Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation

EDAN HABLER, RON BITTON, and ASAF SHABTAI, Ben-Gurion University of the Negev, Israel

The sophistication and complexity of cyber attacks and the variety of targeted platforms have grown in recent years. Adversaries are targeting a wide range of platforms, e.g., enterprise networks, mobile phones, PCs, and industrial control systems. The past few years have also seen various cyber attacks on transportation systems, including attacks on ports, trains, airports, and aircraft. Due to the enormous potential damage inherent in attacking vehicles carrying many passengers and the lack of security measures applied in existing airborne systems, the vulnerability of aircraft systems is one of the most concerning topics in the vehicle security domain. This article provides a comprehensive review of aircraft systems and components and their various networks, emphasizing the cyber threats they are exposed to and the impact of a cyber attack on these components and networks and an aircraft's essential capabilities. In addition, we present a comprehensive and in-depth taxonomy that standardizes the knowledge and understanding of cyber security in the avionics field. The taxonomy divides attack techniques into relevant categories (tactics) reflecting the various phases of the adversarial attack lifecycle and maps existing attacks according to the MITRE ATT&CK methodology. To contribute to increased understanding of the potential risks, we categorize the identified threats related to the various systems based on STRIDE threat model and demonstrate the practical application of this taxonomy in the analysis of real-world attack use cases. Finally, we review various mitigation techniques aimed at addressing security risks related to aircraft systems. Future work directions are presented as guidelines for industry and academia.

CCS Concepts: • **Security and privacy**; • **Computing methodologies** → *Machine learning*;

Additional Key Words and Phrases: Aircraft, security analysis

ACM Reference format:
Edan Habler, Ron Bitton, and Asaf Shabtai. 2023. Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation. *ACM Comput. Surv.* 56, 4, Article 96 (November 2023), 40 pages.
https://doi.org/10.1145/3610772

1 INTRODUCTION

1.1 Security of Aircraft Systems

Given the significant growth in the number of flights over the past decade,[1] traditional **air traffic management (ATM)** systems have difficulty providing relevant and reliable information on the

[1] https://www.statista.com/statistics/564769/airline-industry-number-of-flights/

This work was partially supported by the Israeli Smart Transportation Research Center (ISTRC).

Authors' address: E. Habler, R. Bitton, and A. Shabtai, Ben-Gurion University of the Negev, Beer-Sheva, Israel; emails: {habler, ronbit}@post.bgu.ac.il, shabtaia@bgu.ac.il.

0360-0300/2023/11-ART96 $15.00
https://doi.org/10.1145/3610772

state of an aircraft. As a result, the aviation community is actively taking steps to increase flight traffic safety, capacity, and flexibility, as well as to reduce dependence on outdated infrastructure, by examining and improving national airspace systems. There are two main projects at the forefront of modernization efforts in the aviation industry: the NextGen[2] and SESAR[3] projects, respectively, led by the U.S. **Federal Aviation Administration (FAA)** and the European Commission. Section 1 in the Supplementary material provides an overview of commonly used aircraft risk analysis frameworks, emphasizing flight safety, passenger safety, and system development. These projects are primarily aimed at creating new technologies and procedures to increase the capacity, accuracy, and reliability of air traffic control, while privacy and information security have not been prioritized.

While information security and privacy related to aviation systems have received limited attention, both from industry and academia, the attack surface accessible to cyber attacks continues to grow. According to *Positive Technology's* annual report, the first quarter of 2021 showed a 17% increase in cyber attacks over the same quarter of the previous year [84], a trend that was seen in the transportation industry. Check Point's ransomware report [11] indicated that in the period of June 2020 to June 2021, the transportation industry witnessed a 186% increase in the average number of attacks per week. Moreover, according to the European Air Traffic Management Computer Emergency Response Team [105], 50 aviation-related cyber incidents were reported in 2022 and from 2019 to 2020 there was an increase of 530% in the number of reported incidents.

Rising concern regarding the aviation industry's vulnerability to cyber attacks and the associated increase in efforts to secure it against such attacks are expected to result in substantial growth in the aviation cyber security market in the coming years. Industry forecasts predict a compound annual growth rate of 7.6% in the aviation cyber security market for the period of 2022–2028 [50, 66].

In recent years, researchers in both academia and industry have pointed out weaknesses in airborne systems' design and implementation and demonstrated how some core airborne systems can be tampered with simply by using **commercial off-the-shelf (COTS)** hardware and software; for instance, Costin et al. [14] simulated attacks on the ADS-B system using a COTS **software-defined radio (SDR)** transmitter, and Teso et al. [115] demonstrated how a simple Android device can be used to send radio signals and gain access to an aircraft's navigation controls by exploiting the **aircraft communications, addressing, and reporting system (ACARS)**.

To ensure that strong security measures are in place, the **International Civil Aviation Organization (ICAO)** has developed guidelines for enhancing security measures in the aviation field. These guidelines address a range of security concerns, including security issues related to air traffic management (e.g., the Air Traffic Management Security Manual [76]) and access control management and hardware security (e.g., the Aviation Security Manual [51]). By adhering to these guidelines, **air traffic service providers (ATSPs)** can improve the security of their ATM systems and protect them from potential cyber threats.

1.2 Scope and Purpose

To better classify the attacks associated with different threats, it is important to analyze the vulnerabilities of airborne systems as well as the potential threat actors. Systematically categorizing adversaries' behavior will enable the identification of sensitive points in the various aircraft systems, and the stage of an ongoing attack, as well as preventive actions.

There are a few popular knowledge bases that describe cyber adversary behavior and provide a common taxonomy for both offense and defense aimed at enterprise networks: FireEye's cyber kill

[2] https://www.faa.gov/nextgen/media/NextGenAnnualReport-FiscalYear2020.pdf
[3] http://www.sesar.eu/

chain,[4] Lockheed Martin's cyber kill chain, which is part of their intelligence-driven defense model for identification and prevention [46], and MITRE ATT&CK [112], which maintains a taxonomy for multiple platforms and networks (enterprise, mobile, and industrial control systems). However, no well-defined knowledge base aggregates all information regarding the threat components and provides a taxonomy for the different stages of attacks in the field of transportation and avionics.

The **Space Policy and Architecture Research and Analysis (SPARTA)**[5] program, developed by the Aerospace Corporation, serves as an example of attack knowledge base for spacecraft. The SPARTA initiative aims to provide impartial analysis and recommendations on space policy and architecture issues to various stakeholders, including the U.S. government, military, and civil space communities. While SPARTA's primary focus is on space policy and architecture, rather than on aviation, it covers some topics that are relevant to the aviation industry, such as airspace management and space-based navigation systems. Our article focuses specifically on aircraft systems, examining the links between them and the access points to these systems. By doing so, we aim to improve understanding of the complexities and interdependencies of aircraft systems and contribute to the development of more robust and secure aviation systems.

We take a comprehensive approach: First, we provide a broad overview of avionic systems, emphasizing the security aspects. Then, we present an extension of the MITRE taxonomy adapted for the avionics field, encompassing adversarial behavior associated with the communication, navigation, engagement, surveillance, and complementary systems and devices of aircraft. Following the structure of MITRE ATT&CK's taxonomies, we identified specific actions (techniques) and classified them under categories (tactics) to reflect the various phases of the adversarial attack lifecycle. We also present an ontology that defines the entities through which the various threats and actors that take part in the various attacks can be analyzed.

An aircraft is a complex system that includes various communication systems and devices serving different functions. We examined the aircraft's network infrastructure using the domains defined by the ARINC Airlines Electronic Engineering Committee [9]: the **passenger information & entertainment domain (PIESD)**, **passenger-owned devices domain (PODD)**, **airline information services domain (AISD)**, and **aircraft control domain (ACD)**.

Each domain consists of a set of interconnected systems and components that serve specific purposes and have defined logical responsibilities. Therefore, the adversaries' degree of influence depends on their capabilities as well as the domain to which they have access. This division of domains can be used to identify weak points that can enable an adversary to move between the domains. After defining the avionic assets consisting of the various networks and components, we mapped the various attacks and threats associated with them and analyzed them using the STRIDE [108] threat model, the attacker's capabilities, and the potential impact.

Table 1 compares our study to recent studies [19, 22, 63, 94, 109, 110] that analyze threats to various aviation systems. As can be seen, previous studies have not performed a comprehensive evaluation of all avionic systems, particularly the backend avionic systems, and system connectivity. Our study addresses this gap by providing a detailed analysis of avionic systems, their connectivity, and the attacks targeting them. Moreover, we propose a taxonomy for cyber security analysis of avionic systems that is an extension of the MITRE taxonomy.

1.3 Contributions

The main contributions of this article can be summarized as follows: (1) a comprehensive overview of modern aircraft, including their systems, domains, and networks, highlighting their security

[4] https://www.fireeye.com/content/dam/fireeye-www/company/events/infosec/tech-track-summit-paris.pdf
[5] https://sparta.aerospace.org/

Table 1. Comparison of Our Survey with Existing Aviation Security Surveys

Paper	Assets Evaluated																																	Taxonomy	Security Model
	Comm.			Navigation								Surveillance				Alerting					Backend Avionics & Network								Connectivity					
	SATCOM	CPDLC	ACARS	DME	VOR	NDB	ILS	GNSS	ABAS	SBAS	GNAS	PSR	SSR	MLAT	ADS-B	TCAS	ACAS X	Engine alert	FIS-B	TIS-B	EFB	TWLU/CWLU	FMS	EGM	NIM	CSS	FDR	CIS-MS	ACD	AISD	PIESD	Ext. networks		
Our study	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	STRIDE
[19]	●	●	●	●	●	○	●	●	○	○	○	●	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	CIA
[22]	○	●	●	●	●	○	●	●	○	○	○	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Likelihood & impact
[63]	●	○	○	○	○	○	○	●	○	○	○	●	●	○	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	Categorizes actors in relation to their resources & motivations
[94]	○	●	●	○	○	○	○	●	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Discusses security challenges
[109]	○	●	●	○	○	○	○	○	○	○	○	○	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Examines realistic events & accidents that have occurred
[110]	○	●	●	●	●	●	●	○	○	○	○	●	●	●	●	●	○	○	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	Operational impact

vulnerabilities, attack vectors, and threats; (2) systematic mapping of the different attacks and their required capabilities, targets, and threat categories; (3) a review of diverse mitigation techniques aimed at addressing security concerns; (4) a novel taxonomy that categorizes adversarial behavior targeting the various attack surfaces and systems of aircraft; this taxonomy is an extension of the MITRE taxonomy specifically for the aviation industry; (5) a demonstration of the application and use of the taxonomy with test cases involving cyber attacks on an aircraft.

2 THREAT ANALYSIS

Our security analysis is performed based on the threat analysis ontology presented in Figure 1 in the Supplementary material, which is based on the NIST ontology for evaluating enterprise security risk. The ontology includes the following entities: threat actors, threats, adversarial capabilities (categorized by access, positional, knowledge, and material capabilities in aviation), vulnerabilities, operational impact, e-Enabled domains, target assets, aviation tactics, attack techniques, sub-techniques, and procedures.

To analyze the threat model and define a taxonomy for attacks in the avionics field, we performed the following steps:

(1) We reviewed the various avionic systems, communication networks, and backend components that comprise the aircraft's complete assembly. This review was carried out by examining the *e-enabled domains* to identify the various *target assets* (Section 3).
(2) We mapped the *threats* and concrete attacks targeting each asset (Section 6) to identify its inherent *vulnerabilities*.
(3) We analyzed the various attacks using the *STRIDE threat model*, mapped the *threat actors* (Section 5.1), and identified the various *adversarial capabilities* required to implement the attacks carried out (Section 5.2).
(4) We analyzed the concrete attacks demonstrated in academic work and by industry and derived the *sub-techniques* used to perform the various attacks (summarized in Table 3).
(5) We defined a taxonomy for the avionics field by using the mappings of the potential threat actors, their capabilities, and the concrete attacks demonstrated in both industry and academic work. This taxonomy is presented as an extension of the MITRE framework (Section 7). The proposed taxonomy is defined by specifying the various concrete attacks and *techniques* used by the attackers and considering them as an attacker's means of achieving a goal (i.e., tactic) as part of a multi-stage attack. A demonstration for practical application of the taxonomy is presented in the Supplementary material (Section 5).

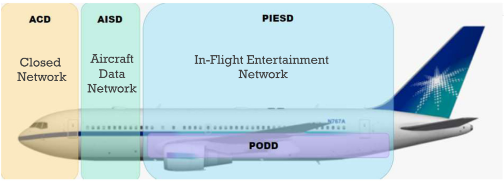


Fig. 1. E-enabled aircraft domains.

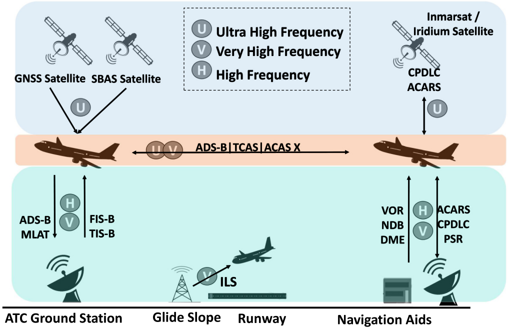


Fig. 2. Aviation systems and technology infrastructure, positioning, and range of operation.

3 THE TARGET ASSETS OF AN AIRCRAFT SYSTEM

Over the past decade, the architecture of avionics and information systems in aircraft has evolved and developed to enable real-time data links between aircraft and the ground for information sharing, i.e., transferring critical control, maintenance, navigation, and operations data. Other changes were driven by the need to decrease fuel expenses, with the aim of reducing the weight of computer and network infrastructure on aircraft to limit fuel consumption and cost. This was achieved by consolidating a number of software systems on **integrated modular avionics (IMA)** computing modules capable of supporting numerous applications and transitioning to Ethernet-based protocols and networks (and more specifically to Avionics Full-Duplex Switched Ethernet, defined in the ARINC-664 report [7]).

Aircraft systems (e.g., passenger engagement systems, critical navigation systems) have different roles and levels of importance and sensitivity. Therefore, the target assets of aircraft systems are divided into three e-enabled domains (see Figure 1): ACD, AISD, and passengers' domain, which includes the PIESD and PODD.

In this section, we briefly describe each of the aircraft e-enabled domains, analyze the various target assets that are part of each domain, and analyze the connectivity between different domains. Specifically, in Section 3.1, we present the systems that are part of the ACD. In Section 3.2, we present the systems that are part of the AISD. In Section 3.3, we present the systems that are part of the PIESD, and in Section 3.4, we present the underlying communication systems. Figure 2 illustrates the various systems, technologies, infrastructures, and range of operation, and Figure 3 illustrates the different avionic assets, categorized according to their purpose and infrastructure.

3.1 Aircraft Control Domain (ACD)

The ACD consists of the systems and networks responsible for the aircraft's safe operation, e.g., **air traffic control (ATC)** service and **aircraft operational control (AOC)** communications. Therefore, the ACD has the most stringent security requirements. It contains two subdomains: the *cabin-core* and the *flight and embedded control system* domains. The *cabin-core* domain is designed to provide the services required to operate the cabin components, such as public address systems, smoke detectors, and air conditioning. The *flight and embedded control system* domain is designed to allow the pilot to control the aircraft from the flight deck. To communicate with onground services, aircraft use different components such as optical diodes and electronic gateway modules. Sometimes, these components are the same as the components that serve the passenger domains; thus, the separation between domains is not absolute. A large number of critical systems are used

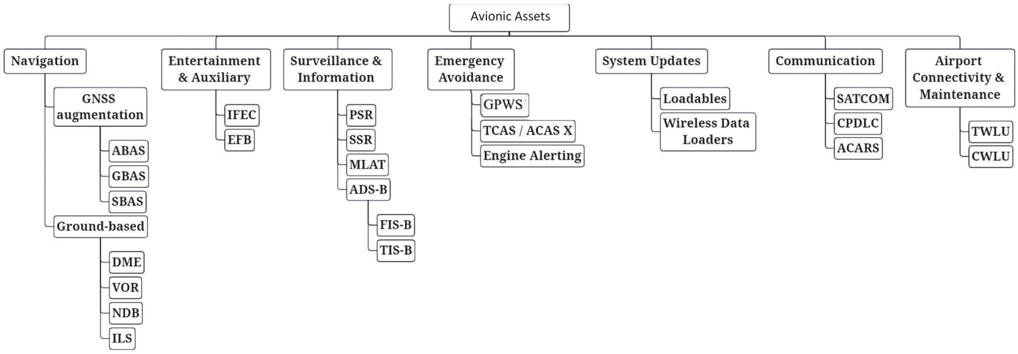


Fig. 3. Categorization of air/ground avionic systems—navigation, entertainment, surveillance, information, communication, and maintenance systems.

by aircraft during flight. We mapped the main systems according to the nature of their function: surveillance, communication, emergency avoidance, system updates, navigation, entertainment, and auxiliary (see Figure 3).

3.1.1 Surveillance and Information Systems. Surveillance systems are responsible for proactive, comprehensive monitoring of the aircraft location, while information systems support the aircraft operators and provide aeronautical information.

- **ADS-B: Automatic Dependent Surveillance–Broadcast** [36] is a "radar-like" system designed to continuously derive the aircraft position from the **global navigation satellite (GPS)** system. ADS-B provides the aircraft's position and velocity with high accuracy, providing a clearer picture of the air traffic than traditional radar systems. ADS-B includes two separate systems: ADS-B In and ADS-B Out. The ADS-B In system allows an aircraft to receive and display messages transmitted by other aircraft within the receiving range. The ADS-B Out system allows an aircraft to continuously generate and broadcast messages over an unencrypted L-band range of frequencies. There are several types of certified ADS-B data links, including the traditional radar frequency link that operates at 1090 MHz and UAT978, which is a technology used for ADS-B (operates at 978 MHz) that provides pilots with weather, traffic, and flight information. ADS-B consists of several types of ADS-B messages, including ADS-B Out messages (position, velocity, identification, surface position, and velocity messages), ADS-B In messages (traffic information service-broadcast and flight information service-broadcast), ADS-B emergency messages, and ADS-B status messages. A detailed description of each type of message and its structure can be found in Mode-S decoding guide.[6]
- **FIS-B Reports:** FIS-B [75] is a critical data link system that provides aircraft operators with real-time flight information, including traffic information, using the **Traffic Information Services-Broadcast (TIS-B)**, and weather information (e.g., wind, pressure, and temperature), using the **Winds and Temperature Aloft (FBW)** and **Notice to Airmen (NOTAMs)** services. FIS-B data is transmitted from ground stations to the aircraft's ADS-B receiver, which is responsible for processing the data and providing a graphical representation of national weather service data and flight restrictions on cockpit displays.
- **PSR: Primary surveillance radar** [98] is a surveillance radar system that does not require any onboard equipment to locate aircraft. PSR uses a radar antenna to emit a radio wave

[6] https://mode-s.org/decode/content/ads-b/1-basics.html

pulse. When directed at an aircraft, the wave is reflected, and the resulting energy is returned back to the PSR antenna. By analyzing the reflected pulse, the system can infer the range and bearing of the aircraft with respect to the antenna position. Since the PSR does not consist of onboard components, it does not represent an avionic asset for the purposes of our research, and therefore, we will not expand on it further in this article.

- **SSR: Secondary surveillance radar** [107] is a surveillance radar system that uses transmitters and transponders as interrogators. The SSR radar antenna transmits a pulse that is received by an onboard transponder. The transponder returns a reply that contains information regarding the aircraft state (e.g., identity code, aircraft's altitude).
- **Mode-S: Mode Select** [62] is a selective interrogation protocol utilized in ATC. Unlike SSR, which relies on transponder-based replies, Mode-S enables ATC to address individual aircraft and request customized information such as altitude, airspeed, and flight identification, resulting in more efficient and accurate aircraft identification and tracking. Additionally, Mode-S can support ADS-B, which provides more precise and frequent positional information from the aircraft. Mode-S has become the preferred technology for aircraft identification and tracking in modern ATC systems due to its enhanced capabilities, replacing SSR as the standard.
- **MLAT: Multilateration** [126] is a technology used for navigation and surveillance. MLAT analyzes a signal's **time difference of arrival (TDOA)**, using multiple sensors in fixed locations to infer the aircraft transmitter location. In aviation, MLAT is used by many stakeholders (e.g., live flight trackers) to track aircraft location. MLAT is often used in conjunction with ADS-B messages to validate location data provided within the ADS-B framework [113], detect malicious ADS-B broadcasts [70], and improve the efficiency of radar control in specific airspace locations [57].

3.1.2 Emergency Avoidance Systems. Emergency avoidance systems are designed to issue an alert when there is a critical failure (e.g., engine failure), increase cockpit awareness of nearby aircraft, and serve as the last defense against mid-air collisions.

- **TCAS/ACAS X:** A **traffic collision avoidance system** [41] that is designed to issue alerts and prevent mid-air collisions. The TCAS uses an onboard surveillance system to interrogate the airspace around an aircraft for other aircraft equipped with an active corresponding transponder (Mode-S transponder). The transponder is used to transmit signals indicating the aircraft's position, altitude, and vertical speed. The TCAS consists of two antennas, one of which is located on top of the fuselage and the other of which is located on the bottom of the fuselage; the monitored aircraft appears on the navigation display. By analyzing the replies from nearby aircraft, the TCAS can predict a potential collision, raise an alert regarding a potential intruder (a nearby aircraft), and request a resolution advisory (maneuver instruction to prevent a collision) for both aircraft. In the past decade, the FAA has funded research aimed at developing a modern approach to collision avoidance—a collision avoidance system known as ACAS X, which will use dynamic programming and provide more accurate alerts; in addition, ACAS X aims to support aircraft equipped solely with passive surveillance mechanisms.
- **Engine Alerting System:** An engine alerting system enables the flight crew to visualize the engine parameters and faults. Two systems are commonly used for engine alerting: The **engine-indicating and crew-alerting system (EICAS)** [33] is an engine alerting system that consists of two monitors, two computers, and a display select panel. The monitors are used to display engine status and maintenance information, the display select panel enables the pilot to decide which of the two computers should provide the engine information to

the monitors (one of the computers provides data and the other one serves as a backup). If an engine failure occurs, then the system alerts the pilot, and the parameters of the event are recorded so they can be analyzed by relevant experts after the event. While the EICAS is mainly deployed on Boeing aircraft, the **electronic centralized aircraft monitor (ECAM)** is the corresponding system deployed on Airbus aircraft. The main difference between the EICAS and ECAM is that ECAM lists the actions required to deal with a failure.

- **GPWS:** A ground proximity warning system [29] is designed to alert pilots if the aircraft is flying too close to the ground or if there is an object nearby that may lead to a collision. This system is based on a radar antenna that is placed on the nose of an aircraft. The antenna can also measure the size of water droplets in the air, allowing the aircraft to detect bad weather conditions.

3.1.3 Navigation Systems. Navigation systems are designed to assist with navigation during all phases of the flight, from takeoff to landing. These systems can operate when flying over different types of terrain and from varying distances from the ground.

- **GNSS and Augmentation Systems:** A **global navigation satellite system** [34, 43] is a group of satellites that send positioning, timing, and velocity data to GNSS receivers. The information received by the receivers is then used to determine the position and velocity of the aircraft. In the aviation field, the GNSS serves as a basic function in other systems, e.g., the ADS-B system uses the GNSS to provide aircraft positions to ATC.
  - **ABAS** An aircraft-based augmentation system is a system that integrates the information obtained from the GNSS with information available on board the aircraft.
  - **GBAS** a ground-based augmentation system is a system that ensures integrity using data obtained from ground sensors.
  - **SBAS** a satellite-based augmentation system that improves the integrity, accuracy, and reliability of the GPS signal, using a number of geostationary satellites that cover vast areas.
- **Ground-based Navigation Systems:** There are four kinds of ground-based navigation systems:
  - **ILS (instrument landing system)** [86] is a radio navigation system that provides short-range precision guidance to an aircraft approaching a runway when visibility is poor and adversely affected by lighting and weather conditions. An ILS uses **very high frequency (VHF)** electromagnetic waves to provide horizontal guidance and **ultra high frequency (UHF)** electromagnetic waves to provide vertical and range guidance; its main components are the localizer, glide slope, and marker beacons.
  - **VOR (VHF omnidirectional radio range)** [125] is a navigation aid system operating in the VHF band. An aircraft equipped with a VOR receiver can determine its clockwise bearing from magnetic north, with reference to the ground station, by transmitting VHF navigation signals at radial angles.
  - **DME (distance measuring equipment)** [125] is a radio navigation aid that uses interrogation to compute the distance between an aircraft and DME equipment on the ground. The aircraft transmits a signal, which is returned by the DME ground equipment after a fixed delay. The aircraft's distance from the ground equipment can be measured based on the delay of the returned signal perceived by the aircraft's DME equipment.
  - **NDB (non-directional radio beacon)** [128] is a navigation aid system that, in contrast to the VOR system, does not include inherent directional information. NDB signals follow the curvature of the Earth, and thus they can be received from much greater distances at lower altitudes. An NDB requires knowledge of the aircraft's exact heading to provide high accuracy, while VOR does not.

3.2 Airline Information Services Domain (AISD)

The AISD provides different types of services for non-essential/third-party applications, e.g., computing power, data storage, and routing. Independent aircraft applications such as avionics, in-flight entertainment, and flight crew and flight attendant applications use the AISD for connectivity purposes. The AISD contains two subdomains: the *administrative* and *passenger support* subdomains. The *administrative* domain is designed to provide the flight deck and cabin with operational and administrative information. The *passenger support* domain is designed to provide information to the passengers.

- **EFB:** The **electronic flight bag** [10] server is a highly customized and flexible component of the aircraft, which is used for information management. The EFB is connected to most of the aircraft's avionic systems and sensors via dedicated interfaces (e.g., ARINC-615 and ARINC-429). Traditionally, Class 3 EFB systems are installed as aircraft equipment that includes an EFB server and a dedicated multi-function display. In recent years, pilots have started using portable and commercial tablets provided by the airlines as an extension to the EFB (Considered as Class 2 EFB systems).[7] Class 2 EFB systems usually contain applications that complement the services provided by the EFB, such as calculation of the takeoff data.

3.3 Passenger Domain (PIESD)

The passenger domain can be divided into two subdomains: *PIESD* and *PODD*. The PIESD is designed to serve the passengers, providing them with Internet and entertainment services. In addition to traditional entertainment systems, this domain allows access to wireless networks, links to passengers' physical devices, and seat adjustments. The PIESD also connects passengers with the flight information system. The PODD consists of external devices that passengers bring on board. To connect these external devices to the aircraft system, a passenger has to go through the PIESD.

- **IFEC system:** The in-flight entertainment and communication system refers to the entertainment applications available to passengers during flight (e.g., TV, audio, Wi-Fi, maps, and games). The IFEC includes content communication systems from external providers that are designed to enable telephony, satellite, and Internet services. These systems usually include display screens, computers with Linux/Windows/Android operating systems, and hosting/storage servers.

3.4 Communication Systems

- **SATCOM:** The aircraft **satellite communication system** [59] is used for reliable data and voice communication. The SATCOM serves as a data link for different uses, such as ADS-B, **controller pilot data link communications (CPDLC)**, and the ACARS. It is composed of the following components:
  - ***Satellite data unit (SDU):*** The SDU allows air and ground communication via a satellite network. The SDU uses a radio frequency unit to connect with a satellite. ARINC-781 [8] is a component that outlines the preferred features of an aviation SATCOM system designed for use across various commercial transport and business aircraft.
  - *Low- and high-gain antennas:* These antennas contain an integrated beam steering unit and receive command information directly from the SDU.
- **CPDLC/FANS-1/ATN:** The **Controller Pilot Data Link Communications** [23] provides a communication method between air traffic controllers and pilots over a data link system. The CPDLC data link is used to transmit nonurgent messages to an aircraft and serves as an

[7] https://www.neowin.net/news/delta-airlines-to-equip-pilots-with-surface-2-tablets/

alternative to voice communications. There are two popular implementations of the CPDLC data link system: the **future air navigation system (FANS-1)**[8] and the **aeronautical telecommunication network (ATN)**[9] system. FANS-1 [26] is an ACARS-based service that primarily employs Inmarsat satellite communication services for air-to-ground communication, but it also has the capability to utilize alternative satellite-based communication services, such as Iridium, for oceanic flights. This feature ensures uninterrupted and reliable communication, particularly in areas where Inmarsat signal coverage may be limited or disrupted. The ATN service is based on a VHF data link and is mainly operated by ARINC and SITA [2].

- **ACARS:** The aircraft communications addressing and reporting system [101] is a digital data link system that enables the transmission of short messages between aircraft and ground stations through a network of transceivers. ACARS messages are used to communicate with ATC and the base operational office. This system is most often used for transmitting departure information, weather information, aeronautical operational control information, and OOOI events ([gate] Out, [wheels] Off, [wheels] On, and [gate] In), which are automatically collected and represent the flight phase and related information (e.g., amount of fuel). The main components of ACARS are:
  - *Onboard equipment:* The onboard equipment consists of a management unit that interfaces with **flight management systems (FMSs)** and a router that enables the aircraft to receive flight plans and weather information from the ground. The management unit enables the airline to update the FMS, and the crew can use this information to evaluate alternative routes.
  - *Ground equipment:* The ground equipment consists of networks of radio transceivers managed by a computer that handles ACARS messages.
  - ***datalink service provider (DSP)**:* The communication between the aircraft and the ground is managed by a DSP, where SITA and ARINC are the two primary providers.

4 DOMAIN CONNECTIVITY

The aircraft networks include inter-connected components that may allow attackers to move between domains. To prevent an adversary from spreading within the aircraft network, it is critical to identify areas within aircraft systems that an attacker can exploit for lateral movement. The division into the different domains and the networks that comprise them is illustrated in Figure 4, along with their backend components and the components that link the networks. Components that overlap between the networks (i.e., link) are marked with a red dot. The figure also specifies the technology enabling communication between the networks and the providers.

4.1 PIESD and AISD Connectivity

The core network cabinet is responsible for data segregation between the PIESD, AISD, and ACD. The core network cabinet consists of several components, i.e., the **Ethernet gateway module (EGM), controller server module (CSM)**, and **crew information system/maintenance system (CIS-MS) file server module (FSM)**. While these components are used to provide cabin services, they must be able to access the AISD for this purpose.

- The EGM includes an Ethernet switch and router for managing the PIESD and AISD connectivity.

[8] https://en.wikipedia.org/wiki/FANS-1/A
[9] http://www.tc.faa.gov/its/cmd/visitors/data/act-300/atn.pdf

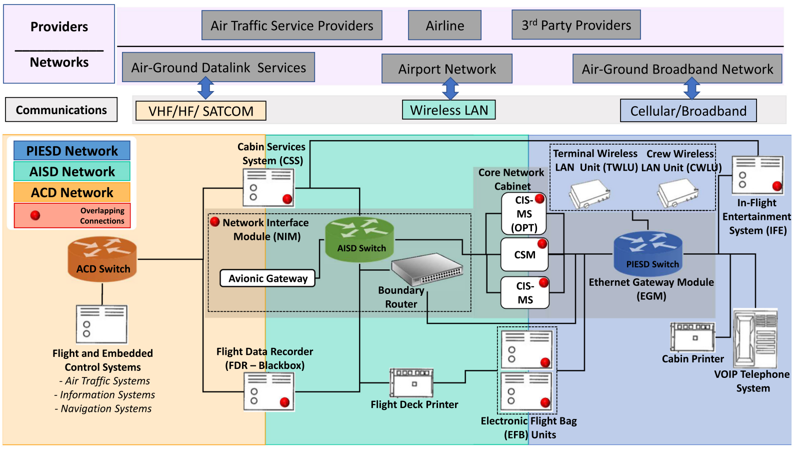


Fig. 4. E-enabled implementation—system and component connectivity. The figure highlights the backend components that comprise the various domains; overlapping components are marked with a red circle.

- The CSM utilizes a dual connection, providing network management services (e.g., DHCP and DNS services) to the PIESD, as well as fault reporting across the AISD and therefore to the ACD, which hosts the maintenance system.
- The CIS-MS FSM is connected to provide the ACD/AISD/PIESD systems' data load services. These services include file transfer, data retention, wireless device control, and communication services.

In addition to the core network cabinet, the EFB also connects the networks. The EFB is connected to the PIESD and AISD via the AISD switch and the EGM. This interconnection allows, for example, problem reports to be offloaded from the aircraft in the event of wireless/broadband satellite, AISD, or PIESD failure, using the e-logbook application hosted on the EFB.

4.2 AISD and ACD Connectivity

The **network interface module (NIM)** includes an avionic gateway that provides network address and protocol translation to connect the AISD to the more secure avionics in the ACD through the ACD switch. To improve the fault isolation capability of the maintenance system, in case of a failure of the NIM boundary router and/or the EGM, the following aircraft systems may also be connected to the ACD switch: the **flight data recorder (FDR)** and **cabin services system (CSS)**.

- The FDR is an optional server that records high-value data that must be available at all times.
- The CSS has dual connections: The connectivity to the IFEC system enables information to be presented to and played by passengers, while the connectivity to the ACD and AISD switches enables the transfer of audio between the pilot and the cabin.

4.3 External Connectivity

Several external connections allow remote access to the aircraft network for the benefit of synchronization, updating information, and maintenance.

- Maintenance laptop connectivity is possible using the connectivity and crew wireless LAN unit, thus enabling external components to access the aircraft network.
- External flight planning systems can communicate with the aircraft crew via ACARS to update navigation plans.

- External terminals provided by trusted parties can be used for wireless communication with data loaders that are used for software updates.
- The aircraft **terminal wireless LAN unit (TWLU)** is used for airport gatelink connectivity, while the connectivity and **crew wireless LAN unit (CWLU)** is used for maintenance laptop connectivity.
- The airport wireless network can be used to access devices on the same LAN, and these components (such as an EFB tablet or passengers' private devices) can have an impact on the aircraft.

- **Loadable system:** A loadable system consists of a **loadable replaceable unit (LRU)**, which is a modular component that is designed to be replaced frequently, and software that can be transferred to an LRU to modify system functionality. Software updates are used for:
  - *OPS and OPC:* update the operational program software/configuration (the operating system data and configurations of the LRUs).
  - *Databases:* update several databases, e.g., the engine data, flight management computer, and flight plans.
  - *AMI:* The airline modifiable information defines software generated by the operator to customize system operations, e.g., customization of the control display unit screens that are displayed to the flight crew.

  The loadable software updates can be transferred to the aircraft using a physical disk or wireless data loaders (e.g., Teledyne Technologies' LoadStar server).

5 ADVERSARIES AND THREAT ANALYSIS

5.1 Threat Actors

There is a wide range of possible adversaries; each type has a different motivation, purpose, and means at their disposal to achieve their goals. We defined six types of adversaries: (1) lone wolves with limited capabilities and financial motives, (2) profit-seeking criminals, (3) politically motivated Hacktivists and unorganized crime groups, (4) economically driven organized crime groups and cyber mercenaries, (5) state-sponsored organizations with advanced offensive capabilities and strategic goals, and (6) intelligence agencies with diverse expertise and objectives. An extended analysis of the adversaries can be found in the Supplementary material (Section 3).

5.2 Adversary Capabilities

To better understand the capabilities required to implement the various attacks, we analyze the different **adversarial capabilities (AC)** adversaries needed to execute various attacks. After examining the existing attacks on aircraft systems, we then classify the adversaries' capabilities based on the type of attack the capabilities facilitate. Figure 5 illustrates the division of the capabilities into groups.

(1) RF - Signaling capabilities

Radio frequency (RF) signaling, which refers to the capability of generating an electromagnetic signal, can be used as a type of communication. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3 kHz to 300 GHz. RF communication is one of the primary means by which an aircraft communicates with its surroundings and ground stations. Therefore, the attacker's ability to transmit signals over specific ranges allows him/her to communicate and influence different systems.

- *AC1 - Transmit HF signals:* An adversary can operate in the high frequency band (3–30 MHz), which is used by international shortwave radio stations in aviation communication. The HF

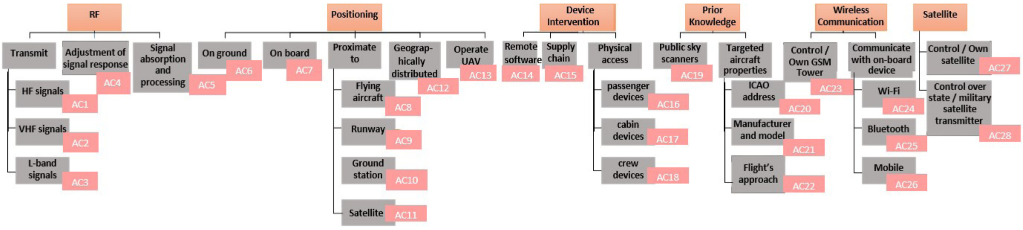


Fig. 5. Adversarial capabilities.

system on an aircraft enables two-way voice communication with ground stations or other aircraft and provides digitally coded signals for such communication.

- *AC2 - Transmit VHF signals:* An adversary can operate in the very high frequency band (30–300 MHz). Different systems use the frequencies in this range, e.g., in aviation, the range of 108–118 MHz is used by the VOR and ILS localizer as air navigation beacons, while 118–137 MHz is the airband used for air traffic control, and 121.5 MHz serves as an emergency frequency.
- *AC3 - Transmit L-band signals:* An adversary can operate in the L-band (1–2 GHz), which is the top end of the UHF band. The L-band is used by various aircraft systems, e.g., the ADS-B, TCAS, and DME.
- *AC4 - Adjust signal response:* An adversary can modify or synchronize responses to interrogations. This capability is required to influence systems that depend on the signal's time of arrival to determine the transmitter's location.
- *AC5 - Signal eavesdropping and processing:* An adversary can listen to, record, and decode signals using appropriate hardware (receivers), processors, and parsers (e.g., OpenSky data tools[10] for processing ADS-B traffic).

(2) Positioning capabilities

The adversary's position in relation to the attacked aircraft plays a significant role in terms of the attacker's ability to carry out the different attacks. This importance derives from the systems' mode of operation, the degree of eavesdropping, and the distance at which the threat actor operates. Moreover, an adversary's location directly impacts the attack duration and accuracy, as the aircraft is not a static target.

- *AC6 - On ground:* An adversary located on the ground is limited in his/her ability to perform a prolonged attack on an object moving at high speed and altitude. Ground attacks have the advantage of affecting a defined area.
- *AC7 - On board:* An adversary located on board has a high degree of destructive potential and long-term impact on the aircraft given his/her physical access to a variety of components. However, attackers are limited in terms of the means and tools that they can bring on board to perform the attack, and the degree of difficulty in concealing them is significant.
- *AC8 - Proximate to flying aircraft:* Proximity to the aircraft during flight enables the execution of attacks that depend on physical closeness to the aircraft (e.g., TCAS spoofing and jamming).
- *AC9 - Proximate to the runway:* Proximity to the runway is required to interfere with the aircraft's landing and takeoff (e.g., to abuse the ILS whose operation is activated in the

[10] https://opensky-network.org/data/data-tools

landing phase). The risk inherent in runway proximity is the high chance of being caught due to the presence of security personnel, detection systems, and so on.

- *AC10 - Proximate to the ground station:* Proximity to the ground station can enable the disruption of frequencies near the station and facilitate impersonation attacks by taking advantage of the physical proximity to a legitimate station.
- *AC11 - Proximity to a satellite:* Proximity to satellites poses a potential risk for attacks on entry points to various aviation technologies, such as ADS-B, ACARS, and GPS/GNSS. When a threat actor is physically close to a satellite, they may intercept or disrupt satellite communication, with serious implications for the safety and security of aviation systems.
- *AC12 - Geographically distributed:* A decentralized adversary can perform a synchronized attack in several places at a coordinated time to affect a target. For example, using the multilateration concept, an adversary can spoof GPS signals when they are distributed between different areas.
- *AC13 - Operate unmanned aerial vehicle:* Similar to the AC8 capability, the ability to operate an unmanned aerial vehicle enables the adversary to gain proximity to an aircraft during flight. This route to proximity has several advantages, e.g., it reduces the adversary's exposure.

(3) Device intervention capabilities

Device intervention refers to the ability to affect components and systems on the aircraft through direct or indirect access for the purpose of disrupting or injecting malicious payloads or backdoors.

- *AC14 - Remote software exploitation:* Remote exploitation of software can be a potential threat to aviation systems, as demonstrated in several recent studies. For example, in References [56] and [120], the authors investigated the security of mobile cockpit information systems and aviation software, respectively, and identified vulnerabilities that could be exploited by threat actors. Additionally, in Reference [54], the authors examined the exploitation of Apache Log4j2 in aeronautical, maritime, and aerospace communication. These studies highlight the importance of securing remote software access in aviation systems to prevent potential attacks that could compromise the safety and security of air travel.
- *AC15 - Supply chain:* An adversary can influence the supply chain of various technologies in aircraft to introduce infected components. This attack has vast potential for damage, and its implementation requires extensive knowledge of deployment and procurement processes.
- *AC16 - Physical access to passengers' devices:* Accessibility to passengers' devices can be used to harm components in the PIESD and PODD (e.g., the IFEC system).
- *AC17 - Physical access to cabin devices:* Accessibility to devices within the cabin can be used to harm components in the PIESD and AISD (e.g., the FDR).
- *AC18 - Physical access to crew devices:* Accessibility to the flight crew's devices can be used to harm components in the AISD and ACD (e.g., the EFB).

(4) Prior knowledge capabilities

Prior knowledge is a prerequisite for targeted attacks; gaining information about an aircraft and its trajectory can highly influence how successful and effective an attack can be.

- *AC19 - Public sky scanners:* Access to public databases and scanners, such as OpenSky Network and Flightradar24, enables access to real-time and historical information regarding flight routes and aircraft themselves.
- *AC20 - Obtain ICAO address:* Aircraft are assigned a unique ICAO 24-bit address upon national registration, which becomes a part of the aircraft's certificate of registration. Since

normally this address does not change, obtaining this information allows an adversary to target a specific aircraft and track its route.

— *AC21 - Obtain manufacturer and model information:* Obtaining information concerning the aircraft manufacturer and model can provide the adversary with details regarding the versions of aircraft components and the technologies deployed. An adversary can use such information to detect attack surfaces and design the most suitable vector to achieve his/her goals.

— *AC22 - Flight's approach route*: Obtaining the flight's approach route and the flight plan of a targeted aircraft can help an adversary determine the best location to carry out an attack. This type of information is necessary to interfere with the landing phase (e.g., ILS spoofing and GBAS).

(5) Wireless communication capabilities

Aircraft systems communicate remotely with satellites and ground stations. To access these systems, an adversary must possess the ability to communicate via wireless communication.

— *AC23 - Control/own GSM tower:* Owning a GSM (cell) tower is required for cellular communication with third-party service providers and onboard systems (e.g., IFEC).

— *AC24 - Communicate with an onboard device using Wi-Fi:* Wi-Fi capabilities can be used to influence onboard devices and to communicate with them, e.g., Wi-Fi vulnerabilities can be used to spread between devices connected to the same Wi-Fi network. For instance, the airport Wi-Fi network can be used as an attack surface to infect the devices of pilots and the flight crew (e.g., the EFB terminal).

— *AC25 - Communicate with an onboard device using Bluetooth:* Similar to AC24, an adversary can use Bluetooth exploits to infect nearby components (e.g., passengers' cellular devices).

— *AC26 - Communicate with an onboard device using mobile communications:* An adversary can use cellular communication (e.g., mobile-satellite services, such as Viasat and Intelsat) to maintain continuous communication with components on the aircraft.

(6) Satellite capabilities

Satellites capabilities are often powerful capabilities associated with state or military entities. The use of satellite capabilities can provide a wide range of attack surfaces and facilitate complex attacks that require high transmission intensity.

— *AC27 - Control/own satellite:* An adversary controlling a satellite can obtain accurate information from a wide geographical surface. In addition, such control provides the ability to transmit powerful signals to disrupt communication channels and provide inaccurate information to various stakeholders (e.g., aircraft and ground stations).

— *AC28 - Control state/military satellite transmitter:* An adversary controlling a powerful GPS transmitter can launch GPS spoofing or jamming attacks, as well as leverage military-grade SATCOM transmitters with strong amplifiers to establish secure communication over a wide range, potentially giving them an advantage in military operations.

Table 2 provides a comparison of the threat actors tiers based on the feasibility of acquiring different capabilities to implement an attack. In each cell, we indicate the degree of likelihood of possessing a capability, which ranges from certain likelihood to improbable likelihood.

6 REPORTED AVIONIC ATTACKS

We review existing cyber attacks on the various avionic systems, both attacks presented in academic research and by industry.

(1) ADS-B system cyber attacks: The ADS-B system lacks basic security mechanisms such as authentication, message integrity, and encryption. Because it is used to provide information in

Table 2. Comparison between the Ability of the Different Threat Actors to Achieve the Various Capabilities

Adversary	Adversary Capabilities																											
	RF					Positioning								Intervention					Knowledge				Comm				Satellite	
	AC1	AC2	AC3	AC4	AC5	AC6	AC7	AC8	AC9	AC10	AC11	AC12	AC13	AC14	AC15	AC16	AC17	AC18	AC19	AC20	AC21	AC22	AC23	AC24	AC25	AC26	AC27	AC28
Tier 1	●	●	●	●	●	●	◐	○	○	○	○	○	○	◐	○	○	○	○	●	●	◐	●	○	●	●	●	○	○
Tier 2	●	●	●	●	●	●	◐	○	○	○	○	●	○	◐	○	○	○	○	●	●	◐	●	○	●	●	●	○	○
Tier 3	●	●	●	●	●	●	●	●	○	○	◐	●	●	◐	○	●	○	○	●	●	◐	●	○	●	●	●	○	○
Tier 4	●	●	●	●	●	●	●	●	○	○	◐	●	●	●	◐	●	◐	●	●	●	●	●	●	●	●	●	○	○
Tier 5	●	●	●	●	●	●	●	●	●	●	●	●	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●
Tier 6	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

CERTAIN LIKELIHOOD (●), REASONABLE LIKELIHOOD (◐), IMPROBABLE LIKELIHOOD (○).

real time, these security gaps make the protocol's application in crowded skies risky, exposing the aircraft to different types of attacks. Costin et al. [14] showed that jamming, **denial-of-service (DoS)**, eavesdropping, spoofing, and impersonation attacks are both easy and practically feasible for a moderately sophisticated attacker to apply on the ADS-B system. Both *FIS-B* and *TIS-B* may be susceptible to similar attacks, since they are transmitted over an unauthenticated link and share the same data format. Eskilsson et al. [23] demonstrated how COTS transponders can be used to execute these attacks. A description of attack trees that describes the steps that need to be taken to implement the various attacks is provided in Reference [124], and attack scenarios are listed in Reference [68]. Khandker et al. [55, 56] analyzed the potential risks of attacks over the 1090ES and 978 UAT on systems based on ADS-B information, such as mobile cockpit information systems, as they rely on ADS-B technology. Additionally, the authors performed a practical evaluation of novel and known attacks on the ADS-B system via the RF link that affect various network, processing, and display subsystems.

(2) SSR system cyber attacks: The SSR system is prone to spoofing, jamming, over-interrogation, and radar loss. The SSR system is particularly vulnerable to interrogation overload, which can intentionally or unintentionally compromise its availability. [109]. High interrogation rates can cause transponders to restrict their sensitivity to interrogations and overheat and result in radar's inability to detect objects and its subsequent failure to appear on ATC displays. Osechas et al. [77] and Mostafa et al. [72] showed that SSR systems are prone to jamming attacks using a high-power transmitter at frequencies of 1030 MHz for interrogation and 1090 MHz for replies, and they introduced spoofing attack scenarios, e.g., injecting ghost aircraft into display screens.

(3) MLAT system cyber attacks: As a derivative of the MLAT mode of operation, the MLAT system is not affected by tampering attacks; since the only necessary information is the signal's time of arrival (i.e., ignoring the information passing through the signal), these attacks have not been the subject of prior research. In contrast, GPS spoofing techniques have been discussed in the literature, where they were shown to be a potential attack vector of the MLAT system. Moser et al. [71] demonstrated how a distributed and multi-instrument attacker could disrupt the system and spoof aircraft positions.

(4) TCAS/ACAS X cyber attacks: The TCAS system is designed to reduce the incidence of mid-air collisions with other aircraft; therefore, an attack that disrupts the system's operation or gives the attacker control of the system is a risk to human life. Hannah et al. [40] provided a description of the general landscape of the threat actors, their capabilities, and potential attacks. Both the SESAR and NextGen projects, which are the main modernization efforts in the aviation industry, plan to implement new operational concepts that will reduce the space between aircraft. In addition, the

FAA has funded research and development on ACAS X, which will likely replace the TCAS system. Research [104] has shown several attacks in which ACAS X can be triggered to erode the safety of the aircraft with the use of expensive equipment and distance constraints. While these attacks are difficult to implement, they are particularly dangerous, because once they have been successfully implemented, even an experienced pilot will have difficulty detecting the attack [102].

(5) Engine alerting system cyber attacks: The EICAS is used to display engine parameters and raises alerts regarding configuration or faults. Therefore, the EICAS/ECAM system can be exploited to manipulate the crew's behavior and affect the engine. Security researcher Chris Roberts claimed that he was able to spoof EICAS messages using unsupervised access to the FMS when he was on a flight; his claim was published by Kaspersky Labs [95].

(6) GNSS cyber attacks: As aviation operations increasingly rely on the GNSS to improve navigation performance and support ATC surveillance functions, GNSS vulnerabilities have the potential to cause widespread damage. Industry and academia have shown how jamming, intentional disruptions, and spoofing can influence the GNSS by utilizing the frequencies at which it operates (L1/L2), thus affecting many applications that use satellite information for the purpose of obtaining precise directions or location. Truffer et al. [119] illustrated how GNSS jamming can affect the position displayed on the FMS, while Tanil et al. [114] discussed the potentially catastrophic impact of GNSS spoofing in remote locations where traditional ILS services are unavailable and the landing approach depends on GBASs.

(7) Ground-based navigation system cyber attacks:

- The ILS is a radio navigation system that provides short-range guidance to the aircraft; therefore, exploitation of the system requires the attacker to be located near the aircraft, a requirement that puts the attacker at risk of detection. ILS spoofing was introduced at DEFCON [79] where it was shown that a successful attack requires the placement of a powerful antenna in very close proximity to the airport. There are a few examples in the literature of possible wireless attacks on the ILS, two of which were described in Reference [92]: an overshadow attack and a single tone attack. The overshadow attack requires the attacker to overpower legitimate ILS signals, which causes the receiver to process the attacker's signal. In a single tone attack, an attacker transmits a single frequency tone signal at lower strength than the legitimate ILS signal thus interfering with the original signal. A successful ILS attack can disrupt the aircraft's ability to land safely and can therefore result in property damage, injury, and even death.
- The VOR system is prone to jamming and spoofing attacks [12], but with the development of precision approach systems, the use of non-precision approach systems such as VOR and NDB has significantly decreased today; therefore, the threat posed by attacking this system does not have the potential for much damage.

(8) IFEC system cyber attacks: The IFEC system is troublesome in security contexts, as the system is directly accessible to the passenger and therefore prone to breaches. The IFEC system contains passengers' private information, and an adversary exploiting the system can gain control of the information passengers present on their in-flight screen. Moreover, the system is connected to the Wi-Fi network and network controller that connects the PIESD to the ACD network. Exploiting the IFEC could allow an attacker to pass from the PIESD to more sensitive networks. In References [52] and [1], the researchers showed how the IFEC system's vulnerabilities can be used to enable the attacker to pass between networks, access credit card details, and control cabin lighting and smart screens.

(9) SATCOM cyber attacks: The aircraft's SATCOM data link serves multiple systems (e.g., systems associated with aircraft control and crew devices); the data link is used for voice and data services, allowing an aircraft to communicate via satellite. An exploit targeting the SATCOM infrastructure (protocol, devices, services) can be used to gain remote control of various systems. The impact of SATCOM exploitation used to access passenger and crew devices was discussed in Reference [90], while Santamarta et al. [88, 89] described how an adversary can abuse SATCOM terminals to find a backdoor and retrieve hardcoded credentials. The authors claimed that an adversary exploiting SATCOM terminals may be able to intercept, manipulate, and block communications, and in certain cases, the adversary could remotely hijack the physical device (i.e., terminal).

(10) CPDLC system cyber attacks: The CPDLC system is unencrypted and therefore does not meet basic security and privacy requirements. Gurtov et al. [35] analyzed the CPDLC system's technical features and divided the possible threat actors into active and passive threat actors. The authors described how CPDLC system exploits can be used for eavesdropping, jamming, flooding, injection, alteration, and masquerading attacks, thus enabling an attacker to gain access and control messages, modify their content, and flood ground stations and aircraft with ghost messages. Di Marco et al. [20] presented a more sophisticated attack in which CPDLC systems can be attacked through a **man-in-the-middle (MITM)** attack with the use of open-source tools. In Reference [99], the author expanded on the MITM attack and explained how it can be used to take over an aircraft's communications and transmit CPDLC commands without alerting the legitimate controller. The feasibility of transmitting crafted CPDLC messages was discussed by Eskilsson in Reference [23].

(11) ACARS cyber attacks: The ACARS was developed with no security measures [103]. In recent years, several attack scenarios have been demonstrated by both security researchers and hackers in industry, e.g., in 2012, security researcher Teso showed how malicious ACARS messages can be crafted by an adversary and used to control the flight management system and thereby also control the pilot's displays and control systems, using just a simple mobile phone [115]. An introduction to cyber attacks on the ACARS was also presented at DEFCON [80]; one of the main points raised was the threat posed by the existing physical links between the communication management unit, which is used to route ACARS traffic, and the various avionic systems, whereby a vulnerability in the ACARS has the ability to affect many other systems. In Reference [83], the **European Union Aviation Safety Agency (EAS**A) addressed the ACARS cyber security threats, analyzing two scenarios: weight and balance update events and flight plan update events. The weight and balance update attack deals with an onground attacker who sends crafted ACARS updates to the aircraft, which can result in uncontrollable behavior of the aircraft. The flight plan update attack involves an attacker who transmits falsified flight plan data to a targeted aircraft; in this case, a successful custom attack requires prior knowledge regarding the aircraft's route. This type of attack can result in deviations from the desired route.

(12) Loadable cyber attacks: Aircraft systems can be modified using loadable software; this allows their configuration to be updated without physical intervention. Modifications and replacements can be made via remote wireless services or pluggable devices. Security researchers have demonstrated they can interfere with the update process by impersonating a legitimate operator or obtaining unauthorized physical access. With the ability to update loadable software, they showed how the navigation database [4] on the flight management system can be manipulated, as well as how an attacker can take control of onboard systems using an AMI wireless data loader [116].

(13) EFB cyber attacks: The EFB connects to multiple systems and has the ability to access those systems and multiple applications, including: the flight management system, passenger information list, performance applications, technical logs, weight and balance applications, and flight planning application. Turtiainen et al. [120] investigated EFB applications and GDL 90 decoding software, which led to the practical demonstration of DoS attacks on popular EFB software running on mobile devices. The portable nature of the EFB and its ability to connect to public networks put the EFB tablet at high risk. For example, exposure to public networks may allow the system to be attacked through Wi-Fi vulnerabilities [1]. Despite the importance and vulnerability of the system, surveys show that most airlines do not have a cyber security plan in place for the tablet-based EFB used by their pilots [58]. An example of attack vectors for connecting the FMS, retrieving sensitive data, accessing flight planning and navigation applications, and even modifying weight and balance calculations are presented in Reference [78].

Table 3 contains a list of the attacks known to academia and industry with a short description of the sub-technique used in the attack. We used the STRIDE [97] threat model to group the attacks into different categories. This model consists of six threat categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges. The table includes references for academic studies and industry implementations; these are the *procedures* in which the various cyber attacks are described and implemented, the required capabilities (listed in Section 5.2) required, the vulnerabilities exploited, and the threat posed by the attack according to the STRIDE threat model.

7 EXTENDING MITRE FRAMEWORK FOR AVIONICS

To standardize the knowledge on and understanding of threats to cyber security in the avionics field, we followed the **ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)** model utilized by MITRE [69] to classify attack tactics, techniques, sub-techniques, and procedures. The MITRE model systematically describes the adversary's actions to be executed within the target domain or on the target system or device from an adversary's perspective. MITRE ATT&CK covers the enterprise, mobile, and industrial control system fields. In this section, we divide existing and possible actions in the aviation domain into a variety of tactics, techniques, and sub-techniques.

- **Tactics** represent the *"why"* of the technique: the adversary's tactical goals during an attack.
- **Techniques** represent *"how"* an adversary achieves a tactical objective by performing an action.
- **Sub-techniques** are more specific descriptions of the adversarial behavior used to achieve a goal, while techniques represent the broad actions an adversary takes to achieve a tactical goal,
- **Procedures** are the specific implementation the adversary uses to perform techniques or sub-techniques. In this work, a procedure is a reference to the implementation of a technique as applied in academic research or in industrial applications.

We opted to align our taxonomy with the ATT&CK model, because the attack sequence diagram can indicate the adversary's behavior and capabilities, limitations on how adversaries (or a specific group/APT) can compromise the system, and the loosely protected systems and connections that require more rigorous security. Moreover, the matrix representation helped us build a systematic categorization and taxonomy based on the known attacks and retain the attack phases as a sequence chart. The matrices in Figure 6 represent the various tactics in the avionics field (columns) and the techniques used to achieve them (the individual cells).

7.1 Reconnaissance

Using the reconnaissance tactic, the adversary tries to gather information and identify and select targets. The adversary collects information that can be used to support the targeting and selection

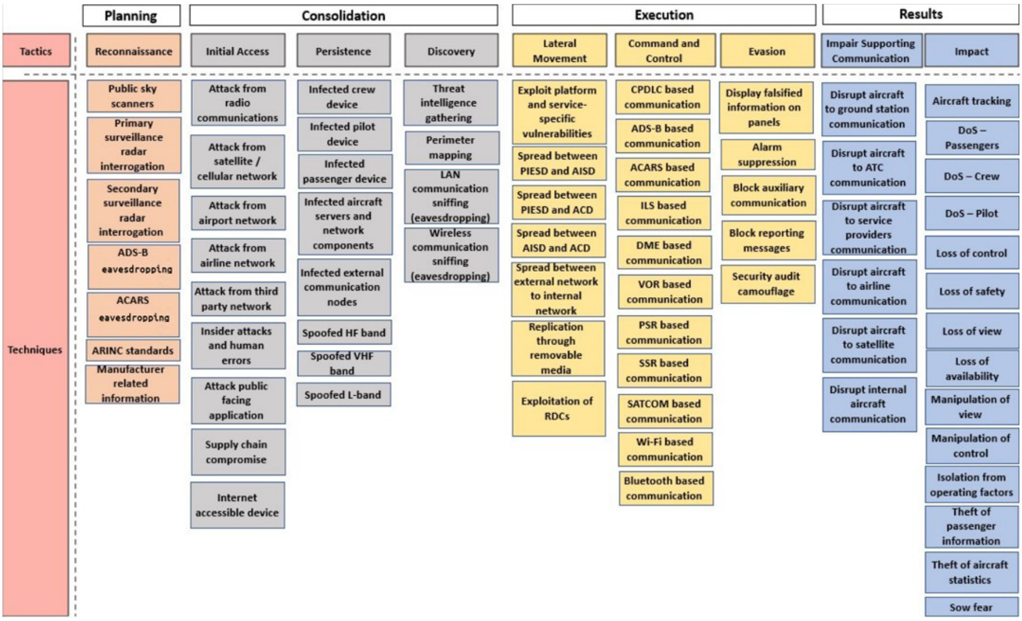
Table 3. Risk Assessment of Aviation Systems—Known Attacks, Impact, Vulnerabilities, Required Capabilities, Target Assets, and Identified Threats

Asset	Technique	Procedures	Sub-Technique	Impact	Capabilities	Vulnerabilities	STRIDE
ADS-B	Aircraft reconnaissance	[14, 68, 124] [23, 120]	Receive, parse, and collect messages with a radio receiver	Aircraft tracking	AC5 , AC6, AC19	No Confidentiality	Information disclosure
	Aircraft flood denial		Create destructive signal interference (1090 MHz)	Loss of view	AC3, (AC6 | AC7)	No Availability	Denial of service
	Ghost aircraft injection		Transmit signal that conforms to a protocol and mirrors legitimate traffic	Manipulation of view	AC3, (AC6 | AC7)	No Authentication	Spoofing
	Virtual trajectory modification		Bit flipping to modify ADS-B messages	Manipulation of control	AC3, AC5, (AC6 | AC7)	No Integrity	Tampering
	Aircraft disappearance		Transmit destructive or constructive interference	Loss of view	AC3, AC5, (AC6 | AC7)	No Availability	DoS
MLAT	Missynchronization	[44, 71]	Block GPS signals to interfere with MLAT ground receiver synchronization	DoS – Pilot	(AC2 | AC3), AC12	No Authentication	Spoofing
	Spoof locations		Use multiple devices to spoof GPS signals	Manipulation of view	(AC2 | AC3), AC12	No Authentication	Spoofing
SSR	Overloading interrogations	[72, 77, 109]	Flood interrogations at 1030 MHz to exceed the acceptable standard	Loss of view	AC3, (AC6 | AC7)	No Availability	DoS
	Block SSR signals		Delete SSR transmissions		AC3, (AC6 | AC7), AC20	No Authentication	Spoofing
	Ghost aircraft		Spoof fake SSR transmissions	Manipulation of view	AC3, (AC6 | AC7)	No Integrity	Tampering
	Tampering with SSR transmission		Use an SDR that an attacker can alter, block, and inject Mode A, Mode B, Mode C, and Mode S messages		AC3, (AC6 | AC7)		
ILS	Overshadow	[79, 92]	Overpower legitimate signals using specially crafted ILS signals	Loss of safety	AC2, AC6, AC9 AC21, AC22	No Availability	Spoofing
	Single tone		Cause deflections in the course deviation indicator needle				
VOR	Aircraft reconnaissance	[12, 72, 92]	Receive, parse, and collect messages with a radio receiver	Aircraft tracking	AC2, AC5	No Confidentiality	Information disclosure
GNSS SBAS ABAS GBAS	Disrupt landing approach	[74, 114] [81, 119]	Spoof GNSS and GNSS augmentation system (SBAS, ABAS, GBAS) using GPS signals	Loss of safety	AC3, AC20 AC27, AC28	No Availability	DoS
	Deceive a GPS receiver		Transmit a slightly more powerful signal than that received from the GPS satellites	Manipulation of view			
	Display unreliable position information		Transmit interference signals to affect displayed FMS position data			No Integrity	Tampering
DME	Aircraft reconnaissance	[38]	Receive, parse, and collect messages with a radio receiver	Aircraft tracking	(AC2 | AC3), AC5, AC10	No Confidentiality	Information disclosure
ACARS	Aircraft reconnaissance	[20, 23, 99] [80, 103, 115]	Receive, parse, and collect ATC, AOC, AAC, OOOI messages with a radio receiver	Aircraft tracking	AC5, AC6	No Confidentiality	Information disclosure
	Bogus flight plan update		Issue and transmit malicious message (ATC, AOC, AAC) that conforms to a protocol and mirrors legitimate ACARS traffic	Loss of control	(AC1 | AC2), AC6, AC11, AC20, AC22	No Authentication	Spoofing
	Weight and balance manipulation				(AC1 | AC2), AC6, AC11, AC20, AC21		
	Malicious requests for passenger information			Theft of passengers' information	(AC1 | AC2), AC6		
	Distort weather information			Loss of view			

(Continued)

Table 3. Continued

CPDLC	Read and collect control messages	[14, 68] [23, 100]	Receive, parse, and collect messages with a radio receiver	Theft of aircraft statistics	AC5	No Confidentiality	Information disclosure
	Impersonate an ATC		Craft and inject messages claiming to be a CPDLC unit on the ATC end	Manipulation of control	AC2, AC20	No Authentication	Spoofing
	Disrupt communication between aircraft and an ATSU		Block legitimate messages and compromise an ongoing CPDLC connection handover	DoS - Pilot	AC2, AC8, AC20	No Integrity	Tampering
	Selective message jamming		Block session termination message			No Availability	DoS
	Aircraft flood denial		Reduce CPDLC channel's capacity by filling the channel with noise	Isolation from operating factors			
	Aircraft ghost messaging		Transmit unauthorized CPDLC messages	Manipulation of control	AC2, AC20	No Authentication	Spoofing
	Issue incorrect commands		Transmit unauthorized CPDLC messages		AC2, AC20, AC21		
SATCOM	Disrupt, intercept, or modify in-flight Wi-Fi	[88–90]	Block traffic from Satcom Direct router to cause a denial of service	DoS - Passengers	AC2,(AC27 |AC28)	No Availability	DoS
	Control crew and passenger devices		Craft and inject information consumed by passengers' devices	DoS - Passengers and crew			
	Compromise aircraft SATCOM to block traffic		Transmit SATCOM communication using destructive interference	Isolation from operating factors			
Loadables	Inject false data to the FMS	[4, 16, 116]	Load configurations to the FMS	Manipulation of control	AC14, (AC16,AC17,AC18) (AC24|AC25|AC26)	No Integrity	Tampering
	Update the FMC with corrupted navigation data		Load configurations to the FMCS and NDB				
	Remotely update malicious AMI		Load malicious malformed airline modifiable information				
TCAS ACAS X	Aircraft reconnaissance	[32, 40, 100] [102, 104]	Receive, parse, and collect messages with a radio receiver	Theft of aircraft statistics	AC5, AC6	No Confidentiality	Information disclosure
	Ghost aircraft		Respond to interrogations to maintain false track and declare a threat	Loss of safety	AC3	No Authentication	Spoofing
	Alpha-beta drop		Issue corrupted response on behalf of targeted aircraft to damage its reliability		(AC6|AC13)	No Availability	DoS
	Address flooding		Craft and inject multiple aircraft acquisition squitters with unique ICAO address numbers		AC20	No Authentication	Spoofing
Engine Alert	Engine data manipulation	[21, 95]	Inject malicious engine alerting messages	Loss of safety	AC7, AC17		
IFEC	Display messages on panels	[1, 52]	Gain control of passenger's display systems	Sow fear	AC3, AC7, AC17 (AC23|AC26 | AC27)	No Integrity	Tampering
	Control cabin lightning		Gain control of cabin attendant panel			No Authorization	Elevation of privileges
	Access passenger's credit card details		Collect information from IFEC servers	Theft of passengers' information		No Confidentiality	Information disclosure
EFB	Remote control	[58, 78, 123] [56, 120]	Exploit Bluetooth, Wi-Fi, or cellular link	Loss of control	(AC24|AC25|AC26)	No Integrity	Tampering
	Retrieve manuals and technical logs		Collect stored information on applications	Theft of aircraft statistics	AC18, (AC24 | AC25 | AC26)	No Confidentiality	Information disclosure
	Modify flight plan and navigation data		Hack into hosted applications and control their actions; modify navigation database information	Manipulation of control		No Authorization	Elevation of privilege
	Install malicious application		Through removable media/social engineering/malicious device			No Integrity	Tampering
	Control cabin lightning		Abuse hosted applications and modify their storage and responses	Sow fear		No Confidentiality	Information disclosure



	Planning	Consolidation			Execution			Results	
Tactics	Reconnaissance	Initial Access	Persistence	Discovery	Lateral Movement	Command and Control	Evasion	Impair Supporting Communication	Impact
Techniques	Public sky scanners	Attack from radio communications	Infected crew device	Threat intelligence gathering	Exploit platform and service-specific vulnerabilities	CPDLC based communication	Display falsified information on panels	Disrupt aircraft to ground station communication	Aircraft tracking
	Primary surveillance radar interrogation	Attack from satellite / cellular network	Infected pilot device	Perimeter mapping	Spread between PIESD and AISD	ADS-B based communication	Alarm suppression	Disrupt aircraft to ATC communication	DoS – Passengers
	Secondary surveillance radar interrogation	Attack from airport network	Infected passenger device	LAN communication sniffing (eavesdropping)	Spread between PIESD and ACD	ACARS based communication	Block auxiliary communication	Disrupt aircraft to service providers communication	DoS – Crew
	ADS-B eavesdropping	Attack from airline network	Infected aircraft servers and network components	Wireless communication sniffing (eavesdropping)	Spread between AISD and ACD	ILS based communication	Block reporting messages	Disrupt aircraft to airline communication	DoS – Pilot
	ACARS eavesdropping	Attack from third party network	Infected external communication nodes		Spread between external network to internal network	DME based communication	Security audit camouflage	Disrupt aircraft to satellite communication	Loss of control
	ARINC standards	Insider attacks and human errors	Spoofed HF band		Replication through removable media	VOR based communication		Disrupt internal aircraft communication	Loss of safety
	Manufacturer related information	Attack public facing application	Spoofed VHF band		Exploitation of RDCs	PSR based communication			Loss of view
		Supply chain compromise	Spoofed L-band			SSR based communication			Loss of availability
		Internet accessible device				SATCOM based communication			Manipulation of view
						Wi-Fi based communication			Manipulation of control
						Bluetooth based communication			Isolation from operating factors
									Theft of passenger information
									Theft of aircraft statistics
									Sow fear

Fig. 6. Taxonomy—aviation matrix tactics and techniques.

of attack techniques in other phases of the attack lifecycle (i.e., locating potential target systems/networks for initial access). The adversary can use multiple techniques:

Public sky scanners: The adversary can search for available information using online flight trackers (i.e., OpenSky,[11] Flightradar24[12]). Information about flight plans, both **visual flight rules (VFRs)** and **instrument flight rules (IFRs)**, can also be found online using services such as SkyVector.[13]

PSR interrogation: The PSR surveillance sensor is used to locate aircraft without the need for any onboard equipment; therefore, an attacker can use PSR equipment to gather information about the aircraft's location without any dependence on its components.

SSR interrogation:The ability to use SSR interrogation depends on the components installed on the aircraft, as the SSR relies on targets equipped with a radar transponder. Aircraft equipped with transponders are capable of operating in different modes. Mode A equipment only transmits an identifying code, Mode C equipment automatically obtains the aircraft altitude or flight level, and Mode S equipment has altitude capability and enables data exchange.

ADS-B eavesdropping: ADS-B is a surveillance technique that relies on aircraft broadcasting their identity, position, and other information obtained from onboard systems (e.g., GNSS). An adversary can capture broadcast ADS-B messages using an ADS-B IN receiver and obtain information about an aircraft's GPS location, altitude, ground speed, and more.

ACARS eavesdropping: ACARS data processing can provide an adversary with extensive information about air traffic control, aeronautical operational management, and airline administrative control, e.g., route updates, weather updates, and even information about special passengers.

[11] https://opensky-network.org/
[12] https://www.flightradar24.com/
[13] https://skyvector.com/

ARINC standards: The adversary can gather information about the ARINC standards on avionics, cabin systems, protocols, and interfaces provided by Rockwell Collins.[14]

Manufacturer-related information: To obtain supporting information that can be leveraged by the adversary in other attack phases. Collecting information regarding relevant devices implemented onboard is crucial and can be found on different forums and sites, i.e., the FAA engineering database [25], specification forums [106], manufacturer specifications,[15] and patents (e.g., Boeing's patent for the e-Enablement network implementation [13]).

7.2 Initial Access

With the initial access tactic, the adversary tries to establish an attack vector by gaining access to the targeted system/environment. By examining all means of access into the system from the outside world and public network, various entry vectors that enable an adversary to obtain an initial foothold in an aviation system could be identified.

Attack via radio communication: Radio communication typically refers to ground-based communication using HF and VHF to communicate with the aircraft. This method of communication can be utilized by an attacker to enter the aircraft's network by transmitting to various aircraft systems (e.g., ILS, ACARS, VOR, DME, ADS-B) using simple, commercially available equipment. While using these means of communication may require the attacker to have a line of sight to the target system, it should be noted that an attacker could potentially use a drone/UAV/UAS or satellite to overcome the line-of-sight limitation and access the aircraft through communication channels that enable remote control or transmission to a distant intermediary. In this scenario, the attacker could operate from a remote location while still being able to exploit vulnerabilities in the communication channels.

Attack from satellite/cellular network: The aircraft systems use satellites for communication and navigation. For example, satellite voice-equipped aircraft can initiate calls using Inmarsat[16] or Iridium[17] assigned security phone numbers, and IFEC in-flight Wi-Fi uses a satellite-based Wi-Fi system (e.g., Viasat[18]). In addition, air traffic management systems, such as the ADS-B and CPDLC, use satellite data links. To this end, satellite range control can provide a diverse attack surface for PIESD and ACD networks while controlling a wide geographical area.

Attack from airport network: While aircraft connect to the airports' wireless networks for maintenance, both wireless and cellular connections can be compromised by adversaries. Examples of potential devices that can be exploited using wireless vulnerabilities (e.g., KRACK vulnerability [28]) include standalone EFB tablet devices, the aircraft's TWLU used for airport gatelink connectivity, the connectivity and CWLU used for maintenance laptop connectivity and the wireless data loaders used for software updates.

Attack from airline network: By penetrating the airline network, an attacker can achieve wide access to the aircraft it operates while interfering with control, operation, and maintenance processes. In addition, an attacker can tamper and interfere with pilot communication using systems such as VHF voice CPDLC, and ACARS.

Attack from third-party networks: Many services have access to various systems and different functions in the aircraft. These services can be used to bypass aircraft systems. Examples of

[14] https://www.rockwellcollins.com/
[15] https://modernairliners.com/
[16] https://www.inmarsat.com/
[17] https://www.iridium.com/
[18] https://www.viasat.com/enterprise-and-mobility/aviation/commercial/

possible targeted services include maintenance services (e.g., ACT services[19]) management services (e.g., Teledyne Technologies[20]) flight-planning services (e.g., Honeywell,[21] Lido[22]) support services (e.g., AMETEC[23]) and development services (e.g., Keysight[24]).

Insider attacks and human errors: Insider attacks involve both intentional attacks and unintentional mistakes by a human with access to any component of the avionics ecosystem. An insider can be a crew member, maintenance worker, or any other airport/airline employee. Human errors and insider assistance can be used to bypass various security measures and gain physical access to components, and they are often leveraged by adversaries as initial access techniques.

Public-facing application: The adversary can exploit a public-facing application that does not require special access privileges; such applications can be used to seek and obtain access points to aircraft systems. Examples of potential surfaces are the EFB application server/store, administration websites, and airline websites.

Supply chain compromise: Supply chains can be used to gain access to platforms around the world. Devices and software can become compromised if an adversary tampers with the manufacturing process of a product by installing a rootkit or hardware-based spying component. The targeted devices include various sensors, **remote data concentrators (RDCs)**, actuators, cabin devices (e.g., IFEC cell modems, SATCOM modems, and smart monitors).

Internet accessible devices: An adversary can infect Internet-accessible devices such as an IFEC content server or maintenance laptop. More sophisticated vectors can target SATCOM antennas, as illustrated by Santamarta et al. [88].

7.3 Persistence

The persistence tactic aims to allow continuous access to aviation systems. To maintain access in the face of system restarts, credential changes, and other interruptions, there is a variety of actions an adversary can perform, ranging from changing settings to interfering with system files or hardware.

Infected crew device: An adversary can gain access to the flight crew terminals or their personal devices (e.g., mobile phones) thus ensuring consistent access to the aircraft.

Infected pilot device: Infecting pilot-owned devices, such as the EFB tablet, ensures network access to the aircraft's core systems and information on the pilot's activities during the flight.

Infected passenger device: Attacking passenger devices allows persistence but only for the duration of the passenger's flight. Connectivity to a passenger's device may allow connectivity to the cabin systems, particularly the IFEC system, and the aircraft's Wi-Fi network.

Infected aircraft servers and network components: To gain access to the aircraft servers and network components, adversaries can use different techniques in the ATT&CK enterprise taxonomy, for example:

- *Modify configurations* - An adversary can gain access to a system by editing the configuration file that defines its features. Examples of configuration files in the aircraft core systems

[19] https://www.actservices.de/
[20] https://www.teledyne.com/en-us
[21] https://aerospace.honeywell.com/
[22] https://www.lhsystems.com/solutions/flight-operations-solutions/lido-flight-planning-solutions
[23] https://www.ametekmro.com/
[24] https://www.keysight.com/us/en/home.html

include loadable media CONFIG.LDR and EXCONFIG.LDR files, **operation program configuration (OPC)** files, and **airline modifiable information (AMI)** files.

- *Modify programs and applications* - An adversary can modify a program to affect the way it interacts with other systems and devices. Modified applications can be used to add new logic that enables persistence on the host device. For example, the EFB device has many applications (e.g., weight and balance applications, flight planning applications, and performance applications) that can serve as an attack surface.
- *System firmware* - Device firmware updates can be delegated using a software update package provided remotely [47].
- *Module firmware* - Device firmware such as software loadables, LRUs, and other modular hardware devices can be installed or modified to achieve persistence and provide secret access points. The vulnerability of firmware in embedded devices has long been established, as evidenced by a study conducted by Costin et al. [16]. Their extensive research delved into the security of embedded firmware, revealing that more than 690 firmware were affected by at least one vulnerability.

Infected external communication nodes: An adversary can obtain an allegedly authorized data link by penetrating trusted remote service networks such as the CPDLC provider's network, the ATN network (VHF data link operated by ARINC and SITA), and FANS network (satellite communications provided by Inmarsat). Moreover, an adversary can launch rogue endpoints, e.g., rogue GSM towers that communicate with the IFEC system's cell modem or a ground station that transmits FIS-B and TIS-B messages.

Manipulating HF band: By falsifying or manipulating signals within the HF communication range an attacker can maintain contact with an aircraft at short range.

Manipulating VHF band: By falsifying or manipulating signals within the VHF communication range, an adversary can operate and affect various systems (e.g., the ILS, DME, and VOR systems) utilizing the reception range of the system. Sathaye et al. [92] demonstrated an overshadow attack on the ILS system from a distance of 9.45 kilometers.

Manipulating L-band: By falsifying or manipulating signals within the UHF communication range and its upper bound (L-band) communication range, an adversary can operate and influence satellite-based systems (e.g., the TCAS, ACAS X, and ADS-B systems) from far away. For instance, the maximum distance of TCAS is 30 nautical miles [122]; ADS-B has much better coordinate resolution and an effective range of 100–200 nautical miles [3].

7.4 Discovery

To gain knowledge on the environment, adversaries use the discovery tactic. This tactic consists of a collection of techniques designed to allow an attacker to determine the options for advancing, what measures to take, and how to spread within the network.

Threat intelligence gathering: An adversary can use dedicated search engines (e.g., Shodan[25] and Censys[26]) that gather information about vulnerable devices and networks to identify exposed critical nodes that are sometimes visible on public networks due to misconfigurations.

Perimeter mapping: Devices' communication patterns can be discovered using connection enumeration. An adversary can use different tools to determine the role of a device on the network and identify its connections to other systems. Moreover, adversaries may attempt to obtain a list

[25] https://www.shodan.io/
[26] https://censys.io/

of different systems and components using network identifiers (e.g., MAC addresses, TTL values). By obtaining IP addresses and identifying the type of operating system, an adversary can choose how and where to spread.

LAN communication sniffing (eavesdropping): Adversaries can use sniffing tools to monitor or capture information transmitted through the network, e.g., eavesdrop file transfer services traffic to discover data and credentials. Sniffing can also be useful for detecting the current aircraft state by capturing the OOOI events from sensors and gateways.

Wireless communication sniffing (eavesdropping): Adversaries can use the wireless range to obtain location signals, e.g., Mode-S (1030/1090 MHz frequency) or report ACARS signals at a frequency of 131.550 MHz.

7.5 Lateral Movement

The lateral movement tactic consists of techniques used by adversaries to spread between components in the aircraft. An adversary might want to move between different domains to gain access to more critical systems, e.g., move from the PIESD to the AISD or ACD. This tactic is usually applied after performing discovery techniques and identifying a target destination.

Exploit platform and service-specific vulnerabilities: While many components within the aircraft run popular real-time operating systems (e.g., VxWorks, QNX, ThreadX), significant weaknesses have been found in some of these systems. For example, the Armis Security team identified 11 vulnerabilities (URGENT/11) [93] in the VxWorks OS kernel, e.g., an opcode stack overflow that can lead to arbitrary code execution. To abuse an existing platform, an adversary can use different utilities to inject hooks or abuse APIs (e.g., Frida[27]).

Spread between the PIESD and AISD: As described above in Section 4.1, there are overlapping connections between both networks (PIESD and AISD). Since the AISD contains information services systems, the attacker can use the AISD network to communicate with third-party providers to gain accessibility and cause information leakage or as part of further lateral movement to the ACD network.

Spread between the PIESD and ACD: The passenger-related networks and the control systems should be separated. However, in practice, there are overlapping connections between the networks (e.g., the CSS has dual connections: a connection to the in-flight entertainment system and a link to the ACD switch designed for transferring audio between the pilot and the cabin.

Spread between the AISD and ACD: As described in Section 4.2, there are overlapping connections between the networks for non-essential applications (e.g., the cabin services system and flight deck recorder) used to connect the cockpit systems to other aircraft systems. An adversary that reaches the ACD network can access the core air traffic, information and navigation systems.

Spread between the external network and internal network: As described in Section 4.3, the aircraft serves as a flying domain controller; therefore, it depends on communication between the ground, its surroundings, and satellites. Thus, an external network that provides access to the internal network of an aircraft can provide an attacker with many access points.

Replication through removable media: To achieve access to hardened components/networks (e.g., air-gapped devices), adversaries may opt to choose the replication through removable media technique. Aircraft contain different systems with portable USB connections (e.g., cabin panels,

[27] https://frida.re/

smart screens, EFB tablets, and IFEC crew terminals), and shellcode and payloads can be activated when devices are plugged in via AutoRun [117].

Exploitation of RDCs: An adversary can abuse RDCs to access controllers, systems, and actuators. For example, the ability to control the **actuator control electronics unit (ACE)** gives the adversary direct control of the flight control surface by allowing the adversary to obtain all inputs and communicate with the flight computer.

7.6 Command and Control

After initial access to one of the aircraft systems has been obtained and various types of utilities (tools and malware) have been distributed between the aircraft components, adversaries must establish a communication channel to command and control the scattered assets. To create a stable method of communication, an attacker will usually try to find a stealthy or seemingly legitimate method of communication. To achieve this goal, an adversary can abuse communication methods embedded in the aircraft's systems (termed as *Standard Protocol/Datalink Misuse*). To apply this technique, an adversary can utilize aircraft systems and protocols that communicate with the outside world (e.g., satellites, ground stations, airports, airlines, service providers) to receive or transmit information. The following air-to-ground communication methods provide examples of the channels an adversary can use for command and control purposes:

VHF/HF/SATCOM-based communication - Used by the ACD as part of the flight and embedded control systems and cabin systems (e.g., ADS-B, CPDLC, ACARS).

Wireless LAN-based communication - Used by the AISD as part of administrative support, flight support, and maintenance (e.g., communication with airport network).

Broadband/cellular-based communication - Used by the PIESD as part of the in-flight entertainment and passenger Internet systems. All of these means of communication can allow an adversary to transmit and receive data from different ranges with varying degrees of accuracy.

7.7 Evasion

The evasion tactic consists of techniques that adversaries use to avoid detection once they have gained access to the system. Usually these tactics' techniques require active steps to conceal the adversary's presence or to remove evidence of their presence.

Display falsified information on panels: Adversaries can modify the content of different panels (cockpit control panels, crew terminal panels, EFB applications, graphical interfaces) to disrupt the behavior of the crew or pilot or evade detection.

Suppress alarms: Adversaries may manipulate failure alert systems (e.g., collision or engine failure alert systems) to avoid the detection of system damage.

Block auxiliary communication: Adversaries can block the CPDLC to disable communication between an aircraft and the ground station.

Block sensor data: Adversaries can block sensor or RDC communication to interfere with signals that indicate the aircraft state.

Spoof/block reporting messages: Adversaries can spoof and block ACARS signals, OOOI events (engine performance, monitoring, fault reports, fuel status reports, selective calls, passenger services, maintenance reports, and other information such as load and balance) to hide actions that affect the aircraft state [21, 131].

Security audit camouflage: Security audit camouflage refers to any means by which an adversary can remain undetected from audit measures within the systems and software. The following methods are taken from the ATT&CK enterprise framework, as currently there is no evidence for audit camouflage in avionic systems, however, at the same time the actions required to prevent detection are similar in enterprises and avionic systems:

- *Masquerading*: Adversaries can use masquerading techniques to disguise a malicious application or executable as another file (e.g., log files, config files).
- *Indicator removal on host*: Adversaries may delete or alter artifacts on a host system, including logs or captured files, in their efforts to cover their tracks.
- *Rootkit*: Rootkits are programs that hide their existence and the presence of malware by intercepting the operating system's API calls that supply relevant information. Adversaries can use rootkits to hide their malicious tools and payloads.
- *Exploitation for evasion*: Adversaries can exploit a software vulnerability to take advantage of an error in a program, a service, the operating system, or kernel itself, to evade detection.

7.8 Impair Supporting Communication

This tactic is an addition to those proposed by ATT&CK. Avionic systems consists of various communication, navigation, display, and management systems, which are integrated in aircraft to perform individual functions. The proper functioning of these systems depends on continuous operation and collaboration with external services (e.g., ground stations, satellites, airports, airlines, operators). In a multi-stage attack vector, one of the attacker's goals will likely be to disrupt such collaboration and the supporting systems. Some of the types of collaborations an adversary can disrupt are presented below:

Collaboration between aircraft and ground station - Disrupting ground-based and navigation communication aids has an impact on the navigation systems, e.g., the DME, VOR, NDB, and ILS.

Between aircraft and ATC - Disrupting communication with ATC ground stations usually refers to VHF and L-band spoofing or jamming, e.g., interference with ADS-B, FIS-B, TIS-b, SSR interrogations. Disruption of these collaborations is highly problematic, as it affects the perception of the pilot, crew, and operators regarding the aerial state.

Collaboration between aircraft and service providers - Disrupting communication with third-party providers of satellite services (e.g., Inmarsat, Iridium, Viasat, Teledyne Technologies, Honeywell, AMETEC, Keysight) can have major impact on an aircraft's ability to communicate with the outside world.

Collaboration between aircraft and airlines - Disrupting communication channels with airlines, e.g., **airline operational control (AOC)** and **airline administrative control (AAC)** messages.

Between aircraft and satellites - An adversary can disrupt **satellite communication (SATCOM)** by using a powerful transmitter to beam a jamming message towards the satellite.

Internal aircraft connections - Disrupting communication between internal systems and the network that transfers information between them (e.g., by harming the AISD or PIESD switches).

7.9 Impact

As described in Section 5, adversaries have different goals with regard to impact. The impact tactic consists of techniques the adversary uses to disrupt, compromise, destroy, and manipulate the integrity and availability of an aircraft's components and systems. While the effect some impact techniques have on those on the aircraft is less obvious, such techniques can directly affect the privacy or personal safety of those onboard.

Aircraft tracking: Adversaries can determine the exact location of an aircraft and follow its route.

DoS - Passenger: Adversaries can control cabin operations (e.g., the passenger panels, Wi-Fi, and content server).

Dos - Crew: Adversaries can control the IFEC crew terminal, interfering with the cabin crew's ability to control the IFEC system.

DoS - Pilot: Adversaries can take control of the cockpit control panels and EFB device to interfere with the pilot's ability to make decisions and act on them.

Loss of control: Adversaries can obtain control of different sensors and actuators that are crucial for the aircraft's functionality. For example, access to the ACE component can be used to gain full control of actuators and RDCs.

Loss of safety: Adversaries can cause dangerous situations that affect the safety of the passengers and crew, such as landing failure (spoofed/jammed ILS signals [92] or GPS signals [61, 67]), triggering false TCAS alerts or harming the TCAS system [39, 40, 79], manipulating the engine alerting system or navigation system, or interfering with the ADS-B surveillance system [14].

Loss of availability: Adversaries may attempt to disrupt essential components or systems to prevent the proper transfer of information by interfering with the channels used to communicate with ground stations (e.g., SATCOM/HF/VHF).

Manipulation of view: Adversaries can interfere with the pilot's view, causing a sustained or permanent loss of view by compromising the flight deck instrument display system (EFIS). The EFIS normally consists of a **primary flight display (PFD)**, **multi-function display (MFD)**, and an engine indicating display.

Manipulation of control: Adversaries can manipulate the set point values and parameters, such as the intermediate waypoints in the navigation database. Since waypoints can be used to change routes, modifying them can affect the flight route. As a case in point, Turtiainen et al. [120] demonstrated an exploitation chain that started with exploiting the ADS-B protocol and ended with the control of autopilot systems by manipulating GDL-90 inputs that directly interface with the autopilot and resulted in manipulation of control.

Isolation from operating factors: Adversaries may try to interfere with the ability of the pilot and flight crew to receive messages from ground stations and operators to ensure their complete isolation and prevent them from receiving guidance or assistance.

Theft of passenger information: Adversaries can exploit IFEC systems to steal passengers' data (i.e., credit card details, passport numbers).

Theft of aircraft statistics: Access to information stored on the aircraft and collected from the various sensors may be used by adversaries to obtain information about the aircraft's activity for various malicious purposes, including industrial espionage.

Sow fear: Adversaries can take control of the aircraft's smart monitors and display messages.

8 E-ENABLED AIRCRAFT SYSTEM MITIGATION TECHNIQUES

To increase efficiency in modern aircraft, the aviation industry is using electronic data exchange and digital network connectivity, with the IoT playing a significant role. Although this provides many benefits, it increases the risk of cyber attacks on aircraft systems. To address this issue, various methods have been proposed to secure avionic systems and mitigate the associated risks. Table 2 in the Supplementary material provides a comparison of proposed solutions for modern aircraft systems in terms of their performance, efficiency, and accuracy.

(1) Secure system topologies. These topologies effectively mitigate cyber security risks in modern aircraft systems. Mahmoud et al. [64] introduced SecMan, a secure system topology that provides secure and reliable communication between different components of the aircraft system network, e.g., flight deck, ground-based systems, cabin systems. The SecMan topology enables aircraft systems to reconfigure communication paths due to security threats. The integrity and reliability of information were also addressed in other studies proposing blockchain-based systems and topologies aimed at reducing centralized platforms, e.g., AirChain [53], an aircraft maintenance record system that is based on blockchain technology in which the data can be stored in a tamper-resistant manner but is easy to access.

(2) Integrity frameworks. Many prior studies made use of a combination of multiple sensors for data verification and fault finding. An example of such a framework was suggested by Sampigethaya et al. [87], who proposed the use of multi-radar to enforce integrity checks for ADS-B and provide a backup support at hardware and software failure. Darabseh et al. [18] demonstrated an enhanced framework for ADS-B message verification with a minimal amount of onground sensors, while Kovell et al. [60] presented a technique for group verification of ADS-B messages.

(3) Machine and deep learning models. In recent years, researchers have proposed the use of machine and deep learning models for information processing and analysis in novel cyber security solutions for the aviation industry, including methods for anomaly detection in aircraft systems [30]. For example, Habler et al. [36, 37] demonstrated the use of deep learning models to identify anomalous ADS-B traffic. Several cyber-physical attack detection cybersecurity systems based on deep learning are described in Reference [130]. Bitton et al. [10] proposed a network-based intrusion detection system specifically designed for securing the connection between a commercial tablet and an EFB server. These systems require additional processing power but generally do not necessitate significant changes to the system's architecture or hardware, unlike solutions that require topology changes or encryption systems, since they are software-based.

(4) Encryption solutions such as hybrid encryption for flight control systems [49] and encryption-based solutions for data layers such as ACARS [129] and ADS-B [121, 127] have been proposed for various flight control systems to provide privacy. The implementation of encryption mechanisms and protocols usually requires protocol and system hardware changes, resulting in higher costs. In addition, the exchange of encryption keys can pose a challenge due to the multiple commercial participants and the speed of the aircraft.

(5) Network segmentation involves dividing a network into smaller segments to limit the impact an adversary can have by attacking a single segment. The use of firewalls and VPNs can help in segmenting the network and preventing unauthorized access (e.g., the Satcom Direct router provides a VPN connection between the aircraft and ground-based systems). The need for this separation is also noted by Shetty et al. [96], who addressed the potential impact of integrating passenger, crew, and sensor communication on a single data link.

(6) Intrusion detection and prevention system solutions can be used to detect and prevent attacks such as DoS, malware infection, port knocking, and scans. Intrusion detection and prevention systems commonly used in the avionics industry include:

- *Honeywell Forge Cybersecurity Suite* [45], which includes a network intrusion detection system and firewall designed specifically for aviation systems. This firewall provides a secure gateway between the aircraft's onboard network and ground-based systems, preventing unauthorized access to critical flight systems.
- *Satcom Direct Cybersecurity Solutions* [91] provides threat monitoring within the cabin network and helps detect external attacks aimed at executing a malicious action on the airborne network.

— *Airbus Skywise Security* [5] is an open data platform that enables airlines, manufacturers, and other aviation stakeholders to gather, share, and analyze data from various sources across the aviation ecosystem, thereby improving the ability to process and identify threats. A report published by the European Cyber Security Organisation [42] highlights the need for a data platform for predictive maintenance that can be used by all major aviation players. IATF [48] is another significant framework, which aims to establish a standardized agreement and managed services for data exchange among aviation industry stakeholders.

(7) Proactive security analysis. Studies and demonstrations conducted on aircraft systems and communication lines, yielding valuable results and conclusions. In such works, attacks are actively implemented under strict working assumptions, and their effect on the various systems is examined. To implement these experiments, flight simulators and laboratories that represent the work environment are required. The most realistic and accessible labs were introduced in References [15, 82, 111]. For example, True et al. [118] performed cyber security analysis on the EFB, AID, and IP data links of the aircraft and made recommendations for additional security measures where required. Sathaye et al. [92] performed further demonstrations utilizing an FAA-certified flight simulator (X-Plane), which revealed the vulnerability of aircraft instrument landing systems to wireless attacks.

(8) State-of-the-art lab setups. State-of-the-art lab setups are critical for assessing and validating cyber security in aviation systems. Several recent papers highlight the importance of such setups and the main objectives in designing the relevant experiments. Strohmeier et al. [111] proposed a design for an avionics laboratory that prioritizes realism, independence, complete accessibility, and physical wireless interfaces, covering SATCOM, ADS-B, TCAS, CPDLC, and EPIRB-ELL extensible. Similarly, Predescu et al. [82] presented the aviation security lab, which includes a diverse range of avionic systems and components, network infrastructure, and cyber security tools, and covers ARINC-429 [6] and ARINC-664 [7]. Costin et al. [15] proposed a unified cyber security testing lab for satellite, aerospace, avionics, maritime, and drone technologies and communications, with virtual environments, physical testbeds, and network emulation, the lab covers ADS-B, EFB, ACARS, EPIRB-ELL extensible and cross-channel for the aviation field.

9 SCIENTIFIC GAPS AND RESEARCH DIRECTIONS

This section deals with the scientific gaps and subjects requiring further investigation identified in our work. We also discuss issues arising from the lack of complete and reliable information available in the field of offensive cyber security and suggest directions for further research.

(1) Verification of disclosed information. Research on offensive cyber security, especially when critical systems are involved, is challenging, as publicly available information does not include extensive details regarding potential vulnerabilities or exploits to prevent exploitation or misuse. However, the specific details are reported in a responsible manner to airlines, component manufacturers, and system manufacturers (following the agreed policies, e.g., FAA vulnerability disclosure policy [27]), allowing for the necessary security updates to be installed and implemented. For example, IOActive performed responsible disclosure [24], reporting vulnerabilities found on the onboard SATCOM system providing Internet to passengers to the European Union Aviation Safety Agency. In addition, there have been several cases where the veracity of claims was questionable. For example, in 2015, avionics experts disputed a security researcher's claim that they accessed in-flight entertainment and flight systems from their seat on an aircraft [31]. In another incident, in 2017, experts working with the U.S. Department of Homeland Security claimed that they had successfully hacked into a legacy Boeing 757 commercial aircraft remotely, in a non-laboratory setting, by accessing its systems through radio frequency communications. CBS News reported on these claims [73], and in response, Boeing issued a statement stating that according to their estimates, the test did not identify any cyber vulnerabilities in the 757 or any other aircraft produced by Boeing [85]. Therefore, to confirm some of the attack vectors presented, additional experiments should be conducted.

(2) Scientific Gaps. In the field of avionics, there are several scientific gaps and areas where there is insufficient knowledge and understanding. This lack of understanding poses a real danger, and there is a need for further research to reduce threats to aircraft and those on board.

- **Protection Methods** Many studies have addressed the need for protection against attacks on specific systems. The solutions proposed generally require redesigning the system or its components, adding components or sensors, and so on. However, there is a need for a solution that takes a wide view of an aircraft as a broad and uniform computerized platform with many intrusion surfaces. In this article, we show how different systems and components can be used throughout the stages of an attack to achieve the adversary's goals and desired impact, raising the need for research that examines the use of multiple systems as part of an attack vector.
- **Adoption and Adaptation of Existing Solutions** The computer systems on an aircraft include real-time systems based on dedicated operating systems and standard Linux/Windows-based operating systems. In addition, there are networks of varying degrees of importance that are logically separated. There is a need to consider and examine the adoption of existing solutions for these systems and networks, such as monitoring products, firewalls, and antivirus products.

(3) Future Research Directions. To expand the taxonomy and make it more accessible and usable, we propose further research in the following areas:

- **Cyber Attacks on Autonomous Systems** Some aircraft systems are autonomous systems that are designed to respond when needed without the explicit involvement of the pilot. An example of this is the **maneuvering characteristics augmentation system (MCAS)** [65], which was designed to stabilize the aircraft without any intervention by the pilot. The MCAS is known to have been involved in several air accidents in recent years [17]. Autonomous systems like the MCAS have the potential to cause significant damage to an aircraft and harm passengers, as the crew's degree of impact on these systems is limited. Research is needed to examine how cyber attacks can affect these systems.
- **Human Factor** Addressing the human factor by training and preparing the aircrew to handle and manage various events is important in the implementation of defense mechanisms in emergencies. For example, when mapping the various risks and threats, it is necessary to examine how new and existing security solutions can be adapted based on the skills and knowledge of the aircrew. Some studies dealing with human responses in emergencies have been performed, including a study conducted by Smith et al. [102] that examined pilots' responses to various cyber attacks. Future research must address the need to generate and provide critical information to the pilot and crew, e.g., data from intrusion detection systems. This can be done by developing new systems, adapting relevant systems, and making the information from such systems clear to better enable the crew to handle exceptional events. The need to provide clear and accessible information to the pilot was addressed by Habler et al. [37], who provided a deep learning-based solution for the detection of anomalous traffic conditions; the proposed solution relied on an explainability technique designed to formulate and conveniently present computational model decisions, for the benefit of pilots.

- **Threat Intelligence Platform** To share knowledge, provide up-to-date examples of threats, collect relevant data, and enrich the taxonomy, there is a need for a uniform **threat intelligence platform (TIP)**, which is accessible to airlines, airports, and manufacturers. Such a platform would be used to collect, aggregate, and organize threat intelligence data of various formats from multiple sources. The TIP will allow security and threat intelligence teams to easily share threat intelligence data with other stakeholders and security systems.

10 CONCLUSION AND DISCUSSION

In this article, we provided a comprehensive overview of aircraft systems and their components and networks, emphasizing the cyber threats they are exposed to and the impact of a cyber attack on an aircraft's essential capabilities. Based on our review and the issues raised in this article, we conclude that a taxonomy dedicated to avionics is needed given the diverse and intricate connections, systems, components, and attack surfaces in avionics systems. Therefore, we presented a comprehensive and in-depth taxonomy that standardizes the knowledge and understanding of known threats to avionic systems identified by industry and academia. The taxonomy deals with the various stages of cyber attacks and covers avionic systems' critical infrastructure, including air-ground communication, radio navigation aids, aeronautical surveillance, and system-wide information management. Additionally, we addressed the different domains of e-Enabled aircraft and provided an analysis of the domains' deployment, emphasizing the points at which various networks overlap. More importantly, though, our research points to the need for comprehensive defensive mechanisms aimed at protecting passengers and crew members and ensuring the safety of the aviation sector; to this end, our article provides a review of various mitigation approaches that can be employed as part of these defensive mechanisms. Once developed and adopted, these mechanisms can be added to the taxonomy, enriching it as they improve safety. To accomplish the enriching of the taxonomy, results published by security researchers must be verified, more studies dealing with avionics defense systems and mechanisms need to be performed, and a unified threat intelligence platform must be adopted for the benefit of all stakeholders. Please see Table 4.

APPENDIX

A ACRONYMS

Table 4. Acronyms

Acronym	Description
ABAS	Aircraft-based augmentation system
ACARS	Aircraft communications addressing and reporting system
ACD	Aircraft control domain
ACE	Actuator control electronics
ACMS	Aircraft condition monitoring system
ADN	Aircraft data network
ADS-B	Automatic Dependent Surveillance-Broadcast
AEEC	Airlines electronic engineering committee
AISD	Airline information services domain
AMI	Airline modifiable information
AOC	Aircraft operational control
ATC	Air traffic control
ATM	Air traffic management
ATN	Aeronautical telecommunication network
CIS-MS	Crew information system/maintenance system
CPDLC	Controller pilot data link communications
CSM	Controller server module
CSS	Cabin services system
CWLU	Connectivity and crew wireless LAN unit
DME	Distance measuring equipment
DSP	Datalink service provider
EASA	European Union Aviation Safety Agency
ECAM	Electronic centralized aircraft monitor
EFB	Electronic flight bag
EFIS	Instrument display system
EGM	Ethernet gateway module
EICAS	Engine-indicating and crew-alerting system
FANS	Future air navigation system
FDR	Flight data recorder
FMS	Flight management systems
FSM	File server module
GBAS	Ground-based augmentation system
GNSS	Global navigation satellite system
GPS	Global Positioning System
GPWS	Ground proximity warning system
HF	High frequency
IFE	In-flight entertainment
IFR	Instrument flight rules
ILS	Instrument landing system
IMA	Integrated modular avionics
LRU	Loadable replaceable unit
MFD	Multi-function display
NIM	Network interface module
OPC	Operational program configuration
OPS	Operational program software
PFD	Primary flight display
PIESD	Passenger information and entertainment domain
PODD	Passenger owned devices domain
RDC	Remote data concentrator
SATCOM	Aircraft satellite communication system
SBAS	Satellite-based augmentation system
SDR	Software-defined radio
SDU	Satellite data unit
TCAS	Traffic collision avoidance system
TWLU	Terminal wireless LAN unit
UHF	Ultra high frequency
VFR	Visual flight rules
VHF	Very high frequency

ACKNOWLEDGMENTS

The authors thank Mr. Tamir Goren and Mr. Dadi Gertler (Israel National Cyber Directorate) for their valuable comments and insights.

REFERENCES

[1] 2017. *How-secure-are-ifec-systems*. Retrieved from http://interactive.aviationtoday.com/how-secure-are-ifec-systems/

[2] Aircraft Communications Addressing and Reporting System. Retrieved from https://www.skybrary.aero/articles/aircraft-communications-addressing-and-reporting-system

[3] ADSBRANGE. 2023. *ADS-B Range*. Retrieved from https://www.faa.gov/air_traffic/technology/adsb

[4] Aerospace Village. 2020. *DEF CON 28 Aerospace Village: Attacking Flight Management Systems*. Retrieved from https://www.youtube.com/watch?v=G4dDRXBikvA

[5] airbusskywise. 2023. *Airbus Skywise - Industry Data Platform to Address Aircraft Operations Challenges*. Retrieved from https://aircraft.airbus.com/en/services/enhance/skywise

[6] ARINC429. 2005. *ARINC-429 TUTORIAL & REFERENCE*. Retrieved from https://www.ueidaq.com/arinc-429-tutorial-reference-guide

[7] ARINC664. 2005. *ARINC664 AFDX Data Transmission System for Aircraft, Airbus Patent*. Retrieved from https://worldwide.espacenet.com/patent/search?q=pn%3DUS6925088

[8] ARINC781. 2019. *ARINC-429 TUTORIAL & REFERENCE*. Retrieved from https://standards.globalspec.com/std/13448227/arinc-781

[9] ARINC821. 2008. *ARINC821 Report*. Retrieved from https://www.aviation-ia.com/products/821-aircraft-network-server-system-nss-functional-definition-2

[10] Ron Bitton and Asaf Shabtai. 2019. A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers. *IEEE Trans. Depend. Sec. Comput.* 18, 3 (2019), 1164–1181.

[11] Check Point Blog. 2021. *Checkpoint's Cyber Security Report 2021*. Retrieved from https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/

[12] Gaurav Choudhary, Vikas Sihag, Shristi Gupta, and Shishir Kumar Shandilya. 2022. Aviation attacks based on ILS and VOR vulnerabilities. (2022).

[13] The Boeing Company. 2007. Boeing e-Enablement patent. Retrieved from https://patentimages.storage.googleapis.com/9c/12/93/43a3858b71b5aa/WO2007117285A2.pdf

[14] Andrei Costin and Aurélien Francillon. 2012. Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA* (2012), 1–12.

[15] Andrei Costin, Hannu Turtiainen, Syed Khandker, and Timo Hämäläinen. 2023. Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications. *arXiv preprint arXiv:2302.08359* (2023).

[16] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. 2014. A large-scale analysis of the security of embedded firmwares. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14)*. 95–110.

[17] Crash Report 2019. *Preliminary Crash Report*. Retrieved from https://www.npr.org/2019/04/04/709766379/preliminary-crash-report-says-ethiopian-airlines-crew-complied-with-procedures

[18] Ala' Darabseh, Hoda AlKhzaimi, and Christina Pöpper. 2020. MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 53–64.

[19] Gaurav Dave, Gaurav Choudhary, Vikas Sihag, Ilsun You, and Kim-Kwang Raymond Choo. 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Comput. Secur.* 112 (2022), 102516.

[20] Doris Di Marco, Alessandro Manzo, Marco Ivaldi, and John Hird. 2016. Security testing with controller-pilot data link communications. In *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES'16)*. IEEE, 526–531.

[21] Hélène Duchamp, Ibrahim Bayram, and Ranim Korhani. 2016. Cyber-security, a new challenge for the aviation and automotive industries. In *Proceedings of the Seminar in Information Systems: Applied Cybersecurity Strategy for Managers*. 1–4.

[22] Ahmed Abdelwahab Elmarady and Kamel Rahouma. 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access* 9 (2021), 143997–144016.

[23] Sofie Eskilsson, Hanna Gustafsson, Suleman Khan, and Andrei Gurtov. 2020. Demonstrating ADS-B and CPDLC attacks with software-defined radio. In *Proceedings of the Integrated Communications Navigation and Surveillance Conference (ICNS'20)*. IEEE, 1B2–1.

[24] European Union Aviation Safety Agency. 2021. EASA engaged in responsible disclosure of cybersecurity issues through coordination. Retrieved from https://www.easa.europa.eu/en/newsroom-and-events/news/easa-engaged-responsible-disclosure-cybersecurity-issues-coordination

[25] FAA DB. 2022. *FAA Data Base*. Retrieved from https://www.faa.gov/airports/engineering/aircraft_char_database

[26] Federal Aviation Administration. 2012. FANS-1A Over Iridium Status. Retrieved from https://www.icao.int/APAC/Meetings/2012SOCM2/WP04_USA%20AI.2.1%20-%20FANS%201A%20over%20Iridium%20Status.pdf

[27] Federal Aviation Administration. 2021. Vulnerability Disclosure Policy. Retrieved from https://www.faa.gov/web_policies/vulnerability_disclosure_policy

[28] Dávid János Fehér and Barnabás Sandor. 2018. Effects of the WPA2 KRACK attack in real environment. In *Proceedings of the IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY'18)*. IEEE, 000239–000242.

[29] Davor Franjković, Tino Bucak, and Nikica Hoti. 1999. Ground proximity warning system-GPWS. *Promet-Traf. Transport.* 11, 5 (1999), 293–301.

[30] Anna Baron Garcia, Radu F. Babiceanu, and Remzi Seker. 2021. Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview. In *Proceedings of the Integrated Communications Navigation and Surveillance Conference (ICNS'21)*. IEEE, 1–8.

[31] Samuel Gibbs. 2015. *Aviation Experts Dispute Hacker's Claim He Seized Control of Airliner Mid-flight.* Retrieved from https://www.theguardian.com/technology/2015/may/19/hacker-chris-roberts-claim-seized-control-boeing-airliner-disputed-experts

[32] Timothy Michael Graziano. 2021. *Establishment of a Cyber-Physical Systems (CPS) Test Bed to Explore Traffic Collision Avoidance System (TCAS) Vulnerabilities to Cyber Attacks.* Ph. D. Dissertation. Virginia Tech.

[33] M. Greene and K. Greene. 1996. An EFIS EICAS for general aviation. In *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA'96)*, Vol. 2. IEEE, 429–432.

[34] M. Grzegorzewski, J. Cwiklak, H. Jafernik, and A. Fellner. 2008. GNSS for an aviation. *TransNav: Int. J. Marine Navig. Safety Sea Transport.* 2, 4 (2008).

[35] Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. 2018. Controller–pilot data link communication security. *Sensors* 18, 5 (2018), 1636.

[36] Edan Habler and Asaf Shabtai. 2018. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. *Comput. Secur.* 78 (2018), 155–173.

[37] Edan Habler and Asaf Shabtai. 2021. Analyzing sequences of airspace states to detect anomalous traffic conditions. *IEEE Trans. Aerosp. Electron. Syst.* (2021).

[38] Martin Hagmüller, Horst Hering, Andreas Kröpfl, and Gernot Kubin. 2004. Speech watermarking for air traffic control. In *Proceedings of the 12th European Signal Processing Conference*. IEEE, 1653–1656.

[39] John Hannah, Robert Mills, and Richard Dill. 2020. Traffic collision avoidance system: Threat actor model and attack taxonomy. In *Proceedings of the New Trends in Civil Aviation (NTCA'20)*. IEEE, 17–26.

[40] John W. Hannah. 2021. A cyber threat taxonomy and a viability analysis for false injections in the TCAS. (2021).

[41] William H. Harman. 1989. TCAS—A system for preventing midair collisions. *Linc. Lab. J.* 2, 3 (1989), 437–457.

[42] Nina Hasratyan, Nina Olesen, Adrien Becue, Ulrich Seldeslachts, Sadio Bâ, Andrea Chiappetta, Andrei Costin, Janine Dobelmann, Christopher Henny, Pouria Sayyad Khodashenas, Gabriele Rizzo, Rémy Russotto, Jayant Sangwan, Eva Schulz-Kamm, Lorraine Wilkinson, Thorsten Wollweber, Athanasios Drougkas, Christophe Gransart, Hana Guyaux-Pechackova, François Hausman, John Hird, Dennis Kutschke, Jérôme Morandiere, Francisco Pastrana, and Markus Tschersich. 2020. ECSO transportation sector report, cyber security for road, rail, air, and sea. WG3 I sectoral demand. Retrieved from https://hal.archives-ouvertes.fr/hal-02531033/

[43] Christopher J. Hegarty and Eric Chatre. 2008. Evolution of the Global Navigation Satellite System (GNSS). *Proc. IEEE* 96, 12 (2008), 1902–1917.

[44] Horst Hering, G. Kubin, et al. 2003. Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the VHF voice communication. In *Proceedings of the 22nd Digital Avionics Systems Conference (DASC'03)*. IEEE, 4–E.

[45] Honeywell 2023. *Honeywell Cybersecurity.* Retrieved from https://prod-edam.honeywell.com/content/dam/honeywell-edam/pmt/hps/products/software/cyber-security/smx/Honeywell-Forge-Cybersecurity-Brochure.pdf

[46] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, et al. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lead. Iss. Inf. Warfare Secur. Res.* 1, 1 (2011), 80.

[47] IATA Best Practices 2020. *IATA - Best Practices for Loadable Software Management and Configuration.* Retrieved from https://docplayer.net/15768767-Best-practices-for-loadable-software-management-and-configuration-control.html

[48] IATF 2023. *International Aviation Trust Framework*. Retrieved from https://www.icao.int/airnavigation/Pages/IATF.aspx

[49] Maksim Iavich, Sergiy Gnatyuk, Elza Jintcharadze, Yuliia Polishchuk, and Roman Odarchenko. 2018. Hybrid encryption model of AES and ElGamal cryptosystems for flight control systems. In *Proceedings of the IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC'18)*. IEEE, 229–233.

[50] Mordor Intelligence. 2021. Global Aviation Cybersecurity Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021–2026). Retrieved from https://www.mordorintelligence.com/industry-reports/global-aviation-cybersecurity-market

[51] International Civil Aviation Organization. 2011. ICAO guidance on aviation security (restricted), Ed. 8. (2011), 748. Doc 8973.

[52] IOActive. 2016. *Ioactive-discovers-in-flight-entertainment-system-vulnerabilities*. Retrieved from https://ioactive.com/article/ioactive-discovers-in-flight-entertainment-system-vulnerabilities/

[53] Wictor Lang Jensen, Sille Jessing, Wei-Yang Chiu, and Weizhi Meng. 2022. A practical blockchain-based maintenance record system for better aircraft security. In *Proceedings of the 4th International Conference on Science of Cyber Security*. Springer, 51–67.

[54] Arttu Juvonen, Andrei Costin, Hannu Turtiainen, and Timo Hämäläinen. 2022. On Apache Log4j2 exploitation in aeronautical, maritime, and aerospace communication. *IEEE Access* 10 (2022), 86542–86557.

[55] Shahidul Islam Khandker, Hannu Turtiainen, Andrei Costin, and Timo Hamalainen. 2021. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures. *IEEE Trans. Aerosp. Electron. Syst.* (2021).

[56] Shahidul Islam Khandker, Hannu Turtiainen, Andrei Costin, and Timo Hämäläinen. 2022. On the (in)security of 1090ES and UAT978 mobile cockpit information systems—An attacker perspective on the availability of ADS-B safety- and mission-critical systems. *IEEE Access* 10 (2022), 37718–37730.

[57] Hennadii Khudov, Andrii Fedorov, Dmytro Holovniak, and Galina Misiyuk. 2018. Improving the efficiency of radar control of airspace with the multilateration system use. In *Proceedings of the International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'18)*. IEEE, 680–684.

[58] Mary Kirby. 2014. *Most Airlines Lack EFB Cyber-security Plan: Report*. Technical Report.

[59] Oltjon Kodheli, Eva Lagunas, Nicola Maturo, Shree Krishna Sharma, Bhavani Shankar, Jesus Fabian Mendoza Montoya, Juan Carlos Merlano Duncan, Danilo Spano, Symeon Chatzinotas, Steven Kisseleff, et al. 2020. Satellite communications in the new space era: A survey and future challenges. *IEEE Commun. Surv. Tutor.* 23, 1 (2020), 70–109.

[60] Brandon Kovell, Benjamin Mellish, Thomas Newman, and Olusola Kajopaiye. 2012. Comparative analysis of ADS-B verification techniques. *Univ. Color., Bould.* 4 (2012).

[61] Dejan V. Kovzovic and Dragan Z. Durdevic. 2021. Spoofing in aviation: Security threats on GPS and ADS-B systems. *Vojnotehnicki glasnik/Military Technic. Cour.ier* 69, 2 (2021), 461–485.

[62] Mauro Leonardi and Fabrizio Gerardi. 2020. Aircraft mode S transponder fingerprinting for intrusion detection. *Aerospace* 7, 3 (2020), 30.

[63] Georgia Lykou, George Iakovakis, and Dimitris Gritzalis. 2019. Aviation cybersecurity and cyber-resilience: Assessing risk in air traffic management. In *Critical Infrastructure Security and Resilience*. Springer, 245–260.

[64] Mohamed Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano, and Antoine Varet. 2010. An adaptive security architecture for future aircraft communications. In *Proceedings of the 29th Digital Avionics Systems Conference*. IEEE, 3–E.

[65] Sebastián Mako, Marek Pilat, P. Svab, J. Kozuba, and M. Cicvakova. 2020. Evaluation of MCAS system. *Acta Avionica J.* 40 (2020), 21–28.

[66] MarketWatch. 2023. Aviation Cyber Security Market 2023: Size and Forecast to 2031. Retrieved from https://www.marketwatch.com/press-release/aviation-cyber-security-market-2023-size-and-forecast-to-2031-2023-03-28

[67] Damian Miralles, Aurelie Bornot, Paul Rouquette, Nathan Levigne, Dennis M. Akos, Yu-Hsuan Chen, Sherman Lo, and Todd Walter. 2020. An assessment of GPS spoofing detection via radio power and signal quality monitoring for aviation safety operations. *IEEE Intell. Transport. Syst. Mag.* 12, 3 (2020), 136–146.

[68] Kayvan Faghih Mirzaei, Bruno Pessanha de Carvalho, and Patrick Pschorn. 2019. *Security of ADS-B: Attack Scenarios*. Technical Report. EasyChair.

[69] MITRE Website 2022. *MITRE ATT&CK*. Retrieved from https://attack.mitre.org/

[70] Márcio Monteiro, Alexandre Barreto, Research Division, Thabet Kacem, Jeronymo Carvalho, Duminda Wijesekera, and Paulo Costa. 2015. Detecting malicious ADS-B broadcasts using wide area multilateration. In *Proceedings of the IEEE/AIAA 34th Digital Avionics Systems Conference (DASC'15)*. IEEE, 4A3–1.

[71] Daniel Moser, Patrick Leu, Vincent Lenders, Aanjhan Ranganathan, Fabio Ricciato, and Srdjan Capkun. 2016. Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. 375–386.

[72] Mohamad Mostafa, Okuary Osechas, and Michael Schnell. 2016. Vulnerability analysis of the CNS-infrastructure: An exemplarily approach. In *Proceedings of the IEEE/AIAA 35th Digital Avionics Systems Conference (DASC'16).* IEEE, 1–9.

[73] CBS News. 2018. Homeland Security "hacked" Boeing 757 jetliner? Experts aren't so sure. *CBS News.* Retrieved from https://www.cbsnews.com/news/homeland-security-hacked-boeing-757-jetliner/

[74] Washington Y. Ochieng, Knut Sauer, David Walsh, Gary Brodin, Steve Griffin, and Mark Denney. 2003. GPS integrity and potential impact on aviation safety. *J. Navig.* 56, 1 (2003), 51–65.

[75] Rajee Olaganathan. 2018. Safety analysis of automatic dependent surveillance–broadcast (ADS-B) system. *Int. J. Aerosp. Mechan. Eng.* 5, 2 (2018).

[76] International Civil Aviation Organization. 2013. ICAO guidance on the security of air traffic management system (restricted), Ed. 1. (2013), 174. Doc 9985.

[77] Okuary Osechas, Mohamad Mostafa, Thomas Graupl, and Michael Meurer. 2017. Addressing vulnerabilities of the CNS infrastructure to targeted radio interference. *IEEE Aerosp. Electron. Syst. Mag.* 32, 11 (2017), 34–42.

[78] Pen Test Partners. 2021. *EFB-tampering*. Technical Report.

[79] PenTestPartners. 2020. *DEF CON 28: ILS and TCAS Spoofing*. Retrieved from https://www.pentestpartners.com/security-blog/ils-and-tcas-spoofing/

[80] PenTestPartners. 2020. *DEF CON 28: Introduction to Acars*. Retrieved from https://www.pentestpartners.com/security-blog/introduction-to-acars

[81] Jason Pollack and Prakash Ranganathan. 2018. Aviation navigation systems security: ADS-B, GPS, iff. In *Proceedings of the International Conference on Security and Management (SAM'18).* The Steering Committee of the World Congress in Computer Science, Computer, 129–135.

[82] Adrian-Viorel Predescu and Tim H. Stelkens-Kobsch. 2022. Aviation security lab: A testbed for security testing of current and future aviation technologies. In *Proceedings of the IEEE/AIAA 41st Digital Avionics Systems Conference (DASC'22).* 1–5.

[83] PTsecurity. 2018. *Impact Assessment of Cyber security Threats*. Technical Report.

[84] PTsecurity. 2021. *PTsecurity Report Q1 2021.* Technical Report.

[85] Steve Ragan. 2017. Homeland Security team remotely hacked a Boeing 757. Retrieved from https://www.csoonline.com/article/3236721/homeland-security-team-remotely-hacked-a-boeing-757.html

[86] FRANK Roepcke. 1990. ILS-past and present. *IEEE Aerosp. Electron. Syst. Mag.* 5, 5 (1990), 9–11.

[87] Krishna Sampigethaya, Radha Poovendran, Sudhakar Shetty, Terry Davis, and Chuck Royalty. 2011. Future e-enabled aircraft communications and security: The next 20 years and beyond. *Proc. IEEE* 99, 11 (2011), 2040–2055.

[88] Ruben Santamarta. 2014. SATCOM terminals: Hacking by air, sea, and land. *DEFCON White Paper* (2014).

[89] Ruben Santamarta. 2014. A wake-up call for SATCOM security. *Technical White Paper* (2014).

[90] Ruben Santamarta. 2018. *Last Call for SATCOM Security*. IOActive.

[91] Satcomdirect. 2023. *Satcom Direct.* Retrieved from https://www.satcomdirect.com/land-mobile/cybersecurity-solutions/

[92] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. 2019. Wireless attacks on aircraft instrument landing systems. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security'19).* 357–372.

[93] Ben Seri, Gregory Vishnepolsky, and Dor Zusman. 2019. Critical vulnerabilities to remotely compromise VxWorks, the most popular RTOS. *White Paper, ARMIS, URGENT/11* (2019).

[94] Farooq Shaikh, Mohamed Rahouti, Nasir Ghani, Kaiqi Xiong, Elias Bou-Harb, and Jamal Haque. 2019. A review of recent advances and security challenges in emerging E-enabled aircraft systems. *IEEE Access* 7 (2019), 63164–63180.

[95] Ilja Shatilin. 2015. *Hacking an Aircraft: Is It Already Real.* Technical Report. Kaspersky.

[96] Sudhakar Shetty. 2008. System of systems design for worldwide commercial aircraft networks. In *Proceedings of the 26th International Congress of the Aeronautical Sciences (ICAS'08).*

[97] A. Shostack, S. Lambert, and S. Hernan. 2006. Uncover security design flaws using STRIDE. *MSDN Mag.* (Nov. 2006).

[98] Merrill I. Skolnik. 2008. *Radar Handbook.* McGraw-Hill Education.

[99] Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2021. You talkin'to me? Exploring practical attacks on controller pilot data link communications. In *Proceedings of the 7th ACM on Cyber-physical System Security Workshop.* 53–64.

[100] Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2017. Analyzing privacy breaches in the aircraft communications addressing and reporting system. *arXiv preprint arXiv:1705.07065* (2017).

[101] Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2018. Undermining privacy in the aircraft communications addressing and reporting system (ACARS). *Proc. Privac. Enhanc. Technol.* 2018, 3 (2018), 105–122.

[102] Matthew Smith, Martin Strohmeier, Jon Harman, Vincent Lenders, and Ivan Martinovic. 2020. A view from the cockpit: Exploring pilot reactions to attacks on avionic systems. (2020).

[103] Matt Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2016. On the security and privacy of ACARS. In *Proceedings of the Conference on Integrated Communications Navigation and Surveillance (ICNS'16)*. IEEE, 1–27.

[104] Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2020. Understanding realistic attacks on airborne collision avoidance systems. *arXiv preprint arXiv:2010.01034* (2020).

[105] SOCRadar 2023. *SOCRadar Report*. Retrieved from https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

[106] Specifications 2022. *Aircraft Specifications*. Retrieved from http://www.axonaviation.com/commercial-aircraft/aircraft-data/aircraft-specifications

[107] M. C. Stevens. 1985. New developments in secondary-surveillance radar. *Electron. Power* 31, 6 (1985), 463–466.

[108] STRIDE 2009. *STRIDE Threat Model*. Retrieved from https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[109] Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. 2020. Securing the air–ground link in aviation. In *The Security of Critical Infrastructures*. Springer, 131–154.

[110] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. 2016. On perception and reality in wireless air traffic communication security. *IEEE Trans. Intell. Transport. Syst.* 18, 6 (2016), 1338–1357.

[111] Maximilian Strohmeier, Gianluca Tresoldi, Lucas Granger, and Vincent Lenders. 2022. Building an avionics laboratory for cybersecurity testing. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*. 10–18.

[112] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. 2018. *MITRE ATT&CK: Design and Philosophy*. Technical report.

[113] Skylar Stroman. 2021. *Automatic Dependent Surveillance Broadcast (ADS-B) Security Mitigation through Multilateration*. University of North Florida.

[114] Cagatay Tanil, Samer Khanafseh, and Boris Pervan. 2016. An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches. In *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+'16)*. 2981–2990.

[115] Hugo Teso. 2013. Aircraft hacking: Practical aero series. In *Proceedings of the 4th Hack in the Box Security Conference in Europe*.

[116] Hugo Teso. 2013. *Hugo Teso - Digging Deeper Into Aviation Security*. Retrieved from https://conference.hitb.org/hitbsecconf2013kul/materials/D2T1%20-%20Hugo%20Teso%20-%20Digging%20Deeper%20Into%20Aviation%20Security.pdf

[117] Vinoo Thomas, Prashanth Ramagopal, and Rahul Mohandas. 2009. The rise of autorun-based malware. *McAfee Avert Labs., McAfee Inc* (2009).

[118] Willard True, Todd Kilbourne, Aloke Roy, and Noureddin Ghazavi. 2021. Cybersecurity for flight deck data exchange. In *Proceedings of the IEEE/AIAA 40th Digital Avionics Systems Conference (DASC'21)*. IEEE, 1–13.

[119] Pascal Truffer, Maurizio Scaramuzza, Marc Troller, and Marc Bertschi. 2017. Jamming of aviation GPS receivers: Investigation of field trials performed with civil and military aircraft. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+'17)*. 1258–1266.

[120] Hannu Turtiainen, Shahidul Islam Khandker, Andrei Costin, and Timo Hamalainen. 2022. GDL90fuzz: Fuzzing "GDL-90 data interface specification" within aviation software and avionics devices—A cybersecurity pentesting perspective. *IEEE Access* (2022).

[121] Edward Valovage. 2006. Enhanced ADS-B research. In *Proceedings of the IEEE/AIAA 25th Digital Avionics Systems Conference*. IEEE, 1–7.

[122] John Van Dongen and Leo Wapelhorst. 1991. *Data Link Test and Analysis System/TCAS Monitor User's Guide*. Technical Report.

[123] Mathy Vanhoef and Frank Piessens. 2017. Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 1313–1328.

[124] Camilo Andres Pantoja Viveros. 2016. *Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts*. Ph. D. Dissertation. University of Tartu Tartu, Estonia.

[125] A. B. Winick and DM Brandewie. 1970. VOR/DME system improvements. *Proc. IEEE* 58, 3 (1970), 430–437.

[126] Marion Loren Wood and Richard Wright Bush. 1998. *Multilateration on Mode S and ATCRBS Signals at Atlanta's Hartsfield Airport*. Technical Report. Massachusetts Institute of Technology, Lexington, Lincoln Lab.

[127] Zhijun Wu, Tong Shang, and Anxin Guo. 2020. Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. *IEEE Access* 8 (2020), 122147–122167.

[128] Ning Yu. 1994. *Development of a Modern Non-directional Radio Beacon Aircraft Navigation System*. Lamar University-Beaumont.

[129] Meng Yue and Xiaofeng Wu. 2010. The approach of ACARS data encryption and authentication. In *Proceedings of the International Conference on Computational Intelligence and Security*. IEEE, 556–560.

[130] Jun Zhang, Lei Pan, Qing-Long Han, Chao Chen, Sheng Wen, and Yang Xiang. 2021. Deep learning based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA J. Automat. Sinic.* 9, 3 (2021), 377–391.

[131] Ru Zhang, Gongshen Liu, Jianyi Liu, and Jan P. Nees. 2017. Analysis of message attacks in aviation data-link communication. *IEEE Access* 6 (2017), 455–463.

Received 3 September 2022; revised 14 May 2023; accepted 11 July 2023