Picture credit: Getty

SECURING THE SKIES

Lucas Young *discusses how innovative new technology can effectively protect an airport from perimeter to plane*

By their very nature airports throw up a wide range of potential security concerns

There are few that take security as seriously as airport operators. Safely managing the movement of thousands of people daily onto a highly sophisticated, yet potentially vulnerable form of transport, requires more cutting-edge technology than ever to ensure it continues to be one of the safest forms of travel. The issue of aircraft safety has been highlighted more recently through the marked rise in drone sightings around airport perimeters, leading to large numbers of flight delays and cancellations.

Drone sightings are a modern type of nuisance with the potential to cause great damage. But inside airports there are also many other forms of more traditional criminality. For example, many terminals have evolved to accommodate significant shopping concourses as a means of both enhancing the customer experience and boosting airport revenues. On show are a tempting display of highly desirable products for both organised criminal gangs and the opportunistic shoplifter alike. Additionally, theft of bags and luggage is a huge challenge at some locations, with large numbers of tired travellers perhaps not paying as much attention as they normally might.

With so many threat vectors to monitor both inside and out, airports are perfectly positioned to benefit from the advantages that connected devices and the Internet of Things (IoT) are bringing to the physical security market. A connected security system is far greater than the sum of its parts and can offer protection from perimeter to plane using increasingly cost-effective solutions.

One of the most immediate opportunities for network video, for example, is at the airport perimeter. The sheer size of an airport has made it difficult in the past to effectively monitor the entire perimeter, and reports of breaches in security are all too common. In many cases, intruders may trigger an alarm, but tracking their progress across the airfield without video is tough, especially at night.

But technology has progressed rapidly; today's network video cameras are incredibly light sensitive and are able to provide high-quality video in conditions that up until recently would have been considered simply too challenging. By utilising integrated security platforms, this video data can be combined with information from traditional monitoring technologies, such as fence alarms and motion detection sensors, to provide a robust multi-functional solution. Security platforms can provide the user with live or forensic video evidence of a security breach by harnessing the smart interconnectivity of, for example, thermal and PTZ cameras, which actually work together to detect and track multiple intruders in total darkness.

FACIAL RECOGNITION IS FAST BECOMING A CRITICAL COMPONENT OF PASSENGER SECURITY

Low-light cameras additionally have a bigger part to play than just shooting video at night. Planes can be monitored for loading and take-off in adverse weather conditions, with object detection analytics, optimised with machine learning, able to identify fallen luggage or other objects that might be hazardous at the stand and on the runway. Similarly, cameras with a combination of low-light capability and a high dynamic range (HDR) are now being widely utilised in conjunction with an array of different drone detection solutions to positively verify and provide evidence of drone intrusions.

But networked surveillance technology isn't just for the airport's perimeter and airfield; it also has many applications inside the terminal. At check-in and passport control, facial recognition is becoming a critical component of passenger security by providing early warning that someone may be on a no-fly list, for example.

SPOTTING SUSPICIOUS BEHAVIOUR

There are other opportunities too, such as intelligent analytics systems, which have been developed for retail environments. These can identify suspicious behaviour, such as customers loitering next to high-value items or ATMs. A 'smart' camera can directly instruct a connected speaker to play an automated announcement subtly informing the individual that they have been seen or the camera might send an alert containing an image of the suspect person to a member of staff via a handset.

But as security systems digitise and mature, they become more multi-functional with the data they provide having real commercial value. The lessons from retail are that security cameras can host analytics, which identify the build up of queues and alert the organisation to provide more staff at key points. What works for checkouts can also work for passport control. Taking that one step further, video data can be combined with other sources of data for long-term analysis and planning for future developments and even emergency situations. Being able to evidence footfall numbers with video is a strong argument for premium price tags on retail and advertising space. Similarly, understanding customer flows can help identify potential pinch points in an evacuation scenario.

All of these technologies are feasible today and are becoming increasingly cost effective to deploy. The key is the transition to digital data for all parts of a system, and the ability to connect cameras to door controls to perimeter alarms and more. Truly intelligent airport security is here, and passengers should expect no less ●

Lucas Young is Business Development Manager (Transportation – UK and Northern Europe) at Axis Communications. Prior to his current job he worked as the performance improvement manager at Gatwick Airport.