Smart Security, a joint initiative of the International Air Transport Association (IATA) and Airports Council International (ACI), envisions a future where passengers proceed through security checkpoints with minimal inconvenience; where security resources are allocated based on risk and where airport facilities are optimised, thus contributing toward an improved journey from kerb to airside. Guido Peetermans looks at the progress being made and reports on innovations that may soon be coming to an airport near you.

Airport security checkpoints are a critical element of the aviation security system and, in the face of an ever-evolving threat picture, authorities and front-line staff are working hard every day to stay ahead of people with malign intent.

That doesn’t mean though that security measures necessarily have to be disruptive to efficient airport operations or a major stress factor for the passenger. In fact, it is entirely within the realm of possibilities to design checkpoints that are highly effective in detecting threats while at the same time processing higher numbers of passengers and reducing the hassle factor.

Under the Smart Security programme the International Air Transport Association (IATA) and Airports Council International (ACI) have been working with forward-thinking governments, airports, airlines and solution providers to demonstrate the viability of innovative concepts and technologies that will contribute to more effective security, increased operational efficiency and enhanced passenger experiences.

For most passengers the idea of passing through airport security with minimal interruption may appear to be far removed from everyday reality but great strides have in fact already been made to turn this compelling vision into reality and a new wave of innovations is on the verge of maturity.
Traditionally, passenger screening processes focused mostly upon the detection of metallic threats using walk-through metal detectors (WTMDs). In many jurisdictions these have now been supplemented with manual pat-downs and/or additional measures such as explosive trace detection (ETD) swab tests.

Security scanners provide a readily available alternative that addresses metallic and non-metallic threats in a single process while better respecting the privacy of passengers, thanks to the anonymised format of images and automatic target recognition that allows for targeted searches and thus reduces the need for full body pat-downs.

Smart Security trials have demonstrated that up to 240 passengers per hour can be processed with a single security scanner in a sustainable manner. Through the utilisation of multiple resolution screens this number can be increased. Hence, in most operational environments, this type of equipment can be deployed as primary screening device without negative impact on throughput.

Where higher throughput is required or where other factors come into play, these systems can be deployed as a secondary screening method. Either way they will increase the detection capability compared to a conventional setup with WTMDs without negative impact on operational efficiency and while enhancing the passenger experience.

Over time, detection capabilities will further improve while false alarm rates will drop, due largely to the evolution of detection and decision support algorithms. We expect to see standards emerge that will enable decoupling of hardware and software which will spur even more innovation in this area.

Due to current limitations of some passenger screening equipment in some jurisdictions, passengers still need to remove their shoes for screening. As simple as this requirement might seem, it negatively impacts passenger experience and is disruptive to the process. With the emergence of new technologies, such as non-touch ETD, it should be possible to find an effective solution to this problem.

In the longer term the combination of different technologies into a single piece of screening equipment will open the door to material discrimination (i.e. detecting the nature of the objects found) and an overall improved detection capability in the face of ever-evolving threats.
Cabin baggage screening

Conventional stand-alone, single-view X-ray equipment has been the standard for a long time and the effectiveness is highly dependent on the operators’ training and experience. Multi-view X-ray equipment, which is increasingly prevalent, provides the operator with more information by showing multiple viewing angles of the same bag or tray. The capabilities of these systems are now expanding and are enabling the deployment of advanced equipment intelligence but, thus far, this has not led to a reduction in divestment requirements.

Technologies such as Computed Tomography (CT) and X-ray Diffraction (XRD), which have been used successfully in hold baggage screening, are now starting to make their way into the checkpoint environment and will effectively enable more items such as laptops and liquids to be left in passengers’ bags during the screening process as well as providing more accurate explosive detection capabilities.

In comparison to multi-view X-ray, CT displays the image in a three-dimensional projection that can be rotated freely, allowing the operator to see around objects. This can be complemented with software capabilities like virtual separation of objects, allowing the X-ray operator for instance to virtually ‘remove’ a laptop from the image of the cabin baggage and to inspect the bag and the laptop separately in a 3D view.

Characteristics such as belt speed and false alarm rate of CT systems are rapidly improving and several vendors are submitting their equipment for certification. We expect to see these systems entering operation in the not too distant future.

Checkpoint configuration

Due to the growing number of passengers, additional security requirements and increasing capacity constraints, the pressure is on to keep passengers moving through the checkpoint and to optimise resource utilisation.

By far the biggest game-changer we have seen in recent years is the emergence of Centralised Image Processing (CIP), also referred to sometimes as remote screening, in the checkpoint environment. The conventional setup, where an X-ray operator sits next to the machine to view and analyse the contents of cabin baggage and other passengers’ items as they pass through it, is inherently suboptimal and often creates a bottleneck that limits the performance of the entire system. CIP allows for networking of cabin baggage screening equipment so that the images can be reviewed and analysed by an officer without the need to be physically located next to the equipment. Instead, the officer could be located in another lane (local matrixing) or in a central screening room (remote matrixing). This also opens the door for further optimisation, for instance, by assessing images from passenger, crew and staff checkpoints in a single control room or by centralising across terminals or even across airports in a long distance scenario – provided that the appropriate network security measures are in place.

While CIP has the ability to dramatically increase X-ray image processing capacity, the benefits will be even more substantial when CIP is combined with optimised lane configuration and automation, starting with innovative divest solutions to maximise the in-feed and reduce X-ray starvation, either through automation and optimisation of the conventional linear loading system or alternatively by switching to a parallel loading system. An increasing number of airports are experimenting with the latter which has the added benefit of allowing passengers to overtake one another in the process, thus reducing the stress factor as passengers can take their time to unpack without holding up the queue. Parallel divestment can provide significant benefits even without CIP with some airports reporting up to 20 percent increase in lane throughput using such configuration.
An optimised CIP lane will also require further automation, such as the use of tray handling systems and an automated diverter to ensure that bags/trays that are selected for secondary search are duly separated in the process without the need for human intervention.

Furthermore these lanes will have to be equipped with secondary screening workstations, allowing the secondary search officer to precisely identify what caused the bag to be rejected by the remote X-ray operator.

The performance of such an optimised CIP operation depends of course on the way the system was designed in response to the specific airport’s objectives in terms of resource optimisation versus throughput optimisation but the results observed have generally been impressive. Significant reduction in total passenger processing time – by an average of 30 seconds at some airports – leads to sustainable throughput of well above 200 passengers per hour per single lane (i.e. per X-ray), with one airport even reporting the ability to process over 400 passengers per hour per lane in their particular configuration.

Research being carried out under the Smart Security umbrella has found no evidence that an optimised CIP setup would negatively impact threat detection.

In addition, the networking of equipment yields a wealth of data that can be mined for performance management purposes and to drive further process improvements, ultimately leading to better checkpoint management. CIP also allows for further steps to be taken in terms of equipment intelligence and automated decision making. The emergence of auto clear solutions that can autonomously clear low clutter images without the need for human intervention are a good example of this.

It should be emphasised that CIP is not just a technical solution but a new way of working that may have a profound impact on operating procedures and work processes, workstation design, roles and responsibilities, training and performance management and other human factor elements. The lessons learned from early adopters will be invaluable to facilitate wider implementation.
Unpredictability and risk-based differentiated screening of passengers

If we had advanced screening technologies able to detect threats with high accuracy yet with minimal disruption to the process and a low false alarm rate, and if such technologies were economically viable, we would equally apply them to all passengers and be done with the job.

However, as such technologies are unlikely to be available in the foreseeable future, the next best thing is to apply differentiated screening measures to passengers on an unpredictable basis and, where possible taking into account a risk assessment of the person being screened, thus moving away from the conventional one-size-fits-all screening paradigm.

This evolution will take time as the regulatory framework will need to be adapted and will probably start with the selection of higher risk passengers for enhanced screening before we see expedited screening benefits being extended to passengers that are deemed to be of lower risk. For such risk assessment to be robust we expect that a hybrid approach will be required, for instance combining intelligence-driven and data-driven selections, itinerary-based differentiation, behaviour detection at the airport and trusted traveller schemes.

Forward-looking regulators and airports are already experimenting with the infrastructure that will underpin differentiated screening of passengers. Using biometric or sensor technologies, passengers and their belongings can be traced through the screening process with the algorithms on security scanners and X-ray systems being varied in real time.

Such dynamically adapting security lanes could be used initially to implement randomness and unpredictability in a more sophisticated manner but they are also an indispensable prerequisite for risk-based differentiated screening.
Evolution, not revolution

In summary, today’s state-of-the-art security lanes provide improved detection capability through the use of security scanners and multi-view X-ray systems equipped with explosive detection systems (EDS). Security scanners allow for a reduction in full body pat-downs and thus a better passenger experience while centralised image processing and innovative lane configuration drive improvements in throughput and asset utilisation. The networking of equipment, and the ease of data collection that comes with it, supports the development of sophisticated checkpoint management systems. While this hardly represents a paradigm shift it cannot be denied that we have seen more change in the past three years than we have seen in the three decades before.

The next three years will see further progress that brings us ever closer to our vision. Next generation X-ray systems equipped with advanced EDS and the capability to virtually separate objects will finally make possible the effective screening of cabin baggage without the need to remove electronics and liquids. Security scanners will continue to improve and the dynamic switching of algorithms on security scanners and X-ray systems will enable differentiated screening of passengers and their belongings, initially driven by randomness and unpredictability but also providing the infrastructure for a gradual move toward risk-based selection. And centralised image processing will live up to its full potential when it will be used in a multi-airport configuration, providing benefits to large and small airports alike.

Indeed, the evolution is underway.

This is just the beginning.
Work with us to deliver the future.
About IATA

The International Air Transport Association (IATA) represents some 264 airlines comprising 83% of global air traffic. IATA’s mission is to represent, lead and serve the airline industry.

About Guido Peetermans

Guido Peetermans works for the International Air Transport Association (IATA), where he leads the Smart Security initiative. In close cooperation with regulators, screening authorities, airports, airlines, solution providers and members of the research community, the programme aims to provide a roadmap for passenger-friendly security checkpoints at airports, while strengthening security and improving operational efficiency. For further information, see www.iata.org/smart-security, or contact the author at smartsecurity@iata.org.

This article was originally published in Aviation Security International magazine (www.asi-mag.com)