JOINT POSITION PAPER

Artificial Intelligence in civil aviation

ECA
Piloting Safety

IFALPA

Executive Summary

This position paper provides the perspective of European Pilots and IFALPA on the development, use, and regulation of AI in civil aviation context.

A broad view and briefing, covering topics such as human perception and assistance systems, calibrated trust, creativity and intuition, human-centered systems design, data governance, cybersecurity, training, accountability, and flight data monitoring, is contained within the paper.

ECA and IFALPA as the voice of the profession, believes that within this wide landscape there are three key, urgent challenges that need to be addressed politically or through regulation, if AI is to be an advantageous and successful addition to the aviation system.

I. DATA – RIGHTS OF AVIATION PROFESSIONALS

Most systems classified as AI either require or benefit from large datasets to train, refine or validate their functioning. Pilots, air traffic controllers, maintenance personnel, and other aviation professionals typically generate large amounts of data, such as that captured by a Flight Data Monitoring program. This practice is consented to on the basis that it is used solely for safety monitoring and investigation purposes, remains confidential, is protected against misuse (including for criminal, administrative or commercial purposes) and may not be transferred out of the defined FDM program without specific further consent.

It is essential for the acceptance of AI in aviation, and the respect and compliance with the data rights of the professionals who generate this data, that it is only used with their collective specific consent, is subject to clear regulatory safeguards, and includes provisions for periodic oversight. The ongoing value or commercial benefit of any systems this data enables should be reflected in a legal agreement that collectively compensates the involved professionals. The value of this data should not be appropriated by those who did not generate it but may hold it or wish to develop products with it.

II. LIMITS – ROLE, AUTHORITY AND LIABILITY OF AI SYSTEMS

The role of AI in the operation of a flight should always be to support the humans in the system. For this to be effective, whatever the intended capability of an AI system, it should: only present options to a pilot, never a fixed outcome. There should also be transparency to the pilot as to how these options have been selected, and the level of confidence associated with them. The pilot must remain in control of which option is chosen, if any, and initiating execution of any action, and any automation fed by an AI system must be overridable by pilot action if required.

Were decision making or executive action to be outsourced to or shared with an AI system, it may also be unclear where responsibility or liability lies between the pilot and system. This may drive unwanted behaviors intended to offload liability that conflict with best outcome decision making. The authority and therefore liability of AI systems should remain commensurate with that of any normal aircraft system.

III. SAFETY – REGULATION OF AI SYSTEMS TO EXISTING SAFETY AND TRANSPARENCY STANDARDS

AI systems, especially those onboard aircraft, in safety systems, in air traffic control, or in maintenance, must be regulated and certified to the same standard as any other system in civil aviation. In order for this to happen, the way in which they function or generate output must be transparent, open to scrutiny, and accessible in the event of failure or to permit improvement. 'Black box' systems, whose inputs, processing, and decision-making cannot be understood or traced, are therefore considered unsuitable for such applications. . Finally, simply because a system is labelled 'AI' should not mean a lower level of scrutiny or understanding is possible or required.

There has also been some focus from regulators on ensuring or creating 'trust' or 'confidence' in AI systems. An attempt to foster trust in AI systems as a branding exercise is inappropriate and will in fact compromise its effectiveness and safety level. 'Trust' should be a result of transparency and thorough certification, understanding and training of any system. Professionals interacting with AI systems should have only an appropriate level of trust in each system based on an accurate understanding of how they work and their limitations, including challenging or pressure testing AI outputs as necessary. A blind 'faith' in AI systems will introduce safety risks of its own, and is not desirable for its own sake or as a precursor to deployment.

Introduction

The integration of artificial intelligence (AI) in civil aviation is envisaged as a means to enable significant improvements in the areas of efficiency, safety and automation. At the same time, it presents new challenges for pilots, engineers and passengers, particularly in terms of perception, trust in technical systems and the role of human capabilities such as creativity and intuition.

This paper examines the impact of AI on these key human aspects.

1 HUMAN PERCEPTION AND ASSISTANCE SYSTEMS

Artificial intelligence can support decision-making processes in aviation through complex assistance systems. Nevertheless, human perception remains a critical factor. Humans can react to unpredictable situations based on sensory impressions and experiences. Humans also remain superior in knowing "what to look for". Assistance systems that complement all of the above must be designed in such a way that they do not impair the pilot's ability to perceive but rather reinforce it. Over-reliance – an excessive or uncritical dependence on automated systems – can lead to pilots neglecting their own sensory abilities, which can be dangerous in critical situations.

2 TRUST IN ASSISTANCE SYSTEMS

Trust in AI-supported systems is crucial for their successful implementation in civil aviation. Pilots and crew members must be able to trust that these systems will work reliably and provide the right support in emergencies. However, overconfidence can be problematic if it reduces the pilot's constant vigilance. The goal is to foster calibrated trust - a level of trust that is proportionate to the system's actual capabilities and limitations. This means ensuring that users neither overtrust nor undertrust the AI, but instead maintain an informed, appropriate reliance on it. The challenge is to find a balance between trust in technology and the ability of humans to intervene quickly when necessary. One must be able to understand and verify how AI reached a presented output. Transparency and traceability of the decisions made by AI systems are particularly important here to strengthen this trust.

3 CREATIVITY AND INTUITION

While AI is able to make decisions based on large amounts of data, it remains limited in terms of creative and intuitive problem solving. Creativity and intuition are human skills that play a crucial role, especially in unpredictable or new situations. An experienced pilot can use intuition and creativity to find solutions that lie outside the logical decision trees of AI systems. Whereas humans can anticipate future situations AI-based systems may stop providing responses when the limits of the operational design domain (ODD) have been reached, or even suggest "made-up solutions", so-called hallucinations, without making this clear to the end-user. It is therefore important that AI systems in aviation are not seen as a replacement but as a supplement to these unique human capabilities.

4 SYSTEM DESIGN: THE FOCUS IS ON PEOPLE

The design of AI-supported systems must always keep users in the loop. Systems based on machine learning must not disempower pilots but must offer them room for maneuver- and decision-making. The challenge is to develop systems that interact with the pilot in an intuitive way, based upon ergonomic principles, leaving them in control, while at the same time making optimal use of AI's ability to process large amounts of data.

5 DATA SELECTION AND MONITORING

Providing the AI model with the right training data is crucial to ensure the resulting outputs match the desired intentions. The AI model should be a means to an end and not an end in itself. The actions of frontline operators (e.g., flight-crew, ATCOs, maintenance personnel) should be captured as they perform their day-to-day activities, without interfering – directly or indirectly. Periodic re-evaluations and oversight must be conducted not only to account for change but also to ensure that AI systems remain aligned with technological advancements and operational needs. In addition, the data captured must be protected by clear regulatory standards in terms of privacy and against any misuse, such as the use of the data for criminal- or administrative proceedings against individuals. The way data is collected, stored and used must be transparent and considered fair by those individuals from whom the data is being collected.

6 DATA: PROTECTION, OWNERSHIP AND PRIVACY

Furthermore, pilot-derived data shall not be used for commercial purposes by manufacturers through the aggregation of such data. Safeguards must be in place to protect the ownership rights of the data and to prevent the exploitation of this data for financial or competitive advantages, ensuring that its use remains strictly within the scope of the originally certified system.

Biomonitoring technologies—such as eye tracking, heart rate monitoring, or EEG—are increasingly being explored to enhance training and operational awareness by providing real-time insights into pilot workload, attention, or fatigue. While these tools may offer valuable data for safety and performance optimization, their use must be approached with great caution. Biomonitoring data is deeply personal, and its collection raises serious ethical, legal, and privacy concerns. Clear boundaries must be established to ensure that such data is used strictly for supportive and safety-related purposes, and not for surveillance, punitive action, or commercial exploitation. Transparency, voluntary participation, and strict data protection protocols are essential to maintain trust and respect for individual rights.[1]

7 CYBERSECURITY RISKS IN AI-DRIVEN AVIATION SYSTEMS

As AI becomes more integrated into civil aviation, cybersecurity risks must be addressed to ensure safety and system integrity. AI models are vulnerable to various attacks that can manipulate their outputs, compromise data, or degrade performance. Some of the identified risks include:

Adversarial & Data Poisoning Attacks: Attackers can modify input data or corrupt training datasets to mislead AI systems, leading to incorrect decisions or unsafe recommendations.

Privacy and Model Inversion Attacks & Bias Exploitation: AI models may inadvertently expose sensitive operational or personal data, violating privacy regulations and increasing security risks. AI models with inherent biases can be manipulated to create unfair outcomes.

Insecure Output Handling: Even when AI systems function as designed, the way their outputs are interpreted or integrated into operational workflows can introduce risks. If AI-generated outputs are not validated with scrutiny, understood, or are presented without sufficient context, they may lead to incorrect system behaviour. The failure to sanitize and validate the output against its intended context may lead to unwanted situations. This risk is amplified in high-stakes and highly integrated environments like aviation.

Supply Chain Attacks: Malicious actors may introduce hidden backdoors during development or compromise AI hardware/software components, leading to potential security breaches.

Denial-of-Service & Automated AI Cyberattacks: AI systems can be overloaded with malicious queries, reducing performance, while AI-driven malware and phishing increase cyber threats.

To mitigate these risks, aviation must implement strong authentication and encryption, real-time anomaly detection, strict access controls, secure AI training and updates, and AI explainability with pilot override to ensure human control in case of anomalies. A proactive cybersecurity framework is essential to safeguard AI-driven aviation systems.

[1] See also ECA Position paper on the Use of Digital Applications for Flight Crew

8 EFFECTS ON TRAINING

The introduction of AI systems also reshapes the training requirements for pilots and technical personnel. In addition to traditional technical knowledge, pilots must increasingly learn how to interact effectively with AI-supported systems. Training in skills such as critical thinking, decision-making in stressful situations and the use of intuition are becoming increasingly important. Training must ensure that pilots continue to develop their creative and intuitive skills despite high levels of automation.
Additionally, AI-based applications and tools are increasingly being integrated into training and performance evaluation. These systems can assist in developing training materials, capturing, analyzing, grading and therefore evaluating performance data. However, their implementation must consider key factors for all personnel involved in developing, certifying, administering, conducting, and receiving training:

- Transparency and understandability of AI models to ensure trainees and instructors can interpret AI-driven evaluations.
- Mitigation of biases within AI models, systems, and tools to prevent unfair assessments.
- Data protection and privacy considerations to safeguard sensitive training and performance data.
- Comprehensive training on the use of AI-driven systems to ensure personnel can effectively integrate AI insights while maintaining human oversight.

9 CONTROL AND ACCOUNTABILITY IN AI-DRIVEN AVIATION

With the increasing integration of AI-based systems into aviation operations, maintaining clear lines of control and accountability is essential. While AI can enhance decision-making and automation, ultimate responsibility still lies with human operators, including pilots, air traffic controllers (ATCOs), and maintenance personnel. As long as these end-users remain accountable for the outcomes of AI-assisted decisions, they must retain a commensurate degree of control, understanding and authority over these systems.

AI should function as a support tool rather than an autonomous decision-maker. Pilots must have the ability to override AI-driven actions when necessary, ensuring human judgment prevails in complex or unforeseen situations. Similarly, ATCOs and maintenance personnel must be able to audit, adjust, and challenge AI outputs, particularly when safety is at stake. A human should always be the final authority in decision-making. Transparent decision-making processes and AI explainability mechanisms are crucial to maintaining operator confidence and ensuring AI recommendations can be critically assessed. To ensure transparency and understandability, while also allowing for improvements of the application, one must be able to reliably reconstruct what was shown to a human operator at any given time without bias from the learning model.

Furthermore, any AI elements integrated into aviation must be regulated to the same standards as other critical components. This includes ensuring full transparency of how the system functions, avoiding “black box” AI models whose decision-making logic cannot be understood or traced. AI systems must meet equivalent risk and safety requirements, and be fully integrated into the Safety Management Systems (SMS). Continuous performance monitoring, risk assessment, and iterative improvement of AI components must be maintained on par with all other safety-critical systems in aviation.

To uphold accountability, regulatory frameworks must clearly define who is responsible when AI systems increasingly influence decision-making. This includes establishing guidelines on AI's role, limits of automation, and the responsibilities of human operators. As AI continues to evolve, ensuring a balance between automation and human oversight will be key to increasing safety in civil aviation.

10 AI IN FLIGHT DATA MONITORING (FDM)

The application of AI to Flight Data Monitoring (FDM) holds potential, particularly in recognizing complex patterns and anomalies within large datasets that would be difficult or time-consuming for humans to detect. AI tools can enhance early detection of safety risks and operational trends by sifting through vast amounts of critical flight data efficiently. However, despite these advantages, human oversight remains essential. FDM is fundamentally aimed at understanding the underlying causes of abnormal patterns or deviations, not just detecting them. AI may identify correlations or outliers, but without human interpretation, there is a risk of misattributing causes or overlooking critical operational nuances. Therefore, while AI can support FDM by enhancing data processing capabilities, final analysis and judgment must remain in the hands of experienced personnel to ensure that findings are correctly contextualized and actionable.

Conclusion

The future of civil aviation will be influenced by the integration of artificial intelligence. However, it is essential that the development of these systems not only takes humans and their unique abilities - such as perception, creativity and intuition - into account, but also specifically supports them, keeping them at the core of the system.

Maximizing the benefits of AI-usage in civil aviation will rely on the human ability to build systems that enhance, rather than replace, human judgment. This includes ensuring that AI systems remain a support tool whose authority and liability are commensurate with other certified aviation systems, that pilots retain full control and override capability, and that any automation fed by AI is fully transparent in how outputs are generated and the confidence levels attached to them.

Effective integration of AI will only be possible with highly transparent AI systems, full traceability of their decision-making, continuous effort to build calibrated trust in the new technology, dedicated pilot training on AI use, strong protection of data privacy and the ownership rights of the professionals who generate operational data, as well as cybersecurity awareness to address the existing risks. Any use of professional-generated data must have collective specific consent, be subject to clear regulatory safeguards, and include provisions for periodic oversight.

In the safety-critical domain of commercial aviation, the deployment of new systems or technologies and particularly any reliance on them must be approached with caution, ensuring they are fully understood by those who operate them and that robust mechanisms for oversight and control are in place before integration into operations.

Synopsis

Human Perception and Assistance Systems
AI assistance systems may enhance decision-making in future applications, but human perception and judgment remain essential. These systems should support, not replace, pilot input and decision making to avoid dangerous over-reliance on automated systems.

Trust in Assistance Systems
Successful implementation of AI in aviation requires calibrated trust, that means pilots must rely on systems appropriately without overconfidence or doubt. Transparency and traceability of AI decisions are key to building such balanced trust.

Creativity and Intuition
AI can process vast data but cannot provide human creativity and intuition, which are vital in unpredictable situations. Thus, AI should supplement rather than replace human problem-solving abilities in aviation.

System Design: The focus is on People
AI-supported systems in aviation should be designed around pilots, ensuring intuitive interaction, and preserving their decision-making authority while leveraging AI's data-processing strengths.

Data Selection and Monitoring
AI systems in aviation must be trained on carefully selected, transparently collected data that reflect real operational practices without interfering with frontline work. Continuous oversight and periodic re-evaluations will be essential to keep systems aligned with evolving needs, while strict regulations ensure data privacy, fairness, and protection against misuse.

Data: Protection, Ownership and Privacy
Pilot-derived data must not be used for others' commercial benefit, with strict safeguards in place to protect ownership rights and prevent exploitation beyond certified system use. Any possible usage of biomonitoring data requires transparency, voluntary participation, and strict protection to avoid ethical, legal, and privacy violations.

ECA Piloting Safety
IFALPA

Cybersecurity Risks in AI-Driven Aviation Systems
AI-driven aviation systems face multiple cybersecurity risks, including data manipulation, privacy breaches, biased outcomes, insecure output handling, supply chain attacks, and AI-targeted cyberattacks. Mitigation requires robust security measures, real-time monitoring, explainable AI, and human oversight to maintain safety and system integrity.

Effects on training
In the future, pilots may need to combine traditional technical knowledge with the ability to work effectively use AI systems, while maintaining critical thinking, decision-making, and intuitive skills despite high automation. Also, where AI tools are used to support training , they must remain transparent, unbiased, privacy-protected, and accompanied by comprehensive instruction to ensure proper human oversight. Pilot performance evaluation should only ever be decided by trained pilots.

Control and Accountability in AI-Driven Aviation
As AI becomes more integrated into aviation, humans should retain executive control and accountability, with AI serving only as a support tool. Transparent, explainable AI, rigorous regulation, and continuous monitoring will be essential to ensure safety, allow human oversight, and maintain clear lines of responsibility.

AI in Flight Data Monitoring (FDM)
AI can enhance Flight Data Monitoring by efficiently detecting patterns, anomalies, and safety risks in large datasets. However, human oversight remains essential, as experienced personnel must interpret findings to ensure accurate context and actionable insights.

ECA
European Cockpit Association

IFALPA