I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Air Transport Safety and Security: Current Developments

Aparna Malhotra [1*], Ojaswini Malhotra [3]
[1] Professor, Department of Law, MMH College, Ghaziabad, Uttar Pradesh, India
[2] Lecturer/Teaching Fellow, Department of Law, MMH College, Ghaziabad, India

Corresponding Author: * Aparna Malhotra

DOI: https://doi.org/10.5281/zenodo.20846716

Abstract

Air transport remains one of the safest modes of travel, but the modern risk landscape is no longer defined only by traditional accidents or hijacking scenarios. Contemporary aviation governance now has to manage cyber threats, unmanned aircraft systems, insider risks, biometric data practices, artificial intelligence, and the uneven safety capacity of airports and regulators across regions. This article examines current developments in air transport safety and security with a focus on the 2025–2026 policy cycle. It argues that the sector is moving from a narrow, reactive model toward a more integrated and intelligence-led framework that links operational safety, aviation security, cybersecurity, and digital governance. Drawing on ICAO strategy documents, IATA safety reporting, NASA's recent blockchain trials, and recent Indian aviation-security analysis, the article identifies five major trends: stronger global strategic coordination, deeper digitalization of airports and security processes, expansion of cybersecurity governance, growing concern over drones and new entrants, and continued dependence on data-driven oversight. The article concludes that the central challenge is not a lack of rules, but the gap between advanced global frameworks and uneven implementation on the ground.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 10-05-2026
- **Accepted:** 16-06-2026
- **Published:** 25-06-2026
- **IJCRM:**5(SP1); 2026: 11-14

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Malhotra A, Malhotra O. Air Transport Safety and Security: Current Developments. Int J Contemp Res Multidiscip. 2026;5(SP1):11-14.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Air transport, aviation safety, aviation security, cybersecurity, ICAO, IATA, drones, blockchain.

1. INTRODUCTION

Air transport has long been described as the safest mode of transport because it is built on layered regulation, standardised procedures, technical redundancy, and a strong reporting culture. Yet the phrase can become a bit too comfortable if repeated without context. A system may be statistically safe and still face severe vulnerability when risk changes shape faster than institutions adapts. That is precisely the current problem in aviation.

Safety and security overlap, but they are not identical. Safety is generally concerned with preventing accidents, incidents, and operational harm arising from technical, human, environmental, or organisational causes. Security, by contrast, focuses on protecting civil aviation against acts of unlawful interference such as sabotage, terrorism, insider abuse, or malicious technological disruption. ICAO's Annex 17 remains the core international instrument for aviation security, setting Standards and Recommended Practices to prevent and suppress acts of unlawful interference (ICAO, 2025a). ICAO's current strategic framing also treats safety and security as a single foundational goal: every flight should be safe and secure, with continuous protection for passengers, cargo, staff, and the public (ICAO, 2025b).

Recent scholarship mirrors this shift from siloed thinking to integrated governance. Aviation's high safety standards are continually challenged by unlawful interference and the need for constant technological upgrading, while Shudharshini (2025) argues that recent aviation-security reforms increasingly rely on preventive, intelligence-driven, and technology-enabled approaches. These observations are especially relevant in a period where cybersecurity, biometric identity systems, rogue drones, and AI-assisted monitoring are no longer future possibilities but present operational issues.

2. Global Governance is Being Reset Around Long-Term Resilience

One of the clearest recent developments is the restructuring of aviation governance at the international level. ICAO's Strategic Plan 2026–2050 projects global air traffic reaching 12.4 billion passengers by 2050 and frames the sector's future around a safe, secure, and sustainable international civil aviation system (ICAO, 2025c). In other words, the old model of simply preserving existing performance is no longer enough. The governance logic is now resilience under growth.

This strategic change became more concrete at the 2025 ICAO Assembly. ICAO reported that Member States adopted updated global frameworks for safety, security, cybersecurity, air navigation, and innovation, including the 2026–2028 Global Aviation Safety Plan and the second edition of the Global Aviation Security Plan (GASeP) (ICAO, 2025d). The Assembly also linked these updates to emerging risks such as weaponised unmanned aircraft systems, Global Navigation Satellite System interference, and the need for stronger cyber resilience (ICAO, 2025d).

The significance of GASeP lies in its insistence that States and industry share responsibility for implementation. Annex 17 of Convention on International Civil aviation relates to security. SARPs tenth edition, April 2017 issued by ICAO relates to Annex 17 Security: safeguarding International Civil Aviation Against Acts of Unlawful Interference (ICAO, 2023). GASeP emphasises that States must ensure Annex 17 Standards are fully and effectively implemented through their national civil aviation security programmes, while industry stakeholders also play a crucial role in delivering security enhancements (ICAO, 2023). That shared-responsibility model matters because modern aviation threats do not respect neat institutional boxes. A weak contractor, a poorly secured regional airport, a software vulnerability, or a cross-border intelligence gap can all undermine the same network.

3. Digitalization is Reshaping Both Safety and Security

Air transport safety and security are increasingly mediated through digital systems. Passenger identity verification, baggage tracing, screening analytics, flight data exchange, and airport surveillance are all becoming more automated, networked, and data-intensive. This shift creates efficiency and situational-awareness gains, but it also expands the attack surface. The shiny machine becomes a larger shiny machine with more wires sticking out of it.

Recent Indian developments show how quickly this digital transition is unfolding. Shudharshini (2025) describes the DigiYatra initiative as a major biometric-processing reform that uses facial recognition for seamless passenger processing, alongside wider deployment of advanced imaging scanners, explosive detection systems, AI-based CCTV, and RFID-enabled cargo tracking. The same article notes pilot use of blockchain tracking for high-value cargo and a broader move toward real-time surveillance and traceability in airport operations.

At the research frontier, NASA has begun testing blockchain-based systems designed to protect flight data from interception or manipulation. In January 2026, NASA reported successful drone-based testing of a decentralised blockchain framework that could securely transmit and store registration data, flight plans, and telemetry in real time, with potential application to autonomous air traffic management, urban air mobility, and high-altitude operations (NASA, 2026). This is not evidence that blockchain is a magic safety dust to sprinkle on aviation. It is, however, evidence that trusted data exchange is now seen as a core safety-and-security problem rather than a backroom IT detail.

4. Cybersecurity: Technical Subtopic to Strategic Necessity

Cybersecurity is now central to aviation governance because the system depends on digital trust. Airports, airlines, air navigation services, baggage systems, passenger databases, and maintenance platforms are all potential targets for ransomware, data manipulation, denial-of-service attacks, and stealthier integrity failures. In that setting, a cyber incident is not merely an information-security issue; it can become a safety issue very quickly

ICAO's Aviation Cybersecurity Strategy explicitly states that the global civil aviation sector should be resilient to cyber-attacks while remaining safe and secure, and it organises this objective around seven pillars: international cooperation,

governance, legislation and regulation, cybersecurity policy, information sharing, incident management, and capacity building (ICAO, 2025e). The 2025 ICAO Assembly reinforced this approach by calling on States to implement the strategy and action plan, designate competent authorities, and build robust cybersecurity risk management frameworks (ICAO, 2025d). National practice is starting to reflect this shift. Shudharshini (2025) reports that India's Directorate General of Civil Aviation issued new cybersecurity guidelines in 2023, including vulnerability assessment and penetration testing requirements for civil aviation stakeholders. The same analysis notes ongoing concern about cyber threats at major airports and the need for stronger coordination across the national aviation-security architecture. The lesson is fairly plain: cybersecurity cannot be bolted on after digital systems are deployed; it must be designed into aviation governance from the outset.

5. New Entrants and New Threat Actors are Changing the Risk Map

Another major development is the rise of drones, remotely piloted systems, and advanced air mobility concepts. These technologies promise economic and operational benefits, but they also complicate surveillance, conflict-zone risk, airport perimeter protection, and airspace management. ICAO's 2025 Assembly outcomes specifically highlighted the need for legally compliant and safe integration of RPAS, UAS, and advanced air mobility, together with stronger security guidance and international cooperation to manage cross-border risks (ICAO, 2025d).

India offers a useful example of how this threat is being operationalised in law and policy. Shudharshini (2025) notes that India's Drone Rules 2021 and Counter Rogue Drone Technology Guidelines 2022 prohibit unauthorised drone operations near airports and seek to empower authorities to detect and neutralise suspicious systems. Yet the same study points out that anti-drone capabilities remain costly and unevenly deployed, particularly at smaller regional airports. That tension between policy ambition and implementation capacity is not uniquely Indian; it is a structural problem across global aviation.

The broader security challenge is that acts of unlawful interference are no longer limited to classic hijacking or airport attacks. Annex 17 still provides the legal backbone for preventing unlawful interference (ICAO, 2025a), but the operational meaning of interference has widened to include insider threats, digital manipulation, supply-chain compromise, and exploitation of airport contractors or service providers. Security, in other words, has become more distributed and less theatrical. Fewer movie villains; more messy system vulnerabilities.

6. Strong Operational Safety Performance, but not Uniform

Despite emerging threats, aviation safety performance remains strong by historical standards. IATA's 2025 Annual Safety Report states that global safety performance remained strong overall and continued its long-term improvement trajectory, even though fatal accidents and onboard fatalities rose in 2025 because of a small number of severe events (IATA, 2026a). The report identifies take-off, landing, and ground operations as the main concentration points for current operational risk, with runway excursions, landing gear events, and ground damage among the most common occurrences (IATA, 2026b).

This point matters because public debate often swings between two bad extremes: either 'aviation is perfectly safe' or 'one bad year means the system is failing'. The evidence supports neither cartoon. IATA's data suggest a sector that remains highly safe overall, but one where risk is concentrated in rare, high-consequence events and where regional disparities remain significant (IATA, 2026a; IATA, 2026b). For example, Africa recorded the highest accident rate of any region in 2025, while other regions performed materially better on the same metric (IATA, 2026c).

This unevenness reinforces ICAO's emphasis on capacity-building, auditing, and regional cooperation. The 2025 ICAO Assembly recognised the importance of regional safety oversight organisations and related cooperative mechanisms in assisting States with limited technical capacity and resources (ICAO, 2025d). Current developments in aviation safety are therefore not only about new technology, but also about who has the institutional depth to use standards, audits, training, and data effectively.

7. Persistent Challenges

Three persistent challenges stand out. First, implementation gaps remain the weak joint in the whole machine. Global frameworks are becoming more sophisticated, but smaller airports, lower-capacity regulators, and outsourced service chains often lag behind. Shudharshini (2025) identifies regional airports, insider threats, inconsistent enforcement, and fragmented coordination as continuing vulnerabilities in India; similar problems are visible in other parts of the world whenever capacity does not match regulatory ambition.

Second, digital security and civil-liberties concern now move together. Biometric processing, predictive analytics, AI-assisted surveillance, and large-scale data sharing may improve throughput and threat detection, but they also raise questions about privacy, governance, data retention, bias, and due process. A system that is secure but opaque can still undermine trust, and trust is not decorative in aviation; it is functional.

Third, strategic adaptation must keep pace with technological convergence. Safety, security, cyber resilience, and innovation governance can no longer be managed as separate domains. ICAO's recent frameworks already reflect this integration by linking zero fatalities, cybersecurity implementation, AI governance, conflict-zone risk, and new entrant aircraft into one strategic

picture (ICAO, 2025b; ICAO, 2025d). The task now is to make those linkages real in everyday operational practice.

8. CONCLUSION

Current developments in air transport safety and security show a sector in transition from mature rule-based control toward adaptive, data-driven, and network-aware governance. The most important changes are not symbolic. They are visible in ICAO's 2026–2050 strategic framework, the updated Global Aviation Security Plan, the elevation of cybersecurity to a

strategic pillar, experimentation with secure data architectures such as blockchain, wider use of biometric and AI-enabled airport systems, and stronger attention to drones and advanced air mobility.

At the same time, the core truth remains delightfully unglamorous: aviation safety and security depend on disciplined implementation, transparent data, competent oversight, and international cooperation. The challenge ahead is not just inventing smarter tools, but ensuring that all parts of the aviation ecosystem, from major hubs to regional airports, from regulators to contractors, can actually use them well. That is where current developments become real safety and security, rather than shiny policy wallpaper.

REFERENCES

1. International Air Transport Association. IATA releases 2025 safety report. Montreal: IATA; 2026 Mar 9. Available from: https://www.iata.org/en/pressroom/2026-releases/2026-03-09-01/
2. International Air Transport Association. IATA Annual Safety Report Executive Summary. Montreal: IATA; 2026. Available from: https://www.iata.org/en/publications/safety-report/executive-summary/
3. International Civil Aviation Organization. Global Aviation Security Plan. 2nd ed. Montreal: ICAO; 2023. Available from: https://www.icao.int/sites/default/files/sp-files/Security/Documents/GLOBAL%20AVIATION%20SECURITY%20PLAN%202nd%20Ed.EN.pdf
4. International Civil Aviation Organization. Annex 17 – Aviation security. Montreal: ICAO; 2025. Available from: https://www.icao.int/aviation-security-policy-section/Annex17
5. International Civil Aviation Organization. Every flight is safe and secure. Montreal: ICAO; 2025. Available from: https://www.icao.int/strategic-goals/every-flight-safe-and-secure
6. International Civil Aviation Organization. ICAO strategic plan 2026–2050. Montreal: ICAO; 2025 [cited 2026 Jun 20]. Available from: https://www.icao.int/about-icao/Council/strategic-plan-2026-2050
7. International Civil Aviation Organisation. ICAO enhances global aviation safety and security framework. Montreal: ICAO; 2025 Oct 3. Available from: https://www.icao.int/news/icao-enhances-global-aviation-safety-and-security-framework
8. International Civil Aviation Organization. Aviation cybersecurity strategy. Montreal: ICAO; 2025. Available from: https://www.icao.int/aviation-cybersecurity/strategy
9. National Aeronautics and Space Administration. NASA develops blockchain technology to enhance air travel safety and security. Washington (DC): NASA; 2026 Jan 16. Available from: https://www.nasa.gov/general/nasa-develops-blockchain-technology-to-enhance-air-travel-safety-and-security/
10. Shudharshini E. Recent developments in aviation security in India – A critical analysis. Int J Creat Res Thoughts. 2025;13(11).