USI Monograph No 5 - 2026

Certification of Artificial Intelligence in Aviation: Global Approaches, Challenges, and Roadmap for India with Focus on the Indian Aviation

Air Commodore Mukhvinder Pal Singh Virk

Sumedh Singh Virk

(Estd. 1870)

United Service Institution of India (USI)

New Delhi

About the Monograph

This paper examines the rapidly expanding integration of Artificial Intelligence (AI) in aviation systems and the opportunities it presents for enhanced automation, efficiency, and operational decision-making. While AI adoption in aviation is still at an early stage, it introduces significant certification and regulatory assurance challenges due to its probabilistic behaviour, data dependency, and limited transparency when compared with traditional deterministic avionics. Global regulatory bodies such as the Federal Aviation Administration, Radio Technical Commission for Aeronautics, European Union Aviation Safety Agency, International Civil Aviation Organization, and the Society of Automotive Engineers are actively developing frameworks for the certification and assurance of AI in aerospace systems. In India, the Directorate General of Civil Aviation has begun modernising aviation legislation through the Bharatiya Vayuyan Adhiniyam (2024). However, a structured certification pathway for AI in aviation—particularly for safety-critical and mission-critical applications—remains absent. This paper critically reviews international AI certification models, compares them with India's current regulatory position, and proposes a comprehensive civil–military AI certification roadmap aligned with national requirements. It extends the analysis to military aviation by proposing the establishment of a Defence AI Aviation Certification Authority to oversee AI applications across the Indian Air Force, Defence Research and Development Organisation, Hindustan Aeronautics Limited, and defence unmanned systems. The paper further evaluates relevant assurance standards such as DO-178C, DO-330, DO-326A, assurance of machine learning in aviation systems, runtime assurance architectures, and AI explainability requirements. Finally, it recommends regulatory interventions and institutional mechanisms to accelerate trustworthy AI adoption while safeguarding flight safety, national security and public trust.

Certification of Artificial Intelligence in Aviation: Global Approaches, Challenges, and Roadmap for India with Focus on the Indian Aviation

Certification of Artificial Intelligence in Aviation: Global Approaches, Challenges, and Roadmap for India with Focus on the Indian Aviation

Air Commodore Mukhvinder Pal Singh Virk

Est 1870

United Service Institution of India (USI)
New Delhi

Published by USI of India

Website: usiofindia.org

First Published in India in 2026

₹350

The views expressed in this book are of the author in his personal capacity

and do not represent the views of the USI.

Contents

"Victory smiles upon those who anticipate the changes in the character of war, not on those who wait to adapt themselves after the changes occur"

- *Giulio Douhet*

Introduction

Artificial intelligence (AI) has emerged as a transformative force in both civil and military aviation. Enabling applications such as predictive maintenance, flight safety monitoring, air traffic optimisation, autonomous taxiing, acting as pilot decision support, aiding in mission planning and swarm control in Unmanned Aerial Systems (UAS). Despite its operational potential, AI is fundamentally difficult to certify under traditional aviation regulations because it introduces probabilistic behaviour. Non-deterministic outputs and data-driven decision logic challenge existing software certification norms designed for deterministic avionics systems.[1,2]

Traditional aviation certification frameworks such as DO-178C for airborne software, DO-326A for cybersecurity, and AS9100 for quality management are insufficient to ensure AI trustworthiness without supplementary assurance methods.[3,4,5] AI applications introduce risks such as dataset bias, explanation gaps, model drifts, and training data contamination. These are not addressed by current certification practices designed for rule-based software systems as a result.[6,7] Regulators worldwide are moving towards evidence-based AI assurance frameworks rather than compliance-only models.

Globally, Federal Aviation Administration (FAA) and European Union Aviation Safety Agency (EASA) have taken leadership roles in developing AI certification strategies. EASA released its AI Roadmap 2.0, introducing a maturity-based four-level AI assurance model, as shown in Table 1. The FAA collaborates with Radio Technical Commission for Aeronautics (RTCA) committees such as SC-240 and SC-228 to shape guidelines for Machine Learning (ML) in airborne systems through 'Learning Assurance' concepts. Additionally, Assurance of ML for Autonomous Systems (AMLAS) offers a structured safety case method for verifying AI models used in aircraft systems.[8] These evolving frameworks acknowledge that AI certification requires lifecycle assurance—from data management and model validation to continuous monitoring and runtime safety.

India's Position and Regulatory Gaps

India's civil aviation regulatory body, the Directorate General of Civil Aviation (DGCA), enforces compliance through Civil Aviation Requirements (CARs)—but no dedicated AI certification framework currently exists. The Bharatiya Vayuyan Adhiniyam (BVA) (2024) replaced the old Aircraft Act of 1934. However, AI still needs to be addressed in the updated legislation, creating a vacuum in the policy for AI deployment in aviation. AI is currently used primarily in non-safety-critical, assistive roles, such as airline scheduling, fuel optimisation, and predictive maintenance trials. However, there is currently no established certification pathway for safety-critical or autonomous operations. Recently, during the Quality and Innovation Conclave (2025), the Defence Research and Development Organisation (DRDO) presented guidelines for the Verification and Validation (V&V) of AI software for military

applications. While the document is not in the public domain, open-source data suggests that the focus is on module-centric rather than system-algorithm-centric, periodic (initial) rather than continuous monitoring, and internal (V&V) rather than independently audited system. However, it is still a good beginning.

Military Gap–Focus on Indian Air Force

While the Indian civil sector lags in AI certification, military aviation too requires AI integration with urgency, due to evolving threats across Electronic Warfare (EW), autonomous combat platforms, and Manned-Unmanned Teaming (MUM-T). Programmes such as Combat Air Teaming System by Hindustan Aeronautics Limited (HAL) and warrior loyal wingman by DRDO rely on autonomous behaviour and AI-powered decision systems—yet India has no military AI airworthiness or safety certification authority equivalent to North Atlantic Treaty Organization's (NATO) Standardization Agreement (STANAG)-4671 or the United States (US) Department of Defense's (DoD) Airworthiness Certification System.[9]

In India, a Task Force for Implementation of AI was set up in 2019. The Defence Artificial Intelligence Council (DAIC) and Defence AI Project Agency (DAIPA) were setup as per its recommendations. The DAIC handles guiding and provides structural support, while the DAIPA has been set up to facilitate AI-based processes across defence organisations.[10] However, certification responsibility in respect to AI in aviation domain is not exclusively mentioned as task in the open domain.

Therefore, this monograph proposes a Defence AI Aviation Certification Authority (DAACA) to develop AI airworthiness and certification standards for the Indian Air Force (IAF), DRDO, HAL, and defence aerospace industry. The monograph sets up a civil–military AI certification roadmap for India up to 2035, aligned with the FAA and EASA's best practices.

Objectives

This monograph examines international AI certification frameworks in aviation to draw relevant lessons for India. It evaluates existing regulatory gaps and assesses India's preparedness to integrate AI within civil and military aviation systems. Based on this analysis, the study proposes a DGCA-approved AI certification framework tailored to CARs and recommends a corresponding defence AI certification model for the IAF and DRDO. It further develops a phased roadmap for AI certification in India for the period 2025-2035, outlining a structured pathway for safe, accountable, and mission-ready adoption of aviation AI.

Chapter 1

Literature Review

The certification of AI in aviation remains an emerging academic and regulatory field with contributions from aerospace engineering, safety certification, computer science, systems engineering, and aviation law. The literature surveyed spans global regulatory guidance, AI assurance methodologies, and aviation safety frameworks, while also finding challenges unique to AI deployment in safety-critical avionics and defence aviation.

Artificial Intelligence in Safety-Critical Aviation Systems

AI is increasingly deployed across aviation domains including predictive maintenance, health monitoring, navigation diagnostics, autopilot augmentation, air traffic control optimisation, and autonomous taxi systems.[11,12] But its lack of explainability, uncertainty in decision-making, and data sensitivity raises certification challenges.[13] Unlike legacy avionics software, AI behaviour cannot be tested exhaustively due to infinite state possibilities and hidden dependencies.[14] This introduces risks of unpredictable outputs, majorly impacting airworthiness and regulatory acceptance.[15]

Beyond regulatory frameworks, the certification ecosystem for aviation safety is shaped by institutional agencies whose mandates are now gradually expanding to include AI. Globally, civil aviation certification continues to be managed by agencies such as the FAA in the US and the EASA. Both have set up confidence in aviation systems

through deterministic design assurance. Their traditional roles include type certification of aircraft, oversight of avionics and software assurance, operational approvals, continuing airworthiness surveillance, and incident investigation. However, the emergence of AI is pushing these agencies into new and uncharted domain. EASA has taken a lead by being proactive through its structured AI Roadmap and Trustworthy AI framework. Meanwhile, the FAA is collaborating with RTCA to evolve learning assurance and runtime oversight principles. Complementing these regulators are bodies such as International Civil Aviation Organization (ICAO), RTCA, and Society of Automotive Engineers (SAE) International, which function as bridges by developing globally harmonised guidance, technical specifications, and data governance models, thereby, helping aviation stakeholders gradually gain confidence in AI-enabled systems.

In the Indian context of civil aviation, the DGCA functions as the principal authority for aircraft certification, regulatory enforcement, airworthiness oversight, and operational safety management. Traditionally, the DGCA's role has been centred on compliance with the conventional safety certification norms. But, as AI begins to influence areas such as predictive maintenance, decision support, autonomous taxi, and eventually safety-critical aviation functions, the DGCA will also have to adapt to new requirements. Hence, its evolving responsibility lies not only in certifying AI systems, but in creating structured policy frameworks, ensuring data integrity and regulatory

sandboxes, and building confidence before AI is allowed to flight safety directly. Unlike the EASA and FAA, India currently lacks a dedicated AI-specific civil certification concept. Hence, it reinforces the need for the DGCA to expand its mandate into AI assurance and lifecycle governance.

On the military aviation side, agencies such as the Centre for Military Airworthiness and Certification (CEMILAC) and Directorate General of Aeronautical Quality Assurance (DGAQA) have historically safeguarded aircraft safety through design approvals, production oversight, and flight clearance processes for the IAF, DRDO, and HAL. Their primary function has been to ensure airworthiness, structural integrity, system reliability, and compliance with established military certification standards. However, military aviation is also at the threshold of AI adoption. This will cover mission planning, predictive maintenance, autonomous MUM-T, Intelligence, Surveillance, and Reconnaissance (ISR) analytics, and mission autonomy. This demands that these institutions evolve beyond conventional certification to include AI safety assurance, resilient cybersecurity, robust testing, and continuous lifecycle monitoring. Global military frameworks such as NATO's STANAG or US's DoD's certification practices provide direction, but India must evolve its own pathway. The ongoing discussions within CEMILAC and the emerging idea of a dedicated AI Aviation Certification processes reflect an important shift—from static certification philosophies to dynamic, evidence-based AI assurance suited for both safety and mission.

Regulatory Framework for Artificial Intelligence Certification

The FAA and EASA have acknowledged AI as a technology that requires changes in certification frameworks rather than new structures. The EASA's AI Roadmap (2020-2025) is the first structured regulatory response at four levels.[16]

EASA AI Level	Description
Level 1	AI as a tool (offline use)
Level 2	Human-assisted AI (advisory)
Level 3	Context-specific autonomy with human oversight
Level 4	Full autonomy in safety-critical operations

Table 1: European Union Aviation Safety Agency's Artificial Intelligence Level (Description of Levels 1-4)

The EASA has five AI assurance requirements: safety, explainability, certifiability, ethics, and societal acceptance. Likewise, the FAA collaborates with National Aeronautics and Space Administration and RTCA through SC-240 (AI in aviation) and SC-228 (autonomy). It is working toward learning assurance and runtime safety concepts.

Artificial Intelligence Assurance Frameworks

Research in this domain emphasises AI assurance through structured safety cases. The AMLAS framework, developed at the University of York, offers a six-step lifecycle-based

assurance process. This combines hazard analysis, data assurance, and model validation to produce credible evidence for certification.[17] Table 2 shows additional AI safety frameworks.

Framework	**Purpose**	**Relevance to Aviation**
DO-178C	Software certification	Baseline standard
DO-330	Qualification of software tools	AI tool validation
DO-326A	Cybersecurity process	Protect ML models from attacks
ISO/IEC 23894:2023	AI risk management	Applicable to aviation AI
SAE G-34/ European Organisation for Civil Aviation Equipment WG-114	AI assurance	Drafting aviation AI standards

Table 2: Artificial Intelligence Assurance Frameworks

Researchers stress that data is a part of the safety argument in AI systems.[18] The assurance process should examine data coverage, bias, representativeness, and edge-case validation to avoid unsafe ML behaviour.[19]

Gaps in Certification for Artificial Intelligence

Academic studies consistently highlight that traditional software verification techniques cannot satisfy AI certification needs due to lack of explainability, lack of determinism, model drift after deployment, bias and adversarial vulnerability, test incompleteness in ML systems.[20]

Furthermore, post-deployment monitoring and lifecycle assurance have been identified as critical for certification as AI models degrade over time due to environmental changes—a risk that aviation regulators cannot ignore. [21]

Chapter 2

Global Artificial Intelligence Certification Frameworks in Aviation

As the adoption of AI in aviation is gaining pace, regulatory agencies are moving from exploratory methods to structured certification strategies. But there is no single global standard for AI certification yet. Instead, a combination of existing aviation certification standards and emerging AI assurance guidelines is being used to evaluate AI-based systems. This section compares the AI certification approaches of major regulatory bodies: FAA (US), EASA (Europe), ICAO (global), RTCA, SAE, and others.

Federal Aviation Agency, United States

The FAA currently does not have a formal certification standard for AI. Instead, AI-enabled systems should demonstrate compliance with existing safety regulations under title 14 of the Code of Federal Regulations and software assurance via DO-178C. The FAA accepts AI challenges, and it is, therefore, collaborating with RTCA's SC-240 on AI systems assurance and SC-228 for autonomy in aviation.

Key ongoing FAA initiatives under progress include developing AI Roadmap for flight safety, guidance for learning assurance in AI, emphasis on runtime safety monitoring, and certification through means of compliance rather than AI-specific rules.

Strengths of this approach are safety-first perspective and, hence, it has robust certification legacy. However, it does have weaknesses as conservative adoption can delay AI innovation. At present, AI is permitted only in non-critical decision support roles.

European Union Aviation Safety Agency, Europe

The EASA is the global leader in AI regulation for aviation. It introduced the first official AI Roadmap in 2020 and expanded it in 2022 under Trusted AI Concept. The EASA's framework is maturity-based and risk-based, as shown in Table 3.

EASA AI Level	AI Capability	Use Case Example
Level 1	AI as a tool	Aircraft design optimisation
Level 2	Human-in-the-loop	Predictive maintenance
Level 3	Human-on-the-loop	Autonomous taxi
Level 4	Autonomous AI	Full autonomy (future stage)

Table 3: European Union Aviation Safety Agency's Artificial Intelligence Level Use Cases

The EASA's Roadmap 2.0 includes developing ethical AI principles, fostering explainability requirements, and strengthening AI trustworthiness framework sandbox testing for AI in aviation. Strengths of this approach are clear

strategy and being innovation friendly. It does have weaknesses as it has yet to certify Level 3+ AI systems. However, it is the most progressive AI certification regulator globally.

International Civil Aviation Organization, Global Aviation Standards

The ICAO does not certify aircraft but sets global civil aviation standards. It acknowledges the use of AI in its aviation cybersecurity strategy (2022–2030) and AI concept note[22,23], recommending global harmonisation of AI certification to avoid fragmented regulation.

The ICAO currently offers only guidance and not certification, promotes standardisation, and interoperability, and encourages responsible AI use and multinational collaboration. The role of ICAO is only limited to coordination and guidance. The fact that it does not has the certification authority power highlights the existing gap.

Society of Automotive Engineers, International Artificial Intelligence Safety Standards

The SAE leads technical standards for AI assurance in aviation through committee SAE G-34 or European Organisation for Civil Aviation Equipment WG-114. Their upcoming standard ARP6983 introduces AI safety requirements for training data, verification and validation, human oversight and AI behaviour bounding.[24]

The key SAE focus is on Operational Design Domain (ODD) for aviation AI, ML safety case and risk-based AI qualification. A technical standard for AI safety in aviation is expected during 2025-2026.

Radio Technical Commission for Aeronautics, Machine Learning Assurance

The RTCA is working with FAA on AI certification. The SC-240 committee is developing guidance for learning assurance, while SC-228 addresses autonomy for UAS. Here, the key focus is on testing ML at system level, dataset traceability, fallback architecture, and runtime assurance with safety guardrails.

Comparison of Global Artificial Intelligence Certification Approaches

There are many approaches to AI certifications and various standards for it. Table 4 compares the major standards.

Regulator or Standard	**AI Regulation Status**	**Applicability**
FAA	Conservative, safety-first	Deterministic + Learning AI with safety evidence
EASA	Most advanced AI roadmap	Level 1–3 AI evolving
ICAO	Policy alignment only	Advisory
RTCA	Technical assurance	Dataset and learning assurance
SAE G-34	AI safety standard	Forthcoming
International Organization for Standardization and International Electrotechnical Commission	AI governance	Supplemental

Table 4: Comparison of Global Artificial Intelligence Certification Approaches

Chapter 3

Artificial Intelligence Assurance and Safety Frameworks in Aviation

Traditional aviation software certification relies on deterministic logic and traceable requirements. But AI-based systems behave differently due to their probabilistic nature and dependence on data-driven learning. This introduces new categories of aviation safety risks, requiring supplementary assurance frameworks beyond conventional certification practices. This section covers the essential AI assurance frameworks used (or proposed) for aviation certification—DO-178C-based assurance, AMLAS, Explainable AI (XAI), Runtime Assurance Architectures (RTA), Design Assurance Levels (DAL), and data integrity evaluation frameworks.

DO-178C–Baseline Software Certification Standard

The RTCA's DO-178C remains the primary certification standard for airborne software. It defines software development assurance levels based on the effect of system failure on aircraft safety, as summarised in Table 5.

Relevance to AI: DO-178C still applies to AI systems at the integration level, but not adequate on its own to verify ML components, because it lacks guidance for data traceability, model explainability, learning behaviour, and uncertainty quantification.

DAL	Failure Impact	Certification Rigour
DAL A	Catastrophic Failure	Maximum
DAL B	Hazardous or Severe (major)	Very High
DAL C	Major	High
DAL D	Minor	Medium
DAL E	No Safety Effect	Minimal

Table 5: Defence Design Assurance Levels (A to E)

Assurance of Machine Learning in Aviation Systems

Developed by the University of York in partnership with Rolls-Royce and Thales, AMLAS provides a structured evidence framework for certifying ML components. The AMLAS lifecycle involves defining ML safety requirements, ensuring data safety and integrity, performing model verification and validation, conducting hazard analysis, justifying training and test data, and assembling a safety case. Its main strength lies in generating structured safety arguments for ML components, while a key limitation is the need to integrate with broader system safety standards such as DO-178C.

Explainable Artificial Intelligence

AI black-box models are not certifiable without explainability. Regulators emphasise that AI in aviation should justify its decision paths. Explainability requirements include model transparency (how decisions were made), feature traceability (input influence), and auditable logic (testable explanations). These are mandatory for Level 3 or safety-related AI techniques used include SHapley Additive exPlanations values, local interpretable model-agnostic explanations, and attention layers.

Runtime Assurance

RTA enables safe deployment of AI by supervising AI decisions in real time. It implements a safety monitoring system that intervenes to override AI actions whenever unsafe behaviour is detected. Applied in Unmanned Aerial Vehicle (UAV) autonomy and military aviation safety, this FAA-supported concept in AI safety operates under pilot supervision for autonomous taxiing and flight systems.

Data Integrity and Dataset Certification

Unlike conventional software, data is a part of the safety argument for AI. Certification requires dataset coverage across operational conditions, bias assessment, adversarial resilience, validation on edge cases (weather, sensor failure, Global Navigation Satellite System [GNSS] Jamming), and secure data provenance.

The DGCA and CEMILAC should enforce dataset audits that are mandatory for both civil and military AI, as shown in Figure 1.

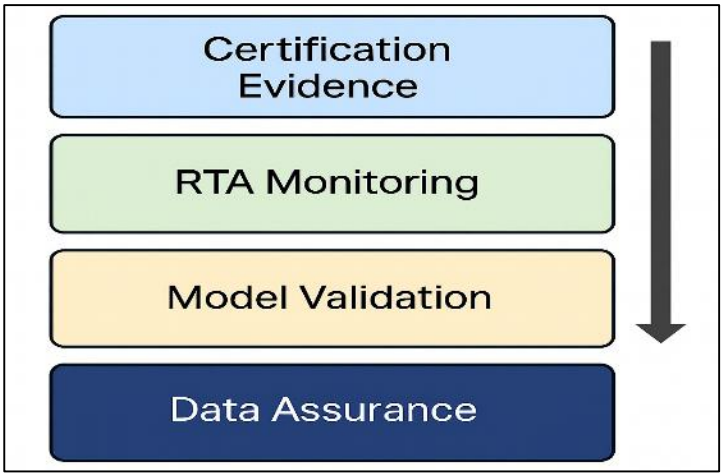

Figure 1: Artificial Intelligence Assurance Framework Overview

Chapter 4

Challenges in Artificial Intelligence Certification for Aviation

The adoption of AI in aviation can bring enhanced safety, efficiency, autonomy, and mission support. But it also raises certification challenges. Unlike conventional software, AI operates on probabilistic logic, evolves through trained models, and depends on data quality and contextual adaptability. These create certification uncertainties. This section identifies technical, regulatory, operational, ethical, legal, and security-related challenges associated with AI certification in civil and military aviation.

Technical Challenges

Table 6 outlines the challenges of certifying AI, particularly due to its non-deterministic nature and related technical complexities.

Challenge	Description	Certification Impact
Non-determinism	AI outputs vary even under similar conditions	Violates reproducibility needed for DO-178C
Explainability gaps	Black-box AI models lack transparency	Hard to trace safety failures
Edge-case risks	AI may fail in rare or unseen real-world scenarios	Incomplete testing

Challenge	Description	Certification Impact
Model drift	AI performance degrades over time	Continuous certification required
Domain shift	AI performs poorly outside trained environment	Inadequate validation evidence
Sensor fusion errors	AI misinterprets combined sensor inputs	Wrong classification decisions

Table 6: Technical Challenges

Data and Validation Challenges

Certification authorities emphasise that data quality equals safety in AI. Poor dataset quality can cause catastrophic errors in airborne AI systems. The main challenges include limited availability of Indian aviation datasets, absence of standardised criteria for dataset auditing, biases in environmental and operational data, vulnerability to data poisoning and adversarial attacks, and data confidentiality risks in defence AI systems. For instance, an AI-based collision avoidance system trained solely on clear-weather data may fail under Indian conditions such as Himalayan turbulence or dust storms in Rajasthan.

Regulatory Challenges

Current regulations (FAA, EASA, ICAO, and DGCA) do not define AI certification requirements directly. Table 7 summarises these aspects.

Regulatory Gap	Impact
No AI-specific civil aviation requirements by DGCA	India has no approval pathway
No airworthiness guidance for ML	Slows AI avionics adoption
No DO-178C adaptation for AI	Safety evidence remains unclears
Certification for adaptive AI denied	Only frozen models allowed today

Table 7: Regulatory Challenges Worldwide

Ethics and Accountability Challenges

Key challenges in this domain include assigning responsibility for AI system failures—whether to the Original Equipment Manufacturer (OEM), developer, airline, organisations like HAL and DRDO, or the pilot. Additional issues involve the lack of clearly defined ethical constraints for lethal military AI, the need for a human-in-command policy in defence applications and ensuring certification frameworks incorporate a well-defined accountability chain.

Cybersecurity Challenges

AI systems are vulnerable to data poisoning attacks, model inversion attacks, adversarial spoofing, sensor hacking, and communication link hijacking (UAVs). Certification should integrate DO-326A cybersecurity assurance with AI safety verification.

Operational and Training Challenges

These require pilots and crew to trust AI systems through certification evidence. DGCA and CEMILAC inspectors should be equipped with AI safety training, and military doctrines should incorporate clear rules for AI integration.

Chapter 5

India's Current Position on Artificial Intelligence Certification in Aviation

India is on the path toward modernisation in aviation domain. However, AI regulation and certification in aviation are still in a formative stage. In contrast to the FAA and EASA, India has yet to establish formal certification guidance specifically addressing the use of AI in safety-critical aviation functions. But several policy actions and reforms provide a foundation upon which an Indian AI certification framework can be built.

Bharatiya Vayuyan Adhiniyam, 2024–Legal Foundation

The BVA, 2024, replaced the Aircraft Act of 1934.[25] It is modernising India's civil aviation legal framework to align with erstwhile safety, regulatory, and technological needs. The Act vests powers in the Central Government and its designated agencies, such as DGCA. These provisions collectively empower the government to frame technical standards, investigate system-related failures, and delegate certification authority to specialised agencies. Table 8 highlights the major sections of the BVA.

BVA Section	Provision Summary
Section 10–Power of Central Government to make rules	Empowers the government to make rules for conducting the purposes of the Act, including aircraft airworthiness, operations, personnel licensing, and aerodrome management.
Section 11–Power to make rules to implement international conventions	Authorises the government to frame rules and give effect to the ICAO and other international obligations.
Section 12–Power to make rules for investigation of accidents	Provides authority to make rules for investigation of aircraft accidents.
Section 18–Power to regulate construction or obstructions near aerodromes	Permits regulation of structures, trees, and obstacles affecting safe flight operations.
Section 21–Power to delegate	Allows the government to delegate powers to authorities such as DGCA, or Aircraft Accident Investigation Bureau (AAIB).

Table 8: Relevant Provisions of Bharatiya Vayuyan Adhiniyam for Future Artificial Intelligence Regulation

Role of Directorate General of Civil Aviation: Regulatory Gaps

The DGCA regulates aircraft certification. It is done through CARs. As of 2025, AI is not addressed in any CAR section. Certain CAR provisions, while not explicitly designed for AI, are indirectly applicable to AI assurance. Table 9 show cases these regulatory gaps.

DGCA CAR Section	**Link to AI Certification**
Section 2– Airworthiness (Series F)	Could include AI system approvals
CAR 21	Type certification–future AI integration point
CAR 145	AI predictive maintenance oversight
CAR M	Continuing airworthiness– runtime AI monitoring
CAR on Digital Sky (UAS)	AI used in drone autonomy

Table 9: DGCA Regulatory Gaps

But no CAR exists for ML or AI assurance, creating a regulatory vacuum for AI avionics and autonomy certification in India.

Ministry of Civil Aviation (MoCA) Position and National Artificial Intelligence Readiness

The MoCA encourages digital transformation. But it has not yet published AI guidance for civil aviation safety. AI is mentioned only within the Digital Sky Policy for drones and is not addressed in aircraft certification frameworks. India needs a national AI assurance policy for aviation, along with a joint DGCA–MoCA task force on AI certification and a public regulatory sandbox to support aviation AI testing.

Directorate General of Civil Aviation Artificial Intelligence Use Cases Allowed Today (Limited)

AI Limited to Non-Safety-Critical Roles. Currently, DGCA permits AI only in non-safety-critical roles such as predictive maintenance analytics, airline safety audits, passenger flow management, engine health monitoring, and flight schedule optimisation. Meanwhile, AI-based flight control, autonomous taxi or landing, AI flight decision authority, and MUM-T (civil) are not allowed yet.

Need for Urgent AI Certification in India. New Delhi has begun taking steps toward developing certification frameworks and structures for deploying AI in aviation, as noted earlier. However, there are gaps, and it is fragmented as the processes are still evolving. Table 10 brings out reasons along with drivers for accelerating AI certification.

Driver	**Reason**
Aviation safety	Increasing traffic and pilot workload
Indigenous AI avionics	HAL, DRDO, private aerospace start-ups
Civil-military dual use	Needed for UAS traffic management and AI
Global compliance	FAA and EASA's mutual recognition need AI rules
Economic growth	AI services market boost

Table 10: Artificial Intelligence Safety Evidence Checklist

Chapter 6

Proposed Artificial Intelligence Certification Roadmap for Civil Aviation in India (Directorate General of Civil Aviation Framework)

India lacks certification processes for AI-enabled aviation systems in Indian civil aviation. The DGCA needs to establish an AI certification framework in a phased manner. This approach can align with global regulatory trends set by the FAA, EASA, and ICAO, while also addressing India-specific constraints.

Artificial Intelligence Certification Levels for India (Proposed Directorate General of Civil Aviation Model)

Like EASA's AI levels, India should adopt a four-tier AI classification framework for certification. Table 11 brings out these aspects.

DGCA AI Level	Application Type	Certification Requirement
Level 1–AI as Tool	Data analytics, diagnostics	CAR-based approval
Level 2–Advisory AI	Pilot decision support, Maintenance AI	DGCA notification
Level 3–Safety-Related AI	Collision avoidance assist	Restricted operational certification
Level 4–Safety-Critical AI	Flight control AI, autonomous taxi	Full AI certification

Table 11: Certification Metrics (Key Performance Indicators [KPIs])

Proposed Directorate General of Civil Aviation Certification Phases (2025–2035)

Table 12 proposes a phased map for DGCA certification till 2035 to bring in AI certification.

Phase	Timeline	Milestone
Phase 1	2025–2026	DGCA AI Regulatory Cell established
Phase 2	2026–2028	AI CAR issued for Level 1–2
Phase 3	2028–2031	Level 3 AI certified under sandbox testing
Phase 4	2031–2035	Level 4 AI Type Certification

Table 12: Proposed Certification Phases

Phased Roadmap for Certification of Artificial Intelligence Systems in Civil Aviation

For India, the most pragmatic approach to AI certification in aviation is a confidence-building roadmap that begins with non-safety-critical applications before progressively moving toward safety-related and safety-critical AI functions. The DGCA may initially produce AI systems that support analytics, maintenance predictions, operational monitoring, documentation processing, airline decision-support, airport management, and advisory cockpit applications that do not directly affect aircraft control or flight safety. These systems allow regulators, airlines, and OEMs to gain experience without exposing passengers or airspace users to operational

risk. This phased progression mirrors global regulatory thinking, where sandbox approvals, learning assurance, and structured AI safety cases are first matured on lower-risk use-cases before granting authority to AI systems affecting critical flight operations.[26]

Once sufficient, operational confidence, audit capability, and incident learning frameworks are established, the DGCA may expand certification toward safety-related AI and, eventually, safety-critical aviation applications. These include collision-avoidance support, assisted taxiing, anomaly detection which affect flight safety, and autonomous decision support under strict human-in-the-loop control. At this stage, certification must combine DO-178C system assurance with AMLAS-based AI safety cases and continuous post-deployment monitoring. Runtime safety and oversight mechanisms will be essential to ensure that AI behaviour remains accountable across its service life. This measured evolution ensures that India aligns with FAA-EASA trajectories while protecting public trust and aviation safety.[27]

Directorate General of Civil Aviation Artificial Intelligence Certification Architecture

Certification should combine DO-178C aviation safety, along with AMLAS AI assurance and runtime safety architecture. Key requirements include data verification, model validation and safety testing, explainability documentation, bias risk audit, and cybersecurity verification (DO-326A).

Artificial Intelligence Approval Workflow–Directorate General of Civil Aviation

The proposed AI certification workflow under the DGCA should follow a structured, risk-based approach suited to adaptive aviation systems. The process would begin with classification of AI system within a defined DGCA framework to determine the level of regulatory scrutiny. This should be followed by risk assessment through development assurance level mapping to align certification rigour with operational criticality. Safety assurance must then be demonstrated through a ML safety evidence package, which is consistent with AMLAS principles, including data governance, validation, and performance reliability. Controlled flight evaluation within a regulatory AI sandbox should enable supervised operational testing under defined constraints. On satisfactory compliance to above guidelines, certification may be granted through an AI-type certificate supplement, thus, integrating AI-specific requirements within existing airworthiness frameworks while ensuring continued safety oversight.

India Civil Artificial Intelligence Certification Authority: Proposal

A new unit must be created within the DGCA, named AI Certification Directorate of Aviation (AICDA). The corresponding functions are outlined and summarised in Table 13. This includes reviewing AI compliance evidence, approving AI training data sources, and monitoring changes in AI behaviour after certification.

Feature	**DGCA (Proposed)**	**EASA**	**FAA**
AI Levels	Four	Four	Not formalised
AI Sandbox	Yes	Yes	Limited
Runtime Safety	Required	Required	Required
Explainability	Mandatory	Mandatory	Under Review

Table 13: Directorate General of Civil Aviation Artificial Intelligence Certification vs the European Union Aviation Safety Agency and Federal Aviation Agency (Comparative)

Chapter 7

Artificial Intelligence Certification Roadmap for Military Aviation in India (with Focus on the Indian Air Force)

Military aviation places unique demands on AI assurance because operations occur in contested degraded and adversarial environments. This is because mission outcomes—not only flight safety—drive certification thresholds. India's military aviation ecosystem (IAF, DRDO, HAL, Aeronautical Development Agency [ADA], CEMILAC, or DGAQA) requires a mission-assurance–centric and security-hardened certification pathway that complements civil airworthiness while addressing EW/cyber threats, classified datasets, export controls, and coalition interoperability.

Rationale for a Distinct Defence Artificial Intelligence Certification Pathway

Operational Context. Combat air patrol, contested airspace, Global Navigation Satellite Systems (GNSS) denial, EW jamming/spoofing, and high-tempo sortie generates stress AI robustness beyond civil use.

Mission Assurance vs Flight Safety. Flight safety remains necessary but is not sufficient; AI should also demonstrate mission survivability and combat utility under adversarial conditions.

Security Constraints. Datasets, models, and test artefacts are often classified, limiting open evidence exchange and reuse of civil testbeds; this requires secure enclaves and red/black separation for model development and evaluation.

Human Command and Legal Accountability. Doctrine should codify human-in-the-loop/over-the-loop for targeting, weapon release, and strategic decision-support functions.

Proposed Institutional Mechanism: Defence Artificial Intelligence Aviation Certification Authority

DAACA is a joint entity under the Ministry of Defence (MoD). It should have participation from IAF (customer), DRDO/ADA (Research and Development), HAL (OEMs), DGAQA/CEMILAC (quality/airworthiness), and Indian Computer Emergency Response Team (CERT-In)/ National Technical Research Organisation (cyber). The core mandates should emphasise mission-aware certification of AI/ML functions across manned aircraft, UAS/ Unmanned Combat Aerial Vehicle (UCAV) and Command, Control, Communications, Computers, ISR systems. This will ensure operational relevance and safety assurance. The framework must incorporate robust adversarial testing through EW and cyber red-teaming simulations, supply-chain risk assessment, model tracking, Software Bill of Materials (SBOM) formulation, and authenticated firmware. It should also ensure classified data governance through accredited data pipelines, use of differential privacy where feasible, and maintenance of auditable model lineage. Further,

comprehensive lifecycle oversight must be ensured through model freeze protocols, defined update cycles, continuous field performance monitoring, and incident forensics supported by secure ML 'Black Box' mechanisms.

Defence Design Assurance Levels (D-DAL)

Civil DAL (A to E) should be extended with a mission dimension to capture operational consequences, even when flight safety ensured. These steps are highlighted in Table 14.

D-DAL	Description	Examples	Evidence Emphasis
D-A	Catastrophic mission and safety impact	Autonomous recovery/ landing, flight controls, weapon safety interlocks	DO-178C/AMLAS + RTA + EW/cyber red-team; formal methods where feasible
D-B	Severe mission impact, potential safety risk	Sense-and-avoid assist, autonomous taxi in contested bases	Model robustness, ODD bounding, fail-safe envelopes

D-DAL	Description	Examples	Evidence Emphasis
	Major mission impact	Target recognition cueing, mission replanning aids	Data assurance (theatre-specific), operator Human–Machine Interface (HMI) explainability
D-D	Minor mission impact	Maintenance AI, logistics routing	Performance monitoring, drift alarms
D-E	No mission/ safety effect	Back-office analytics	Basic quality assurance

Note: D-DAL augments, not replaces, civil DAL. For mixed-use platforms, the higher applicable level governs.

Table 14: Defence Design Assurance Levels

Defence Artificial Intelligence Certification Lifecycle

A secure AI lifecycle should integrate AMLAS principles with mission certification and runtime assurance to ensure operational safety and resilience. The process should begin with mission hazard analysis and ODD definition, considering factors such as theatre conditions, weather, and

EW posture, followed by secure architecture design and supply-chain assurance through SBOMs, code provenance, and model authentication. It must incorporate robust data governance through classified data environments, adversarial data testing, and red-team validation. Model development and verification should ensure resilience to cyber and EW perturbations, supported by uncertainty quantification and effective human–system integration through explainable interfaces and operator training. Validation should be undertaken through range trials and synthetic-to-live evidence generation, including Hardware-in-the-Loop (HWIL) and high-fidelity test environments. Field deployment should include runtime assurance mechanisms such as safety monitors, disengagement protocols, and graceful degradation. This should be followed by continuous post-deployment surveillance, drift detection, and structured incident forensics supported by secure ML black box systems.

Secure Test Infrastructure (Synthetic-to-Live)

Digital twin and HWIL laboratories should enable theatre-specific simulation environments incorporating radio frequency threat injection, GNSS denial scenarios, extreme weather conditions, and sensor failure modelling to validate system resilience. Testing should further be conducted on accredited ranges using UAS/UCAV and surrogate aircraft corridors with graduated autonomy thresholds, progressing from advisory functions to supervised execution and bounded autonomy. Additionally, coalition interoperability

cells should facilitate evidence exchange for non-lethal functions such as ISR and logistics with friendly air forces, aligned where feasible with NATO-like STANAG principles to promote standardisation and operational compatibility.

Deployment Gates for Autonomy (Defence)

A gated progression ensures measured risk escalation. Table 15 proposes these four gates below.

Gate	Operational Mode	Examples	Exit Criteria
G1: Advisory	AI advises, operator executes	Average true range cueing, tanker rendezvous suggestions	Accuracy, false-alarm bounds, user experience validation
G2: Supervised Execution	AI acts within bounded envelope; operator veto	Autonomous taxi in base, automated route following	RTA efficacy, handover latency, EW resilience

Gate	Operational Mode	Examples	Exit Criteria
G3: Bounded Autonomy	AI plans/executes within geo/mission guardrails	Loyal wingman station-keeping, autonomous cargo in secured corridors	Mission success KPIs, red-team pass, abnormal case handling
G4: Expanded Autonomy (Limited)	AI adapts within certified ODD; human override	UCAV ISR in low-threat sectors	Continuous monitoring, re-cert triggers for ODD change

Table 15: Deployment Plan

Priority Use Cases for the Indian Air Force (2025–2033)

These cases are:

- Predictive maintenance and fleet health (D-D/C)—fleet readiness, spares optimisation.
- Mission planning and re-planning aids (D-C)—constraint-aware, EW-informed routes.

- ISR automatic target recognition cueing (D-C/B)—multi-sensor fusion, explainable cues, operator consent.
- Autonomous taxi and ground operations (D-B) —supervised in home bases first.
- MUM-T loyal wingman behaviours (D-B/A) —tight ODD, strict RTA, Return on Equity (ROE) bound.
- Autonomous Cargo Corridors (D-B) – fixed routes, rear echelons, corridor geofencing.

Centre for Military Airworthiness and Certification Safety of Flight and Production Clearance of Artificial Intelligence Software

In military aviation, the safety of flight remains the most fundamental certification parameter, even when AI applications extend beyond conventional avionics. The CEMILAC under DRDO has traditionally overseen design, production, and airworthiness clearances for aircraft and airborne systems across HAL, IAF, and private defence industries. With the growing inclusion of AI-based functionalities—ranging from decision-support software to predictive health monitoring—CEMILAC's airworthiness philosophy is now being adapted to accommodate ML-enabled and data-driven systems.

AI introduces variability in system behaviour, making it difficult to assess deterministically under legacy standards as per Indian Military Technical Airworthiness Requirements

(IMTAR) 2021 ver 2.0 (IMTAR 21, v.2, 2023).[28] These frameworks primarily assess software through static internal V&V (independent V&V) cycles. However, AI and ML models require continuous performance validation, explainability, and runtime monitoring, as system accuracy may change after deployment.

CEMILAC has, therefore, begun introducing AI-adapted evaluation criteria for safety-of-flight clearance. Recent seminar discussions at the CEMILAC AI Assurance in Aerospace Systems Workshop (Bengaluru, 2024) highlight efforts to define a 'Non-flight-critical AI Classification'—a category intended to enable the limited use of ML software in maintenance, diagnostic, and mission-support functions, without imposing the stringent DAL A/B rigour reserved for flight-critical controls.

CEMILAC has also recognised that the rate of AI software modification—driven by frequent retraining or code tuning—outpaces traditional modification classification protocols. To address this, the agency is undertaking pilot studies for the certification of AI/ML-based non-flight-critical applications, with evaluation templates derived from DO-178C, DO-330, and AMLAS.

These early steps indicate a transition from static software certification to a lifecycle assurance model that aligns with global trends at FAA and EASA. The CEMILAC is planning to release the detailed document as 'Airworthiness Directive' regarding use of AI/ML in military aviation (augmentation to Subpart C6 of IMTAR 21). This proposed

document will focus on development and certification methodology for non-safety critical military airborne software with ML components.

CEMILAC's evolving role reflects a pragmatic understanding that AI certification in military aviation cannot yet match standards of determinism—but it can achieve bounded safety and evidence-based assurance. These developments form a critical foundation for future collaboration between CEMILAC and the proposed DAACA to jointly manage certification of safety-of-flight and mission-assurance AI systems for the IAF and DRDO ecosystem.

Phased Certification Roadmap for Artificial Intelligence in Military Aviation

For military aviation, the rationale for an AI certification roadmap in stages is even stronger due to contested-environment risks, cybersecurity exposure, and mission-assurance requirements. CEMILAC and IAF should first approve non-safety-critical AI systems. These include predictive maintenance, health monitoring, mission planning aids, optimisation of logistics, and ISR decision-support where human operators retain execution authority. These categories allow CEMILAC to evolve AI assurance processes, dataset validation methods, adversarial testing, and model-tracking without directly influencing flight control systems or weapon-release functions.[29] This phase also helps crews and commanders to build the trust of operators. This

is a critical prerequisite for eventual acceptance of more autonomous functions.

Only after this maturity stage, CEMILAC should begin structured certification pathways for safety-related and safety-critical AI, such as autonomous taxi, sense-and-avoid, loyal-wingman behaviours, bounded autonomy in UCAVs, and mission-execution AI operating under doctrinal human-in-command structures. Certification in this phase must integrate D-DAL-based risk classification, EW/cyber adversarial testing, runtime assurance with deterministic fallback logic, secure model provenance, and classified-environment dataset governance. It is important that each upward progression in autonomy must be evaluated, evidence-backed and doctrine-aligned. This allows India to operationalise AI power while preserving the safety ethos of military aviation and national security imperatives.[30]

Governance, Doctrine, and Rules of Engagement

The rules are:

- **Human-in-the-Loop/Over-the-Loop Policies**. Mandatory for targeting and weapon release; AI cannot authorise lethal effects.
- **Change Authority**. Model updates via Change Control Boards with security and airworthiness sign-off.
- **Operator Training**. Certification includes crew proficiency on AI failure modes and override protocols.

- **Legal and Accountability**. Define responsibility allocation (OEM, integrator, operator) and evidence standards for Boards of Inquiry.

Cybersecurity and Supply-Chain Assurance

DO-326A/ED-202A standards should be ensured to establish robust cyber process assurance for avionics systems. The framework must ensure SBOM, source verification, secure boot code testing and authenticated software updates to strengthen system integrity. It should further incorporate resolute red-team programmes to assess vulnerabilities such as model extraction, data poisoning, adversarial manipulation, and sensor spoofing. Additionally, secure zero-trust communication architectures should be adopted for UAS command and control links, supported by anti-tamper protections for flight-critical computing systems to enhance operational resilience.

Phased Timeline (Defence) 2025–2035. Table 16 gives a roadmap till 2035 for defence applications involving certification by CEMILAC.

Phase	**Years**	**Outcome**
P0–Stand-up	2025–2026	DAACA formed; secure labs/ranges accredited; initial doctrine issued
P1–Trials	2026–2028	Advisory and supervised functions (G1–G2) certified for limited ops

Phase	**Years**	**Outcome**
P2–Operationalisation	2029–2032	Bounded autonomy (G3) in corridors; MUM-T limited missions
P3–Scale and Harmonise	2033–2035	Expanded autonomy in defined ODD; coalition interop for non-kinetic roles

Table 16: Phased Timeline (Defence) 2025–2035

KPIs for Certification Decisions. Performance evaluation should be based on clearly defined safety, mission, robustness, and governance metrics. Safety indicators should include loss-of-separation rates, frequency of RTA interventions, and the success of abnormal procedure handling. Mission effectiveness should assess objective achievement under EW conditions, reduction in operator workload, and improvements in sortie throughput. System robustness must be evaluated through performance under over loading, adversarial attacks, and timely detection of drift in model. These indicators provide a comprehensive basis for assessing effectiveness and regulatory compliance.

Civil vs Military Artificial Intelligence Certification (India). Table 17 compares the certification for civil and military in aviation.

Dimension	**Civil (DGCA)**	**Military (DAACA proposed)**
Primary Objective	Flight safety, public trust	Mission assurance +safety
Data Treatment	Open/industry datasets where possible	Classified datasets, secure enclaves
Evaluation	DO-178C+AMLAS+sandbox	D-DAL+AMLAS +EW/cyber red-team
Runtime Safety	RTA+ operator oversight	RTA + doctrinal overrides + kill-switch
Evidence Sharing	Public/peer review	Need-to-know; coalition memoranda of understanding
Dimension	**Civil (DGCA)**	**Military (DAACA proposed)**
Update Policy	Frozen models; controlled updates	Controlled updates; field hot fix with audits

Table 17: Civil vs Military Artificial Intelligence Certification (India)

Risks and Mitigations (Defence)

Potential risks must be addressed through measures to ensure safe and reliable deployment of AI-enabled systems in aviation. Spoofing of model deployed and risk of data poisoning should be managed through regular red-team testing, control for data traceability, and anomaly detection processes. The risk of ODD creep requires strict geofencing measures and clearly defined recertification triggers to prevent unauthorised expansion of system capabilities. Over-reliance of operator on automated systems should be addressed through effective HMI, planned training, and periodic drills to ensure fail-safe use. Vulnerabilities in supply-chain must be mitigated by ensuring proper contracts and selection of vendors. The proposed DAACA pathway offers a practical framework for India to operationalise AI capabilities in military aviation by ensuring safety, accountability, and control. This is supported by defined D-DAL levels, secure simulated-to-live testing environments, and phased autonomy deployment.

Chapter 8

Integrated Policy and Certification Framework for India (Civil–Military Alignment)

Institutional Architecture: Governing Bodies

Safety oversight is handled by DGAQA and CEMILAC, which are initiating AI/ML certification protocols, with responsibility set to transition to DAACA for operational AI systems. To operationalise AI certification in aviation, India should establish a two-tier dual-use governance structure. Table 18 tries to propose and summarise governing setups through new bodies for incorporating AI in civil and military domains in aviation.

Level	**Civil Aviation**	**Military Aviation**
Regulatory Authority	DGCA	MoD
AI Certification Body	AICDA (within DGCA)	DAACA
Safety Oversight	AAI+DGCA Directorate of Air Safety	DGAQA+CEMILAC
Standards Alignment	ICAO standards and recommended practices, FAA, EASA, RTCA, SAE	STANAG (optional), MoD Joint Doctrine, DRDO

Level	**Civil Aviation**	**Military Aviation**
National Testbeds	Civil AI Flight Test Corridors	Classified AI Test Ranges
Policy Input	MoCA + NITI Aayog + Bureau of Indian Standards' AI Standards	Headquarters Integrated Defence Staff, Integrated Headquarters of MoD (Air)

Table 18: Safety Oversight in India

These bodies operate under a National Aviation AI Assurance Council, chaired by MoCA and MoD for civil–military synchronisation.

Legal and Regulatory Pathway

The following legal instruments will be activated to introduce AI certification, as highlighted in Table 19.

Legal Provision	**Relevance**
BVA, 2024–Section 10	DGCA may regulate technical standards including AI
BVA, Section 14	Central Government can introduce AI certification via DGCA
DGCA CAR (New)–CAR-AI/2025	Introduces AI-based Aircraft system approval

Legal Provision	Relevance
Defence Order–DAACA/2026	Establishes military AI airworthiness
MoCA Advisory	Enables AI sandbox trials
Data Protection (Digital Personal Data Protection [DPDP] Act 2023)	Governs AI data privacy
Cybersecurity (CERT-In)	AI system cyber compliance

Table 19: Regulatory Pathway in India

Artificial Intelligence Certification Pillars for India

The AI certification framework will follow six non-negotiable pillars. Table 20 brings out the proposed AI certification pillars and requirements for the same.

Pillar	Requirement
Safety by Design	DO-178C+DO-330+AMLAS integration
Trustworthy AI	Explainability, verifiability, traceability
Runtime Assurance	Fallback safety systems required
Data Assurance	Validated Training datasets with provenance
Cyber Resilience	DO-326A security compliance
Auditability	Certification evidence+ black box logging

Table 20: Artificial Intelligence Certifications Pillars

Artificial Intelligence Certification Process–Civil Aviation (Directorate General of Civil Aviation)

The proposed DGCA AI certification workflow should follow a structured and progressive regulatory process. It would begin with application submission by the OEM or airline, outlining the AI system classification and intended operational use. The DGCA would then categorise the system according to defined AI levels and conduct a hazard assessment by mapping the system to an appropriate DAL. This would be followed by submission of an AMLAS-based ML safety case demonstrating system reliability and safety assurance. Validation would include simulation-based evaluation and limited flight trials, after which the DGCA may grant sandbox authorisation through an AI Sandbox Experimental Certificate for controlled operational testing. AI behaviour and safety data would be continuously monitored and reviewed prior to certification, which may be issued as an AI-Type Certificate Supplement. The process would conclude with post-certification surveillance through continuous monitoring mechanisms to ensure sustained operational safety and compliance.

Artificial Intelligence Certification Process–Military Aviation (Indian Air Force/Defence Research and Development Organisation/Hindustan Aeronautics Limited)

The military certification workflow incorporates additional security and mission risk considerations to address operational complexities. The process begins with mission

classification based on the operational environment, such as benign, contested, or hostile theatres, followed by assignment of an appropriate D-DAL level through mission risk-based evaluation. Systems are then subjected to rigorous adversarial testing, including EW scenarios, spoofing attempts, and adversarial AI attacks. A mandatory human authority layer is enforced to ensure command oversight and override capability. This is followed by secure trial deployment on restricted test ranges to validate operational performance under controlled conditions. Upon satisfactory evaluation, Operational AI Approval may be granted, enabling phased and controlled introduction of the system into operational squadrons. Table 21 proposes the mechanisms to operationalise AI in aviation.

Mechanism	**Description**
AI Sandboxes	Establish AI test corridors in India
National AI Testbeds with DRDO/DGCA	For high-fidelity AI test simulation
India AI Aviation Registry	Logs all certified AI systems
Model Update Approval Board	Ensures controlled AI model updates
AI Incident Reporting Protocol	Standard for AI-related accident investigation

Table 21: Implementation Mechanisms

Certification Documentation Requirements

Every AI system should be supported by documentation to ensure safety, transparency, and accountability throughout lifecycle. This should include an AI risk log to identify potential hazards and mitigation measures. Further, a data safety case outlining data governance practices and validation procedures, along with an XAI report describing system decision-making processes, needs to be ensured. In addition, a detailed AI behaviour monitoring plan should be provided for continuous oversight of performance, along with cybersecurity threat analysis to address system vulnerabilities. The submission should also include a defined lifespan and model update strategy to manage system evolution and continued airworthiness. These requirements are summarised in Table 22 for civil and military applications.

Deliverable	**Civil (DGCA)**	**Military (DAACA)**
AI Test Plan	Required	Classified
Data Integrity Report	Required	Strict + theatre data
Cybersecurity Test	Zero-trust compliance	EW hardened
Behaviour Trace Logs	Submitted monthly	Real-time encrypted stream

Deliverable	**Civil (DGCA)**	**Military (DAACA)**
Flight Trials	Airport sandbox	Weapon range/HWIL simulation

Table 22: Artificial Intelligence Certification Deliverables (Civil–Military Comparison)

Chapter 9

Ethical, Legal, and Human Factor Considerations for Artificial Intelligence Certification

AI in aviation cannot be certified on technical merit alone. It should also satisfy ethical compliance, legal accountability, and human–system integration requirements. These dimensions form a part of trustworthy AI assurance. The same has now been recognised by both EASA (2022) and ICAO (2023) as mandatory certification domains. For India, especially with national security implications in military AI deployment, these considerations are critical to building institutional legitimacy and public trust.

Ethical Governance in Artificial Intelligence Aviation

Ethical certification should be embedded through principles, process, and control mechanisms, as shown in Table 23.

Core Ethical Requirement	**Implication in Aviation**
Human Responsibility	AI must assist, not replace, pilot/commander authority
Safety Priority	AI design must minimise harm beyond compliance
Fairness	Data must reflect operational diversity (terrain, weather, sensor quality)
Transparency	AI decisions must be explainable and auditable

Core Ethical Requirement	Implication in Aviation
Accountability	Duty of care must be assigned to operators and OEMs
Dual-Use Caution	AI must not drift toward unintended military lethality

Table 23: Ethical Governance in AI Aviation

Guidance for India can align with EASA Ethics in AI Framework Organisation for Economic Co-operation and AI principles under, United Nations Educational, Scientific and Cultural Organization's AI Ethics Charter.[31,32]

Legal Accountability Challenges

The use of AI introduces complexities in liability and forensic investigation after incidents. Certification should require a legal chain of accountability to manage AI-assisted or AI-induced accidents. Table 24 highlights these issues.

Legal Issue	Certification Response
Fault attribution	AI Responsibility Matrix in system logs
Evidence management	AI black-box logging + model state archive
Liability assignment	Shared accountability clauses—OEM + operator
Incident investigation	AI-Accident Inquiry Protocol required

Legal Issue	Certification Response
Compliance with law	DPDP Act (India), aviation law, defence secrecy

Table 24: Legal Challenges

AI certification in India should amend the AAIB procedures to include AI failure analysis methodology.

Human Machine Interface

Pilots must remain at the centre of aircraft control, with AI designed to assist rather than replace human authority. Accordingly, system certification should always ensure clear human override priority and provide explainable decision displays to support pilot awareness and trust. It should include training to build confidence in managing AI-enabled systems and address risks of complacency due to automation. Certification must reinforce the pilot-in-command doctrine. This will ensure that ultimate operational responsibility and control remain with the human operator. For military AI certification, systems must not be allowed to make critical decisions independently. The framework should ensure that ROE ensure human-in-the-loop control for all critical actions. This is to maintain human authority, accountability, and ethical oversight in operational decision-making.

Societal Acceptance and Trust

Certification should include public trust-building mechanisms for AI-powered aviation. The DGCA and IAF should adopt AI transparency reports while protecting security-sensitive information. For civil AI systems,

mandatory public disclosure is needed to provide clear information about the system's intended purpose, operational security scope, and known limitations. It should provide compliance with ethical standards and applicable AI certification class. This will promote public trust, regulatory compliance, and accountability. However, in the defence context, transparency should be exercised in a controlled manner. This should be done by ensuring proper oversight through reporting to the Parliament by the MoD and review by the Comptroller and Auditor General.

Certification Ethics Checklist for India (Proposed)

Table 25 below summaries this checklist.

Requirement	**Civil Aviation**	**Military Aviation**
AI usage disclosure	Yes	Controlled
Human control policy	Mandatory	Mandatory
Bias control	Yes	Yes
Explainability	Yes	Required evidence
Accountability model	Shared responsibility	Command authority with OEM audit
Lethal AI	Prohibited	Human authorisation only

Table 25: Proposed Certification Ethics Checklist

Chapter 10

Full Artificial Intelligence Certification Model for India (Process, Compliance Templates, and Key Performance Indicators)

This section presents a complete operational AI certification model designed for India's civil and military aviation ecosystems. Aligning with the DGCA and proposed DAACA frameworks, the model integrates internationally recognised certification methods (DO-178C, AMLAS, EASA AI levels, SAE G-34) into a single structured pathway with clear certification steps, document templates, audit requirements, and compliance metrics.

Artificial Intelligence Certification Lifecycle–India Framework

The proposed AI certification lifecycle for India aligns with global aviation safety principles while addressing data-driven system assurance needs nine-stage certification lifecycle, as shown in Table 26.

Stage	Description	Output
1. AI Classification	Determine AI Level (1–4)	AI System Classification Note
2. DAL/D-DAL Assign	Map to Design Assurance Level	Hazard and DAL Assessment

Stage	**Description**	**Output**
3. AI Requirements	Define AI Safety/ Functional Requirements	ML Requirement Specifications (MLRS)
4. Data Assurance	Verify dataset validity	Data Safety Report
5. Model Verification and Validation	Robustness, adversarial, XAI testing	V&V Compliance Report
6. System Integration	Safety integration with avionics	Interface Control Docs
7. Simulated and Flight Testing	AI testing in sandbox	Evaluate Flight Evidence Report
8. Certification and Approval	DGCA/ DAACA audit	AI Compliance Certificate
9. Post-Cert Monitoring	Model drift+ updates tracking	AI Surveillance File

Table 26: AI Certification Lifecycle–India Framework

Artificial Intelligence Certification Document Set (Mandatory Templates)

Table 27 proposes necessary documents to generate traceability for AI certification.

Document	**Purpose**
AI System Intent and ODD Document	Operational scenario and risk
AI Risk Assessment	Hazard identification
MLRS	Safety + functional ML behaviour
Data Management Plan	Dataset lineage and quality
Model Validation Report	Verification of ML integrity
XAI-R	Explainability + Traceability
Runtime Assurance Plan	AI Failover operational safety
Model Update Plan	Governance of upgrades
Certification Compliance Matrix	Evidence mapping to requirements

Table 27: Proposed Mandatory Documents to Generate Traceability

These templates will become DGCA Annexures under CAR-AI and DAACA Defence Annexures (DA-Form AI-1 to AI-9).

Certification Metrics for Approval

AI certification approval should be based on quantifiable safety and reliability KPIs, as brought out in Table 28.

KPI Category	**Metric**
Safety KPIs	Loss-of-separation rate, AI-induced false alarms, emergency disengagement frequency
Data KPIs	Coverage completeness index, dataset bias ratio, ODD representation
Explainability KPIs	Percentage of interpretable outputs logged explanation latency
Runtime Assurance	Numbers of RTA interventions/hour, fallback execution time
Resilience	EW attack resilience score, anomaly detection rate

Table 28: Certification Metrics for Approval

These KPIs be monitored during certification testing and operational deployment.

Compliance Levels (CL) and Audit Structure

AI systems will follow tiered-compliance audits, as shown in Table 29.

Compliance Level	Audit Requirement
CL A–Basic AI Compliance	For Level 1 and Level 2 AI
CL B–Restricted AI Safety Approval	For Level 3 AI
CL C–Full AI Type Certification	For Level 4 AI (civil)
CL M–Mission AI Certification	For defence autonomy and MUM-T

Table 29: Compliance Levels and Audit Structure

Each audit also assigns a model update risk score to govern future model updates.

Artificial Intelligence Safety Evidence Checklist

Table 30 provides a safety checklist with AI in aviation.

Requirement	Civil (DGCA)	Defence (DAACA)
DO-178C compliance	Required	Required
AMLAS safety case	Required	Required
Explainability logs	Required	Required
Runtime safety guard	Level 3–4	Mandatory
EW/cyber testing	Optional	Mandatory

Requirement	**Civil (DGCA)**	**Defence (DAACA)**
Model Retrain approval	DGCA	DAACA Security Board
AI black box recording	Mandatory	Mandatory (encrypted)

Table 30: Checklist for Artificial Intelligence Safety

Certification Decision Logic for India (Proposed)

An AI system may be approved when it meets defined safety and assurance requirements. Approval should be contingent upon safety performance indicators remaining within accepted thresholds, validation of human-in-command override capability and limited RTA interventions within prescribed limits. The system must also demonstrate adequate dataset representativeness, verified cybersecurity resilience, and bias levels within acceptable bounds. Conversely, certification should be denied if the system fails to provide sufficient explainability evidence, exhibits unsafe performance drift, undergoes unauthorised retraining, or relies on unverifiable training data. Systems that fail to meet established safety case audit requirements should likewise be rejected.

Chapter 11

India Artificial Intelligence Certification Roadmap (2025–2035)

This section proposes a phased implementation plan for civil and military aviation (DGCA+IAF/DRDO+HAL). This will enable safe and adoption of AI in Indian aviation. This roadmap aligns with global certification timelines. It considers India's regulatory readiness, capability gaps, and national security priorities.

Roadmap Objectives

The proposed roadmap provides a structured pathway for the safe deployment of AI in civil aviation. This is under DGCA oversight while enabling mission-grade assurance for AI applications within the IAF. It also aligned with international regulatory frameworks such as FAA, EASA, and ICAO. Hence, this ensures facilitating global interoperability and export potential. In addition, this framework contributes to the development of dedicated AI safety standards for the Indian aerospace industry. Hence, it strengthens indigenous capability and advances the objectives of *Atmanirbhar Bharat* (self-reliant India) in aviation AI.

As a preparatory step, the pre-phase activity (2024–2025) envisages CEMILAC initiating pilot studies on certification of AI/ML systems in non-flight-critical applications and evaluation of adaptive software. These studies are intended to generate technical and regulatory evidence necessary for the design and implementation of the proposed DAACA framework.

Artificial Intelligence Roadmap in Civil Aviation

Table 31 proposes the phased roadmap for civil use under the DGCA.

Phase	**Timeline**	**Objective**	**Key Actions**
Phase 1– Foundation	2025–2026	Establish AI regulation	CAR-AI released; AICDA formed
Phase 2– Assistive AI	2026–2028	Approve non-safety AI	Certify Level 1–2 AI
Phase 3– Safety-Assisted AI	2028–2031	Introduce flight assistance AI	Certify Level 3 AI + sandbox
Phase 4– Semi-Autonomy	2031–2035	Limited autonomous taxiing/ATC assist	Certify Level 4 AI

Table 31: Phased Artificial Intelligence Roadmap (Civil)

Military Aviation Artificial Intelligence Roadmap

Table 32 proposes phased roadmap for defence use under the IAF, DRDO, and DAACA.

Phase	Timeline	Objective	Mission Focus
Defence Phase 0	2025	Establish DAACA	Create national military AI safety doctrine
Phase 1 – Trials	2026–2028	Supervised AI	MUM-T, ATR (target recognition), EW resilience
Phase 2 – Bounded Autonomy	2028–2032	Corridor autonomy	UCAV escort operations; secure cargo
Phase 3 – Operational AI	2032–2035	Broad AI deployment	Mission autonomy under IAF command

Table 32: Phased Aviation Artificial Intelligence Roadmap (Military)

Key Government Enablers Required

The proposed roadmap envisages the establishment of key institutional and regulatory mechanisms to support safe and accountable deployment of aviation AI. It includes the creation of a DGCA AI Directorate to certify civil AI systems and a resolute DAACA framework for classification and assurance of military AI applications. The roadmap also

proposes a National AI Flight Test Range to provide a dedicated corridor for testing drones and autonomous systems. In addition, an Aviation AI Safety Act (2026) is envisaged to address legal liability and accountability, supported by an AI Ethics Charter to ensure continued human control in aviation AI. These elements are illustrated in the proposed roadmap shown in Figure 2.

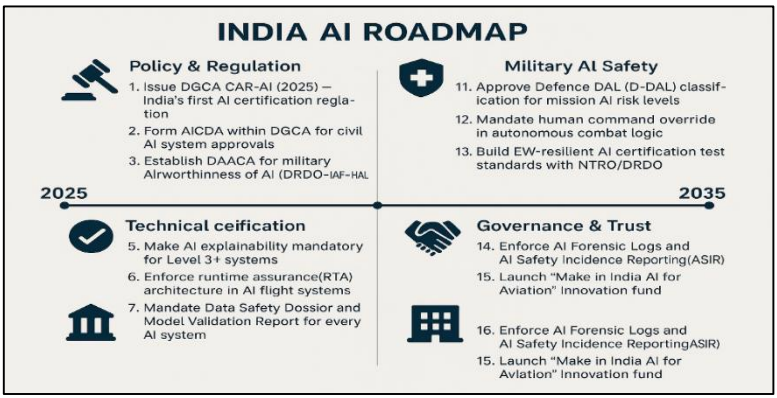

Figure 2: India Artificial Intelligence Roadmap

Chapter 12

Recommendations

Civil Aviation

Non-Safety-Critical AI Systems. These are applications that do not directly influence aircraft control or immediate safety outcomes. India should begin here to build regulatory confidence. The DGCA should first authorise AI in areas such as predictive maintenance, airline analytics, flight data assessment, airport management systems, and advisory decision-support tools. A resolute DGCA AI Regulatory Cell should be established to register AI systems, approve datasets, and monitor behaviour trends. AI deployments should initially operate under a controlled 'Sandbox' regime with monitored performance rather than blanket approvals. Airlines and OEMs should be required to maintain records of AI behaviour, bias testing, dataset sources, and performance drift. Training programmes should prepare regulators, engineers, and airline safety teams to understand AI behaviour and evaluation principles.

Safety-Related and Safety-Critical AI Systems. These systems may influence aircraft safety, pilot decision-making, or flight operations. The DGCA should delay full certification of safety-critical AI until sufficient confidence is gained from non-critical deployments. The human-in-the-loop governance must bind safety AI—AI may assist, but human control must remain final. Certification should combine existing DO-178C frameworks with AI-specific assurance like structured test cases, oversight during runtime, and though monitoring post-deployment. Explainability

must be mandatory. AI decisions influencing safety must be understandable, traceable, and auditable. Civil aviation should prioritise introduction of AI, beginning with advisory functions such as collision avoidance assistance and anomaly detection before moving to higher autonomy.

Military Aviation

Non-Safety-Critical and Mission-Support AI. These include AI roles that support readiness and efficiency without directly controlling aircraft behaviour. The CEMILAC and IAF should initially approve AI for predictive maintenance, fleet health monitoring, logistics optimisation, mission planning aids, and ISR cueing where human authority remains absolute. These systems should help establish confidence in AI certification processes, dataset integrity, and modification control methods. A structured governance framework should oversee model retraining approvals, cyber-security validation and dataset accreditation. Operator trust is essential. AI systems should be phased into operations only after user training, operational exposure, and confidence building.

Safety-Critical and Combat-Relevant AI. This category includes AI systems that have bearing on aircraft control, autonomy, combat decision-support, or weapon-related outcomes. India must adopt a cautious and phased approach. Such AI should only be authorised when adequate safeguards, runtime assurance, and doctrinal controls are established. Safety assurance must be supported by defence-specific layers, which should include EW resilience, cyber-

hardening, classified data governance, and secure model provenance. However, human command must remain central. Critical decisions such as targeting or weapon release should never occur without explicit human authorisation. Certification authority should transition towards the proposed DAACA for oversight. Progression towards autonomy must be driven based upon evidence, evaluated in simulated-to-live environments, and should remain ethically aligned with India's strategy.

Overarching National Imperatives

Across both civil and military domains, India should move towards a clear and organised system of AI governance. Transparency, accountability, and explainability must remain at core of development and use of AI systems. Strong cyber safety measures are necessary to protect them from misuse or interference. At the same time, building indigenous AI capabilities will help to ensure technological self-reliance for India. It is also important to maintain public confidence through transparency and a safety in AI use.

Conclusion

AI is poised to reshape the future of aviation by enhancing safety, efficiency, autonomy, and mission effectiveness across both civil and military domains. Yet, its adoption in aviation cannot proceed based on technological promise alone. Unlike conventional deterministic software, AI systems are probabilistic, data-dependent, and potentially adaptive, making them difficult to certify under legacy aviation regulatory structures. This creates a pressing need for India to move beyond conventional compliance-based approaches and adopt an evidence-based certification architecture tailored to AI-enabled aviation systems.

The global regulators such as the FAA and EASA are gradually developing structured pathways for AI assurance through lifecycle monitoring, learning assurance, explainability, data governance, and runtime safety. India, by contrast, remains at an early stage. While the BVA, 2024, provides a modern legal foundation, no dedicated AI certification framework yet exists within the DGCA regulations. In military aviation, too, despite growing AI applications in mission planning, predictive maintenance, unmanned systems, and MUM-T, India lacks a dedicated authority for certifying AI-enabled airborne systems under operational and combat conditions.

This monograph, therefore, argues that India must adopt a dual-track yet harmonised approach. In civil aviation, the DGCA should progressively develop an AI certification regime, beginning with non-safety-critical applications and later moving towards safety-related and safety-critical functions. In military aviation, a specialised DAACA is

necessary to address mission assurance, cybersecurity, adversarial robustness, and doctrinal human control. In both sectors, certification must rest on core principles of safety, explainability, accountability, data assurance, runtime monitoring, and cyber resilience.

A phased roadmap for 2035 offers India a realistic pathway to build regulatory capacity, institutional competence, and operational trust. The emphasis must remain on bounded, auditable, and human-supervised AI rather than unchecked autonomy. AI is not a replacement for skill, discipline, or judgement in aviation; rather, as it continues to evolve, it should be treated as an enabler, guided by robust oversight and ethical restraint. When used carefully and responsibly, AI can strengthen safety, efficiency, and mission effectiveness without undermining the safeguards on which aviation depends. If pursued with strategic foresight, India can emerge as a responsible leader in safe, ethical, and mission-ready AI aviation.

Endnotes

[1] Federal Aviation Administration, *Roadmap for Artificial Intelligence Safety Assurance,* (Washington, DC: US Department of Transportation, 2024).

[2] European Union Aviation Safety Agency, *EASA Artificial Intelligence Roadmap 2.0: A Human-Centric Approach to AI in Aviation,* (Cologne: EASA, 2023).

[3] Radio Technical Commission for Aeronautics, *DO-178C: Software Considerations in Airborne Systems and Equipment Certification,* (Washington, DC: RTCA Inc., 2011).

[4] Radio Technical Commission for Aeronautics, *DO-326A: Airworthiness Security Process Specification,* (Washington, DC: RTCA Inc., 2014).

[5] AS9100, *AS9100D: Quality Management Systems—Requirements for Aviation, Space and Defense Organizations,* (International Aerospace Quality Group / SAE International, 2016).

[6] Guy Katz, Clark Barrett, David L Dill, Kyle Julian, and Mykel J. Kochenderfer, "Neural Network Verification for Aircraft Collision Avoidance Systems", *Journal of Guidance, Control and Dynamics* 44, no. 10 (2021): 1989–2002, accessed 11 Mar 2026, https://doi.org/10.2514/1.G005640

[7] Radio Technical Commission for Aeronautics, *Special Committee 240 — Guidance for Learning Assurance and AI in Aviation,* (Washington, DC: RTCA Inc., 2023).

[8] Richard Hawkins, Ibrahim Habli, Tim Kelly, John McDermid, and Philippe Guillaume, *Assurance of Machine Learning for Use in Autonomous Systems (AMLAS),* (York: University of York, 2021).

[9] NATO Standardization Office, *STANAG 4671: Unmanned Aircraft Systems—Airworthiness Requirements,* (Brussels: NATO, 2019).

[10] Ministry of Defence, Government of India, "Task Force for Implementation of AI", Press Release No. 1810442, *Press Information Bureau*, New Delhi, 28 Mar 2022, accessed 10 Mar 2026, https://pib.gov.in/PressreleaseiframePage.aspx?PriD=1810442

[11] Mykel J Kochenderfer, *Decision Making Under Uncertainty: Theory and Application,* (Cambridge, MA: MIT Press, 2015).

[12] International Civil Aviation Organization, *Aviation Cybersecurity Strategy 2022–2030,* (Montreal: ICAO, 2022).

[13] Saleema Amershi, Daniel S. Weld, Mihaela Vorvoreanu, Adam Fourney, Besmira Nushi, Penny Collisson, Raymond Garnett, Eric Horvitz, Ece Kamar, Walter S Lasecki, and Jennifer W Vaughan, *Guidelines for Human–AI Interaction,* (New York: Association for Computing Machinery, 2019).

[14] S Ghosh, P Roy, and A Banerjee, "Assurance of Learning Systems in Mission-Critical Applications: Challenges and Methods", *IEEE Systems Journal* 16, no. 4 (2022): 5500–5512, accessed 13 Mar 2026, https://doi.org/10.1109/JSYST.2022.3145678

[15] Geoffrey E Hinton, "Deep Learning and the Future of Intelligent Systems", *Communications of the ACM* 61, no. 11 (2018): 58–65, accessed 12 Mar 2026, https://doi.org/10.1145/3132698

[16] European Union Aviation Safety Agency, *Artificial Intelligence Roadmap (2020–2025): Towards Trustworthiness in AI*, (Cologne: EASA, 2020).

[17] International Organization for Standardization, *ISO/IEC 23894:2023—Information Technology—Artificial Intelligence—Guidance on AI Risk Management,* (Geneva: ISO, 2023).

[18] R Salay, R Queiroz, and K Czarnecki, "A Safety Analysis Approach for Machine-Learning Components in Automotive Software Systems", in *Proceedings of the Automotive Software Engineering Conference* (2019), 12–25.

[19] Kush R Varshney, *Trustworthy Machine Learning,* (Sebastopol, CA: O'Reilly Media, 2022).

[20] Gary Marcus, "The Next Decade in AI: Four Steps Toward Robust Artificial Intelligence", *AI Magazine* 41, no. 3 (2020): 5–24, accessed 14 Mar 2026, https://doi.org/10.1609/aimag.v41i3.5301

[21] Bryce Goodman and Seth Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation", *AI Magazine* 38, no. 3 (2017): 50–57, accessed 13 Mar 2026, https://doi.org/10.1609/aimag.v38i3.2741

[22] International Civil Aviation Organization, *Aviation Cybersecurity Strategy 2022–2030,* (Montreal: ICAO, 2022).

[23] International Civil Aviation Organization, *Concept Note: Artificial Intelligence in Aviation Governance,* (Montreal: ICAO, 2023).

[24] SAE International, *Aerospace Recommended Practice 6983: AI in Aviation Safety Standards* (draft), (Warrendale, PA: SAE International, 2025).

[25] India, *The Bharatiya Vayuyan Adhiniyam, 2024 (Act No. 16 of 2024),* enacted 11 Dec 2024, commenced 01 Jan 2025, accessed 13 Mar 2026, https://upload.indiacode.nic.in/view-casepdf?type=act&id=AC_CEN_36_

[26] European Union Aviation Safety Agency, *Artificial Intelligence Roadmap 2.0: Toward Trustworthy AI in Aviation*, (Cologne: EASA, 2022).

[27] RTCA, *DO-178C: Software Considerations in Airborne Systems and Equipment Certification*, (Washington, DC: RTCA, 2012).

[28] Centre for Military Airworthiness and Certification, *Indian Military Technical Airworthiness Requirements (IMTAR*), v. 2.0, (Bengaluru: Government of India, Ministry of Defence, 2021).

[29] RTCA, *DO-326A: Airworthiness Security Process Specification,* (Washington, DC: RTCA, 2014).

[30] SAE International, *SAE G-34/EUROCAE WG-114 Artificial Intelligence in Aviation (Draft Standard),* (Warrendale, PA: SAE, 2025).

[31] Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence,* (Paris: OECD Publishing, 2019);

United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence*, (Paris: UNESCO, 2021).

About the Authors

Mukhvinder Pal Singh Virk was commissioned into the Aeronautical Engineering Branch of the Indian Air Force (IAF). An alumnus College of Defence Management (CDM), Aeronautical society of India (AeSI) and Indian Institute of Technology-Madras, he is presently serving as Principal Director with the IAF at the Aeronautical Development Agency (ADA). He is simultaneously pursuing a doctorate in Defence and Strategic Studies at Savitribai Phule Pune University. He was awarded with certificate of merit and commendation, by the Chief of Defence Staff during Ran Samwad 2026 on topic 'Integration of Intelligence, Surveillance, and Recognition in Multi-Domain Opeartions for Decision Superiority in Defence Services'.

Sumedh Singh Virk is pursuing Bachelors of Technology in Computer Science and Engineering (Artificial Intelligence/Machine Learning [AI/ML]) at Bhusanayana Mukundadas Sreenivasaiah College of Engineering, Bengaluru. He is an enthusiast in AI/ML and autonomous technology research and development for India.

About the USI

The United Service Institution (USI) of India was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor 'For the furtherance of interest and knowledge in the Art, Science, and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. The USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd).

Rao Tula Ram Marg,
Opposite Signals Enclave,
New Delhi-110057
Tele: 2086 2316/Fax: 2086 2315, E-mail: dircpl@usiofindia.org

₹350