Dean&Francis
ISSN 2959-6157

Reliability and Safety Analysis of Intelligent Flight Control Systems for Civil Aircraft

Haoyang Sun[1, *]

[1]School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, S102TN, UK
*Corresponding author: sunhysun@outlook.com

Abstract:

Civil aviation is moving toward intelligent flight control. This shift improves automation and operational efficiency. However, the use of intelligent systems also introduces new challenges for reliability and safety. This study investigates key reliability measures for intelligent flight systems. These include rates of in-flight interruptions and delays. It also examines the maintenance technologies that support these systems. One important trend is the move to data-driven predictive maintenance. This approach uses big data and machine learning. Training for maintenance technicians is also a key factor for overall system reliability. The study also looks at risks from cybersecurity threats. Examples include ADS-B spoofing attacks. Results show that intelligent flight systems in civil aircraft need to combine advanced methods. These methods include reliability and safety co-design, explainable AI (XAI), and digital twin verification platforms. Together, they help create a defense with multiple layers. A key part of this is strict network separation between critical and non-critical areas. Looking ahead, integrated frameworks and cooperation across different fields will be important. This will support further progress in intelligent flight systems toward improved reliability and safety.

Keywords: Intelligent flight control systems; reliability and safety; predictive maintenance; explainable AI.

1. Introduction

With the development in artificial intelligence, big data technology and the Internet of Things, civil aviation is becoming more intelligent and autonomous. Intelligent flight control systems bring together perception, decision-making and control, which improves automation and operational efficiency in aviation. However, these intelligent systems also create new challenges for reliability and safety. In aviation, safety standards are very high. Any system failure or security issue could lead to serious outcomes. Therefore, research on the reliability and safety of intelligent flight systems in civil aircraft is important and

ISSN 2959-6157

has practical value [1].

2. Reliability of Intelligent Flight Control Systems

2.1 Introduction

The reliability of an intelligent flight control system is the probability and ability of the system to perform all assigned functions successfully without error under specified conditions and for a specified time. In addition to the stability of hardware, the reliability of an intelligent flight control system also depends on the robustness of software algorithms, the reliability of input data, and the level of human–machine interaction.

According to Pei et al. (2024), the reliability of civil aircraft includes interruption rate, delay rate, cancellation rate and unscheduled component replacement rate. These parameters are interconnected and form a multi-level reliability framework including aircraft level, system level and function level objectives [2]. Intelligent flight systems make the monitoring and assurance of these parameters more complicated.

Generally, intelligent flight systems adopt certain systematic architectures and redundancy designs to ensure the reliability of the entire system. In traditional flight processes, the reliability of systems mainly depends on the pilots' individual skills and experiences, which may vary greatly among different operators. However, intelligent flight control systems can ensure the same level of operational performance based on certain systematic algorithms and experiences.

In recent years, the application of artificial intelligence technology in aviation safety has developed rapidly. Fault prediction, risk management, and decision-making are the main application scenarios of artificial intelligence in aviation [3]. Machine learning and deep learning technologies have become important means to improve aviation reliability and safety, and are widely used in accident analysis, pilot state monitoring, system health, and many other links.

2.2 The Role of Data-Driven Approaches and Intelligent Maintenance in Enhancing Reliability

Although intelligent flight control with flight control algorithms improves reliability through consistency, the performance of the two systems is data-intensive. Hence, data-related issues significantly affect the reliability of intelligent flight systems in civil aviation. However, aviation intelligent systems are prone to data contamination, labeling errors, and adversarial attacks [4]. These anomalies may cause model performance degradation and even mislead intelligent decisions. In addition, due to the "black-box" characteristics of artificial intelligence models, the modes of artificial intelligence faults are harder to predict and interpret than those of conventional flight control systems. This adds to the difficulty of reliability assurance.

With the development of big data and artificial intelligence technologies, data-driven predictive maintenance has gradually become an important method to enhance aircraft reliability [5]. Ahmed pointed out that machine learning–based predictive maintenance systems can analyze historical and real-time data to detect early indicators of component failures and thus prevent unexpected component failures and related operational failures [6]. For example, Rolls-Royce used AI in engine health management and achieved significantly higher operational safety and economic efficiency. Furthermore, the application of intelligent support systems such as the Electronic Flight Bag (EFB) and Health and Usage Monitoring System (HUMS) provide pilots and maintenance personnel with richer situational information and decision support. This is because maintenance training is an important aspect of reliability engineering, and aircraft maintenance is the main cause of accidents [7]. These systems predict faults and manage lives using data from onboard sensors, maintenance history, and environmental conditions, thereby optimizing maintenance and enhancing the reliability and availability of aircraft.

3. Safety of Intelligent Flight Control Systems

3.1 Safety of Intelligent Flight Systems

The safety of an intelligent flight control system (IFCS) is defined as the ability of an IFCS to perform its designated functions without causing the aircraft to enter a hazardous condition or cause personal injury or property damage. Therefore, safety is the life line of civil aviation.

Intelligent flight systems inherently have stringent requirements for functional safety. This means that the system should do the right thing when presented with an input and, more important, do a good job in handling failures. Traditional aviation safety engineering includes well-defined methodologies specified in standards such as SAE ARP4761 (Safety Assessment Process) and ARP4754A (Systems Development). These standards require that the process of hazard analysis, risk assessment, and definition of Design Assurance Levels (DALs) be strictly followed. The level of rigor required in development is correlated

with the severity of failure conditions.
However, the inclusion of intelligence, e.g., IFCSs based on AI and ML, presents new safety concerns that go beyond what traditional standards are intended to address. While deterministic algorithms exhibit well-defined behaviour, ML models can be considered ‚black boxes' and their behaviour is sensitive to the completeness and quality of training data. Hence, the V&V challenges of an IFCS also include ensuring the safety of the aforementioned intelligent components, which must guarantee robustness to out-of-distribution (OOD) data, sensor degradation and unknown environmental conditions (e.g., lightning or icing of sensors). V&V of these aspects as well as mechanisms to ensure robustness via system integrity, fault-tolerance (e.g., dissimilar sensors, triple modular redundancy) and provision of safe ‚fallback' or ‚degradation' modes are part of the safety architecture considerations.

3.2 Cybersecurity of Intelligent Flight Systems

Beyond functional safety, the intelligent flight system must also be resilient to potential cybersecurity threats. As a highly connected Cyber-Physical System (CPS), the intelligent flight system of tomorrow has a rapidly expanding attack surface and a lucrative target. Ukwandu et al. [8] stated that the primary cyber threats to the cyber security of aviation come from Advanced Persistent Threat (APT) groups sponsored by Nation States. Their objectives include stealing intellectual property, surveillance and impairing the aviation capabilities of other countries.
The attack vectors are plentiful, starting from ground-to-air communication links to onboard networks and maintenance ports. For instance, Automatic Dependent Surveillance–Broadcast (ADS-B) is a core enabling technology in modern aviation surveillance. However, as stated by Sampigethaya et al. [9], the unencrypted and unauthenticated broadcast nature of the standard makes it vulnerable to spoofing, jamming and message injection attacks. These attacks are both easy and practically feasible for a moderately skilled attacker to launch. This is because the protocol lacks basic security such as authentication and message integrity, and encryption [10]. If these vulnerabilities were to be exploited, they could result in the creation of ‚ghost' aircraft, diversion of flight paths, loss of communications and even collision avoidance opportunities by providing false situational awareness to pilots and air traffic control.
Therefore, security-by-design principles must be incorporated at the system design stage; a „bolt-on" security approach is insufficient for safety-critical systems. A robust, multilayered Defense-in-Depth architecture is essential. This architecture must combine strong encryption technologies for data links (like ADS-B and ACARS), strict network segmentation to isolate critical flight control domains from non-critical cabin systems (e.g., using Avionics Full-Duplex Switched Ethernet - AFDX gateways), and robust Intrusion Detection Systems (IDS) specifically designed for avionics protocols. Furthermore, real-time monitoring mechanisms and a secure software development lifecycle (SSDLC) are required to ensure the overall safety and resilience of intelligent flight systems against these evolving cyber threats.

4. Co-Design of Reliability and Safety

The reliability and safety of intelligent flight control systems are not independent attributes but are closely related and mutually influential. A system cannot be considered reliable if it is not reliable, and a system cannot be considered truly reliable if its failures lead to safety consequences. This interdependence implies that the systems must be designed and analysed together..
Koschuch et al. [11] recommended that the causal chains of reliability and safety should be combined into a single analytical framework, thus forming an overall "fault–error–failure–hazard" propagation model: a fault (e.g., a hardware defect / bug) causes an error (a deviation from the correct state), leading to a functional failure (loss of a required function), which may result in a hazard (a condition leading to a safety incident). This is important because developers can follow a single initiating event, such as a security vulnerability, through the operational chain: a single security vulnerability may lead to system errors, which may in turn cause system functional failures that may lead to a safety incident.

4.1 The Necessity of Integrated Assurance

Although their goals are different (reliability ensures that a system is available and its performance is consistent over time; safety ensures that the system does not enter a hazardous state), the design activities for reliability and safety must converge. In modern, complex intelligent systems, there is a high risk that Common-Cause Failures (CCF) such as data corruption events or generic software faults simultaneously decrease reliability and safety. Hence, a purely sequential approach (design for reliability; next design for safety) is not sufficient.
The increase of AI/ML components make this separation even more challenging. The system may be technically reliable (i.e., running consistently) but unsafe due to a limitation in the intelligent algorithm's perception/decision boundary, an issue referred to as Safety of the Intended Functionality (SOTIF). This calls for an integrated approach that includes:

ISSN 2959-6157

Functional Safety (ARP4754A/4761): Handle known deterministic hardware/software faults.
Cybersecurity: Handle malicious faults & external attacks (interphase with Section 3.2).
SOTIF: Handle non-malicious algorithm limitations in complex novel operating environments.

4.2 Co-Engineering Methodologies

Based on the analysis above, co-engineering approach must be adopted in the development of intelligent flight control systems to integrate reliability engineering and safety engineering starting from the conception. The holistic dependability assurance can rely on using analysis techniques bridging traditionally separate domains:
Integrated Risk Assessment: Joint risk assessments must be performed, where the results of Threat Modeling (from cybersecurity) and Failure Mode and Effects Analysis (FMEA) (from reliability) directly feed into Fault Tree Analysis (FTA) and Safety Assessment Process (SAP), such that a cyber-attack vector is treated as a potential fault mode leading to an unacceptable safety hazard.
Unified Architectural Design: The architecture must have shared features that serve both ends. For example, triple modular redundancy (TMR) is a reliability mechanism; however, masking hardware errors directly benefits the overall safety function. Similar to reliability, strict network segmentation (a cybersecurity feature) also increases reliability by preventing a failure in a non-critical system from propagating to the flight control system.
The Safety/Dependability Case: The final assurance argument should be a coherent Dependability Case (a superset of the conventional Safety Case) that evidence-based argument that the system, including its intelligent components, satisfies both its quantitative reliability requirements (e.g., Mean Time Between Failures) and its qualitative safety requirements (e.g., absence of catastrophic risk) throughout its entire lifecycle.
Through a co-engineering approach, aviation organizations can transcend viewing reliability and safety as separate checklists and manage them as a single common goal towards the safe and reliable long-term operation of next-generation intelligent aircraft.

5. Challenges and Future Directions

Although the application of intelligent flight control technology shows distinct advantages over traditional manual operation in terms of reliability and safety, there are still many challenges to its practical application. Based on the analysis of related literature, these challenges can be generalised into the following four aspects.
1) Data Quality and Standardisation: Intelligent models require large amounts of high-quality labelled data. Aviation data are currently scattered, heterogeneous and lack standardisation.
2) System Complexity and Certification Difficulty: The behaviour of intelligent systems cannot be fully predicted, and current airworthiness standards, such as ISO 26262 and ARP4754, cannot fully cover the behaviour of autonomous flight.
3) Human–Machine Collaboration Reliability: The division of responsibilities and interaction methods between pilots and intelligent systems are yet to be determined.
4) Conflict Between Cybersecurity and Real-Time Performance: Encryption and security mechanisms may cause communication delays, and thus affect the real-time performance of the control system.
Future research on the reliability and safety of intelligent flight systems should focus on the following aspects.
1) Building an integrated reliability–safety framework for intelligent flight control, including functional safety, information security and safety of intended functionality.
2) Encouraging the use of explainable AI in aviation to improve model interpretability.
3) Developing digital-twin-based virtual verification platforms to support testing and certification of intelligent flight systems.
4) Enhancing cross-domain collaboration to facilitate experience sharing and standardisation among the aviation, automobile and communication industries.

6. Conclusion

The research on the reliability and safety of intelligent flight control systems for civil aircraft is of great significance. This paper analysed the challenges and opportunities faced by intelligent flight systems for civil aircraft from the perspectives of reliability parameters, cybersecurity, data-driven maintenance and human–machine collaboration based on several recent studies. In the future, through continuous technological innovation, standard improvement and cross-industry collaboration, it is hoped that we can achieve safer, more reliable and more efficient intelligent aviation transportation technology, which will accelerate the process of civil aviation full-scale intelligentization and, eventually, realize autonomous flight in the aviation field.

References

[1] N. Muecklich, I. Sikora, A. Paraskevas, and A. Padhra, "Safety and reliability in aviation – A systematic scoping review of normal accident theory, highreliability theory, and resilience engineering in aviation," Safety Science, 2023, vol. 162, p.

106097.
[2] Pei. Y, Ni. Z, Gong Q, and Li. S, "Reliability Improvement Methods for Civil Aircraft: A Review," 2024 Global Reliability and Prognostics and Health Management Conference (PHM-Beijing), Beijing, China, 2024, pp. 1-8.
[3] Demir, G., Moslem, S. & Duleba, S. Artificial Intelligence in Aviation Safety: Systematic Review and Biometric Analysis. Int J Comput Intell Syst, 2024, 17, 279.
[4] Li. J, Peng. W, Zeng. Z, and Xu. M, "A Review of Reliability Verification Technology for Aviation Intelligent Systems," 2024 11th International Conference on Dependable Systems and Their Applications (DSA), Taicang, Suzhou, China, 2024, pp. 172-181.
[5] Salvador. M, Yacout. S, and AboElHassan. A, "Using Big Data and Machine Learning to Improve Aircraft Reliability and Safety," Annual Reliability and Maintainability Symposium (RAMS), 2022.
[6] Ahmed, Waqas. "Artificial Intelligence in Aviation: A Review of Machine Learning and Deep Learning Applications for Enhanced Safety and Security." Intelligence 3, 2025: 100013.
[7] Serdar. D, "Improving aircraft safety and reliability by aircraft maintenance technician training," Engineering Failure Analysis, 2017, vol. 82, pp. 687–694.
[8] Ukwandu, Elochukwu, et al. "Cyber-security challenges in aviation industry: A review of current and future trends." Information 13.3, 2022, 146.
[9] Sampigethaya, Krishna, and Radha Poovendran. "Aviation cyber–physical systems: Foundations for future aircraft and air transport." Proceedings of the IEEE 101.8, 2013: 1834-1855.
[10] Habler. E, Bitton. R, and Shabtai. A, "Assessing aircraft security: A comprehensive survey and methodology for evaluation," ACM Computing Surveys, 2023, vol. 56, no. 4, pp. 1–40.
[11] Koschuch. M, Sebron. W, Szalay. Z, Török. A, et al, "Safety & Security in the Context of Autonomous Driving," 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), Graz, Austria, 2019, pp. 1-7.