INSE 6680
System Physical Security

Project Report
on

Security Concerns in Air Traffic Control

Submitted to:

Professor Dr. Mohsen Ghafouri

Submitted by:

Student Name	Student ID
Athira Dinesh Mangaparambil	40258046
Chris Regy Vallikunnathu	40232485
Harleen Kaur	40232489
Hussain Sayyed	40262414
Neha Roy	40227230

Fall 2024.

HOW CAN THE SECURITY OF ATC SYSTEMS BE IMPROVED?

Abstract - Air Traffic Control (ATC) systems play a crucial role in maintaining the safety and efficiency of modern air transportation, especially as global air traffic surges due to the increase in commercial flights and the growing use of unmanned aerial vehicles (UAVs). ATC technologies, originally developed for military applications such as radar and navigation, have faced new security challenges in their transition to civilian use. Civil aviation depends on international collaboration, which favors standard cryptographic solutions. However, the slow adoption of modern security practices within the industry has resulted in ATC systems that are not built with "security by design," instead relying on redundancy to ensure safety. This paper addresses the cybersecurity challenges in ATC systems, emphasizing vulnerabilities associated with wireless communication and automation. It explores the disconnect between aviation and cybersecurity expertise, highlighting the need for integrated approaches to safeguard air traffic management. Specific vulnerabilities are analyzed, including common attack vectors such as signal jamming and data manipulation, along with their potential impact on ATC operations. To address these threats, the paper proposes AI-driven solutions to enhance cyber-physical security, improve system resilience, and enable real-time threat detection. Additionally, it discusses strategies for embedding robust cybersecurity measures into ATC workflows to protect the future of air travel, emphasizing the critical need for proactive cybersecurity in the evolving aviation landscape.

Index terms - Air Traffic Control (ATC), signal jamming, data manipulation, ADS-B vulnerabilities, AI-driven threat detection, UAV security, cyber-physical security, aviation system resilience.

I. INTRODUCTION

With the ever-increasing popularity of air travel, we have witnessed an unprecedented rise in global passenger numbers over the last few years. The International Air Transport Association (IATA) reports that more than 4.5 billion passengers flew worldwide in 2023[1]. This figure is expected to nearly double by 2040. In Canada alone, over 150 million passengers enplaned and deplaned at Canadian airports in 2023 [2]. This consistent growth in the aviation industry has made security in air traffic management systems more essential than ever before as they must now handle more aircraft, more efficiently and safely, in increasingly congested airspaces.

Air Traffic Control (ATC) systems are the backbone of the aviation network. These critical systems are responsible for ensuring the safety and efficiency of flights, managing air traffic, and ensuring safe flight through controlled airspaces and airports. ATCs use sophisticated protocols and technologies to manage every phase of the flight - takeoff, en-route travel, and landing. Given the critical nature of these systems, numerous aviation regulatory organizations have introduced modernization efforts. The Next Generation Air Transportation System (NextGen) introduced by the Federal Aviation Administration (FAA) in the United States is a key example. The NextGen program has upgraded air traffic control infrastructure to enhance the safety, efficiency, capacity, and resilience of U.S. aviation [3]. These modernization initiatives have placed a key focus on increased digitization of ATC operations, to improve the precision and responsiveness of air traffic management.

However, modernizations introduce several security challenges. Unlike conventional ATC systems that are largely isolated, modern ATC systems are often connected to broader digital networks. This makes them more vulnerable to cybersecurity threats. The transition towards interconnected, digitalized infrastructure has exposed ATC systems to several risks, including cyberattacks which aim to disrupt or hijack air traffic management operations. However, risks are not limited to cyber threats alone. Increasing dependence on advanced technologies has opened doors to vulnerabilities in software reliability, data integrity, and communication protocols.

In Section I, we discuss the working of modern ATC systems and airspace management, focusing on how airspace is structured and controlled for safety and efficiency. Section II examines cybersecurity concerns and explores the need for integration between aviation and cybersecurity expertise. In Section III, we analyze specific system vulnerabilities which arise from wireless communication and automation. Section IV explores security attacks on ATC, including common attack vectors like signal jamming and data manipulation. Section V examines the impact of these attacks on ATC operations. Section VI identifies areas for improvement in ATC cybersecurity, proposing AI-driven methods to enhance cyber-physical security. Section VII outlines future research and strategies, focusing on integrating cybersecurity into ATC workflows and improving system resilience against cyber threats.

ATC working methodology

Conventional ATS systems relied on ground-based radars to track all aircrafts. These systems were unable to keep up with the rapid pace of industry growth primarily due to limitations in accuracy, coverage, and dependency on the line-of-sight communication [4]. Automatic Dependent Surveillance–Broadcast (ADS-B) was introduced considering these challenges.

ADS-B significantly improves situational awareness for both pilots and controllers by providing accurate and continuous updates about aircraft positions and movements [5]. It comprises two key components: ADS-B Out, which transmits flight data to ATC and other aircraft, and ADS-B In, allowing aircraft to receive and display this information. ADS-B uses Global Navigation Satellite Systems (GNSS) like GPS to determine the aircraft's precise position. This data, along with information on speed, altitude, identification, and climb/descent rates, is broadcast via Mode-S transponders on 1090 MHz (Extended Squitter) or 978 MHz (Universal Access Transceiver) frequencies. The 1090 MHz frequency is used globally for high-altitude flights, while 978 MHz is reserved for low-altitude general aviation in the U.S [6][7].

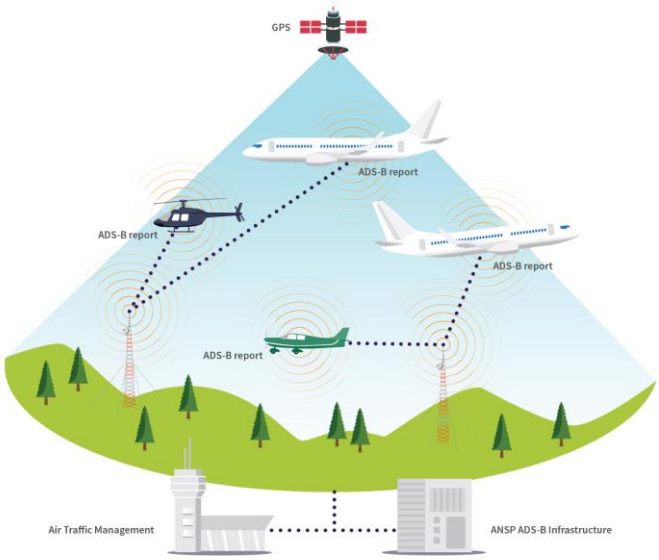

Figure 1: Overview of ADS-B System [9]

Ground-based ADS-B stations receive these signals and relay them to ATC systems, where they are integrated with traditional radar for redundancy. Additionally, ADS-B In enables aircraft to directly receive broadcast data from other aircraft, enhancing situational awareness in regions lacking radar coverage. While ADS-B provides better coverage, cost efficiency, and capacity, its reliance on unencrypted broadcasts poses security risks, such as signal spoofing and jamming [8]. To mitigate these, researchers are developing authentication protocols and integrating ADS-B with other surveillance technologies. ADS-B is a transformative advancement in ATC, addressing the limitations of conventional systems while paving the way for safer and more efficient airspace management.

Airspace Management:

The airspace management system ensures security by restricting non-airspace users and managing aircraft and air traffic operations. The International Civil Aviation Organization (ICAO) developed an international air transportation system, classifying airspace into seven categories (Class A to Class G) based on operations like separation, clearance, traffic information, and flight rules. Countries may adapt these classifications and regulations for added safety and security.
Airspace is divided into controlled (Class A to Class E) and uncontrolled (Class G) categories. Controlled airspace is managed by Air Traffic Control (ATC), while uncontrolled airspace (Class G) operates without ATC oversight and follows Instrument Flight Rules (IFR) or Visual Flight Rules (VFR). Class G has minimal restrictions, allowing maximum operation without ATC clearance. However, to ensure safety, some regulations for UAV operations in Class G airspace are recommended [10].

II. ATC SYSTEM CYBERSECURITY CONCERNS

Knowledge Gap Between Aviation and Cybersecurity Experts:

Currently, there is a disconnect between aviation and cybersecurity experts. Aviation professionals may not fully grasp the severity of cybersecurity threats, while many wireless security experts lack aviation expertise. Bridging these gaps is essential for a realistic assessment of wireless security in aviation. Significant research has been conducted on aviation cybersecurity, particularly in wireless communications and future avionics systems, with a focus on securing "e-enabled" aircraft and digital avionics systems [11].

Additionally, to assess the gap in knowledge among aviation experts regarding security of wireless communication technologies used in the industry, a survey was conducted [11]. Three main research questions that the survey looks to answer were:
a) Which technologies are considered to have the biggest impact on safety?
b) Are aviation stakeholders aware of security issues in the wireless technologies they utilize?
c) If yes, are these issues considered a concern towards safety?

The results of the survey proved that there was a high uncertainty (>15% of respondents) regarding the security

of even the most well-known wireless communication technologies. The survey was planned and conducted with the help of private pilots and full-time professional air traffic controllers. The investigation conducted by the authors indicates that aviation professionals at large are unaware of the state of security in aviation technology. A majority of participants falsely believe, for example, that even the most common surveillance technologies offer authentication, clearly contrasting with the security community's knowledge. The findings in the paper indicate the existence of expert blind spots [11].

Other Cybersecurity concerns:

Air traffic communication systems rely on more than a dozen wireless technologies throughout various phases of flight. Conceptually, all these technologies are inherently insecure, as security was not a consideration in their original design. Recently, researchers and the hacking community have exploited these vulnerabilities to demonstrate attacks on some of these systems [11]. According to [12], the following are the cybersecurity concerns in Air traffic Control system:

Increased Air Traffic Density: Growing complexity in air traffic management due to more advanced airframes.

Modernization through NextGen: FAA's NexGen system requires replacing isolated ATC systems with internet-based information systems, increasing vulnerability.

Rising Cyber Threats: Cyber threats targeting aviation have increased over the last decade. Earlier ATC systems were relatively isolated, making them harder for remote attackers to access.

GAO Recommendations: The U.S. Government Accountability Office continues to evaluate FAA's cybersecurity efforts, focusing on internet-connected systems.

Vulnerabilities in ADS-B and GPS: ADS-B, relying on vulnerable GPS and having a broadcast nature, is prone to cyberattacks like spoofing, jamming, flooding, and data injection.

Data Link Communication Concerns: Data links like Controller-Pilot Data Link Communications (CPDLC) and navigation aids (e.g., ILS, GBAS) face risks of failure or cyberattack.

Unclear Protection Plans: There are no clear publicly available plans for securing existing and future NextGen ATC systems.

FAA's Cybersecurity Efforts: The FAA's ATO Cybersecurity Group is responsible for security but has not clearly outlined how ATC systems will be protected.

Lack of Robustness in ATC Systems: Recent incidents suggest ATC systems may be vulnerable to accidental data corruption and signal jamming.

MITRE Corporation Involvement: MITRE and FAA have outlined the cyber architecture for National Airspace System (NAS) security, but no specific mention of protecting ATC systems.

Security in Unmanned Air traffic management system:

The global adoption of Unmanned Aerial Vehicles (UAVs) has significantly increased, especially for government and commercial applications such as traffic monitoring, criminal surveillance, search and rescue operations, and unmanned airstrikes. A 2019 report by Grand View Research projects that the UAV market will grow to $129.33 billion by 2025. The precision, efficiency, and reliability of UAV technology make it vital for the advancement of future technological societies [10].

However, the expanding use of UAVs also introduces heightened security and privacy concerns, as their wireless communication systems are vulnerable to cyberattacks. Attackers may intercept or manipulate data transmitted between UAVs and ground control stations. To address these risks, security solutions similar to those used in Mobile Ad Hoc Networks (MANETs) have been suggested for threat detection and mitigation. It is essential for UAV manufacturers to integrate these security measures into their systems. This paper explores the need for implementing security and privacy mechanisms or algorithms in UAV technologies [10].

Security requirements: The increasing presence of UAVs (Unmanned Aerial Vehicles) in the airspace introduces significant security and privacy risks. It is essential to protect UAV systems from unauthorized access, communication disruptions, and data tampering. Key security and privacy requirements for UAVs include ensuring the confidentiality of communications between UAVs and their base stations, such as flight plans and control commands, by using robust cryptographic methods. Data integrity must be maintained across the system through encryption to prevent unauthorized modifications. Availability is another critical factor, requiring UAV systems to remain functional and accessible to authorized users, which can be supported by deploying Intrusion Detection Systems (IDS) to guard against Denial of Service (DoS) attacks. Authenticity must be ensured by verifying the identities of users and UAV components through secure communication

protocols, while non-repudiation is necessary to hold users accountable for their actions during missions, preventing them from denying their involvement. Furthermore, authorization controls are required to restrict access based on user roles, and non-disclosure measures are needed to prevent the sharing of sensitive information with unauthorized entities [10].

III. ANALYZING VULNERABILITIES IN ATC

Historically, there have been a few incidents involving the malicious exploitation of air traffic control (ATC) communication technologies, which has contributed to a perception that security measures are unnecessary [11]. However, the availability of inexpensive tools like software-defined radios (SDRs) has eroded aviation's technical edge, making cyberattacks on ATC systems more feasible. Traditional threat model assumptions include Inferior technological capabilities, Inferior financial capabilities, Requirement of inside knowledge and Use of analog communication. Recent notable incidents, such as hijacked emergency signals and radar disruptions, have heightened concerns over air traffic security. While some experts argue that aviation's extensive checks and balances mitigate these risks, hackers and researchers have demonstrated vulnerabilities in modern ATC protocols and avionics systems [11].

In [11], the authors have outlined a modern threat model for aviation systems. Modern threat model assumption includes the following:

- Increased digitization and automation: Aviation is increasingly using unauthenticated digital communication, making attacks easier to execute and harder to detect, particularly on automated systems.
- Increased technological capabilities: Cheap software-defined radios (SDRs) are widely available, making wireless attacks accessible to a broad audience with minimal financial barriers.
- Easy availability of aviation knowledge: Attackers can access aviation communication protocols and procedures through public sources like forums, websites, and captured communication data [11].

Security considerations in wireless technologies used

The following section discusses the Wireless communication technologies used in ATC and their respective security considerations focusing on lack of knowledge among professionals in the aviation industry. ATC protocols enable communication between controllers and pilots or their aircraft. They establish information about the aircraft's position and intent and thus the safety of the airspace [11].

Voice VHF:

Voice communication is carried out using analog radio on VHF for most areas and HF when beyond VHF range, such as over oceans. It serves as the primary method of communication between air traffic control (ATC) and aircraft.

Security considerations: The success of VHF (Very High Frequency) communication hinges on clear message understanding between parties, factoring in human elements and ensuring signal quality. However, simultaneous frequency use can result in partial or complete denial of service (DoS). Although VHF uses amplitude modulation (AM), which allows multiple channel reception, it struggles against intentional interference. Military flights have authentication protocols, but these are time-consuming and not applied to civil flights. Without CPDLC (Controller-Pilot Data Link Communications) in most areas or in unequipped aircraft, there is no backup for VHF, which poses significant risks in crowded airspaces. VHF is perceived as the least trusted communication protocol. Many experts have encountered unauthorized uses of VHF, with some citing its vulnerability to malicious emulation or pirate radio interference. While intruders are usually detected through signal changes, only 30-40% of VHF users believe it has integrity and authenticity checks. Additionally, attackers could disable VHF by jamming it, forcing reliance on less-secure backup systems like unauthenticated CPDLC data links [11].

Controller Pilot Data Link Communications (CPDLC):

CPDLC is a messaging service that provides an alternative to voice communication between air traffic control (ATC) and pilots. Through a terminal, ATC can use CPDLC to send clearances or requests.

Security Considerations: Compared to VHF, relying on unauthenticated data links, such as CPDLC, presents a greater security risk because attacks are harder to detect without voice recognition. Less than 10% of respondents are aware that CPDLC is not authenticated, despite future plans to rely more heavily on it. Many respondents incorrectly believe CPDLC offers security. Attacks on its availability are less concerning since it currently serves as a secondary communication layer, but undetected protocol attacks, such as message manipulation, are severe. Without authentication, it is easy to eavesdrop, spoof, or alter messages, allowing attackers to impersonate air traffic control (ATC) units and issue dangerous instructions to pilots, potentially leading to unsafe maneuvers or unnecessary inquiries from ATC [11].

Primary Surveillance Radar (PSR):

Primary Surveillance Radar (PSR) is a non-cooperative system for aircraft localization that relies on radar technology. It typically uses a rotating antenna that emits a highly directional, pulse-position-modulated electromagnetic beam in the low GHz frequency range. Reflected pulses from targets are analyzed to determine their position based on bearing and round-trip time.

Security Considerations: PSR (Primary Surveillance Radar) systems, which use signal-based detection, are not vulnerable to protocol attacks like message injection. However, they can be jammed, although the power requirements make this more feasible for military electronic warfare. Missing PSR data from jamming typically doesn't affect controllers, as key target information (position, identification, altitude) is provided separately, which may explain why nearly 60% of controllers mistakenly believe PSR has integrity checks. While military PSR includes security features like frequency hopping, these are not available in civil aviation. PSR may also be vulnerable to time-based attacks, such as GPS manipulation, but overall, it remains relatively secure compared to other technologies. However, as PSR is phased out in favor of newer data communication protocols and satellite systems, long-term security may decline due to increased reliance on unauthenticated technologies [11].

Secondary Surveillance Radar (SSR):

The transponder modes A, C, and S (collectively referred to as Mode A/C/S) are components of Secondary Surveillance Radar (SSR). This cooperative technology enhances ATC radar by providing additional target information, whereas PSR only identifies target positions without any supplementary data.

Security considerations: With the availability of Mode S software-defined radio (SDR) implementations online, attackers can manipulate, jam, or inject Mode A/C/S messages, distorting the airspace view for air traffic control (ATC). Mode S messages, carrying aircraft identifiers, can be spoofed using trusted IDs to avoid detection. Emergency codes like 7500 (hijacking) can be injected, causing confusion at busy ATC stations. As Mode S is the sole information source for ATC radar, any tampering or jamming poses a severe threat, with no backup systems in place. Alarmingly, over 40% of respondents, including 60% of controllers, mistakenly believe Mode S has built-in security. Mode S is also vulnerable to amplification attacks, where an attacker exploits interrogations to cause large-scale interference on the 1090 MHz channel, leading to a denial of service (DoS) as important data is lost. Aircraft transponders can overheat due to excessive interrogations, causing a complete loss of targets on ATC displays, exacerbating the DoS threat [11].

Automatic Dependent Surveillance - Broadcast

(ADS-B): The ADS-B protocol is used by aircraft to continually broadcast their own ID, position and velocity as well as further information such as intent or urgency codes. These broadcasts happen twice a second in case of position and velocity, and once every 5 seconds for identification.

Security Considerations: The ADS-B 1090 Extended Squitter (1090ES) data link, based on unauthenticated Mode S, is vulnerable to both passive and active attacks. For instance, an attacker can selectively jam an aircraft's ADS-B messages, making it disappear from the ADS-B channel. This is easier than jamming Mode S, as ADS-B broadcasts more frequently and predictably. Additionally, ADS-B broadcasts aircraft positions, enabling new attack vectors using easily available hardware. Attackers can inject fake ADS-B messages or modify an aircraft's trajectory by jamming its messages and sending altered data, creating discrepancies in its position as seen by ATC. Given that ADS-B is intended to be the primary ATC protocol, with the FAA considering phasing out Mode A/C/S transponders, these vulnerabilities are concerning. Yet, fewer than 20% of pilots and controllers are aware of these risks [11].

Multilateration (MLAT):

It determines the position of an aircraft by measuring the time differences in signal arrival at multiple receivers. MLAT is not a standalone protocol but works with existing systems like Secondary Surveillance Radar (SSR) or ADS-B

Security considerations: In theory, Multilateration (MLAT) offers a security advantage because it operates at the signal level, independent of message content. This allows MLAT to identify the sender's location even if the message, such as an ADS-B signal, is compromised. The technique leverages physical properties like the speed of electromagnetic wave propagation, which are difficult to manipulate. However, in practice, MLAT systems often rely on combining signal-based location data with message content (e.g., identification and altitude from SSR), leaving the system vulnerable to compromised messages. Moreover, an avid attacker can modify the time of signal arrival at MLAT receivers to generate a false location. Though more receivers reduce attack feasibility, such attacks are still possible. Despite being a favored backup for SSR, MLAT is expensive to implement and prone to issues like multipath signal interference, limiting its widespread use [11].

IV. SECURITY ATTACKS ON ATC.

With terrorist and organized crime groups showing increased interest in targeting Air Traffic Control (ATC) systems, various vulnerabilities and attack vectors have emerged, particularly with wireless ATC technology, which is inherently unsafe.

Categories of attackers

Outsider Threat: This attacker has access to commercially available software-defined radios (SDRs) and can launch ground-based attacks such as injecting, altering, or jamming transponder signals. They may attack from multiple locations but lack perfect synchronization and coordination [13].

Insider Threat: This attacker impersonates a legitimate participant in a crowdsourcing system to insert false data into the network. The primary focus is on moderately resourced attackers who can launch these attacks from one or multiple ground-based locations [13].

The following sections provide an overview of modern ATC technology, vulnerabilities, and potential wireless attacks.

A. Modern ATC Technologies

Secondary Surveillance Radar (SSR): SSR is a cooperative ATC technology that provides digital target information via transponder modes A, C, and S. Aircraft respond to interrogations on 1030 MHz by returning data on 1090 MHz, which contains altitude, identity, and other information.

Automatic Dependent Surveillance-Broadcast (ADS-B): This technology enables aircraft to broadcast their position, velocity, and additional data (such as status and emergency codes) twice per second without being interrogated by ground control. However, ADS-B lacks cryptographic protection, making it vulnerable to cyberattacks.

Both SSR and ADS-B were designed without security considerations, allowing attackers to manipulate the airspace picture [13].

B. Wireless Attack Vectors Against the ATC Infrastructure

Since SSR and ADS-B are wireless, they are susceptible to attackers using easily available hardware. Common attack vectors include:

Injection of Ghost Aircraft: Attackers can create fake airplanes that appear legitimate by crafting transponder signals with plausible flying parameters. This can overwhelm air traffic controllers, possibly leading to a loss of situational awareness or even accidents.

Label Modification: Attackers can change the identity, altitude, and velocity of genuine aircraft on the ATC radar screen, jeopardizing airspace safety.

Jamming or Denial of Service (DoS): Attackers can jam the frequencies utilized by ATC systems, disrupting communication and potentially causing radar screens to go blank. Jamming can be indiscriminate (affecting all signals) or targeted (affecting only certain aircraft signals) [13].

C. Crowdsourced Security Methods for ATC

OpenSky: The OpenSky Network is a crowdsourced system that collects data from a global network of sensors to improve ATC security. It is composed of both registered and anonymous sensors, with registered sensors operated by known community members and anonymous sensors operated by unknown individuals. OpenSky continuously verifies the trustworthiness of sensor data by comparing it with data from trusted sensors, ensuring reliable information is used for air traffic monitoring. An OpenSky-based crowdsourced security system detects attacks on ATC protocols using data from multiple sources [13]. To identify suspicious activity, the system applies four independent approaches, each with its own sensor requirements and complexities:

Plausibility Checks: Simple rules are employed to determine the validity of received flight data. These checks include an aircraft position outside sensor range, sudden appearances in the region, messages not following standard technical rules, and aircraft reporting unrealistic speeds, altitudes, or incorrect model details [13]**.**

Cross-Referencing Data: If multiple sensors cover the same area, their data is compared. Any anomalies, such as differing information from the same aircraft or one sensor failing to receive data while others do, raise concerns about a potential attack [13].

Multilateration: This method uses data from three or more sensors to calculate the source of an aircraft's signal and verify its location. This technique not only confirms an aircraft's position but can also help identify the attacker's location [13]**.**

Statistical Analysis: In areas with limited sensor coverage, statistical methods are used to detect anomalies in signal arrival times. A statistical test checks if the received signal matches expected patterns, immediately identifying possible attacks [13].

TABLE 1: OVERVIEW OF CROWDSOURCED ATTACK DETECTION METHODS

Method	Number of Receivers	Complexity	Attack Localisation
Plausibility Checks	1	Low	No
Cross Referencing	2 or more	Low	No
Multilateration	3 or more	High	Yes
Statistical Analysis	2 or more	Moderate	No

Attack Handling with OpenSky

If an anomaly is identified, the aircraft's track may be reported as unreliable and further inspected. Abnormal messages are deleted and removed from the radar display, protecting controllers from being overwhelmed with false data. If sufficient receiver data is available, the system can pinpoint the source of the attack for further investigation [13].

Security Analysis: There are **two** types of attacks: outsider attacks and insider attacks.

i) Outsider Attacks on Real-World ATC

Jamming Attacks: These can be either indiscriminate (affecting all planes) or targeted (affecting specific aircraft). The crowdsourced sensor network detects these threats by analyzing data from overlapping sensors [13].

Injection Attacks: Attackers can inject ghost aircraft into the radar system. Multiple sensors in the crowdsourcing network can detect these false signals using cross-referencing and multilateration techniques [13].

Modification Attacks: Attackers can alter the data transmitted by genuine aircraft. For example, transmitting at higher strength can obscure the aircraft's actual message. Crowd-sourced sensors can identify such changes by comparing data from multiple sources [13].

ii) Insider Attacks on OpenSky

Single Sensor Data Manipulation: A rogue sensor may feed incorrect data into the system, either after gaining trust or by hijacking a trustworthy sensor. Redundant sensor coverage allows the system to detect such manipulation by comparing data from several sensors [13].

Sybil Attacks: In this complex attack, the adversary controls multiple sensors to flood the legitimate network with false data. This is mitigated by monitoring irregular sensor behavior and using trust-based security layers [13].

V. IMPACT OF ATTACKS ON ATC

Cyberattacks on ATC systems can lead to severe consequences, threatening aviation safety, disrupting operations, causing economic losses, damaging reputations, and resulting in regulatory challenges. Below is an in-depth exploration of these impacts along with references to support the information.

1. Safety Risks

ATC systems play a crucial role in maintaining safe distances between aircraft, ensuring accurate navigation, and coordinating emergency responses. Cyberattacks on these systems can lead to the following [11].

Loss of Aircraft control

Loss of Aircraft control or Separation from ATC poses a significant threat to aviation safety, stemming from communication disruptions, data corruption, or malicious cyber activities. Such issues reduce air traffic controllers' ability to monitor and manage aircraft effectively, increasing the chances of mid-air collisions or close calls [11].

One notable risk is cyberattacks targeting Automatic Dependent Surveillance-Broadcast (ADS-B) systems. These attacks can insert false data into air traffic systems, creating "ghost aircraft" that appear on radar screens. These phantom targets confuse controllers, forcing them to divert attention from real aircraft and complicating airspace management. This misdirection may lead to unnecessary course changes, increased pilot-controller workloads, and disruptions in flight operations [11].

Another concern is interference with communication systems. Jamming or signal obstruction can prevent timely exchanges between pilots and controllers, making it difficult to relay critical instructions. This problem is especially dangerous in crowded airspace or challenging weather, where precise coordination is vital to maintaining safe distances between aircraft [11].

Data inaccuracies in navigation and surveillance systems also heighten the risk of separation loss. Delayed or incorrect position information from onboard systems can lead to flawed flight path representations, prompting controllers to issue potentially unsafe instructions. The reliance on digital systems, including satellite-based navigation, further exposes aviation to cyber threats that may compromise system reliability [11].

The increasing presence of unmanned aerial vehicles (UAVs) adds complexity. Unauthorized drones or compromised UAVs can disrupt traffic flow, forcing deviations from planned routes and jeopardizing the safe separation of aircraft [11].

Countermeasure: Addressing these challenges requires comprehensive measures. Implementing stronger cybersecurity protocols, enhancing system redundancies, and training air traffic controllers to recognize and handle potential cyber threats are essential steps. Additionally, fostering international cooperation to develop secure aviation standards and protocols will help counter evolving threats and maintain the integrity of aircraft separation systems [11].

Navigation Errors

Manipulation of navigation systems like Global Positioning Systems (GPS) or Instrument Landing Systems (ILS) can have severe repercussions for aviation safety. These systems are vital for ensuring that aircraft maintain their designated flight paths and approach patterns, especially in challenging environments or poor visibility conditions. Any compromise in their accuracy or reliability can result in deviations that increase the risk of conflicts, near misses, or accidents [14].

One critical vulnerability is GPS spoofing, where false signals are transmitted to deceive an aircraft's navigation system. Such attacks can lead to the aircraft straying off its planned route without the crew's awareness. This unintentional deviation not only disrupts air traffic flow but also creates potential mid-air collision scenarios in busy airspace or near restricted zones [14].

Similarly, disruptions to ILS, which provides critical guidance during landing approaches, can have catastrophic consequences. For instance, deliberate interference with ILS signals could mislead pilots about their approach angle or alignment with the runway. This could result in hard landings, runway overruns, or even crashes, particularly in low-visibility conditions where pilots rely heavily on instruments [14].

Another factor exacerbating navigation errors is the reliance on digital data streams for en-route guidance and terminal area operations. Cyberattacks targeting these streams, such as data tampering or denial-of-service (DoS) attacks, can compromise the situational awareness of both pilots and air traffic controllers. In extreme cases, such disruptions could necessitate emergency evasive actions, increasing stress and workload for the flight crew. Attacks on communication channels or data integrity may hinder effective emergency responses, prolonging crises and putting lives at greater risk [14].

Countermeasure: Encryption and authentication of navigation signals can reduce the likelihood of spoofing or interference. Additionally, integrating backup systems, such as inertial navigation systems, can provide resilience in the event of primary system failure. Regular testing and validation of navigation infrastructure, along with increased pilot training to recognize and respond to anomalous navigation inputs, are also crucial [14].

2. Operational Disruptions

Cyber incidents disrupt the smooth functioning of ATC operations, causing either or all of the following.

Flight Delays and Cancellations: System outages caused by ransomware attacks or denial-of-service (DoS) incidents can have widespread impacts on airport operations, often necessitating the grounding of flights and leading to extensive delays. For instance, a significant cyberattack in 2024 targeted Seattle-Tacoma International Airport, disrupting systems for several days and resulting in prolonged flight delays. Such incidents highlight the vulnerability of critical aviation infrastructure to cyber threats. When operational systems are compromised, airlines and airports face challenges in managing schedules, passenger rebooking, and logistics, exacerbating passenger dissatisfaction and economic losses [14].

Airspace Closures: Cyber threats targeting Air Traffic Control (ATC) systems can lead to the temporary closure of affected airspace, creating a ripple effect of operational inefficiencies. When ATC systems are compromised, rerouting aircraft becomes a necessity, often resulting in congestion in neighboring airspace sectors. These diversions increase fuel consumption and extend flight durations, significantly raising operational costs for airlines. The resulting congestion can also overwhelm controllers in unaffected sectors, increasing the risk of errors [12].

Communication Failures: Attacks on communication protocols like Controller-Pilot Data Link Communication (CPDLC) pose significant risks to the seamless functioning of aviation operations. CPDLC is vital for exchanging critical instructions between pilots and air traffic controllers, especially in high-traffic or remote regions. A successful cyberattack targeting CPDLC could lead to miscommunication or a complete breakdown in communication. This loss can create confusion for flight crews, delay responses to dynamic air traffic situations, and potentially compromise flight safety [12].

3. Economic Consequences

Cyberattacks on ATC systems impose substantial financial burdens. This section discusses such impacts.

Airline Revenue Losses: Flight cancellations and delays lead to substantial revenue losses for airlines, including decreased ticket sales, higher compensation payouts, and logistical inefficiencies. A 2024 global IT outage caused by a cybersecurity update disruption severely impacted

aviation services, leaving airlines with hefty operational costs [15].

Airport Operational Costs: Airports face increased financial strain during disruptions, with extended operational hours, additional security protocols, and rising labor costs to manage passenger flows. These measures aim to maintain functionality but significantly inflate day-to-day expenditures [15].

Broader Economic Impact: Delays and cancellations ripple through the economy, disrupting cargo logistics, hindering business travel, and affecting tourism-dependent industries. The cumulative effect slows economic activity and reduces productivity in interconnected sectors reliant on timely transportation [15].

4. Reputational Damage

Repeated or severe cyber incidents can erode trust in aviation systems. Cyberattacks that compromise safety or operational reliability may lead to reduced passenger confidence in flying, potentially decreasing air travel demand [12]. Airlines and ATC authorities suffering frequent breaches may gain a reputation for being unprepared, damaging their market position.

5. Regulatory and Legal Implications

Cyber incidents bring increased scrutiny and potential legal repercussions. Authorities may impose penalties on organizations failing to implement adequate cybersecurity measures.
Cyber incidents often lead to the introduction of stricter standards and audits for ATC and airline operations. The U.S. Government Accountability Office (GAO) has consistently evaluated FAA's cybersecurity efforts, emphasizing the need for robust protection of internet-connected systems [16].

Recent Incidents of Cyber Attacks on ATC:

Seattle-Tacoma International Airport Cyber Attack (2024): In 2024, a cyberattack targeting Seattle-Tacoma International Airport led to widespread flight delays and baggage handling disruptions that persisted for several days. This incident exposed critical vulnerabilities in the airport's IT systems, affecting not only passenger services but also the coordination of flight schedules. The attack underscored the aviation sector's growing dependence on digital infrastructure and the urgent need for robust cybersecurity strategies to prevent such disruptions in the future. It also highlighted the potential cascading effects on airlines, passengers, and neighboring airports, emphasizing the importance of coordinated response mechanisms [14].

Global IT Outage (July 2024): In July 2024, a faulty update from a prominent cybersecurity firm triggered widespread disruptions across aviation, banking, and healthcare sectors. The outage affected airport operations globally, causing flight delays, cancellations, and logistical chaos. This incident highlighted the interconnected nature and inherent fragility of modern digital systems, emphasizing the critical need for rigorous testing and fail-safes in cybersecurity updates. It also underscored the importance of cross-sector collaboration to mitigate cascading failures in critical infrastructure [15].

File corruption in the National Airspace System (NAS): In January 2023, an outage in the FAA's Notice to Air Missions (NOTAM) system grounded aircraft across the National Airspace System (NAS). Although no cyberattack was found, the issue was caused by accidental database file corruption, which can also result from cyberattacks. This incident highlighted the ATC system's reliance on cyber functionality and the potential cascading effects of disruptions [12]. Additionally, GPS jamming incidents have disrupted ATC systems, including a 33-hour disruption at Denver International Airport and a 44-hour disruption at Dallas-Fort Worth (DFW) International Airport. In Denver, pilots reported issues with GPS, TCAS, and other systems, while at DFW, flights were rerouted, and the jamming source remains unknown [12].

VI. IMPROVEMENT SCOPE OF CYBER-PHYSICAL SECURITY IN ATCs

Crew based cybersecurity in ATC

A robust approach to cybersecurity in air traffic control (ATC) systems requires enhancing awareness, education, and training for both pilots and air traffic controllers (ATCOs), who operate systems that are increasingly vulnerable to cyberattacks. Despite their responsibility for critical aviation assets, many crew members lack fundamental cybersecurity knowledge. Some in the industry argue that adding cybersecurity duties to already demanding roles is unnecessary, but the expanding threat landscape makes comprehensive training essential to help crew members manage both their primary responsibilities and potential cyber threats [12].

Currently, advisory systems inform pilots of system failures requiring action but do not provide explanations, particularly in cases involving cyberattacks. Pilots have expressed a desire for more control over cybersecurity incidents during flights, emphasizing the need for better training. Research indicates that some pilots struggle to identify cyberattacks, such as GPS spoofing, during simulations, highlighting gaps in their preparedness. To address these challenges, industry is starting to develop tools like onboard intrusion detection systems to assist pilots in responding to cyber threats [12].

Air traffic controllers face even greater obstacles, as they receive no specialized training or tools to handle cyber incidents. Cyberattacks can compromise ATCOs' situational awareness, increase their workload, and reduce their trust in systems. However, current ATCO training programs lack any focus on cybersecurity. The paper advocates for incorporating cybersecurity scenarios into ATCO training to enhance their ability to detect and respond to attacks [12].

To build resilience, it is crucial to integrate cybersecurity with crew autonomy and cyber-physical security measures. Introducing cyber situational awareness tools and incorporating cyberattack scenarios into training programs would significantly enhance system security. Leveraging existing ATC simulators that replicate cyberattack scenarios can increase awareness and assess ATCO readiness, ultimately strengthening their response to potential threats [12].

Using Machine Learning in ATC Cybersecurity

Recent research has focused on using machine learning (ML) techniques to detect attacks on Automatic Dependent Surveillance-Broadcast (ADS-B) systems. Models such as Long-Short Term Memory (LSTM), Deep Neural Networks (DNN), Logistic Regression, Naïve Bayes, and K-Nearest Neighbor (KNN) have been explored for this purpose. However, these approaches often require extensive datasets, significant computational resources, and longer processing times. Due to these challenges, the Kalman Filter has emerged as a more efficient alternative, offering benefits like reduced data requirements, lower computational overhead, and faster processing [12].

In the aviation sector, particularly within Air Traffic Control (ATC) systems, time-critical responses are crucial. Air Traffic Control Officers (ATCOs) rely on precise and timely information for effective situational awareness, decision-making, and communication. The Kalman Filter addresses this need by rapidly providing threat intelligence from ADS-B data. Moreover, its compatibility with various devices—including desktops, laptops, tablets, and mobile phones—enhances mobility, making it a practical tool for both ATCOs and pilots. This flexibility allows for ADS-B data analysis on mobile platforms. A long-term objective is to integrate this lightweight solution into platforms like the Electronic Flight Bag (EFB), which receives ADS-B data in real-time [12].

Improvements with AI

The following are potential areas for improvement in Air Traffic Control (ATC) security using AI:

Enhanced system robustness AI Techniques: In air traffic control (ATC) systems, efficiently managing large volumes of data is crucial. Traditional tuning of data frameworks uses a lot of time. Use of AI can help enhance the system robustness and efficiency in ATC. AI-driven auto-tuning using Generative Adversarial Networks (GANs) streamline this process. GANs involve two competing neural networks – a generator that creates various configurations and a discriminator that evaluates them. Through continuous iteration, GANs identify optimal settings, reducing tuning time and resource use, thereby allowing faster data processing and more responsive air traffic management, which is essential for safety and flow control [18].

Enhanced system stability and safety with AI-drive predictions and ML models: To ensure system stability under N-1 security conditions, installing Thyristor-Controlled Series Capacitors (TCSC) strategically at optimal locations in power systems enhances available transfer capability. Evolutionary algorithms help identify the best locations for TCSC installation, leading to improved transmission efficiency and system reliability [19].

Increasing system safety and efficiency is possible through AI-driven predictive analytics for weather, delay forecasting, and traffic management which are among the enhancements to ATC systems. Automation enhances decision-making, conflict resolution, and situational awareness, reducing controller workload. Furthermore, auto-tuning with GANs optimizes data handling, while TCSC deployments improve system robustness, resulting in safer and more efficient air traffic management [17] [18] [19].

AI can significantly improve weather forecasting and predict its impact on air traffic, enabling proactive rerouting to minimize delays and enhance safety. Machine learning models can predict flight delays, allowing ATC to optimize schedules and manage resources, especially during adverse weather conditions [17].

Conflict Detection and Resolution with AI: AI enables real-time detection of anomalies, increasing safety by identifying unusual aircraft behavior. Additionally, AI can autonomously detect and resolve conflicts in aircraft trajectories, reducing the need for manual intervention and enhancing response efficiency [17].

Air Traffic Flow Management (ATFM) with AI capabilities and ML models: AI-driven ATFM adapts traffic flow based on real-time conditions, leading to increased efficiency and reduced congestion. Machine learning models forecast traffic density, improving airspace management and minimizing delays during peak traffic [17].

AI analyzes aircraft density and flow, helping controllers manage congested airspaces. AI systems estimate airspace demand and capacity, allowing ATC to adjust flight paths or impose traffic limits to ensure safety. AI assists in emergency response by analyzing real-time data and suggesting actions based on historical incident responses [17].

AI provides data-driven insights and alternative solutions, supporting controllers in making complex decisions under various air traffic conditions. AI-based algorithms optimize scheduling, runway usage, and aircraft movements, reducing operational delays and improving overall efficiency [17].

Human-Machine Interface (HMI) Enhancements: Cognitive Human-Machine interfaces support controllers by providing predictive insights and assisting with routine tasks, reducing their workload. Explainable AI (XAI) approaches increase controllers' confidence in AI-driven recommendations by offering transparency, helping them make informed decisions [17].

Security Techniques to safeguard UAV systems

To safeguard Unmanned Aerial Vehicle (UAV) systems from unauthorized access, several advanced security techniques can be utilized. Intrusion Detection Systems (IDS) can monitor network traffic for suspicious activities, while Symmetric Key Encryption can protect communications from interception. Physical Unclonable Functions (PUF) create unique device identifiers for secure authentication, and Blockchain technology offers decentralized, tamper-resistant ledgers to verify transactions. Elliptic Curve Cryptography (ECC) provides robust public key encryption with smaller key sizes, and Digital Signatures are used to confirm the authenticity of transmitted messages. Homomorphic Encryption enables computations on encrypted data without needing decryption, ensuring privacy, especially in cloud services. Secure Hash Algorithms (SHA) generate compact, secure data hashes, while Hyperelliptic Curve Cryptography (HECC) extends ECC capabilities for enhanced confidentiality. Anonymous Batch Authentication (ABA) allows simultaneous authentication of multiple requests, and Federated Learning ensures privacy by processing data locally on edge devices rather than centrally. Finally, the Chinese Remainder Theorem (CRT) is used for efficient computation of large integers, aiding secure data management in UAV systems [10].

VII. FUTURE SCOPE and STRATEGIES

Kalman filter: To ensure resilience, integrating cybersecurity with crew autonomy and cyber-physical security is crucial. Introducing cyber situational awareness tools and cyberattack scenarios into training would strengthen system security [12]. Using existing ATC simulators that mimic cyberattacks can raise awareness and evaluate ATCO readiness, the study in [12] offers insights into how threats impact decision-making and situational awareness.

In [12] authors have worked on the use of Machine Learning to detect attacks on ATC systems. Recent studies explore machine learning (ML) based systems to detect Automatic Dependent Surveillance-Broadcast (ADS-B) attacks, utilizing models like Long-Short Term Memory (LSTM), Deep Neural Network (DNN), Logistic Regression, Naïve Bayes, and K-Nearest Neighbor (KNN). However, these models require large datasets, substantial resources, and longer computation times. These limitations led to the adoption of the Kalman Filter, which offers advantages in terms of reduced data requirements, lower overhead, and faster computation. In the Aviation domain, time-criticality is essential, especially for Air Traffic Control (ATC) systems. Air Traffic Control Officers (ATCOs) need accurate and timely information for situational analysis, decision-making, and communication. The Kalman Filter meets this demand by providing rapid threat intelligence related to ADS-B data. Additionally, the Kalman Filter's performance across platforms, such as desktops, laptops, tablets, and mobile phones, enhances mobility. This makes it a viable tool not only for ATCOs but also for pilots, enabling them to analyze ADS-B data on mobile devices. A future goal is to integrate this lightweight system into platforms like the Electronic Flight Bag (EFB), which receives ADS-B data [12].

Potential areas of future research

Divergence between crew state awareness and the actual system state is a known safety risk in the National Airspace System (NAS). Researchers should explore vulnerabilities in crew awareness under cyber threat scenarios, both with and without the use of a Kalman-Filter (KL)-based cyber aid, aiming to eliminate divergence and its hazardous consequences. Studying crew reactions will provide insights into failures in perception and state projection, improving system design. Multi-agent divergence, such as inconsistencies between pilot and Air Traffic Control Officer (ATCO) awareness, should also be addressed [12].

A key requirement for the cyber aid is ease of use and seamless integration into crew procedures. The intelligence added to the Air Traffic Control (ATC) display must be intuitive, helping crews manage emerging situations, such as alerting them to the physical impact of cyberattacks or malfunctioning devices. The design must minimize nuisance alerts, which can reduce crew attention and lead to serious consequences [12].

Human factors research will be crucial in developing cyber aid. Future studies should assess its usability and functionality in both lab and operational environments, evaluating crew responses to alerts and addressing subjective factors like nuisance alerts. This feedback will refine the algorithms and improve the ATC crew display interface [12].

VIII. CONCLUSION

The security of Air Traffic Control (ATC) systems is paramount to the safety and reliability of global air travel, yet these systems face mounting cybersecurity challenges as they transition from isolated, traditional structures to interconnected, digital frameworks. This paper has consolidated the work of various authors and explored the cybersecurity and cyberphysical risks in ATC, analyzing vulnerabilities in communication protocols, surveillance systems, and automated processes as well as physical functionalities. Through experimental insights, it is evident that ATC systems are susceptible to various cyber as well as physical threats, such as signal interference, data falsification, and denial-of-service attacks, which can compromise flight safety, disrupt operations, and lead to significant economic and reputational consequences.

To address these threats, it is essential for ATC stakeholders to implement robust security protocols, including encryption, machine learning-based threat detection, physical defenses and comprehensive cybersecurity training. Future ATC resilience also depends on integrating advanced technologies such as AI for anomaly detection and real-time response mechanisms. By fostering collaboration between aviation and cybersecurity experts, the industry can build an integrated defense framework, fortifying ATC systems against evolving cyber threats and ensuring the ongoing safety and integrity of global air traffic management.

VIII. REFERENCES

[1] ‘Airline Industry - Passenger Traffic Worldwide 2024’. Statista, https://www.statista.com/statistics/564717/airline-industry-passenger-traffic-globally/ . Accessed 22 Oct. 2024.

[2] Government of Canada, Statistics Canada. *Airport Activity: Air Carrier Traffic at Canadian Airports, 2023*. 4 July 2024, https://www150.statcan.gc.ca/n1/pub/51-004-x/51-004-x2024001-eng.htm.

[3] Federal Aviation Administration, "NextGen," [Online]. Available: https://www.faa.gov/nextgen. Accessed: Oct. 22, 2024.

[4] Ali, B.S. (2018). Aircraft Surveillance Systems: Radar Limitations and the Advent of the Automatic Dependent Surveillance Broadcast (1st ed.). Routledge. https://doi.org/10.4324/9781315566382

[5] *Automatic Dependent Surveillance-Broadcast (ADS-B) | Federal Aviation Administration*. https://www.faa.gov/air_traffic/technology/adsb. Accessed Oct 22, 2024.

[6] International Civil Aviation Organization, "Overview of ADS-B Out," presented at ADS-B Implementation Meeting, 2021. [Online]. Available: https://www.icao.int/NACC/Documents/Meetings/2021/ADSB/P01-OverviewADSBOut-ENG.pdf

[7] Federal Aviation Administration, "ADS-B Out Explained," FAA Safety Team. [Online]. Available: https://www.faasafety.gov/files/events/SO/SO15/2024/SO15132063/ADS-B_Out_Explained.pdf

[8] Z. Wu, T. Shang and A. Guo, "Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey," in IEEE Access, vol. 8, pp. 122147-122167, 2020, doi: 10.1109/ACCESS.2020.3007182

[9] Introduction to ADS-B," Civil Aviation Authority of New Zealand, 2023. [Online]. Available: https://ads-b.aviation.govt.nz/introduction/#how-does-ads-b-work

[10] Agarwal, Piyush, et al. Security Techniques in Unmanned Air Traffic Management System’. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 2023, pp. 641–46. IEEE Xplore, https://doi.org/10.1109/ICSSIT55814.2023.10061115.

[11] Strohmeier, Martin, et al. ‘On Perception and Reality in Wireless Air Traffic Communication Security’. IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 6, June 2017, pp. 1338–57. IEEE Xplore, https://doi.org/10.1109/TITS.2016.2612584.

[12] Atkins, Garett, and Krishna Sampigethaya. ‘Air Traffic Control System Cyber Security Using Humans and Machine Learning’. 2023 Integrated Communication, Navigation and Surveillance Conference (ICNS), 2023, pp. 1–14. IEEE Xplore, https://doi.org/10.1109/ICNS58246.2023.10124305

[13] M. Strohmeier, M. Smith, Matthias Schäfer, V. Lenders, and I. Martinovic, “Crowdsourcing security for wireless air traffic communications,” May 2017, doi: https://doi.org/10.23919/cycon.2017.8240336.

[14] **Lovett**, "Seattle-Tacoma Airport deals with delays five days after detecting cyberattack," *The Wall Street Journal*, Nov. 20, 2024. [Online]. Available: https://www.wsj.com/articles/seattle-tacoma-airport-deals-with-delays-five-days-after-detecting-cyberattack-957c149c. [Accessed: Nov. 22, 2024].

[15] *Worldwide Computer Breakdown: Airports, Banks and Hospitals Disrupted by the Biggest Computer Failure in History*. 19 July 2024. *Le Monde*, https://www.lemonde.fr/en/pixels/article/2024/07/19/airports-banks-and-hospitals-disrupted-by-biggest-it-outage-in-history_6690699_13.html.

[16] Office, U. S. Government Accountability. *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks | U.S. GAO*. 9 Oct. 2020, https://www.gao.gov/products/gao-21-86.

[17] Risya Emha Abdillah, H. Moenaf, Luthfi Fadullah Rasyid, Said Achmad, and Rhio Sutoyo, “Implementation of Artificial Intelligence on Air Traffic Control - A Systematic Literature Review,” Jan. 2024, doi: https://doi.org/10.1109/imcom60618.2024.10418350.

[18] Li, Mingyu, et al. ‘ATCS: Auto-Tuning Configurations of Big Data Frameworks Based on Generative Adversarial Nets’. IEEE Access, vol. 8, 2020, pp. 50485–96. IEEE Xplore, https://doi.org/10.1109/ACCESS.2020.2979812.

[19] W. Tang, W. Pan, K. Zhang, and C. Liu, “Study of the location of TCSC for improving ATC considering N-1 security constraints,” May 2014, doi: https://doi.org/10.1109/ccdc.2014.6852526.