

# AVIATIONsecurity

international

The Journal of Airport & Airline Security

JUNE 2005 : Volume 11 Issue 3

ISSN 352-0148 USPS 010-807



## General Aviation: the next challenge

**G8 Summit Security:**  
an aviation perspective

**Passenger Profiling:**  
dispelling the myths

**SAFE:**  
a European solution for airborne security

**Integrated Products:**  
the continuation of  
technology development

Sponsored by:



**communications**

**Security & Detection Systems**

[www.L-3com.com/xray](http://www.L-3com.com/xray)



# Futuristic Avsec Available Today

by Philip Baum

**A**round the globe, scientists, academics and visionaries are hard at work developing the next weapon in the aviation security industry's arsenal to combat criminal attacks.

Manufacturers are investing in enhancing their own equipment's detection capabilities and throughput rates, whilst striving to reduce false alarms. Regulators are spending public funds in private coffers where there is reason to believe that a huge leap in technological capability is around the corner. And, inventors are traipsing around trade shows, surfing the internet and capitalising on friendships as they go in search of funding for the realisation of their dreams.

However, what do we really want from the airport or airline security system of the future? The simple answer is total protection from all known threats. Given that, in all reality, that is unachievable, we are left with the task of minimising the number of ways in which those with bad intent can circumvent our defences.

Before we look at which technologies we actually want to deploy, we need to be clear about what we wish our security system to be able to identify or prevent. An effective aviation security regime is one that can identify individuals who may pose a threat to either a given flight or to airline/airport facilities and then neutralise that threat in a timely manner.

Gone are the days where we could safely assume that our mission was simply to prevent hijackers, armed with guns and grenades, from boarding flights. We've achieved much success in that area, given our deployment of X-ray machines and metal detectors at passenger screening points. Small wonder that such incidents are now few in number.

We still have, however, a large number of other incidents taking place around the globe. Incidents that cannot be prevented with the technologies currently deployed.

Let's consider what I believe to be the five most significant attacks against aviation since 11 September 2001:-

- Richard Reid's attempt to blow up an American Airlines flight in December 2001
- the missile attack on an Arkia jet in

Mombassa in November 2002

- David Robinson's attempt to hijack a Qantas flight en route to Tasmania in May 2003
- the simultaneous bombing of two Russian airliners in August 2004
- the attempted hijacking of a Kato Airline flight in Norway in September 2004

The most worrying fact about these incidents is that in four out of five cases, the perpetrators were suicidal (those targeting Arkia didn't even need to go to the airport). Furthermore, in only one case (Kato Air) might the incident have been prevented by the aforementioned technologies that are standard issue at most airports.

I don't think therefore that it is too much to ask that our aviation security system reflect this trend and embrace those technologies that are better suited to identify the suicidal individual, be the cause terrorism or mental instability.

At the same time we must reflect on the other major criminally instigated cause of death and injury at airports – airport bombings and check-in attacks. In recent years, including this April in Hat Yai, Thailand, we have witnessed significant incidents in Spain, the Philippines and the United States, and we have been forced to address the dilemma of screening, not only the passengers, but all those who may wish to enter aviation facilities.

It is also only a matter of time until the two combine together and we bear witness to a suicidal attack on an airport.

One glance at Air Watch in this issue will illustrate some of the other recurring problems to which we have to respond. There have been a worrying number of acts of civil disturbance, especially in South America, where it would appear that protestors have ended up demonstrating on the runways of international airports. So much for sterile zones! Meanwhile, the actions of disruptive passengers continue to plague the industry on a daily basis. Often an issue distanced from aviation security discourse, yet a problem that definitely compromises the security of a flight.

The absence of other forms of attacks, such as aircraft sabotage via checked luggage or cargo, should not undermine our efforts to

prevent them from happening. Yet, we must ask ourselves the question why so much effort and investment is being channelled into one area and so little into others.

Given the above and our need to create a comprehensive security system in which our airlines and airports can operate, perhaps now is the time to look to the future and consider what technologies we would like to see deployed. In doing so, whilst security is a fundamental requirement, we must also ensure that we don't create a military environment where it becomes unpleasant to fly.

If our system must ensure that passengers themselves are not knowingly a threat to flights, then we need to acknowledge the necessity of screening them for non-metallic weapons. News of the recent trials of passenger X-ray technology, such as Rapiscan's Secure 1000, is extremely encouraging. It would appear that some customers are even buying the system. Whether we opt for X-ray or millimetre wave or some other advanced screening technology, we need to see beneath people's clothing! And, in the checkpoint of the future, we need to combine the technology with both explosive and metal detection capability.

Let's not restrict our focus to screening people in portals. There are a number of other innovative ways of determining whether a person poses a threat to a flight or not. The sceptics amongst you might not like the idea of gait analysis, whereby a computer can tell by the way somebody walks whether or not they have positive or negative intent, nor may you embrace the idea of facial analysis that can identify heat spots on the face or brow that might indicate undue stress, but the ever-cautious banking industry is not ridiculing such technologies just yet. After all, it is the credit card companies and other financial institutions that are already using voice stress analysis (voice pattern recognition) to determine whether a telephone caller is telling the truth or not. Indeed, some form of polygraph (lie detector) test is really the answer to our dreams. We have the technology to enable check-in staff to assess a passenger's intent. Immigration and customs officers would benefit too. We can do

all this without having to determine the exact nature of the threat, as it could even identify the passenger intent on hijacking an aircraft with a shoelace or knife from a meal tray – the passenger who would breeze through airport security checkpoints but remain a threat.

There have been huge advances in the screening of checked luggage in recent years. New approaches are constantly being mooted but we are primarily talking about refining existing technologies. However we have yet to seriously address the issue of screening such baggage for chemical, biological, radiological or nuclear weapons. Again, the technology exists, but it is not being deployed. Of course, if we trusted the passenger, we would not be so bothered about their luggage.

As has been widely reported in both the trade and general press, the screening of air cargo is woefully absent from most airports. Novel approaches, including the resurrection of old-fashioned techniques such as the deployment of canine detection teams, can and should be part of our basic screening system. Whether we opt for PFNA, TNA, stoichiometry or simply adapt explosives detection technology to the cargo environment (as in the case of the shake 'n' bake system), to do nothing is a neglect of duty.

From an airline perspective, we are likely to see new aircraft fitted with countermeasures, either infrared or flare-based, to reduce vulnerability from a surface-to-air missile. However, a retrofit of existing aircraft is unlikely. As an alternative, we may well see airports and air traffic control authorities purchasing software tools. One example is Rontal's SimGuard which can predict the likely launch sites of missiles, based on aircraft type, local topography and meteorological conditions, enabling the authorities to either deploy foot patrols appropriately or alter the arrival or departure corridors of the aircraft.

Whilst, in this editorial, I have made every effort only to focus on technology-based solutions, when faced with the problem of the disruptive passenger, restraint kits aside, I'm afraid that the answer is all about human factors: the training of aircrew to react both verbally and physically to a wide range of potential scenarios. Training that currently, in many cases, is non-existent.

I have left the hardest part to last. We have the technologies to screen passengers and all that goes onto aircraft, but ensuring security at the airport itself is a huge undertaking. All the measures taken elsewhere are worthless unless we can guarantee that only authorised personnel have access to restricted areas of an airport and only persons with good intent gain entry to even the public areas.

Monitoring of public concourses by CCTV

equipment, nowadays enhanced with threat detection software, airfield demarcation by climb-proof fencing, enhanced by perimeter intrusion detection systems, and staff screening systems now resembling passenger screening checkpoints, are a start. But, given the number of people who need daily access to airports and the impossibility of effectively screening the tools of their trade (it's beyond me why we use mirrors to search the underside of vehicles, or run mechanics' toolboxes through X-ray machines!), our efforts must be concentrated on ensuring that, at the time of appointment, we are convinced that the staff we are employing to work in restricted areas pose no threat. It is frightening to read report after report about staff employed at airports who are part of criminal gangs, or have invalid identification papers or have questionable backgrounds. What use an access control system based on biometric

identifiers if the people we are registering on the system are a threat?

It's all too easy to say that this is one of the realities of the airport life and that there will always be some bad eggs. However, if we believe we can effectively screen millions of passengers worldwide and prevent hijackings and bombings, then we must make it our responsibility to certify all those who can endanger the effectiveness of the programme. Maybe this is one other area where the polygraph test could again come into play?

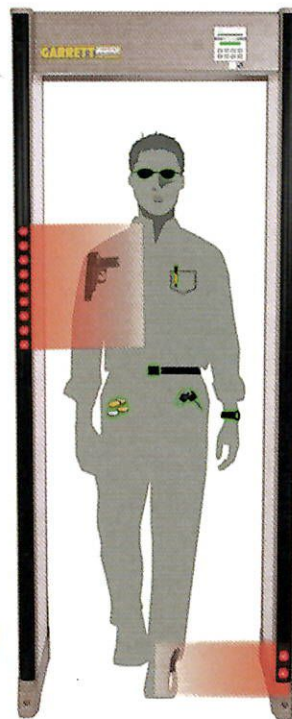
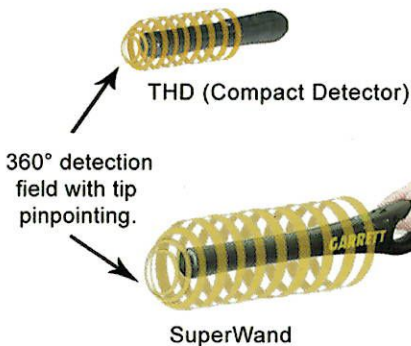
Technology is key to aviation security. Yet from a deployment perspective, there are more technologies on display at the trade shows than are actually in regular use in airports. For too long we've been considering futuristic solutions. It's now time to deploy them. Cost? I'm not sure. But, the cost of our not doing so is higher still...

## Others detect metal. We **PINPOINT** it.

Close isn't good enough when it comes to locating potentially harmful metal weapons. That's why Garrett Metal Detectors offers you advanced pinpointing technology in the PD 6500i walk-through metal detector as well as the SuperWand and new, compact THD hand scanners.

Don't let another harmful metal pass you by. Let Garrett help you pinpoint the danger!

Call or visit us online today!



**GARRETT**  
METAL DETECTORS



Tel: 1 972 494 6151  
Web: www.garrett.com  
Email: international@garrett.com