Dealing with rising airport security threats demand more innovative solutions

With the rise in large security threats since the commencement of this century, security of airports has become paramount. Looking into this issue Ashley Smith, BSIA (British Security Industry Association) Civil Aviation Security Section Chairman, explains how a mix of properly interfaced security systems working in conjunction with monitoring and response staff offers a cost-efficient and flexible solution.

Airport sites present peculiar security challenges. For example, detecting perimeter breaches and intrusion in relatively remote areas away from the airport’s hub is particularly difficult. However, as security systems become more sophisticated, reliable and competitively priced, and there is better integration of products from different equipment manufacturers, these challenges and vulnerabilities can be overcome with effective solutions.

When evaluating and drawing up risk assessment specifications for airport security, a broad range of issues need to be considered, to combat potential threats ranging from those more commonly
anticipated at other types of site - such as vandalism, thefts and arson attacks - to incidents posing more specific hazards towards aviation. These include environmental protesters staging break-ins to cause damage and disruption and, of course, terrorist attacks on infrastructure, aviation & airline staff, and passengers.

**Turning security weaknesses into strengths**

One of the perceived weaknesses of a large airport site can be transformed into a potential strength. A large site helps provide early warning of suspicious behaviour, for example along a perimeter fence - before an unwelcome visitor can reach their target. The physical distances involved can also be used to the site's advantage using a mix of intrusion detection, monitoring equipment and security guarding responses. Along an airport's outer perimeter, fencing can present both a

A large airport site may be perceived as a weakness but this can provide an early warning of suspicious behaviour, for example along a perimeter fence

physical and electronic deterrence. Decisions regarding the specifications and complexity of fencing equipment can be based on parameters such as proximity of vulnerable and important elements that include airfield power supplies, runways, hangars and cargo storage facilities.

**Using perimeter and surveillance solutions working together to offer the best protection**

In conjunction with the physical fencing hardware, vibration and movement detectors will provide proactive warnings to security staff in the airport's security control room, alerting operators to the scaling of a fence and other breaches requiring a response. Such an approach minimises requirement of repetitive and avoidable labour intensive patrols that not only add to greater
manpower costs but also increases the risk of missing out on security infringements occurring elsewhere. Related to the improvements in efficiency are additional electronic security systems such as vandal resistant day/night CCTV cameras with powerful optical zooms, linked to advanced detection methods including thermal (i.e. infrared lighting) and radar techniques.

Use of perimeter fencing together with movement detectors can provide proactive warnings to security staff

By using multiple, integrated technologies, intruders can be detected and tracked in real-time. Alerted CCTV operators can then use the thermal images to direct colleagues on the ground to apprehend the intruders. Security cameras can work in all weather or lighting conditions using these complementary techniques, providing evidential quality recorded images for follow-up prosecutions using digital video storage.

Thermal imaging techniques enable the selective use of ‘white’ (or visible) light, including floodlamps. This ensures, for instance, that aircraft pilots are not suddenly distracted or even blinded by security lighting.

Network IP - an essential tool for system flexibility

The use of IP (Internet Protocol) connectivity also provides flexibility in optimising security camera
placement, with wireless transmission methods such as 3G mobile phone signals meaning that physical connections such as fibre optic cabling are not required, with their associated cost and installation disruption. The relative ease of IP-enabled cameras' installation can serve a dual purpose, helping keep an eye on staff working in remote areas of the airfield for both security and health and safety purposes. Managers can also dial-in to a camera network remotely, to view images without needing to visit the control room.

Use of video analytics software in airport security solution

Video analytics provides an advanced surveillance-related filter that helps to sort through multiple scenarios that security teams are routinely faced with
Video analytics provides an advanced surveillance-related filter that helps to sort through multiple scenarios that security teams are routinely faced with. This type of analysis is also benefiting from ongoing investment by systems suppliers who are addressing the need for cost effective, meaningful, reliable and user-friendly software. As a ‘force multiplier’ that frees up security personnel to be more effective, video analytics is becoming increasingly attractive with its added value functionality that helps pay for its own deployment. In practical terms, video analytics involves software processing algorithms that analyse security camera data from a scene, detect situations that meet a certain set of conditions, filter them for possible false alarms and then, if verified, issue an alert that security staff can react to Appropriately. Use of such advanced video analytics software is a step up from traditional video motion detection and offers significant future potential in combating crime threats. At an airport perimeter, the technology could, for example, use what’s called a ‘virtual tripwire’ - essentially an area of the scene that triggers an alarm when an object enters that zone. Closer to the centre of passenger operations, video analytics technology can also flag up the presence of left baggage in a terminal or other sensitive area.

Managing airport access control systems

Besides the detection and monitoring of movements at an airport, security staff and systems must also control, manage and verify a high volume of round-the-clock traffic, including passengers, staff, contractors, maintenance crews, suppliers and other visitors. This management process begins again at the perimeter, allowing back-up time and resources to be deployed in the event of problems. Physical measures including gates, barriers and bollards can be used to control vehicles intent on access, while validation processes check the identity of individuals and their vehicle contents.

Depending on the type of airport facility involved, its geographic location within the airfield and related risk factors, these checks can vary in size and scale. They can range from use of temporary contractors’ permits using a paper based logging system through to photo ID working in conjunction with access control cards carrying a magnetic stripe, barcode or RFID chip for more convenient proximity reading of card details and activation of gates, turnstiles or vehicle barriers. It is important
to verify the daily influx of visitors for more than security purposes because airports, like other companies, have a legislated ‘duty of care’ towards every visitor, requiring them to ensure that non-employees are not exposed to health and safety risks.

**Security team training**

Monitoring of passenger and airport staff is highly dependent on the type of airport facility

A holistic security systems environment will involve different types of protective equipment communicating collectively to contribute more than the sum of their parts. For instance, CCTV cameras on automatic area ‘tours' will immediately react to the opening of a vehicle barrier by instantly refocusing on this area and triggering the digital recording of the event for subsequent identity validation or prosecution purposes. BSIA member companies provide a range of effective systems based solutions, as well as the trained and skilled manpower to both implement and manage them. For example, competent, flexible and observant CCTV operators will need to work with adaptable, self-reliant and resourceful security officers to provide the necessary response to identified incidents. These staff can also provide a variety of added value roles during their daily duties that contribute towards the airport's overall operating efficiency and effectiveness.

Working in tandem with physical and electronic security, security teams are a fundamental element
within an increasingly integrated security ‘envelope’ designed to ensure realistic and cost-effective protection for the wide span of airport operations.

Ashley Smith
Civil Aviation Security Section Chairman
British Security Industry Association (BSIA)