PERSPECTIVES FOR AERONAUTICAL RESEARCH IN EUROPE

Perspectives for Aeronautical Research in Europe

2019 Report

CHAPTER 5
Ensuring Safety and Security

Final Version

www.pareproject.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769220. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

List of Figures

List of Tables

Chapter 5 – Ensuring Safety and Security

Aviation safety has steadily improved (section 5.1) including in the mitigation of weather hazards (section 5.2). Aviation has been one of the preferred targets of malicious actions, stressing the importance of physical security (section 5.4) and resilience to internal and external attacks (section 5.5). Progress also brings new challenges, such as the integration of 'drones' (section 5.3) that contributes to the need for vast safe exchanges of data (section 5.6).

**** Flight 2050 goal 14: "European air transport system has less than one accident per million commercial aircraft flights"***

Aviation is the safest mode of transport. In addition, aviation safety has steadily improved to the point where no hull loss was recorded in one year. It can be expected that more years will come without a single major aviation accident. The safety target in the goal 14 can be achieved by strengthening the cradle-to-grave safety chain of aviation: (i) aircraft design based on the most reliable scientific methods, validated and tested in the more stringent conditions; (ii) meeting comprehensive certification standards in all aspects related to operations and safety; (iii) control of the supply of raw materials, documentation of fabrication processes and production quality checks; (iv) qualification of all human actors, including pilots, maintainers and air traffic controllers; (v) provision and maintenance of all support systems and equipment at the required standards; (vi) strict implementation of safety rules and procedures; (viii) reporting of incidents, without identification or blame, before they become accidents; (viii) swift implementation of protective measures once a potential hazard has been identified; (ix) continuous search for best practices and their timely implementation; (x) use of existing and development of new monitoring, fault-tolerant and adaptive systems and emergency intervention strategies.

Safety fundamentally contributes to the sustainable growth of a sound and economically viable international civil aviation system. The report 'Flightpath 2050 Europe's Vision for Aviation' sets a goal for the year 2050 of reducing the accident rate of commercial aircraft flights to less than ***one per ten million flights***, i.e. half the reached current level. However, whilst the aviation accident rate continues to decline, the rate of decline has slowed markedly since 2004 and at the same time, we are seeing continued growth in the number of flights, which are set to almost double by 2030. As consequence, in order to preserve the current low level of fatalities resulting from air accidents, we ***must ensure*** that the rate of accidents continues to decline to counterbalance the predicted growth in the number of flights.

To improve the currently existing levels of aviation safety (somewhere in a text flight safety and aviation safety are used in the same meaning, but in general case, an ***aviation safety*** is considered as much wider and deeper term, including *flight safety, aviation security, environmental safety*, etc. [M. Kulyk]), especially when considering the continuing growth of the industry, additional measures are required. One such measure is to encourage individual aircraft operators to introduce their own Safety Management System (SMS).

SMS is an organized approach to managing safety. The system in the concept of SMS means a framework of functions to manage safety. Management is about controlling the function of the system towards the safety objectives. Another goal of the introduction of SMS is the facilitation of safety oversight by the national authorities. Two arguments drive the promotion of SMS by the regulatory authorities. Furthermore, due to the growth of aviation activities, budget constraints in the safety oversight function of the authorities require a new way of safety oversight that reduces costs [Dijkstra A.]. Also, safety levels vary considerably. There have been specific years without a hull loss by major airlines. In contrast, accident rates are much higher in remote regions subject to harsh weather, in third-world countries with less technological and regulatory resources and other aviation sectors like private and agricultural.

Europe has started to implement a Safety Management System to become more pro-active in the identification of hazards and with the ultimate goal of further reducing our already good safety record. This system complements the existing system of developing safety regulations, complying with them and investigating accidents and serious incidents when they occur [EASA EASp 2014 – 2017]. One of the key elements of an SMS is managing safety risks, which means identifying hazards, assessing the risks and making decisions on the best course of action to mitigate those risks.

International regulations and standards (including ICAO Standards and Recommended Practices, SARPs, especially of the Annex 11 "Air Traffic Services" [ICAO Annex 11], in paragraph 2.26.5, and Annex 14 "Aerodromes" [ICAO Annex 14], in paragraph 1.4, Single European Sky Common Requirements [EU Regulation 1035/2011] and EUROCONTROL Safety Regulatory Requirements - ESARRs) require that any change to a system that has an impact on the safety of aerodrome operations or air traffic services (ATS) shall be subject to a risk assessment and mitigation process to support its safe introduction and operation. Within the ICAO *Safety Management Manual* [ICAO Doc. 9859] a safety assessment process is defined by a seven-step process (Figure 5.1).

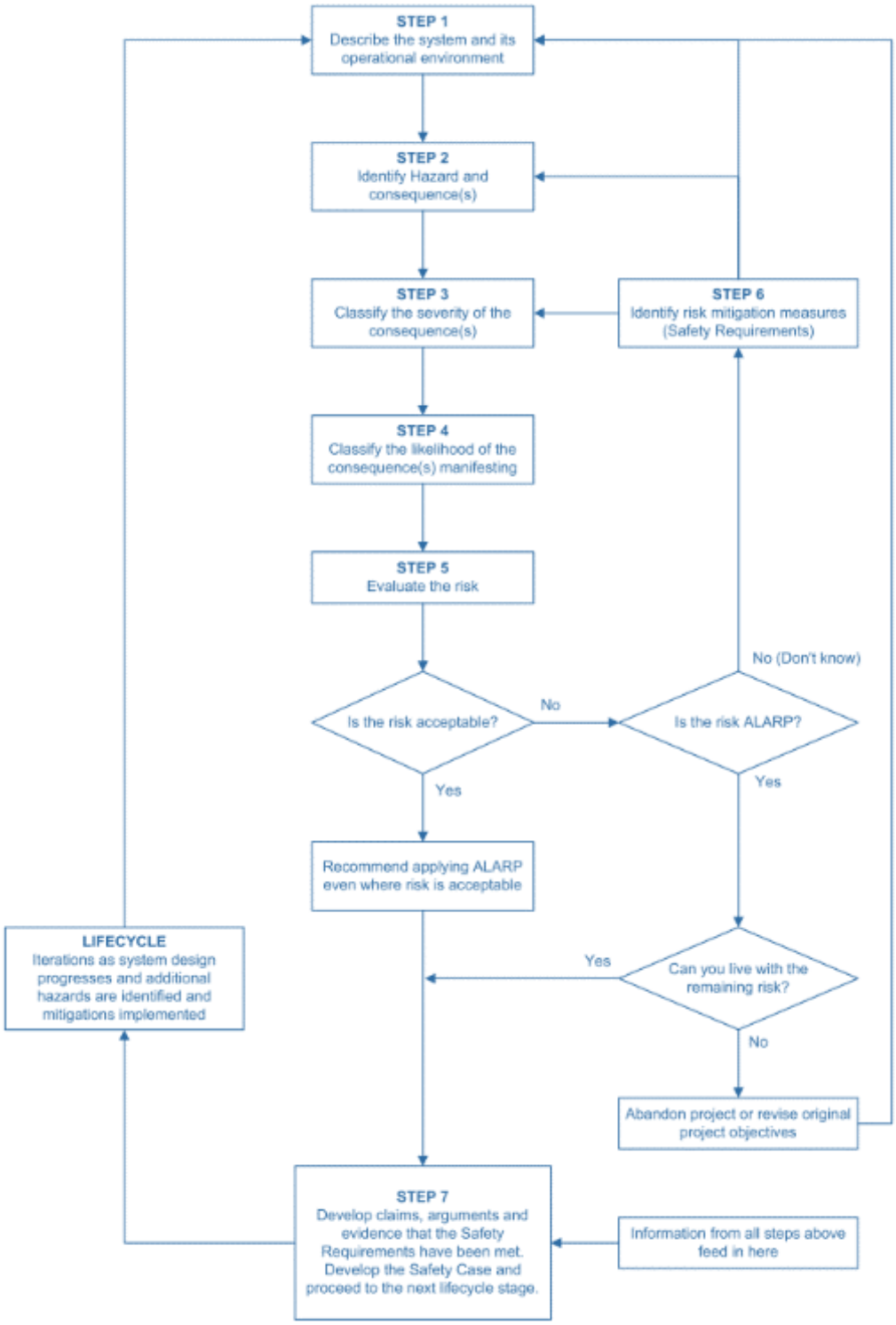


Figure 5.1. The Seven-Step Approach to Safety Assessment Process [ICAO Doc. 9859]

The terms 'system' and 'project' are used throughout this report and should be considered to include the following constituents:

a) Any equipment;

b) Any procedure (e.g. operational procedure used by the aerodrome operator or air traffic service provider or, alternatively, a maintenance procedure for related equipment); and

c) The people involved and their organization.

Aerodrome and ATS projects commonly pass through a variety of phases during their life from initial concept through to decommissioning. Safety needs to be planned for and addressed in all of these phases although the depth of risk assessment will vary depending upon the stage of the project and the degree of risk that exists [UK CAA CAP 760].

Risk management is generally understood as the holistic process involved in recognizing possible risks and the measures undertaken to reduce and monitor them. It thus comprises a modular cycle of communication, documentation, control, early warning mechanisms, and advancement (Figure 5.1).

Performing risk assessment early in the project can identify hazards that impact on the design of the system. These hazards and their impact should be identified early in a project so that the system can be designed to take account of them, rather than incurring expense trying to change a design or retrospectively to generate safety assurance evidence later in a project.

Early in the project, it is beneficial to identify the Applicable Safety Regulatory Requirements, including National and International SARPs, local Regulations and guidance material applicable to the intended system. These will influence the design of the system and compliance with these standards and regulations will often mitigate hazards inherent to the project. For example, for ATS systems the following may be applicable:

a) ICAO SARPs, e.g. ICAO Annex 11 and others;

b) Single European Sky Interoperability Rules and Common Requirements;

c) European Standards e.g. Eurocae MOPS (Minimum Operational Performance Specifications), Eurocontrol ESARRS (European Safety Regulatory Requirements);

d) National Civil Aviation Authority (CAA) Safety Requirements.

For example, for aerodrome projects the following may be applicable [UK CAA CAP 760]:

a) ICAO SARPs e.g. ICAO Annex 14;

b) European Standards, e.g. EUROCONTROL ESARRs;

c) CAA Safety Requirements for Licensing of Aerodromes;

d) CAA Safety Requirements for Aerodrome Survey Information;

e) CAA Safety Requirements for Airside Safety Management;

f) CAA Safety Requirements for the Assessment of Runway Surface Characteristics;

g) CAA Safety Standards for the Competence of Rescue and Fire Fighting Service (RFFS). Personnel Employed at Licensed Aerodromes;

h) CAA Safety Requirements for Aircraft Fuelling and Fuel Installation Management.

Several reasons why the accident rates in aviation sector vary so much between different parts of the world (Figure 5.2). The first that comes to mind is that *safety cultures* vary between countries and airlines. It is not an easy task to establish *a safety culture*—it is more a development which takes time and commitment and must be understood by everyone within an organization. An organization's culture is defined by what the people do and which decisions they make. This reveals the basic values of an organization. A *positive* safety culture will move a company forward to a maximum achievable safety level, despite business cycles and times of recession where financial pressure is evident. A positive safety culture can be split into four different components: Informed culture; Reporting culture; Just culture and Learning culture.

Figure 5.2 - Fatal accident rate of scheduled passenger and cargo fatal accidents per 10 million flights, by region of the world, using the regions defined by the ECCAIRS taxonomy from 2004 to 2013 [EASA EASp 2014 – 2017]

Theoretically, differences should not exist because air traffic management rules are international and almost all countries are ICAO members, thus they have adopted its regulations and recommendations. Another noticeable aspect is that there are only a few manufacturers of airliners in the world and their standards are practically equal. From this aspect there should be no differences between the different regions and countries because all airlines are customers of these companies and their training and maintenance programmes. However, significant differences exist in the age of the aircraft, resources allocated to their maintenance and regulatory oversight and the problem should be solved efficiently. One solution would be large scale knowledge and information interchange between actors in the airline industry.

In order to improve aviation safety in Europe, it is vital that the output of the safety analysis process is used to support the data-driven approach to the identification and prioritization of actions of the European Plan for Aviation Safety (EPAS) [EASA Annual Safety Review 2016].

The Safety Risk Management (SRM) process aims to establish a clear framework that supports the EPAS (Figures 5.1 and 5.3). The resulting actions on the safety issues that are identified in the SRM process will translate into rulemaking activities, focused oversight, research activities, safety promotion and potentially also in actions for the Member States.

Figure 5.3. Safety risk management cycle

The 5 steps of the Safety Risk Management Cycle include:

1. The identification of safety issues (or hazards) that affect the European aviation system;

2. The assessment of safety issues (or hazards), which aims at assessing the risks associated with the consequences of the safety issues (or hazards) identified in the previous phase;

3. The definition and programming of safety actions seeking to identify strategies (or mitigation actions) to address those issues (or hazards) whose level of risk cannot be tolerated following the assessment;

4. The implementation and follow-up of safety actions aimed at tracking the status of and report on the agreed strategies; and

5. Safety Performance aimed at reviewing identified risk areas to assess if the risks previously identified have been mitigated and to compare them with safety performance indicators.

All safety issues in aviation are monitored. Aircraft operators, organizations that maintain aircraft, as well as other entities in aviation are required to report any safety issues they detect. The reports are analysed to identify any concerns. This continuous monitoring allows the early detection of potential problems. EASA takes immediate and appropriate action to ensure that the highest safety standards are maintained.

Improving the standards of aviation safety and environmental protection requires rules to be continuously reviewed and improved based on the latest scientific knowledge. The rules are drafted and adapted to reflect the changing technology and needs of aviation with safety as the first priority. EASA advises the European Commission on safety rules and is responsible for describing in technical terms the best ways to achieve a high level of safety. Rules are reviewed in consultation with industry and citizens to ensure they are proportional to the aims they aspire to.

The introduction of Risk-based Oversight (RBO) in the aviation sector, as can be seen today [EASA TE.GEN.00400-003], will allow for a more effective use of the available oversight resources. Risk assessment and mitigation is a structured and systematic process for the identification of hazards and the assessment of the risk associated with each hazard, or group of hazards. The acceptability of the risks is determined by comparing the assessed level of risk to the predetermined safety assessment criteria or Safety Objectives. The chart below (Figure 5.4) gives an overview of the RBO's benefits. While aviation is growing, traditional oversight will remain but will also request a similar increase in the number of required resources. RBO, through increased efficiency, would keep this requested increase at a lower level. Moreover, it would also increase the effectiveness of oversight and contribute to achieving the objective of keeping a reducing trend in the number of accidents in spite of the increased exposure.

At State's level, RBO provides a mechanism for better identifying hazards, measuring associated risks as well as demonstrating effective mitigation of these risks. Ultimately it allows the Competent Authority to focus its attention on organizations that require additional or higher attention, strengthening the efficiency of the oversight. At the same time, an improved understanding of the risks across the aviation system will enable better calibration of the oversight, on the basis of an improved risk picture that takes into account the causal factors of all safety occurrences, from isolated events to incidents and accidents.

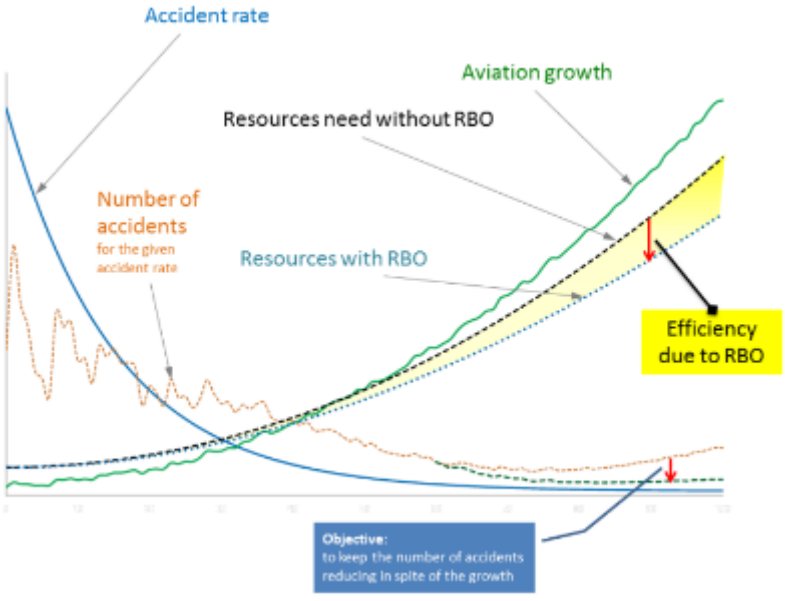


Figure 5.4 - Benefits of Risk-based Oversight implementation in aviation sector [EASA TE.GEN.00400-003]

5.1 Ultra-Low Accident Rate in Commercial Flight

**** Flight 2050 goal 14: "European air transport system has less than one accident per million commercial aircraft flights"***

Aviation is the safest mode of transport. Air safety 2010-2015 on EU territory with EU-registered aircraft: 188 fatalities in commercial air transport (the 155 fatalities in 2015 occurred in three accidents: one in Slovakia (4 fatalities), one in Spain (1 fatality), and one in France (150 fatalities), (Figures 5.5 and 5.6) and 1 196 in other categories [Eurostat 2017]. In January 2016, a Bombardier CRJ-200 operated by a cargo operator from one of the EASA Member States (EASA MS) crashed in Sweden, killing the two-flight crew. This was the only fatal accident involving any EASA Member State operators of Commercial Air Transport involving aeroplanes during 2016. In the last decade, there have been a total of 12 fatal accidents involving operators from the EASA Member States, one every year since 2014.

Figure 5.7 shows the evolution of the number of fatal accidents and fatalities for Commercial Air Transport Large Aeroplane operations (MTOW above 5,700 kg) – CAT Aeroplane for the period 2007-2016. Security-related occurrences, such as the Russian A320 of Metrojet that exploded over the Sinai Peninsula (Egypt), the A321 Daala Airlines in Mogadishu and the MH17 was shot down over Ukraine, are not included within this review. The Germanwings accident, the A320 Egypt Air over the Mediterranean Sea (terrorist action not yet confirmed) and the missing MH370 aircraft are still included.

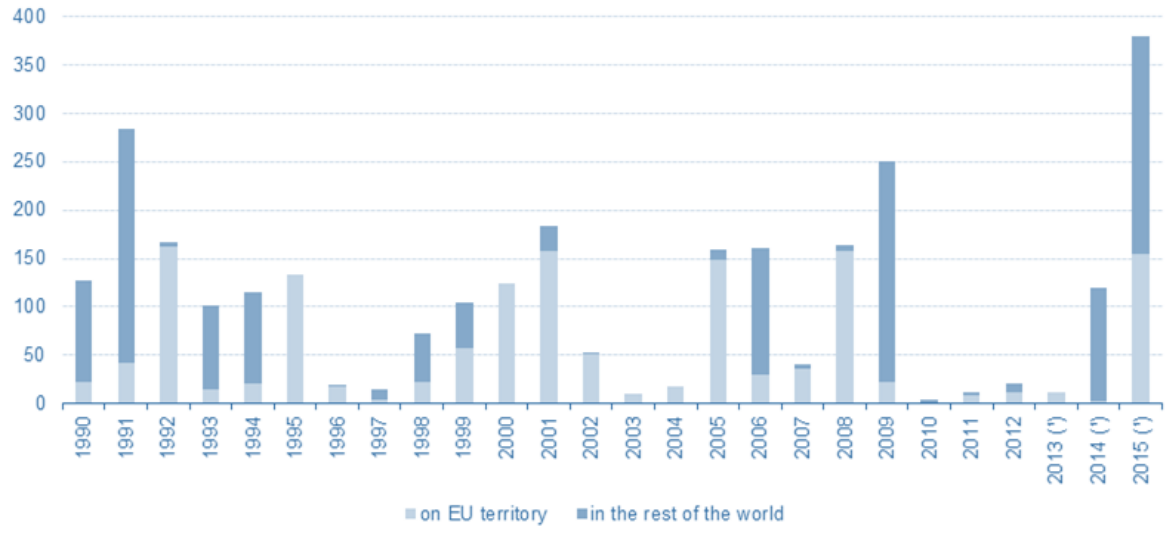


Figure 5.5. Commercial Air Transport by EU-28-registered aircraft, number of persons killed in air transport accidents (Source: Eurostat)

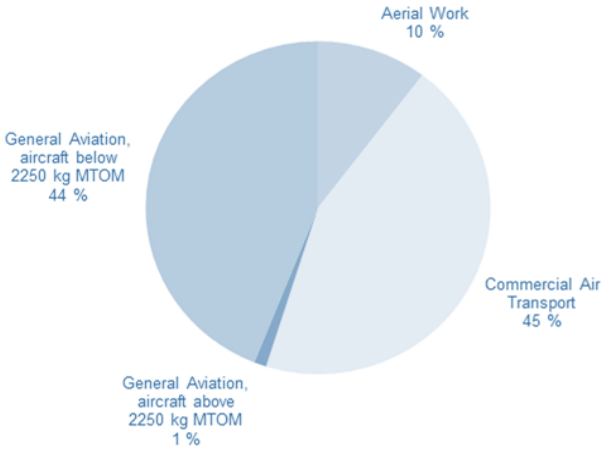


Figure 5.6 - Persons killed in air accidents on the territory of the EU, involving aircraft registered in EU-28 countries, 2015, by aviation category (Source: Eurostat)

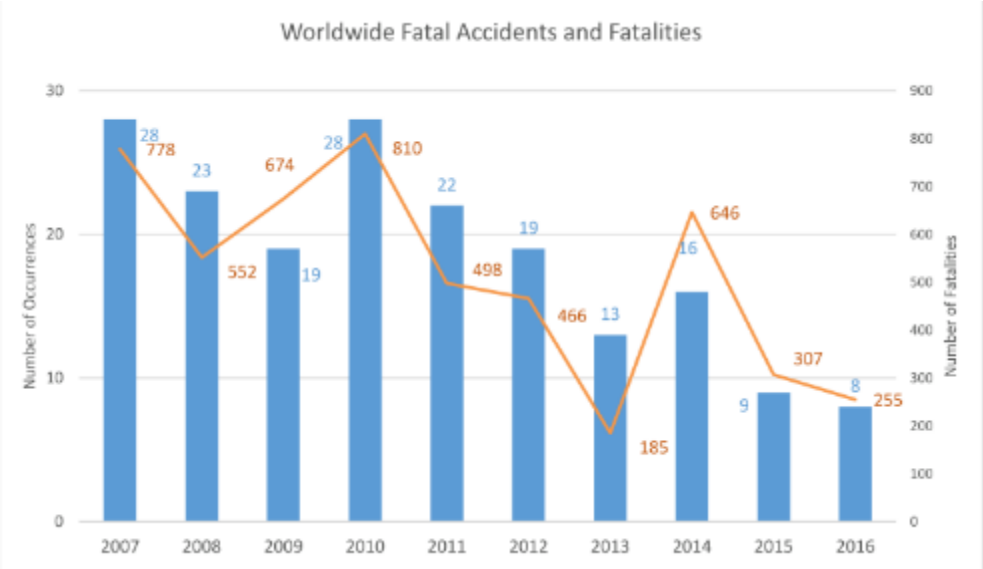


Figure 5.7. Worldwide Fatal Accidents and Fatalities - 2007 to 2016 [EASA Preliminary Safety Review 2017]

The actual number of accidents in the previous 10-year series varies from the lowest in 2009 with 17 accidents to a maximum of 31 accidents in 2012. In 2015 there were 25 accidents, which is within the average of the historical series. In terms of fatalities, the single fatal accident resulted in 150 fatalities, which is higher than the 10 years average. There was also a slight increase in serious injuries with 11 compared with 9.2 over the previous 10 years. At the same time, there was a 24% reduction in the number of serious incidents over the same period with a total of 58 serious incidents compared with the average of 75.8. EASA MS AOC holders show a lower rate of fatal accidents per one million departures than the rest of the world. The rate has remained well below 0.5 fatal accident per million departures since 2006 (Figure 5.8):

Figure 5.8 - CAT aeroplane fatal accident rate per million departures world-wide vs EASA MS [EASA Annular Safety Review 2016]

The split in terms of operation type of the aircraft involved in accidents or serious incidents in 2015 shows passenger or cargo commercial transport the main player and the presence of other operation types such as military operations or pleasure flights where they have interacted with CAT aeroplane operations in occurrences (Figure 5.9). These two last ones being part of near mid-air collisions.

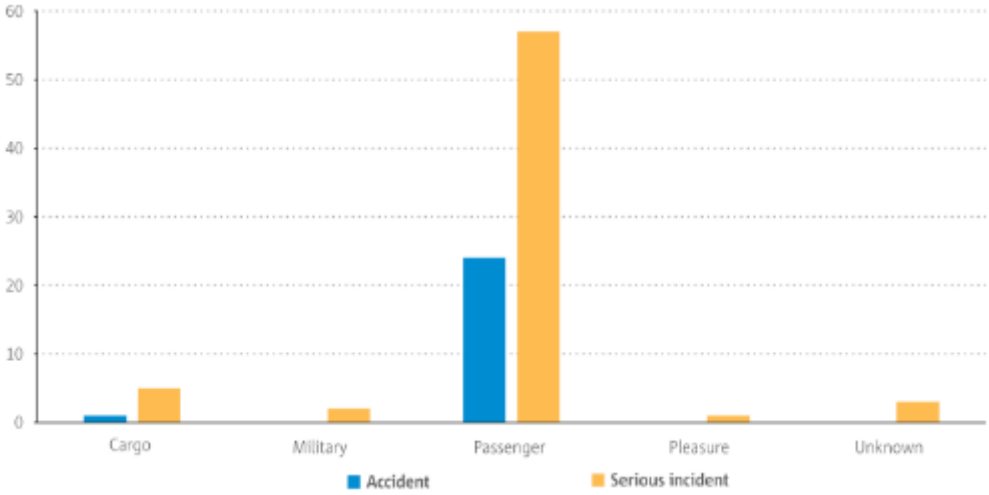


Figure 5.9 - CAT aeroplane accidents and serious incidents by operation [EASA Annular Safety Review 2016]

The counting of accidents and serious incidents is not a good risk measure. The introduction of the European Risk Classification Scheme in 2017, as part of the implementation of Regulation (EU) 376/2014, will help to provide a better picture of the existing safety risks. The Scheme will help to shift the focus to the probable potential harm of identified hazards to the European aviation system (risk level associated to hazards) instead of directly measuring the severity of a realized outcome (fatalities, injuries, damage). The Aeroplanes Safety Risk Portfolio is the result of the identification of safety issues through the analysis of safety data (historical occurrence data), and includes the joint expert judgment of the Agency, the Member States and industry, through the Network of Analysts (NoA) and the Collaborative Analysis Group in the Commercial Air Transport domain (CAT CAG), respectively. In terms of timeframe,

the data populating safety issues covers a 5 years period (2011-2015), while for the safety issues risk areas the data covers 10 years. This is to increase the representativeness of the data for risk areas that are mainly associated with accidents, which are less frequent in the CAT aeroplane domain.

Figure 5.10 compares the average number of CAT EASA MS accidents and serious incidents for the period 2007-2015 with that for 2016. The number of occurrences (accidents and serious incidents) for all Key Risk Areas, except for System Failure and Runway Excursion, remains very similar to the average for the period 2007-2015; thus, showing a stable pattern. Considering the positive trend in the period 2007-2015, followed by that in the period 2015-2016, the Key Risk Areas of System Failure, Airborne Conflict and Runway Excursion show a negative change in 2016 (from stable to increasing or from decreasing to increasing) in contribution to fatal accidents in the last 10 years with 18% of those accidents.

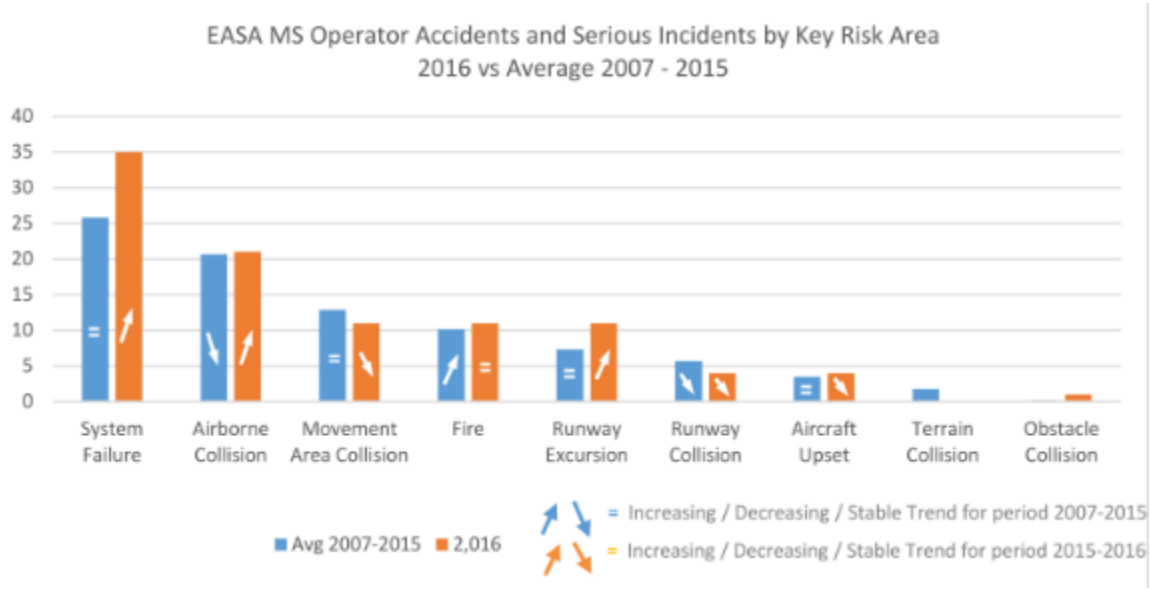


Figure 5.10 - EASA MS Operator Accidents and Serious Incidents by Key Risk Area –average 2007 to 2015 compared with 2016 [EASA Annular Safety Review 2016]

Safety Issues are the areas of safety concern that may cover one or more identified safety deficiencies that may lead to an accident. The Safety Issues are defined following an analysis of the causal and contributory factors involved in occurrences, using neutral language for the wording of the issue. Within each Safety Risk Portfolio, the Safety Issues are grouped usually into the areas of Operational, Technical, Human and Organizational. They are then ordered by the number of fatal accidents, accidents, serious incidents and incidents (taken from the ECR) in which those Safety Issues are seen to be present or involved. This ordering is then used to support initial prioritization of follow up analysis. In the Safety Risk Portfolios, Event Types in the ECCAIRS/ADREP Taxonomy have been matched as closely as possible to the different Safety Issues but this was not a perfect match in all cases and therefore the numbers should be taken as indicative of the general number of occurrences related to each Safety Issue. A total of 64% of fatal accident outcomes involve “loss of control” (Figure 5.9), which has been the most frequent fatal accident type during the last 10 years. This risk area also includes events that are direct precursors

to a loss of control event, such as a deviation from flight path, abnormal airspeed or triggering of stall protections. Below are the actions currently ongoing in the European Plan for Aviation Safety (EPAS) that are related to this key risk area.

Accidents and Serious Incidents mostly involve complex situations involve multiple causes and contributors. The graph below (Figure 5.11) highlights the origins of the causal and contributory factors behind the Accidents and Serious Incidents involving EASA Member State Operators between 2007 and 2016.

The safety target in the goal 14 can be achieved by strengthening the cradle-to-grave safety chain of aviation: (i) aircraft design based on the most reliable scientific methods, validated and tested in the more stringent conditions; (ii) meeting comprehensive certification standards in all aspects related to operations and safety; (iii) control of the supply of raw materials, documentation of fabrication processes and production quality checks; (iv) qualification of all human actors, including pilots, maintainers and air traffic controllers; (v) provision and maintenance of all support systems and equipment at the required standards; (vi) strict implementation of safety rules and procedures; (viii) reporting of incidents, without identification or blame, before they become accidents; (viii) swift implementation of protective measures once a potential hazard has been identified; (ix) continuous search for best practices and their timely implementation; (x) use of existing and development of new monitoring, fault-tolerant and adaptive systems and emergency intervention strategies.

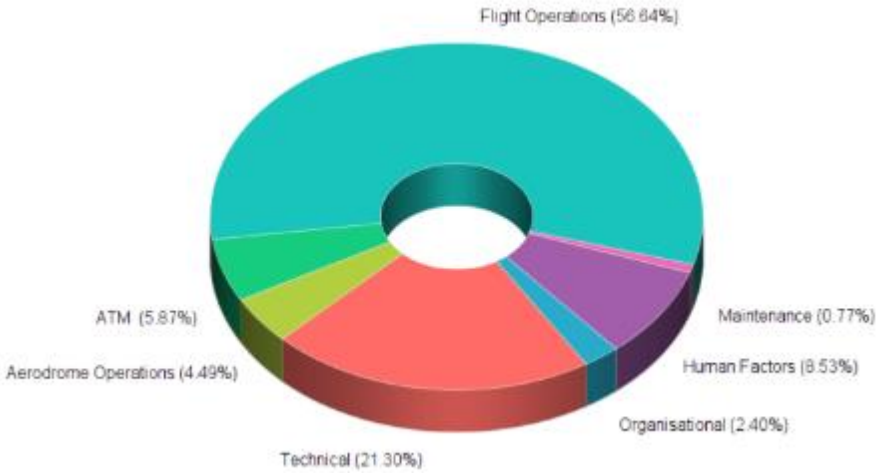


Figure 5.11 - The causal and contributory factors behind the Accidents and Serious Incidents involving EASA Member State Operators between 2007 and 2016

Safety levels in Europe are also influenced by events in countries outside the European Union. Aircraft fly into the US and Europe from all over the world, and the F.A.A. first and subsequently EASA too have banned flights by foreign airlines with dubious safety or maintenance standards. Conflicts around the world continue to challenge aviation authorities in their efforts to ensure the safe transport of passengers. The new threats highlight the need to further strengthen the links with security agencies. Safety and security risks are taking new forms through cybersecurity weaknesses and threats. The European

Commission and the Member States through the EASA Management Board have endorsed the Agency's Cybersecurity strategy which is currently being implemented. Due to the increasing population of unmanned aircraft systems (drones), EASA has been very active in this field, having proposed a flexible regulatory scheme to ensure the operation of drones does not affect the safety of the rest of the aviation system. Also, the Agency together with manufacturers and scientists, are assessing the risk of collisions between drones and other aircraft.

5.2 Weather Hazards and Risk Mitigation

**** Flightpath 2050 goal 15: "Weather and other hazards from environment are precisely evaluated and risks properly mitigated"***

Atmospheric conditions continue to be a major factor in aircraft operations, although much progress has been made in flying safety through what were, in the past, hostile scenarios. As safety progresses former hazards are overcome, and new ones are discovered, that were previously hidden behind other events. For example, wind shear or microbursts must have been the cause of accidents in the past of aircraft flying through storms but were identified clearly only 3 decades ago, as other safety hazards were overcome. General weather predictions and on-board sensors like weather radar are basic indicators of potential hazards; laser Doppler radar is a good complement not generally fitted to airliners. The information from flights of preceding aircraft on similar routes can also be a useful warning.

An example is a wind shear associated with a microburst: (i) a toroidal vortex lies above the ground; (ii) it creates a downflow through its core; (iii) the following horizontal flow changes from head wing to tailwind as an aircraft flies under the core; (iv) the combination of downflow and tailwind can lead to stall and/or crash. The wind shear is most readily detected by LIDAR that measures wind speed; it can be detected by the weather radar if the microburst is associated with rain. The indications of an aircraft that has recently flown a similar path are a warning for the safest option of wind shear avoidance.

The mitigation of weather hazards thus requires: (i) supplementing meteorological data by information from ground-based or airborne weather radars or lidars and flight reports; (ii) early warning of the flight concerned on the type and severity of the hazard likely to be encountered; (iii) accurate assessment of the risk, survival tactics and timely decision of avoidance if appropriate. The training of pilots on mitigation strategies is the last-ditch defence if warnings have failed. For example, in wind shear, the best strategy is to fly at maximum power and angle-of-attack to minimize altitude loss and sink speed (rather than dive trying to gain speed and lift). Other weather hazards like winds, clear air turbulence, various types of clouds, rain, icing, lightning, volcanic ash clouds, hail, require different strategies.

The severe weather-related accidents and incidents can be attributed to the following weather-related hazards [EUROCONTROL Report]:

- In-flight icing;
- Severe air turbulence (convective cloud origin);

- Hail damage;
- Lightning strike;
- Low visibility due to fog or precipitation;
- Strong low level/surface winds and wind shear.

As seen in Figure 5.12 the risk indicator for accidents due to extreme weather is calculated to be zero [EWENT D5.1]. This ensures the calculations which were done by taking into account the accident rates during the last years (accidents caused by adverse weather). Congruent with the risk indicators of other transport modes the highest risk indicator is in Hungary and Poland where high population and transport density together with low GDP and low quality of infrastructure produce a high-risk level. However, the risk level in aviation is significantly lower than in a railway or road transport.

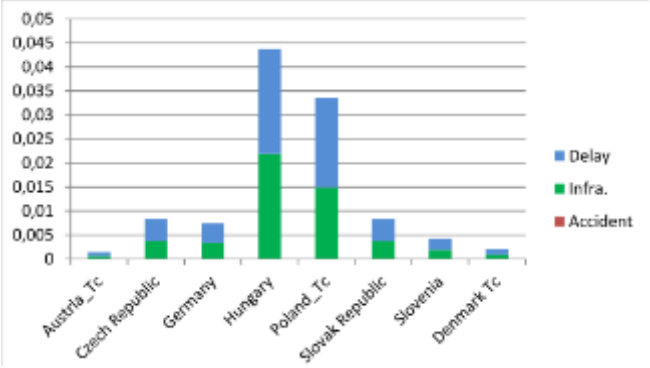


Figure 5.12 - Risk indicators in the Temperate Central region for aviation passenger's transport due to extreme weather events [EWENT D5.1]

The differences concerning the prevailing weather events in this eastern part of the temperate region in comparison to the ones in the western part are not the same from a meteorological point of view. In the Eastern Temperate region, the most likely aviation disturbing weather phenomena seem to be snowfalls (over 1 cm/d) and cold waves when temperature drops under -0 °C. Due to these phenomena, there exist operating restrictions which lead to delays and increased fuel consumption because of airborne holding for arriving aircraft [EWENT D5.1].

Also, delays for flight cancellation are possible (Figure 5.13). Compared to other modes of transport even slight disruptions in the flight plans at airports being at their capacity limit can lead to massive disruptions throughout Europe and the rest of the world.

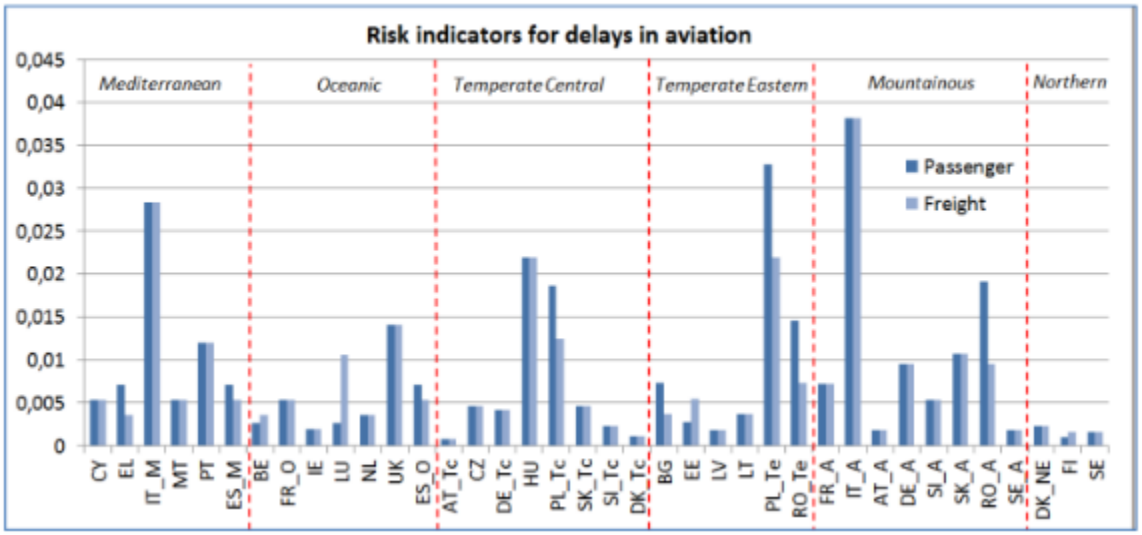


Figure 5.13 - Risk indicators for delays in EU [EWENT D5.1]

At the European level, estimates of accidents costs resulting from extreme weather for aviation, the two significant cost items were operator costs resulting from cancellations of flights and time costs for passengers. Operator costs were calculated for selected airports, covering 88% of daily volumes in Europe based on the reported number of bad weather days on which an average rate of cancellations was calculated. For passenger time costs, the Eurocontrol official values of time were used to calculate the average delay for each passenger during the number of bad weather days reported for 2010 at the major European airports (the average cancellation rate has been 10 per cent of daily flights). The average delay represents the fact that accumulated delays in major airports result in a continuous problem of delays during the day and sensitivity analyses were carried out concerning the estimated duration of the delay for each passenger.

The annual operator costs for aviation in 2010 were 606 million euros. This is calculated on the bases of 10% cancellation rate for medium jets. The annual time costs for aviation in 2010 were 980 million euros. This calculation is based on 30 minutes average delay/flight on selected airports (Figure 5.14) [EWENT D5.1]. The data shows the annual impact of cancellations for those airports reviewed by Eurocontrol. The reason why the Northern European climate region dominates the calculation is naturally the volume of extreme weather days compared to other regions. Due to the regional classification between the Temperate Eastern and the Temperate Central regions, no airports reviewed feature in the Temperate Eastern region.

Aviation has the most advanced and standardized safety and operational regulations, naturally due to the very strong weather-related safety risks, and these are and must be followed with precision (Figure 5.15). The severe weather impact can be associated with two different, yet interdependent, risks, notably *Flight Safety Risk* and *Flight Efficiency Risk*. The *Flight Efficiency Risk* is associated with the likelihood and potential extent of incurred flight delays or even cancellations made due to severe weather risk management. The Flight Safety Risk is the ultimate driver for the existence of severe weather impact

management. Flight Safety Risk can have different sources and manifestations: In-flight Safety Risk (impact on the flight crew and to put the *Hazard Encounter Risk* at the core of the approach as it is the original reason for the existence of the array of activities associated to severe weather risk management) and ATCO Excessive Overload Risk. For this approach, the management of the Hazard Encounter Risk is described using two generic risk management functions: *risk prevention* and *risk mitigation*.

Risk prevention is understood as any action aimed at avoiding the materialization of the risk. These actions are further assigned to three-time phases:

- Pre-tactical prevention – all actions taken before the day of operation;
- Tactical prevention – all actions taken on the day of operation, but before the commencement of the flight (off-block);
- In-flight prevention – all actions taken after the commencement of the flight (off-block) but before hazard encounter.

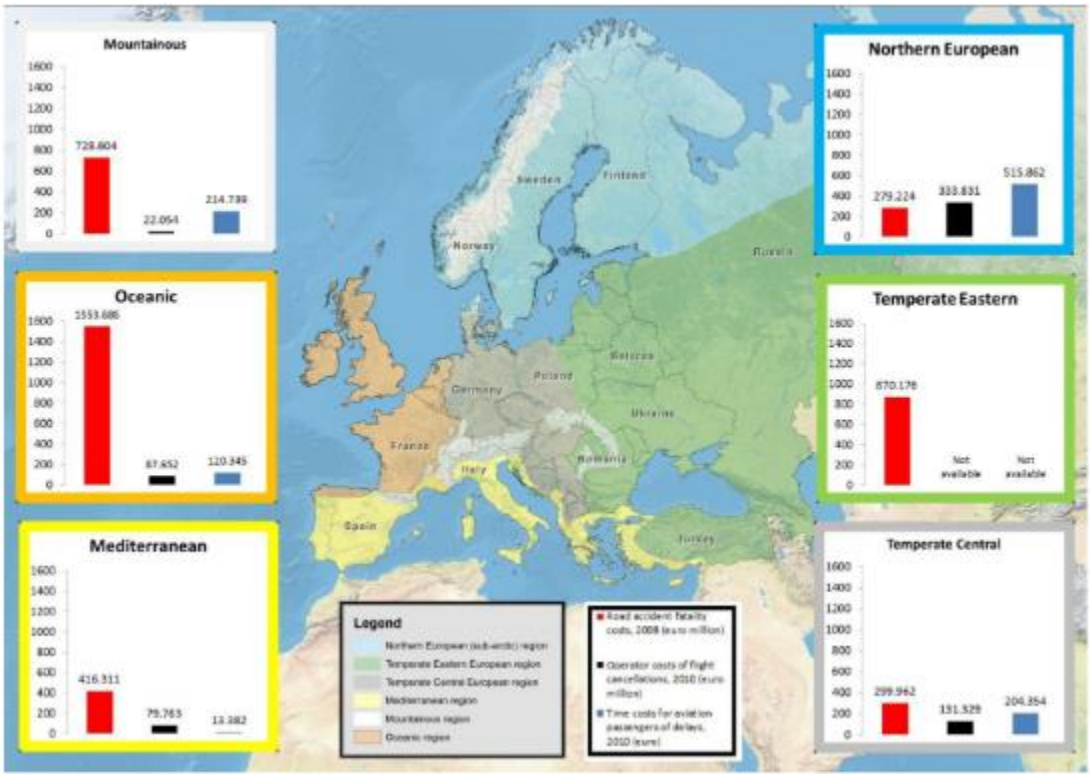


Figure 5.14. Costs (mill. €) for road accidents' fatalities (red; socio-economic costs) and aviation cancellations (black; operators' costs) and aviation delays (blue; passenger time costs) by climate regions [EWENT D5.1]

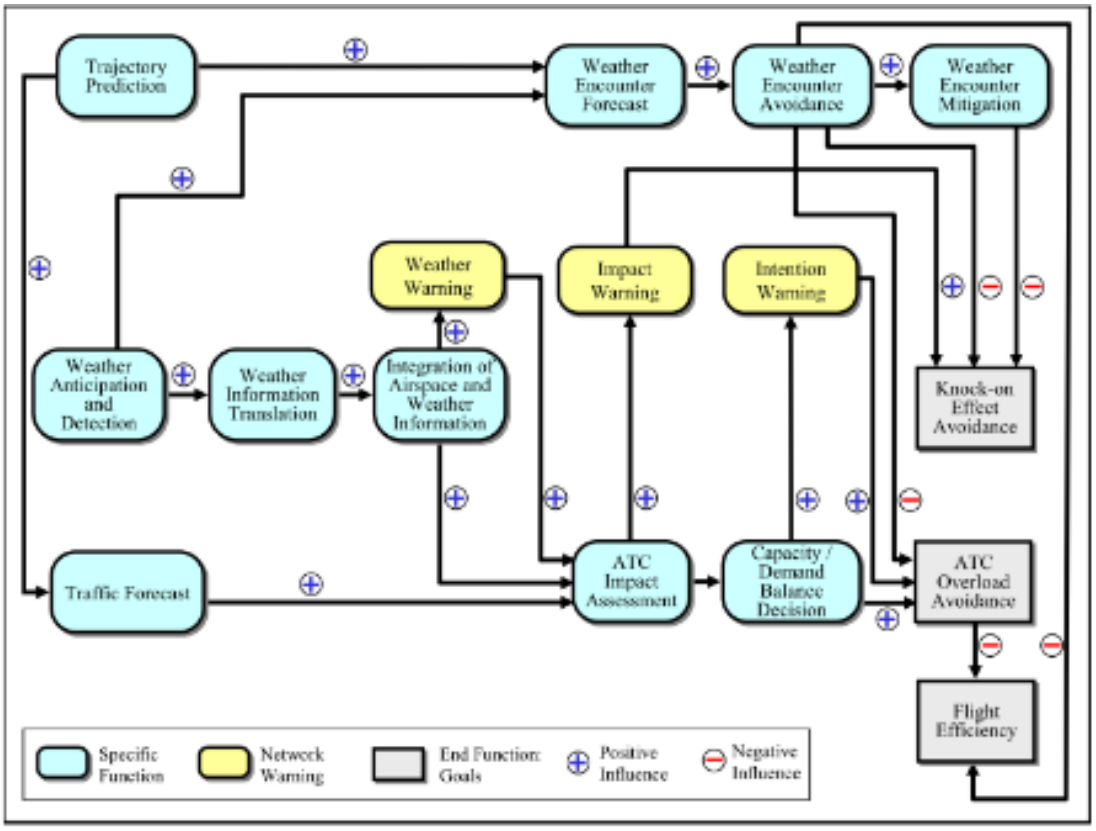


Figure 5.15 - Hazard encounter risk management model [EWENT D5.1]

Risk mitigation could be described as the actions taken by the concerned actors to contain the impact and minimize potential adverse safety effects on ATM and flight operations following hazard encounter or when the encounter is imminent. Expected further elaborations for that in meteorology [Gerz T.]:

- Need for system-wide information sharing among all aviation stakeholders;
- … necessary for their collaborative decision-making processes;
- Derive simple, unambiguous and standardised products;
- Combine different hazards when and where appropriate: seamless, and in the aviation sector;
- Develop impact scenarios for various stakeholders
- Derive business cases to tailor MET info to the user's needs.

5.3 Integrating Drones in Manned Airspace

**** Flightpath 2050 goal 16: "The European air transport system operates seamlessly through interoperable and networked systems allowing manned and unmanned air vehicles to safely operate in the same airspace"***

The term "drones", although possibly inaccurate or inappropriate, is used for brevity as in colloquial language, to designate UAVs (Unmanned Air Vehicles), RPVs (Remotely Piloted Vehicles), Remotely Piloted Aircraft Systems (RPAS), AAVs (Autonomous Air Vehicles), etc … The use of drones currently falls into 3 categories:

- Long-range global operations like "Global Hawk" imply take-off and climb and descent and landing in restricted military airspace and cruise above airline traffic at altitudes of 18 km or more;
- Flight in line-of-sight, in good weather, not overflying populated areas, at a limited altitude (usually below 100 m), as an extension of the traditional radio-controlled aircraft models;
- Unrestricted flight in remote, uncontrolled war-torn regions like Afghanistan, Syria or Iraq, with lack of safety standards or their enforcement.

Two main areas are identified within the UAS spectrum in terms of the types of operation: 1) the professional use of drones for various security, safety, survey and other tasks and 2) the recreational use where the general public are using drones for fun and private activities.

Ensuring safety with Unmanned Aircraft requires a different approach (Figure 5.16) that [Stark B.]:

1. Incorporates dynamic risk management systems;
1. Has built-in mechanisms for improvement, and,
2. Scales appropriately to risk.

In Risk Assessment, Quantitative Statistics is a basic element. The number of drones within the EU has multiplied over the last 2 years. EASA has already introduced a technical opinion to initiate the definition of the regulatory framework required at EU level. Most of the occurrences in this RPAS analysis were related to either airspace infringements which occasionally lead to a near collision with an aircraft. Analysis of RPAS occurrences in the European Central Repository identified 584 occurrences of all severity levels, of which 37 accidents had been classed as accidents (2011-2015), none of the accidents involved fatalities and there were only four minor injuries reported in the period since 2010 (Figure 5.17). The application of the definition of accident in relation to RPAS has improved since new definitions were provided in ICAO Annex 13.

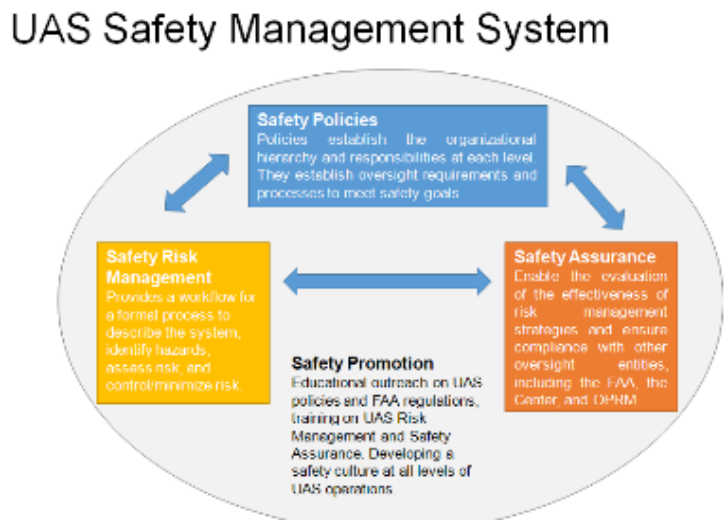


Figure 5.16 - UAS Safety Management System [Stark B.]

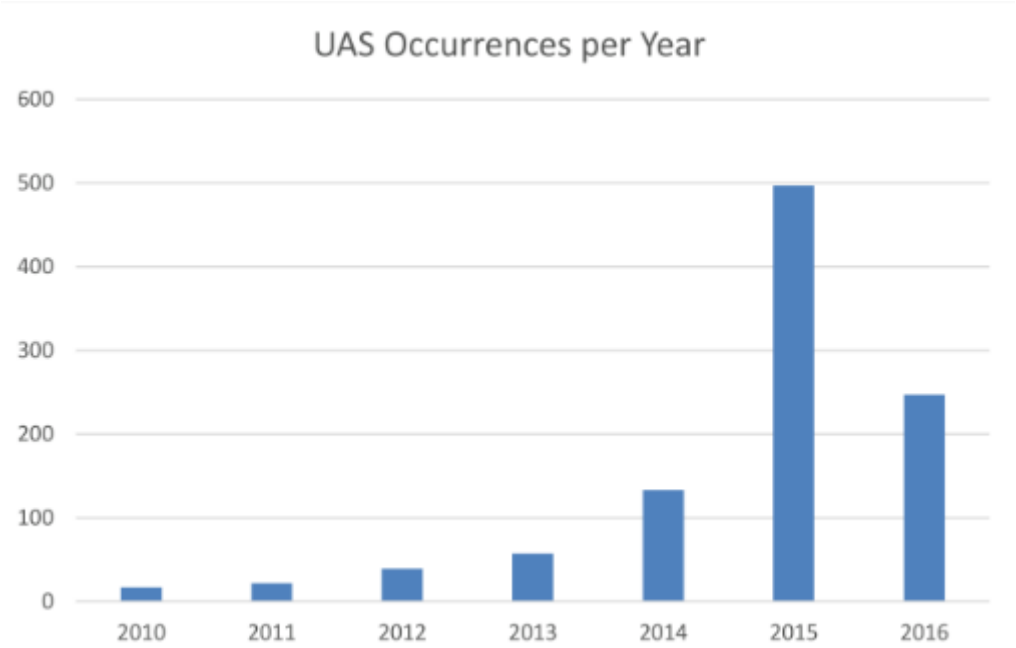


Figure 5.17 - RPAS occurrences per year – 2010 to 31 May 2016 [EASA SM1.1]

This graph (Figure 5.17) shows an increasing trend in the number of reported UAS occurrences (both accidents and incidents) per year from 2010 to June 2016 that involve UAS, with a clear and significant jump in 2014. Up to 31 May 2016, the number of occurrences in 2016 reached 50% of those in 2015 and this does not take into account the reporting process time lag between an occurrence happening and it being reported through an NAA to the ECR. In considering the risk of a collision between a manned aircraft and a small unmanned aircraft, the EU Task Force considered that the key risk to address was firmly centred on a collision with a large commercial aeroplane; this view was supported by the responses received to the related survey question as shown in the Figure 5.18:

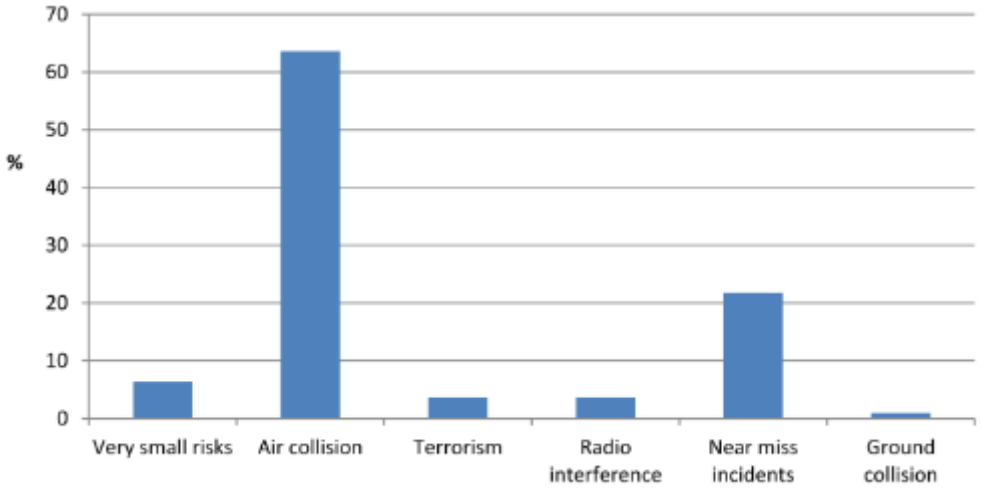


Figure 5.18 - Responses to the question on "Main Perceived Risks" [EASA SM1.1]

Figure 5.19 shows the initial Event Types analysis in which precursors to Airborne Conflict accidents unsurprisingly feature highly. These include Airspace infringements and Loss of Separation, as well as near-collisions. The vast majority of the Safety Issues subsequently identified, and the analysis that follows covers this outcome category. It can be seen that 63% of occurrences are related to Airborne Conflict, which is the main Key Risk Area. This means that airspace infringements and proximity of drones to other aircraft are causing a significant number of occurrences.

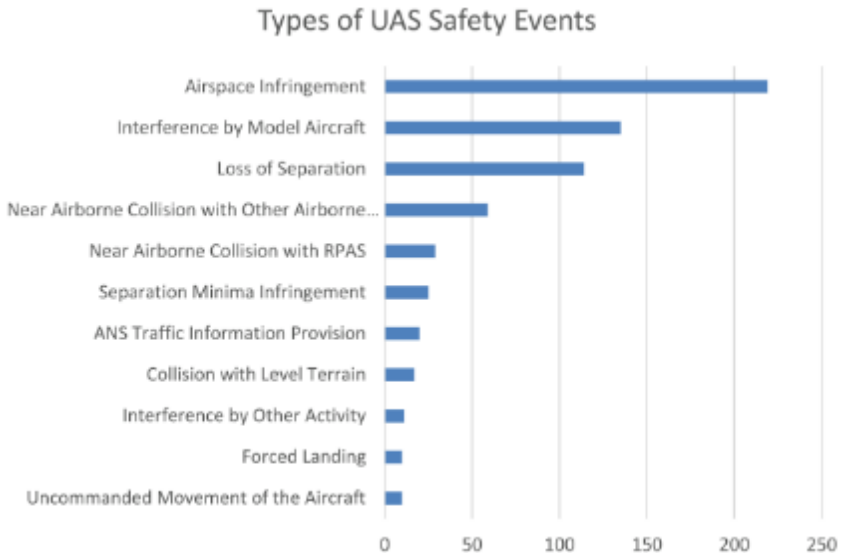


Figure 5.19 - UAS Occurrences 2010- May 2016 - Safety Events [EASA SM1.1]

Figure 5.20 shows the number of reported Airborne Conflict occurrences taken from the ECR which highlights the different numbers across the EASA MS. Further data is becoming available from other sources in individual States (such as from the ANSV – Accident Investigation Board Italy). The data from operators collected through the CAT Aeroplanes CAG were used to cross-check the number of occurrences in different states.

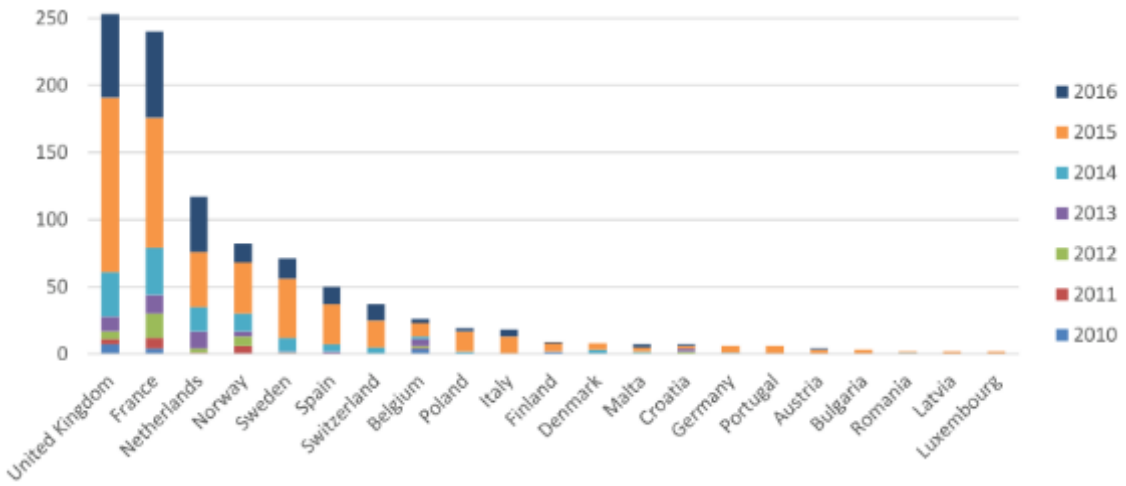


Figure 5.20 - UAS Airborne Conflict occurrences per state. Time period 2010-May2016 [EASA SM1.1]

Figure 5.21 provides details of the airspace class where occurrences took place (limited to the occurrences where this information was available) provided also with the flight phase of the aircraft that reporting the occurrence. The graph shows that the highest number of occurrences took place in D and G class airspace. Class D – Controlled airspace: IFR and VFR flights are permitted, and all flights are provided with air traffic control service, IFR flights are separated from other IFR flights and receive traffic information in respect of VFR flights, VFR flights receive traffic information in respect of all other flights (ICAO Airspace Classifications). Class G – Uncontrolled airspace: IFR and VFR flights are permitted and receive flight information service if requested. It can also be seen that most of the occurrences happen during Approach and en route phases of the flight. It also needs to be considered that many occurrences do not have any airspace information coded which limits the usability of the data.

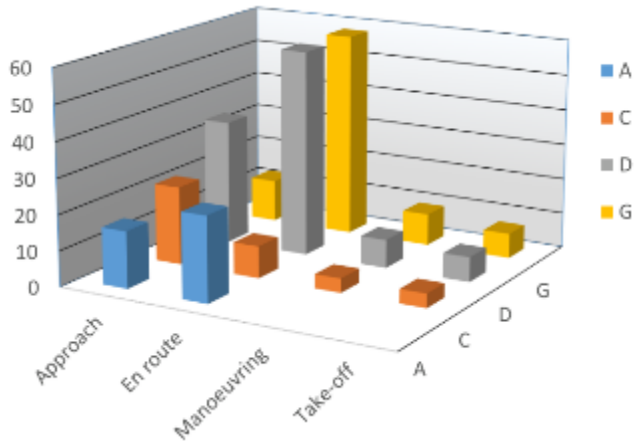


Figure 5.21. UAS Occurrences in Relation to Airspace by Flight Phase. Time period 2010-May2016 [EASA SM1.1]

In contrast with this limited use, there is a vast potential to be exploited, and no shortage of highly visible candidates like Amazon and Google wanting to offer delivery, surveillance and other services. These services and experiments can be authorized on a case-by-case basis to ensure safety. Prospective users

like Google have suggested blanket approvals like: all space below 100 m reserved for drones; ignoring that low altitude air space is used by police helicopters, emergency medical services, etc..... The safety risks are well documented by a variety of incidents involving unauthorized use of drones violating legal rules, such as: (i) numerous cases of drones flying near airports, including cases in which the aircraft had manoeuvre to avoid a collision; (ii) landing a drone in the lawn of the White House in the US, the building of the prime minister of Japan, a North Korean drone near the office of the prime minister of South Korea; (iii) several overflights of French nuclear power stations by drones; (iv) a drone seen on television crashing just behind an alpine skier in a competition it was filming; (v) ISIL used drones to drop rudimentary bombs in Iraq and Syria. Setting aside unauthorized use and the difficulties in preventing it, the main question in what conditions should drones be allowed to share airspace with manned aircraft? At least 4, namely:

- Professionalism: The record of aviation as the safest mode of transport relies on the highest professional standards: the engineers who design the aircraft, the authorities that certify it, the pilots that fly it, and the air traffic controllers that direct it. Where fits a layman flying a drone? What qualifications, training and safeguards are needed so that this is not the weak, unprofessional link?

- Quality: Commercial aircraft are high-quality products in the design, testing, materials, production and operation, all of which are neither easily achievable nor cheap. Can a cheap drone, produced, without quality control be a safe partner in congested airspace, or must it meet at least the same quality standards?

- Sense and avoid: This is the issue discussed most often concerning the safety of removing the local pilot and remote air traffic controller from the critical process of collision avoidance. If the traffic density is too high collision avoidance may become impossible: how does a drone recognize this? How is it avoided?

- Capacity: Air Traffic Management (ATM) capacity has been broadly sufficient to cope with manned air traffic, with occasional delays or disruptions. It has managed to keep ahead of air traffic growth, not a mean feat, though not by a wide margin. Is there the spare capacity for a large number of drones? How to limit their number if demand turns out to be huge as market prospects suggest?

Analyse the existing studies on the subject of impact between drones and aircraft:

- Study the vulnerabilities of aircraft (windshields, engines, and airframe) taking into account the different categories of aircraft (large aeroplanes, general aviation, and helicopters) and their associated design and operational requirements.
- Consider the possibility to do further research and perform actual tests (for example on windshields).

The regulatory framework for the safe operations of drones in Europe currently being developed by EASA already addresses the issue of a collision between drones and aeroplanes. A combination of measures is envisaged such as: operate in visual line of sight, fly under 150 m height above ground, be equipped with identification and geo-limitation functions and be registered. Any operation of drones close to aerodromes would require specific authorization from the national aviation authority based on a risk assessment.

The Key Risk Areas (Outcomes) identified from the data were [EASA SM1.1]:

- Airborne Conflict: The number of reported near-miss occurrences between drones and aircraft has increased significantly in the past 2 years. There have been a small number of collisions between drones and GA aircraft, fortunately with no fatalities so far. However, it should be noted that many of the reports of near-misses with UAS are unconfirmed and might, in fact, involve other objects such as birds. Indeed, some of the reports of near-misses with UAS have occurred at altitudes where UAS are not normally able to operate.

- Aircraft Upset. The 2nd Key Risk Area identified involved Aircraft Upset, which covers the full range of Loss of Control situations, which presents the potential for injuries to people on the ground.

- System Failures. Both System/ Component Failure Power plant and Non-Power plant feature in the outcome types and therefore is also included in the Key Areas as it could also lead to injuries to people on the ground, especially in certain types of UAS operation.

- Third-Party Conflict. The final Key Risk Area covers the risk of UAS conflicts (collisions) with people or property (i.e. not involving aircraft) where they may cause injuries or damage. There were no occurrences involving such damage or injuries, but expert judgement identified this as a key risk area that could occur through causes not associated with loss of control (Aircraft Upset) or technical failure in situations where a drone operator accidentally flies into people or property.

Control Strategies and the Hierarchy of Controls is shown in Figure 5.22:

Figure 5.22 - Control Strategies for UAS safety management [Stark B.]

5.4 Comprehensive and Unobtrusive Security Measures

**** Flight 2015 goal 17: "Efficient boarding and safety measures allow seamless security for global travel with minimum passenger and cargo impact. Passengers and cargo pass through security controls without introduction"***

Aviation safety has seen steady and spectacular progress into the safest mode of transport (sections 5.1 – 5.2). The recent societal threat going back to barbarism seeks to maximize loss of life through terrorist acts aimed at most transports.

The ingenuity that has achieved the safety of air transport must also be applied to ensure its security at all stages of travel: (i) at the departure airport, through check-in, passport and luggage inspection; (ii) in the transit to the aircraft; (iii) in-flight; (iv) at the arrival airport. Terrorists who fail their murderous attempts may still see some success in the disruption caused by the safety measures needed to foil their evil intents. While the patience and understanding of passengers are essential there should be the minimum of delay, intrusion and disruption in the implementation of safety measures, through the use of the most appropriate equipment and airport architectures. The standards of European airports may not be taken for granted at some remote or holiday destinations, possibly requiring further security initiatives.

The policy instruments have shaped ICAO's aviation security programme direction, and provided a focus for priority setting for the Organization [ICAO A39-WP/14]:

a) Declaration on Aviation Security adopted through Resolution A37-17, which reaffirmed Member States' commitment to strengthen global aviation security;

b) The ICAO Comprehensive Aviation Security Strategy (ICASS), which emphasizes seven Strategic Focus Areas of the Organization over two triennia (2011-2016) mandated by the 37th Assembly;

c) Conclusions and recommendations of the 2012 High-level Conference on Aviation Security aimed at strengthening the global aviation security framework, particularly by mitigating the risks to air cargo and mail security and addressing the insider threat; and

d) Resolutions adopted by the ICAO Assembly on the consolidated statement of continuing ICAO policies related to aviation security.

The 39th ICAO Assembly (in 2016), recognizing the need to strengthen aviation security worldwide, in light of the continuing threat to civil aviation, including the attempted sabotage of Northwest Airlines flight 253 on 25 December 2009; and acknowledging the value of the joint declarations on civil aviation security emanating from regional conferences held with a view to enhancing international cooperation, hereby urges Member States to take the following actions to enhance international cooperation to counter threats to civil aviation [ICAO A39-WP/16]:

1) strengthen and promote the effective application of ICAO Standards and Recommended Practices, with particular focus on Annex 17 [ICAO Annex 17] — Security, and develop strategies to address current and emerging threats;

2) strengthen security screening procedures, enhance human factors and utilize modern technologies to detect prohibited articles and support research and development of technology for the detection of explosives, weapons and prohibited articles in order to prevent acts of unlawful interference;

3) develop enhanced security measures to protect airport facilities and improve in-flight security, with appropriate enhancements in technology and training;

4) develop and implement strengthened and harmonized measures and best practices for air cargo security, taking into account the need to protect the entire air cargo supply chain;

5) promote enhanced travel document security and the validation thereof using the ICAO Public Key Directory (PKD) in conjunction with biometric information, and the commitment to report on a regular basis, lost and stolen passports to the INTERPOL Lost and Stolen Travel Documents Database to prevent the use of such travel documents for acts of unlawful interference against civil aviation;

6) improve Member States' ability to correct deficiencies identified under the Universal Security Audit Programme (USAP) by ensuring the appropriate availability of audit results among the Member States, which would enable better targeting of capacity-building and technical assistance efforts;

7) provide technical assistance to States in need, including funding, capacity building and technology transfer to effectively address security threats to civil aviation, in cooperation with other States, international organizations and industry partners;

8) promote the increased use of cooperation mechanisms among Member States and with the civil aviation industry, for information exchange on security measures in order to avoid redundancy, where appropriate, and for early detection and dissemination of information on security threats to civil aviation, including through the collection and transmission of advance passenger information (API) and passenger name record (PNR) data, as an aid to security, whilst ensuring the protection of passengers' privacy and civil liberties; and

9) share best practices and information in a range of key areas, such as: screening and inspection techniques, including assessments of advanced screening technology for the detection of weapons and explosives; document security and fraud detection; behaviour detection and threat-based risk analysis; screening of airport employees; the privacy and dignity of persons; and aircraft security.

A more integrated approach to aviation safety and security is needed, as illustrated by issues such as cybersecurity and remotely-piloted aircraft systems; aviation security requires a cross-functional approach that ensures appropriate coordination with facilitation, aviation safety, air navigation and other relevant fields. More real-time sharing of critical information between States and industry, and between aviation security professionals and partners who need to know should be encouraged, as highlighted by recent events related to civil aviation operations near conflict zones.

The main components for defining the GASeP, as illustrated in Figure 5.23, should be built around six key themes, under which specific goals and targets (Table 5.1) could be pursued. It also includes four broad areas of "enablers", which contribute towards achieving goals related not only to one key theme but across all themes. While further details of the GASeP would need to be elaborated and refined, the six key themes of the GASeP, could be used to help frame the deliberations [ICAO A39-WP/15].

Key objectives from 2017 used for ICAO comprehensive aviation security strategy and development of the ICAO GASeP [ICAO A39-WP/14]:

Strategic Focus Area 1: *Addressing new and existing threats*. ICAO made continued efforts to enhance risk awareness, promote risk policy, and implement a risk-driven security culture with to ensure risk-based Standard-setting and rule-making on the basis of guidance material such as the Aviation Security Global Risk Context Statement. *Key objectives for 2017-2019*: Continue efforts to ensure States take substantial steps to incorporate effective threat and risk assessment methodologies and mechanisms into their national aviation security programmes.

Strategic Focus Area 2: *Promoting innovation in aviation security*. ICAO focused on innovation, collaborative actions and coordinated efforts such as through the organization of an ICAO Symposium on Innovation in Aviation Security (2014), supporting the ACI Airport Excellence (APEX) programme, the establishment of an AVSEC Panel Working Group on Innovation in Aviation Security (WGIAS) and enhancements to the AVSECPaedia within the ICAO secure portal (https://portal.icao.int); all designed to

stimulate innovative, effective, and efficient security approaches to aviation security. *Key objectives for 2017-2019*: Promote the increased sharing among States of best practices and emerging trends in aviation security systems and technologies utilizing ICAO platforms.

Figure 5.23 - Key themes, under which GASeP specific goals and targets could be pursued [ICAO A39-WP/15]

Goals	Targets
1: Improved capacity to address all threats to aviation security	1. By 20xx, States have utilized effective threat and risk assessment methodologies; 2. By 20xx, States have made significant efforts to promote risk-based measures and approaches; 3. By 20xx, States have implemented mechanisms to ensure greater threat information sharing;
2: Achieve higher levels of effective implementation of ICAO Annex 17	4. By 20xx, compliance by States and Regions to substantially improve levels of aviation security;

	5. By 20xx, mobilize additional financial resources for effective implementation of aviation security; 6. By 20xx, substantial reduction of States with significant security concerns (SSeCs);
3: Promote development of human resources in aviation security	7. By 20xx, substantial steps taken by States to promote security culture across all organizations; 8. By 20xx, significant efforts by States to promote greater capacities of security professionals;
4: Effective and efficient security measures through process and technology innovation	9. By 20xx, States have strengthened technological capacity to address the threat posed by LAGs; 10. By 20xx, substantial efforts made by States to enhance research and to foster innovation; 11. By 20xx, all States have utilized ICAO platforms for sharing screening best practices; 12. By 20xx, greater efforts by States to recognize other States' systems where determined equivalent;
5: Enhance implementation through capacity building	13. By 20xx, enhance regional partnerships for implementing effective and targeted capacity-building activities to support regional initiatives and plans;
6: Integrated approach to aviation safety, security and other disciplines	14. By 20xx, more efforts by all States to ensure a cross-functional approach to aviation security.

Table 5.1 - Indicative list of GASeP goals and targets

Strategic Focus Area 3: *Sharing of information*. Efforts have been made to continuously strengthen ICAO capacity to securely gather, collate and disseminate information on security incidents, threat and risk concerns, and trends through improved functionalities of the relevant ICAO platforms, particularly the Point of Contact (PoC) Network, which currently includes PoCs from nearly all ICAO Member States, the Acts of Unlawful Interference Database, and information on Universal Security Audit Programme (USAP) audit results and Significant Security Concerns (SSeCs). *Key objectives for 2017-2019*: Improve mechanisms for the reporting by States of acts of unlawful interference in accordance with Annex 17 and the dissemination of relevant information.

Strategic Focus Area 4: *Promoting global compliance and establishing sustainable aviation security oversight capability of States*. Throughout the triennium, ICAO ensured greater coherence and coordination in rectifying deficiencies identified by the USAP including the Comprehensive Regional Implementation Plan for Aviation Security and Facilitation in Africa (AFI SECFAL), which was launched as an ICAO Programme to enhance the coordination of assistance activities in Africa [ICAO A39-WP/20,

A39-WP/28]. Key objectives 2017-2019: Enhance implementation and address deficiencies in States identified through audit and monitoring activities, capacity-building and resource mobilization to support effective implementation of regional plans and initiatives focused on assisting developing States to achieve improved levels of security.

Strategic Focus Area 5: *Improving human factors and security culture*. Increased emphasis was placed on addressing the continuing need for global and regional aviation security training, by collaborating with the institutions within the ICAO ASTC Network, which now comprises 30 members. *Key objectives 2017-2019*: Enhance aviation security training efforts by collaborating with the institutions within the ICAO Aviation Security Training Centre Network.

Strategic Focus Area 6: *Mutual recognition of aviation security processes*. Continued efforts in promoting mutual recognition of aviation security processes were made through extensive collaboration with stakeholders and industry, including dissemination of the newly developed guidance material Recognition of Equivalence of Security Measures as well as information exchange and debate through the AVSEC Panel. *Key objectives 2017-2019*: Reduce unnecessary duplication of measures towards the optimal use of aviation security resources, to achieve the desired and appropriate balance between the effectiveness of security measures and the efficiency of air transport, including optimized facilitation.

Strategic Focus Area 7: *Emphasizing the importance of aviation security worldwide*. Increased outreach activities at the national, regional and international levels led to improved awareness of the global aviation security threat environment. For example, to strengthen air cargo security, ICAO carried out a range of joint initiatives with the World Customs Organization (WCO), designed to heighten awareness among aviation security authorities, customs administrations and stakeholders of the need to strengthen aviation and border security while facilitating the flow of cargo. Intensified ICAO/WCO collaboration included, for example, Joint ICAO/WCO Conferences, alignment of regulatory frameworks, joint training courses and the publication of a document entitled *Moving Air Cargo Globally*. *Key objectives 2017-2019*: Improve awareness of the global aviation security threat environment and promotion of dialogue on new and emerging aviation security challenges.

The foundational element of the framework should be based on the notion of progressive aviation security enhancement as the core objective, consistent with ICAO's Strategic Objective. For practical purposes, aviation security enhancement is defined as the improvement in the effectiveness and efficiency of aviation security to mitigate the risk of acts and attempted acts of unlawful interference, and to mitigate its consequences; it is the achieving and acquiring of qualitative improvement while managing security costs [ICAO A39-WP/15].

5.5 Resilience to External and Internal Threats

**** Flightpath 2050 goal 18: "Air vehicles are resilient by design to current on-board and on the ground security threat evolution, internally and externally to the aircraft"***

The safety door limiting access to the cockpit is an example that safety measures can in some cases function in intended and unintended ways: (i) in most cases it may have prevented hijackings; (ii) in the isolated case of the mentally disturbed German Wings co-pilot it prevented the captain from entering the cabin and preventing an intentional crash. The security measures also depend on the perceived level of threat and accepted level of risk: (i) El Al aircraft are equipped with DIRCM (Directed Infra-Red Counter Measures) to counter shoulder-fired anti-aircraft missiles, whereas most other airliners do not have such systems, originally developed for military aircraft; (ii) Israeli and at same time U.S. commercial aircraft have armed Sky Marshalls, although the use of firearms in a pressurized aircraft has risks.

Security issues can lead to difficult dilemmas: if a liner is hijacked, and refuses to follow the flight and landing instructions from an armed interceptor aircraft, and heads to a major inhabited area like 9/11, should weapons be used? An alternative would be to take over control of the aircraft remotely by building in this capability at the design stage. Doing so assumes that: (i) it is possible to decide remotely if the aircraft has been hijacked, the crew has suicidal intents or is unconscious due to hypoxia or other problems: (ii) the communications and controls allow safe flight to the closest suitable airport; (iii) the systems are immune to spoofing, cyber-attack or other malicious use. Ultimately people on board, if not controlled, have several means to cause a crash, reinforcing the need for airport security and preventive measures.

The EU is facing one of the greatest security challenges in its history [EC JOIN REPORT]. Threats are increasingly taking non-conventional forms, some physical such as new forms of terrorism, some using the digital space with complex cyber-attacks. Others are subtler and are aimed at the coercive application of pressure including misinformation campaigns, and media manipulation. Recent coordinated cyber-attacks across the globe, for which attribution has proved challenging, have demonstrated the vulnerabilities of our societies and institutions. EU leaders have placed security and defence at centre-stage in the debate about the future of Europe. This was acknowledged in the Rome Declaration of 25 March 2017 which set out a vision of a safe and secure Union committed to strengthening its common security and defence.

Security has become a major factor in civil and commercial aviation. Aviation security system to be "[r]ecognized as the world leader in civil aviation security—identifying and countering aviation-related threats to U.S. citizens worldwide" [Federal Aviation Administration]. The strategic goal stated in the plan was to let "[n]o successful attacks against U.S. civil aviation" occur. In comparison to the breadth and depth of the post-9/11 focus on aviation security, the desired key results stated in this document in retrospect seem quite modest and the goal tragically unattained.

In recent decades, the number of threats to aviation security has grown significantly. Current and emerging threats have been clustered into the following eight threat categories [COPRA SECURITY D5.1]:

- Improvised Explosive Devices (IED), firearms and close range destructive threats;
- Chemical, Biological, Radioactive, Nuclear and Explosive (CBRNE) threats;
- Ground-to-air threats;
- Ground-to-ground threats;
- Cyber threats;
- Electromagnetic threats;
- Sabotage, seizure and hijacking;
- Bluff threats and threats from social media.

Threat assessment defines the level of the threats against critical assets by evaluating the types, means and possible tactics of those who may carry them out. In a threat assessment, it is important to be aware of national threats and to identify the threats specific to the airport and to the airlines serving it. For in-depth analysis, it is also interesting to identify the history of criminal or disruptive incidents in the area surrounding the airport, but not primarily directed toward the airport operations (Figure 5.24).

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 [Bart E.].

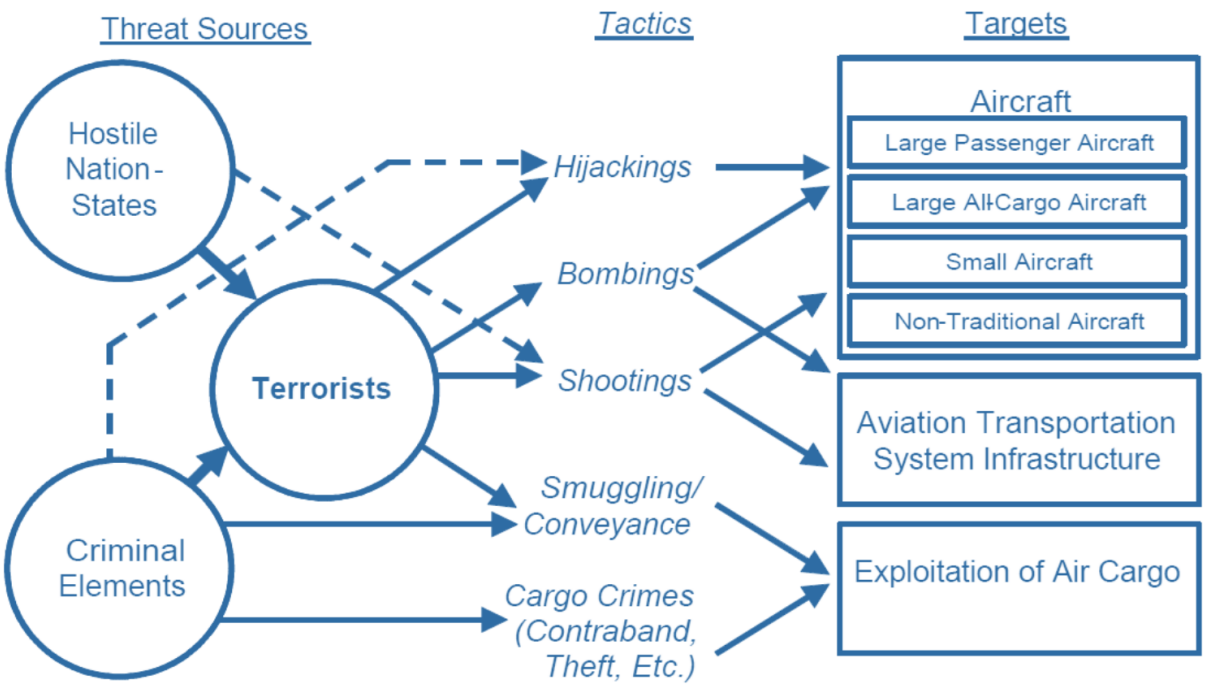


Figure 5.24 - Aviation Security Threat Sources, Tactics, and Targets [Bart E.]

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). (Figure 5.25)

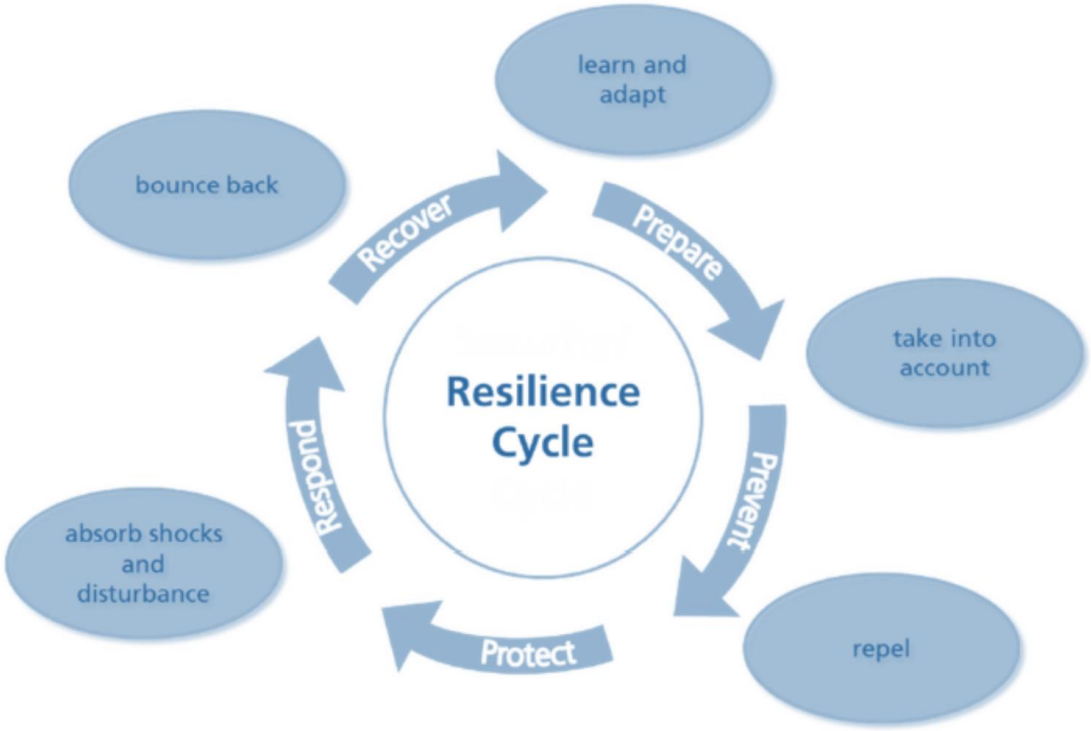


Figure 5.25 - Resilience cycle depicting possible actions associated with the different phases

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.

Security concepts should aim at involving different measures at different stages of the passengers' travel. The COPRA Aviation Security Research Roadmap [COPRA SECURITY D5.1] 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 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. For example, 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 [COPRA SECURITY D5.1]:

- Pre-incident issues (i.e. Prepare, prevent),
- Inter-incident issues (protect) and
- Post-incident issues (respond, recover).

A visual representation of the roadmap with all roadmap items plotted in a chart was designed and shown in Figure 5.26:

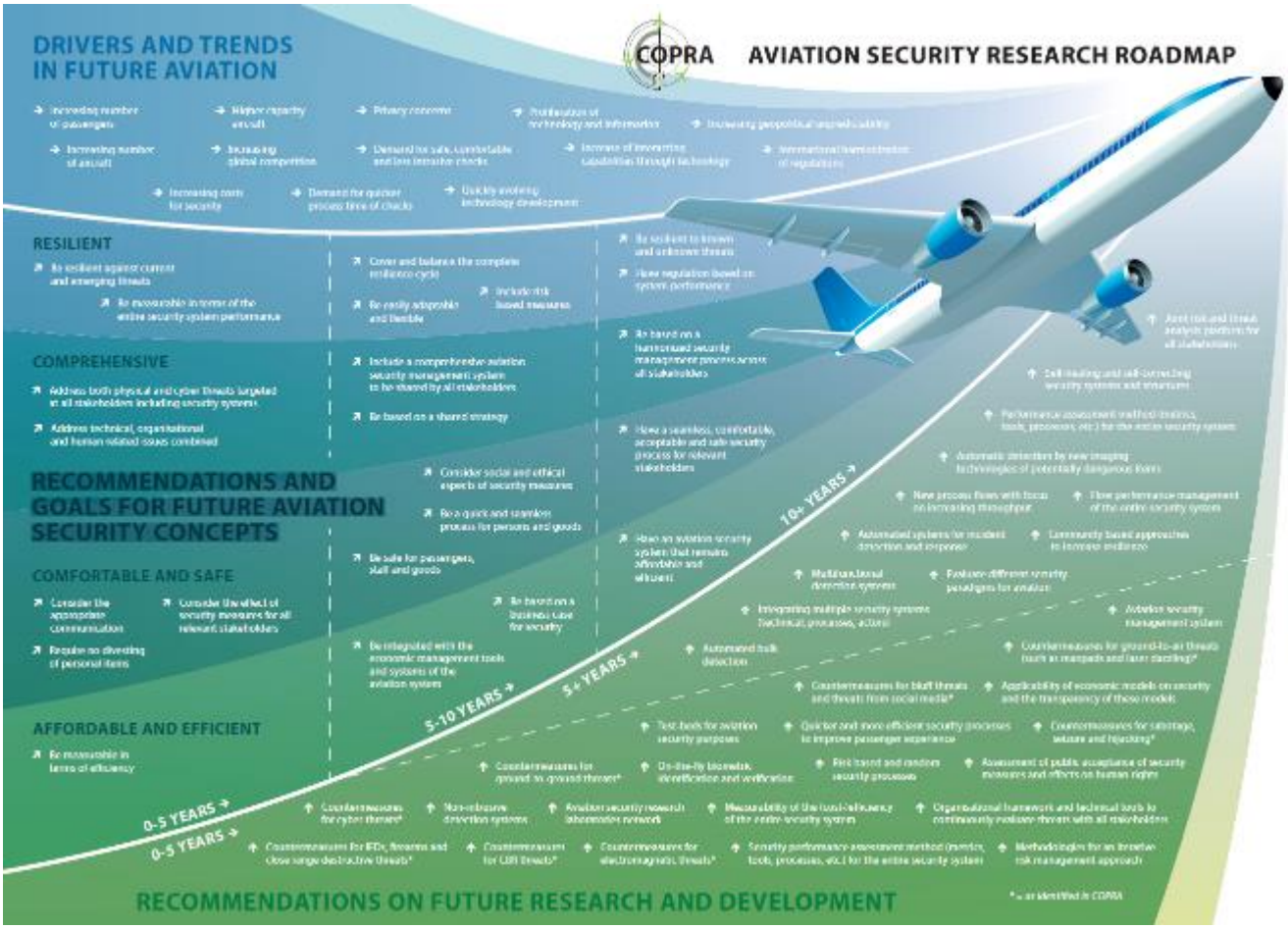


Figure 5.26 - Recommendations and goals for future aviation security concepts [COPRA SECURITY D5.1]

5.6 High-Bandwidth Data Resilient to Cyberattacks

**** Flightpath 2050 goal 19: "The air transport system has fully secured global high bandwidth data network, hardened and resilient by design to cyber-attacks"***

So far there have been no major reports of jamming of civil aircraft communications or cyberattacks on air traffic infrastructure. Some isolated incidents from the past indicate that it can happen: (i) a Tornado aircraft flying over Radio Free Europe in southern Germany may have suffered loss of control due to high power radio transmissions interfering with on board systems; (ii) the Iranian television showed an American UAV intact (except for undercarriage) that did an emergency landing (US version) or was remotely diverted (Iranian version). It is not without reason that all airliner flights request switching off of electronic devices or changing to flight mode. It is known that the standard GPS navigation signals can be easily jammed, leading at least in the U.S., to the development of "jam-resistant" GPS versions and entirely separate alternative navigation systems. The operation of air traffic will require increasing

amounts of data exchanging, needing larger bandwidth; this will give more opportunities for jamming and more entry points for a cyberattack. There are countermeasures and protection methods, some developed by the military that should be sufficient to stop a not too sophisticated attacker.

The vulnerabilities that need to be taken into account are: (i) in a large, complex interconnected system there are many entry points for cyber intrusion and many links to spread the cyber-attack; (ii) the weakest node may be the preferred entry point, for example small suppliers of equipment or codes well protected by large industries or government bodies. Cyber protection involves hardware and software and their human users in very diverse scenarios; the civilian and military cyber training events are a way to gain and update skills and tend to have a regular and expanding participation. In some cases, the hosts are the victims of cyber-attacks that have experienced their consequences and want to avoid similar situations in the future.

The principles of cyber-defence are: (i) protect each node against intrusion by multiple identification/screening/rejection measures, some of which can be quite simple; (ii) have an independent monitoring of the network capable of detecting and locating anomalies and quickly isolating them; (iii) design the system for cyber-security so that affected parts can be isolated, and the lost functions can be allocated elsewhere. It should be borne in mind that: (i) the only code that cannot be broken in that used only once; (ii) It is not possible to protect software 100% with another software.

A cyber-attack can be conducted for numerous reasons in general case:

- Disruption of airport operations, perhaps in advance of a physical attack
- Theft, Loss of data, Embarrassment to the airport and its management
- Or for no reason at all
- A cyber-attack can be carried out by numerous actors:
- Disgruntled passenger
- Hacktivists
- Criminals
- Anonymous
- Insider threats
- Nation-states, Terrorists

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 can collect and use the data resulting from different security checks [COPRA SECURITY D5.1]. A seamless end-to-end process for goods and cargo

requires a continuous flow of information on 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.

The use of digital data and the level of interconnection of IT systems are strongly increasing in civil aviation. Consequently, stakeholders of the air transport system like airlines, airports and air traffic control are more and more interlinked (Figure 5.27) and, thus, depend on secure means of data exchange.

ISO 27002 is a Security Program Benchmark and stresses a holistic approach to cybersecurity. Airport approach to cybersecurity management:

- Recognize the Reality and Don't Underestimate the Problem
- Cybersecurity is a Top Management Issue
- Think Aviation Industry-Wide
- Establish a Security Program
- Perform Risk Assessment and Prioritize Your Defence
- Establish a Strong Patching Program
- Include Cybersecurity in all levels of the Organization
- Increase your Internal Capability/Acquire Qualified External Assistance
- Develop an Adaptive Security Architecture
- Participate in the ACI World IT Security Benchmarking Tool

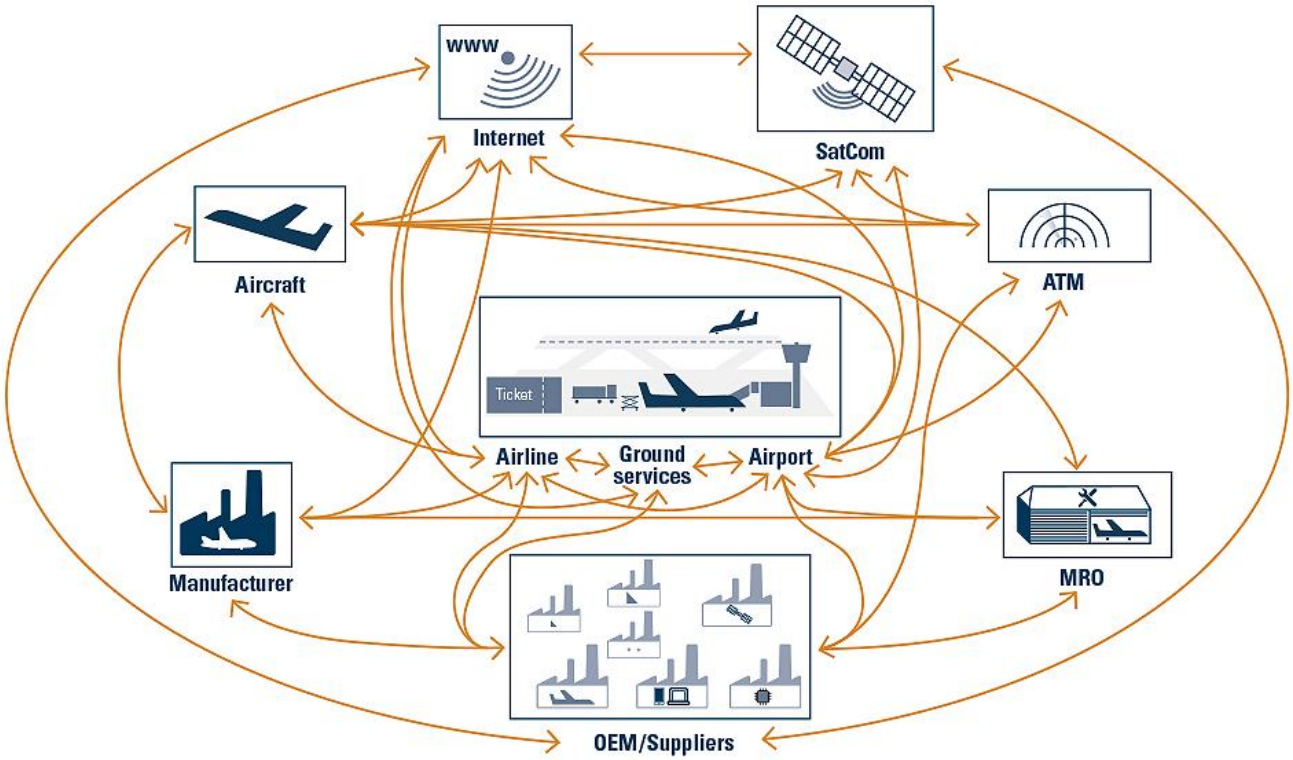


Figure 5.27 - Interconnection of the air transport system: Arrows indicate the interfaces for information exchange and, thus, represent risks for contagion effects in the case of false or missing information

ICAO Assembly calls upon States and industry stakeholders to identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents. Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems [ICAO A39-WP/17].

Cyber-attacks can impact aviation businesses in several ways, from the loss of data and intellectual property to business interruption and more. To protect all key assets and effectively manage cyber risk, it's critical that you understand the cyber scenarios your organization is most likely to face — and how much they can cost your business.

To assess your cyber risk, you should:

- Identify and inventory key assets — data, systems, and infrastructure — that are essential to your operations.
- Review your internal controls and digital profile to identify internal vulnerabilities and external threats.
- Value your cyber assets at risk using modelling and other data and technology tools.

By taking these steps, its possible to objectively measure the cyber risk, and incorporate quantitative data into the risk management decision-making.

Four comprehensive scenarios address different segments of the air transport system and serve as a basis for the analysis of specific attack vectors from internal or external aggressors (Figure 5.28). One scenario, for example, considers an incorrect representation of the airspace during transatlantic flights or near airports. In such a case, the determination of the position of one or more aircraft could be impaired, which would lead to a loss of integrity of the respective airspace. Another scenario addresses a spoofed data link between two air transport stakeholders in an area relevant for safe operation. Here, the entire air transport system could be impacted due to contagion effects.

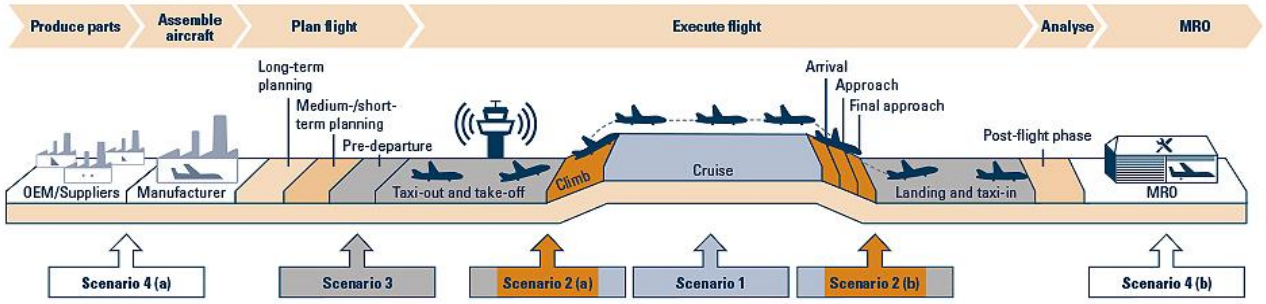


Figure 5.28 - Horizontal scenario space illustration: Both key process steps in the lifetime of an aircraft and each of the scenario spaces are depicted. Own illustration, based on EATMA (European Air Traffic Management Architecture)

Based on these potential threat scenarios, an aviation consortium is able to assess potential threats and risks for the air transport system. The project [Cyber resilience scenario] the developed scenarios will be transferred to a demonstrator to analyse how air traffic resilience could be improved concerning potential cyber threats.

Risk Management for cybersecurity in airports, airlines and flight control organizations is realized in accordance with the system approach and view, it is shown in Figure 5.28. ATC is highly dependent on the availability and integrity of its technical infrastructure, buildings, IT and communications systems. In recent years, particular attention has been given to this topic. But this remains an important area of concern with regard to potential penetrations aimed at causing dramatic incidents (*e.g.*, the SAIFIT project on IT security, SAFEE on advanced aircraft security system).

It is not without reason that all airliner flights request switching-off of electronic devices or changing to flight mode.

The increasing complexity and interconnection of systems provide more entry points for cyber-attacks and more paths for its spread. A cyber-protection system must continuously monitor the whole network, quickly detect anomalies, isolate the affected systems, and restore their functions by other means.

The consideration of safety and security measures indicates the importance of the following topics.

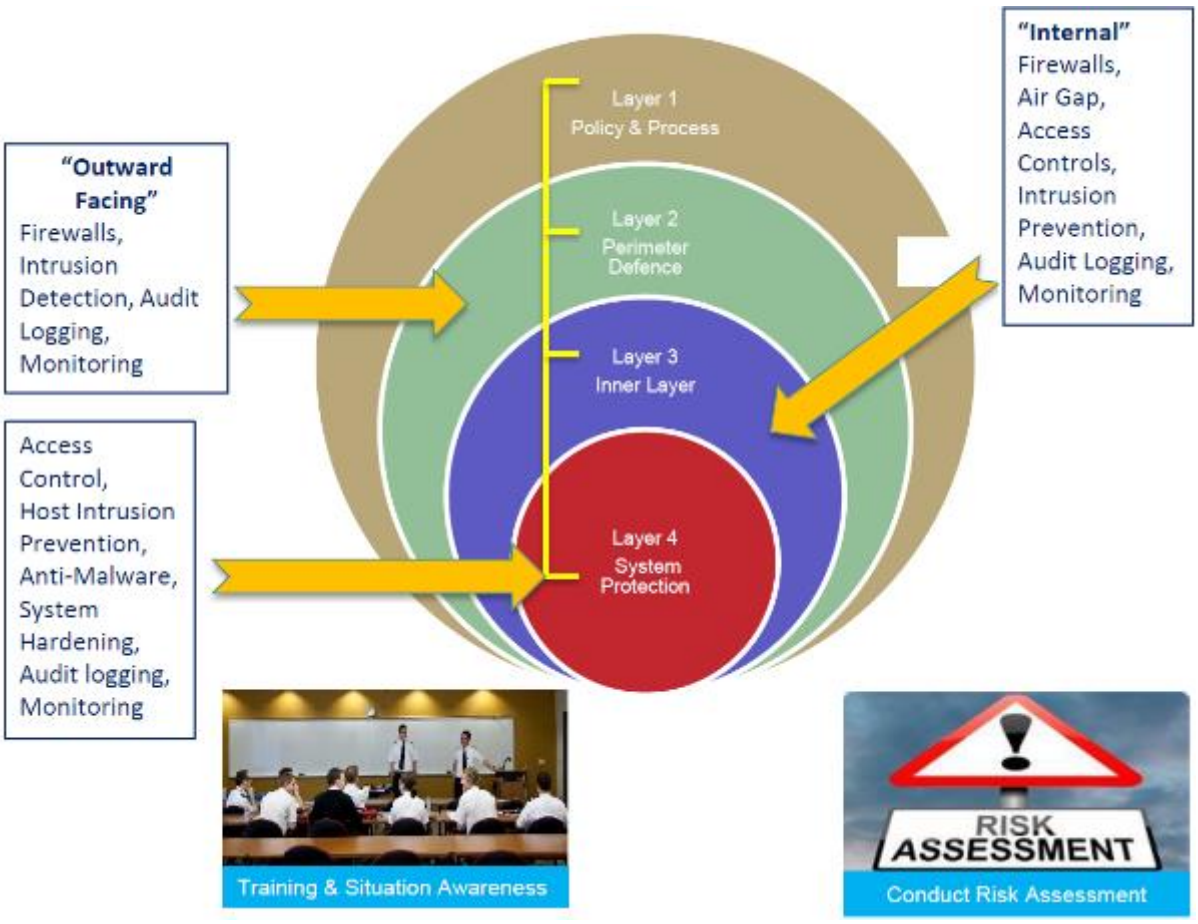


Figure 5.29. Risk Management for cyber security

- The mitigation of weather hazards is one of the safety aspects of air traffic management (Key Topic T5.1).
- A major challenge is the integration of drones in controlled air space (Key Topic T5.2).
- On the ground side airports need to implement comprehensive and unobstructed security measures (Key Topic T5.3).

The provision of high-bandwidth data resilient to cyber-attacks for the aviation sector (Key Topic T5.4) is one aspect of the wider issue of cyber-protection (Key Topic 5.5) for which specific technologies are being developed (Key Topic 5.6).

KEY TOPIC T5.1 – EVALUATION AND MITIGATION OF WEATHER AND OTHER HAZARDS

Goal 15 was defined in Flightpath 2050 as "Weather and other hazards from environment are precisely evaluated and risks properly mitigated".

Comparing the scope in both Flightpath 2050 and SRIA it can be stated that both proposals are coherent between themselves. The objective of ensuring high levels of operational safety make that the

knowledge of most of weather phenomena, other hazards and their possible effects can outcome as a great value in the pursuing of safety through mitigating their related risks.

Moreover, it is necessary to take into account the climate change and the possible effects that could become a reality in the future, either short or long term. In this matter, research and development become essential in order to understand possible new hazards and to set mitigating measures that should be implemented to reduce their associated risks.

Benchmarks

It is a statement that aviation could not exist without the air. This is owing to lift principles being based on the variation of airspeed between intrados and extrados of the wings which generates a variation of pressure that translates into the coming up of an upward force called lift.

This variation of airspeed is extremely important for the aircraft performance thereby airplanes usually take off and land upwind in order to increase this variation of speed between air and aircraft, obtaining a larger lift.

However, usually, wind and other meteorological effects become hazardous for the aircraft operation producing different setbacks such as delays or even incidents and accidents. The following weather hazards should be considered in the air traffic operation [9]:

- **Icing:** one of simplest assumptions made about clouds is that cloud droplets are in a liquid form at temperatures warmer than 0°C and that they freeze into ice crystals within a few degrees below zero. In reality, however, 0°C marks the temperature below which water droplets become 'supercooled' and are capable of freezing. While some of the droplets actually do freeze spontaneously just below 0°C, others persist in the liquid state at much lower temperatures. Aircraft icing occurs when supercooled water droplets strike an aircraft whose temperature is colder than 0°C. The effects icing can have on an aircraft can be quite serious (Figure 5.30) and include:
    - Disruption of the smooth laminar flow over the wings causing a decrease in lift and an increase in the stall speed. This last effect is particularly dangerous. An "iced" aircraft is effectively an "experimental" aircraft with unknown stall speed.
    - Increase in weight and drag thus increasing fuel consumption
    - Partial or complete blockage of pitot heads and static ports giving erroneous instrument readings.
    - Restriction of visibility as the windshield glazes over.

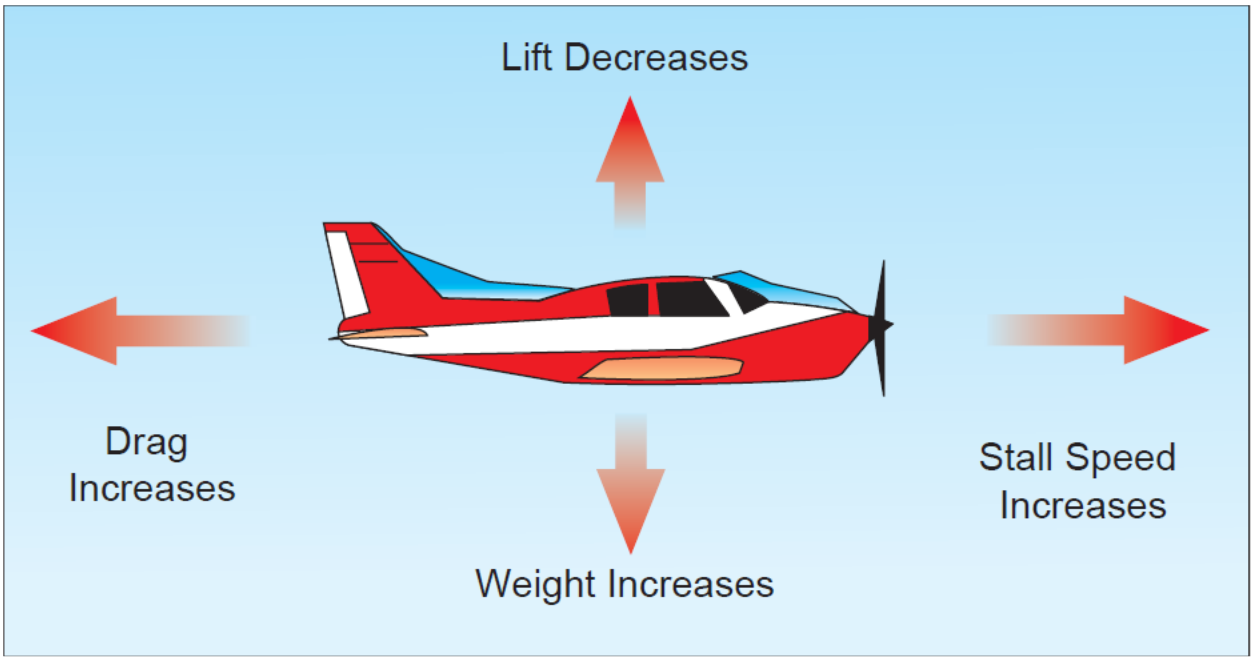


Figure 5.30 - Effects of icing on an aircraft [9]

- **Visibility:** reduced visibility is the meteorological component which impacts flight operations the most. There are several causes of reduced visibility:
    - **Lithometers**: lithometers are dry particles suspended in the atmosphere and include haze, smoke, sand and dust. Of these, smoke and haze cause the most problems. The most common sources of smoke are forest fires. Smoke from distant sources will resemble haze but, near a fire, smoke can reduce the visibility significantly.
    - **Precipitation**: rain can reduce visibility; however, the restriction is seldom less than one mile other than in the heaviest showers beneath cumulonimbus clouds. Drizzle, because of the greater number of drops in each volume of air, is usually more effective than rain at reducing the visibility, especially when accompanied by fog. Besides, snow affects visibility more than rain or drizzle and can easily reduce it to less than one mile. Blowing snow is a product of strong winds picking up the snow particles and lifting them into the air. Freshly fallen snow is easily disturbed and can be lifted a few hundred feet. Under extreme conditions, the cockpit visibility will be excellent during a landing approach until the aircraft flares, at which time the horizontal visibility will be reduced abruptly.
    - **Fog**: it is the most common and persistent visibility obstruction encountered by the aviation community. A cloud-based on the ground, fog, can consist of water droplets, supercooled water droplets, ice crystals or a mix of supercooled droplets and ice crystals. There are different types of fog:

- **Radiation fog**: it begins to form over land usually under clear skies and light winds typically after midnight and peaks early in the morning. As the land surface loses heat and radiates it into space, the air above the land is cooled and loses its ability to hold moisture. If an abundance of condensation nuclei is present in the atmosphere, radiation fog may develop before the temperature-dew point spread reaches zero. After sunrise, the fog begins to burn off from the edges over land but any fog that has drifted over water will take longer to burn off.
- **Precipitation or frontal fog**: it forms ahead of warm fronts when precipitation falls through a cooler layer of air near the ground. The precipitation saturates the air at the surface and fog forms. Breaks in the precipitation usually result in the fog becoming thicker.
- **Steam fog**: it forms when very cold arctic air moves over relatively warmer water. In this case, moisture evaporates from the water surface and saturates the air. The extremely cold air cannot hold all the evaporated moisture, so the excess condenses into fog. The result looks like steam or smoke rising from the water and is usually no more than 50 to 100 feet thick. Steam fog, also called arctic sea smoke, can also produce significant icing conditions.
- **Advection fog**: it forms when warm moist air moves across the snow, ice or cold-water surface.
- **Ice fog**: it occurs when water vapour sublimates directly into ice crystals. In conditions of light winds and temperatures colder than -30°C or so, water vapour from manmade sources or cracks in ice-covered rivers can form widespread and persistent ice fog. The fog produced by local heating systems, and even aircraft engines, can reduce the local visibility to near zero, closing an airport for hours or even days.

- **Wind, shear and turbulence:** unravelling the daily variations of the winds, where they blow and how strong they do remain a problem for meteorologists. The problem becomes even more difficult when local effects such as wind flow through coastal inlets or in mountain valleys are added to the issue. The result of these effects can give one airport persistent light winds while another has nightly episodes of strong gusty winds. Besides, one of the most dangerous effects for aviation is wind shear. It is nothing more than a change in wind direction and/or wind speed over the distance between two points. In the aviation world, the major concern is how abruptly the change occurs. If the change is abrupt, there will be a rapid change of airspeed or track and, depending on the aircraft type, it could take a significant time to correct the situation, placing the aircraft in danger, mostly during take-off and landing. Significant shearing can occur when the surface wind blowing along a valley varies significantly from the free-flowing wind above the valley. Changes in direction of 90° and speed changes of 25 knots are reasonably common in

mountainous terrain. This is the case of Bilbao Airport, where a significant number of go-arounds are registered every year. For example, in 2001, an Embraer ERJ-145 EP operated by Portugalia made a first ILS approach on runway 30. When was on final, the pilot decided to go around and follow the missing approach procedure in order to make a second try. During the second approach, the pilot decided to try again the ILS 30 approach having been informed of variable wind of 250/21 with gusts of 25 kt. The aircraft landed passed half of the runway and seconds later made a runway excursion, stopping over the grass 135 meters far away from runway 12 threshold. Fortunately, none of the passengers and flight crew was seriously injured. Related to that, mechanical turbulence is a form of shear-induced when a rough surface disrupts the smooth wind flow depending on the wind speed, roughness of the obstruction and the stability of the air. Besides, turbulence is the direct result of wind shear in such a way that the stronger the shear, the greater the tendency for the laminar flow of the air to break down into eddies resulting in turbulence. However, not all shear zones are turbulent, so the absence of turbulence does not infer that there is no shear.

- **Lee waves:** when air flows across a mountain or hill, it is disturbed the same way as water flowing over a rock. The air initially is displaced upwards across the mountain, dips sharply on the lee side, then rises and falls in a series of waves downstream. These waves are called "mountain waves" or "lee waves" (Figure 5.31) and are most notable for their turbulence.

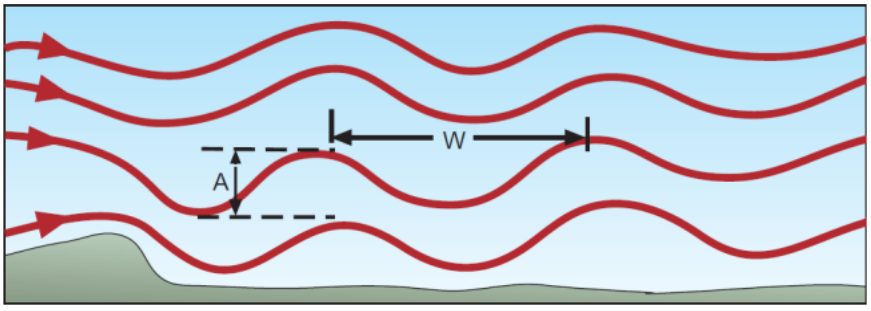


Figure 5.31 - Amplitude (A) and wavelength (W) in lee waves [9]

- **Thunderstorms:** no other weather encountered by a pilot can be as violent or threatening like a thunderstorm. Thunderstorms produce many hazards to the aviation community, and, it's important that pilots understand their nature and how to deal with them. To produce a thunderstorm, there are several drivers which must be in place. These include an unstable air mass, moisture in the low levels, something to trigger them (e.g. daytime heating, upper-level cooling…) and for severe thunderstorms, it is necessary to wind shear. The environment in and around a thunderstorm can be the most hazardous encountered by an aircraft. In addition to the usual risks such as severe turbulence, severe clear icing, large hail, heavy precipitation, low visibility and electrical discharges, other hazards occur in the surrounding environment:

- **The gust front**: it is the leading edge of any downburst and can run many miles ahead of the storm. This may occur under relatively clear skies and, hence, can be particularly nasty for the unwary pilot. Aircraft taking off, landing, or operating at low levels can find themselves in rapidly changing wind fields that quickly threaten the aircraft's ability to remain airborne. In a matter of seconds, the wind direction can change by as much 180°, while at the same time the wind speed can approach 100 knots in the gusts. All of this will likely be accompanied by considerable mechanical turbulence and induced shear on the frontal boundary up to 6,500 feet above the ground.
- **Downburst, macroburst and microburst:** A downburst is a concentrated, severe downdraft which accompanies a descending column of precipitation underneath the cell. When it hits the ground, it induces an outward, horizontal burst of damaging winds. There are two types of downburst, the "macroburst" and the "microburst". A macroburst is a downdraft of air with an outflow diameter of 2.2 nautical miles, or greater, with damaging winds that last from 5 to 20 minutes. Such occurrences are common in the summer but only rarely hit towns or airports. On occasion, embedded within the downburst, is a violent column of descending air known as a "microburst". Microbursts have an outflow diameter of less than 2.2 nautical miles and peak winds lasting from 2 to 5 minutes. Such winds can literally force an aircraft into the ground.

- **Volcanic ash:** a major, but fortunately infrequent threat to aviation is volcanic ash. When a volcano erupts, a large amount of rock is pulverized into dust and blasted upwards. The altitude is determined by the severity of the blast and, at times, the ash plume will extend into the stratosphere. This ash is then spread downwind by the winds aloft in the troposphere and the stratosphere. Of greater concern is the volcanic ash that is ingested by aircraft engines at flight level. Piston-driven engines can fail due to plugged air filters while turbine engines can "flame out" and stop working. That was the case of Eyjafjallajökull in 2010, when it created an ash cloud that led to the closure of most of the European IFR airspace from 15 until 20 April 2010. This meant (Figure 5.32) the disruption of some 100,000 flights and 10 million passenger journeys during these days producing huge economic loses and setbacks.

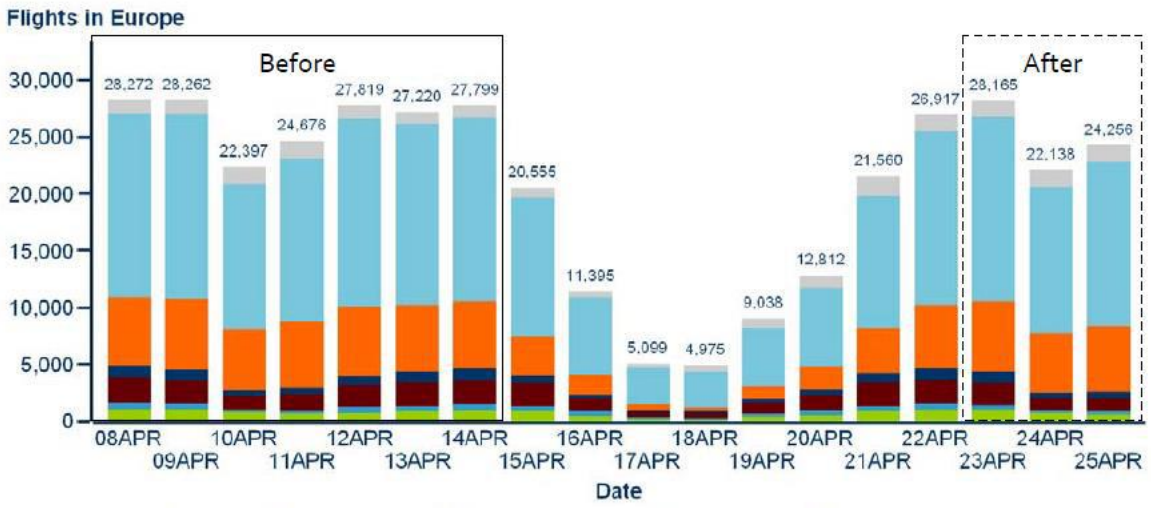


Figure 5.32 - Traffic in Europe before and during the April crisis [10]

This set of hazards for aviation could become into tragedies if they are not found out with enough time to mitigate their impact or to avoid them by setting other routes to be flown. In this manner, phenomena occurred near airports and that affect its operation should be early detected, either through forecasts or actual sighting, in order to implement the appropriate measures, such as advice airplanes to land at another airport.

On the other hand, phenomena occurred along the route that will be followed by the aircraft should be detected before aircraft departs from the airport or far enough from the hazard meanwhile the aircraft is airborne.

In conclusion, these predictive measures lead to the need to develop the current systems and radars used to set both weather and hazards forecasts.

Reference State in 2010

Since the beginning of aviation, weather and its related hazards have been a key factor during air traffic operations, producing an uncountable number of incidents and accidents. These events related to meteorology have also produced uncountable delays in aircraft operations, being one of the main reasons which aircraft cannot take-off or land.

In this context, many studies related to these hazards have been carried out along the last decades. As an example, the National Aviation Safety Data Analysis Centre (NASDAC), which is a part of the Federal Aviation Administration (FAA), issued a Review of Aviation Accidents Involving Weather Turbulence in the United States [11], analysing the accidents occurred during the 1990s. In this document, data was extracted from the National Transportation Safety Board (NTSB) Aviation Accident/Incident Data System. The NTSB is the official U.S. repository of aviation accident data and causal factors.

This study explained that, from 1992 to 2001, there were 4326 weather accidents out of a total of 20332 accidents that occurred in the United States, setting 21,3% of the total. Of these 4326 accidents, 509

were cited as turbulence weather events which nearly 23% of these turbulence-related accidents resulted in fatal injuries to the occupants of the aircraft. The cause or factor most often in the general aviation accidents was downdraft meanwhile in the air carrier accidents was clear air turbulence.

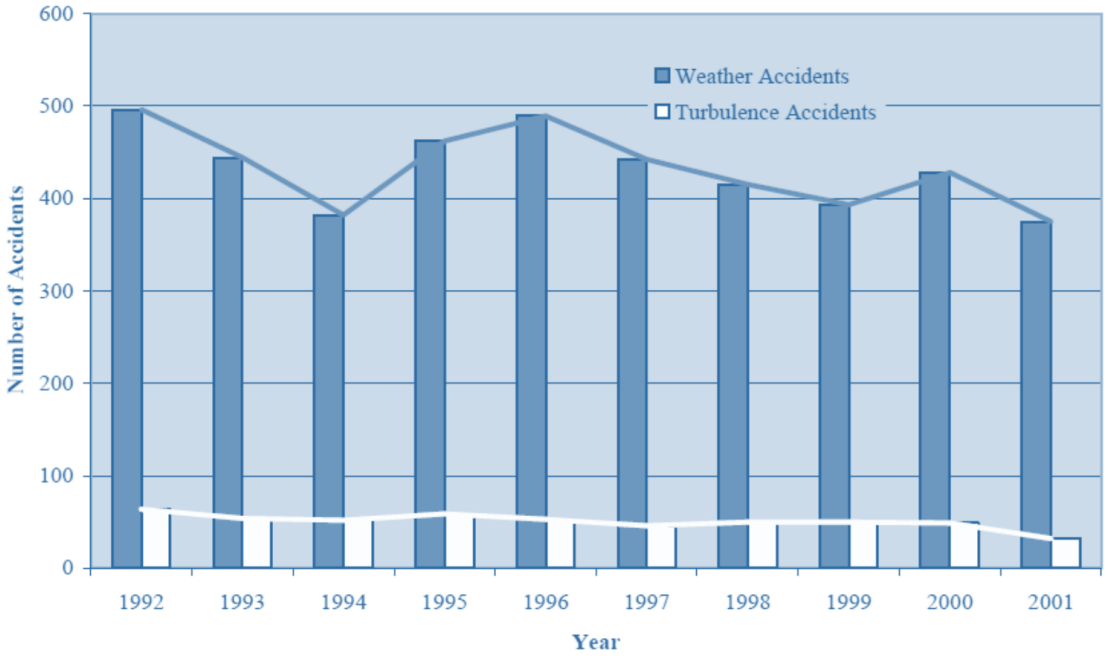


Figure 5.33 - Comparison of weather accidents to weather turbulence accidents 1992-2001 [11]

As can be noticed in Figure 5.33, the number of weather accidents showed a slightly tend to decrease but it also remained approximately steady over the years, which induces to think that no measures or not enough measures were taken in order to make the number of accidents decrease. Additionally, the following Figure 5.34 shows the percentages of each cause or factor related to weather hazards, describing that the most often causes from 1992 to 2001 were wind and visibility.

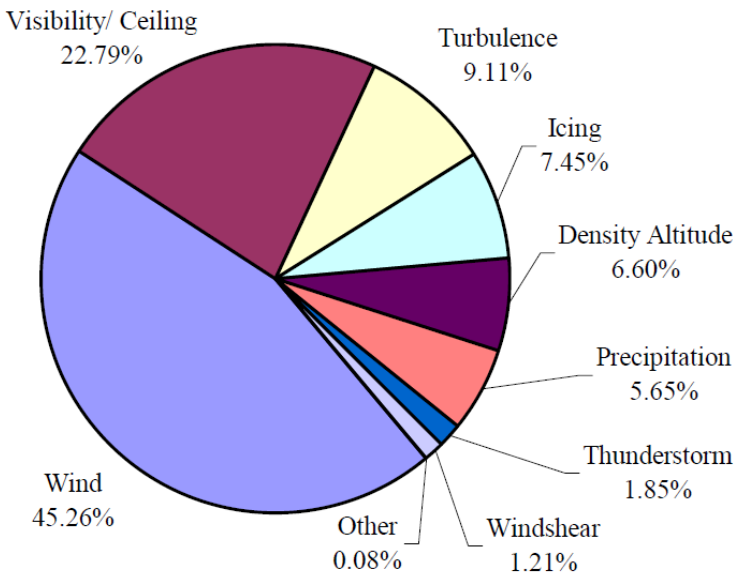


Figure 5.34 - Total weather accidents by phenomenon from 1992 to 2001 [11]

Another study called Weather-related Aviation Accident Study 2003-2007 was issued by the Federal Aviation Administration (FAA) in 2010 [12]. This document reveals that, from 2003 to 2007, there were 8657 aviation accidents which weather was a cause or contributing factor in 1740 accidents setting 20,1% of the total. If this figure is compared with the 21,3% of weather accidents out of the total reported from 1992 to 2001, it can be realized that a slight decrease occurred as it is displayed in the following Figure 5.35:

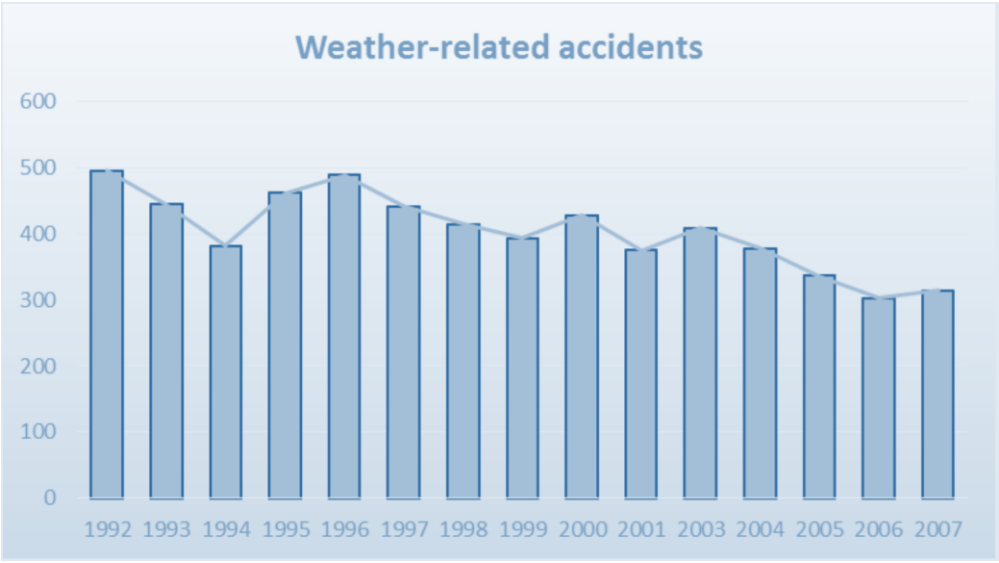


Figure 5.35 - Weather-related accidents from 1992 to 2007 in the US [12]

Concerning the percentages of each cause or factor related to weather hazards, the following Figure 5.36 shows that the most often causes from 2003 to 2007 were also wind and visibility as in the previous period.

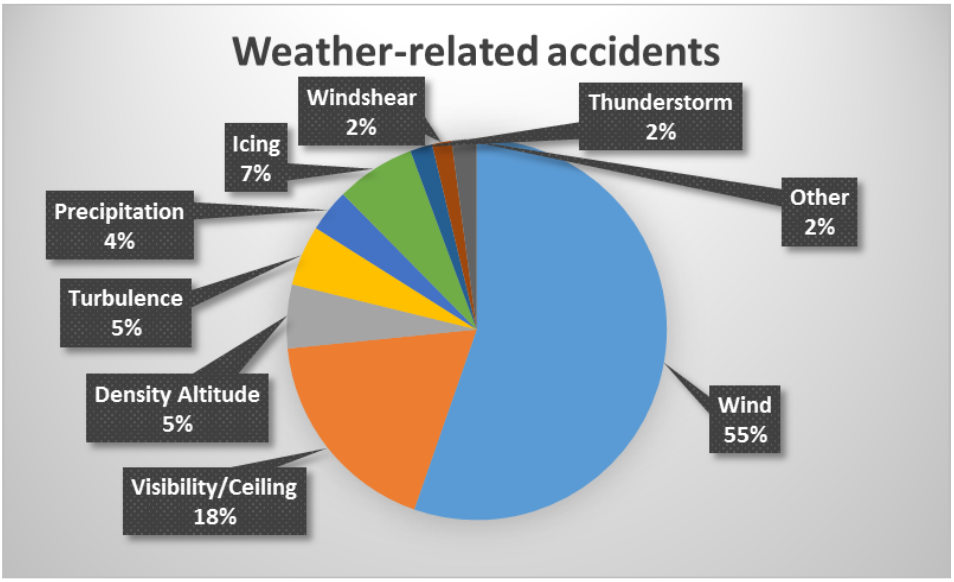


Figure 5.36 - Total weather accidents by phenomenon from 2003 to 2007 [12]

As wind has contributed about 50% of every weather-related accident from 1992 to 2007, it was important to study where on the route these problems had happened to the aircraft. The following Figure 5.37 shows that most of the occurrences had happened during landing at the destination airport (57,7%). Therefore, it is usual to think that different measures to mitigate the impacts of the wind in the operation should be implemented.

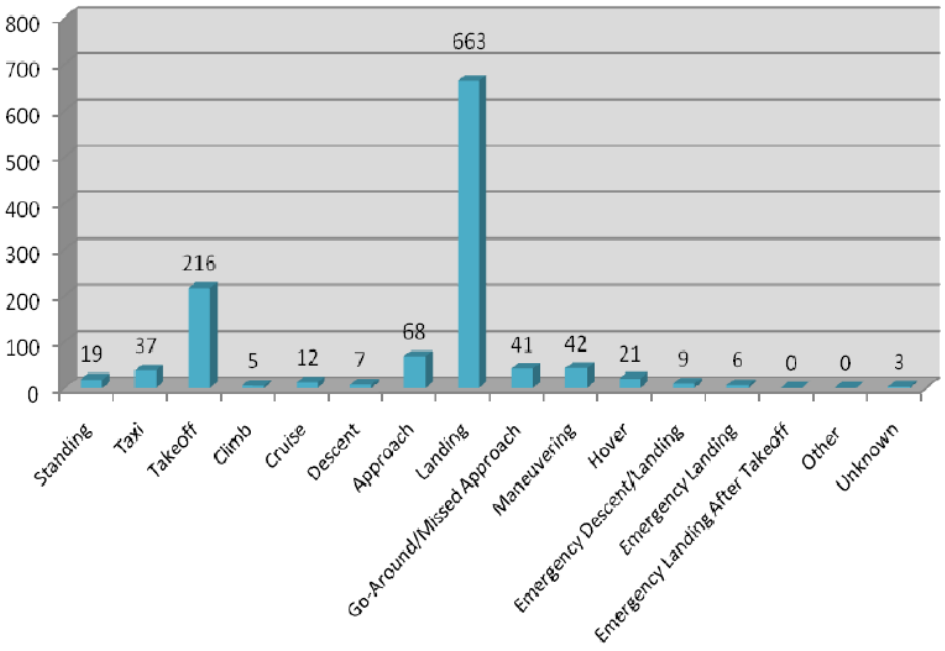


Figure 5.37 - Wind accidents by phase of flight from 2003 to 2007 [12]

Progress Up-to-Now

The decreasing streak in the number of weather-related accidents has continued along the last few years until reaching a historical minimum in 2011. This was explained in the Wake and Weather Turbulence Report issued by the Federal Aviation Administration (FAA) in 2016 [13].

According to the NTSB, 19575 aviation accidents occurred in the United States from 2002 to 2013. During this timeframe, the weather was identified as a cause or contributing factor in 2983 accidents (15.23%). If this number is compared with the previous percentages, it can be noticed that the number of accidents has considerably decreased in the last few years as it is shown in the following Figure 5.38:

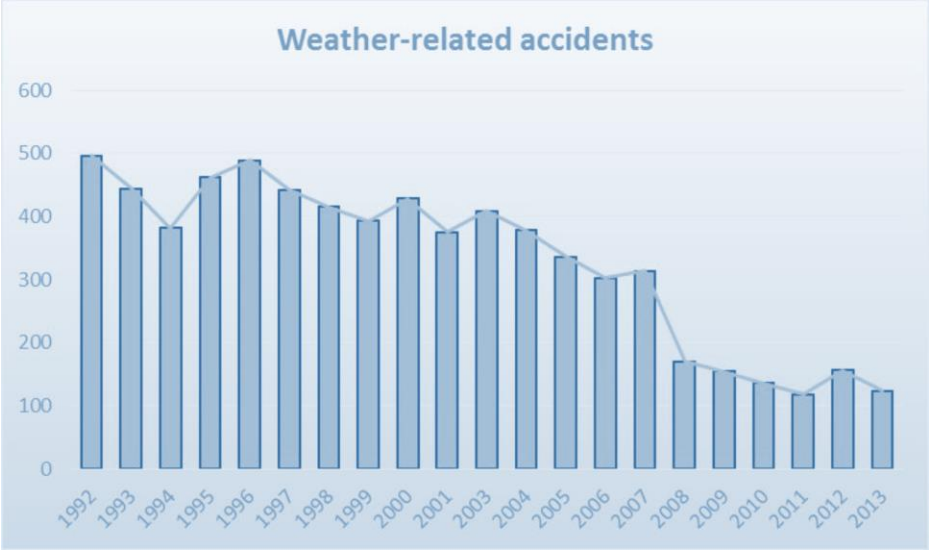
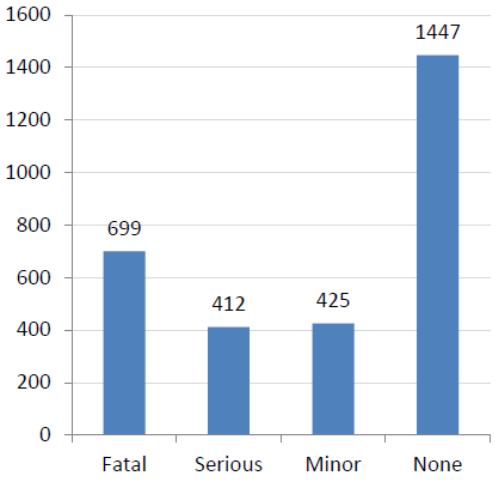


Figure 5.38 - Weather-related accidents in the US from 1992 to 2013 [13]

However, even though the number of accidents due to the weather has steadily decreased until the present time, it is necessary to put into context these accidents in terms of severity. Related to that, covering the period between 2002 and 2013, the following events have been reported:



Severity of Worst Injury Aboard	Number of Weather Events	Percent
Fatal	699	23.4%
Serious	412	13.8%
Minor	425	14.2%
None	1447	48.5%
Total	**2983**	**100.0%**

Figure 5.39 Weather events by worst injury aboard [13]

Assessing the numbers in Figure 5.39, almost half of the events had no consequence for passengers but nevertheless, the high percentage of fatal injury cannot be disregarded.

Therefore, it is necessary to find the right measures to turn these fatal events into no consequence events. Besides, and even more important, it is necessary to focus on continuing to decrease the number of weather-related accidents through new developments either aircraft, ground systems and equipment or detection methods and avoidance strategies. This means that more investments within this field are necessary.

As an example of the type of technology available to detect and predict weather-related hazardous situations, nowadays in the United States, the ground equipment consists of the Next Generation Weather Radar System (NEXRAD) and Terminal Doppler Weather Radar (TDWR) networks [14]. The Next Generation Weather Radar (NEXRAD) system (Figure 5.40) currently comprises 160 sites throughout the United States and selected overseas locations, using the Weather Surveillance Radars–1988 Doppler (WSR-88D).

WSR-88D systems are modified and enhanced during their operational life to meet changing requirements, technology advances, and improved understanding of the application of these systems to real-time weather operations. These new technologies included:

- Mid-Volume Rescan of Low-Level Elevations (MRLE);
- Supplemental Adaptive Intra-Volume Low-Level Scan (SAILS);
- Enhanced Velocity Azimuth Display Wind Profile (EVWP);
- Automated Volume Scan Evaluation and Termination (AVSET);
- Two-Dimensional Velocity Dealiasing Improvement Algorithm.

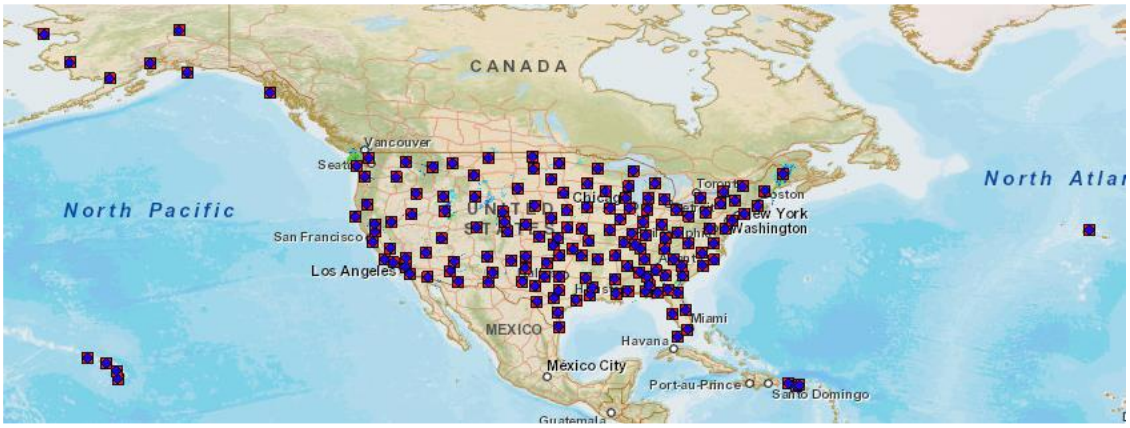


Figure 5.40 - NEXRAD system network [15]

On the other hand, the Terminal Doppler Weather Radar (TDWR) network is a Doppler weather radar system (Figure 5.41) operated by the Federal Aviation Administration (FAA), which is used primarily for the detection of hazardous wind shear conditions, precipitation, and winds aloft on and near major airports situated in climates with great exposure to thunderstorms in the United States [14].

TDWR was developed in the early 1990s to assist air traffic controllers by providing real-time wind shear detection and high-resolution precipitation data and, as of 2014, there were 45 operational TDWR radar systems in major metropolitan locations across the United States and Puerto Rico.

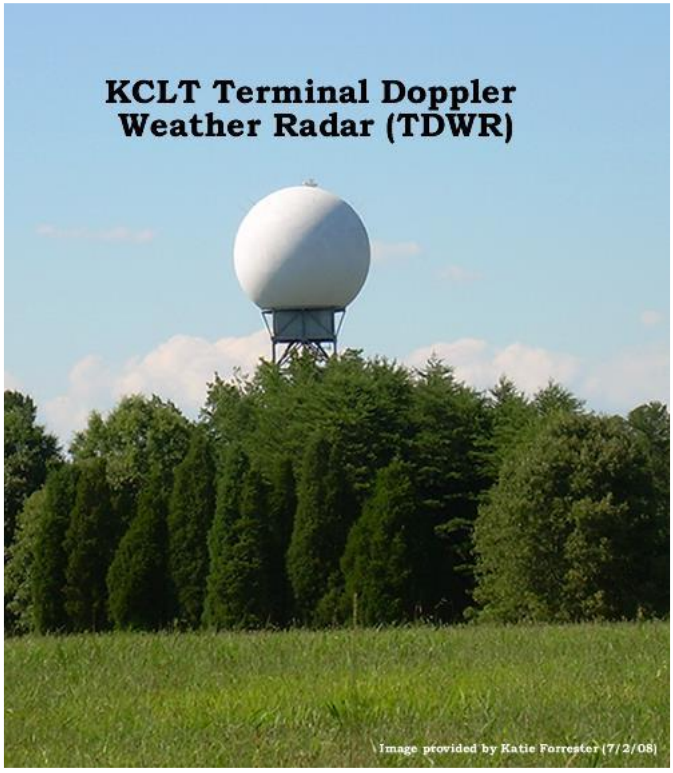


Figure 5.41 Terminal Doppler Weather Radar at Charlotte Airport [14]

Comparing the TDWR to the WSR-88D, the range resolution of the TDWR is finer than what is available in the Weather Surveillance Radar, 1988 Doppler (WSR-88D), or any other FAA radar that has weather channel capability. The TDWR utilizes a range gate resolution of 150 m for Doppler data. It has a resolution of 150 m for reflectivity data within 135 km and 300 m from beyond 135 km to 460 km. By contrast, the WSR-88D employed by the National Weather Service, FAA, and Department of Defence has a maximum range gate resolution of 250 m for Doppler and 1 km for surveillance data.

The angular (azimuth) resolution of the TDWR is nearly twice what is available in the WSR-88D. Each radial in the TDWR has a beamwidth of 0.55 degrees whilst the average beam width for the WSR-88D is 0.95 degrees.

Summarizing, the Terminal Doppler Weather Radar (TDWR) is a high quality, dedicated meteorological surveillance radar usually deployed near the larger airports and it is a great supporting feature to the WSR-88D Radar.

Besides, regarding the airborne operation, deteriorating weather conditions are frequently the cause of changes in flight objectives, and the pilot needs to know quickly where the weather is better and what to do to get there. Related to that, it is necessary an Aviation Weather Information (AWIN) system (Figure 5.42) which consists of, a means for distributing the weather products to the users, and a means to present the information to the users.

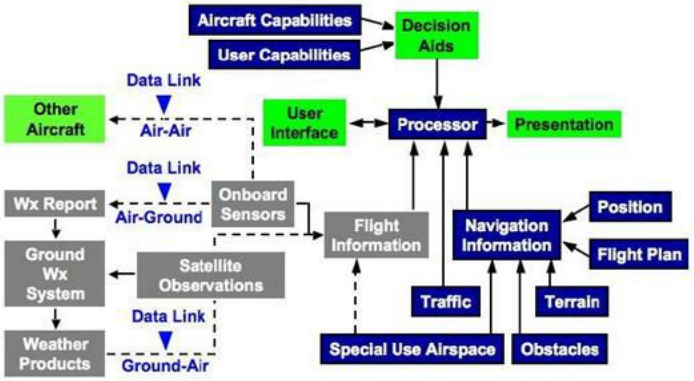


Figure 5.42 - Block diagram of an AWIN system [16]

However, pilots need more than just weather information for in-flight decision making. This includes aircraft capabilities, pilot capabilities, and information on flight-path-relevant terrain, obstacles, air space restrictions, and traffic. For example, light wind shear or other weather disturbance reported by an aircraft on approach can be used to alert the following aircraft and divert them to another airport before the wind shear becomes more hazardous. Data links are needed to exchange information between airplanes and ground stations and, in the same manner, aircraft-to-aircraft links may be needed for timely exchange of in situ weather reports. Information from on-board sensors may be passed to ground-based weather systems for incorporation in updated forecasts and reports that can be subsequently transmitted to aircraft in flight. Data-link weather information systems are intended to provide information for long-term strategic planning and to augment onboard sensors (Figure 5.43) such as weather radar and lightning detectors.

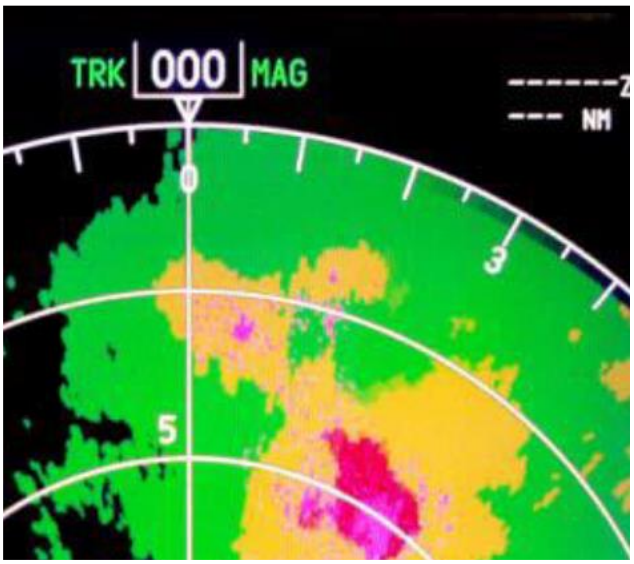


Figure 5.43 - Cockpit radar display of turbulence [16]

In conclusion, further efforts in this field should be done, such as developing the current systems aboard and improving the communications aircraft-ground and aircraft-aircraft via data link.

Predictions Up-to-2025

By far, the largest cause of air traffic delay in the US airspace is the weather. According to the FAA (Figure 5.44) data, the weather caused 69% of system impacting delays (> 15 minutes) over the six years from 2008 to 2013.

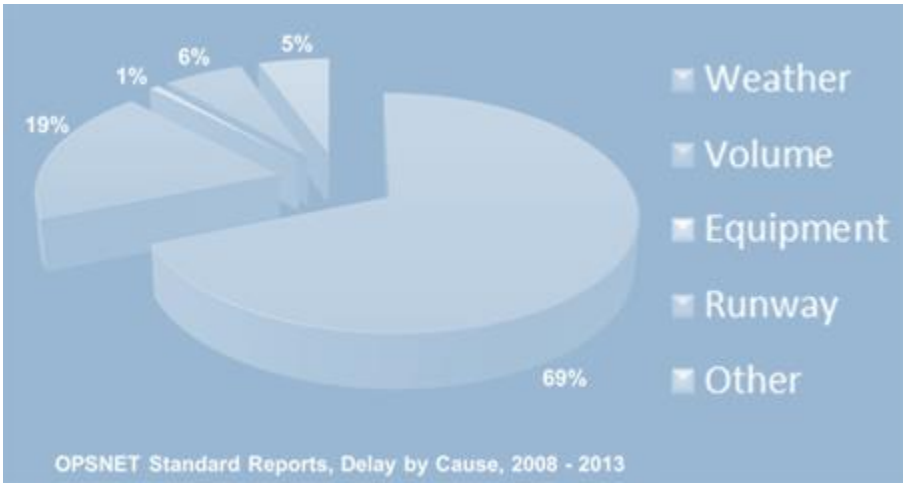


Figure 5.44 - Causes of air traffic delay in the National Airspace System (US)

While the weather is the largest cause of delay (i.e., too much demand for the impacted resources), volume alone (too much demand, even with unconstrained resource capacity) also accounts for 19% of delay. Equipment failure (1%) and runway unavailability (6%) account for smaller portions of the delay, and the final category "Other" accounts for the remaining 5%. These delay statistics include Air Carrier, Air Taxi, General Aviation, and Military classes of aircraft.

The portion of delay due to weather represented nearly 10 million minutes of delay in 2013. Delays translate into real costs for the operators and passengers. Currently, the cost to the air carrier operators for an hour of delay ranges from about $1,400 to $4,500, depending on the class of aircraft, and whether the delay is taken on the ground or in the air. If the value of passenger time is included, the cost goes up an additional $35 per hour (personal travel) or $63 per hour (business travel) for every person on board[CITATION Fed \l 1034]. The Federal Aviation Administration (FAA) has determined two-thirds of this is preventable with better weather information.

As an example, if an en route flight encounter a thunderstorm, aircraft can safely fly over thunderstorms only if their flight altitude is well above the turbulent cloud tops. The most intense and turbulent storms are often the tallest storms, so en route flights always seek to go around them. If a busy jet route becomes blocked by intense thunderstorms, traffic will reroute into the neighbouring airspace, which can become overcrowded if the flow is not managed.

In the United States, in the case of a large-scale weather impact, a Severe Weather Avoidance Plan (SWAP) may be put in place to completely relocate demand to another part of the country. The Planning team's strategic placement of Airspace Flow Programs (AFPs) with reduced hourly flow rates allows airlines to prioritize and plan which of their scheduled flights they will route through the restricted airspace. Ground Delay Programs (GDPs) are also used to temporarily hold aircraft at their departure airports to reduce the number of flights coming into an impacted area.

As an example, on September 11, 2013, an approaching cold front caused a broad region of rapid storm development in the New York Centre airspace. An Airspace Flow Program was set about one hour before the weather impact quickly increased, as a way of reducing flow, but west coast traffic bound for New York was already en route. Very few flights could get through the weather-impacted airspace, and many of them were routed northward to avoid the weather. However, the weather continued to progress northward, making for increasingly long reroutes. Even though the New York airports remained clear of weather, the flights bound for New York couldn't get there on time.

As result, there were 69 diversions (meaning aircraft had to land at alternate airports), and 72 taxi-backs (meaning the aircraft pushed back from the gate, ready to take off, but there was no available airspace and they had to return). In addition, there were 55 airborne holding events, and almost 600 departure and arrival cancellations.

In addition to the issues that weather can trigger, stakeholders including airlines, aircraft manufacturers and organizations are concerned that anticipated increases in air traffic over the next 5-15 years will result in crippling convective weather season delays. Therefore, optimizing air traffic management (ATM) to minimize delay in the complicated network environment of airspace requires integrated Weather-ATM decision support tools that explicitly consider airspace structure, network impacts, weather forecast uncertainty, and pilot preferences for weather avoidance.

For example, regarding the pilot decision making on the weather avoidance, a critical first step in the translation of weather forecast into air traffic impacts is a validated model for airspace that pilots will seek to avoid. In research funded by NASA Ames Research Centre, Lincoln Laboratory developed an en route Convective Weather Avoidance Model (CWAM1) that outputs three-dimensional weather avoidance fields. The probabilistic Weather Avoidance Fields (Figure 5.45) identify regions of airspace that pilots are likely to avoid due to the presence of convective weather[CITATION Mas \l 1034].

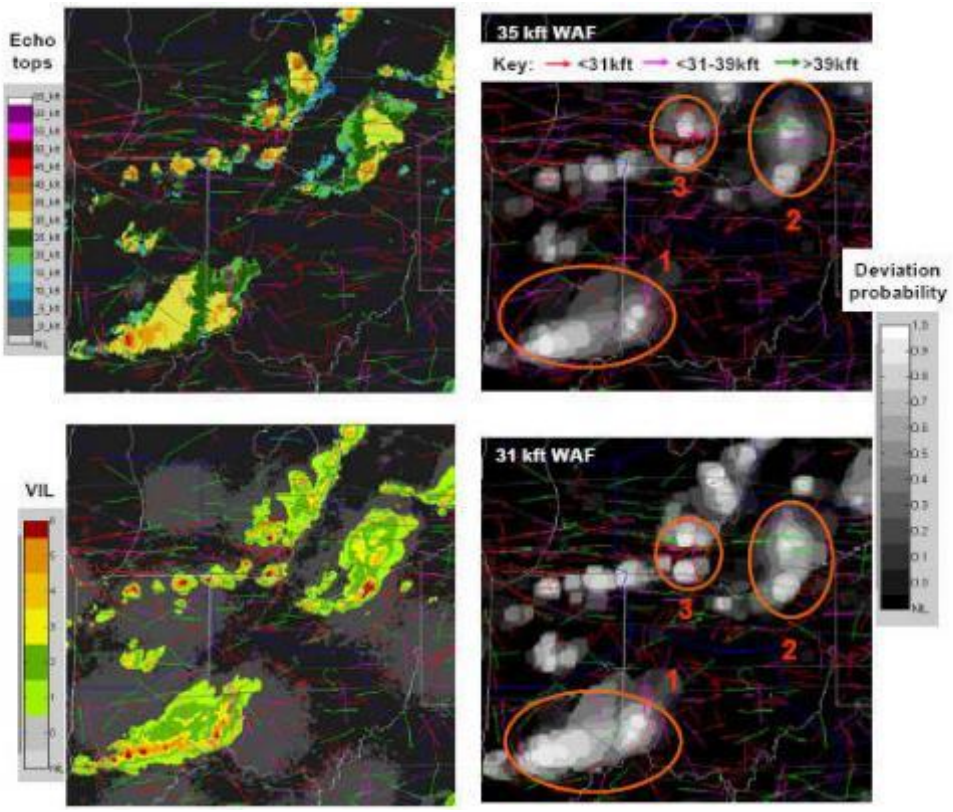


Figure 5.45 - Weather Avoidance Fields example [CITATION Mas \l 1034]

The model used Corridor Integrated Weather System (CIWS) Vertically Integrated Liquid (VIL) and echo top fields and National Lightning Detection Network (NLDN) data to predict aircraft deviations and penetrations. The statistical results showed that the difference between flight altitude and the radar storm top was the most important factor in explaining pilot deviations. The second most important factor was the precipitation intensity.

A second study (CWAM2) extended the analysis to additional Centres and included several additional deviation predictors. The additional predictors captured information about storm growth and decay, vertical structure and weather type (convective or non-convective). Even with all the additional information, the difference between flight altitude and radar storm top was again the top predictor of pilot deviation to avoid convective weather [CITATION Mas \l 1034].

Most deviation prediction errors occurred for flights that encountered echo tops near the flight altitude, for which pilots can legitimately make different choices. The following Figure 5.46, illustrates two flights on the same route at roughly the same flight altitude, 10 minutes apart. The first pilot deviates widely to avoid the weather, while the second fly extremely close to the high storm tops. The model correctly predicted the second pilot's behaviour, but not the first.

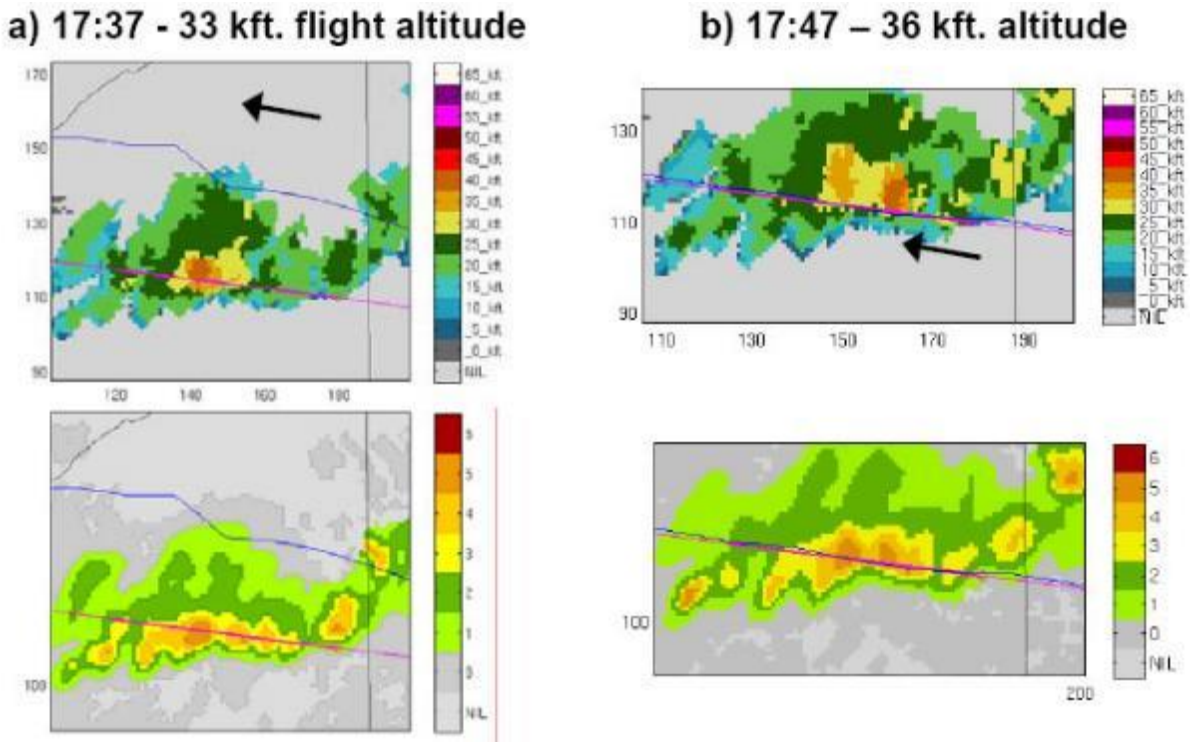


Figure 5.46 - Deviation prediction example [CITATION Mas \l 1034]

A third CWAM study (CWAM3) is currently being planned. It will be the first to include operational information, such as time of day (daylight, twilight, and night), aircraft type, airline, airspace congestion, etc., as potential predictors of deviation. Lincoln Laboratory is also investigating the visual cues available in the cockpit to gain a better understanding of which aspect of the weather the pilot considers hazardous[CITATION Mas \l 1034].

Summarizing, during the following years research programs will focus on facilitating the decision-making to the professionals involved in the aircraft operation, such as pilots and air traffic controllers, during the en route phase through better forecasts and real-time deployments of the weather situation in the cockpit.

Evolutionary Progress Up-to-2050

During the flight in en route area, aviation is only disrupted marginally by weather phenomena. But during start and landing, it is very sensitive to those effects. Especially fog, snow and wind can disrupt the operations with even a low intensity. This weather impact will increase in future. Past has shown that particular airports, operating at their capacity limit, are affected by bad weather phenomena. Due to the expected increase in aviation, more and more airports will operate in this area close to their overall capacity, and therefore, they will be more affected by the weather. But especially high-density airports transfer delay to the next day as they do not have the capacity to reduce accumulated aircraft queues during regular operations.

Looking at the expected development for aviation, it can be stated that the influence of weather on aviation will increase in future. The reason here is not primarily climate change, but the prognosis for growth in worldwide air traffic.

The effects of climate change for air traffic can be hardly foreseen, as there are many overlapping effects, which can offset or accumulate. Below you can find some examples[CITATION Fra12 \l 1034]:

- A reduced number of fog situations leads to avoidance of higher separation and finally in higher yearly capacity;
- An increased number of thunderstorms result in a more temporary closure of airspace or airport and so in a lower yearly capacity;
- Increasing temperatures reduce the necessity for the de-icing procedure, resulting in shorter turn-around times and hence in an increase of capacity;
- More sandstorms in the Mediterranean region reduce the visibility, which leads to an increase in separation and so in a loss of capacity.

But due to the expected growth in aviation, an increasing number of airports will operate near their capacity limit and hence will be more sensitive to disturbances by weather phenomena. An increase of the capacity by airport extension programs is especially in Central Europe very difficult due to environmental restrictions and the noise awareness within the vicinity of an airport. Therefore, technical and procedural developments are needed to face this challenge and maintain the high standards of safety and quality in air travel.

For example, NextGen weather vision is focused on providing multiple users common weather picture, consistent and reliable weather information and improved weather information and data storage approach containing observation and forecast data enabling NextGen dissemination capabilities (called the 4-D Data Cube).

A Net-centric capability is envisioned for NextGen, and it is referred to as “Network Enabled”: an information network that makes information available, securable, and usable in real-time, information may be pushed to known users and is available to be pulled by others and weather information sharing is two-way. This contains a “virtual” repository with no single physical database or computer: conceptually unified source distributed among multiple physical locations and suppliers, of which the National Oceanic and Atmospheric Administration (NOAA) is the leading data supplier.

Comparing the situation nowadays to the new requirements by NextGen, the differences are the following (Table 5.2):

Today	New requirements by NextGen
Not integrated into aviation decision support systems (DSS)	Totally integrated into decision support systems (DSS)
Today's requirements can lead to inconsistent weather information	Updated requirements/Nationally consistent
Low temporal resolution (for aviation decision making purposes)	High temporal resolution
Disseminated in minutes	Disseminated in seconds
Updated by schedule	Updated by events
Fixed product formats (graphic or text)	Flexible formats

Table 5.2 - New requirements by NextGen[CITATION Eur14 \l 1034]

Following this guideline, FAA recommendations for weather information display in the cockpit are:

- Provide an integrated display of weather data.
- Incorporate decision-making aids referenced to a specific pilot and flight profile.
- Emphasize hazardous weather directly relevant to flight profile (per known pilot prioritizations).
- Indicate reliability of forecast information (i.e. probabilities associated with specific forecasts).
- Provide access to lower levels of detailed data without full-time display of same.

If we talk about Europe position, NextGen and SESAR project were compared in 2008 to identify similarities and differences of both projects with regards to weather. The following excerpt seems to be correct at present as well.

The primary difference between SESAR and NextGen concerning weather is how information is acquired. In NextGen, a centralized government-run weather service is anticipated, while in SESAR the information will be derived from a variety of traditional sources. A more net-centric solution would be to allow each carrier to be able to choose whatever information is available from certified sources to provide maximum safety.

In the case of SESAR, the information will be derived from a variety of (traditional) sources including an increased reliance on remote sensing systems, aircraft derived data and satellite-based weather information. With enhanced digital communications services, the provision of Meteorology (MET) information will encompass ground-based and potentially airborne automation systems and human users.

On the other hand, NextGen foresees weather as moving from a stand-alone display to an integrated decision-making element. A primary objective of NextGen is the establishment of a single authoritative weather service available to all systems communicating within the network. While little is said about how this service will be run, great detail is provided on what type of service will be available. The service will draw data from traditional weather reporting systems, aircraft and other sensors in route including UAVs specifically deployed for weather collection, commercial weather services which will augment the system at the basic provision rate and presumably at premium rates as a choice of individual carriers and aircraft and potentially airborne automation systems and human users as well as from weather national service.

Furthermore, it is also important to consider pilots' requirements about weather information[CITATION Eur14 \l 1034]:

- Access to information has to be continuous and it has to be available on the ground and in the air, from early pre-flight planning maybe days in advance until the flight is completed.
- Information content has to be displayed in easy to grasp, i.e. graphical form.
- Weather graphics shall make use of colour to highlight important phenomena.
- Information transfer technologies shall have a role to play, like the internet, which should deliver access to a pan-European portal of weather information. This shall be extended to include information for all areas of the world as far as it can be provided.
- Real-time advanced radar and satellite pictures with flight path added, continuously updated forecasts that have 3 hours or less between forecast times.
- Pilot-selectable, specialized weather information for special situations, i.e. tropical systems, high winds, volcanic eruptions, winter weather or fog.
- Playback capability for all information.
- Wireless devices shall support laptops, tablets, eFBs that pilots might use.

Thinking about how climate change will affect until 2050, it is inevitable to talk about the main uncertainties in climate projections: internal variability of the climate system that exists even in the absence of any external forcing; uncertainty in radiative forcing due to future emissions of greenhouse gases and aerosols; and model uncertainty.

Based on the EWENT project results using the six Regional Climate Model (RCM) simulations, the frequency of snowfall events (Figure 5.47) is projected to decrease 1-5 days in southern Europe, with changes in the frequency of snow days increasing progressively northward, to 10-20 days in Scandinavia compared to 1971-2000. The sign of change is consistent among all six RCMs, except in the Mediterranean and the western part of the continent. Contrary to the general decrease in snow days, the probability of extreme snowfall (> 10 cm) increases over large areas of Scandinavia and north-eastern Russia (1-5 days/year). This increase is partly due to the anticipated increase of total precipitation in the future but also due to warmer temperatures since heavy snowfall tends to occur close to near-zero

degrees Celsius. As shown in the upper limit maps, some models indicate a more robust increase in the frequency of 10 cm and especially 20 cm snowfall/day for several central and eastern European countries. The anticipated decrease in snowfall and frozen precipitation would have a positive impact on road, rail and air transportation reducing the cost of maintenance in many European countries; however in the Nordic countries, where heavy snowfall is already one of the most common disruption factors, it seems to become a more severe phenomenon[CITATION Fra12 \l 1034].

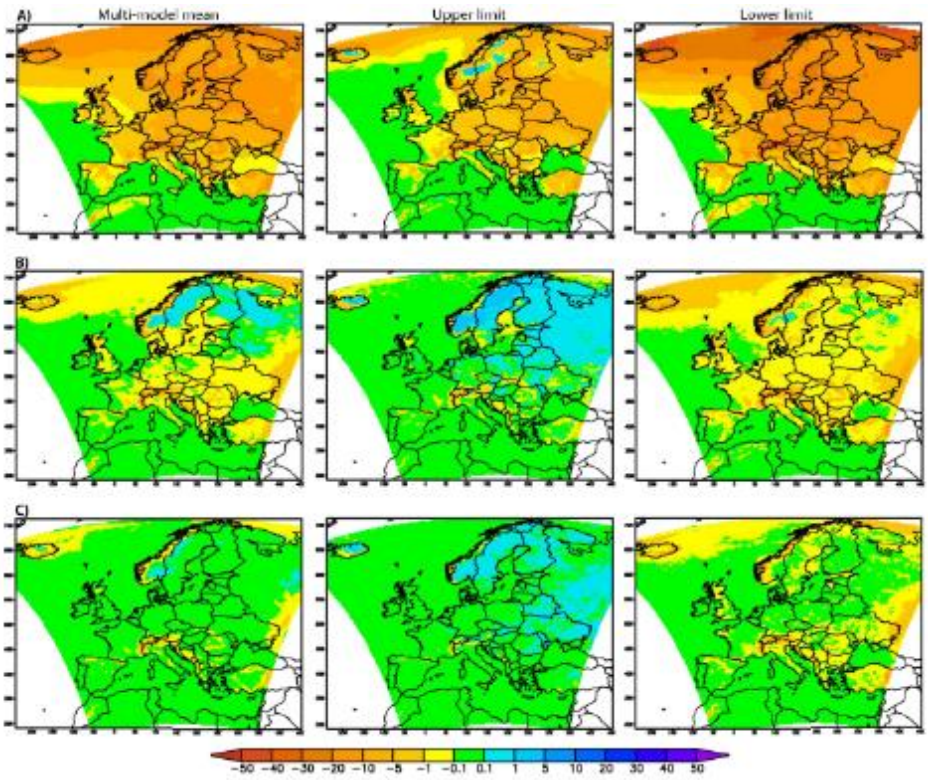


Figure 5.47 - Multi-model mean, upper and lower limit of changes in annual snowfall days from 1971-2000 to 2041-2070 exceeding (A) 1 cm, (B) 10 cm and (C) 20 cm based on six RCM simulations[CITATION Fra12 \l 1034]

Concerning warm days (mean temperature above 25ºC), they will become (Figure 5.48) more prevalent by the 2050s. Scandinavia will experience 5 more warm days/year and Southern Europe 30-40 more days/year. In western and central parts of the continent, the projections suggest warm days will become more frequent by 20-30 days/year. This change implies that mid-latitudinal regions may experience as many days with heatwaves by 2070 as the Mediterranean countries do in the present climate. As for the frequency and spatial variation of days above 43 °C, more countries will be affected than nowadays, with most of south and southeast Europe experiencing extreme heat waves, their number increasing by 5 days/year. Some of the climate models indicate an increase of 20 days/year for the Mediterranean countries [CITATION Fra12 \l 1034].

The projected increase in the duration and intensity of hot days will have a negative impact on transportation and infrastructure during the summer months, especially in those countries which already experience high temperatures.

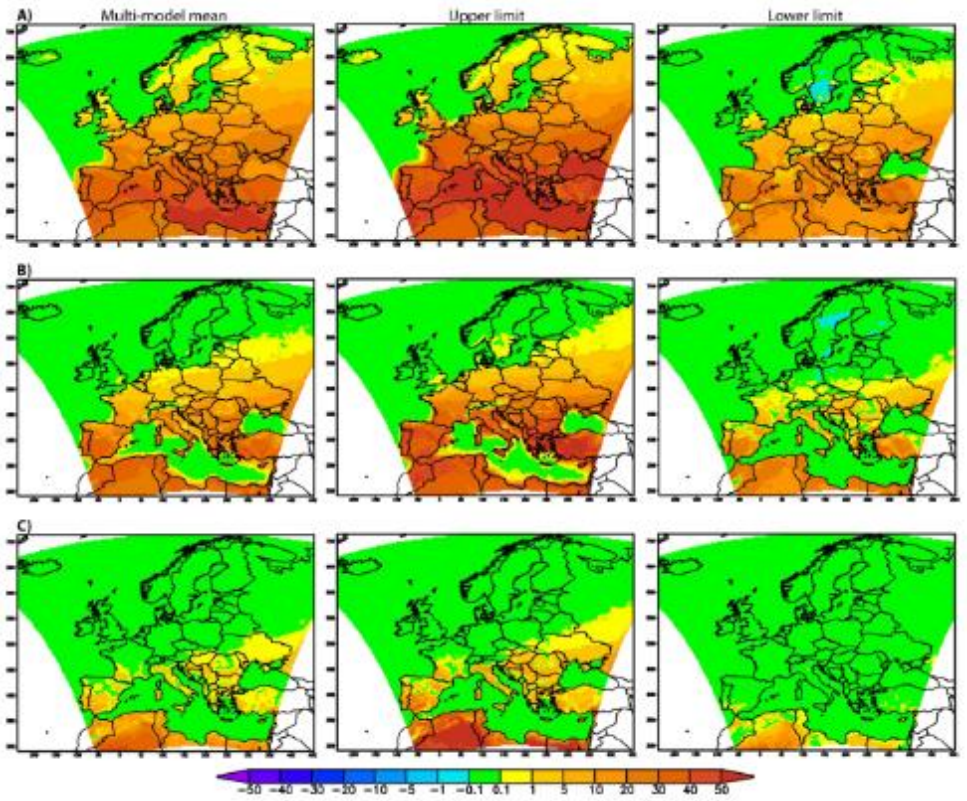


Figure 5.48 - Multi-model mean, upper and lower limit of changes in annual heat-spells days from 1971-2000 to 2041-2070 exceeding (A) 25 °C, (B) 32 °C and (C) 45 °C based on six RCM simulations[CITATION Fra12 \l 1034]

Additionally, the simulated cold extremes (Figure 5.49) decline in occurrence substantially by 2070 over the whole continent, most strongly over Northern Europe. The decrease in the frequency of frost days (0 °C) varies between 20-30 days/year in Northern Europe and decreases gradually towards Southern Europe, with a decrease of 1-5 days/year. Most of the six models agree on the amplitude of change over land. This implies that Finland, Sweden and Norway are likely to experience as many frost days in the 2050s as some mid-latitude countries (such as the Baltic countries, Poland and Ukraine) do in the current climate[CITATION Fra12 \l 1034].

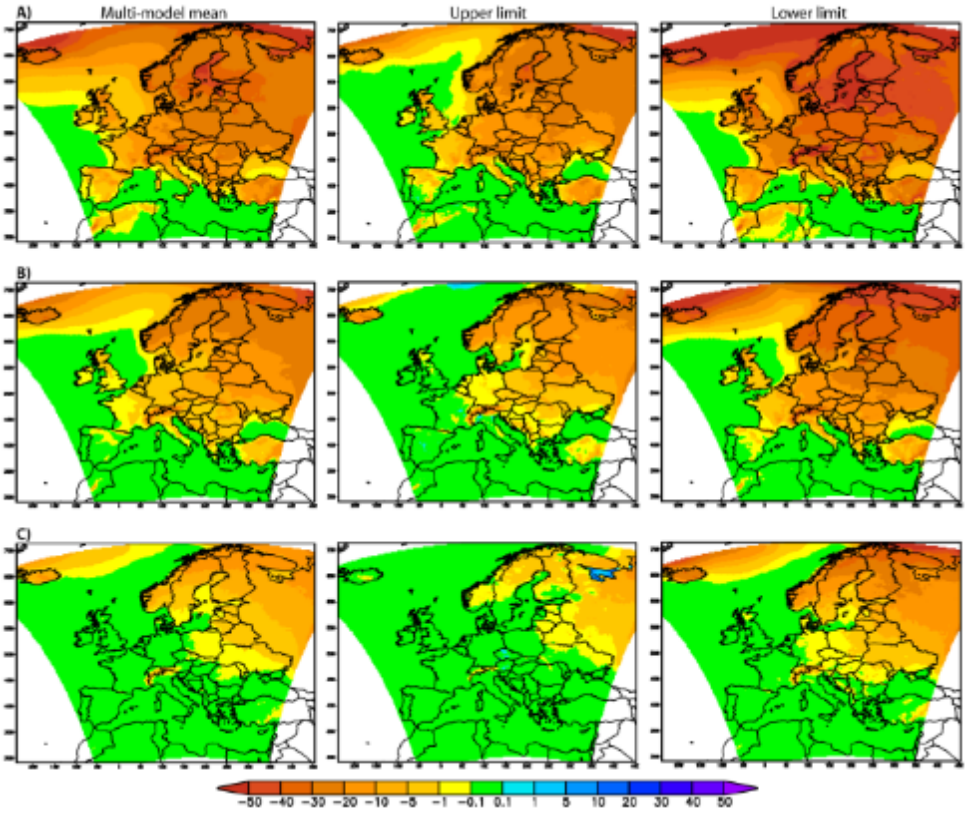


Figure 5.49 - Multi-model mean, upper and lower limit of changes in annual cold-spell days from 1971-2000 to 2041-2070 exceeding (A) 0 °C, (B) -7 °C and (C) -20 °C based on six RCM simulations [CITATION Fra12 \l 1034]

Concerning other meteorological hazards such as precipitation extremes, wind extremes or blizzards, they are more difficult to assess due to the large variation in the results among the models. For example, precipitation extremes are expected to increase by 1-5 days/year over Europe except for the Mediterranean, where no significant change or a sporadic decrease is expected. On the other hand, wind extremes are expected to decrease over the Atlantic and the Mediterranean Sea but a slight decrease or no significant change in either direction is expected over the continent.

In conclusion, future systems related to weather forecasts as radars and other systems related to weather information streaming as data link should be developed considering future meteorological conditions, which it is expected to be quite different than current conditions.

Possible or Predictable Breakthroughs

The following breakthroughs could be expected:

- Development of new technologies concerning radars throughput.
- Improved connectivity air-ground and air-air allowing predictive decision-making.
- More complete and more accurate forecasts due to new technologies.
- Improved meteorological predictive models.

- Integration of outputs from meteorological models and cockpit and ground radars.

Identification of Gaps

Looking at the expected development for aviation, it can be stated that the influence of weather on aviation will increase in the future. The reason here is not primarily climate change, but the prognosis for growth in worldwide air traffic.

The growth of air traffic will lead to the saturation of the entire air traffic network, containing both airports and airspace. Airports will operate near their capacity limit and hence they will be highly sensitive to disturbances caused by weather-related phenomena, just the same case as airspace. If any disturbance occurs, it could drive into the generation of severe delays which would spread throughout the entire air traffic network affecting the different stakeholders. In order to make the air traffic network resilience to disturbances and hence improve its throughput, research must be focused on developing the current atmospheric models, so that it would help to produce more accurate forecasts, both short and long-term.

Moreover, the effects of climate change for air traffic can be hardly foreseen, as there are many overlapping effects, which can offset or accumulate. For example, a reduced number of fog situations would lead to avoidance of higher separation and finally in a higher capacity. On the other hand, an increased number of thunderstorms would result in a more temporary closure of airspace or airport and finally in a lower capacity. In this manner, as it is likely that climate change forecasts are not enough accurate, stakeholders and governments should focus on the new technology that will allow air traffic operators to handle any change relative to today's situation.

Considering the trend of increasing regionalization and globalization in response to user's needs for globally harmonized and seamless services, it is recognized the need for the meteorological community to respond to the associated shift in modes of service delivery. These must include the development of new business models, utilization of the latest information technologies and scientific research, harnessing new and innovative methods of service delivery and being able to leverage a higher level of regional and international cooperation to bridge existing and future gaps.

One of the key gaps that should be considered is the cooperation between stakeholders, which must be improved in order to fulfil the goals set for the future. Currently, several projects related to that are being carried out. It is the case of the Aircraft Met Data Relay (AMDAR) which consists of collecting, processing, formatting and transmitting meteorological data to ground stations via satellite or radio links. This meteorological data is collected using existing aircraft onboard sensors, computers and communications systems.

The World Meteorological Organization (WMO) global AMDAR system (Figure 5.50) now (May 2017) produces over 700,000 high-quality observations per day of air temperature and wind speed and direction, together with the required positional and temporal information and with an increasing number of humidity and turbulence measurements being made. The data collected is used for a range of

meteorological applications, including, public weather forecasting, climate monitoring and prediction, early warning systems for weather hazards and, importantly, weather monitoring and prediction in support of the aviation industry[CITATION Wor1 \l 1034].

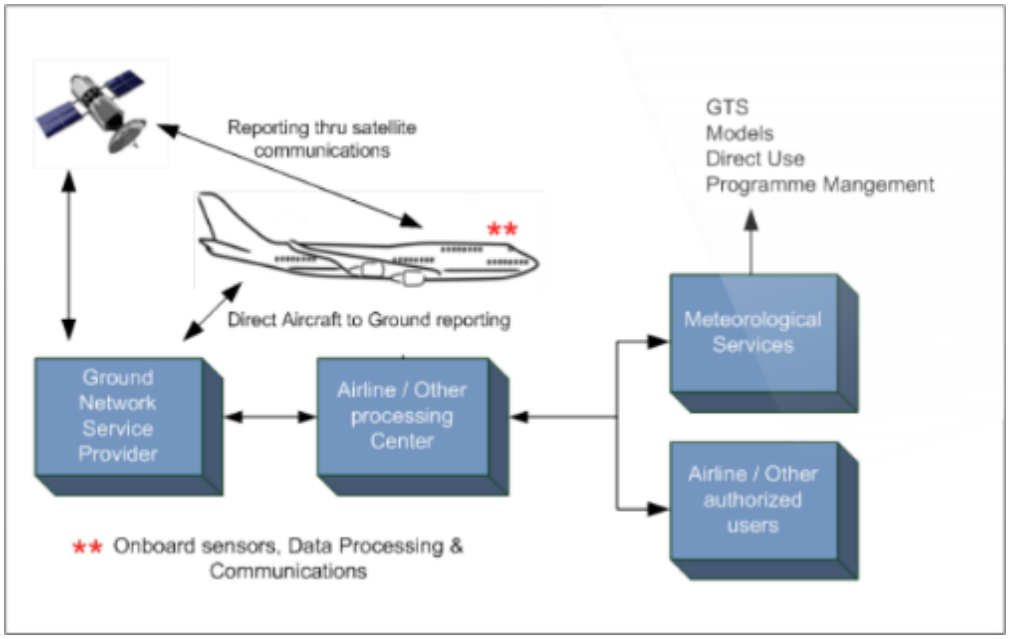


Figure 5.50 - AMDAR overview [CITATION Wor1 \l 1034]

In this context in which a global and interrelated network is the main goal, issues may arise concerning the physical management of the information (including meteorological information) as system-wide information management (SWIM) will underpin the future ATM system. This will require appropriate governance arrangements to be developed, including data management policies for both the providers and consumers of the information within SWIM.

Furthermore, understanding the requirements for the integration of the meteorological information into the ATM decision-making processes in support of trajectory-based operation (TBO) will be crucial. Entering into an increasingly automated decision-making environment will require respective automation of the MET information generation and sharing and will require a close dialogue with users. One of the problems related to a highly-automated, data-rich digital environment that could show up is that National Meteorological Services (NMHSs) may lose contact with the end-users, e.g. pilots, relative to the situation today. Similarly, with quality as a global concern, feedback from the users may be lost. As a consequence, mechanisms to ensure that effective interfaces and interactions between provider and consumer can be sustained will need to be studied [CITATION Wor171 \l 1034].

Therefore, if technical and procedural developments are not carried out properly, it could turn into a difficult situation in order to reach the proposed objectives and also in order to maintain the high standards of safety and quality in air travel.

KEY TOPIC T5.2 - INTEGRATION OF UNMANNED AIRCRAFT IN MANNED AIRSPACE

Goal 16 was defined in Flightpath 2050 as "The European air transport system operates seamlessly through interoperable and networked systems allowing manned and unmanned air vehicles to safely operate in the same airspace".

Comparing both Flightpath 2050 and SRIA goals it can be realized that the goal has been set in the safety framework which makes sense because, although Unmanned Aircraft System (UAS) represent an infinite world with multiple applications still to be explored, they are also coming up strongly as a new risk area. Contextualizing, Unmanned Aircraft System (UAS), of which the Unmanned Aerial Vehicle (UAV) is the airborne component, comprise two fundamental types [17]:

- Remotely-Piloted Aircraft Systems (RPAS), a class of UAS which has a 'pilot' operating the Remotely-Piloted Aircraft (RPA) from a Ground-Control Station (GCS).
- UAS with no remote pilot, or autonomous air vehicles.

These Unmanned Aerial Vehicles constitute a new threat in the European airspace as demonstrated by the occurrence of several incidents involving conventional aircraft and UAVs. As example, in the 2016 Annual Safety Report (Figure 5.51) issued by EUROCONTROL [18], which relies on data received from the Member States, the highest number of reports amounts to over 40 events in 2015; hence, in order to reduce the number of incidents related to RPAS, it is necessary to contribute to the seamless accommodation and integration of RPAS into the European ATM.

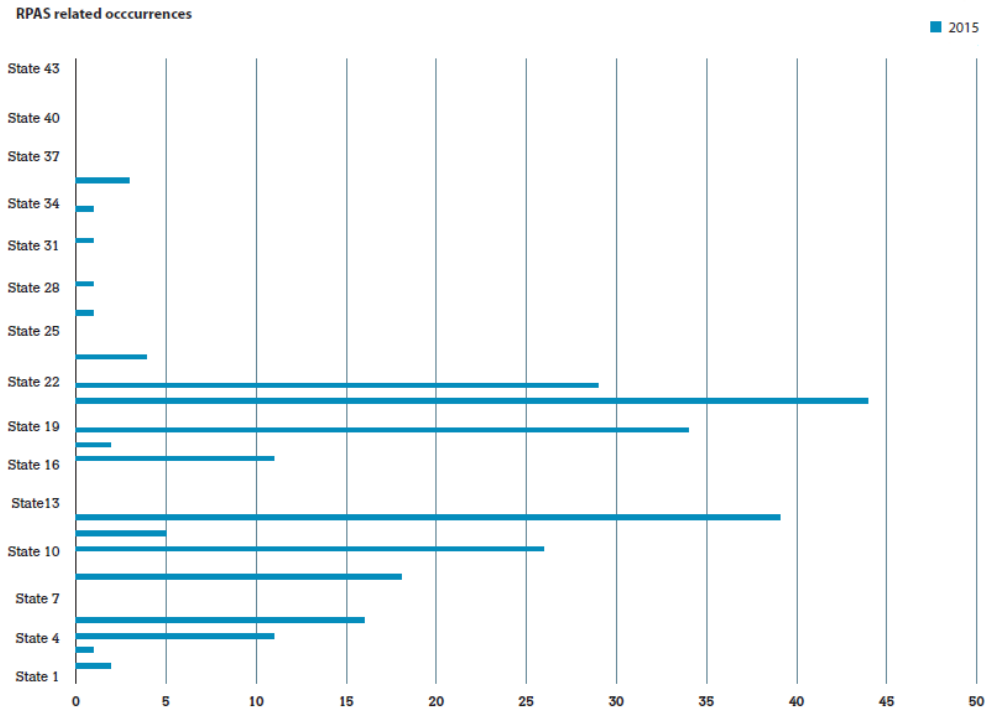


Figure 5.51 - RPAS related occurrences in 2015 [18]

Benchmarks

RPAS have been instrumental in providing new capabilities for European defence and have demonstrated significant growth as a consumer leisure product. At the same time, they are offering public safety and security authorities' new capabilities much in the same way they have for the military and are transforming commercial businesses. A core component to these new capabilities and transformations is the collection of data from strategic vantage points that have been either inaccessible or too expensive to be economically viable today. This core area of data processing is being extended to include the efficient transport of urgently needed goods within a local community or industrial site with longer-term aspirations to transform large commercial vehicles for both cargo transport and also, someday, passenger transport [17].

Related to the stated above, Europe is not alone in this race: United States (US) and China are two key States that are significantly investing into technology and innovative businesses that currently exceed the level of total European investments. In particular, the US is the leader in producing defence drone systems – followed by Israel – and China not only is the leader in producing leisure units that tend to be more and more used for professional purposes but is also becoming the leading exporter of high-end armed military drones that face US export restrictions. Therefore, Europe should focus on developing the use of drones in as many sectors as possible since UAS will create significant benefits that should be pursued in the following years.

In addition, it is expected that commercial and professional users demand drones in both rural and urban settings. Examples of some of the most influential missions, in terms of the potential number of drones and economic impact, include the following [17]:

- Agriculture sector where over 100000 drones are forecasted to enable precision agriculture to help drive increased levels of productivity that are required.
- Energy sector where close to 10000 drones limit the risk of personnel and infrastructure by performing preventative maintenance inspections.
- Public safety and security where a forecasted fleet of approximately 50000 drones would provide authorities like police and fire forces the means to more efficiently and effectively locate endangered citizens and assess hazards as they carry out civil protection and humanitarian missions.
- Delivery purposes where there is potential for a fleet of nearly 100000 drones to provide society with some kind of urgent service capabilities, such as transporting emergency medical supplies, and "premium" deliveries. This is the case of different companies such as Amazon or Google. Related to this, many studies are currently carrying out: as for example, in 2016 Airbus signed a contract with the Civil Aviation Authority of Singapore (CAAS) allowing them to test a UAV parcel delivery service on the campus of the National University of Singapore (NUS) under its project

"Skyways". This project (Figure 5.52) aims to provide efficient delivery of small packages using UAVs.

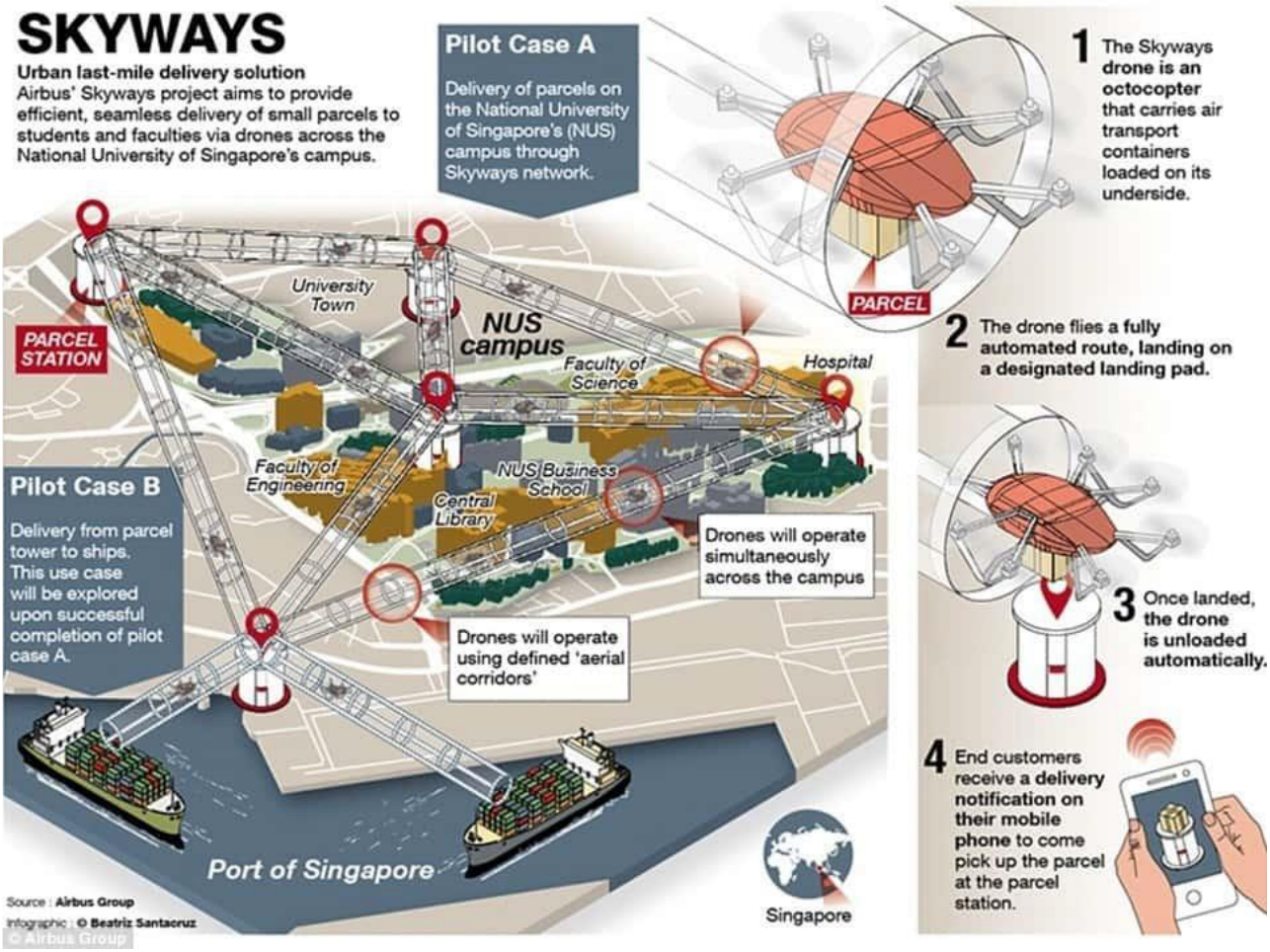


Figure 5.52- "Skyways" project developed by Airbus

In this case, the UAV is a fully autonomous octocopter that carries air transport containers located on its underside and flies an equally fully automated route called "aerial corridors" landing on a designated landing pad where it is automatically unloaded and then the customer receives a delivery notification on their smartphone saying their parcel is ready for pick up at the parcel station.

Projects like "Skyways" are interesting because they could help to evolve the regulatory framework for self-piloted aircraft systems operations if the outcomes demonstrate that "Skyways" and associated infrastructure can safely operate over the National University of Singapore.

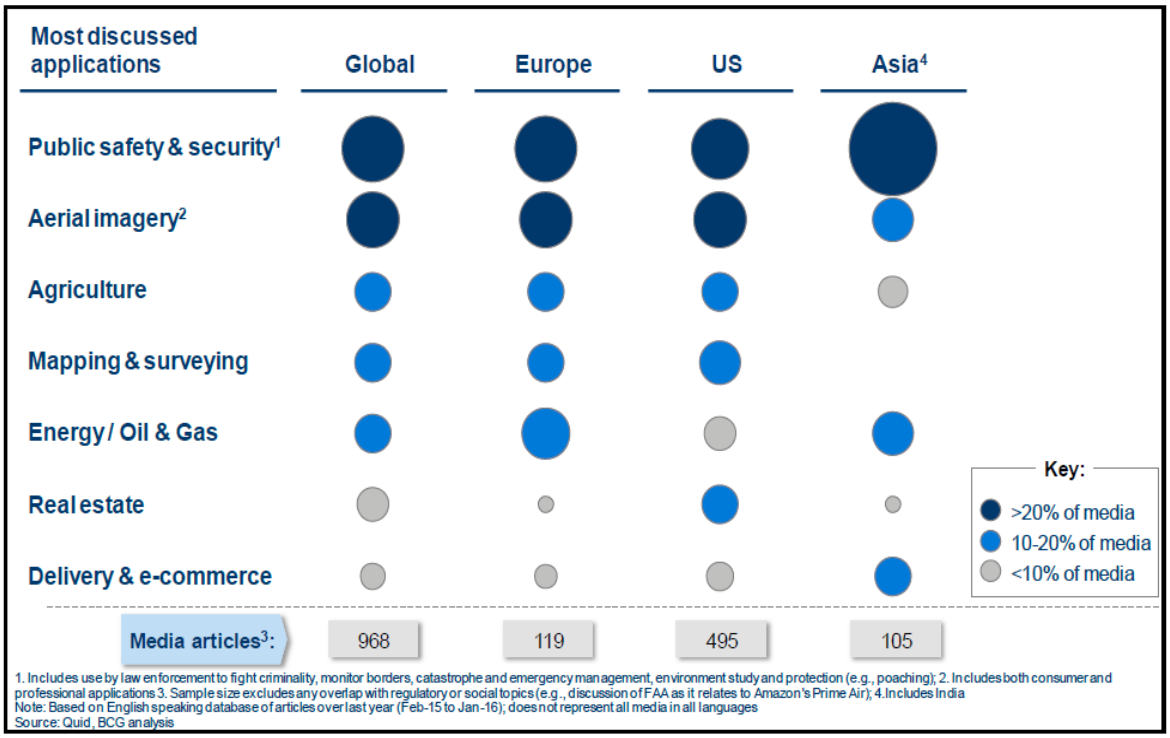


Figure 5.53 - Applications by region based on media attention [17]

Further actions taken at the European Union level will need to occur rapidly given the pace of global development in drones, especially as the US and China are already (Figure 5.53) the leaders in different forms of production and investing more heavily than the European Union. One example of this is the UAS Traffic Management (UTM) system that is currently being developed by NASA in the US. This system has been described properly in Benchmarks for Goal 4.

Much of what still needs to be done include technology (detect and avoid, Datacom), air traffic management, security & cyber reliance along with the availability of authorized & safe testing environments. As a main finding of the study and based on the expectations of the market to unlock demand and global competitiveness, these improvements need to be completed within a window of opportunity limited to the next 5-10 years. Completion within such a timespan requires that an ecosystem is created at European Union level around both technology and regulation to ensure a proper "home" for drones that brings all key public and private stakeholders together [17].

Regarding research and development, European Union funding levels need to be re-assessed to stimulate this emerging marketplace and establish a European level ecosystem. Based on expectations of the market, an estimated total of at least EUR 200 million in additional R&D over the next 5-10 years is required to address remaining gaps related to Very Low Level (VLL) activities that will represent the majority of future drone operations. Required additional investments should be supported by a mix of both public and private stakeholders reinforcing the importance of a European level ecosystem for R&D. This same mix of stakeholders will also be needed to ensure fast implementation of comprehensive

regulation. Speed will be essential for Europe to obtain a global leadership position, especially as the value in services remains in the early stages of development in all markets. It is therefore also critical that R&D coordination at European Union level results in leveraging and bringing together numerous initiatives that are presently fragmented across the Member States and industry stakeholders [17].

One of the keys in this subject is the technology related to air traffic management in such a way that the demand for UAVs on all areas of airspace highlights the critical nature of air traffic management. UAVs will create new forms of traffic, especially (Figure 5.54) at very low levels of airspace with high demand in densely populated areas where risk levels will increase. As a result, appropriate new and adapted procedures along with the development of technology related to the management of airspace are a "must-have" for safely accommodate the growth of UAVs. Besides, the absence of a pilot on board of the aircraft raises the question of how to detect and avoid other traffic, or objects, and how to handle dangerous situations. Airborne collision avoidance systems can protect unmanned aircraft from damage, but they are not designed to deal with denser traffic. This is comparable to the situation with road traffic: As long as there are just a few vehicles on the road, the driver is able to control the situation and avoid other vehicles or obstacles; but the denser traffic becomes, the more traffic control in the form of, for example, traffic lights are needed [19].

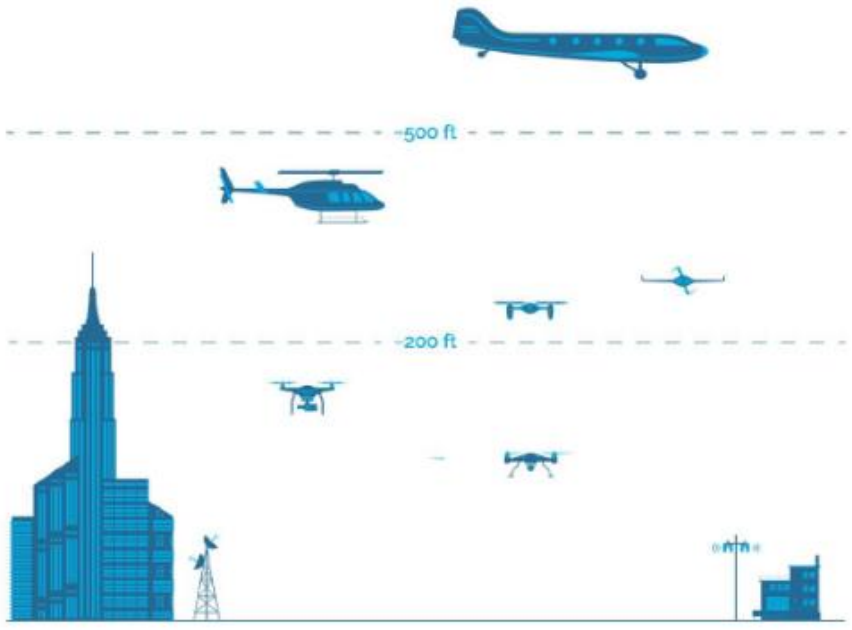


Figure 5.54 - UAVs operations by altitudes [19]

Related to that, conventional air traffic management cannot be applied to unmanned aircraft. It relies on voice communication between air traffic controllers and pilots, and radar detection. Larger drones may be equipped with voice recognition/speech synthesis radio and have a significantly larger radar cross-section. However, many drones are too small, and operate too close to the ground, for radar to

be of any use. Current airspace management and air traffic flow management systems are not predicted to have the capabilities to handle the type of operations relevant to drones. Besides, the forecasted traffic density of drones is far beyond the capabilities of current air traffic management systems, which were never designed to handle large amounts of dense heterogeneous traffic with widely varying performance characteristics [19].

In this context, the Member States of the European Union should be at the forefront of this matter, developing the UTM system that allows UAVs to fly joining manned aircraft and also implementing the regulatory framework regarding the integration of UAS into busy airspace as it is European airspace.

Besides, it is important to set the differences between the UTM concept and the UTM system [19]:

- On the one hand, the UTM concept is a complex system in which several stakeholders contribute to ensuring the required safety level of UAS operations, i.e. is a system of stakeholders and technical systems collaborating in certain interactions and according to certain regulations, to maintain safe separation of unmanned aircraft, between themselves and from ATM users, at very low level, and to provide an efficient and orderly flow of traffic.
- On the other hand, a UTM system is a concrete technical implementation comprising software, the necessary infrastructure for running the software and the drones themselves, all contributing to the achievement of UTM. This UTM system should cover the needs of both RPAS and autonomous unmanned aircraft and also consider all sort of UAS operations: VLOS (Visual Line of Sight), EVLOS (Extended Visual Line Of Sight) and BVLOS (Beyond Visual Line Of Sight).

As it can be noticed, the most likely stakeholders of a UTM system could be composed of national aviation authorities, supranational institutions, drone pilots, operators, drone owners, conventional aviation pilots, conventional ground, rail or sea traffic, law enforcement, emergency services, drone manufacturers or UTM service providers. This cluster of stakeholder's evidence that the UTM domain will have to deal with different and heterogeneous organizations that should address this issue as a solid and collaborative group.

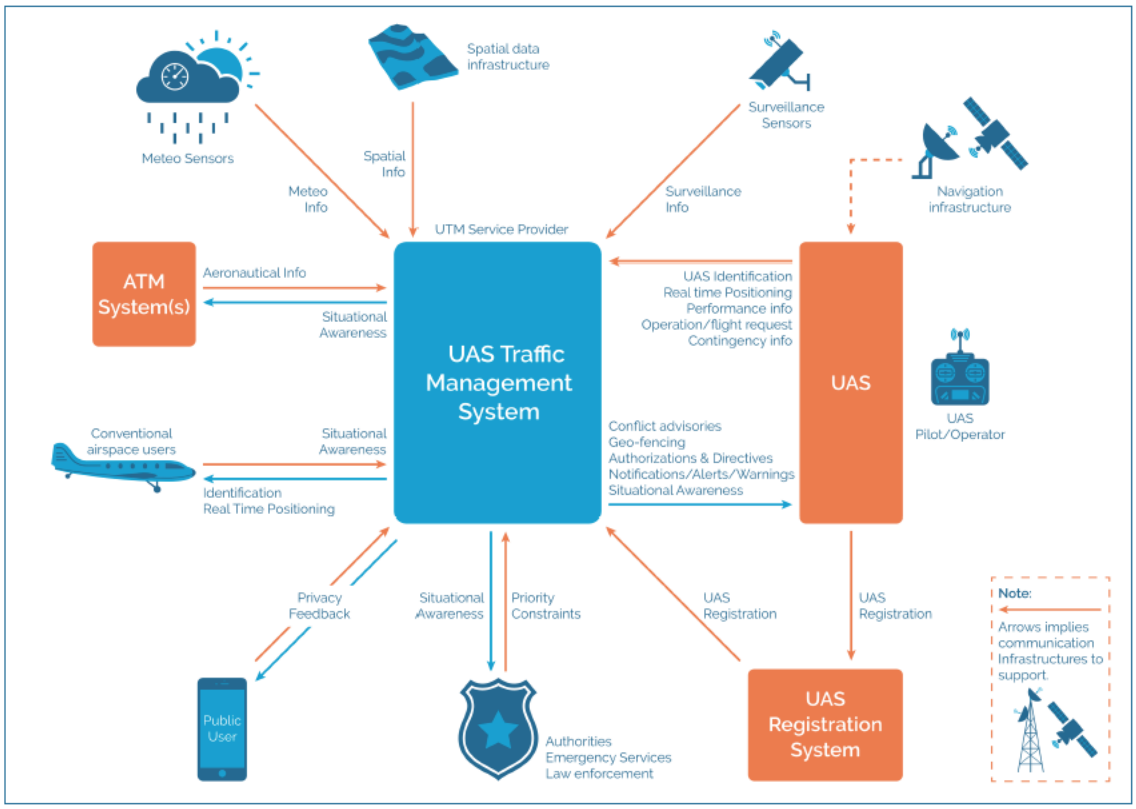


Figure 5.55 - Example of an UTM system

Related to Figure 5.55, each UTM system can be modelled as a set of functional blocks in mutual interaction to accomplish the system mission. This proposal is a logical breakdown not aimed at constraining possible deployments, which may vary in the physical architecture according to the specific deployment case. The breakdown is rather aimed at highlighting important information exchanges, inputs for service, and data protocol definitions [19].

Another possible breakdown is the one proposed by NASA, which shows (Figure 5.56) how a UTM system will be deployed in the United States and which has been described in Goal 4.

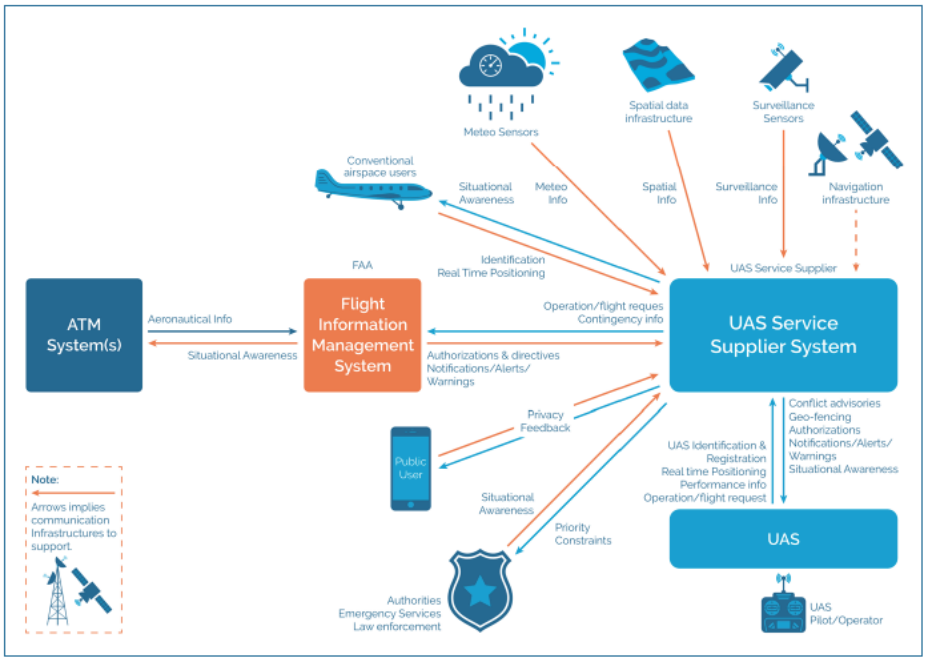


Figure 5.56 - NASA UTM system [19]

Reference State in 2010

Drones have been used since long time ago, as demonstrate the first prototypes which date from XIX century. These first steps of the UAVs addressed to develop them for military and security issues during the XX century, in such a way that they were used in different wars such as the Second World War or the Cold War.

However, since not so long ago -about 20 years ago- governments and private stakeholders started to try to extend their range of action to a civilian application. Thus, stakeholders had to consider the new concepts for a civilian application: whilst the ultimate goal in a military application is the completion of the mission, the ultimate goal in a civilian application is safety. That means that in military application aircraft could crash but only after the mission is completed, nevertheless in civilian application aircraft could never crash. Consequently, technology development was needed for UAVs civilian application due to different specifications meant different systems.

Focusing on the European Union, several projects about UAVs were carried out during the first years of the XXI century within the Fifth Framework Programme. This Fifth Framework Programme set out the priorities for the European Union's research, technological development and demonstration (RTD) activities for the period 1998-2002.

Some of these projects are explained below [20]:

- **UAV-NET**: this project addressed a Thematic Network on the subject of advancing the utilization of UAVs into the civilian commercial sphere UAVs have proven their capability within the military

fields. The many civilian applications addressed in this project were environmental monitoring, communications relays, law enforcement surveillance, earth observation, etc. where the benefits of UAVs were only beginning to be understood. The Thematic Network served as a forum for information exchange, for setting new policies and for launching activities in critical technology research and technology platform validation studies at the next stage.

- **CAPECON**: this project (Figure 5.57) aimed to advance the utilization of safe and low-cost Unmanned Air Vehicles (UAVs) in the civilian commercial sphere. CAPECON surveyed in-depth applications of potential users and produced safety and cost assessments. It also was compared different aerodynamic configurations and it was defined as possible civil UAV configuration ready for engineering development. This project was a research synthesis of critical technologies, configuration design, simulation and cost appraisal methods, aimed at the design and production of safe and commercially viable, civilian UAVs. The project also focused on configurations and technologies suited to High and Medium Altitude Long Endurance (HALE and MALE) missions and also to Rotary UAVs. At that moment, the commercial potential for the civilian use of UAVs was largely untapped; hence CAPECON aimed to enable the EU to gain a leading role in this emerging technology.

Figure 5.57 - UAVs studied in CAPECON Project

- **USICO**: the main goals of this project (Figure 5.58) was to improve operational capability and safety of UAVs. Related to that, the scope of work gathered the following issues:

- Recommendations for UAV system airworthiness certification procedures and standards.
- Recommendations for UAV operations regulations.
- Technology for seeing and avoid.
- Proposals for research into image recognition and sensors and adapted ADS-B technology.
- Flight simulation of UAV ATC/ATM process. For example, USICO simulated a civil UAV safely flight in Frankfurt airspace using the concepts developed by the USICO project.

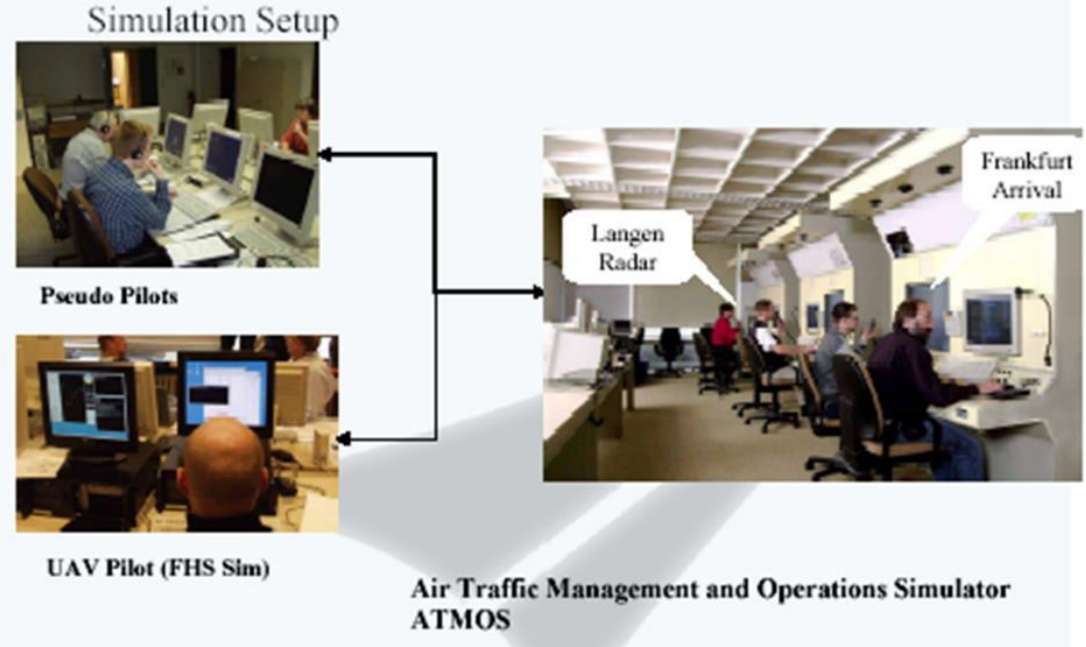


Figure 5.58 - USICO simulation in Frankfurt airspace

Progress Up-to-Now

During the last decade, the disruptive concepts related to UAVs systems and manufacturing were developed in such a way that the civil use of UAVs has sharply increased. Nowadays, besides the different uses of UAVs such as public safety, deliveries, surveillance, weather monitoring, and agriculture and so on, it is usual to know someone who owns a drone for leisure. As a result, the number of drones within the European Union has multiplied over the last 2 years.

These new users of airspace are generating new conflicts which have shown up during the last few years. Concerning that, EASA analyses in its Annual Safety Reviews the occurrences related to UAS in the European airspace and, in the 2017 Annual Safety Review [21], the outcomes show that most of the occurrences are related to either airspace infringements that occasionally lead to a near collision with an aircraft or issues with controlling the RPAS's flight path.

In this manner, the analysis of UAS occurrences in the European Central Repository (ECR) identified 606 occurrences (Figure 5.59) of all severity levels for the last 5 years, of which 37 had been classified as accidents, and fortunately none of them involved fatalities. The collection of data on UAS occurrences is still in its infancy and there is still a lot of work to be done to ensure the correct application of taxonomy terminology related to UAS. This work should be done due to the fact that the increase in the number of non-fatal accidents and serious incidents demonstrate the rapid development of drone operations [21].

	Fatal Accidents	Non-Fatal Accidents	Serious Incidents
2011-2015 average	0	2.6	0.3
2016	0	15	7
% difference	-	470%	2230%

	Fatalities	Serious Injuries
2011-2015 average	0	0
2016	0	0

Figure 5.59 - Key statistics about UAS accidents and serious incidents from ECR occurrence database [21]

Figure 5.60 shows the development of reported UAS occurrences for the last 5 years. These occurrences, observations and sightings come mostly from pilots flying commercial aircraft owing to it are rare that UAS pilots report the occurrences that they encounter concerning UAS operations. As can be noticed from Figure 5.58, the difference in terms of percentage between both periods of time is extremely high. Moreover, this yearly growth of occurrences can also be perceived in the following figure 5.60 in which data from the European Central Repository and additional data reported to EASA from several European operators have been used.

Figure 5.60 - UAS reported occurrences per year 2012-2016 [21]

Fortunately, most of these occurrences have not been classified as accidents as can be seen in the following Figure 5.61. However, further effort is necessary to decrease a large number of incidents and accidents reported during the last few years.

Figure 5.61 - UAS accidents and other occurrences during 2012-2016 [21]

An additional study has been carried out based on the available data containing altitude information. It can be noticed in the following Figure 5.62 that when the drones are spotted the manned aircraft is most often in the area from 0-6000 feet above the ground and the distance from the aircraft to the drone is from 0-1000 feet. This reflects the main range of drones, which can reach different altitudes but most often they usually operate in low-altitude airspace, hence a regulatory framework that take into account an environment where both unmanned and manned aircraft coexist should be implemented.

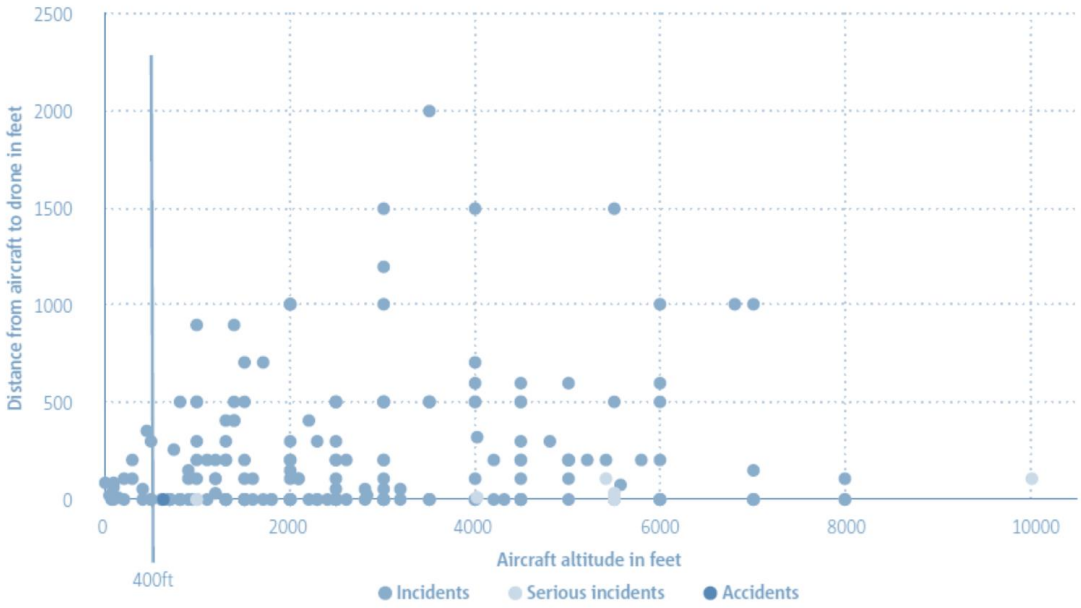


Figure 5.62 - Aircraft altitude vs distance from drone at the time of detection 2010-2016 [21]

Regarding the most severe incidents reported during the last years, three key risk areas have been set [21]:

- The first one is the aircraft upset: most of the accidents are related to drone pilots losing control of the drone as demonstrate the fact that 50% of the RPAS accidents are related to such incidents. These incidents usually result in damage and most often, the destruction of the aircraft.
- The second one is the airborne collision: even though there are very few occurrences where actual collisions between a drone and a manned aircraft happen, the risk is considered to be substantial and, with a steady exponential increase of unmanned aircraft of all sizes and shapes, it is vital to monitor this area closely and to work on solutions that prevent actual collisions.
- The third one is the obstacle collision in flight: drones used in aerial work operations and space-constrained areas are susceptible to higher collision risk than manned aircraft.

Therefore, it is evident that further regulations should be developed and implemented as soon as possible in the European Union. These regulation frameworks should regard the control of the UAS flight path, use of automation and also regard airspace infringement and airborne separation, which is a hard task since nowadays smaller drones do not have transponders onboard.

Predictions Up-to-2025

Today's evolution of UAVs framework depends on technology, ATM, regulations and societal acceptance. The increase of automation up to the potential of robotics in the sky is not brand new, however more robust technology is still required before many applications are commercially viable and accepted. Additionally, regulation and societal concerns related to privacy and safety remain constraints for some applications already feasible from a technical perspective.

In terms of regulation, a new framework around the operations of drones should be proposed by the European Union as a common basis to harmonize regulation across Europe and enable more applications. Related to that, European Member States have already been at the forefront of regulation with over 15 Member States holding legislation related to drones. Included in this legislation are initial permissions for beyond visual line of sight (BVLOS) drone operations that are critical for many of these operations to be economically viable opportunities. Examples of such BVLOS permissions include Spain allowing BVLOS for drones under 2 kg and France allowing these flights for drones under 2 kg with no lateral limitation and additionally for drones under 25 kg that operate within 1 kilometre (km) of the remote pilot. The above examples begin to indicate the remaining opportunity for harmonization across States in order to unlock future potential[CITATION SES16 \l 1034].

Even though EU countries have been at the forefront of legislation, the regulation still limits the extent to which drones can operate on their own and the ease of to which operations can expand across countries using the same drones and certifications. Critical parts of the evolving regulation will be the extent to which drones can be operated BVLOS, in populated areas or/and without a dedicated pilot per each drone (i.e. allowing a single pilot to operate or monitor more than one drone at the same time).

Furthermore, societal worries on privacy and accidents create an additional barrier that drones must overcome for regulators to allow flights in populated areas. These concerns over safety are magnified

by the fact that drones are bringing aviation capabilities to a group of new users. The inexperience of these users in the aviation framework increases the number of issues that regulators must consider.

Traffic management solutions associated to required drone technologies (e.g. detect and avoid, datalink, geofencing) are key enablers for safety, and it is essential that they demonstrate together safety performance in-line with the high standards of the aviation industry. The ability to address how drones will be safely integrated into European airspace and also how cybersecurity threats will be mitigated, would be factors in determining the pace at which the industry will grow over the coming years.

Additional technology advancements will also be important to increase the value that drones generate for end users. Big Data analytics related to services such as industrial preventative maintenance, precision agriculture and research purposes are still in their early phases of development and must continue to evolve for drone's applications to successfully transform businesses and processes. Components and systems related to engines, propulsion and batteries will be needed to achieve required levels of reliability and durability performance that commercial users demand. High-precision navigation, like that in development as part of the EU's Galileo and EGNOS satellite navigation systems, could also be considered for drones to improve reliability and support their integration in non-segregated airspace[CITATION SES16 \l 1034].

The progression of regulation, ATM procedures, technology and societal acceptance will likely continue to take shape rapidly, both in Europe and in other global markets. It is, therefore, necessary that Europe helps to develop the stated above through facilitating to set the regulatory framework and also investing in the projects carried out by the stakeholders.

Evolutionary Progress Up-to-2050

The role of drones is likely to expand still for many years, thus driving the need to understand mission types that are being established today and also those yet to come. Different sectors could illustrate the opportunity that drones have to transform how businesses operate, to increase Europe's global competitiveness, to provide new jobs and to deliver both economic and environmental benefits. These sectors, shown together with some of the societal benefits that drones may generate within each, are the following [CITATION SES16 \l 1034]:

- **Agriculture:** Drones could help to enable precision agriculture that will be critical to meet productivity needs for Europe and support greener farmer practices that are a focus of the EU Common Agricultural Policy (CAP) of 2020.
- **Energy:** Drones may reduce a variety of risks including to personnel performing hazardous tasks, to the environment by properly maintaining assets and to the infrastructure overall by limiting the amount of downtime to Europe that already is a heavy importer of resources and pays higher energy prices than other regions.

- **Public safety and security:** Drones could be used by a variety of authorities to better assess and monitor hazardous situations, complete search and rescue missions, gather evidence for investigations and detect other crises.
- **E-commerce and delivery:** Urgent packages, including medical supplies, could be completed in a fraction of the time and online retailers could benefit from increased accessibility in both urban and remote areas.
- **Mobility and transport:** The infrastructure of today, i.e., railways, may be monitored and kept secure and future forms of passenger aircraft could someday operate safely without the requirement of onboard pilots.

These many applications will lead (Figure 5.63) to a sharply increase in the number of drones in the following decades as forecasts show. Overall, in terms of the order of magnitude, military defence assets are expected to increase from high hundreds to multiple thousands, leisure units from close to 1 million to approximately 7 million and, finally, government and commercial units from multiple thousands to hundreds of thousands. Leisure unit growth is expected to mature in the near term with defence and the government and commercial growth will continue out through 2050. These numbers can be seen in the following Figure.

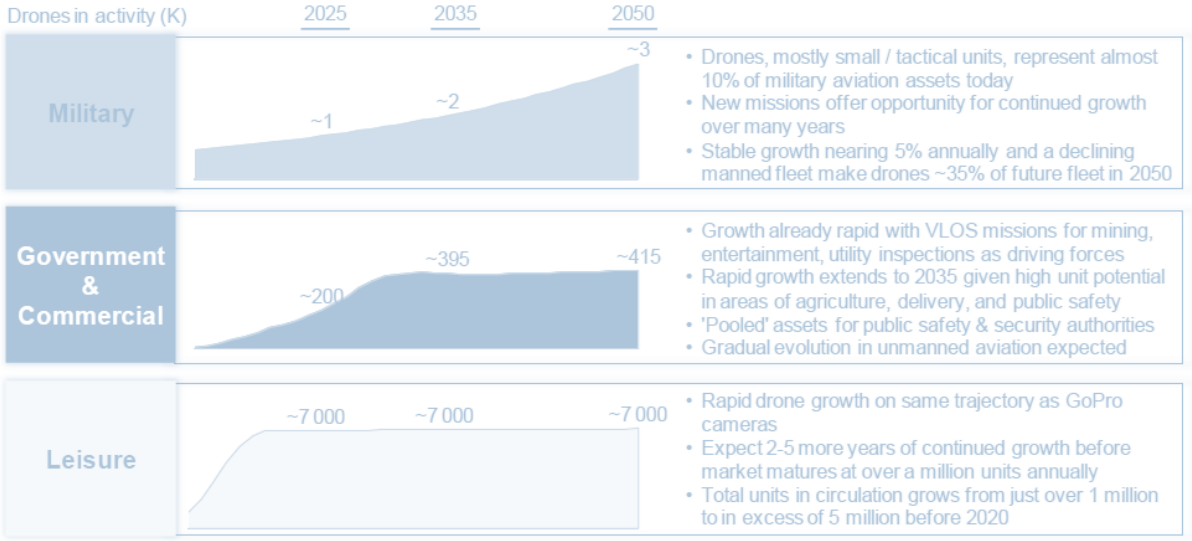


Figure 5.63 - Total fleet size forecast (current through 2050) [CITATION SES16 \l 1034]

As can be seen, the largest increase will correspond to leisure drones, which will operate at very low levels of the airspace. It is expected a continued annual unit growth for another 3 years that would increase the total from just over 1 million units sold to nearly 7 million (with annual sales exceeding a million units). The recent history of action-based cameras, led by GoPro, provides a comparable case to highlight these expectations, especially given filming and imaging are a leading driver of consumer usage. GoPro is expected to reach the maturity of its annual unit sales this year after a period of 9 years of growth, of which the first 6 were a near-identical match to drones (see the following Figure 5.4. After

2-5 more years of annual sales growth in drones, the total consumer base should remain relatively stable for a significant period.

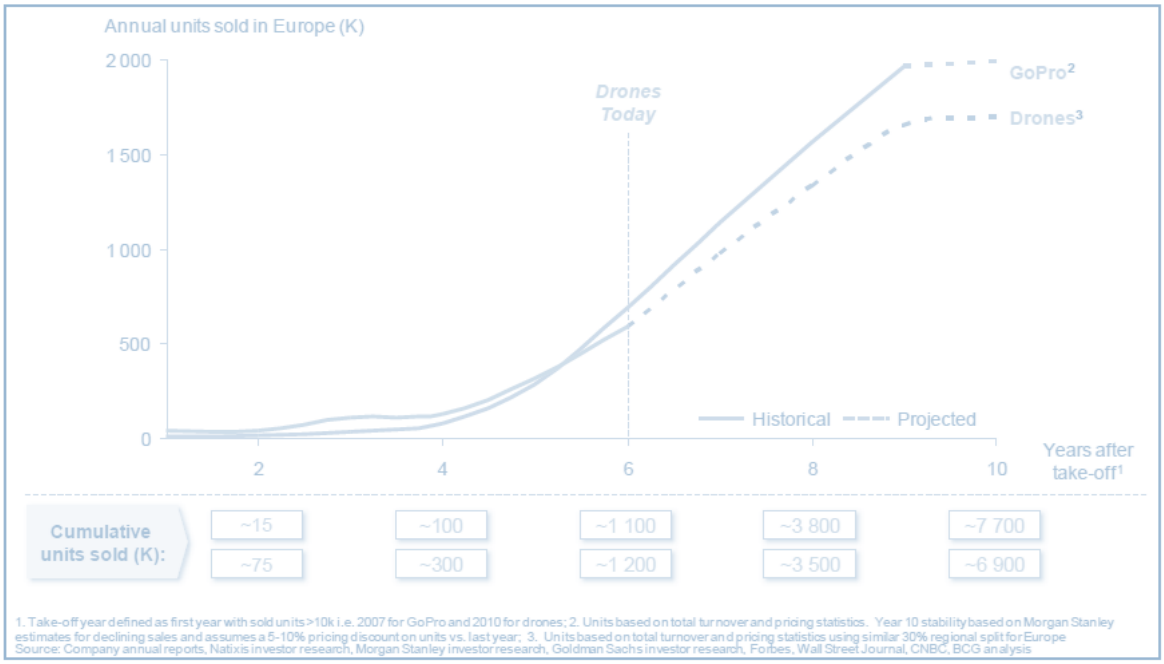


Figure 5.64 - Comparison of growth in leisure drones to GoPro action cameras [CITATION SES16 \l 1034]

Talking about the demand forecast classified by mission type, the use of drones for local surveying that is mostly within visual line of sight (VLOS) has the potential to increase rapidly as result of energy infrastructure inspections (solar farms, wind turbines, power plants, dams, refineries, oil platforms), public safety and security (police and fire response using in-vehicle units), mining and construction (both quarries and industrial construction sites with the potential for residential surveying in future), insurance (property inspections) and media (new coverage) among other. Together, it is estimated the potential for over 100.000 drones by 2035 and 2050. These drones have a relatively low regulation hurdle to overcome as many of these operations can be performed within visual line of sight. However, as exemplified by police and fire missions, these drones will need to be able to fly in densely populated areas to reach this forecasted potential.

Beyond visual line of sight, capabilities yield even greater potential. For mapping and surveying alone, 180.000 drones are estimated for 2035 with fixed-wing drones being the primary operating type. This includes agriculture remote sensing of crops and livestock, an inspection of the power line, pipeline, and railway networks that currently require expensive helicopters. In the future, they could be used by public authorities to operate drones directly from each station and could complement or replace VLOS units carried in vehicles. Media drones used to cover traffic conditions or sporting events such as cycling are also opportunities along with use at larger construction and mining sites and for conducting new forms of research by universities and other institutes.

The majority of light load drone missions are also expected to operate beyond visual line of sight with 90.000 drones forecasted by 2035 mostly for delivery purposes and flying at low altitudes. This includes emergency medical deliveries, lightweight industrial deliveries (e.g., from a port to a vessel or transfer of tools across a large industrial construction site) and completing traditional forms of delivering parcels and couriers to businesses and consumers. Agriculture chemical spraying and seeding represents a smaller portion, approximately 25.000, of the estimate for light load drones flying at these low altitudes.

More complex certified drones are expected primarily in public safety and security and mobility sectors. Drones with longer endurances and flying well above 150 meters are expected for border security, maritime surveillance and other environment assessments (e.g., forestry and national park surveillance). As a result, they will likely be acquired by national and regional authorities and represent a low volume (a fleet size close to 100 units in total which could reach a few hundred over the time). These capabilities are likely to be in the form of technology transferred from the military.

Complex certified drones also include remotely piloted or highly automated aviation capabilities for today's aircraft fleet, including rotorcrafts and commercial airlines. As stated above, public acceptance will be essential along with ensuring the robustness of the technology which is likely to come from the military. A gradual shift towards systems with no pilot onboard over multiple decades is expected to occur according to the evolution of the society with regards to automation. Therefore estimates (Figure 5.65) are inclusive of optionally piloted systems. Approximately 10.000 units are estimated in 2050 on the basis of the market starting first for cargo aircraft sometime after 2030 and then for human transport at earliest 2035, representing a lag of at least 10 years after the launch of fully autonomous self-driving vehicles anticipated for 2025[CITATION SES16 \l 1034].

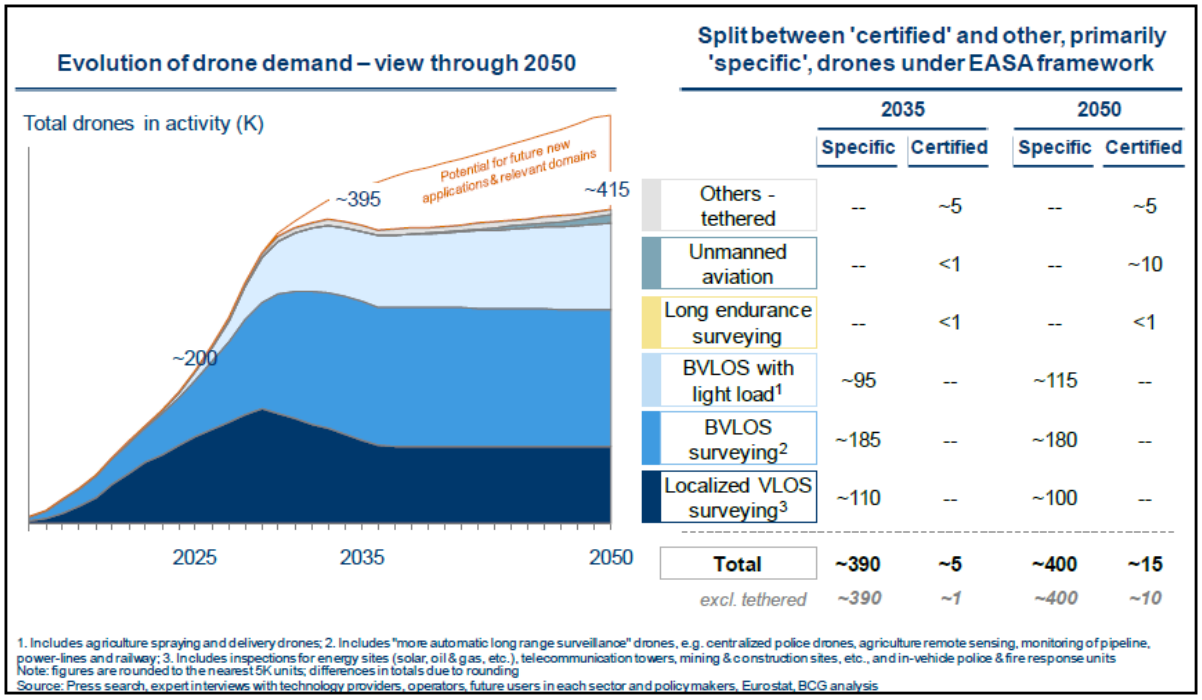


Figure 5.65 - Demand outlook by type of mission [CITATION SES16 \l 1034]

The potential for drones across many different settings in the years to come has considerable implications for airspace management. Future forms of optionally piloted and unmanned aircraft for mobility purposes are estimated to represent approximately 20% of the future fleet meaning that air traffic management would need to account for millions of such flights in controlled airspace by 2050. The safe integration of these drones in ATM will also need to include ground operations particularly in airports where automated taxiing capabilities are required.

Possible or Predictable Breakthroughs

Enabling successful safe operations beyond visual line of sight is the core of commercial and government market potential and this will require the availability of a variety of technologies. Further, many of these technologies will require multiple forms to account for the various types of missions being performed at very low levels and also in controlled and uncontrolled airspace (i.e., different development to prevent a collision with a static building than a collision with a fast travelling manned aircraft). Several of these technologies are suggested to require European level support to effectively bring them to market in the context of the global marketplace. This set of technologies is further detailed below individually [CITATION SES16 \l 1034]:

- **Detect and Avoid** (D&A) capabilities are seen as a key enabler for drone operations in all classes airspace and are expected to have a positive impact on safety and social acceptance. This technology depends on the flight rules: in IFR the D&A system performs the collision avoidance function against cooperative and non-cooperative traffic, whilst in VFR/VLL drones will need to be able to detect and avoid cooperative and non-cooperative traffic and multiple types of obstacles (power lines, buildings, trees, birds etc.). Although some investments to develop solutions supporting the safe integration of drones in non-segregated airspace have been made, it still requires large investments to bring performances to the required level. Lower levels of investment in detecting and avoid for very low level operating drones are also impacted by the remaining gap of a clear vision on the future concepts of operations and regulatory framework, making it risky to invest and difficult to align players towards industry standards and hence the development of appropriate solutions.
- **Datacom and spectrum** issues are critical to enabling BVLOS and long endurance surveying missions to happen in safe conditions. Appropriate datalinks are necessary for command and control (C2) as well as potentially for communication with air traffic control (ATC) or future forms of VLL drone management. The biggest challenges when it comes to datalinks are the identification, allocation and protection of the necessary spectrum. Also to ensure that safety is not compromised by interruption of links, or that there are redundant or alternate links.
- **Security and cyber resilience** is a priority area of development to mitigate the risk that drones could be subjected to malicious or accidental takeovers of datalinks leading to accidents, theft or deliberate use of the aircraft to damage infrastructure or hurt civilians. Those issues could have a severe negative impact on public acceptance. Private initiatives are exploring potential solutions such as

digital identification, but clear concepts of operations, requirements and standards are needed to drive research into a more advanced and coordinated phase.

- **Human factors and training** will need additional R&D efforts to ensure that the situation awareness for pilots of drones matches that of pilots in cockpits. Additionally, there will be a requirement to manage the transition from remotely piloted drones to more automated drones that are only monitored. In order to achieve those goals, effective solutions regarding contingency, failure management etc. will need to be put in place. Harmonization of the operator's environment is likely to lead to more appropriate training and higher safety. Training and qualification is an underlying topic that requires immediate action from the EU to provision new, well-trained pilots. Achieving EU-wide accepted pilot licenses would accelerate the creation of drone service companies.
- **Validation and demonstration** will be important to increase public acceptance of drone operations and will support the regulatory work. Although some validation exercises are performed at a national level, broader authorized and safe testing environments to perform integrated demonstrations involving different systems (manned and unmanned operating simultaneously) will be needed. In addition to that, EU level coordination on the allowance to let some pioneer applications operate will be of high importance. Indeed, pioneer applications that would be allowed under a risk-based logic would enable the collection of data and observations to further refine concepts of operations and regulation while increasing public acceptance.
- **Air traffic management (ATM)** is a critical area that requires further research and development. All previously mentioned R&D topics depend on how ATM will integrate drones in all classes of airspace. The basic principles of drone traffic management as defined by the concepts of operations will lead to precise requirements on which industry standards will be developed, thereby assuring a strong basis for future investments and partnerships across private industry players and public member states and stakeholders.

Identification of Gaps

Leisure drones, while increasing dramatically in number, are still on average only flown for a few hours annually. Beyond visual line of sight (BVLOS) operations, including above the very low level (VLL), may impact all classes of airspace and have a much greater impact on the airspace than leisure drones given they will likely fly multiple hours a day. This is expected to be especially true in the long term for delivery and public safety & security drones operating in urban environments.

Unmanned aircraft, including station-operated beyond visual line of sight drones, will need to safely operate alongside manned aviation and delivery drones in dynamically changing locations. In total, all operations that are primarily performed at very low levels are estimated to represent the majority of flight time to be accounted for and thus will require additional technology to support safe operations.

To maintain high levels of safety similar to manned aviation, multiple technology areas should be taken into account, which is highly aligned to these same categories as detect & avoid, datacom & spectrum,

human factors, security & cyber resilience and validation & demonstration are all included and represent direct synergies with ATM.

The issue is that in the lower levels of airspace, i.e. uncontrolled airspace and very low-level airspace, the road to the safe integration of drones is even more challenging and currently less addressed than in controlled airspace. Drones in those types of airspace will need to be able to cope with non-cooperative air traffic, multiple sorts of obstacles and aircraft operating under visual flight rules (VFR). The safe integration of unmanned aviation at those lower levels is likely to require a new drone management system and approach (i.e. unmanned aircraft traffic management (UTM)). The exact shape of this drone management system is yet to be defined and will likely require EU level coordination and harmonization of all stakeholders.

Furthermore, European Union support is necessary to create a competitive drone market, able to improve connectivity, growth and jobs just as has been done in EU aviation. Related to that, boosting innovation and regulation in a manner that matches or outpaces that of the global drone marketplace needs harmonization and coordination. The numerous initiatives on drones remain fragmented across industry participants and Member States such that it are important that increased coordination and pooling is urgently put in place. Facilitating cooperation and public-private co-developments is a role which has to be orchestrated at the EU level and it will be critical to developing an ecosystem that welcomes the full range of relevant public and private stakeholders.

Overall, from a technological standpoint, most developments need to occur over the next 5 to 10 years. The improvement of security & cyber resilience, as well as improved datacom & spectrum and a deeper understanding of human factors, are key R&D areas that will reinforce safety and the hence public acceptance of drones. On top of that, privacy and security, as well as regulation awareness to attain social acceptance, should be addressed. The next five years, however, will be crucial to unlocking a majority of the market potential while assuring that Europe remains globally competitive. If Europe has difficulty allowing for technically mature missions at an efficient pace, capabilities will be more likely to develop abroad and export their expertise to Europe at a later stage thereby limiting economic potential locally. Success during these next 5 years can only occur with immediate actions and support at an EU level to the required drive investment and regulatory support[CITATION SES16 \l 1034].

KEY TOPIC T5.3 – PASSENGER AND LUGGAGE SCRENING AT AEROPORTS

Scope of the Goal

Comprehensive and unobtrusive security measures		
<u>Goal 17:</u> Efficient boarding and safety measures allow seamless security for global travel with minimum passenger and cargo impact. Passengers and cargo pass through security controls without intrusion		
Comparison with 2017 SRIA document	Why	Lacks

Coherent	Both the SRIA document and the reporting mark that security must be addressed continuously during operations to ensure the safety of staff and passengers and continuity of service. This must be achieved while maintaining system safety as well as performance, with acceptable levels of capacity and delay.	Security must be supported by intelligence that provides the information necessary to develop a comprehensive and detailed catalogue of threats and system vulnerabilities. Tools such as a security radar or a horizon scanning will be needed to automate the detection of aviation incidents, a gathering of associated information, and forensic analysis

Table 5.3 – ACARE/SRIA security targets

Benchmarks

Today's security measures as passenger and baggage security screening have as consequence delays and queues, which are the most frequent sources of traveller dissatisfaction. Therefore, the ACARE goal for the future is to achieve the minimum of delay, intrusion and disruption in the implementation of safety measures, through the use of the most appropriate equipment and airport architectures.

One of the current initiatives which have as an objective to improve the passenger experience and to strengthen security is the project called Smart Security, a joint initiative of the International Air Transport Association (IATA) and Airports Council International (ACI). This project defines a future where passengers proceed through security checkpoints with minimal inconvenience, where security resources are allocated based on risk, and where airport facilities are optimized. This will be achieved through the implementation of new technologies and processes that will result in the following benefits:

- Security improvement.
- Better passenger experience.
- Operational efficiency improvement.

New technologies

Conventional X-ray scanners and metal detectors are the standard security methods used nowadays but they imply delays and troubles for passengers. Advanced screening technologies (Figure 5.66) will allow for effective threat detection while reducing the burden for passengers. Some solutions proposed to improve security measures are the following ones:

- Passenger screening: security scanners which are increasingly being adopted by airports can improve security and passenger experience outcomes since they have the capacity to detect concealed items on the body regardless of the substance and the ability to facilitate a targeted search. These security scanners together with automated decision support algorithms could help the security officers to carry out better and quicker inspections of passengers and, at the same time, respecting better their privacy.

- Cabin baggage screening: new technologies which are currently in development such as Dual/multi-view X-rays and Computed Tomography (CT) could help operators to examine in more accurately the cabin baggage. For example, Dual/multi-view X-rays assist provides images of multiple angles of the same bag while the CT capacities include the ability to produce 360-degree images from the bag, which will allow having a better view of its content.
- Alternative measures: alternative screening methods could enhance the overall effectiveness of the security checkpoints, while at the same time support operational efficiency and improved passenger experience. Some of these new alternative methods are the Explosive trace detection (ETD) or the Explosive detection dogs (EDD). On the one hand, ETD equipment can detect trace amounts of explosives on a person, their clothes or their belongings. These detection capabilities, as well as their portability, makes ETD a passenger-friendly, especially because these devices allow a process less intrusive. On the other hand, Dogs can be used to detect passengers who may be carrying or have recently been in contact with explosive materials. They offer several advantages such as more operational flexibility than fixed screening equipment and, also, they are usually considered more unobtrusive than other security measures.

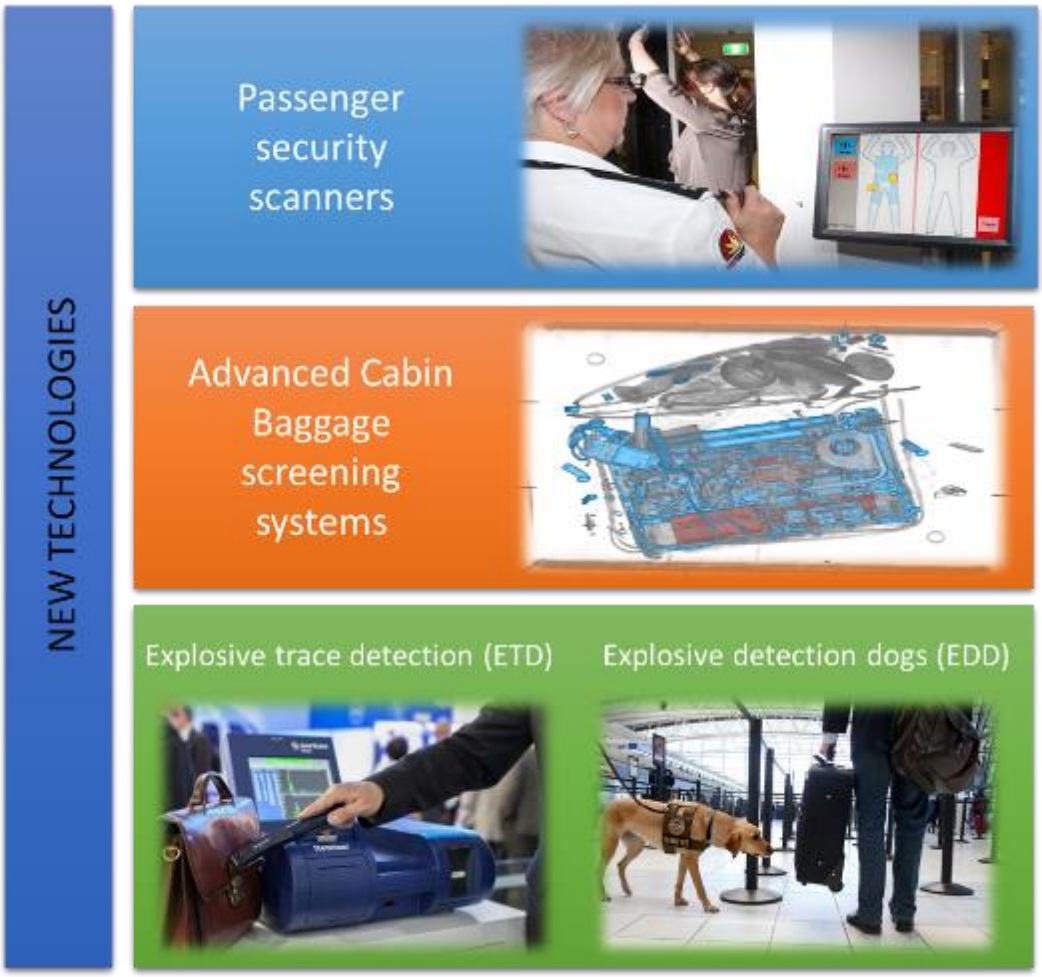


Figure 5.66 - Technologies for Comprehensive and unobtrusive security measures

New Procedures

Until now, most risk-based decisions regarding the checkpoint have focused on assessing the risk of a particular item but considering all passengers as equals. Therefore, the risk-based differentiation concept is introduced, which focuses its attention on "the person" in the assessment of threats, instead of focusing on the items risk. As a result, based on a reasoned process of selection, different people would be screened in different ways. For example, people who have been identified as low risk people will have a quicker screening process while people identified as high-risk people will have a slower screening process since additional measures will be applied to them.

Five examples 'risk categories' are illustrated in the diagram below (Figure 5.67), where the majority of passengers could be considered as 'normal risk'. Some passengers will require enhanced search while a small proportion will not be allowed to fly or will be exempt from screening.

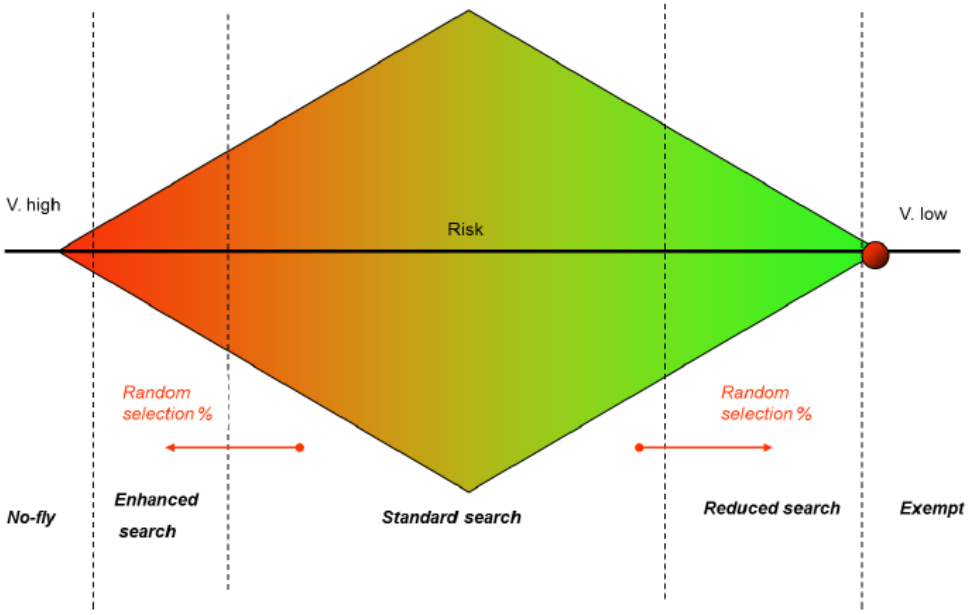


Figure 5.67 - Operational procedures for Comprehensive and unobtrusive security measures

In this way, the passenger would undergo some kind of "risk filter", which would classify them into higher or lower risk passengers. Therefore, the higher risk passenger would be submitted to additional screening measures prior to travel. These filters could be based on population-based data (category of passengers or journey) or based on individual passenger data. Data collection can start prior to the booking of a trip for known travellers, through check-in and baggage acceptance right up to the screening process. Each touchpoint by the passenger provides an opportunity to collect additional data, which may be used in the analysis of risk. As technology increases, new automatic screening methods could be used to detect behavioural anomalies and to collect data. This information could be digitally transferred to a security officer who will ensure that the passengers with a major risk are submitted to

additional security measures. Selection procedures such as these would not inhibit the passenger's journey through the airport and the passenger would not be aware of them.

- Benefits

Taking into account that, on average, passengers spend 20 minutes waiting in line to get to the security screening checkpoint, these new technologies and procedures could significantly reduce these waiting times.

In addition, new technologies would allow to process about 360 passengers per hour while conventional procedures such as X-ray metal detectors can process about 150 passengers per hour.

Reference State in 2010

The attempted sabotage liquid explosives of Northwest Airlines Flight 253 on 25th December 2009 and the thwarted plot to sabotage two cargo aircraft in October 2010 with improvised explosive devices concealed in freight shipments at airports in the United Arab Emirates and the United Kingdom lead to relevant ICAO actions on 2010.

In 2010 ICAO finalized a new comprehensive strategy for enhancing aviation security worldwide (ICASS ICAO Comprehensive Aviation Security Strategy) and the 37th Session of the ICAO Assembly unanimously adopted the Declaration on Aviation Security in light of the continuing threat to civil aviation. Annex 17 to the Chicago Convention was updated and strengthened to reflect the mayor risk and concerns to aviation, particularly in relation to staff screening, security equipment capabilities, hazardous substances in liquids, aerosols and gels (LAGs), cyber threats and air cargo. In January 2010 ICAO Secretariat established a database on the secure Aviation Security (AVSEC) website to disseminate information on acts of unlawful interference (AUI) efficiently and effectively manner, instead of distributing these data by way of an annual print summary. Following the attempted sabotage on 25 December 2009, ICAO used the secure Aviation Security (AVSEC) Point of Contact (PoC) Network to communicate information and recommendations to participating States, numbering 99 members at the time.

Historically, airport security measures have focused on checkpoint screening using magnetometers to detect metallic weapons on passengers and X-ray systems to examine carry-on items. However, these measures result in wait times and queues, which are one of the main reasons for traveller dissatisfaction. These methods have changed little since they were first implemented but new initiatives are emerging with the purpose of improving screening effectiveness through the deployment of new technologies. The objective is to enhance and strengthen security measures to detect efficiently threats as the entry of dangerous items on commercial aircraft but allowing freedom of movement for passengers. To that purpose, there have been several advances in technology screening during recent years.

These advanced technology aims to achieve the following benefits:

- Enhancing detection devices capability;

- Improving efficiency in security checkpoints;
- Preserving passenger privacy and dignity.

With these objectives, several advanced passenger and baggage screening technologies begun to be deployed in 2010, such as Advanced Technology (AT) X-ray, Bottled Liquid Scanners (BLS), Advanced Imaging Technology (AIT), Chemical Analysis Devices (CADs), and Explosive Trace Detectors (ETD). These technologies (Figure 5.68) allow to detect explosive threats and prohibited items on passengers and their baggage but preserving their privacy and dignity while increasing their safety.

Advanced Technology X-ray (AT): They are penetration X-ray based technologies that are used to screen carry-on luggage. They provide an enhanced view of a bag's contents through improved image resolution. AT X-ray creates multiple views/angles, clearer and more detailed images of baggage than traditional single-view X-ray.

Advanced Imaging Technology (AIT): AIT is a new imaging capability that will be used to inspect a passenger's body for concealed weapons (metal and non-metal), explosives, and other prohibited items. In addition, the AIT offers operators the opportunity to review anomalies on an individual, to determine if a hand wand and/or physical pat-down inspection is required. However, passenger privacy concerns raised related to this kind of equipment because this technology can provide a whole-body image that can reveal anomalies underneath passenger clothing. As a result, passengers show displeasure because these devices display highly personal details of their bodies. In order to ensure passengers privacy, the officer viewing the image is in a separate room and never see the passenger being screened while the officer attending to the passenger never see the image.

Bottle Liquid Scanner (BLS): BLS's are hand-held or table-top devices which are used to discriminate explosive or flammable liquids from common, benign liquids carried by passengers. BLS's were introduced because X-ray systems were unable to distinguish liquid explosives from common liquids. The devices analyse substances within a container, measuring particular characteristics of the content's and distinguishing between benign and hazardous liquids in a matter of seconds.

Chemical Analysis Devices (CAD): CADs are portable systems that can be used to identify a range of chemical agents and explosives threats. These devices are used to assess suspicious substances in the possession of passengers travelling through security checkpoints.

Explosive Trace Detectors (ETD): They are used to examine articles, analysing their content for the presence of potential explosive residue explosives residue. A swab is used to collect samples, which are then analysed for traces of explosives residue. The first joint meeting of the International Explosives Technical Commission (IETC) and the Ad Hoc Group of Specialists on the Detection of Explosives (AH/DE) reviewed progress made in testing, implementing and deploying advanced security screening technologies, including body scanners. The explosives experts concluded that trace detection technology continues to play an important role in airport screening and noted that further research to validate when and how this technology can be used for air cargo is underway in many States.

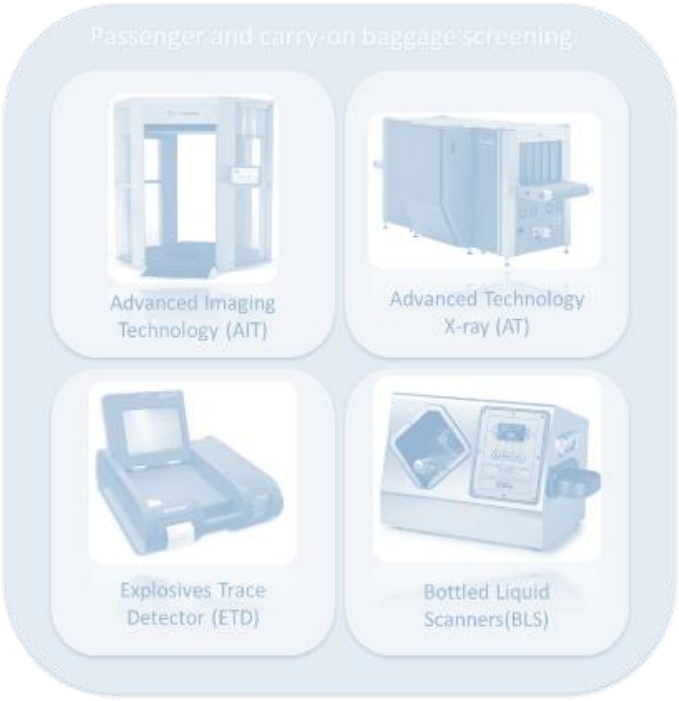


Figure 5.68 - Security technologies in 2010.

The common ICAO, AITA and ACI workshop on the next generation screening process for passengers and cabin baggage in Geneva in 2010 in collaboration reviewed planned and ongoing initiatives for developing a "**checkpoint of the future**" that will improve passenger flow as well as provide effective security. In particular, it examined how certain elements, such as the use of passenger data for identifying high-risk passengers, might be incorporated in the screening process. The Declaration on Aviation Security urged the Member States to increase cooperation to ensure the early detection of threats and dissemination of information on threats to civil aviation. Collection and transmission of advance passenger information (API) and passenger name record (PNR) data are recognised as facilitators while acknowledging the importance of protecting passengers' privacy. In 2010 more than 180 States had issued machine-readable passports (MRPs) in conformity with ICAO specifications by 1 April 2010, and another five States achieved compliance by year's end.

Progress Up-to-Now

Since 2010, there have been advances in passenger and baggage screening through the development of new technologies and the improvement of the processes. Firstly, there have been enhancing in existing checkpoint and checked baggage screening technologies, such as Advanced Imaging Technology, Advanced Technology X-Ray, Enhanced Metal Detectors, Explosives Detection Systems, and Explosives Trace Detection to increase detection capabilities and efficiencies. However, traditional threats to aviation security remain and new types of threats are emerging. As a result, passenger and baggage screening must adapt to face evolving threats and changes. For that reason, in addition to enhancing existing technologies, it has invested in new technologies such as automation and the use of risk-based

algorithms to screen passenger more efficiently and quicker. Through this type of initiatives which are currently in development, security and overall traveller experience are improved, by expediting physical screening for passengers who are considered the lower risk to aviation security.

The existing technologies which have been updated and enhanced are the following ones:

- **Advanced Imaging Technology:** This technology allows to screen safely passengers for metallic and non-metallic items, such as weapons, explosives and other objects concealed under layers of clothing. There have been improvements in this technology since 2010, for example, images with more quality, enhanced detection capabilities and false alarms rates reduced. However, there are still some airports that do not have this technology deployed, which can be considered a system vulnerability because these airports can be used as entry points.
- **Advanced Technology X-Ray**: These systems detect threats in carry-on baggage, by providing a high definition x-ray image of its content. This technology is deployed in most airports. Enhancements in Advanced Technology X-Ray include updating software or adding an infrared operator sensor and a queuing conveyor.
- **Boarding Pass Scanners:** a new technology that allows reading two-dimensional barcodes located on boarding passes. These systems reduce the need for manual verification of boarding passes and also validates the authenticity of the passenger's boarding pass at the security checkpoints using bar code readers and encryption techniques. The system temporarily captures and displays the photograph from the passenger's ID, helping security officers to compare the photo of the person carrying the ID. If the encoded data on the passenger's ID match with the data on the boarding pass, the passengers are allowed to fly.
- **Bottled Liquids Scanners**: they can discriminate explosives or flammable liquids from common, benign liquids carried by passengers. Efforts are dedicated to developing capabilities that detect a broader range of threats, enable the screening of opaque containers, and detect smaller quantities of liquid explosives.
- **Enhanced Metal Detectors:** these devices are used for locating potential metallic threats on a person where Advanced Imaging technology is not deployed. Some advances in this technology are intended to improve threat detection and discrimination capabilities, assuring at the same time passengers' privacy and dignity.
- **Explosives Trace Detectors:** the detection capability of these devices has been enhanced, allowing better operational performance and the ability to detect new threats. They are employed in checkpoint and checked baggage screening for traces of explosives. Transportation security officers swab a piece of carry-on or checked baggage, or a passenger's hands, and then place the swab inside the unit to analyse it for the presence of potential explosive residue.

Passenger screening statistics

Thanks to the technological improvements in passenger screening developed in recent years, the number of passengers screened has improved as it can be seen in Figure 5.69:

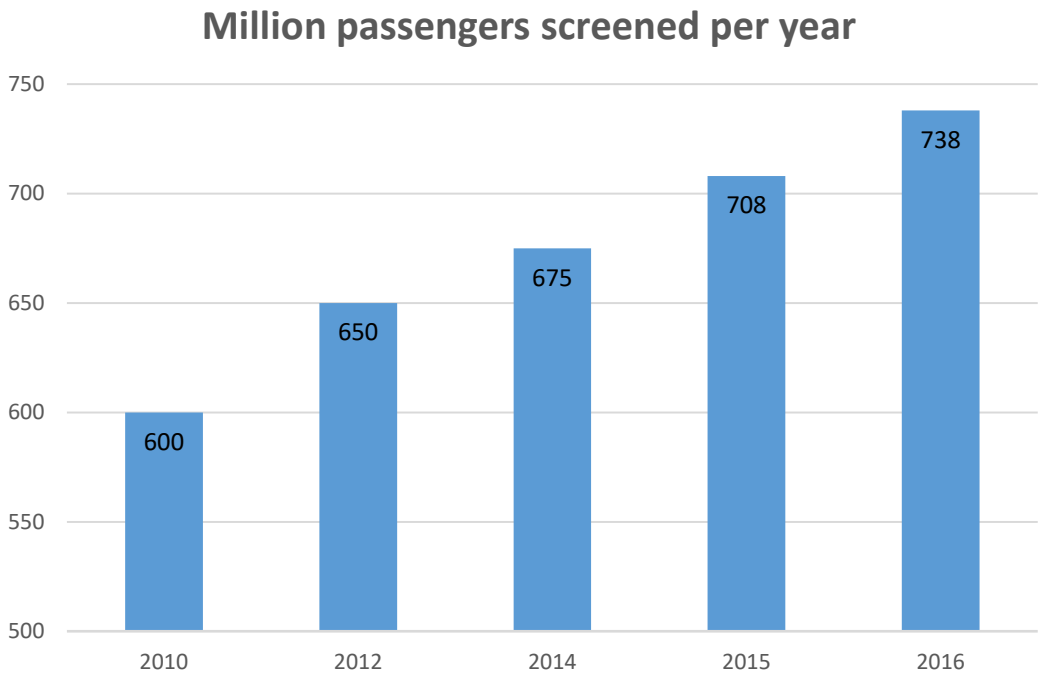


Figure 5.69 - Million passengers screened according to TSA statistics

In addition, baggage screening has also improved from 432 million checked bags in 2015 to 466 million checked bags in 2016.

KEY TOPIC T5.4 – EXPANDED USE OF PROTECTED COMMUNICATIONS

Scope of the Goal

High –bandwidth data resilient to cyberattacks		
<u>Goal 19:</u> The air transport system has fully secured global high bandwidth data network, hardened and resilient by design to cyber-attacks		
Comparison with 2017 SRIA document	Why	Lacks

Coherent	In both documents, it is pointed out that one of the main concerns in the future will be cybersecurity. In addition, technological advances may also introduce new vulnerabilities. Therefore, it will be required an aviation system that is resilient by design to the possible attacks.	Security must be supported by intelligence that provides the information necessary to develop a comprehensive and detailed catalogue of threats and system vulnerabilities. Tools such as a security radar or a horizon scanning will be needed to automate the detection of aviation incidents, a gathering of associated information, and forensic analysis.

Table 5.4 – SRIA Targets for cyber-resilience

Benchmarks

Cyber-attacks on the aviation industry are becoming a matter of concern. The 2012 report by the British Centre for the Protection of National Infrastructure (CPNI) highlighted that the interface and interdependence inherent to ICT-use has raised the vulnerability of aircraft and aviation systems. This is because the aviation encompasses one of the most integrated and complex information and communications technology (ICT) systems from the development and construction of aircraft to communications and navigation instruments, along with all the thousands of connections that link the various parts of an airport.

As in other fields, the digitalisation and placement online of such complex instrumentation have introduced considerable problems associated with cybersecurity. As a result, due to the onboard and ground computer systems, navigation systems and the use of complex data networks, cyber-attacks and data breaches are perceived to be growing threats for the aviation sector. With increasing inter-connectivity which is expected in the future, the system will be more vulnerable and exposed to multiple points of attacks. Ensuring secure aviation systems and staying ahead of the possible threats requires that the aviation sector establishes a cybersecurity culture, sets measures to strengthen the defence system and develops mitigation/prevention strategies for the threats identified.

Figure 5.70 summarizes aviation's information and communications technology (ICT) environment. Simply stated, ICT is pervasive across the aviation ecosystem, from designing and developing aircraft to flight operations, maintenance, communications, navigation, and air traffic management.

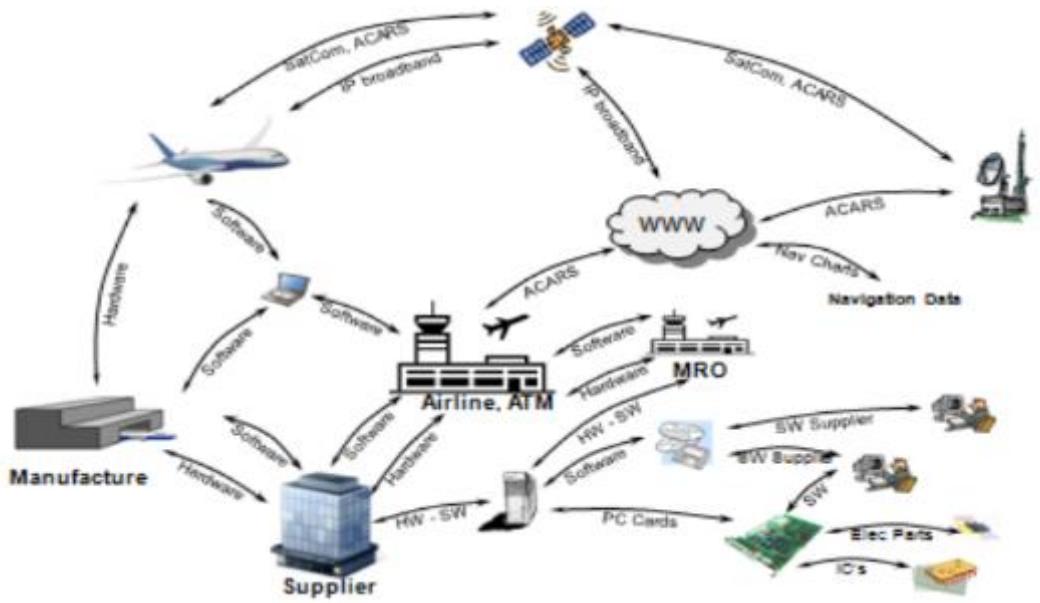


Figure 5.70 - ICT technologies in civil aviation. Source: American Institute of Aeronautics and Astronautics, A Framework for Aviation. Cybersecurity, August 2013, p. 8, http://www.aiaa.org/aviationcybersecurity.

Therefore, in order to face the future cyber-attacks, firstly, it would be necessary to identify the multiple threats that could compromise aviation security as well as to identify the systems which could be vulnerable to attacks. Then, it would be required to develop strategies in order to mitigate the threats identified. The following are some of the main threats identified in cybersecurity:

- Phishing threats: phishing is a type of security attack that attempts to obtain sensitive/valuable information such as usernames, passwords and credit card details, often for malicious reasons.
- Jamming attacks: an attacker could alter the projection and mapping of airplanes or delete their position from the radar screen. This type of attack could have serious consequences as the hackers could compromise the accuracy of data provided to the aircraft management, such as speed, location and direction of nearby airports and other planes.
- Remote hijacking: Security gaps in communication technologies used in the aviation industry could allow hackers to remotely attack/control the flight and on-board systems. Cybercriminals could attack critical systems such as flight controls, engine and fuel systems, surveillance systems, etc.
- DDoS attacks: Distributed-denial-of-service attacks are attempts to make an online service unavailable by overwhelming it with traffic from multiple sources and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system could result in a crash of the platform, thereby denying service to legitimate users or systems.

- Wi-Fi-based attacks: there are vulnerabilities in the onboard system that could allow hackers to use the on-board Wi-Fi signal or inflight entertainment system to hack into the plane's avionics equipment and disrupt or modify satellite communications.

Currently, there is no common vision, or common strategy, goals, standards, implementation models, or international policies defining cybersecurity for commercial aviation. Ensuring a secured aviation system and staying ahead of evolving ICT threats is a shared responsibility, involving governments, airlines, airports, and manufacturers. The aviation community is working on the development of a framework to offer an approach to increasing the effectiveness of cybersecurity for aviation. To achieve the 2050 goal of an air transport system **fully secured global high bandwidth data network**, **hardened and resilient by design** to cyber-attacks a triple approach is needed that encompasses the **technological, operational and societal/human dimension** of the problem as indicated in figure 5.71:

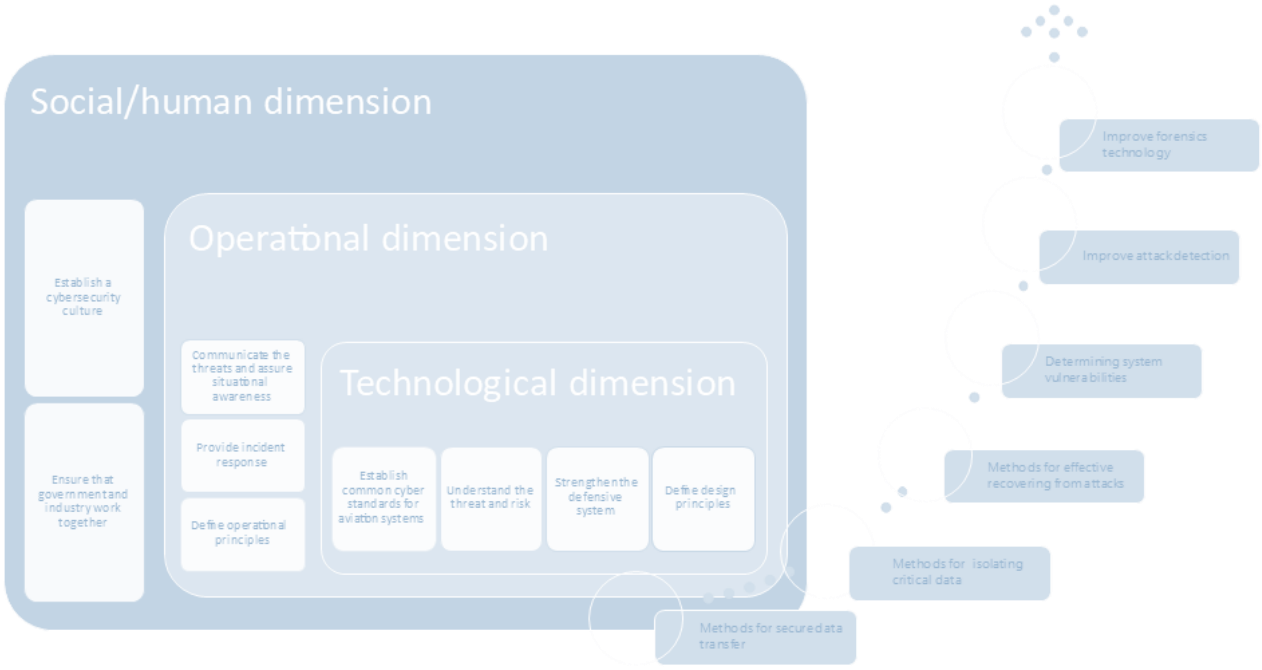


Figure 5.71 - Technological, operational and societal/human dimension of goal 19 Benchmarks

From a **technological dimension,** the following benchmarks must be achieved:

- **Establish common cyber standards for aviation systems**: Although aviation system is now one of the most complex ICT and control systems in the world, yet there is not a recognized common vision, or common strategy, goals, standards, and practices to further safeguard aviation against the evolving cyber threats. Application of common standards or practices can help provide mitigation, including against insider threats. For example, applying common encryption standards for aviation communications could reduce the risk of interference for future enhancements to the system.

- **Understand the threat and the risk** by identifying the elements of the aviation system that need protection; determining how to protect these elements with systems and standards and understanding the timeliness required for responding to threats.
- **Strengthen the defensive system** including: (1) hardening the Internet backbone, including IPS malware detection and prevention; (2) securing power sources; (3) adding public-key infrastructure (PKI) or other encryption technologies; and (4) technology and procedural upgrades to critical systems. Long-term solutions may require architectural changes to aviation's networks and control systems.

Define and agree on design principles: The internet design principles, that all nodes are known and trusted are no longer valid for aviation. Aviation must define design principles for its networks and control systems that consider the evolving nature of the cyber threat. This would include identifying architectures and design principles that help us protect our systems and platforms against known attack methods, defining quality assurance standards for critical systems, and ensuring that aviation systems are resilient against unknown threat scenarios.

From an operational dimension, the following benchmarks must be achieved:

- **Communicate the threats and assure situational awareness** by establishing a protected forum for industry and government information exchange on current and emerging cyber threats to the commercial aviation system and creating secure mechanisms to extend information exchange to the international community.
- **Provide incident response** able to provide the aviation community with a means to mitigate evolving threats.
- **Define operational principles**: These principles focus on the operational principles of systems after they are deployed in the field. This would include operational standards and best practices that mitigate threats to our systems and platforms to assure its resiliency. Items to consider would be system upgrades and patches, the timeliness of system changes, decisions on when to upgrade or retire obsolete systems, maintenance practices, access control, and personnel processes such as credentials, training, and inadvertent human errors that expose vulnerabilities that can aid an attacker.

From a **social/human dimension,** the following benchmarks must be achieved:

- **Establish a cybersecurity culture:** The same disciplined approach that created aviation's safety culture (i.e., a common vision and strategy, clear goals, common understanding, a collaborative risk-based decision-making model, non-punitive reporting structures, open communication of failures, training, etc…) must also be applied to securing cyber systems across the air transportation system.
- **Ensure that government and industry work together to coordinate national aviation cybersecurity strategies, policies, and plans. This will imply:** (1) Establish a private/public cyber partnership that includes "business continuity elements" for the aviation sector; (2) Establish policies

for the near- and long-term development for cybersecurity; (3) Define accepted international rules of behaviour; (4) Consequences for bad behaviour must be enforced; (5) Governments need to move cybersecurity to a high priority on the diplomatic agenda.

On top of that, it would be necessary to conduct necessary research and development on technical and operational assets. The aviation community, government and academia need to define and conduct necessary research and development to support the design and operational principles for enhancement to the aviation system. This would include:

1. Creating secure network architectures, including methods for maintaining secure data transfer, isolating critical data, and effectively recovering from attacks;
1. Determining system vulnerabilities;
2. Improving attack detection, and (4) improving forensics technology.

Reference State in 2010

In 2010 aviation stakeholders start to realise the need to create a common framework for cybersecurity in aviation and start to construct a holistic approach to this problem. The current European response to this threat although considers the extension and streamline of regulation, but first focusses on understanding the risks and building a holistic, coherent, affordable and adaptable response, and then establishing mitigating measures. The most relevant initiatives at that moment are summarized hereafter from different perspectives.

A. Legislative and Regulatory Developments

- ICAO

ICAO's Annex 17 to the Convention on International Civil Aviation, Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference, sets minimum standards for aviation security worldwide and creates a global policy and legal framework. ICAO Aviation Security Manual (Doc 8973) provides guidance, including on minimum measures to protect critical information systems against unauthorised access and use. In 2010 Annex 17 was updated and strengthened to reflect the mayor risk and concerns to aviation, in particular cyber threats. In 2012 a new Annex 17 Recommended Practice 4.9 recognizes cyber- attacks as a distinct threat to the aviation industry that needs attention.

In 2010 ICAO finalized a **new comprehensive strategy for enhancing aviation security worldwide (ICASS ICAO Comprehensive Aviation Security Strategy)** that recognize cyber-attacks on aviation systems, including Air Traffic Management systems as a new and evolving threat to aviation. The **Diplomatic Conference on Aviation Security**, held in Beijing from 30 August to 10 September 2010 **criminalizing the act of cyberattack on air navigation facilities.**

- The Digital Agenda for Europe

The European Commission launched in March 2010 the Europe 2020 Strategy 1 to exit the crisis and prepare the EU economy for the challenges of the next decade. Europe 2020 sets out a vision to achieve high levels of employment, a low carbon economy, productivity and social cohesion, to be implemented through concrete actions at EU and national levels. The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of Information and Communication Technologies (ICT) will have to play if Europe wants to succeed in its ambitions for 2020.

In the Digital Agenda for Europe, the Commission committed itself to **establish a CERT for the EU institutions,** as part of the EU's commitment to a reinforced and high-level EU Networking and Information Security Policy in Europe. In August 2010 the Commission requested four cyber-security experts known as the "Rat der IT Weisen" to make recommendations on how to set up such a CERT. Their report was finalised in November 2010.

The Digital Agenda also calls on all Member States to establish their own CERTs, paving the way to an EU-wide network of national and governmental Computer Emergency Response Teams by 2012 (see IP/11/395). The EU's Council of Telecoms Ministers adopted conclusions on 27th May 2011, confirming this objective.

AT the Digital Agenda Commission also committed to:

- Present in 2010 measures aiming at a reinforced and high-level Network and Information Security Policy, including legislative initiatives such as a **modernised European Network and Information Security Agency (ENISA)**, and measures allowing faster reactions in the event of cyber-attacks, including a CERT for the EU institutions;
- **Present measures, including legislative initiatives**, **to combat cyber-attacks against information systems by 2010**, and related rules on jurisdiction in cyberspace at European and international levels by 2013.

B. Standardisation Activities

- ECAC

ECAC Study Group on Cyber Threats to Civil Aviation was settled in 2009. Since then it has been recognised their valuable contribution on Cybersecurity in Aviation, notably the works of its Study Group on Cyber Security in Civil Aviation, including the updated **ECAC Doc 30**; as well as its **Vulnerability assessments on cybersecurity** since 2011.

The Group has also achieved international outreach with provisions on cybersecurity in ICAO Annex 17, sharing of information with ICAO and common Europe-USA paper at ICAO Assembly.

C. Services

- CERT-EU

After a pilot phase of one year and a successful assessment by its constituency and its peers, the EU Institutions have decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies **on September 11th, 2012**. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, and Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies. CERT-EU will gradually extend its services, based on the requirements of its constituency and taking into account the available competencies, resources and partnerships.

In recent years, CERTs have been developed in both private and public sectors as small teams of cyber-experts connected to the internet that can effectively and efficiently respond to information security incidents and cyber threats, often on a 24-hours a day-7days a week basis.

Progress Up-to-Now

Aviation cyber-security is a fast-moving topic and a very dynamic area with strong political and technical involvement by many players. As a consequence, the last years have seen many developments in this domain, proposed and actual. Latest developments in terms of legislative and regulatory changes, standardisation activities, pan-European research and development, etc. are updated and summarised hereafter. However, the dynamism of this area makes the shelf life of any analysis limited. The most relevant initiatives until now are summarized hereafter from different perspectives.

A. Legislative and Regulatory Development

- ICAO

The last updates of ICAO's Annex 17 and ICAO Aviation Security Manual regarding cybersecurity were in 2014.

The 39th ICAO Assembly, held in September/October 2016, included (item 16) a progress report on the global aviation security policy framework and implementation of the ICAO Comprehensive Aviation Security Strategy (ICASS), including developments in risk assessment, innovation and cyber-security. Cyber-security was also expected to be addressed in other relevant items, such as RPAS (Item 33). The General Assembly passed a high-level resolution on cyber.

The Working Group on Threat and Risk has added cyber-security to the Risk Context Statement which should be used by all ICAO members to inform their national risk assessments. This includes a specific risk matrix for ATM.

- FAA

FAA has revised its cybersecurity strategy recently. The five components of the strategy include – improved governance model, continued improvements to the protection and defence of the FAA mission, data-driven risk management approaches applied to cyber, focus on building a cyber workforce and enhanced collaboration with external partners. The regulatory side of FAA is targeting its improvements

via a **program named Aircraft Systems Information Security/Protection (ASISP)** – examining potential gaps and improvements via a risk-based framework.

For ATM systems, the FAA is currently focused on cyber resilience and has an active effort underway to characterize threats to the mission (service threads vs. individual systems). This effort will create and maintain a **National Airspace level threat model** to help FAA prioritize its cyber-related activities investments. FAA has also ramped up its operational exercises to include more realistic scenarios and has increased its participation in national-level cyber exercises. To this end, a **cyber-test facility was established in 2015** to facilitate more comprehensive tests and exercises.

- European Union

The **General Data Protection Regulation (EU) 2016/679 (GDPR)** applies to personal data and imposes additional legal obligations on data processors, stipulates that Data Protection Impact Assessments and risk assessment and mitigation, along with prior approval of the DPA for high risks. Data protection law is extended to all foreign companies processing data of EU residents, and a single set of rules is introduced for all EU Member States.

In July 2016 the **Network and Information Security (NIS) Directive (2016/1148)** was adopted, establishing minimum standards for the Member States and operators of critical national infrastructure. It implies risks assessment and adoption of appropriate measures to ensure a secure and trustworthy environment; mandatory reporting of any incident seriously compromising the networks and information systems. Member States shall establish effective Computer Emergency Response Teams (CERT) and designate one or more competent authorities, which will be part of a secure European-wide electronic data interchange network to allow the sharing of cybersecurity-related information especially, for incident reporting.

In **October 2016, a new unit (A5) in DG MOVE dealing with all security aspects in transport has been established** integrated Maritime Security (former A4) and Aviation Security (former A2).

- EASA

In November **2015 EASA has developed a Cybersecurity Roadmap** that identified 4 main objectives: Situational Awareness, Readiness & Resilience, Reactiveness, and Cyber-Security Promotion. Since then, EASA is working on its implementation and a number of initiatives to better address cybersecurity risks in aviation improving resilience and fostering built-in security:

- EASA has been tasked to facilitate a **Strategic European Coordination Platform** including representatives of key industry stakeholders, Member States and EU Institutions.
- EASA is supporting the creation of **a European Centre for Cybersecurity in Aviation** (ECCSA) and providing the initial operational capabilities in collaboration with CERT-EU, to promote voluntary information sharing and expert collaboration.

- EASA is undertaking a **gap analysis of all Implementing Rules.** These are started to identify areas of action.
- It is expected that EASA will release a **Notice of Proposed Amendment (NPA) for a single, horizontal rule by the end of 2017.** This will be followed by an opinion sent to the European Commission by the end of 2018, and a rule in force by the end of 2019.
- **Negotiations on the EASA Basic Regulation** is on-going and it might give EASA the competency to address cyber-security although it is noteworthy that the European Council proposal does not address cyber-security and the Parliament proposal considers cyber-security as one additional source of concern for Safety
- **EASA has also joined the FAA in the information-security Aviation Rulemaking Advisory Committee (ARAC**). The FAA tasks the ARAC to provide advice and recommendations concerning a full range of aviation-related issues, in this case, information/cyber-security. However, this is focused on aircraft cyber-security and does not address ATM, since in the US ATM systems are of federal interest only.

➢ High-Level Conference Cybersecurity in Civil Aviation Krakow 8-9 November 2017

The Conference discussed the progress achieved for aviation ground systems, including institutional set-up, legislation advancement, risk assessment methodology, cybersecurity promotion, research activities, commitments and resources devoted to cybersecurity. All this in order to establish a ground for the future European strategy for Cybersecurity in Aviation and the Cybersecurity Road Map that will define the future actions that have to be undertaken at European level to ensure a secure environment for aviation covering the cyber-space.

B. Standardisation Activities

➢ CEN

It has published in 2014, **EN 16495** Information security for organisations supporting civil defining guidelines and general principles, structured in line with ISO 27002, for the implementation of an information security management system.

➢ EUROCAE

The Eurocae sub-group from WG-72 (Aeronautical Information Systems Security) is producing a **Process Specification for the security accreditation of ATM systems** throughout the lifecycle of data exchanged between aircraft and ATM systems: this includes the creation, origination, storage, transmission, processing and decommissioning of data. It will address the design of a security

accreditation method for ground ATM systems analogous to airworthiness certification. The scope will have a broad approach focusing on safety, operational and economic impact.

- ECAC

An **ECAC Study Group on Cyber Threats to Civil Aviation is updating Document 30 ('Doc. 30') to better address cyber-risks**. Doc. 30 builds upon ICAO Annex 17 and can define higher standards. Amendments to the overarching principles in Chapter 14, and prescriptive annexes, as well as supporting guidance material are expected to be developed and included within the **ECAC Aviation Security Handbook** within the next couple of years.

- Industry High-Level Group (IHLG)

In **2014**, ICAO, ACI, CANSO, IATA and the International Coordinating Council of Aerospace Industry Associations (ICCAIA) signed a **Civil Aviation Cybersecurity Action Plan** aimed at more effective coordination across all stakeholders to effectively respond to cyber challenges. Since then there has been progress with:

- **Sharing of best practices**: IHLG organisations have identified key practices and guidance, to be held on an ICAO-based dedicated cybersecurity web-page. There is a recognition that specific guidance for different entities may be appropriate, with overarching guidance at the ICAO level (drawing on international standards such as ISO/IEC 27002).
- **Developing a common set of terms:** The IHLG identified a number of existing glossaries and have facilitated sharing those among the aviation community through the cyber portal established by ICAO.
- **Preparing civil aviation against future challenges:** The IHLG agreed on a common set of key messages such that a consistent view could be presented publicly. Many efforts were also made to promote the cyber-security topic as a priority.
- **Proposing a declaration for the ICAO 39th Assembly**: The IHLG proposed a declaration intended to consolidate and align cyber-related policy statements and directions to facilitate defining the general objective. This was scheduled for the end of September 2016.

- ACI World Cybersecurity Task Force (2015)

The Task Force was initially set up with the focus of enhancing cyber-security information-sharing between airports and industry partners; educating airport management and information technology staff on cyber-security issues; representing ACI's interests with other organisations who are also

concerned with the growing risks posed by cyber-terrorism in the air transport industry. The task force has also developed the **IT Airport Cybersecurity Benchmark**, a web-based system addressing the specific information security needs of the airport community. It is aligned to ISO/IEC 27002 controls.

- ASD Civil Aviation Cyber Security Task Force

The **Task Force was launched in October 2015 with** the goals of developing an ASD position on civil aviation cyber-security and coordinating ASD inputs to external bodies on the subject. International work has been through the ICCAIA and has contributed to ICAO's Assembly and AVSEC Panel, including the IHLG declaration (see above). European work to-date has centred on coordinating with and providing input to, EASA (especially on the Basic Regulation and cyber-security roadmap) and ECAC. High-level objectives for the manufacturing industry and for operators have been developed. The Task Force was set up as a temporary entity so in autumn 2016 decisions will be taken on whether to extend and on any future work programme.

- CANSO ATM Security Working Group

CANSO has an ATM Security Working Group (ASWG) that address all aspects of security, including cyber-security. The third ASWG meeting was held in December 2015. A working paper on cyber-security was presented to the fifth ICAO EURNAT EUR/NAT Aviation Security Group (ENAVSECG) in May 2016. Ongoing activities within CANSO Vision 2020+ include:

- Security promotion, awareness and Just Culture
- ATM security human factors in the whole ATM lifecycle
- Identification of Security standards and best practices applicable to ATM environment in the light of sustainability and regulatory compliance
- Audit and oversight issues
- ADS-B Working Group activities for secure surveillance

2016 has also seen cooperation between CANSO and NEASCOG (NATO-EUROCONTROL Security Coordination Group).

In 2017 CANSO and EUROCAE commit on the joint development of aviation industry standards, with particular focus on ATM, USAS and Cybersecurity.

C. Functions and Services

- European Centre for Cyber Security in Aviation

One of the enablers identified in the EASA Cyber-Security in Aviation project and roadmap is the European **Centre for Cyber Security in Aviation (ECCSA).** CCSA's mission is to provide information and assistance to European aviation manufacturers, airlines, maintenance organizations, air navigation service providers, etc. in order to protect the critical elements of the system such as aircraft, navigation and surveillance systems, datalinks, airports, etc. ECCSA will cover the full spectrum of aviation. ECCSA's

capabilities will be rolled out with a stepped approach, providing during the first implementation phase, 2017 – 2018, the following services:

- A public website reporting cybersecurity news and ECCSA initiatives,
- Open Source Intelligence services for members,
- A collaboration platform for members to exchange sectorial cybersecurity information.

➢ Aviation-ISAC

The Aviation Information Sharing and Analysis Centre (A-ISAC) is a US / Boeing led membership group for relevant security information sharing for the aviation sector. It combines both industry and government participants to share timely and actionable information pertaining to threats, vulnerabilities, incidents, etc. In addition, it aims to foster cooperation and provide best practices and educational awareness. Membership is open to European organisations, and Airbus will be an "anchor" member to address European issues and engagement with the government when needed.

➢ EU-Aviation ISAC (EA ISAC)

A similar initiative to the Aviation-ISAC has been proposed by Airbus and Lufthansa, with informal discussions considering its formal launch. Discussions between the US and European efforts on potential collaboration are ongoing with a meeting held in September 2016 on the Aviation-ISAC's European strategy. NDA and MoU are being drafted to frame the EA-ISAC activities.

D. Research and Development Activities

Civil aviation cybersecurity research and development activities are currently fragmented across national and EU funding sources. The latest High-level conference on cybersecurity in civil aviation has suggested EU institutions to ensure a high level of priority of aviation-relevant subjects in the next Research Framework Programme (FP9).

These different perspectives must be coherent and complementary: civil aviation cybersecurity must be fully integrated with the EU Research agenda in order to increase efforts to develop technologies and competencies at the European level.

A more coordinated research and development work programme need to be implemented with short-term flexible research activities. EU commitment should serve for development activities to improve the safe operation of the civil aviation transport system, whilst research and development activities for business continuity could remain within the existing funding instruments. As part of this strategic vision and master plan, EASA needs to be involved to ensure there is a good link between science, innovation development, deployment and policy.

➢ European ATM Master Plan

The 2015 Edition of the Master Plan makes explicit reference to cyber-risks to ATM. A risk identified within the Master Plan is that the deployment of SESAR solutions leads to unaddressed cyber-security vulnerabilities. The mitigations identified were to (a) ensure efforts on ATM cyber-security are coordinated and assess policy options for strengthening cyber-security and resilience, and (b) establish principles and processes for ensuring cybersecurity and resilience are included appropriately within the SESAR R&D work programme.

The draft 2016 Deployment Programme both refines the specific Families related to SWIM cyber-security and reports on the identified cyber-security requirements to be considered in the deployment of each Family, having specific regard to the potential cyber-threats linked to the increased connectivity associated to the full PCP deployment. The SDM is of the opinion that some components of some families are particularly exposed to cyber-security risks and that stakeholders should take appropriate action to mitigate them. The Commission also requested to the SESAR Deployment Manager to consider cyber-security requirements at the project level in the Deployment Programme by proposing guidance material.

- SESAR 2020

The SESAR 2020 multi-annual work programme identified cyber-security as a research topic to address. PJ19 (Content Integration) coordinates cyber-security activities and guidance provided across all projects, by the appointment of Security/Cyber-Security ATM Focal points in each project. Each SESAR solution shall develop a security case to demonstrate that self-protection and collaborative support has been correctly addressed. As part of this, projects will undertake security risk assessments and identify resulting security requirements – both include the cyber dimension. SESAR has developed a study on the research and development (R&D) needed to ensure ATM cybersecurity that sets out the elements needed to introduce a holistic approach to cyber-security. In addition, the SJU is currently developing a cyber-security strategy to clarify what will be delivered as part of SESAR's output regarding cyber-security and the 'securability' of SESAR solutions. It will define the responsibilities of the SJU in the frame of the whole system - and service - lifecycle. Topics such as the role of operational mitigations to system vulnerabilities are likely to be addressed. The strategy is expected to be published in Q4 2016.

- ACARE Security Sub-Group

In June 2015, at the request of the EC, a dedicated security sub-group was created within the WG/4 (Safety & Security) of the Advisory Council for Aviation Research and Innovation in Europe (ACARE). It accounts for both the evolution of technology as well as radical changes or 'technology shocks'. It has identified objectives for operators and manufacturers as well as short term, medium and long-term challenges.

- GAMMA

The Global ATM Security Management Project (GAMMA) is a European research project (2013- 2017) whose goal is to develop solutions to emerging air traffic management vulnerabilities backed up by

practical proposals for the implementation of these solutions. During 2016 the focus has moved towards translating the GAMMA concept into a set of prototypes to validate in exercises. The Security Management Platform (SMP) prototype represents the central instantiation of the GAMMA concept as it is the security information sharing platform which lies at the heart of the GAMMA proposal for managing ATM security in Europe.

- EUROCONTROL Agency Research Team (ART)

A dedicated ART Workshop on 'ATM Security and Cybersecurity' was held in Q1 2016, giving a broad overview of different areas of activities within the field.

- European PPP on Cyber Security ECS

The European Commission has signed on July 2016 a PPP with the private sector for the development of a common approach and market on cybersecurity. The Aim of this partnerships is: 1) Foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). 2) Stimulates cyber-security industry, by helping align the demand and supply sectors to allow the industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance). 3) Coordinate digital security industrial resources in Europe. The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4years). Cybersecurity market players are expected to invest three times more.

- FAA

FAA is in the process of leveraging useful research in cyber defence and resilience conducted by partner agencies in the US Federal government. The research focus areas are – cyber resilience, self-adaptive systems, data analytics for cyber, and design assurance in mixed-trust environments.

The following Figure 5.72 summarizes the progress achieved up to new in this goal.

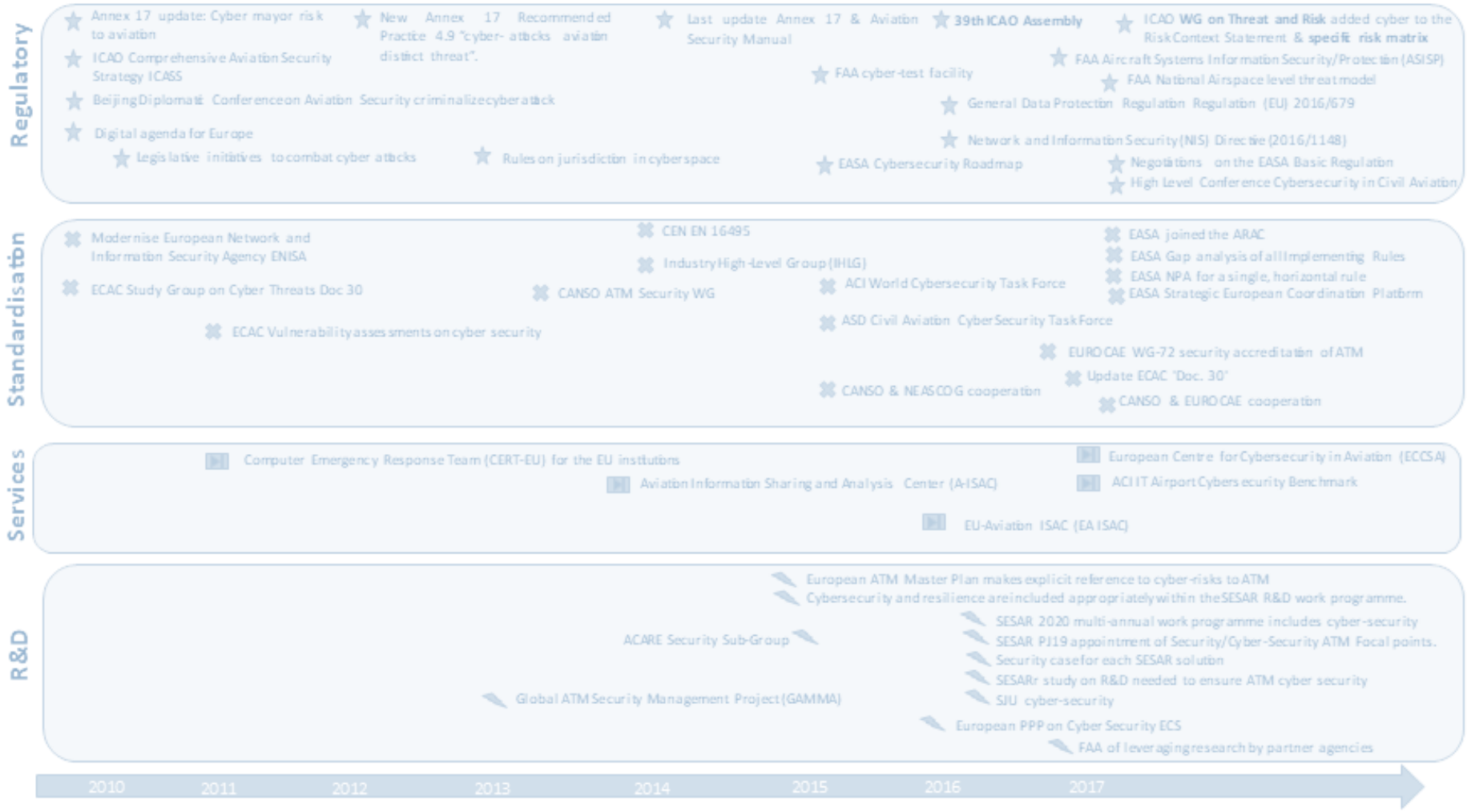


Figure 5.72 - Progress achieved up to now in goal 19.

Predictions Up-to-2025: Existing Technologies and Evolutionary Progress Up-to-2025

In the next years, the measures which are used nowadays to screen passengers and baggage are expected to be enhanced and strengthened in order to improve efficiency and security. The enhanced capabilities include the ability to detect an expanded set of threat materials with higher detection probabilities, lower false-alarm rates, and faster throughput rates, all at lower lifecycle costs, resulting in less impact to airport operations and the passengers. In addition, these advances will allow each year to screen more an increasing number of passengers and baggage per hour.

The existing technologies which will be updated and enhanced in the next years are the following ones:

- Advanced Imaging Technology;
- Advanced Technology X-Ray;
- Boarding Pass Scanners;
- Bottled Liquids Scanners;
- Enhanced Metal Detectors;
- Explosives Trace Detectors.

The main types of scanning and detection devices currently deployed by European and international airports are based on traditional X-ray technologies as well as EDS and ETD detection systems. Therefore, these technologies are developed, and their maturity level achieved is number 9. However, not all of them have been deployed in all airports. Therefore, it is still necessary to expand this technology on a global scale, especially at large airports.

As time passes, the detection capabilities of these security measures will improve as well as their efficiency. For example, in the case of baggage screening, the primary detection component is the explosives detection systems. These systems provide imaging, screening, and detection capabilities through x-ray technology to identify possible threats and create images of the bag contents.

Explosives detection systems technologies are categorised into three different groups:

- High-speed: Throughput ~ 900 bags per hour;
- Medium-speed: 400 ~Throughput < 900 bags per hour; and
- Reduced-size: 100 <Throughput< 400 bags per hour.

At this time, only reduced-size and medium-speed have been deployed while high-speed is in development. Therefore, in the short-time horizon, all the explosives detection systems will be faster, allowing higher performance.

However, despite enhances in the existing measures, it will reach a point in which these measures achieve a limit, so that it cannot be possible to increase the number of passengers screened. At that moment, it will be necessary to develop new technologies that allow an important breakthrough.

Possible or Predictable Breakthroughs: Emerging Technologies

As it was mentioned before, the existing technologies will be enhanced and updated in order to improve airport security and efficiency. However, these current measures will achieve a limit sometime, in which the number of passengers screened cannot be improved. Taking into account that during the past years the passenger flow at airports has increased significantly, it is expected that in the future that number increases. For that reason, it is necessary to evaluate new technologies and capabilities in order to maximize threat detection and efficiency. Some examples of the emerging trends in technology are the following ones:

Biometrics

One of the main emerging technologies is biometric identification, which is being considered as an alternative to traditional access control methods.

The implementation of biometrics at airports would simplify, streamline and enhance the passenger travel process, including border controls and security while reducing costs. For example, by implementing biometrics screening it could be possible to remove the hassle of checking identification documents for both travellers and airport security personnel, instead of carrying all the documents to pass through airport security (ticket, passport, etc.).

Traditionally, there are two ways to authenticate that a person is who that person claims to be: 1) by something one knows (a password, a PIN); 2) and by something one has (a key, an ID card, a token); and 3) by something that one is (a biometric, such as a fingerprint). Items such as keys and PINs can be compromised, and, for that reason, a new identification method arises like biometric identification, such as a fingerprint. Biometric represents the most secure and convenient authentication tool because it cannot be borrowed, stolen, or forgotten.

Biometric identification is a technology that verifies a person's identity through his or her fingerprints, facial features or other physical characteristics. However, before the ability to access authentication systems is granted to a person, that person's data must be pre-recorded, or "enrolled" into the database. Users "enrol" by having their biometric information (fingerprint, iris pattern or face) scanned by the system.

Therefore, biometric systems use a person's unique physical characteristics to verify a person's identity. This could all be accomplished several methods that can quickly identify a person and automatically approve his or her progression through the normally onerous process of getting on an airplane:

- Biometric face recognition systems (Figure 5.73) will collect data from the users' face and store them in a database for future use. It will measure the overall structure, shape and proportion of features on the user's face such as distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth and other expressions.
- Fingerprint is the low cost and widely accepted technology. Fingerprint-based systems match passengers to their bags at check-in. Their index finger scan is then stored in the passenger register, matching it to the details on the baggage tag.

- Iris recognition systems will scan the iris in different ways. It will analyse over 200 points of the iris including rings, furrows, freckles, the corona and other characteristics. After recording data from each individual, it will save the information in a database for future use in comparing it every time a user wants access to the system.

One of biometrics technology which is used in security systems recently is DNA biometrics since it is impossible to fake this characteristic because each person's DNA is unique.

Biometric technology (Figure 5.73) has many advantages such as improved security and effectiveness, reduced fraud and password administrator costs and ease of use. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, this new technology will improve security processes at airports.

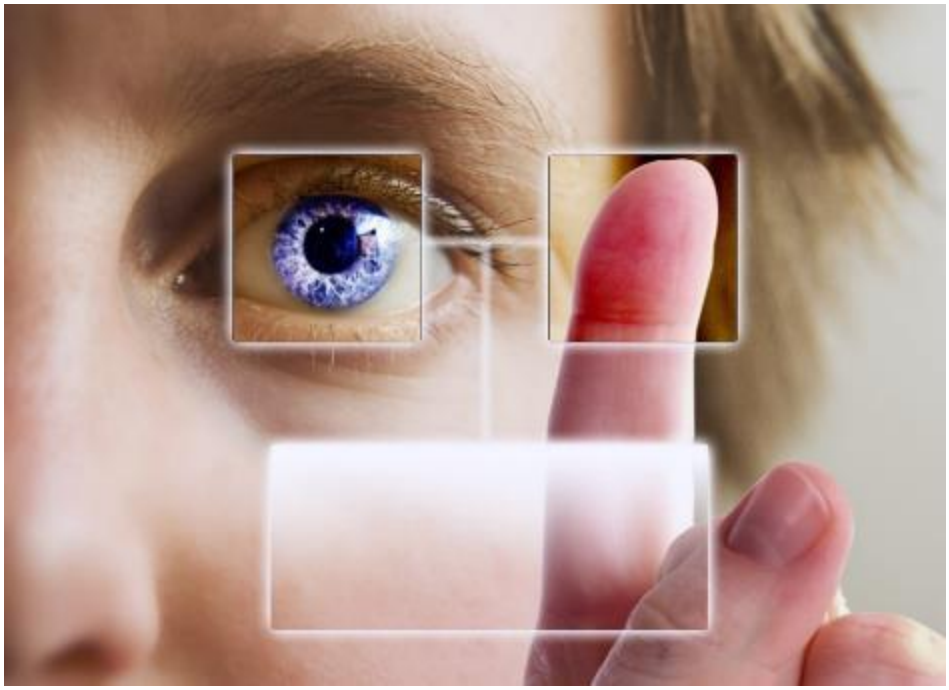


Figure 5.73 – Biometric Face recognition system

➢ CT Scanners

Another new technology that could improve airport security screening is computed tomography (CT) scanning (similar technology to what is used for scans in hospitals).

A CT scan (Figure 5.74) creates a full 3-D image by rotating a narrow band of x-rays around whatever it's inspecting, and digitally compiling the result into a multi-coloured image that gives a lot more data. The results are nuanced and detailed, and the screener can change the colours or contrast to make certain materials stand out. It could be also possible to manipulate the image with pinch and zoom gestures to get a good look from every angle.

The benefit of CT technology, in general, is that passengers could keep laptops and liquids in the bag when they reach the checkpoint.

Another difference between CT scanners and other X-ray scanner solutions is the amount of data they can collect: the conventional equipment doesn't collect as much data as CT equipment. So, a spinning source in a relatively similar amount of time will collect much more data about what it's looking at compared to a conventional X-ray, which may have just one, two or three cameras that are taking a photo.

This type of technology would provide better customer experience, in terms of shortening waiting times and allowing for faster processing through the checkpoint, while maintaining the highest levels of security.

Figure 5.74 – Computer tomography scanning creates 3-Dimension Image

Facial Scanning

Other future technologies that would improve security at airports are using facial recognition software (Figure 5.75) to identify ticketed passengers. This face-scanning technology would replace traditional boarding passes, by scanning own face and comparing it with the photo of own passport. These systems would allow video surveillance to match faces to a database of previously identified individuals.

However, there is some concern about how accurate these new procedures will be. Apparently, facial recognition technology doesn't recognize all people will the same accuracy. White women and black people aren't as easily recognized as white men, meaning there could be some mismatching of identities. Some are also concerned that this is crossing the line in terms of passenger privacy.

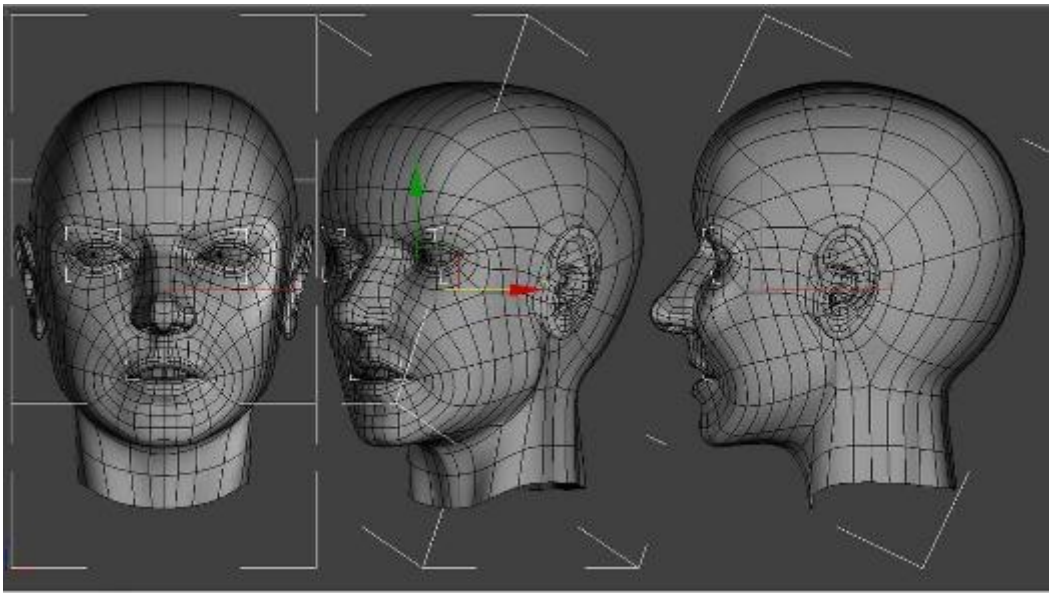


Figure 5.75 – Facial recognition software

Behavioural Analytics

Essentially, this is software that continuously scans surveillance video feeds for suspicious behaviour. These techniques focus (Figure 5.76) on analysing the passengers' intentions and emotions, instead of analysing the content of carry-ons. Speedier and less intrusive than metal detectors, these systems would improve efficiency to the airplane boarding process. Therefore, with this type of systems it could be possible to detect a person's reaction to certain stimuli by reading body temperature, heart rate and respiration signals a terrorist unwittingly emits before he plans to commit an attack.

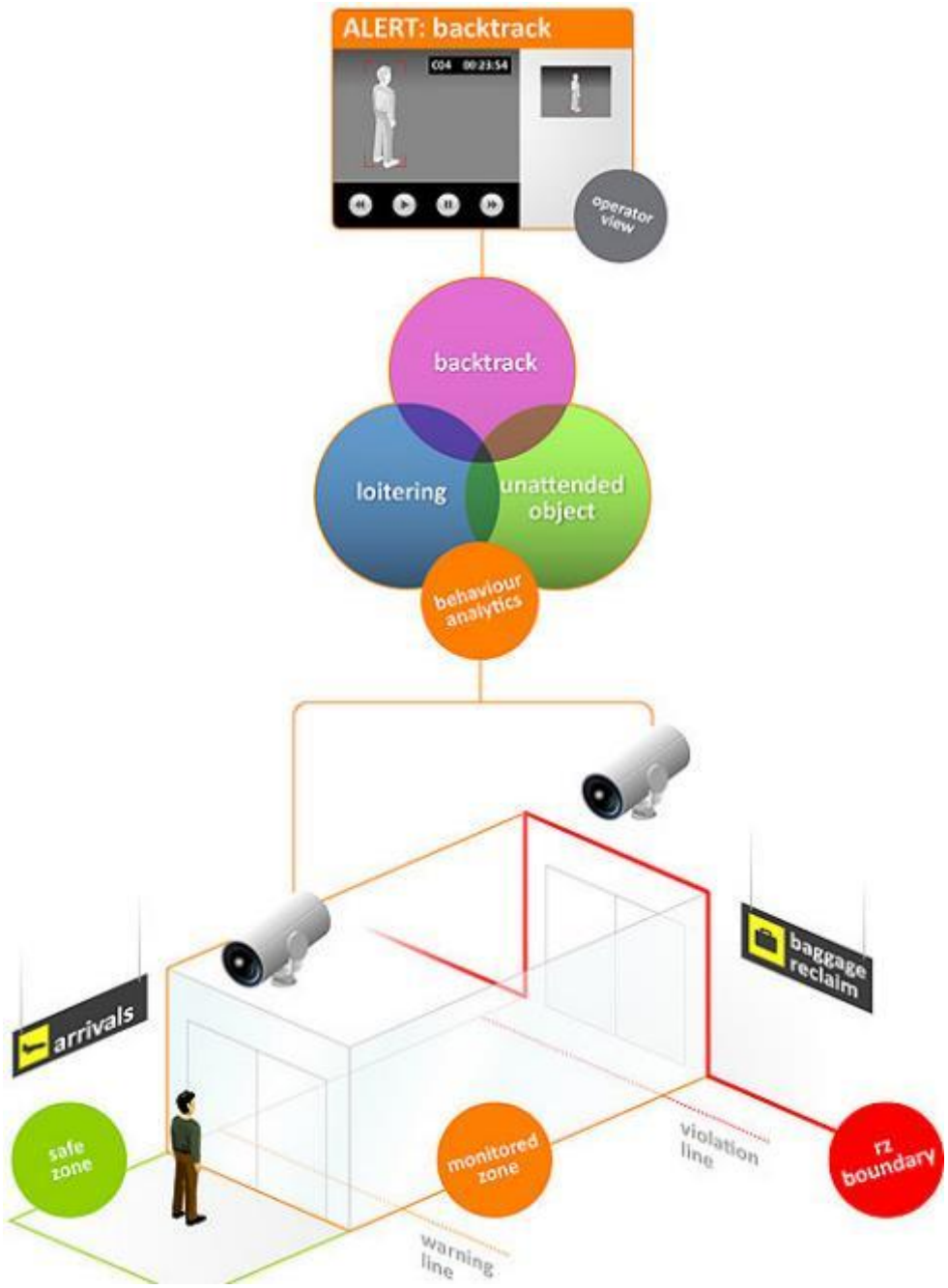


Figure 5.76 – Behavioural analytics

Integrated Security System

Airports present a particular security challenge due to their operational complexity because they are composed of a huge number of subsystems, people, technology, and interest groups involved. Due to its challenging environment, the information and data that flows in this system must be accurate, intelligent, quick, and easy to understand to make decisions and share between all the actors involved. In addition, it is necessary to develop methods to protect infrastructure, equipment, and especially passengers. One of the possible measures foreseen for the future is to create (Figure 5.77) an integrated security system, so that all the airport security systems are integrated, such as video surveillance cameras, alarm systems, intrusion detection devices, and object tracking systems, closed-

circuit television, and other sensor systems. All the data provided by these systems would improve situational awareness and enable a quick response to any emergency. In this way, the huge volumes of information provided by the several systems could be stored and shared to all actors in real-time, allowing a great increased in detection capabilities and efficiency within the airport security measures. Moreover, integration efforts will reduce the number of screening procedures required for each passenger and they will allow increasing passengers flow. The systems which are necessary to be integrated are shown in Figure 5.78:

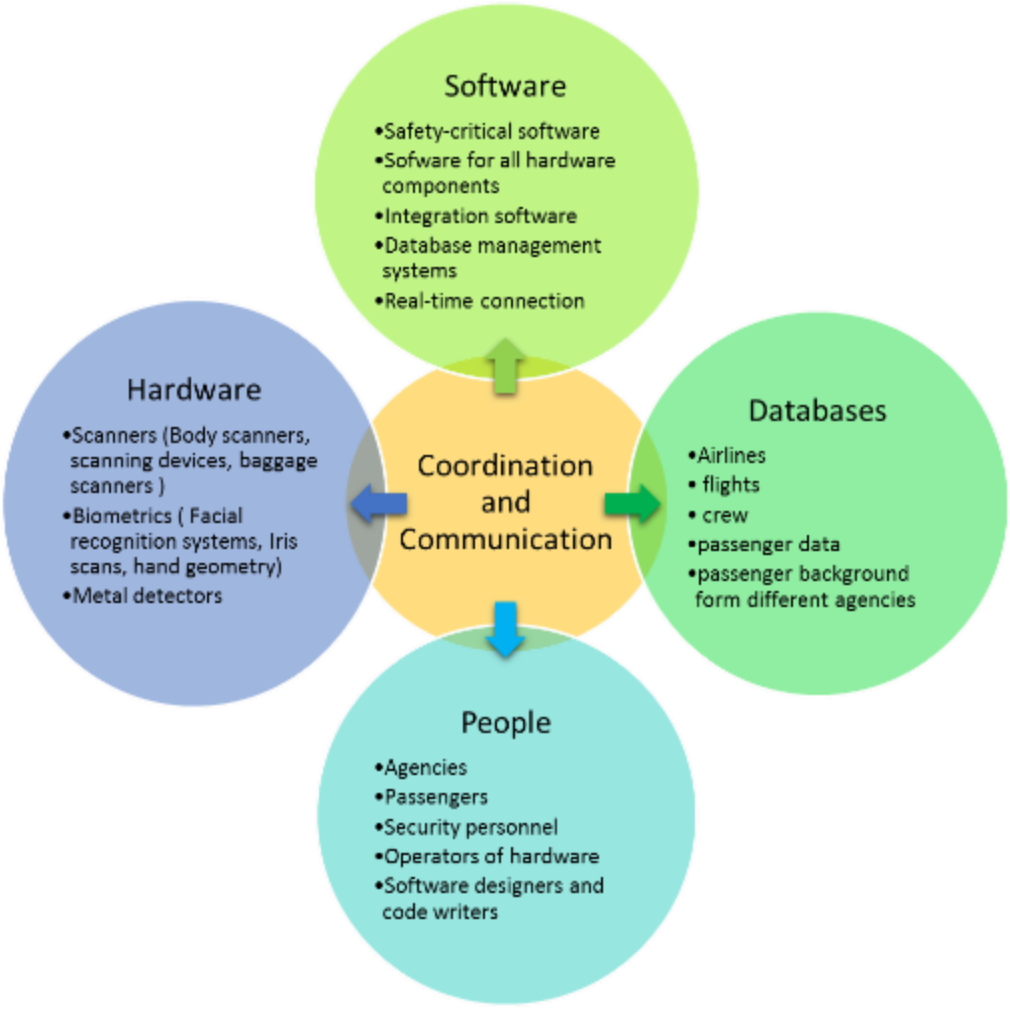


Figure 5.77 - Communication and Coordination among security subsystems, people, and all involved parties

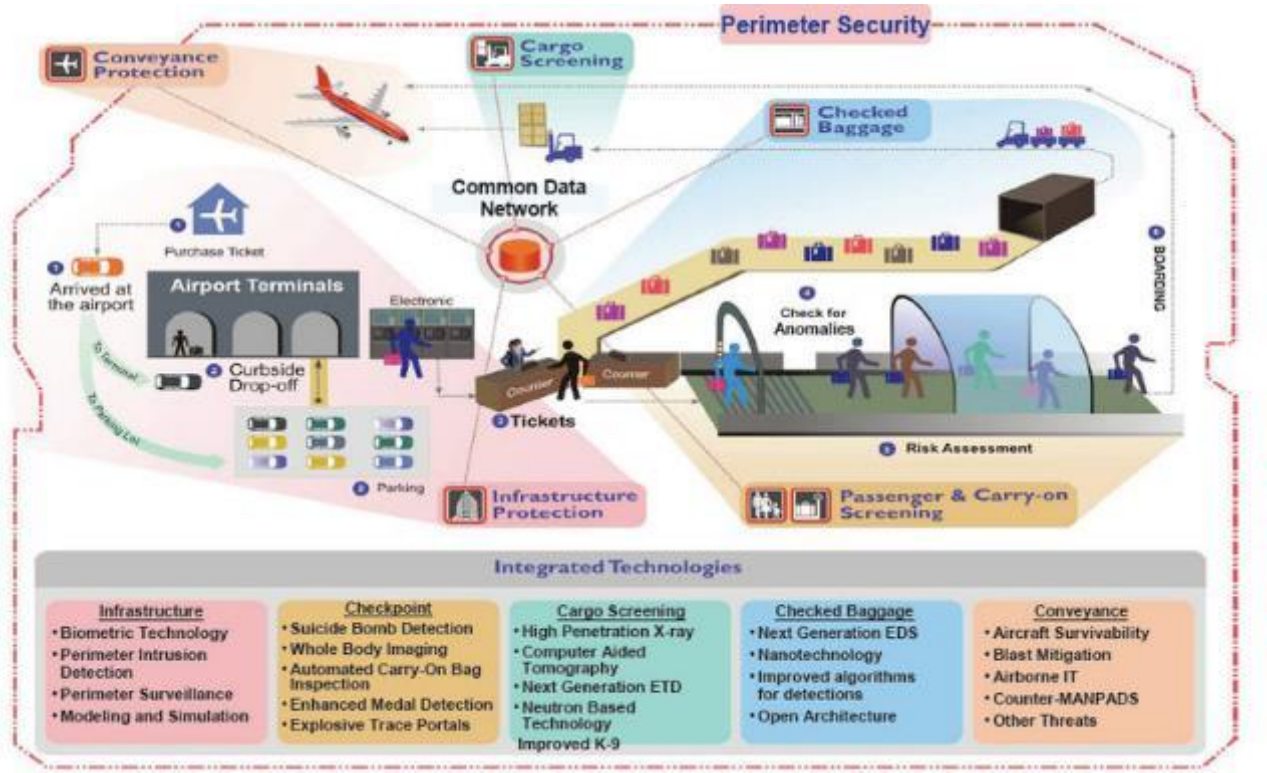


Figure 5.78 - Integrated security system

It is important to highlight that all the new technologies mentioned before are in **the first level of maturity**, since all of them are not still in development, so they are in the concept phase.

Projection and Identification of Gaps

As it was mentioned before, the existing technologies will be enhanced and updated in order to improve airport security and efficiency. However, it will reach a point in which these measures achieve a limit, in which the number of passengers screened cannot be improved. From that moment, it will be necessary to introduce new technologies and capabilities in order to maximize efficiency. Taking this into account it can be estimated the trend that this sector will follow in next years in terms of a number of passengers screened as indicated in Figure 5.78:

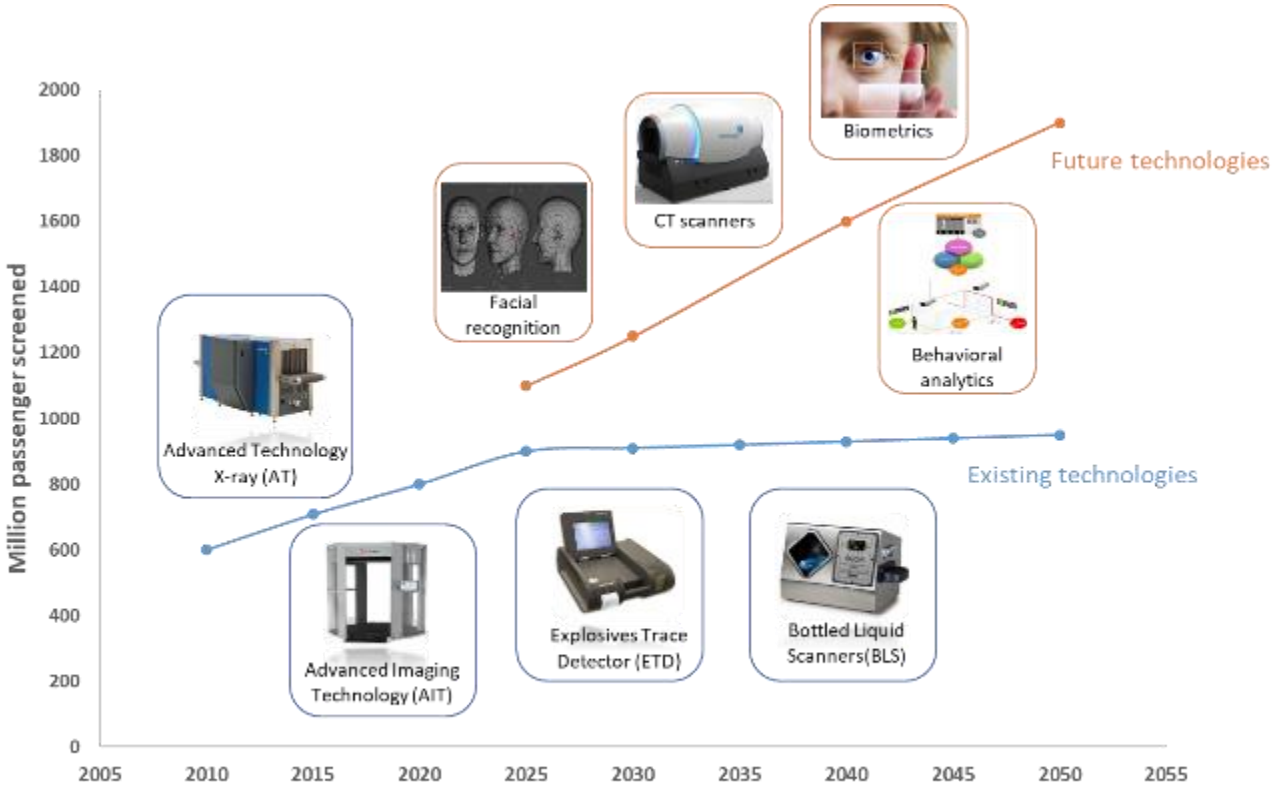


Figure 5.79 – Prediction of the growth in the number of passengers to be received at airports.

KEY TOPIC 5.5 – GUIDELINES FOR CYBER PROTECTION AND SECURITY

Reference State in 2010

The state of the art within Europe was reviewed in **Cyber Europe 2010** (**CE2010)** – the first pan-European exercise on Critical Information Infrastructure Protection. It was organized by the EU Member States, facilitated by the European Network and Information Security Agency (ENISA) and supported by the Joint Research Centre (ENISA, 2011).

The objective of the exercise was to trigger communication and collaboration between countries in Europe to try to respond to large-scale attacks. During the CYBER EUROPE 2010 exercise, experts from the participating public bodies of European countries worked together to counter simulated attempts by hackers to paralyze the Internet and critical online services across Europe.

The simulation exercise was based on a fictitious scenario on a fictitious Internet interconnection infrastructure, with a limited number of Internet Interconnection Sites (IIS1) between countries. During the exercise, Internet connectivity between European countries was gradually lost or significantly reduced, requiring cooperation between the Member States to avoid a total network crash.

The key findings of CE2010 were as follows:

- The planning phase of the CYBER EUROPE 2010 exercise benefited from the interaction among the participants, which allowed the interests and concerns of all parties to be taken into account and enabled a fruitful and highly appreciated exercise.
- The Member States should continue to work on the points of contact that were established during the exercise and to establish a solid European CIIP-network. The consolidation of trust between MS and partners should be a continuing objective.
- The exercise increased in several ways the understanding of how cyber incidents are handled, both on a European level (between the Member States) and a national level (between players). It is, however, worth mentioning that the artificiality of the scenario limited this scope of understanding to a certain extent. A more realistic scenario could lead to a deeper insight of how cyber incidents are handled.
- The exercise accentuated the necessity to be able to establish and locate relevant points of contact within Europe. Since each country is organized differently, it is very important to know who to contact in case of an incident or, more generally, who is able to answer a specific question.
- The exercise demonstrated the need for efficient communications, leading not only to greater understanding but also illustrating the differences in structure between the Member States. How to achieve efficient communication will need more gathering of requirements and analysis work.

Progress Up to Now

A Worldwide Perspective on the Aviation Sector

With the development of new technologies such as the Internet, the global aviation industry is subject to a new and growing type of threat coming from cyberspace. As in the other industries, cyber threats purposes are for example the robbery of information, political actions, make a profit, or simply weaken one stakeholder of the industry (Duchamp et al, 2016).

The global aviation industry has many layers overseeing the safety of all the stakeholders involved, from aircraft manufacturers to the passenger boarding a flight. Overall, these different actors can be classified into 4 categories:

- One international organization: The International Civil Aviation Organization (ICAO), part of the UN. It codifies the rules of investigation internationally and designs international civil aviation Standards and Recommended Practices in collaboration with its member states.
- Governments: National investigation organizations, virtually security agencies that investigate on behalf of countries involved in the accident. France's Bureau d'Enquêtes et d'Analyses (BEA) or the USA's National Transportation Safety Board (NTSB) are the main examples of such organizations. On top of ICAO's guidelines, they may develop additional safety standards (for example, the NTSB developed smoke detectors in aircraft toilets).
- Trade organization of airlines: International Air Transport Association (IATA) oversees standards at the industry level and is directly in contact with most of the world's airlines.

- Manufacturers of aircraft and security systems: Many large corporations such as Boeing, Dassault, Thales, Honeywell, etc. They constantly update their systems to face new threats with the advice of the different boards described above.

Because of its complexity and its weight in the economy, breaking the aviation industry's security constitutes a great challenge for hackers and terrorists. Moreover, this industry relies more and more on information and communication technology (ICT). As an industry that is well known for providing one of the safest type of transportation, it is mandatory for all its stakeholders to understand the risks and to prevent any malicious events for the good of the industry, the economy, the population and the environment.

The aviation sector is not immune to the cybersecurity risks that have been critical issues for all the other industries. Modern aircraft are very complex systems that rely on many transponders to communicate their position to air traffic control. It's quite difficult to hack all systems at once, including the on-board radios and the Aircraft Communications Addressing and Reporting System (ACARS), used to send messages or information about the airplane rather than voice transmissions. Consequently, "an attacker with a deep knowledge of the plane's system could intentionally cause serious problems with its normal operation" (Paganini, 2014). Major cyber-security incidents in the aviation sector strengthen this observation, and the threat is not as recent as one might think.

In her research paper, security specialist Ruben Santamarta exposed the backdoors and remote control of SATCOM aviation radios, reaching the rather alarming conclusion that "the current status of the products [we] analysed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices" (Santamarta, 2014).

It is not just navigation systems that have been subject to cyber-attacks. An attack on the internet in 2006 forced the US Federal Aviation Administration to shut down some of its air traffic control systems in Alaska. In July 2013, an attack led to the shutdown of the passport control systems at the departure terminals at Istanbul airport, causing many flights to be delayed. Finally, an attack that possibly involved malicious hacking and phishing targeted 75 airports in the USA in 2013. These are just a few examples among many more, but they justify the needs to prevent such threats that could lead to dramatic consequences.

Communication between people and devices, the rise of computing performance, price erosion and software developments are all ingredients shared by all the industries that enhance the necessity to consider seriously the cyber threats in the aviation sector. Indeed, aviation security remains a critical topic despite all the investments and measures that have been made, especially when the examples above point out that this threat is not a new trend at all.

One of the major explanation for this new type of threat in this sector is the greater use of computer-based systems: sophisticated air navigation systems, onboard aircraft control and communication systems, airport ground systems including flight information and security screening, day-to-day data management systems.

In the same time, cyber threats have been developed regardless of the industries but in relation to technologies: computer viruses, malicious attacks, etc. Because of an increasing number of travellers, the creation of new modern airports, the introduction of more complex aircraft, the use of IT and advanced computer-based systems, the risks will increase considerably with time. In addition to this, it is important to consider the digitalization of the sector with electronic ticketing for example or the goal of reducing costs by the reduction of manpower for example.

Like any other industry, it is possible to consider two types of cybersecurity breaches:

1. "Opportunistic": the goal is to exploit mistakes made by internal users like employees using the IT systems with to causing inconvenience and nuisance to any entity involved in the aviation ecosystem.
1. "Calculated and premeditated": it concerns any malicious attacks to disrupt operations or threaten lives. This category is critical as terrorism are fully aware of the potential of technologies and cyber-attacks.

Then, like in the other industry, we can mention different factors that would influence the cybersecurity strategy:

- There are more and more interactions between people, devices and services. This increase and diversity in the interactions make the paths of attacks less and less predictable.
- Innovation and cost reduction made by the ecosystem transform non-existent or unavailable technologies into common goods. Moreover, the software is more and more used to provide effective solutions and digital experience to the workers of this industry and passengers. Consequently, this evolution exposes more and more internal and external systems to potential threats.

For example, a report from NASA (2009) highlights the rise of software complexity in all industries:

- Flight software lines of code have increased 10 times in ten years.
- From 1960 to 2000, the functionality provided by the software to pilots has grown from 8% to 80%.

Moreover, despite this new complexity, aviation systems seem not to be prepared. Indeed, since the creation of the first aviation network, the systems ran isolated and were designed more for high availability than for security.

With the rise of software complexity in the aviation sector, software security cannot be totally guaranteed. This is the reason why it is important to handle vulnerabilities in this sector, to deploy software updates to prevent any attacks and of course to test regularly the security of critical systems.

With the complexity and the high number of stakeholders in this industry, the number and the origins of breaches could be substantial. In the same way, establishing the stakeholder accountable for a breach or an attack could be difficult. Some previous cases in the aviation sector have led to some observations. For example:

- When a vulnerability or a breach is discovered, vendors do not always address or fix it;
- No stakeholder would accept to be accountable for a breach or a vulnerability: the suppliers blame each other, the main manufacturers such as Airbus or Boeing blame the suppliers, the airplane operators blame the manufacturers and so on;
- Critical systems and cabin systems on airplanes are not isolated properly from external threats
- The principal internal communication protocol, Avionics Full DupleX (AFXD), had poor security solutions implemented.

As cyber-attacks against the aviation industry have increased considerably, setting the cybersecurity as a major concern, all 4 categories of industry stakeholders as pointed out earlier worked together to address these cyber threats.

The major efforts made by these stakeholders are the following:

- With the increase of cyber-attacks in all the industries and the increase of computer-based solutions used, ICAO encourages better and stronger collaboration between all the stakeholders to identify as many threats and risks as possible.
- ICAO organized a discussion to define responsibilities on cybersecurity for the aviation industry.
- ICAO would like to encourage countries to implement a strong cybersecurity strategy and management. The goal is to implement more policies and measures to prevent any cyber-attacks that could lead to dramatic consequences. This recommendation by the ICAO includes crisis management and business resilience.
- More and more countries started to work on cybersecurity a few years ago.
- More and more airports started to implement measures to secure any IT systems already exposed. They also started to consider upstream the cybersecurity issues for future projects.
- With safety as a top priority, IATA conducts yearly audits mandated by governments and provides airlines with a cyber-security toolkit that has a traditional risk assessment approach.
- Finally, manufacturers have made some efforts as well: for instance, Boeing implemented additional security measures on the 777 aircraft to prevent onboard hacking of critical computer systems (Federal Register, 2013)

Although a lot of efforts have been made, there still exist a lot of issues to be addressed.

➢ Cyber Europe 2012

On 4 October 2012 more than 500 cyber-security professionals across Europe participated in Cyber Europe 2012, the second pan-European Cyber Exercise. The exercise built on extensive activities at both the national and European level to improve the resilience of critical information infrastructures.

As such, Cyber Europe 2012 was a milestone in the efforts to strengthen cyber-crisis cooperation, preparedness and response across Europe (ENISA, 2012).

Cyber Europe 2012 had three **objectives**:

1. Test the effectiveness and scalability of mechanisms, procedures and information flow for public authorities' cooperation in Europe.

2. Explore the cooperation between public and private stakeholders in Europe.

3. Identify gaps and challenges on how large-scale cyber-incidents could be handled more effectively in Europe.

Twenty-nine EU (European Union) and EFTA (European Free Trade Association) Member States were involved in the exercise; 25 of them participated actively in the exercise, while the other four were involved as observers. In addition, several EU Institutions participated. Following up on a key recommendation of Cyber Europe 2010, the private sector actors took part in this exercise. Cooperation between public and private players took place at the national level, while public authorities also cooperated across borders.

Cyber Europe 2012 resulted in the following **recommendations**:

• Cyber Europe 2012 proved valuable in enhancing pan-European cyber-incident management. It is therefore important to continue the efforts and further develop the European cyber exercise area. EU Member States and EFTA countries should cooperate towards new pan-European and national cyber exercises in order to enhance transnational cyber-incident management. The Good Practice Guide on National Exercises, developed by ENISA, provides additional support in this area.

• Future cyber exercises should explore inter-sectoral dependencies and be more focused on specific communities.

• Cyber Europe 2012 provided an opportunity for international-level cooperation and strengthening of the European cyber-incident management community. To foster international cooperation, it is essential to facilitate the exchange of good practices in cyber exercises, lessons learned, expertise and the organization of conferences. This will ensure a stronger community that is able to tackle transnational cyber-crises.

• EU Member States and EFTA countries should further improve the effectiveness, scalability of, and familiarity with, existing mechanisms, procedures and information flow for the cooperation of public authorities in Europe. Lessons learned from Cyber Europe 2012 provide an excellent starting point.

• All stakeholders in the area of international cyber-crisis cooperation need to be trained on the use of procedures in order to know how to adequately work with them.

• The involvement of private sector organizations as players was of added value to this exercise. Therefore, EU Member States and EFTA countries should consider the involvement of the private sector in future exercises.

• The European cyber-incident management community could be strengthened with input from other European critical sectors (e.g. health, transportation) that are relevant to the handling of large-scale crises.

- Cyber Europe 2014

In May 2014, a European-wide cyber warfare exercise - The Cyber Europe 2014 (CE2014) - was organized by the Crete-based European Union Agency for Network and Information Security (ENISA). Representatives of 200 organizations and some 400 cybersecurity professionals from all the EU member states and those in the EU Free Trade Space (ENISA, 2014).

The event was designed to simulate unrest and political crisis at a pan-European level and to test cybersecurity response across public and private sectors. The objective of this first phase was to analyse how the events escalate and de-escalate, to understand these processes at all technical, operational, and strategic levels, as well as to understand the related public affairs issues linked to cyber threats.

The exercise, however, came in for stinging criticism. The main concern was the fundamental problems of inter-governmental communication and disparate incident response standards across borders. Also, some believed that war games might have done little more than act as a communication exercise. Cross-border crises are hard to conceive especially if they are multi-sector because different sectors will have different vulnerabilities. These war games were not designed to test whether they all had defences that were up to the job of combating the latest malware, only the older recognized malware.

However, the 2014 war game was a step up from previous years with more technical demands of the participants than previously. This was a valuable exercise with as many as 16 different types of case studies, but any real attack would have surprises no-one expected, and the key question of any war game would be how to prepare for the 'unexpected'.

CE2014 demonstrated that strong cross-border cooperation was necessary for the EU member states, and the public and private sector. This kind of cooperation between the EU and EFTA countries was crucial for the strengthening of cross border, transnational cyber-incident management.

A report on CE2014 concluded with five key **findings**:

1. Cyber Europe exercises, as well as any cooperation activity at European level during real cyber crises, build upon existing relations between the Member States. ENISA and the Member States will continue to invest in trust-building activities to maintain and further develop existing trust.
1. ENISA and the Member States should further develop the operational procedures which drive the cooperation activities during a cyber crisis, taking into account existing and future cooperation frameworks, to bring these procedures to a maturity level similar to those found in other sectors such as civil protection and aviation.
2. ENISA and the Member States will seek further integration with national and regional activities.

3. ENISA will address future Cyber Europe activities as a program containing both pieces of training as well as small and large-scale exercises, in order to provide a better experience and achieve greater impact.
4. Lastly, ENISA will further develop the Cyber Exercise Platform to offer a richer experience to both players and planners, as well as to support the organization of national and regional exercises, fostering the development of a cyber exercise community.

- Cyber Europe 2016

Cyber Europe 2016 was the fourth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA). Over 1 000 participants working mostly in the ICT sector, from public and private organisations from all 28 Member States of the European Union and two from the European Free Trade Association (EFTA), joined in a programme of activities ranging from training sessions and communication checks to technical competitions and cooperation exercises. The exercise simulated a realistic crisis build-up over an actual period of 6 months, culminating in a 48 hours event on 13 and 14 October 2016 (ENISA, 2017).

Cyber Europe 2016 was based on three pillars essential to the successful mitigation of large-scale crises caused by cybersecurity incidents: cooperation at national and international levels and sound cybersecurity capabilities.

First, the exercise fostered cooperation between targets of simulated cybersecurity incidents, security providers and national authorities, shedding light on national-level public-private and private-private cooperation. Participants had to follow existing business processes, agreements, communication protocols and regulations to mitigate effectively the situations presented to them. Such mechanisms were not always in place for all participants, which hindered the overall ability to reach full EU-level situational awareness. The EU network and information security directive identifies many of the associated shortcomings and proposes measures that ENISA and the Member States are already implementing to improve the situation.

Second, Cyber Europe 2016 helped participants understand how cybersecurity authorities would cooperate with each other and EU bodies in the event of a large-scale crisis. Undoubtedly, crisis cooperation at EU level is very much maturing and improving. Most, if not all, Member States have come to realise the importance of sharing structured information across national borders. With the active support of ENISA, they have leveraged the benefits of EU-level situational awareness for their own crisis management activities. Yet despite such progress, Cyber Europe 2016 highlighted, as previous exercises did, the absence of a cooperation framework at EU level for crises stemming from cybersecurity incidents, officially endorsed cooperation procedures or a centralised hub. The creation of the EU CSIRTs Network and the European Commission initiative to publish a crisis cooperation blueprint in 2017 are excellent developments in that regard. They will surely benefit from the detailed findings in this report.

Last, the exercise offered countless opportunities for participants to enhance their cybersecurity capabilities, from their technical and operational expertise to their capacity to handle crisis communication. Organisational and individual cybersecurity preparedness and capabilities in the EU were excellent overall. Technical expertise, business continuity and crisis communications procedures were of a high standard. Nevertheless, the vision required to link technical- and operational-level response activities to strategic crisis management mechanisms was sometimes lacking, which proved detrimental to fostering crisis exit strategies supporting decision-making.

Additionally, many lessons were learned from the use of the prototype platforms developed by ENISA to support cooperation at EU level; they will reflect positively on the development of the EU-level crisis cooperation infrastructure financed by the Connecting Europe Facility (CEF).

A report on CE2016 concluded with these key **findings**:

Participating organisations responded adequately to most challenges they faced during the exercise. Cybersecurity experts employed in a wide array of sectors in the EU demonstrated high levels of expertise and appetite to resolve complex cybersecurity issues. Their ability to cooperate in the most difficult times is an important finding.

No participant questioned the essence of cyber incident cooperation at EU level. Rather, all actors focussed their efforts on lifting the remaining barriers. Such cooperation was particularly insightful and led to a full understanding of all facets of the crisis within a few hours, which supported the swift mitigation of a simulated large-scale attack against EU interests. In particular, the EU Cyber Standard Operational Procedures helped to provide EU-level situational awareness and structured cooperation activities.

The exercise in itself proved to be an excellent opportunity to increase individual and collective knowledge in the field of cybersecurity. Participants developed skills, procedures and relationships. Most importantly, they reiterated their appreciation in the exercise series: 99% indicated interest to participate in the next exercise.

Innovation and transformation were at the heart of Cyber Europe 2016. From a product, process, rhetoric and service perspectives, the exercise planning team, composed of Member States and ENISA representatives, pushed established boundaries to transform the EU cybersecurity society. The European Union Ombudsman underlined this joint effort in March 2017 with an award for excellence in innovation and transformation.

Participants repeatedly asked for more opportunities to test their technical skills regularly against a variety of advanced scenarios. Many were grateful for the multiple options offered by ENISA to involve media, legal and financial policy experts and hope for more to come as leaders across the EU realise that cybersecurity goes beyond information security.

The Cyber Crisis Cooperation Platform prototype developed by ENISA provided numerous insights into technical means supporting EU-level cooperation. These will be of paramount importance in order to ensure the buy-in from the Member States in such a cooperation platform, currently under development.

The Cyber Exercise Platform proved to be a powerful tool to plan, conduct and evaluate the exercise. In particular, the simulated environment developed by ENISA supported the crisis build-up in a realistic fashion with an unprecedented emphasis on written and visual storytelling.

Cyber Europe 2016 resulted in the following **recommendations**:

1. Following their revision, the operational procedures which drive the cooperation activities during a cyber crisis should be endorsed by the CSIRTs Network established by the Network and Information Security Directive. Training opportunities on the use of these procedures and tailored exercises should be offered regularly.

2. An EU-level cyber crisis cooperation framework is currently being developed by the European Commission. It should build upon these findings to develop interconnections between cooperation mechanisms, identify and empower key actors, from CSIRTs to law enforcement, and set a clear vision for the future of EU cyber response.

3. Future Cyber Europe should focus on cooperation activities on technical and operational topics. Other options should be pursued to offer training and exercise opportunities on a variety of other topics increasingly associated with cybersecurity. In particular, ENISA should support EU-wide capacity building on cyber crisis communication.

- Research Findings Elsewhere

Problem: despite the fact that lack of security of commercial-grade multi-million ADS-B technology has been widely covered by previous academic studies, and more recently by the hacking community, the fundamental architectural and design problems of ADS-B have never been addressed and fixed. As noted by Costin and Francillon (2012), it has been demonstrated that a low-cost hardware setup combined with moderate software effort is sufficient to induce potentially dangerous safety and operational perturbations via the exploitation of missing basic security mechanisms such as message authentication. Also, given the efforts in terms of time and money invested so far, it is unclear why such mission-critical and safety-related protocol does not have a security chapter in the main requirements specifications document.

Approach: raising awareness among the academic, industrial and policy-making sectors on the fact that critical infrastructure technologies such as ADS-B require real security in place in order to operate safely and according to the requirements.

Directions for future research: not identified

Problem: recently, as a result of the rapid increase in air traffic, the construction of the CNS/ATM next-generation ATC system has been accelerated. To ensure the safe navigation of more aircraft in limited air space, CNS/ATM has to predict accurate traffic flows on the basis of flight plans and accurate

positioning of aircraft. ADS-B is able to provide accurate navigation information, such as the location, altitude, and identification information of aircraft; consequently, it is the core technology in CNS/ATM. However, the transmission of ADS-B data between ADS-B sensor and ATC is carried out in an unencrypted (or unprotected) communication channel; therefore, it is vulnerable to security threats such as spoofing, eavesdropping, and data modification (Lee et al 2014).

Approach: the ideal method of countering this security threat toward ADS-B would be to issue X.509 certificates to all planes and provide a certificate-based security service, but this is difficult in reality. As proposed by Lee et al 2014, a more realistic approach would be to protect the ADS-B data transmitted between the ADS-B sensor and ATC. In the proposed method, the ADS-B sensor is identified using SPKI four tuple certificates and further authorized to transmit ADS-B data to ATC using SPKI six tuple certificates. An authorized ADS-B receives symmetric keys from ATC and utilizes them to encrypt the ADS-B data. It is believed that application of this method to the next-generation ATC system could facilitate an effective response to the security threats to ADS-B data transmitted between ADS-B sensors and ATC, such as spoofing, eavesdropping, and data modification.

Directions for future research: implementing the proposed security framework, improving it through validation at the laboratory level, analysing the benefits of the application to CNS/ATM, and performing tests to link the actual data with an ATC system in operation.

Problem: securing ADS-B and preventing attackers from exploiting its open-text open broadcast nature in order to launch attacks against ATC operations.

Approach: a novel intrusion detection system operating with minimal overhead and demonstrating promising performance values (Kacem et al 2016).

Directions for future research: not identified

Problem: although simulation can support the operation of critical infrastructures in various levels and applications, it is easy to overlook the difficulties involved in setting up the simulation testbed with enough fidelity and level of realism to ensure its effectiveness in supporting these activities.

Approach: a system based solely on open source tools and designed to support activities that cannot be conducted in the real environment. Current features are already powerful enough to perform a variety of studies, including the one presented in ADS-B, which has been a much-discussed topic in the literature recently (Monteiro et al 2016).

Directions for future research: developing an automatic pilot module to comprehend voice commands, execute the instructions of controllers and reply to the orders using voice synthesizers.

Problem: with the increase in the number of UAVs in the sky, the need for UAV traffic management arises. Unmanned air traffic management system (UTMS), especially in the urban airspace, could be

considered as a critical infrastructure, which – if disrupted – can lead to severe monetary losses and even casualties. As a computerized system, UTMS is susceptible to cyber-attacks ranging from cyber vandalism to cyber warfare. An emphasis on building security into products counters the all-too-common tendency for security to be an afterthought in development. Addressing existing vulnerabilities and patching security holes as they are found can be a hit-and-miss process.

Approach: using the "secure by design" philosophy to systems engineering when the system is designed from the start to be secure. This approach contrasts with less rigorous approaches including security through obscurity, security through minority and security through obsolescence, which has proven themselves to be ineffective (Sidorov et al 2017).

Directions for future research: not identified

Problem: cybersecurity does not fully comprise technological solutions and is actually a three-fold notion based on technology, people, and processes. People are considered one of the most influential factors in cybersecurity. They could knowingly or unknowingly compromise systems, could wilfully or by negligence violate protocols, and might not be aware of the consequences of their actions from the point of view of cybersecurity.

Approach: approaches to human resources management and personnel education need to be designed with cybersecurity in mind. Moreover, processes are required to ensure sustainable cybersecurity. Internal processes of the organization need to be designed to include technology maintenance, security incident response actions, security incident information management, self-adjustments in view of changes in the cyber threat landscape, etc. It is also important to ensure that people and processes are connected with every process having a manager as the authority for reinforcing the process. Properly designed and setup technology takes care of all the heavy lifting in ensuring cybersecurity: encryption, resiliency, fool-proofing, filtering, reducing human factor, etc. (Sidorov et al 2017).

Directions for future research: not identified

Problem: the need for increased surveillance due to increase in flight volume in remote or oceanic regions outside the range of traditional radar coverage has been fulfilled by the advent of space-based Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance systems. ADS-B systems have the capability of providing air traffic controllers with highly accurate real-time flight data. ADS-B is dependent on digital communications between aircraft and ground stations of the air route traffic control centre (ARTCC); however, these communications are not secured. Anyone with the appropriate capabilities and equipment can interrogate the signal and transmit their own false data; this is known as spoofing. The possibility of this type of attacks decreases the situational awareness of the airspace concerned.

Approach: designing a secure transmission framework to prevent ADS-B signals from being spoofed. Three alternative methods of securing ADS-B signals can be evaluated: hashing, symmetric encryption,

and asymmetric encryption. Research is needed to determine the security strength of the design alternatives. Feasibility criteria can be determined by a comparative analysis of alternatives. Economic implications and possible collision risk can be determined from simulations that model the airspace concerned (Amin et al. 2014).

Directions for future research: not identified

Problem: a space-based system plays a vital role within national critical infrastructures. They are being incorporated into energy distribution software, advanced air-traffic management applications, rail signalling systems, etc. Unfortunately, these infrastructures are susceptible to a broad range of security threats; the end-users of communications, location sensing and timing applications often fail to understand these infrastructures. Potential cyber-attacks may overthrow many of the safety assumptions that support the condition of critical space-based services. These safety assumptions are based on standard forms of hazard analysis that ignore cyber-security considerations. This is a significant limitation when, for instance, security attacks can simultaneously exploit multiple vulnerabilities in a manner that would never occur without a deliberate enemy seeking to damage space-based systems and ground infrastructures. Moreover, it is unclear how to represent and reason about the safety concerns that are created by the diverse security threats to GNSS architectures, including jamming, spoofing and the insider threat to ground-based systems. Such concerns invalidate many of the assumptions that support the provision of critical services.

Approach: identifying attack scenarios that justify the allocation of additional design resources so that safety barriers can be strengthened to increase the flexibility against security threats. One approach would be to extend the application of argumentation techniques such as GSN from safety-related applications to represent security argumentation. The ultimate goal would be providing an integrated, risk-based approach to the identification of attack scenarios that can help assess the resilience of safety cases to security threats (Sharma et al. 2016).

Directions for future research: not identified

Problem: security of Cyber-Physical Systems (CPS) against cyber-attacks is an important yet challenging problem. Since most cyber-attacks happen in erratic ways, it is difficult to describe them systematically. Deception attacks (or false data injection attacks), which are performed by tampering with system components or data, are not of particular concern if they can be easily detected by the system's monitoring system. However, intelligent cyber attackers can avoid being detected by the monitoring system by carefully design cyber-attacks. The main objective then is to investigate the performance of such stealthy deception attacks from the system's perspective.

Approach: investigating three kinds of stealthy deception attacks according to the attacker's ability to compromise the system. Based on the information about the dynamics of the system and existing hypothesis testing algorithms, one can derive the necessary and sufficient conditions under which the attacker could perform each kind of attack without being detected (Kwon et al. (2013).

Directions for future research: using the conditions under which the deception attacks successfully bypass the monitoring system, one could not only evaluate the vulnerability level of a given CPS but also develop secure system design methodologies against stealthy deception attacks.

Problem: currently UAVs are used for a wide range of missions such as border surveillance, reconnaissance, transportation and armed attacks. UAVs are presumed to provide their services at any time, be reliable, automated and autonomous. To fulfil their missions, UAVs need to collect and process data. The amount and kind of information enclosed make UAVs an extremely interesting target for espionage and endangers UAVs of theft, manipulation and attacks (Hartmann and Steup 2013).

Approach: developing a scheme for the risk assessment of UAVs based on the provided service and communication infrastructures. The components to be analysed could be the type of communication system, data storage, sensor system, environmental factors, and fault handling mechanisms. Risk can then be defined as the result of the product of the susceptibility of a UAV, the probability of occurrence of a specific attack on a component's vulnerability, and the severity of the attack.

Directions for future research: not identified

Problem: current autopilot systems for UAVs were not built with cybersecurity considerations taken into account and are thus vulnerable to cyber-attack. To develop a cyber secure autopilot architecture, a study is needed on potential cyber threats and vulnerabilities of the current autopilot systems. The ultimate goal would be to build a controller the current UAV autopilot system making it robust to cyber-attacks (Kim et al, 2012).

Approach: to attain the goal, one needs to develop a more sophisticated and accurate model to simulate the GPS attack coupled with a sensitivity study. Then, one needs to develop a collision avoidance algorithm for the ADS-B attack scenario and carry out a numerical analysis of simulated multiple aircraft.

Directions for future research:

- One should focus on more sophisticated attacks that utilize multiple points of attack or multiple methods.
- One should also evaluate possibilities for a coordinated attack where the attacker uses several attacks in a certain manner to induce more effective faults into the autopilot system.
- One should consider possibilities for the disguised attack where the attacker can mask an attack to induce a false reaction from the autopilot in order to remedy the attack.
- A purely analytical approach could also bring valuable insights; for instance, certain Kalman filtering algorithms might be vulnerable to a special form of induced error in measurements which cannot be detected.

- There is an acute need for developing metrics for cyber-attacks; until now a metric for measuring either likelihood or a damage potential of cyber-attacks on a UAV autopilot does not exist.
- Algorithms for detecting cyber-attacks need to be developed.

Predictions up-to-2025 and evolutionary progress up to 2050

Blockchain technology

Although the maturity of blockchain technology is still relatively low and the technological know-how is still concentrated to a small group of blockchain users in the world, blockchain technology (more globally know as distributed ledger technology or DLT) is becoming more and more extensively accepted as the best unbreakable solution for securing Internet communications.

Findings show that while there were only a small number of companies active in the enterprise DLT (distributed ledger technology) space in 2013, interest in 'blockchain technology' quickly grew in 2014 with a significant increase in the number of companies providing DLT service. 2015 was the year that the DLT industry took off in terms of new entrants, with the number of start-ups growing by 108% over 2014 [CITATION Gar17 \l 3082]. According to his study existing DLT deployment plans: 15% of OPSIs (Other Public Sector Institutions) plan to deploy DLT-based applications this year, and another 23% plan to do so within the next two years; the timetable for central banks is more conservative than for OPSIs (most of their deployment plans consider periods longer than 10 years).

There are however several drawbacks and limitations previously described (throughput, latency, size and bandwidth, possibility of a 51% attack, wasted resources, usability, versioning, hard forks, multiple chains and scalability), that made its application in aviation, air transport and air traffic management uncertain, and that will be required further research in the coming years. It is expected that when more Blockchain solutions are taken in use with larger numbers of users, it will trigger the need to conduct more research on the challenges and limitations, particularly in topics related to scalability, security and privacy

In 2017 a few companies start to design applications of Blockchain in the aviation industry:

- Aeron (https://aeron.aero/#en) is working on the development of a smart blockchain-based solution called "airline in a pocket". It includes a pilot's application that is used by a pilot for personal flight logging. A company application that collects and verifies data from aircraft operators, maintenance organizations, flight schools and fixed base operators. In case of any mismatch in data between any Aeron data source with either the Air Traffic Control, pilot, or operator, aviation authorities can quickly detect and eliminate the problem. Aviation authorities can also detect any pilots operating with an expired license. As a consumer, or flight school student, you have access to the verified global database through aerotrips.com. The project is expected to be fully available within two years.

- The BASTONET project (www.bastonet.com), based on the Etheruem network, seeks to engineer the blockchain use in the airline and travel industry, in booking and ticketing processes of airlines, and in transfer of data and value within the network in association with other airline services like air cargo movement, crew management, passenger data transfer and aircraft maintenance scheduling, loyalty programs, etc.
- Airbus has been working to identify several business challenges worth addressing with blockchain. These include instances of a high cost of trust, a slow process but time-sensitive interactions, compliance issues, high overhead cost for data reconciliation and multiple parties with whom to share data. Ideas that emerged as viable use cases include 3D printing and the applicability of blockchain to distributed manufacturing at a local level; keeping identity, achievements and certificates attached to each pilot is immutable data; dispute management in which complex transactions can obscure the fact that money is unnecessarily blocked; and quality process tracking, which would benefit from greater transparency and an early-warning trigger system.
- The Blockchain.aero Consortium is promoting the concept of Proof-of-flight protocol and McFly token based on blockchain technology to speed up on the air taxi market, (invoice, charge and land), as a way to use eVTOLs and other infrastructure elements (pads, chargers, maintenance and repair shops) and pay for that use. Their full service is expected to be deployed by 2020. This technology is envisaged as an enabler that paves the way for the introduction of global single passenger tokens, as blockchain technology offers us the potential to provide a new way of using biometrics. It could enable biometrics to be used across borders, and at all airports, without the passenger's details being stored by the various authorities.

All these previous applications addressed an individual not interconnected aspect of the aviation and the air transport industry not involved in real-time operation. All represent individual company's initiatives to take advantage in the short term of the blockchain technology as a way to get contact with it, safely and profitably.

In 2017 SITA has published research on blockchain technology FlightChain, conducted with British Airways, Heathrow, Geneva Airport, and Miami International Airport. FlightChain was designed as a private permissions blockchain—using Ethereum and Hyperledger-Fabric—which stores flight information and uses a smart contract to reconcile any conflicting data. During the trials conducted between British Airways, Geneva Airport, Heathrow and Miami International Airport, FlightChain handled and stored more than two million flight changes. The project has demonstrated that blockchain is a viable technology to provide a single source of truth for data for airlines and airports, specifically for real-time flight information.

Blockchain is also being explored as a way to address drone cybersecurity by keeping a high-speed, assured ledger of airspace activity and information regarding the drone and its operator and distributing it to all appropriate parties.

Some initiatives are also been put in place to apply blockchain to secure VoIP (https://www.dyrnan.com/enterprise/), that if prove to be efficiency might be also translated to the aviation domain for real-time pilot controller communication. In 2017 the first pioneer of blockchain-based VoIP service was born: EncryptoTel, a company that raised $3 million during a crowdfunding campaign (another sign of blockchain's significance) and is expected to launch by the summer of 2018. The company is promising a secure VoIP and B2B blockchain communications infrastructure for its service. According to EncryptoTel, a hosted PBX provider available to anyone in the world, users of different hosted PBX sources can start and accept encrypted VoIP calls while also get access to popular messenger applications.

Effective adoption of blockchain as a standard in the industry will require a more coordinated and regulated approach, based on shared standards and solid agreement between the stakeholders involved. The development cycle of these blockchain applications is around two years. The development of real-time aviation application build upon standards and stakeholders agreement will be subject to the longer development cycles of the aviation, considering that for this purpose the technology has been validated in lab and in other environments (TRL4) but it still to be validated in relevant environment (TRL5).

As with many emerging technologies, there are still concerns in the market regarding the security and reliability of blockchain. The development of standards and regulations for blockchain has a role to play in establishing market confidence and supporting the eventual commercial implementation of blockchain technology. Australia will host the first international blockchain standards meeting for ISO/TC 307 in April 2017. JWS will publish further updates as new developments in the standards and Australian law relating to blockchain arise. These standards are recognized as temporal and are not applicable to aviation by itself. It has to be considered that the full cycle of standards development will still to be accomplished in aviation after the technology has achieved TRL 9 (system proven in an operational environment) for critical safety aviation real-time applications.

- Future of ATM cybersecurity

The reliance of future ATM on wireless networks and interfaces, implementation of Internet Protocols and VoIP for air to ground communications will make it more vulnerable to malicious attack unless enough protections are including in the system design. SESAR and NextGen will radically increase the 'attack surface' for any future malware [CITATION Joh \l 3082]. Neither of SESAR nor NEXTGEN has to define appropriate security standards at both physical and logical. In 2015, separate reports were published looking at the vulnerability of both the NextGen and SESAR systems to cyber-attacks and how best to protect against them. Both NextGen and SESAR are introducing a computer system named System Wide Information Management (SWIM), which will handle all ATM information including aeronautical, flight, aerodrome, meteorological, air traffic flow, and surveillance. Both reports note that introduction of SWIM, which represents a more interconnected ATM system that operates through an Internet Protocol (IP) network, means there are increased cybersecurity risks.

Moreover, the inherent vulnerabilities of the Radio frequency-based ATM technologies' have not been sufficiently addressed not overcome by the future ATM (such as those of unencrypted ADS-b, Radio

Aids, etc,). The current ADS-B system openly transmits sensitive aircraft information over a shared link, allowing flight information to become available to everyone with the right ADS-B equipment.

To avoid these limitations some authors [CITATION Ata13 \l 3082] recommend:

- Authentication mechanism to be introduced on NextGen/SESAR to reduce the complexity of detecting malicious actors,
- Use of a combination of secret keys and secret numbers will allow the communication between aircraft to aircraft and aircraft to ground to be authenticated,
- Use of digital certificates, message validation to reduce the risk of malicious activities on the aircraft infrastructure. Digital certificates should be implemented at different phases of operation, when the aircraft is parked on the ground or when it is airborne. In addition, they can be embedded in an individual device of the aircraft network or one common digital certificate can be used for the entire network. Defining common criteria to implement and manage digital certificates on an aircraft can be of a great benefit to the airline industry allowing the lifecycle process of the digital certificate to be closely and carefully inspected and maintained.

More than a dozen wireless technologies are currently used by air traffic communication systems during different flight phases. From a conceptual perspective, all of them are insecure as security was never part of their design. Recent contributions from academic and hacking communities have exploited this inherent vulnerability to demonstrate attacks on some of these technologies. The International Civil Aviation Organization (ICAO), EUROCONTROL, and the FAA have started planning for further upgrades of the current communications systems and are seeking to develop new data links.

Specifically, L-band Digital Aeronautical Communications System (L-DACS) and Aeronautical Mobile Airport Communications System (Aero-MACS) are supposed to replace the current VHF system. Since these systems can provide much higher data throughput compared to the existing data links, some of the applications currently provided by other technologies could also utilize these new technologies one day. Thankfully, L-DACS and AeroMACS have begun to at least consider the issue of wireless security and some corresponding designs are already included by the specifications or will be in the future.

Unfortunately, L-DACS is still in the very early specification phase and in line with typical technological cycles in aviation will not be deployed before the 2030s [CITATION Int13 \l 3082]. Furthermore, since its specification is not finished – many parts are up in the air and there are still competing proposals – they could strongly benefit from an immediately increased awareness about security concerns in aviation, which we aim to provide with our work.

AeroMACS takes the form of a profile of IEEE 802.16- 2009 (IEEE Std 802.16-2009, 2009), known as WiMAX. It intends to provide a surface data link for use at the airport, allowing ATC, airlines, and airports to communicate with the aircraft [CITATION NFi16 \l 3082]. It has a line-of-sight range of up to 3 km per cell and uses commodity radios to communicate. While the current standards include

cryptography, making it a serious step forward, AeroMACS will not solve the security problems currently found in aviation. Besides the prevalent issue of long deployment time frames (the beginning of deployment is not projected before the middle of the next decade), many security questions such as the protection of management frames are still undecided [CITATION SES14 \l 3082]. Most importantly, AeroMACS will only be able to replace current data links on the ground and in the immediate vicinity of an airport, leaving the vast amount of air traffic communication unprotected. AeroMACS is further along in the development cycle compared to L-DACS, with test deployments going on at some airports around the world. However, at the time of writing, many of the necessary avionics standards and specifications were still in the planning phase. Thus, it was not possible to include it in our survey but, like L-DACS, it should see strong input from the security community as soon as possible.

Possible or Predictable Breakthroughs

- The prospect of quantum computing and the post quantum cryptography.

Although not yet in existence but theoretically viable, the vision of quantum computing and its capacity to decrypt secure network traffic captured and archived today[1], raises concerns about the long-term robustness of encrypted solutions, including blockchain applications. The achievement of quantum computing may destabilize all these technologies and applications.

Currently, the lead developer of quantum computing technology is Google. They expect to have a 49-qubit quantum computer this year[6]. For hardwa***re, the key metric in the roadmap for a quantum computer is building scalable qubits with 2-***qubit gate errors below 0.1-0.2% [CITATION JMM15 \l 3082]. For software, a new "quantum-supremacy" test that can demonstrate the exponential power of a quantum processor by checking its output with a classical computer, which is intractable for even the world's most advanced classical supercomputer beyond 42-50 qubits will be described. Google aims to perform this experiment in the next 2 years. Google's quantum computer roadmap plans commercialisation of the technology in 5 years and IBM is feeling similarly optimistic.

Now that Google and other companies involved in quantum computing have mastered much of the fundamental science behind creating high-quality superconducting qubits, the big challenge facing these firms is scaling these systems and reducing their error rates. Alan Ho, an engineer in Google's quantum AI lab, predicts that it will be 2027 before we have error-corrected quantum computers, so useful devices are still some way off.

The projection by the experts is that in the 2030s, there will be quantum computers significantly better than supercomputers today, but they most likely won't be accessible to governments and companies until the 2040s. Eventually, at the 2050s they'll shrink down to size and cost viable for consumer use.

[1] [2] "The quantum clock is ticking on encryption – and your data is under threat", Wired 2016, http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption

Besides this long-term projection for quantum computing, the magnitude of concerns is enough for researchers across the world to the study of new methods for online encryption and the hiding of messages, known as **Post-Quantum Cryptography**.

Researchers add complexity to the algorithms that encode our messages while hackers attempt to break them. For now, researchers are able to outpace the majority of these malicious attempts. However, quantum computing would compel the use of keys so long that most public-key systems in use today would not be practical. This necessitates a complete redesign of the algorithms involved in online encryption.

There is currently no standard of encryption against a quantum computing attack. But there are known quantum-safe algorithms.

The U.S. National Institute of Standards and Technology, which in December 2016 launched a post-quantum crypto project designed to identify quantum-resistant public-key cryptographic algorithms. It has been recognized by the experts that full transition to cryptograph alternatives takes a long time (possibly > 10 years) in any industry, and these times will be much higher in aviation because of the high level of interoperability and standardization.

- Quantum Communications

Quantum communication is a field of applied quantum physics closely related to quantum information processing and quantum teleportation. It's the most interesting application is protecting information channels against eavesdropping using quantum cryptography.

The most well-known and developed application of quantum cryptography is quantum key distribution (QKD). QKD describes the use of quantum mechanical effects to perform cryptographic tasks or to break cryptographic systems.

Quantum communication encryption is secure against any kind of interception because the information is encoded in a quantum particle in such a way that it will be destroyed as soon as the system detects any intrusion attempts. The principle of operation of a QKD system is quite straightforward: two parties (Alice and Bob) use single photons that are randomly polarized to states representing ones and zeroes to transmit a series of random number sequences that are used as keys in cryptographic communications. Both stations are linked together with a quantum channel and a classical channel. Alice generates a random stream of qubits that are sent over the quantum channel. Upon reception of the stream Bob and Alice — using the classical channel — perform classical operations to check if an eavesdropper has tried to extract information on the qubits stream. The presence of an eavesdropper is revealed by the imperfect correlation between the two lists of bits obtained after the transmission of qubits between the emitter and the receiver. One important component of virtually all proper encryption schemes is true randomness which can elegantly be generated by means of quantum optics.

Recently China has taken one more step forward towards achieving success in Quantum communication technology and launched the World's 1st 'Hack-Proof' Quantum Communication Satellite into orbit aboard a Long March-2D rocket in order to test the fundamental laws of quantum

mechanics at space. The satellite, dubbed Quantum Science Satellite, is designed to develop a 'Hack-Proof' communications system in this age of global electronic surveillance and cyber-attacks by transmitting uncrackable encryption keys from space to the ground. But if successful, the QUESS satellite would vastly expand the range of un-hackable communication to long distances as well.

KEY TOPIC T5.6 – THE BLOCKCHAIN PROCESS AS AN EXAMPLE OF CYBERSECURITY

Airport transportation systems are cyber-physical systems that serve passengers, air traffic system under the supervision of human controllers or unmanned. It is forecasted that the volume of these operations will grow more than in recent years. Therefore, the cyber-physical system will become more important to work uninterrupted and secure. According to Sampigethaya and Poovendran (2013), aviation information systems contain physical components, including electronics, hardware, infrastructure, and humans which use digital computing, storage, software, or data networking to generate, process, present and consume data. However, the increasing density of these interactions between physical and cyber systems warrant a surgical consideration of cyber-physical interactions and potential performance risks from cyber and physical threats. Authors demonstrated 'cyber' layer benefits for helping future aircraft, airports, and freight movement systems to overcome 21st century challenges.

In another study, Johnson (2012) studied air traffic management systems safety for developing a technology roadmap and proposed the extreme need on raising awareness about the potential threats to safety-related systems amongst regulators and senior management. He stressed that without greater strategic leadership there would be security breaches that might leave major vulnerabilities.

It is well-known that there is a great number of studies regarding Industry 4.0 and Internet of Things applications. Furthermore, the same vulnerability problems arise on these issues also. Hence, it is thought to create an analogy and mention a growing research trend on Blockchain technologies.

Globalization becomes more reasonable with the developments in network technologies and the internet. In this age, digital platforms changing the business models and whole society by enabling connected structure via cloud-based systems (Kushida et al., 2011; Pon et al., 2014; van Alstyne et al. 2016). This perspective can enable a light-weight financial system, inter-organizational record-keeping and multiparty data aggregation (Greenspan, 2016).

One of these technologies is Blockchain which is accepted as a general-purpose technology (GPT) today like a steam engine, electricity, and the internet examples (Catalini and Gans, 2016). GPTs typically lead to subsequent innovation and productivity gains across multiple industry verticals, sustaining new technological paradigms and economic growth for multiple years (Bresnahan and Trajtenberg, 1995; Helpman and Trajtenberg, 1998; Rosenberg and Trajtenberg, 2001; Moser and Nicholas, 2004; Basu and Fernald, 2007). According to Naughton (2016) Blockchain technology will be the most important IT invention of our age.

When the historical background of Blockchain examined it can be seen that Satoshi Nakamoto proposed Bitcoin as an electronic payment system based on a decentralized peer-to-peer network,

without the need for intermediation in a White paper published in 2008 (Nakamoto, 2008). The Blockchain platform is created for Cryptocurrency exchange by Nakamoto but it is not mentioned in the report (Mattila, 2016). However, the technology used in Blockchain gives insights to many other scholars with different application areas today. Underlying technology came with Bitcoin is Blockchain which is a protocol and widely acknowledged as a major breakthrough in fault-tolerant distributed computing, after decades of research in this field.

Briefly, Blockchain can be defined as a distributed ledger that contains all transaction executed in the Bitcoin network. This technology described with three words as disintermediated, censorship-resistant, and tamper-proof (Seppala et al., 2016). The ledger network is open, and participants do not need to trust each other to interact. All transactions are verified and recorded by the nodes of the network through cryptographic algorithms, without supervisors, central authority, human intervention, and any other third-party organizations. The reliability of the network is provided by the majority of nodes even some of them dishonest or malicious. For making a human intervention or controlling authority unnecessary verification is performed by a mathematical mechanism called proof-of-work. Proof-of-work systems run by "mining[2]" and "mining" does not serve the purpose of verifying transactions, but of building a credible commitment against an attack. Consensus about the true state of a distributed ledger therefore emerges and becomes stronger as time (and blocks) go by. If a bad actor wanted to reverse a past transaction it would have to spend a disproportionate amount of resources to do so. This is the result of the bad actor not only having to outpace the growth rate of the legitimate chain, but also of having to recompute all blocks after the one that is being manipulated. Since the network always takes the longest, valid chain as the true state of the ledger (i.e. as the "consensus"), the task of altering a past block of transactions and imposing it on the rest of the network becomes increasingly difficult as the chain is extended. As a result, in proof-of-work systems, a blockchain is only as secure as the amount of computing power dedicated to mining it. This generates economies of scale and a positive feedback loop between network effects and security: as more participants use a cryptocurrency, the value of the underlying token increases (because the currency becomes more useful), which in turn attracts more miners (due to higher rewards), ultimately increasing the security of the ledger.

The main idea of Blockchain protocol is decentralization and permission-less attendance. However, there are different blockchains as permissioned, private, public etc. The steps of Blockchain protocol can be demonstrated in Figure 5.80:

[2] Mining: Nodes in the network compete to solve a mathematical puzzle that requires the consumption of computing power. Once the puzzle solved the new block of transactions is accepted by the network and committed to the Blockchain. The network nodes which is called miners rewarded with newly generated coins.

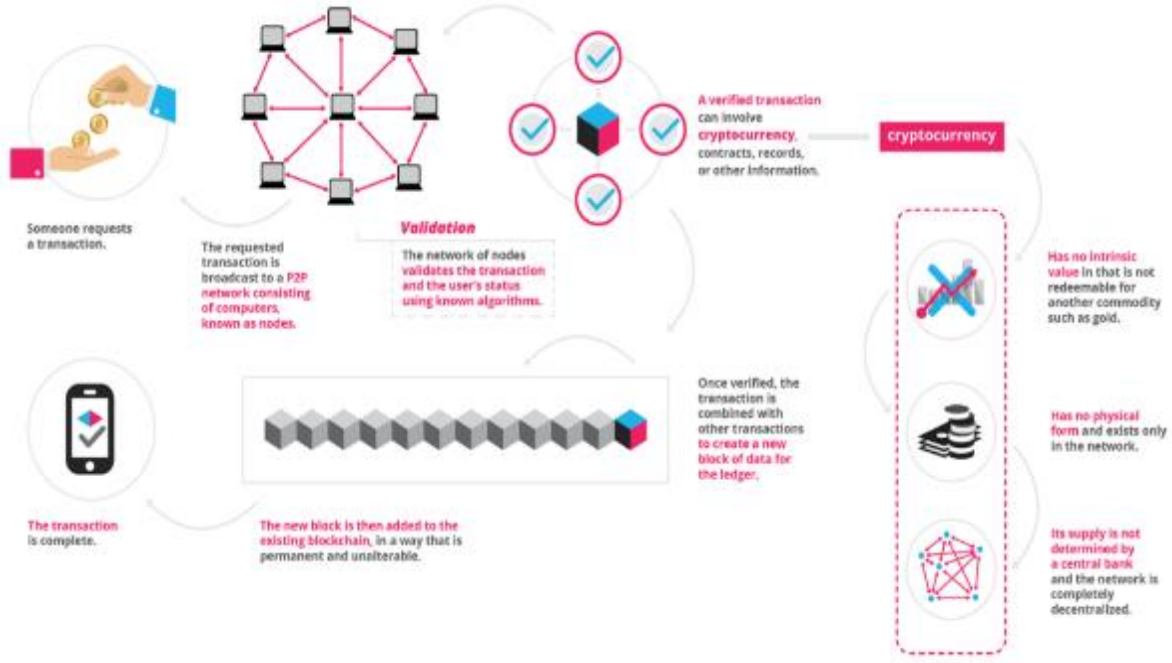


Figure 5.80 - Blockchain Process (Source: https://blockgeeks.com/wp-content/uploads/2016/09/infographics0517-01-1.png Access Date: 19.10.2017)

It is clear with the explanation of blockgeeks.com that blockchain process is paperless, disintermediated, unaltered, reliable and free. These characteristics make this system more popular especially for reducing transaction costs at first. These costs are; the cost of verification and the cost of networking (Catalini and Gans, 2016). By the blockchain protocol, for the first time in history value could be reliably transferred between two distant, untrusting parties without the need for a costly intermediary.

However, Blockchain technology has also some technical challenges and limitations that have been identified. Swan (2015) presents seven technical challenges and limitations for the adaptation of Blockchain technology in the future:

Throughput: The potential throughput of issues in the Bitcoin network is currently between 4 to 7 tps (transactions per second) and it is limited when compared to VISA and PayPal.

Latency: To create sufficient security for a Bitcoin transaction block, it takes currently roughly 10 minutes to complete one transaction. To achieve efficiency in security, more time has to be spent on a block, because it has to outweigh the cost of double spending[3] attacks. Bitcoin protects against double-spending by verifying each transaction added to the blockchain, to ensure that the inputs for the transaction have not been spent previously. This makes latency a big issue in Blockchain currently. Making a block and confirming the transaction should happen in seconds while maintaining security. To complete a transaction e.g. in VISA takes only a few seconds, which is a huge advantage compared to Blockchain.

[3] Double-spending is the result of successful spending of money more than once.

Size and bandwidth: At the moment, the size of a Blockchain in the Bitcoin network is over 100GB (December 2016 - http://www.coinfox.info/news/6700-bitcoin-blockchain-size-reaches-100-gb Access Date 19.10.2017). When the throughput increases to the levels of VISA, Blockchain could grow 214PB in each year. The Bitcoin community assumes that the size of one block is 1MB, and a block is created every ten minutes. Therefore, there is a limitation in the number of transactions that can be handled (on average 500 transactions in one block). If the Blockchain needs to control more transactions, the size and bandwidth issues have to be solved.

Security: The current Blockchain has the possibility of a 51% attack. In a 51% attack, a single entity would have full control of the majority of the network's mining hash-rate and would be able to manipulate Blockchain. To overcome this issue, more research on security is necessary.

Wasted resources: Mining Bitcoin wastes huge amounts of energy ($15million/day). The waste in Bitcoin is caused by the Proof-of-Work effort. There are some alternatives in industry fields, such as proof-of-stake. With Proof-of-Work, the probability of mining a block depends on the work done by the miner. However, in Proof-of-Stake, the resource that is compared is the amount of Bitcoin a miner holds. For example, someone holding 1% of the Bitcoin can mine 1% of the "Proof-of-Stake blocks". The issue with wasted resources needs to be solved to have more efficient mining in Blockchain.

Usability: The Bitcoin API for developing services is difficult to use. There is a need to develop a more developer-friendly API for Blockchain. This could resemble REST APIs.

Versioning, hard forks, multiple chains: A small chain that consists of a small number of nodes has a higher possibility of a 51% attack. Another issue emerges when chains are split for administrative or versioning purposes.

Beyond these limitations according to Yli-Huumo et al. (2016) scalability is also an issue that needs to be solved for future needs. Therefore, to identify and understand the current status of research conducted on Blockchain, it is important to gather all relevant research. It is then possible to evaluate what challenges and questions have been tackled and answered, and what are the most problematic issues in Blockchain at the moment.

Because the maturity of blockchain technology is still relatively low, the technological know-how is still concentrated on a small group of blockchain users in the World. However, in a decade the Blockchain platform has been approved with its bespoken characteristics. Hence, the idea behind it makes the technology became widespread and it can be envisioned that the perspective will have the potential to be improved with these common applications. For today there are many application areas of Blockchain and here some of them are mentioned.

As an irreversible and tamper-proof public records repository for documents, contracts, properties, and assets, the blockchain can be used to embed information and instructions, with a wide range of applications from private to public (Atzori, 2015). The most popular application is smart contracts which can be described as tamper-proof, self-executing and automatically enforceable. Based on Mattilla et al. (2017) American cryptographer Nick Szabo published an article in which he outlined the concept of smart contracts in 1994 at first. However, because of the immature technology and IT

infrastructure at that time, the idea couldn't have opportunity to be applied. Beyond Szabo's smart contract definition today smart contracts are accepted as a set of promises in a digital form including protocols within which the parties perform on these promises. Blockchain technology enables smart contracts, to be programmed and embedded in the system easily. Moreover, it can be envisioned that these smart contract systems may be improved with self-execution and self-enforcement to be fully automatized in autonomous organizations. With these improvements in smart contracts it is envisioned to reach Decentralized Autonomous Organization/Corporations/ Societies (DAOs/DACs/DASs). In this concept, self-sufficient agents derived from artificial intelligence and capable to execute tasks without human involvement, for which the blockchain can provide additional functionality. DAOs operate independently of their developers. In their structure, humans are moved from the centre of the organization to its outskirts, as the system is used to organize human activity algorithmically. An open organization based on smart contracts may solve the problem of bad leadership or issues with the transparency of the organization. However, if left unregulated and ungoverned, errors in the programming code may prove to be very harmful or even dangerous. The DAO is in the development stage and so it reveals new types of risks. The organizational characterof The DAO in itself raises the question of, for instance, the distribution of liability for damages within such new types of applications. In addition, it involves ties to the question of determining the correct legal entity in economic activity based on new models of co-operation, as is the case with The DAO. Hence, developing technology is not only adequate for making the application common but also social side should be handled with a holistic perspective.

Smart property concept is another application area and applied to digital ownership of tangible and intangible assets. By the way, it can change the patent system with a distributed perspective and can democratize the triadic perspective. By embedding the patent system into the blockchain, idea-owners do not need third-party approval but need acceptance by nodes in the network. The execution of instructions by a cryptographic code with the protection of participants against risks of fraud and a significant reduction of management overheads. Because of the remarkable advantages related to automation, transparency, auditability and cost-effectiveness, the blockchain may represent a disruptive innovation for many varieties of contracts and business activities.

A decentralized voting system may be demonstrated as an important application area for blockchain for public administration field. Tamper-proof ballots and election results can create transparency and strengthen democracy. Due to the fact that blockchains can be designed to be public yet anonymous, anyone can easily verify the voting outcome and also check that their own vote has been taken into account accordingly, while still maintaining ballot secrecy. Blockchain technology can, therefore, help to reduce corruption in political systems and act as a safeguard against rigged elections.

Blockchain technology may be used in improving IoT with smart, censorship-resistant, tamper-proof, and disintermediated data interchange. This may add value to industry 4.0 applications also with same technology perspective.

Another market may be the music industry for applying Blockchain technology. According to a report of Middlesex University (2016), Blockchain technology could revolutionize the music industry with a

networked database for music copyright information, fast payments, transparency in the chain and Access to alternative sources of capital. As can be seen in the application examples, the idea behind blockchain technology, which may be called as a paradigm, has been becoming popular evolutionary.

Because of these evolutionary improvements in Blockchain, Swan (2015), described blockchain technology as "fundamental for forwarding progress in society as Magna Charta or the Rosetta Stone". Again, based on Mattila (2016) blockchain technology is shifting society in two aspects. Firstly, blockchain technology enables directly and reliable transactions of any assets over the internet between any parties by providing censorship-resistant, disintermediated, tamper-proof digital platforms (Mattila & Seppälä, 2015; Mattila, 2016). Secondly, for enterprise- and industry- level systems, blockchain technology is providing efficiency gains on top of existing structures by removing the constant need for actively intermediated data-synchronization and concurrency control by a trusted third party (Mattila, 2016; Mattila et al., 2016). Therefore, blockchain platform can be described as more democratic and equal for all nodes in the network. The main idea is accepting all parties sharing the same platform without having privileges and no third-party that will provide ones with these privileges. So, blockchain technology can enable all the participants to produce a platform together in a distributed manner, without having to trust each other in almost any capacity (Seppälä & Mattila, 2016; Mattila, 2016).

It is thought that the potential of Blockchain regarding security, smart contract structure and peer-to-peer network design may be applied for improving the Aviation cyber-physical systems. It can be proposed that research studies may be directed to understand the sub-systems to apply blockchain logic to the aviation industry in future.