

The logo for ACI Europe is a blue square containing the letters 'ACI' in a large, white, serif font. Below 'ACI', the word 'EUROPE' is written in a smaller, white, sans-serif font. A white, curved line sweeps across the logo from the bottom left towards the top right.

ACI EUROPE POSITION
on
Aviation Security
Technology Roadmap

AIRPORTS COUNCIL
INTERNATIONAL

9 April 2013

Introduction

1. The European Commission has established a Technology Roadmap Group, involving different Commission services, industry stakeholders and EU Member States and observers. The aim of the group will be: to develop a consensus vision of what technology will be needed and be available for aviation security at different points in the future; to develop a strategy and concrete actions regarding research funding and pre-commercial procurement; and to monitor and support the European Commission Security Equipment Industrial Policy. ACI EUROPE strongly supports this initiative and will offer industry expertise to help fully realise a successful outcome. This Position Paper outlines all the steps required for the successful introduction of new aviation security equipment, from identifying the objectives and requirements through to final implementation.

Background

2. The current EU process to develop, certify and deploy new technology is excessively lengthy and fragmented when viewed from a global aviation business perspective. Before 9/11, security accounted for up to 8% of operating costs at European airports. Today, that figure is on average 27% of airport operating costs, of which a significant percentage is related to the purchase, running, maintenance and staffing costs of different screening technology. Currently, on average, 41% of airport personnel in Europe are employed in security-related functions, with the majority performing screening tasks. The development of technology plays a crucial part in ensuring the detection of threats and providing reassurance to the travelling public. Any technological advances that improve the passenger experience, reduce the burden on security screening staff is welcome, but must be fit-for-purpose and meet operational requirements. We feel that the current system for the development of aviation security technology for use in airports is inadequate and needs a more coherent approach to satisfy the needs of the airport users, manufacturers, and regulators.

3. The aviation industry is, by its very nature, global and therefore any new process that is developed must be mutually acceptable to major trading partners. The EU, with international partners, should support initiatives aimed at developing new technology such as high-speed detection system technology, as well as others technologies allowing for a smoother throughput of passengers, baggage and cargo at security controls at airports. Those new technologies should contribute to a simpler and more efficient security operations, processes and, if possible, security regulations.

4. In order to introduce and operate new aviation security equipment there needs to be a clear, auditable, coherent process that follows all the steps from “cradle to grave” of any project.

5. The current EU process of technological development is piecemeal, fails to address fundamental requirements and lacks coordination. Some of the elements are in place and by themselves deliver good results in discrete functions and it is noted that the European Commission is exploring some measures to address some of the shortcomings with the current process.

6. Aviation security equipment systems are sophisticated and technologically complex, and require ever increasing levels of systems integration. Before a new technology is safely introduced into an aviation security product it must undergo rigorous verification and validation. This may be achieved by a combination of modelling, simulation, laboratory testing and operational field testing. A new technology, or combination of technologies, require final testing in an environment close to operations and at full scale, so demonstration at the system level is an essential means to manage the high level risks in the innovation process. To secure efficiency a seamless integration of design and manufacturing capabilities must be achieved routinely and cooperatively between all stakeholders throughout the whole supply chain.

7. A fair and balanced set of regulations and standards must be in place to create a global level playing field. This includes efficient certification of aviation security products: A European certification process must be streamlined, efficient and low cost, and should be widely applied at component, product and system levels, and it should be capable of anticipating and adapting to new technologies in the future.

8. New capabilities to ‘design for operations’ are required that must facilitate and contribute to the more efficient ‘time to market’, despite (or perhaps because of) more complex design challenges. This requires new standards and procedures for system and procedure development and a more joined-up approach between certification, operator approval and licensing in identifying and managing system risk. Security in the design phase has to link up more transparently to security in the operational phase of the system lifecycle.

The Current System

9. The current system deals with only partial elements of the normal project process for the introduction of new technology and does not consider operational implications at all, which was quite evident when regulations

relaxing restrictions on Liquids, Aerosols and Gels (LAGs) were introduced in 2010.

10. The certification of security equipment is the verification of compliance with given security technical standards through formal laboratory evaluation.

11. Current EU security standards are based on collaborative work in the European Civil Aviation Conference (ECAC) of the ECAC Members Civil Aviation Authorities.

12. The ECAC Common Evaluation Process (CEP) harmonises the technical evaluation of security equipment and gives member states the ability to set their own national certification. The ECAC CEP was launched in 2010 and has proven to be a significant improvement over the previous piecemeal national evaluation system. In general the CEP works well, although there needs to be improvements in the feedback mechanism to manufacturers and administrative arrangements for notifying successful compliance with EU technical standards for security equipment.

13. Currently operational trials are carried out on an ad hoc basis by individual airports (500 + in the EU) to evaluate the operational effectiveness of security equipment in an airport environment as part of their pre-procurement process. No formal operational trials programme or facilities exist.

Technology – From Requirement to Implementation

14. There are a number of basic principles and processes that should be followed before any type of new technology or aviation security equipment can be deployed and put into operation; these are:

- Objective. Setting out the objective is a fundamental first step in the decision process for technological development. This objective could be political, technical, procedural or regulatory.
- Identifying the Requirement. The new requirement could come about for a number of reasons, such as the identification of a new threat, the identification of new technology to better address existing threats or a re-examination of activities to see if security measures can be carried out in a better or more coherent way.
- Threat and Risk Assessments. Assessments should review old threats and examine new or emerging threats and explore current or new measures or technology to mitigate the threats. The risk assessment will determine the level of acceptable risk and examine a number of

potential courses of action, which might lead to the conclusion that the development of new technology or combination of new technology and new processes is the preferred (or only) option.

- Identification of Potentially Suitable Technologies. Security equipment manufacturers should be approached to provide an initial assessment of possible technological solutions to address threats.
- Identification of privacy, ethical and societal implications of technology. It is an inherent element in the development process of new technology to consider implications affecting privacy, ethics or the societal dimension.
- Statement of Requirements. The statement of requirements should include, *inter alia*, the following elements:
 - The main objective, the threat to be mitigated and the risk analysis.
 - An outline impact assessment to define, in broad terms, the implications (advantages and disadvantages) of introducing a new piece of aviation security technology in the EU.
 - Setting of technical detection specifications, technical standards and requirements. A classified technical annex might be required to spell out specific technical detection specifications.
 - Operational specifications and requirements. These could include:
 - Passenger facilitation requirements e.g. passenger or baggage throughput requirements;
 - Human factors considerations e.g. ergonomics of equipment, man/machine interface;
 - Staffing and training requirements to include selection criteria for staff and the amount of staff necessary to operate equipment;
 - Concept of operations. Where the new equipment would be installed and how it would be integrated in the overall process;
 - Infrastructure implications e.g. weight, dimension requirements of new equipment;
 - Standardisation of image and transmission protocols (for example TIP data base), where appropriate;
 - Power requirements;
 - Maintenance requirements;
 - Impact on and interface with other systems and procedures;
 - Life-cycle of equipment and return on capital investment.

- Laboratory testing. Appropriate laboratory testing facilities need to be identified for the type of equipment to be tested. This may include a common testing methodology if items of equipment are tested across different testing facilities.
- Operational field testing requirements. Appropriate operational field testing facilities need to be identified that cover a range of different operating environments (small, medium, large, hub airports).
- Approvals and certification process.
 - Timetable. An outline timetable should be drawn up to include, *inter alia*: Threat projection; project definition; product research and development; laboratory testing; concept of operations (basic rules for the immediate handling of the equipment); operational field testing; (according to Regulation 185/2010, Point 12.8); evaluation and analysis of results; product refinement;
 - If development is successful then: EU Regulation for the use, and technical specifications for certification of new equipment; product certification and approval (including CE-mark and health and safety approval); manufacturing production; individual end user evaluation of the product and implementation (to include: tender and Procurement requirements; infrastructure requirements; delivery and installation; staff training requirements; product acceptance).
- Acceptance tests. Acceptance tests are required both for laboratory tests and operational field tests. The analysis of laboratory and operational testing results should be conducted and feedback to manufacturers should be given so they can refine their products. Information to end users should be given on what equipment has met the technical specifications, technical standards and requirements and operational requirements.
- Full Impact Assessment. After equipment has been developed and tested, both in the laboratory and in the field, an in-depth impact assessment should be produced to consider all the implications of introducing a new item of aviation security technology, including economic and societal factors.
- Timetable. Updated timetable (from the items listed in the outline timetable above) to include actual results from preceding work.
- Impact Assessments. The conclusions of the full impact assessment and an updated timetable should be considered when developing new

EU Regulations for the use of new aviation security equipment along with realistic implementation timelines.

Research and Development (R&D)

15. The European Commission Framework Programme for research is a multi-annual, multi-million euro programme that provides funds for research and development across the EU. However, because of the legal constraints established when setting up the programme there is no possibility to fund research for specific applied technical solutions. As a result much of the research can be characterised as academic or ethereal with little added value to solve real and timely aviation security needs. Thus, the EC should explore ways of providing more direct funding for research and development of new security technology.

Certification and Testing

16. The European Commission has embarked upon a project to establish an EU wide certification system; something industry has been seeking for some time. An EU-wide certificate not only simplifies matters but also creates the premise for a stronger EU security market. To achieve this will require:

- Technical specifications and detection requirements;
- Assessment/development of conformity testing standards;
- An EU accreditation and certification system;
- Trialling facilities.

17. Operational trialling of security equipment could take a number of forms:

- Continue with the current ad hoc arrangements;
- Establish public/private partnership facilities where the expertise of manufacturers of security equipment and the operational expertise of end users is used in a facility funded by national governments and/or the EU;
- Establish private facilities at airports, funded by the EU, where real time operational trialling could take place. There would need to be a number of facilities to provide data and analysis on the impact of new security equipment on small, medium and large airports.

The Global Context

18. ICAO Annex 17 Chapter 2 (2.5.1) recommends "Each Contracting State should promote research and development of new security equipment, processes and procedures which will better achieve civil aviation security

objectives and should cooperate with other Contracting States in this matter.” The EU, in cooperation with major trading partners, should work towards common detection requirements for existing and future equipment performance to optimise the overall screening operational performance. Also EU and major trading partners should work towards the mutual recognition of security equipment on the basis of harmonised standards based on the conformity of standard setting, testing and certification to bring security technology products to market faster and reduce overall costs. There should be a common roadmap for screening automation through enhanced technologies that allows for a long term strategic vision and planning between major international partners.

Conclusion

19. To introduce and operate new technologically advanced aviation security equipment there needs to be a clear, auditable, coherent process that follows all the normal steps of a major project. The challenge for new technology is to find a way of implementing an increasingly complex set of security requirements, while maintaining smooth and efficient airport operations with a minimum of disruption to traveling schedules. Passenger expectations regarding security, safety, health, privacy and service have to be fulfilled to ensure successful implementation of new technology.

20. A more coherent process needs to be agile and iterative, making adjustments based on findings at each stage. The key will be in the setting of operational requirements and technical specifications, which should include full definitions. Failure to establish a full and proper process mean that there is a distinct danger technical requirements are set but the technology (usually bounded by the science) cannot be delivered, resulting in limitations that then drive a different approach (for example LEDS Type C – airports wanted the ability to screen multiple LAGs, the manufacturers achieved that but the technology is unable to deliver this in an operationally efficient way). It would be catastrophic if Regulators who are balancing the manifold political issues fail to recognise the need for structured fluidity throughout the technology process. The fundamental requirement is a fully collaborative process, with appropriate involvement and responsibilities, throughout the life-cycle of aviation security technology development.

FLOWCHART FOR SUCCESSFUL SECURITY TECHNOLOGY DEVELOPMENTS

