



WORKING PAPER

ASSEMBLY — 42ND SESSION

TECHNICAL COMMISSION

Agenda Item 25: Other issues to be considered by the Technical Commission

MODERNIZING AVIATION SAFETY TRAINING: INCLUDING ARTIFICIAL INTELLIGENCE AND CYBERSECURITY INTO ICAO COMPETENCY STANDARDS FOR ATSEP

(Presented by the International Federation of Air Traffic Safety Electronics Associations (IFATSEA))

EXECUTIVE SUMMARY

The Aviation industry is becoming more complex every day with technological advancements such as Artificial Intelligence, automation and digitization. These technologies are reshaping and redefining the execution of technical operations in a fast-paced manner. Given the fact the Aviation Industry is highly reliant on the achievement of high safety standards, it will serve the industry best for the professionals at the centre of these technical operations to be proficient in the use and management of these technologies which have found their way into the civil aviation operations. This paper recommends an update to the *Manual on Air Traffic Safety Electronics Personnel Competency-based Training and Assessment* (Doc 10057), to incorporate Artificial Intelligence (AI) and cybersecurity as a distinct and essential training domain. These rapidly evolving technologies present both challenges and transformative opportunities for the aviation sector. Embedding them in ICAO's training guidance, alongside provisions in the *Procedures for Air Navigation Services – Training* (Doc 9868) is crucial to ensuring preparedness, safety, and resilience across all Member States.

Action: The Assembly is invited to:

- a) endorse the inclusion of an AI and cybersecurity domain into ICAO Doc 10057;
- b) task ICAO Secretariat to initiate drafting and consultation with relevant experts; and
- c) encourage Member States to pilot new training modules and share outcomes.

<i>Strategic Goals:</i>	This working paper relates to <i>Every Flight is Safe and Secure, Aviation is environmentally sustainable, Aviation Delivers Seamless, Accessible, and Reliable Mobility For All and No Country is Left Behind.</i>
<i>Financial implications:</i>	To be determined
<i>References:</i>	Doc 10057, <i>Manual on Air Traffic Safety Electronics Personnel Competency-based Training and Assessment</i> Doc 9868, <i>Procedures for Air Navigation Services – Training</i>

¹ English Arabic, Chinese, French, Russian and Spanish versions provided by IFATSEA.

1. INTRODUCTION

1.1 The civil aviation industry is undergoing a technological revolution. Automation, predictive analytics, and digital security are redefining how civil aviation operations is managed, operated, and secured. AI is being used in civil aviation operations and control systems, crew scheduling, safety analysis, and passenger services. Increasing cyber threats necessitate a robust and skilled cybersecurity workforce across aviation systems. To keep pace with this evolution, *The Manual on Air Traffic Safety Electronics Personnel Competency-based Training and Assessment* (Doc 10057) must be updated to include structured guidance on developing training programs in AI and cybersecurity.

1.2 Including an AI and cybersecurity training domain in ICAO Doc 10057 will equip air traffic safety electronics personnel (ATSEP) professionals across regions with a unified skillset, enhancing competence in air traffic management, data sharing, and cybersecurity response.

1.3 ATSEP proficiency in AI and cybersecurity strengthens system resilience and fosters a proactive culture to prevent, mitigate, and recover from digital threats.

1.4 To align ICAO's competency frameworks with technological realities, Doc 10057 should be updated to offer structured guidance on AI and cybersecurity, complementing the foundational training principles in the *Procedures for Air Navigation Services — Training* (PANS-TRG, Doc 9868).

2. DISCUSSION

2.1 AI and cyber security threats are transforming the civil aviation industry and global air traffic management (ATM) systems with heavy emphasis on digitalisation, automation, data-centricity, and interoperability. These developments will have significant implications for ATSEP professionals, whose role is central to ensuring the safety and performance of ATM systems.

2.2 ATSEP professionals will increasingly work with emerging technologies such as:

- a) AI-driven automation;
- b) digital information-sharing platforms;
- c) modular and virtualised infrastructure; and
- d) real-time system performance tools.

2.3 The scope of ATSEP work is gradually expand beyond maintenance and operation of legacy systems to managing integrated, digital, and dynamic infrastructures.

2.4 Given the fact civil aviation systems are shifting towards Systems Integration and Cybersecurity, ATSEP will be crucial in:

- a) designing, implementing, and securing interconnected systems;
- b) ensuring cyber-resilience in a highly networked ATM environment;

- c) support human-in-the-loop and human-on-the-loop systems;
- d) develop and maintain tools that enable controllers and systems to co-manage airspace operations; and
- e) ensure systems are intuitively designed, traceable, and responsive to real-time operational needs.

3. CONCLUSION

3.1 Including an AI and Cyber Security training domain in Doc 10057, ICAO sets the stage for a more resilient, unified, and forward-thinking global aviation community through the following:

Collaborative Course Development

- a) Encourages joint curriculum initiatives among ICAO Member States, aviation academies, and industry partners.
- b) Empowers lower-resourced nations to leverage global expertise and localize cutting-edge training programs.

Collective Innovation

- a) Shared training stimulates cross-pollination of ideas between States and operators, helping develop smarter, safer technologies.
- b) Fosters a culture of collaboration, where AI solutions and cybersecurity frameworks benefit from diverse perspectives and pooled research.

3.2 Including an AI and Cyber Security training domain in Doc 10057 encourages development of training pathways for emerging economies to participate in aviation innovation. It will also reduce the digital divide by democratizing access to essential AI and cybersecurity education.

3.3 ICAO-led coordination will ensure curricula incorporate AI and cybersecurity modules consistent with Doc 9868 frameworks.

3.4 Cyber-aware professionals would be better equipped to defend aviation infrastructure against escalating threats like ransomware and system breaches.

3.5 The Assembly is asked to consider the Actions contained within the Executive Summary.