The Evaporation of Liability: Forensic Analysis of AI Integration in Heavy Kinetic Aviation Infrastructure

In May 2026, a highly sanitized public relations demonstration took place in the skies over California and Alaska.[1] As reported by CNN, a Cessna Grand Caravan accelerated down a runway, climbed into the air, and navigated complex terrain without its safety pilot touching the controls.[1] Tim Burns, the Chief Technology Officer of autonomous flight startup Merlin Labs, joked over the intercom while test pilot Matt Diamond kept his hands resting on his knees.[1] To the casual observer, this event represented a seamless leap into a safer, automated future of air travel.[1]

To forensic aerospace analysts and autonomous systems experts, however, the flight was a calculated corporate demonstration masking a deep structural crisis. The aviation industry is actively preparing to transition heavy kinetic infrastructure—multi-ton platforms carrying passengers and cargo at high velocities and altitudes—to fundamentally unpredictable, non-deterministic software layers.[6] This transition is not born out of an absolute safety imperative, but rather out of intense macroeconomic pressures, pilot labor shortages, and an industry-wide effort to bypass traditional liability frameworks.[8]

The Economic Underbelly of Cockpit Depopulation

The narrative surrounding cockpit automation has long been framed as a pursuit of absolute safety, with corporate public relations presenting artificial intelligence as the ultimate solution to "human error".[1] Yet, a forensic examination of the industry's balance sheets reveals that the shift toward autonomous flight control is driven by labor economics.[10]

Airlines operate on thin capital margins, highly sensitive to fluctuating fuel costs and escalating labor expenditures.[8] European low-cost carriers, for instance, must maintain a costly ratio of approximately 10 to 11 type-rated pilots per airframe to satisfy strict flight-and-duty-time limitations and scheduling redundancies.[10] Furthermore, the regional cargo and feeder logistics sectors face chronic pilot shortages, as major passenger carriers continuously drain the labor pool of experienced captains.[5]

To counter these margin-eroding forces, major aircraft manufacturers, led by Airbus and Dassault, have aggressively lobbied aviation regulators to approve Extended Minimum Crew Operations (eMCO).[13] The initial goal of eMCO is to reduce flight deck staffing during the cruise phase of flight from two pilots to a single operator, with the eventual aim of complete cockpit depopulation.[9]

This corporate push has encountered intense opposition from pilot unions, such as the European Cockpit Association (ECA) and the Air Line Pilots Association (ALPA).[9] Industry union representatives caution that removing the secondary pilot eliminates a critical human safety layer.[9] Under the current two-pilot paradigm, cognitive cross-checking, mutual monitoring, and real-time fatigue mitigation prevent minor anomalies from cascading into catastrophic hull losses.[9]

In June 2024, the Dutch Parliament highlighted these safety concerns by passing a motion declaring that new cockpit technologies must only be certified if they demonstrably enhance flight safety, rather than merely reducing airline operational overhead.[13] Despite this warning, the industry's economic momentum remains focused on automation.[10]

Operational Metric	Conventional Two-Pilot Flight Deck	Extended Minimum Crew Operations (eMCO)	Uncrewed Autonomous Cargo Fleet
Crew Overhead per Airframe	Baseline (100% Cost Index) [10]	30% to 40% Reduction [10]	80% to 90% Reduction [11]
Regulatory Framework	FAA Part 121 / 135 Standard [12]	EASA RMT.0739 (Smart Cockpits) [13]	FAA Special STC (Normal Category) [7]
Fatigue & Duty Limits	Highly restrictive duty-hour caps [12]	Complex sleep inertia & break protocols [9]	Eliminated; continuous routing enabled [14]

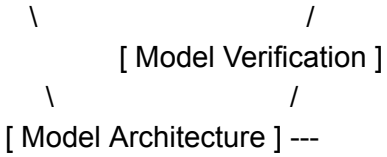
Primary System Safety Layer	Dual-human cross-checking & validation [9]	Single-pilot monitored by basic AI [9]	Real-time statistical inference engines [7]

The Black Box Certification Conundrum

For over a decade, commercial airborne software has been governed by RTCA DO-178C (Software Considerations in Airborne Systems and Equipment Certification).[15] The foundation of DO-178C is absolute determinism.[6] For software classified as Design Assurance Level A (DAL-A)—where a failure would result in a catastrophic loss of the aircraft—the developer must provide objective evidence of 100% Modified Condition/Decision Coverage (MC/DC).[15] Every single logical pathway must be traceable from high-level system requirements to low-level source code, and ultimately to the executable object code running on the flight control computer.[15]

Deep learning and neural networks break this entire certification paradigm.[6] A convolutional neural network (CNN) used for flight control or situational intelligence does not operate on human-defined rules.[6] Instead, it uses millions of statistical weights adjusted during training.[6] Requirements cannot be directly traced to specific lines of code.[7] The decision-making process is fundamentally non-deterministic and functions as an un-auditable "black box".[7]

To address this challenge, organizations like EASA and the FAA are attempting to establish new regulatory frameworks based on the Concepts of Design Assurance for Neural Networks (CoDANN).[7] Under CoDANN and its subsequent iterations, developers are abandoning classical software verification in favor of the **W-shaped development process**.[7]



The W-shaped process establishes assurance through a three-stage verification pipeline [7]:

1. **Dataset Verification:** The training, validation, and testing datasets must be rigorously curated, balanced, and proven to cover the entire operational flight envelope.[6]
2. **Model Verification:** Online, in-flight learning is strictly prohibited.[6] The neural network is trained exclusively in a laboratory environment.[7] Once the model achieves acceptable

error rates, its weights are frozen.[6] The frozen weights are treated as Parameter Data Items (PDIs) under DO-178C, forcing the system to behave deterministically at runtime.[6]

3. **Inference Verification:** Statistical Learning Theory is used to mathematically bound the generalization error of the model within its defined operational domain.[7]

To provide safety bounds, engineers employ generalization performance limits, ensuring the empirical risk $\hat{R}(f)$ of the model f over a dataset of size n bounds the true risk $R(f)$ with a high probability:

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

where d represents the Vapnik-Chervonenkis (VC) dimension of the neural network architecture.

Despite these mathematical frameworks, the statistical uncertainty of neural networks remains too high for primary flight controls.[7] Consequently, developers are forced to implement a dual-architecture paradigm.[6]

The non-deterministic AI model is isolated within a partitioned environment, while a traditional, deterministic DO-178C-compliant safety monitor acts as an external governor.[6] If the AI controller commands an input that violates pre-defined flight envelope limits—such as an excessive pitch rate or roll angle—the deterministic legacy system overrides the command and takes control.[6]

This architectural partitioning requires significant physical computing power.[7] Running high-resolution Convolutional Neural Networks (CNNs) in real time requires approximately one Tera Operation per Second (TOPS).[7] This requirement has led to the development of specialized, certifiable hardware, such as the Daedalean Tensor Accelerator (DTA) implemented on Intel Agilex FPGAs.[7]

Using ARINC 653 partitioning standards, these high-performance accelerators are separated from the primary, safety-critical Real-Time Operating System (RTOS) running on the Integrated Modular Avionics (IMA) cabinets.[7] This design ensures that a software lockup in the AI layer cannot propagate to the primary flight control surfaces.[17]

The Defense Pipeline as an Operational Sandbox

The certification and validation of these autonomous systems are heavily accelerated by military development programs.[20] Foremost among these is DARPA's Air Combat Evolution (ACE) program, which uses air-to-air dogfighting as a high-stress test case for autonomous flight algorithms.[20]

The primary platform for this research is the General Dynamics X-62A Variable In-flight Simulation Test Aircraft (VISTA).[20] Developed by Lockheed Martin Skunk Works and Calspan, the X-62A is a modified Block 30 F-16D equipped with a System for Autonomous Control of

Simulation (SACS) and Multi-Axis Thrust Vectoring (MATV).[20] The SACS architecture allows the X-62A to emulate the flight-handling qualities of entirely different aircraft types, while running experimental AI agents in live flight.[20]

In April 2024, the U.S. Air Force and DARPA completed the first-ever in-air autonomous dogfight between the AI-controlled X-62A and a human-piloted F-16.[22] During these engagements, the AI-controlled aircraft successfully managed aggressive, post-stall maneuvers at high angles of attack.[23]

To build trust in these automated systems, the Air Force Test Pilot School uses dual-seat jet trainers equipped with physiological sensors.[24] These sensors measure pilot biometrics, such as heart rate, skin conductivity, and eye-tracking patterns.[24] This data allows researchers to mathematically model "trust calibration"—the precise moment a human pilot decides to hand over control to an AI agent during a high-workload scenario.[24]

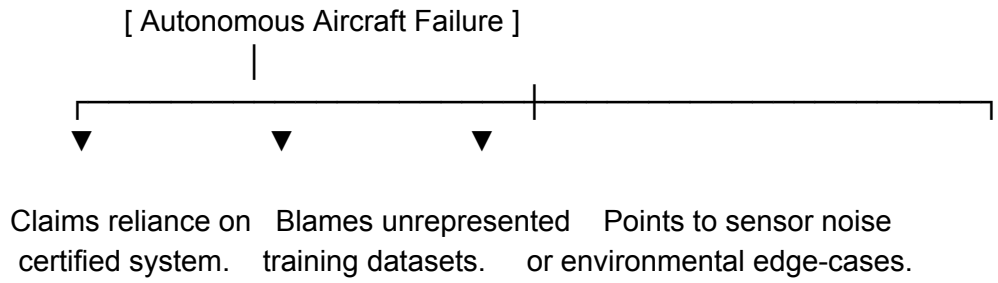
This military research is directly accelerating commercial autonomous cargo programs.[21] Companies like Merlin Labs and Xwing have directly leveraged the flight-test methodologies, safety architectures, and simulator-to-real-world transition data validated by the X-62A VISTA program.[5]

The Evaporation of Liability

The integration of non-deterministic AI pilots into commercial airspace highlights a profound legal irony: the complete erosion of traditional liability frameworks.[8] Traditional aviation law is built on a clear chain of accountability.[8] Responsibility flows directly from the certified human pilot in command to the operating airline, and ultimately to the original equipment manufacturer (OEM) if a mechanical or structural system fails.[8]

In an autonomous or single-pilot eMCO environment, this chain of accountability dissolves.[8] Because deep learning networks operate statistically, they are prone to unpredictable "hallucinations" or failures when encountering novel, out-of-distribution edge cases.[8]

If an autonomous cargo aircraft misinterprets a severe weather phenomenon or an unusual sensor input and crashes, assigning fault becomes highly complex.[8]



Responsibility diffuses across a complex network of contributors:

- **The Airline (Operator):** Argues that the autonomous system was certified by EASA/FAA and operated in accordance with manufacturer parameters, deflecting operational negligence.[8]
- **The Software Developer / Model Provider:** Claims the system performed exactly as trained, blaming gaps or unrepresented variables in the training datasets provided by third parties.[8]
- **The Original Equipment Manufacturer (OEM):** Points to external factors, such as sensor noise, environmental anomalies, or hardware-accelerator limitations.[8]

This legal ambiguity creates a significant gap between corporate governance policies and actual operational risk.[28] While airlines can establish high-level "AI Ethics Charters," these frameworks do not address the core issue.[28] Traditional flight data recorders (FDRs) log physical inputs, such as control column deflections and engine parameters.[28] They are not designed to record the high-dimensional internal state activations of a deep neural network during an incident.[28] This makes it nearly impossible for forensic investigators to reconstruct the exact reasoning behind an automated flight control failure.[8]

This challenge has prompted regional legislative responses.[29] In the United States, Utah's Artificial Intelligence Policy Act (SB 149) represents an early state-level attempt to enforce strict disclosure and liability rules when generative or autonomous AI is utilized in regulated professional occupations.[29]

Similarly, the European Union's AI Act structures AI governance as a strict product safety regime, categorizing aviation systems as "high-risk".[30] This framework forces developers to undergo conformity assessments and obtain CE markings.[30] This creates a complex regulatory landscape where software developers are treated as hardware manufacturers, facing strict liability for the statistical outputs of their models.[8]

Cyber-Physical Threat Vectors and Adversarial Exploitation

Treating the modern aircraft as a flying edge-compute data center introduces unprecedented cybersecurity vulnerabilities.[31] In fully autonomous architectures, the neural network sits directly on the primary data buses, continuously translating raw sensor inputs into physical control commands.[19] This tight integration exposes the system to **adversarial machine learning (AML)** attacks.[32]

Unlike traditional cyberattacks that exploit programming bugs or logic errors, AML attacks exploit the mathematical foundations of machine learning models.[33] An adversary can introduce subtle, human-imperceptible perturbations to the inputs of an aircraft's sensors—such as optical cameras, LiDAR, or weather radar—and cause the model to make catastrophic errors.[33]

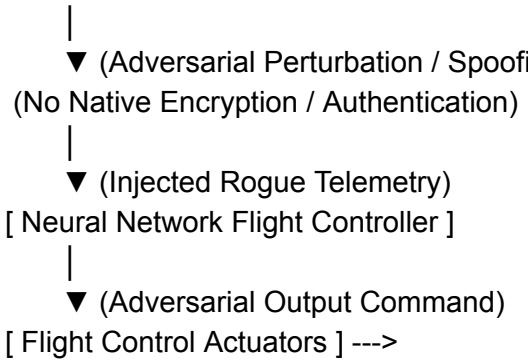
The vulnerability of these systems has been demonstrated in physical tests.[38] Researchers at Tencent's Keen Security Lab successfully deceived the lane-detection neural network of a Tesla

on autopilot by placing three small stickers on a road surface.[38] The stickers fooled the model's pattern recognition, causing the vehicle to identify an incorrect lane and swerve into oncoming traffic without alerting the driver.[38]

In aviation, a similar physical attack could involve projecting subtle laser or infrared patterns onto a runway during landing, or placing adversarial designs on airport signage, which could cause a vision-based landing system to deviate from the centerline.[19]

This risk is compounded by the insecure design of legacy aviation communication networks.[39] The primary commercial avionics bus, **ARINC 429**, is a unidirectional, 32-bit structured word protocol designed without any native encryption or cryptographic authentication.[39] Any device that gains physical or electrical access to the bus can inject spoofed data words directly into the flight computer.[39]

The ease of this process has been demonstrated by patented test systems like "Mudbucket," which can edit data on active avionics buses in real time without introducing detectable protocol latency.[41]



Furthermore, the **Automatic Dependent Surveillance-Broadcast (ADS-B)** protocol, which broadcasts real-time aircraft position, heading, and velocity to ground stations and nearby aircraft, is completely unencrypted.[42] This unencrypted architecture makes ADS-B highly vulnerable to spoofing and jamming.[42]

While developers have built deep-learning-based anomaly detection systems to identify spoofed ADS-B signals, these defenses are themselves vulnerable to adversarial attacks.[42] Using the Time Neighborhood Accumulation Iteration Fast Gradient Sign Method (TNAI-FGSM), adversaries can generate temporal perturbations that bypass these AI-based anomaly detectors, allowing spoofed flight telemetry to enter the air traffic management system undetected.[42]

The software supply chain also introduces a significant vulnerability.[32] If an adversary gains access to the datasets used to train a flight control neural network, they can perform a data-poisoning attack.[33] By introducing subtly mislabeled or altered samples, they can insert a hidden "Trojan" or backdoor into the model.[33]

The model will perform perfectly under standard testing conditions.[33] However, if it encounters a specific trigger in the field—such as a unique sequence of radio signals or a specific visual pattern—the backdoor is activated, causing the flight controller to command an immediate, unprompted attitude shift.[33]

To defend against these threats, researchers are developing advanced, real-time edge architectures.[44] The Mamba-KAN-Liquid (MKL) hybrid architecture, for example, combines selective-scan state-space models with learnable activation functions and liquid neural networks.[44]

This architecture allows resource-constrained edge systems to continuously adapt to temporal distribution shifts without explicit retraining.[44] Running on onboard systems with only 2.5 million parameters and a 47.3 millisecond inference latency, the MKL architecture can detect zero-day cyber-physical exploits with 89.4% accuracy, providing a potential defense against adversarial attacks.[44]

Strategic Signal: The Depopulated Flight Deck Timeline

The transition to single-pilot and eventually fully autonomous commercial flight is progressing along a structured regulatory and operational timeline.[13] Despite ongoing resistance from pilot unions, the economic incentives of cockpit depopulation continue to drive the regulatory agenda.[10]

The regulatory framework is currently being established through EASA's Rulemaking Task RMT.0739, which was launched in early 2025 under the European Plan for Aviation Safety (EPAS).[13] This program is developing the safety standards for "smart cockpits" and eMCO, with formal legislative "Opinions" scheduled for submission to the European Commission by 2029.[13] If approved, these regulations will permit single-pilot cruise operations across Europe by 2030.[13]

2025: Rulemaking Task RMT.0739 Commences (EASA)
  |
2027: Stakeholder Consultations on eMCO Drafts
  |
2029: Formal Legislative "Opinion" Submitted to European Commission

|
2030: Single-Pilot Cruise Operations Implemented Across Europe
|
2032+: Pilot-Free Regional Cargo Operations Launch
|
2035+: Zero-Pilot Passenger Flights Face Initial Regulatory Evaluation [2]

This regulatory timeline aligns with a significant transition in the air logistics industry.[2] While passenger flights will retain a two-pilot configuration to maintain public trust, the regional air cargo and feeder networks are serving as the operational proving ground for full autonomy.[2] In remote locations, such as Alaska and northern Canada, operators like Everts Air Cargo have partnered with technology developers to validate autonomous operations in harsh weather and over difficult terrain.[3]

By 2032, these regional cargo operations are expected to transition to fully uncrewed flights, removing human pilots from the cockpit entirely.[2] The logistics industry will restructure its supply chains around these automated feeder networks, enabling continuous, round-the-clock aircraft routing unaffected by human duty-time limits.[11]

However, this transition will introduce a complex financial trade-off for fleet operators.[8] While eliminating human flight crews can reduce direct crew costs by up to 80%, operators will face escalating capital expenditures for secure ground control stations, redundant satellite telemetry, and regular software-supply-chain validation.[7]

Additionally, the insurance industry will likely charge high premiums for autonomous operations until liability and cybersecurity frameworks are legally resolved.[8]

For corporate leaders and technology executives, the strategic lesson is clear: the automation of flight controls is not a simple, linear progression toward safer operations.[27] It represents a fundamental restructuring of aerospace engineering, liability, and cyber-physical security.[8] Organizations that prepare for these non-deterministic and systemic risks will be positioned to lead the next era of global logistics.[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/faa-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.beca.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-program
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=13118802900088 41&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/