https://doi.org/10.3311/PPtr.37153

Periodica Polytechnica Transportation Engineering, 53(2), pp. 169–183, 2025

Cybersecurity in Aviation: Exploring the Significance, Applications, and Challenges of Cybersecurity in the Aviation Sector

Mahmoud Eleimat[1*], Arnold Őszi[2]

[1] Doctoral School on Safety and Security Sciences, Obuda University, Népszínház u. 8, H-1081 Budapest, Hungary
[2] Bánki Donát Faculty of Mechanical and Safety Engineering, Obuda University, Népszínház u. 8, H-1081 Budapest, Hungary
[*] Corresponding author, e-mail: Eleimat.mahmoud@uni-obuda.hu

Received: 21 April 2024, Accepted: 23 December 2024, Published online: 23 January 2025

Abstract

The increasing reliance on digital technologies in the aviation industry has amplified the need for robust cybersecurity measures. This article examines the critical issue of cybersecurity in aviation, exploring its importance, applications, and associated challenges. Through an analysis of real-world examples of cyber-attacks against aviation, the article highlights the potential consequences of inadequate security measures. Various applications of cybersecurity in aviation are explored, including air traffic management (ATM) Security, blockchain technology, airports, and aircraft systems protection. Furthermore, the article delves into the challenges faced by the industry in implementing effective cybersecurity protocols, considering factors such as evolving cyber threats, system interconnectivity, and the need to balance security with operational efficiency. The findings underscore the vital role of cybersecurity in safeguarding critical systems, protecting passenger data, and maintaining the integrity of aviation operations. The article concludes by emphasizing the necessity for continuous collaboration, information sharing, and investment in research and development to address emerging threats and ensure a secure future for the aviation industry.

Keywords

cybersecurity, aviation security, air traffic management (ATM) security, cyber threats, smart airports

1 Introduction

Aviation and air travel continue to play a vital role in facilitating international trade, tourism, and everyday activities, serving as significant social and economic catalysts (Torok and Heinitz, 2013). The demand for air traffic has always been growing very fast if compared with the demand for other transportation systems (Mantecchini et al., 2013). The air traffic rate has increased by more than 86% over the past 20 years (Cokorilo, 2020). The increase in population has caused an increase in the demand for mobility in general (Saif et al., 2019). Commercial aviation, by a large margin, maintains its status as the safest mode of transportation and is projected to retain this distinction throughout the current century. The civil aviation sector experienced an unprecedented period of growth in the early 20th century (Kővári and Török, 2010), and with the increasing reliance on computer systems, technological advancements and improved connectivity have greatly enhanced aviation safety, efficiency, and customer satisfaction (Eißel and Peng Chu, 2014).

Numerous aspects of the aviation industry heavily depend on connectivity, encompassing flight operations, passenger reservations, cargo handling and shipping, passenger embarkation and disembarkation procedures, air traffic control systems, and flight control navigation computers, among many others. Consequently, the potential impact of a cyber-attack extends to a larger number of aviation stakeholders. Disruption to the computer systems within any of these elements could trigger a cascading and catastrophic effect, causing significant economic and social upheaval worldwide. The ramifications would extend beyond the aviation sector, affecting various critical sectors such as banking and finance, telecommunications, healthcare, transportation, infrastructure, government services, education centres, power, energy generation, and distribution, as well as military defence (Eißel and Peng Chu, 2014).

According to the definition provided by Cambridge's dictionary, cybersecurity can be described as "ways of

Cite this article as: Eleimat, M., Őszi, A. (2025) "Cybersecurity in Aviation: Exploring the Significance, Applications, and Challenges of Cybersecurity in the Aviation Sector", Periodica Polytechnica Transportation Engineering, 53(2), pp. 169–183. https://doi.org/10.3311/PPtr.37153

protecting computer systems against threats such as viruses". Cybersecurity in the aviation sector involves the implementation of measures and protocols aimed at safeguarding computer systems from malicious attacks and breaches. These protective measures are crucial to maintaining the integrity, confidentiality, and availability of sensitive information and critical systems within the aviation industry. By fortifying the security infrastructure, the aviation sector can effectively counter cyber threats and ensure the uninterrupted operation of essential functions and services (Shah, 2024). The computer systems relevant to aviation cybersecurity encompass a wide range of components, both on the ground and in flight. These systems include crucial back-end servers housing valuable information, as well as systems responsible for coordinating and supporting flight operations. Additionally, there are systems that operate mid-air during a flight, such as in-flight entertainment systems and electronic flight bags. Each of these computer systems plays a significant role in the overall aviation infrastructure, and ensuring their security is vital to protect against potential cyber threats and maintain the smooth functioning of aviation operations (Kagalwalla and Churi, 2019).

The introduction of cutting-edge and groundbreaking technology in the aviation industry has led to the interconnectivity of all systems, ensuring seamless communication and collaboration. Furthermore, the ubiquity of the Internet allows access to it from any location, including high altitudes more than thirty thousand feet above the ground, bringing unprecedented connectivity even during mid-flight (Almedires and Almaiah, 2021; De Gramatica et al., 2015). Although the implementation of state-of-the-art technologies brings significant benefits, it is crucial to acknowledge the security challenges they introduce. Therefore, it is imperative to thoroughly assess these potential risks and develop comprehensive strategies to effectively mitigate and counter any threats that may arise. Proactive planning and robust security measures are essential to ensure the continued integrity and safety of these advanced systems (Kagalwalla and Churi, 2019; Nobles, 2017).

This paper is structured as follows. It begins with a background section that outlines the current cybersecurity landscape in the aviation industry. Next, the importance of cybersecurity is discussed, supported by real-world examples of cyber-attacks in aviation. The subsequent section briefly explores key applications of cybersecurity in aviation, including air traffic management (ATM) security and the protection of critical systems. Finally, the paper examines the challenges faced in implementing effective cybersecurity measures in aviation, considering evolving threats and the need to balance security with operational efficiency. This structured approach aims to provide a comprehensive understanding of the role of cybersecurity in safeguarding the aviation industry against cyber threats.

2 Background

The rise in cyber-attacks indicates the susceptibility of computer systems and networks, which is further exacerbated by outdated systems and inadequate information assurance practices. The vulnerability of critical infrastructures to cyber-attacks remains a major concern for both public and private organizations, primarily due to national security implications. Cybercriminals, hackers, and hostile nations are continually developing sophisticated capabilities to carry out these attacks. The cyber domain holds allure for terrorists due to its low cost, the potential to remain anonymous, and the ability to launch attacks at their convenience (Jarvis et al., 2013). Current data shows a consistent annual increase in the number of attacks (Odekon, 2015), making it only a matter of time before terrorists execute a devastating cyber-attack on a valuable critical infrastructure. The growing reliance on technological advancements, combined with the overdependence on outdated systems, escalates the risks associated with cyber security, leaving critical infrastructures, including the transportation sector, vulnerable to exploitation.

Cyberattacks have evolved beyond being an isolated objective and have become a powerful tool for achieving diverse purposes. The range of potential cyberattacks is only constrained by the imagination and creativity of those who execute them. Broadly speaking, cyberattacks can be classified into three categories based on their impact on information: attacks that compromise confidentiality, attacks that compromise integrity, and attacks that compromise availability (Janisz et al., 2016). All other types of cyberattacks can be considered variations or derivatives of these fundamental categories. It is important to emphasize that the core components of information security, and consequently cybersecurity, revolve around the principles of confidentiality, integrity, and availability, commonly referred to as the CIA triad (Janisz et al., 2016; Ukwandu et al., 2022). These three aspects form the fundamental pillars of ensuring the protection and robustness of information.

In 2022, a thorough investigation was undertaken by Ukwandu et al. (2022) to conduct a comprehensive study. The primary objective of their research was to identify and

analyze cyber-security incidents reported within the aviation sector spanning the years 2001 to 2021. The conducted research concluded that in the examination of the analyzed attacks, a significant portion of 71% was dedicated to the exploitation of login credentials, including administrative passwords, through illicit means such as malicious hacking. The primary objective of these attacks was to gain unauthorized access to the IT infrastructure. Following closely behind were denial-of-service attacks, specifically the notorious distributed denial of service (DDoS) attacks, accounting for 25% of the total. These attacks were designed to compromise data availability. Furthermore, a smaller subset of approximately 4% targeted the manipulation of file integrity, either by intercepting files during transit or when stored, with the intention of corrupting them. Fig. 1 illustrates these findings.

3 Importance

Aviation safety holds the utmost significance and could be very costly (Čokorilo et al., 2010), and the advancements in technology, particularly in electronics and computing, have brought about significant transformations in the aviation industry over the past few decades. An aircraft is a complex entity comprising various mechanical and electronic subsystems that are controlled by software (Cavka and Cokorilo, 2012). It is often remarked within the aviation community that a modern aircraft can be likened to "a computer with wings." (Zalewski et al., 2019).

In contemporary aircraft, there are numerous software-intensive systems in place, such as flight control systems equipped with autopilot capabilities, displays, navigation systems, communication systems, engine control systems, ground steering mechanisms, thrust reversers, air data systems, landing gear systems, collision avoidance systems, environmental control systems, electrical power systems, in-flight entertainment systems, and more

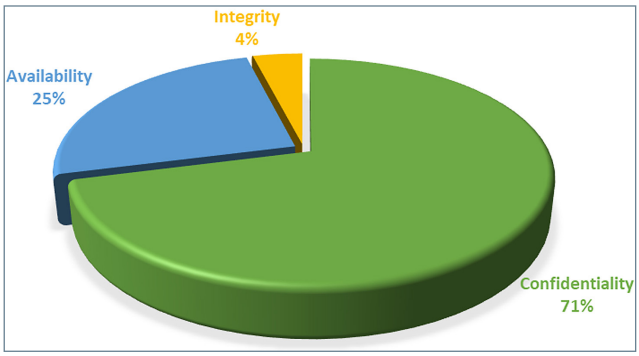

Fig. 1 Categorization of cyber attacks based on the security triad (Ukwandu et al., 2022)

(Bagdi et al., 2023; Jakovljević et al., 2017; Sándor, 2019). It is evident that different systems may have varying impacts on the overall safety of the aircraft. This integration of software-intensive systems in aviation highlights the critical role that software plays in ensuring the safe operation of aircraft. These systems are vital for the control, communication, navigation, and various other functions necessary for the safe and efficient operation of an aircraft. However, they also introduce new challenges and considerations in terms of system reliability, software security, and potential vulnerabilities that may affect the overall safety of the aircraft. In the year 2014, the occurrence of cyber-attacks reached unprecedented levels, surpassing 40 million incidents, marking a significant 50 percent surge compared to the previous year (Nobles, 2017; Shackelford and Bohm, 2016). This sharp increase in cyber-attacks highlights the escalating nature of the threat landscape during that period (Dombrowski and Demchak, 2014). The cumulative financial losses resulting from significant cyber-attacks have been approximated at an astounding figure of 700 billion dollars (Shackelford and Bohm, 2016). This substantial amount emphasizes the immense economic impact of cyber-attacks and underscores the urgency for effective cybersecurity measures to mitigate such financial ramifications. In today's interconnected world, as individuals and organizations increasingly rely on cyberspace for their daily operations, malicious actors and cybercriminals are also capitalizing on this digital landscape to instil fear, intimidate, steal, and engage in various forms of criminal activities. The borderless nature of cyberspace, coupled with the presence of valuable access points worldwide, creates an environment that is highly attractive to cybercriminals. This can be exemplified by the staggering numbers, with 1.5 billion Internet users and 4.5 billion cell phone users, highlighting the vast potential for cybercriminals to exploit this widespread connectivity (Nielsen, 2012). Cyberspace serves as an ideal platform for cyber terrorists to operate covertly or overtly due to its inherent characteristics. The anonymity and global reach provided by cyberspace offer these malicious actors fertile ground to carry out their activities. They can hide their identities, launch attacks from any location, and target individuals, organizations, or even critical infrastructures with relative ease. In previous years, many cyber-attack was reported against aviation. For instance, in March 2012, a report titled "Assessing cyber threats to Canadian infrastructure" highlighted that

various elements of the Canadian infrastructure, including passenger and cargo flights, as well as airport facilities, have been targeted in acts of terrorism conducted by al-Qaeda as part of their economic jihad against Western nations (Klenka, 2021). Specifically, a plot referred to as "Operation Overt" by British law enforcement agencies in 2006 resulted in the apprehension, conviction, and subsequent sentencing to life imprisonment of a terrorist cell inspired by al-Qaeda (Klenka, 2021). This cell had planned suicide bombing attacks on trans-Atlantic flights bound for North America, In the aftermath of a foiled plot in 2010, known as "Operation Hemorrhage", where an attempt was made to detonate an explosive device on an air cargo flight over eastern North America, the operational planner affiliated with al-Qaeda revealed their primary objective (Gendron and Rudner, 2012). Rather than aiming to inflict maximum casualties, their intention was to inflict substantial financial losses on the American economy. This strategic approach highlights the broader motivations of such terrorist organizations, emphasizing their desire to disrupt economic stability and create widespread fear and disruption through targeted attacks on critical infrastructure like the aviation industry. In April 2014, a member of the Shumouk Al-Islam jihadist forum engaged in a discussion regarding the findings of Hugo Teso, a Spanish expert. Teso had discovered a potential method for hijacking aeroplanes by exploiting vulnerabilities in the Android smartphone platform (Iasiello, 2013). This method involved gaining unauthorized access to the plane's steering system, which could potentially result in a catastrophic plane crash. The discussion on the forum highlighted the alarming implications of such vulnerabilities and the potential threats posed to aviation security, emphasizing the need for robust measures to address and mitigate these risks. In January 2015, a group calling themselves the, Lizard Squad – Official Cyber Caliphate' claimed responsibility for breaching the website of Malaysia Airlines. While the group was able to deface the website, the company asserted that no unauthorized access had occurred to their server (Urban, 2017). These incidents underscore the ongoing threat posed by terrorist organizations to the aviation sector and the importance of robust security measures to prevent such attacks and safeguard the safety of passengers and aviation infrastructure. It is important to acknowledge the challenges in quantifying the financial losses resulting from cybersecurity breaches (Ukwandu et al., 2022; Zalewski et al., 2019). The lack of transparency in record-keeping, documentation, and public disclosure of relevant incidents hinders the accurate assessment of these losses for public knowledge. The monetary value of industry payments due to cybercrime, including compensation to victims and ransom payments during ransomware attacks, remains undisclosed and unrecorded. Additionally, the extent of disruptions experienced by airports, such as shutdowns and the number of lost flight hours resulting from cyber incidents, are not documented (Ukwandu et al., 2022). This lack of transparency and comprehensive reporting makes it difficult to fully understand the economic impact of cyber-attacks on the aviation industry. It also underscores the need for improved data collection and sharing practices to gain insights into the scale and consequences of cyber incidents. Enhancing transparency and disclosure would not only facilitate a better understanding of the financial implications but also enable stakeholders to develop more effective strategies to prevent and respond to cyber threats in the aviation sector.

4 Applications of cybersecurity in aviation

The aviation industry is heavily reliant on digital systems and interconnected networks, making it susceptible to various cyber threats (Abeyratne, 2020). To safeguard critical infrastructure and ensure the safety and efficiency of aviation operations, cybersecurity applications play a vital role. One essential application is the protection of aircraft systems, which encompass flight control, communication, navigation, and entertainment systems (Habler et al., 2022). Robust cybersecurity measures are necessary to prevent unauthorized access, tampering, and disruption that could compromise flight safety. Additionally, the security of air traffic management systems is crucial to ensure the safe routing and coordination of aircraft. This involves safeguarding radar systems, communication networks, and ground control systems from cyber threats (Szyliowicz, 2004). Airport security is another crucial aspect, as surveillance cameras, access control systems, and baggage handling systems must be protected to prevent unauthorized access and disruptions to airport operations (Gopalakrishnan et al., 2013; Kelemen, 2003). Data protection is paramount, requiring stringent measures to safeguard sensitive information such as passenger data and flight plans (Enerstvedt, 2017). Advanced threat intelligence tools and continuous monitoring systems are employed to detect and respond to cyber threats in real-time. Effective incident response and recovery protocols are established to minimize the

impact of cyber incidents and swiftly restore normal operations (Niksic and Arıkan Ozturk, 2022). Moreover, regular cybersecurity training and awareness programs are conducted to foster a strong cybersecurity culture among aviation personnel (Dave et al., 2022). By implementing these cybersecurity applications, the aviation industry can enhance its resilience and mitigate risks posed by evolving cyber threats. In this section, the authors illustrate the main applications of cybersecurity in the aviation field.

4.1 Air traffic management (ATM) security

Air traffic management (ATM) systems play a critical role in safeguarding aviation safety by ensuring the effective separation of aircraft from both each other and potential obstacles present on the ground (Grebenšek and Magister, 2012). According to a study made by (Čokorilo, 2020), it was found that until the year 2000, ATM (air traffic management) controllers were involved in approximately 17% of aircraft accidents. The validation process for both the infrastructure and ATM systems necessitates multiple iterations to guarantee their compliance with technical readiness levels and safety requirements (Stelkens-Kobsch et al., 2017). Although established safety procedures for designing, implementing, and operating ATM systems are well-defined, there has been a noticeable absence of an equivalent procedure that focuses specifically on cybersecurity (Rezo and Steiner, 2020; Stelkens-Kobsch et al., 2017). Engaging in wrongful acts, such as blocking, intercepting, or manipulating information associated with ATM systems or unauthorized access to them, can introduce significant risks to flight safety. Consequently, implementing security measures that ensure confidentiality, prevent unauthorized disclosure, maintain data integrity, prevent improper or malicious modifications, and guarantee information availability when required becomes crucial. These security requirements are not only essential for protecting the integrity of ATM systems but also for safeguarding human lives (Asgari et al., 2016)

To address cyber threats and mitigate risks effectively, it is imperative to identify and manage cybersecurity risks throughout the entire lifecycle of ATM systems, including their design, implementation, and operation. Taking a proactive approach by incorporating cybersecurity measures from the outset is essential to ensure ATM systems' long-term resilience and security (Stelkens-Kobsch et al., 2017).

SESAR (single european sky ATM research) and the next generation air transportation system (NextGen) are two prominent programs aimed at modernizing and transforming air traffic management (ATM) systems in Europe and the United States, respectively (Brooker, 2008). Europe's SESAR initiative is structured into three phases, each with specific goals and objectives (Keller, 2007). The first phase, which took place from 2004 to 2008, focused on developing new concepts of operation for air traffic management (Bolić and Ravenhill, 2021; Keller, 2007). Building upon these initial concepts, the development phase spanning from 2008 to 2013 concentrated on the implementation of innovative technologies to improve the safety, efficiency, and environmental impact of ATM operations (Bolić and Ravenhill, 2021; Keller, 2007). The deployment phase spanned from 2014 to 2020. This phase aimed to bring significant changes to trajectory management by introducing 4D trajectories. This approach involves planning the location of aircraft over time, from their point of departure, to achieve greater operational efficiencies (Bolić and Ravenhill, 2021). By avoiding the need for frequent trajectory adjustments as aircraft transition between sectors, inefficiencies can be minimized. This new vision also emphasizes the coordination of trajectories across member states through the integrated exchange of data, encompassing proposed routings, meteorological information, and airport details (Keller, 2007). Facilitating this secure communication and information exchange among ATM stakeholders is the SESAR system-wide information management (SWIM) middleware, which provides the necessary mechanisms for efficient and reliable data sharing. Through these phases and advancements, SESAR strives to revolutionize ATM operations in Europe, enhancing safety, efficiency, and collaboration among aviation stakeholders (Bolić and Ravenhill, 2021; Keller, 2007).

The NextGen initiative, the United States counterpart to SESAR, is a comprehensive project that is scheduled to be implemented from 2012 to 2025 (Brooker, 2008). Similar to SESAR, NextGen aims to achieve various objectives, including reducing flight distances, fuel consumption, and holding times for airport arrivals while enhancing safety through improved separation procedures (Brooker, 2008; Darr et al., 2008). The coordination of NextGen is overseen by the joint planning and development office (JPDO), which is comparable to the SESAR joint undertaking (SJU) (Brooker, 2008). NextGen incorporates four key technologies to transform the U.S. aviation system. The automatic dependent surveillance-broadcast (ADS-B) technology is particularly significant as it replaces traditional radar

infrastructure. Instead, aircraft utilize GPS enhancements to track their position and broadcast it to both ground stations and other aircraft (Becker et al., 2009). Similar to SESAR, NextGen also relies on precise meteorological data to optimize routes (Becker et al., 2009; Bolczak et al., 2009). The next generation network enabled weather (NNEW) system is a crucial component within the future U.S. National Airspace system, ensuring accurate and timely weather information (Bradford, 2014). Improved communication is facilitated by the implementation of a standardized national airspace system voice switch (NVS) to enhance airspace communications (Darr et al., 2008). Lastly, the next generation data communications infrastructure serves as a major component of NextGen, relying on increased digital data exchange to support the program's optimization objectives, aligning with SESAR's emphasis on data exchange for optimization purposes (Brooker, 2008). In summary, NextGen is a significant initiative in the United States aimed at transforming air transportation. It shares similarities with SESAR, including objectives related to route optimization, fuel savings, capacity enhancement, and safety improvements (Bradford, 2014). Key technologies, such as ADS-B, NNEW, NVS, and enhanced data communications infrastructure, are at the core of NextGen's implementation strategy, enabling advanced surveillance, accurate weather information, improved communication, and increased digital data exchange (Becker et al., 2009). By implementing these technologies, NextGen aims to revolutionize the U.S. aviation system and achieve its optimization goals.

4.2 Blockchain

Blockchain technology has emerged as a groundbreaking tool within the financial sector, initially gaining recognition as the underlying platform for the cryptocurrency Bitcoin (Vujičić et al., 2018). However, its applicability and value extend far beyond cryptocurrency, finding utility in various entrepreneurial sectors. At its core, blockchain is a decentralized database that relies on a network of computers to maintain and validate transactions, eliminating the risk of misinformation. To illustrate its potential, consider a scenario where a bank aims to assess the creditworthiness of a prospective client. By leveraging the transparency and immutability of blockchain, the bank can trace and analyze the detailed transaction history recorded within the blockchain (Hassani et al., 2018). This enables a more accurate evaluation, reducing the reliance on potentially unreliable or incomplete information.

Conceptually, a blockchain can be likened to a ledger, such as a spreadsheet akin to Excel. However, unlike a traditional spreadsheet, where data can be easily modified, information stored within a blockchain is immutable. This immutability ensures the integrity and trustworthiness of the recorded data. Furthermore, blockchain's security is bolstered through cryptographic mechanisms, making it highly resistant to hacking attempts. Notably, there is no central authority governing the blockchain, as the information is distributed among multiple nodes in the network rather than being centralized or decentralized.

The operation of a blockchain relies on a consensus algorithm, which determines the inclusion of data within the blockchain based on the agreement of its network participants (Porter and Heppelmann, 2014). This consensus mechanism ensures that all participants reach a common understanding and validation of transactions, fostering trust and reliability within the system. When fully automated, blockchain promises increased transparency, enabling informed business decisions, heightened accountability, and consistent execution of processes. Blockchain technology offers immense potential beyond its origins in cryptocurrency. Its decentralized nature, immutability, and cryptographic security provide entrepreneurs with a robust tool to track transactions, mitigate the risk of misinformation, and foster transparency. With the ability to automate processes and ensure consensus among participants, blockchain holds promise for enhancing decision-making, accountability, and execution within businesses (Stylianou et al., 2015).

Blockchain technology has significant potential in the field of air transport for managing and sharing data sources. For instance, in processes like advance passenger information (API) (Banerjea-Brodeur, 2003), and passenger name records (PNR), where data records are involved, Blockchain can offer a secure platform for sharing data and information. Similarly, ticketing and loyalty programs can be streamlined by using Blockchain to sell e-tickets in real-time through partner airlines within alliances. Additionally, loyalty program points can be integrated into the Blockchain system, allowing passengers to use their earned points as currency.

In the realm of air freight, Blockchain can greatly reduce the burden of paperwork by digitizing the various information required for freight management. Personnel licensing and aircraft registration can also benefit from Blockchain's anti-tampering mechanism, ensuring the accuracy and security of records. Blockchain can function as a registry of

mobile assets, potentially replacing the international registry of mobile assets (Altenhoff et al., 2019). Furthermore, Blockchain can be extended to transactions within the aviation industry, including aircraft leasing, parts purchasing, and tracking flight operation costs, all of which can be recorded in the decentralized database.

Regulatory authorities can leverage Blockchain to monitor service providers and their compliance with regulations effectively. By storing contracts in transparent digital databases with robust security measures, Blockchain provides assurance to aircraft manufacturers and airlines that their contracts will remain intact and protected from hacking, deletion, tampering, or revision (Adhikari and Davis, 2020). Each transaction, payment, or task recorded in the Blockchain database is identifiable, verifiable, and properly stored, eliminating the need for intermediaries such as lawyers, brokers, and bankers. This allows seamless transactions between machines and individuals, revolutionizing the way business is conducted and facilitating economies and social systems (Iansiti and Lakhani, 2017).

However, Blockchain technology does have limitations. From a legal perspective, it can be challenging to tie Blockchain to a specific jurisdiction as the servers hosting the digital ledger can be located anywhere. This poses a legal challenge in identifying the location of transactions or addressing fraud or erroneous transactions. The anonymity provided to Blockchain users can also bring about concerns regarding transparency and accountability (De Filippi and Wright, 2018). Additionally, while Blockchain introduces efficiency in operations, users must have a clear understanding of how it can be applied to achieve their specific objectives.

Finally, Blockchain technology presents numerous opportunities for improving various aspects of the aviation industry, including data management, ticketing, freight, regulatory compliance, and contractual processes. While there are legal and operational considerations, the adoption of Blockchain can drive innovation, streamline operations, and enhance security within the aviation sector.

4.3 Airports

Airports have a significant impact on the global economy as they serve as hubs for connecting people worldwide (Mirosavljević et al., 2012; Selymes et al., 2010), promoting business expansion, facilitating international tourism, and generating revenue through commerce and taxes (Distefano and Leonardi, 2014; Florida et al., 2015). Research studies have highlighted the correlation between airports and regional economic growth, emphasizing the importance of accessibility in fostering tourism and enabling collaboration between geographically distant businesses, as well as facilitating the swift transportation of goods and accelerating trade (Baker et al., 2015; Florida et al., 2015). Additionally, airports contribute to local economies by creating employment opportunities during construction and for various operational tasks, including management, maintenance of airport infrastructure and aircraft, and day-to-day operations. Consequently, airports undergo gradual modernization to accommodate the ever-increasing number of travellers and enhance service quality by adopting emerging technologies.

As airports continue to expand their infrastructure complexity, they are now involving a greater number of stakeholders. To enhance their effectiveness, airports are leveraging the Internet of Things (IoT) technology and intelligent applications, enabling interoperability. According to Pethuru (Raj and Raman, 2017), the evolution of airports can be categorized into three main phases:

- Airport Phase 1.0 (Basic): In this phase, airports primarily focus on the essential capabilities required for the safe and efficient management of aircraft operations, such as landings and departures. They offer basic passenger services, including check-in, boarding, security, baggage handling, and modest retail, food, and beverage services.
- Airport Phase 2.0 (Agile): As airports adapt to the changing digital landscape, they embrace enabling technology collaboration throughout their operations, spanning different business units. These airports implement a converged network architecture that facilitates shared services on a unified platform, covering the entire airport.
- Airport Phase 3.0 (Smart): In the smart airport phase, airports fully harness the potential of emerging IoT technologies, leveraging advanced and pervasive sense-analyze-respond capabilities. The airport's digital grid becomes its nervous system, enabling comprehensive management of every interaction point. By facilitating real-time information exchange, fostering collaboration, and integrating processes across the entire airport, smart airports greatly enhance operational efficiencies, passenger services, and advanced security capabilities.

In accordance with G. Lykou et al. (Lykou et al., 2018), airports in Europe and the USA have undergone a classification process into Basic, Agile, and Smart categories. This classification is determined based on the airports' self-assessment of their smart airport status and their reported utilization of IoT applications within their facilities. The purpose of this classification is to provide a more comprehensive evaluation of airports' cybersecurity preparedness by considering the complexity of their information and communication technology (ICT) infrastructure and their level of technological advancement. The outcomes of this classification reveal that 16% of airports fall into the Basic category, while 56% are classified as Agile, and the remaining 28% are designated as Smart airports, and these statistics are visually represented in Fig. 2.

These evolutionary phases demonstrate how airports are embracing technological advancements to transform their operations and provide improved services. By leveraging IoT and advanced analytics, smart airports optimize their infrastructure and enhance their ability to manage interactions, ultimately delivering enhanced operational efficiency, superior passenger experiences, and advanced security measures (Alansari et al., 2019). As per the european union agency for cybersecurity (ENISA), smart airports are defined as airports that leverage networked and data-driven response capabilities. These capabilities serve two primary objectives: enhancing the travel experience for passengers and ensuring higher levels of security for the safety of passengers, operators, and the general public (European Union Agency for Cybersecurity, 2017). Given that safety and security are paramount in the aviation industry, it is crucial to proactively address complex

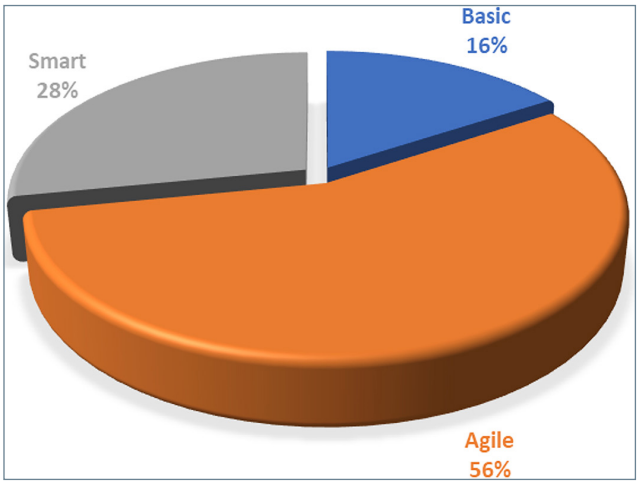

Fig. 2 Airports' classification based on IoT apps in Europe and USA

cybersecurity challenges to maintain a safe environment while minimizing disruptions to airport operations. One key aspect of cybersecurity in smart airports is the protection of critical infrastructure and data (Khadonova et al., 2020). As airports become more interconnected, with numerous systems and devices connected to the IoT, they become potential targets for cyber threats (Bouyakoub et al., 2017). Therefore, implementing stringent access controls, encryption mechanisms, and intrusion detection systems is vital to safeguarding sensitive information and infrastructure integrity.

Moreover, collaboration and information sharing among airport stakeholders play a crucial role in strengthening cybersecurity. Airports must establish strong partnerships with airlines, government agencies, law enforcement bodies, and cybersecurity organizations to exchange threat intelligence, best practices, and response strategies. By fostering a collective defence approach, smart airports can enhance their ability to detect, prevent, and respond to cyber incidents effectively.

Another critical aspect of cybersecurity in smart airports is the training and awareness of personnel (Bite, 2010). Employees at all levels, from frontline staff to senior management, should receive comprehensive cybersecurity training to understand the potential risks, recognize suspicious activities, and follow secure practices (Göçmen, 2021). Regular drills and simulations can also help in testing incident response plans and ensuring preparedness for various cyber threats. To maintain continuous cybersecurity improvement, smart airports must conduct regular vulnerability assessments and penetration testing to identify potential weaknesses in their systems. By conducting proactive risk assessments and staying up to date with emerging cyber threats, airports can address vulnerabilities promptly and apply necessary patches and security updates (Alansari et al., 2019). Furthermore, compliance with regulatory standards and frameworks is essential for smart airports. Adhering to industry-specific regulations and guidelines, such as the international civil aviation organization's (ICAO) cybersecurity framework, can provide a roadmap for implementing robust cybersecurity measures. Additionally, engaging third-party auditors to conduct independent security assessments can help validate the effectiveness of cybersecurity controls.

Finally, as airports embrace digital transformation and enter the era of smart airports, cybersecurity becomes a critical aspect of their operations. By adopting a

comprehensive approach that encompasses technological measures, collaboration, employee training, vulnerability assessments, and regulatory compliance, smart airports can mitigate cybersecurity risks and ensure the safety and seamless functioning of their operations in an increasingly interconnected world.

4.4 Aircraft systems protection

With the rapid digitization of aircraft systems, the aviation industry has experienced a significant transformation, resulting in increased interconnectivity and reliance on advanced technologies (Haass et al., 2016). However, this model shift has also introduced new and complex cybersecurity challenges, making robust protection mechanisms a pressing concern (Abeyratne, 2020; Haass et al., 2016). This section provides an overview of the most crucial strategies and technologies employed to mitigate potential risks, emphasizing the need for comprehensive protection measures to enhance the security posture of aircraft systems and ensure the safety, reliability, and integrity of air transportation: threat landscape analysis.

Conducting a thorough analysis of the threat landscape is a fundamental aspect of aircraft systems' protection (Choo, 2011). This analysis encompasses both internal and external threats that pose potential risks to aviation infrastructure. Internal threats may include malicious insiders, disgruntled employees, or inadvertent errors, while external threats encompass malicious actors, unauthorized access attempts, and potential vulnerabilities within aircraft systems (Choo, 2011; Iasiello, 2013). Understanding the specific threats and their potential impact is crucial for developing appropriate security controls and countermeasures (Iasiello, 2013). Threat modelling techniques, vulnerability assessments, and penetration testing can aid in identifying weaknesses and vulnerabilities within aircraft systems, enabling proactive risk mitigation strategies: secure system design.

Designing aircraft systems with security in mind is paramount to establishing a strong foundation for protection (Moir and Seabridge, 2012). Secure coding practices, such as following secure development methodologies, and adhering to industry best practices, play a vital role in mitigating vulnerabilities (Moir and Seabridge, 2012). Emphasizing secure software development life cycles and conducting code reviews can help identify and address potential security flaws early in the development process. Robust authentication mechanisms, including multifactor authentication and strong encryption protocols, enhance the integrity and confidentiality of aircraft systems (Jenkinson et al., 1999; Kundu, 2010). The adoption of secure communication protocols and encryption standards strengthens data protection and confidentiality during data transmission between components of aircraft systems (such as avionics, communication systems, and ground infrastructure): network segmentation.

Network segmentation is a critical defence mechanism for protecting aircraft systems (Simpson and Foltz, 2021). By dividing the network into distinct segments or zones, each with its own security controls and access permissions, the potential for lateral movement by attackers is significantly reduced (Wagner et al., 2016). Network segmentation enables the compartmentalization of critical systems and limits the blast radius in the event of a breach. By isolating different components and functionalities, such as flight controls, avionics, passenger services, and maintenance systems, potential attackers face additional hurdles in compromising the entire aircraft system. Moreover, segmenting the network helps prevent unauthorized access to critical systems and reduces the attack surface (Simpson and Foltz, 2021). Implementing strong network access controls, firewalls, and intrusion prevention mechanisms at segment boundaries further fortifies the security of aircraft systems: intrusion detection and prevention systems (IDPS).

Deploying intrusion detection and prevention systems (IDPS) is crucial for proactive protection of aircraft systems (De Cerchio and Riley, 2011). IDPS continuously monitors network traffic, analyzing it in real-time to detect anomalous behaviour and potential cyber threats (Sharifi et al., 2014). Advanced techniques such as machine learning, behavioural analysis, and anomaly detection algorithms enable IDPS to identify deviations from normal patterns, detect known attack signatures, and discover new attack vectors (Sharifi et al., 2014). Upon detection, IDPS generates alerts or triggers automated actions to mitigate risks promptly (Scarfone and Mell, 2007). Integrating IDPS into the aircraft systems' infrastructure adds an additional layer of defence, augmenting the overall security posture (Guan et al., 2020). However, careful consideration should be given to the performance impact and potential false positives to avoid operational disruptions: patch management and updates.

Regular and timely patch management is critical to maintaining the security of aircraft systems

(De Cerchio and Riley, 2011; Thanthry and Pendse, 2004). As vulnerabilities are discovered, software vendors release security patches and updates to address these weaknesses (Ladstaetter et al., 2011). Promptly applying these patches and updates helps mitigate known vulnerabilities, reducing the likelihood of successful cyber attacks (Bogoda, n.d.; Ladstaetter et al., 2011). A robust patch management process, which includes thorough testing of patches before deployment, ensures the timely application of necessary updates while minimizing disruption to aircraft operations (Zalewski et al., 2019). Automation tools and centralized patch management systems can streamline the patch deployment process, ensuring consistent and efficient updates across the entire ecosystem of aircraft systems: collaboration among stakeholders.

Collaboration among various stakeholders is essential for effective protection of aircraft systems (Amaeshi and Crane, 2006). This collaborative approach involves sharing threat intelligence, best practices, and response strategies among airlines, government agencies, law enforcement bodies, and cybersecurity organizations (Abeyratne, 2020; Amaeshi and Crane, 2006). Establishing information, sharing platforms, participating in joint exercises, and coordinating incident response mechanisms facilitate timely and effective responses to emerging cyber threats (Abeyratne, 2020; Habler et al., 2022). Public-private partnerships, industry consortiums, and regulatory frameworks that encourage collaboration can foster a collective defence approach, enabling proactive identification and mitigation of potential risks (Payán-Sánchez et al., 2018). Regular communication channels, training programs, and collaboration frameworks enhance the collective knowledge and expertise of stakeholders involved in safeguarding aircraft systems.

Finally, aircraft systems' protection is a critical aspect of cybersecurity in aviation, ensuring air transportation's safety, reliability, and integrity in the face of evolving cyber threats (Abeyratne, 2020). By implementing comprehensive strategies that encompass threat landscape analysis, secure system design, network segmentation, IDPS deployment, regular patch management, and collaboration among stakeholders, the aviation industry can enhance the security posture of aircraft systems (Urban, 2017). Continuous monitoring, regular staff training on cybersecurity best practices, and active engagement with emerging technologies is essential for staying ahead of evolving threats (Kagalwalla and Churi, 2019). With a robust and proactive approach to aircraft systems' protection, the industry can safeguard critical aviation infrastructure, adapt to emerging cyber threats, and secure the future of aviation in the digital age (Abeyratne, 2020).

5 Challenges

The aviation industry faces significant challenges in maintaining cybersecurity due to limited resources, budget constraints, and a shortage of expertise in the field. Each year, the number and complexity of cyber threats targeting aviation systems continue to rise dramatically. According to a 2018 survey conducted by SITA on Airline IT Trends, a major obstacle to implementing cybersecurity measures is the lack of resources, affecting 78% of organizations (Κοσσένα, 2019). This challenge is compounded by limited budgets allocated to cybersecurity, which is a problem for 70% of organizations. However, investments in cybersecurity by airlines and airports have been steadily increasing and are expected to reach a total of $3.9 billion in 2040 (Babić et al., 2017). Despite this, smaller regional airlines may struggle to allocate sufficient funds to cybersecurity, leaving them more vulnerable to cyber-attacks compared to larger international carriers.

According to Cerchio et al. (De Cerchio and Riley, 2011), the recruitment and retention of cybersecurity experts is another critical issue which affects 47% of organizations, along with the availability of training facilities for staff at 56%. Training employees to effectively counter evolving cyber threats is a complex task that requires highly experienced personnel and adequate resources to simulate threat scenarios. Developing skills and expertise is crucial in protecting airborne network environments from cyber-attacks. To address these challenges, airlines need to augment their internal resources with external expertise. Securing operational technologies like supervisory control and data acquisition (SCADA) and industrial control systems (ICS) presents a challenge for 38% of organizations (Kagalwalla and Churi, 2019). SCADA technology is particularly adept at secure data logging, access control, and automation. Its scalability, robustness, and reliability make it suitable for critical processes in aviation, where security and performance are paramount. While data protection is considered essential, it remains a problem for many organizations. The constant introduction of new functionalities and technologies in the aviation industry increases the number of potential attack vectors that need analysis. Securing each vector becomes challenging in a

rapidly evolving technological landscape. Areas such as cloud computing and the internet of things (IoT), widely utilized by airlines, also require monitoring and protection. The insider threat is another significant challenge in implementing aviation cybersecurity, involving airline employees or individuals with knowledge of protocols and vulnerabilities. Continuously monitoring the actions of employees presents a daunting task. The interconnected systems within the aviation industry support efficient air traffic management operations, but they also raise the risk of cyber-attacks. As a critical infrastructure and a vital participant in passenger transportation and commerce, the global aviation sector remains a primary target for malicious actors seeking to cause substantial harm or damage reputation (Iasiello, 2013). According to another study conducted by PricewaterhouseCoopers (Tonn et al., 2019), it was found that a significant proportion of airline CEOs, precisely 85%, have expressed their concerns regarding cybersecurity risks; this percentage is notably higher compared to CEOs in other industries, where 61% have reported similar concerns, this data highlights the elevated level of apprehension among airline executives regarding potential cybersecurity threats.

Aviation ICT environments often include legacy systems or applications with less secure communication mechanisms, such as the ADS-B system. These systems lack protection, encryption, and proper security measures, increasing the potential risk of security breaches. Mission-critical systems like flight information display systems, airfield lighting controls, baggage handling systems, and access control devices are particularly vulnerable (Murphy et al., 2015). The security threats to civil aviation operations are sophisticated and challenging to manage (Lekota and Coetzee, 2019). Several cyber-attacks within the aviation community have been reported between 2013 and 2018 (Gopalakrishnan et al., 2013). Various initiatives have been implemented to enhance aviation cybersecurity in response to these challenges. The US aviation and transportation security act (ATSA) and post-9/11 regulations provide a framework to prevent further attacks and protect critical transportation modes (Calderwood and DeHaan, 2002). Collaboration among governments, industry stakeholders, and associations like IATA and EASA is crucial for establishing global information security standards and sharing relevant information to proactively address emerging threats (Skaves, 2015). To sum it up, addressing the challenges and mitigating cybersecurity risks in the complex and expansive aviation sector requires extensive collaboration among government agencies, industry partners, and associations. Adequate allocation of resources, budgetary considerations, skill development, and safeguarding of critical systems are essential elements in protecting the aviation industry from cyber threats.

6 Conclusion

In conclusion, this article has explored the critical issue of cybersecurity in the aviation industry. Through the examination of various aspects, including the introduction, background, importance, applications, and challenges, a comprehensive understanding of the subject matter has been presented. The significance of cybersecurity in aviation cannot be overstated. The examples of cyber-attacks against the aviation sector demonstrate the potential consequences of overlooking or underestimating the importance of robust security measures. These incidents serve as stark reminders of the vulnerabilities within the industry and the pressing need for effective cybersecurity protocols. The applications of cybersecurity in aviation are diverse and far-reaching. From air traffic management (ATM) Security to the utilization of blockchain technology, the various sectors within the aviation industry must proactively implement robust security measures. By safeguarding critical systems, protecting passenger data, and ensuring the integrity of airport infrastructure, cybersecurity plays a pivotal role in maintaining the safety and reliability of aviation operations.

However, despite the advancements and growing recognition of the importance of cybersecurity in aviation, significant challenges persist. The evolving nature of cyber threats, the interconnectivity of systems, and the constant need to balance security with operational efficiency pose ongoing challenges to stakeholders in the industry. Addressing these challenges requires continuous collaboration, information sharing, and investment in research and development to stay ahead of emerging threats.

Finally, the field of cybersecurity in aviation is a complex and multifaceted domain that demands the utmost attention from all stakeholders. By recognizing the potential risks, implementing robust security measures, and staying abreast of emerging technologies and practices, the aviation industry can mitigate cyber threats and ensure a safer future for air travel.

References

Abeyratne, R. (2020) "Aviation in the digital age", Springer International Publishing. ISBN 978-3-030-48217-6 https://doi.org/10.1007/978-3-030-48218-3

Adhikari, S., Davis, C. (2020) "Application of blockchain within aviation cybersecurity framework", AIAA Aviation 2020 Forum, 1 PartF, pp. 1–3. https://doi.org/10.2514/6.2020-2931

Alansari, Z., Soomro, S., Belgaum, M. R. (2019) "Smart airports: Review and open research issues", Springer, 285, pp. 136–148. https://doi.org/10.1007/978-3-030-23943-5_10

Almedires, M., Almaiah, M. (2021) "Cybersecurity in industrial control system (ICS)", presented at 2021 International Conference on Information Technology, ICIT, Amman, Jordan, July, 26. https://doi.org/10.1109/ICIT52682.2021.9491741

Altenhoff, A. M., Levy, J., Zarowiecki, M., Tomiczek, B., Vesztrocy, A. W., Dalquen, D. A., Müller, S., Telford, M. J., Glover, N. M., Dylus, D., Dessimoz, C. (2019) "OMA standalone: orthology inference among public and custom genomes and transcriptomes", Genome Research, 29(7), pp. 1152–1163. https://doi.org/10.1101/GR.243212.118

Amaeshi, K. M., Crane, A. (2006) "Stakeholder engagement: A mechanism for sustainable aviation", Corporate Social Responsibility and Environmental Management, 13(5), pp. 245–260. https://doi.org/10.1002/CSR.108

Asgari, H., Haines, S., Waller, A. (2016) "Security risk assessment and risk treatment for integrated modular communication", presented at Proceedings – 2016 11th International Conference on Availability, Reliability and Security (ARES) Salzburg, Austria, Dec, 15. https://doi.org/10.1109/ARES.2016.6

Babić, R. Š., Tatalović, M., Bajić, J. (2017) "Air transport competition challenges", International Journal for Traffic and Transport Engineering, 7(2), pp. 144–163.

Bagdi, Z., Csámer, L., Bakó, G. (2023) "The green light for air transport: sustainable aviation at present", Cognitive Sustainability, 2(2), pp. 1–7. https://doi.org/10.55343/cogsust.55

Baker, D., Merkert, R., Kamruzzaman, M. (2015) "Regional aviation and economic growth: cointegration and causality analysis in Australia", Journal of Transport Geography, 43, pp. 140–150. https://doi.org/10.1016/j.jtrangeo.2015.02.001

Banerjea-Brodeur, N. P. (2003) "Advance passenger information/ passenger name record: privacy rights and security awareness", Level (PhD), McGill University.

Becker, K., Nam, T., Kirby, M., Mavris, D. N. (2009) "A process for future aviation environmental impacts: A surrogate fleet analysis approach for NextGen", 9th AIAA Aviation Technology, Integration, and Operations Conference (ATIO) and Aircraft Noise and Emissions Reduction Symposium (ANERS). ISBN 978-1-60086-977-8 https://doi.org/10.2514/6.2009-6934

Bite, K. E. (2010) "Staff access control at airports", Periodica Polytechnica Transportation Engineering, 38(1), pp. 9–12. https://doi.org/10.3311/pp.tr.2010-1.02

Bogoda, L. (n.d.) "A risk-oriented systems engineering approach to appraise cyber security risks of CNS/ATM and avionics systems", Level (PhD), RMIT University.

Bolczak, C. N., Fong, V., Jehlen, R. (2009) "NextGen flight security risk assessment information concept", presented at 2009 IEEE/AIAA 28th Digital Avionics Systems Conference, Orlando, FL, USA, Dec, 04. https://doi.org/10.1109/DASC.2009.5347451

Bolić, T., Ravenhill, P. (2021) "SESAR: The past, present, and future of European air traffic management research", Engineering, Elsevier, 7(4), pp. 448–451. Retrieved June 8, 2023. [online] Available at: https://www.sciencedirect.com/science/article/pii/S2095809921000503 [Accessed: 22 December 2024]

Bouyakoub, S., Belkhir, A., M'hamed Bouyakoub, F., Guebli, W., (2017) "Smart airport: An IoT-based Airport Management System", In: ACM International Conference Proceeding Series, New York, NY, USA, pp. 1–7. ISBN 9781450348447 https://doi.org/10.1145/3102304.3105572

Bradford, S. (2014) "NextGen progress and ICAO", In: 2014 Integrated Communications, Navigation and Surveillance Conference (ICNS) Conference Proceedings, Herndon, VA, USA, pp. 1–22. ISBN 978-1-4799-4891-8 https://doi.org/10.1109/ICNSurv.2014.6820057

Brooker, P. (2008) "SESAR and NextGen: Investing in new paradigms", Journal of Navigation, 61(2), pp. 195–208. https://doi.org/10.1017/S0373463307004596

Calderwood, J. A., DeHaan, R. A. (2002) "The aviation and transportation security act", Journal of Transportation Law, Logistics and Policy, 69(4), pp. 345–375.

Cavka, I., Cokorilo, O. (2012) "Cost-benefit assessment of aircraft safety", International Journal for Traffic and Transport Engineering, 2(4), pp. 359–371. https://doi.org/10.7708/ijtte.2012.2(4).06

Choo, K.-K. R. (2011) "The cyber threat landscape: Challenges and future research directions", Computers and Security, 30(8), pp. 719–731. https://doi.org/10.1016/J.COSE.2011.08.004

Čokorilo, O. (2020) "Civil aviation pilot education, coaching and beyond: building capacity in the cockpit", International Journal for Traffic and Transport Engineering, 10(1), pp. 1–14. https://doi.org/10.7708/ijtte.2020.10(1).01

Cokorilo, O. (2020) "Urban air mobility: safety challenges", Transportation Research Procedia, 45, pp. 21–29. https://doi.org/10.1016/j.trpro.2020.02.058

Čokorilo, O., Gvozdenović, S., Vasov, L., Mirosavljević, P. (2010) "Costs of unsafety in aviation", Technological and Economic Development of Economy, 16(2), pp. 188–201. https://doi.org/10.3846/tede.2010.12

Darr, S., Ricks, W., Lemos, K. A. (2008) "Safer systems: A NextGen aviation safety strategic goal", In: 2008 IEEE/AIAA 27th Digital Avionics Systems Conference, St. Paul, MN, USA, pp. 2.A.1-1-2.A.1-8. ISBN 978-1-4244-2207-4 https://doi.org/10.1109/DASC.2008.4702772

Dave, G., Choudhary, G., Sihag, V., You, I., Choo, K.-K. R. (2022) "Cyber security challenges in aviation communication, navigation, and surveillance", Computers and Security, 112, 102516. https://doi.org/10.1016/J.COSE.2021.102516

De Cerchio, R., Riley, C. (2011) "Aircraft systems cyber security", In: 2011 IEEE/AIAA 30th Digital Avionics Systems Conference, Seattle, WA, USA, pp. 1C3-1-1C3-7. ISBN 978-1-61284-798-6 https://doi.org/10.1109/DASC.2011.6095969

De Filippi, P., Wright, A. (2018) "Blockchain and the law: The rule of code", Harvard University Press. ISBN 978-0674976429 https://doi.org/10.2307/j.ctv2867sp

De Gramatica, M., Massacci, F., Shim, W., Tedeschi, A., Williams, J. (2015) "IT interdependence and the economic fairness of cybersecurity regulations for civil aviation", IEEE Security and Privacy Magazine, 13(5), pp. 52–61. https://doi.org/10.1109/MSP.2015.98

Distefano, N., Leonardi, S. (2014) "Risk assessment procedure for civil airport", International Journal for Traffic and Transport Engineering, 4(1), pp. 62–75. https://doi.org/10.7708/ijtte.2014.4(1).05

Dombrowski, P., Demchak, C. C. (2014) "Cyber war, cybered conflict, and the maritime domain", Naval War College Review, 67(2), pp. 70–96.

Eißel, D., Peng Chu, C. (2014) "The future of sustainable transport system for Europe", AI & Society, 29, pp. 387–402. https://doi.org/10.1007/s00146-013-0461-3

Enerstvedt, O. M. (2017) "Protection of privacy and data protection in aviation security", Springer, 37, pp. 19–63. https://doi.org/10.1007/978-3-319-58139-2_2

European Union Agency for Cybersecurity (2017) "Securing smart airports", European Network and Information Security Agency. ISBN 978-92-9204-185-4 https://doi.org/10.2824/865081

Florida, R., Mellander, C., Holgersson, T. (2015) "Up in the air: the role of airports for regional economic development", The Annals of Regional Science, 54(1), pp. 197–214. https://doi.org/10.1007/S00168-014-0651-Z

Gendron, A., Rudner, M. (2012) "Assessing cyber threats to Canadian infrastructure", Canadian Security Intelligence Service, Ottawa, Canada.

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. W., Phares, B. M. (2013) "Cyber security for airports", International Journal for Traffic and Transport Engineering, 3(4), pp. 365–376. https://doi.org/10.7708/IJTTE.2013.3(4).02

Göçmen, E. (2021) "Smart airport: evaluation of performance standards and technologies for a smart logistics zone", Transportation Research Record, 2675(7), pp. 480–490. https://doi.org/10.1177/03611981211019740

Grebenšek, A., Magister, T. (2012) "Traffic variability in benchmarking of air navigation services providers cost-effectiveness", International Journal for Traffic and Transport Engineering, 2(3), pp. 185–201. https://doi.org/10.7708/ijtte.2012.2(3).03

Guan, R., Wang, S., Xiong, S., Nie, X. (2020) "Preliminary study on intrusion prevention system of small aircraft applied to large hydropower station", IOP Publishing, 1549(5), 052107. https://doi.org/10.1088/1742-6596/1549/5/052107

Haass, J., Sampigethaya, R., Capezzuto, V. (2016) "Aviation and cybersecurity: opportunities for applied research", Tr News, 304, 39.

Habler, E., Bitton, R., Shabtai, A. (2022) "Evaluating the Security of Aircraft Systems", ArXiv Preprint, 2209, 04028. https://doi.org/10.48550/arXiv.2209.04028

Hassani, H., Huang, X., Silva, E. (2018) "Banking with blockchain-ed big data", Journal of Management Analytics, 5(4), pp. 256–275. https://doi.org/10.1080/23270012.2018.1528900

Iansiti, M., Lakhani, K. R. (2017) "The truth about blockchain", Harvard Business Review, 95(1), pp. 118–127.

Iasiello, E. (2013) "Getting ahead of the threat: Aviation and cyber security", Aerospace America, 51(7), pp. 22–25.

Jakovljević, I., Čokorilo, O., Dell'Acqua, G., Mirosavljević, P. (2017) "Aircraft departure control systems-hidden safety risks", International Journal for Traffic and Transport Engineering, 7(3), pp. 298–311. https://doi.org/10.7708/ijtte.2017.7(3).02

Janisz, K., Korchenko, O., Gnatyuk, S., Odarchenko, R. (2016) "Model for cybersecurity requirements definition in civil aviation", Engineering, Computer Science, 17(12), pp. 630–634.

Jarvis, L., Macdonald, S., Nouri, L. (2013) "The cyberterrorism threat: findings from a survey of researchers", Studies in Conflict & Terrorism, 37(1), pp. 68–90. https://doi.org/10.1080/1057610X.2014.853603

Jenkinson, L., Simpkin, P., Rhodes, D. (1999) "Civil jet aircraft design", American Institute of Aeronautics and Astronautics, Inc., ISBN 978-1-56347-350-0 https://doi.org/10.2514/4.473500

Kagalwalla, N., Churi, P. P. (2019) "Cybersecurity in aviation: an intrinsic review", In: 2019 5th International Conference on Computing, Communication Control and Automation, (ICCUBEA), Pune, India, pp. 1–6. ISBN 978-1-7281-4042-1 https://doi.org/10.1109/ICCUBEA47591.2019.9128483

Kelemen, Z. (2003) "Latest information technology development in the airline industry", Periodica Polytechnica Transportation Engineering, 31(1–2), pp. 45–52.

Keller, K.-H. (2007) "European research center position and contribution in European R&D for single european sky air traffic management research programme-SESAR", presented at 1st CEAS Conference, Berlin, Germany, Sept, 11.

Khadonova, S. V, Ufimtsev, A. V, Dymkova, S. S. (2020) ""Digital smart airport" system based on innovative navigation and information technologies", In: 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, pp. 1–6. ISBN 978-1-6654-0448-8 https://doi.org/10.1109/EMCTECH49634.2020.9261529

Klenka, M. (2021) "Aviation cyber security: legal aspects of cyber threats", Journal of Transportation Security, 14(3–4), pp. 177–195. https://doi.org/10.1007/S12198-021-00232-8

Κοσσένα, Μ. (2019) "Cyber security in air transportation", Level (MSc), University of the aegean school of business studies. [online] Available at: http://hdl.handle.net/11610/18829 [Accessed: 22 December 2024]

Kővári, B., Török, Á. (2010) "Social benefit estimation of travel time shortage of air transport in Europe", Periodica Polytechnica Transportation Engineering, 38(2), pp. 73–77. https://doi.org/10.3311/pp.tr.2010-2.03

Kundu, A. K. (2010) "Aircraft design", Cambridge University Press. ISBN 978-0521885164

Ladstaetter, G., Reichert, N., Obert, T. (2011) "It security management of aircraft in operation: A manufacturer's view", SAE International, Portishead, England, (Rep. 2011-01-2717). https://doi.org/10.4271/2011-01-2717

Lekota, F., Coetzee, M. (2019) "Cybersecurity incident response for the sub-Saharan African aviation industry", presented at International Conference on Cyber Warfare and Security, Johannesburg, Republic of South Africa, Aug, 10.

Lykou, G., Anagnostopoulou, A., Gritzalis, D. (2018) "Smart airport cybersecurity: Threat mitigation and cyber resilience controls", Sensors, 19(1), 19. https://doi.org/10.3390/s19010019

Mantecchini, L., Gualandi, N., and Paganelli, F. (2013) "Integration and concentration of european air transport market", International Journal for Traffic and Transport Engineering, 3(2), pp. 204–219. https://doi.org/10.7708/ijtte.2013.3(2).08

Mirosavljević, P., Gvozdenović, S., Čokorilo, O. (2012) "Oro transporto paskirstymo modelis oro uosto oro taršos valdymo sistemoje" (A model of air traffic assignment as part of airport air pollution management system), Aviation, 15(4), pp. 92–100. (in Lithuanian) https://doi.org/10.3846/16487788.2011.651792

Moir, I., Seabridge, A. (2012) "Design and development of aircraft systems", John Wiley & Sons. ISBN 978-1119941194

Murphy, R. J., Sukkarieh, M., Haass, J., Hriljac, P. (2015) "Guidebook on best practices for airport cybersecurity", The National Academies Press. ISBN 978-0-309-30880-9 https://doi.org/10.17226/22116

Nielsen, S. C. (2012) "Pursuing security in cyberspace: strategic and organizational challenges", Orbis, 56(3), pp. 336–356. https://doi.org/10.1016/J.ORBIS.2012.05.004

Niksic, L., Arıkan Ozturk, E. (2022) "US/Europe comparison of ATC-related accidents and incidents", International Journal for Traffic and Transport Engineering, 12(2), pp. 155–169. https://doi.org/10.7708/ijtte2022.12(2).01

Nobles, C. (2017) "Cyber threats in civil aviation", In: Security Solutions for Hyperconnectivity and the Internet of Things, Dawson, M., Eltayeb, M., Omar, M. eds., IGI Global, pp. 272–301. ISBN 9781522507413 https://doi.org/10.4018/978-1-5225-0741-3.CH011

Odekon, M. (2015) "Booms and busts: An encyclopedia of economic history from the first stock market crash of 1792 to the current global economic crisis", Routledge. ISBN 9781315706078 https://doi.org/10.4324/9781315706078

Payán-Sánchez, B., Plaza-Úbeda, J. A., Pérez-Valls, M., Carmona-Moreno, E. (2018) "Social embeddedness for sustainability in the aviation sector", Corporate Social Responsibility and Environmental Management, 25(4), pp. 537–553. https://doi.org/10.1002/CSR.1477

Porter, M. E., Heppelmann, J. E. (2014) "How smart, connected products are transforming competition", Harvard Business Review, 92(11), pp. 64–88.

Raj, P., Raman, A. C. (2017) "The internet of things: Enabling technologies, platforms, and use cases", CRC press. ISBN 9781315270395 https://doi.org/10.1201/9781315273095

Rezo, Z., Steiner, S. (2020) "European airspace fragmentation typology", International Journal for Traffic and Transport Engineering, 10(1), pp. 15–30. http://doi.org/10.7708/ijtte.2020.10(1).02

Saif, M. A., Zefreh, M. M., Torok, A. (2019) "Public transport accessibility: A literature review", Periodica Polytechnica Transportation Engineering, 47(1), pp. 36–43. https://doi.org/10.3311/PPtr.12072

Sándor, Z. (2019) "Challenges caused by the unmanned aerial vehicle in the air traffic management", Periodica Polytechnica Transportation Engineering, 47(2), pp. 96–105. https://doi.org/10.3311/PPtr.11204

Scarfone, K., Mell, P. (2007) "Guide to intrusion detection and prevention systems (IDPS)", NIST Special Publication, 800, 94. https://doi.org/10.6028/NIST.SP.800-94

Selymes, P., Legeza, E., Torok, A. (2010) "Investigation of European air transport traffic by utility-based decision model", Aviation, 14(3), pp. 90–94. https://doi.org/10.3846/aviation.2010.14

Shackelford, S. J., Bohm, Z. (2016) "Securing critical North American infrastructure: A comparatice case study in cybersecurity regulation", Canada-United States Law Journal, 40(1), 9.

Shah, I. A., Jhanjhi, N. Z., Brohi, S. (2024) "Cybersecurity issues and challenges in civil aviation security", Cybersecurity in the Transportation Industry. ISBN 9781394204267 https://doi.org/10.1002/9781394204472.CH1

Sharifi, A. A., Noorollahi, B. A., Farokhmanesh, F. (2014) "Intrusion detection and prevention systems (IDPS) and security issues", IJCSNS International Journal of Computer Science and Network Security, 14(11), pp. 80–84.

Simpson, W. R., Foltz, K. E. (2021) "Network segmentation and zero trust architectures", In: Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE), London, UK, pp. 201–206. ISBN 978-988-14049-2-3

Skaves, P. (2015) "FAA aircraft systems information security protection overview", In: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), Herdon, VA, USA, pp. A1-1-A1-17. ISBN 978-1-4799-8952-2 https://doi.org/10.1109/ICNSURV.2015.7121212

Stelkens-Kobsch, T. H., Finke, M., Carstengerdes, N. (2017) "A comprehensive approach for validation of air traffic management security prototypes: A case study", In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, pp. 1–10. ISBN 978-1-5386-0365-9 https://doi.org/10.1109/DASC.2017.8102082

Stylianou, N., Buchan, I., Dunn, K. W. (2015) "A review of the international burn injury database (iBID) for England and Wales: descriptive analysis of burn injuries 2003–2011", BMJ Open, 5(2), e006184. https://doi.org/10.1136/BMJOPEN-2014-006184

Szyliowicz, J. S. (2004) "Aviation security: Promise or reality?", Studies in Conflict and Terrorism, 27(1), pp. 47–63. https://doi.org/10.1080/10576100490262160

Thanthry, N., Pendse, R. (2004) "Aviation data networks: Security issues and network architecture", In: 38th Annual 2004 International Carnahan Conference on Security Technology, Albuquerque, NM, USA, pp. 77–81. ISBN 0-7803-8506-3
https://doi.org/10.1109/CCST.2004.1405372

Tonn, G., Kesan, J. P., Zhang, L., Czajkowski, J. (2019) "Cyber risk and insurance for transportation infrastructure", Transport Policy, 79, pp. 103–114.
https://doi.org/10.1016/j.tranpol.2019.04.019

Torok, A., Heinitz, F. M. (2013) "Economic impacts on destination air traffic following a flag carrier's market exit: a case study for Budapest", Aviation, 17(4), pp. 161–169.
https://doi.org/10.3846/16487788.2013.861226

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., Bellekens, X. (2022) "Cyber-security challenges in aviation industry: a review of current and future trends", Information, 13(3), 146.
https://doi.org/10.3390/info13030146

Urban, J. A. (2017) "Not your granddaddy's aviation industry: The need to implement cybersecurity standards and best practices within the international aviation industry", Albany Law Journal of Science and Technology, 27(1), pp. 62–93.
http://doi.org/10.2139/ssrn.2787476

Vujičić, D., Jagodić, D., Randić, S. (2018) "Blockchain technology, bitcoin, and Ethereum: A brief overview", In: 2018 17th International Symposium on Infoteh-Jahorina, (Infoteh) East Sarajevo, Bosnia and Herzegovina, pp. 1–6. ISBN 978-1-5386-4907-7
https://doi.org/10.1109/INFOTEH.2018.8345547

Wagner, N., Sahin, C. S., Winterrose, M., Riordan, J., Pena, J., Hanson, D., Streilein, W. W. (2016) "Towards automated cyber decision support: A case study on network segmentation for security", In: 2016 IEEE Symposium Series on Computational Intelligence, (SSCI), Athens, Greece, pp. 1–10. ISBN 978-1-5090-4240-1
https://doi.org/10.1109/SSCI.2016.7849908

Zalewski, J., Kornecki, A. (2019) "Trends nad challenges in the aviation systems safety and cybersecurity", TASK Quarterly, 23(2), pp. 159–175.
https://doi.org/10.17466/tq2019/23.2/a