with connected audio can assist in monitoring situations of challenging passenger behaviour, recording audio when raised voices are detected, helping to ensure that there is both video footage and audio recordings of an incident. Equally, outer vehicle cameras can be used to provide a bus-wide system of surveillance to help determine the real cause of a situation and providing accurate video evidence to save transport companies money by helping to protect against any unproven insurance claims.

When it comes to airports, security is taken to a whole new level. Managing thousands of people from arrival to take-off, landing to leaving, is a complex logistics challenge with many variables. Despite heightened levels of security, airports share many of the same challenges as other large transport hubs. Safety has to be the top priority and passengers are now well used to bag searches, x-ray scans and metal detectors designed to prevent prohibited items from being taken onto planes. Airports must maintain high levels of operational efficiency, and security is paramount to ensuring passenger safety and providing an improved experience.

Facial recognition technology has multiple applications in an airport setting. Automated border control systems utilise face-recognition technology, combined with data stored in biometric passports to verify a traveller's identity. In the future, it may play a significant role in the rapid and frictionless transit of a passenger through a terminal to help ease congestion. In restricted areas, to ensure that only staff with appropriate levels of authorisation can gain access, facial recognition data can also be integrated with traditional access control, such as a key card, or HR records, to alert staff if an employee's credentials have been compromised.

Airport perimeter security is a critical issue with many challenges for those in the field of aviation. Fences can be many miles long, and hard to secure and monitor. It's not unusual for breaches to happen, and to remain undetected for some time. Many cameras on the market

feature sensors that are still capable of producing highly detailed images even in rain, fog or at night. Motion detection algorithms can work with existing perimeter alarms to improve the ability to detect intrusions rapidly, and the ease and reduced cost of deployment also means that blanket coverage of a perimeter is much more feasible.

A CENTRALLY MANAGED SYSTEM CAN BE MORE EASILY KEPT IN LINE WITH GDPR REQUIREMENTS

These networks can reduce operating overheads dramatically, by cutting down the number of false positive alerts. Better images provide remote agents with the ability to accurately assess a situation before despatching a ground team. Combining visual data with other sources, such as infra-red imaging, can improve this further. At a distance, a skulking human and a plastic bag might appear the same on a monitor, but add in thermal data and the difference is obvious both to a human operator and to an AI assistant.

There are benefits which can be delivered from cloud platforms for video surveillance beyond security too. The same analytics used to detect anti-social behaviour are also delivering business insights that improve customer experience or drive efficiencies elsewhere in the operations. Footage from carefully positioned security cameras, for example, can be analysed in real-time to detect the build-up of large queues at check-in, which could cause bottlenecks – ensuring that staff are on hand to appropriately manage the situation.

The same system can be used to trigger an automatic audio announcement, directing customers to an alternative waiting area, for example, or informing them that further check-in areas are becoming available. It can be used for analysing footfall in certain areas of a transit terminal, which in turn can help to guide pricing for retail rents or help to assess the impact of marketing.

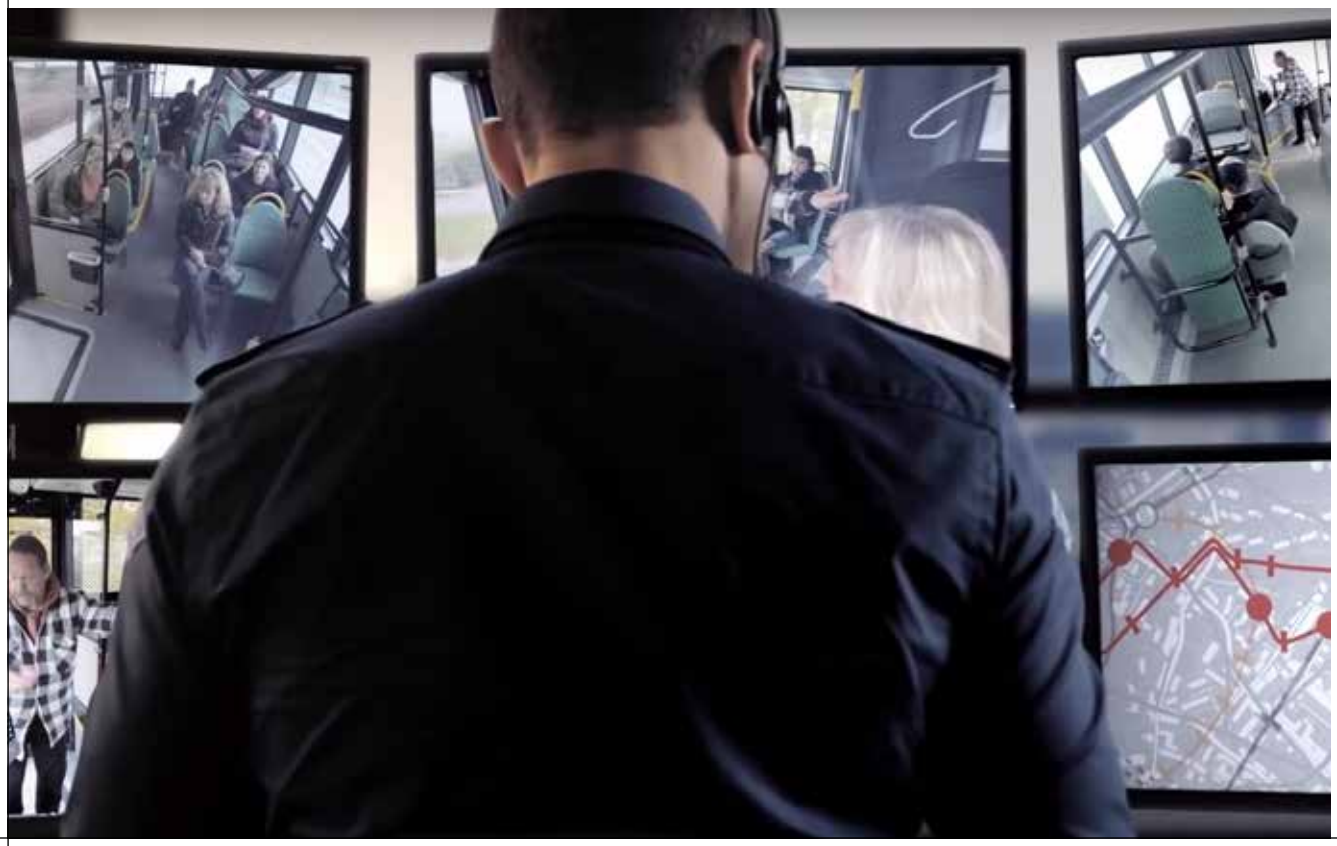
Digitalisation is revolutionising the business model of video security, too. Just as the as-a-service model has changed the way we buy software applications, computing power or storage, so it is changing the way that we buy and sell video security.

Moving to a video-surveillance-as-a-service (VSaaS) model, rather than investing in physical servers, means that an organisation always has access to the latest version of the application, with new features and security upgrades added when they are available. Per-camera licensing models for applications or even rental of the cameras themselves could continue to drive down up-front costs and introduce even more flexibility for end customers.

Networked cameras are also easier to maintain, as they can be managed from a central source regardless of their physical location. Health monitoring functions can notify an operator if a camera fails or send an advance alert to raise awareness of a fault that is developing. Cyber security updates and firmware upgrades can be pushed to end devices without the need to despatch technicians. What's more, in a world growing increasingly sensitive to the use of video surveillance and its impact on end-user privacy, a centrally managed system can be more easily kept in line with new regulations, such as the EU's General Data Protection Regulation (GDPR).

All of these capabilities are available now, and in the future as the technologies mature, more and more use cases and advantages will be found for cloud-based video security. These will help to provide more utility, security and return on investment from existing camera deployments. All of which means better, more comprehensive security for both the travelling public and our diligent staff ●

Lucas Young is Axis' Business Development Manager for Northern Europe, responsible for transport sectors. Lucas comes from a risk management and security consultancy background and has worked extensively in the transport sector including ports, maritime, rail and airport environments.



Onboard cameras with connected audio can assist in monitoring challenging passenger behaviour on buses

Picture credit: Axis