Safety and Security Considerations on the Airbus Wake Energy Retrieval Program "fello'fly"

Thomas Ewert and Nils Mäurer
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{thomas.ewert, nils.maeurer}@dlr.de

***Abstract*—Faced with climate change and global warming, the reduction of greenhouse gas emissions, such as carbon dioxide, is a modern day focus of politics, industry and society. The aviation industry, responsible for about 3.5% of worldwide greenhouse gas emissions, is currently heavily depending on fossil fuels. As such, efforts are made to move towards a sustainable green aviation and carbon neutrality. Projects undertaken by authorities, airlines or manufacturers vary from new technologies like electric propulsion or Sustainable Aviation Fuel (SAF), to adjustments of operating procedures such as the retrieval of wake energy. [22] One already tested Wake Energy Retrieval (WER) technology is Airbus' *fello'fly* project.**

Hereby, different aircraft are positioned closely together on intercontinental flights, such that the succeeding aircraft can benefit from upward air movement within the wake created by the preceding one. Flight trials conducted in 2021 have shown a significant opportunity to reduce fuel consumption and therefore the carbon dioxide emissions and costs on long-range flights. However, to benefit from wake energy requires a reduction in currently established safety distances between aircraft. As introduction into service is envisioned as early as 2025, the *fello'fly* system will be based on already existing technologies.

This paper focuses on possible safety and security implications created by this combination of reduced safety distances and reliance on legacy communication, navigation and surveillance technologies. First, regulations governing aircraft separation will be introduced, followed by an introduction to the concept of *fello'fly*. Furthermore, the paper offers an overview of the employed technologies and underscores their known cybersecurity vulnerabilities. The implications of using these systems alongside reduced separation in an evolving threat landscape are examined. The paper concludes by proposing necessary enhancements for a secure implementation of wake energy retrieval.

***Index Terms*—Wake Energy Retrieval, Air Traffic Management, Aeronautical Communications Security, Aircraft Separation**

I. Introduction

For decades in aviation history, aircraft performance and efficiency has been a major point of interest for aircraft designers and manufacturers [48]. With climate change being attributed to the human-made emission of greenhouse gases, such as carbon dioxide, the aviation industry has become of greater public focus, as it has been found to contribute up to 3.5% to the human-driven factors [41]. As current aircraft thrust generation is heavily depending on fossil fuels, the viability of alternative propulsion methods is being explored by both the research and industry sectors. As battery performance continues to advance, the potential use of electric engines in aviation is becoming increasingly compelling [24]. Further, the German Aerospace Center (DLR) and its partners are actively developing a hydrogen fuel-cell powered electric flight demonstrator, while Airbus has projected the use of liquid hydrogen as fuel replacement in its advances in decarbonization [3], [19].

Although these technologies may hold promise in reducing emissions in aviation, not all of them may be suitable for every application area, or they may require extended development periods.

One attempt to close this time gap are Sustainable Aviation Fuels (SAFs), which are often based on renewable bio-based resources or derived from synthesis and enable a reduction of CO2 emissions by 80% over the fuel's life cycle. Current fuel specification blending limits allow to mix conventional fuels up to 50% with SAF. Required changes to current aircraft design are being evaluated, but flights with 100% SAF have already been conducted and manufacturers strive for a final certification state by they year 2030. However, to this date, production of SAF is limited and it covers less than 0.1% of yearly consumed jet fuel. [2], [12], [39]

Therefore, a variety of projects are undertaken to reduce the amount of used fuel in the short term. In the past, nature has often been a source of inspiration for various innovations in aviation, with wingtip fences or winglets being an example, inspired by the way birds curl their wingtip feathers upward during flight [5]. This type of engineering, which comprises the study and attempted imitation of naturally occurring habits or characteristics, can be summarized by the term "biologically inspired engineering" - or biomimicry. As an example, Airbus is mimicking birds in programs to explore aero-elastic wing or enhanced wingtip designs to reduce energy consumption [1], while the operator Lufthansa Cargo is replicating the aerodynamic characteristics of a shark's skin using a foil to provide up to 3% in fuel savings [45].

Inspired by birds that achieve energy savings by flying in a V-shaped formation, Airbus is investigating the feasibility of applying a similar approach to aircraft. Lift generation results from creating a pressure differential over the wing surfaces, characterized by the lowest pressure on the upper wing surface and the highest pressure below the wing. This pressure variation causes the airflow behind the wing to roll up,

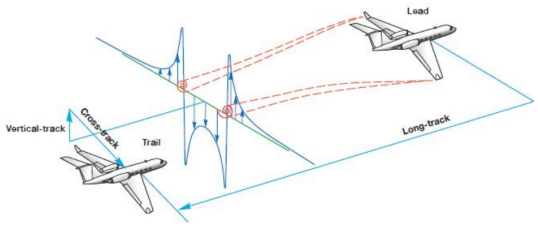

Fig. 1: Concept of *riding the wake* of previous aircraft [31]

creating swirling air masses that extend downstream. Directly following the generating aircraft, the roll-up region sees the wake from individual components undergo rapid changes as a result of self-induced velocities. Further along, the plateau region features vortices that either merge or stabilize when sharing the same rotation direction. Proceeding downstream, the decay region is where vortices gradually weaken due to factors such as viscosity or turbulence. Placing a trail aircraft wingtip into the section with continuous updraft, reduces the induced drag and consequently the amount of required fuel. [21], [26], [30]

This idea is approached in Airbus' program *fello'fly*, which foresees two aircraft flying in a formation allowing the trailing aircraft to benefit from the updraft created by its predecessor. To optimally utilize this wake energy, the following aircraft must be positioned much closer than the standard separation distance currently employed. As no new Communication, Navigation and Surveillance (CNS) systems are envisioned for its operation, guidance is achieved using legacy systems already in use today.

Within this paper, a possible introduction of the Airbus *fello'fly* system into the current CNS environment will be analyzed. First, an overview of current regulations governing aircraft spacing is given, followed by a detailed explanation of the step-by-step process involved in two aircraft flying in formation. The pertinent legacy CNS systems will be explained shortly along with an overview of their known security vulnerabilities. Throughout the discussion, known attacks will be applied to the *fello'fly* scenario and their potential impact on system reliability will be assessed. The paper concludes by addressing the changed threat landscape and suggesting necessary improvements of used technologies towards a more secure and safety-oriented implementation.

II. Background

In this chapter, regular spacing between aircraft in flight as well as the concept of Airbus "fello'fly" will be introduced.

A. Aircraft Spacing

The proposed technique to benefit from preceding aircraft's wake energy is requiring a certain longitudinal distance from another. To provide context, a brief explanation of the minimum spacing currently used for aircraft will be given. Historically, separation requirements between subsequent aircraft have their cause in either CNS, collision avoidance or reduction of wake turbulence encounters [15]. Different phases of flight require different minimum separations, which can further be influenced by the aircraft class, weight, relative speeds and flight paths of the involved aircraft [34], [36]. Since WER technologies are anticipated to be used in oceanic cruise operations [4], the following will primarily address the regulations related to the North Atlantic (NAT). Despite being the busiest oceanic airspace with more than 730,000 flights in 2017, Direct Controller Pilot VHF voice communication (DCPC VHF) or radar surveillance is not available in most areas. To accommodate and manage the high number of air traffic, certain operational procedures and standards are being developed by a dedicated NAT Systems Planning Group (SPG). [38]

The North Atlantic Organized Track System (NAT-OTS) offers a set of daily updated, pre-defined routes, which depend on prevailing meteorological conditions. While about 50% of traffic operates on those tracks, operators are only required to use them if their preferred flight path lies within the NAT-OTS area. With the introduction of the tracks, ensuring separation between aircraft traveling along adjacent routes for the entire oceanic crossing, the throughput of the airspace has been increased. [36], [43]

Further, different separation standards have been defined for aircraft operating within the NAT High Level Airspace (HLA). These standards establish the minimum horizontal and vertical distances between aircraft based on their navigation capabilities and the accessibility of surveillance data. As CNS systems have continued to improve, minimum distances could progressively be reduced. [37] To maintain safety and efficiency at the same time, Performance Based Communication and Surveillance (PBCS) criteria have been implemented within the NAT HLA. Performance of systems such as Automatic Dependent Surveillance - Contract (ADS-C) and Controller Pilot Data Link Communication (CPDLC) of FANS 1/A+ are being monitored against certain requirements (RCP 240 and RSP 180), allowing for a reduced lateral and longitudinal separation.

The ability for Air Traffic Services (ATS) to receive surveillance data, such as aircraft Automatic Dependent Surveillance Broadcast (ADS-B) signals via a network of Low Earth Orbiting Satellite (LEOS), has driven the motion to increase airspace efficiency even further. After having conducted trials in 2019, the Advanced Surveillance-Enhanced Procedural Separation (ASEPS) standards have now been implemented and published in the corresponding International Civil Aviation Organization (ICAO) documentations. [36]

The following summarizes the development of separation requirements over the North Atlantic. The analysis of mandated distances is limited to aircraft that are traveling on the same or parallel tracks with similar speeds, as the relation of flown track to each other, as well as level changes and speed differences, can affect these distances.

1) Vertical Separation: Vertical separation between aircraft varies with altitude, with separations of 1,000 ft below and 2,000 ft above Flight Level (FL) 290 [34]. Advances in altimeter accuracy as well as auto-flight, surveillance and

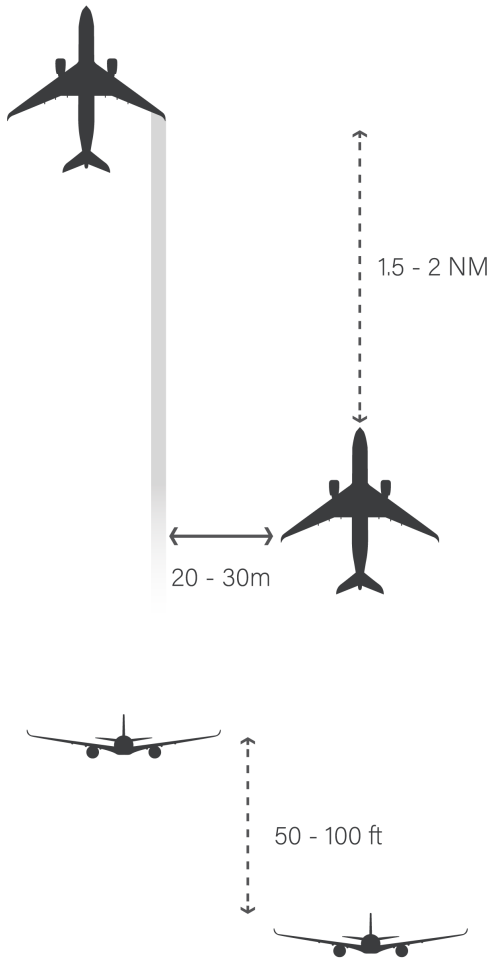

Fig. 2: Final aircraft spacing when the OPTI position has been reached.

alerting systems have led to the introduction of Reduced Vertical Separation Minimum (RVSM) airspace, providing a vertical spacing of 1,000 ft up to FL 410 inclusive [35]. Reduced vertical separation is applied within the NAT HLA airspace, while only RVSM approved aircraft are granted operation within [36].

2) Lateral Separation: Within the NAT, standard separation is defined as 60 Nautical Miles (NM) or 1 degree. To ensure that separation does not fall below 50.5 NM, the latter distance, which varies with latitude, is used as the reference point [23], [36]. Reductions are possible among aircraft fulfilling certain CNS requirements. 50 NM is required between Required Navigation Performance (RNP) 10 aircraft, which can be further reduced to 23 NM if PBCS criteria are fulfilled. Providing further availability of surveillance data, lateral separation can be minimized to 19 NM within the ASEPS concept. [36]

3) Longitudinal Separation: Aircraft flying on the same track over the NAT airspace have commonly been separated via the Mach Number Technique (MNT), in which pilots need to adhere to speed restrictions given by Air Traffic Control (ATC) [23]. A ten minutes spacing is hereby applied to aircraft travelling at the same speed, which can be reduced to five minutes if PBCS is fulfilled. Alternatively, in the latter case, certain mileage-based separation can be assigned, varying between 30 to 50 NM depending on the RNP capability and the ADS-C contract rate. Similarly to lateral minimum distances, introduction of ASEPS allows a reduction to as little as 14 NM. [36]

4) Summary: The current minimum distances can now be summarized as 14 NM longitudinally, 19 NM laterally as well as 1,000 ft vertically, while only one has to be fulfilled at the same time. The minima are based on the availability of ADS-B and performance based communication, navigation and surveillance systems.

B. Airbus Wake Energy Retrieval (WER)

The concept of WER goes back decades with different flight experiments and various used aircraft and technologies. The German Institute for Fluid Mechanics has conducted first trials in 1986 using DO-228, manually flown aircraft. In the beginning of the century, the National Aeronautics and Space Administration (NASA) Dryden Flight Research Center (DFRC), United States Air Force (USAF) Test Pilot School (TPS) and Boeing have conducted several tests, including Boeing F/A-18 Hornet and large military transport aircraft, such as the Boeing C-17. Various longitudinal spacing options have been examined, with separations surpassing a distance of over 10 wingspans classified as *extended formation*. Fuel savings have been noted, with greater reductions achievable when aircraft are in closer proximity. [30], [31]

Airbus has been working on its own implementation of a WER technology, which is marketed under the name *fello'fly*[1]. With the first flight trials in 2016 and multiple following in the past years, fuel savings from up to 10% could be demonstrated. In order for fello'fly to be implemented into the NAT airspace, a collaboration between Air Network Service Providers (ANSPs), Airlines, Airports and Airworthiness authorities is needed. The latter have, among other points, to adapt current regulations described in Chapter II-A to allow for reduced separations in formation flying. While different points still have to be addressed, the following will give a summary of the individual steps of the formation and the used CNS systems. [4]

1) Flying in Formation: The procedure for pairing two individual aircraft, the formation keeping, and separation will be briefly introduced in the following.

a) Rende-vouz: The preparation for a formation flight begins before takeoff, with airlines indicating their intention to participate in the program in the submitted flight plan. While initial pairing estimates can be made at this stage with the help of software, more precise matching is typically done after

[1]Please note that the details presented in this work regarding the *fello'fly* implementation are based solely on publications by Airbus, as the system itself is proprietary to the company. The authors do not have access to information regarding program logic or system design as they are not publicly available at the time of writing.

departure. If a suitable partner is located, the flight crew will receive information such as the starting waypoint and required flight levels. This can be communicated via ATC, which in turn can assign a specific time of arrival for, e.g., the oceanic entry point, in order to facilitate the pre-positioning. With formation flights covering over 2,000 nautical miles, it can even be efficient to adjust the speed of one aircraft if their initial distance does not exceed 50 nautical miles, leading to a *catch-up* of the follower. Flight automation is expected to assist during this maneuver, until the trailing aircraft reaches a position 1,000 feet below and 1.5-2 nautical miles behind the formation leader. This marks the completion of the *Rendevous* procedure, and separation is still within the regulatory minimums as described in section II-A.

b) Pre-OPTI Position: In order to start WER, responsibility for maintaining the separation is transferred from ATC to the two aircraft through custom pilot assistance functions. With the follower aircraft trailing the formation leader at a distance of 1.5 to 2 NM, it will now climb to a position on the same flight level, while shifting laterally to a distance of 300 meters from the leader's wingtip. At this point, there is no effect of any wake experienced. While own separation keeping is usual in visual flight conditions during, e.g., parallel approaches, *fello'fly* operates in Instrument Meteorological Conditions (IMC) and therefore does not require any visual contact with the leader. Separation is solely kept via the autoflight system and data received via the on-board CNS systems. The *pre-OPTI* position is also utilized in case of any abnormal situations occurring during formation flight or if maneuvers are anticipated from the formation leader. This is to ensure that unintentional crossing of the moving wakes is avoided.

c) OPTI Position: To retrieve energy from wakes, the aircraft will now move laterally closer to the leader's flight path until wakes are detected, which should occur at a lateral wingtip distance of around 20 to 30 meters. As the wakes descend, the follower's final position will also be adjusted vertically downward by roughly 50 to 100 feet, while small adjustments to keep the optimal positions will be continuously made. Overall, the distance between the two aircraft can be summarized as follows:

- vertical: 50 - 100 ft
- lateral: 20 - 30 meters (0.011 - 0.016 NM)
- longitudinal: 1.5 - 2.0 NM

Compared with the lowest separation minima from section II-A, this corresponds to a reduction of up to 90% longitudinally (i.e., absolute minimum of 14 NM compared to 1.5 NM in OPTI position). Airbus justifies this by the fact that the follower is equipped with autoflight systems, monitoring the leader's position and keeping the required distance automatically.

d) Breakaway: To provide the possibility of adequate separation between the aircraft in case of unanticipated events, such as system malfunctions or the need for flight path separation due to differing destinations, ATC allocates an empty flight level 1,000 feet beneath the formation. If such a situation arises, the follower aircraft should shift to the pre-OPTI position, descend to the lower level, and re-establish separation in compliance with existing regulatory requirements.

2) Utilized CNS Technologies: CNS, during the different phases in *fello'fly*, is based on currently available technologies. It is not foreseen, that any specialized systems, such as air-to-air data link communications within the formation, are needed.

Communication with ATC will take place via Very High Frequency (VHF) voice and CPDLC in the pre-oceanic airspace. With the availability of satellite-based data links, connectivity for CPDLC will be maintained, and High Frequency (HF) will replace VHF as a backup during the later stages of the flight. Typically in formation flights, only the leader communicates with ATC and can coordinate flight path changes within the formation using unoccupied VHF voice frequencies. With increasing usage of the *fello'fly* system, the availability of free voice channels might become a restricting factor.

The follower will change its active frequencies and conduct Selective Calling System (SELCAL) or SAT voice callback checks, similarly to the leader. However, since ATC will not issue direct instructions to the follower, the leader must ensure these instructions are relayed. In case of contact loss within the formation, ATC should still be able to able to reach the follower via a data link or HF connection, but establishing communication may take longer.

Navigation is based on common sources such as GPS and on-board inertial reference systems, while requirements by the current Flight Information Region (FIR) have to be observed.

Airspace surveillance and monitoring of aircraft within the formation are accomplished using standard transponder information, such as Mode S responses or ADS-B broadcasts. Although these systems can function similarly to current operations, modifications to on-board collision avoidance systems like Traffic Alert and Collision Avoidance System (TCAS) are necessary. Given the significantly reduced separation between the two aircraft, TCAS logic must be adjusted to accommodate this scenario and prevent false traffic resolution advisories. [4]

III. Method

The previous section has highlighted the concept of the *fello'fly* system. Currently planned implementations do not require any new communication systems but are relying upon existing technologies, such as VHF/HF voice and CPDLC for communications, ADS-B, SSR, TCAS and GPS for navigation and surveillance. Although various terms have been previously introduced already, this section provides a brief overview of the legacy systems' characteristics and security concerns, serving as a foundation for discussing potential risks associated with implementing WER operations using these systems. A more in depth analysis of the security of digital aeronautical communication can be found in [51].

1) VHF/HF Voice Communication: Voice communication is still providing the primary means of communication between aircraft and ATC. In regions where reception of the VHF signal is not possible, such as remote or oceanic air spaces, HF is available as a backup system. Frequency bands

assigned to VHF voice are situated between 117.975-137 MHz, while the HF range can be found from 2-30 MHz. Analogue VHF Double Side-Band Amplitude Modulation provides the communication technique, while authenticity or integrity protection has not been implemented [51]. Any individual with the required hardware, mostly available on the free market, can participate in the communication if the correct frequency is known. [51], [62]

Various incidents with spoofed voice communication have been documented already [6], [42], [53], with the potential to cause severe disruptions in air traffic services. Although an unauthorized person is usually quickly identified through discrepancies in voice and signal levels compared to regular controllers, future developments in artificial intelligence and the proliferation of *deepfake* technologies may hinder such detection [14], [62].

2) CPDLC: To address the growing issue of frequency congestion and mitigate transmission challenges associated with long-range HF communication, the CPDLC system was developed. While two different implementations, Future Air Navigation Systems (FANS) 1/A+ and ATN-B1 exist, only FANS 1/A+ is implemented over the NAT. It contains CPDLC as well as ADS-C and operates upon the Aircraft Communications Addressing and Reporting System (ACARS) network, which in turn provides two main data links, VHF Data Link mode 2 (VDLm2) as well as SATCOM via Iridium and Inmarsat. [25], [33], [51]

CPDLC allows the exchange of text-based messages and thus reduces required voice transmissions and miscommunication [27]. The protocol has not been designed with any security or privacy measures foreseen, and various studies and demonstrations have shown the susceptibility of the system to attacks such as message alteration or injection [27], [46], [57]. Similar is true for underlying VHF/HF data links, such as ACARS or VDLm2 [13]. To address those issues, the security framework ACARS Message Security (AMS) is specified and incorporates message authentication, integrity and confidentiality protection. However, due to higher service charges, it is hardly in use today [51]. Although satellite-based data links incorporate certain cybersecurity measures as well, their use is sometimes optional, or they are based on vulnerable technologies, such as 3rd Generation Public-Private Partnership (3GPP) 3G technologies combined with Inmarsat SB [51]. The authors of [59] have demonstrated that ACARS communication transmitted through satellite downlink can be decoded, thereby compromising the privacy of the information contained within. Depending on the used data link, communication via CPDLC can be seen as vulnerable to message alteration and injection as well.

3) Secondary Surveillance Radar (SSR): Within the domain of surveillance, primary radar, which relies on radio wave reflections from aircraft and calculates distance through runtime measurements, has been the principal information source for air traffic controllers. It is a non-cooperative position determination system, as it solely depends on the reflective surface and the available radiation power. However, due to potential errors like artifacts in radar imagery and diminishing accuracy as distance from the radar station increases, alternative technologies have been introduced. The SSR is a cooperative localization system which utilizes an interrogation and response scheme to provide more detailed information for the controller. Different modulations and frequencies are utilized for the two signals, with 1030 MHz allocated for interrogation and 1090 MHz for response. The initial transponder modes A and C transmitted only the assigned *squawk* code and pressure altitude. The more versatile data link extension, Mode S, enables ATC to request specific information in the aircraft's response, such as the selected altitude, and employs a globally unique aircraft identifier. [58], [62]

Despite its importance, since this system is largely the only source for extended information on air traffic, security has not been implemented and it is vulnerable to a variety of attacks such as message spoofing, injection or jamming [62]. As no authentication is in place, a malicious attacker could also send out unauthorized requests on the interrogation channel, leading to significant interference [50].

Real world incidents have also shown, that rogue interrogation can lead to transponders operating beyond their design limits resulting in a loss of signal and therefore disappearance in the radar image [20].

4) ADS-B Transmissions: To address the limitations of interrogations per second in Mode S transponders and in order to decrease traffic on the 1030 MHz channel, ADS-B was created as an extension to Mode S. Different implementations exists, but only the 1090ES (Extended Squitter) version is used in commercial airliners. Unlike Mode S operation, ADS-B transmits data at regular intervals, typically twice a second for velocity and position, and once every five seconds for identity information. It differs from traditional SSR that it does not require any interrogation, however is dependent on Global Navigation Satellite System (GNSS) based position. [51], [62]

ADS-B is crucial for air-traffic safety, requiring operational, performance, and security compliance. However, as it is based on the unsecured Mode S, it also inherits its vulnerabilities and therefore lacks essential security measures, including entity authentication, message signatures, and encryption. Additionally, it doesn't have challenge-response or ephemeral identifier mechanisms, leaving it vulnerable to replay and privacy tracking attacks. While a secure mode for Mode S/ ADS-B operation exists, it is currently only available to military users [17], [62].

Due to the regular broadcast, jamming an aircraft's ADS-B messages is simpler to do compared to Mode S' interrogation system with its irregular, directional antenna-based interrogations. Different studies have demonstrated the viability of conducting attacks against ADS-B using commercially available off-the-shelf hardware. These attacks involve inserting virtual aircraft into a controlled airspace, which are indistinguishable from genuine traffic at the link layer. More importantly, the modification of the ADS-B reported aircraft flight path is possible by selectively jamming a single aircraft's transmission and replacing it with a modified one, influencing the situational

awareness of controllers and adjacent flight crews. [17], [56], [62]

Instances of ADS-B data tampering have already been reported. Signals received by the aircraft tracking website *FlightRadar24* have inaccurately suggested that a WestJet flight was transmitting a distress transponder code, when in reality, no such event took place [11]. Moreover, the Federal Aviation Administration (FAA) has issued warnings about false ADS-B transmissions, which have previously resulted in the triggering of TCAS Random Accesss (RAs) [47].

5) TCAS: Transponder signals find application in TCAS, an airborne collision avoidance system which provides the flight crew with information about potential intruders and issues Traffic Advisories (TA) and Resolution Advisories (RA). The current version, TCAS II, is further capable of coordinating the direction of escape maneuvers with the involved aircraft. Simultaneously, the transponder also informs ATC that a RA is ongoing which prohibits the intervention of the controller. However, security vulnerabilities in the underlying transponder technology are hereby inherited to the higher level system as well. This is especially troubling, as modern airliners (such as the Airbus A350) have the ability to react to TCAS RA without any action by the flight crew needed [54]. Malicious tampering with such data over the radio link could therefore result in automatic system responses.

Studies have identified potential vulnerabilities that can be exploited using affordable Software Defined Radios (SDRs) [8], and attack demonstrations have been presented at international conventions like DEFCON [44]. Furthermore, researchers have analyzed potential deviations, and Smith et al. [58] discovered a theoretical success rate ranging from 44% to 79%, with an average deviation of 590 feet. With the knowledge of flight paths, extensions to attacks utilizing fake Mode S messages can be seen as a realistic attack vector [29].

6) GNSS: Different versions of satellite based navigation system exist, such as GPS (USA), Galileo (Europe) or Beidou (China). However, mainly Global Positioning System (GPS) is in use in the aviation industry today. Originally developed by the US military, it has become indispensable for various civilian applications. Position determination is based on the reception of multiple satellite signals and identifying the range to each one by the measurement of time delays. However, civilian GPS signals, which are neither encrypted nor authenticated, were not designed for safety- or security-critical applications but are now utilized heavily in applications such as aircraft navigation. [64] Various security research has shown the feasibility of jamming and spoofing attacks which can cause the GPS receiver to calculate an incorrect physical position [52]. GPS is used in modern aircraft for navigational purposes, but also in the surveillance broadcast of ADS-B. If the receiver is tricked into calculating a position different from the actual one, it may result in erroneous position reports by the affected aircraft. This, in turn, could potentially cause flight path deviations depending on the current navigation mode. While there have been numerous reports of spoofed GPS signals in the news, scientific approaches to externally alter the trajectories of both Unmanned Aerial Vehicles (UAVs) and a yacht have been demonstrated as well [10], [40].

IV. Results and Discussion

The previous section described that most of the CNS technologies utilized by fello'fly do not offer significant security features or enable direct air-to-air communication. Table I summarizes different vulnerabilities described in research, but also lists known real-world incidents. With this in mind, possible attacks on the underlying systems are transferred to a WER scenario. Further, possible events occurring during operation are compared to the available technologies.

A. Analysis of Possible Disruptive Events

We classify events that could interrupt the fello'fly operation as either accidental (internal) or deliberate (external).

1) Internal Interference: Disruptions resulting from unexpected malfunctions in aircraft equipment are considered internal, originating from the systems used during operation. This discussion focuses on components essential for maintaining formation, as there are numerous other systems that could prevent the formation from occurring in the first place. The following points serve as an example and are not exhaustive.

a) Equipment Failures: Due to the reduced distance in *fello'fly*, equipment malfunctions may present increased risks compared to standard operations. While voice or data link communication disruptions might not directly affect formation keeping, failure of surveillance equipment could lead to a loss of controlled separation. Some issues, such as GPS outages, may be subtle, but inconsistencies among different surveillance sources can lead to unexpected system responses.

Nonetheless, the cruising phase typically features stable flight conditions, allowing modern flight warning computers sufficient time to detect and address errors, such as by disengaging the formation if necessary.

b) Engine Failures: While aircraft engines have evolved over time, making Extended Range Twin Operations (ETOPS) operation possible, an engine failure in flight is still deemed critical. Most transport category aircraft cannot maintain cruising altitude with only one engine operating. The first effect would be a reduction in air speed, shortly after which a drift down has to be initiated to ensure the operational envelope is not left. Engine failures of the follower aircraft are hereby deemed less critical, as the formation would just be considered terminated and conventional ATC separation has to be achieved [4].

If the leader must take actions, the follower can only detect the motion through ADS-B broadcasts, as no air-to-air data link communication between the aircraft exist. While the occurring speed reduction will happen relatively quickly, depending on aircraft weight and altitude, we consider transmitted position updates every 0.5 seconds as frequent enough to give the following aircraft systems enough time to execute an evasive maneuver. Should the follower aircraft determine that the formation is broken and descend to a lower flight level, it may cause further separation reduction as the

TABLE I: Assumed CNS technologies in the Airbus fello'fly proposal with exemplary security vulnerabilities and incidents.

	VHF/HF voice	**CPDLC**	**SSR**	**TCAS**	**ADS-B**	**GPS**
Technology	Analog	Digital	Digital	Digital	Digital	Digital
Used in fello'fly	Communication for air-to-ground and air-to-air	Communication between ATC and leader aircraft	TCAS	Safeguard to other traffic and to aircraft in formation	Main source for position reports	position determination
Backup available	air-to-ground: data link air-to-air: no	yes: VHF/HF voice	partially ADS-B (depending on version of TCAS)	no	not with same accuracy	not with same accuracy
Attack described in	no exploit needed due to off-the-shelf hardware available	[27], [46], [55], [57]	[50]	[9], [28], [56], [63]	[17], [56]	[10], [40], [52], [64]
Incidents happened	yes [6], [42], [53]	none reported	yes [20]	yes [47]	yes [11], [47]	yes [10], [40]

leader aircraft is forced to descend through that flight level as well. Depending on the follower's initial maneuver, a TCAS RA could be activated, potentially conflicting with the desired actions in this situation.

c) Miscommunication: Aircraft in the formation mainly communicate via the VHF channel, which inherits basic difficulties of voice communication. Regional differences in accents of the English language, non-standard communication phrases or background noise could lead to misinterpretation of instructions. While ATC has the means to verify the correct execution of the instructions, the lead aircraft's pilots might be missing some information depending on the available cockpit displays. Due to the reduced separation, room for error is already reduced and small deviations might lead to the triggering of evasive maneuvers. While safety might be reduced but not impaired, passenger comfort might be negatively affected.

2) External Interference: Security vulnerabilities and associated attack vectors presented in previous chapter can be deployed against the *fello'fly* operation as well. As separation is based on software, acquiring all needed information automatically, tampering with the data might lead to severe safety implications.

a) Signal Jamming and Denial of Service: Denial of Service (DoS) attacks can substantially affect all CNS systems, with consequences resembling those of a system failure. However, detecting such events may prove more challenging than identifying a simple device outage. Flight warning computers can more easily recognize internal errors, but differentiating between a signal outage caused by failure in another aircraft and signal jamming may be more difficult. DoS attacks may also involve overwhelming receivers with seemingly legitimate messages. Depending on the device's properties, excessive throughput could lead to message loss or delays, which may be challenging to detect.

Through available signal jamming or DoS, an attacker could render the aircraft unable to determine their own or their partner's location. If the aircraft is not able to maintain a minimums separation based on the sensed wake, the formation would be flying "blind" at this point. Any not coordinated flight path parameter alterations of either aircraft could lead to a separation reduction below the minimums established for the operation. Jamming and outage detection capabilities have to be in place, which would require thoughtful designs to prevent frequently breaking the formation due to single interfered radio signals.

b) Signal Injection and Alteration: While jamming a signal alone might stay undetected for a period of time, especially in the cruise phase of a flight due to reduced pilot's vigilance, it should latest be discovered upon mandatory reporting events, by the absent of valid transmission or error indications in certain CNS systems.

Detecting spoofed or altered messages often requires that doubt is raised regarding their authenticity. Especially with subtle changes or instructions matching the current phase of flight, suspicion or system alerts might not be triggered quickly.

Voice communication via analog channels is prone to easy unauthorized message injection. Due to the vicinity of both aircraft, it is reasonable to assume, that the imitated aircraft receives the rogue transmission as well, which could raise attention with its flight crew. Nevertheless, an attack could use previous communication of the leader flight crew to train a voice imitation algorithm and, after successful insertion of the message, jam the channel. While the follower pilots can read back the instructions, the leader has no means to correct the illegal instructions via voice anymore.

Likewise, the transmission of unauthorized CPDLC messages could result in unintended crew or aircraft maneuvers. Since these transmissions are directed at a specific aircraft, they remain unnoticed by other flight crews in the formation. As a result, if no suspicion is raised regarding the instruction, such unauthorized messages may also go undetected.

Spoofing attacks on communication channels have in common, that due to required crew actions, pilots are given an opportunity to detect unusual patterns in transmitted messages, which may indicate unauthorized transmissions. Validating

the requested action against current mission parameters could prevent the execution of potentially harmful instructions. [55]

The situation differs when received signals are used to supply data to the aircraft's autoflight system. As described in Chapter III, all surveillance technologies used by fello'fly are vulnerable to message spoofing or alteration attacks. Previous research has demonstrated that altering flight paths in ADS-B transmissions is possible, and it is reasonable to assume that ADS-B will serve as one of the primary sources for position determination within the fello'fly system. While researchers at NASA have deemed the ADS-B channel as sufficient for WER operation, only the performance for position accuracy was considered in their flight trials. Affects by deliberate signal modifications have not been taken into account. [30] Similar signal alterations or replacements can be executed against the GPS signal, if the attacker manages to influence the position calculation by only one aircraft, i.e., through low transmission power from within the aircraft.

By selectively interfering with and modifying the leader's ADS-B transmissions, an attacker could deceive the follower into believing that the distance is increasing, prompting the follower to adjust its speed and inadvertently causing an actual loss of separation. A similar situation could arise if the follower's position determination is manipulated, leading it to believe it is falling behind in the formation. While TCAS remains active and can potentially resolve this situation through resolution advisories, a more calculated attacker may employ sophisticated combinations of attacks.

By altering both aircraft's ADS-B transmissions and tampering with transponder responses, the autoflight system could be deceived into thinking it is maintaining a valid formation, even as the actual separation continues to shrink. This could lead to an alarmingly close formation, jeopardizing the safety of all aircraft involved.

The presence of active TCAS systems in both participating aircraft may exacerbate the effects of previously demonstrated attacks. Any false resolution advisory achieved might be automatically triggered in both aircraft, potentially creating an avalanche effect in dense airspaces. While the TCAS operation ensures safe spacing from other aircraft during activation, disruptions to the WER procedure are likely to occur.

B. Attacker Model

To assess the probability of intentional interference during *fello'fly* operations, we have consolidated the prerequisites for a successful attack into three key criteria: the attacker's knowledge of the critical system, the equipment required to execute the plan, and the opportunity to carry out the attack.

1) Knowledge: The security vulnerabilities of the CNS systems in use have been extensively discussed in previous research, as illustrated in Table I. The relevant papers are publicly accessible on the Internet, and some attacks have even been explained and demonstrated on platforms like YouTube [44]. Tutorials, such as those provided by the Aerospace Village of DEFCON 28, further contribute to increased accessibility and reach [51]. Consequently, a potential attacker has the opportunity to acquire knowledge from an extensive collection of documents. Although some research may be over two decades old, it can still be considered current, as the analyzed systems have experienced minimal to no changes since then.

While research papers alone provide the necessary knowledge, translating theoretical vulnerabilities into functional software would typically require advanced engineering skills. However, the widespread availability of freely accessible code repositories and instructions has made this step unnecessary. Software for transmitting ADS-B Out messages [65], decoding 1090 MHz messages [18], and CPDLC encoders can be easily found through a simple Internet search.

As a result, the specific knowledge and skills required for carrying out an attack can be significantly reduced, depending on its complexity. This facilitates attacks by so-called "script kiddies," who merely utilize existing code without the need for additional expertise.

2) Equipment: With the use of cheap Commercial off-the-shelf (COTS) and Software Defined Radio (SDR), even layman adversaries may attack aeronautical communication services using the open source libraries and tutorials described above. Projects such as GNURadio [16] allow to build sending-blocks which can be used for aeronautical communication and thus possibly message injection. [51] Dropping costs to acquire sending equipment leads to less funding required and therefore a potential greater amount of possible attackers with varying backgrounds.

3) Opportunity: While signal alteration is feasible in all mentioned CNS systems, it still requires the attacker to be at least within line-of-sight of the formation. It can be argued, that due to the remote location of the oceanic airspace the presence of an attacker is unlikely. Nonetheless, some routes still pass through areas near inhabited locations, including regions in Greenland or Iceland. Further, similar to the reduction in cost for SDR equipment, the entry costs for unmanned drones have dropped significantly, imposing possible airborne attacks as well. Although the range of drones may not be sufficient to operate in close proximity to NAT airspace, high-altitude balloons drifting along jet streams could serve as platforms for potential attackers. Since aircraft typically seek jet streams depending on their travel direction, such devices could float in similar directions above traffic, awaiting suitable or specific aircraft to initiate an attack. Furthermore, due to the lack of primary radar coverage in most NAT areas, the detection of such threats could be impeded or delayed. Further, a highly motivated attacker might also bring the required equipment along as a passenger. Due to the proximity to the aircraft's antennas, lower transmission power is needed for a successful interference in this case.

Attacks of this nature do not need to last long to be effective. At an altitude of 36,000 ft under standard temperature conditions, the speed of sound is approximately 573 knots. By inducing the follower aircraft to increase its Mach number by 0.01 using any of the previously described attack vectors, the closing rate would be roughly 6 NM per hour,

which is sufficient to reduce the distance to close proximity within 15 minutes if no other protective measures intervene. For comparison, the same change in speed in a 10-minute MNT separation would take over 10 hours to achieve a similar closure. This underscores the importance of properly functioning CNS systems when planning to fly in formation.

C. Potential Threat Mitigation

Although the potential for cyberattacks has steadily increased in recent years, countermeasures have not been deployed to the same extent, as system architectures have remained largely unchanged. We consider it of utmost importance to take into account the work and warnings of researchers and refrain from using insecure technologies in safety-critical applications. As aviation strives to enhance safety and security, the implementation of *fello'fly* relying on legacy, insecure CNS technology, can be viewed as a step in the wrong direction. Despite their vulnerabilities, technologies like ADS-B are widely used in modern ATC systems. Through its availability, reduced separation is introduced, and new technologies such as In-Trail Procedures (ITP) are implemented, allowing for more frequent flight level changes as conflicting traffic is monitored via an onboard ADS-B receiver.

In the following sections, we propose potential actions based on the identified issues to guide to a more secure and safe implementation of *fello'fly*.

1) Securing Legacy Technologies: A logical approach involves enhancing the security of the aforementioned technologies. Researchers have proposed various potential adaptations to secure individual systems, in parallel with disclosing vulnerabilities [32], [49], [60], [61]. Measures may range from incorporating cybersecurity algorithms for authenticity and integrity protection to using specialized antennas for spoofing detection.

Moreover, ensuring that the autoflight system employs *tamper-aware* algorithms capable of identifying irregularities in signals or discrepancies between different aircraft surveillance systems could prove beneficial.

Nevertheless, instead of attempting to retrofit outdated systems to conform to current cybersecurity standards, it may be more efficient to invest time and resources in developing new, future-ready technologies.

2) Secure Air-To-Air Datalink: All potential threats discussed in this paper stem from the vulnerabilities of the communication, navigation, and surveillance technologies employed. By addressing these issues, the benefits will naturally extend to the WER implementation as well. Implementing an integrity-protected, bi-directional data link communication between the aircraft in formation could prevent most attacks related to ADS-B, transponder, and VHF spoofing. Through cooperative protocols, aircraft intentions could be instantly communicated.

During flight trials led by NASA and USAF, a military data link was used for communication [31], which typically includes certain protection mechanisms. By employing a similar secure link, aircraft could exchange data specific to the *fello'fly* operation, which might encompass weather, turbulence, and other information enabling a more reliable formation. Furthermore, failures and interference could be detected more quickly if an aircraft fails to respond within a preset time interval.

One example of a secure, civilian air-to-air data link is the LDACS Air-to-Air mode. This technology is currently in the initial stages of development and aims to provide means for aircraft to establish and organize independent communication via ad-hoc networks [7]. New systems can be designed with security in mind, as demonstrated by the Air-to-Ground mode of LDACS, which is undergoing the standardization process with ICAO. Researchers have proposed various methods to enable secure communication prior to its utilization, and similar advancements can be anticipated for the A2A mode as well.

3) Open Source Technology: History in cybersecurity has shown, that (cryptographic) systems designed upon the *security-by-obscurity* approach have posed significant vulnerabilities. Thus, especially in the development of complex system such as encryption standards, the research and industry community was involved to provide the best feedback and improvements. A similar open-source approach would be desirable in the implementation of the *fello'fly* technology in order to give the opportunity to vet the system thoroughly and thus reduce the risks of disruptions in operation or safety in later operation.

V. Conclusions

In this paper, we present a comprehensive analysis of the potential implementation of the WER project *fello'fly* within the existing CNS technology landscape. Our study begins by outlining the background of initiatives aimed at reducing emissions in the aviation sector. We then introduce the prevailing legislative parameters governing aircraft separation, followed by a detailed description of the individual steps involved in the *fello'fly* operation.

Given that no new CNS technologies are anticipated for integration during the project's introduction to service, we have conducted a security analysis of the currently employed systems. Our findings reveal that the majority of these systems lack any significant security measures. In recent years, research has identified numerous vulnerabilities across various systems, and real-world incidents have demonstrated that the potential for attacks is not merely theoretical.

We have extrapolated known attacks to the *fello'fly* environment to emphasize their potential consequences. Our research indicates that a substantial body of scientific literature on cybersecurity in aeronautical communications, publicly accessible code repositories for specific protocols such as ADS-B, and the declining cost of equipment due to the introduction of SDR, have made it easier for potential attacks to be executed. Consequently, we consider the implementation of a highly reduced separation and an automatically operating wake energy retrieval system that relies on these insecure communication methods to be of significant concern.

ACRONYMS

ACARS	Aircraft Communications Addressing and Reporting System
ADS-C	Automatic Dependent Surveillance - Contract
ADS-B	Automatic Dependent Surveillance Broadcast
ANSP	Air Network Service Provider
ASEPS	Advanced Surveillance-Enhanced Procedural Separation
ATC	Air Traffic Control
ATS	Air Traffic Services
CNS	Communication, Navigation and Surveillance
COTS	Commercial off-the-shelf
CPDLC	Controller Pilot Data Link Communication
DoS	Denial of Service
DFRC	Dryden Flight Research Center
ETOPS	Extended Range Twin Operations
FAA	Federal Aviation Administration
FANS	Future Air Navigation Systems
FIR	Flight Information Region
FL	Flight Level
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HF	High Frequency
HLA	High Level Airspace
ICAO	International Civil Aviation Organization
IMC	Instrument Meteorological Conditions
ITP	In-Trail Procedures
LEOS	Low Earth Orbiting Satellite
MNT	Mach Number Technique
NASA	National Aeronautics and Space Administration
NAT	North Atlantic
NAT-OTS	North Atlantic Organized Track System
NM	Nautical Miles
PBCS	Performance Based Communication and Surveillance
RA	Random Access
RNP	Required Navigation Performance
RVSM	Reduced Vertical Separation Minimum
SAF	Sustainable Aviation Fuel
SDR	Software Defined Radio
SELCAL	Selective Calling System
SPG	Systems Planning Group
SSR	Secondary Surveillance Radar
TCAS	Traffic Alert and Collision Avoidance System
TPS	Test Pilot School
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
VDLm2	VHF Data Link mode 2
VHF	Very High Frequency
WER	Wake Energy Retrieval

REFERENCES

[1] Airbus, "Biomimicry - Imitating nature's best-kept secrets," https://www.airbus.com/en/innovation/disruptive-concepts/biomimicry, accessed 03/15/2023.

[2] ——, "Sustainable aviation fuel - A proven alternative fuel for immediate CO2 reduction," https://www.airbus.com/en/sustainability/respecting-the-planet/decarbonisation/sustainable-aviation-fuel, accessed 03/15/2023.

[3] ——, "ZEROe - Towards the world's first zero-emission commercial aircraft," https://www.airbus.com/en/innovation/zero-emission/hydrogen/zeroe, accessed 03/19/2023.

[4] ——, "fello'fly: Wake Energy Retrieval - Concept of Operation," https://flipbook.mms-airbus.com/fellofly/index.html#/page/0, accessed 02/26/2023, 08 2021.

[5] APPEL News Staff - National Aeronautics and Space Administration (NASA), "This Month in NASA History: Winglets Helped Save an Industry," https://appel.nasa.gov/2014/07/22/this-month-in-nasa-history-winglets-helped-save-an-industry/, accessed 03/15/2023, 07 2014.

[6] L. T. Archives, "Fake Air Controller Tried To Give False Landing Orders to Jet," *Los Angeles Times*. [Online]. Available: https://www.latimes.com/archives/la-xpm-1987-08-18-mn-2195-story.html

[7] M. Bellido-Manganell and M. Schnell, "Towards modern air-to-air communications: the ldacs a2a mode," 09 2019.

[8] P. Berges, B. Shivakumar, T. Graziano, R. Gerdes, and Z. B. Celik, "On the feasibility of exploiting traffic collision avoidance system vulnerabilities," 06 2020.

[9] P. M. Berges, B. A. Shivakumar, T. Graziano, R. Gerdes, and Z. B. Celik, "On the feasibility of exploiting traffic collision avoidance system vulnerabilities," in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–6.

[10] J. Bhatti and T. Humphreys, "Hostile control of ships via false gps signals: Demonstration and detection," *Navigation*, vol. 64, pp. 51–66, 03 2017.

[11] Bloomberg News, "Westjet hijack signal called false alarm," *Bloomberg*, January 2015. [Online]. Available: https://www.bloomberg.com/news/articles/2015-01-10/westjet-hijack-signal-called-false-alarm

[12] Boeing, "Boeing Commits to Deliver Commercial Airplanes Ready to Fly on 100% Sustainable Fuels," https://tinyurl.com/2syy9kas, accessed 03/15/2023, 01 2021.

[13] C. Bresteau, S. Guigui, P. Berthier, and J. M. Fernandez, "On the security of aeronautical datalink communications: Problems and solutions," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, 2018, pp. 1A4–1–1A4–13.

[14] A. Chadha, V. Kumar, S. Kashyap, and M. Gupta, "Deepfake: An overview," in *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, P. K. Singh, S. T. Wierzchoń, S. Tanwar, M. Ganzha, and J. J. P. C. Rodrigues, Eds. Singapore: Springer Singapore, 2021, pp. 557–566.

[15] J. Cheng, A. Hoff, J. Tittsworth, and W. A. Gallo, *The Development of Wake Turbulence Re-Categorization in the United States (Invited)*. [Online]. Available: https://arc.aiaa.org/doi/abs/10.2514/6.2016-3434

[16] G. R. Community, "Gnu radio," https://www.gnuradio.org/, 2023, accessed: 2023-04-04.

[17] A. Costin and A. Francillon, "Ghost in the air(traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices," Network and Security Department, EURECOM, Tech. Rep., 07 2012.

[18] de61bd564f1aa929bae414a70e421acd0b81789a, "Dump1090," https://github.com/antirez/dump1090, 2020.

[19] G. A. C. (DLR), "DLR and MTU Aero Engines study fuel cell propulsion system for aviation," https://www.dlr.de/content/en/articles/news/2020/03/20200805_dlr-and-mtu-aero-engines-study-fuel-cell-propulsion-system-for-aviation.html, accessed 03/15/2023, 03 2020.

[20] EASA, "Technical Investigation on Radar Detection Losses in June 2014," *Annual Safety Review 2014*. [Online]. Available: https://www.easa.europa.eu/sites/default/files/dfu/203807_EASA_SAFETY_REVIEW_2014.pdf

[21] Federal Aviation Administration (FAA), "Advisory Circular - Aircraft Wake Turbulence." [Online]. Available: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-23G.pdf

[22] ——, "Next generation air transportation system (nextgen)." [Online]. Available: {https://www.faa.gov/nextgen}

[23] ——, "FAA Order JO 7110.65Z - Air Traffic Control," Online, November 2022.

[24] B. Garrett-Glaser, "The Batteries Behind the Electric Aircraft Revolution," https://www.aviationtoday.com/2020/09/08/batteries-behind-electric-aircraft-revolution/, accessed 03/15/2023, 09 2020.

[25] Global Aerospace Design Corporation, "Future Air Navigations Systems (FANS) 1/A+," 06 2021. [Online]. Available: https://gadc.aero/wp-content/uploads/GR0134-WPR_FANS_Rev-B.pdf

[26] Gupta, Manjul, "Investigation of Active Control of Aircraft Wing Tip Vortices and Wake Turbulence." [Online]. Available: {http://etd.auburn.edu/bitstream/handle/10415/2796/thesisfinal.pdf?sequence=2&isAllowed=y}

[27] A. Gurtov, T. Polishchuk, and M. Wernberg, "Controller–pilot data link communication security," *Sensors*, vol. 18, no. 5, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/5/1636

[28] J. Hannah, R. Mills, R. Dill, and D. Hodson, "Traffic collision avoidance system: false injection viability," *The Journal of Supercomputing*, vol. 77, no. 11, pp. 12 666–12 689, 2021. [Online]. Available: https://doi.org/10.1007/s11227-021-03766-9

[29] J. W. Hannah, "A Cyber Threat Taxonomy and a Viability Analysis for False Injections in the TCAS," https://scholar.afit.edu/cgi/viewcontent.cgi?article=5903&context=etd, accessed 04/13/2022, march 2021.

[30] C. Hanson, J. Pahle, J. Reynolds, S. Andrade, and N. Brown, "Experimental measurements of fuel savings during aircraft wake surfing," NASA Armstrong Flight Research Center, Tech. Rep., 2018, accessed: 2023-04-02. [Online]. Available: https://ntrs.nasa.gov/api/citations/20180004526/downloads/20180004526.pdf

[31] ——, "Recent nasa wake surfing flight research," NASA Armstrong Flight Research Center, Tech. Rep., 2018, accessed: 2023-04-02. [Online]. Available: https://ntrs.nasa.gov/api/citations/20180004610/downloads/20180004610.pdf

[32] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, and J. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," 01 2008, pp. 2314–2325.

[33] International Civil Aviation Organization. (n.d.) Gold: Global operational data link document, second edition. International Civil Aviation Organization. Accessed: 2023-04-02. [Online]. Available: https://www.icao.int/apac/documents/edocs/gold_2edition.pdf

[34] International Civil Aviation Organization (ICAO), "Procedures for Air Navigation Services - Air Traffic Management," Online, November 2001.

[35] ——, "Appendix G to Part 91—Operations in Reduced Vertical Separation Minimum (RVSM) Airspace," Online, December 2003.

[36] ——, "ASEPS using ADS-B Implementation Plan and Task List," Online, June 2019.

[37] ——, "APPLICATION OF SEPARATION MINIMA NORTH ATLANTIC REGION," Online, December 2022.

[38] ——, "North Atlantic Operations and Airspace Manual," Online, January 2023.

[39] International Energy Agency (IEA), "Aviation," https://www.iea.org/reports/aviation, accessed 03/15/2023, 09 2022.

[40] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned aircraft capture and control via gps spoofing," *Journal of Field Robotics*, vol. 31, 07 2014.

[41] P. D. Lee, "Aviation contributes 3.5% to the drivers of climate change that stem from humans," https://www.mmu.ac.uk/news-and-events/news/story/12787/, accessed 03/15/2023, 09 2020.

[42] G. Leff, "Nightmare Scenario: Man Arrested for Impersonating Air Traffic Control, Issuing Fake Takeoff Instructions," *View from the wing*. [Online]. Available: NightmareScenario:ManArrestedforImpersonatingAirTrafficControl, IssuingFakeTakeoffInstructions

[43] Y. Liang, A. Izadi, N. Hinze, and A. Trani, *Performance Assessment of the North Atlantic Organized Track System Using the Global Oceanic Model*. [Online]. Available: https://arc.aiaa.org/doi/abs/10.2514/6.2018-3351

[44] A. Lomas, "TCAS and ILS Spoofing Demonstration," https://www.youtube.com/watch?v=VbCzABE6jec, accessed 04/13/2022, August 2020.

[45] Lufthansa Technik, "Cutting emissions with sharkskin technology," https://www.lufthansa-technik.com/aeroshark, accessed 03/15/2023.

[46] D. d. Marco, A. Manzo, M. Ivaldi, and J. Hird, "Security testing with controller-pilot data link communications," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 526–531.

[47] R. Mark, "Faa warns of ads-b false alerts," *Flying Magazine*, March 2017. [Online]. Available: https://www.flyingmag.com/faa-warns-ads-b-false-alerts/

[48] B. Mattos, A. Macedo, and D. S. Filho, *Considerations About Winglet Design*. [Online]. Available: https://arc.aiaa.org/doi/abs/10.2514/6.2003-3502

[49] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548211000229

[50] C. Middleton, "Risk assessment planning for airborne systems: An information assurance failure mode, effects and criticality analysis methodology," 2012.

[51] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187454822200035X

[52] P. Papadimitratos and A. Jovanovic, "Gnss-based positioning: Attacks and countermeasures," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–7.

[53] G. PETRAUSKAITE, "Pseudo air traffic controller arrested after faking radio orders to aircraft," *Aerotime Hub*. [Online]. Available: https://www.aerotime.aero/articles/27133-fake-radio-orders-flight-crew

[54] Safe Handling of TCAS Alerts, "BAROUX, Christophe and CARDONA, Florence and CORRAL, Cédric and DUREPAIRE, Xavier and LOPEZ VILLAREJO, Maria Luisa and VILLENEUVE, Christine," *Airbus*, 09 2021. [Online]. Available: https://safetyfirst.airbus.com/safe-handling-of-tcas-alerts/

[55] H. Sathaye, G. Noubir, and A. Ranganathan, "On the implications of spoofing and jamming aviation datalink applications," in *Proceedings of the 38th Annual Computer Security Applications Conference*, ser. ACSAC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 548–560. [Online]. Available: https://doi.org/10.1145/3564625.3564651

[56] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," 06 2013, pp. 253–271.

[57] J. Smailes, D. Moser, M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "You talkin' to me? exploring practical attacks on controller pilot data link communications," ser. CPSS '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 53–64. [Online]. Available: https://doi.org/10.1145/3457339.3457985

[58] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "Understanding realistic attacks on airborne collision avoidance systems," *Journal of Transportation Security*, vol. 15, 06 2022.

[59] Smith, Matthew and Moser, Daniel and Strohmeier, Martin and Lenders, Vincent and Martinovic, Ivan, "Undermining privacy in the aircraft communications addressing and reporting system (acars)," in *Proceedings on Privacy Enhancing Technologies 2018*, 04 2018.

[60] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, and C. Neeteson, "Towards a more secure atc voice communications system," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, 2015, pp. 4C1–1–4C1–9.

[61] M. Strohmeier, V. Lenders, and I. Martinovic, "Intrusion detection for airborne communication using phy-layer information," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, M. Almgren, V. Gulisano, and F. Maggi, Eds. Cham: Springer International Publishing, 2015, pp. 67–77.

[62] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1338–1357, 2017.

[63] Timothy Michael Graziano, "Establishment of a cyber-physical systems (cps) test bed to explore traffic collision avoidance system (tcas) vulnerabilities to cyber attacks."

[64] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 75–86. [Online]. Available: https://doi.org/10.1145/2046707.2046719

[65] L. Yusupov, ""ads-b out" add-on for softrf-emu, stratux, etc..." https://github.com/lyusupov/ADSB-Out, 2021.

April 18-20, 2023