international journal of critical infrastructure protection 38 (2022) 100549

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Security in Digital Aeronautical Communications
A Comprehensive Gap Analysis

Nils Mäurer [a,*], Tobias Guggemos [b,d], Thomas Ewert [a], Thomas Gräupl [a], Corinna Schmitt [c], Sophia Grundner-Culemann [d]

[a] Institute of Communication and Navigation, German Aerospace Center (DLR), Wessling, Germany
[b] Remote Sensing Technology Institute, German Aerospace Center (DLR), Wessling, Germany
[c] Research Institute CODE, Universität der Bundeswehr München, Munich, Germany
[d] MNM-Team, Ludwig-Maximilian Universität (LMU) München, Munich, Germany

ARTICLE INFO

Keywords:
Security
Cybersecurity
Privacy
Safety
Digital Aeronautical Communications

ABSTRACT

Aeronautical communications still heavily depend on analog radio systems, despite the fact that digital communication has been introduced to aviation in the 1990's. Since then, the digitization of civil aviation has been continued, as considerable pressure to rationalize the aeronautical spectrum has built up. In any modern digital communications system, the threat of digital attacks needs to be considered carefully. This is especially true for safety-critical infrastructure, which aviation's operational communication services clearly are. In this article, we reverse the traditional approach in the aeronautical industry of looking at a system from the safety perspective and assume a security-oriented point of view. We use the lens of security properties to review the requirements and specifications of aeronautical communications infrastructure as of 2021 and observe that most standards lack cybersecurity as a key requirement. Furthermore, we review the academic literature to identify possible solutions for the lack of cybersecurity measures in aeronautical communications system. We observe that most systems have been thoroughly analyzed within the academic security community, some for decades even, with many papers proposing concrete solutions to missing cybersecurity features. We conclude that there is a systematic problem in the design process of aeronautical communication systems. We provide a list of eight key findings and recommendations to improve the process of specifying such systems in a secure manner.

1. Introduction

ATC is the backbone for safe and secure civil air traffic, which enabled the aerial transport of 4.5 billion passengers and 61.3 million tonnes uplift in 2019 [1]. Until 2020, civil air traffic grew constantly at a compound rate of 5.8% per year and despite the severe impact of the COVID-19 pandemic, air traffic growth is expected to resume very quickly in post-pandemic times [2]. As civil air traffic grows and the demand for digital services for aircraft guidance and business operation of airlines increases, overall communication increases as well. To cope with this growth, ATM systems must make more efficient use of their dedicated, limited spectrum. Therefore, the digitalization of ATM services is unavoidable [3].

Historically, Communication, Navigation and Surveillance (CNS) systems in civil aviation evolved from military aircraft guidance [4]. Over the last decades, several civil systems have been developed for different flight domains (e.g., airport, continental and remote), communication partners (e.g., air-to-ground, ground-to-air and air-to-air), and communication links (e.g., terrestrial and satellite), as depicted in Fig. 1. Furthermore, a shift to digital data communications for the provision of safety-critical services, which are still mainly carried out via VHF voice services, is expected to increase efficiency as well as safety and security.

To this day, there exists no scientific survey providing a comprehensive overview of the violation of common security measures in civil aeronautical communications systems on applications, networks, and corresponding data link layers. This gap is closed by this survey, pursuing the following objectives:

(1) Showing that protocol security is important for future aeronautical communications (cf. Section 3),

* Corresponding author.
E-mail addresses: nils.maeurer@dlr.de (N. Mäurer), guggemos@nm.ifi.lmu.de (T. Guggemos), thomas.ewert@dlr.de (T. Ewert), thomas.graeupl@dlr.de (T. Gräupl), corinna.schmitt@unibw.de (C. Schmitt), grundner-culemann@nm.ifi.lmu.de (S. Grundner-Culemann).

https://doi.org/10.1016/j.ijcip.2022.100549
Received 14 April 2021; Received in revised form 2 May 2022; Accepted 3 July 2022
Available online 6 July 2022

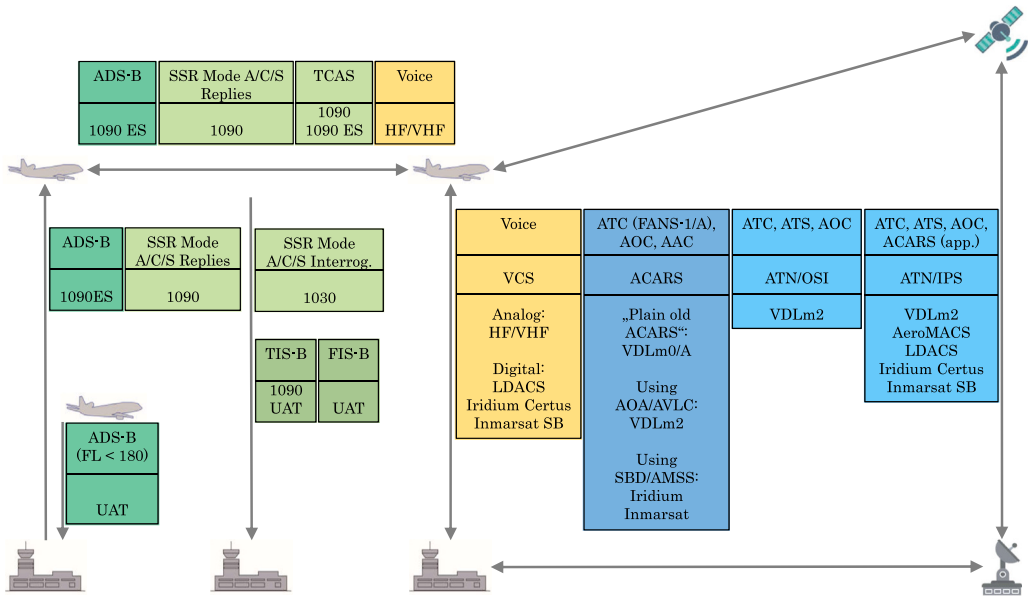

Fig. 1. Aeronautical Air Traffic Management (ATM) communications services, networks, and data links are depicted here. Surveillance is indicated in green, voice service in orange and data in blue. Abbreviations follow below:
1090 MHz Extended Squitter (1090ES), Airline Administrative Control (AAC), Automatic Dependent Surveillance-Broadcast (ADS-B), Aircraft Communications Addressing and Reporting System (ACARS), Aeronautical Mobile Satellite Service (AMSS), ACARS over AVLC (AOA), Aeronautical Operational Control (AOC), Air Traffic Communications (ATC), Aeronautical Telecommunications Network (ATN), Air Traffic Services (ATS), Aviation VHF Link Control (AVLC), Future Air Navigation System (FANS), Flight Information System-Broadcast (FIS-B), High Frequency (HF), Internet Protocol Suite (IPS), L-band Digital Aeronautical Communications System (LDACS), Open Systems Interconnection (OSI), Swift Broadband (SB), Short Burst Data (SBD), Secondary Surveillance Radar (SSR), Traffic Alert and Collision Avoidance System (TCAS), Traffic Information System-Broadcast (TIS-B), Universal Access Transceiver (UAT), Voice Communication System (VCS), VHF Data Link mode A (VDLm0), VHF Data Link mode 2 (VDLm2), Very High Frequency (VHF).

(2) Pointing out issues that arise when common security properties are not met (cf. Section 3), and
(3) Showing that, as of mid 2021, aeronautical systems presented in Section 4, do not offer the desired security properties (cf. Section 5) and to point to work done up until 2022 in that field which gradually improves the status quo.

As such, our contribution is to list concrete security objectives and all relevant aeronautical communications applications, networks and data links. We map these objectives to technologies, essentially pointing the research and standardization community to concrete security gaps that need to be closed.

The scope of this work is operational aeronautical communication, i.e., communication related to safety and regularity of flight, as well as for the business operation of the airline. Communications systems for in-flight entertainment (e.g., Internet access or video on demand for passengers) are not addressed in this paper since such services are installed in a physically separated security domain of the aircraft. However, we do consider issues in use cases where operational links are applied for purposes other than their intended use (e.g., validation of a passenger's credit card over a link intended for safety-critical aeronautical communications).

In Section 2 existing work is presenting proving that a gap in research exists for security issues. Security properties for aeronautical communications is presented throughout Sections Section 3 having the request to support security fundamentals in mind. In the future it is expected that more and more wireless communications technology will be included and highly relevant for aviation as briefly described within Sections Section 4. With the gained knowledge about the situation in aeronautics a gap analysis concerning security issues is presented in Section 5. Finally, a conclusion is drawn in Section 7.

2. Related work

In the following, we point out prominent examples for single technology security issues, namely ADS-B, ACARS, TCAS and CPDLC, before presenting scientific studies looking at the security of a multitude of aeronautical communications technologies.

The first case is ADS-B, for which Valovage [5] identified weaknesses of the system in 2006 and consequently proposed security additions to mitigate these vulnerabilities. In 2012, Costin [6] demonstrated these vulnerabilities to be exploitable at Blackhat 2012 and Strohmeier et al. [7] largely confirmed the previously identified security weaknesses. Wesson et al. [8] asked the question whether cryptography is sufficient to secure ADS-B and concluded that an asymmetric-key based elliptic curve digital signature algorithm on the ADS-B messages would prove effective. However, it is likely unacceptable to users of the system due to the increased complexity and overall low bandwidth of the channel ADS-B messages are transmitted by. Instead of using signatures, Berthier et al. [9] proposed a security concept relying on Timed Efficient Stream Loss-tolerant Authentication (TESLA) instead of signatures, which they also successfully demonstrated in a lab environment.

Another case is the security of ACARS, which also has been identified to offer limited security capabilities by Roy [10] and Risley et al. [11] in 2001. Both works provide countermeasures, with Risley et al. even demonstrating them. However, later, subsequent works by Smith et al. in 2017 [12] and 2018 [13] still revealed either the lack of or use of weak cryptography only, resulting in relating privacy issues.

Berges pointed out vulnerabilities in TCAS by exploitation via cheap Software Defined Radio (SDR) in 2019 [14]. At DEFCON 28, Lomas et al. demonstrated Instrument Landing System (ILS) and TCAS spoofing in 2020 [15]. Hannah [16] built on the work of Berges and introduced a TCAS threat taxonomy in 2021. By extending the initial capability of generating false TCAS mode S message by pairing this with known flight paths, the work concludes that this "present a true attack vector for adversaries" [16]. Lastly, Smith et al. presented attacks on TCAS in 2022, which successfully trigger a collision avoidance alert in 44% of the test cases [17].

In an early CPDLC requirement analysis by Cote [18] in 1998, a Federal Aviation Administration (FAA)-induced study, chapter 7 lists

the security requirements for CPDLC, stating that validity and authenticity of all CPDLC messages shall be verifiable by the respective ground system. Despite these requirements, later regulatory documents such as ICAO Doc 4444 [19] (version 1 in 2001 to version 17 in 2021) or Radio Technical Commission for Aeronautics (RTCA) DO-290 [20], including its updates until change 3 [21] (version 1 in 2004, change 3 in 2019), did not clearly define any mechanisms to realize the requirements. Di et al. [22] demonstrated a viable packet injection and manipulation attack via a man-in-the-middle attack on CPDLC in 2016. In 2018, Gurtov et al. identified eavesdropping, jamming, flooding, injection, alteration and masquerading as possible threats while also pointing out countermeasures [23]. Eskilsson et al. [24] showed in 2020 with cheap, publicly available SDR hardware that CPDLC and ADS-B messages can be successfully spoofed, received and processed in a controlled lab environment, demonstrating the feasibility of injecting FANS-1/a messages by malicious actors. Lehto et al. [25] followed up on that work in 2021 and published a publicly available CPDLC decoder for SDRs. A secure logon procedure for CPDLC was proposed by Khan et al. [26] in 2021 and its security formally verified using the ProVerif tool. Lastly, Smailes et al. [27] captured real world CPDLC traffic and evaluated the amount of cell handovers, which are exploitable by an attacker to position himself as a man-in-the-middle. The team concluded that with a ground-based SDR, a range of roughly 300 km can be covered, with handovers occurring every 6 to 21 min and proposed cryptographic countermeasures to prevent attackers exploiting the CPDLC handover procedure.

While all the presented work mostly focuses on one technology, the following works aimed on providing an overview. Already in 2014, Mahmoud et al. [3] focused on the transition from analogue to digital aeronautical communications along with accompanying security implications. They list relevant aeronautical communications technologies, state the issue of aeronautical spectrum scarcity as a reason for the transition and introduce a threat rating taxonomy for threats against digital aeronautical communications. In 2016, Strohmeier et al. [28] performed a survey among aviation experts, such as pilots and air traffic controllers, on the perceived security of various systems. They conclude that there is a wide gap between the actual security of the used systems and the perceived security by its users. They suggest that closing this knowledge gap is one of the most important steps in increasing digital aeronautical communications security, as regulators first need to be made ware of the problem. In 2020, Strohmeier et al. [29] again report on security incidents and vulnerabilities within ATC and point toward various works on countermeasures. They suggest that data sharing on security vulnerabilities should be improved in the domain [29]. Elmarady et al. presented a cybersecurity risk assessment methodology [30] for ATC in 2021. Applying the methodology on various aeronautical legacy communications technologies, a tendency of specific threats to each systems becomes visible. Dave et al. provide a summary of SDR attack vectors to CNS technologies [31] and Ukwandu et al. presented a review of actual cyber-attack incidents within civil aviation [32] in 2022.

3. Security properties for aeronautical communications

The **Security** of communication systems is no end in itself but protects people, nations, and businesses. Some security measures are therefore also required by law. In this section, we argue that protocol security in aeronautical communications is not only necessary to protect the communication system itself against digital attacks, but is essential to ensure **Safety** during the flight and to respect passenger's right to **Privacy**.

This paper does not aim at rating the *risk* associated with violating any of these properties from the perspective of different threat actors (e.g., nation states, activists, terrorists) or evaluating its consequences (e.g., in case of medical or safety-critical emergencies). We define an aeronautical communications system to be designed in a secure manner if and only if neither **Security**, **Safety** nor **Privacy** are violated. Hence, we treat all violations of any of these properties as equivalent, while the actual risk evaluation is out of scope of this paper and needs to be done during the implementation of the system.

Throughout this chapter, we refer to the Internet Engineering Task Force (IETF) "Internet Glossary version 2", RFC 4949 [33], the International Organization for Standardization (ISO) standard on information security, ISO 27001 [34], and the International Electrotechnical Commission (IEC) standard on IT security of industrial communication networks, IEC 62443 [35], and use the following definitions:

Security is defined as a system's condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

Safety is defined as the property of a system being free from risk of causing harm (especially physical harm) to its system entities.

Privacy is the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

We use the word *System* for any aeronautical communications system that fits into the definition of the ISO-OSI reference model [36] for communication. In that regard, we specify anyone who is able to read, access or change the wireless communications between aeronautical peers as an *attacker*. The examples given include both: issues where security is not implemented for a certain service itself, or if it is missing on the respective OSI-layer and its underlying protocol stack.

ISO 27001 [34] defines the term *information security* as the combination of the properties *confidentiality*, *integrity* and *availability* together with the not mandatory *authenticity*, *accountability*, *non-repudiation* and *reliability*.

IEC 62443 [35] defines the term *communication security* as two distinct things:

(1) measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities
(2) state that is reached by applying security services, in particular, state of data confidentiality, integrity, and successfully authenticated communications entities.

The upcoming seven sections each define one of these properties, present exemplary implementations in well-known security protocols, and state possible issues regarding *Safety* and *Privacy* when the respective property is not achieved in aeronautical protocols. We inspect each of the properties independent of each-other, hence it is certainly possible that solving one issue also solves another. However, we argue that only by solving all issues independently, the system can be considered secure. For example, even if data encryption may solve a privacy issue when *integrity* is not provided, we still consider the lack of integrity an issue for privacy. Each section closes with real-world examples where absence of the respective property was the cause of a dangerous situation.

3.1. Confidentiality

RFC 4949 [33] defines confidentiality as *the property that data is not disclosed to system entities unless they have been authorized to know the data*. In comparison, the ISO 27001 (2.13) [34] defines it as *the property that information is not made available or disclosed to unauthorized individuals, entities, or processes*. Lastly, IEC 62443 [35] defines it as *assurance that information is not disclosed to unauthorized individuals, processes, or devices*.

Hence *confidentiality* is violated whenever an unauthorized entity (e.g., persons, industries, states) can read the content of aeronautical communications. Unauthorized and possibly malicious entities are therefore able to access typical contents ATM transmissions, such as information about the location, state, fuel level, or destination of an aircraft. Attackers can use such information to expose the system's state, leading to an increased attack surface. Additionally, business data (e.g., credit card information for buy-onboard services) are accessible for an attacker. The following three examples demonstrate two possible **Safety**- and one **Privacy** issue, which directly result from **Security** violations:

Safety #1: If control- or system messages are not confidential, an attacker can perform well-directed attacks to disturb the connection at the link layer. By e.g., obtaining knowledge of the fuel level, the attacker can execute a targeted attack which delays the landing so long that the plane is forced to land under dangerous circumstances due to fuel shortage. In contrast to an attacker blocking all communication to an aircraft, such an attack is much more difficult to discover by authorities or automatic intrusion detection systems.

Safety #2: If control- or system messages are not confidential, an attacker can perform well-directed digital attacks, if other security properties (e.g., integrity, authenticity) are not met as well. As before, an attacker could change or delete only safety critical messages or inject malicious safety critical control commands at well-selected time-points during the communication and would thereby be much more difficult to discover.

Privacy: Passenger data (e.g., medical emergencies) reported from the aircraft to the ground may be accessible by an attacker, which violates the passenger's privacy.

Real world examples:

ACARS, ADS-B and Mode S messages are mostly sent in unencrypted form. This allows platforms such as OpenSky [37] to collect them and publish these datasets to the scientific community. Smith et al. [12] examined ACARS encryption and detected that the used encryption could be broken on the fly by simple methods such as frequency analysis. This revealed information such as the existence of the aircraft, its destinations, and state - although the aircraft was assumed to maintain confidentiality in Air-to-Ground (A2G) communications. A later, more extensive study by the same team [13] explained that assumed confidentiality, e.g., of the existence of an aircraft, enabled by a blocking mechanism called Blocked Aircraft Registration Request (BARR), can be completely broken, due to no or weak encryption on ACARS messages. Overall, the lack of confidentiality allows tracking of the aircraft's information, e.g., its status, communication and passengers.

How this violates security has been practically shown at DEFCON 28 [38]. For example, it was reported that a certain airline had used an unencrypted link meant for safety-critical aeronautical communications to process credit card data, such that it was possible to eavesdrop on passengers' personal information. Passengers using the buy-onboard service were not aware at the time that their credit card data was transmitted in an insecure fashion. Secondly, it was demonstrated that BARR is easily bypassed and since aircraft broadcast their IDs during flight, this becomes a security problem when flight or aircraft IDs are linked to a certain group of people. Practical examples of traceability are CEOs using company-owned private jets with unique IDs or head-of-states using dedicated state-owned-aircraft, the most famous example being the Air Force One.

Additionally, the tracking of humans without their knowledge is a clear violation of privacy, demonstrated by the following example: Elon Musks's private jet was identified as Gulfstream G650ER, that can be tracked, which in and by itself is not an issue. Also manually tracking aircraft by spotters is not an issue by itself. However, combining the information about the passenger, the plane and its movements becomes a privacy problem as it is highly likely that a certain passenger, e.g., the owner, travels with that plane and hence, can be traced while airborne. Further, Elon Musk's private jet tracks were published on Social Media and the publisher ultimately received messages by Musk asking to take the account down, which again proves the privacy issue when flight tracks and aircraft ownership information are combined. [39]

Common practice

Confidentiality is typically ensured by encrypting messages. This can be done by asymmetric schemes (e.g., RSA cipher algorithm [40]), where the public key of the aircraft is stored at the ground station (and vice-versa). Alternatively, security protocols (e.g., Transport Layer Security (TLS) [41] or IPsec [42]) can be used to implement an asymmetric key exchange resulting in a shared secret, which can then be used for symmetric encryption (e.g., by the Advanced Encryption Standard (AES) [43]), which is typically faster than asymmetric encryption.

3.2. Integrity

RFC 4949 [33] defines integrity as *the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner*. The ISO 27001 (2.40) [34] instead defines it as *the property of accuracy and completeness*, while IEC 62443 [35] defines it as *quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data*.

Hence, whenever an unauthorized entity (e.g., persons, industries, states) can change the communication content, or when accidental changes (e.g., due to lossy physical connection) are not identified, *integrity* is breached. An attacker can then alter messages carrying system information (e.g., fuel level, position), or control (e.g., steering) or business data (e.g., credit card information for in-flight sales). As an example, "turn right by 5 degrees" can be changed to "turn left by 5 degrees" or a payment of $10 could be changed to $1,000. The following two examples demonstrate one possible **Safety**- and one **Privacy** issue, which directly result from **Security** violations:

Safety: Safety-critical messages (e.g., for collision avoidance) may be altered secretly, reduced, delayed, or destroyed by an attacker.

Privacy: If the metadata of information (e.g., recipient address) is altered during the communication, sensible (e.g., medical) information may be redirected to third parties.

Real world examples:

One of the most widespread systems that is also infamous for a lack of integrity-protection is ADS-B. This gap became well-known when it was discussed at Black Hat USA conference 2012 by Costin et al. [6], where several attacks were demonstrated. Some examples for problems that arise from a lack of integrity-protection are ghost aircraft injections, ghost aircraft flooding, virtual trajectory modification, false alarm attacks, ground station flooding, aircraft disappearance or aircraft spoofing [44]. Despite constant suggestions from the research community [7,44–51], the most relevant documents (the Minimum Operational Performance Standards (MOPS) of ADS-B, defined by the RTCA [52] or the ICAO relevant document for ADS-B, and the *Manual on Airborne Surveillance Applications* [53]) do not include any improvements to these issues.

Common practice

Integrity is typically provided by attaching an integrity check value to the message sent on the link. The tag is usually generated by a cryptographic hash function. Using a collision-resistant cryptographic hash function (e.g., SHA-256 or SHA-3) ensures that it is difficult for an attacker to introduce changes to the messages that result in the same integrity tag. Please note that this only ensures integrity if the integrity tag itself cannot be altered by an attacker. Most security protocols (e.g., TLS [41] or IPsec [42]) therefore implement message authentication codes, which provide both integrity and authenticity (see Section 3.4).

3.3. Availability

RFC 4949 [33] defines availability as *the property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them*. ISO 27001 (2.9) [34] defines availability as *the property of being accessible and usable upon demand by an authorized entity*. In turn, IEC 62443 defines it as *probability that an asset, under the combined influence of its reliability, maintainability, and security, will be able to fulfill its required function over a stated period of time, or at a given point in time*.

Hence, whenever an attacker is able to disturb communication (e.g., by jamming or denial of service attacks) or is able to modify it in a way that makes access to the airplane's information or control services impossible, *availability* is restricted. An attacker may be interested in disturbing systems performing security checks, that involve remote entities (i.e., AAA servers) so that other security or safety services are not available. Another attack vector are downgrade attacks: By forcing the plane to change to a weaker security system, an attacker can make some security features unavailable.

The following two examples demonstrate possible **Safety** issues, which directly result from **Security** violations:

Safety #1: If communication is not available due to unauthorized allocation of resources (by e.g., jamming, denial of service attacks), safety critical messages (e.g., such used for collision avoidance) may not reach the desired receiver, which can cause accidents.

Safety #2: If communication systems are not available, it may be impossible to perform safety checks involving remote entities.

Real world examples:

Skybrary, a EUROCONTROL, ICAO and Flight Safety Foundation supported website [54], maintains a list of accidents and serious incident reports which include A2G communication as a causal factor [54]. The inability to communicate provoked a range of dangerous incidents like landing without clearance, taking-off without clearance, near mid-air collisions, incorrect readback gone unnoticed, call sign confusion, and more [54]. Especially problematic are short periods of unavailable communication links or short outages during the transmission of crucial aircraft- or trajectory details. They can lead to misunderstandings and accidents related to aircraft actions without clearance.

Common practice

On the physical layer, jamming and spoofing attempts can be mitigated by implementing physical robustness measures. These include increasing the Signal-to-Interference-plus-Noise-Ratio (SINR) by either using more transmission power, or increasing the antenna gain, such as beamforming or fast frequency hopping. Techniques against smart jamming include pilot symbol scrambling jamming additionally. Lastly, redundancy in location, time, or frequency, or any combination thereof, can also help mitigate jamming and spoofing attacks [55]. Please note that most civil systems do not implement any physical robustness measure due to limited spectrum, expensive transmitter technology or a differing use case than military systems [55]. As such, in this work, a system is considered as achieving availability even if physical layer robustness techniques are neglected.

Simple measures can support availability, e.g., the correct configuration of a system: Setting a minimum requirement of the used version and define no service below that minimum version mitigates downgrade attacks. This has been done to protect TLS against downgrade attacks such as "Poodle" [56].

Access control supports availability as a cryptographic measure [41, 56], typically implemented by rolling out access credentials, e.g., in form of asymmetric cryptography and digital signatures in combination with a Public Key Infrastructure (PKI). By only allowing processing of messages signed with trusted public keys, the receiver of a message can deny unauthorized message processing and reserve resources for authorized (see Section 3.4) messages. In combination with measures like sequence numbers, which are implemented in security protocols (e.g., TLS [41] or IPsec [42]) and prevent overloading communication peers, the systems resources are available when needed.

3.4. Authenticity

(Data) authenticity is defined as *the property of being genuine and able to be verified and trusted* by RFC 4949 [33]. ISO 27001 (2.8) [34] specifies it as *the property that an entity is what it claims to be*. In the context of communication, the property of *data source authenticity* is important as well, Therefore, RFC 4949 [33] specifies it as *a corroboration that the source of data is as claimed*. IEC 62443 [35] does not specify the term authenticity but defines authentication as *security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information*.

Hence, whenever an attacker is able to communicate on behalf of another entity (e.g., convincing an aircraft that she is a trusted ground station), *authenticity* is violated. An attacker can inject unauthorized control messages to the airplane or simply plain wrong information (e.g., system information, business data) from the airplane to the ground station. Additionally, so-called *man-in-the-middle-attacks* become possible and *confidentiality, integrity*, etc., cannot be met even if security protocols like TLS or IPsec are applied. The following two examples demonstrate a possible **Safety**- and one **Privacy** issue, which directly result from **Security** violations:

Safety: If authenticity of safety critical messages (e.g., those used for collision avoidance) is not guaranteed, anyone can inject such messages and can provoke dangerous accidents or technical problems.

Privacy: If metadata of information (e.g., recipient address) is altered during the communication, sensible information may be redirected to unauthorized third parties. In contrast to the same attack vector for *Integrity*, the owner of the information would believe the receiving entity to be eligible.

Real world examples:

Having surveyed 242 aviation experts, Strohmeier et al. [57] conclude that "VHF is an increasingly common communications signal to be maliciously emulated by non-involved parties. [...] Anyone can buy an aviation transceiver without licence". The lack of authenticity, here for the VHF voice data link, allows anyone who knows the ATC specific language, the right frequencies, and has access to an aviation transceiver, to issue commands towards an aircraft. Even a 2002 EUROCONTROL study of VHF security reaches similar conclusions [58] (but was not followed by suitable measures). Also, the lack of authenticity allows injection, modification or erasure of aircraft as highlighted above in the case study about integrity of ADS-B [6].

Common practice

Authenticity is typically implemented by digital signatures. By signing an integrity tag of a message – either with an asymmetric private key or a pre-shared symmetric key – the receiver can ensure that the message can only originate from the owner(s) of the respective key. In combination with a PKI that maps verified identities to the key(s), this ensures data source authenticity.

3.5. Accountability

RFC 4949 [33] defines accountability as *the property of a system or system resource that ensures that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions*. ISO 27001 (2.8) [34] specifies it as *the assignment of actions and decisions to an entity* and IEC 62443 [35] as *property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions*.

Hence, whenever communication happens of which the sender is not uniquely identifiable – and therefore traceable – actions and information cannot be considered as trusted. Hence, *accountability* is violated. In that case, security services (e.g., intrusion detection or AAA services) cannot doubtlessly retrace responsibilities. The following two examples demonstrate one possible **Safety**- and one **Privacy** issue, which directly result from **Security** violations:

Safety: If the origin of a (safety critical) control message is not traceable, it may be more difficult to investigate accidents.

Privacy: If accountability is not in place, illicit communication of private data cannot be traced for law enforcement.

Real world examples:

As accountability requires identification and authentication, and then securely logging all relevant actions, examples from case studies under Section 3.4 – Authenticity – also apply. Other examples for the lack of accountability are when an aircraft transponder malfunctions and the steps identification, authentication, authorization and secure logging of actions cannot be carried out anymore [59]. This makes attributing actions to a certain actor impossible, if no further information for identification is transmitted.

Other examples are commands transmitted by ghost controllers [60]. Without further attributes such as voice matching, signal origin localization and so forth, it is impossible to hold the ghost controller accountable for his or her actions.

Common practice

Ensuring accountability requires identification of entities with access to a system, otherwise entities can be impersonated. As every signed action can be traced back to the originating identity (c.f., *Authenticity*), digital signatures need to be created with keys that were identified within a PKI, building up a chain-of-trust.

3.6. Non-repudiation

RFC 4949 [33] distinguishes between the (i) **proof of origin** and the (ii) **proof of receipt**. The first provides the *recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny having sent the data*. The second proof provides *the originator of data with evidence that the data was received as addressed, and thus protects the originator against an attempt by the recipient to falsely deny having received the data*. In contrast, ISO 27001 (2.54) [34] defines the concept of non-repudiation as *the ability to prove the occurrence of a claimed event or action and its originating entities*. Lastly, IEC 62443 [35] defines it as *security service that provides protection against false denial of involvement in a communication*.

Hence, whenever an entity can plausibly deny having sent or received a message or if an attacker is able to modify or intercept the corresponding confirmation, *non-repudiation* is violated. In that case, none of the communication peers can be held accountable for enforcing actions or for sending information. Additionally, an attacker can replay messages and force the receiver to perform a certain action multiple times but the original sender cannot notice the replay and is therefore not liable for the action. The following four examples demonstrate three possible **Safety**- and one **Privacy** issue, which directly result from **Security** violations:

Safety #1: Without mechanisms for uniquely verifying the origin of a message, an attacker may replay control messages unnoticeably and thereby harm the safety of the aircraft or its passengers without needing to fear consequences.

Safety #2: If control messages are not acknowledged by a unique receipt, another aircraft may replay the information and thereby cause the same harm as an attacker.

Safety #3: If safety critical messages are missing a proof of reception, any entity can deny having received the message.

Real world examples:

In ICAO Annex 10 Volume II chapter 5.2.1 [61] Radiotelephony (RTF) message formats are listed. The first part of a message is the call sign, containing information about the addressee and the originator of the message. The second part is text. ICAO Doc 4444 [19] further specifies air traffic control clearances and instructions and information for readback. Both documents are referring to voice communication. Overall there is a certain protocol for human air traffic communications in place, such as readbacks and standard phraseology. However, the transmission of voice communications as well as the origin of data or correct sequencing of messages is left to the underlying communications system. For example, HF or VHF do not provide such acknowledgments of reception of data, and thus the acknowledgment of information is still mostly left to human operators. Therefore, uniqueness and origin of message as well as an non-repudiable acknowledgment of reception could arguably also be a countermeasure for incidents such as *ACN: 1581222* [62], listed in National Aeronautics and Space Administration (NASA)'s Aviation Safety Reporting System (ASRS): Here, two flights with similar sounding call signs both reported a descent at the same time, thus blocking radio transmission without being aware of it and then immediately starting their descent at the same time. ATC could intervene and prevent a collision, such that both aircraft landed safely, but the dangerous situation could have been avoided overall.

Common practice:

Ensuring non-repudiation requires identification of entities that are eligible to send and receive information. The use of digital signatures of data with signing keys that were identified with a PKI allows verification of the data's origin. In combination with protocol mechanisms that provide uniqueness of a message, e.g., message sequence numbers, the signature originality becomes uniquely verifiable. In turn, a digitally signed and unique *receipt* allows verifying the reception of data.

3.7. Reliability

RFC 4949 [33] defines reliability as *the ability of a system to perform a required function under stated conditions for a specified period of time*, and ISO 27001 [34] states reliability as *consistent intended behavior and results.* Similarly, IEC 62443 [35] specifies it as *ability of a system to perform a required function under stated conditions for a specified period of time*. Please note the distinction between availability and reliability: Availability refers to the probability that a system is operational at a given point in time and reliability means that a piece of equipment

Table 1
Summary of relevant terrestrial digital aeronautical data links.

	VDL m0/A	VDLm2	VDLm4	UAT	1090ES	AeroMACS	LDACS
Use	A2G, G2A	A2G, G2A	A2G, G2A, A2A	A2G, G2A, A2A	A2G, G2A, A2A	A2G, G2A	A2G, G2A
Type	Selective	Selective, Broadcast	Selective, Broadcast	Selective, Broadcast	Selective, Broadcast	Selective, Broadcast	Selective, Broadcast
Sender	Air, Ground	Air, Ground	Air, Ground	Air, Ground	Air	Air, Ground	Air, Ground
Receiver	Air, Ground	Air, Ground	Air, Ground	Air, Ground	Air, Ground	Air, Ground	Air, Ground
Frequency (MHz)	129–137	118–137	118–137	978	1090	5091–5150	FL:1110-1156 RL:964–1010
Data rate	2.4 kbps	31.5 kbps	19.2 kbps	1 Mbps	1 Mbps	1.8-9.2 Mbps	0.6–2.8 Mbps
Modulation scheme	MSK	D8PSK	GFSK	CPFSK	OOK	Adaptive QPSK- 64-QAM	Adaptive QPSK- 64-QAM
Access method	CSMA	CSMA	S-TDMA	CSMA	CSMA	Scheduled	Scheduled
Adoption	In use	In use	Parts of the world	Parts of the world	In use	Parts of the world	In preparation
ICAO ref.	–	[65]	[66]	[67]	[68]	[69]	[70]
RTCA ref.	–	[71]	–	[72,73]	[74]	[75]	–

performs its intended function under stated conditions for a specific time interval without failure.

Availability is typically measured in percentage of the time a system is expected to be available while reliability is measured via Mean Time Between Failures (MTBF). Thus, if an attacker is able to alter communications behavior, or force the system to alter its intended outputs in a way that prevents authorized parties to communicate as intended, *reliability* is not given and a failure of the system occurs. The following two examples demonstrate possible **Safety** issues, which directly result from **Security** violations:

Safety #1: If safety critical messages are not delivered reliably, hence the communications equipment behaves in unintended ways due to an attack, serious harm may come to the plane or its passengers.

Safety #2: If messages include system information of the plane and are not delivered to the ground stations or their content altered, there is no way to prevent safety issues, and again, the system function (i.e., enabling communications between two entities) is limited.

Case studies

As ADS-B relies on the availability of Global Navigation Satellite System (GNSS) data, jamming GNSS can effectively disable ADS-B as learned from various flights recorded in the OpenSky data base in [63]. As such, due to the availability restriction of GNSS, the ADS-B system cannot perform its intended system function anymore and its reliability is restricted. A simpler way to obstruct ADS-B is the injection of messages by an illegitimate party, as described for *Authenticity* in Section 3.4 or in [64]. Furthermore, the second attack might be more dangerous, as availability outages of GNSS propagate to ADS-B, which can be defined as intended system behavior. However, to predict ADS-B behavior while under message injection attacks is much harder and most likely, intended system behavior is not defined while under such attacks. As a result ADS-B functions and outputs are modified in unpredictable ways.

Common practice:

A reliable communication system ensures that unauthorized third parties are not able to disturb the communication in such a way, that authorized entities cannot communicate anymore. Therefore, physical layer robustness measures as mentioned in Section 3.3 also apply here as countermeasure. Additionally, combining digital signatures, an identification, and an access control service ensures that unauthorized entities cannot access communications and start reliability attacks from that angle.

4. Wireless communications technologies in aviation

In order to argue why aeronautical communications as of 2021 require improvements in security, an understanding of relevant aeronautical communication services, networks, and data links is required. This section presents a systematic overview and is divided into three parts: digital aeronautical data links, aeronautical communications networks, and aviation communication services. Digital aeronautical data links provide the necessary physical and link layer technology for network layer services, such as ACARS, ATN/OSI (i.e., ATN) and recently ATN/IPS (i.e., Internet Protocol Suite (IPS)), to support aviation communication services such as CM, CPDLC, and Automatic Dependent Surveillance (ADS). An overview of the aeronautical communication landscape is provided in Fig. 1.

4.1. Digital aeronautical data links

The technical term for wireless communication technologies to transmit data between aircraft and ground is “digital aeronautical data link”. One commonly differentiates between terrestrial and space-based systems, which are designed for different flight domains. Terrestrial systems are used for short- or long-range continental communication in the Airport (APT), Terminal Maneuvering Area (TMA), or En-Route (ENR) domain, while space-based systems cover the Oceanic Remote Polar (ORP) domain [61,76]. Tables 1 and 2 provide an overview.

4.1.1. Terrestrial data links

VHF Data Link (VDL) mode 0/A, m2, m3, and m4 are a family of terrestrial digital aeronautical data links operating in the VHF band. In 1983 ICAO initiated a special committee on FANS to investigate necessary steps to deploy ATM [77]. At the 10th air navigation conference in 1991, a concept was presented including the use of digital data links supporting the automation of ATM [77]. Key concepts were the Aeronautical Telecommunications Net- work (ATN) [78] and a data link bridging the air gap between ground station and aircraft. This data link was initially VDLm0/A, the initial installment of ACARS, providing a data transmission rate of 2400 baud [79]. VDLm0/A was updated during the 1990s to VDLm2, which increased the data rate to 31.5 kbps using Differential 8 Phase Shift Keying (D8PSK), and Carrier Sense Multiple Access (CSMA) on multiple channels in the 118 MHz to 137 MHz band [65]. VDLm2 originally operated on a single common signaling channel, however, the number of channels has been increased recently to address capacity problems. Comparing VDLm0/A and VDLm2 revealed that VDLm2 increased message exchange and processing by at least 4.6 times [80]. VDLm3 [81] supported digital voice using Time Division Multiple Access (TDMA). However, VDLm3 was

never adopted. Standardization did not continue beyond 2002 [79,81]. VDLm4 was designed for navigational and surveillance purposes, can broadcast ADS data and establish an A2G and Air-to-Air (A2A) links without the need for ground infrastructure. Similar to VDLm3 it was never widely deployed and standardization ceased after 2004 [66,79]. It is, however, used in remote areas in Sweden and Russia.

The development of the **UAT** began in 1995. It was initially designed specifically for the transmission of ADS-B messages [82]. It operates on 978 MHz on a single common wideband channel, offers up to 1 Mbps and is capable of supporting multiple broadcast applications such as ADS-B, FIS-B, or TIS-B. UAT is standardized in Doc. 9861 by ICAO [67] and in RTCA's DO-282B [72]. The use of UAT for ADS-B is restricted to aircraft operating below 18,000 ft [67]. Newer developments include a feasibility study for UAT based Alternative Positioning Navigation and Timing (APNT) solutions in 2015 [83] and the use of UAT for drones in the UK. UAT is mainly deployed in general aviation in Alaska.

1090ES operates in a single channel at 1090 MHz. It is used by aircraft to broadcast detailed information on their position and intent. Contrary to SSR, also operating on this channel and using similar data formats, it does not require interrogation, but transmits periodically (ES stands for "Extended Squitter", implying this in aeronautical jargon). 1090ES is required for all aircraft operating over 18,000 ft to implement ADS-B. Guidance material for compatibility with ADS-B implementations using other data links (i.e., UAT) can be found in RTCA's DO-260B [74]. The dual link approach for ADS-B (1090ES and UAT) in different air spaces was initiated by the FAA with the European Union Aviation Safety Agency (EASA) also supporting both links for compatibility reasons since 2012 [84].

The **Aeronautical Mobile Airport Communications System (AeroMACS)** is a digital aeronautical data link for APT and TMA related communications [75]. It is based on the IEEE 802.16 WiMAX technology [85] and provides safety (ATS) and non-safety (AOC) related services at the airport. Safety related services can be provided via AeroMACS since it operates in the protected and licensed aviation C-band from 5091 MHz to 5150 MHz [70]. Currently AeroMACS is deployed at more than 40 airports worldwide [85]. Besides A/G communication with aircraft, AeroMACS is also used to interconnect remote airport infrastructure. Since it was developed based on IEEE 802.16, it has incorporated cybersecurity measures from WiMAX [86] and trust is based on a PKI approach [87]. AeroMACS is part of ICAO's Global Air Navigation Plan (GANP) [88].

The **L-band Digital Aeronautical Communications System (LDACS)** is a ground-based digital communications system for flight guidance and communications related to safety and regularity of flight in continental airspace [89]. It is under standardization by ICAO [90] and IETF [91] as of 2022. The main services provided by LDACS are ATS, AOC and future applications such as sectorless ATM, 4D trajectories or providing secure Ground Based Augmentation System (GBAS) data [92–94]. It provides up to 2 Mbps data rate, which is at least an order of magnitude more net capacity than the system it shall augment and replace, VDLm2 [95]. Strong cybersecurity is one requirement within the standardization efforts [96], however its cybersecurity design is not completed but ongoing work [97–104].

4.1.2. Space-based data links

Especially the Oceanic Remote Polar (ORP) domain and the Asia-Pacific region have been a particular focus for the developments of SATCOM for ATM data links. Reasons for that are the geographical scale or the remoteness of certain regions, which make the use of terrestrial data links not viable. ICAO Aeronautical Mobile-Satellite (Route) Service (AMS(R)S) [109] Standards and Recommended Practices (SARPS) [105] define three classes of satellite links (class A, B and C). Class C is used for current time-based ATM in ORP domains, class B is foreseen to cover trajectory-based operations, and class A is foreseen for performance-based operations [110].

Table 2
Summary of relevant space-based digital aeronautical data links.

	Inmarsat SB	Iridium Certus
Use	A2G, G2A, A2A	A2G, G2A, A2A
Type	Selective, Broadcast	Selective, Broadcast
Sender	Air, Ground, Space	Air, Ground, Space
Receiver	Air, Ground, Space	Air, Ground, Space
Frequency (MHz)	FL: 1626.5-1660.5, 1668-1675 RL:1518-1559	1616–1626.5
Data rate	432 kbps	22–704 kbps
Modulation scheme	A-BPSK, A-QPSK	QPSK
Access method	Scheduled	Scheduled
Adoption	In use	In use
ICAO ref.	[105,106]	[105,106]
RTCA ref.	[107,108]	[107,108]

Inmarsat was established in 1979 originally for maritime applications. Currently the sixth generation of Inmarsat −6 satellites is fully deployed, with the next generation Inmarsat −7 satellites scheduled for launch in 2023 [111]. The Inmarsat aeronautical network is ICAO SARPS [105] and RTCA DO-262D [107] compliant and provides ATC and AOC two-way voice and data services at various data rates [111]. The first service in that domain was Inmarsat Aero-H Mobile Satellite Communication (MSC) providing 10.5 kbps in the global beam. Aero-H was extended to Aero-H+ using higher transmission power. This made it compliant with ICAO's requirements to support CNS or ATM. Thus, ACARS messages could be transmitted via Aero-H+. Aero-H+ was later upgraded to Aero-HSD+, which provides 64 kbps. Other Inmarsat services are: Aero-I, Aero Mini-M, Aero-C, Aero-L, Swift64 (Aero-M4), SwiftBroadband (SB), Aeronautical Jet ConneX (JX) [111]. The Inmarsat Iris system is a certified class B system (with possible evolution to class A). It is based on the Inmarsat SwiftBroadband technology [112], supports IPv4 (which introduces some problems when deploying the IPv6-based ATN/IPS) and offers up to 432 kbps [111]. The latest JX system offers higher Quality of Service (QoS) and up to 50 Mbps on the forward and 5 Mbps in the reverse data link per beam. It also provides a secure end-to-end connection, from cockpit to the ground Communications Service Provider (CSP) or Aeronautical Network Service Provider (ANSP) for voice and data paths and mutual authentication and data integrity protection controls [112].

Founded in 1991 [111], the **Iridium** company started its aeronautical services over an Iridium communications circuit offering between 600–2400 bps [113]. In an upgrade the Iridium NEXT second-generation satellites offer services in the L-band and provide 22–88 kbps in the midband and 128–704 kbps in the broadband [114]. Iridium currently offers one class B system (with possible evolution to class A), which is the Iridium Certus system [115]. Iridium Certus data offers IPv4 services (with similar problems as Inmarsat with regard to the IPv6-based ATN/IPS) and is expected to be deployed via the Iridium NEXT constellation [116]. Minimum Aviation System Performance Specifications (MASPS) for the Iridium Certus system are defined in RTCA's DO-243C [108] and MOPS in RTCA's DO-262D [107]. Iridium Certus offers security features such as application layer data security via the IPSec Encapsulated Security Payload (ESP) protocol using Internet Key Exchange v2 (IKEv2) with an Iridium based PKI [117].

Future Constellations: While Iridium and Inmarsat already have satellites for aeronautical communications deployed, companies like SpaceX with Starlink [118], OneWeb [119], and TeleSat with Lightspeed [120] are entering the market to provide Low Earth Orbit (LEO) IP SatCOM for aeronautical communications.

The massive scale of the envisioned constellations (i.e., 42,000 planned satellites with Starlink) offer low end-to-end latency rates and

high data-rates at relatively low-cost. The three main disadvantages are a rapid handover rate [121], a possibly high-interference rate and a multitude of different system users. The latter is especially challenging for security, as the systems can be used for safety-critical and non-safety critical communications at the same time [122]. There are studies that envision massive LEO constellations as a single solution for aeronautical communications [123]. However, the study gives no solutions for critical issues, such as rapid handovers, interference, and the sharing the service with multiple, non-safety-critical-communications-requiring users.

Out of the three different communications domains declared by ICAO [124] – (1) passenger entertainment services, (2) aircraft information services, (3) and aircraft control data – only the first can be provided with the current state of these massive LEO constellations. The required reliability for safety-critical aeronautical communications (2,3) is above 99.999%, while for regular commercial data links reliability can be lower than 99.9% [122]. Before safety-critical data at high reliability can be provided via these solutions, the aforementioned problems of LEO based SatCOM will need to be addressed.

4.2. Aeronautical network and transport layer services

In this part, we explain the different aeronautical communications networks, thus covering the underlying aeronautical network architecture, bringing aeronautical data links and applications together.

The **Aircraft Communications Addressing and Reporting System (ACARS)** had its origins in the necessity that flight crews had to report flight times via voice communication to ground radio operators, as they were paid differently for being airborne or on ground. Voice communications being quite error prone, the text-based ACARS system was launched in July 1978 in an effort to improve the accuracy of reports, to reduce crew workload, and to improve data integrity in general [125]. Technically ACARS is a character-based Telex point-to-point protocol. Later, different services were added to be communicated via ACARS such as ATC, AOC or AAC information [126]. ATC over ACARS is implemented as the Future Air Navigation System (FANS) 1/A package. It consists of the CPDLC and Automatic Dependent Surveillance-Contract (ADS-C) applications. ACARS is one of the first systems in the aeronautical communications ecosystem that supported the exchange of digital information. Originally a Medium Shift-Keying (MSK) modem was used to send the data via a dedicated VHF channel, resulting in a data rate of 2.4 kbps [126].

ACARS predates modern concepts of layered network stacks and was implemented as an integrated system. This combination of the ACARS Telex protocol, applications, and VDLm0/A is often called Plain Old ACARS (POA).

In modern implementations ACARS is viewed as an application or overlay network over another data link i.e., Telex messages are encapsulated in packets of the underlying network. In case of VDLm2 this is implemented by the combination of the ACARS-Over-AVLC (AOA) and Aviation VHF Link Control (AVLC) protocols. A similar compatibility layer for satellite communications, Aeronautical Mobile Satellite System (AMSS) for Inmarsat and Short Burst Data (SBD) for Iridium, exists. ACARS over IP is also defined. Thus, with the integration of different newer data links into the aeronautical communications ecosystem, ACARS messages can be transmitted via the following links: (1) VHF, (2) VDLm2, (3) HF data link, (4) AeroMACS, (5) LDACS, (6) Inmarsat satcom and (7) Iridium satcom [126]. For use cases not related to safety and regularity of flight ACARS is also used over non-aviation IP data links like IEEE 802.11 (WiFi).

Security and privacy of ACARS was already analyzed in previous works [10,127] with the result, that the original ACARS message protocol offered no protection for any of the cybersecurity properties defined in Section 3. To address this issue, Aeronautical Radio, Incorporated (ARINC) made a concerted effort to develop a security framework, AMS for ACARS messages, described in ARINC specifications 823P1 [128] and 823P2 [129]. In [128], they describe AMS including methods for message authentication, data integrity and confidentiality. In [129], the key management for AMS is explained in depth. Even though this security framework exists, it is hardly in use today, as ANSPs charge extra for this service [127]. As AMS secured ACARS messages and plain text ACARS messages still coexist, we will regard them as separate entities in the gap analysis in Section 5.

The **Aeronautical Telecommunications Network (ATN)/Open Systems Interconnection (OSI)** was first described in ICAO Doc. 9705 [130] in 1998 as "... application entities and communication services which allow ground, air-to-ground and avionics data sub networks to interoperate by adopting common interface service and protocols based on the International Organization for Standardization (ISO) open systems interconnection (OSI) reference model" [130]. In 2010, ICAO Doc. 9705 was superseded by ICAO Doc. 9880 [131]. The general goal was to establish a common internetwork for aeronautical services, enabling interoperability across worldwide air traffic control. The two most important applications are CPDLC and ATS Message Handling Service (ATSMHS). This can also be seen within the structure of ICAO Doc. 9880 [131], as it consists of four parts, the first defining air–ground, mostly the text-based message exchange between pilot and controller (CPDLC), the second part ground–ground applications (ATSMHS) which is used for the worldwide exchange of flight plan data. Part III defines ULCS, which defines the DS and covers session, presentation and application layer. Lastly, part IV defines directory services, security, and identifier registration and is therefore the focus part of this work. We show the ATN/OSI protocol stack and security implementation in Fig. 2. The ATN/OSI protocol stack consists of Link Layer, M-SNDCF, CLNP, and TP4. ATN ULCS is responsible for establishing a session among communicating peers on the airborne and ground sides and also handles security as depicted on the left side of Fig. 2 [130].

According to ICAO Doc. 9705 [130], the ULCS implements the ASE serving as the DS. From there, data is transferred either (1) without security additions via the ACSE or (2) with security additions via S-ASO. In the second case, SESE for handling the transfer of security information and SSO for cryptographic primitives' implementation are used. To simplify the security implementation in the ATN/OSI stack and to be compatible with the requirements of ATN/IPS in ICAO Doc. 9896 [132], the security measures were shifted from S-ASO to the Secure Dialogue Service (SecDS). To the best of the authors' knowledge, the only standard being able to validate the security requirements from ICAO Doc. 9880 IV-B [19], was the ARINC standard 823 [128] for AMS. Hence, the terms "Secure Dialogue Service" and "ACARS Message Security (AMS)" can be used interchangeably for now.

Aeronautical Telecommunications Network (ATN)/Internet Protocol Suite (IPS) The GANP of ICAO [88] and the Air/Ground Data Communications Strategies of the European Union (EU), Single European Sky ATM Research (SESAR),[1] and NextGEN in the United States (US),[2] strive for a globally harmonized aviation communications ecosystem that includes a communication infrastructure based on IPv6. This network infrastructure is considered the successor to the ACARS and ATN/OSI networks. The first specification with details about ATN/IPS was released in 2010 in ICAO Doc. 9896 [132], with the third edition in preparation as of 2021. The specification has four abstraction layers, namely the link layer, which can be filled by any aeronautical data link technology discussed above, the internet or IP layer, the transport layer and the application layer, where aeronautical applications are served. The ATN/IPS architecture is depicted in Fig. 3. Further requirements such as mobility, multilink, management, interface and naming conventions, transport layer, network layer, IPS routing and security requirements are defined in RTCA DO-379 [133].

[1] https://www.sesarju.eu/ July 07, 2022.
[2] https://www.faa.gov/nextgen/ July 07, 2022.

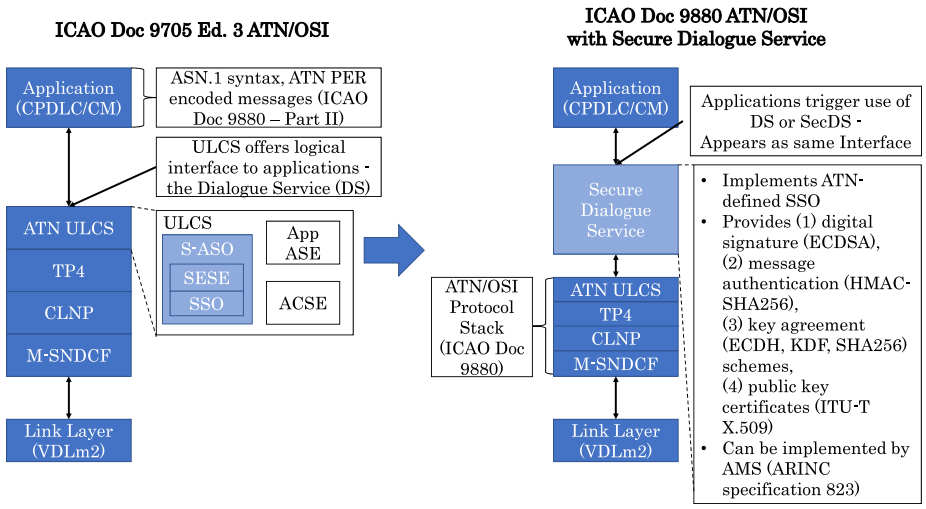

Fig. 2. Aeronautical Telecommunications Network (ATN)/OSI protocol stack is depicted with security measures as defined in ICAO Doc. 9705 [130] and in ICAO Doc. 9880 [131]. Abbreviations follow below:
Association Control Service Element (ACSE), ACARS Message Security (AMS), Air/Ground Application Service Element (ASE), Abstract Syntax Notation One (ASN.1), Aeronautical Telecommunications Network (ATN), ConnectionLess Network Protocol (CLNP), Context Management (CM), Controller Pilot Data Link Communications (CPDLC), Dialogue Service (DS), Elliptic Curve Diffie-Hellmann (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA), Keyed-Hash Message Authentication Code (HMAC), International Telecommunication Union (ITU), Key Derivation Function (KDF), Mobile Sub-Network Dependent Convergence Function (M-SNDCF), Packed Encoding Rules (PER), Security-Application Service Object (S-ASO), Secure Dialogue Service (SecDS), Security Exchange Service Element (SESE), Secure Hash Algorithm (SHA), Security Service Object (SSO), Transport Protocol class 4 (TP4), Upper Layer Communications Service (ULCS), VHF Data Link mode 2 (VDLm2).

For the scope of this work, it is important to note, that a total of 18 security requirements are defined in [133], which are incorporated in the ARINC standard P858 [134]. ATN/IPS defines three security layers: *Application security*, which provides end-to-end security for data exchanged between IPS nodes, such as airborne and ground nodes. The basis for application security can be found in transport layer security, namely the incorporation of TLS [41] or Datagram Transport Layer Security (DTLS) [135] depending on the underlying transport protocol (i.e., TCP or UDP). Due to the multilink requirements (i.e., interchangeable use of terrestrial or space-based data links, resulting on highly diverse Round Trip Time (RTT)) the default transport protocol will be UDP with reliability extensions according to [133] defined in [132]. *Network-security* describes intra-network security, protecting ground-based IPS nodes within an administrative domain, and inter-network security, which protects the communication between ground-based nodes across different administrative domains. ICAO Doc. 9896 [132] defines inter-network security mechanisms, such as the usage of the BGP protocol version 4 [136] (c.f. Fig. 3), to ensure global interoperability. Lastly, it is foreseen that *data link security* is handled by the respective aeronautical data link (e.g., AeroMACS, LDACS, SATCOM), providing mostly access control mechanisms to the overall ATN/IPS network infrastructure. The mismatch between IPv6 in the ATN and IPv4 in the satellite data links is an open issue. The standardization and roll-out of ATN/IPS is, as of 2021, an ongoing process and most aeronautical applications are still served via ACARS or ATN/OSI in Europe.

4.3. Aviation communication services

Aviation communication services or aeronautical applications can be split into Air Traffic Services (ATS) applications [76], which enable interactions between aircraft and ANSPs, and Aeronautical Operational Control (AOC) applications, which concern flight planning, weather, dispatching, ground handling, and messaging of the airline. Current and future ATS applications include:

FANS-1/A RTCA DO-258 A [137] defines the original FANS-1/A applications as ATS Facilities Notification (AFN) messaging, ADS-C position reporting, CPDLC text-based controller-pilot communications, using the ACARS protocols A2G message transfer (i.e., defined in ARINC P622 data communication).

FANS-1/A+ upgrades FANS-1/A communications, by including a message latency detection function.

Baseline 1 (B1) is a subset of the ICAO ATN application set defined under ICAO Doc. 9705 [109] and 9880 [19]. RTCA DO-280B [138] defines B1 services as CM, ADS, CPDLC and Flight Information System (FIS). Additional applications are ADS-B, FIS-B, and TIS-B informational services. B1 applications will be provided primarily via ACARS or ATN/OSI.

Baseline 2 (B2) systems are data link equipped aircraft and ground systems compliant with RTCA DO-350 A [139]. The shift from B1 to B2 is a major expansion of ATN capabilities, including 4D Trajectory (4DT) based operations and airport services. As with B1 applications being designed mainly for usage via the DS defined in ATN/OSI [19], these services will be accommodated on IPS using the IPS Dialogue Service (DS) specified in ICAO Doc. 9896 [132].

ARINC standards 702 A and 620 [140,141] define a multitude of AOC services, such as the "FLTPLAN" service – "Flight Plan" –, which prepares the flight plan in accordance with AOC and loads it into avionics, or the "NOTAM" service – "Notice to Airmen" –, which alerts the flight crew of special circumstances such as airspace restrictions. In this work, aviation communication services are differentiated by their usage for air traffic control and for aeronautical information services.

Tables 3 and 4 provide an overview. The following section characterizes the different systems mentioned in the Tables 3 and 4 briefly.

4.3.1. Air traffic control

ATC [28,76] provides flight guidance, thus performs communication related to safety and regularity of flight. The main purpose of ATC is to "to prevent a collision between aircraft operating in the system and to organize [...] the flow of traffic" [142]. As a result, communications technologies can be seen as the enabler for ATC procedures and provider for the communication between air traffic controllers and pilots.

The **HF, VHF, or "airband"** [143] **technology** is still the primary communication between ATC and aircraft today [70]. Frequency bands of 2–30 MHz have been assigned to HF, while VHF voice is

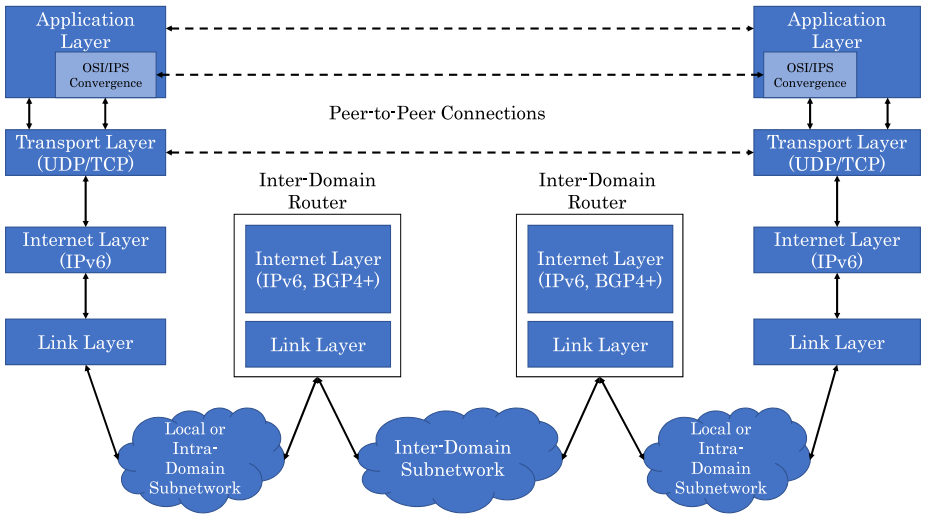

Fig. 3. ATN/IPS protocol architecture is depicted as defined in ICAO Doc. 9896 [132]. Abbreviations follow below:
Border Gateway Protocol (BGP), Internet Protocol (IP), Internet Protocol Suite (IPS), Open Systems Interconnection (OSI), Transport Control Protocol (TCP), User Datagram Protocol (UDP).

located between 117.975-137 MHz [143]. The underlying communication technique still relies on analogue VHF Double Side-Band Amplitude Modulation (DSB-AM), which has been in use since 1948 [70]. Main purpose of this technology is to provide voice-based Aeronautical Mobile (Route) Service (AM(R)S) [78], thus to provide necessary information to conduct flights safely such as clearances, weather information and flight information services [144]. Voice transmission sites are connected to ATC centers via dedicated VCSs. Modern VCSs use voice over IP according to ED-137 [145].

A data link application allowing the exchange of data messages between ATC and flight crew [106] is realized by **CPDLC**. Mainly used for clearances and requests, the operators can either use pre-selected key words or free text to send messages either in A2G or Ground-to-Air (G2A) direction. CPDLC holds several advantages over voice communications, such as the reduction of misunderstandings between pilot and air traffic controller due to acoustic noise or the transmission of long or complex information such as weather data or flight plan changes. Furthermore, CPDLC paves the way for semi-automatic or fully automatic flying. This is important especially for new entrants, such as Unmanned Aeronautical System (UAS). DO-280B [146] mentions a CPDLC Protected Mode (PM). However, ICAO Doc. 10037 [106] clarifies, that this is simply another term for the VDLm2 system. Currently, the main underlying data link used worldwide for CPDLC is VDL Mode 2 [28,106] with a few areas of the world also supporting VDL Mode 4 [79]. It mainly uses the ACARS network outside of Europe. In Europe the transition to ATN/OSI has already begun. Other areas plan to migrate directly to ATN/IPS without intermediate steps.

Secondary Surveillance Radar (SSR) is a cooperative surveillance technology which provides target information such as aircraft identity and altitude [147]. In the context of our paper we can think of it as a digital means to exchange position data. It relies on SSR ground stations that broadcast interrogations to aircraft transponders. There are several aviation transponder interrogation modes: Mode 1 to 5 for military use and Mode A, B, C, D and S for civilian use [148]. Mode A provides a 4-digit octal identification code for the aircraft, which is referred to as *Squawk Code* and often assigned by ATC prior to the flight [149]. Pressure altitude can be transmitted using Mode C, which is often combined with Mode A in alternating interrogations [150]. More complex information can be sent utilizing Mode S, with each aircraft having assigned a 24-bit ICAO address [148]. Mode S will substitute Mode A and C, which also allows the specific interrogation of a single aircraft instead of requesting information from all aircraft in broadcast range (S stands for "selected"). SSR uses 1030 MHz for interrogations and 1090 MHz for replies [147]. Evaluating the 1090 MHz responses, a SSR system can obtain airspace monitoring information, such as aircraft positions and velocities [151]. SSR has no network layer in the conventional sense, although SSR data is exchanged over the ground network using the ASTERIX message format. ASTERIX messages may be exchanged via IP networks or X.25 networks.

ADS-B is a GNSS dependent surveillance technology where aircraft automatically broadcast their GNSS based position [47,152]. The tracking data is intended for ATC ground stations, and therefore replaces active interrogations of those or other aircraft in the vicinity, providing situational awareness [7]. Furthermore, ADS-B broadcasts can also be received by Low Earth Orbit (LEO) satellites (such as e.g., Iridium-Next) in order to enable traffic surveillance over ORP areas [153]. With that, FAA and EUROCONTROL named ADS-B "the satellite successor of Primary Surveillance Rader (PSR) and SSR" [28]. Updates happen every 0.5 s for position and velocity and every 5 s for identification [154]. Broadcast data can be sent via two competing data links: UAT or 1090ES [44,73]. As UAT requires new hardware, ADS-B and SSR Mode S has been fused to the 1090ES link for easier deployment [74]. ADS-B has no network layer, since data is directly exchanged between aircraft. If ADS-B data is used for surveillance on the ground, it is treated like SSR data i.e., exchanged using ASTERIX. In 2014, a first work by the German Aerospace Center (DLR) demonstrated the technical feasibility of space-based 1090ES ADS-B surveillance [153]. In 2019, Baker informed about the deployment of commercial space based ADS-B by different SatCOM manufacturers [155]. However, since the space-based ADS-B technology also relies on the 1090ES data-link, the same vulnerabilities apply, except that spoofing space-based ADS-B messages can prove more difficult due to related satellites using beam-forming antennas to deliver the ADS-B message [156].

4.3.2. Information services

The **TCAS** is an SSR transponder signal based, ground ATC independent aircraft collision avoidance system designed to mitigate the risk of mid-air collisions [162]. The version in use as of 2021, TCAS II, specified in RTCA's DO-185 [163], uses information such as identity, altitude, position, bearing or velocity from available ATC data, such as Mode C, S or ADS-B. This information is then displayed to the pilot to provide a traffic surveillance overview of all aircraft in the vicinity and are used to trigger advisories [164]. If a transponder equipped aircraft is evaluated as an intruder, a Traffic Advisory (TA) is issued which raises pilot awareness and aids in visually detecting the correct

Table 3
Summary of ATC systems [28].

	Voice	CPDLC	SSR	ADS-B
System description	Voice comm ATC-cockpit	Data comm ATC-cockpit	Cooperative aircraft detection, positioning, data exchange	Broadcast aircraft, ATC data, Collision avoidance
Contents	ATC, AOC	ATC, ATS, AOC	A: 4-digit codes, C: Altitude, S: ADS-B-like without position	SAC, SIC, TOD, FL,position, TID,
Network layer	VCS	ACARS, ATN/OSI, ATN/IPS	ASTERIX messages over IP/X.25-ground networks	–
Link layer	HF, VHF	VDLm2/m4, AeroMACS, LDACS, Inmarsat SB, Iridium Certus	1090	UAT 1090ES,
Signal	Analogue	Digital	Digital	Digital
Adoption	In use	In use	In use	In use
ICAO Ref.	[78,106]	[78,106]	[78,147]	[53,152]
RTCA Ref.	[157,158]	[139,159]	[160,161]	[52,74,154]

Table 4
Summary of aeronautical information systems [28].

	ACARS	TCAS	FIS-B	TIS-B
System description	Data Communications	Collision Avoidance	Flight Information	Traffic Information for non ADS-B equipped aircraft
Contents	Flight ID, Position, Weather, Maintenance, Engineering, more	Transponder Status, Position	Weather NOTAM	Traffic Information
Link layer	VDL m0/A/m2/m4, AeroMACS, LDACS, Inmarsat SB, Iridium Certus	Mode S, 1090ES	UAT	UAT, 1090ES
Signal	Digital	Digital	Digital	Digital
Adoption	In use	In use	Parts of US	Parts of US
ARINC Ref.	[125,126]	–	–	–
RTCA Ref.	–	[163,171]	[167,172]	[74,173]

traffic. If the aircraft becomes hazardous, TCAS can further provide a Resolution Advisory (RA). This is a suggested, vertical maneuver designed to preserve or increase separation from conflicting aircraft, which pilots are expected to follow immediately. If both involved aircraft are equipped with TCAS II, the maneuvers can be coordinated between the individual TCAS units utilizing 1030/1090 MHz for coordination interrogations as well [165]. Currently all this information is received via interrogation of nearby aircraft with an update rate of 1 Hz. However, hybrid solutions relying on ADS-B data for distant aircraft have been proposed [165]. In the future, full incorporation of ADS-B can make interrogation unnecessary [28].

The **FIS-B** is a G2A broadcast service via the UAT data link of meteorological and aeronautical information (e.g. Notice To Airman (NOTAM), Next-Generation Radar (NEXRAD) or Significant Meteorological Information (SIGMET)) [166]. MOPS are specified in DO-358 [167]. An aircraft needs to be equipped with an UAT receiver and data are transmitted on 978 MHz [168]. Currently, FIS-B is mainly deployed in US airspace and the FAA provides data mainly for flights below 24,000 ft [166].

TIS-B, defined in DO-260B [74], presents a timely overview of nearby aircraft positions based on the combined information of GNSS and ground-based radar [169]. TIS-B information is either broadcast via 1090ES or UAT, and thus it uses the same frequencies and even the same message format as ADS-B [74]. The system is mainly used in the US and intended for aircraft that are not equipped with ADS-B receivers, yet [170].

5. Gap analysis: Security in aeronautical communications

In this section we map the seven security properties defined in Section 3 to the respective aeronautical data links, networks or services described in Section 4. For each communication technology, we analyze whether or not the security properties are found in one of the following three categories:

1. **Requirements:** A system's operational requirements are defined by ICAO Standards and Recommended Practices (SARPS), or RTCA Minimum Operational Performance Standards (MOPS).

2. **Specifications:** System specifications are either ICAO system manuals or relevant documents defined by RTCA, EUROCAE or ARINC.

3. **Literature:** Scientific literature refers to conference contributions, journal papers or book chapters, that typically address one or more security property for one technology.

The results are presented in Tables 5–7, where ✔ means that the property is defined and ✘ depicts its absence. (✔) depicts that the property is defined as optional in the respective documents. A grayed-out row indicates that either no security work has been published on a respective system or the documentation is not publicly accessible. In addition, the respective (scientific) sources are annotated in every cell. We consider a security property to be achieved according to the following rule-set:

Confidentiality: A system implements (1) a secure key establishment and key derivation mechanism (2) between authorized parties and (3) uses established and derived keys to encrypt exchanged messages.

Integrity: A system implements (1) a secure key establishment and key derivation mechanism (2) between authorized parties and (3) uses established and derived keys to integrity-protect exchanged messages, while (4) also implementing self-tests to check for logical correctness of the system.

Availability: A system is (1) configured with a certain minimum security version to mitigate downgrade attacks, (2) implements access control and (3) redundancy.

Authenticity: A system (1) is correctly incorporated in a trust infrastructure, e.g., a PKI, and it implements (2) authentication measures such as using signatures verifiable by trusted public keys, (3) measures ensuring that trusted keys are still valid, e.g., by implementing certificate revocation measures, and (4) data origin authenticity for relevant messages.

Accountability: A system implements (1) authenticity measures, hence access control, and (2) users and system entities are forced to authenticate before any action on a system is performed and (3) these actions are securely and uniquely traceable logged.

Non-Repudiation: A system implements the same measures as for accountability, but additionally implements (1) measures that guarantee uniqueness of messages and (2) relevant messages are signed by the responsible user or system entity.

Reliability: A system is (1) correctly configured for the intended use case, (2) implements measures addressing at least integrity, availability and authenticity.

Table 5
Aeronautical data links: Summary of existence of security properties as specified in requirements, specification or scientific literature.

	Confidentiality	Integrity	Availability	Authenticity	Accountability	Non-repudiation	Reliability
Requirements - MOPS, MASPS (RTCA), SARPS (ICAO)							
VDLm0/A	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]
VDLm2	✘[71,78]	✘[71,78]	✘[71,78]	✘[71,78]	✘[71,78]	✘[71,78]	✘[71,78]
VDLm4	✘[174]	✘[174]	✘[174]	✘[174]	✘[174]	✘[174]	✘[174]
UAT	✘[72,73]	✘[72,73]	✘[72,73]	✘[72,73]	✘[72,73]	✘[72,73]	✘[72,73]
1090ES	✘[74,147]	✘[74,147]	✘[74,147]	✘[74,147]	✘[74,147]	✘[74,147]	✘[74,147]
AeroMACS	✔[75,175]	✔[75,175]	✔[75,175]	✔[75,175]	✔[75,175]	✔[75,175]	✔[75,175]
LDACS	(✔)[90]	✔[90]	✔[90]	✔[90]	✔[90]	✔[90]	✔[90]
Inmarsat SB	(✔)[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]
Iridium Certus	(✔)[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]	✔[107,108]
Specification - Manual (ICAO, RTCA)							
VDLm0/A	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]	✘[125]
VDLm2	✘[65]	✘[65]	✘[65]	✘[65]	✘[65]	✘[65]	✘[65]
VDLm4	✘[66]	✘[66]	✘[66]	✘[66]	✘[66]	✘[66]	✘[66]
UAT	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]
1090ES	✘[68]	✘[68]	✘[68]	✘[68]	✘[68]	✘[68]	✘[68]
AeroMACS	✔[69,86]	✔[69,86]	✔[69,86]	✔[69,86]	✔[69,86]	✔[69,86]	✔[69,86]
LDACS	✘[95]	✘[95]	✘[95]	✘[95]	✘[95]	✘[95]	✘[95]
Inmarsat SB	(✔)[108]	(✔)[108]	(✔)[108]	(✔)[108]	(✔)[108]	(✔)[108]	(✔)[108]
Iridium Certus							
Literature - Academic							
VDLm0/A	✔[10]	✔[10]	✔[10]	✔[10]	✔[10]	✘[10]	✔[10]
VDLm2	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]
VDLm4							
UAT	✔[5,46]	✔[5,46]	✔[46]	✔[5,46]	✔[46]	✔[46]	✔[46]
1090ES	✔[7,50,191]	✔[7,50,191]	✔[7,50,191]	✔[7,50,191]	✔[7,50,191]	✔[7,50,191]	✔[7,50,191]
AeroMACS	✔[85]	✔[85]	✔[85]	✔[85]	✔[85]	✔[85]	✔[85]
LDACS	✔[98,102,104]	✔[98,102,104]	✔[98,102,104]	✔[98,102,104]	✔[98,102,104]	✔[98,102,104]	✔[98,102,104]
Inmarsat SB	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]
Iridium Certus	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]	✔[177,178]

Table 6
Aeronautical communications networks: Summary of existence of security properties as specified in requirements, specification or scientific literature.

	Confidentiality	Integrity	Availability	Authenticity	Accountability	Non-Repudiation	Reliability
Requirements - MOPS, MASPS (RTCA), SARPS (ICAO)							
ACARS	✘[179]	✘[179]	✘[179]	✘[179]	✘[179]	✘[179]	✘[179]
ACARS AMS	✔[128]	✔[128]	✔[128]	✔[128]	✔[128]	✔[128]	✔[128]
ATN/OSI	✘[180]	✘[180]	✘[180]	✘[180]	✘[180]	✘[180]	✘[180]
ATN/IPS	✔[133]	✔[133]	✔[133]	✔[133]	✔[133]	✔[133]	✔[133]
Specification - Manual (ICAO, RTCA)							
ACARS	✘[125,126]	✘[125,126]	✘[125,126]	✘[125,126]	✘[125,126]	✘[125,126]	✘[125,126]
ACARS AMS	✔[128,129]	✔[128,129]	✔[128,129]	✔[128,129]	✔[128,129]	✔[128,129]	✔[128,129]
ATN/OSI	✘[19]	✔[19]	✔[19]	✔[19]	✔[19]	✔[19]	✔[19]
ATN/IPS	✔[132,134]	✔[132,134]	✔[132,134]	✔[132,134]	✔[132,134]	✔[132,134]	✔[132,134]
Literature - Academic							
ACARS	✔[10,127,181]	✔[10,127,181]	✔[10,127,181]	✔[10,127,181]	✔[10,127,181]	✔[10,127,181]	✔[10,127,181]
ACARS AMS	✔[182,183]	✔[182,183]	✔[182,183]	✔[182,183]	✔[182,183]	✔[182,183]	✔[182,183]
ATN/OSI	✘[184]	✔[184]	✔[184]	✔[184]	✔[184]	✔[184]	✔[184]
ATN/IPS	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]	✔[176]

Overview:

Even at the very first glance, the tables show that security is lacking in most data links and services. Only in aeronautical network technologies (c.f., Table 6), security seems to be slightly more elaborated. On the other hand, all tables show a gap between research and requirements and specifications, which will be the first part of the following in-depth analysis (Section 5.1). For better readability, we guide through this analysis by raising questions on some aspects of the tables. On top, we show that these issues will worsen in the future, as a multitude of new attacker types is on the horizon (Section 5.2). We close this chapter with some recommendations (Section 5.3) on how the gaps can be overcome and attacks can be prevented in the future. Our major findings and recommendations are then summarized in Section 6 (See [174–190]).

5.1. Gap between research, standards and implementation

One of our key findings is: *Security provisions at only one layer already secure aeronautical data substantially. Unfortunately, combinations of data-links, network services or applications that bear no security features at all are still prevalent, which is the key reason why aeronautical data is vulnerable on the wireless data link.*

This is the case when unsecured aeronautical service data (c.f., Table 7) is delivered via an unsecured aeronautical network (c.f., Table 6) and transmitted via an unsecured data link (c.f., Table 5). At a first glance, with a multitude of common security measures available for all layers, one may assume this to be a very rare circumstance. Still, attacking such system has been multiply demonstrated, e.g., in [6, 9,12–15,28,38,57,63,92,127,191,193–196]. The question that remains unanswered is:

Table 7
Aeronautical communication services: Summary of existence of security properties as specified in requirements, specification or scientific literature.

	Confidentiality	Integrity	Availability	Authenticity	Accountability	Non-Repudiation	Reliability
Requirements - MOPS, MASPS (RTCA), SARPS (ICAO)							
CPDLC	✘[139,185]	✘[139,185]	✘[139,185]	✘[139,185]	✘[139,185]	✘[139,185]	✘[139,185]
SSR	✘[160,161]	✘[160,161]	✘[160,161]	✘[160,161]	✘[160,161]	✘[160,161]	✘[160,161]
ADS-B	✘[52,154]	✘[52,154]	✘[52,154]	✘[52,154]	✘[52,154]	✘[52,154]	✘[52,154]
TCAS	✘[163,192]	✘[163,192]	✘[163,192]	✘[163,192]	✘[163,192]	✘[163,192]	✘[163,192]
FIS-B	✘[167,172]	✘[167,172]	✘[167,172]	✘[167,172]	✘[167,172]	✘[167,172]	✘[167,172]
TIS-B	✘[173,186]	✘[173,186]	✘[173,186]	✘[173,186]	✘[173,186]	✘[173,186]	✘[173,186]
Specification - Manual (ICAO, RTCA)							
CPDLC	✘[106,187]	✘[106,187]	✘[106,187]	✘[106,187]	✘[106,187]	✘[106,187]	✘[106,187]
SSR	✘[68,188]	✘[68,188]	✘[68,188]	✘[68,188]	✘[68,188]	✘[68,188]	✘[68,188]
ADS-B	✘[53]	✘[53]	✘[53]	✘[53]	✘[53]	✘[53]	✘[53]
TCAS	✘[189,190]	✘[189,190]	✘[189,190]	✘[189,190]	✘[189,190]	✘[189,190]	✘[189,190]
FIS-B	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]
TIS-B	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]	✘[67]
Literature - Academic							
CPDLC	✔[22,23]	✔[22,23]	✔[22,23]	✔[22,23]	✔[22,23]	✔[22,23]	✔[22,23]
SSR	✘[193]	✘[193]	✘[193]	✘[193]	✘[193]	✘[193]	✘[193]
ADS-B	✔[7,45,49]	✔[45,49]	✔[45,49]	✔[45,49]	✔[45,49]	✔[45,49]	✔[45,49]
TCAS	✘[14,17]	✘[14,17]	✘[14,17]	✘[14,17]	✘[14,17]	✘[14,17]	✘[14,17]
FIS-B	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]
TIS-B	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]	✔[50]

Why do many of the everyday services (e.g., CPDLC, ADS-B or voice communications) offer such an obvious attack vector?

A main reason is the high cost to replace or update widely deployed legacy systems, such as analogue VHF, ACARS, CPDLC via ACARS via VDLm2 that make use of years-old radio hardware of an aircraft. For example, AMS exists since 2007, but ANSPs charge extra for that service [127] which makes it not very widely adopted. Also, the first specification of ATN/OSI in 1998 did not include security requirements, which were only incorporated in later drafts of ICAO Doc. 9705 and 9880 [131,132]. To this day, the only deployed technology being able to validate the security requirements of ICAO Doc. 9880 in the form of the Secure Dialogue Service is AMS. Only with the transition from ATN/OSI to ATN/IPS, security becomes a mandatory requirement for the very first time in the corresponding ICAO Doc. 9896 standard [132].

Why do security and therefore safety-relevant changes in standards and specifications in the aeronautical industry require decades?

Interestingly enough, ICAO specifies in one of its most important documents regarding aeronautical datalinks, the "Global Operational Data Link (GOLD) Manual", that "[t]he ANSP should develop appropriate procedures or other means to [...] ensure that data are correct and accurate, including any changes, and that security of such data is not compromised[.]" [106]. One possible interpretation is, that the legal responsibility regarding security of information lies with the ANSPs. However, ANSPs only cover parts of the aeronautical informational communications chain, and it takes all stakeholders (e.g., regulators, ANSPs, airlines, and radio manufacturers) to develop and maintain a sound cybersecurity strategy in civil aviation.

Why is it not sufficient to implement existing standardized security measures for the network or transport layer (e.g., IPsec or TLS)?

No matter the application or data link, security measures like IPsec or TLS allow the data to be delivered between two endpoints in a secure manner. Consequentially, the worldwide adoption of ATN/IPS and incorporation of the secure Future Communications Infrastructure (FCI) data links is one of the most vital steps for long-term aeronautical digital communications security. On the downside, this does not make the entire system "secure". First of all, not all data links used today and, in the future, have security measures foreseen or implemented. Even with network or transport layer security being implemented, an aircraft always has to contact the ground-based radio and hence the first connection happens on physical and then on link layer. That means, that the initial contact between air- and ground infrastructure is not secured at all. Consider VDLm2: An attacker can still launch a very easy Man-in-the-Middle (MitM) attack with consequences such as Denial-of-Service (DoS), message injection, eavesdropping and more, even if IPsec and/or TLS were implemented. By simply forcing the aircraft to connect to a rogue ground-station and, once a connection has been established, intercept and block or redirect all traffic between that aircraft and a valid ground-station, sensitive data that is send only on the link layer (e.g., control data of the data link) are accessible for the attacker.

What makes implementing physical layer security measures so difficult?

All civil aeronautical data links are built in a reliable way, tolerating very high Bit Error Rate (BER), however, they are not hardened against dedicated jamming or spoofing attacks [197]. Thus, in addition to adopting the ATN/IPS and recent FCI data link candidates, legacy link layer technology, such as VDLm2 must also receive security updates and for the future, all those and future data links, especially for UAS communications must be hardened against dedicated physical layer attacks.

Why is there such a obvious gap between standards and research?

Having a closer look at Tables 5–7, it can clearly be observed that there is a huge difference between requirements, actual specifications and work in the scientific community. Especially older systems (i.e., specified before the 2000s) do not specify any security by modern standards. Basically, everyone with appropriate equipment and the knowledge of the correct frequency and aeronautical phraseology can participate in aeronautical communications [28,57]. However, also more recent communication datalinks, such as AeroMACS, LDACS or the newer SatCOM links (c.f., Table 5), and networks like ATN/OSI or ATN/IPS (c.f., 6) do specify security properties. Still, application security experienced a lot of research, which did not make it in any specification or manual documents (c.f., Table 7).

For almost every system so far, the scientific community has provided security solutions or ideas. This knowledge was, however, not collected in requirements documents or specifications of aeronautical communications systems. One possible explanation is, that retrofitting legacy technologies is simply too expensive. This points to a large

demand for the early exchange of security and aviation experts in the regulatory institutions (e.g., ICAO, EASA, RTCA, EUROCONTROL or FAA). If that knowledge transfer happens, security requirements and procedures can find their way into aeronautical standards early on. Security experts often state the need for "security by design", and ADS-B is a good example for the validity of this statement. ADS-B provides aeronautical services over *UAT*, *1090ES*, and *LDACS*. The insecurity of ADS-B was already demonstrated in 2003, discussed in 2006 at the 25th DASC [5], and attacks were made available to a broader public at DEFCON 17 [198] in 2011 and at Black Hat USA conference 2012 [6]. As stated above, the overall insecurity of ADS-B is the result of an *unsecure application, delivered via unprotected aeronautical networks and unsecure data link technology*. However, despite much work on the subject in the scientific community, ADS-B requirements still do not contain any demand for cybersecurity solutions, and rolled-out worldwide in 2020 with most systems unprotected from malicious adversaries. And, as stated before, no changes to this are likely to happen, as it is mostly economically infeasible to secure a system once it was rolled out. In addition, such an extensive retro-fitting would contradict the ICAO ethos written in large letters on the ICAO headquarter in Montreal: "No country left behind". This brings us back to our recommendation: security and aviation experts need to talk to each other as early as possible, so that security can find its way in standards and specifications early on, as progressively done in the ATN/IPS ICAO standard [132].

Why is security required but sometimes not part of the system's specification, as in Inmarsat SB, Iridium Certus or AMS (c.f. Table 6)?

Sometimes, security is actually specified but optional, and even if it is specified, it does not mean the link is actually secure. Both satellite communication systems – Inmarsat SB and Iridium Certus – define a so-called "security gateway" [107], which includes appropriate techniques to meet all security properties, but specifies it as optional. Although, for safety relevant applications, the Inmarsat SB standard makes invoking the security gateway mandatory [107].

As another example, AMS offers information security measures to ensure all mentioned security properties in Section 3, but it is not mandatory to send ACARS messages in the AMS format. As AMS is only used for ACARS messages at a surcharge, this results in an almost non-existent deployment of AMS [127]. Inmarsat SB has adopted parts of the 3rd Generation Public–Private Partnership (3GPP) 3G security architecture [107], which itself has its flaws [199]. Also, AMS was analyzed and problems in the authentication and key agreement part identified [200]. The main takeaway here is, that once security is specified for a certain system, *it shall not be made optional*, *it must be constantly scrutinized for vulnerabilities* and once some have been identified, *these must be fixed*.

5.2. Increased attack surface

While many combinations of aeronautical data links, network technologies or services (c.f., Tables 5–7) miss to define, specify or implement security solutions, a major issue for the security of aeronautical communications system is on the horizon [7,57]. With the use of cheap Commercial Off-The-Shelf (COTS) and SDR, even layman adversaries may attack aeronautical communication services as there are open source libraries for decoding VDLm2, ADS-B, Mode S or 1090ES packets such as VDLM2DEC [196] or dump1090 [195]. Tutorials such as provided by the Aerospace Village at DEFCON 28[3] make the entire topic more accessible to a broader audience and projects such as GNU-Radio [201] would allow for building sending blocks for aeronautical communications and thus possibly injecting messages. As pointed out in Section 2, many publications by the scientific community [6,12–17,22–25,27,32] demonstrated the lack of security, weaknesses and vulnerabilities of a multitude of aeronautical communications technology on application, network and data-link layer. The aviation industry must recognize this changed threat landscape and start adapting to these rising challenges fast. This recognition is happening now, as of 2021, in the area CNS infrastructure for UAS addressing semi- or fully-automated flying. The requirement catalogue for the C2 [202,203] datalink already includes sound cybersecurity measures from the physical layer up. One possible interpretation of this is that the community is recognizing the fact that ensuring safety of UAS, without the human-in-the-loop as security control instance, now requires sound cybersecurity measures.

With this, we want to further emphasize to speed up the process of using combinations of data links, networks and services, that implement security measures at least on some level, as the accessibility to potential attack hardware and knowledge how to use it, is spreading fast. Thus, the aeronautical community must act faster.

5.3. Recommendations

With ICAO Doc. 9880 and 9896 [131,132], RTCA DO-377, DO-379 [133,203] or ARINC P823, P858 [128,134], all aforementioned regulators have recognized the problem and started working on formal specification for cybersecurity for selected areas in aeronautical communications. In 2016 by Resolution A39-19 (Addressing Cybersecurity in Civil Aviation), ICAO founded the ICAO Secretariat Study Group on Cybersecurity (SSGC) with its focus on countering cyber threats to civil aviation [204]. Assembly Resolution A40-10 (Addressing Cybersecurity in Civil Aviation) [204] superseded previous resolutions [204] and specifically calls upon states to implement a cybersecurity strategy for civil aviation. Finally, in October 2019, ICAO released a high-level cybersecurity strategy [205]. Also, ARINC standard P858 [134], specifying security defined in ICAO Doc. 9896, has been finalized in June 2021. All these developments show, that security has finally found its way into the working groups of these organizations.

While this is certainly great progress, insecure combinations of data link, network and application services, as well as legacy systems will remain in the aeronautical ecosystems for decades.

6. Summary of findings and recommendations

The preceded analysis is summarized in the following eight key findings and recommendations:

1. **Civil aviation suffers from a lack of security in most legacy systems.** They do not specify and do not implement security. Unfortunately, they are mostly used in such a combination, that there are no security measures on any communications layer.
2. Cases such as ADS-B reveal that **security in aviation has to be specified before the system is released**, since later changes are very unlikely to be economically feasible.
3. Security and aviation experts have to **work closer together and a broader knowledge transfer has to happen** in order to anchor cybersecurity in avionic standards.
4. The **current pace** in which **aviation is adapting to the changed threat landscape** of wireless communications [57] **is too slow**. Development, certification and deployment of aeronautical communications systems is too slow and too expensive at its current pace.
5. New communication systems like the proposed LDACS must include a **modular cybersecurity approach from the start of their development**, such that the system design reflects cybersecurity demands and later updates are feasible.
6. Even with upcoming secure aeronautical network systems, **link layer and physical layer robustness must be gradually integrated into the CNS landscape**.

[3] https://aerospacevillage.org/defcon-28/ July 07, 2022.

7. Section 3 shows different threats, if either **Security**, **Safety** or **Privacy** are violated, hence we only consider a system to be secure if all three aspects are covered. In practice, a *threat and risk analysis* may reveal some aspects to be more important for a system, hence an informed decision needs to be made. This is only possible if the standards itself provide **Security by Design** for all three aspects, which is a must for current and upcoming aeronautical data links, networks and services.
8. Lastly, **security is not a state, but a process**. Once a system requirements has been made clear, those must be scrutinized by security experts. Once it has been defined, the specification must be scrutinized. Once a prototype is tested, this has to be scrutinized. Once it is rolled-out, the system must still be scrutinized. And in every step, **security vulnerabilities must be fixed and those fixes integrated in the requirements, specifications, prototypes and systems-in-use.** If done properly in every step, it helps not only making systems a lot more secure, it is also way, way cheaper.

7. Conclusions

This work analyzes the importance of cybersecurity properties in aeronautical communications and services. Case studies and a close review on the impact of the absence of said properties on security, safety or privacy, reveal attacks that can be performed by powerful state-level attackers or even with cheap commodity hardware. Hence, cyber- and protocol security are the most important corner stone for the future development of ATM. A detailed description of each ATM service and corresponding data links is provided, as well as information about air traffic services and data links. A gap analysis shows that most aviation communication technologies lack cybersecurity protection mechanisms in their requirements or specification document.

On the one hand, systematic problems are discussed such as the urgent need for the integration of cybersecurity into aeronautical systems from the start of their development. On the other hand, we believe that the cybersecurity research community provides suitable security solutions for existing and future systems. We thereby identify a major gap and the necessity of knowledge exchange of security and aviation experts.

For the short-term future, the aviation industry must recognize the changed threat landscape where cheap wireless hardware allows a wide range of adversaries to pose a threat to aeronautical communications systems. Thus, erasing low hanging fruits, such as the lack of entity authentication, message authentication or confidentiality by incorporating these solutions on higher protocol layers can be a first step. In the mid-term, the security knowledge of the scientific community must be reflected in the requirements and specifications of aeronautical communications system. ICAO already started this process in 2017 by forming the Study Group on Cybersecurity (SSGC) and many other regulators, such as EASA, RTCA or ARINC, are now working on cybersecurity relevant regulations and recommendations.

One important step in improving cybersecurity in the aviation industry would be the reduction of costs. It is the key factor that prevents security updates to aeronautical systems, as even the smallest change of cryptographic algorithms requires new certification. At the end, this reduces safety in aviation and thereby counteracts the means of safety relevant certification

Meaningful protection of aviation, requires the landscape and mindset of the industry to shift. In the long term, data links with security rooted into their inner core must be the standard and not the exception. If done right, digitization of aeronautical services brings the opportunity to further enhance safety in aviation and may even reduce operational costs. For example, it enables better, smoother and faster aeronautical operations ensuring on protocol level, that a message has been fully and correctly transmitted and received without it being tampered. Cybersecurity thereby is simply the enabler for digitization and a safe and secure evolution of civil aviation.

Acronyms

1090ES	1090 MHz Extended Squitter
64-QAM	64-Quadrature Amplitude Modulation
A-BPSK	Aviation-BPSK
A-QPSK	Aviation-QPSK
A2A	Air-to-Air
A2G	Air-to-Ground
AAC	Airline Administrative Control
ACARS	Aircraft Communications Addressing and Reporting System
ACSE	Association Control Service Element
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance-Broadcast
ADS-C	Automatic Dependent Surveillance-Contract
AeroMACS	Aeronautical Mobile Airport Communications System
AFN	ATS Facilities Notification
AM(R)S	Aeronautical Mobile (Route) Service
AMS	ACARS Message Security
AMS(R)S	Aeronautical Mobile-Satellite (Route) Service
AMSS	Aeronautical Mobile Satellite Service
ANSP	Aeronautical Network Service Provider
AOA	ACARS over AVLC
AOC	Aeronautical Operational Control
APNT	Alternative Positioning Navigation and Timing
APT	Airport
ARINC	Aeronautical Radio, Incorporated
ASE	Air/Ground Application Service Element
ASN.1	Abstract Syntax Notation One
ATC	Air Traffic Communications
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Services
ATSMHS	ATS Message Handling Service
AVLC	Aviation VHF Link Control
BGP	Border Gateway Protocol
CLNP	ConnectionLess Network Protocol
CM	Context Management
CNS	Communication, Navigation and Surveillance
COTS	Commercial Off-The-Shelf
CPDLC	Controller–Pilot Data Link Communications
CPFSK	Continuous Phase Frequency Shift Keying
CSMA	Carrier Sense Multiple Access
CSP	Communications Service Provider
D8PSK	Differential 8 Phase Shift Keying
DS	Dialogue Service
DSB-AM	Double Side-Band Amplitude Modulation
DTLS	Datagram Transport Layer Security
EASA	European Union Aviation Safety Agency
ECDH	Elliptic Curve Diffie–Hellmann
ECDSA	Elliptic Curve Digital Signature Algorithm
ENR	En-Route
ESP	Encapsulated Security Payload
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCI	Future Communications Infrastructure
FIS	Flight Information System
FIS-B	Flight Information System-Broadcast
FL	Flight Level
G2A	Ground-to-Air

GANP	Global Air Navigation Plan
GBAS	Ground Based Augmentation System
GFSK	Gaussian Frequency Shift Keying
GNSS	Global Navigation Satellite System
HF	High Frequency
HMAC	Keyed-Hash Message Authentication Code
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange v2
ILS	Instrument Landing System
IP	Internet Protocol
IPS	Internet Protocol Suite
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KDF	Key Derivation Function
LDACS	L-band Digital Aeronautical Communications System
LEO	Low Earth Orbit
M-SNDCF	Mobile Sub-Network Dependent Convergence Function
MASPS	Minimum Aviation System Performance Specifications
MOPS	Minimum Operational Performance Standards
MSC	Mobile Satellite Communication
MSK	Medium Shift-Keying
NASA	National Aeronautics and Space Administration
NEXRAD	Next-Generation Radar
NOTAM	Notice To Airman
OOK	On-Off Keying
ORP	Oceanic Remote Polar
OSI	Open Systems Interconnection
PER	Packed Encoding Rules
PKI	Public Key Infrastructure
PSR	Primary Surveillance Rader
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RTCA	Radio Technical Commission for Aeronautics
RTF	Radiotelephony
RTT	Round Trip Time
S-ASO	Security-Application Service Object
S-TDMA	Self-organized TDMA
SAC	System Area Code
SARPS	Standards and Recommended Practices
SB	Swift Broadband
SBD	Short Burst Data
SDR	Software Defined Radio
SecDS	Secure Dialogue Service
SESAR	Single European Sky ATM Research
SESE	Security Exchange Service Element
SHA	Secure Hash Algorithm
SIC	System Identification Code
SIGMET	Significant Meteorological Information
SINR	Signal-to-Interference-plus-Noise-Ratio
SSO	Security Service Object
SSR	Secondary Surveillance Radar
TCAS	Traffic Alert and Collision Avoidance System
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TID	Target Identification
TIS-B	Traffic Information System-Broadcast
TLS	Transport Layer Security
TMA	Terminal Maneuvering Area
TOD	Time Of Day
TP4	Transport Protocol class 4
UAS	Unmanned Aeronautical System
UAT	Universal Access Transceiver
UDP	User Datagram Protocol
ULCS	Upper Layer Communications Service
US	United States
VCS	Voice Communication System
VDL	VHF Data Link
VDLm0	VHF Data Link mode A
VDLm2	VHF Data Link mode 2
VHF	Very High Frequency

Declaration of competing interest

No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to https://doi.org/10.1016/j.ijcip.2022.100549.

Acknowledgment

We thank Martin Strohmeier for his valuable input and years of dedicated work in improving cybersecurity in the aeronautical ecosystem.

References

[1] IATA, IATA Industry Statistics - Fact Sheet, Tech. Rep., International Air Transport Association (IATA), 2020.

[2] S.M. Iacus, F. Natale, C. Santamaria, S. Spyratos, V. Michele, Estimating and projecting air passenger traffic during the COVID-19 coronavirus outbreak and its socio-economic impact, Saf. Sci. 129 (2020) 1–11, http://dx.doi.org/10.1016/j.ssci.2020.104791.

[3] M. Slim, B. Mahmoud, A. Pirovano, N. Larrieu, Aeronautical communication transition from analog to digital data: A network security survey, Comp. Sci. Rev. 11 (2014) 1–29, http://dx.doi.org/10.1016/j.cosrev.2014.02.001.

[4] V.P. Galotti, The Future Air Navigation System (FANS): Communications, Navigation, Surveillance–Air Traffic Management (CNS/ATM), Vol. 1, Routledge, 2019, http://dx.doi.org/10.4324/9780429435614.

[5] E. Valovage, Enhanced ADS-B research, in: 2006 IEEE/AIAA 25th Digital Avionics Systems Conference, Portland, OR, USA, 2006, pp. 1–7, http://dx.doi.org/10.1109/DASC.2006.313672.

[6] A. Costin, A. Francillon, Ghost in the air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices, in: EURECOM (Ed.), BLACKHAT 2012, Las Vegas, NV, USA, 2012, pp. 1–10.

[7] M. Strohmeier, M. Schäfer, V. Lenders, I. Martinovic, Realities and challenges of nextgen air traffic management: the case of ADS-B, IEEE Commun. Mag. 52 (5) (2014) 111–118, http://dx.doi.org/10.1109/MCOM.2014.6815901.

[8] K.D. Wesson, T.E. Humphreys, B.L. Evans, Can cryptography secure next generation air traffic surveillance?, 2014, https://rnl.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf. (Accessed 13 April 2022).

[9] P. Berthier, J.M. Fernandez, J.-M. Robert, SAT: SEcurity in the air using TESLA, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference, DASC, IEEE, St. Petersburg, FL, USA, 2017, pp. 1–10, http://dx.doi.org/10.1109/DASC.2017.8102003.

[10] A. Roy, Secure aircraft communications addressing and reporting system (ACARS), in: 20th DASC. 20th Digital Avionics Systems Conference, Vol. 2, Cat. No. 01CH37219, IEEE, Daytona Beach, FL, USA, 2001, pp. 7A2/1–7A2/11 2, http://dx.doi.org/10.1109/DASC.2001.964182.

[11] C. Risley, J. McMath, B. Payne, Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages, in: 20th DASC. 20th Digital Avionics Systems Conference, Vol. 2, 2001, pp. 7D4/1–7D4/8 2, http://dx.doi.org/10.1109/DASC.2001.964200.

[12] M. Smith, D. Moser, M. Strohmeier, V. Lenders, I. Martinovic, Economy class crypto: exploring weak cipher usage in avionic communications via ACARS, in: International Conference on Financial Cryptography and Data Security, Springer, Sliema, Malta, 2017, pp. 285–301, http://dx.doi.org/10.1007/978-3-319-70972-7_15.

[13] M. Smith, D. Moser, M. Strohmeier, V. Lenders, I. Martinovic, Undermining privacy in the aircraft communications addressing and reporting system (ACARS), Proc. Priv. Enhanc. Technol. 2018 (3) (2018) 105–122, http://dx.doi.org/10.1515/popets-2018-0023.

[14] P.M. Berges, Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation, 2019, Virginia Tech.

[15] A. Lomas, TCAS and ILS Spoofing Demonstration, DEFCON 28 Aerospace Village, 2020, https://www.youtube.com/watch?v=VbCzABE6jec. (Accessed 13 April 2022).

[16] J.W. Hannah, A cyber threat taxonomy and a viability analysis for false injections in the TCAS, 2021, Air Force Institute of Technology.

[17] M. Smith, M. Strohmeier, V. Lenders, I. Martinovic, Understanding realistic attacks on airborne collision avoidance systems, J. Transp. Secur. (2022) 1–32, http://dx.doi.org/10.1007/s12198-021-00238-2.

[18] F. Cote, Initial Requirements Document for Controller Pilot Data Link Communications (CPDLC) Service, Tech. Rep., Federal Aviation Administration (FAA), 1998.

[19] ICAO, Doc 4444 - Procedures for Air Navigation Services (PANS) - Air Traffic Management, Tech. Rep., 17th ed., International Civil Aviation Organization (ICAO), 2021, Doc 4444.

[20] RTCA, DO-290, Safety and Performance Requirements Standard for Air Traffic Data Link Services in Continental Airspace (Continental SPR Standard), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2004, DO-290.

[21] RTCA, DO-290, Safety and Performance Requirements Standard for Air Traffic Data Link Services in Continental Airspace (Continental SPR Standard) - Change 3, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2019, DO-290, Change 3.

[22] D. Di Marco, A. Manzo, M. Ivaldi, J. Hird, Security testing with controller-pilot data link communications, in: 2016 11th International Conference on Availability, Reliability and Security, ARES, IEEE, Salzburg, Austria, 2016, pp. 526–531, http://dx.doi.org/10.1109/ARES.2016.104.

[23] A. Gurtov, T. Polishchuk, M. Wernberg, Controller–pilot data link communication security, Sensors 18 (5) (2018) 16–36, http://dx.doi.org/10.3390/s18051636.

[24] S. Eskilsson, H. Gustafsson, S. Khan, A. Gurtov, Demonstrating ADS-B and CPDLC attacks with software-defined radio, in: 2020 Integrated Communications Navigation and Surveillance Conference, ICNS, 2020, pp. 1B2–1–1B2–9, http://dx.doi.org/10.1109/ICNS50378.2020.9222945.

[25] A. Lehto, I. Sestorp, S. Khan, A. Gurtov, Controller pilot data link communication security: A practical study, in: 2021 Integrated Communications Navigation and Surveillance Conference, ICNS, 2021, pp. 1–11, http://dx.doi.org/10.1109/ICNS52807.2021.9441649.

[26] S. Khan, A. Gurtov, A. Breaken, P. Kumar, A security model for controller-pilot data communication link, in: 2021 Integrated Communications Navigation and Surveillance Conference, ICNS, 2021, pp. 1–10, http://dx.doi.org/10.1109/ICNS52807.2021.9441637.

[27] J. Smailes, D. Moser, M. Smith, M. Strohmeier, V. Lenders, I. Martinovic, 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, Association for Computing Machinery, New York, NY, USA, 2021, pp. 53—64, http://dx.doi.org/10.1145/3457339.3457985.

[28] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic, On perception and reality in wireless air traffic communication security, IEEE Trans. Intell. Transp. Syst. 18 (6) (2016) 1338–1357, http://dx.doi.org/10.1109/TITS.2016.2612584.

[29] M. Strohmeier, I. Martinovic, V. Lenders, Securing the air–ground link in aviation, in: The Security of Critical Infrastructures: Risk, Resilience and Defense, Springer International Publishing, 2020, pp. 131–154, http://dx.doi.org/10.1007/978-3-030-41826-7_9.

[30] A.A. Elmarady, K. Rahouma, Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment, IEEE Access 9 (2021) 143997–144016, http://dx.doi.org/10.1109/ACCESS.2021.3121230.

[31] G. Dave, G. Choudhary, V. Sihag, I. You, K.-K. Raymond Choo, Cyber security challenges in aviation communication, navigation, and surveillance, Comput. Secur. 112 (2022) 102516, http://dx.doi.org/10.1016/j.cose.2021.102516.

[32] E. Ukwandu, M.A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovic, X. Bellekens, Cyber-security challenges in aviation industry: A review of current and future trends, Information 13 (3) (2022) http://dx.doi.org/10.3390/info13030146.

[33] R.W. Shirey, Internet security glossary, version 2, in: Request for Comments, (4949) RFC Editor, 2007, http://dx.doi.org/10.17487/RFC4949, URL https://www.rfc-editor.org/info/rfc4949.

[34] ISO/IEC, Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary, Vol. 4, (27000:2016) International Standardization Organization (ISO)/International Electrotechnical Commission (IEC), 2016, ISO/IEC 27000:2016(E).

[35] IEC, Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models, 2017, IEC/TS 62443-1-1.

[36] ISO/IEC, Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model, Tech. Rep., International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).

[37] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, M. Wilhelm, Bringing up OpenSky: A large-scale ADS-B sensor network for research, in: IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks, IEEE, Berlin, Germany, 2014, pp. 83–94, http://dx.doi.org/10.1109/IPSN.2014.6846743.

[38] M. Strohmeier, Dissecting wireless privacy in aviation, 2020, DEFCON 28 Aerospace Village, https://www.youtube.com/watch?v=rSDQDhB7Qtg. (Accessed 13 April 2022).

[39] N. Vigdor, A Teenager Tracked Elon Musk's Jet on Twitter. Then Came the Direct Message, New York Times, 2022, https://www-nytimes-com.translate.goog/2022/02/03/technology/elon-musk-jet-tracking.html. (Accessed 18 April 2022).

[40] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126, http://dx.doi.org/10.1145/357980.358017.

[41] E. Rescorla, The transport layer security (TLS) protocol version 1.3, in: Request for Comments, (8446) RFC Editor, 2018, http://dx.doi.org/10.17487/RFC8446, URL https://www.rfc-editor.org/info/rfc8446.

[42] S. Frankel, S. Krishnan, IP Security (IPsec) and internet key exchange (IKE) document roadmap, in: Request for Comments, (6071) RFC Editor, 2011, http://dx.doi.org/10.17487/RFC6071, URL https://www.rfc-editor.org/info/rfc6071.

[43] J. Daemen, V. Rijmen, The Design of Rijndael, Vol. 2, Springer, 2002, http://dx.doi.org/10.1007/978-3-662-60769-5.

[44] M. Schäfer, V. Lenders, I. Martinovic, Experimental analysis of attacks on next generation air traffic communication, in: International Conference on Applied Cryptography and Network Security, ACNS, Springer, Banff, AB, Canada, 2013, pp. 253–271, http://dx.doi.org/10.1007/978-3-642-38980-1_16.

[45] D. McCallie, J. Butts, R. Mills, Security analysis of the ADS-B implementation in the next generation air transportation system, Int. J. Crit. Infrastruct. Prot. 4 (2) (2011) 78–87, http://dx.doi.org/10.1016/j.ijcip.2011.06.001.

[46] W.-J. Pan, Z.-L. Feng, Y. Wang, ADS-B Data authentication based on ECC and X. 509 certificate, J. Electr. Sci. Technol. 10 (1) (2012) 51–55, http://dx.doi.org/10.3969/j.issn.1674-862X.2012.01.009.

[47] M. Strohmeier, V. Lenders, I. Martinovic, On the security of the automatic dependent surveillance-broadcast protocol, IEEE Commun. Surv. Tutor. 17 (2) (2014) 1066–1087, http://dx.doi.org/10.1109/COMST.2014.2365951.

[48] T. Kacem, D. Wijesekera, P. Costa, Integrity and authenticity of ADS-B broadcasts, in: 2015 IEEE Aerospace Conference, IEEE, Big Sky, MT, USA, 2015, pp. 1–8, http://dx.doi.org/10.1109/AERO.2015.7119293.

[49] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, X. Zhang, A practical and compatible cryptographic solution to ADS-B security, IEEE Internet Things J. 6 (2) (2019) 3322–3334, http://dx.doi.org/10.1109/JIOT.2018.2882633.

[50] S. Sciancalepore, R. Di Pietro, SOS: STandard-compliant and packet loss tolerant security framework for ADS-B communications, IEEE Trans. Dependable Secure Comput. (2019) http://dx.doi.org/10.1109/TDSC.2019.2934446.

[51] Z. Wu, T. Shang, A. Guo, Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey, IEEE Access 8 (2020) 122147–122167, http://dx.doi.org/10.1109/ACCESS.2020.3007182.

[52] RTCA, DO-338, Minimum Aviation System Performance Standards (MASPS) for ADS-B Traffic Surveillance Systems and Applications (ATSSA), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2012, DO-338.

[53] ICAO, Doc 9994 — Manual on Airborne Surveillance Applications, Tech. Rep., 1st ed., International Civil Aviation Organization (ICAO), 2014, Doc 9994.

[54] EUROCONTROL, Accident and Serious Incident Reports: AGC, Tech. Rep., 1st ed., EUROCONTROL, 2022.

[55] Y.-S. Shiu, S.Y. Chang, H.-C. Wu, S.C.-H. Huang, H.-H. Chen, Physical layer security in wireless networks: A tutorial, IEEE Wirel. Commun. 18 (2) (2011) 66–74, http://dx.doi.org/10.1109/MWC.2011.5751298.

[56] B. Möller, T. Duong, K. Kotowicz, This POODLE bites: exploiting the SSL 3.0 fallback, Secur. Advis. 21 (2014) 34–58.

[57] M. Strohmeier, Security in Next Generation Air Traffic Communication Networks (Ph.D. thesis), University of Oxford, 2016, http://dx.doi.org/10.13140/RG.2.2.21924.48006.

[58] EUROCONTROL, VHF SECURITY STUDY - FINAL REPORT, Tech. Rep., EUROCONTROL, 2002.

[59] EUROCONTROL, Impact of Transponder Failure on Safety Barriers, Tech. Rep., first ed., EUROCONTROL, 2022.

[60] D. Brudnicki, K. Chastain, B. Ethier, Application of Advanced Technologies for Training the Next Generation of Air Traffic Controllers, Tech. Rep., MITRE Corporation, 2007.

[61] ICAO, Annex 10 - Aeronautical Telecommunications - Volume II - Communication Procedures including those with PANS status, Tech. Rep., International Civil Aviation Organization (ICAO), 2016, seventh ed..

[62] NASA, ASRS Database Report Set Pilot / Controller Communications, Tech. Rep., National Aeronautics and Space Administration (NASA), 2018.

[63] E.B. Ala'Darabseh, B. Tedongmo, Detecting GPS jamming incidents in OpenSky data, in: Proceedings of the 7th OpenSky Workshop, Vol. 67, Zurich, Switzerland, 2019, pp. 97–108, http://dx.doi.org/10.29007/1mmw.

[64] J. Baek, Y.-j. Byon, E. Hableel, M. Al-Qutayri, Making air traffic surveillance more reliable: a new authentication framework for automatic dependent surveillance-broadcast (ADS-B) based on online/offline identity-based signature, Secur. Commun. Netw. 8 (5) (2015) 740–750, http://dx.doi.org/10.1002/sec.1021.

[65] ICAO, Doc 9776 - Manual on VHF Digital Link (VDL) Mode 2, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2015, Doc 9776.

[66] ICAO, Doc 9816 - Manual on VHF Digital Link (VDL) Mode 4, Tech. Rep., first ed., International Civil Aviation Organization (ICAO), 2004, Doc 9816.

[67] ICAO, Doc 9861 — Manual on the Universal Access Transceiver (UAT), Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2012, Doc 9861.

[68] ICAO, Doc 9871 — Technical Provisions for Mode S Services and Extended Squitter, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2012, Doc 9871.

[69] ICAO, Doc 10044 - Manual on the Aeronautical Mobile Airport Communications System (AeroMACS), Tech. Rep., first ed., International Civil Aviation Organization (ICAO), 2019, Doc 10044.

[70] ICAO, LDACS White paper–a roll-out scenario, in: COMMUNICATIONS PANEL –DATA COMMUNICATIONS INFRASTRUCTURE WORKING GROUP - THIRD MEETING, International Civil Aviation Organization (ICAO), 2019.

[71] RTCA, DO-281C, Minimum Operational Performance Standards (MOPS) for Aircraft VDL Mode 2 Physical Link and Network Layer, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2018, DO-281C https://www.rtca.org/products/do-281c-electronic/. (Accessed 13 April 2022).

[72] RTCA, DO-282B with Corrigendum 1, Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance - Broadcast, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2011, DO-282B.

[73] RTCA, DO-282B, Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2011, DO-282B.

[74] RTCA, DO-260B, Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2011, DO-260B.

[75] RTCA, DO-346, Minimum Operational Performance Standards (MOPS) for the Aeronautical Mobile Airport Communication System (AeroMACS, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2014, DO-346.

[76] ICAO, Annex 11 - Air Traffic Services, Tech. Rep., 15th ed., International Civil Aviation Organization (ICAO), 2018.

[77] J.N. Bradbury, ICAO And future air navigation systems, in: Automation and Systems Issues in Air Traffic Control, Springer, 1991, pp. 79–99, http://dx.doi.org/10.1007/978-3-642-76556-8_8.

[78] ICAO, Annex 10 - Aeronautical Telecommunications - Volume III - Communication Systems, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2007.

[79] G.G.E. Leonardo, O.T.J. Eduardo, VHF Data link communications to provide air traffic services in Colombia, in: 2012 IEEE/AIAA 31st Digital Avionics Systems Conference, DASC, IEEE, Williamsburg, VA, USA, 2012, pp. 5E2–1–5E2–10, http://dx.doi.org/10.1109/DASC.2012.6382375.

[80] J. Kitaori, A performance comparison between VDL mode 2 and VHF ACARS by protocol simulator, in: 2009 IEEE/AIAA 28th Digital Avionics Systems Conference, IEEE, Orlando, FL, USA, 2009, pp. 4.B.3–1–4.B.3–8, http://dx.doi.org/10.1109/DASC.2009.5347498.

[81] ICAO, Doc 9805 — Manual on VHF Digital Link (VDL) Mode 3, Tech. Rep., first ed., International Civil Aviation Organization (ICAO), 2002, Doc 9805.

[82] Y.H. Chen, S. Lo, S.-S. Jan, G.J. Liou, D.M. Akos, P. Enge, Design and test of algorithms and real-time receiver to use universal access transceiver (UAT) for alternative positioning navigation and timing (APNT), in: 27th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2014, Institute of Navigation, Tampa, Florida, USA, 2014, pp. 1738–1746.

[83] S. Lo, Y.-H. Chen, P. Enge, Flight test of universal access transceiver (UAT) transmissions to provide alternative positioning navigation and timing (APNT), in: Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2015, Institute of Navigation, Tampa, Florida, USA, 2015, pp. 1468–1477.

[84] EASA, Approval Requirements for Air-Ground Data Link and ADS-B in Support of Interoperability Requirements, Tech. Rep., European Aviation Safety Agency (EASA), 2013, CRDTO NPA2012-19—RMT.0559(20.016).

[85] B. Kamali, AeroMACS: An IEEE 802.16 Standard-Based Technology for the Next Generation of Air Transportation Systems, Vol. 1, John Wiley & Sons, 2018, http://dx.doi.org/10.1002/9781119281139.

[86] ICAO, AeroMACS Safety and Security Analysis, Tech. Rep., International Civil Aviation Organization (ICAO), 2014, SESAR project P15.02.07 Deliverable 08.

[87] B. Crowe, Proposed AeroMACS PKI specification is a model for global and national aeronautical PKI deployments, in: WiMAX Forum At 16th Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2016, pp. 1–19, http://dx.doi.org/10.1109/ICNSURV.2016.7486405.

[88] ICAO, DOC 9750 - Global Air Navigation Plan, Tech. Rep., sixth ed., International Civil Aviation Organization (ICAO), 2019, DOC 9750.

[89] M.A. Bellido-Manganell, T. Gräupl, O. Heirich, N. Mäurer, A. Filip-Dhaubhadel, D.M. Mielke, L.M. Schalk, D. Becker, N. Schneckenburger, M. Schnell, LDACS Flight trials: Demonstration and performance analysis of the future aeronautical communications system, IEEE Trans. Aerosp. Electron. Syst. (2021) 1–19, http://dx.doi.org/10.1109/TAES.2021.3111722.

[90] ICAO, Finalization of LDACS Draft SARPs - Working Paper WP05 Including Appendix, Tech. Rep., International Civil Aviation Organization (ICAO), 2018.

[91] N. Mäurer, T. Gräupl, C. Schmitt, L-band Digital Aeronautical Communications System (LDACS), Tech. Rep., Internet Engineering Task Force, 2022, draft-ietf-raw-ldacs-10. Work in Progress, URL https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-10.

[92] N. Mäurer, T. Gräupl, M.A. Bellido-Manganell, D.M. Mielke, A. Filip-Dhaubhadel, O. Heirich, D. Gerbeth, M. Felux, L.M. Schalk, D. Becker, N. Schneckenburger, M. Schnell, Flight trial demonstration of secure GBAS via the L-band digital aeronautical communications system (LDACS), IEEE Aerosp. Electr. Syst. Mag. 36 (4) (2021) 8–17, http://dx.doi.org/10.1109/MAES.2021.3052318.

[93] T. Gräupl, N. Mäurer, Performance-optimizing secure GBAS over LDACS, in: 21th Integrated Communications, Navigation and Surveillance Conference, IEEE, 2021, pp. 1–9, http://dx.doi.org/10.1109/ICNS52807.2021.9441559.

[94] N. Mäurer, M. Caamano, D. Gerbeth, T. Gräupl, C. Schmitt, A secure broadcast service for LDACS with an application to secure GBAS, in: 2021 IEEE/AIAA 40th Digital Avionics Systems Conference, DASC, IEEE, 2021, pp. 1–10, http://dx.doi.org/10.1109/DASC52595.2021.9594504.

[95] T. Gräupl, C. Rihacek, B. Haindl, LDACS A/G Specification, Tech. Rep., German Aerospace Center (DLR), 2020.

[96] A. Bilzhause, B. Belgacem, M. Mostafa, T. Gräupl, Datalink security in the L-band digital aeronautical communications system (LDACS) for air traffic management, Aerosp. Electr. Syst. Mag. 32 (11) (2017) 22–33, http://dx.doi.org/10.1109/MAES.2017.160282.

[97] N. Mäurer, A. Bilzhause, Paving the way for an IT security architecture for LDACS: A datalink security threat and risk analysis, in: 18th Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2018, pp. 1A2/1–1A2–11, http://dx.doi.org/10.1109/ICNSURV.2018.8384828.

[98] N. Mäurer, A. Bilzhause, A cybersecurity architecture for the L-band digital aeronautical communications system (LDACS), in: 37th Digital Avionics Systems Conference, DASC, IEEE, London, UK, 2018, pp. 1–10, http://dx.doi.org/10.1109/DASC.2018.8569878.

[99] N. Mäurer, C. Schmitt, Towards successful realization of the LDACS cybersecurity architecture: an updated datalink security threat- and risk analysis, in: 19th Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2019, pp. 1–13, http://dx.doi.org/10.1109/ICNSURV.2019.8735139.

[100] N. Mäurer, T. Gräupl, C. Schmitt, Evaluation of the LDACS cybersecurity implementation, in: 38th Digital Avionics Systems Conference, DASC, IEEE, San Diego, CA, USA, 2019, pp. 1–10, http://dx.doi.org/10.1109/DASC43569.2019.9081786.

[101] N. Mäurer, T. Gräupl, C. Schmitt, Comparing different diffie-hellman key exchange flavors for LDACS, in: 39th Digital Avionics Systems Conference, DASC, IEEE, Online, 2020, pp. 1–10, http://dx.doi.org/10.1109/DASC50938.2020.9256746.

[102] N. Mäurer, T. Gräupl, C. Schmitt, Cybersecurity for the L-band digital aeronautical communications system (LDACS), in: H. Song, K. Hopkinson, T.d. Cola, T. Alexandrovich, L. D. (Eds.), Aviation Cybersecurity: Foundations, Principles, and Applications, IET, London, UK, 2021, pp. 1–38.

[103] N. Mäurer, C. Gentsch, T. Gräupl, C. Schmitt, Formal security verification of the station-to-station based cell-attachment procedure of LDACS, in: 18th International Conference on Security and Cryptography, SECRYPT, SCITEPRESS, 2021, pp. 603–610, http://dx.doi.org/10.5220/0010580906030610.

[104] N. Mäurer, T. Gräupl, C. Gentsch, T. Guggemos, M. Tiepelt, C. Schmitt, G.D. Rodosek, A secure cell-attachment procedure of LDACS, in: 2021 IEEE European Symposium on Security and Privacy Workshops, EuroS PW, 2021, pp. 113–122, http://dx.doi.org/10.1109/EuroSPW54576.2021.00019.

[105] ICAO - AERONAUTICAL COMMUNICATIONS PANEL (ACP), DRAFT AMS(R)S SARPs, Tech. Rep., Working Paper, International Civil Aviation Organization (ICAO), 2005.

[106] ICAO, Doc 10037 - Global Operational Data Link Document (GOLD), Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2017, Doc 10037.

[107] RTCA, DO-262D, Minimum Operational Performance Standards for Avionics Supporting Next Generation Satellite Systems (NGSS), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2019, DO-262D.

[108] RTCA, DO-343C, Minimum Aviation System Performance Standard for AMS(R)S Data and Voice Communications Supporting Required Communications Performance (RCP) and Required Surveillance Performance (RSP), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2020, DO-343C.

[109] ICAO, Doc 9925 — Manual on the Aeronautical Mobile Satellite (Route) Service, Tech. Rep., first ed., International Civil Aviation Organization (ICAO), 2010, Doc 9925.

[110] D. Fernández, M. Admella, L. Albiol, J.M. Cebrián, Satellite communications data link solution for long term air traffic management, in: SESAR Innovation Days, Madrid, Spain, 2014, pp. 1–8.

[111] S.D. Ilčev, Airborne satellite CNS systems and networks, in: Global Aeronautical Distress and Safety Systems, GADSS, Springer, 2019, pp. 437–582, http://dx.doi.org/10.1007/978-3-030-30632-8_5.

[112] N. Ricard, The Satellite Communications System for Safe and Secure Air Traffic Management Data Links and Voice, Tech. Rep., European Space Agency (ESA), 2020.

[113] P.W. Lemme, S.M. Glenister, A.W. Miller, Iridium (R) aeronautical satellite communications, IEEE Aerosp. Electr. Syst. Mag. 14 (11) (1999) 11–16, http://dx.doi.org/10.1109/62.809197.

[114] M. Zolanvari, R. Jain, T. Salman, Potential data link candidates for civilian unmanned aircraft systems: a survey, IEEE Commun. Surv. Tutor. 22 (1) (2019) 292–319, http://dx.doi.org/10.1109/COMST.2019.2960366.

[115] R. Zaruba, Air/ground data communication radios for future ATM, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference, DASC, IEEE, Prague, Czech Republic, 2015, pp. 2F4–1–2F4–10, http://dx.doi.org/10.1109/DASC.2015.7311383.

[116] S.L. Barbera, A. Miglietta, S. Sureda-Perez, K. Mineck, N. Fistas, R. Zaruba, S. Tamalet, L. Albiol, Future satellite communications data link in SESAR 2020 and ESA Iris programme, in: 2019 Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2019, pp. 1–11, http://dx.doi.org/10.1109/ICNSURV.2019.8735277.

[117] B. Phillips, A. Roy, D. Byrne, M. Schnell, D. Bharj, L. Sienkiewicz, D. Nellis, ICNS 2019 Panel discussion, in: 2019 Integrated Communications, Navigation and Surveillance Conference, ICNS, Herndon, VA, USA, 2019, pp. i–xiv, http://dx.doi.org/10.1109/ICNSURV.2019.8735367.

[118] J.C. McDowell, The low earth orbit satellite population and impacts of the spacex starlink constellation, Astrophys. J. Lett. 892 (2) (2020) 1–36, http://dx.doi.org/10.3847/2041-8213/ab8016.

[119] O.B. Osoro, E.J. Oughton, A techno-economic framework for satellite networks applied to low earth orbit constellations: Assessing starlink, OneWeb and Kuiper, IEEE Access 9 (2021) 141611–141625, http://dx.doi.org/10.1109/ACCESS.2021.3119634.

[120] P. Zong, S. Kohani, Design of LEO constellations with inter-satellite connects based on the performance evaluation of the three constellations SpaceX, OneWeb and Telesat, Korean J. Remote Sens. 37 (1) (2021) 23–40, http://dx.doi.org/10.7780/kjrs.2021.37.1.3.

[121] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao, J. Shi, Broadband LEO satellite communications: Architectures and key technologies, IEEE Wirel. Commun. 26 (2) (2019) 55–61, http://dx.doi.org/10.1109/MWC.2019.1800299.

[122] A. Baltaci, E. Dinc, M. Ozger, A. Alabbasi, C. Cavdar, D. Schupke, A survey of wireless networks for future aerial communications (FACOM), IEEE Commun. Surv. Tutor. (2021) http://dx.doi.org/10.1109/COMST.2021.3103044.

[123] J. Sekera, A. Novák, The future of data communication in aviation 4.0 environment, INCAS Bull. 13 (3) (2021) 165–178, http://dx.doi.org/10.13111/2066-8201.2021.13.3.1.

[124] Y. Albagory, Modelling, investigation, and feasibility of stratospheric broadband mm-wave 5G and beyond networks for aviation, Electronics 9 (11) (2020) 1872, http://dx.doi.org/10.1109/MWC.2019.1800299.

[125] ARINC, Aircraft Communications Addressing and Reporting System, Tech. Rep., 1998 ed., Aeronautical Radio, Incorporated (ARINC), 1998, ARINC Report 597.

[126] ARINC, Air/Ground Character-Oriented Protocol Specification, ARINC Report 618-7, Aeronautical Radio, Incorporated (ARINC), 2016.

[127] M. Smith, M. Strohmeier, V. Lenders, I. Martinovic, On the security and privacy of ACARS, in: 2016 Integrated Communications Navigation and Surveillance, ICNS, IEEE, Herndon, VA, USA, 2016, pp. 1–27, http://dx.doi.org/10.1109/ICNSURV.2016.7486395.

[128] ARINC, Datalink Security Part 1 – ACARS Message Security, ARINC Report 823P1, Aeronautical Radio, Incorporated (ARINC), 2007, https://standards.globalspec.com/std/1039315/ARINC823P1. (Accessed 13 April 2022).

[129] ARINC, Datalink Security Part 2 – Key Management, ARINC Report 823P2, Aeronautical Radio, Incorporated (ARINC), 2008.

[130] ICAO, Doc 9705 - Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN), Tech. Rep., third ed., International Civil Aviation Organization (ICAO), 2002, Doc 9705.

[131] ICAO, Doc 9880 — Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part I-IV, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2016, Doc 9880.

[132] ICAO, Doc 9896 — Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, Tech. Rep., International Civil Aviation Organization (ICAO), 2015, https://standards.globalspec.com/std/10026940/icao-9896. (Accessed 13 April 2022).

[133] RTCA, DO-379, Internet Protocol Suite Profiles, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2019, DO-379.

[134] Aeronautical Radio, Incorporated (ARINC), Internet Protocol Suite (IPS) for Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements, Tech. Rep., ARINC, 2021.

[135] H. Feng, J.A. Salowey, T. Petch, R. Gerhards, Datagram transport layer security (DTLS) transport mapping for syslog, in: Request for Comments, (6012) RFC Editor, 2010, http://dx.doi.org/10.17487/RFC6012, URL https://www.rfc-editor.org/info/rfc6012.

[136] Y. Rekhter, S. Hares, T. Li, A border gateway protocol 4 (BGP-4), in: Request for Comments, (4271) RFC Editor, 2006, http://dx.doi.org/10.17487/RFC4271, URL https://www.rfc-editor.org/info/rfc4271.

[137] RTCA, DO-258A, Interoperability Requirements for ATS Applications Using ARINC 622 Data Communications (FANS1/A Interop Standard), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2005, DO-258A.

[138] RTCA, DO-280B, Interoperability Requirements Standard for ATN Baseline 1 (INTEROP ATN B1), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2007, DO-280B.

[139] RTCA, DO-350A Volume I and II - Safety and Performance Standard for Baseline 2 ATS Data Communications, Initial Release (Baseline 2 SPR Standard), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2016, DO-350A Volume I and II.

[140] ARINC, ADVANCED FLIGHT MANAGEMENT COMPUTER SYSTEM, ARINC Report 702A, Aeronautical Radio, Incorporated (ARINC), 2018.

[141] ARINC, DATALINK GROUND SYSTEMS STANDARD and INTERFACE SPECIFICATION (DGSS/IS), ARINC Report 620-11, Aeronautical Radio, Incorporated (ARINC), 2020.

[142] FAA, Air Traffic Control, Tech. Rep., Federal Aviation Administration (FAA), 2019, JO 7110.65Y.

[143] ICAO, Doc 9718 - Handbook on Radio Frequency Spectrum Requirements for Civil Aviation, Tech. Rep., fifth ed., International Civil Aviation Organization (ICAO), 2009, Doc 9718.

[144] ICAO, The Convention on International Civil Aviation - Annexes 1 to 18, Tech. Rep., International Civil Aviation Organization (ICAO), 2012.

[145] EASA, ED-137 - INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS VOLUME 1: RADIO, VOLUME 2: TELEPHONE, VOLUME 3: EUROPEAN LEGACY TELEPHONE INTERWORKING, VOLUME 4: RECORDING, VOLUME 5: SUPERVISION, Tech. Rep., European Aviation Safety Agency (EASA), 2012, ED-137.

[146] RTCA, Change 1 to DO-280B, Interoperability Requirements Standard for Aeronautical Telecommunication Network Baseline 1 (ATN B1 Interop Standards), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2014, Change 1 to DO-280B.

[147] ICAO, Annex 10 - Aeronautical Telecommunications - Volume IV - Surveillance Radar and Collision Avoidance Systems, Tech. Rep., fifth ed., International Civil Aviation Organization (ICAO), 2014.

[148] R.E. Boisvert, V.A. Orlando, ADS-Mode S system overview, in: [1993 Proceedings] AIAA/IEEE Digital Avionics Systems Conference, IEEE, Fort Worth, TX, USA, 1993, pp. 104–109, http://dx.doi.org/10.1109/DASC.1993.283562.

[149] A. Seifer, SSR Code Management – Ein Überblick, Tech. Rep., Deutsche Flugsicherung (DFS), 2020.

[150] H. Mensen, Handbuch Der Luftfahrt, Vol. 2, Springer Berlin Heidelberg, 2013, http://dx.doi.org/10.1007/978-3-642-34402-2.

[151] K. Shiomi, S. Aoyama, Development of passive surveillance radar, in: Proc. 29th Congress of the International Council of the Aeronautical Sciences, St. Petersburg, Russia, 2014, pp. 1–7.

[152] ICAO, ADS-B IMPLEMENTATION and OPERATIONS GUIDANCE DOCUMENT, Tech. Rep., 11.0 Edition, International Civil Aviation Organization (ICAO), 2018.

[153] K. Werner, J. Bredemeyer, T. Delovski, ADS-B Over satellite: global air traffic surveillance from space, in: 2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, TIWDC/ESAV, IEEE, Rome, Italy, 2014, pp. 47–52, http://dx.doi.org/10.1109/TIWDC-ESAV.2014.6945446.

[154] RTCA, DO-242A, Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2002, DO-242A.

[155] K. Baker, Space-based ADS-B: performance, architecture and market, in: 2019 Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, 2019, pp. 1–10, http://dx.doi.org/10.1109/ICNSURV.2019.8735307.

[156] S. Yu, L. Chen, S. Li, X. Zhang, Adaptive multi-beamforming for space-based ADS-B, J. Nav. 72 (2) (2019) 359–374.

[157] RTCA, DO-169, VHF Air-Ground Communication Technology and Spectrum Utilization, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 1979, DO-169.

[158] RTCA, DO-225, VHF Air-Ground Communications System Improvements Alternatives Study and Selection of Proposals for Future Action, DO-225, Radio Technical Commission for Aeronautics (RTCA), 1994.

[159] RTCA, DO-351A Volume I and II - Interoperability Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 Interop Standard), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2016, DO-351A Volume I and II.

[160] RTCA, DO-144A, Minimum Operational Characteristics-Airborne ATC Transponder Systems, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2008, DO-144A.

[161] RTCA, DO-181E, Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S) Airborne Equipment, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2011, DO-181E.
[162] T. Williamson, N.A. Spencer, Development and operation of the traffic alert and collision avoidance system (TCAS), Proc. IEEE 77 (11) (1989) 1735–1744, http://dx.doi.org/10.1109/5.47735.
[163] RTCA, DO-185, Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) – Change 2, Vol. 04, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2013, DO-185.
[164] D. De, N. Chattoraj, A review: Theoretical analysis of TCAS antenna: Traffic collision avoidance system for aircraft, in: 2014 International Conference on Green Computing Communication and Electrical Engineering, ICGCCEE, IEEE, Coimbatore, India, 2014, pp. 1–7, http://dx.doi.org/10.1109/ICGCCEE.2014.6922248.
[165] Federal Aviation Administration (FAA), Introduction to TCAS II: Version 7.1, 2011, https://www.faa.gov/documentlibrary/media/advisory_circular/tcasiiv7.1introbooklet.pdf. (Accessed 13 April 2022).
[166] P. Freeman, M. Garcia, R. Smith, FIS-B Service tiering and recommended avionics processing algorithms, in: 2011 Integrated Communications, Navigation, and Surveillance Conference Proceedings, IEEE, Herndon, VA, USA, 2011, pp. C7–1–C7–7, http://dx.doi.org/10.1109/ICNSURV.2011.5935268.
[167] RTCA, DO-358A, Minimum Operational Performance Standards (MOPS) for Flight Information Services Broadcast (FIS-B) with Universal Access Transceiver (UAT), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2019, DO-358A.
[168] T.-H. Cho, I.-S. Song, E.-M. Jang, W.-O. Yoon, S.-B. Choi, A study on FIS-B design and implementation for providing air traffic informations, J. Adv. Nav. Technol. 15 (6) (2011) 970–976, http://dx.doi.org/10.12673/jant.2011.15.6.970.
[169] S.S. Silva, L. Jensen, R.J. Hansman, Pilot perception and use of ADS-B in traffic and weather services (TIS-B and FIS-B), in: 15th AIAA Aviation Technology, Integration, and Operations Conference, MIT, 2015, pp. 28–49, http://dx.doi.org/10.2514/6.2015-2849.
[170] R. Chamlou, TIS-B: Calculation of navigation accuracy category for position and velocity parameters, in: 2004 IEEE/AIAA 23th Digital Avionics Systems Conference, Vol. 1, DASC, IEEE/AIAA, Salt Lake City, UT, USA, 2004, pp. 1.D.3–11, http://dx.doi.org/10.1109/DASC.2004.1391248.
[171] RTCA, DO-300A, Minimum Operational Performance Standards (MOPS) for Traffic Alert and Collision Avoidance System II (TCAS II) Hybrid Surveillance, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2013, DO-300A.
[172] RTCA, DO-267A, Minimum Aviation System Performance Standards (MASPS) for Flight Information Services- Broadcast (FIS-B) Data Link, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2004, DO-267A.
[173] RTCA, DO-286B, Minimum Aviation System Performance Standards (MASPS) for Traffic Information Service – Broadcast (TIS-B), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2007, DO-286B.
[174] EASA, ED-108A - MOPS for VDL Mode 4 Aircraft Transceiver, Tech. Rep., European Aviation Safety Agency (EASA), 2005, ED-108A.
[175] IEEE, IEEE Standard for local and metropolitan area networks part 16: Air interface for broadband wireless access systems, in: IEEE Std 802.16-2009, Revision of IEEE Std 802.16-2004, 2009, pp. 1–2080, http://dx.doi.org/10.1109/IEEESTD.2009.5062485.
[176] M. Niraula, J. Graefe, R. Dlouhy, M. Layton, M. Stevenson, ATN/IPS Security approach: Two-way mutual authentication, data integrity and privacy, in: 2018 Integrated Communications, Navigation, Surveillance Conference, ICNS, Herndon, VA, USA, 2018, pp. 1A3–1–1A3–17, http://dx.doi.org/10.1109/ICNSURV.2018.8384829.
[177] K. Bernsmed, C. Fr, P.H. Meland, T.A. Myrvoll, et al., Security requirements for SATCOM datalink systems for future air traffic management, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference, DASC, IEEE, St. Petersburg, FL, USA, 2017, pp. 1–10, http://dx.doi.org/10.1109/DASC.2017.8102083.
[178] J.P. Mitchell, R.L. Bortz, S.J. Zogg, F.R. Chisholm, K. Delaney, D. McClatchy, R.R. Stefani, Advance mobile communications gateway with satcom backhaul access and a modularized data security system and method for data and secure key distribution to aircraft, 2016, Google Patents. US Patent 9, 509, 394.
[179] RTCA, DO-219, Minimum Operational Performance Standards for ATC Two-Way Data Link Communications, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 1993, DO-219.
[180] RTCA, DO-240, Minimum Operational Performance Standards (MOPS) for Aeronautical Telecommunication Network (ATN) Avionics, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 1997, DO-240.
[181] M. Yue, X. Wu, The approach of ACARS data encryption and authentication, in: 2010 International Conference on Computational Intelligence and Security, IEEE, Nanning, China, 2010, pp. 556–560, http://dx.doi.org/10.1109/CIS.2010.127.
[182] P.E. Storck, Benefits of commercial data link security, in: 2013 Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2013, pp. 1–6, http://dx.doi.org/10.1109/ICNSurv.2013.6548566.
[183] C. Bresteau, S. Guigui, P. Berthier, J.M. Fernandez, On the security of aeronautical datalink communications: Problems and solutions, in: 2018 Integrated Communications, Navigation, Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2018, pp. 1A4–1–1A4–13, http://dx.doi.org/10.1109/ICNSURV.2018.8384830.
[184] V. Patel, ICAO Air-ground security standards strategy, in: 2016 Integrated Communication, Navigation and Surveillance Conference, ICNS, IEEE, Herndon, VA, USA, 2016, pp. 1–31, http://dx.doi.org/10.1109/ICNSURV.2016.7486397.
[185] RTCA, DO-353A, Interoperability Requirements Standard for Baseline 2 ATS Data Communications, ATN Baseline 1 Accommodation (ATN Baseline 1 - Baseline 2 Interop Standard), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2016, DO-353A.
[186] RTCA, DO-239, Minimum Operational Performance Standards for Traffic Information Service (TIS) Data Link Communications, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 1997, DO-239.
[187] ICAO, Doc 9694 - Manual Of Air Traffic Services Data Link Applications, Tech. Rep., first ed., International Civil Aviation Organization (ICAO), 1999, Doc 9694.
[188] ICAO, Doc 9684 - Manual of the Secondary Surveillance Radar (SSR) Systems, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2004, Doc 9684.
[189] EUROCONTROL, Airborne Collision Avoidance System (ACAS), Tech. Rep., first ed., EUROCONTROL, 2017.
[190] ICAO, Doc 9863 - Airborne Collision Avoidance System (ACAS) Manual, Tech. Rep., second ed., International Civil Aviation Organization (ICAO), 2012, Doc 9863.
[191] M.R. Manesh, N. Kaabouch, Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system, Int. J. Crit. Infrastruct. Prot. 19 (2017) 16–31, http://dx.doi.org/10.1016/j.ijcip.2017.10.002.
[192] RTCA, DO-184, Traffic Alert and Collision Avoidance System (TCAS) I Functional Guidelines, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 1983, DO-184.
[193] M. Leonardi, F. Gerardi, Aircraft mode S transponder fingerprinting for intrusion detection, Aerospace 7 (3) (2020) 30, http://dx.doi.org/10.3390/aerospace7030030.
[194] E. Harison, N. Zaidenberg, Survey of cyber threats in air traffic control and aircraft communications systems, in: Cyber Security: Power and Technology, Springer, 2018, pp. 199–217, http://dx.doi.org/10.1007/978-3-319-75307-2_12.
[195] FlightAware, dump1090, 2022, GitHub, https://github.com/flightaware/dump1090. (Accessed 13 April 2022).
[196] T. Leconte, VDLM2DEC, 2020, GitHub. https://github.com/TLeconte/vdlm2dec, (Accessed 13 April 2022).
[197] D.M. Mielke, T. Gräupl, On the vulnerability of random access channels in aeronautical communications, in: 2020 AIAA/IEEE 39th Digital Avionics Systems Conference, DASC, IEEE, Online, 2020, pp. 1–7, http://dx.doi.org/10.1109/DASC50938.2020.9256780.
[198] R. Kunkel, Air traffic control: Insecurity and ADS-b, 2011, DEFCON 17. https://www.youtube.com/watch?v=aU8NpyYf9wY. (Accessed 13 April 2022).
[199] K. Boman, G. Horn, P. Howard, V. Niemi, UMTS Security, Electr. Commun. Eng. J. 14 (5) (2002) 191–204, http://dx.doi.org/10.1049/PBTE051E.
[200] B. Blanchet, Symbolic and computational mechanized verification of the ARINC823 avionic protocols, in: 2017 IEEE 30th Computer Security Foundations Symposium, CSF, IEEE, Santa Barbara, CA, USA, 2017, pp. 68–82, http://dx.doi.org/10.1109/CSF.2017.7.
[201] D. Kozel, M. Braun, M. Lichtmann, GNURadio, 2022, GNURadio, https://www.gnuradio.org/, (Accessed 13 April 2022).
[202] RTCA, DO-362, Command and Control (C2) Data Link Minimum Operational Performance Standards (MOPS) (Terrestrial), Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2016, DO-362.
[203] RTCA, DO-377, Minimum Aviation System Performance Standards for C2 Link Systems Supporting Operations of Unmanned Aircraft Systems in U.S. Airspace, Tech. Rep., Radio Technical Commission for Aeronautics (RTCA), 2019, DO-377.
[204] ICAO, ADDRESSING CYBERSECURITY IN CIVIL AVIATION, Tech. Rep., International Civil Aviation Organization (ICAO), 2019.
[205] ICAO, Aviation Cybersecurity Strategy, Tech. Rep., International Civil Aviation Organization (ICAO), 2019.