A Survey of Security Challenges and Solutions for Advanced Air Mobility and eVTOL Aircraft

Mahyar Ghazanfari, Iman Sharifi, Peng Wei
George Washington University, Washington, D.C. 20052, USA

Noah Dahle, Abel Diaz Gonzalez, Austin Coursey, Bryce Bjorkman, Cailani Lemieux-Mack, Robert Canady, Abenezer Taye, Bryan C. Ward, Xenofon Koutsoukos, Gautam Biswas
Vanderbilt University, Nashville, TN, 37212, USA

Maheed H. Ahmed, Hyeong Tae Kim, Mahsa Ghasemi, Vijay Gupta
Purdue University, West Lafayette, IN, 47907, USA

Filippos Fotiadis, Ufuk Topcu
The University of Texas at Austin, Austin, TX, 78712, USA

Junchi Lu, Alfred Chen
University of California, Irvine, Irvine, CA, 92697, USA

Abdul kareem Ras, Nischal Aryal, Amer Ibrahim, Amir Shirkhodaie
Tennessee State University, 3500 John Merritt Blvd, Nashville, TN, 37221, USA

Heber Herencia-Zapana, Saqib Hasan, Isaac Amundson
Advanced Research and Technology, Collins Aerospace, Cedar Rapids, IA, 52498, USA

This survey reviews the existing and envisioned security vulnerabilities and defense mechanisms relevant to Advanced Air Mobility (AAM) systems, with a focus on electric vertical takeoff and landing (eVTOL) aircraft. Drawing from vulnerabilities in the avionics in commercial aviation and the automated unmanned aerial systems (UAS), the paper presents a taxonomy of attacks, analyzes mitigation strategies, and proposes a secure system architecture tailored to the future AAM ecosystem. The paper also highlights key threat vectors, including Global Positioning System (GPS) jamming/spoofing, ATC radio frequency misuse, attacks on TCAS and ADS-B, possible backdoor via Electronic Flight Bag (EFB), new vulnerabilities introduced by aircraft automation and connectivity, and risks from flight management system (FMS) software, database and cloud services. Finally, this paper describes emerging defense techniques against these attacks, and open technical problems to address toward better defense mechanisms.

I. Introduction

Advanced Air Mobility (AAM) represents a transformative approach to aviation, aiming to integrate a new class of electric, highly automated aircraft—including eVTOL vehicles—into the national airspace to provide short- to medium-range transportation solutions for both passengers and cargo. AAM addresses the growing need for efficient, scalable mobility across urban and regional settings by leveraging advancements in electric propulsion, autonomy, and coordinatedair traffic management [1, 2].

Unlike conventional rotorcraft or general aviation systems, AAM platforms feature novel connected aircraft and rely on highly automated operations across all phases of flight. These aircraft are expected to operate in complex, high-density, and dynamically evolving airspace environments that span a broad range of altitudes. Within the AAM ecosystem, Urban Air Mobility (UAM) is a critical subset that focuses on operations within densely populated metropolitan areas, whereas Regional Air Mobility (RAM) extends the operational range by connecting smaller cities and rural communities over longer distances [3].

While much attention has been directed toward physical infrastructure and regulatory policy, securing the digital infrastructure, spanning navigation, communication, flight control, and system data integrity, is equally critical. As

the National Aeronautics and Space Administration (NASA), the Federal Aviation Administration (FAA), and other stakeholders advance the AAM framework, the integration of eVTOL operations into the National Airspace System (NAS) introduces a host of technical and security challenges. Chief among them is cybersecurity, which has emerged as a vital concern. The increasing reliance on GPS navigation, automated flight control, aircraft connectivity, data links, and cloud-connected services renders eVTOL platforms especially vulnerable to cyber threats such as spoofing, jamming, man-in-the-middle attacks, and denial-of-service (DoS) disruptions.

Building and maintaining public trust in AAM operations, particularly those involving eVTOL aircraft, requires more than compliance with airworthiness standards and operational efficiency. It demands resilient architectures, secure communication channels, and end-to-end data protection. As noted by the Secure Airspace Technology Group (SATG), cybersecurity must be a foundational component of AAM system design rather than a reactive consideration [4]. This paper explores the cybersecurity landscape of eVTOL and AAM platforms by surveying known vulnerabilities of commercial avionics, discussing envisioned risks introduced by aircraft automation and connectivity, analyzing potential attack surfaces, and reviewing recent advancements in defense strategies aimed at ensuring system integrity, availability, and confidentiality.

While prior surveys have examined cybersecurity risks in aviation and UAM more broadly, their focus differs from the scope of this work. Existing reviews either analyze high-level threat taxonomies across conventional aircraft systems [5] or provide generalized vulnerability overviews for early UAM concepts [6]. In contrast, our work concentrates specifically on eVTOL platforms and their operational ecosystem, offering a deeper, system-oriented analysis of vulnerabilities and defense mechanisms tailored to the sensing, autonomy, communication, and cloud-integration requirements unique to AAM environments.

The remainder of this paper is organized as follows. Section II provides background on the fundamental concepts of AAM and eVTOL systems. Section III outlines current vulnerabilities and potential cyberattacks targeting these platforms, and presents defense strategies and mitigation techniques corresponding to these threats. Finally, section IV concludes the paper.

II. Background

AAM is an evolving aviation paradigm that seeks to integrate next-generation, highly automated, and often electric aircraft into existing airspace systems to provide efficient, safe, and flexible transportation for both passengers and cargo. AAM encompasses a wide spectrum of operations, from short-range urban flights to regional and intercity missions, and aims to alleviate surface transportation congestion, increase connectivity, and improve accessibility in both densely populated and underserved areas. The AAM framework is being actively advanced by the FAA, NASA, and a broad range of industry and academic stakeholders to enable scalable and equitable air mobility solutions across diverse operational environments.

Within this broader framework, UAM is a key operational subset of AAM focused specifically on transportation within and around metropolitan regions. UAM introduces aerial mobility solutions that are optimized for high-density, short-range travel, particularly in congested urban areas. A central enabler of UAM operations is the eVTOL aircraft, which features electric propulsion, vertical lift capability, and reduced noise signatures. These vehicles are designed for point-to-point operations between dedicated infrastructure nodes, such as vertiports and vertistops, often with autonomous or remote piloting capabilities. Their compact footprint and operational flexibility make them well-suited for high-frequency flights in urban airspaces.

A notional UAM architecture, depicted in [7], illustrates the relationships among the principal actors involved in UAM operations. This architecture operates within the larger AAM ecosystem and is centered around a federated service network that manages information flow between the FAA, UAM operators, infrastructure providers, and public stakeholders. It emphasizes interoperability through standardized data formats and communication protocols, enabling safe, coordinated, and scalable integration of UAM into the NAS.

Communication systems are foundational to the safe and scalable operation of eVTOL aircraft. These systems must accommodate dense, three-dimensional urban traffic, ensure low-latency data exchange, and operate reliably under variable environmental and network conditions. eVTOL communication architectures are centered around air-to-ground, air-to-air, and potentially satellite communication to support command and control (C2), situational awareness, and coordination among vehicles and infrastructure. Communication requirements for eVTOLs include ultra-reliable coverage, high data rate (up to 100 Mbps for remote piloting), and low end-to-end latency (as low as 10 ms for safety-critical maneuvers) [8]. Fifth-generation (5G) cellular networks and their upcoming 6G counterparts offer promising infrastructure for wide-area eVTOL connectivity. These technologies support low-latency, high-bandwidth

communication and can be supplemented with rooftop-mounted base stations or dedicated urban nodes to improve coverage in dense environments [8].

Navigation systems for eVTOLs combine conventional aviation tools with advanced onboard autonomy to support precise flight in complex urban airspaces. Position estimation is primarily achieved through Global Navigation Satellite System (GNSS) and Inertial Navigation System (INS) integration, in which GPS signals are fused with inertial measurement units (IMUs) using Kalman filtering. Loosely coupled architectures offer computational simplicity, while tightly coupled methods provide enhanced reliability in GNSS-challenged urban environments [9]. In scenarios where GNSS signals are degraded or unavailable, perception-based localization methods such as Light Detection and Ranging (LIDAR) and visual-inertial simultaneous localization and mapping SLAM have been shown to be promising [10]. Radio Detection And Ranging (Radar) systems, particularly frequency-modulated continuous-wave (FMCW) radar, enhance obstacle detection and situation awareness under adverse weather conditions. These onboard systems complement Navigation part by extending perception range and enabling all-weather operability. To further improve robustness, multi-sensor fusion architectures integrate data from GNSS, IMU, LiDAR, RADAR, and possibly visual sensors to take advantage of all sensors at the same time.

Surveillance systems such as RADAR and Automatic Dependent Surveillance–Broadcast (ADS-B) remain essential for safety and conformance monitoring. Radar plays a critical role in the surveillance infrastructure required for safe and scalable eVTOL operations, particularly in urban environments where visibility may be limited and traffic density is high. Ground-based radar systems have been demonstrated to effectively detect and track non-cooperative aircraft and obstacles, enabling reliable detect-and-avoid capabilities. For instance, NASA's distributed sensing research has shown that radar, when deployed as part of a networked ground infrastructure, significantly enhances situational awareness by providing persistent coverage, even under poor lighting or weather conditions [11]. Radar's numerous capabilities and its real-time response make it an indispensable component for low-altitude airspace surveillance in AAM scenarios.

Flight Management Systems (FMS) are foundational components of modern aviation, responsible for automating and optimizing a wide range of flight operations. These systems integrate data from multiple onboard sources, including GPS, INS, air data sensors, and navigation databases, to provide the flight crew with continuous guidance and decision support across all phases of flight. From pre-flight initialization to approach and landing, the FMS facilitates navigation accuracy, fuel efficiency, and workload reduction. FMS functionality is deeply integrated into the avionics architecture of an aircraft. Most systems operate within a closed environment where data flows between the FMS and other subsystems are managed through avionics-specific Local Area Networks (LANs). External communication occurs through structured channels such as the Aircraft Communications Addressing and Reporting System (ACARS), enabling the exchange of flight plans and operational updates between the aircraft and ground-based control centers. These updates are processed through well-defined mechanisms that maintain the consistency and correctness of flight plan data.

Across both domestic and international airspaces, FMS plays an essential role in supporting evolving air traffic management strategies. In the United States, the FAA has introduced the Next Generation Air Transportation System (NextGen), which focuses on enhancing the efficiency and predictability of air traffic through digital coordination and trajectory-based operations. Similarly, the Single European Sky ATM Research (SESAR) initiative in Europe promotes cross-border interoperability and seamless traffic flow using advanced automation and network-centric frameworks. Within these modernized ecosystems, the FMS functions as a key enabler of trajectory management, facilitating dynamic re-routing and real-time performance-based navigation.

As air traffic systems adopt more collaborative and data-driven paradigms, the role of the FMS is also expanding. Ground operation centers increasingly provide initialization data prior to departure, while en route updates can adjust flight trajectories in response to changing conditions such as weather, airspace congestion, or scheduling demands. The integration of these capabilities into the FMS allows for more efficient aircraft turnaround, enhanced situational awareness, and optimized mission execution.

The general architecture of a modern Flight Management System has been illustrated in figure 1. The architecture presents a high-level schematic showing how the FMS interfaces with both internal aircraft subsystems and external data sources. The FMS is centrally connected to the aircraft's avionic LAN, allowing it to exchange data with navigation sensors, performance monitoring modules, and flight deck displays. Internally, the system receives and processes inputs from the crew and from other aircraft systems to support flight planning, guidance, and optimization functions. As indicated in the diagram, potential adversarial attack vectors include tampering with sensory data inputs or injecting malicious information through datalink communications and other external data sources. These channels, designed to support integration with ground systems, external databases, and application-level interfaces, present opportunities for attackers to compromise flight planning or mislead onboard systems if not properly secured. The diagram also emphasizes the structured nature of these data flows, with clear boundaries between aircraft-internal and external

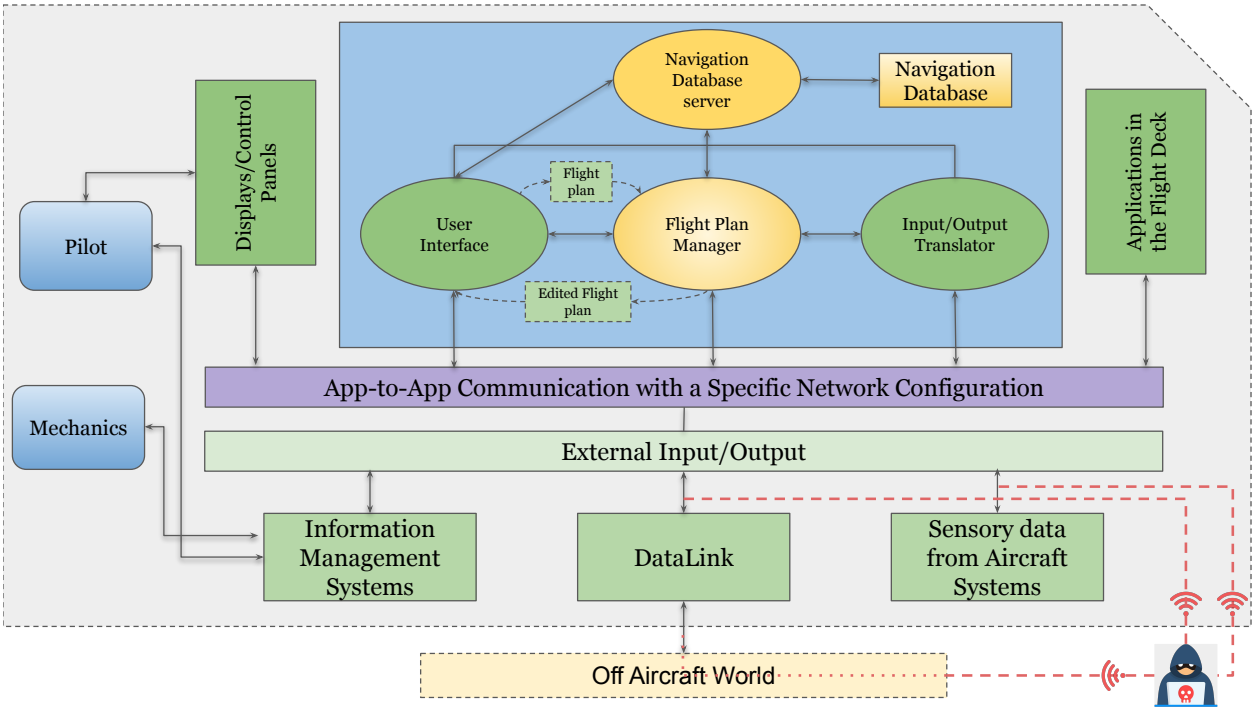

Fig. 1 Illustrative architecture of a commercial Flight Management System (FMS), highlighting potential adversarial attack vectors.

networks.

This system-level integration positions the FMS as a central decision-support component, capable of synthesizing inputs across the aircraft and external airspace infrastructure. As such, the architecture supports both conventional operations and the more dynamic, data-driven environments anticipated in future airspace systems.

III. Vulnerabilities and Defense Mechanisms

AAM and eVTOL systems integrate a diverse set of sensors, communication links, navigation modules, cloud services, and automated flight control components. Each subsystem introduces unique attack surfaces and operational constraints, making the overall ecosystem highly susceptible to multi-vector cyber–physical threats. In the following subsections, we examine the major vulnerabilities across GNSS, communication channels, perception modules in autonomy stacks, avionics functions, data links, and cloud-based UAM service providers. To provide a consolidated view, Table 1 summarizes the key threats identified for each subsystem and outlines the corresponding defense mechanisms discussed throughout this section. Furthermore, Tables 2–6, as well as Tables 8–11, present these vulnerabilities and their proposed solutions in greater detail, together with the associated references.

A. Vulnerabilities of onboard avionics and sensors

The risks and vulnerabilities in this subsection often exist in commercial aviation aircraft, helicopters and general aviation aircraft.

1. GNSS/GPS Jamming, Spoofing, and Degradation in Urban Environments

For the effective operation of various General Aircraft and eVTOL vehicles utilized in AAM, it is critical that each aircraft can accurately localize its own position (defined as *navigation* in aviation). This level of accuracy is crucial for multiple aircraft to operate simultaneously within the same airspace, since both precise self-localization and real-time awareness of other aircraft positions are necessary to prevent collisions. Unlike conventional aircraft, eVTOLs for air mobility are typically designed to operate in densely populated areas, where they need to fly at lower altitudes and closer

Table 1 Threats and defense mechanisms for key eVTOL / AAM Subsystems in summary.

Subsystem / Domain	Existing Threats	Defense Mechanisms
GNSS / GPS Jamming, Spoofing, NLOS Degradation	GNSS denial through jamming; spoofed satellite signals causing incorrect positions; multipath and NLOS degradation; altitude instability; long-duration measurement loss; drift from stale sensor states.	RTK failover; redundant GNSS references; INS/IMU fusion; LiDAR-, radar-, vision-based navigation; UWB and LEO localization; ML-based spoofing mitigation; robust switching logic; switched-system controllers for GPS-loss states.
RF / ATC Voice–Data Impersonation	SDR replay of ATC; AI voice cloning; forged digital advisories; masking legitimate transmissions; timing and phraseology anomalies causing unsafe deviations.	PKI-signed advisories; mutual authentication; RF fingerprinting with transmitter checks; deterministic conflict policy; hold-on-mismatch behavior; EUROCAE secure-voice/data alignment.
TCAS / ACAS-X Spoofing and RA Manipulation	Ghost aircraft via Mode S / ADS-B spoofing; spurious or conflicting RAs; self-tracking anomalies; oscillatory autopilot responses; trust erosion; vulnerability of 1030/1090 MHz links.	MLAT cross-check; radar altimeter validation; optical verification; signal-level feature checks (RSSI/TDoA/AoA); trajectory feasibility filters; RA monitoring companions; ATC procedural support and training.
ADS-B Spoofing, Identity Manipulation, Saturation	Plaintext broadcast enabling spoofing; ghost tracks; identity manipulation; message flooding/DoS; overshadowing/bit-flips; congestion degrading surveillance and DAA.	MLAT/TDoA verification; onboard sensor fusion; kinematic/TOA filters; congestion-aware track prioritization; confidence scoring via SDSPs; exploration of authenticated ADS-B extensions.
Camera and Visual Sensors	Adversarial patches hiding aircraft; lighting, weather, and glare degradation; optical deception; multi-sensor adversarial corruption; sensitivity to blur/noise/OOD data.	LiDAR–camera geometric consistency; distributed sensing; corruption-aware training (AugMix); anomaly detection (Energy/OE); certified fusion architectures; PatchGuard/PatchCleanser; neural-backdoor defenses (Neural Cleanse/STRIP).
LiDAR / Radar Sensors	False-echo insertion; spoofed returns; range saturation; degraded altitude measurements; cross-sensor adversarial attacks.	Pulse coding/authentication; multi-band correlation; TOF consistency; redundant-sensor voting; fusion with vision + IMUs for integrity monitoring.
Electronic Flight Bag (EFB)	Malware on tablets; untrusted Wi-Fi/LTE; tampered performance apps; local database modification; OS vulnerabilities; cross-domain propagation into avionics.	ML intrusion detection; domain firewalls; signed/versioned content; encrypted sync; certificate-based auth; MDM policy enforcement; rapid rollback; architectural segmentation (AISD/ACD/PIESD).
FMS & Avionics Supply Chain	GNSS spoofing corrupting FMS state; ACARS injection; navigation DB tampering; ARINC 664 lateral-movement attacks; supply-chain malware; poisoned cloud routing data; ATM–FMS multi-stage vulnerability propagation.	Authenticated ACARS; redundant inertial/barometric sources; avionics segmentation; ARINC 664 intrusion detection; STRIDE mitigation; safety-II operational resilience; SBOMs + supply-chain hardening frameworks.
Telemetry Data Links	Potential spoofing/tampering of fleet telemetry; identity spoofing; rate manipulation; ARINC 429 DoS indirectly suppressing telemetry; cloud-based dependencies.	Encrypted telemetry; anti-replay freshness windows; segmentation; anomaly monitoring; redundancy + rate limiting; baseline cross-checking of incoming telemetry streams.
Navigation Database (Data Attacks)	Corruption of vertiport/obstacle/corridor data; poisoned routing; tampering during uplink; ARINC 429 DoS delaying DB transfers; lack of provenance for UAM 3D models.	Cloud cybersecurity; strict data handling; segmentation; bus-health monitoring; rate-limits; onboard consistency checks; provenance-tracking + integrity auditing (e.g., Merkle-based).
C2 Link (Command/Control)	Jamming during handovers; MitM; roaming-related latency spikes; spoofed commands; insecure 5G slices; session hijacking; compromised gateways.	Dual-path diversity (5G + aviation band); spread-spectrum + beamforming; authenticated encryption (TLS/DTLS with AEAD); slice-binding; secure time sources; authenticated control messages; graceful-degradation behaviors.
Cloud Architecture / PSUs / SDSP APIs	Compromised API credentials; replayed tokens; poisoned SDSP feeds; MitM on cloud channels; stale/incorrect constraints; cascading multi-domain failures.	OAuth2 + mTLS; signed payloads with freshness; PSU–SDSP cross-validation; immutable audit logs; secure API gateways; provenance tracking; graceful fallback to last-good state.

to urban environments. Therefore, obtaining and maintaining precise localization signals is crucial for their safe and stable operation. As a result, instability or compromise of positional information (caused by cybersecurity threats such as spoofing, jamming, or various other communication attacks) can lead to severe malfunctions. Most eVTOLs rely heavily on GNSS or GPS signals for their localization. In the GNSS framework, eVTOL aircraft receive signals from multiple satellites and utilize them for geopositioning or navigation through trilateration techniques [26]. Depending on the country of operation, GNSS systems are known by different names. For instance, GPS is operated by the United States, Beidou by China, GLONASS by Russia, and Galileo by the European Union. For simplicity, this section will collectively refer to these systems as GNSS or GPS. In positioning via GNSS, the accuracy of the calculated location increases with the number of satellite signal sources utilized. Therefore, to ensure a stable and precise GNSS-based positioning system, it is crucial to guarantee the secure reception of these signals.

Existing Threats: Accurate reception of GNSS signals is crucial for the localization of eVTOLs. The performance of the system is clearly vulnerable the unavailability of a (GPS) signal for synchronization, whether due to urban canyons or intentional jamming. In the event of such measurement losses, eVTOL aircraft may suffer from poor performance and potentially lose stability or display unacceptable performance otherwise. There exist multiple ways to attack the signals received by a vehicle, with GPS jamming being the most representative. GPS jamming [12, 13] refers to an attack technique similar to signal jamming, in which specific radio signals are transmitted to overwhelm GPS satellite signals. Through such interference, the GNSS signals received by the vehicle can be blocked or destabilized, significantly degrading positional accuracy and ultimately compromising localization and navigation capabilities. Beyond jamming,

Table 2 GNSS and GPS threat patterns for eVTOL navigation and representative mitigation strategies.

Threat class	Effect on eVTOL operation	Representative mitigation
Jamming of GNSS signals	Loss or severe degradation of satellite measurements, position dropouts, unstable altitude estimates, and possible loss of stability in low-altitude UAM corridors [12–14].	RTK failover with ground reference stations [15], redundant GNSS sources, and fail-safe switching mechanisms for RTK networks under instability [16].
Spoofing and counterfeit satellites	Receiver locks onto fake constellations, computes erroneous positions, and may follow misleading trajectories or be displaced from intended corridors [17, 18].	Multi-sensor fusion with INS, LiDAR, and vision-based navigation to cross-check GNSS solutions [19–23]; machine-learning-based correction and anomaly detection [24, 25].
NLOS and multipath in urban canyons	Reduced number of usable satellites, biased ranges, degraded vertical position, and long-duration measurement gaps in dense urban environments [14, 26].	Alternative positioning sources such as LEO or cellular signals [27, 28] and UWB hyperbolic navigation [29, 30], combined with robust sensor fusion for altitude stabilization.
Long-duration measurement loss	Drift of navigation states when controllers reuse stale positions, leading to large deviations or instability.	Using local sensing (IMU, visual, LiDAR) as temporary primary navigation during outages, and designing switched-system controllers that explicitly model GPS-available and GPS-denied modes.

GPS spoofing [17, 18] represents another method of undermining GNSS-based localization. Signal spoofing deceives the GNSS receiver by generating counterfeit satellite signals, thereby injecting false positioning data. As a result, the vehicle calculates its position based on inaccurate information, leading to erroneous localization that can cause severe system failures or even enable hijacking scenarios. In addition to these external attacks, environmental factors can also degrade the accuracy of GNSS systems. GNSS precision deteriorates when a vehicle operates in a Non-Line-of-Sight (NLOS) environment, where the direct path between the satellite and the vehicle is obstructed. For instance, operations in dense urban areas surrounded by tall buildings, or in valleys or mountainous regions, significantly reduce the likelihood of receiving Line-of-Sight (LOS) GPS signals, making stable signal acquisition difficult and thus leading to degraded GNSS performance. In such cases, signal blockage caused by the surrounding environment prevents the receiver from obtaining accurate data, ultimately lowering overall GPS positioning accuracy. Among the positional coordinates, altitude values are known to be particularly unstable compared with latitude and longitude [14]. While the latter can be corrected or stabilized using supplementary sensor data, inaccuracy in altitude measurements poses a critical risk. This altitude uncertainty can be especially hazardous for eVTOL operations within UAM environments, where precise vertical positioning is essential for safe navigation and separation management. Therefore, although GNSS/GPS remains a fundamental component in eVTOL localization, reliance on a single source of positioning information renders the system highly susceptible to the aforementioned cybersecurity and environmental vulnerabilities. To enhance system robustness, it is imperative to integrate complementary navigation and localization methods, thereby achieving greater resilience and reliability.

Defense Mechanisms: To address the vulnerabilities of GNSS/GPS-based positioning and navigation systems, a naïve approach is to allow the controller to use the last available measurement in the event of a measurement loss, and bound the maximum allowable duration of the loss to guarantee stability. However, the duration of measurement loss may easily exceed the maximum allowable duration to guarantee stability due to the fact aircraft dynamics are extremely fast and may therefore not be able to maintain stability under the longer measurement loss durations in GPS signal losses. Moreover, even for measurement loss durations smaller than this threshold, large position and velocity drifts can occur due to the controller repeatedly using the incorrect (last available) measurement. Therefore, multiple studies have been conducted to improve the robustness of the GNSS/GPS system while addressing these issues. First, research has been carried out to enhance fail-safe mechanisms in cases of GPS signal failure. To compensate for the instability of GPS signal reception, the Real-Time Kinematic (RTK, [15]) system has been developed. This method utilizes a stable GNSS signal received at a stationary base station to correct unreliable GPS values and improve accuracy. Based on this concept, [16] proposed fail-safe switching mechanisms that ensure redundancy in RTK-GPS during network instabilities caused by various threats. Next, some studies focus on integrating multiple sensors to mitigate navigation errors arising from GPS vulnerabilities. For instance, alternative or supplementary sensors can be utilized to support or replace conventional GPS-based navigation under such threat conditions. These include the use of Inertial Navigation Systems (INS) employing IMU sensors [19], localization and navigation using LiDAR sensors [20, 21], improving altitude and positional accuracy through vision sensors [22, 23, 31], backup navigation using Low Earth Orbit (LEO) satellites or cellular signals [27, 28], and hyperbolic navigation methods using Ultra-Wideband (UWB) signals [29, 30]. Finally, various machine learning techniques have also been applied to enhance positioning accuracy under potential GPS threats. For example, Recurrent Neural Network [24] or Convolutional Neural Network [25] can be employed to

Table 3 RF and ATC link impersonation in AAM corridors: attack modes and protection layers.

Voice replay on aeronautical channels
Capability: Records and replays authentic ATC clearances with correct phraseology [7]. **Symptom:** Duplicate or conflicting clearances, unexpected altitude/corridor changes. **Defense:** Query–hold policies; cross-check against signed digital advisories.
AI voice cloning of controllers
Capability: Real-time imitation of ATC voices using neural voice-cloning models [32]. **Symptom:** Highly realistic but unauthorized instructions consistent with prior interactions. **Defense:** RF fingerprinting, TOA validation of transmitters [33, 34]; pilot training for anomaly detection.
Carrier interference and masking
Capability: Transmits noise or blocking signals on the ATC frequency [35]. **Symptom:** Broken / clipped transmissions, missing clearances in dense UAM corridors. **Defense:** Channel monitoring, automatic fallback channels, deterministic loiter-on-silence procedures [7, 36].
Coordinated voice + data forgery
Capability: Spoofed digital advisories aligned with forged voice commands. **Symptom:** Very high plausibility due to synchronized voice–data deception. **Defense:** Mutual TLS, PKI, anti-replay for digital advisories [37]; signed data overrides voice.

improve the accuracy of GPS signals by compensating for inaccuracies that arise during operation.

Gaps and Open Problems: Despite substantial studies and notable progress in developing robust GNSS-based localization systems for eVTOLs, there is still no widely accepted or standardized integrated framework to address this issue. Instead, many researchers and operators rely on their own proprietary or ad-hoc methods to ensure the navigation accuracy of GNSS systems. Furthermore, variations in international and organizational regulations have hindered the establishment of lightweight civil-signal authentication mechanisms for GNSS suited for eVTOL applications. In addition, there remains a lack of certifiable machine learning–based jamming and spoofing detectors implemented in practical settings.

For robustness to improve the reliability of the system, there needs to be a process by which when the GPS measurement is lost at an eVTOL aircraft, local sensing (based on IMU and visual sensors, or signal triangulation from LEO with respect to a pre-fed map of landmarks) is temporarily used for primary control in place of GPS signal to provide navigation. One complication here is that each eVTOL may operate with GPS-based or local-sensing based control at any time instant, depending on the availability of GPS measurements at that aircraft. More research is needed on how to analyze the resulting system and control architecture as a nonlinear switched system and possibly design distributed controllers to guarantee safety of all the aircraft in the same airspace.

2. RF/ATC Link Impersonation and Unauthorized Frequency Use

In the United States and other countries, government bodies such as the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) regulate the radio frequency (RF) spectrum and reserve certain frequency bands for aeronautical mobile communications, such as those between eVTOL crews and remote supervisors or air traffic control. Anyone with suitable radio equipment has the capability to broadcast on a given RF frequency band, meaning that an adversary can transmit on the same aeronautical voice or ground radio channels used by eVTOL crews or remote supervisors and imitate a controller or vertiport dispatcher. In the absence of defense mechanisms, an adversary may fabricate messages, replay prior clearances, or splice phrases timed to blend with legitimate traffic. In dense, low-altitude corridors with high tempo operations, such forgeries can be wrongly accepted, producing off-nominal trajectory changes (wrong corridor/altitude or incorrect vertiport turn-in). This risk is recognized for UAM voice/data exchanges and human–automation coordination in FAA UAM ConOps v2.0 [7].

Existing Threats: Since broadcast transmissions from entities are unencrypted by default, an adversary may record transmissions and use them to construct an attack. A simple example would be a voice replay attack where the adversary transmits a previously recorded clearance message from ATC with correct phraseology and timing to make an eVTOL

Table 4 TCAS and ACAS-X security-relevant layers, failures, and mitigation concepts.

ACAS-X Security and Vulnerability Overview			
Layer	**Role in TCAS / ACAS-X**	**Security vulnerability**	**Mitigation direction**
Surveillance inputs	Mode S and ADS-B replies on 1030/1090 MHz provide range, altitude, and closure rate for intruder aircraft [38, 39].	Unauthenticated messages enable ghost tracks, replay attacks, and self-tracking anomalies, which can trigger spurious RAs [5, 40].	Multi-source validation using MLAT and radar, plus signal-level checks (RSSI, TDoA, AoA) to flag inconsistent or physically impossible tracks [41, 42].
Decision policy (ACAS-X tables)	Markov decision process optimized tables select RAs that balance safety and operational costs [43, 44].	Tables assume honest surveillance; adversarial trajectories can drive the system into unnecessary or conflicting advisories.	Companion monitoring of RA histories, trajectory feasibility checks, and future formal verification under adversarial input models [42, 45].
Flight deck integration	Advisories appear on cockpit displays and may be coupled to the autopilot for automatic execution [45, 46].	Coupling to autoflight can produce oscillatory behavior or large altitude deviations when corrupted inputs persist; repeated false alerts reduce crew trust [47, 48].	Training and procedures for recognizing abnormal alert patterns, guidance for reverting to TA-only modes, and joint ATC–airline reporting workflows for anomaly investigation [5, 48].
Operational ecosystem	TCAS and ACAS-X form the last airborne safety net on top of pilot vigilance and ATC separation [45].	Lack of message authentication and incomplete standards for secure surveillance keep CAS exposed to targeted spoofing campaigns.	Development of lightweight authentication or integrity protection for surveillance channels, co-designed with CAS logic and certification constraints.

crew believe they have clearance when they should not. A more sophisticated version of this would be to use AI voice cloning technology [32] to mimick the voice of a controller in real-time. An adversary may also listen to transmissions to determine a time when they want to transmit an unauthorized carrier on some channel as a form of RF interference [35] to mask or preempt legitimate transmissions, preventing a given entity from receiving important information. Since operators often trust corroboration between voice and data channels, an even more sophisticated attack would be to simultaneously forge a voice transmission and digital advisory to increase plausibility. These attacks can have observable symptoms and operational impacts such as timing irregularities, atypical phraseology, or RF fingerprints inconsistent with authorized ground transmitters. They can result in loss of separation or missed approach sequencing in corridors or vertiports as noted in AAM concepts of operation [36].

Defense Mechanisms: An obvious defense mechanism for digital communications is the use of cryptography. Mutual authentication and freshness for digital advisories could be achieved through the use of Mutual Transport Layer Security (mTLS) and public key infrastructure (PKI) with cryptographic nonces and timestamps to prevent replay attacks, aligning with EUROCAE VTOL information security guidance [37]. For analog communications, RF transmitter fingerprinting [33, 34] through monitoring carrier, time of arrival (TOA), and in-phase and quadrature (IQ) artifacts and comparing them to known transmitter locations for ground stations can provide a means of identifying impersonated communications, subsequently triggering query/hold policies. When comparing digital and analog communications, a deterministic conflict policy can be applied such that, if voice and signed data disagree, the eVTOL can default to hold/loiter until the conflict is resolved. This approach would be consistent with safety-first fallbacks in the UAM ConOps [7].

Gaps and Open Problems: Interoperable secure voice and data procedures tailored for AAM are still maturing. There are limited urban-multipath radio voice datasets for spoofing and anomaly detection, and there is limited certification guidance for time-critical RF communication [7, 37].

3. TCAS and ACAS -X Vulnerabilities

Collision Avoidance Systems (CAS) represent one of the most critical airborne safety mechanisms, designed to reduce the risk of mid-air collisions by continuously monitoring the surrounding airspace and issuing maneuvering instructions when the risk of collision becomes imminent [45]. These systems operate independently of ground-based infrastructure and use transponder replies from nearby aircraft to determine range, altitude, and closure rate [38]. The CAS logic continuously evaluates time to closest point of approach and generates alerts when separation thresholds are predicted to be violated [45]. Such airborne self-separation capabilities serve as a final protective layer in the air traffic management hierarchy, supplementing both pilot vigilance and ATC separation procedures [45, 46].

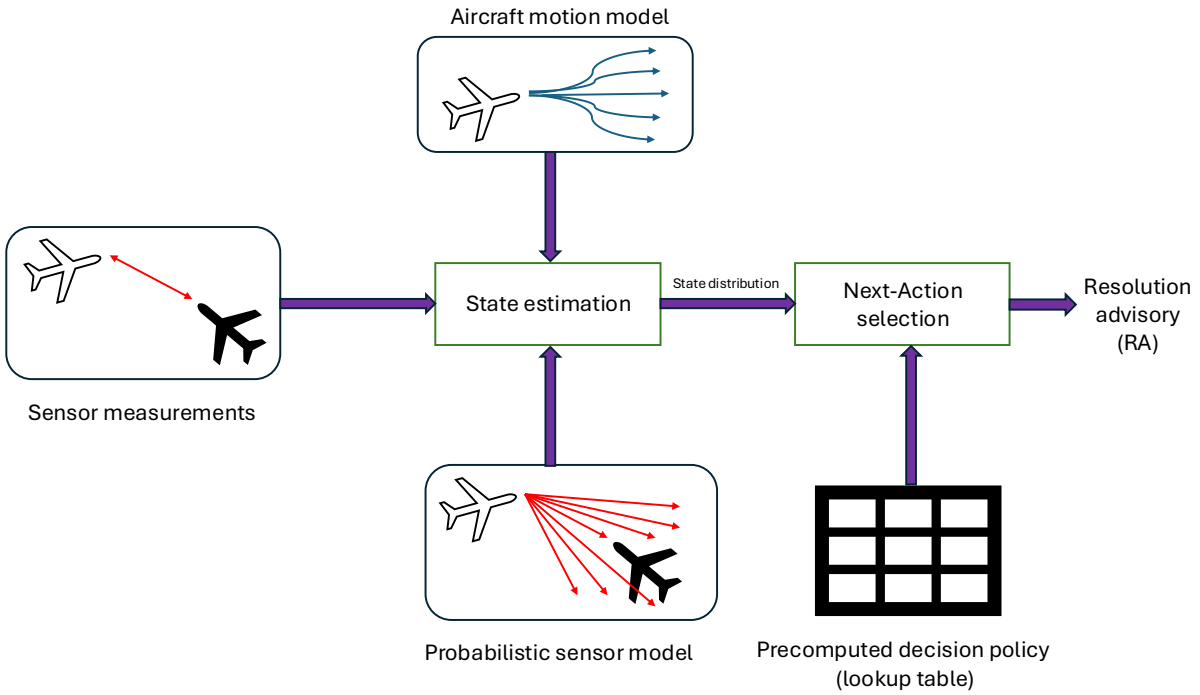

Fig. 2 ACAS-X continuously updates its aircraft state estimates as new sensor measurements become available. The system represents uncertainty using a probability distribution, which determines the appropriate region of the lookup table from which to select the corresponding resolution advisory.

The Traffic Collision Avoidance System (TCAS) [46], standardized as ACAS II by the International Civil Aviation Organization (ICAO), constitutes the current operational realization of CAS in commercial aviation. TCAS operates independently of ground-based air traffic control by using transponders to interrogate the airspace around an aircraft [39]. TCAS performs active surveillance by transmitting Mode S interrogations on 1030 MHz and receiving replies on 1090 MHz from aircraft equipped with transponders [45]. Based on closure rate, altitude difference, and vertical speed, TCAS issues *Traffic Advisories (TAs)* and *Resolution Advisories (RAs)* that instruct the pilot to climb or descend to maintain safe separation [5, 45, 46]. These advisories are presented on cockpit displays and, in advanced implementations, can be linked with the flight director or autopilot to enable automatic execution [5]. The system has been highly successful in reducing mid-air collisions, but its reliance on unauthenticated transponder data remains a critical security concern [5, 45].

The Airborne Collision Avoidance System X (ACAS-X) represents the next generation of collision avoidance technology, developed under a joint FAA–MIT Lincoln Laboratory program to address TCAS limitations in logic efficiency and operational acceptability [43]. ACAS-X retains the existing surveillance infrastructure (Mode S, ADS-B) but replaces the rule-based logic tables of TCAS with a decision policy obtained through large-scale Markov decision process optimization [43]. Its alerting tables are derived offline from probabilistic encounter models that balance safety metrics and operational costs, significantly reducing unnecessary advisories and alert reversals [38]. Figure 2 shows the architecture of the proposed ACAS-X. Multiple variants have been proposed, such as ACAS Xa for manned aircraft, ACAS Xu for unmanned systems, and ACAS Xr for rotorcraft [44], extending its applicability to future AAM and eVTOL operations.

Existing Threats: While ACAS-X enhances operational robustness compared to TCAS, it inherits several fundamental vulnerabilities from the underlying surveillance infrastructure. Both systems depend on transponder-based inputs transmitted over unauthenticated 1030/1090 MHz channels (Mode S, Secondary Surveillance Radar (SSR), ADS-B), which are susceptible to spoofing, replay, and signal injection. Prior studies such as [40] have demonstrated that adversaries can fabricate synthetic aircraft tracks through manipulated ADS-B or Mode S transmissions, leading to erroneous threat evaluations and, in some cases, the generation of unnecessary or conflicting RAs. Experiments

conducted using standardized ACAS-X code and real traffic datasets showed that such false inputs can trigger spurious advisories in approximately 44 percent of the simulated encounters, increasing to nearly 79 percent within the altitude range of 2,350–13,300 ft AGL. The induced deviations averaged roughly 590 ft, indicating a significant operational impact even when the attack is limited to radio-layer manipulation [45].

Beyond direct signal spoofing, the interaction between TCAS or ACAS-X and other avionics subsystems introduces additional pathways for exploitation. The exchange of data among the transponder, display units, and autoflight systems can propagate corrupted inputs or stale advisories, amplifying the effects of an external disturbance. The coupling between TCAS and autopilot functions, particularly when RAs are executed automatically, can result in hazardous oscillations or mode confusion when multiple systems respond simultaneously to falsified data [42]. Moreover, sustained false or nuisance alerts have been observed to erode pilot trust, prompting flight crews to revert to TA-ONLY or STBY modes, thereby disabling the last line of airborne collision protection [47]. Notably, FAA operational guidance acknowledges that ACAS II and ACAS Xa may generate false or self-tracking RAs due to surveillance or tracking anomalies, including instances where an aircraft may momentarily track itself as a threat. These spurious advisories can lead to large altitude deviations if not properly identified, and flight crew are explicitly instructed to report such anomalies for post-event safety investigation [48]. As highlighted in previous analyses, the absence of message authentication and the reliance on assumed integrity in Mode S replies remain the principal attack vectors for CAS technologies across both legacy and next-generation implementations [5].

Defense Mechanisms: Several mitigation strategies have been proposed to reduce the exposure of TCAS/ACAS-X and related collision avoidance systems to spoofing and signal manipulation. One class of defenses focuses on enhancing the integrity of surveillance data through multi-source validation. By cross-referencing ADS-B or Mode S inputs with independent sensors such as multilateration (MLAT) [41], radar altimeters, or optical detection systems, it becomes possible to identify injected or inconsistent tracks before they influence the decision logic. Research efforts have shown that incorporating signal-level characteristics, including received power, time difference of arrival, or angle-of-arrival estimates, can substantially improve the ability to distinguish genuine aircraft replies from fabricated ones [42]. Additionally, These parameters can be used to compute reliability estimates for intruder tracks or to reject trajectories that violate physical feasibility, thereby preventing false alerts caused by manipulated or corrupted surveillance inputs. From an architectural standpoint, layered monitoring systems have been proposed to operate in parallel with ACAS-X logic. These companion monitors would evaluate real-time trajectory consistency and alert reliability, flagging sequences of repeated false RAs that may indicate a spoofing or replay campaign [42]. Furthermore, procedural defenses such as standardized crew responses, ATC coordination protocols, and training for recognition of abnormal alert patterns have been recommended to complement technical safeguards [5].

Gaps and Open Problems: Although ACAS-X provides measurable improvements in alerting logic, several open research and certification challenges persist. The foremost gap concerns the absence of authenticated or integrity-protected surveillance inputs. No globally standardized method currently exists to validate Mode S or ADS-B messages within the latency and interoperability constraints of commercial avionics. As a result, ACAS-X decision policies continue to rely on unverified sensor data, leaving the system vulnerable to targeted signal manipulation. Another critical issue lies in the formal verification of the ACAS-X decision policy under adversarial or degraded conditions. Existing validation processes focus on nominal encounter models and do not account for maliciously crafted input trajectories that could exploit the decision table boundaries or cost-function discontinuities. Furthermore, the growing degree of integration between ACAS-X advisories and automated flight control systems raises concerns regarding closed-loop stability and pilot situational awareness in the presence of false or oscillatory RAs. Addressing these gaps will require the development of certified, lightweight authentication mechanisms for surveillance data, extended verification frameworks incorporating adversarial inputs, and human-factors studies focused on maintaining trust and compliance under abnormal alerting conditions.

4. ADS -B Attacks and Spectrum Saturation

The Automatic Dependent Surveillance–Broadcast (ADS-B) system, mandated by civil aviation authorities worldwide, is a cornerstone of modern air traffic management. It enables each aircraft to periodically broadcast its identity, position, velocity, and operational status, thereby supporting surveillance, conformance monitoring, and detect-and-avoid (DAA) functions. The simplicity of message decoding and the availability of low-cost software-defined radios (SDRs) have further accelerated ADS-B adoption in both civil and unmanned aviation domains.

Table 5 ADS-B misuse patterns and defense principles for high-density AAM corridors.

Attack Type	Impact on Surveillance / DAA	Defense Strategy (Refs.)
Ghost track injection	Fabricated aircraft clutter displays and mask real conflicts [49–51].	Cross-validate ADS-B using MLAT (TDoA), LiDAR–inertial localization, or optical sensing to confirm track legitimacy [19–21].
Identity manipulation	Spoofed Mode S/ADS-B identifiers disrupt conformance monitoring and separation [51, 52].	Identity-integrity scoring, track-continuity validation, and cooperative confidence sharing between PSUs/SDSPs [31].
Flooding / 1090 MHz congestion	Message flooding saturates channel capacity, degrading surveillance reliability [51, 53].	Congestion-aware filtering prioritizing nearby/conflict-relevant targets; rate limiting and deprioritizing low-confidence tracks [22].
Plaintext broadcast	Unauthenticated broadcast enables eavesdropping and low-cost spoofing with SDRs [49, 50].	Research toward authenticated ADS-B extensions balancing scalability, confidentiality, and backward compatibility.

However, ADS-B's open and unauthenticated broadcast nature makes it inherently vulnerable to cyberattacks. Because messages are transmitted in plaintext without encryption or authentication, adversaries can intercept, modify, or fabricate signals to inject false tracks or manipulate aircraft identifiers. Past research works have demonstrated that injection, identity manipulation, and flooding attacks can be executed using inexpensive SDR equipment [49, 50, 52]. In dense or low-altitude UAM environments, where surface or corridor surveillance may fuse ADS-B tracks for conformance and DAA, these injected or duplicate tracks can obscure genuine conflicts and trigger nuisance advisories, undermining situational awareness and airspace safety [51]. Additional vulnerabilities include denial-of-service (DoS) through message flooding or spectrum congestion, message modification via overshadowing or bit-flipping, and jamming of the 1090 MHz frequency band used by ADS-B [53]. As urban airspace becomes increasingly populated with eVTOL operations, spectrum saturation may happen. Therefore, the ADS-B system, while critical for UAM operation, exposes a significant cyber attack surface for both intentional and unintentional interference.

Defense Mechanisms: Effective defenses against ADS-B exploitation combine data cross-validation, signal-level filtering, and adaptive prioritization. First, cross-validation techniques correlate ADS-B reports with independent surveillance or onboard sensing modalities, such as multilateration (MLAT) using time-difference-of-arrival (TDoA), LiDAR–inertial localization, or optical perception systems, to verify the plausibility of received tracks [19, 20]. Second, kinematic and time-of-arrival (TOA) filtering rejects tracks that exhibit implausible dynamics, inconsistent timestamp patterns, or physically infeasible motion signatures [21]. Finally, priority management under congestion ensures that surveillance and traffic management systems allocate bandwidth and processing resources to nearby or conflict-relevant tracks, while rate-limiting or deprioritizing distant or low-confidence data. These confidence scores can be shared between service providers, such as Provider of UTM Services (PSU) or Supplemental Data Service Providers (SDSP), to maintain common situational awareness under saturation conditions [31].

Gaps and Open Problems: Despite ongoing research, there remains no globally adopted framework for authenticated yet privacy-preserving ADS-B communication suited to high-density UAM operations. Current cryptographic proposals face scalability and backward-compatibility challenges, while physical-layer cross-validation depends heavily on network geometry and sensor availability. Moreover, public, vendor-neutral trials quantifying ADS-B resilience under urban-density conditions are still limited. Future work should focus on certifiable, privacy-aware surveillance protocols and empirical testing in representative eVTOL and UAM corridors to evaluate the effectiveness of saturation and spoofing defenses [22].

5. Electronic Flight Bag (EFB)

Electronic Flight Bags (EFBs) have evolved as essential digital tools that replace traditional paper-based flight materials, providing flight crews with electronic access to navigation charts, operational manuals, and aircraft checklists [54]. Initially implemented as laptop-based systems performing operational and flight management functions, EFBs now accommodate a wide range of software applications that automate tasks traditionally carried out manually, such as takeoff performance, weight and balance, and landing calculations [55]. Their adoption by commercial airlines, supported by early digital operations suites offered by major avionics manufacturers, has demonstrated measurable gains in operational efficiency and flight safety [56, 57]. Compared with standard laptop software, EFBs offer the advantage of not requiring separate storage procedures below 10,000 feet, which simplifies in-flight usage [58].

Modern EFBs are designed to enhance situational awareness, safety, and efficiency by integrating seamlessly with the FMS and other avionics to display an aircraft's real-time position, weather overlays, and relevant operational data [54, 59]. [60] shows example screens from a commercial EFB application, illustrating typical functionality for flight planning, procedure display, weather visualization, and digital checklists. Advanced configurations, including Class 3 EFB systems, enable integration with (ADS-B) and polarimetric radar technologies, further supporting route optimization and improved pilot decision-making [61, 62]. These digital systems also facilitate faster information exchange between the cockpit and ground support, streamlining flight operations and business processes.

Research indicates that EFBs generally improve flight crew performance by providing quick access to preflight information without significantly increasing workload under normal conditions [63]. However, studies such as [64, 65] report that during unexpected or high-stress scenarios, EFB interactions can temporarily elevate pilot workload. Despite these operational trade-offs, EFBs remain a cornerstone of modern cockpit digitalization, offering substantial advantages in safety, efficiency, and accessibility over conventional paper-based methods.

Existing Threats: [66] emphasizes that EFB enhances efficiency and reduces onboard weight compared to paper-based systems. However, the connectivity that enables these advantages also expands the attack surface: a compromised or malware-infected EFB could serve as an entry point for denial-of-service or similar attacks against interconnected avionics systems. [5] demonstrates that this interconnectivity creates a pathway for adversaries to pivot between passenger, administrative, and control networks if domain separation fails. As commercial off-the-shelf tablets are increasingly used as Class 2 EFBs, they inherit vulnerabilities from consumer ecosystems, including malicious applications, overheating-induced shutdowns, software crashes, and unverified data updates [56]. Furthermore, EFB reliance on wireless connectivity for database synchronization and NOTAM updates introduces exposure to spoofed or manipulated data transfers, echoing the broader avionics threat surface observed in FMS and ACARS links [5, 67]. The portable nature of the EFB and its ability to connect to public networks put the device at high risk, since exposure to open Wi-Fi can permit remote exploitation through unpatched software vulnerabilities [68].

Recent investigations highlight additional operational and cyber risks unique to EFB deployments. According to [69], inconsistencies in EFB classification and certification standards among operators lead to uneven security postures, where some devices are treated as portable consumer tablets rather than regulated avionics components. [70] further reveals that many EFBs connect via unsecured public Wi-Fi, LTE, or hotel networks without adequate authentication or isolation, exposing them to malware infection or unauthorized access. More critically, [71] demonstrate that tampering with EFB-based performance-calculation applications, such as altering runway length, surface condition, or aircraft weight, can result in incorrect takeoff parameters, potentially leading to runway excursions. Even when pilots perform verification, airlines that rely on a single EFB device for takeoff computation remain vulnerable to unnoticed manipulation. Finally, [72] show that critical takeoff and configuration data stored locally on EFB databases can be silently modified, underscoring the risk of data integrity compromise within an ecosystem increasingly built on heterogeneous hardware and non-standardized software. Figure 3 shows how different types of target data in the EFB can be exposed to various attack vectors.

Defense Mechanisms: To address the growing attack surface of connected EFB architectures, recent studies propose both proactive and layered defense approaches. [73] developed a network-based Intrusion Detection System (NIDS) that employs machine learning and anomaly detection to secure Remote Desktop Protocol (RDP) and Remote Framebuffer Protocol (RFB) connections between commercial tablets and EFB servers. The system classifies Transmission Control Protocol (TCP) traffic at the packet level using a decision tree and k-means clustering, detecting malicious packets carrying real exploits with a true positive rate of 0.863 and a false positive rate of 0.0001. This fine-grained detection mechanism functions as an inline proxy between the EFB client and server, preventing code execution, privilege escalation, and authentication bypass attacks without degrading operational performance. [74] describes a defense-in-depth architecture that combines robust software design, firewalls between avionics domains, certificate-based authentication, application-level encryption, and link-layer integrity checks. The inclusion of segregated networks such as the Airline Information Services Domain (AISD), the Aircraft Control Domain (ACD), and the Passenger Information and Entertainment Services Domain (PIESD), along with controlled physical access and redundant data links, further enhances availability and resilience. Together, these mechanisms establish both algorithmic and architectural safeguards against EFB-originated or propagated cyber threats.

Gaps and Open Problems: Despite the growing awareness of EFB-related cybersecurity vulnerabilities, current research remains fragmented and predominantly focused on usability, human factors, or hardware reliability rather than

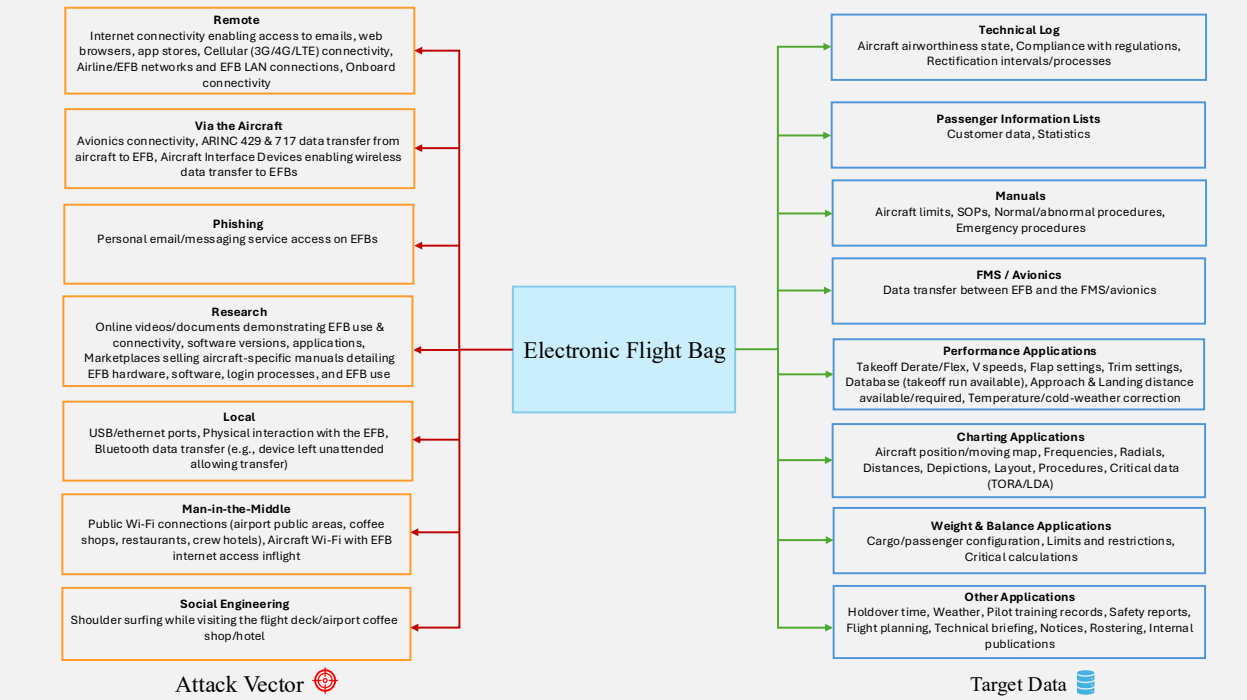

Fig. 3 Attack vectors and target data categories for EFBs, highlighting how operational, technical, and passenger-related data may be compromised through remote, local, or human-based threats.

comprehensive adversarial threat modeling. [56] emphasize that EFB certification and regulatory frameworks still center on operational and environmental compliance, such as decompression, battery safety, and usability, without mandating security-by-design practices. Although [5] extend the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege) frameworks to aviation systems, there is still no validated taxonomy tailored to EFB-specific threat vectors, such as tampering of performance-calculation applications or manipulation of local databases, as demonstrated in recent operational analyses [71, 72]. Moreover, while recent work proposes machine-learning-based intrusion detection for EFB server communications [73] and defense-in-depth architectures for flight-deck data exchange [74], these studies are limited to controlled environments and do not evaluate end-to-end resilience under realistic airline or eVTOL operational conditions. There remains a lack of standardized datasets, validation frameworks, and cross-domain testing methodologies for assessing how EFB-originated threats could propagate into avionics networks. Consequently, the integration of EFB cybersecurity into system-level safety assessments, coupled with empirical evaluation of proposed defenses in distributed and networked cockpit architectures, represents a critical and unresolved research frontier.

6. FMS and Avionics Software Supply Chain

The FMS is an integrated suite designed to achieve optimal flight control through the coordination of multiple aircraft subsystems. The FMS enables automation across all phases of flight and provides flight crews with the necessary operational data through a unified interface. Its primary component, the Flight Management and Guidance Computer (FMC), computes the aircraft's three-dimensional position, performance metrics, and other critical parameters required for precise and efficient flight along a predefined trajectory. These computations are derived from both manually entered and automatically acquired data. The Multipurpose Control and Display Unit (MCDU) serves as the pilot's interface for data entry and system communication with the FMC. The Flight Control Unit (FCU) governs the aircraft's lateral and vertical flight profiles, while the Flight Management Source Selector manages the selection of input sources used by the FMC. Finally, the display system presents key flight data and system information to the flight crew in real time [85].

Existing Threats: The FMS, as a core element of the aircraft control domain, is increasingly exposed to cyber threats due to its integration with open communication protocols and external data links such as GNSS and ACARS. [75] shows

Table 6 FMS and avionics software supply-chain risks for eVTOL and AAM operations.

Vulnerability	Failure mode	Impact on FMS	Mitigation
GNSS disruption feeding the FMS	Jamming or spoofing corrupts GNSS-derived position/velocity estimates [75, 76].	Incorrect aircraft state estimates driving wrong lateral/vertical path computations, unstable approaches, and incorrect leg transitions.	Cross-check GNSS with inertial and barometric sources; anomaly recognition procedures; authenticated ACARS links [76].
Navigation database tampering	Modified or corrupted approach/runway records [5, 76].	Incorrect glide paths, minima, missed-approach points, or procedure legs → potential CFIT or corridor deviations.	Controlled DB processes, cryptographic integrity checks, AISD/ACD isolation [5, 77].
Inter-domain connectivity (ARINC 664)	Ethernet-based avionics enlarge cross-domain attack surfaces [5].	Injected or delayed messages entering the FMS route manager or sensor integration modules → corrupted internal state or stale routing updates.	Segmentation, encrypted cross-domain pathways, ARINC-664-aware intrusion detection [5, 78, 79].
Software supply-chain compromise	Malicious upstream components propagate into FMS/autonomy software [80, 81].	Incorrect route generation, hidden logic triggers, degraded guidance algorithms, or inconsistent performance computations.	Supply-chain hardening, SBOM transparency, version attestation [82, 83].
Human and organizational factors	Operators patch issues informally, masking underlying problems [84].	Incorrect FMS entries, inconsistent performance profiles, or unreported anomalies leading to degraded trajectory planning.	Safety-II practices, structured reporting, collaborative monitoring [84].

how GNSS disruptions, even at modest jammer powers could corrupt the outputs of the FMS. Additionaly, simulation studies in [76] demonstrated that spoofing and jamming of GNSS signals can cause erroneous position inputs into the FMS during critical approach phases, while ACARS—used for flight plan and performance data uplink—lacks authentication and can be exploited to inject falsified route data or modify flight parameters. Moreover, they show that compromising the FMS navigation database itself poses a critical integrity threat: by altering stored approach data such as runway threshold altitudes or final approach fix geometry, attackers could cause the FMS to compute descent profiles leading below the intended glide path, potentially resulting in controlled flight into terrain under low-visibility conditions. As shown in [5], FMS is categorized within the Aircraft Control Domain (ACD), where interconnection between domains (ACD, AISD, and passenger domains) and the transition to Ethernet-based avionics (ARINC 664) expand the attack surface. Attack vectors include malicious data injection, cross-domain privilege escalation, and exploitation of unsecured wireless links. From a broader ATM perspective, [67] emphasizes that vulnerabilities across surveillance (ADS-B), communication, and navigation subsystems can propagate to the FMS, as demonstrated by prior events where false ADS-B and ACARS data led to spurious guidance or control anomalies. They further highlight that the growing interconnection between airborne and ground infrastructures has transformed ATM into an open cyber–physical ecosystem, where attackers can exploit correlated vulnerabilities and, through reinforcement learning and structured threat graphs, autonomously identify and chain multiple weaknesses, potentially propagating cyberattacks from ATM subsystems into the FMS itself. These works converge on the finding that modern FMSs—once isolated—now operate within a networked cyber–physical ecosystem where inadequate segmentation [77], legacy protocols, and lack of cryptographic protection represent systemic weaknesses.

Given that modern eVTOL FMS and autonomy modules will depend on software components, cloud-based routing services, and third-party data feeds, there is a real risk of software supply-chain compromise. Foundational research such as [80], demonstrates that supply chains lacking properties such as transparency, validity, and separation are vulnerable to poisoning and unauthorized modification. In addition, frameworks and methodologies such as [82], [83] provide taxonomies, checklists, and defense strategies for securing these chains in critical infrastructure. Real-world incidents, such as the SolarWinds breach, further illustrate how upstream compromise can propagate widely across dependent systems [81]. Although these risks are general to any software supply chain, they indicate a potentially high risk for eVTOL applications.

Defense Mechanisms: Across the reviewed studies, several layers of defense mechanisms are proposed to mitigate these vulnerabilities. [76] recommends procedural defenses such as enhanced pilot training for anomaly recognition and operational cross-checks between independent navigation sources to detect spoofed inputs. They also propose system-level mitigations including authentication of ACARS messages and the use of redundant inertial or barometric navigation references. [5] extends these measures through a taxonomy of mitigation techniques based on the STRIDE threat model [78, 79], including network segmentation between avionics domains, encryption of inter-domain data exchanges, and adoption of intrusion detection systems tailored for ARINC 664 traffic. Complementing these technical

defenses, [84] stresses the human and organizational dimension, advocating Safety-II resilience models where crews and operators adaptively respond to system irregularities, transforming potential failure cases (e.g., FMS misbehavior) into resilient success through anticipatory monitoring and collaborative response protocols through effective communication between agents in the system.

Gaps and Open Problems: While taxonomies such as MITRE ATT&CK [86] have been extended to aviation, offering a structured framework to map multi-stage attack chains and support proactive vulnerability assessment, no unified or validated threat model yet exists specifically for avionics and FMS integration, leaving limited empirical evidence on real-world exploitability. [76] underscores the lack of large-scale experimental validation under operational conditions—existing simulator trials are limited in scope and primarily focus on pilot reactions rather than system resilience metrics. [67] identifies insufficient automation in vulnerability correlation and attack-path discovery for complex ATM–FMS networks, calling for reinforcement-learning-driven knowledge graphs to anticipate evolving attack patterns. Finally, [84] reveals a socio-technical gap: organizational and training frameworks lag behind technological advances, with safety management systems remaining reactive rather than predictive. Collectively, these studies indicate that future research must integrate system-level cybersecurity modeling, real-time anomaly detection, and human-centered resilience frameworks to achieve trustworthy and adaptive FMS protection.

B. Potential risks from aircraft automation, autonomy and connectivity

The risks and vulnerabilities in this subsection are not common in commercial aviation aircraft, helicopters and general aviation aircraft yet, but they are expected with increasing automation and connectivity from the novel AAM aircraft, such as Joby, Wisk, Archer, EHang, etc.

1. Cameras and Visual Sensors

Visual sensors are a cornerstone of autonomous eVTOL operations because they provide rich situational awareness and centimeter-level precision without depending on external navigation infrastructure. In eVTOL missions, onboard cameras support critical perception tasks such as pad detection, obstacle avoidance, and precision landing, where radar or GPS alone may fail due to multipath interference, urban canyon effects, or satellite denial. The motivation for using visual sensing systems stems from their ability to emulate a pilot's perception while enabling real-time semantic understanding of complex urban environments. These sensors, when fused with inertial or LiDAR data, allow eVTOLs to identify landing zones, estimate motion during GNSS outages, and achieve safe autonomy under constrained weight and energy budgets. NASA's vision-based datasets demonstrate that camera-centric approaches can reconstruct reliable approach and landing trajectories even under variable illumination and cluttered rooftop environments [87]. Complementary research highlights that vision systems integrated with inertial and marker-based localization enable precise vertiport detection and multi-stage descent strategies that maintain sub-meter accuracy without GPS [88]. Furthermore, comprehensive reviews emphasize that vision and perception subsystems are indispensable for eVTOL autonomy, forming the sensory foundation for navigation, safety assurance, and decision-making across all phases of flight [89]. Table 7 demonstrates a mapping between sensing, perception, and the corresponding task. [90, 91] show real-world eVTOL operations at designated vertiports, illustrating how onboard visual sensing and scene understanding support safe approach and landing procedures in complex urban environments.

Existing Threats: NASA researchers formalized sensing and cybersecurity considerations for AAM vertiports, emphasizing that glass reflections, signage, and bright illumination can distort camera perception and compromise pad-detection accuracy [92]. Further studies quantified the impact of adverse lighting, rain, and specular reflections on VTOL vision-aided navigation and recommended multi-sensor redundancy to mitigate environmental degradation [93]. At the algorithmic level, physical adversarial patches and projected light patterns can mislead deep-learning detectors, showing that aerial vision models are susceptible to optical spoofing [94]. Universal adversarial patches capable of inducing false classifications across viewpoints have also been demonstrated [95], while vulnerabilities in multi-sensor fusion indicate that simultaneous camera–LiDAR attacks can corrupt integrated perception pipelines [96]. Even without adversaries, common corruptions such as blur, noise, and brightness shifts drastically degrade model accuracy, underscoring the brittleness of current vision models in real-world conditions [97]. Collectively, these studies establish that eVTOL vision systems are vulnerable to both natural interference and intentional optical deception. [98] introduced a scale-adaptive adversarial patch framework, called Patch-Noobj, which dynamically adjusts the patch size according to the aircraft's scale in the image to make the aircraft vanish from detection results. Unlike pixel-level digital

Sensing	Perception	Task
GPS – Provides absolute global position (latitude, longitude, altitude) used for georeferencing and navigation.	**Visual–inertial odometry (VIO)** – Estimates precise relative motion by fusing camera and IMU data to track position and orientation when GPS is unreliable.	**Path planning** – Generates safe, energy-efficient trajectories considering flight constraints and environmental conditions.
IMU – Measures linear acceleration and angular velocity for estimating attitude, velocity, and short-term motion dynamics.	**Semantic segmentation** – Classifies each pixel of an image into categories (e.g., sky, building, ground) to enable terrain and obstacle understanding.	**Landing guidance** – Identifies safe landing zones and aligns vehicle trajectory for vertical descent using fused sensor data.
Vision cameras – Capture high-resolution imagery for scene perception, localization, and visual tracking.	**Object detection** – Recognizes and localizes key objects (e.g., vehicles, people, obstacles) within the visual scene for safe maneuvering.	**Obstacle avoidance** – Detects, predicts, and re-routes around obstacles in real-time using fused visual and range data.
Ultrasonic, LiDAR, radar, or range sensors – Provide depth, distance, and velocity information for obstacle proximity and 3D environment reconstruction.	**Scene understanding** – Builds a high-level situational model of the environment by integrating semantic, geometric, and dynamic cues.	**Specified mission tasks** – Executes higher-level autonomous functions (e.g., inspection, delivery, surveillance) based on mission goals.

Table 7 Functional mapping of sensing, perception, and task modules in eVTOL and autonomous aerial systems.

noise, these physically printable patches can mislead detectors such as YOLOv3, YOLOv5, and Faster R-CNN, reducing the average precision by up to 48 percent across multiple datasets. This attack demonstrates that eVTOL vision modules relying solely on CNN-based object detection could be compromised by small, visually innocuous overlays. They also illustrate how clean aircraft detections are removed after applying such adversarial patches, underscoring a realistic threat to safety-critical perception systems.

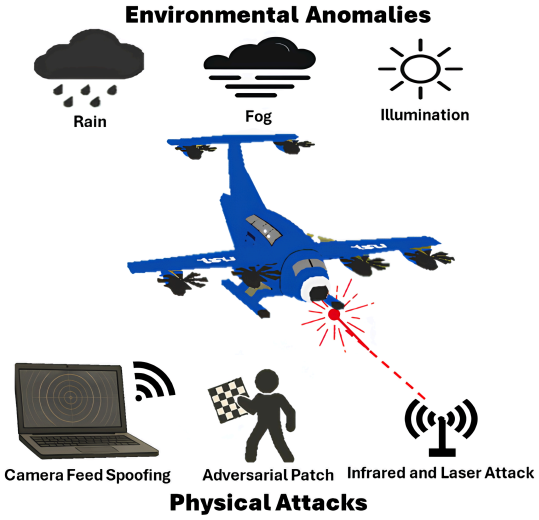

Fig. 4 Threat channels affecting eVTOL visual perception on approach.

Table 8 Command and control (C2) link threats across heterogeneous AAM networks.

Threat family	Scenario	Mitigation strategies
Availability	Selective jamming of 5G or A2G links during handovers disrupts control loops and triggers emergency loiter or diversion behaviors [112–114].	Dual-path diversity (for example 5G plus 5030–5091 MHz aviation channels) and spread-spectrum or beamforming techniques for robust links [115–117].
	Frequent handovers and roaming at low altitude introduce timing vulnerabilities and gaps [113].	Empirical characterization of handover behavior and robust fallback modes that maintain safe loiter or return-to-home behavior.
Integrity	Adversary manipulates or delays control commands by exploiting weak authentication or freshness guarantees in 5G or A2G protocols [118, 119].	Authenticated encryption with AEAD, DTLS or TLS with secure time sources, and strong anti-replay windows [120, 121].
	Misconfigured network slices or roaming policies introduce unexpected latency spikes or expose C2 traffic to untrusted domains [113, 119].	Slice binding and policy-controlled roaming that cryptographically ties credentials to authorized slices and operators [122, 123].

Defense Mechanisms: To counter these vulnerabilities, several researchers have advanced system-level and model-level defenses. A LiDAR–Camera cross-verification framework was proposed to detect spoofing through geometric consistency checks [99]. The Vision-Based Distributed Sensing (VIDIS) architecture integrates multiple cameras and inertial units to maintain pad visibility under illumination changes [100], while complementary work extended this into a distributed vertiport sensor network fusing radar, IMU, and camera data for integrity monitoring [101]. Explainable-AI-driven, certifiable fusion designs suitable for Size, Weight, and Power (SWaP) constrained avionics have been explored [102, 103]. Corruption-aware training via AugMix improves baseline robustness [104], and out-of-distribution screening through Outlier Exposure and energy-based anomaly detection provides complementary safety layers [105, 106]. To defend against localized tampering, PatchGuard [107] and PatchCleanser [108] restrict receptive-field influence and provide provable robustness guarantees. Addressing supply-chain threats, Neural Cleanse identifies and mitigates backdoor attacks [109], while STRIP offers runtime trojan detection [110]. Together, these contributions outline a layered perception-security paradigm encompassing cross-sensor verification, robust model training, anomaly detection, and integrity auditing.

Gaps and Open Problems: Despite this progress, open challenges persist. No standardized AAM benchmarks currently evaluate perception under combined environmental, adversarial, and multi-modal perturbations. Certification procedures for machine-learned defenses remain undefined [102, 103], while regulatory frameworks such as FAA and EUROCAE focus on lighting and geometry but omit adversarial validation criteria. The field therefore lacks eVTOL-specific datasets and evaluation protocols that integrate weather, motion, and spoofing factors. Moving forward, researchers and regulators must jointly establish explainable and certifiable fusion frameworks supported by benchmark-driven robustness metrics and dynamic trust scoring to ensure safe, verifiable visual perception in Advanced Air Mobility operations [111].

2. Command/Control (C2) Link Attacks

Existing Threats: The command-and-control (C2) link in UAM operations is a crucial channel that transmits important information from the ground control to an automated aircraft (e.g. Wisk's aircraft), such as flight plan updates, contingency commands, etc. These C2 links may incorporate diverse communication infrastructures, including cellular networks (4G/5G), aviation-specific air-to-ground (A2G) channels, and satellite communication (SATCOM) systems [112, 113]. This multi-link configuration enhances connectivity but expands the cyber attack surface, as any active bearer can become a target for jamming, spoofing, or session hijacking.

A primary threat concerns availability attacks through continuous or reactive jamming. Selective interference, especially during handovers between cellular and aviation links, can interrupt control loops or trigger automated autopilot fallbacks such as loiter, divert, or return-to-home maneuvers [114]. Even though the Federal Aviation Administration (FAA) and International Telecommunication Union (ITU) have reserved the 5030–5091 MHz band for AAM C2 operations [115], many early UAM concepts depend on commercial or unlicensed spectrum for redundancy and cost efficiency [116]. An adversary equipped with modest radio-frequency (RF) capability can exploit these channels by raising the noise floor or selectively jamming uplink control packets. In addition, in low altitudes, the aircraft experience frequent handovers and roaming across network providers. In addition, brief synchronization loss or misconfigured 5G network slices can introduce unacceptable latency or control gaps for UAM systems [113].

Integrity and confidentiality attacks are also equally significant. Weak freshness guarantees or missing authentication in 5G or A2G protocols invite replay, man-in-the-middle (MitM), or impersonation attacks [118, 119]. A compromised

Table 9 Telemetry data links for eVTOL fleets: potential risks and early defense concepts.

Concern	Implication and mitigation
Dependence on heterogeneous networks	Telemetry often traverses airport networks, public clouds, and vendor platforms, creating a broad attack surface [91, 124]. Network segmentation and system hardening are recommended to isolate telemetry paths from general IT infrastructure [124].
Indirect effects of avionics bus attacks	ARINC 429 flooding can suppress or delay navigation or system-status data which may feed ground telemetry streams [125]. Bus monitoring, rate limiting, and redundant channels can help preserve critical data under denial-of-service conditions [125].
Lack of demonstrated telemetry-specific attacks	Existing work highlights telemetry as a potential target but provides no experimental exploitation of eVTOL links [124]. Encrypted telemetry with authentication and anti-replay, along with anomaly detection based on baseline cross-checking, offers a forward path [126].

ground gateway could inject delayed or falsified commands, while an adversary positioned between network nodes might suppress critical alerts or modify telemetry streams. These vulnerabilities underscore the absence of a unified, aviation-grade security baseline for C2 link.

Defense Mechanisms: Defending the C2 channel requires coordinated safeguards across the radio, network, and protocol layers. At the physical layer, radio-link robustness can be enhanced through spread-spectrum signaling, adaptive beamforming or null-steering, and dual-path diversity (e.g., 5G + dedicated A2G), as recommended in recent AAM communications resilience studies [117]. Such diversity enables graceful degradation rather than total control loss during interference. At the data-link and transport layers, authenticated encryption with anti-replay protection should be mandatory. Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) using Authenticated Encryption with Associated Data (AEAD), coupled with secure time sources, can ensure both confidentiality and freshness in control messages [120]. In multi-operator networks, enforcing slice binding and policy-controlled roaming helps preserve end-to-end trust. By cryptographically binding each credential to an authorized network slice and disallowing roaming beyond approved domains, the system can prevent cross-operator spoofing and hijacking attacks [122]. Together, these measures provide layered assurance against interference, replay, and unauthorized control insertion.

Gaps and Open Problems: Despite ongoing standardization efforts, there is limited vendor-neutral data on handover reliability for low-altitude, high-mobility eVTOL operations. Public datasets covering link transitions at urban altitudes and speeds remain scarce, making it difficult to certify acceptable fallback or recovery behaviors across heterogeneous network providers [123]. Additionally, there is no harmonized definition of certifiable C2 fallback behavior across commercial, aviation, and satellite operators. Future work should prioritize empirical studies on link-layer resilience at eVTOL altitudes, formal definitions of fail-safe C2 states, and development of certifiable standards for secure handover and slice-based policy enforcement within the UAM communications architecture.

3. Telemetry Data Link Attacks

Existing Threats: Telemetry data links are communication channels that transmit real-time aircraft information, including position, speed, system status, navigation data, aircraft health status, battery information, and other sensor readings, between the aircraft and ground-based systems such as flight monitoring centers, air traffic management, or fleet operations platforms [124]. In eVTOL and urban air mobility (UAM) operations, telemetry links are critical for enabling autonomous flight management, collision avoidance, traffic coordination, and integration with airport networks and AAM ecosystems. Current literature does not report experimentally demonstrated telemetry data link attacks specifically targeting eVTOLs. The ARINC 429 study [125] shows that bus-flooding denial-of-service attacks can suppress navigation data in conventional avionics systems, which could indirectly affect telemetry streams if data is transmitted to ground operators. SkyGrid [91] and the PARAS report [124] highlight that telemetry links, particularly those dependent on cloud-based services or airport networks, represent potential cyber-attack surfaces. However, no actual attacks or incidents are documented, making this threat largely hypothetical.

Defense Mechanisms: While direct telemetry attacks on eVTOLs have not been demonstrated, several defensive strategies are suggested in the literature. SkyGrid [91] emphasizes the use of secure communication frameworks, including encryption, authentication, and resilient cloud-based protocols, to protect the integrity and confidentiality of

Table 10 Navigation database risks for low-altitude eVTOL operations.

Element	Risk / Impact	Mitigation
Vertiport and corridor records	Incorrect pad coordinates or corridor definitions may route aircraft into obstacles or restricted zones.	Provider-side cybersecurity, provenance tracking, and validation of nav-data layers [91, 127–129].
3D obstacle and terrain models	Manipulated obstacle/terrain data can hide structures or degrade separation margins.	Strong cloud-side data handling, airport network protections, and onboard plausibility checks [91, 124].
Onboard nav-database handling	Corrupted or incomplete updates cause inconsistent or unsafe procedures.	Integrity checks comparing new updates to trusted baselines; automatic rejection and rollback [126].
Data-bus transport (ARINC 429)	Bus-level DoS delays or blocks internal nav-data transfers.	Bus health monitoring, rate limiting, and redundant avionics networks tailored for eVTOL [125].

telemetry data. Also [124] recommends network segmentation and system hardening to isolate telemetry networks from broader airport IT systems and to enable monitoring for anomalous traffic. ARINC 429 [125] implies that redundancy, rate limiting, and bus-monitoring mechanisms could help mitigate potential denial-of-service disruptions that affect telemetry. Additionally, techniques from US Patent [126], such as cross-checking incoming data against trusted baselines, could be adapted to monitor telemetry streams for anomalies, although these methods have not been specifically validated in eVTOL operations.

Gaps and Open Problems: There is no unified standard or certification guidance for secure telemetry operations or onboard anomaly detection in eVTOLs. The end-to-end telemetry chain in eVTOLs involves heterogeneous networks, including onboard avionics buses, wireless communication links, and cloud services, and the literature notes that protecting this integrated system remains an open challenge [91, 124]. Finally, proposed defense techniques such as encryption, redundancy, or baseline verification have not been validated in operational eVTOL systems or tested against realistic threat scenarios. Overall, telemetry links are recognized as critical for eVTOL operations, yet both threat evaluation and standardized defense mechanisms remain largely unexplored areas for future research in urban air mobility (UAM) cybersecurity.

C. Dataset and data stream attacks

1. Attacks on the Navigation Database (Data Attacks)

Existing Threats: The eVTOL navigation database is a specialized digital dataset designed to support safe, automated, and efficient flight in UAM environments. It incorporates traditional aviation data such as waypoints, airspace boundaries, airports, navaids, and standard procedures, while also integrating UAM-specific elements, including vertiport locations, designated sky corridors, detailed 3D obstacle maps (buildings, power lines, bridges, cranes), geofenced no-fly zones, micro-weather layers, and energy-based routing information for electric propulsion. Because eVTOLs operate at low altitudes in dense urban areas, these databases must include high-resolution terrain and obstacle models, dynamic operational restrictions, and real-time updates. Major providers adapting their datasets for eVTOL operations include Jeppesen [127], Lido Navigation [128], and Navblue [129], alongside emerging UAM data and traffic management suppliers such as Altitude Angel, SkyGrid, and ANRA Technologies. Despite the rapid growth of eVTOL and UAM systems, there is a notable lack of publicly available reports or academic studies demonstrating attacks specifically targeting navigation databases for these aircraft. Nevertheless, some sources, such as US Patent [126], describe methods for detecting and mitigating tampering of flight management system (FMS) navigation databases. Although the patent is not eVTOL-specific, the underlying technology—digital navigation databases, waypoints, and terrain/obstacle data—is also utilized in eVTOL systems, suggesting that database manipulation or corruption attacks could plausibly occur in this context. Similarly, while the ARINC 429 cyber-vulnerability study does not address eVTOLs directly, many eVTOL designs employ ARINC 429 for avionics communications. This implies that bus-flooding denial-of-service attacks, as demonstrated in the study[125], could technically affect eVTOL systems relying on the interface.

Defense Mechanisms: Several sources highlight the need for stronger cybersecurity practices, but few offer concrete, technically validated defenses for protecting onboard navigation databases. SkyGrid's white paper emphasizes the importance of *modern, cloud-centric cybersecurity frameworks* to protect the third-party navigation, routing, and UTM services on which eVTOLs depend [91]. Their analysis identifies cloud service providers as high-value targets

Table 11 Cloud-centric AAM ecosystem: risks at the PSU, SDSP, and API boundary.

Actor / interface	Role in AAM architecture & cybersecurity concern	Mitigation and references
Provider of Services for UAM (PSU)	Manages flight intents, approval, and strategic deconfliction for eVTOL operations [7, 130]. Compromised credentials or replayed tokens allow flight-plan manipulation or large-scale service disruption [131, 132].	Strong authentication and encryption (OAuth2 authorization, mutual TLS, and cryptographically signed payloads with bounded freshness) ensure that only verified entities exchange valid, non-replayable data [121, 133].
Supplemental Data Service Providers (SDSPs)	Supply weather, traffic, terrain, and constraint layers consumed by PSUs and operators [7]. Poisoned or stale data can mislead routing and conflict detection across fleets [131, 134].	Redundancy and cross-validation among SDSPs and PSUs improve integrity by comparing rapidly changing inputs to flag inconsistencies [134]. If mismatches occur, graceful degradation reverts to the last known good state.
Provider APIs and shared cloud infrastructure	Provider APIs connect aircraft, operators, PSUs, SDSPs, and vertiports [130]. Insecure or deprecated API calls resemble connected-EV vulnerabilities, enabling data exfiltration or control overreach [135]. Cloud coupling can propagate cascading failures across operational domains [131].	Secure API gateways, unified authentication/authorization, and immutable audit logs for forensic readiness [131, 134]. Long-term challenges include certifiable, scalable cloud architectures integrating provenance tracking and redundancy-aware validation.

and stresses the need for resilient authentication, continuous monitoring, and strict data-handling controls to prevent manipulation of navigation or routing data delivered to aircraft. Similarly, [124] warn that the increasing integration of eVTOLs with airport IT networks expands the cyber attack surface and requires improved network segmentation, data governance, and system hardening to protect critical operational data flows. The ARINC 429 denial-of-service study demonstrates the feasibility of bus-flooding attacks that can suppress or delay navigation information on conventional aircraft data buses [125]. While not developed for eVTOL platforms, this work implies that eVTOL architectures relying on ARINC 429 may require rate limiting, bus health monitoring, and redundant communication channels to mitigate similar disruptions. The US patent, [126], on navigation database tampering proposes onboard integrity checks that compare incoming aeronautical data with trusted baselines to detect corruption or unauthorized modification of FMS navigation datasets. These techniques represent promising building blocks for eVTOL navigation-data protection, but lack specific validation or certification guidance.

Gaps and Open Problems A gap in current research and industry practice is the absence of a unified, trusted provenance and integrity-assurance standard for eVTOL navigation data. While existing providers such as Jeppesen [127], Lido [128], and Navblue [129] supply high-quality aeronautical datasets, there is limited publicly available guidance on guaranteeing the authenticity, lineage, and tamper resistance of the expanded UAM-specific data layers they now include (e.g., 3D city models, sky corridors, geofencing constraints). A related open problem is the lack of certification requirements or technical standards for onboard auto-rejection logic capable of detecting and rejecting corrupted, manipulated, or inconsistent navigation database entries.

D. Cloud security concerns with AAM architecture and service providers

1. AAM Architecture and eVTOL–Cloud Interactions (PSUs, SDSPs, Provider APIs)

AAM systems, particularly those involving eVTOL aircraft, operate within a distributed digital ecosystem that depends heavily on cloud-based infrastructure. These systems support mission-critical functions such as flight plan approval, real-time conflict monitoring and alerting, weather forecast, and data exchange among diverse stakeholders. Unlike traditional aviation which has been dominated by centralized FAA control and fixed communication channels, the emerging AAM framework adopts a decentralized, service-oriented architecture [7].

Within this model, several cloud-dependent entities play key operational roles. Providers of Services for UAM (PSUs) manage flight plans and strategic deconfliction, ensuring coordinated airspace use. Supplemental Data Service Providers (SDSPs) supply vital information such as weather updates, traffic surveillance, and terrestrial obstacle data, often distributed via Discovery and Synchronization Services. Meanwhile, Provider APIs serve as the connective framework, facilitating secure communication between PSUs, SDSPs, eVTOL aircrafts, and ground systems [130]. Each link in this interconnected chain—from an aircraft's onboard system to PSU and SDSP cloud interfaces—represents a potential cybersecurity exposure that must be carefully managed.

Existing Threats: Interactions between eVTOL aircraft and third-party cloud services expand the potential attack surface, exposing AAM infrastructure to familiar but high-impact cybersecurity threats. These include man-in-the-

middle exploits, credential theft, data replay, and spear-phishing attacks capable of manipulating or corrupting critical operational data [131]. For instance, compromised access credentials or replayed authentication token could allow attackers to infiltrate PSU networks, inject unauthorized commands, or alter flight data in real time [130]. Such breaches could disrupt mission operations—grounding entire eVTOL fleets or preventing authorized flights from departure [132].

Provider APIs, which enable cross-system communication, also present a well-documented vector for exploitation. Vulnerabilities common in other connected electric vehicle (EV) platforms, such as deprecated or poorly secured API calls, could similarly be leveraged in AAM contexts to exfiltrate sensitive operational data or compromise flight integrity [135]. These risks highlight the urgent need for rigorous authentication, continuous monitoring, and standardized cybersecurity frameworks across all cloud interaction layers within the AAM ecosystem.

Defense Mechanisms: AAM architectures can mitigate these threats through layered, standards-based security protocols. Strong authentication and encryption—such as OAuth2 authorization, mutual Transport Layer Security, and cryptographically signed payloads with bounded freshness [121, 133]—help ensure that only verified entities exchange valid and non-replayable data. Redundancy and cross-validation among PSUs and SDSPs further enhance integrity by comparing time-sensitive inputs (e.g., weather, flight intents, and airspace constraints) to identify inconsistencies or stale updates before they propagate through the system [134]. In cases of service disruption or data mismatch, graceful degradation mechanisms allow eVTOL management systems to revert to the last known good state, defer new commitments, and alert human supervisors—while maintaining immutable audit trails to support post-incident forensics and traceability.

Gaps and Open Problems: The AAM ecosystem lacks a unified, certifiable framework for trusted data exchange across service providers. Current FAA specifications define functional APIs and message formats but do not prescribe verifiable provenance, redundancy validation, or freshness requirements for data originating from PSUs, SDSPs, or third-party clouds [7]. This absence complicates certification of safety-critical cloud services and prevents end-to-end assurance that flight systems consume authentic, timely information.

Moreover, as illustrated in Figure 1, cloud connectivity through PSUs and SDSPs forms the critical information backbone linking UAM vehicles, operators, vertiports, and regulatory oversight. Compromised cloud channels can therefore amplify vulnerabilities across multiple operational domains simultaneously, yet no framework currently exists for reasoning about cascading failures or cross-system attack propagation through shared cloud infrastructure. Developing scalable, certifiable architectures that integrate provenance tracking, redundancy verification, cross-system integrity checks, and latency-aware security remains an open challenge for safe AAM deployment at scale.

IV. Conclusion

The expansion of AAM and eVTOL technologies represents a major step toward more automated, connected, and digitally dependent air transportation. As these systems evolve, their safety and reliability will increasingly depend on how well emerging cyber-physical risks are understood and addressed. This paper examined the primary vulnerabilities affecting modern aerial platforms and outlined the technical and procedural measures that can strengthen their resilience.

Looking ahead, several areas demand urgent attention. First, the continued reliance on unauthenticated surveillance channels such as Mode S, SSR, and ADS-B remains a critical exposure for collision avoidance and traffic coordination. Second, GNSS jamming and spoofing present a high-impact threat for eVTOL aircraft navigation in dense urban environments, where loss of positional integrity can rapidly lead to unsafe flight states. Third, the radio based voice communication, and communication channels for air-to-ground and air-to-air need to be secured. Fourth, the increasing dependence on camera-based perception and machine learning introduces new risks from adversarial manipulation, sensor degradation, and multi-modal spoofing. Fifth, cloud-connected AAM services, including PSUs and SDSPs, create systemic vulnerabilities that may propagate across fleets if provider APIs or synchronization services are compromised. Finally, electronic flight bags and onboard software supply chains require stronger guarantees of data provenance, update integrity, and device hardening to prevent operational misuse.

Addressing these risks will require close collaboration across avionic engineering, cybersecurity, flight operations, and regulatory communities, along with a commitment to integrating security and integrity safeguards into every stage of AAM system development, certification, and flight operation. As eVTOLs transition into everyday transportation systems, establishing trust in their digital resilience will be central to ensuring the safe and scalable deployment of future urban air mobility.

Acknowledgments

This material is based upon work supported by the NASA Aeronautics Research Mission Directorate (ARMD) University Leadership Initiative (ULI) under cooperative agreement number 80NSSC24M0070. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Aeronautics and Space Administration.

References

[1] Chancey, E., Politowicz, M., Buck, B., Ballard, K., Unverricht, J., Houston, V., Saephan, M., and Le Vie, L., "Foundational Human-Autonomy Teaming Research and Development in Scalable Remotely Operated Advanced Air Mobility Operations: Research Model and Initial Work," 2023. https://doi.org/10.2514/6.2023-1066.

[2] Maven Research Inc., "Optimal Locations for Air Mobility Vertiports," Tech. rep., NASA Aeronautics Research Mission Directorate, 2022. URL https://ntrs.nasa.gov/api/citations/20220005871/downloads/Final%20Report%20v2%20-%20ARMD%20Air%20Mobility%20Vertiports%20Maven%20Research%20Inc%2025JAN2022.pdf, contract NOIS2-049-RFTP.

[3] Antcliff, K., Borer, N., Sartorius, S., Saleh, P., Rose, R., Gariel, M., Oldham, J., Courtin, C., Bradley, M., and Roy, S., "Regional air mobility: Leveraging our national investments to energize the American travel experience," Tech. rep., NASA, 2021.

[4] Freeman, K., and Garcia, S., "A survey of cyber threats and security controls analysis for urban air mobility environments," *AIAA Scitech 2021 Forum*, 2021, p. 0660.

[5] Habler, E., Bitton, R., and Shabtai, A., "Assessing aircraft security: A comprehensive survey and methodology for evaluation," *ACM Computing Surveys*, Vol. 56, No. 4, 2023, pp. 1–40.

[6] Tang, A. C. B., "A Review on Cybersecurity Vulnerabilities for Urban Air Mobility," *NASA Secure Airspace*, 2020. NASA Ames Research Center.

[7] Federal Aviation Administration, "Urban Air Mobility (UAM) Concept of Operations Version 2.0," Tech. Rep. Version 2.0, U.S. Department of Transportation, Federal Aviation Administration, April 2023. Available online: https://www.faa.gov/sites/faa.gov/files/Urban%20Air%20Mobility%20%28UAM%29%20Concept%20of%20Operations%202.0_1.pdf.

[8] Zaid, A. A., Belmekki, B. E. Y., and Alouini, M.-S., "eVTOL Communications and Networking in UAM: Requirements, Key Enablers, and Challenges," *IEEE Communications Magazine*, Vol. 61, No. 8, 2023, pp. 154–160. https://doi.org/10.1109/MCOM.004.2300061.

[9] Wei, H., Lou, B., Zhang, Z., Liang, B., Wang, F.-Y., and Lv, C., "Autonomous Navigation for eVTOL: Review and Future Perspectives," *IEEE Transactions on Intelligent Vehicles*, Vol. 9, No. 2, 2024, pp. 4145–4171. https://doi.org/10.1109/TIV.2024.3352613.

[10] Ye, S., Wan, Z., Zeng, L., Li, C., and Zhang, Y., "A vision-based navigation method for eVTOL final approach in urban air mobility(UAM)," *2020 4th CAA International Conference on Vehicular Control and Intelligence (CVCI)*, 2020, pp. 645–649. https://doi.org/10.1109/CVCI51460.2020.9338487.

[11] Ippolito, C. A., Martin, R. A., Kawamura, E., Gorospe, G., Holforty, W., Kannan, K., Stepanyan, V., Lombaerts, T., Brown, N., and Dolph, C., "Enabling Smart Urban Airspaces through Distributed Sensing Technologies," *AIAA SCITECH 2025 Forum*, 2025, p. 0344.

[12] Li, X., Chen, L., Lu, Z., Wang, F., Liu, W., Xiao, W., and Liu, P., "Overview of jamming technology for satellite navigation," *Machines*, Vol. 11, No. 7, 2023, p. 768.

[13] Hu, H., and Wei, N., "A study of GPS jamming and anti-jamming," *2009 2nd international conference on power electronics and intelligent transportation system (PEITS)*, Vol. 1, IEEE, 2009, pp. 388–391.

[14] Team, G. P., "Global positioning system (GPS) standard positioning service (SPS) performance analysis report," *GPS Product Team: Washington, DC, USA*, 2014.

[15] Boquet, G., Vilajosana, X., and Martinez, B., "Feasibility of Providing High-Precision GNSS Correction Data through Non-Terrestrial Networks," *IEEE Transactions on Instrumentation and Measurement*, 2024.

[16] Um, I., Park, S., Kim, H. T., and Kim, H., "Configuring RTK-GPS architecture for system redundancy in multi-drone operations," *IEEE Access*, Vol. 8, 2020, pp. 76228–76242.

[17] Altaweel, A., Mukkath, H., and Kamel, I., "GPS spoofing attacks in fanets: A systematic literature review," *IEEE Access*, Vol. 11, 2023, pp. 55233–55280.

[18] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., and Lachapelle, G., "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, Vol. 2012, No. 1, 2012, p. 127072.

[19] Rhudy, M., Gross, J., Gu, Y., and Napolitano, M., "Fusion of GPS and redundant IMU data for attitude estimation," *AIAA Guidance, Navigation, and Control Conference*, 2012, p. 5030.

[20] Opromolla, R., Fasano, G., Rufino, G., Grassi, M., and Savvaris, A., "LIDAR-inertial integration for UAV localization and mapping in complex environments," *2016 international conference on unmanned aircraft systems (ICUAS)*, IEEE, 2016, pp. 649–656.

[21] Petrlík, M., Krajník, T., and Saska, M., "LiDAR-based stabilization, navigation and localization for UAVs operating in dark indoor environments," *2021 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, 2021, pp. 243–251.

[22] Kim, H. T., and Kim, H., "Precise localization of a UAV with single vision camera and deep learning," *GLOBECOM 2020-2020 IEEE Global Communications Conference*, IEEE, 2020, pp. 1–6.

[23] Yol, A., Delabarre, B., Dame, A., Dartois, J.-E., and Marchand, E., "Vision-based absolute localization for unmanned aerial vehicles," *2014 IEEE/RSJ International Conference on Intelligent Robots and Systems*, IEEE, 2014, pp. 3429–3434.

[24] Zhou, Q., Li, Q.-S., Han, X.-L., Lu, B., Wan, J.-W., and Xu, K., "Improvement of GPS displacement measurement accuracy for high-rise buildings by machine learning," *Journal of Building Engineering*, Vol. 78, 2023, p. 107581.

[25] Brossard, M., Barrau, A., and Bonnabel, S., "AI-IMU dead-reckoning," *IEEE Transactions on Intelligent Vehicles*, Vol. 5, No. 4, 2020, pp. 585–595.

[26] Hofmann-Wellenhof, B., Lichtenegger, H., and Collins, J., *Global positioning system: theory and practice*, Springer Science & Business Media, 2012.

[27] Shamaei, K., Khalife, J., and Kassas, Z. M., "Exploiting LTE Signals for Navigation: Theory to Implementation," *IEEE Transactions on Wireless Communications*, Vol. 17, No. 4, 2018, pp. 2173–2189. https://doi.org/10.1109/TWC.2018.2789882.

[28] Khalife, J., Neinavaie, M., and Kassas, Z. M., "The First Carrier Phase Tracking and Positioning Results With Starlink LEO Satellite Signals," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 58, No. 2, 2022, pp. 1487–1491. https://doi.org/10.1109/TAES.2021.3113880.

[29] Nguyen, T. M., Zaini, A. H., Guo, K., and Xie, L., "An ultra-wideband-based multi-UAV localization system in GPS-denied environments," *2016 International Micro Air Vehicles Conference*, Vol. 6, 2016, pp. 1–15.

[30] Shule, W., Almansa, C. M., Queralta, J. P., Zou, Z., and Westerlund, T., "UWB-based localization for multi-UAV systems and collaborative heterogeneous multi-robot systems," *Procedia Computer Science*, Vol. 175, 2020, pp. 357–364.

[31] Chen, N., Fan, J., Yuan, J., and Zheng, E., "OBTPN: A vision-based network for UAV geo-localization in multi-altitude environments," *Drones*, Vol. 9, No. 1, 2025, p. 33.

[32] Barrington, S., Cooper, E. A., and Farid, H., "People are poorly equipped to detect AI-powered voice clones," *Scientific Reports*, Vol. 15, No. 1, 2025, p. 11004. https://doi.org/10.1038/s41598-025-94170-3, URL https://doi.org/10.1038/s41598-025-94170-3.

[33] Soltanieh, N., Norouzi, Y., Yang, Y., and Karmakar, N. C., "A Review of Radio Frequency Fingerprinting Techniques," *IEEE Journal of Radio Frequency Identification*, Vol. 4, No. 3, 2020, pp. 222–233. https://doi.org/10.1109/JRFID.2020.2968369.

[34] Rehman, S. U., Sowerby, K. W., and Coghill, C., "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, Vol. 80, No. 3, 2014, pp. 591–601. https://doi.org/https://doi.org/10.1016/j.jcss.2013.06.013, URL https://www.sciencedirect.com/science/article/pii/S0022000013001220, special Issue on Wireless Network Intrusion.

[35] Malik, A., and Rao, M., "Radio Frequency Interference, Its Mitigation and Its Implications for the Civil Aviation Industry," *Electronics*, Vol. 14, No. 12, 2025. https://doi.org/10.3390/electronics14122483, URL https://www.mdpi.com/2079-9292/14/12/2483.

[36] Federal Aviation Administration, "Advanced Air Mobility Implementation Plan," Tech. Rep. Version 1.0, U.S. Department of Transportation, Federal Aviation Administration, July 2023. Available online: https://www.faa.gov/sites/faa.gov/files/AAM-I28-Implementation-Plan.pdf.

[37] WG-112, "ED-305 | Information Security Guidance for VTOL and Collaborative Systems," Tech. rep., EUROCAE, 2025. Available online: https://www.eurocae.net/product/ed-305-information-security-guidance-for-vtol-and-collaborative-systems/.

[38] EUROCONTROL, "ACAS Guide: Airborne Collision Avoidance, Chapter "Future of Collision Avoidance: ACAS X"," Tech. rep., EUROCONTROL, December 2017. URL https://www.eurocontrol.int/sites/default/files/2019-03/safety-acas-2-guide.pdf, available from EUROCONTROL, Brussels, Belgium.

[39] Federal Aviation Administration, "Introduction to TCAS II Version 7.1," Tech. rep., Federal Aviation Administration (FAA), 2011. URL https://www.faa.gov/documentlibrary/media/advisory_circular/tcas%20ii%20v7.1%20intro%20booklet.pdf.

[40] Cybersecurity and Infrastructure Security Agency, "CISA Advisory ICSA-25-021-01: Traffic Collision Avoidance System (TCAS II)," , 2025. URL https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-01?utm_source=chatgpt.com, accessed: 2025-02-02.

[41] Strohmeier, M., Martinovic, I., and Lenders, V., "Securing the air–ground link in aviation," *The Security of Critical Infrastructures: Risk, Resilience and Defense*, Springer, 2020, pp. 131–154.

[42] Kuba, S., and Babiceanu, R. F., "Navigating Threats: A Vulnerability Analysis of TCAS Interaction with Other Aircraft Systems," *2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*, IEEE, 2024, pp. 1–6.

[43] Kochenderfer, M. J., Holland, J. E., and Chryssanthacopoulos, J. P., "Next-generation airborne collision avoidance system," 2012.

[44] Guendel, R. E., and Wu, S., "Collision Avoidance for Rotorcraft in Urban Airspace with ACAS Xr," *AIAA AVIATION FORUM AND ASCEND 2025*, 2025, p. 3668.

[45] Smith, M., Strohmeier, M., Lenders, V., and Martinovic, I., "Understanding realistic attacks on airborne collision avoidance systems," *Journal of transportation security*, Vol. 15, No. 1, 2022, pp. 87–118.

[46] Harman, W. H., "TCAS- A system for preventing midair collisions," *The Lincoln Laboratory Journal*, Vol. 2, No. 3, 1989, pp. 437–457.

[47] Smith, M., Strohmeier, M., Harman, J., Lenders, V., and Martinovic, I., "A view from the cockpit: Exploring pilot reactions to attacks on avionic systems," 2020.

[48] Federal Aviation Administration, "Advisory Circular AC 90-120: Operational Use of Airborne Collision Avoidance Systems," Tech. rep., U.S. Department of Transportation, Federal Aviation Administration, 2024. URL https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-120.pdf, sections 2.12.1.4–2.12.1.5, *ACAS Failures and Anomalies*.

[49] Pearce, B., et al., "Signal injection attacks on ADS-B: Analysis and detection," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 57, No. 5, 2021, pp. 3451–3464.

[50] Slimane, H., et al., "ADS-B vulnerabilities and countermeasures: A comprehensive survey," *Journal of Air Transport Management*, Vol. 104, 2022, p. 102203.

[51] Khan, M., et al., "A survey on ADS-B spoofing and detection methods for modern aviation," *Aerospace Science and Technology*, Vol. 150, 2024, p. 108216.

[52] Shang, B., Zhao, X., and Wang, J., "Multi-device spoofing attacks on ADS-B systems using SDRs," *IEEE/AIAA Digital Avionics Systems Conference (DASC)*, IEEE, 2019, pp. 1–10.

[53] Popper, C., and Capkun, S., "Investigation of signal manipulation attacks on ADS-B systems," *Proceedings of the ACM Conference on Wireless Network Security (WiSec)*, ACM, 2011, pp. 331–340.

[54] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., and Bellekens, X., "Cyber-security challenges in aviation industry: A review of current and future trends," *Information*, Vol. 13, No. 3, 2022, p. 146.

[55] Melnichuk, A., Nesterov, V., Sudakov, V., and Kirill, S., "Development of electronic flight bag software based on expert system for computing of optimal aircraft performance," *2019 Twelfth International Conference" Management of large-scale system development"(MLSD)*, IEEE, 2019, pp. 1–4.

[56] Bhardwaj, P., and Purdy, C., "Safety and human factors for electronic flight bag usage in general aviation," *2019 IEEE National Aerospace and Electronics Conference (NAECON)*, IEEE, 2019, pp. 181–184.

[57] Samosir, J., Sihombing, S., Kuntohadi, H., Kurniawan, J., and Akbar, A. N., "Effect of Effectiveness of Use of Electronic Flight Bags on Flight Safety at PT. Garuda Indonesia," *Annals of the Romanian Society for Cell Biology*, Vol. 25, No. 3, 2021, pp. 112–122.

[58] Mecham, M., "New 777 Introduces Electronic Flight Bag," *Aviation Week & Space Technology*, Vol. 157, No. 23, 2002, pp. 64–64.

[59] Marinos, N., "AVIATION CYBERSECURITY: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," 2020.

[60] ForeFlight LLC, "ForeFlight Mobile Electronic Flight Bag," , 2025. URL https://foreflight.com/products/foreflight-mobile/, screenshots retrieved from the ForeFlight Mobile product page.

[61] Lupidi, A., Lischi, S., Berizzi, F., Baldini, L., Facheris, L., Cuccoli, F., et al., "Contributing towards sustainable aviation through an electronic flight bag for processing signals from avionic polarimetric weather radars," *2015 International Symposium on Sustainable Aviation (ISSA)*, 2015.

[62] Zelazo, E., "An electronic flight bag for NextGen avionics," *Head-and Helmet-Mounted Displays XVII; and Display Technologies and Applications for Defense, Security, and Avionics VI*, Vol. 8383, SPIE, 2012, pp. 171–176.

[63] Chandra, D. C., Yeh, M., Riley, V., Mangold, S. J., et al., "Human factors considerations in the design and evaluation of electronic flight bags (EFBs): Version 2," Tech. rep., United States. Department of Transportation. Federal Aviation Administration, 2003.

[64] Suppiah, S., "Impact of electronic flight bag on pilot workload," Master's thesis, Embry-Riddle Aeronautical University, Daytona Beach, Florida, 2019.

[65] Lopes, N. M., Aparicio, M., and Neves, F. T., "Supporting situational awareness on aviation pilots: key insights affecting the use of electronic flight bags devices," *World Conference on Information Systems and Technologies*, Springer, 2022, pp. 93–101.

[66] Wolf, M., Minzlaff, M., and Moser, M., "Information technology security threats to modern e-enabled aircraft: A cautionary note," *Journal of Aerospace Information Systems*, Vol. 11, No. 7, 2014, pp. 447–457.

[67] Liu, C., Wang, B., Li, F., Tian, J., Yang, Y., Luo, P., and Liu, Z., "Optimal attack path planning based on reinforcement learning and cyber threat knowledge graph combining the ATT&CK for air traffic management system," *IEEE Transactions on Transportation Electrification*, 2024.

[68] Anonymous, "How Secure Are IFEC Systems?" 2017. URL https://interactive.aviationtoday.com/how-secure-are-ifec-systems/, retrieved from Aviation Today website.

[69] Partners, P. T., "EFB Tampering Part 1: Introduction and Class Differences," , 2023. URL https://www.pentestpartners.com/security-blog/efb-tampering-1-introduction-and-class-differences/, accessed: 2025-10-31.

[70] Partners, P. T., "EFB Tampering Part 2: Device Integrity," , 2023. URL https://www.pentestpartners.com/security-blog/efb-tampering-2-device-integrity/, accessed: 2025-10-31.

[71] Partners, P. T., "EFB Tampering Part 3: Take-Off (Pt.1)," , 2023. URL https://www.pentestpartners.com/security-blog/efb-tampering-3-take-off-pt1/, accessed: 2025-10-31.

[72] Partners, P. T., "EFB Tampering Part 3: Take-Off (Pt.2)," , 2023. URL https://www.pentestpartners.com/security-blog/efb-tampering-3-take-off-pt2/, accessed: 2025-10-31.

[73] Bitton, R., and Shabtai, A., "A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers," *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 3, 2019, pp. 1164–1181.

[74] True, W., Kilbourne, T., Roy, A., and Ghazavi, N., "Cybersecurity for flight deck data exchange," *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, IEEE, 2021, pp. 1–13.

[75] Truffer, P., Scaramuzza, M., Troller, M., and Bertschi, M., "Jamming of aviation GPS receivers: Investigation of field trials performed with civil and military aircraft," *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, 2017, pp. 1258–1266.

[76] Geister, R. M., Buch, J.-P., Niedermeier, D., Gamba, G., Canzian, L., and Pozzobon, O., "Impact study on cyber threats to GNSS and FMS systems," 2018.

[77] Shetty, S., "System of systems design for worldwide commercial aircraft networks," *at 26th International Congress of the Aeronautical Sciences*, 2008.

[78] Khan, R., McLaughlin, K., Laverty, D., and Sezer, S., "STRIDE-based threat modeling for cyber-physical systems," *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6. https://doi.org/10.1109/ISGTEurope.2017.8260283.

[79] Howard, M., and Lipner, S., *The security development lifecycle*, Vol. 8, Microsoft Press Redmond, 2006.

[80] Okafor, C., Schorlemmer, T. R., Torres-Arias, S., and Davis, J. C., "SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties," *Proceedings of the 1st ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED)*, 2024, pp. 15–24. https://doi.org/10.1145/3560835.3564556.

[81] Martínez, J., and Durán, A., "Software Supply Chain Attacks — A Threat to Global Cybersecurity: SolarWinds' Case Study," *International Journal of Security and Its Applications*, Vol. 15, No. 5, 2021, pp. 123–136. https://doi.org/10.18280/ijsse.110505.

[82] Welsh, B., Finnsson, J., Stefánsson, S., and Neukirchen, K., "Towards Socio-Technical Topology-Aware Adaptive Threat Detection in Software Supply Chains," *CoRR*, Vol. abs/2510.21452, 2025. ArXiv:2510.21452.

[83] Dong, X., Lee, H., Xing, W., Ahmed, M., and Avgoustakis, G., "The '4W+1H' of Software Supply Chain Security Checklist for Critical Infrastructure," *CoRR*, Vol. abs/2510.26174, 2025. ArXiv:2510.26174.

[84] No, H. W., and Cha, W. C., "A Study on Flight Crew's Resilient Behavior Through Integration of Safety-I and Safety-II: Analysis of Aviation Safety Cases," 2025.

[85] Ribarić, B. Z., Vasiljević, D., Vasiljević, J., and Mikanović, B. R., "Aviation Cyber Security," *Transport and Traffic Theory and Practice (TTTP)*, 2023. https://doi.org/10.7251/JTTTP2302037R, received: September 13, 2023; Accepted: September 29, 2023.

[86] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., and Thomas, C. B., "Mitre ATT&CK: Design and philosophy: Technical report," *He MITRE Corp*, 2018.

[87] Brown, N., Kawamura, E., Bard, L., Jaffe, A., Ringelberg, W., Kannan, K., and Ippolito, C. A., "Visual & inertial datasets for an eVTOL aircraft approach and landing scenario," *AIAA SciTech 2024 Forum*, 2024, p. 1386.

[88] Xiang, S., Ye, M., Zhu, S., Gu, J., Xie, A., and Men, Z., "A Multi-stage Precision Landing Method for Autonomous eVTOL Based on Multi-marker Joint Localization," *2022 IEEE International Conference on Robotics and Biomimetics (ROBIO)*, IEEE, 2022, pp. 1–6.

[89] Xiang, S., Xie, A., Ye, M., Yan, X., Han, X., Niu, H., Li, Q., and Huang, H., "Autonomous eVTOL: A summary of researches and challenges," *Green Energy and Intelligent Transportation*, Vol. 3, No. 1, 2024, p. 100140.

[90] GmbH, V., "Volocopter Demonstration Flight at Groupe ADP / Skyports Vertiport Testbed," https://www.volocopter.com, 2023. Accessed: 2025-11-16.

[91] SkyDrive, I., "SkyDrive SD-05 eVTOL at Urban Vertiport Demonstration," https://en.skydrive2020.com, 2024. Accessed: 2025-11-16.

[92] Mendonca, N., Murphy, J., Patterson, M. D., Alexander, R., Juarex, G., and Harper, C., "Advanced air mobility vertiport considerations: A list and overview," *AIAA AVIATION 2022 Forum*, 2022, p. 4073.

[93] Veneruso, P., Opromolla, R., Tiana, C., Gentile, G., and Fasano, G., "Sensing requirements and vision-aided navigation algorithms for vertical landing in good and low visibility UAM scenarios," *Remote Sensing*, Vol. 14, No. 15, 2022, p. 3764.

[94] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., and Song, D., "Robust physical-world attacks on deep learning visual classification," *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 1625–1634.

[95] Brown, T. B., Mané, D., Roy, A., Abadi, M., and Gilmer, J., "Adversarial patch," *arXiv preprint arXiv:1712.09665*, 2017.

[96] Cao, Y., Wang, N., Xiao, C., Yang, D., Fang, J., Yang, R., Chen, Q. A., Liu, M., and Li, B., "Invisible for both camera and LiDAR: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," *2021 IEEE symposium on security and privacy (SP)*, IEEE, 2021, pp. 176–194.

[97] Hendrycks, D., and Dietterich, T., "Benchmarking Neural Network Robustness to Common Corruptions and Perturbations," *Proceedings of the International Conference on Learning Representations*, 2019.

[98] Lu, M., Li, Q., Chen, L., and Li, H., "Scale-adaptive adversarial patch attack for remote sensing image aircraft detection," *Remote Sensing*, Vol. 13, No. 20, 2021, p. 4078.

[99] Zhang, H., Li, Z., Cheng, S., and Clark, A., "Cooperative perception for safe control of autonomous vehicles under lidar spoofing attacks," *arXiv preprint arXiv:2302.07341*, 2023.

[100] Kawamura, E., Kannan, K., Lombaerts, T., Stepanyan, V., Dolph, C., Brown, N., and Ippolito, C. A., "Vision-Based Distributed Sensing at Vertiports for Advanced Air Mobility and Urban Air Mobility Approach and Landing," *AIAA SCITECH 2025 Forum*, 2025, p. 0346.

[101] Ippolito, C. A., Martin, R. A., Kawamura, E., Gorospe, G., Holforty, W., Kannan, K., Stepanyan, V., Lombaerts, T., Brown, N., and Dolph, C., "Enabling Smart Urban Airspaces through Distributed Sensing Technologies," *AIAA SCITECH 2025 Forum*, 2025, p. 0344.

[102] Mishra, S., and Palanisamy, P., "Autonomous advanced aerial mobility—An end-to-end autonomy framework for UAVs and beyond," *IEEE Access*, Vol. 11, 2023, pp. 136318–136349.

[103] Hu, L., Yan, X., and Yuan, Y., "Development and challenges of autonomous electric vertical take-off and landing aircraft," *Heliyon*, Vol. 11, No. 1, 2025.

[104] Hendrycks, D., Mu, N., Cubuk, E. D., Zoph, B., Gilmer, J., and Lakshminarayanan, B., "AugMix: A Simple Data Processing Method to Improve Robustness and Uncertainty," *Proceedings of the International Conference on Learning Representations (ICLR)*, 2020.

[105] Hendrycks, D., Mazeika, M., and Dietterich, T., "Deep Anomaly Detection with Outlier Exposure," *Proceedings of the International Conference on Learning Representations*, 2019.

[106] Liu, W., Wang, X., Owens, J., and Li, Y., "Energy-based Out-of-distribution Detection," *Advances in Neural Information Processing Systems*, 2020.

[107] Xiang, C., Bhagoji, A. N., Sehwag, V., and Mittal, P., "{PatchGuard}: A provably robust defense against adversarial patches via small receptive fields and masking," *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 2237–2254.

[108] Xiang, C., Mahloujifar, S., and Mittal, P., "{PatchCleanser}: Certifiably robust defense against adversarial patches for any image classifier," *31st USENIX security symposium (USENIX Security 22)*, 2022, pp. 2065–2082.

[109] Wang, B., Yao, Y., Shan, S., Li, H., Viswanath, B., Zheng, H., and Zhao, B. Y., "Neural cleanse: Identifying and mitigating backdoor attacks in neural networks," *2019 IEEE symposium on security and privacy (SP)*, IEEE, 2019, pp. 707–723.

[110] Gao, Y., Xu, C., Wang, D., Chen, S., Ranasinghe, D. C., and Nepal, S., "Strip: A defence against trojan attacks on deep neural networks," *Proceedings of the 35th annual computer security applications conference*, 2019, pp. 113–125.

[111] Levitt, I., Phojanamongkolkij, N., Horn, A., and Witzberger, K., "Uam airspace research roadmap-rev. 2.0," 2023.

[112] Tang, Y., et al., "Cybersecurity Considerations for Urban Air Mobility," Tech. rep., NASA Ames Research Center, 2021. NASA Technical Report, UAM Cybersecurity Assessment.

[113] Stouffer, K., et al., "Communications, Navigation, and Surveillance (CNS) Architecture for Urban Air Mobility," Tech. rep., National Institute of Standards and Technology (NIST), 2020. NIST Technical Report.

[114] Kuba, S., and Babiceanu, R. F., "Navigating Threats: A Vulnerability Analysis of TCAS Interaction with Other Aircraft Systems," *AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*, IEEE, 2024, pp. 1–6.

[115] "Command and Control (C2) Link for Unmanned Aircraft Systems (UAS)," Tech. rep., Federal Aviation Administration (FAA), 2016. FAA Spectrum Designation 5030–5091 MHz for UAS C2.

[116] Ullah, I., Khan, S., and Alsaadi, F. E., "Leveraging 5G Communication for CNS in Urban Air Mobility: Challenges and Security Implications," *AIAA Aviation Forum*, AIAA, 2025.

[117] Smith, M., Strohmeier, M., Harman, J., Lenders, V., and Martinovic, I., "A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems," *IEEE/AIAA Digital Avionics Systems Conference (DASC)*, IEEE, 2020, pp. 1–10.

[118] Fonyi, B., Török, P., and Kovács, D., "Security of 5G-Enabled Communications for Aerial Mobility and Cooperative UAV Networks," *IEEE Aerospace Conference*, IEEE, 2024, pp. 1–10.

[119] Corporation, T. M., "Security Analysis of 5G Connectivity for Urban Air Mobility Systems," Tech. rep., MITRE Technical Report, 2023.

[120] Federal Aviation Administration, "Advisory Circular AC 90-120: Operational Use of Airborne Collision Avoidance Systems," Tech. rep., U.S. Department of Transportation, Federal Aviation Administration, 2024. URL https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-120.pdf, sections 2.12.1.4–2.12.1.5, ACAS Failures and Anomalies.

[121] Rescorla, E., "The transport layer security (TLS) protocol version 1.3," Tech. rep., 2018.

[122] Strohmeier, M., Martinovic, I., and Lenders, V., "Securing the Air–Ground Link in Aviation," *The Security of Critical Infrastructures: Risk, Resilience and Defense*, edited by G. Bóna, Springer, 2020, pp. 131–154.

[123] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., and Bellekens, X., "Cyber-Security Challenges in the Aviation Industry: A Review of Current and Future Trends," *Information*, Vol. 13, No. 3, 2022, p. 146.

[124] René Rieder, J., "Security Considerations for Advanced Air Mobility (AAM) Operations at Airports," PARAS Technical Report PARAS 0041, Burns Engineering, Inc., June 2023. URL https://www.sskies.org/images/uploads/subpage/PARAS_0041.AAMOperations_.FinalReport_.pdf, program for Applied Research in Airport Security, National Safe Skies Alliance.

[125] Trask, C., Movit, S., Clutter, J., Clark, R., Herrera, M., and Tran, K., "ARINC 429 Cyber-vulnerabilities and Voltage Data in a Hardware-in-the-Loop Simulator," *arXiv preprint arXiv:2408.16714*, 2024.

[126] Anonymous, "Data Corruption Detection in Navigation Databases," , 2020. URL https://patents.google.com/patent/US20200013243A1/en, describes detection and mitigation of tampering in flight management system navigation databases.

[127] "NavData – Aeronautical Navigation Data," https://ww2.jeppesen.com/navigation-solutions/navdata/, 2025. Accessed: 2025-11-21.

[128] Systems, L., "Lido Developer Portal: Easily accessible, high-quality aeronautical data," , 2024. URL https://cdn.lhsystems.com/2024-05/Lido_Developer_Portal.pdf, accessed: 2025-11-21.

[129] "Navigation+," https://www.navblue.aero/product/navigation-plus/, 2025. Accessed: 2025-11-21.

[130] Lewis, T., Ali, H., and Freeman, K., "Developing a Cybersecurity Architecture for Extensible Traffic Management (xTM)," *AIAA SCITECH 2025 Forum*, 2025, p. 2720.

[131] Freeman, K., and Garcia, S. W., "Immutable secure data exchange and storage for urban air mobility environments," *AIAA SCITECH 2022 Forum*, 2022, p. 1092.

[132] Samanani, S., "Implementing comprehensive cybersecurity to secure the Advanced Air Mobility Ecosystem," , May 2025. URL https://www.skygrid.com/implementing-comprehensive-cybersecurity-to-secure-the-advanced-air-mobility-ecosystem/.

[133] Campbell, B., Bradley, J., Sakimura, N., and Lodderstedt, T., "OAuth 2.0 mutual-TLS client authentication and certificate-bound access tokens," *Internet Requests for Comments, IETF, RFC 8705*, 2020.

[134] Zhong, J., Zhang, H., and Miao, Q., "Enhancing aircraft reliability with information redundancy: A sensor-modal fusion approach leveraging deep learning," *Reliability Engineering & System Safety*, Vol. 261, 2025, p. 111068.

[135] Saleem, B., Rehman, A., Hassan, M. A., and Muhammad, Z., "Cybersecurity Risks in EV Mobile Applications: A Comparative Assessment of OEM and Third-Party Solutions," *World Electric Vehicle Journal*, Vol. 16, No. 7, 2025, p. 364.