FROST & SULLIVAN

Airport Security: New Technology to Meet Evolving Threats

Anthony Leather, Research Analyst, Europe – Aerospace, Defence & Security

Introduction

The decade following the attacks on the World Trade Center in New York has seen the global airport market face intense scrutiny. It continues to face evolving threats and difficult challenges, including integrating new technology into airports and maintaining passenger satisfaction. The US Transportation Security Administration (TSA) released figures in July 2011 that showed there had been over 25,000 breaches of security since 2001. While the nature of threats has remained similar, the delivery, method and execution have continued to evolve. Naturally, terror attacks such as the recent incident at Moscow's Domodedovo Airport in January 2011, in which 35 people died and over 100 people were injured, take most of the headlines. They have the potential to, and sometimes do, cause the greatest damage; however for airport operators the perception of less sensational threats remains equally high.

Technology provides a key resource to deter and obstruct those with criminal intent. Its role and prevalence in airports is only likely to increase. However, the technological growth in airports has faced problems and controversy. Integrating existing security systems with newer technologies has caused issues in reliability. Advanced screening equipment has been branded invasive and contrary to human rights regulations, while the rise in biometric controls has also been met with criticism and scepticism from passengers.

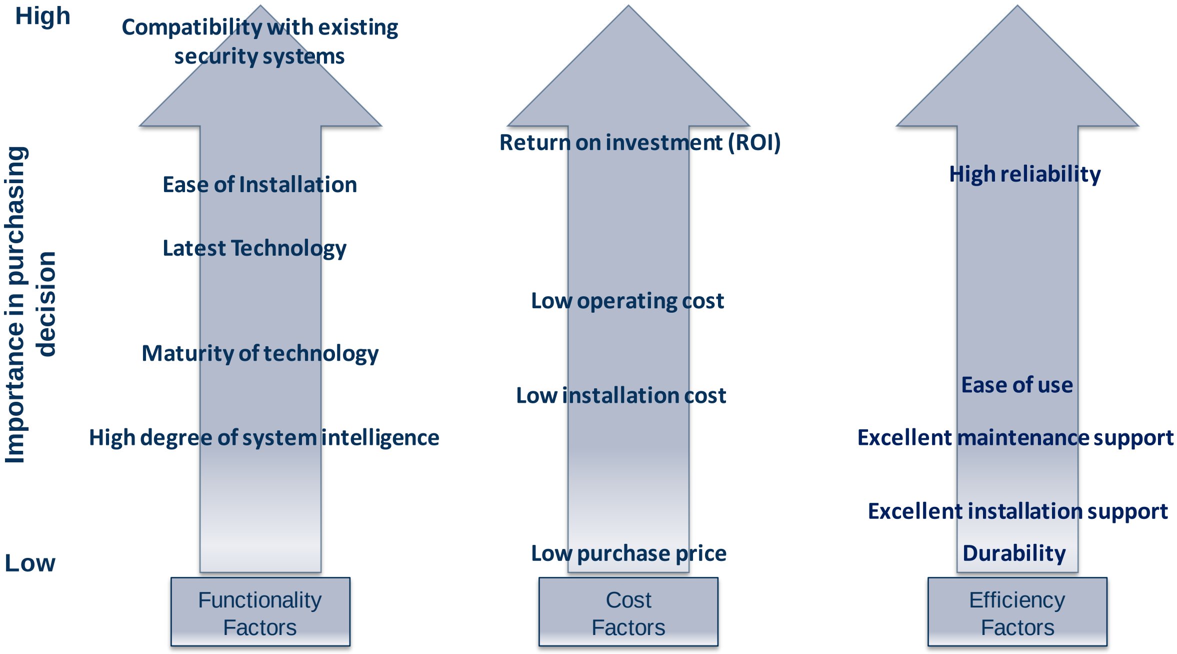
The key challenge that airport operators face is finding a way to provide robust and effective security measures that can prevent and identify the full spectrum of threats while ensuring passenger satisfaction and legislative compliance. This challenge can be segmented into three key end-user requirements:

- **Functionality –** The compatibility of newly procured equipment with existing systems is the greatest consideration for the airport operator. It is vital that new equipment can be easily integrated to fit in to and interact with existing systems to prevent any gaps in security. Furthermore, the maturity and specification of the equipment is also a significant factor in the procurement decision. Operators want modern and effective equipment, but maturity and proven reliability remain high priorities.

- **Cost –** Airport security is one of few markets that has been relatively unaffected by the global economic crisis and expenditure is likely to increase over the coming decade. However, financial consideration will always influence the selection of equipment. Value for money will continue to be a significant driver in the decision making process. Personnel costs comprise the largest proportion of airport security expenditure; however, in some cases modern technology can perform these roles more efficiently and effectively, creating opportunities to reduce cost.

- **Efficiency –** Long queues to get through check-in and passenger screening have been a feature in major airports throughout the world. Airport operators have increased efforts to reduce queue times. However, their primary concern is to ensure that security continues to identify the full spectrum of threats while complying with relevant legislation and without impinging on passengers' rights. High reliability of the equipment and clear identification of any threat is vital.

Airport Security Market: Influences on Purchasing Decision for Video Surveillance for Airport Operators (Europe), 2010



Source: Frost & Sullivan Research

Current Technology in the Airport Security Market

Perimeter Security

Perimeter security provides the first line of protection for an airport area. Large perimeters that have to be secured and monitored present security challenges, especially at major international airports. Technology has shifted focus away from security personnel patrols that were both expensive and unable to monitor the entire perimeter.

Perimeter Intrusion Detection Systems (PIDS) have solved some of these challenges and serve three functions:

- **Deter** any individual or group from gaining easy access to the airport site.
- **Detect** any attempted breech of the perimeter through a range of different sensors, identifying vibration, noise, or fencing breaches.
- **Delay** and monitor the assailants long enough to dispatch an appropriate level of response - either a security team or police force.

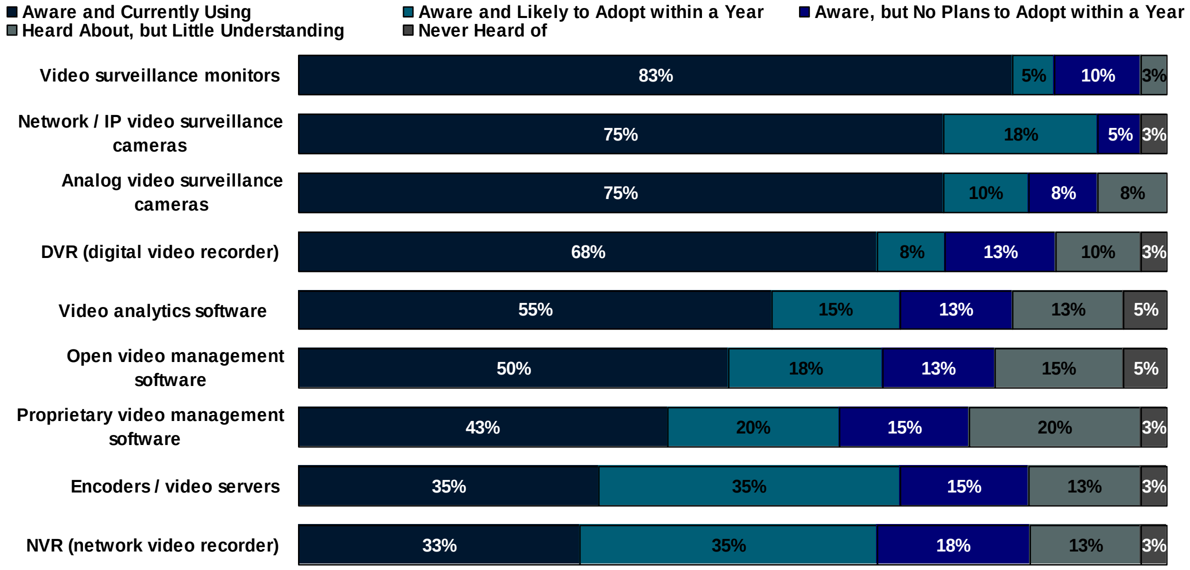
There are a range of different barriers and fences that are available from industry and can form the perimeter boundary of an airport. Chain link fences are the most common for economic rather than efficacy reasons. However, there are also a range of sensors that have entered the market which alert the central control room when an intrusion is detected. Many airports have deployed PIDS which integrate alerts to surveillance cameras that can automatically focus on the sector where the alarm was triggered. False alarms remain the key challenge to perimeter security and industry continues to strive to improve sensors to keep nuisance alerts to a minimum.

One of the most recent and technologically advanced PIDS systems was installed at Changi Airport (Singapore) in partnership with ST Electronics. It is the first time that Fibre Brag Grating sensors have been used in airport perimeter. The Agil Fence PIDS was chosen as it could adapt to its environment and would not be affected by environmental electromagnetic and radio frequency interference, consequently improving detection and minimising false alarms.

Surveillance

Integrated surveillance cameras continue to evolve in airport security. The chart below demonstrates the current usage, awareness, and adoption by airport operators in Europe. It shows that there is still room for growth and expansion in the airport surveillance market.

Airport Security Market: Current Usage, Awareness and Adoption Plans by Types of Video Surveillance Technology (Europe), 2011



Source: Frost & Sullivan research

Integrated systems now commonly use Video Content Analysis (VCA) and real-time analytics, which analyses data as it is recording. As the above chart shows this is an area of video surveillance that will continue to grow. The software recognises any break of the pre-programmed or 'traditional rules', highlights suspicious activity, and triggers an alarm that will appear on the screen in the control room. Personnel in the control room have the opportunity to view the situation in real time as well as instant access to recorded footage of the incident. A potential scenario could be if somebody should leave their baggage unattended, the smart cameras can highlight the package and alert the control room. The controller will be able to see recorded footage of the event to determine the person responsible as well as dispatch the appropriate security response.

Such video analytics are deployed globally in many airports. Schipol Airport in Amsterdam uses such an IP-based system to monitor accidental or malicious intrusion in their runway or hangar areas. Indigo Vision installed over 3700 cameras in an IP surveillance system in Terminal 3 at Delhi airport. The analytics in the system includes 'virtual tripwires' for secured areas and 'abandoned object' highlighting for suspected packages to help improve response to such incidents.

'Terrorist' Cameras

Terrorist cameras are cameras reportedly capable of picking out suspected terrorists. They work on the principle of behaviour screening, in which a passenger's body language is assessed and alerts triggered by specific peculiarities. The analysis covers mannerisms, facial expressions and even excessive levels of perspiration. Central to the technology is an extensive database containing thousands of human actions. The camera is able to decipher 'normal' human actions from 'irregular' action that may be an indicator of hostile intent.

3D Face Recognition Technology

3D facial recognition technology has the potential to be widely adopted within the market. It allows for integration of biometric facial recognition technology with IP-enabled CCTV to accurately identify terrorists and criminals known to the intelligence services. The technology tackles some of the previous challenges associated with integrated facial recognition and surveillance.

Screening

Over the last decade Advanced Imaging Technology (AIT) has significantly improved the identification of concealed metallic and organic contraband materials attempting to pass through checkpoints. However the new screening techniques have raised privacy concerns. Some groups and passengers have even suggested that detailed images seen by security personnel constitute a breach of human rights. In response, much of the screening equipment has now been developed to produce a generic or image-free solution. The image only highlights areas of the body that are concealing contraband material, as opposed to giving the operator an exact outline of the passenger.

Backscatter X-ray Machines

Backscatter X-ray machines have been declared a highly innovative and effective means of finding out whether a passenger has concealed weapons or explosives at the screening stage. In spite of the security benefits, the technology has gained more publicity due to privacy concerns. Advancements have been made to display a generic image that is not intrusive to the individual. However a study released in the 'Journal of Transportation Security' argued that Backscatter X-ray machines may not be as effective as first suggested. Leon Kaufman and Joseph Carlson, two professors from the University of California, San Francisco argue that it would be possible for terrorists to place materials on the body in such a position that it would be very challenging for the machine and operator to pick it up.

Millimetre Wave Portals

A more popular screening solution for airports is Millimetre Wave (MMV) Portals. The technology uses safe radio waves to detect prohibited objects or materials under a passenger's clothes. At inception these machines too faced privacy issues. The EU Parliament warned the technology 'violated the fundamental human rights of citizens'; the US Congress also took a similar view. However manufacturers have managed to combat this in a similar way, by producing a generic image of the body. This solution has now provided an effective alternative to traditional metal detectors, although the cost of the equipment remains high. Implementation of MMV Portals is growing. L-3 Communications Security and Detection Systems have installed more than 240 of their ProVision screening systems in 40 airports in the US with more ordered from the TSA. Prevalence of these portals is likely to increase.

Passive Millimetre Wave Imaging

For many years Passive Millimetre Wave Imaging has been heralded as the great hope for airport security. In theory the passive system can screen a number of people simultaneously from a distance of up to ten meters. The passenger would simply have to walk into view of a millimetre wave camera which would instantly identify whether they had any concealed weapons or explosives, without producing an intrusive image. However the technology has faced technical difficulties and has yet to be perfected. Brijot Imaging Systems have an operational system and are seen as the market leader in this regard. Other companies are also investing time and money in the technology as many believe this could be the solution to airport security in the next five to ten years.

Advanced Threat Detection X-Ray Machines

As with passenger screening, X-ray machines have developed over the last decade. Much clearer images of contents and screening machines that can view baggage in dual and multi-view perspectives are now available. These have become more effective at identifying potentially harmful objects or materials within bags. Smiths Detection, a global leader in the screening market has produced the HiSCAN 6040aTiX. This system quickly provides comprehensive analysis of the contents of baggage-including detection of liquids and explosives-to ensure efficient passenger movement.

Explosive Trace Detection Systems

While X-ray machines have become more advanced and effective, Explosive Trace Detection continues to be carried out manually. These systems can also be deployed to trace narcotic substances and help tackle international drug trafficking. Currently the process is both time and manpower-intensive. Inspection guidelines in the UK instruct that the trace collection be focussed on specific areas of the bag rather than its full content, consequently increasing queuing times. Only one in three items passing through the X-ray is selected at random for this inspection.

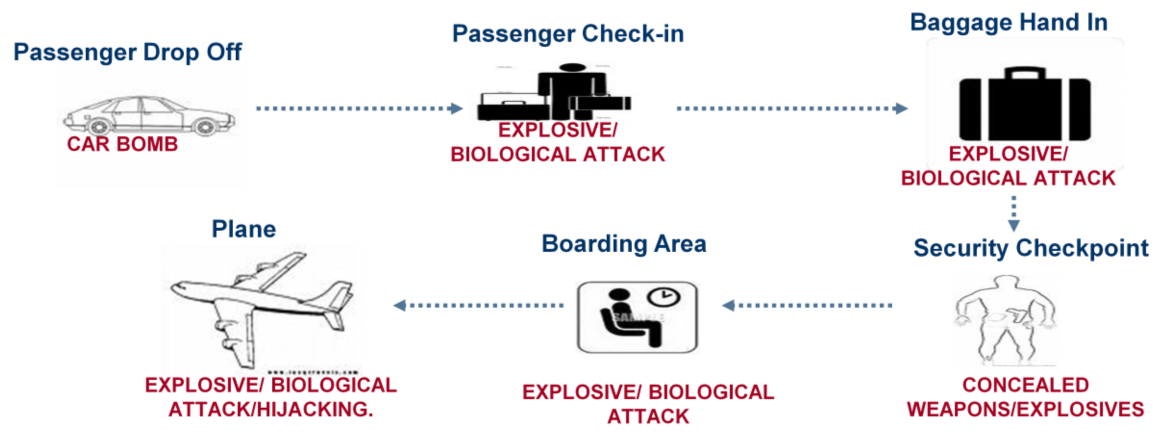
In 2006 liquid explosives came to prominence in the market after a plot to detonate such a device on transatlantic flights was exposed by UK intelligence services. Since then the market has striven to find a solution to accurately and efficiently screen liquids carried through to the boarding lounge.

Nuctech has recently released the LS1516BA Liquid Inspection System, complying with the EU Liquid Explosive Detection Systems (LEDS) Standard 1 Type C. The scanner comprehensively analyses any container and can identify disguised separation and any potentially harmful liquid. However, the new scanner still requires the liquid container to be removed from the baggage and placed separately into a machine. While the scanner is effective, the process is time-consuming and will not help the flow of passengers through checkpoints. Furthermore, competitors are expecting to release LEDS Standard D scanners over the next few years; these will be able to screen liquids even when left in the baggage. Once these enter the market, equipment such as the LS1516BA will be rendered obsolete.

The Technology Gap and New Threats

Reports on all the different technologies and security measures in airports create an uncomfortable environment for those attempting to deceive authorities. However, all the readily available information also means that individuals or organisations with criminal intent know exactly what to expect. This helps terrorist groups to develop new ways to achieve their objectives. The chart below maps the conventional stages of threat and screening in UK airports.

Airport Security Market: Stages of Threat (United Kingdom), 2011


Passenger Drop Off
CAR BOMB
Passenger Check-in
EXPLOSIVE/ BIOLOGICAL ATTACK
Baggage Hand In
EXPLOSIVE/ BIOLOGICAL ATTACK
Plane
EXPLOSIVE/ BIOLOGICAL ATTACK/HIJACKING.
Boarding Area
EXPLOSIVE/ BIOLOGICAL ATTACK
Security Checkpoint
CONCEALED WEAPONS/EXPLOSIVES

Source: Frost & Sullivan Analysis

One of the latest methods that terrorist groups are reportedly attempting is to surgically implant improvised explosive devices in attackers' bodies. Reports of such incidents are limited in number, however in August 2009 Assistant Interior Minister of Saudi Arabia, Prince Muhammad bin Nyef al-Saud (responsible for counterterrorism) was the target of an assassination attempt by Al Qaeda in the Arabian Peninsula (AQAP). Reports suggested the assailant had detonated explosives planted within his body. The implanted device had evaded security checks, including a full screening.

Current technologies deployed in airports would also have been unlikely to have picked this up. Having eluded the technological security checks, the last line of detection that could have identified the threat is security personnel. Although not successful on this occasion, the personnel and human factor remains vital to the security of an airport and still performs functions that technology cannot carry out. Identifying suspicious behaviour and analysing signs that technology is unable to detect continues to be an important security measure. As such, money will continue to be invested in human factors, and specifically the training of personnel to bolster the security at airports.

Another way to approach this problem and to decrease queue times at security checkpoints is to increase pre-screening. At the beginning of October 2011 the TSA began 'PreCheck', a pilot programme that thoroughly pre-screens passengers' details in four US airports, enabling authorities to make an intelligence-based risk assessment. Frequent flyers who volunteer to provide more information may then be directed to an expedited security process at the airport. The pilot project has been implemented after public concern over queue times and the invasive nature of screening methods, including pat-downs. Despite all the advances in technology, this signifies that the best way to secure the airport is to identify threats before they reach it. Of course, this will not always be possible and the pre-screening programme only identifies a very small percentage of passengers; however, current security systems can help bridge the gap.

Airports remain a target because of the prestige and level of devastation or impact that an attack can achieve. Technology and security systems have always striven to stay one step ahead of the potential threats. They have now reached a position which challenges those with criminal intent to be one step ahead. While security can never be 100% effective, further investment, innovation, and advancement in airport security technology will continue to make it very hard for such groups and individuals to carry out attacks.

About Frost & Sullivan