AVIATION SECURITY TECHNOLOGY

Airport Requirements

ACI EUROPE Technology Panel

1. Introduction

ACI EUROPE is the unique European trade association representing a vast majority of airports in Europe (500 out of about 800 aerodrome engaged in commercial aviation across continental Europe). ACI EUROPE goal is to promote professional excellence amongst airports in Europe and beyond.

One of ACI EUROPE area of expertise is aviation security (AVSEC). As part of the ACI EUROPE work on AVSEC, a dedicated working group (referred as the "Security Technology Panel") has been meeting for a number of years in order to focus on various issues related to security technology. One of the groups objectives is to inform suppliers and the innovation community of airports' requirements.

The airports industry and the security community need to continuously understand and keep track of a sector where technologies evolve permanently while the ultimate objective remains: continuously improve ways of meeting security standards while achieving reasonable operational performance, and equally, ensuring the satisfaction of users and travellers.

2. Background

The ACI EUROPE Security Technology Panel working group, formed by technical subject matter experts from European airport operators, has also been a forum for direct engagement between airport experts and suppliers.

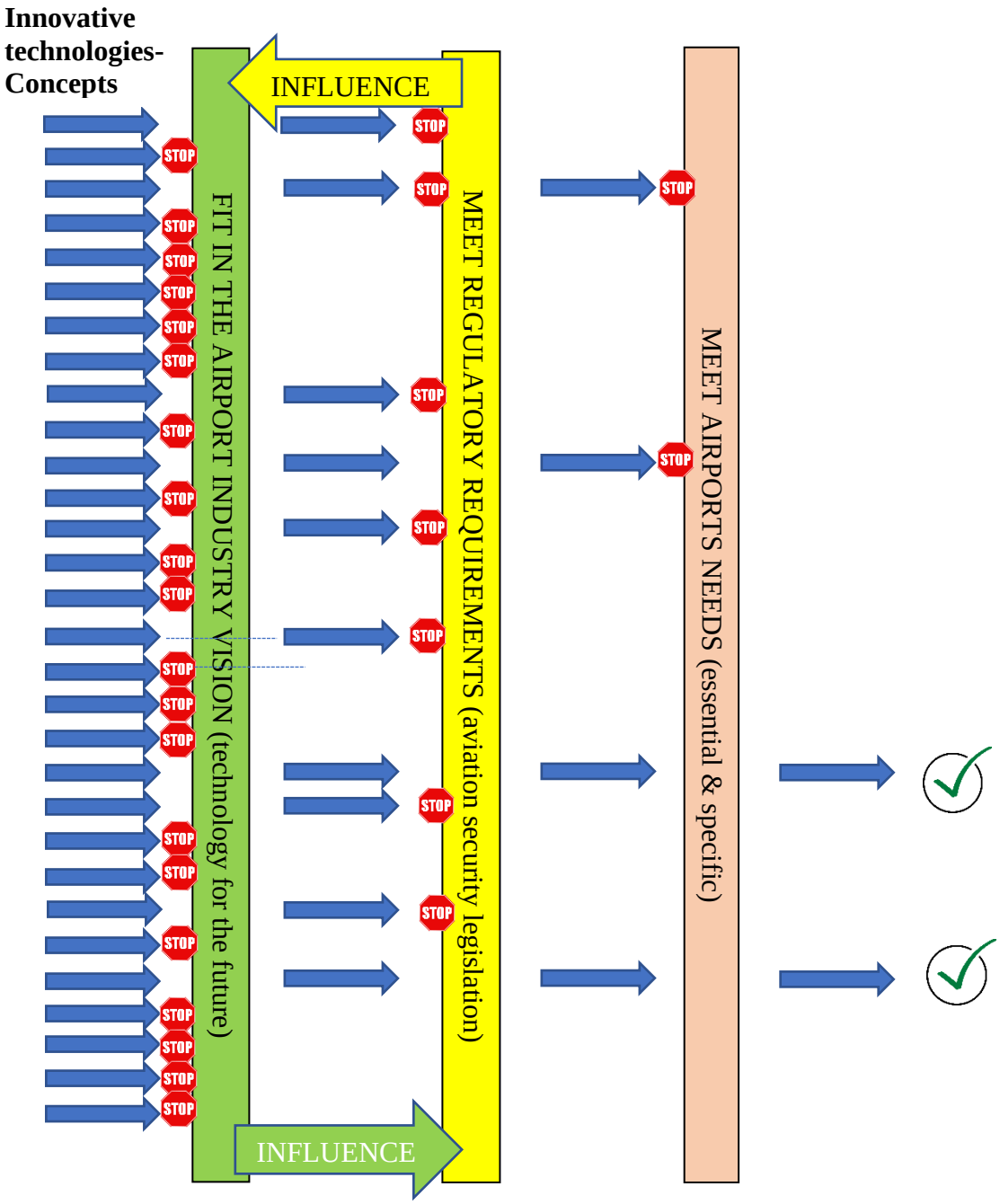
Some of these interactions have led to direct and fruitful partnerships between suppliers and airport operators partnering on operational trials, or on the deployment of innovative technologies…etc.

On the other hand, the ACI EUROPE Technology Panel working group observes that the expectations of airports with regards to security technology are not always clear or well understood by suppliers and developers.

ACI EUROPE therefore recognises that it is has a responsibility to raise awareness and promote more clearly what airports' want and more clearly explain to an audience as large as possible, what the airports essential requirements are when it comes to technology and innovation needs. Doing so, the ACI EUROPE Security Technology Panel believes that suppliers or solutions providers' chances to fulfil airports needs will increase, ultimately benefitting all parties. And so will their chances to access the airport security market significantly increase.

3. Innovation in Airport Security Industry: State of Play

The key prerequisites to any investment in innovative technology development should meet the following requirements:



a) Technology: Meeting the Airports Vision in Security

Aviation security of tomorrow is envisaged to take account of the following considerations **(Note: some of the goals below listed will require legislative changes of the current regulatory framework)**:

i. Passenger experience improved:

- ✓ Seamless, with more and more integrated steps in the overall security and identity process, and less fragmented:
    i. End-to-end considerations, requiring *de facto* more connectivity and interdependences too.
- ✓ Less intrusive, more customer-friendly.
- ✓ Faster security processes.
- ✓ Inclusive of disabilities (visible and invisible), reduced mobility and respectful of personal rights and privacy.

ii. Security and risk situational awareness strengthened:

- ✓ Combined identity and security processes.
- ✓ Enhanced situational awareness and more integrated risk picture (as opposed to isolated sensors or monitoring in silos in the security process).
- ✓ Not only protecting the aircraft but the whole of airports and the surrounding landside. Look at an holistic threat picture:
    i. considering not only terrorist threats but threats to business;
    ii. tackling threat vectors from the ground;
    iii. physical security including landside areas;
    iv. cyber threat vectors;
    v. threat vectors from within (insiders); and
    vi. threat vectors by the air e.g. drones.
- ✓ In this respect, the passenger checkpoint is no longer seen as the primary layer of defence at airports in the future. Slowly moving from pure AVSEC to airport security with the frontier between airport security and public security blurred.
- ✓ Enhanced identity management (not only security management) while respecting privacy rights.

- ✓ Stronger technological decision-making assistance for security decision makers:

    i. Better detection of threats (higher capability of security sensors).
    ii. Interoperable systems (systems of systems) and interoperable sensors able to connect with an array of new interfaces (towards an integrated management), allowing for better informed decision-making and higher situational awareness.
    iii. User friendly technology and processes (for staff AND passengers), “easy to use” software and hardware.
    iv. More reliable technology such as higher technology availability – e.g. increased Mean Time Between Failure (MTBF) by favouring foreseeable or predictive maintenance, and more efficient response to unforeseen, hence disruptive corrective maintenance.
    v. Reduce as much as possible the number of primary false alarms or reject alarms at primary level of security controls.
    vi. Develop solutions and concepts with no or minimal human intervention at primary controls level and subsequent control levels (i.e. alarms resolution). The feasibility of semi and fully automated concepts such as those developed for border controls and self-service security should be explored.

iii. Increase operational efficiency to avoid capacity constraints:

- ✓ More sustainable security operations (capable to sustain growing volume/flows while keeping the same level of security). Move towards eliminating the human element at the level of security controls and screening, while shifting human resources to the secondary level of screening (alarm resolution).

- ✓ Scalable system able, where possible, to adjust capacity needs with demand.

- ✓ Other ways of doing security checks while respecting passengers and security legislation (e.g. less divestment, less intrusive controls…etc.).

- ✓ Technology breakthrough is welcome even if this involves a paradigm change in security legislation.

- ✓ Upgradable technology, guaranteeing a minimum degree of futureproofing over the full life cycle of a technology product or system (including both hardware and software).
- ✓ Move away from a planned obsolescence approach, unless inevitable (e.g. for health or safety reasons…etc.).

- ✓ Software technology: interoperability becomes a must (move away from end-to-end proprietary systems solutions and favour interoperable interfaces).

iv. Human-machine interface:

- ✓ As user friendly as possible, easy to use and easy to get started, intuitive (including hardware & software interfaces).
- ✓ Compliant with privacy, Health & Safety requirements.
- ✓ Ergonomic.
- ✓ Upgradable.

v. Develop semi to fully automated systems where human intervention is reduced to a minimum (i.e. maintenance, certain alarm resolution protocols and verifications, feasibility of remote assistance concepts for some controls etc.). Other considerations:

- Security as a service (SaaS) opportunities depending on the business case. The SaaS concept is one possibility for the future with airports only offering the square meters and outsourcing all security operations to a third party.
- Innovative solutions providers and developers should no longer think of an airport as being one single entity but as a part of a system of airports. As airports are interacting more and more, new solutions must support this. Example of one possible use case: a passenger flying from Oslo to Sidney via London: a passenger security data status and/or the X-rayed bags images cleared in Oslo can be shared with the airport operator and/or local authorities in London for verification with their “own digital detection or screening” tools. The next step is that these passenger security data-status are transferred to Sidney where local authorities or/and airport operator can also look for prohibited food at immigration as part of their national requirements as one example of requirement at destination (also based on the digital data). For manufacturers this could mean developing computers and platforms which only runs algorithms and miscellaneous digital tools. Passenger’s bag(s) get only screened once physically and its associated images or security data status get shared across the journey locations (with appropriate data transaction receipts). Subsequent verification get done mainly via digital processes. Bag physical rescreening remains naturally an option at transfer or at destination as needed. When the journey is safely completed, the data can get deleted.

vi. Regulatory Considerations:

- ✓ Move away from a prescriptive approach towards an outcome focused approach that allows acceptable means of compliance or alternatives means of compliance as long as proven and deemed equivalent or better.
- ✓ More agile regulatory framework enabling a quicker response to new threats and mitigation measures.
- ✓ Faster testing and approval of procedures and CONOPS for new technology.
- ✓ Standardisation of technology CONOPS to remove legal uncertainty.

Future screening solutions will turn airport passenger checkpoints into walk-through "gateways" that will leverage data and overall risk scores to assist faster and better informed decisions. Other solutions will emerge such as off-airport baggage screening, stand-off and on-the-fly detection systems, CCTV with smart surveillance algorithms and behaviour analysis, biometrics and identity management, advanced and automated detection of prohibited items etc. All of which in a much more integrated and interoperable way for a more holistic risk-based security decision-making process.

b) Technology: Meeting Regulatory Requirements

Aviation security is regulated in the European Union by a common European framework regulation (EU Regulation 300 and its implementing rules). Amongst the EU AVSEC Implementing Regulations, there is the Implementing Regulation 1998/2015 serving as a base to common interpretation by all EU Member States of the ICAO Annex 17 standards.

EU Regulation 2015/1998 sets mandatory obligations for airport operators pertaining to various domains, as follows:

Chapter 1: Airport Security
Chapter 2: Demarcated Area of Airports (see EU Regulation 1254/2009)
Chapter 3: Aircraft Security
Chapter 4: Passenger and Cabin Baggage
Chapter 5:Hold Baggage
Chapter 6: Cargo and Mail
Chapter 7: Air Carrier Mail, Air Carrier Materials
Chapter 8: Inflight Supplies
Chapter 9: Airport Supplies
Chapter 10: In Flight Security Measures
Chapter 11: Staff Recruitment and Training
Chapter 12: Security Equipment

Any technology developed must, therefore, meet the standards set by legislation, where appropriate. In particular, those laid down in Chapter 12 “Security Equipment”. For instance, the European Commission sets the legal standards that ECAC use when testing through the ECAC Common Evolution Process (CEP) the abovementioned security equipment.

For more information about the ECAC CEP: https://www.ecac-ceac.org/cep-main

Naturally, vendors and solutions developers have to check for national standards depending on regions/countries, since detection requirements may vary:

- US: set by the Transportation Security Administration (TSA)
- China
- Etc.

c) Technology: Meeting Airport Needs

Most airports would likely share the above general vision of security of the future, but airports also recognise that there will always be unique customer requirements. As a general recommendation, a good innovation strategy for any given security service and technology products should take account of the vision while handling unique customer requirements on a case-by-case basis.

4. Aviation Security – Constraints on Innovation

- Legislation has a huge impact on airport security operations;
- The aviation security industry is a closed and difficult market to enter for outsiders;
- Only few airports have R&D departments. Innovation is more about purchasing products or services that are on the market. And they must then fulfill all needs and requirements as an off-the shelf solution;
- Most airports are more focused on existing operations. They struggle with day to day compliance. Little to no time is left or taken to reflect on holistic challenges and come up with long-term solutions;
- Innovation in the market is often based on the latest threats;
- Innovation in the market often fails to meet open architecture standard practices, with a need to move away from end to end proprietary solutions and favour interoperable interfaces;

- European funding programmes for research (e.g. *Horizon2020*) are often considered too much hassle to apply for and rarely offer concrete solutions for practical implementation;

- There is a misfit between security innovations that some companies invest into and develop and what the airports are looking for or really need. For instance, higher passenger throughput, better operational performance, security compliance and better customer satisfaction;

- Airports have a long list of challenges they need to deal with already while recognising their responsibility to shape current aviation security measures and processes, what innovation should address in the future.

5. Innovation - What Can Be Improved?

On the one hand, airports have the ambition to create sustainable growth with things like more turnover, added value and more profit. To enable such growth, they need innovative products, services and technologies. As an organisation, they also need to be adaptive to new circumstances. To increase the likelihood of this change happening, airports need real abilities to innovate thus need to **define their requirements to innovate and ensure these requirements are promoted and known**.

On the other hand, airports depend on enterprises to help them with innovations. As the airport security market is rather "closed", partly due to security and confidentiality, **new players are struggling to get a clear picture of airport needs**, procedures, networks and legislation. It reduces the attractiveness of entering the industry and thus the possibilities of airports to benefit from new products and services.

As a consequence, one way to improve the current state of play can be to invest extra attention in order to stimulate innovation at both airports and enterprises including SME's etc. This can help to bridge the gap between the supply and the demand, that is often observed. ACI EUROPE should play a more active role to boost innovation by:

- Define more clearly and more visibly the essential needs and requirements of airports.

- Establish a platform that facilitates matching and brokerage between the supply and the demand of innovation:

    - Organise sessions in which airports can improve their innovation capabilities;
    - Develop a website repository of updated airport's needs;
    - Articulate airport needs;
    - Support and develop matchmaking events/opportunities;

- Undertake and support research and innovation;
- Develop "**net stopper**" tools for SMEs and solutions developers to safeguard their limited resources and investments at the earliest stage possible in order to limit "financial waste", especially where funds are utilised and where it comes clear that there is little if no chance for a product or service "to break through" in the airport security market;
- Suggest or initiate EU level projects; and
- Share knowledge amongst airports.

6. Define More Clearly The Essential Airport Requirements

Below are some of the important considerations for suppliers for any new airport security solution based on the introduction of (new) technology:

Must come in response to a functional need and satisfy passenger and user (staff) experience. Does the product or service help to achieve the airport strategic goals? Airports are likely to embrace more automation and digitalisation to enable more efficient operations, better traveller experience, staff ergonomic and operational performance. Before COVID-19 it is recognised that in too many airports, capacity is close to "maxed out", hence requires vital optimisation in every single domain.

- Automation should not be understood as digitalisation and vice versa. For example, airports may not want to get rid of the human interface with their customers across the entire journey as this is not what passengers want. The airport industry should keep diversifying the products it offers to its customers while seeking continuous performance efficiencies. Digitalisation must, therefore, first respond to a functional need of the end user and also enable business efficiencies (e.g. self-service).

- Should enable equivalent or better overall security (e.g. more efficient threat detection).

- Should improve the passenger experience and facilitation (e.g. better throughput, less intrusive security checks, etc.).

- Be customer and user-friendly.

- Reliable with high levels of technology uptime / availability.

- Safe and secure, with no unintended safety impact and be cybersecurity resilient.

- Must consider the privacy of users.

- Compliant with legislation (e.g. health and safety, cybersecurity, and also meet security standards).

- Serviceable, like smart maintenance features, both predictive and like self-diagnostic and corrective.

- Upgradeable (**hardware & software**) depending on the type of technology.

- User compatibility.

- Intuitive to use.

- Provision of a complete support system for mitigating any difficulties in the necessary learning curve and transition phase between buying, installing, using and maintaining.

- Take into account a modern approach to training.

- Considerations for the user audience.

- Degree of interoperability, ability to integrate in a wider technological environment, especially as airport end users observe a shift from stand-alone systems to “systems of systems” with more being integrated and networked.

- Anticipation of change management required (if any) that comes with any new deployed technology.

- Establish adequate IT architecture from the start, based on open standard principles as the use of open standards can support good cybersecurity practices towards more resilience.

- New technology shall be able to be implemented in the airport architecture and follow recognised open architecture standards, if required.

- Any new technology must come with a cost-benefits justification to make a business case. Note: benefits can also be non-material or non-tangible and for instance consist in improving the passenger experience.