PARE Article

Ensuring Safety And Security

October 2019

Based on

Chapter 5 of the 1st Yearly Report of the PARE project

Prepared by

PERSPECTIVES FOR AERONAUTICAL RESEARCH IN EUROPE

INTRODUCTION

In 2050, European aviation must have achieved unprecedented levels of safety and security and continue to improve. The accident rate in commercial flight must be less than one per million flights and all types of aircraft and rotorcraft must safely operate in the same airspace and in most weather conditions. On the other hand, security processes for passengers and cargo must allow seamless and non-intrusive security, air vehicles must be resilient to internal and external threats, and air transport data networks must be hardened against and resilient to cyberattacks.

To ensure that all of these goals are met, the Advisory Council for Aeronautics Research in Europe (ACARE) established the specific Flightpath 2050 goals 14 to 19, which are addressed in the 5th chapter of PARE's 1st year report, entitled “Ensuring Safety and Security”.

ULTRA – LOW ACCIDENT RATE IN COMMERCIAL FLIGHT

The aviation accident rate has been declining throughout the years, nevertheless, the rate of decline has slowed markedly since 2004 and, at the same time, we are seeing a continued growth in the number of flights, which are set almost to the triple by 2050. In 2015, the accident rate of the European Union Aviation Safety Agency (EASA) Member States (MS) operators of Commercial Air Transport (CAT) aeroplanes was approximately 3 accidents per million flights. By 2050, the European air transport system must have reduced this rate to less than one accident per million commercial aircraft flights.

Ensuring Safety And Security

KEY FINDINGS

- From 2010 to 2015, on EU's territory and with EU–registered aircraft, there were 188 fatalities (155 fatalities in 2015 from the 3 accidents) in CAT aeroplanes and, in 2016, there was only one fatal accident involving any EASA MS operator of CAT aeroplanes;

- The Key Risk Areas identified by EASA MS operators for accidents and serious incidents are: (a) system/technical failure, (b) airborne collision/conflict – collision of two aircraft in the air, (c) movement area collision or ground collision/handling, (d) fire, (e) runway excursion or abnormal runway contact, (f) runway collision, (g) aircraft upset – full range of loss of control situations, (h) terrain collision/conflict – aircraft collision with terrain, and (i) obstacle collision;

- Comparing the average number of CAT EASA MS accidents and serious incidents by Key Risk Area for the period 2007 – 2015 with that of 2016, the Key Risk Areas (a), (b) and (e) show a negative change in 2016 (from stable trend to increasing or from decreasing to increasing) in contribution to fatal accidents in these 10 years, accounting for 18% of those accidents. Aircraft upset represents only 3% of the accidents and serious incidents involving an EASA MS operator in 2016, but continues to be the most fatal Risk Key Area for EASA MS operators;

- With 45% of fatal accidents involving technical failures in some way during the 2007 to 2016 period, this is both a major accident outcome and a precursor to other types of accident. Over these 10 years, 27% of fatal accidents involved ground collision and other associated ground events;

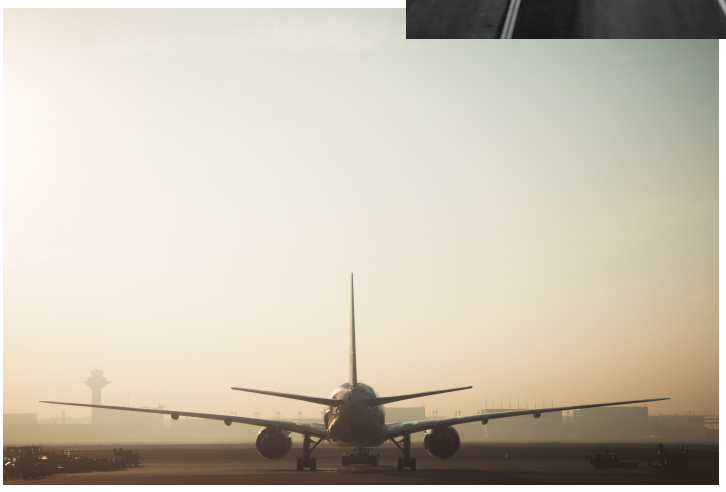
- The origins of the causal and contributory factors behind the accidents and serious incidents involving EASA MS operators between 2007 and 2016 are: flight operators (56.64%), technical (21.30%), human factors (8.53%), Air Traffic Management (ATM) (5.87%), aerodrome operations (4.49%), organisational (2.40%) and maintenance (0.77%).

KEY ACTIONS

The safest mode of transport can only benefit from being made even safer, which requires investigating accident classes, finding preventive and corrective actions and proving that they can be implemented. It is recommended that accident causes are considered by order of statistical occurrence and that appropriate safeguards for each class are identified and implemented.

WEATHER-HAZARDS AND RISK MITIGATION

The aviation system is highly sensitive against disturbing weather effects that can become hazardous for the aircraft operation by producing setbacks such as delays and accidents/incidents. Moreover, 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. To ensure safety, by 2050, weather and other hazards from the environment must have been precisely evaluated and risks properly mitigated.



Ensuring Safety And Security

KEY FINDINGS

- Weather is responsible for: 13% of all aircraft losses between 1995 and 2004, 33% of all accidents/incidents from 2004 to 2007 and 40-50% of delays at European airports;
- The severe weather-related accidents and incidents can be attributed to the following weather–hazards: wind, wind shear and turbulence; in-flight icing; low visibility due to lithometers, fog or precipitation; lee waves; hail damage; thunderstorms; and volcanic ash;
- During the flight in en-route area, aviation is only disrupted marginally by weather phenomena. However, during start and landing, it is very sensitive to those effects, especially fog, snow and wind, which can disrupt the operations with even a low intensity;
- The severe weather impact can be associated with two different, yet interdependent, risks, notably Flight Safety Risk and Flight Efficiency Risk (likelihood and potential extent of incurred flight delays or even cancellations made due to severe weather risk management). The Flight Safety Risk can have different sources and manifestations: In-flight Safety Risk (impact on flight crew), which is divided into Hazard Encounter Risk and Knock-on Flight Safety Risk, and ATCO Excessive Overload Risk. In particular, the Hazard Encounter Risk is described using two generic risk management functions: risk prevention and risk mitigation.

KEY ACTIONS

Besides collecting higher-quality and more comprehensive weather data with higher spatial and temporal resolution (see ACARE goals 5 – Article Chapter 2 - and 13 – Article Chapter 4), its effects on aircraft dynamics must be modelled to identify effective prevention and corrective actions that must be simulated and further validated. Therefore, it is recommended that a low–cost basic research on flights in adverse weather conditions (e.g. wind, rain, ash clouds, lightning, icing, storms and weather fronts) is promoted and promising advances are selected for demonstration.

INTEGRATING DRONES IN MANNED AIRSPACE

The record of aviation as the safest mode of transportation is based on the highest engineering standards and professional qualifications as regards aircraft and cannot be compromised for Unmanned Aerial Vehicles (UAVs) operating in the same airspace. These UAVs constitute a new threat to the European airspace as demonstrated by the occurrence of several incidents involving conventional aircraft and UAVs. However, in 2050, the European air transport system must operate seamlessly through interoperable and networked systems allowing manned and UAVs to safely operate simultaneously in the same airspace.

KEY FINDINGS

- Unmanned aerial system (UAS), of which the UAV is the airborne component, comprises two fundamental types: Remotely-Piloted Aircraft Systems (RPAS), a class of UAS that has a “pilot” operating the Remotely-Piloted Aircraft (RPA) from a Ground-Control Station (GCS); and UAS with no remote pilot, or autonomous air vehicles (AAVs). The term “drone” although possibly inaccurate or inappropriate, refers to all types of UAS;

- There are two types of UAS operations: 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. The Key Risk Areas identified in UAS operations are: (a) airborne conflict/collision – the collision of UAs with aircraft in the air, (b) aircraft upset, (c) system failure and (d) third party conflict – the collision of UAS with people or property;

...

Ensuring Safety And Security

- There is an increasing trend in the number of reported UAS occurrences (both incidents and accidents) per year from 2010 to May 2016 inclusive (which may be due to the increasing number of drones within the EU), from which 63% are related to Airborne Conflict, which is the main Key Risk Area. This means that airspace infringements and proximity of drones to other aircraft if causing a significant number of occurrences;

- Within the previous time period, the highest number of occurrences took place in D and G airspace classes and during approach and en-route phases of the flight. Regarding the altitude, when the drones are spotted the manned aircraft is most often in the area from 0-6000 feet (≈ 0-1829 meters) above the ground and the distance from the aircraft to the drone is from 0-1000 feet (≈ 0–305 meters);

- Conventional ATM cannot be applied to unmanned aircraft and therefore the EU needs to develop a UAS Traffic Management (UTM) system that allows UAVs to fly jointly manned aircraft and implement the regulatory framework regarding the integration of UAS into busy airspace as it is European airspace. Also, the use of partially unused airspace could provide testing area and additional capacity for UAVs to prove to be at least equal to manned aircraft in terms of safety.

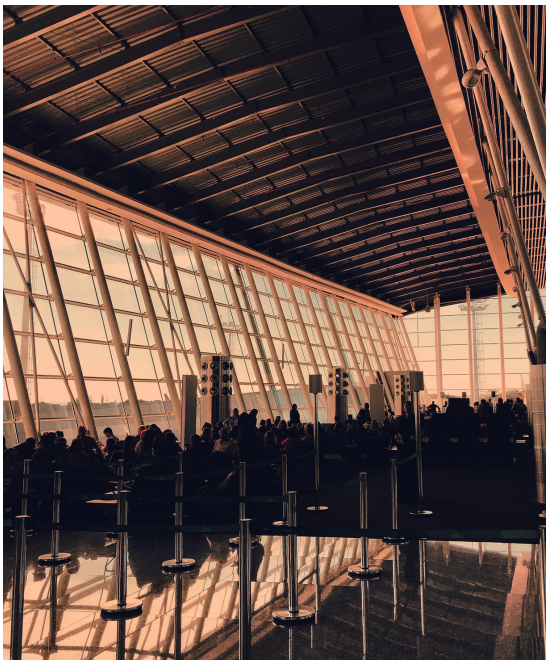
KEY ACTIONS

It is recommended that:

1. The evolution of air traffic capacity in Europe compared with the growth of air transport is assessed to identify the spare capacity available to other users like UAVs;
2. The qualifications required of operators of UAVs and other aircraft compared with airline pilots and air traffic controllers are established to ensure that aviation remains the safest means of transport;
3. The design, production, certification and maintenance procedures for UAVs and other aircraft are defined to preserve or improve on the safety levels of current airliners that operate in the same airspace;
4. The increased use of partially underused airspace is explored to enable the expansion of operations by new types of aircraft.

COMPREHENSIVE AND UNOBTRUSIVE SECURITY MEASURES

The recent societal threat of terrorist acts at airports or during flight implies the reinforcement of security measures to prevent those acts to happen, resulting in delays and queues, which are the most frequent sources of traveller dissatisfaction. While the patience and understanding of passengers are essential, there should be a minimum of delay, intrusion and disruption in the implementation of safety measures, through the use of the most appropriate equipment and airport architectures. In 2050, efficient boarding and security measures must allow seamless and non-intrusive security for global travel, with minimum passenger and cargo impact.



KEY FINDINGS

- The main types of scanning and detection devices currently deployed by European airports are based on the following existing technologies: Advanced Imaging Technology (AIT), Advanced Technology (AT) X-Ray, Boarding Pass Scanners, Bottled Liquids Scanners (BLS), Chemical Analysis Devices (CAD), Enhanced Metal Detector (EMD) and Explosives Detection Dogs (EDD) and Explosives Trace Detector (ETD);

- Passengers spend on average 20 minutes waiting in line to get to the security screening checkpoint. New technologies and procedures could significantly reduce these waiting times, allowing to process about 360 passengers per hour instead of the approximately 150 passengers per hour that are processed nowadays;

- Examples of emerging trends in technology for threat detection that could improve airport security and efficiency while reducing the burden for passengers are biometrics screening, computed tomography (CT) scanning, facial scanning and behavioural analytics. Nevertheless, all of these new technologies are in the first level of maturity, i.e., in the concept phase;

...

- 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. A new risk-based differentiation concept is introduced, which focuses its attention on “the person” in the assessment of threats, instead of focusing on the risk of the item. As a result, based on a reasoned process of selection, different people would be screened in different ways;

- The project Smart Security, a joint initiative of the International Air Transport Association (IATA) and Airports Council International (ACI), 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, through the implementation of new technologies and processes.

KEY ACTIONS

It is recommended that non-intrusive passenger screening methods and foolproof luggage checking that allow fast flow through registration, border and boarding procedures are developed.

RESILIENCE TO EXTERNAL AND INTERNAL THREATS

The EU is facing one of the greatest security challenges in its history. Threats are increasingly taking non-conventional forms, some physical such as new forms of terrorism, some using the digital space with complex cyberattacks. Nevertheless, by 2050, air vehicles must be resilient by design to current and predicted on-board and on the ground security threat evolution, internally and externally to the aircraft.

KEY FINDINGS

- Current and emerging threats to aviation security have been clustered into the following eight threat categories: 1) Improvised Explosive Devices (IED), firearms and close range destructive threats; 2) Chemical, Biological, Radioactive, Nuclear and Explosive (CBRNE) threats; 3) Ground-to-air threats; 4) Ground-to-ground threats; 5) Cyber threats; 6) Electromagnetic threats; 7) Sabotage, seizure and hijacking; and 8) Bluff threats and threats from social media;

- Currently, aviation security is primarily based on the preventive phase and is inflexible to new threats. This is also mirrored in the research landscape for aviation security once most projects concentrate on preventive measures such as the detection of CBRNE-substances. However, the aviation security system should be resilient to the evolving threat situation, thus be based on the complete resilience cycle which has the following phases: prepare (take into account), prevent (repel or thwart), protect against (absorb or mitigate), respond to (cope with) and recover from (and adapt to).

KEY ACTIONS

It is recommended that:

1. Aircraft are designed and procedures are established to (a) prevent unauthorised entry into the cockpit, (b) allow remote take-over up to safe landing in the case of an identified flight anomaly while (c) designing the system to be immune to the most sophisticated hacking;
2. An independent observatory of external risks to aircraft overflights is set up to advise airlines, or failing that, warn passengers;
3. A worldwide airliner flight monitoring system and accident data recorders are designed to ensure that accident/incident data is available regardless of time and location of occurrence

HIGH–BANDWIDTH DATA RESILIENT TO CYBER ATTACKS

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, airport and air traffic control (ATC) are more and more interlinked and, thus, depend on secure means of data exchange. In the future, it is expected an increase in this inter-connectivity, which means the air transport system will be even more vulnerable and exposed to multiple points of attacks. Taking this into account, in 2050, the air transport system must have a fully secured global high-bandwidth data network, hardened and resilient by design to cyberattacks.

KEY FINDINGS

- 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. On the other hand, the L-band Digital Aeronautical Communications System (L-DACS) and Aeronautical Mobile Airport Communications System (Aero-MACS) that are supposed to replace the current Very High Frequency (VHS) system, 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;

...

- The assessment of cyber risk involves: 1) identification and inventory of key assets – data, systems and infrastructure – that are essential to operations; 2) revision of internal controls and digital profile to identify internal vulnerabilities and external threats; 3) valuation of the cyber assets at risk using modelling and other data and technology tools;

- The vulnerabilities that need to be taken into account are: (a) in a large, complex interconnected system there are many entry points for cyber intrusion and many links to spread the cyber-attack; (b) 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;

- In order to face the future cyberattacks, firstly, it would be necessary to identify the multiple threats that could compromise aviation security (e.g. phishing threats, jamming threats, remote hijacking, distributed-denial-of-service (DDoS) attacks and Wi-Fi-based attacks) 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;

- Blockchain is one of the favourites current technologies focused on cyber-security. However, Blockchain has also some technical challenges and limitations (throughput, latency, size and bandwidth, security – the current blockchain has a possibility of a 51% attack, wasted resources, usability, etc.) that made its application in aviation, air transport and ATM uncertain, and that will require further research in the future.

KEY ACTIONS

It is recommended that:

1. The evolution of bandwidth requirements required to cope with increasing telecommunication needs associated with improved navigation, on-board systems monitoring, passenger connection and other services, is assessed;
2. Evolving standards for protection against cyberattacks are established, with different levels, the highest for flight systems and the lowest but non-trivial for ticketing, bearing on mind the risk of intrusion from lower levels.

For more information about these topics, you can access the full chapter **here**.