SEVENTH FRAMEWORK PROGRAMME

AIRBUS
AN EADS COMPANY

DE LA RECHERCHE À L'INDUSTRIE
cea

EBS Business School

EOS
European Organisation for Security

Fraport

Fraunhofer
EMI

KLM
Royal Dutch Airlines

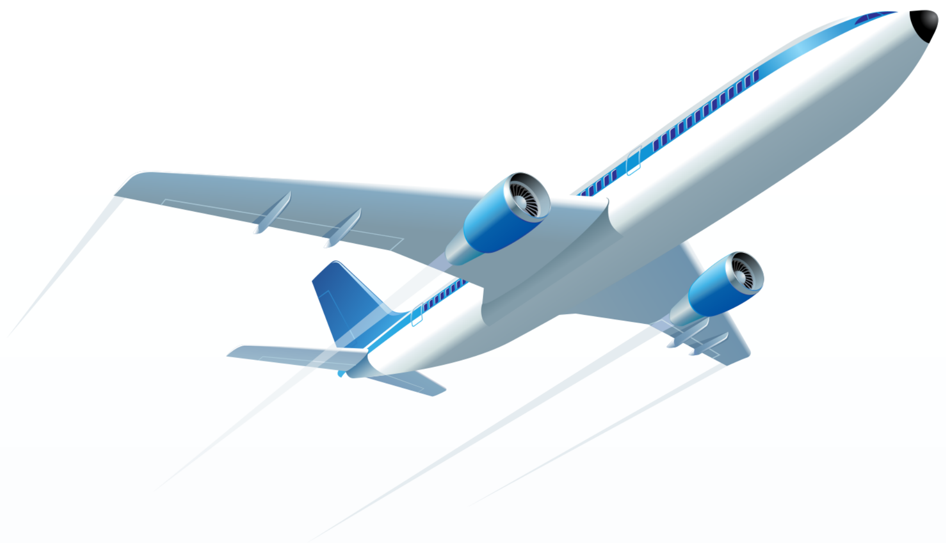
SAFRAN
Morpho

smiths detection
bringing technology to life

TNO innovation for life

Univerza *v Ljubljani*
Fakulteta *za družbene vede*

1961
2011



COPRA

Aviation Security Research Roadmap

Roadmap Document

D 5.1

Project co-funded by the European Commission within the Seventh Research Framework Programme (2007-2013)

Document Evolution				
Revision	Date	Organisation	Name	Reason of change
Rev. 0_9	20/02/2013	EBS	Christoph Georgi	Review
Rev. 0_9	20/02/2013	MPH	Stéphane Revelin	Review
Rev. 0_9	20/02/2013	UL	Iztok Prezelj	Review
Rev. 0_95	21/02/2013	TNO	Imelda van de Voorde	Update
Rev. 0_95	23/02/2013	EMI	Julia Ziehm	Review
Rev. 0_99	25/02/2013	TNO	Imelda van de Voorde	Update
Rev. 0_99	25/02/2013	EMI	Tobias Leismann	Review
Rev. 1_0	27/02/2013	TNO	Imelda van de Voorde	Update and finalizing

Executive Summary

This document is one of the three final deliverables of the EU funded project “COPRA Comprehensive European Approach to the Protection of Civil Aviation” within the Seventh Framework Programme. The project aims to develop recommendations for future research activities, which could lead to a more resilient, flexible and comprehensive approach. Previous work packages inventoried stakeholder requirements, the state of the art and current legal framework (WP1); collected current, emerging and new threats to airports, aircraft and auxiliary infrastructures (WP2); compiled security measures and security concepts to counter these threats (WP3); and assessed and prioritized the security concepts based on security benefit, costs, impact on the aviation system and public acceptance and constraints (WP4).

Based on these previous studies, a research roadmap was created consisting of three layers (WP5):

- Drivers and Trends in Future Aviation
  Developed by considering demographic, economic, social-cultural, technological, environmental and political factors (DESTEP), a total of 13 drivers and trends are considered most important in determining the shape of aviation security in the upcoming 15 years by the consortium and experts.
- Recommendations and Goals for Future Aviation Security Concepts
  Clustered into four headlines (Resilient, Comprehensive, Comfortable and Safe, Affordable and Efficient), a total of 23 recommendations and goals for Future Aviation Security Concepts have been compiled; eight for the short term (0-5 years), ten for the mid-term (5-10 years) and five for the long-term (10+ years).
- Recommendations on Future Research and Development
  Based on the previous two layers and the previous work packages, a total of 33 recommendations on Future Research and Development have been compiled; 21 for the short term (0-5 years) and twelve for the mid- to long-term (5+ years).

The third layer contains detailed recommendations for a European Research Agenda for Aviation Security. Tackling 70 existing and potential threats to aviation security identified during the COPRA project, the research roadmap supports the drafting of national and European research agendas that intend to create the knowledge and the technologies to ensure secure aviation in the years to come.

Abbreviations

COPRA	Comprehensive European Approach to the Protection of Civil Aviation
A/C	Aircraft
AIR	Airport
ATC	Air Traffic Control
ATM	Air Traffic Management
AUX	Auxiliary Infrastructure
BRIC	Brazil, Russia, India and China
CBRNE	Chemical, Biological, Radioactive, Nuclear and Explosive
CT	Computer Tomography
DESTEP	Demographic, Economic, Social-cultural, Technological, Environmental, Political
EC	European Commission
EM	Electromagnetic
EMP / EMI	Electromagnetic Pulse / Electromagnetic Impulse
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
FASC	Future Aviation Security Concept
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technology
ID	Identity Document
IED	Improvised Explosive Device
ISO	International Organization for Standardization
IT	Information Technology
JRC	Joint Research Centre
NRF	Nuclear Resonance Fluorescence
R&D	Research and Development
RFASC	Recommendation on Future Aviation Security Concept
RFID	Radio-Frequency IDentification
ULD	Unit Load Device
USA	United States of America
WP	Work Package

Table of recommendations

Recommendations and Goals on Future Aviation Security Concepts

Recommendations on Future Research and Development

Ref.	Recommendation	Page
a.	Countermeasures for IEDs, firearms and close range destructive threats	28
b.	Countermeasures for CBR threats	29
c.	Countermeasures for ground-to-air threats	30
d.	Countermeasures for ground-to-ground threats	30
e.	Countermeasures for cyber threats	31
f.	Countermeasures for electromagnetic threats	31
g.	Countermeasures for sabotage, seizure and hijacking	31
h.	Countermeasures for bluff threats and threats from social media	32
i.	Test-beds for aviation security purposes	32
j.	Aviation security research laboratories network	32
k.	Security performance assessment method (metrics, tools, process, etc.) for the entire security system	33
l.	Risk based and random security processes	33
m.	Automated bulk detection	33
n.	Multifunctional detection systems	34
o.	Automated systems for incident detection and response	35
p.	Self-healing and self-correcting security systems and structures	35
q.	Organisational framework and technical tools to continuously evaluate threats with all stakeholders	36
r.	Aviation security management system	36
s.	Methodologies for an iterative risk management approach	37
t.	Evaluate different security paradigms for aviation	38
u.	Joint risk and threat analysis platform for all stakeholders	38
v.	Community based approaches to increase resilience	38
w.	Assessment of public acceptance of security measures and effects on human rights	40
x.	Non-intrusive detection systems	40
y.	Quicker and more efficient security processes to improve passenger experience	41

Contents

Introduction

1.1 The COPRA Aviation Security Research Roadmap

Security has become a major factor in civil and commercial aviation. In recent decades, the number of threats to aviation security has grown significantly. This has led to even more security regulations as the threats evolved. Thereby, security procedures have become exceedingly complex, time consuming and invasive to passenger privacy. At the same time, passenger and cargo traffic are expected to double in the next 15 years. It is clear that the current complex security system cannot be adapted to such growth. It has already and will increasingly become a major market restraint.

Therefore, the project COPRA was initiated under the Seventh Framework Programme of the European Commission to develop requirements and recommendations for future research activities, which could lead to a more resilient, flexible and comprehensive approach.

To that aim, COPRA brought together a well-balanced consortium of research organisations, industry players and major air transport providers with a wide range of European stakeholders who contributed in expert workshops. Taking into account previous and existing activities in aviation security, COPRA partners and experts collected, analysed and categorised 70 current, emerging and new threats to airports, aircraft and auxiliary infrastructure. The team then went on to compile 387 possible security measures to counter these threats. Over 50 conceptual ideas for overarching approaches to passenger, cargo and external security concepts were identified and assessed according to the balance of security benefit, costs, impact on the aviation system and public acceptance and constraints. Using these results as a basis, the requirements for future research and development have been laid out in the **COPRA Aviation Security Research Roadmap**.

The present document describes this roadmap in detail. A separate deliverable (D5.3) gives a visual overview of the roadmap.

1.2 Objective of the Roadmap

The COPRA Aviation Security Research Roadmap has been developed in the final Work Package of the COPRA project. The goal of the roadmap is:

’To provide the European Commission and the Member states with clear guidelines for future R&D activities responding to operational and economic market needs while being attentive of the acceptance by citizens’

The input for these guidelines are gathered throughout all previous work packages of the project and especially the expert workshops that were held. In a structured roadmap process, the results of the previous tasks were analysed and discussed to eventually become a roadmap that gives structured and motivated recommendations for future aviation security concepts as well as research and development requirements to be able to tackle the current and future challenges in European aviation security.

1.3 Roadmap Structure

Technology roadmapping has been one of the most widely used and appreciated methodologies for innovation management planning in the last 15 years. Developing technology roadmaps supports organizations to make solidly based decisions on future R&D areas that need to be addressed in order to be prepared for future challenges and ambitions.

Although there are many ways to create and present a roadmap, the overall framework of a roadmap is always based upon a layered structure that can also be recognized in the COPRA roadmap. Figure 1 shows the general outline as applied for COPRA.

A roadmap looks at the topic of interest from different 'viewpoints' or 'perspectives'; these perspectives are generally called **roadmap layers**. There can be many perspectives, depending on the level of detail of the roadmap, but the three main perspectives are always:

- Strategic perspective
  In this layer the 'WHY-question' for innovation is answered. What are the strategic considerations for innovation? Items described in this layer can be based upon the internal strategic goals and ambitions of an organisation, but also on external factors such as drivers, trends, threats etc. For the COPRA roadmap this layer contains the **drivers and trend in future aviation** that are most relevant for future innovations in aviation security systems.

- Functional perspective
  This second layer describes WHAT should be done or developed to reach, tackle or be prepared for the items that were described in the strategic layer. In general, this can be either products, capabilities or concepts. Although some specific aviation security concepts were identified in WP 3 of COPRA, it was decided not to recommend specific concepts in this layer, but to give more general recommendations and goals for future aviation security concepts.

- Resources perspective
  The third layer describes the HOW, i.e. the technologies and other resources that are necessary to be able to develop the products, capabilities and/or concepts described in the functional layer. In the COPRA Aviation Security Research Roadmap, this layer gives recommendations for future research and development. This is the actual research agenda that the consortium recommends and that will contribute to and address the current and future challenges in aviation security.

Because a roadmap is a plan, it has a timeframe. For the COPRA roadmap a three-window timeframe was used: A short term timeframe with a horizon of 5 years, a mid-term timeframe with a horizon between 5 and 10 years and a long term timeframe with an horizon of 10 years plus.

However, this three-window timeframe was not used for all three layers of the roadmap: The trend and drivers have no time dimensions and the recommendations for future research and development are plotted only on the short term (0-5 years) and mid/long term (5+ years) timeframe.

A very important aspect in a roadmap process is that both technology push and technology pull forces are addressed. Especially in defining the elements of the functional and the technological layers, not only technologies that are needed for the functions should be defined (top down), but also functions that derive from new technological possibilities should be considered (bottom up).

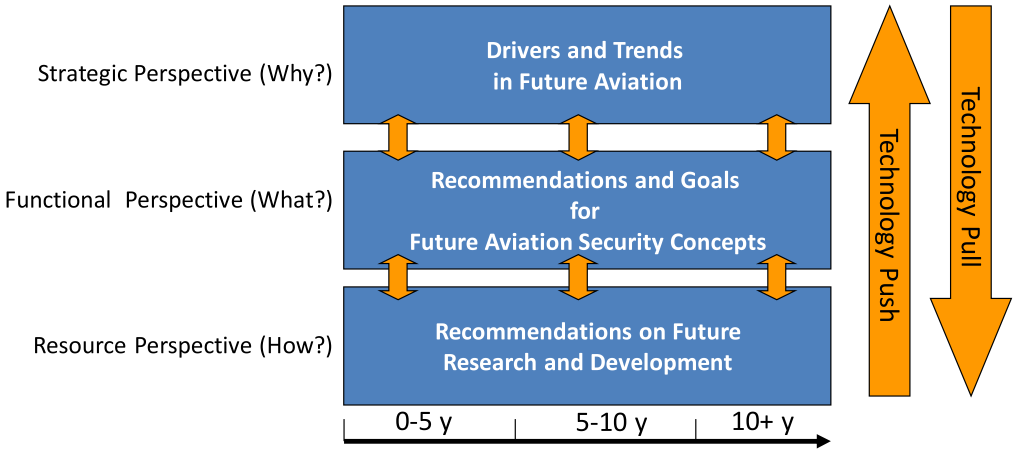

Strategic Perspective (Why?)
Functional Perspective (What?)
Resource Perspective (How?)
Drivers and Trends in Future Aviation
Recommendations and Goals for Future Aviation Security Concepts
Recommendations on Future Research and Development
0-5 y
5-10 y
10+ y
Technology Push
Technology Pull

Figure 1 **COPRA Roadmap Structure**

1.4 Roadmap Development Process

The Roadmap is the final deliverable of COPRA. All consortium partners and expert groups were involved in the developing process of the roadmap. Input to this process were the results and deliverables of the previous work packages, especially the requirements, future and emerging threats, possible security measures and possible security concepts.
The roadmap was developed in seven phases:

1. A one day consortium workshop in Ljubljana on September 19 2012. At this workshop, the roadmap structure was determined and a first set of possible roadmap elements was drafted for all three layers of the COPRA Research Roadmap.
2. A desk research period in which all consortium partners worked on long-lists of roadmap elements for each of the three layers. In this process all previously developed deliverables of the COPRA project where used as input. In the final long-lists approximately 40 drivers and trends, 50 goals and recommendations on future concepts and 50 research topics were identified.

3. A two day consortium workshop in The Hague on November 21 and 22 2012. At this workshop the long-lists were discussed, clustered and condensed to become the short-lists of 13 drivers and trends, 23 recommendations and goals on future security concepts and 33 research topics contained in the roadmap now.
4. A first draft of the roadmap was created, based upon the outcome of the two day consortium workshop.
5. A consortium review in Toulouse on January 10 and 11 2013. The roadmap draft was reviewed and discussed by the consortium partners.
6. The draft version was presented at the COPRA Final Seminar on January 30 2013 in Brussels.
7. Finalisation of the roadmap using input from the expert groups and a final review by all consortium partners and the coordinator until February 28 2013.

1.5 Roadmap manifestations

The COPRA Aviation Security Research Roadmap is presented in two ways.

First, a **visual representation** of the roadmap with all roadmap items plotted in a chart was designed (Page 14). This chart is deliverable D5.3 of the COPRA Project and is also included in this deliverable. It can be printed and handed out on A3.

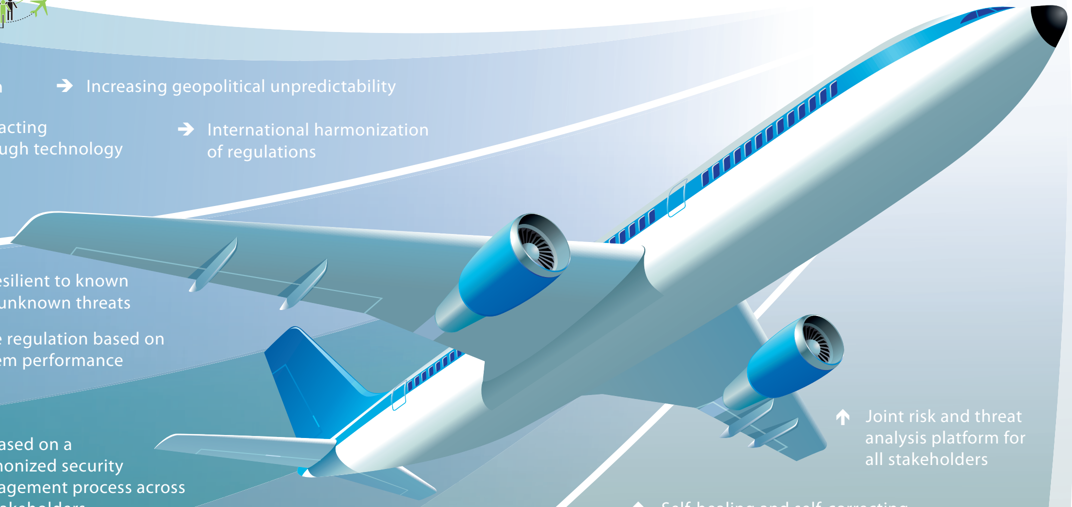
The advantage of the visual representation is that it shows the roadmap at one glance in its entirety. However, only very little information can be added about the considerations, backgrounds and details of the roadmap items. Therefore the roadmap is also described in detail in this **roadmap document report**, deliverable D5.1.

COPRA

AVIATION SECURITY RESEARCH ROADMAP

DRIVERS AND TRENDS IN FUTURE AVIATION

- → Increasing number of passengers
- → Higher capacity aircraft
- → Privacy concerns
- → Proliferation of technology and information
- → Increasing geopolitical unpredictability
- → Increasing number of aircraft
- → Increasing global competition
- → Demand for safe, comfortable and less intrusive checks
- → Increase of interacting capabilities through technology
- → International harmonization of regulations
- → Increasing costs for security
- → Demand for quicker process time of checks
- → Quickly evolving technology development



RECOMMENDATIONS AND GOALS FOR FUTURE AVIATION SECURITY CONCEPTS

0-5 YEARS → 5-10 YEARS → 10+ YEARS →

RESILIENT

- ↗ Be resilient against current and emerging threats
- ↗ Be measurable in terms of the entire security system performance
- ↗ Cover and balance the complete resilience cycle
- ↗ Be easily adaptable and flexible
- ↗ Include risk based measures
- ↗ Be resilient to known and unknown threats
- ↗ Have regulation based on system performance

COMPREHENSIVE

- ↗ Address both physical and cyber threats targeted at all stakeholders including security systems
- ↗ Address technical, organisational and human related issues combined
- ↗ Include a comprehensive aviation security management system to be shared by all stakeholders
- ↗ Be based on a shared strategy
- ↗ Be based on a harmonized security management process across all stakeholders

COMFORTABLE AND SAFE

- ↗ Consider the appropriate communication
- ↗ Consider the effect of security measures for all relevant stakeholders
- ↗ Require no divesting of personal items
- ↗ Consider social and ethical aspects of security measures
- ↗ Be a quick and seamless process for persons and goods
- ↗ Be safe for passengers, staff and goods
- ↗ Have a seamless, comfortable, acceptable and safe security process for relevant stakeholders

AFFORDABLE AND EFFICIENT

- ↗ Be measurable in terms of efficiency
- ↗ Be based on a business case for security
- ↗ Be integrated with the economic management tools and systems of the aviation system
- ↗ Have an aviation security system that remains affordable and efficient

RECOMMENDATIONS ON FUTURE RESEARCH AND DEVELOPMENT

0-5 YEARS → 5+ YEARS →

- ↑ Joint risk and threat analysis platform for all stakeholders
- ↑ Self-healing and self-correcting security systems and structures
- ↑ Performance assessment method (metrics, tools, processes, etc.) for the entire security system
- ↑ Automatic detection by new imaging technologies of potentially dangerous items
- ↑ New process flows with focus on increasing throughput
- ↑ Flow performance management of the entire security system
- ↑ Automated systems for incident detection and response
- ↑ Community based approaches to increase resilience
- ↑ Multifunctional detection systems
- ↑ Evaluate different security paradigms for aviation
- ↑ Integrating multiple security systems (technical, processes, actors)
- ↑ Aviation security management system
- ↑ Automated bulk detection
- ↑ Countermeasures for ground-to-air threats (such as manpads and laser dazzling)*
- ↑ Countermeasures for bluff threats and threats from social media*
- ↑ Applicability of economic models on security and the transparency of these models
- ↑ Test-beds for aviation security purposes
- ↑ Quicker and more efficient security processes to improve passenger experience
- ↑ Countermeasures for sabotage, seizure and hijacking*
- ↑ Countermeasures for ground-to-ground threats*
- ↑ On-the-fly biometric identification and verification
- ↑ Risk based and random security processes
- ↑ Assessment of public acceptance of security measures and effects on human rights
- ↑ Countermeasures for cyber threats*
- ↑ Non-intrusive detection systems
- ↑ Aviation security research laboratories network
- ↑ Measurability of the (cost-)efficiency of the entire security system
- ↑ Organisational framework and technical tools to continuously evaluate threats with all stakeholders
- ↑ Countermeasures for IEDs, firearms and close range destructive threats*
- ↑ Countermeasures for CBR threats*
- ↑ Countermeasures for electromagnetic threats*
- ↑ Security performance assessment method (metrics, tools, processes, etc.) for the entire security system
- ↑ Methodologies for an iterative risk management approach

** = as identified in COPRA*

2 The Strategic Perspective: Drivers and Trends in Future Aviation

The top layer of the COPRA Research Roadmap shows the key drivers and trends in future aviation. This layer presents the palette of rationales for future innovation in aviation security. It is in a sense thus the foundation of the research roadmap.

Within this layer, factors have been captured that have an important influence on the (shape of the) future aviation security. If a specific direction of this influence is expected (e.g. growing or shrinking) we call this factor a **trend**, while for **drivers** it is still unclear in which direction the influence will manifest.

Of course there are many drivers and trends which will influence the aviation security system. In this research roadmap though, only the drivers and trends are included that seemed to the consortium and experts most important in determining the shape of aviation security in the upcoming 15 years.

2.1 Drivers and Trends

The list of drivers and trends is developed by considering demographic, economic, social-cultural, technological, environmental and political factors (DESTEP). First a long list was established, of approximately 40 drivers and trends. In a consortium workshop, this list was reduced to the list captured in the research roadmap. In the resulting short list, trends are discernible by specific words in their description denoting the expected direction (e.g. “increasing”, “quicker”). Drivers do not have such a designation in their description.

The drivers and trends captured in the COPRA Aviation Security Research Roadmap are:

- **Increasing number of passengers**
  Passenger and cargo traffic are expected to double in the next 15 years. Furthermore, a shift may be expected in the regions of origin. It is widely recognised that the current complex security system cannot be adapted to such growth. It has already and will increasingly become a major restraint. So the increase in passengers (and cargo) will definitively have an important influence on the shape of aviation security in the future.
- **Higher capacity aircraft**
  A tendency is that aircraft get larger, carrying more passengers and/or more cargo at once. This implies an increased amount of passengers and cargo will need to pass security at the same time. The security system thus needs to be able to cope with higher peak loads (not only with the general increase due to the previous trend).
- **Increasing number of aircraft**
  Given the expected growth in passengers and cargo, an increase in the number of aircraft should also be expected. This implies that airports need to be able to process an increasing number of aircraft, aggravating the security around air traffic control, airplane manoeuvring, piers, etc.
- **Increasing global competition**
  The increase of global competition, for instance industry players from BRIC countries, but also between different carriers, is also likely to transform the shape of aviation security in the future.

- **Demand for quicker process time of checks**
  Quicker process times are not only important from the passenger perspective, who want to pass security quickly and with the least hassle possible. But also from an economic perspective this is an important trend for both the operator and other stakeholders at the airport (such as retail).
- **Increasing costs for security**
  There are many ways in which costs for security will increase in the upcoming years, e.g. increase of labour costs, increase in number of passengers and cargo that need to be checked, increase in costs of operating security systems.
- **Privacy concerns**
  Privacy concerns entail both physical aspects, like pat-downs at security checks, and digital aspects, like the use and exchange of data. It is considered a driver, because although people are currently very concerned with privacy, there is also a movement (especially in social media) which shows this may change in the upcoming future.
- **Demand for safe, comfortable and less intrusive checks**
  The demand for safer, comfortable and less intrusive checks is not only important from the passenger perspective, who want to pass security in a safe and comfortable manner with the least hassle possible. But also for other stakeholders this is a factor of influence, as it will improve understanding, behaviour and utilization of security by passengers and, as such, increase efficiency.
- **Quickly evolving technology development**
  Technology is evolving at a very high speed, making more effective and efficient systems and processes available long before the old ones are obsolete. Even if the technology of the near future is not known yet, it would be wise to take them into account by designing security systems and processes that are flexible. Keeping the possibility to adjust or replace part of the security system with newer technologies.
- **Proliferation of technology and information**
  Partly due to the previous trend, there is an acceleration of the adoption of new technologies, enabling a broadening public to use such new technologies. It is also easier for people to be aware of how new technology may be misused, maliciously or just ignorantly. Therefore proliferation also causes an increase in available weapons, as even apparently harmless technologies may be misused to instigate (new) threats.
- **Increase of interacting capabilities through technology**
  In aviation there is a steep increase in (inter)connectivity, interactivity and interacting capabilities. Not only for crew and maintenance, as part of the operation of airlines and airports, but also for the passenger enjoying and demanding in-flight information, communication and entertainment. This development and the increased dependency on such capabilities, elicit the need for further and new types of (digital) security. It is a new dimension to take into account, which alters (the shape of) aviation security.
- **Increasing geopolitical unpredictability**
  It is expected that the geopolitical unpredictability in the world will not yet fade, resulting in a more divers palette of states with diverging security levels. Aviation security should be able to cope with such diversities, still ensuring an adequate level of security.

- **International harmonization of regulations**
  The need for harmonization of regulations becomes more and more apparent. This may be even broadened outside of the EU, by including the USA, Canada, Australia, Asia, etc.

3 The Functional Perspective: Recommendations on Future Aviation Security Concepts

The second layer of the COPRA Research Roadmap consists of recommendations on future aviation security concepts (FASC). These recommendations and goals are clustered into four headlines, since the general recommendation is that FASCs should be:

- Resilient
- Comprehensive
- Comfortable and Safe
- Affordable and Efficient

These headlines should not be thought of as isolated themes – they are tightly connected and mutually interdependent. This chapter contains a description for each headline as well as the recommendations and goals therein as proposed by the COPRA consortium. The proposed recommendations will address and contribute to the current and future challenges in aviation security. For ease of reference, the recommendations are listed with an individual upper case letter.

3.1 Resilient

3.1.1 Description

Within COPRA, resilience is defined as the ability to

- prepare (take into account),
- prevent (repel or thwart),
- protect against (absorb or mitigate),
- respond to (cope with) and
- recover from (and adapt to)

real or potential adverse events. In a general sense, adverse events are either catastrophes or processes of change with (possibly) catastrophic outcome, which have human, technical or natural causes. As COPRA is only concerned with security (not safety), all adverse events considered are man-made and the nature of these events is malicious.

The above definition can be depicted in a cycle of consecutive phases (Figure 3). Attending to the full resilience cycle, utilising all phases as fully as possible, enables synergetic combinations of measures and the possibility to learn from (and thus also adapt to) security incidents occurring in aviation.

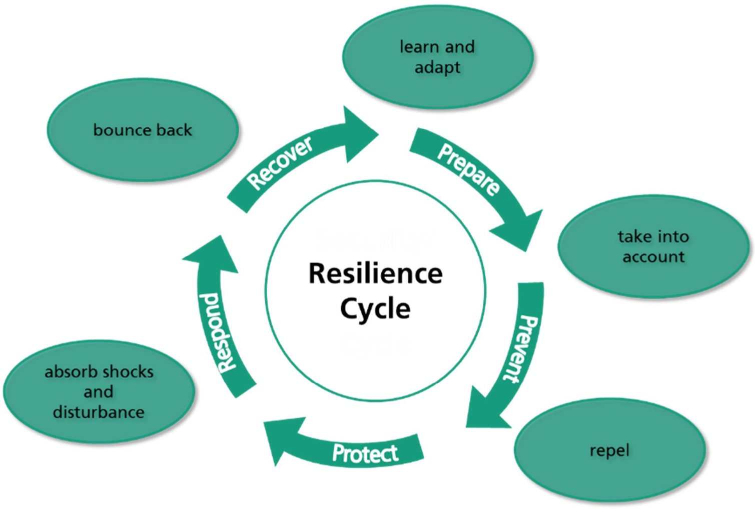


Figure 3: Resilience cycle depicting possible actions associated with the different phases.

The aviation security system should be resilient to the evolving threat situation. It should therefore be based on the complete resilience cycle of “prepare, prevent, protect, respond and recover”. This should enable stakeholders to “learn and adapt” instead of exclusively be ruled by reactive, strict and inflexible regulations.

Currently, aviation security is primarily based on the preventive phase and is inflexible to new threats. This is also mirrored in the research landscape for aviation security: Most projects concentrate on preventive measures such as the detection of CBRNE-substances. COPRA recommends that the future aviation security system (and research) should be based on all elements of the resilience cycle in a well-balanced composition. It should embrace processes and technologies to support each phase of the resilience cycle.

3.1.2 Recommendations and Goals on Future Aviation Security Concepts

On the short term (0-5 years), it is recommended that security concepts should

A. **Be resilient against current and emerging threats**
During the COPRA project and in one of the workshops, together with a broad spectrum of stakeholders, an assessment was made of current and emerging threats to the aviation security system. It is advised that security measures and concepts should take into account at least all these threats. For the purpose of the research roadmap, these current and emerging threats have been clustered into the following eight threat categories:
    - IEDs, firearms and close range destructive threats
    - CBR threats
    - Ground-to-air threats
    - Ground-to-ground threats
    - Cyber threats
    - Electromagnetic threats
    - Sabotage, seizure and hijacking
    - Bluff threats and threats from social media

B. **Be measurable in terms of the entire security system performance**
This is a prerequisite to some of the other short- and mid-term recommendations because

having the tools to measure the security performance is crucial when desiring to improve the security system. Especially when the entire system needs to be improved as a whole, allowing local decreases/downgrades as long as the overall performance improves.
There has already been done some research in this direction. However, the challenges raised in this field are rather large and need more research effort in order to tackle them convincingly.

On the mid-term (5-10 years), it is recommended that security concepts should

C. Cover and balance the complete resilience cycle

Nowadays, the high security standard in the passenger critical part of the airport is mostly ensured by the security check point, which bundles all detection systems to avoid dangerous objects in sensitive areas. It represents the "last-line-of-defence", which gives this single process element the ultimate significance to ensure security. It also makes the checkpoint complex, puts a lot of pressure on the security staff at the checkpoint, causes waiting lines at peak hours and allows for malicious persons to study all sub-processes trying to find a weakness that might be exploited. Once a dangerous object passes this last-line-of-defence, its use cannot be inhibited and the bearer will be unhindered to pursue any malicious objective.
Instead, security concepts should aim at involving different measures at different stages of the passengers' travel. The measures should be adequate for the respective stage and even further reduce the risk of attacks. The security concepts should thus make sure not only to concentrate on the prevention of dangerous objects to be brought into the airport or aircraft, but also should contain elements of the other phases of the cycle. E.g., measures in the "protect" phase of the cycle could remove the need for prevention of tiny incidents or could mitigate large events to make them manageable; measures in the "prepare" phase could take into account analysis of evolving threats in order to be able to adjust the other phases accordingly. Measures at each phase should thus correspond and connect to measures in the other phases of the resilience cycle.
Therefore, covering and balancing the complete resilience cycle means that as much emphasis as required is to be put on

- pre-incident issues (i.e. prepare, prevent),
- inter-incident issues (protect) and
- post-incident issues (respond, recover).

D. Be easily adaptable and flexible

In order to obtain a security system (and according regulation) based on system performance, it is necessary to be able to easily adapt this system and be flexible to new threats or to temporary changes in the significance of threats. As threats will change, the system needs to be adjustable accordingly.This is an important prerequisite to goal F. Only a system that is easily adaptable can react quickly to a new and previously unknown threat situation.

E. Include risk based measures

A risk refers to all feared events performed by malicious people with the intention to damage or disrupt. A risk is a combination of likelihood and impact associated with such an event. The likelihood is the probability of occurrence, while the impact expresses all the possible consequences among different dimensions (casualties, delays, damage, etc.) in case of such an event. The risk level is a quantitative value of the risk, a combination of likelihood and impact, established in the risk assessment.

Risk based measures should be included in aviation security, e.g. by detecting both persons with malicious intentions and dangerous items at the security checkpoints for cargo and passengers. As of today, some bulk detection systems for hold luggage are crudely risk based (on the destination and origin). The potential of using risk-based processes and algorithms must be explored much further, taking into account not only destination data but extending this approach to e.g. cargo, passengers and carry-on luggage.

On the long term (10+ years), it is recommended that security concepts should aim to

F. **Be resilient to known and unknown threats**
In recent decades, the number of threats to aviation transport has grown significantly and this growth has not yet come to a standstill. Of course it is imperative that dangerous objects and materials are not introduced into certain areas, where they potentially may lead to catastrophic results. Therefore, technology will always be crucial to detect those objects. Yet, what exactly constitutes as being a "dangerous object" has evolved and will evolve further in the years to come. An even further evolvement is that threats might also be derived from other threat vectors, which are not based on objects. For instance, harm can also be done by abusing information and communication technologies. To have a resilient and comprehensive approach, not only dangerous objects but also the perpetrator himself needs to be considered and hindered to get into critical areas, both physically and in networked ICT systems.

G. **Have regulation based on system performance**
Currently, regulation prescribes the items which are prohibited in aviation and the ways how to make sure such items are barred. However, as threats change and new innovative ways to exert them arise, this implies a constant need for additions to the existing security system. This does not only take time (resulting in a security system which actually is out of date most of the time) but also increasingly strains the security system by adding security measures on existing ones without considering a more integrated approach.
There is only one way to be able to cope with the everlasting changing landscape of threats and actors in aviation. This is to prescribe performance levels for security concepts instead of rigid single actions focusing on prohibited items. This way, the aviation security system can be adjusted as soon as the need occurs to be fully prepared for all threats relevant at that specific moment.

3.2 Comprehensive

3.2.1 Description

Aviation security involves the actions and interactions of a wide range of actors. Each actor constitutes an integral part of what can be called the "Aviation Security System". Together, all actors strive towards the common goal of secure civil aviation: protecting persons, goods and assets against potential adverse events. At the same time, each actor brings its own perspective and requirements and tries to achieve own goals, which might diverge from each other. Improvement or optimization of the status quo for a single stakeholder or even several stakeholders not seldomly cuts short on the overall objective of improving the aviation security system in its entirety. Therefore, it is necessary to consider aviation security in its comprehensiveness, rather than as a collection of separate and disconnected stakeholders and measures. This is necessary to be able to make aviation security sustainable for the expected growth in air traffic and to ensure security in the years to come.

Therefore, within COPRA aviation security is deemed comprehensive if

- it encompasses all different stakeholders
  (such as airports, airlines, public authorities, industry, passengers, freight forwarders, etc.)
- it addresses all (sub)purposes
- it covers the entire end-to-end path
- it is coherent and overarching

This headline thus comprises recommendations on future aviation security concepts that support the efforts of including all air transport stakeholders and addressing the threats they encounter.

A comprehensive view must be adopted to reach an aviation security system which works for all participants of the system. By addressing (the needs of) all stakeholders and trying to reach the perfect balance of all different requirements, the system itself can be improved. This becomes more and more important in an increasingly complex/polarized environment with a growing number of (global) actors involved in the system. Understanding the complexities of the system and the evolving threat situation in its entirety will support finding the right balance for all stakeholders while developing the security concepts of the future. This will make security concepts sustainable for the expected growth in air traffic and ensure its security in the years to come.

3.2.2 Recommendations and Goals on Future Aviation Security Concepts

On the short term (0-5 years), it is recommended that security concepts should

H. **Address both physical and cyber threats targeted at all stakeholders including security systems**
The protection of stakeholders’ assets is the general goal of an aviation security system. “Asset” is a very general term that describes something of value which needs to be protected against all forms of threats. Its most important one includes the protection of the lives of passengers and staff, but can also refer to the protection of infrastructures, goods, the continuation of business processes, etc.
The protection of the security measures themselves is a means to ensure the continuation of security (and therefore the protection of assets), which is gained by implementing that measure. Security measures can, on the one hand, be disabled in order to not being able to perform the tasks (surveillance camera which is physically destroy or cut off from the surveillance system). On the other hand, security measures can be altered with the same goal of not correctly performing its task (e.g. surveillance camera showing recorded material to avoid detection).
Both need to be addressed to ensure secure aviation, where all types of threat need to be considered simultaneously and all stakeholders comprehensively, to ensure everything is covered in its entiety.

I. **Address technical, organisational and human related issues combined**
Complex and critical security activities still rely on human actions, especially as a central precondition for good decisions and handling of nonconformities. In spite of the fact that the human beings in the system can make mistakes, they are also a source of robustness and have the, sometimes, necessary ability to improvise in the event of an unexpected course of

events. Increased knowledge of the interaction between technical and organisational elements - and the people using these - is crucial. It will improve the interaction between people and technology/organisation.
There are many technical, organisational and human factors which need to be addressed when (the operation of) security systems are concerned. On each factor there has already been done research, enabling knowledge on how to address this factor. However, it is imperative to look at all factors in coherence, to view them as combination including interdependencies and address them comprehensively. Although such research has also been conducted, it is recommended to put more effort into this to tackle such issues more convincingly.

On the mid-term (5-10 years), it is recommended that security concepts should

J. **Include a comprehensive aviation security management system to be shared by all stakeholders**
In order to have a harmonized security management process across all stakeholders in the end, one of the steps is to achieve a security management system that all stakeholders are willing to employ and possibly even share. Using the same management system enables a common approach for risk analysis, threat and performance assessment of the security system.

K. **Be based on a shared strategy**
Harmonization and a comprehensive approach in aviation security's complex environment with its many stakeholders, each bringing their own perspective and requirements, is infeasible without a shared strategy as basis. There should be a consensus of the common aviation security objectives and the methods employed to reach this objective, which need to be shaped by all stakeholders of the aviation security system. Only by knowing the common strategy, possible further harmonization efforts can be widely accepted and implemented.

On the long term (10+ years), it is recommended that security concepts should aim to

L. **Be based on a harmonized security management process across all stakeholders**
Aviation allows people and goods to move nationally and internationally. Therefore, the different stakeholders of the aviation security system are confronted with different state authorities and regulations. The harmonization of the management process is one way to reduce the challenges posed by compliance efforts. It increases transparency and, thereby, acceptability of the entire system by all stakeholders. It also makes other objectives easier to reach, such as having regulation based on system performance.

3.3 Comfortable and Safe

3.3.1 Description

It is recommended that future aviation security concepts are comfortable and safe for all stakeholders. In this research roadmap, "comfortable" entails a quick flow and no intrusiveness (both of persons and goods), user friendliness and good service. "Safe" involves minimizing the impact on health, environment, privacy and damages to goods.

All relevant stakeholders should be taken into account – not only the passengers/goods that need to be checked. For instance, the impact on health should not only be considered for passengers going through security checks but also for the occupational safety of operators/staff who are engaged in work concerning aviation security.

Therefore, within COPRA, an aviation security system is deemed comfortable if it is/has

- Quick (flow of persons and goods)
- Not intrusive
- User friendly
- High service-level

and it is deemed safe if it has no/minimal impact on

- Health
- Goods (damage)
- Privacy
- Environment

Note: Privacy is part of comfortable as well as safe. For comfortable it is part of "not intrusive" (both physically and digitally). For safe it is mentioned explicitly, as this entails the information of each stakeholder is not misused and is protected against misuse by thirds.

3.3.2 Recommendations and Goals on Future Aviation Security Concepts

On the short term (0-5 years), it is recommended that security concepts should

M. Consider the effect of security measures for relevant stakeholders
When considering (the implementation of) new security measures, it is important to consider all different types of effects the measure may have on all relevant stakeholders. This does not only include health, social and ethical issues (which are addressed in a separate recommendation). E.g., also effects on and restrictions due to existing infrastructure should be taken into account.

N. Consider the appropriate communication
Skepticism of the new and unknown is a basic sentiment of many. If that "new" changes the known system, which has kept a population secure for a long time, the reaction to it might not only be based on logic but, instead, be emotional. If, on top of that, misinformation is brought in the mix, a potentially helpful device or procedure might not be accepted by the public. Even an information campaign afterwards might not be able to change that. Thus, security concepts should consider from the start the effect the suggested change might have on the public as well as on all stakeholders. The information strategy should be an integral part of the concept development and involve all relevant stakeholders. Communication in a clear and transparent way will create more support for security measures by stakeholders. It will also help them in understanding the measure better, being less disturbed by it. Knowing what is expected will in turn even speed up the security process. At the same time any security measures must remain unpredictable for potential perpetrators.

O. Require no divesting of personal items
It is recommended to strive for a security system in which passengers do not need to remove items from their carry-on luggage or clothing, such as belts and coats, during the security check. This will not only improve passenger experience but also the flow performance (throughput) and the efficiency at security checkpoints.

On the mid-term (5-10 years), it is recommended that security concepts should

P. **Be a quick and seamless process for persons and goods**
This topic addresses the speed of the security checks as well as its user friendliness. A process is considered seamless when passengers, staff and goods do not have to stop for security checks. The necessary checks should be performed while moving through the airport (or even before arriving at the airport). To ensure a seamless process future aviation security processes should be as automatic as possible. This will improve the throughput. Moreover, to achieve a fully seamless experience, future aviation security concepts should be optimized from a logistical perspective.

Q. **Consider social and ethical aspects of security measures**
Although this is of course part of any security measure/system, social and ethical aspects are considered important to be explicitly included as recommendation. It is to be ensured that no issues from a social or ethical perspective arise once new security systems emerge in the future.

R. **Be safe for passengers, staff and goods**
Similar to the previous, this is a general recommendation which is part of any security measure/system. But as new (maybe even radically different) security systems may emerge on the short- or mid-term, safety needs are required to be kept aligned. Not only health issues for passengers (to be checked) but also occupational safety and health issues of staff and other people in the vicinity of security checks need to be addressed. Potential sources of damage to goods should also be taken into consideration.

On the long term (10+ years), it is recommended that security concepts should aim to

S. **Have a seamless, comfortable, acceptable and safe security process for relevant stakeholders**
Demands of passengers and freight-forwarders evolve. One demand is an evermore quicker and less intrusive process at security checks. In order to meet such demands, it is necessary to have a security process which is seamless, comfortable and, of course, safe for all relevant stakeholders. If the security process is not acceptable, other modes of transport will be prefered, effectively rendering security superfluous as aviation itself depends on people willing to travel or send goods by air.

3.4 Affordable and Efficient

3.4.1 Description

Affordability and efficiency are two aspects that are very important in any business. Within COPRA, we have the following understanding of these aspects:

- Affordability
  A security system is affordable as long as the cost do not exceed the price the customers are willing to pay. The lower the costs are, relative to the amount the customer is willing to pay, the higher the affordability.
- Efficiency
  Efficiency describes the extent to which all resources (time, effort and/or cost) are well

used for the intended purpose[1]. It is an important factor in determining performance. Efficiency is an important attribute because resources are scarce. Time, money and raw materials are limited, so it makes sense to try to conserve them while maintaining an acceptable level of security. To be efficient, a security system should thus aim for an optimal balance between resources needed and security level achieved (cost-benefit).

Thriving towards a higher efficiency, thus reducing the use of resources (e.g. cheaper, smaller, quicker, more automated processes) and/or raising the performance level, is part of achieving a (more) affordable security system.

3.4.2 Recommendations and Goals on Future Aviation Security Concepts

On the short term (0-5 years), it is recommended that security concepts should

T. Be measurable in terms of efficiency
This is a prerequisite to some of the other short- and mid-term recommendations as having the tools to measure the efficiency is crucial when desiring to improve the security system. Especially when the entire system needs to be improved as a whole, allowing local decreases/downgrades as long as the overall performance improves. There has been some research in this direction: efficiency is measurable for certain security measures, but not in a general sense and as part of a larger or even the entire system. The challenges raised in this field are extensive and need further research efforts in order to tackle them convincingly.

On the mid-term (5-10 years), it is recommended that security concepts should

U. Be integrated with the economic management tools and systems of the aviation system
Having management tools and systems specifically for aviation security is obviously useful. However, having them integrated with the aviation system management is even more useful, as common causes, trends or emerging features may be easier to find when addressing security not by itself but as part of aviation. This will give the opportunity to steer aviation and its security in coherence, enabling synergies and the possibility to strengthen the system as a whole.

V. Be based on a business case for security
In order to make proper choices between different ways to ensure security (measures, concepts, etc.) it is important to build a business case, capturing the rationale behind and expressing the value of alternatives. This will ensure for the chosen option that required capabilities are available, resources are used most efficiently, the necessary performance is achieved, inter-dependencies are covered, etc.

On the long term (10+ years), it is recommended that security concepts should aim to

W. Have an aviation security system that remains affordable and efficient
It should be clear that any aviation security system should be affordable and efficient – this is currently the case. However, given the proposed research and extensions to the system, the security system may be changed dramatically. It needs to be ensured that any changes will not lead to a situation in which affordability and efficiency conditions are no longer

[1] Not to be confused with effectiveness, which is mainly concerned with how well objectives are achieved. This difference can also be illustrated by the saying "Efficiency is doing things right, while Effectiveness is doing the right things." Effectiveness is therefore included in the headline Resilient.

met.
Also, this goal is to be seen as an integrated matter: It should be at the base of any research activities to think about affordability and efficiency (including the related short- and mid-term recommendations in this headline).

4 The Resource Perspective: European Research Agenda for Aviation Security

The third layer of the COPRA Research Roadmap shows the recommendations on future research and development (R&D). These recommendations describe how the second layer's goals may be reached.

This chapter therefore contains the details on the COPRA European Research Agenda for Aviation Security proposed by the COPRA consortium. Tackling the research items will help to adress and contribute to the current and future challenges in aviation security.

A single R&D recommendation may support several recommendations on future aviation security concepts (RFASC) or even several headlines, although the contribution may be manifested in different ways for each. In this chapter, the recommendations on R&D are clustered by the four headline to which they mainly contribute. Each section is dedicated to a specific headline and will start with an overview of the recommendations on R&D, including the RFASC it mainly contributes to. Subsequently, for each recommendation on R&D a more detailed description is given. For ease of reference, the recommendations are listed with an individual lower case letter.

4.1 Resilient

The research roadmap contains 16 recommendations on R&D which contribute mainly to the headline Resilient. Table 1 contains a summary of these recommendations; detailed descriptions are given below the table.

Table 1: Summary of recommendations on R&D which contribute mainly to "Resilient"

Recommendation on R&D	**Term**	**Contributes (mainly) to**
Countermeasures for IEDs, firearms and close range destructive threats[2]	Short	Be resilient against current and emerging threats
Countermeasures for CBR threats[2]	Short	Be resilient against current and emerging threats
Countermeasures for ground-to-air threats (such as manpads and laser dazzling) [2]	Short	Be resilient against current and emerging threats
Countermeasures for ground-to-ground threats[2]	Short	Be resilient against current and emerging threats
Countermeasures for cyber threats[2]	Short	Be resilient against current and emerging threats
Countermeasures for electromagnetic threats[2]	Short	Be resilient against current and emerging threats
Countermeasures for sabotage, seizure and hijacking[2]	Short	Be resilient against current and emerging threats
Countermeasures for bluff threats and threats from social media[2]	Short	Be resilient against current and emerging threats
Test-beds for aviation security purposes	Short	Be measurable in terms of the entire security system performance
Aviation security research laboratories network	Short	Be resilient against current and emerging threats
Security performance assessment method (metrics, tools, process, etc.) for the entire security system	Short	Be measurable in terms of the entire security system performance
Risk based and random security processes	Short	Include risk based measures
Automated bulk detection	Mid/ Long	Cover the complete resilience cycle; Include risk based measures
Multifunctional detection system	Mid/ Long	Be easily adaptable and flexible; Include risk based measures
Automated systems for incident detection and response	Mid/ Long	Cover the complete resilience cycle
Self-healing and self-correcting security systems and structures	Mid/ Long	Cover the complete resilience cycle; Be easily adaptable and flexible

a. Countermeasures for IEDs, firearms and close range destructive threats[3]

[2] Threats as identified in COPRA
[3] Threats as identified in COPRA

Current (planned and conducted) emerging threats are often related to detonation of high explosives, deflagration, fire or impacts of objects. These threats are either meant to damage or destroy aircraft structures, physical infrastructure or to endanger persons, critical equipment and goods on the ground. Besides the known suicide bombers wearing explosive vests, terrorists become more adventurous and creative in placing and packing of explosives. Due to this variety in threats, resilience against such threats should be based on a defence in depth strategy. While concentrating on prevention through detection, pre-emptive protective solutions should be developed as well as response and recover strategies and technologies. Especially as there are public parts (landside) at airports, where less security procedures are applied and a 100% security level is even less achievable, a resilient security concept is necessary.

Research should focus, on the one hand, on e.g. (protective) building structures, building design (escape routes, flexible usage of building parts etc.) or close range protection for persons. On the other hand, auxiliary infrastructure should be considered, which is not only exposed to cyber threats. Physical threats like IEDs, firearms and close range destructive threats could destroy auxiliary infrastructure and, hence, lead to even worse cascade effects regarding aircraft and airport infrastructure. Therefore, research should include or focus on protective measures for auxiliary infrastructure against these kind of threats.

The fact that aircraft have to be made of lightweight structures, makes it even more challenging in being resilient. Advances in materials research have shown that new materials can be developed to have properties that combine lightweight with certain degrees of robustness or even self-healing capabilities to cope with being resilient. Therefore, research projects could not only focus on the continuous development of such materials and robust construction principles but also include processes and protocols to be observed in case of an incident. In a risk based resilience approach, researchers should consider possible threat situations, not only probable ones.

b. Countermeasures for CBR threats[3]

Current and emerging Chemical, Biological and Radiological (CBR) threats depict the release of chemical, biological or radiological agents or the poisoning of either water or food. These threats are meant to be exposed to people, either in the airport or on the aircraft. The health of all people exposed will be affected if such a threat is manifested, which will become apparent immediately or after a certain period of time. Therefore, resilience against such threats is needed, by regarding every phase of the COPRA resilience cycle.

Research should tell for each CBR threat (i) which phases of the resilience cycle lack countermeasures or are not fully taken advantage of, (ii) which countermeasures may be applied for those phases and (iii) how (much) they will improve resilience. The variety of threats in this cluster implies countermeasures will possibly differ, yet for parts of the resilience cycle it may be possible to apply the same countermeasure for several of the CBR threats.

c. Countermeasures for ground-to-air threats[3]

Aircraft in starting and landing phase may be vulnerable to threats that can be controlled from outside the airport perimeter. Resilience measures against these threats need to be developed.

Examples of ground-to-air threats are manpads and laser dazzling: Both are executed by a perpetrator standing just outside of the airport, aiming at an aircraft. For instance, laser systems are widely available and used in different applications such as major events (national celebration, concerts, etc.) and can be bought or built easily. The use of this type of device against an aircraft during landing and take-off occurs often (each day) and disturbs this critical phase of a flight.

Research should assess a way to detect the threats and to mitigate the effect of such threats. Two types should be investigated:

1) Active system (which reacts immediately to threat occurrence)

2) Passive system

Prototype development should be integrate in the project process. It is expected that action under this topic provide significant improvement in the security of aircraft during take-off and landing phases, as well as in innovative protective solutions.

d. Countermeasures for ground-to-ground threats[3]

This topic covers all threats that can be applied from just outside the airport perimeter, damaging infrastructure on the ground (e.g. runway, ATC tower, airport building, hangar, fuel supply, etc.) within the airport perimeter. Resilience measures against these threats should be developed, covering the entire resilience cycle.

One important part of the research topic is to assess the vulnerability of the air traffic control tower. This critical component of the airport can be a target of deliberate acts of terrorism. The research should focus on vulnerability assessment and on development of resilient solutions and strategies to limit the risks.

Besides focusing on the ATC tower, research can also cover all other physical infrastructure components that can be attacked from outside using e.g. rockets or radio controlled airplanes with or without explosives on board. Hence research should be conducted on the development of new materials and construction principles to jointly deal with the protection of all ground based infrastructures against all kinds of conventional and unconventional threats, thus hardening the physical structures at airports (protect). Also, research on ways to stop the attack before it occurs (prevent), as well as any other possibility to keep the influence on the whole aviation system as low as possible, should be conducted.

It is expected that actions under this topic provide significant improvement in the security and resilience of airport infrastructures. Research should analyse in an innovative way the vulnerabilities of the various parts (e.g. communications with satellites, ground stations and aircraft) and propose solutions to reach a higher level of resilience. Within all this, economic impact should be considered and, more generally, also the societal impacts.

e. Countermeasures for cyber threats[3]

Airports, aircraft and auxiliary infrastructure must be protected against cyber threats in a resilient way. Ground environments from airports and other stakeholders might be the target of cyber threats, for instance aiming at defeating connected security systems like detection scanners or access control solutions.

The recent evolution from proprietary and isolated systems to standardized and connected systems, especially for aircraft and ground systems directly interacting with them, increases the possibilities for cyber-attacks. Such attacks include malware and spyware, viruses that can wipe out a system or hackers that target a specific device, system or organization. Research should focus on solutions to the security problems raised by those new threat vectors, including RFID, GPS, mobile devices and open-world wireless communications.

f. Countermeasures for electromagnetic threats[3]

Electromagnetic (EM) threats on aircraft and aeronautical auxiliary infrastructures are of growing concern – they can disrupt or even damage systems and networks. Electromagnetic radiations (e.g. due to cyber-attacks, intentional electromagnetic interferences, spoofing can cause severe disturbances of operations at the airport and can lead to a large disorganization of the entire airport, which will also affect the passengers and the local economy. They can even affect severely the security of aircraft especially during take-off and landing, which are critical phases.

It is expected that action under this topic provide significant improvements in the security of systems and networks in airports and aircraft. Research should analyse the vulnerabilities of the various components of the systems and propose ways to improve resilience, e.g. on architecture or innovative protective solutions.

Also, emerging EM threats should be considered in the design phase of a new airport and the retrofitting of existing airports. Review of the threats and counter measures will be addressed. The research activities should yield guidelines and methodologies to design resilient airport infrastructure. It is expected that results under this topic help designers and architects with solutions to develop airport/auxiliary infrastructures which are resilient to EM threats.

g. Countermeasures for sabotage, seizure and hijacking[3]

Aircraft are vulnerable to threats like sabotage, seizure and hijacking, both on ground and in the air. Executers of such threats may be part of the passengers or staff (maintainers, crew, etc.) or may have gained access to the aircraft illegally.

Research should tell for each threat which phases of the resilience cycle lack countermeasures or are not fully taken advantage of, which countermeasures may be applied for those phases and how (much) they will improve resilience. Due to the strong variety of the threats in this cluster, countermeasures will possibly differ. However, where possible, it should be encouraged to apply the same countermeasure for several of the threats.

h. Countermeasures for bluff threats and threats from social media[3]

Traditionally, bluff threats are expressed through communication channels like the telephone and mail. There is already a well-functioning method established on how to deal with such bluff threats. However, one should not lose sight of the possibility that this method may be improved by considering new developments (e.g. technological, social media). Research should focus on which new developments may indeed improve this traditional method and how the improvement may be effectuated.

Social media can also contain some threatening rhetoric by various actors. In the past, it has been shown that some of the threats have been realized in the form of an attack while others have been a bluff. In this respect, research should be conducted on how to determine the seriousness of the threats expressed through social media (internet, Facebook, etc.) and how to react on such threats in the field of civil aviation. Past cases of threats through social media should be analysed, including the follow-up reaction. Also, equivalent past cases of "bluff threats" and related reactions should be assessed. The research should propose good practices in reacting to threats uttered in social media.

i. Test-beds for aviation security purposes

The impact of emerging threats should be checked on test-bed aircraft, airport as well as auxiliary infrastructures (for auxiliary infrastructure, the test bench should consider all the security systems and not be limited to check points only). The test-beds will allow to analyse the impact of a threat and to demonstrate the efficiency and effectiveness of different countermeasures.

Research done in the test-beds should consist of reproducing the threat and assessing the vulnerability of the complete system, using real or representative pieces of equipment.

It is expected that action under this topic enables the opportunity of facilitating the development of specific measures against emerging threats as well as the security performance assessment of the system as a whole.

j. Aviation security research laboratories network

The aviation community would benefit from a networking activity similar to the ERNCIP activities coordinated by the EC's JRC. The objective is to create an aviation security network of laboratories in Europe to address all security issues of aviation. All types of threats (current, emerging and new) should be considered. Divided in working groups dedicated to specific combinations of threat and target (aircraft, airport and/or auxiliary infrastructure), this network should be able to analyse the effect of a certain threat against targets, possibly even in "real time".

The research network could be divided in two parts:

1) A network of high level experts in the field of air security issued from research and test laboratories, aircraft industry members, airport operator, security system providers, etc. (the connections developed under the COPRA project are an example of what could be a part of the network of high level experts);

2) A network of test centres to validate the security systems developed by the security providers/working groups.

k. Security performance assessment method (metrics, tools, process, etc.) for the entire security system

In order to be able to change aviation security systems systematically it is important to adapt security performance assessment methods. There is a trend to implement security measures in a more dynamic (and risk based) way. This means that (combinations of) measures can change over a certain time period (even on a daily basis) and from sub-system to sub-system. As a consequence, it is necessary to validate the security system on a performance focused basis.

Measuring security performance of the entire system (as a whole) is a long term achievement. However we should start researching methods for this on the short term, as they are at the basis of all systematic optimizations and of possible risk based measures and approaches. Current methods for assessing the security performance focus on single components or sub-systems and basically check compliance with standards. Some methods, like red-team-testing, lack on realism for the entire security system. Existing as well as new methods should be examined to generate a set of meaningful security performance assessment methods for the entire security system.

l. Risk based and random security processes

Current checkpoints are functioning within the existing regulatory framework. However, from an operational perspective they are close to their limits. The future of the checkpoint will be challenged by a necessity to find new security practices that will facilitate risk-based screening and decision making, allowing unpredictable (random to outsiders) alternation of approved methods and targeting as deemed appropriate for individual passengers. Core elements for the future security process include the development of better passenger identification techniques that will inform the screening process, and screening technology with increased intelligence that will provide more flexibility in the automation, data fusion and data combination. The unpredictability/randomness is important as it remains a challenge to keep the security system non-transparent to persons with potential malicious intentions. As long as they are not capable to find weakness that might be exploited, security is ensured as much as possible.

Even today, some bulk detection systems for hold luggage are crudely risk based (on the destination of luggage). The potential of using risk-based detection processes and algorithms must be explored much further, taking into account not only destination data and also extending the approach to cargo, passengers and hand luggage. Also research on differentiation of passengers and goods in groups with, on the one hand, higher security attention and, on the other hand, less security attention will be useful to reach a risk based approach.

m. Automated bulk detection

Prediction is that the number of passengers as well as the overall cargo volume will dramatically increase in the coming years. Extrapolation of the current effort for security shows that the advancement of seamless security gateways (concerning required manpower, throughput and cost, while retaining the same level of detection sensitivity) is an important challenge that must be faced soon. This requires automated detection systems for quick and easy non-intrusive inspection of luggage, goods and cargo. Systems need to be developed to be able to automatically detect potentially dangerous items and substances on-the-fly, speeding up the inspection process while easing time- and cost-intensive burden of manual or visual inspection by security staff. These networked systems should combine multi-physics approaches (conventional and dual- or even multi-energy X-Ray, backscatter or NRF (Nuclear

Resonance Fluorescence)-based techniques) with image acquisition based on computer vision algorithms in order to perform with a defined level of reliability. Both of these fields – inspection methods in 2D and 3D as well as computer-assisted image processing and interpretation – are interconnected in several ways and need to be advanced together in order to address the challenges of tomorrow.

In order to speed up the process of cargo, Unit Load Devices (ULD) should be scanned on the whole. It is also important to efficiently find contraband (such as explosives, illicit drugs, illegal imports, weapons and nuclear materials) in air cargo. Air cargo is nowadays mostly packed inside lightweights aluminium containers (ULDs) and on pallets. The process of unpacking, inspecting and repacking is labour intensive and very time consuming. Cargo movements have a time critical nature concerning the needs of clients. It has a major impact on business-to-business relationship and business-to-client relationship. There is thus a need for improved cargo screening systems.

In order to have a quick, safe and smooth air cargo scanning, a broad range of contraband in air cargo containers should be distinguished and provide density, shape and composition images with minimal false detection. It is also important to comply with strict radiation safety requirements for both operating staff and cargo irradiation. Developments are needed in the area of automatic detection of illegal materials and objects e.g. image matching, object recognition of illegal objects or computer vision, as well as in the field of new imaging technologies, such as 3D freight detection systems with intelligent algorithm and automatic operator support. New process flows/cycles should be developed with a focus on increasing throughput, e.g. pipelining processes for goods, use of intelligent tracking systems, time device transport systems or multi-stage control processes.

n. Multifunctional detection systems

Technical advancement has benefited mankind with many new gadgets, but unfortunately has broadened the range and availability of potentially dangerous items as well. Security inspection systems do not only need to detect metal handguns and one type of explosives today; they must find a whole variety of advanced, well-concealed and mostly miniaturized threats or substances in an ever larger growing and faster moving cargo volume.

To address that challenge, multifunctional detection systems need to be developed, that allow for automated detection of any potentially dangerous item or substance. Because of the variety of threats, approaches that combine physically complementary, advanced detection techniques together with information systems and intelligent computer vision algorithms should be taken into account. This includes well known and technically advanced methods like 2D X-Ray and Multi-Energy methods for material discrimination, but extends to fast 3D-techniques that deliver not only material information but also shapes and volumes.

Other physical approaches include backscatter or fluorescence methods that can combine 3D data with information about the physical properties of the elements in the suspicious volume region. Examples could be the development and improvement of multi view X-ray detection systems by e.g. computer tomography (CT) combined with X-ray detection multi energy systems and automatic explosive discrimination. The combination of these techniques should deliver more accurate values of small amounts of dangerous items and materials such as explosives. Advancing the detection and decision capabilities of intelligent interpretation software would assist the user in assessing threats and so not only improve detection probability but also the throughput– therefore maximizing security and minimizing the costs.

o. Automated systems for incident detection and response

In aviation, a quick and coordinated response to security incidents is crucial during and in post-incident phases, i.e. recovering from an incident by supporting first responders. While automated systems for detection and response are state-of-the-art for safety related issues, most prominently for fire or structural health monitoring, such systems are not yet widely available, let alone used, for security incidents.

Therefore, versatile systems that can be used and adapted for several classes of security incidents need to be developed. Research must also take into account the social and organisational questions involved in putting such systems into actions. Examples for such systems are: sensor systems to give instant situational awareness in case of explosions either in airports or on aircraft for incident detection or systems for dynamic indoor navigation for incident response.

p. Self-healing and self-correcting security systems and structures

As far as the aircraft structure is concerned, self-healing is a very valuable characteristic to design into a material since it effectively expands the lifetime use of the product and has desirable economic and human safety attributes. Self-healing materials are polymers, metals, ceramics and their composites that could have, in case of damage through thermal, mechanical, ballistic or other means, the ability to heal and restore the material to its original set of properties.

Related to aircraft systems, one key aspect is that there is no IT security administrator aboard the aircraft to detect, analyse and react upon a potential security attack. As a consequence, it is of interest to investigate on solutions allowing a critical system to autonomously:

- maintain its health (robustness through diversity and redundancy etc.)
- monitor its own health (performance log analysis etc.) , and check for faults periodically
- perform its recovery to the normal state

One challenging aspect is the certifiability of such mechanisms, as it includes automatic reaction decisions to be taken.

4.2 Comprehensive

The roadmap contains six recommendations on R&D that contribute mainly to the headline Comprehensive. Table 2 contains a summary of these recommendations; detailed descriptions are given below the table.

Table 2: Summary of recommendations on R&D which contribute mainly to “Comprehensive”

Recommendation on R&D	**Term**	**Contributes (mainly) to**
Organisational framework and technical tools to continuously evaluate threats with all stakeholders	Short	Address both physical and cyber threats targeted at all stakeholders including security systems
Aviation security management system	Short	Include a comprehensive aviation security management system to be shared by all stakeholders
Methodologies for an iterative risk management approach	Short	Include a comprehensive aviation security management system to be shared by all stakeholders
Evaluate different security paradigms for aviation	Mid/Long	Be based on a shared strategy
Joint risk and threat analysis platform for all stakeholders	Mid/Long	Include a comprehensive aviation security management system to be shared by all stakeholders
Community based approaches to increase resilience	Mid/Long	Be based on a shared strategy

q. Organisational framework and technical tools to continuously evaluate threats with all stakeholders

Being able to evaluate threats across different stakeholders is a requirement for a comprehensive aviation security management system. To do so on a continuous or regular basis

Research should analyse how to build up an organizational framework that enables the interaction between all stakeholders taking into account their needs regarding how to evaluate threats. This research includes the discussion of the legal possibilities and requirements. Furthermore, technical tools should be developed that support this interaction and exchange of threat evaluation in a safe and a secure way, and such must be supporting organizational processes.

r. Aviation security management system

Research should investigate possible ways in which a common aviation security management system can be set up. This system should be seamless between stakeholders, balance the burden of security between stakeholders and cover the entire security cycle.

To ensure resilience in aviation security activities, the ISO27000 standard series provides clear guidelines to establish, implement, monitor, maintain and improve the Aviation Security Management System. The aviation security needs to be reactive and flexible to reach these objectives.

New governance bodies in line with the ISO27001 standard could be set up to manage the dynamic and adaptive security environment and to develop an overall and agreed framework reaching the following objectives:

- Comprehensive: Cover the entire aviation security
- Seamless: No gaps between stakeholder
- Efficient: Every covered piece is robust enough to mitigate the assumed threats to be countered
- Balanced: Burden of aviation security risks management is equally shared between stakeholders

s. Methodologies for an iterative risk management approach

To avoid incidents or attacks on airplanes and passengers, measures are applied at airports. These methods and measures basically try to prevent the existence of prohibited items on sensitive areas (e.g. inside an aircraft). One example for these measures is the walk through metal detector, which prevent potential perpetrators from bringing metal weapons inside the airplane. These kinds of instruction of regulations that prevent certain types of items in airplanes can be seen as a static approach. One important disadvantage is the fact that for each new dangerous item a new regulation and, probably, a new screening technology must be installed. A dynamic approach that takes risks into account can overcome that disadvantage. Based on a certain risk, different measures can be applied dynamically. This could be done e.g. individually for each traveller, for certain destinations, different time frames or combinations of these.

Research projects should examine what kind of risks might be useful to know in general or for certain areas and even airports. Also different parameters (e.g. daytime, destination) that may have a relation to risk should be distinguished. Mitigation measures can be identified for each type of risk. One important parameter for mitigation measures will be the implementation or reaction time for an identified risk. Iteratively implemented mitigation measures can be triggered by different types of risks cumulatively. The analysis of different methodologies for that iterative risk management approach might lead to a more dynamic and, therefore, more effective and secure system.

Research should also be done to find new or adapt current methodologies for risk management, which will take into account all stakeholders as well as the entire resilience cycle (Figure 3). The outcome should be one method that will be commonly used by all stakeholders in an iterative way. This ensures all stakeholders will have the same view on and understanding of the risks involved.

Risk management realizes different activities to identify the risk, estimate its likelihood, evaluate its level, identify ways to lower the risk and accept the residual risk. The residual risk is the risk expected after the implementation of chosen ways to lower the risk. To perform risk management activities, a security context needs be defined and agreed upon. It should at least contain:

- Stakeholders
- Assumptions
- Threats’ taxonomy
- Perpetrator profiles
- Impact table, class & criteria
- Risk acceptance grid

Among the parameters defined in the security context, the security acceptance grid provides the threshold between acceptable and unacceptable risks. All risks evaluated as unacceptable must be lowered by implementing security measures, which, in total, reduce the risk to an acceptable level.

t. Evaluate different security paradigms for aviation

It is important to find out how far one can go with "risk based approaches" compared to "random based approaches" and in which way they may be combined and what the relation is between different sub-topics, like defence in depth. For this, all stakeholders must be considered to be able to come up with a good strategy for the entire security system.

Studies concerning security strategies have to be repeated in an appropriate frequency to evaluate the results and the effect of potentially integrated new security strategies and to develop an on-going strategy.

u. Joint risk and threat analysis platform for all stakeholders

Risk assessment is a major enabler for efficient security. In the aviation system, risk assessment is performed differently across countries and stakeholders. Research is required to reconcile all approaches in order to make risk analyses compatible, shareable and, thus, usable by all relevant stakeholders.

A joint and comprehensive risk analysis platform for all stakeholders will ensure further that the assessments are performed consistently across countries and stakeholders. It could consist of common technologies and test procedures to allow for informed decision making on all levels.

When optimizing existing or introducing new security measures, an objective risk assessment should be taken into consideration. The goal is to only introduce the necessary amount of security to find the perfect balance between ensuring security and costs, mobility, etc. Elements of risk analysis have been studied in the past and should be used in a way forward, but there is an urgent need for research on a collaborative approach on risk analysis, which involves all relevant stakeholders and gives a comprehensive perspective on the risks and required security measures and concepts.

The research should focus on defining the methodology of risk assessment that includes all necessary information and intelligence. Furthermore, possible implementation strategies for Europe need to be advised, including the appropriate embedment in existing public structures such as existing or possible new authorities to implement and supervise the risk assessment efforts.

v. Community based approaches to increase resilience

Community based approaches should be investigated to increase resilience. Passengers as well as non-security staff and others present in the aviation system can be actively involved in aviation security in order to further enhance the security process. The community could be used to enrich security information. Actively involving non-security staff (e.g. airport retailers, airline crew) in the security process may lead to a willingness to report suspicious behaviour. This could significantly enrich the information position of the security system. With these extra eyes and ears it is possible to quickly create a complete picture of a threat, allowing for earlier intervention. This will speed up the entire security process – also for the passengers.

However, there is also a risk of information overload and a risk that the quality and reliability of the information is insufficient. It is therefore important that the employees concerned are, to some extent, trained to recognize suspicious behaviour and situations. Modern personal communication devices or app's can be used to facilitate and support the information exchange process.

Also in the response phase the public can be used: Most of the passengers traveling today use mobile smart phones or other mobile devices as well as mobile social media. Particularly in the first minutes of the response phase of an incident these media may be used to improve the situational awareness. Information obtained from social media can help first responders to build up a better picture of the incident.

In addition, it is for instance also possible to determine the location of a public agglomeration by scanning the locations of mobile devices. Using this information, the situational awareness about the incident can be further enhanced.

Finally, targeted messages to mobile devices can be sent to inform specific groups about the incident. This information may include advice on how best to respond.

4.3 Comfortable and Safe

The research roadmap contains eight recommendations on R&D that contribute mainly to the headline Comfortable and Safe. Table 3 contains a summary of these recommendations; detailed descriptions are given below the table, their descriptions are listed below.

Table 3: Summary of recommendations on R&D which contribute mainly to "Comfortable and Safe"

Recommendation on R&D	**Term**	**Contributes (mainly) to**
Assessment of public acceptance of security measures and effects on human rights	Short	Consider the effect of security measures for all relevant stakeholders
Non-intrusive detection systems	Short	Require no divesting of personal items
Quicker and more efficient security processes to improve passenger experience	Short	Be a quick and seamless process for persons and goods
On-the-fly biometric identification and verification	Short	Be a quick and seamless process for persons and goods
Automatic detection by new imaging technologies of potentially dangerous items	Mid/Long	Be a quick and seamless process for persons and goods
New process flows with focus on increasing throughput[4]	Mid/Long	Be a quick and seamless process for persons and goods
Flow performance management of the entire security system[4]	Mid/Long	Be a quick and seamless process for persons and goods
Integrating multiple security systems (technical, processes, actors)	Mid/Long	Be a quick and seamless process for persons and goods

w. Assessment of public acceptance of security measures and effects on human rights

Existing and new security concepts and measures in the field of civil aviation need to be legitimate, legal and proportional to the threat. Social acceptance and public support are crucial to achieve a balanced security approach.

Future research in this field should develop a methodological framework for assessing the public acceptance of security measures and effects on human rights (e.g. right to privacy, health and religion) as well as carry out a qualitative assessment of this in several EU countries and a cross-national quantitative assessment based on several samples of EU passengers. The research should recommend practices for improving public acceptance and minimizing the effects on human rights.

x. Non-intrusive detection systems

The limits of some of the current imaging technologies for bags requires the divestment of dense electrical items to allow operators to accurately analyse bag contents. Liquids, aerosols and gels have been regulated to be below a certain size and have to be divested to reduce the risk of devices being constructed on board an aircraft since many currently deployed systems do not automatically screen for liquid explosives. Passenger screening systems have evolved to

[4] Although this is also an important contributor to the headline Affordable and Safe, the description can be found in this section.

mostly use automated detection algorithms rather than the analysis of images by operators. Still, the passenger is required to divest of layers of outer clothing, belts, jewelry, watches, wallets and so on, as they can be a cause of false alarms where and when not fully divested.

For both the screening of passengers and their carry-on luggage there is the need to make technical improvements to screening capabilities that reduce or remove the requirement for divestment and increase privacy while improving automated threat detection capabilities and minimizing false alarm rates (this is particularly with regards to body imaging where false alarms resolution typically requires intrusive pat-down searches).

Air Cargo screening is another key area where currently deployed technology has limitations. Improvements to automated screening technologies and imaging technology would provide enormous benefits in terms of analysis time, reducing the number of consignments that have to be broken down into smaller packages, hand-searched or screened using other methods.

y. Quicker and more efficient security processes to improve passenger experience

In a context where current security processes are a sum of more and more security measures, the consequences are a decrease in throughput and an increase in security processes costs. They are not appropriate to modern threats and have an impact on passenger experience. Thus, new processes are required for quicker and more efficient security checks in order to improve passenger experience regarding person and (carry-on) luggage screening. The screening processes have to be security-oriented while bringing operational efficiency and passenger facilitation. The goals are to clear passenger and luggage from prohibited objects and substances as well as to increase efficiency of security measures (reducing false alarm, improved management of security alerts, improve staff productivity). This would results in better passenger experience by reducing waiting time and providing comfortable and safe processes.

Several approaches could be implemented to achieve the goals such as separate screening severity according passenger profile; integrated targeted (i.e. risk based) screening and enhanced detection (explosive, body scanner, etc.); flexible checks and passenger tracking; automated and do-it-yourself security measures; etc.

These processes and approaches are also applicable to staff screening either as-is or in a little different implementation. Therefore, security checks for staff would also benefits from the research in this area and improve staff experience as well.

z. On-the-fly biometric identification and verification

Travellers’ identity verification or identification is a very important issue when dealing with security measures. There are several locations in the security process where identity checks of passengers are needed or helpful.

Biometrics technologies provide very reliable means to perform such control. Verification means that the identity of the person is compared to a claimed identity, using an electronic ID document for instance. A typical use case is to verify whether or not the person boarding the aircraft is the one that is registered. Biometric samples are acquired by sensors and then compared to the ones stored in the chip of the electronic ID document or against a database of enrolled/registered passengers. Identification implies a less cooperative mode where authorities aim to identify potential perpetrator among the passengers through capture of biometric samples with appropriate sensors and performing a comparison against a watch list.

For a seamless process, the development of reliable on-the-fly biometric systems would bring flexible and comfortable solutions. On-the-fly biometrics means that the biometric capture is performed automatically and naturally while the traveller is going through the security process. It could be a capture on the move while the passenger is in motion or at a distance but requiring a short pause in the motion. Biometrics modalities concerned are primarily fingerprint, face or iris recognition, but it could also be vein or gait recognition. On-the-fly biometrics could also be used to perform identity verification at several point in the infrastructure, enabling person tracking capabilities.

Research needs to be conducted to develop such on-the-fly biometric systems. This is a broad research topic with high challenges regarding performances (accuracy, speed) and operational requirements. This research topic has been tackled very recently for some biometric modalities, but need to be pushed forward.

aa. Automatic detection by new imaging technologies of potentially dangerous items

Currently deployed screening technologies rely heavily on operators for image interpretation. While operators can become very skilled, there is the potential for threats to pass through the checkpoint due to operator fatigue or inattention. Also, the dependency on operators introduces a limit on the throughput, which is probably improved (or even absent) when utilising automatic detection techniques.

Intelligent image data processing systems research should be done for digital image data processing systems with automatic image recognition. This implies automatic target analysis and pattern recognition. These systems should have intelligent database systems able to recognise and keep images in memory.

Visual recognitions systems already exist for medical application but are not used for security aspects up to now. Research should be performed into applicability of these for aviation security.

bb. New process flows with focus on increasing throughput

The current lay-out and process flows of security check points exists for a long time. Research under this topic could include logistical concepts and the design of process flows (including alternate lay-outs to remove bottle necks). It should take into account the evaluation of the efficiency of the security system. Research solutions should demonstrate how lay-out and process flows could be designed, such that an improvement of efficiency is achieved.

cc. Flow performance management of the entire security system

Research should be conducted on operational information gathering (throughput time and knowing where persons or object are in the system), analysis and algorithms to optimize the operational performance of the security system. Based on the analysis, operational system adjustments can be performed for flow optimization. A system should be developed which can perform the necessary analysis and optimization.

dd. Integrating multiple security systems (technical, processes, actors)

Different security systems are currently used stand-alone and their results are not necessarily combined to achieve a combined assessment. Aviation systems such as for booking, check-in, security scanning (carry-on luggage and goods) or access control all work using completely different techniques; each system is unique and works on its own without any connection between them. A network of information as well as process interactions should be developed that are able to collect and use the data resulting from different security checks.

A seamless end-to-end process for goods and cargo requires a continuous flow of information of different security systems. For reasons of efficiency, systems should be integrated to interact with each other in order to be able to provide a security solution for all stakeholders by exploiting synergic effects. For example, analytic systems could be connected with different information gathering systems such as results of luggage checks or booking, boarding and travel information systems. The joint information might be used as input in, for example, behavioural pattern recognition algorithms for achieving improved results. Such connected and auto-analytic systems might also solve situations where several quasi-simultaneous events – each of which not a conspicuous situation as such – could lead to a potential security relevant event.

Therefore, integrated security systems and the corresponding algorithms should be developed that are able to collect, merge and analyse data from completely different sources/systems across all stakeholders in aviation. These systems should facilitate the creation of completely seamless security processes.

4.4 Affordable and Efficient

The roadmap contains five recommendations on R&D which contribute mainly to the headline Affordable and Efficient. Table 4 contains a summary of these recommendations; detailed descriptions are given below the table.

Table 4: Summary of recommendations on R&D which contribute mainly to “Affordable and Efficient”

Recommendation on R&D	**Term**	**Contributes (mainly) to**
Applicability of economic models on security and the transparency of these models	Short	Be measurable in terms of efficiency; Be based on a business case for security
Measurability of the (cost-)efficiency of the entire security system	Short	Be measurable in terms of efficiency
Performance assessment method (metrics, tools, process, etc) for the entire security system	Mid/Long	Be integrated with the economic management tools and systems of the aviation system
New process flows with focus on increasing throughput[5]	Mid/Long	Be a quick and seamless process for persons and goods
Flow performance management of the entire security system[6]	Mid/Long	Be a quick and seamless process for persons and goods

[5] As this recommendation is also an important contributor to the headline Comprehensive, please find the description on page 38.

[6] As this recommendation is also an important contributor to the headline Comprehensive, please find the description on page 38.

ee. Applicability of economic models on security and the transparency of these models

As aviation is a business in which yields are volatile and marginal, it is important to base (security) decisions on an accurate and integrated economic model.

Research should be conducted on new and existing economic models (both from non-security and from security outside the aviation domain), to gain insight in how they may be (partly) applicable to aviation security or if they contain some relationships that will be profitable if included in an economic model for aviation security. Part of this research is also to look into which costs to include/exclude when considering security, also considering to include non-obvious costs such as missed retail income, uncertain costs, indirect costs, societal costs, avoided costs (like the perspective insurance companies often use), etc., in order to achieve a clear demarcation.

ff. Measurability of the (cost-)efficiency of the entire security system

Although some measures of efficiency exist for individual machines used for security, there is no possibility yet to measure the (cost-)efficiency of the entire security system (as a whole). However, to be able to make a proper evaluation of efficiency and/or to be able to choose between different possible compositions, it is necessary to measure the efficiency of the entire security system. It may even be possible that certain combinations of security systems are performing more efficient than others, even if the individual systems are not the most efficient by themselves.

Research should be conducted on finding methods to measure the efficiency of the entire security system (as a whole), including all kinds of different systems, processes, etc. and all phases of the resilience cycle.

gg. Performance assessment method (metrics, tools, process, etc.) for the entire security system

There is a trend to implement security measures in a more dynamic (and risk based) way. This means that (combinations of) measures can change over a certain time period (even on a daily basis) and from sub-system to sub-system. As a consequence, it is necessary to be able to assess the efficiency performance of a security system on a more frequent basis and to integrate these assessments with the main economic management systems. The short-term research recommendation on measurability ensures a foundation for this, yet to measure (cost-)efficiency on a frequent basis requires also metrics, tools and processes supporting this activity.

Research should be conducted on finding metrics, tools and processes that can support assessment of (cost-)effectiveness of the entire security system on a frequent basis. Existing as well as new methods should be examined to generate a meaningful (cost-)efficiency assessment method for the entire security system. Prefeably, this will be integrated with the security performance assessment method (headline Resilient), in order to perform an cobined assessment on both efficiency and effectiveness. Such a combined assessment would serve as decision support and simplify the choice for a certain security system design.