Technology for aviation security: innovation to improve the passenger experience

Alan Xavier Tan
Vice President, Aerodrome Safety & Aviation Security, Changi Airport Group

The article aims to reflect on the current state of aviation security and to tease new thinking on how we could conduct aviation security differently in the future. Take this as an ideation reading – "dream big, think big, act wisely". As the topic of aviation security is far too wide to be covered in one article, the discussion that follows will centre on passenger screening.

With the series of successful attacks on the aviation system and uncovered plots that aim to disrupt aviation, the International Civil Aviation Organization (ICAO) had revised the Risk Context Statement several times to elevate the risk level for some specific types of threats. Coupled with rapid aviation growth, the sustainability of aviation security is crucial. There is great impetus to make smarter use of technology to create capacity, raise efficiency and even possibly design different concepts of operations for the future.

Airport security for passenger screening – the single layer of defence

The current operating concept has inevitably made the security checkpoint the single layer of defence for the passenger journey. As a result, it is infamous for long queues, inconveniences and being intrusive. Why has the checkpoint become this huge bottleneck? With evolving threats and new modus operandi to conceal threat items, many screening processes and technologies have been added to the checkpoints in the last ten years, such as explosive trace detectors (ETDs), advanced imaging technology (a.k.a body scanners), bottle liquid screeners (BLS) and many other random checks. These add-ons are necessary for airport security but place more demand for airport real estates, increase the cost of operations and manpower requirements and negatively impact passenger facilitation.

To ease the checkpoint congestion, there were attempts to develop a newer concept of operations, such as the Next Generation Checkpoint (the famous three tunnels at one point in time) to allow passenger differentiation and to screen them differently. Such concept continues to thrive on the principle of risk-based security. However, not all concepts can be immediately realised and mammoth efforts to coordinate across different state agencies and industry players would be needed. The Smart Security programme evolved from the Next Generation Checkpoint with huge successes as technology development and concepts such as centralised image processing and CT X-ray were operationalised in stages of tests and implementation, which led to higher screening capacity and less need to divest items for screening. What more can we do to improve passenger screening?

Framing the passenger screening problem statements

By framing the security problem statements, we could consider better use of technology or even allow other technology developers to work on solutions to serve the aviation sector better.

› PROBLEM STATEMENT 1
How to achieve better detection and lower false alarms?
This is the core problem statement for all security screening, which will not change over time. However, can we review the level of detection needed if we improve the risk-based security system?

› PROBLEM STATEMENT 2
How to increase screening capacity and efficiency?
If problem statement 1 is achieved, it could address some parts of statement 2, as re-check and false rejects would be reduced.

› PROBLEM STATEMENT 3
How can we turn more people into "whitelist" and look out for people in the "blacklist"?
By adopting a risk-based security concept, more people can be in the "whitelist", which reduces the need to put in additional measures at the checkpoint.

› PROBLEM STATEMENT 4
How can we develop continuous security that is dynamic and able to react to an evolving threat environment?
The current concept of operations will not address this problem statement. Are there better ways?

Technology to the rescue

Technology is not the solution but how we use technology is the winning formula. How should we steer technology developments towards a more holistic solution to meet aviation security needs? Based on the above four problem statements, we could consider these two strategies (that most people already know):

a) Strategy 1 – Continue the search for better detection capabilities
Continue to look out for and explore technologies that will improve checkpoint efficiency and effectiveness (better detection and lower false alarms). Until we find a more effective concept of operations that can change how security is conducted for passenger screening, we need to continue this search for better technology solutions (addressing problem statements 1 and 2).

b) Strategy 2 – Think outside the box
Explore and use technology to design a different operating concept for aviation security (addressing problem statements 3 and 4). There will be many considerations in such a new concept development, thus the process of ideation must continue if the problem statements hold true.

(1) Extracted from InnerEye website (https://www.innereye.ai/)

Strategy 1
Continue to search for better detection capabilities

Security screening equipment development is ongoing and the recent introduction of the advanced cabin baggage screening system a.k.a. CT x-ray is a huge milestone for aviation security. More machines of similar capabilities will be introduced as detection algorithm continues to improve.

HOW CAN WE INCREASE EFFICIENCY AND EFFECTIVENESS AT THE SCREENING CHECKPOINT?

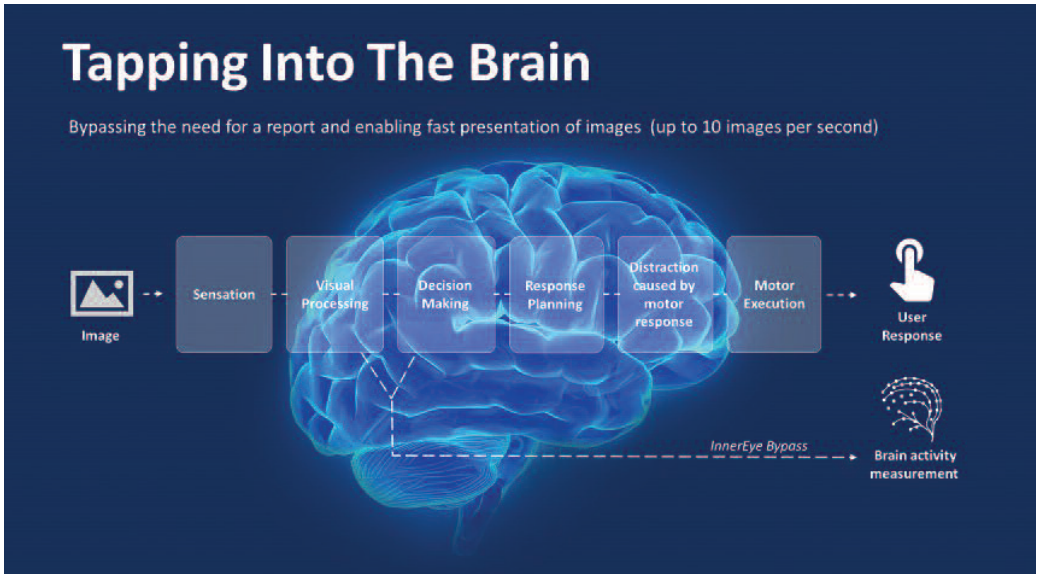
The potential of artificial intelligence (AI) in screening could be the next big thing. Can AI perform faster and better to meet the need of image analysis and classification that is currently performed by security screeners? Do note that image classification is fundamentally different to threat detection algorithm, which is an analytical tool to aid the screeners. In the search for AI technologies for image classification, a product called InnerEye (https://www.innereye.ai/) was introduced by ICTS Europe at Passenger Terminal Expo 2017 and 2018 in collaboration with InnerEye, and this product was also shared at the ICAO High-Level Security Conference 2017.

AI for image classification is a deep-learning model that requires massive training sets of labelled images. In short, for AI to work, the human must first label those images with threat and non-threat items. Deep-learning models will also demand that the data set be continually updated for accuracy and to address new targets. There is great potential to AI but it will take years before it could be fully deployed.

> "Without humans, artificial intelligence is still pretty stupid…"
>
> Wall Street Journal, 12 Nov. 2017

InnerEye's innovative solution combines human and artificial intelligence in one hybrid platform, allowing real-time human-machine interface for fast and accurate visual recognition tasks. InnerEye technology bypasses the need to record overt responses from the user (like button presses or speaking), reading the visual recognition signals directly from the user's brain and combining it, together with the visual data, into a unified artificial intelligence system. This combination overcomes a bottleneck of human performance, as well as capitalises on the merging of human neural processing and deep artificial neural networks (1). What this simply means is that the same operator can now process more images faster in a networked setting. At their trial, human experts can process up to three images per second.

© phonlamaiphoto - AdobeStock

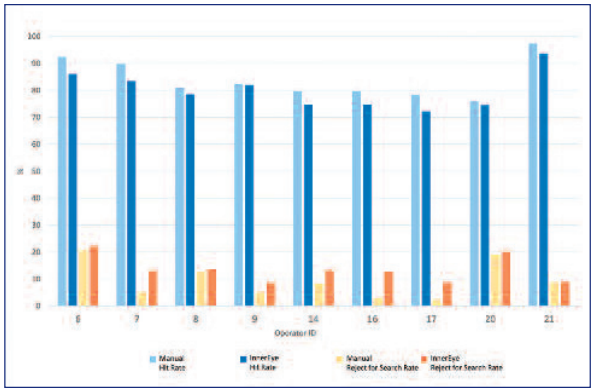


Extracted from InnerEye's presentation

While it is good to process each image faster, the detection accuracy needs to be high. From operational and training experience, we know that every screener has different capabilities and there are blind spots in their analytical capabilities. A proof of concept (POC) was set up between Changi Airport Group, InnerEye and ICTS Europe to establish if image analysis could be faster and more accurate if we could present the same image to a few operators at the same time who have different capabilities. The combined analytical abilities will give better detection and at the rate the brain processed the image, efficiency could still be achieved. Indeed, the results from the POC were promising and Changi is working with ICTS Europe and InnerEye to refine this technology with a view to deploying it in time.

Strategy 2
Think outside the box

Problem statements 3 and 4 require a rethink of how we conduct passenger screening and a relook at some fundamental principles and assumptions. First, are all passengers a threat to aviation? The answer is "no" as the majority of passengers are bona fide travellers. A threat is defined by its intent and capability and thus far security measures have focused on detecting the "capability" (threat items carried by the passenger) at the checkpoint. It is very hard to detect intent at the screening checkpoint due to the high passenger numbers and the time available to make such assessment.



PROMISING RESULTS
Following the successful creation of operator's brainwave EEG, image screening was reduced from 5 seconds per image to 0.5 second and the POC demonstrated potential for combined operator screening (higher hit rate and lower false alarm).

HOW CAN WE BUILD A "WHITELIST" OF PASSENGERS?

If we do not want to treat every passenger the same, we need some ways to differentiate them. Security vetting of passenger information has been used to effect border clearance, and passenger enrolment programmes such TSA's pre-check are available to differentiate passengers for screening – but cover only a small portion of travellers. For these groups of trusted travellers, a reduced security check is applied. There are practical considerations to using passenger data due to privacy challenges and the huge amount of resources needed for the administration of enrolment programmes.

Fast forwarding into the future, how can technology help to build a case on an individual's propensity to commit a nefarious act (how to detect intent?)? Can behavioural science and analysis be used to assess an individual's intent? Technology for facial detection, mood detection, extreme motion detection and body temperature detection are tools which could be combined to provide an assessment of an individual's propensity to commit a nefarious act. If trigger points to

behavioural changes are added into this dimension, e.g. presence of security personnel or robots with overt surveillance, it could trigger a natural response in physiological ways in someone who is planning or about to commit the nefarious act, due to fear and anxiety. If we couple this with stand-off threat detection capabilities to remove larger threats like arms, weapons and improvised explosives devices (IEDs), it is possible to provide an assessment of whether a person is a threat (intent + capability). This will be a new security layer that complements security screening. At this stage, it could be hypothesised that the majority of passengers are already "whitelisted". The challenge will be building a policy and an assessment tool for this to determine that the person is not an immediate threat.

HOW CAN THIS ASSESSMENT BE MADE DYNAMICALLY AND CONTINUOUS THROUGHOUT THE PASSENGER JOURNEY?

It will be a very powerful application if we could track persons who have not been "whitelisted" throughout the passenger journey. The use of facial recognition and attire recognition could be an effective mode, as we are dealing with someone who has presented themselves physically at the airport and therefore the facial and attire recognition is current. This is different from trying to use facial recognition to identify persons of interest (POI), which could produce significant false alarms. Should POIs be detected, or the person is highlighted as a threat concern, continuous tracking and assessment of the persons could take place. For instance, someone who appeared to be angry and had huge movements when they first arrived at the airport could have calmed down after checking in. Their behaviour could have been driven by stress: late for check-in or just had an argument with someone prior to arriving at the airport. The continuous tracking and assessment of such individuals could then help to reduce their threat level and so they would eventually be "whitelisted". For those that remained a concern, an enhanced process could be introduced to intercept them for questioning, or enhanced checks could be conducted at the checkpoint. A final security assessment of the person would be made, and the system could be updated by the security personnel for that specific passenger.

WHAT WOULD CHANGE IF WE WERE ABLE TO ACHIEVE THIS WHITELISTING OF PASSENGERS?

If we can build an assessment tool as proposed, the screening of the passengers will start from the moment they present themselves physically at the airport. This new security layer means threats can be intercepted earlier, and we could also turn an "initial assessed threat" to a whitelisted passenger. The assessment tool could also be applied at different stages of the passenger journey to identify changes in behaviour so that intervention can be conducted at the earliest detection of change in threat level.

When passengers are already "whitelisted", the degree and type of checks needed at the checkpoint could be further calibrated and additional random checks could be eliminated. This provides the basis to let technology do more of the screening work as the checkpoint screening could be more algorithm-based to look for IEDs and specific prohibited items only. To push this concept further, if we can include passenger data for vetting as part of this physical threat assessment process, even if a passenger is found to have brought along his Swiss Army knife, there is no need to remove it as the passenger has no propensity to commit a nefarious act.

Conclusions

The security checkpoint problems will not be solved easily, thus the need to continue to search and use better equipment and technologies to address the challenges. We should not limit screening capabilities to just screening equipment and detection algorithms. The human capabilities must be maximised to respond to emerging threats.

Nonetheless, it is untenable to continue to rely on the security checkpoint as the single layer of defence. To ensure a sustainable security system, there is great impetus to re-think the security concept to "whitelist" more passengers from the moment they arrive at the airport facilities as a new layer of defence. If the aviation security threat is presented from the moment it set foot at the airport, the earlier we can detect it, the better we are at preventing the next successful attack. This layer can also serve to improve landside security since the threat assessment starts from the public area. To sum it up, we must seriously consider leveraging on a combination of technologies to develop a multilayered and more robust security system for the aviation system to grow safely. There is no silver bullet in any single technology solution today. ■

As Vice President Aerodrome Safety and AVSEC in the Changi Airport Group (CAG), **Alan Tan**'s responsibilities include directing, planning and coordinating security operations, aviation security policies and compliance. He is responsible for implementing security enhancement and developmental projects, managing the contracted security services, undertaking aviation security audits and inspection and promoting security culture and awareness. He also works with different regulatory entities to ensure CAG meets the security requirements to support Changi's infrastructure developments and passenger services projects. He is the immediate past chairman of ACI World Security Standing Committee and chairman of ACI Asia Pacific Security Committee. He is also a member of the SMART Security Management Group. As the SMS manager, he oversees the Aerodrome Safety Unit (ASU) and is responsible for Changi's Safety Management System (SMS). ASU works with different internal stakeholders to ensure compliance with safety requirements to maintain the aerodrome certificate. Under his leadership, ASU successfully achieved the aerodrome re-certification in 2015. Prior to joining CAG, Mr Tan was a senior police officer holding various key appointments in his 12 years with the Singapore Police Force.