Secure Skies

The European Pilots' perspective on improving aviation security

ECA Piloting Safety

European Cockpit Association

Secure Skies

The European Pilots' perspective on improving aviation security

Contents

Foreword

© ECA

Nico Voorbach
ECA President

Aviation security has become an important challenge for the air transport industry especially during the last decades. In the 60s a number of hijacks have shaken the industry. In 1963 the Tokyo Convention was adopted to establish global measures against acts of unlawful interference in aviation.

As professional airline pilots we are involved in the work carried out by ICAO, the EU and National Authorities. ECA provides the pilots' perspective on how security and facilitation are currently handled and where extra or different measures should be implemented. I have had the privilege to be involved in this work with aviation organisations during my participation in IFALPA and ECA activities in security for many years.

My close involvement in aviation security dates back to 1999 when the focus was to prevent weapons being brought on board aircraft. Then the Lockerbie disaster demonstrated that hold baggage should be screened for explosives. However on 11th September 2001 the aviation security world changed. We were confronted with terrorists willing to commit suicide while taking the aircraft down and using it as a weapon of destruction. Security agencies reacted by looking for different ways to counter this new threat. A number of reactive counter measures were put in place at airport checkpoints since 2001 but the option of adding every time new layers is no longer sustainable and does not improve security. At the same time, it is a real financial burden for airlines and it affects passenger travelling experience.

This is why we have to rethink the way we are securing air transport operations. This document based on the tremendous work of the ECA Security Working Group, presents how professional pilots see the current aviation security and facilitation regimes and how they should be improved to enhance the security and by consequence the safety of our flights Looking for bad people instead of bad objects in one way but in any case it should be encompassed in a comprehensive Security Measurement System.

I am sure that together regulators, airports, airlines, pilots and the travelling public will benefit from these proposed changes.

Nico Voorbach

Key Recommendations

Improving aviation security is an ambitious task which requires a holistic approach. Key elements of such strategy are stepping from a reactive perspective to a more proactive and predictive one, integrating threat assessment, risk management, differentiation, unpredictability, randomness with global and harmonised solutions. In this paper, ECA maps out the key areas for aviation security today and tomorrow as well as the pilots' perspective on improving aviation security.

AIRPORT SECURITY

» ***Passenger differentiation:*** ECA supports the concept of passenger differentiation provided it is based on factors other than nationality, race, religion and gender. Profiling can be carried out on basis of behavioural analysis, travel document analysis and questioning techniques, as proven by a number of successful trial projects across the globe. Differentiation must also be implemented in a cost-effective way.

» ***Pilot differentiation:*** Certain categories of people who are responsible for and entrusted with the safety and security of aircraft, such as airline pilots, should have different screening than passengers. When States investigate the possibility of differentiation, pilots should be used as a trusted population to perform initial passenger differentiation trials. Ultimately that would also enable efficient flow of personnel at airports.

» ***Crew ID card:*** A common air crew ID card should be developed throughout Europe to ensure the highest possible security. Any Crew ID should include biometric data to positively match the card holder to the level of clearance and should be based on standard Crew Identification Card (CMC) standards from ICAO.

» ***In-flight and airport supplies:*** In-flight and airport supplies should be screened at a more frequent level than currently performed.

» ***Security scanners:*** ECA accepts the introduction of millimetre wave imaging and other technologies as long as they are proven safe and harmless for health. ECA however rejects X-ray based technologies, and privacy issues must be taken into account when considering security scanners.

IN-FLIGHT SECURITY

» ***Cockpit security:*** Airlines must put in place robust procedures and access video cameras to ensure that the cockpit door – an essential barrier that protects all critical systems of an aircraft – is sufficiently protected and truly acts as a deterrent to those who would try to access the cockpit.

» ***Hijack and bomb threat response:*** In case of a hijack or bomb threat the primary responsibility of where to divert to is still with the Captain of the aircraft. He/she is the one who decides what the safest solution is for the passengers and the crew. This may result in the aircraft diverting to a non-designated airfield. A regular review of bomb and threat hijack response plans by airline groups, pilots and police should be carried out by the States. Any response plan must be in accordance with international standards.

» ***In-Flight Security Officers:*** Government employees acting as In-Flight Security Officers can be deployed provided they are appropriately trained and under direct control of the pilot-in-command as recommended by ICAO.

» ***Deportees:*** Transporting deportees can only be done when the pilot-in-command agrees, taking into account the safety of the flight. It should be agreed with operator and pilot-in-command and he/she must be promptly informed before boarding.

» ***Unruly passengers:*** Unruly passenger behaviour should be made an international offence and clear, harmonised global enforcement and prosecution procedures for disruptive passenger incidents should be introduced. Standard Operating Procedures, company policies, adequate staff training and mandatory reporting of incidents must be introduced to tackle unruly passengers.

» ***MANPADs:*** Governments should use non-proliferation policies and share intelligence to disrupt terrorist plans and to exchange information. Airports, municipalities and law enforcement organisations should keep areas around major airports under surveillance to counter all types of standoff and threats, incl. MANPADs.

» ***Laser attacks:*** Laser attacks must be addressed at a global level, particularly under leadership of ICAO. States have to be encouraged to adopt and enforce legislation against laser illumination. In parallel, the public must be properly informed about the risks associated with pointing lasers at cockpits. Better reporting and coordination efforts between pilots, ATC and police should be established to facilitate finding and prosecuting perpetrators.

» ***CBRN:*** ECA recommends updating and implementing the ICAO Document 9811 dealing with the threat of chemical, biological and radio-active and nuclear weapons and devices. Awareness-raising and training programs for crew must be created.

© shutterstock / Michal Bednarrek

» ***Cargo security:*** The current cargo security system is a good basis but should be further improved by increasing the number of checks, including introducing unannounced checks. In addition, the quality of the system as a whole needs to be assessed and measured. There should be no difference in security measures for cargo carried on board of all cargo aircraft or on passenger aircraft.

» ***Comloss interceptions:*** Steps should be taken to overcome loss of communication and optimise communication between ATC and pilots. These include expansion of the use of data link, or the emergency frequency to be used for safety issues only.

» ***Unmanned Air Vehicles/Remotely Piloted Aircraft Systems:*** The security standards by which UAV/RPAS systems are developed must be equivalent to those applied to manned aircraft. Therefore, all factors should be considered, including employees, location, accessibility technology, design properties, link protocols, command structure, etc. Such systems should be able to prevent 'denial of service', assure 'integrity of data' and provide 'confidentiality of operations'.

» ***Cyber Security:*** Cyber security, especially against aircraft systems, should be taken seriouslyn by the aviation industry. It is vital to build awareness about the vulnerabilities and of the precautionary measure that could be taken. Equally, the integration of security systems at airports must allow for real time data transmission within a well-protected, secure network.

CONCLUSION:

ECA promotes safe and secure flights while ensuring efficiency and competitiveness for European Airlines. Airline pilots play an important role in the security chain and are the last line of defence in most of the aircraft security incidents. They are entrusted and responsible for the safe carriage of passengers and cargo. Their role is and should further be recognised. ECA and its national Member Associations are committed to work hand in hand with the European Commission, EU Member States, the European Parliament and other aviation stakeholders to contribute to reshaping and strengthening aviation security.

Introduction

Professional pilots give prominence to aviation safety and security. The concept of safety is at the core of pilots' training and operations. This concept is later applied to security where pilots try to relate the same approach i.e. to incorporate procedures into their day-to-day work aimed at protecting crews and passengers from acts of unlawful interference[1], such as seizure of aircraft, hostage-taking, forcible intrusion on board of an aircraft, etc.

The difference between safety and security is not always known by the general public. The difference between both concepts still needs to be explained and in particular from an aviation point of view. To fulfil this purpose, the International Civil Aviation Organisation (ICAO) has come up with two very specific definitions about safety and security:

Safety: The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.

Security: Safeguarding civil aviation against acts of unlawful interference or acts which, whether or not they are offences, may or do jeopardize the safety of the aircraft or of persons or property therein or which jeopardize good order and discipline on board. This objective is achieved by a combination of measures and human and material resources.

The purpose of this publication is to address the concepts of aviation security and facilitation[2] and explain how airline pilots operate in this environment. One can always argue that the purpose of safety and security are different but the experience and expertise of pilots in safety, including Safety Management Systems (SMS), enable the implementation of a structured approach to managing aviation security as an integral part of the aviation system.

[1] See overleaf

[2] ICAO Annex 9 defines "facilitation" as follows: Contracting States shall adopt appropriate measures for the clearance of aircraft arriving from or departing to another Contracting State and shall implement them in such a manner as to prevent unnecessary delays.

1 **Acts of unlawful interference** as defined by the Tokyo Convention are acts or attempted acts such as to jeopardize the safety of civil aviation, including but not limited to:

- unlawful seizure of aircraft;
- destruction of an aircraft in service;
- hostage-taking on board aircraft or on aerodromes;
- forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes;
- use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment; and
- communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

Achieving Smart Security:

» How to Implement Risk Based Security

The approach to aviation safety management has evolved towards the set up of holistic model. Safety Management Systems also encompass the notion of risk management – a tool designed to find efficient solutions to safety deficiencies. Increasingly, provisions are being made in the security regulations that require a threat assessment and afterwards the implementation of risk management methodologies to adapt the security provisions to that evaluation. The whole purpose of this approach is to move from a reactive framework (i.e. producing new regulations and procedures *only* after an attack or an attempted attack has taken place) to a more proactive[1] and, if possible, predictive[2] one.

In security, neither threat nor risk is specifically defined, although threat assessment and risk management is required to implement some of the regulations and provisions.

Threat could be defined as a condition or object with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.

Risk could be defined as the assessment, expressed in terms of predicted likelihood and severity, of the consequence(s) of a threat taking as reference the worst, most probable, foreseeable situation.

In a risk management model it is necessary to first define the threats, then list the specific consequences of each threat, assess the risk of each specific consequence and then, if deemed necessary, implement the most efficient mitigating measures to lower the risk (as low as possible) below a pre-defined threshold.

Risk Based Screening (RBS) is today broadly used in the aviation cargo security environment. The basic concept requires pre-defining the "trustworthiness" of a shipment through specific criteria and then to adapt the security screening requirements according its risk. It thereby allows for different screening processes to be implemented according a risk management methodology.

[1] The proactive method looks actively for the identification of risks through the analysis of the organization's activities

[2] The predictive method captures system performance as it happens in real-time normal operations to identify potential future problems

This concept is not yet applied to passengers, cabin or hold baggage screening. The paradigm of "one-size-fits-all" approach continues to be implemented. A change of mindset is needed to address the future screening requirements from a holistic and more efficient point of view. It is foreseen that security checkpoints at airports will be the single most limiting factor in the overall growth of the aviation industry. Risk management, differentiation, unpredictability, randomness, behavioural analysis, biometric identification, data analysis, etc. are concepts and possible solutions that are being evaluated today to try to integrate the available methodologies to improve aviation security, and specifically passenger experience and traffic.

Some States and organisations are striving to apply these new, more effective methodologies. In the US, Transport Security Administration's Pre✓™ and Known Crewmember® programs are good examples of possible ways forward to implement new methodologies in passenger and staff screening. Also Canada, with its Restricted Area Identity Card (RAIC) program has implemented some of the aforementioned procedures into the airport security environment. Additionally, International Aviation Transport Association (IATA) and the Airports Council International (ACI) are continuously developing their joint 'Smart Security'[1] project where security resources are allocated based on risk management methodologies.

> "The US with its TSA Pre✓™ and Known Crewmember® programs are perfect examples of ways forward to implement new methodologies in passenger and staff screening."

[1] http://www.iata.org/whatwedo/security/Pages/smart-security.aspx

Security management Systems (SeMS)

The most effective system available today to incorporate all aspects of security in a country or a given organisation, such as an airline, is the SeMS. It may be defined as a formal, risk-driven method of integrating security into an organisation, that requires coordination of activities, responsibilities, practices, procedures, processes and resources (i.e. it has to be Systematic, Proactive and Explicit).

In other words, SeMS is a holistic approach to security striving to move from a classical (reactive) perspective to a more proactive and predictive one. It moves away from a "one-size-fits-all" to a more tailored system. Still, restrictive baseline measures may be necessary, but flexibility should be allowed in the system to let it adapt to cope with the specific threats and security needs of an organisation.

© shutterstock / Alvaro German Vilela

Operational decisions and planning should be consciously considered at every level of an organisation at all times, and every process in the organisation has to be consistent with a predefined plan but it also must have capability to adapt to the evolving environment.

An effort has to be made within corporations to connect all management systems in the organisation to work in coordination with the others (SMS, QMS, EMS, OHSMS, etc.[1]).

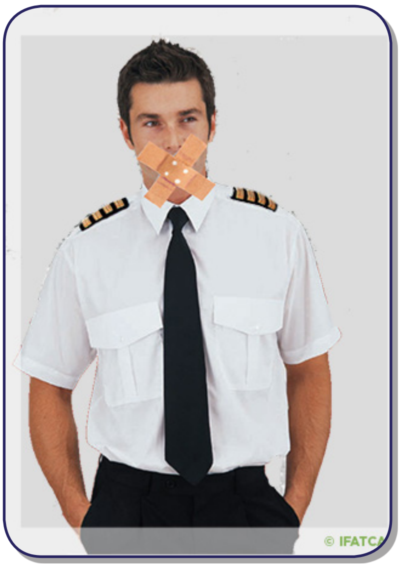
[1] SMS : Safety Management System
QMS : Quality Management System
EMS : Environmental Management System
OHSMS : Operational Health and Safety Management System

Security Performance

Security Training + Security Culture + Security Reporting + System Services

Security training and a good security culture (including Just Culture[1]) are of paramount importance to achieve an acceptable level of security performance. National Training Programs must require that organisations' training programs include, at minimum, recurrent security awareness training for all personnel that play a role in aviation security.

The effective implementation of a mandatory and/or voluntary confidential security reporting system is a necessary tool to collect data and other security information. Motivation of personnel is a key factor for maintaining the security of operations, and the effective implementation of reporting systems gives the right message to the personnel that aviation security is everyone's responsibility.



> "The effective implementation of reporting systems gives the right message to the personnel that aviation security is everyone's responsibility."

[1] As defined in the EU Occurrence Reporting Regulation 376/2014, Art. 2(12): " 'Just Culture' means a culture in which front-line operators or other persons are not punished for actions, omissions or decisions taken by them that are commensurate with their experience and training, but in which gross negligence, willful violations and destructive acts are not tolerated."

© shutterstock / Josef Hanus

Airport Security

Critical Parts / Restricted Areas

There are two basic areas in a given airport setup: landside and airside.

Landside is the area of an airport and buildings to which both travelling passengers and the non-travelling public have unrestricted access. Lately, landside security has been recognised as a priority of public civil aviation security policies with new policies expected to be developed in the near future.

Airside is the part of an airport where aircraft and supporting vehicles are, together with the adjacent terrain and buildings or portions thereof, access controlled.

Airports are required to develop their own Airport Security Programs (ASP) which also define the landside and airside parts. The ASP approach to airport security uses the design of three concentric circles with the outer circle representing the landside area and the security measures to protect it. The second circle is the landside/airside boundary or restricted area and the various security measures designed to protect it from unauthorized access. These would include the designation of the airside area, physical security barriers (e.g. fences, gates), intrusion detection systems, surveillance systems, together with the access control measures to restrict access to authorized persons, vehicles and articles. The inner circle represents the Security Restricted Areas (SRAs) which comprise the Critical Parts Security Restricted Areas (CPSRAs)[1]. Before entering such an area, any persons, articles and vehicles may be subject to screening or other security controls.

[1] Critical parts shall be established at airports where more than 40 persons hold airport identification cards giving access to security restricted areas.

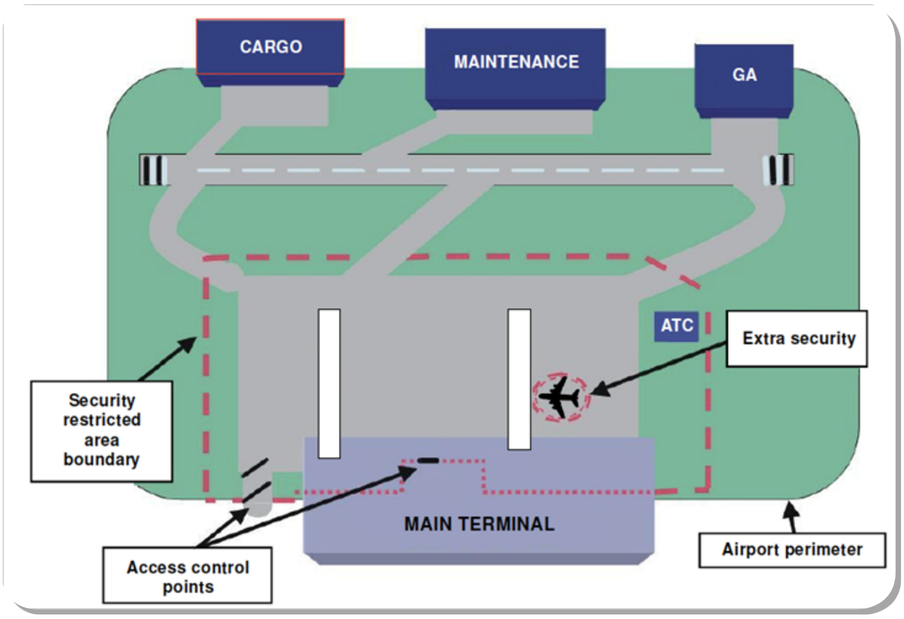
The SRAs and CPSRAs are specifically designed to protect aircrafts from acts of unlawful interference. SRAs and CPSRAs are defined in the airport's plans (as specified in the ASP). These areas could include and are not limited to:

a. Passenger departure area between the security screening point and aircraft

b. Ramp

c. Baggage make-up areas

d. Cargo sheds, mail centre, airside catering and aircraft cleaning premises



To access a CPSRA, 100% access control and screening procedures are implemented to anyone trying to enter such an area, including airport staff. These screening methods have recently been modified, allowing different techniques to be implemented for the screening of non-passengers that include exemptions to introduce some items that are normally prohibited for passengers.

As explained in the following sections, ECA is of the view that certain categories of people – including airline pilots – should be screened on a random basis.

Passenger Differentiation

Following the occurrence of terrorist attacks on aviation, new security measures were developed to close the gaps exploited by the perpetrators. These measures are commonly applied to all passengers and are mainly based on the principle of an equal threat. The same security measures are applied indifferently to everyone. However, terrorists tend to seek ways to circumvent security measures, which has resulted in a continuous need to create new security technologies.

The threat environment is constantly changing. This means that a security system needs to be flexible in order to be successful. Past attacks have revealed a lack of coordination and sharing of information between agencies and (national) authorities. Security processes need to be more resilient and more focused. The detection of intent is as important as the detection of devices. Technology is key, but technology alone will never be the solution.

New measures should be based on resilience, improved passenger experience and better use of intelligence and information (such as behavioural recognition). Basic characteristics of such measures should include: better use and integration of intelligence and information, behavioural analyses, randomness, (integration of) technology and human interaction.

Due to the increasing number of air passengers, an "equal security" approach translates into growing costs, lengthening of security queues and increased passenger discomfort. Under these conditions, an "equal security" approach is not sustainable. A step in the right direction would be to review security measures, integrating screening of people based on randomness and unpredictability.

There is a wide consensus in the industry that instead of focusing on suspicious objects, the focus needs to be put on identifying suspicious persons. Passenger differentiation enables to distinguish trusted passengers from individuals who have been identified as posing a threat because of lack available information about them or because they demonstrate suspicious behaviour. This method enables to ease the flow of passengers through security gates and increase overall efficiency.

ECA supports the concept of passenger differentiation. However, it is crucial to emphasise that differentiation should never be based on an individual's nationality, race, religion or gender. It has been demonstrated that a terrorist can present any combination of these characteristics. Furthermore, the scope of aviation security goes beyond preventing terrorism in its traditional form and aims at preventing various acts of unlawful interference.

© shutterstock / Nico El Nino

As well as being impartial, differentiation needs to be implemented in a cost-effective way by allocating existing resources more efficiently. Adding additional layers of security simply increases costs. Each security measure should be evaluated for its results and target the area and individuals who present the most significant risk.

There are several approaches to differentiation. One approach is to examine an individual's background by analysing the available data from authority registries and shared databases. ECA recognises the paradox that exists between background checks and Europe's pro-privacy culture and legislation. However, it is important to keep an open mind when considering new means of identifying threats.

Another approach is the profiling of passengers in the airport environment. This profiling can be carried out through behavioural analysis, travel document analysis and questioning techniques which do not necessarily require the collection of background data. Trained and skilled behavioural analysts have demonstrated they have the required skills to identify individuals who can pose a threat.

IATA and ACI have taken a leading role in making passenger differentiation a reality. ECA supports this joint project called "Smart Security" initiative (previously named "Checkpoint of the Future") which is currently being developed. The concept seeks to incorporate several differentiation techniques with the aim of enhancing passenger flow and comfort. We encourage European countries and the European Commission to be supportive of this project and consider removing legal constraints that prevent its implementation. As pilots we consider vital to draw our sight into "whom we carry" instead of spending our resources into finding nail clippers or children's juice bottles.

Pilot Differentiation

Airline pilots are, by definition, the ultimate line of defence because they are responsible for, and entrusted with, the security of their aircraft and its passengers. Pilots are responsible for safely transporting their aircraft, passengers and cargo from their point of departure to their destination. Pilots do so by considering relevant factors such as weather, fuel, fatigue, runway environment, and operational efficiencies. Of the multitude of factors that pilots must consider, the operational security of their flight is one of the most fundamental and important concerns that they address on a daily, flight-to-flight basis.

In order to make these decisions, pilots are granted authorities in international protocols and conventions (e.g. Tokyo Convention) and passengers and crewmembers are required to follow their instructions. In addition, access to the flight deck is granted by the aircraft commander. In fact, the aircraft commander can in all respects be considered de facto as the "security manager" of the flight.

ECA therefore believes that trial tests should first be used on trusted individuals such as pilots before passenger differentiation trials. This is because pilots present the following advantages in trustworthiness:

- Pilots are responsible for the safety and security of the aircraft.
- EU legislation requires pilots' background to be initially and periodically checked, hence they are pre-screened already.Pilots have a high level of training and qualification.
- Pilots have a high level of training and qualification.
- Pilots work as part of a crew and are monitored by their peers and colleagues.

The current airport security procedures and the hurdle they sometimes impose to crew members on duty should not be underestimated. The delays at the security checkpoints, and sometimes the excessive meticulousness in the application of the different procedures to already trusted personnel, may result in an unnecessary deviation of attention that could affect their state of mind and ultimately have an impact on the operation's safety. Again, it is important to highlight that pilots are not seeking to be exempted from screening but that security controls which take into consideration the trustworthiness of each person would enable to increase the efficient flow of personnel and improve the personnel's journey to the workplace.

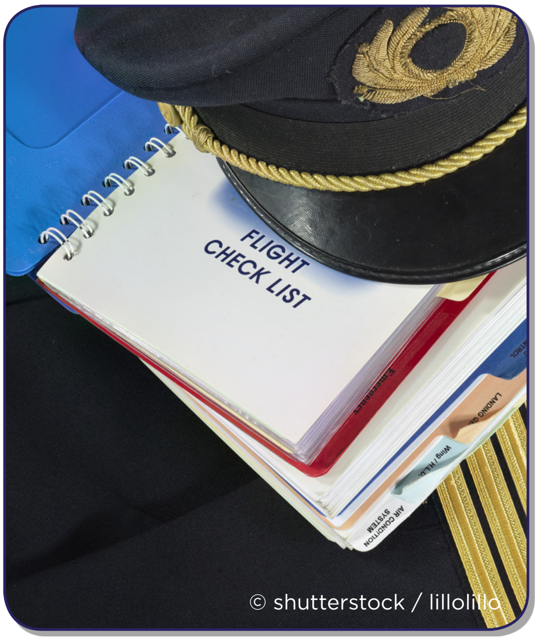
To close any potential gap, a common crew ID system should be developed throughout Europe to ensure that the person who is granted facilitation through smoother access through airport's security checkpoints is not being impersonated.

Crew Identification

Both individual countries and the industry have launched programs that aim at demonstrating the applicability of new screening methods which encompass identity screening. These programs are at varying degrees of implementation at the operational level (SURE – Netherlands; Outcome Focused - Risk based initiative – UK; Known Crew Member and Pre Check Programs – U.S.; Restricted Area Identity Card – Canada; Checkpoint of the Future – IATA and ACI Smart security etc.).

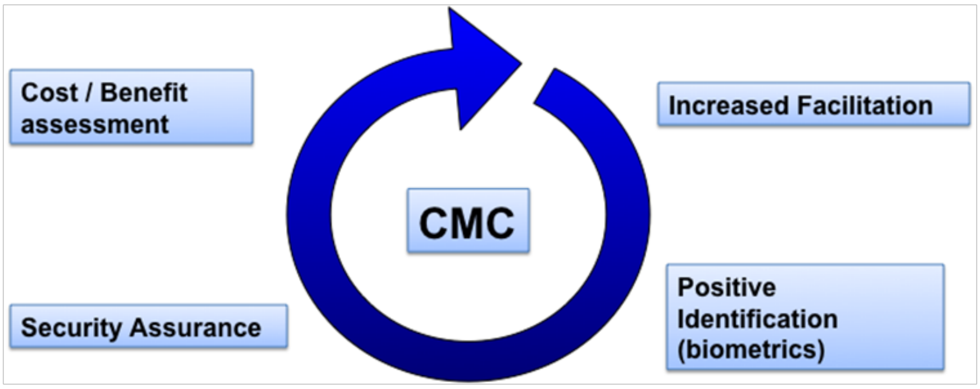
Today, there is a lack of European harmonisation in the design of the different crew ID cards – Crew Member Certificates (CMC) that grant access to the security restricted areas of the different airports. The use of an international standard would help in the mutual recognition and implementation of the ID cards in countries throughout Europe. An effective implementation of a CMC system at European level would be a first step in the right direction to harmonise and to continue applying risk-based approaches to access and security controls in an airport environment.

To apply this risk-based approach concept, relying on the level of trustworthiness of each person, the system is required to positively identify each person entering a restricted area. For instance, a security background check on a security personnel would be worthless if one's identity could be impersonated by someone else carrying a forged airport badge. In order to avoid this risk any CMC and security badge should include biometric data to positively match the card holder to the level of clearance granted by his/her badge.



© shutterstock / lillolillo

The basic requirements that a Crew ID system based on ICAO's guidance would have to meet to be successful are defined in different areas:


Cost / Benefit assessment
Increased Facilitation
CMC
Security Assurance
Positive Identification (biometrics)

1. Increased Facilitation.
2. Positive identification of crew members, possibly with the introduction of biometric technology. However, data gathered for biometric identification has to be safeguarded and used exclusively for this purpose.
3. Security Assurance: a security assurance methodology would need to be incorporated into the system to ensure the level of security remains at least equivalent to the current one.
4. Cost/Benefit assessment: the final product would have to be financially viable.

Regulatory and specific technical requirements would have to be developed to cover the above aspects. These should include the integration into this new structure of random, unpredictable and other methodologies that may be appropriate, through a risk-based analysis, to make the system more robust. A joint undertaking by states, industry and different stakeholders may be necessary to achieve this goal.

In ICAO's doc. 9303 on Machine Readable Travel Documents, various options on how to develop a CMC are laid out. At European level a specific standard, accepted by all States, could be defined and thereby efficiently comply with the requirements defined in Annex 9, Chapter 3, Section N[1].

The success of a common European CMC system would be greatly beneficial to states and industry. Data would be gathered that could be applied further to other aviation related staff and, at a later stage, to passengers. Airline pilots being a trusted link of the security chain they should be identified as the population to perform the first trials on differentiation. ECA and its members are willing to support these projects.

[1] 3.63 Contracting States shall establish measures, with the cooperation of aircraft operators and airport operators, to expedite the inspection of crew members and their baggage, as required at departure and upon arrival.
3.64 Contracting States shall facilitate and expedite the process under which aircraft operators based in their territories can apply for Crew Member Certificates (CMCs) for their crew members.
Note. — The CMC was developed as a card for use for identification purposes by crew members, leaving the crew licenses to serve their primary purpose of attesting the professional qualifications of the flight crew members.
3.65 If Contracting States issue Crew Member Certificates, then these shall be issued only in the form of machine readable cards in accordance with the specifications of Doc 9303, Part 3.

© shutterstock / Oleandra

In-flight & Airport Supplies

In-flight supplies[1] (i.e. catering, cutlery and/or any other supplies that are necessary for on-board service) and airport supplies[2] (i.e. goods that may be available to the general public trough airport retailers) have to meet the same security requirements. When introducing the "Known Supplier" of In-flight and airport supplies, the legislation implemented the principle of a safe supply chain, already known in airfreight security, for supplies that are being used onboard the aircraft and/or in the airport itself.

For a company to become a "trusted entity" it has to either agree to an on-site inspection of its shipments to an airport has to be inspected, using an unpredictable procedure of selection, on a monthly basis. This procedure is clearly insufficient to define an entity as trusted and multiple gaps are left open for anyone to exploit.

Additionally, goods which are not supplied by a known in-flight or airport supplier, the means or methods employed need to take into consideration the nature of the supply and have to be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the supply. Today, these procedures, according to ECA, do not provide sufficient safeguards to maintain reasonable level of security. The same situation occurs for airport supplies. In both cases, these procedures are insufficient and are not based on robust risk assessment.

ECA also advocated – and continues to do so – for more stringent requirements for in-flight supplies since supplies taken to the airport do not undergo the same risk assessment as supplies loaded directly onto a commercial aircraft and, therefore, accessible to anyone on board. The application of more stringent requirements has become critical since the last regulatory package also allows blunt and sharp objects to be introduced as in-flight and airport supplies.

Finally, an alternative way of complying with current security requirements for supplies includes the possibility of such supplies to be accompanied by security staff that will also monitor the unloading process and ensure no prohibited items are being introduced during the critical parts of the chain. However, the actual and efficient implementation of this option has proven to be challenging.

The in-flight and airport supply scheme, as it stands today, must be improved. The current system does not work and is highly ineffective and the latest regulatory update is not compatible with a sound security system.

[1] All items intended to be taken on board an aircraft for use, consumption or purchase by passengers or crew during a flight

[2] All items intended to be sold, used or made available for any purpose or activity in the security restricted area of airport

Security Scanners

To improve the results and performance of security checks in terms of weapons found, a variety of methods are used to optimise or complement currently used detection systems. Nevertheless, these systems are still limited by their performances, cost and/or their impact on health. Any tool based on a technology that does not harm health and that ensures a satisfying level of security would be potentially acceptable for flying crews.

Against this background, ECA accepts the introduction of:

- Millimetre wave imaging;
- Other technologies as long as they are proven to be safe and not harmful to the health in a global context (e.g. the Explosive Trace Detection Portals).

ECA rejects the use of:

- **X-ray based technologies;**
- **Other technologies as long as they have not been proven safe for pilots.**

Medical aspects:

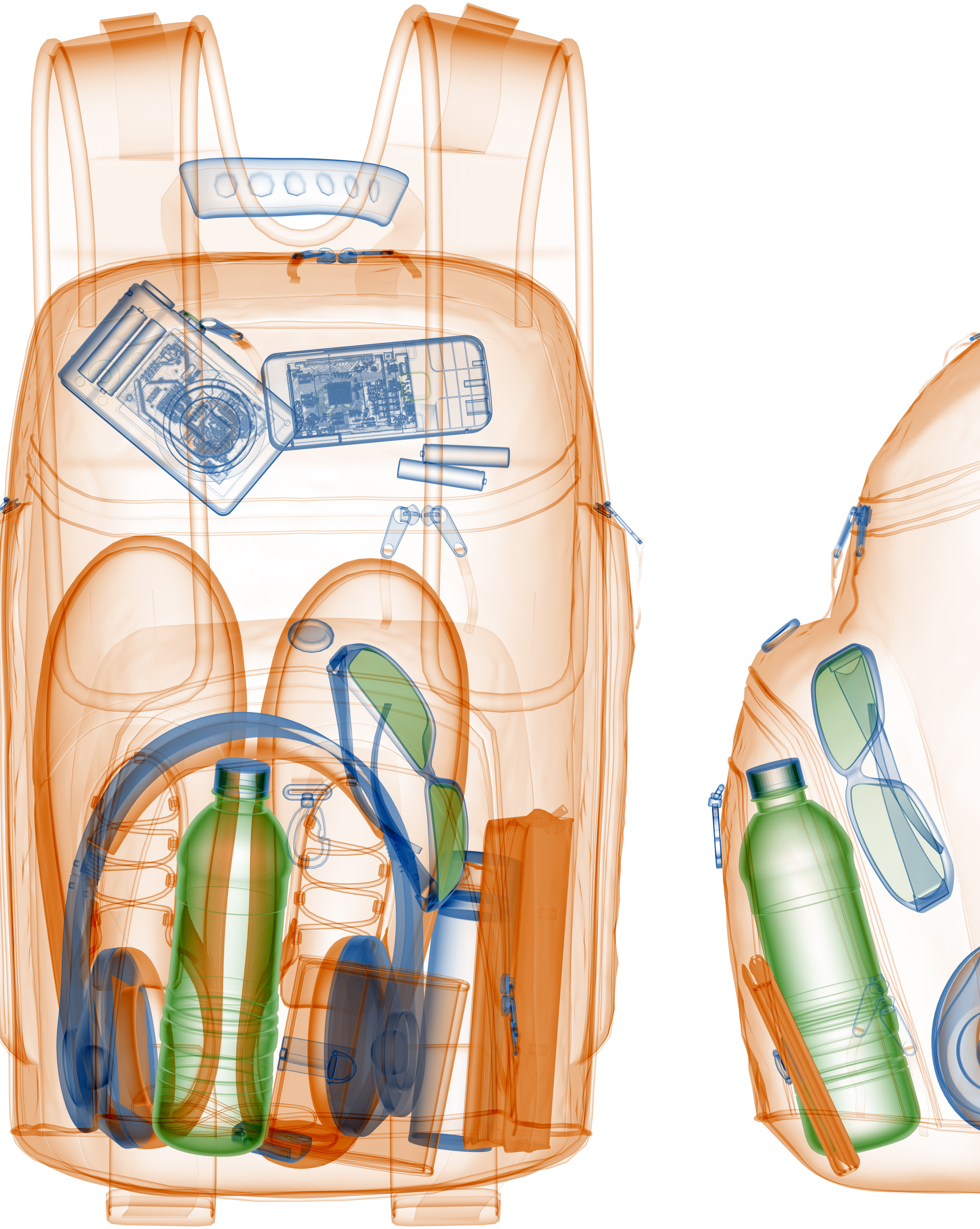
Crews are already exposed to cosmic radiations at high altitude. Records of their ionising radiations data (as required by the Council Directive Euratom 96/29) show yearly figures between 3 and 6 mSv[1] (for long haul flights). While 1mSv is the limit above which the health risks are not negligible, other radiation sources have to be added. The following aspects are relevant:

- “Natural radiation” is considered to be between 1 and 3mSv per year,
- Ionisation is a cumulative process, all radiations absorbed during a lifetime remain in the body and therefore increase with the number of flights and screenings
- The exposure to cosmic radiation is higher for ultra long range flights.

Privacy aspects:

A number of privacy issues exist in the use of scanners which manufacturers must overcome by using software that only shows a schematic representation of the human body rather than a real picture of the body. In addition, pictures taken by the scanners must not be recorded or stored.

[1] millisievert



© shutterstock / Kasza

Cockpit Security

Cockpit security is in essence the protection of the cockpit from unlawful interference from the passenger cabin whilst the aircraft is in flight. The cockpit of a modern airliner is the one place where all the critical systems of an aircraft come together.

The world has seen the results of the actions of terrorists and hijackers when they gained access to the cockpit. To date, the main method of cockpit protection involves a robust door, remotely activated locks with an active CCTV surveillance system. This door and its frame are ballistically and impact strengthened but not proof.

It is most important to recognise that if during a flight the cockpit door becomes the actual last line of defence then those wanting to harm are already on board. Nothing onboard the aircraft is a substitute for better and appropriate airport security. However the risk of a cockpit door breach must not be overlooked. Airlines must put in place robust procedures to ensure that the cockpit door truly acts as a deterrent to those who would attack.

Secondary barriers have a place on aircraft whose operations involve either all cargo or flights to challenging destinations. They consist of an extra fence to prevent the access to cockpit door when this later is open. In many instances the secondary barrier consists of strong wires placed as a fence. Their use is currently limited to certain airlines or to certain type of operations. Secondary barriers can also be improvised: a trolley placed in front of the access to the cockpit door will be an obstacle to reach the cockpit.

Hijack & bomb threats response

Since the 1970s aviation has been a high profile target for terrorists. Hijacking aircraft can draw attention to a cause quickly and will ensure maximum publicity all over the world. In the past, these situations, though scary for passengers and crew, were often resolved with little loss of life. However since Lockerbie and other attacks around the world, that calculation is no longer valid. The 9/11 attacks demonstrated that aircraft can be used as weapons of destruction and cause large scale losses.

In terms of hijack response, some designated airfields have been prepared to receive suspect aircraft. But the primary responsibility of where to divert to is still with the Captain of the aircraft. He/She is the one who will decide what is best for the passengers and crew on the day. This may result in the aircraft diverting to a non-designated airfield. As a result police forces in many different airports must have a bomb threat/hijack response plan to deal with such an inbound aircraft.

ECA recommends that these should be reviewed regularly with pilot and airline groups so that a co-ordinated and reliable response is formulated and understood by all concerned. With the number of foreign airliners in EU airspace, it is crucial to ensure that any response is in accordance with international norms of behaviour for aircrew so allowing them to maintain the safety of their passengers and crew.

In-Flight Security Officers

In-Flight Security Officers (IFSOs), also known as sky marshals or air marshals, are placed on some flights to counter aircraft hijackings. These can be supplied either by the airline or by the country of aircraft registration.

The deployment of IFSOs is a matter for national authorities and ECA does not object their deployment provided some basic principles are followed:

- IFSOs must always be government employees and must be appropriately trained.
- An IFSO must be part of the crew and always act under the direct control of the pilot in command. That is not to say that IFSOs need permission to carry out their duties but that they will always be considered in light of the Tokyo Convention. Their responsibilities and tasks should be laid down in the rules of engagement and based on the guidelines as laid down in the ICAO Security Manual (Doc 8973).
- If for reasons identified by the company a flight requires an IFSO, then special measures should be put in place to maintain the safety of the flight. If the level of safety is or might be impaired then the flight should not take place.

© shutterstock / pcruciatti

Deportees

It is not unusual for aircraft operators to have to transport deportees, inadmissible persons or persons in lawful custody. Strict guidelines should be followed to ensure that both the safety and the security of the flight are not compromised. In any case, the final decision on accepting such passengers and any escort onboard should rest with the pilot-in-command.

Passengers whose risk assessment includes at least one of the following factors should be classified as high risk:

- The passenger's escape would be highly dangerous to the public, the law enforcement authorities or the security of the state;
- The passenger's record, current behaviour or outside contacts indicate that the standard security procedures will not be adequate;
- The passenger is considered dangerous or likely to pose a security threat or control problem;
- The passenger is in custody and travelling against their will.

When such passengers are to be transported on a particular aircraft, state authorities should seek the operator's agreement prior to making any travel arrangements. Before the boarding of these passengers, the state or the operator should also provide the pilot-in-command with:

- The identity and seat number of these passengers;
- The persons' criminal record, if applicable ;
- The reason for transportation/deportation.

Carriage of high risk passengers should preferably take place on state aircraft. Civil air transport passenger flights should only be used for that purpose in exceptional circumstances, and when there is no alternative. In such cases, not more than one such person should be allowed on any flight, and then only when escorted by two or more law enforcement officers.

Whilst many inadmissible persons, deportees and persons in custody will travel peacefully, such passengers may also present a security risk. Proper risk assessment should systematically be carried out by the authorities, with the results provided in writing to the operator in sufficient time for the pilot-in-command to be informed. This will help the operator and the pilot-in-command decide whether any extra security measures or safeguards are required. The pilot-in-command should always be satisfied with the proposed security arrangements.to be informed. This will help the operator and the pilot-in-command decide whether any extra security measures or safeguards are required. The pilot-in-command should always be satisfied with the proposed security arrangements.

Unruly Passengers

ICAO defines an unruly passenger as[1]:

A passenger who fails to respect the rules of conduct at an airport or on board an aircraft or to follow the instructions of the airport staff or crew members and thereby disturbs the good order and discipline at an airport or on board the aircraft.

Examples of unruly/disruptive behaviour include:

» **Illegal consumption of narcotics;**

» **Refusal to comply with safety instructions;**

» **Verbal and/or physical confrontation with crew members or other passengers;**

» **Uncooperative passenger;**

» **Making threats;**

» **Sexual abuse / harassment.**

IATA has seen a dramatic rise in unruly or disruptive behaviour in recent years. Since 2007 reported incidents have increased more than 600 per cent with 8217 reported incidents in 2013. To minimise the impact on safety and the cost involved in potential diversion of the flights, IATA has developed some guidelines to handle unruly passengers[2].

Safety in the air begins on the ground, and unruly passenger incidents are best managed in a preventive manner by keeping unruly behaviour on the ground and off the aircraft. In-flight, unruly passenger events can impact the well-being of passengers, interfere with crew performance and/or threaten the safety of a flight and result in aircraft diversion. Because they require unplanned landings, these diversions create additional safety risks.

Despite the complexity of the issue, there are practical steps that can be taken to prevent and manage unruly passenger incidents which can contribute to increased safety and reduction of costs for air carriers:

» Establishment of Standard Operating Procedures (SOPs);

» Air carriers should have a definitive company policy for dealing with unruly passengers. Dealing firmly with disruptive behaviour will likely serve as a deterrent;

» Prevention: early signs of potential unruly behaviour can often be observed. An unruly person is easier dealt with on the ground where the assistance of security and/or the authorities is readily available.

» Staff training;

» Mandatory reporting of incidents;

» Post incident response.

A disruptive passenger is a real and serious safety issue. When an incident occurs on board an aircraft, the pilot-in-command has the ultimate authority on how to address the situation. The Powers and Immunities bestowed upon them by the Tokyo Convention 1963 need to be guaranteed anytime these "powers" are legally used.

[1] ICAO Annex 17 to the Convention on International Civil Aviation (the Chicago Convention) Security Safeguarding International Civil Aviation Against Acts of Unlawful Interference (March 2011)

[2] http://www.iata.org/policy/Documents/2013-V1-PUBLIC-Guidance-on-Unruly-Passenger-Prevention-and-Management.pdf

Jurisdiction

Whatever the reasons for the rising number of unruly passengers are, this kind of behaviour on a commercial flight is intolerable, where safety and order must be maintained at the highest level. ECA is of the firm view that unruly behaviour should be prosecuted and punished in order to show it is illegal and to deter others from doing the same. In practice, crew members have few tools to deal with unruly passengers. The end result is almost always the same with the perpetrator leaving free and unpunished by the authorities he/she has been delivered to. In some cases the perpetrator has even pressed charges against the crew. The main reasons why such offences go unpunished are uncertainty about jurisdiction, inadequate national legislation of the state where the perpetrator is delivered and the lack of extradition agreements.

The Tokyo Convention governs what actions an airline may take to address offences and other acts that occur on board during a flight. Also the jurisdiction of (contracting) states to take appropriate criminal, administrative and other measures is determined in the Tokyo Convention. However, loopholes that enable many offences to escape legal action still exist.

The Montreal protocol of 2014 amends and updates the Tokyo Convention, extending the jurisdiction, including the jurisdiction of the state where the aircraft lands, in addition to the country where the aircraft is registered, in an attempt to close this loophole. The protocol also addresses unruly/disruptive passengers and will come into force once the 22 signatory states ratify it.

Although the Montreal protocol improves aviation security, the cross-border prosecution of both criminal and civil offences will continue to suffer from severe lack of uniformity. In some cases, communication and cooperation amongst the various national authorities involved is at best deficient. In other cases, there is a complete lack of uniformity between the different applicable regulatory regimes. Furthermore, the Convention does not impose any obligation to prosecute an offender. Neither is there an obligation on a state to assert jurisdiction in relation to offences and crimes committed on board a foreign aircraft. Besides, even if a state is willing to prosecute, many states have not adopted appropriate legislation to deal with unruly/disruptive passenger incidents.

ICAO, realising the importance of the problem, published Circular 288, Guidance Material on Legal Aspects of Unruly/Disruptive Passengers. This model law with the main purpose of achieving a harmonised enforcement procedure and a uniform set of fines and penalties is still not implemented in a large number of states. The lack of adequate national legislation undermines the Tokyo Convention and Montreal protocol's effectiveness as a legal instrument in the fight against intolerable behaviour.

Even if a state decides not to expand their traditional territorial, personal or protective jurisdiction in case of an unruly/disruptive passenger incident, ECA strongly believes there should be a system in place that encourages the international cooperation and assistance between states for extradition in order to prosecute and eventually punish the offender in his/her own state or the state where the aircraft is registered.

ECA has identified several steps as a way forward:

- States must tackle the problem of unruly/disruptive passenger incidents. To ensure civil aviation remains safe and secure, one way to tackle the issue effectively is to make such behaviour an international offense.
- States must ratify Montreal protocol 2014 to amend the Tokyo Convention.
- States must expand their traditional jurisdictions and implement the Montreal protocol 2014 in their national legislation.
- States must adopt adequate national legislation on unruly/disruptive passengers with a strict level of adherence to the ICAO Circular 288 to maintain international uniformity.
- States must agree on extradition procedures in case of unruly/disruptive passenger incidents to ensure the offender cannot escape prosecution.
- States must implement harmonised enforcement/prosecution procedures for unruly/disruptive passenger incidents in their national legislation.

Stowaways

Stowaways or people who hide aboard a ship or plane in the hope of getting free passage are to date the result of an immigration problem where (illegal) migrants want to leave their country for a better life. Occurrences are almost always fatal for the stowaway, even if a very lucky few survive. Stowaways generally originate in very poor countries, where airport security is relatively low and enables them to hide in the landing gear of the aircraft.

Currently, specialists estimate the security risk as low, but ECA believes this risk will increase in the near future. With airport security making it ever more challenging for terrorists and hijackers to reach the aircraft, stowaways could become an increasing threat. ECA believes stowaways may be used in the near future in further attempts to breach aviation security. Some European airlines ask their crews to deal with potential stowaway situations in the same way they would do with a bomb on board.

Civil aviation is a worldwide business, and a lot of terrorist causes are looking for large media coverage in order to reach their goals. Military aircraft have also been subject to stowaway attempts.

Technically, some people are able to climb on a moving plane facing the real danger of the propellers or reactors, and of the turning wheels, in the hope that they will find a better life on the other side. Some individuals are ready to give their life for their cause, and will try to climb into the landing gear of a major airline's aircraft with the objective of fulfilling their aim. This weak point is no longer only known by pilots, but unfortunately it is a well-known fact, including by terrorist groups. This issue must be addressed at security, safety and political levels.

© shutterstock

MAN-Portable Air Defense Systems

The MANPADS (MAN-Portable Air Defence System) is not new in aviation but in recent years the threat has evolved considerably, and is real and growing. An example is the MANPADS attack in 2003 at Bagdad airport against a DHL Airbus 300. The crew did an outstanding job in landing their crippled aircraft after the left wing was hit by an SA-7 surface-to-air missile, one of the so-called first generation MANPADS. These types of attacks on commercial aircraft have occurred in either warzones or regions of active conflict and terrorism.

One of the side effects of the so-called 'Arab Spring', which started in 2010, was that an increased number of MANPADS became available and eventually found their way into the hands of rebels and terrorist groups. These groups proudly portray themselves on the Internet with the newer third-generation MANPADS. Their acquisition of these more capable MANPADS means a significant increase in their ability to carry out a successful attack. As a result, the threat and danger of MANPADS attacks on aviation is more prevalent than ever, even outside warzones.

MANPADS represent only one element of the multiple threats that aircraft may potentially be confronted during the taxi, takeoff, and landing phases of flight operations. Mortars and rocket-propelled grenades can destroy aircraft, as well as large calibre rifles using incendiary bullets. Long distance rockets can destroy aircraft at typical overflying altitudes.

Large transport category aircraft have a high statistical probability of surviving the damage sustained by a single MANPADS hitting the aircraft, although survival is not guaranteed.

ECA believes that design improvements could be made to improve the odds of surviving single or multiple missile hits. Aircraft could be "hardened" to make them less vulnerable to the damage and loss of primary flight control systems. For instance hydraulic fuse plugs and redundant backup control systems to assure survivability and other enhancements to maintain flight control. Another example is the so-called engine-propulsion control system technology to be used in the event of a damaged or inoperative flight control system, to enable the flight crew to safely fly and land an FMS/FADEC equipped aircraft.

These systems could significantly enhance the ability of an aircraft to survive any type of standoff weapon attack, not just shoulder-launched missiles. They would also prove useful in the event that flight control systems are lost due to other mechanical failure (e.g., United Flight 232 in Sioux City, 1989).

Air transport carriers should develop amendments to their flight training curriculum that instruct flight crews on planning for a MANPADS attack, alternate airport considerations in the event of an actual hit, and what type of emergency flight procedures to use, particularly in cases where flight control by conventional means is lost or impaired.

ECA strongly supports evaluations on the part of the manufacturers and regulators to develop Throttle Only Control (TOC) techniques for each aircraft model, and operators should provide adequate training guidance so that flight crews can achieve a successful landing.

ECA believes that prevention is the most effective countermeasure. Emphasis should be placed on identifying and disabling the "man" in the MANPADS threat. Governments should (continue to) use non-proliferation policies and share intelligence to disrupt terrorist plans and to inform each other and airline companies about this issue. Airports, municipalities, and law enforcement organisations should keep areas around major airports under surveillance to counter all types of standoff threats, including MANPADS. Furthermore, the public should be informed of measures that the government and industry are undertaking to counter MANPADS and to deter terrorists, possibly incorporating "area watch" programs as implemented.

In case of a credible threat, the airline company (in consultation with the authorities) should discontinue their operation over that area or to that airport. Depending on the local situation and the threat at hand, it could be decided to continue operations over that area / to that airport, provided clearly defined alternative procedures are used (e.g. minimum overflying altitude, descending in another area or using alternative procedures or routes). Flight crew members must be briefed on these procedures and should be made aware of the threats associated with a missile attack.

Finally, it is worth noting that although military aircraft have demonstrated the effectiveness of protective systems (i.e. with Directed Infrared Counter-Measure (DIRCM)), ECA believes that on commercial aircraft these systems have not proven to be sufficient, effective, affordable, or available.

Laser Attacks

Laser illumination is unfortunately not new in aviation. In virtually all parts of the world the number of laser attacks spiked in the years 2008 – 2012. In 2010, the numbers reached unprecedented levels and these numbers are still on the rise. This means the laser threat is far from being under control, while the laser itself is becoming more and more powerful and less and less expensive.

A laser aimed at an aircraft's cockpit constitutes an extreme hazard to the safety of the aircraft because it hinders pilots in the performance of their duties, especially in the most critical phases of flight. 90% of laser incidents occur near an airport, predominantly during the approach and landing phase. These are the most critical phases of a flight, due to the fact that the aircraft is close to the ground and in a situation demanding the pilots' maximum attention for safety related issues and tasks.

Internationally recognised standards have endorsed this philosophy by establishing sector wide adopted criteria, such as the 'silent cockpit philosophy' below 10,000 feet and the 'stabilised approach criteria' below 1,000 feet. Any disruption or distraction (i.e. shining a laser) during this phase of the flight must be considered as affecting flight safety, because it interferes with cockpit procedures, crew coordination and communication with air traffic control, to mention just a few.

Additionally, there are the physical and medical issues resulting from directing a laser at an individual (e.g. a pilot). These are the so-called visual effects including glare, flash blindness and afterimage, and ultimately eye injury (see below). These dazzling effects can temporarily blind a pilot or reduce his/her vision or colour perception.

> "There are physical and medical issues resulting from directing a laser at an individual
>
> » **Glare:** Obscuration of an object in a person's field of vision due to a bright light source.
>
> » **Flash blindness**: Visual interference that persists after the source of illumination has been removed
>
> » **After-image**: A transient image left in the visual field after exposure to a bright light source located near the same line of sight.
>
> » **Temporary or permanent eye injury**: The characteristic of the laser light can damage the retina instantaneously for any period of time, ranging from minutes to hours."

The inevitable result will be a reduction in safety ranging from distraction and disruption to disorientation and incapacitation. The highest risk is during critical phases of flight (i.e. approach, landing and take-off) where the ability of the pilot to function unimpaired and unhindered is critical for the safe operation of his aircraft.

In this context, two commonly misconceptions have to be addressed.

The first is that pilots always carry out automatic landings (autoland) using AutoPilot. The fact is that the vast majority of landings are made without the assistance of autoland and AutoPilot (thus manual landing with no Autopilot connected). First of all, not all airports are equipped with facilities that will allow autoland operations (normally only the big airports), and secondly not all aircraft are equipped with the feature. An autoland operation requires special procedures (e.g. distance between sequential aircraft), preparation of crew and systems (of the Auto Flight System and related instruments) and it cannot be transitioned to quickly from a normal manual approach.

The second is that there are always two pilots and therefore the danger is mitigated. It is a fact that today's modern, bigger commercial aircraft require two pilots as a regulatory and a design requirement. They are not designed to be flown by a single pilot, and each pilot has very important complementary roles and responsibilities; one (the "Pilot Flying") actually flies the aircraft and one ("the Pilot Monitoring") performs all the other ancillary functions necessary for safe operation.

In addition to distributing workload, this also maintains "redundancy", another basic principle in aviation; critical systems are always duplicated, and one takes over if the other fails. Failure of a part of this system constitutes an emergency. This also applies to the loss of one pilot.

Finally, in the event of a laser attack, the entire cockpit is illuminated; this has the inevitable effect that both pilots will suffer the full effects of an attack.

It is important to underline that the strength and accuracy of lasers is increasing. High power lasers are being imported from outside the EU, often easily purchased over the internet. Lasers manufactured in other countries may not have the safety features installed in them to reduce their power to EU safe limits[1], which is cause for even more concern if they are pointed deliberately at a plane.

To reduce the number of laser incidents a number of measures should be taken:

- The laser issue must be addressed at a global level. ICAO is the appropriate body to take the lead and incorporate laser illumination in the definition of unlawful interference in Annex 17 (Security) to the Convention on International Civil Aviation. This would have the effect of underscoring the seriousness of this issue.
- States have to be encouraged to adopt legislation against laser illumination and their perpetrator in order to discourage them.
- The general public should be better informed about the risks associated to laser illumination in general and specifically against aircraft. The public still is not sufficiently aware of the dangers that a laser attack entails. This combined with the ease of availability of highly effective and powerful lasers can create highly dangerous situations;
- The issues of controlling the trade of lasers and whether certain lasers should be classified as "weapons" should be considered.
- Tracing and finding perpetrators is difficult. Therefore a better reporting and coordination between pilots, Air Traffic Control (ATC) and local police should be established.
- Implementing the need for a license to use a laser. Customs should then act to prevent the import of license free lasers.

[1] Laser of up to class III.a with power of less than 5 mW are considered safe for momentary exposure (not for prolonged exposure). Class III.b lasers with a power of 5 – 500 mW may cause eye damage after momentarily exposure. Class IV lasers with a power level of more than 500 mW may cause eye and skin damage, even from reflected laser beams.

© shutterstock / Monika Wisniewska

Chemical, Biological, Radio-Active and Nuclear devices

Chemical, Biological, Radio-active and Nuclear (CBRN) weapons or devices are being used to attack civilians (e.g. in Japan on 20 March 1995).

Until now there has been no attack against civil aviation, but terrorist groups have already promoted the use of chloroform for instance (cf. magazine Inspire – April 2012).

In general there is no awareness, preparedness or specific knowledge within the aviation security community and personnel is not trained in this area. ICAO Doc 9811 (2002) is one exception which addresses the issue of CBRN. It explains the difference between CBRN and other devices and provides training and guidelines for crew to deal with chemical and biological weapons during flight. It provides crew with an overview of their responsibilities, gives crew advice and provides crew with specific checklists in different scenarios.

© Wikipedia/Creative Commons

Technical solutions on board are limited, but could and should include provisions like directing the airflow away from the cockpit and to not mix air from the cabin with air in the cockpit. It could be beneficial to develop closed oxygen systems for passengers (already required for cockpit crew) and detection equipment.

ECA therefore recommends updating and implementing of the contents of ICAO Doc 9811 and other ICAO documents referring to it. Awareness should be raised and training programmes should be created for crew, but also for first responders (emergency response teams, airport security agents etc.). Finally, procedures and equipment should be defined.

Cargo Security

ECA has been advocating improvements in the air cargo security regime for a long time. Where passengers and their luggage are screened meticulously, cargo carried on the same aircraft does not get the same treatment.

In the last few years important steps have been made by the EU in establishing a system of securing the supply chain. As a result, screening all cargo at the airport, which would bring the whole process to a halt, is prevented, while at the same time security of the cargo is ensured.

Although this legislation is a big improvement, it should be noted that the whole operation is very much an administrative exercise. Manufacturers can apply for a "trusted status" that enables them to send their goods by air without it being screened. To obtain that status, their security measures are normally checked regularly. Likewise for the freight forwarders who are responsible for the screening of the cargo originating from unknown senders.

ECA believes the current system to be a good basis, but the trust put in the companies involved is obtained too easily. Checks should be increased, and at least some of these checks should be unannounced. In addition, the quality of the system as a whole needs to be assessed and measured. By physically screening one percent of all cargo, the performance of the system could be monitored. Such a physical screening would also serve as an incentive for companies to keep their security at a high level, since prohibited items found could be traced back to the company of origin.

Finally, current legislation allows for a difference in security measures applied to cargo carried by cargo-only aircraft compared to those applied to passenger aircraft. ECA strongly believes this concept to be outdated. With current techniques it is quite easy to time the detonation of an explosive device to be over inhabited areas. ECA therefore advocates a single regime for all air cargo carried on cargo specific aircrafts or passenger aircraft.

COMLOSS - Interceptions

The number of comloss (prolonged loss of communications) is, though stable, relatively high. It is important to state that comloss is primarily a safety issue that can trigger a security response, such as interceptions. It is also important to know that statistics show that none of the reported comloss incidents within Europe have been linked to a security threat.

Communication between an aircraft and ATC is a critical link and human errors do happen. Several issues influence this communication link such as many frequency changes in a relatively small airspace, congested frequencies, long clearances and messages with a frequency change in the end, incorrect hear and read back and transmissions in local language. Pilots and ATC rely on the international emergency frequency 121.50 in case of failures and problems.

Pilots are trained and instructed to constantly monitor this frequency, however it is still widely used by ATC and others to perform operational and functionality tests or to use it in other cases than emergencies (e.g. in the UK where it is used for "practical intercepts"). As a result, this frequency is garbled with non-essential transmissions and the volume is sometimes turned down to guaranty primary contact.

Interceptions are a possible (security) response to this safety issue. Interceptions should be avoided if possible at all, not only because it is costly for governments, but also because it could introduce another safety issue, potentially frighten passengers and give bad publicity. If an interception is unavoidable it should be done in line with provisions of ICAO Annex 9433, Manual Concerning Interception of Civil Aircraft. No one should be held responsible for the costs of interception and no penalties of any nature should be imposed on individuals, unless there is a suspicion of gross negligence. In safety issues this principle is known as 'Just Culture".

© shutterstock

Several steps can be taken to overcome comloss and optimise communication between ATC and pilots which in turn prevents mistakes. These steps include the expansion of the use of datalink, the emergency frequency 121,50 should only be used for safety issues, the status of an aircraft should be investigated using other channels (i.e. ACARS, Datalink, Sellcall, via company and SATCOM). In addition, awareness needs to be raised within the aviation community regarding comloss through awareness campaigns and training.

One initiative that has been taken is EUROCONTROL's CIRS (Comloss Incident Reporting System) as a tool to support investigations, analyse occurrences and draw conclusions and recommendations. The CIRS system is currently only fed by information from EUROCONTROL's side (ANSPs and airlines are reluctant to feed information into the system, mainly due to a lack of resources and liability). As a result, the conclusions of the CIRS must be regarded as little reliable because they show only part of the picture.

Unmanned Air Vehicles & Remotely Piloted Aircraft Systems

An Unmanned Air Vehicle (UAV) or RPAS (Remotely Piloted Aircraft System) is an aircraft that is designed to operate with no human pilot on board. The number of RPAS is growing rapidly, and their size can vary from micro-devices of only 100 grams to high altitude/long range UAV of over 10,000 kg. Their uses vary widely from photography and surveillance to transport for civil and military goals. It is the expectation that the use of UAV's will continue to increase significantly.

This means that UAVs will increasingly utilise the same airspace used by commercial civil aviation. This will not only have safety implications for the industry; it will require a very thorough examination of the security ramifications of UAV operations. Let alone the unregulated UAVs in hand of private owners.

© shutterstock / funkyfrogstock

The safe integration of UAV operations into civil, non-segregated airspace can only be achieved if these UAVs are regarded in all ways as an aircraft, and they and their operations are subject to all existing rules and regulations applicable to the same class of manned aircraft. It is essential that UAVs fit into the existing and future Air Traffic Management environment in all respects. Security of UAV operations is a vital issue, with characteristics and considerations that are both similar and unique when compared with manned aircraft. As a remote pilot station is similar in purpose and design to a typical aircraft cockpit, it must likewise be secure from sabotage or unlawful interference.

© shutterstock / boscorelli

The security standards by which UAV systems are developed must be equivalent to those applied to manned aircraft. Therefore, all factors should be considered including, but not limited to, employees, location, accessibility, technology, design properties, link protocols, command structure, etc. The aircraft itself must be stored and prepared for flight in a manner that will prevent and detect tampering and ensure the integrity of vital components.

UAV systems should be able to prevent 'denial of service', assure 'integrity of data' and provide 'confidentiality of operations'. The protection of the data link, the authenticity of the user and the correctness of data transfer and processing should be protected against threats, attacks and acts of unlawful interference.

Additionally, steps must be taken to ensure that no additional software and/or hardware can be, or have been, added to any systems components for malicious use at a later date, and that hardware and software within all system components will perform the intended function only. In other words, it is essential to ensure that:

- No other function other than the one intended can be performed;
- All uploaded functions will be verified to ensure correctness and authenticity of transfer;
- All users of the system shall be authenticated to the system as authorised users of that system;
- All commands between the system components shall not be corrupted or interfered with
- All commands and/or transmissions between the system components shall be acknowledged. Personnel responsible for operating and remote controlling the UAV should be security background checked in accordance with national laws similar to airline pilots (same as for persons granted unescorted access to security restricted areas of airports).

The location and surrounding property of a remote pilot station shall be regarded as a security-restricted area of an airport, and should be guarded as such. Persons entering the premises of the remote steering facility should be screened in accordance with persons entering security-restricted areas (ICAO). Particular attention must be paid to the veracity and reliability of individuals entering these facilities, including extensive and robust background checks, and biometric identification systems.

Cyber Security

Attacks in the cyber domain are in the news all the time. Everybody knows they should have a virus scanner installed on their computer, not give their passwords away, and not to reply to phishing emails. Criminals and even foreign states are trying to hack into systems either to gather information, to manipulate data or to bring the system down.

Unfortunately, this caution and awareness has not yet been applied to aviation related systems. Operational information is not being protected sufficiently, and information received is too easily believed to be genuine and unaltered. On board system failures due to cyber attacks are believed to be too farfetched by many. ECA begs to differ.

Two decades ago aircraft systems were specifically designed to be used on board, connected to each other, but not the outside world. Cyber vulnerability was limited. But as the world has changed at a stunning pace, so has the aviation industry.

The number of systems on board an aircraft, in the air traffic control and in the airport safety-critical infrastructure has increased dramatically, and they are widely interconnected. Additionally, many airborne systems are connected to ground based systems. There are continuous maintenance connections, WIFI for passengers, systems to communicate with air traffic control, etc. At the same time aircraft manufacturers and airlines alike discovered it is cheaper to use commercial off the shelf devices in the aircraft, than designing specific ones.

In the current generation of aircraft there are networks, computers and protocols similar to the ones that can be found in factories and electric plants for example. Pilots are as dependent on external information as they are. So is there a reason why systems used in aviation would not be hacked? Should all received information be trusted unconditionally? Can the systems on board an aircraft be brought down? Furthermore, in modern aircraft, pilots cannot control the aircraft without the computer that translates their steering inputs into movement of the control surfaces.

It is vital to build awareness about the potential of cyber threats in aviation. Everyone involved in aviation operations should be made aware of the vulnerabilities and of the precautionary measures that can be taken. A potential attack needs to be identifiable and crew need to know how to react in the event of one.

Equally the integration of security systems at airports allow for real time data transmission. Modern security scanners are also based on computer systems. It is of outmost importance to protect these networks or else they could be rendered inoperative.

Cyber security should not be played down by the aviation industry. It should be part of the security plan every entity in the industry must have. Risk analyses have to be made. Information must be protected, the integrity of relevant messages guaranteed. Every company should appoint an executive responsible for cyber security. There are ISO standards ready to be used and that need to start being used today.

Conclusion

ECA promotes safe and secure flights while ensuring efficiency and competitiveness for European Airlines. Airline pilots play an important role in the security chain and are the last line of defence in most of the aircraft security incidents. They are entrusted and responsible for the safe carriage of passengers and cargo. Their role is and should further be recognised. Differentiation and alternative screening methods for pilots could free capacity that can be used for screening persons of whom the trust cannot be established.

In order to maintain a sustainable aviation security environment and ensure its efficiency, the current security methods and equipment used should be rethought and reshaped. Currently a number of initiatives are being tested around the world and we have to ensure joint consultation between governments, international organisation and any stakeholders organisation involved in the security chain.

New threats are permanently emerging and any new security environment should be able to offer the framework to address them and launch the appropriate response. The future security environment has to encompass measures based on appropriate risk assessments. ECA supports the introduction of risk based security measures under the pre conditions that they apply within a robust security management system. The last years have demonstrated that just adding new measures will not be productive but creates bottle necks in the check-in process of airports. Differentiation is part of the solution and it is a necessary tool to reduce queues at security checks, improve passengers' experience and increase security efficiency and effectiveness. As demonstrated by the Known Crew Member program in the US, pilots in Europe have a significant role to play. The introduction of an EU-wide crew ID card, based on biometrics, will be an important step in this respect. Any system should be flexible enough to address evolving threats and be understood by the flying public.

Public awareness, passenger information and appropriate personnel security training will facilitate the identification of a threat at an early stage. A combination of measures is necessary to allow authorities to focus on the threat posed by very few persons. Currently they do focus on a number of item and products, instead. Rethinking security measures finally implies the set up of pro-active measures and not only reactive ones.

ECA and its national Member Associations are committed to work hand in hand with the European Commission, EU Member States, the European Parliament and other aviation stakeholders to contribute to reshaping and strengthening aviation security.

Abbreviations

ACI – Airports Council International

ANSP – Air Navigation Service Providers

ASP – Airport Security Programs

ATC – Air Traffic Control

CBRNe – Chemical, Biological, Radio-active and Nuclear

CCTV – Closed-circuit television

CIRS – Comloss Incident Reporting System

CMC – Crew Member Certificates

CPSRA – Critical Parts Security Restricted Areas

DIRCM – Directed Infrared Counter-Measure

ECA – European Cockpit Association

EMS – Environmental Management System

EU – European Union

IATA – International Aviation Transport Association

ICAO – International Civil Aviation Organisation

IFALPA – International Federation of Air Line Pilots' Associations

IFSO – In-flight Security Officers

MANPADS – MAN-Portable Air Defence System

OHSMS – Operational Health and Safety Management System

QMS – Quality Management System

RAIC – Restricted Area Identity Card

RBS – Risk Based Screening

RPAS – Remotely Piloted Aircraft System

SeMS – Security Management Systems

SMS – Safety Management Systems

SOP – Standard Operating Procedures

SRA – Security Restricted Areas

TOC – Throttle Only Control

TSA – Transportation Security Administration

UAV – Unmanned Air Vehicle

Cover image © shutterstock / ssguy

About ECA

The European Cockpit Association was created in 1991 and is the representative body of Europan pilots at the EU level. It represents over 38.000 European pilots from the national pilots' associations in 37 European states.

European Cockpit Association - AISBL
Rue du commerce 20-22, 1000 Brussels
www.eurocockpit.be