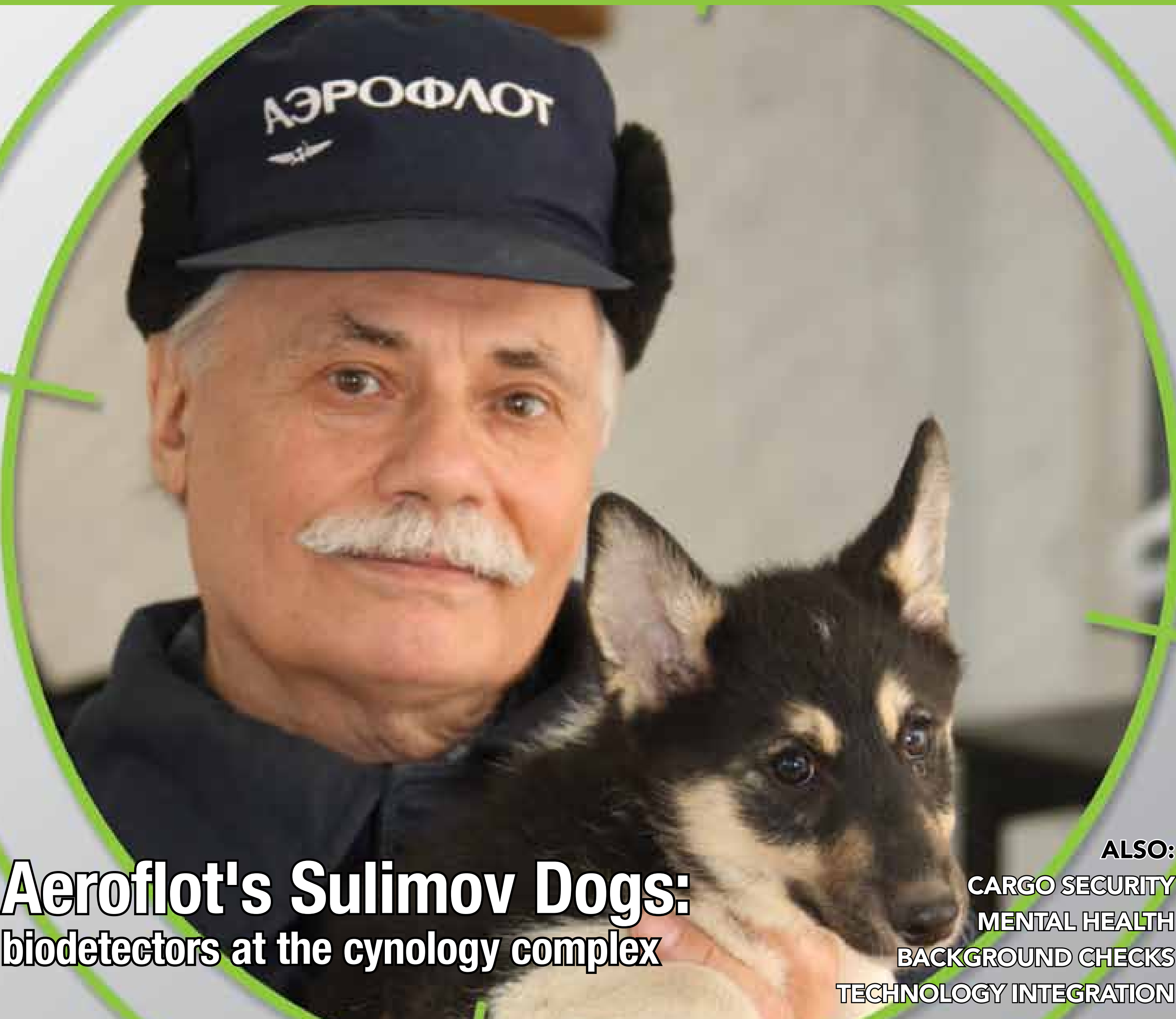
AVIATION SECURITY INTERNATIONAL

www.asi-mag.com

THE GLOBAL JOURNAL OF AIRPORT & AIRLINE SECURITY



Aeroflot's Sulimov Dogs:
biodetectors at the cynology complex

ALSO:
CARGO SECURITY
MENTAL HEALTH
BACKGROUND CHECKS
TECHNOLOGY INTEGRATION

MEDIA SPONSOR TO:

Asia-Pacific AVSEC 2011
Canberra, Australia

PROTECT 2011
Manila, Philippines

COUNTER TERROR EXPO
London, UK

International AVSEC Conference
Hong Kong

DECEMBER 2010 VOLUME 16 ISSUE 6

CARGO BOMB PLOT
SEE PAGE 18

INDUSTRY NEWS
SEE PAGE 42

INTEGRATED SECURITY SCREENING SOLUTIONS: joining the dots

Since the destruction of Pan Am 103, aside from the latest cargo bomb plot, virtually every terrorist attack has been executed via the passenger-screening checkpoint. It seems that the knee-jerk reaction to plug the latest exposed gap is to add another new technology or process to the existing mix of systems. We remove our shoes, dig out our laptops and decant liquids into tiny bottles. "New" systems are pushed into the field, creating confusion for passengers and operators alike. What never seems to be addressed is the fact that the underlying security strategy needs an upgrade. Steve Wolff assesses how the screening process can be enhanced through the analysis of data and the integration of technologies and processes.

The number of terrorists who, since 1994, have succeeded in smuggling items through the checkpoint has proved that a fundamental overhaul of the screening process is now due. The facts are that Ramsay Youssef, Richard Reid, the Chechen "Black Widows" and, most recently, Umar Farouk Abdulmutallab, all beat the checkpoint process. While we've forced them to use (for now at least) more dangerous homemade explosives and less reliable components, these have greater detection challenges especially when combined with cleverly concealed Improvised Explosive Device (IED) components. And that is before they turn to concealment methods that drug smugglers routinely use today.

The checkpoint screening process is much more challenging than hold baggage, yet technologies which are considered unsuitable for hold baggage screening are being embraced at the world's checkpoint lanes. Checkpoints have to contend with disassembled bomb components as well as conventional weapons, none of which have to be carried onboard by the same individual. The threat from knives and other non-projectile weapons has been dramatically reduced thanks to improved cockpit protection and air marshals, not to mention passengers, yet we still ban pocketknives.

The basic strategy in use today was designed to counter the 1960s "Take Me to Cuba" style hijack threat and has not evolved to counter today's dangerously intelligent terrorists, who use explosives and bomb components that are way more sophisticated than the "dynamite and alarm clock" bombs that until recently were included in the "modular bomb kit" for X-ray systems. A good analogy is that we are using early 20th Century manufacturing to try to compete in the 21st Century: today's process treats all passengers the same way and screens on a bag-by-bag and passenger-by-passenger basis, with little or no attempt to integrate and use the information we collect in the next part of the process.

The bolt-on strategy is risky and costly. Aviation security history is replete with technologies that have been rapidly deployed only to fail when it comes to widespread use. Thermal neutrons, trace portals ("puffers"), Quadrupole Resonance systems and cast/bandage scanners are several that come to mind. These technologies could add significant security value if they are appropriately integrated into a systems-based approach. The jury has yet to decide on the security value of millimetre wave and backscatter X-ray-based body imaging systems (AITs) given that, being non-penetrating, there remain body locations where threats can be concealed. If current deployment plans proceed without addressing these operational liabilities, AITs may be one incident away from similarly falling out of favour. A growing opinion is that our underlying passenger screening strategy is outdated, has not evolved with the times and that new scanners are unlikely to counter such threats by themselves. An intelligently integrated combination of data along with new procedures and different devices - including technologies that were prematurely abandoned – is urgently needed. Another problem that needs to be addressed is that much of our checkpoint process is still visible, making it easy for terrorists to study and defeat; as recent attempts have shown us.

Even before Abdulmutallab almost succeeded in destroying NW253, several independent security professionals in the US joined forces to consider how to update the checkpoint to the needs of the 21st Century. Consisting of former US government officials, executives of technology development companies,

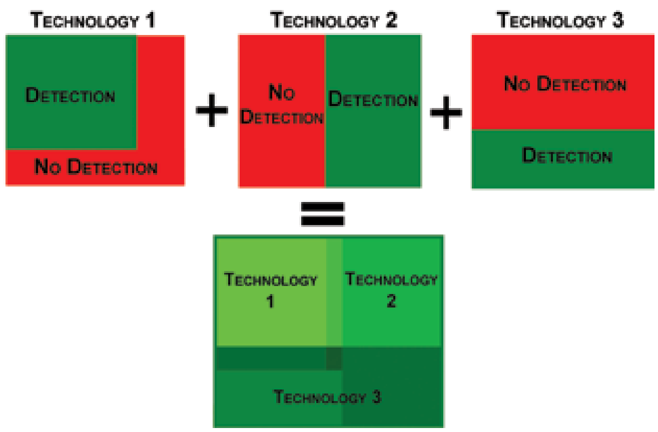


Figure 1: Combining complementary technologies compensates for detection gaps, allowing high levels of detection to be achieved.

airline security managers and airport police officials, the group agreed on several key principles for a new checkpoint strategy:

- Not everyone can be screened to the level needed to find today's sophisticated terrorists, nor is it necessary. Risk-based criteria should be established for pre-screening and segregating passengers into elevated risk, low risk and normal lanes under standard and heightened threat conditions
- An elevated risk lane must include a combination of technologies that are suitably integrated to compensate for each other's weaknesses. Specifically, data integration of pre-screening, scanning technology data and operator decisions is more important than physical cramming different technologies into a single box
- To counter team-based attempts, a method is needed for consolidating and reviewing stored security information on a flight-by-flight basis after passengers have passed through security, coupled with a procedure for resolving any remaining concerns prior to boarding. At a minimum, this should be applied to elevated risk passengers.

The term "integration" can apply to both "physical integration" and "data integration". The need arises as there is no single technology that can do everything, the oft mentioned but elusive "silver bullet." Physical integration is the incorporation of multiple technologies and procedures into a single process. This can be achieved either by using individual devices or by designing multiple technologies into a single shroud. The latter is more difficult to accomplish, as it requires accommodating the different technologies' (sometimes) conflicting needs and, unless well designed, can limit important attributes, such as throughput. Data integration offers the potential to use different technologies without physically combining them into a single box while offering the advantages of a multi-technology approach to an inspection task. It has its own challenges, not least being increased space and the need to track the item being inspected through the various components, but it has the advantage of being flexible and adaptable.

Physical Integration

Key to any integrated detection system is the use of complementary technologies. By appropriately combining systems with different detection strengths and weaknesses, an integrated system can achieve high levels of detection. Figure 1 (opposite) shows how this might be achieved. This is not as far away as it might seem. There has been substantial progress on many areas since 2002, which can be leveraged to provide a solution.

After 9/11, Rapiscan along with the forerunners of Morpho Detection (InVision Technologies, Inc. and Ion Track) joined forces to implement and test the first integrated passenger screening system, known as the Advanced Technology Screening Checkpoint (ATSC). It consisted of an array of complementary technologies for both passengers and bags and addressed the challenge of combining them into a passenger-friendly, operator-usable system.

The ATSC allowed its developers to understand and fully integrate other critical aspects of the inspection process, such as inspection protocols, operator selection, operator training, and motivation. A critical

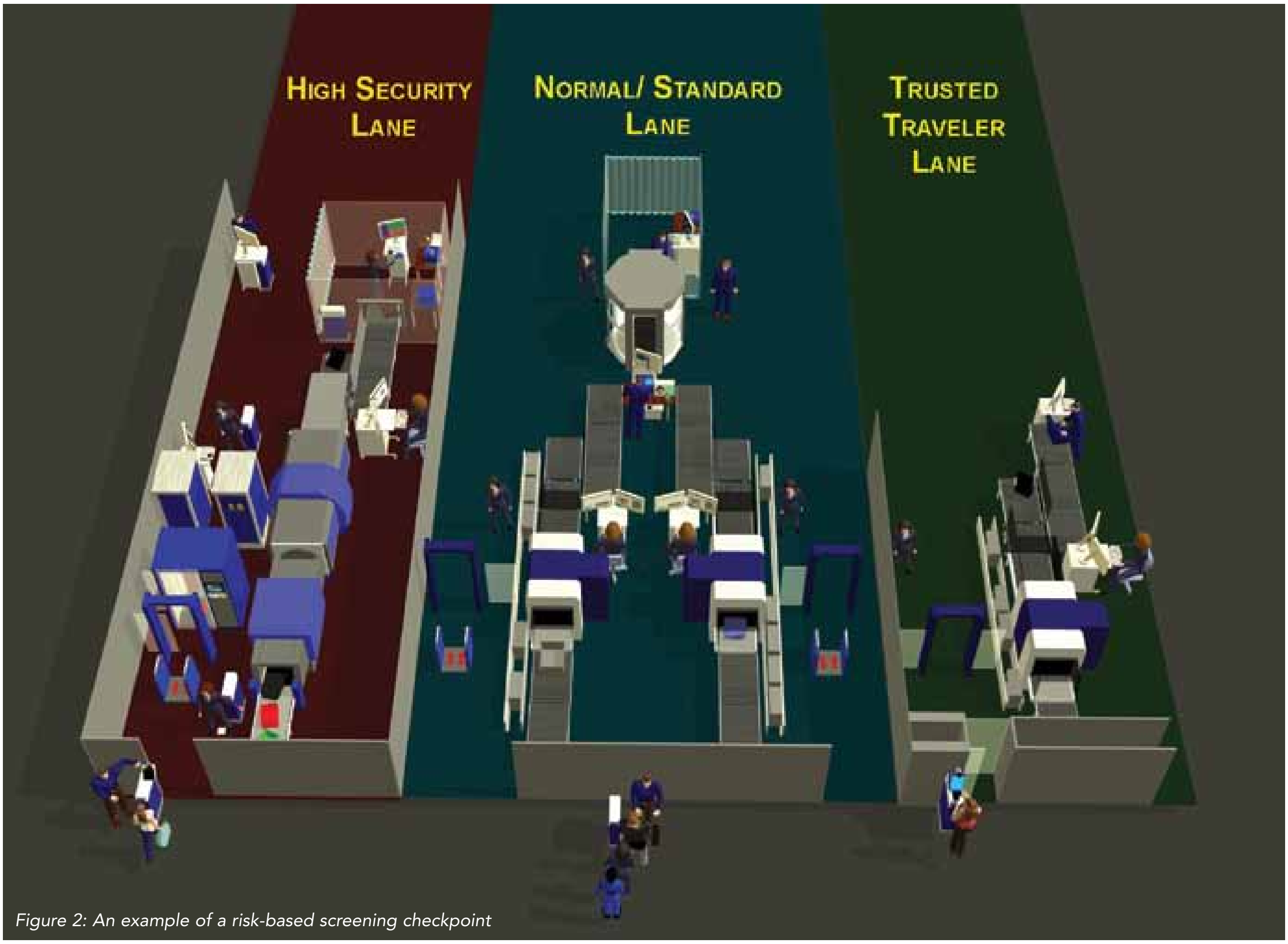


Figure 2: An example of a risk-based screening checkpoint

discovery was that a single inspector needed to see all the information obtained from all devices - including operator decisions - for every passenger and their bags prior to making a final clear or reject decision. Ideally, this information would be consolidated on a single screen (an example of "data integration"). The manufacturers worked with the US National Safe Skies Alliance to trial the ATSC against a 2002-era TSA-style checkpoint for six months at Orlando airport and then tested it using live explosives (with quantities similar to those used by Reid and Abdulmutallab) and other weapons. This work led to two patents for what is now Morpho Detection on the physical process and combining the data into a single user interface. Since then, new technologies and improvements have become available and regulators are taking active steps to deploy them, but not as part of an integrated system.

The proof that this strategy works came out of the 2003 ATSC National Safe Skies Alliance trials. In side-by-side comparison with the TSA checkpoint lane, the ATSC achieved several times better detection especially on different types of explosives even down to the small threat masses, though it was 50% slower. This proved that careful integration of imperfect technologies available today could achieve the same levels of detection as a hypothetical "silver bullet".

"...trusted travellers do not need the same level of physical search as passengers that appear on a government watch-list..."

Data Integration

Data integration offers additional advantages. As more devices and threats are added to the checkpoint, the inspection process becomes more complex and confusing for operators, requiring data to be managed, analysed and presented efficiently and effectively. Capable - though imperfect - scanning technologies exist for passengers and baggage. Likewise, computer systems, networking, analysis and database management tools are all mature, low cost technologies extensively used to integrate business data.

Several efforts have already been made to apply these tools to security. Airline information was consolidated, analysed and used in the 1990s in the US by CAPPS (Computer Assisted Passenger Pre-screening) to direct higher risk passengers' hold bags to explosives detection systems. A few years ago, the US National Science Foundation funded development of SecuriFlo, a system which used hardware and software to collect data from the various checkpoint scanners, correlate them with real bag and passenger images, assemble a passenger security record and store it in a database for use by secondary searchers and auditors. It used commercial off-the-shelf components - computers, image frame grabbers, photocells and cameras linked into a computer network, designed to be manufacturer independent by requiring only superficial attachments to each scanner. SecuriFlo was partially tested in the US and the UK but it lacked priority compared to the bolt-on approach being explored for liquids and AITs. More recently, the US DHS has funded SPAWAR, a communications arm of the US Navy to complete an integrated checkpoint programme and has embarked on common standards (STIP) for image data.

Putting it Together

Sometimes, it is easy to forget that our primary mission is to move passengers rapidly and safely around the world. All stakeholders frequently see security as an increasing impediment to that mission. We must move away from the "one size fits all" approach, as it is not practical to physically screen everyone to the high levels needed to find today's threats.

Software can mine and process existing intelligence data and available airline information to pre-sort passengers into one of three categories without resorting to "profiling". Today, airport workers go through background checks and have full access to aircraft and bags that have already passed through security. The US DHS uses Global Entry, a trusted traveller programme that allows passengers entering the US to bypass long lines and personal interviews at immigration. Such travellers should not need an extensive outbound physical search either. Likewise, governments keep tabs on potentially suspicious travellers via terrorist watch-lists and this information can be combined with a version of CAPPS, perhaps behaviour detection and a random selection element to pre-sort passengers. This process has worked; it thwarted the liquids plotters, identified the Shoebomber and the Times Square car bomber. Arguably, it could have caught Abdulmutallab, too. The process failed because this information was not integrated with the passenger checkpoint process, which allowed him on the aircraft.

> **"...only detonating mechanism failures along with heroic passengers and aircrew have prevented more catastrophes..."**

We can then intelligently prioritise how to apply different screening intensities to passengers based on their risk. Trusted travellers do not need the same level of physical search as passengers that appear on a government watch-list. This approach would allow the deployment and use of thoughtfully integrated advanced technologies and procedures on those passengers that warrant it. A much faster screening process for trusted travellers and an intermediate, less cumbersome process for everyone else can offset the higher cost of screening higher risk passengers. Such an approach would add true security and make more sense to travellers and security providers alike. Figure 2 (p27) shows what a risk-based checkpoint might look like.

However, a fundamentally new process is needed to deal with terrorist teams. This process would consolidate and sort data from the high security lane by flight number. A dedicated, highly trained inspector would use the extra time between security and boarding on a complex task that looks across different elevated risk passengers' data for IED components that might be distributed among different passengers and bags on the same flight. If something is suspected, a mobile security team would be sent the relevant data (likely on a portable display screen) and would intercept the passengers at the gate, interview and re-screen them in a nearby room or possibly at the gate before either allowing them to board or referring them to law enforcement.

To implement flight-based screening, boarding card and government ID scanners would be used to store flight and passenger data alongside the elevated risk lane scanner information in a database. Retrieval and display software would be developed for the flight inspector to use. Such hardware is available and software development is straightforward. Critical would be the ergonomic design along with selection and training of the screeners assigned to this task.

Several organisations are starting to rethink the checkpoint strategy. The International Air Transport Association (IATA) has long been interested in improving the security process and now has convened a global panel of experts to devise a Checkpoint of the Future that aims to focus on higher risk people rather than solely finding problematic items (disclosure: the author is one of several individuals involved with this effort). The Airports Council International (ACI) and several airports in the UK are investigating both the overall strategy and possible new checkpoint lanes configurations to better handle passengers and their bags. IATA's goals are a passenger-friendly security process where the vast majority of passengers pass rapidly through screening. It would focus extra scrutiny on those passengers who might warrant a closer look. Critical to this effort is good government-industry and international cooperation. In that regard, IATA has held top-level meetings with US Dept of Homeland Security Secretary Napolitano and in October presented this concept to the International Civil Aviation Organisation, which has adopted the principle.

To summarise, today's passenger checkpoint strategy is no longer sufficient. It subjects every traveller – regardless of risk - to an invasive, time-consuming, uniform process based on a 40-year-old screening strategy that has consistently been penetrated by terrorists since 1994. Several aircraft have been destroyed and only detonating mechanism failures along with heroic passengers and aircrew have prevented more catastrophes.

A new strategy based on system and data integration is needed so that the costly, labour and technology-intensive, time consuming measures needed to counter today's sophisticated terrorists and terrorist teams can be applied to a small subset of travellers. This can be done without impacting the vast majority of passengers that do not warrant such scrutiny and who can be screened by simpler, cheaper and friendlier processes. An additional advantage is that it provides a migration path for new technologies and processes. As high security lane technologies mature, they can then be rolled out to the other lanes and new inventions introduced to screen elevated risk passengers. This spiral approach gives regulators the opportunity to monitor and refine new systems on a more limited basis and provides developers an initial small market, along with the incentive to improve their products for wider deployment.

Further, much of the security process will be hidden from terrorists and will be transparent to passengers, most of whom will have a more pleasant security experience that makes more sense than our current, burdensome "one size fits all" approach, which has failed so often over the past 15 years. ■

Steve Wolff has 25 years experience developing and marketing advanced aviation security detection systems and was a co-founder of InVision Technologies. He is co-inventor on several checkpoint integration patents and is consulting with companies and international organisations to promote new technologies and processes at the checkpoint and other security applications.