

L'Évaporation de la Responsabilité : Analyse Médico-Légale de l'Intégration de l'IA dans les Infrastructures Aéronautiques Cinétiques Lourdes



En mai 2026, une démonstration de relations publiques hautement aseptisée a eu lieu dans le ciel de la Californie et de l'Alaska.¹ Comme l'a rapporté CNN, un Cessna Grand Caravan a accéléré sur une piste, s'est élevé dans les airs et a navigué au-dessus d'un terrain complexe sans que son pilote de sécurité ne touche les commandes.¹ Tim Burns, le directeur technologique de la startup de vol autonome Merlin Labs, plaisantait à l'interphone pendant que le pilote d'essai Matt Diamond gardait les mains posées sur ses genoux.¹ Pour l'observateur occasionnel, cet événement représentait un bond en avant fluide vers un avenir plus sûr et automatisé du transport aérien.¹

Cependant, pour les analystes aérospatiaux et les experts en systèmes autonomes, ce vol était une démonstration d'entreprise calculée masquant une crise structurelle profonde. L'industrie aéronautique se prépare activement à transférer des infrastructures cinétiques lourdes — des plateformes de plusieurs tonnes transportant des passagers et du fret à des vitesses et des altitudes élevées — à des couches logicielles fondamentalement imprévisibles et non déterministes.⁶ Cette transition ne naît pas d'un impératif absolu de sécurité, mais plutôt d'intenses pressions macroéconomiques, de pénuries de main-d'œuvre parmi les pilotes et

d'un effort à l'échelle de l'industrie pour contourner les cadres de responsabilité traditionnels.⁸

Les Dessous Économiques du Dépeuplement des Cockpits

Le discours entourant l'automatisation des cockpits a longtemps été présenté comme une quête de sécurité absolue, les relations publiques des entreprises présentant l'intelligence artificielle comme la solution ultime à "l'erreur humaine".¹ Pourtant, un examen approfondi des bilans de l'industrie révèle que le passage vers le contrôle de vol autonome est motivé par l'économie du travail.¹⁰

Les compagnies aériennes opèrent sur de faibles marges de capitaux, très sensibles aux fluctuations des coûts du carburant et à l'escalade des dépenses de main-d'œuvre.⁸ Les transporteurs européens à bas prix, par exemple, doivent maintenir un ratio coûteux d'environ 10 à 11 pilotes qualifiés par appareil pour satisfaire aux strictes limites de temps de vol et de service ainsi qu'aux redondances de planification.¹⁰ De plus, les secteurs de la logistique régionale de fret et d'apport font face à des pénuries chroniques de pilotes, car les grands transporteurs de passagers drainent continuellement le vivier de main-d'œuvre des capitaines expérimentés.⁵

Pour contrer ces forces érodant les marges, les principaux constructeurs d'avions, dirigés par Airbus et Dassault, ont agressivement fait pression sur les régulateurs de l'aviation pour qu'ils approuvent les opérations en équipage minimum étendu (Extended Minimum Crew Operations - eMCO).¹³ L'objectif initial de l'eMCO est de réduire le personnel du poste de pilotage pendant la phase de croisière du vol de deux pilotes à un seul opérateur, avec pour but éventuel le dépeuplement complet du cockpit.⁹

Cette pression des entreprises a rencontré une vive opposition de la part des syndicats de pilotes, tels que l'Association Européenne des Pilotes de Ligne (ECA) et l'Air Line Pilots Association (ALPA).⁹ Les représentants syndicaux de l'industrie avertissent que le retrait du second pilote élimine une couche de sécurité humaine essentielle.⁹ Dans le paradigme actuel à deux pilotes, la vérification cognitive croisée, la surveillance mutuelle et l'atténuation de la fatigue en temps réel empêchent les anomalies mineures de se transformer en pertes catastrophiques d'appareils.⁹

En juin 2024, le Parlement néerlandais a mis en évidence ces préoccupations de sécurité en adoptant une motion déclarant que les nouvelles technologies de cockpit ne doivent être certifiées que si elles améliorent de manière démontrable la sécurité des vols, plutôt que de simplement réduire les frais généraux opérationnels des compagnies aériennes.¹³ Malgré cet avertissement, la dynamique économique de l'industrie reste concentrée sur l'automatisation.¹⁰

Métrique Opérationnelle	Poste de Pilotage Classique à Deux Pilotes	Opérations en Équipage Minimum Étendu (eMCO)	Flotte de Fret Autonome Sans Équipage
-------------------------	--	--	---------------------------------------

Frais Généraux d'Équipage par Appareil	Référence (Indice de Coût 100%) ¹⁰	Réduction de 30% à 40% ¹⁰	Réduction de 80% à 90% ¹¹
Cadre Réglementaire	Norme FAA Part 121 / 135 ¹²	EASA RMT.0739 (Cockpits Intelligents) ¹³	FAA Special STC (Catégorie Normale) ⁷
Limites de Fatigue et de Service	Plafonds d'heures de service très restrictifs ¹²	Protocoles complexes d'inertie du sommeil et de pause ⁹	Éliminées ; routage continu activé ¹⁴
Couche de Sécurité Primaire du Système	Vérification et validation par deux humains ⁹	Pilote unique surveillé par une IA de base ⁹	Moteurs d'inférence statistique en temps réel ⁷

Le Casse-Tête de la Certification "Boîte Noire"

Depuis plus d'une décennie, les logiciels embarqués commerciaux sont régis par la norme RTCA DO-178C (Considérations logicielles dans la certification des systèmes et équipements embarqués).¹⁵ Le fondement du DO-178C est un déterminisme absolu.⁶ Pour les logiciels classés au niveau d'assurance de conception A (DAL-A) — où une défaillance entraînerait la perte catastrophique de l'aéronef — le développeur doit fournir des preuves objectives d'une couverture des conditions/décisions modifiées (MC/DC) à 100 %.¹⁵ Chaque chemin logique individuel doit être traçable, depuis les exigences système de haut niveau jusqu'au code source de bas niveau, et finalement jusqu'au code objet exécutable tournant sur l'ordinateur de commande de vol.¹⁵

L'apprentissage profond et les réseaux de neurones brisent ce paradigme de certification dans son intégralité.⁶ Un réseau de neurones convolutifs (CNN) utilisé pour le contrôle de vol ou l'intelligence situationnelle ne fonctionne pas selon des règles définies par des humains.⁶ Au lieu de cela, il utilise des millions de poids statistiques ajustés au cours de l'entraînement.⁶ Les exigences ne peuvent pas être directement tracées à des lignes de code spécifiques.⁷ Le processus de prise de décision est fondamentalement non déterministe et fonctionne comme une "boîte noire" non auditable.⁷

Pour relever ce défi, des organisations comme l'EASA et la FAA tentent d'établir de nouveaux cadres réglementaires basés sur les Concepts d'Assurance de Conception pour les Réseaux de Neurones (CoDANN).⁷ Dans le cadre de CoDANN et de ses itérations ultérieures, les développeurs abandonnent la vérification logicielle classique au profit du **processus de développement en W**.⁷

\\

[Vérification du Modèle]

\ /

[Architecture du Modèle] ---

Le processus en W établit l'assurance par l'intermédiaire d'un pipeline de vérification en trois étapes⁷ :

1. **Vérification du Jeu de Données** : Les ensembles de données d'entraînement, de validation et de test doivent être rigoureusement sélectionnés, équilibrés et prouvés pour couvrir l'ensemble de l'enveloppe de vol opérationnelle.⁶
2. **Vérification du Modèle** : L'apprentissage en ligne, en cours de vol, est strictement interdit.⁶ Le réseau de neurones est formé exclusivement dans un environnement de laboratoire.⁷ Une fois que le modèle atteint des taux d'erreur acceptables, ses poids sont figés.⁶ Les poids figés sont traités comme des éléments de données de paramètres (PDI) selon la DO-178C, forçant le système à se comporter de manière déterministe lors de l'exécution.⁶
3. **Vérification de l'Inférence** : La théorie de l'apprentissage statistique est utilisée pour limiter mathématiquement l'erreur de généralisation du modèle dans son domaine opérationnel défini.⁷

Afin de fournir des limites de sécurité, les ingénieurs emploient des limites de performance de généralisation, s'assurant que le risque empirique $\hat{R}(f)$ du modèle f sur un jeu de données de taille n limite le vrai risque $R(f)$ avec une forte probabilité :

$$R(f) \leq \hat{R}(f) + \mathcal{O}\left(\sqrt{\frac{d}{n}}\right)$$

où d représente la dimension de Vapnik-Chervonenkis (VC) de l'architecture du réseau de neurones.

Malgré ces cadres mathématiques, l'incertitude statistique des réseaux de neurones reste trop élevée pour les commandes de vol primaires.⁷ Par conséquent, les développeurs sont contraints de mettre en œuvre un paradigme à double architecture.⁶

Le modèle d'IA non déterministe est isolé dans un environnement partitionné, tandis qu'un moniteur de sécurité traditionnel, déterministe et conforme à la norme DO-178C, agit comme un gouverneur externe.⁶ Si le contrôleur d'IA commande une entrée qui viole les limites de l'enveloppe de vol prédéfinies — comme un taux de tangage ou un angle de roulis excessif — le système hérité déterministe remplace la commande et prend le contrôle.⁶

Ce partitionnement architectural nécessite une puissance de calcul physique importante.⁷ L'exécution de réseaux de neurones convolutifs (CNN) haute résolution en temps réel nécessite environ une Téra Opération par Seconde (TOPS).⁷ Cette exigence a conduit au développement de matériel spécialisé et certifiable, tel que l'accélérateur tensoriel Daedalean (DTA) mis en œuvre sur les FPGA Intel Agilex.⁷

En utilisant les normes de partitionnement ARINC 653, ces accélérateurs haute performance sont séparés du système d'exploitation en temps réel (RTOS) principal et critique pour la sécurité exécuté sur les armoires d'avionique modulaire intégrée (IMA).⁷ Cette conception garantit qu'un blocage logiciel dans la couche d'IA ne peut pas se propager aux surfaces de contrôle de vol primaires.¹⁷

Le Pipeline de la Défense comme Bac à Sable Opérationnel

La certification et la validation de ces systèmes autonomes sont fortement accélérées par les programmes de développement militaire.²⁰ Le plus important d'entre eux est le programme Air Combat Evolution (ACE) de la DARPA, qui utilise le combat aérien comme cas de test à haute contrainte pour les algorithmes de vol autonome.²⁰

La plateforme principale pour cette recherche est l'aéronef de test de simulation en vol variable General Dynamics X-62A (VISTA).²⁰ Développé par Lockheed Martin Skunk Works et Calspan, le X-62A est un F-16D Block 30 modifié équipé d'un système de contrôle autonome de la simulation (SACS) et d'une vectorisation de poussée multi-axes (MATV).²⁰ L'architecture SACS permet au X-62A d'émuler les qualités de maniabilité de types d'avions entièrement différents, tout en exécutant des agents d'IA expérimentaux en vol réel.²⁰

En avril 2024, l'US Air Force et la DARPA ont achevé le tout premier combat aérien autonome entre le X-62A contrôlé par l'IA et un F-16 piloté par un humain.²² Au cours de ces engagements, l'appareil contrôlé par l'IA a géré avec succès des manœuvres agressives post-décrochage à des angles d'attaque élevés.²³

Pour instaurer la confiance dans ces systèmes automatisés, l'école des pilotes d'essai de l'Air Force utilise des avions d'entraînement à réaction biplaces équipés de capteurs physiologiques.²⁴ Ces capteurs mesurent la biométrie du pilote, comme la fréquence cardiaque, la conductivité cutanée et les modèles de suivi oculaire.²⁴ Ces données permettent aux chercheurs de modéliser mathématiquement l'"étalonnage de la confiance" — le moment précis où un pilote humain décide de céder le contrôle à un agent d'IA lors d'un scénario à forte charge de travail.²⁴

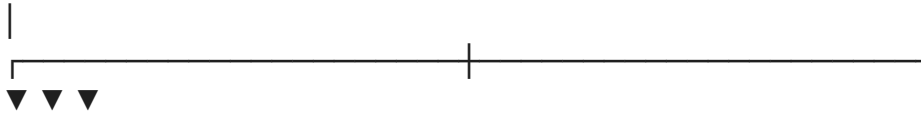
Cette recherche militaire accélère directement les programmes commerciaux de fret autonome.²¹ Des entreprises comme Merlin Labs et Xwing ont directement tiré parti des méthodologies d'essais en vol, des architectures de sécurité et des données de transition du simulateur au monde réel validées par le programme X-62A VISTA.⁵

L'Évaporation de la Responsabilité

L'intégration de pilotes IA non déterministes dans l'espace aérien commercial met en évidence une profonde ironie juridique : l'érosion complète des cadres de responsabilité traditionnels.⁸ Le droit de l'aviation traditionnel repose sur une chaîne claire de responsabilité.⁸ La responsabilité incombe directement du pilote humain certifié aux commandes à la compagnie aérienne exploitante, et finalement au fabricant d'équipement d'origine (OEM) si un système mécanique ou structurel tombe en panne.⁸

Dans un environnement eMCO autonome ou à pilote unique, cette chaîne de responsabilité se dissout.⁸ Étant donné que les réseaux d'apprentissage profond fonctionnent de manière statistique, ils sont sujets à des "hallucinations" imprévisibles ou à des défaillances lorsqu'ils rencontrent des cas limites hors distribution inédits.⁸

Si un avion cargo autonome interprète mal un phénomène météorologique violent ou une entrée de capteur inhabituelle et s'écrase, l'attribution de la faute devient extrêmement complexe.⁸



Revendique la dépendance Blâme les ensembles de Pointe du doigt le bruit des à un système certifié. données non représentatifs. capteurs ou cas limites.

La responsabilité se diffuse à travers un réseau complexe de contributeurs :

- **La Compagnie Aérienne (Opérateur) :** Fait valoir que le système autonome a été certifié par l'EASA/FAA et a fonctionné conformément aux paramètres du fabricant, détournant ainsi la négligence opérationnelle.⁸
- **Le Développeur de Logiciels / Fournisseur de Modèles :** Affirme que le système a fonctionné exactement comme il a été formé, blâmant les lacunes ou les variables non représentées dans les ensembles de données d'entraînement fournis par des tiers.⁸
- **Le Fabricant d'Équipement d'Origine (OEM) :** Pointe du doigt des facteurs externes, tels que le bruit des capteurs, les anomalies environnementales ou les limitations de l'accélérateur matériel.⁸

Cette ambiguïté juridique crée un écart important entre les politiques de gouvernance d'entreprise et le risque opérationnel réel.²⁸ Bien que les compagnies aériennes puissent établir des "chartes éthiques d'IA" de haut niveau, ces cadres ne résolvent pas le problème fondamental.²⁸ Les enregistreurs de données de vol (FDR) traditionnels consignent les entrées physiques, telles que les déflexions du manche et les paramètres du moteur.²⁸ Ils ne sont pas conçus pour enregistrer les activations d'états internes en haute dimension d'un réseau de neurones profonds lors d'un incident.²⁸ Cela rend presque impossible pour les enquêteurs médico-légaux de reconstituer le raisonnement exact derrière une défaillance du contrôle de vol automatisé.⁸

Ce défi a suscité des réponses législatives régionales.²⁹ Aux États-Unis, la loi sur la politique en matière d'intelligence artificielle de l'Utah (SB 149) représente une première tentative au niveau de l'État d'imposer des règles strictes de divulgation et de responsabilité lorsque l'IA générative ou autonome est utilisée dans des professions réglementées.²⁹

De même, la loi de l'Union européenne sur l'IA (AI Act) structure la gouvernance de l'IA comme un régime strict de sécurité des produits, classant les systèmes d'aviation comme étant "à haut risque".³⁰ Ce cadre oblige les développeurs à se soumettre à des évaluations de conformité et à obtenir le marquage CE.³⁰ Cela crée un paysage réglementaire complexe où les développeurs de logiciels sont traités comme des fabricants de matériel, faisant face à une responsabilité stricte pour les résultats statistiques de leurs modèles.⁸

Vecteurs de Menaces Cyber-Physiques et Exploitation Adversariale

Traiter l'avion moderne comme un centre de données volant d'informatique en périphérie ("edge-compute") introduit des vulnérabilités de cybersécurité sans précédent.³¹ Dans des architectures entièrement autonomes, le réseau de neurones se trouve directement sur les bus de données primaires, traduisant en permanence les entrées de capteurs brutes en commandes de contrôle physique.¹⁹ Cette intégration étroite expose le système aux attaques d'**apprentissage automatique adversarial (AML)**.³²

Contrairement aux cyberattaques traditionnelles qui exploitent des bogues de programmation ou des erreurs de logique, les attaques AML exploitent les fondements mathématiques des modèles d'apprentissage automatique.³³ Un adversaire peut introduire des perturbations subtiles, imperceptibles pour l'homme, dans les entrées des capteurs d'un aéronef — comme les caméras optiques, le LiDAR ou le radar météorologique — et amener le modèle à commettre des erreurs catastrophiques.³³

La vulnérabilité de ces systèmes a été démontrée lors d'essais physiques.³⁸ Des chercheurs du Keen Security Lab de Tencent ont réussi à tromper le réseau de neurones de détection de voie d'une Tesla sous pilote automatique en plaçant trois petits autocollants sur la surface d'une route.³⁸ Les autocollants ont trompé la reconnaissance des formes du modèle, amenant le véhicule à identifier une mauvaise voie et à dévier vers la circulation en sens inverse sans alerter le conducteur.³⁸

Dans l'aviation, une attaque physique similaire pourrait consister à projeter des motifs laser ou infrarouges subtils sur une piste lors de l'atterrissage, ou à placer des conceptions adversariales sur la signalisation de l'aéroport, ce qui pourrait amener un système d'atterrissage basé sur la vision à dévier de la ligne médiane.¹⁹

Ce risque est aggravé par la conception non sécurisée des réseaux de communication aéronautiques hérités.³⁹ Le principal bus avionique commercial, **ARINC 429**, est un protocole de mots structurés unidirectionnel de 32 bits conçu sans aucun chiffrement natif ni authentification cryptographique.³⁹ Tout appareil qui obtient un accès physique ou électrique au bus peut injecter des mots de données usurpés directement dans l'ordinateur de vol.³⁹

La facilité de ce processus a été démontrée par des systèmes de test brevetés comme "Mudbucket", qui peuvent modifier les données sur les bus avioniques actifs en temps réel sans introduire de latence de protocole détectable.⁴¹

| ▼ (Perturbation Adversariale / Entrée d'Usurpation) (Aucun Chiffrement Natif / Authentification)³⁹ | ▼ (Télémétrie Malveillante Injectée)



[Actionneurs de Contrôle de Vol] --->

En outre, le protocole **Automatic Dependent Surveillance-Broadcast (ADS-B)**, qui diffuse en temps réel la position, le cap et la vitesse de l'aéronef aux stations au sol et aux aéronefs à proximité, est complètement non chiffré.⁴² Cette architecture non chiffrée rend l'ADS-B très vulnérable à l'usurpation (spoofing) et au brouillage.⁴²

Bien que les développeurs aient conçu des systèmes de détection d'anomalies basés sur l'apprentissage profond pour identifier les signaux ADS-B usurpés, ces défenses sont elles-mêmes vulnérables aux attaques adversariales.⁴²

En utilisant la méthode itérative rapide du signe du gradient avec accumulation de voisinage temporel (TNAI-FGSM), les adversaires peuvent générer des perturbations temporelles qui contournent ces détecteurs d'anomalies basés sur l'IA, permettant à la télémétrie de vol usurpée d'entrer dans le système de gestion du trafic aérien sans être détectée.⁴²

La chaîne d'approvisionnement en logiciels introduit également une vulnérabilité importante.³² Si un adversaire a accès aux ensembles de données utilisés pour former un réseau de neurones de contrôle de vol, il peut mener une attaque d'empoisonnement des données.³³ En introduisant des échantillons subtilement mal étiquetés ou altérés, ils peuvent insérer un cheval de Troie caché ou une porte dérobée dans le modèle.³³

Le modèle fonctionnera parfaitement dans des conditions de test standard.³³ Cependant, s'il rencontre un déclencheur spécifique sur le terrain — tel qu'une séquence unique de signaux radio ou un motif visuel spécifique — la porte dérobée est activée, amenant le contrôleur de vol à commander un changement d'attitude immédiat et spontané.³³

Pour se défendre contre ces menaces, les chercheurs développent des architectures de périphérie ("edge") avancées en temps réel.⁴⁴ L'architecture hybride Mamba-KAN-Liquid (MKL), par exemple, combine des modèles d'espace d'état à balayage sélectif avec des fonctions d'activation apprenables et des réseaux de neurones liquides.⁴⁴

Cette architecture permet aux systèmes périphériques à ressources limitées de s'adapter en permanence aux changements de distribution temporelle sans réentraînement explicite.⁴⁴

Exécutée sur des systèmes embarqués avec seulement 2,5 millions de paramètres et une latence d'inférence de 47,3 millisecondes, l'architecture MKL peut détecter les exploits cyber-physiques zero-day avec une précision de 89,4 %, fournissant une défense potentielle contre les attaques adversariales.⁴⁴

Signal Stratégique : Le Calendrier du Poste de Pilotage Dépeuplé

La transition vers un vol commercial à pilote unique, puis entièrement autonome, progresse selon un calendrier réglementaire et opérationnel structuré.¹³ Malgré la résistance continue des syndicats de pilotes, les incitations économiques au dépeuplement des cockpits continuent de dicter l'agenda réglementaire.¹⁰

Le cadre réglementaire est actuellement établi par le biais de la tâche de réglementation RMT.0739 de l'EASA, qui a été lancée au début de 2025 dans le cadre du Plan européen pour la sécurité aérienne (EPAS).¹³ Ce programme élabore les normes de sécurité pour les "cockpits intelligents" et l'eMCO, avec des "Avis" législatifs formels dont la soumission à la Commission européenne est prévue pour 2029.¹³ S'ils sont approuvés, ces règlements permettront les opérations de croisière à pilote unique à travers l'Europe d'ici 2030.¹³

2025 : Début de la Tâche de Réglementation RMT.0739 (EASA) ¹³ | 2027 : Consultations des Parties Prenantes sur les Ébauches d'eMCO ¹³ | 2029 : Soumission d'un "Avis" Législatif Formel à la Commission Européenne ¹³ | 2030 : Mise en Œuvre des Opérations de Croisière à Pilote Unique en Europe ¹³ | 2032+ : Lancement des Opérations de Fret Régional Sans Pilote | 2035+ : Les Vols de Passagers à Zéro Pilote Sont Soumis à l'Évaluation Réglementaire Initiale ²

Ce calendrier réglementaire s'aligne sur une transition importante dans l'industrie de la logistique aérienne.² Alors que les vols de passagers conserveront une configuration à deux pilotes pour maintenir la confiance du public, les réseaux régionaux de fret aérien et d'apport servent de terrain d'essai opérationnel pour l'autonomie complète.²

Dans des endroits éloignés, comme l'Alaska et le nord du Canada, des opérateurs comme Everts Air Cargo se sont associés à des développeurs technologiques pour valider des opérations autonomes dans des conditions météorologiques difficiles et sur des terrains accidentés.³

D'ici 2032, ces opérations de fret régional devraient passer à des vols entièrement sans équipage, retirant complètement les pilotes humains du poste de pilotage.² L'industrie de la logistique restructurera ses chaînes d'approvisionnement autour de ces réseaux d'apport automatisés, permettant un routage continu des avions, 24 heures sur 24, insensible aux limites de temps de service humain.¹¹

Cependant, cette transition introduira un compromis financier complexe pour les exploitants de flottes.⁸ Bien que l'élimination des équipages de vol humains puisse réduire les coûts directs d'équipage jusqu'à 80 %, les opérateurs seront confrontés à une escalade des dépenses en capital pour des stations de contrôle au sol sécurisées, une télémétrie satellitaire redondante et une validation régulière de la chaîne d'approvisionnement logicielle.⁷

De plus, le secteur de l'assurance facturera probablement des primes élevées pour les opérations autonomes jusqu'à ce que les cadres de responsabilité et de cybersécurité soient légalement résolus.⁸

Pour les dirigeants d'entreprise et les cadres technologiques, la leçon stratégique est claire : l'automatisation des commandes de vol n'est pas une progression simple et linéaire vers des opérations plus sûres.²⁷ Elle représente une restructuration fondamentale de l'ingénierie aérospatiale, de la responsabilité et de la sécurité cyber-physique.⁸ Les organisations qui se préparent à ces risques non déterministes et systémiques seront positionnées pour diriger la prochaine ère de la logistique mondiale.¹¹

Works cited

1. AI Is Learning to Pilot Airplanes, and Aviation Is Beginning to Adopt It. - Ground News, accessed on May 25, 2026, https://ground.news/article/ai-is-learning-to-pilot-airplanes-and-aviation-is-beginning-to-adopt-it_52dacd
2. Autonomous aviation system aims for pilot-free cargo aircraft - New Atlas, accessed on May 25, 2026, <https://newatlas.com/aircraft/merlin-pilot-autonomous-large-cargo-aircraft/>
3. Merlin completes FAA-contracted Alaska flight trials for first air cargo network flown by non-human pilot - Skies Mag, accessed on May 25, 2026, <https://skiesmag.com/news/merlin-completes-faa-contracted-alaska-flight-trials-first-air-cargo-network-flown-non-human-pilot/>
4. AI is learning to fly airplanes — and aviation is starting to embrace it ..., accessed on May 25, 2026, <https://localnews8.com/news/national-world/cnn-national/2026/05/24/ai-is-learning-to-fly-airplanes-and-aviation-is-starting-to-embrace-it/>
5. FAA Awards Contract for Automated Cargo Network Flight Trials in Alaska, accessed on May 25, 2026, <https://www.flyingmag.com/faq-awards-contract-for-fully-autonomous-cargo-flight-trials-in-alaska/>
6. Can Machine Learning Systems be Certified on Aircraft? - Beca, accessed on May 25, 2026, <https://www.becca.com/ignite-your-thinking/ignite-your-thinking/march-2025/can-machine-learning-systems-be-certified-on-aircraft>
7. Certified Machine Learning-Based Avionics - Mobility Engineering ..., accessed on May 25, 2026, <https://www.mobilityengineeringtech.com/component/content/article/50057-certified-machine-learning-based-avionics>
8. AI in aerospace: who's liable when the algorithm crashes the plane ..., accessed on May 25, 2026, <https://blog.richardvanhooijdonk.com/en/ai-in-aerospace-whos-liable-when-the-algorithm-crashes-the-plane/>
9. The Future of Single-Pilot Operations in Commercial Aviation | AirlinePilotCentral.com, accessed on May 25, 2026, <https://www.airlinepilotcentral.com/articles/news/the-future-of-single-pilot-operations-in-commercial-aviation.html>
10. 12 THE SINGLE PILOT COMMERCIAL AIRCRAFT - Aerospace Technology Institute, accessed on May 25, 2026, https://www.ati.org.uk/wp-content/uploads/2021/08/ati-insight_12-single-pilot-commercial-aircraft.pdf
11. Skydio Autonomy™. A New Age Of Drone Intelligence., accessed on May 25, 2026, <https://www.skydio.com/blog/skydio-autonomy-tm-a-new-age-of-drone-intelligence>
12. What's a realistic timeline to be a medivac or cargo pilot? : r/flying - Reddit, accessed on May 25, 2026, https://www.reddit.com/r/flying/comments/1o8ix56/whats_a_realistic_timeline_to

- [be_a_medivac_or/](#)
13. Timeline for the introduction of Single Pilot Operations - European Cockpit Association, accessed on May 25, 2026,
<https://www.eurocockpit.eu/news/timeline-introduction-single-pilot-operations>
 14. Flight Time/Duty Time for Air Cargo - Airline Pilots Association - ALPA, accessed on May 25, 2026,
<http://www2.alpa.org/alpa/DesktopModules/ViewAnnDocument.aspx?DocumentID=5524>
 15. DO-178C - Wikipedia, accessed on May 25, 2026,
<https://en.wikipedia.org/wiki/DO-178C>
 16. GUEST BLOG: The convergence of safety and security -- Five steps to building modern avionics software - Military Embedded Systems, accessed on May 25, 2026,
<https://militaryembedded.com/avionics/safety-certification/guest-blog-the-convergence-of-safety-and-security-five-steps-to-building-modern-avionics-software>
 17. Avionic Real-Time Operating Systems in Modern Aircraft: Safety, Standards, and Emerging Trends, accessed on May 25, 2026,
<https://real-time-consulting.com/wp-content/uploads/2025/04/Avionic-RTOS.pdf>
 18. Certification of machine learning algorithms for safe-life assessment of landing gear - Frontiers, accessed on May 25, 2026,
<https://www.frontiersin.org/journals/astronomy-and-space-sciences/articles/10.3389/fspas.2022.896877/pdf>
 19. Toward Certification of Machine-Learning Systems for Low Criticality Airborne Applications - NASA Technical Reports Server, accessed on May 25, 2026,
<https://ntrs.nasa.gov/api/citations/20210019093/downloads/main.pdf>
 20. X-62A VISTA | Lockheed Martin, accessed on May 25, 2026,
<https://www.lockheedmartin.com/en-us/products/x-62a-vista.html>
 21. X-62 VISTA begins upgrade program, expanding boundaries in flight testing of autonomy and artificial intelligence > Air Force Test Center > News, accessed on May 25, 2026,
<https://www.aftc.af.mil/News/Article/4364122/x-62-vista-begins-upgrade-program-expanding-boundaries-in-flight-testing-of-aut/>
 22. ACE | DARPA, accessed on May 25, 2026,
<https://www.darpa.mil/about/innovation-timeline/ace>
 23. General Dynamics X-62 VISTA - Wikipedia, accessed on May 25, 2026,
https://en.wikipedia.org/wiki/General_Dynamics_X-62_VISTA
 24. ACE Program's AI Agents Transition from Simulation to Live Flight - DARPA, accessed on May 25, 2026,
<https://www.darpa.mil/news/2023/ace-program-transition>
 25. Collaborative Air Combat Autonomy Program Makes Strides - DARPA, accessed on May 25, 2026,
<https://www.darpa.mil/news/2021/air-combat-autonomy-program>
 26. Cubic Collaborates in DARPA's ACE Program, accessed on May 25, 2026,
<https://www.cubic.com/news-events/news/cubic-collaborates-darpas-ace-progr>

[am](#)

27. A Cross-Regional Review of AI Safety Regulations in the Commercial Aviation Industry, accessed on May 25, 2026, <https://www.mdpi.com/2076-3387/16/1/53>
28. AI Governance Is Not Policy. It Is Infrastructure. - Lowenstein Sandler LLP, accessed on May 25, 2026, https://www.lowenstein.com/media/cf4pb1m2/20260318_dp_ai-governance-is-not-policy-it-is-infrastructure.pdf
29. S.B. 149 Artificial Intelligence Amendments - Utah Legislature, accessed on May 25, 2026, <https://le.utah.gov/~2024/bills/static/SB0149.html>
30. An American's Guide to the EU AI Act - Berkeley Technology Law Journal, accessed on May 25, 2026, https://btlj.org/wp-content/uploads/2026/04/40.4_Kaminski.pdf
31. Systematic review of machine and deep learning models for unmanned aerial vehicles cyber threat defense - UBIR, accessed on May 25, 2026, https://ub-ir.bolton.ac.uk/view/pdfCoverPage?instCode=44UOBO_INST&filePid=1311880290008841&download=true
32. How Has Artificial Intelligence Impacted Drone Technology? - Internet Lawyer Blog, accessed on May 25, 2026, <https://www.internetlawyer-blog.com/how-has-artificial-intelligence-impacted-drone-technology/>
33. Trustworthy AI & UAS Technology, accessed on May 25, 2026, https://www.energy.gov/sites/default/files/2022-06/R%26T%20AI%20AIRMP_1.pdf
34. Adversarial Machine Learning for Cyber Security - UPCommons, accessed on May 25, 2026, <https://upcommons.upc.edu/bitstreams/5a8cde84-4c2c-4ee4-9a2b-ac74cbca634c/download>
35. Artificial Intelligence in Cybersecurity: Exploring AI-Powered Threat Detection and Mitigation Strategies - IRE Journals, accessed on May 25, 2026, <https://www.irejournals.com/formatedpaper/1708695.pdf>
36. UniAda: Universal Adaptive Multi-objective Adversarial Attack for End-to-End Autonomous Driving Systems - arXiv, accessed on May 25, 2026, <https://arxiv.org/html/2604.23362v1>
37. Newly discovered principle reveals how adversarial training can perform robust deep learning - Microsoft Research, accessed on May 25, 2026, <https://www.microsoft.com/en-us/research/blog/newly-discovered-principle-reveals-how-adversarial-training-can-perform-robust-deep-learning/>
38. Report 1518 - AI Incident Database, accessed on May 25, 2026, <https://incidentdatabase.ai/reports/1518/>
39. ARINC 429 Cyber-vulnerabilities and Voltage Data in a Hardware-in-the-Loop Simulator, accessed on May 25, 2026, <https://arxiv.org/html/2408.16714v1>
40. Avionics Protocol Converters: Ensuring Seamless Communication - KIMDU Technologies, accessed on May 25, 2026, <https://kimdu.com/avionics-protocol-converters-ensuring-seamless-communication/>
41. cybersecurity - CH-53K Helicopter Parts - Aircraft Maintenance Tools & Ground

- Support Equipment - NSN Parts Catalog, accessed on May 25, 2026,
<https://www.goctsi.com/expertise/cybersecurity>
42. Adversarial Attacks against Deep-Learning-Based Automatic Dependent Surveillance-Broadcast Unsupervised Anomaly Detection Models in the Context of Air Traffic Management - MDPI, accessed on May 25, 2026,
<https://www.mdpi.com/1424-8220/24/11/3584>
 43. Security of ADS-B and Remote ID Systems: Cyberattacks, Detection Techniques, and Countermeasures - PMC, accessed on May 25, 2026,
<https://pmc.ncbi.nlm.nih.gov/articles/PMC12846276/>
 44. UAV Cybersecurity with Mamba-KAN-Liquid Hybrid Model: Deep Learning-Based Real-Time Anomaly Detection - MDPI, accessed on May 25, 2026,
<https://www.mdpi.com/2504-446X/9/11/806>
 45. Autonomous Cargo Flights Complete Test Series - Alaska Business Magazine, accessed on May 25, 2026,
<https://www.akbizmag.com/industry/transportation/autonomous-cargo-flights-complete-test-series/>