6G for Connected Sky
“6G-SKY”

Work Package 1:

Holistic Adaptive Combined Airspace and NTN networks Architecture for 6G

Deliverable D1.4: Safety and Security

6G-SKY Project:

- 2024-05-29
- Rev A (v1.3)

Abstract

D1.4 Safety and Security intends to provide an overview of safety and cybersecurity issues in 6G as related to flying User Equipment in combined Airspace and NTN networks (combined ASN networks). In addition to putting 6G-SKY into a 6G cybersecurity context, and establishing the state-of-the-art in aviation and cybersecurity, the deliverable focuses on the most prominent threat that plagues real-world deployed non-terrestrial communication systems utilizing no encryption, no authentication, and no integrity protection; attack vectors against widely used protocols such as ADS-B and GNSS are analyzed. The deliverable also proposes a novel integrated air traffic management system incorporating the detection and localization of unauthenticated drones constructing a single-source picture of the sky for the safety of dense urban air traffic. Finally, the document describes a safety-security co-evaluation methodology fit for the combined ASN with its flying UEs and conducts a preliminary safety-security co-analysis using the proposed urban air traffic management system as a use case. The analysis, even with a significantly simplified system model, effectively points out the importance of the co-design mindset for networked cyber-physical systems.

Participants in WP 1:

6G-SKY, Work Package 1: Holistic Adaptive Combined Airspace and NTN networks Architecture for 6G

Task 1.6: Safety and security for flying UEs

D1.4 Safety and Security
Editor: Gergely Biczók, AITIA
Reviewer:

- Airbus and Fraunhofer (main 6G-SKY reviewers),
- All partners also contributed to the review process

Contributors: See list of authors

6G-SKY: D1.4 Safety and Security

- Editor: Gergely Biczók, AITIA
- Project coordinator: Dominic Schupke, Airbus
- Technical Project Coordinator: Cicek Cavdar, KTH
- CELTIC published project result

Ericsson AB	Ericsson Hungary
Ericsson Antenna Systems	Airbus
KTH	PTS
SAS	Deutsche Telecom
Fraunhofer	Lakeside Labs
RED Bernard	Logistik Center Austria Süd
AITIA	TWINS
Meshmerize	Skysense
Motius	

Document History

Version	Date	Author(s)/Reviewer	Comment
v0.1	2023-12-07	Gergely Biczók, AITIA	
v0.2	2024-02-23	Gergely Biczók, AITIA András Gazdag, AITIA	
v1.0	2024-04-15	Gergely Biczók, AITIA András Gazdag, AITIA Peng Wang, Skysense Robby de Candido, Skysense	
V1.1	2024-04-19	Nunzio Sciametta, Airbus (review) Gergely Biczók, AITIA (corrections) András Gazdag, AITIA (corrections)	
V1.2	2024-05-03	Dominic Schupke, Airbus (review) Gergely Biczók, AITIA (corrections)	
V1.3	2024-05-29	Gergely Biczók, AITIA	

Executive Summary

This report addresses the critical imperative of ensuring both security and safety in the context of the combined Airspace and Non-Terrestrial Network (ASN) concept proposed by the 6G-SKY project within the broader landscape of 6G technology. It begins by highlighting the unique challenges posed by the cyber-physical nature of 6G-connected aerial vehicles, emphasizing the potential direct impact of cybersecurity threats on safety, including human lives.

In response to these challenges, the report advocates for a comprehensive approach that goes beyond traditional security attributes to address the specific requirements of the combined ASN architecture. It underscores the importance of considering spoofing as a prominent security threat targeting unauthenticated communication protocols, which could compromise critical functionalities like advanced localization and drone detection.

Moreover, the report outlines safety challenges in urban airspace operations, emphasizing the need for coordinated monitoring and management of manned and unmanned[1] aircraft. The report proposes the deployment of a Drone Detection and Positioning System (DDPS) integrated with a ground-based traffic information system to provide a unified view of the airspace including unauthenticated UAVs, thus enhancing safety measures. Such a solution is precisely the manifestation of the proposed joint communication and sensing capability of 6G networks.

A key recommendation put forth is the adoption of a safety-security co-design and co-analysis approach, ensuring the integration of safety mechanisms and cybersecurity countermeasures into the system architecture from the design phase onwards. This integrated approach is essential for achieving security-and-safety-by-design in networked cyber-physical systems like the combined ASN.

Through a safety-security co-evaluation conducted using an integrated urban air traffic management system as a use case, the report demonstrates the critical importance of jointly considering cybersecurity and safety in ensuring the trustworthiness and resilience of the combined ASN, a networked cyber-physical system.

[1] (un)manned is used in the document as a gender-neutral term

List of Authors

Name	Affiliation
Gergely Biczók	AITIA
András Gazdag	AITIA
Robby De Candido	Skysense
Peng Wang	Skysense

Table of Contents

Acronym	Description
A2G	Air to Ground
ACARS	Aircraft Communications Addressing and Reporting System
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance-Broadcast
ANSP	Air Navigation Service Provider
ASN	Airspace and NTN
ATC	Air Traffic Control
ATM	Air Traffic Management
BSS	Broadcasting-satellite service
BVLOS	Beyond visual line-of-sight
CEPT	European Conference of Postal and Telecommunications Administrations
CIS	Common Information Service
CNS	Communication, Navigation and Surveillance
Combined ASN networks	Combined Airspace & NTN networks
DDPS	Drone Detection and Positioning System
DME	Distance measuring equipment
EASA	European Union Aviation Safety Agency
ECO	European Communications Office
eVTOL	Electrical Vertical Take-Off and Landing
FAI	Fédération Aéronautique Internationale
FBW	Fly-by-wire
FCC	Federal Communications Commission
FCS	Flight Control System
FSS	Fixed-satellite service
FW	Fixed Wing
GEO	Geostationary Orbit
HIBS	High Altitude IMT Base Stations (HIBS)
HAO	Higher Airspace Operations
HAPS	High Altitude Platform Station
IAM	Innovative Air Mobility
IATA	International Air Transportation Association

ICAO	International Civil Aviation Organization
ICNS	Integrated Communication, Navigation and Surveillance
ITU	International Telecommunication Union
IMT	International Mobile Telecommunications
IoT	Internet of Things
LAPS	Low Altitude Platform System
LEO	Low Earth Orbit
LOS	Line of sight
MBB	Mobile Broadband
MEO	Medium Earth Orbit
MSS	Mobile-satellite service
NGSO	Non-Geostationary Orbit
NOC	Network Operation Center
NRA	National regulatory authorities
NTN	Non-Terrestrial Network
RPAS	Remotely Piloted Aircraft System
SATCOM	Satellite Communication Systems
SES	Single European Sky
SERA	Standardized European Rules of the Air
SESAR	Single European Sky ATM Research
Smart city	A smart city is an “innovative city that uses information communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects”
SORA	Specific operations risk analysis
STM	Space Traffic Management
STPA	Systems Theoretic Process Analysis
TISB	Traffic Information System-Broadcast
TN	Terrestrial Networks
UAM	Urban air mobility
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communications

USP	UTM Service Provider
UTM	Unmanned Traffic Management
VOR	Very high frequency omnirange station
WET	Wireless energy transfer
WRC	World Radio Conferences
3GPP	3rd Generation Partnership Project

1. Introduction

6G promises trustworthiness that translates to a holistic security architecture on the network level. While existing security solutions from 5G provide a solid foundation, the cyber-physical nature of 6G-connected aerial vehicles requires a thorough investigation. In addition to the traditional security attributes of confidentiality, integrity, and availability, access control and non-repudiation, the combined Airspace and Non-Terrestrial Network (combined ASN) envisioned by the 6G-SKY project must consider that cybersecurity threats which may impact safety (and, thus, human lives) directly.

From the security aspect, the proposed novel non-terrestrial network architecture, making use of heterogeneous links, comes with its own security requirements. On top of the inherent challenges in wireless security, we foresee that thwarting spoofing attacks will become a focus point of related security efforts. Such attacks could potentially cripple two major functionalities of the novel architecture utilizing unauthenticated communication protocols: i) advanced localization (via GNSS spoofing) and ii) the above-mentioned drone detection (via ADS-B spoofing).

From the safety aspect, the greatest challenge regarding safe urban airspace operations is the coordination of flight missions comprising both manned and unmanned aircraft. To this end, a complete single source picture of the sky is indispensable. With non-cooperative/malicious UAVs in urban airspace, we foresee the emergence of a UTM Service Provider (USP) which shall be able to obtain information from a *drone detection and positioning systems* (DDPS) and a ground-based *traffic information system-broadcast* (TISB). An implementation of DDPS is proposed to be based on a sensor-fusion system (e.g., radar and passive-RF) to detect and locate any type of UAVs including unauthorized ones, enabling blacklisting and whitelisting based on customer preferences.

Invoked by the cyber-physical nature of the combined ASN architecture, we advocate for the concept of safety-security co-design and co-analysis. Already in the design phase, it is essential to use a co-evaluation methodology capable of capturing the intricate interplay of security hazards and cybersecurity threats. Such analysis can be the basis of requirement engineering, making sure that adequate safety mechanisms and cybersecurity countermeasures are integrated into the system architecture, ensuring security-and-safety-by-design.

The rest of the document is structured as follows. Section 2 puts 6G-SKY efforts into a 6G context, focusing on identifying defining security/safety properties of the combined ASN architecture: i) its cyber-physical nature, ii) the presence of flying UEs, and iii) the prevalence of unauthenticated and unencrypted communication protocols in the sector. Then, Section 3 establishes the state of the art in aviation cybersecurity including civil aviation and Unmanned Aerial Vehicles (UAVs). Next, we dedicate Section 4 to spoofing threats, focusing on the widely-used non-authenticating ADS-B and GNSS protocols, describing both prevalent attacks and potential countermeasures, also presenting open problems and future research directions. Finally, Section 5 introduces the concept of safety-security co-design and co-analysis. We provide an overview of related concepts, a brief introduction to existing techniques, and a more detailed background study on the co-evaluation method conceived by the EU ECSEL SECREDAS project in the context of connected and autonomous vehicles [1]. We also introduce the idea and system model of our integrated urban air traffic management system utilizing a drone detection and localization system to augment the knowledge base of traditional air traffic management with the location of unauthorized UAVs, thereby creating a single-source picture of the sky. Using the integrated urban UTM system as a use case, we conduct a safety-security co-evaluation, which proves that the joint consideration of cybersecurity and safety is essential in networked cyber-physical systems such as the combined ASN.

2. 6G Security Considerations

2.1. Setting the context

In the ever-evolving landscape of telecommunications, the arrival of each new generation brings unprecedented opportunities and challenges. As we move towards the era of 6G networks, the anticipation for revolutionary advancements is palpable. However, with these advancements come intensified security concerns. Securing 6G networks will demand a proactive, multi-faceted approach that addresses both current vulnerabilities and emerging threats [2].

While still in its conceptual stages, 6G is envisioned to surpass its predecessor, 5G, in speed, latency, capacity, and connectivity. It promises data rates measured in terabits per second, virtually zero latency, and ubiquitous connectivity through advanced technologies like terahertz frequencies, integrated satellite communications, and AI-driven network orchestration. Despite its promises, the very features that make 6G revolutionary also present security challenges. Terahertz frequencies, for instance, offer ultra-fast data rates but are susceptible to signal attenuation and interception. The integration of satellite communications introduces new attack vectors, including space-based threats like satellite jamming or spoofing. Additionally, the proliferation of IoT devices and the reliance on AI for network management open avenues for sophisticated cyberattacks, such as AI-driven malware or deepfake attacks.

To prepare for the rollout of 6G, governments and regulators must develop a comprehensive cybersecurity policy framework. These regulations should cover privacy, data protection, and cross-border security collaboration. These measures are essential to ensure the safe integration of 6G technology and protect user data, fostering global cooperation in addressing security challenges. In light of the intricate global telecommunications landscape, a collaborative security approach is essential. Industry stakeholders, governments, academia, and international organizations must unite efforts to identify vulnerabilities, exchange threat intelligence, and formulate standardized security protocols. This collective endeavor is critical to enhancing the resilience of telecommunications infrastructure against evolving threats and ensuring the integrity and reliability of communication networks worldwide.

Ensuring the resilience of 6G networks against physical attacks is critical due to their reliance on a diverse infrastructure, spanning terrestrial, aerial, and satellite components. These networks are vulnerable to various threats, including sabotage and tampering, which can compromise network integrity and disrupt services. Therefore, implementing robust physical security measures is essential to maintain network integrity and ensure uninterrupted service delivery. By fortifying infrastructure against physical threats, 6G networks can uphold their reliability and continuity, meeting the demands of modern communication needs effectively.

As edge computing becomes ubiquitous in 6G networks, the security of edge devices and gateways becomes paramount. Zero-trust architectures and secure enclaves are essential strategies to mitigate associated risks. These measures ensure that each component is rigorously authenticated and authorized, reducing the potential for unauthorized access or data breaches. By implementing robust edge security protocols, 6G networks can safeguard sensitive data and maintain the integrity of distributed computing resources, thereby enhancing overall network resilience and reliability.

Encryption and authentication stand as indispensable pillars of data security. Encryption serves as a robust shield, safeguarding sensitive data against unauthorized access and interception. Meanwhile, authentication mechanisms act as gatekeepers, verifying the identities of communicating entities to prevent impersonation/spoofing attacks. Given the imperative for ultra-low latency in Ultra Reliable Low Latency Communications (URLLC) scenarios, it's crucial that encryption and authentication protocols are not only secure but also highly efficient. This necessitates the use of lightweight encryption algorithms and streamlined authentication methods that introduce minimal processing delay. Additionally, the adoption of pre-shared keys and certificate-based authentication can help optimize authentication processes while maintaining stringent security standards. Furthermore, seamless integration of encryption and authentication protocols into the network architecture is essential to minimize latency overhead. Leveraging hardware-accelerated cryptographic operations and distributed authentication schemes can further enhance efficiency, ensuring compliance with URLLC requirements while upholding robust security measures.

In the realm of 6G security, AI-powered solutions are emerging as pivotal building blocks [3]. However, AI/ML is a double-edged sword: while ML serves as a powerful enabler for defense mechanisms, it also opens a new attack surface for malicious attackers. Harnessing the power of AI, security systems can detect anomalies, forecast potential threats, and execute autonomous responses to cyberattacks in real-time. However, the integration of AI/ML into security frameworks also introduces new challenges; adversarial attacks, where malicious actors exploit vulnerabilities in AI algorithms, pose significant threats. Furthermore, the reliance on AI for decision-making raises concerns about accountability, transparency, and bias. Despite these challenges, the benefits of AI-powered security are substantial. Machine learning algorithms can analyze vast amounts of data, enabling proactive threat detection and mitigation. Additionally, AI-driven security solutions adapt to evolving threats, enhancing resilience against sophisticated cyberattacks. To maximize the effectiveness of AI in 6G security, robust safeguards must be implemented to mitigate vulnerabilities and ensure algorithmic integrity. This includes rigorous testing, continuous monitoring, and implementing mechanisms to detect and mitigate attacks on the ML pipeline, including poisoning, membership inference, model stealing, etc. Moreover, the design of explainable ML models for network management, e.g., orchestration and resource provisioning, is a crucial step towards the desired trustworthiness of 6G systems.

In 6G, post-quantum security emerges as a pivotal concern, driven by the looming specter of quantum computers threatening the foundations of traditional encryption methods. As quantum computing capabilities advance, the need to fortify communication infrastructures against potential breaches becomes increasingly urgent. Consequently, 6G security initiatives are channeling efforts into the exploration and implementation of post-quantum cryptographic algorithms, which exhibit resilience against quantum attacks. Among these, lattice-based cryptography stands out as a promising avenue, offering robust security in the face of evolving threats. Nevertheless, the integration of post-quantum security into 6G networks necessitates careful navigation of various challenges. Balancing the imperatives of performance, compatibility, and scalability remains a complex task, as stakeholders strive to maintain operational efficiency without compromising on security standards. By embracing post-quantum security measures, 6G networks aim to future-proof communication infrastructures against the disruptive potential of quantum computing. This proactive approach underscores the commitment to safeguarding data confidentiality and integrity, thereby fostering trust in the digital ecosystem. As the trajectory of technological advancement unfolds, the resilience of 6G networks to quantum threats will serve as a cornerstone of digital resilience in the ever-evolving landscape of connectivity.

Given the challenges mentioned above and the complexity of 6G technology and envisioned deployments, adopting a security-by-design approach is crucial. Embedding security considerations at the core of the network architecture ensures that security measures are integrated from the outset rather than retroactively added. This proactive approach helps mitigate vulnerabilities and strengthens the overall resilience of the network against cyber threats. By incorporating security-by-design principles, 6G networks can address emerging challenges such as the proliferation of IoT devices, the adoption of edge computing, the integration of AI-driven technologies, and the preparation for a post-quantum era. Designing networks with security in mind facilitates the implementation of robust encryption, authentication, and access control mechanisms, safeguarding sensitive data and ensuring the privacy of users. Moreover, security-by-design principles promote collaboration between stakeholders, including network architects, developers, regulators, and end-users. By fostering a culture of security awareness and accountability throughout the development lifecycle, organizations can effectively address potential risks and vulnerabilities early on, reducing the likelihood of security breaches and minimizing the impact of cyber-attacks. Furthermore, security-by-design promotes interoperability and compatibility between different components and vendors within the 6G ecosystem. This ensures seamless integration of security measures across diverse network environments and facilitates the implementation of standardized security protocols.

As 6G networks facilitate groundbreaking applications in healthcare, transportation, and energy sectors, aligning security considerations with ethical and societal implications becomes paramount. Balancing innovation with security is crucial to unlocking the full potential of 6G while preserving individual rights and societal values. This entails addressing privacy concerns, ensuring data protection, and promoting transparency in the deployment of 6G technologies. By upholding ethical principles and societal values, 6G can drive positive socio-economic impact while fostering trust and confidence among users and stakeholders alike [4].

In summary, the emergence of 6G networks brings forth unprecedented opportunities alongside heightened security concerns. Addressing these challenges necessitates a proactive, collaborative approach that integrates security measures into the network architecture from the outset. Robust regulatory frameworks, collaborative security initiatives, and a technological focus on physical security, resource-efficient but strong and post-quantum ready cryptography, and AI-driven defenses are essential for safeguarding 6G networks against evolving threats. By adopting a security-by-design approach and aligning security considerations with ethical and societal implications, we can harness the transformative potential of 6G while upholding individual rights and societal values.

2.2. Specifics for combined ASN

The 6G-SKY project put forward an architectural vision for a novel 6G-enabled network termed Combined Airspace and Non-Terrestrial Network (combined ASN) [5]. The envisioned network architecture and operational model have two distinct properties that characterizes its cybersecurity challenges. First, when utilized in a real-world use-case, such as logistics, emergency response, or smart cities, the resulting system is cyber-physical in nature. Second, owing to the integration of flying UEs and infrastructure nodes, such as UAVs, HAPS, and satellites, the architecture inherits the cybersecurity vulnerabilities of aviation and aerial/satellite networks. A dominant threat in such an environment is spoofing when a malicious attacker impersonates a legitimate communicating entity and injects useless or hurtful messages into the communication and/or gains access to otherwise restricted information. While spoofing can be completely mitigated via standard authentication and encryption mechanisms, some of the prevalent communication protocols in aviation and satellite communications, such as ADS-B (Automatic Dependent Surveillance-Broadcast) and (civilian) GNSS (Global Navigation Satellite System) are unauthenticated and unencrypted. Although there are many proposals for hardening these protocols, the standardization, adoption, and real-world deployment of such improvements constitute a lengthy and expensive process.

2.2.1. Cyber-physical characteristics

Cyber-physical security is paramount for the seamless integration of 6G networks and aerial/Non-Terrestrial Networks (NTN). This fusion of advanced telecommunications with physical infrastructure introduces a host of new challenges and vulnerabilities, necessitating robust measures to safeguard against cyber threats and ensure the integrity and reliability of critical systems [6]. Firstly, the convergence of 6G networks with aerial and NTN infrastructure expands the attack surface, increasing the potential for cyber threats [7]. Aerial platforms such as drones and balloons, as well as satellites in NTN, are susceptible to various cyberattacks, including hacking, spoofing, and jamming. These attacks can compromise communication links, disrupt services, or even lead to physical damage, posing significant risks to flying vehicles and public safety. Moreover, the reliance on interconnected systems in 6G and aerial/NTN networks heightens the interdependency between cyber and physical components. A cyber breach can have tangible physical consequences, such as disrupting transportation systems, compromising emergency response operations, or causing environmental hazards. Therefore, protecting against cyber threats requires a holistic approach that addresses both cyber vulnerabilities and their potential physical impacts.

Furthermore, the integration of flying UE and aerial platforms into 6G networks introduces new challenges for authentication, access control, and data protection. Securing communication links between ground stations, satellites, and aerial platforms is essential to prevent unauthorized access or tampering with data. Additionally, ensuring the authenticity and integrity of commands sent to aerial platforms is critical for preventing hijacking or manipulation of these devices. In the context of NTN, securing satellite communications against cyber threats is paramount. Satellites are high-value targets for cyber attackers due to their critical role in providing global connectivity. Protecting satellite networks against cyber threats requires robust encryption, authentication, and intrusion detection mechanisms to safeguard against unauthorized access and tampering.

Moreover, as 6G networks enable transformative applications such as autonomous vehicles, smart cities, and telemedicine, the importance of cyber-physical security becomes even more pronounced. Any compromise in the security of these systems could have far-reaching consequences, including loss of life, economic damage, and erosion of public trust. Hence, a safety-security co-design mindset is crucial to ensure the trustworthiness of both the enabling network and the services provided on them.

2.2.2. Flying User Equipment

Firstly, incorporating flying UE into the combined airspace extends the coverage and capacity of 6G networks to previously unreachable areas. By leveraging drones, balloons, and other aerial platforms equipped with communication capabilities, NTN can provide connectivity in remote regions, disaster zones, or areas with limited terrestrial infrastructure [7]. This expanded coverage enhances the accessibility of high-speed internet and communication services, bridging the digital divide and enabling socio-economic development in underserved communities. Moreover, the integration of flying UE enhances the flexibility and agility of 6G networks, enabling dynamic network optimization and resource allocation. Aerial platforms can serve as mobile relays or base stations, dynamically adjusting their position to meet fluctuating demand or address coverage gaps. This flexibility enhances network resilience and ensures uninterrupted connectivity, even in highly dynamic environments or during emergencies.

Furthermore, flying UE facilitates innovative applications and services across various sectors. In the transportation industry, drones and aerial vehicles equipped with communication capabilities enable real-time monitoring of traffic, weather conditions, and infrastructure. This enhances safety, efficiency, and situational awareness, paving the way for autonomous aerial transportation and delivery services. In emergency response scenarios, flying UE can provide critical communication links for disaster relief operations, search and rescue missions, and remote medical assistance. Aerial platforms equipped with communication and sensing technologies enable rapid deployment of temporary communication networks in disaster-affected areas, facilitating coordination among first responders and improving disaster response efficiency. Additionally, the integration of flying UE into 6G networks enhances the delivery of immersive and interactive experiences in entertainment and media. Aerial drones equipped with high-definition cameras and communication capabilities enable live streaming of events from unique vantage points, enhancing viewer engagement and expanding content creation possibilities.

However, the integration of flying UE into a combined airspace with NTN also presents unique challenges and considerations. Ensuring seamless handovers between terrestrial and aerial networks, managing airspace congestion, and ensuring safety and security are critical aspects that require careful coordination and regulation. Moreover, addressing privacy concerns, spectrum allocation, and environmental impacts are essential for the responsible deployment of flying UE in combined airspace.

2.2.3. Spoofing threats

Spoofing is a prominent threat in aviation and satellite cybersecurity, especially concerning critical communication protocols like ADS-B (Automatic Dependent Surveillance-Broadcast) and GNSS (Global Navigation Satellite System) [8]. These protocols are fundamental to aviation safety and satellite-based navigation, making them prime targets for malicious actors seeking to disrupt operations or compromise security. ADS-B broadcasts essential aircraft location and identification information, which is vital for air traffic management and collision avoidance. Similarly, GNSS provides precise positioning and timing data for navigation and timing synchronization in aviation and various other sectors. However, both systems are susceptible to spoofing attacks, where false information is maliciously broadcast to deceive receivers. Spoofing attacks in aviation and satellite systems can have severe consequences. By broadcasting false ADS-B or GNSS signals, malicious actors can manipulate aircraft positions, deceive air traffic controllers, or inject ghost aircraft. Such disruptions pose significant safety risks, potentially leading to mid-air collisions, unauthorized aircraft intrusions into restricted airspace, or navigational errors. Moreover, spoofing attacks can extend beyond aviation, affecting sectors such as transportation, telecommunications, and emergency response that rely on satellite-based services.

ADS-B (Automatic Dependent Surveillance-Broadcast) and GNSS (Global Navigation Satellite System) can be spoofed due to inherent vulnerabilities in their communication and signal reception mechanisms. ADS-B relies on aircraft broadcasting their position, velocity, and other essential information to ground stations and nearby aircraft. However, because ADS-B transmissions are unencrypted and unauthenticated, they are susceptible to spoofing attacks. Malicious actors can simulate legitimate ADS-B signals by broadcasting false position and identification information, leading to misinterpretation by receivers. Similarly, GNSS signals are susceptible to spoofing because they are transmitted over open frequencies and lack built-in authentication mechanisms. GNSS receivers, such as those used in aircraft navigation systems, rely on signals from multiple satellites to determine precise positioning and timing information. However, these signals can be manipulated by spoofers who broadcast false satellite signals or overpower legitimate signals, causing receivers to calculate inaccurate positions or timestamps.

The vulnerability of ADS-B and GNSS to spoofing attacks stems from their open and unauthenticated nature, which makes them susceptible to manipulation by unauthorized entities [9]. As these systems are widely used in aviation and other critical sectors, safeguarding them against spoofing attacks is essential to ensure the integrity and reliability of navigation and communication systems. This necessitates the implementation of robust security measures, such as encryption, authentication, and signal validation, to detect and mitigate spoofing attempts effectively. Securing ADS-B and GNSS protocols against spoofing is paramount to maintaining the integrity and reliability of aviation and satellite systems. Robust authentication mechanisms, cryptographic safeguards, and anomaly detection techniques are essential for detecting and mitigating spoofing attacks effectively. Implementing these measures would help ensure that information received from ADS-B and GNSS sources is authentic and trustworthy, thereby enhancing the resilience of aviation and satellite operations against malicious exploitation. On the other hand, these protocols are in heavy use in currently deployed systems, and switching to newer, secure versions would have substantial (maybe even prohibitive) collective switching cost. Therefore, proposals for ML-based anomaly detection might be preferred; these do not require the modification of the communication protocols, rather, can be implemented at end devices as a separate computational process.

3. Aviation Cybersecurity

The integration of Information and Communication Technology (ICT) tools into mechanical devices in routine use within the aviation industry has heightened cybersecurity concerns. The extent of the inherent vulnerabilities in the software tools that drive these systems escalates as the level of integration increases. Moreover, these concerns are becoming even more acute as the migration within the industry in the deployment of electronic-enabled aircraft and smart airports gathers pace.

A review of cyber-security attacks and attack surfaces within the aviation sector over the last decades provides a mapping of the trends and insights that are of value in informing on future frameworks to protect the evolution of a key industry. The goal is to identify common threat actors, their motivations, attack types and map the vulnerabilities within aviation infrastructures most commonly subject to persistent attack campaigns. The analyses will enable an improved understanding of both the current and potential future cybersecurity protection provisions for the sector. Evidence is provided that the main threats to the industry arise from Advance Persistent Threat (APT) groups that operate, in collaboration with a particular state actor, to steal intellectual property and intelligence to advance their domestic aerospace capabilities as well as monitor, infiltrate and subvert other sovereign nations' capabilities. A segment of the aviation industry commonly attacked is the Information Technology (IT) infrastructure, the most prominent type of attack being malicious hacking with intent to gain unauthorized access. The analysis of the range of attack surfaces and the existing threat dynamics has been used as a foundation to predict future cyber-attack trends. The insights arising from the review will support the future definition and implementation of proactive measures that protect critical infrastructures against cyber-incidents that damage the confidence of customers in a key service-oriented industry.

3.1. Civil Aviation

This section aims to explore the cybersecurity challenges faced by the civil aviation sector and the potential consequences of cyber-attacks on aviation systems. By understanding the cybersecurity risks faced by civil aviation, this research aims to contribute to the development of robust cybersecurity practices that can safeguard the aviation industry and ensure the safety of passengers and critical infrastructure.

3.1.1. Aerospace and Avionic Systems

Aerospace systems have undergone increasing levels of integration between software and hardware, facilitated by embedded-computing technologies. Consequently, the system faces challenges associated with software vulnerabilities, given the difficulty of ensuring embedded systems' security. Scholars argue that threats to aerospace systems may stem from underlying components like the Operating System (OS) kernel, protective mechanisms, and context switching. Despite employing formal verification methods, it remains challenging to guarantee the absence of vulnerabilities within embedded systems. A primary inference drawn from previous research is that attacks on aerospace computer systems can be classified based on the attacker's proficiency and objectives, which may entail compromising the core functions of the computing system or its fault-tolerance mechanisms, such as error detection and recovery systems [10].

An avionics system plays a crucial role in facilitating the safe operation of an aircraft by providing essential support to crew members and pilots. It encompasses the integration of aviation with electronics, involving embedded systems throughout the lifecycle of aircraft design, development, and operation. Avionic systems serve to gather pertinent data, including weather conditions, positional information, and communication signals. These systems rely on external sensors to capture parameters such as velocity, heading, and atmospheric temperature, which are then routed efficiently through an avionic network to various components within the aircraft. In recent years, there has been efforts towards adopting Ethernet-based networks, such as Avionics Full Duplex Switched Ethernet (AFDX), and protocols like Wireless Flight Management System (WFMS) based on IEEE 802.11 standards. This transition aims to capitalize on the cost-effectiveness of Commercial-Off-The-Shelf (COTS) components and software technologies, thereby enhancing bandwidth capabilities while simultaneously reducing operational costs within avionic networks [10].

Wired avionic communications offer a heightened level of security and reliability, rendering them resistant to unauthorized access and data tampering. Conversely, the adoption of Avionics Wireless Networks (AWN) introduces novel challenges concerning assurance, reliability, and security [11].
Aircraft avionics serve multifaceted purposes, encompassing critical functions such as flight control, navigation, guidance, communications, and system monitoring. The extensive integration involved raises

cybersecurity concerns, particularly evident in Voice-over-the-Radio (VoR) communications utilized between pilots and controllers. VoR suffers from signal latency, especially in scenarios involving concurrent communications, and is susceptible to signal corruption or ambiguity due to noise interference.

In contrast, the Controller Pilot Data Link (CPDLC) operates digitally, offering greater resilience against impairments. Synchronization between air carrier flight operations centers and the flight deck ensures simultaneous reception of signals, facilitating comprehensive risk awareness and informed decision-making. Recent efforts within the aviation community have been directed towards modernizing the National Airspace System (NAS), with an emphasis on enhancing aircraft-ground system interaction through a new communication infrastructure.

More detail on the attack surfaces across different aerospace and avionic components is provided next.

Aircraft Communications Addressing and Reporting System (ACARS)

Aeronautical Radio Incorporated (ARINC)[2] introduced the ACARS data link protocol with the aim of mitigating *crew* workload and enhancing data integrity. ACARS, based on the ARINC 618 standard, functions as an air-to-ground protocol facilitating the exchange of data between onboard avionics systems and ground-based ACARS networks. The ACARS system comprises a Control Display Unit (CDU) and an ACARS Management Unit (MU); the MU facilitates the transmission and reception of digital messages with the ground via existing very high frequency (VHF) radios. Groundside, the system operates through a network of radio transceivers, which receive and transmit data link messages, effectively routing them to respective aircraft within the network.

According to research by Smith et al. [12], the utilization of ACARS by stakeholders has evolved beyond its original purpose to encompass functions such as flight tracking and automated crew timekeeping. The study illustrates how contemporary employment of ACARS raises concerns regarding location privacy infringement; the authors elucidate how sensitive information transmitted over ACARS wireless channels could compromise user privacy, reinforcing the susceptibility of ACARS messages to eavesdropping attacks. The paper concludes by proposing a privacy framework, with additional suggestions from other researchers advocating for encryption and policy measures to counter known eavesdropping threats on the communication channel.

Automatic Dependent Surveillance-Broadcast (ADS-B)

Aircraft autonomously transmit identification and positional data via a broadcast mode utilizing Automatic Dependent Surveillance Broadcast (ADS-B) technology, known as ADS-B Out, and/or receive such data, referred to as ADS-B In, through a data link. This system enhances the safety and capacity of airport surveillance, thereby augmenting situational awareness for both airborne and ground surveillance operations within airport environments. ADS-B Out facilitates various ground applications, including Air Traffic Control (ATC) surveillance in radar and non-radar airspace around the airport, and enables enhanced surveillance capabilities by establishing links with nearby aircraft to receive ADS-B Out messages within their coverage areas (ADS-B In).

The reliability and availability of the ADS-B system are of paramount importance due to its critical role in supporting essential ground and airborne applications. Moreover, ADS-B, which utilizes global satellite navigation systems, enables the creation of precise airspace maps for effective air traffic management. However, the security of ADS-B has emerged as a significant concern because the system transmits comprehensive information about aircraft, including their positions, velocities, and other relevant data, over unencrypted data links.

Researchers conducted an analysis of ADS-B data received from Grand Fork International Airport, which were provided in both raw and archived Global Data Link (GDL-90) format. GDL-90 is specifically designed to transmit, receive, and decode ADS-B messages through an onboard data link by integrating GPS satellite navigation with data link communications. The primary objective was to identify anomalies within the data and subsequently assess the associated risks.
Throughout the study, anomalies such as dropout, low-confidence data, message loss, data jump, and altitude discrepancy were identified. However, particular emphasis was placed on two anomalies: dropouts and altitude deviations. The findings suggest that any failures related to these anomalies possess the potential to impact ATC operations, either at the airspace level, such as dropout and low-confidence data, or at the aircraft level, such as data jump, partial message loss, and altitude discrepancy. These vulnerabilities could

[2] https://content.time.com/time/subscriber/article/0,33009,739806,00.html

be exploited by malicious actors to execute various attacks, including eavesdropping, jamming, message injection, deletion, and modification [10].

Electronic Flight Bag

The Electronic Flight Bag (EFB) functions as a platform for presenting digital documentation, encompassing navigational charts, operational manuals, and aircraft checklists to the flight crew. Additionally, it facilitates basic flight planning computations for crew members. Enhanced EFB systems are planned to undertake intricate flight planning duties and seamlessly integrate into flight management systems, alongside other avionic systems, to exhibit the real-time positioning of an aircraft on navigational charts coupled with weather data. Moreover, EFBs serve as advantageous alternatives to traditional paper-based references carried on board as part of the flight management system, thereby delivering supplementary benefits through weight reduction. However, the integration of advanced EFBs with the Avionic System, unlike their stand-alone paper-based predecessors, introduces a novel vulnerability. For instance, a maliciously infected EFB could potentially instigate denial-of-service attacks on other interconnected on-board systems, thereby presenting a new avenue for security threats [10].

3.1.2. Summary of attack surfaces

Table 1 Some Exploitable Flaws and Components in the Civil Aviation Industry [10]

Component	Weakness
SATCOM terminals	SATCOM terminals can be exploited through some design flaws in areas such as hardcoded credentials, insecure protocol, weak encryption algorithms.
Aerospace systems	Attackers, based on skill level, can exploit issues with integration of OS in embedded systems, such as in OS kernel, context switching, protection mechanisms.
ACARS	The ACARS communication channel is susceptible to eavesdropping and privacy breach.
ADS-B	The ADS-B communication channel is prone to eavesdropping, jamming attacks, message injection, deletion, and modification.
AWN	The Avionic Wireless Network communication channel is prone to data integrity problems such as data assurance, reliability, and security.

3.2. UAV Systems

Unmanned aerial vehicles (UAVs), also known as drones, are becoming pervasive and have been employed in many military and civilian applications. UAVs can be operated either through remote control or via self-government. They play a major and vital role in many military and civilian applications. Because of ease of deployment, and high maneuverability and mobility, UAVs have promoted their considerable use to perform various tasks such as rescue, surveillance, search, aerial base station, and goods delivery. For example, Amazon, FedEx, and Walmart announced that they will utilize UAVs to deliver packages. During the coronavirus pandemic, UAVs were used to measure body temperature, thus avoiding the risk of viral infection. Moreover, UAV swarms have great potential to execute formidable tasks beyond the capability of a single UAV (e.g., investigation and message relay). In a UAV swarm, when one UAV becomes unavailable, other UAVs can quickly replace it, thus greatly ensuring reliability.

With the development of UAV applications, UAV-involved communications are becoming complicated and diverse. Traditional UAV communication architecture is usually composed of two parts: ground control station (GCS) and UAV. The GCS controls the UAV, and the UAV feeds back GCS commands. The two parts are connected through a communication link with unlicensed spectrum (e.g., 2.4 GHz) or Wi-Fi, which can only operate within a visual line-of-sight (LoS) range.

To provide beyond LoS communications, cellular and satellite networks offer a promising solution for UAV communications. On the other hand, UAVs can provide cost-effective wireless communications in a variety of real-world scenarios. For example, UAVs can be utilized as a mobile platform for collecting data from ground sensors or as an aerial base station to offer wireless communications, a complement to the existing cellular networks, for users in case of emergency. Compared to terrestrial wireless communications, UAV-

based communications have many unique advantages, such as on-demand and swift deployment, high flexibility, and mobility, which bring promising gains for UAV applications.

Despite various applications enabled by UAVs, security threats to UAV communications are increasing rapidly. Due to security vulnerabilities in UAV protocols and standards, UAVs are vulnerable to various attacks, including eavesdropping attack, GPS spoofing attack, and denial-of-service (DoS) attack. For example, an RQ-170 Sentinel was hijacked by Iranian forces[3], and software called Skyjack can maliciously search and hijack civilian UAVs. The security issues of UAV communications have become very severe nowadays, which brings big challenges to promoting the widespread use of UAVs.

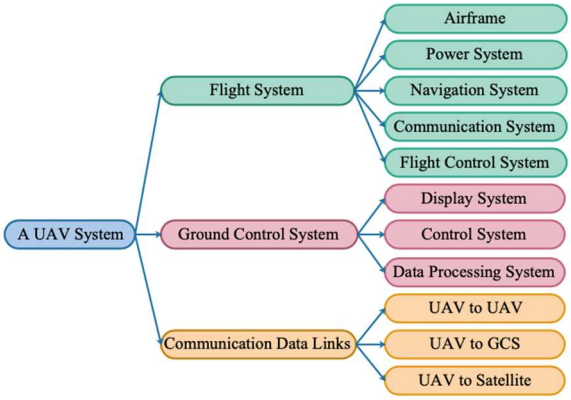


Figure 1 UAV System Components [13]

Components of UAVs

A typical UAV system usually includes a flight system, a set of communication data links, and a ground control system (GCS).

The flight system includes an airframe, a power system, a navigation system, a communication system, and a flight control system:

- The airframe is the supporting platform of a UAV, which can support all the equipment to fly into the sky.
- The power system provides a UAV with long-lasting endurance.
- The navigation system measures and calculates the position, speed, and flight attitude of a UAV with a reference coordinate system. Also, the navigation system guides a UAV to fly according to the designated route, equivalent to a navigator in manned aircraft systems. The navigation system works with other sensors, such as barometers and gyroscopes. The status data of a UAV can be measured and transmitted to a GCS for control signals analysis.
- The communication system provides a data link between the control station system and a UAV.
- The flight control system (GNC – Guidance, Navigation, and Control), also called flight management and control systems, is equivalent to the "heart" part of UAV systems. The main task of the control system is to maintain the stability of the altitude and flight paths of an aircraft [13]. UAVs capable of long distance and endurance flight are typically augmented with autopilot features, capable of stabilizing flight and performing various autonomous functions in case of loss of the Command and Control (C2) link. The autonomy level of the drone is proportional to its GNC capabilities.

The transmission of control information between UAVs and GCSs mainly relies on the communication system, which allows data exchange. The relationship of the three communication links is illustrated in Figure 1.

A Ground Control Station (GCS) constitutes a fundamental component within a UAV system, comprising a display interface, a control mechanism, and a data processing unit. The display interface serves primarily to present real-time flight status information of the UAV, monitoring various parameters such as GPS satellite lock count, gimbal angles, and camera exposure settings. The control mechanism governs aircraft flight either through automated course planning software for flight path determination or manual intervention via the console for direct flight management. The principal tasks of the data processing unit involve the analysis and manipulation of data received from the UAVs, facilitating real-time transmission of flight parameters to the

[3] https://phys.org/news/2011-12-rq-drone-ambush-facts-iranian.html

control system. Subsequently, this processed data is disseminated to the display interface via established data transmission links.
In order to keep UAVs fly safely, UAVs also consist of support equipment, which can be used for maintenance, recovery, fault diagnosis, etc. [13].

3.2.1. Drone's operational modes

Modern-day UAVs utilize an array of sensors, with Global Navigation Satellite Systems (GNSS) being paramount for tasks such as positioning, orientation determination, path profiling, guidance, and navigation. In addition to GNSS, drones and missiles commonly employ various other sensors, including but not limited to Inertial Measurement Units (IMUs), Terrain Contour Matching (TERCOM) systems, accelerometers, magnetometers, gyroscopes, and barometers. Nonetheless, our focus pertains solely to GNSS-based guidance, navigation, and control (GNC) systems, excluding the discussion of non-GNSS alternatives. Within the realm of GNSS, the Global Positioning System (GPS) stands out as the most prevalent system, owing to its widespread adoption and free global coverage. The reliance of drones on GPS is contingent upon factors such as autonomy levels, intended applications, and operational flight modes.

The various ''Flight Modes'' of modern drones, can be grouped under three broader operational categories: Manual, Semi-Autonomous Assisted, and Autonomous. A brief introduction of these operational modes is given below.

Manual mode

In manual mode, drones are regulated all the time through a Remote Control (RC) usually known as telemetry, within Visual Line Of Sight (VLOS) and do not require GPS for guidance, though this mode requires technical skills on part of the operator to control the aircraft. Since GPS is never used in the manual mode, drones in this mode are not vulnerable to GPS-based threats. However, manually operated drones can still be subjected to those threats which target air to ground or air to air (e.g., slave drone in a swarm) C2 links [14].

Semi-autonomous assisted

Drones in semi-autonomous assisted mode are also governed by a ground operator, with assistance from the autopilot, constituting various sensors including GPS. As an example, various automated flight modes of ArduPilot (https://ardupilot.org/plane/docs/flight-modes.html), a widely used open-source auto pilot system, such as circle, drift, follow, loiter, zig zag and return to launch (RTL), use GPS for executing commands and fall under semi-autonomous category. Other similar functions like stabilize, alt hold, and land make use of additional connected Micro Electro-Mechanical Systems (MEMS) sensors like altimeter, accelerometer, and other vision-based sensors. These commands can be manually relayed to the drone while operating in semi-autonomous mode. In such a case, drones are dependent on both the C2 link and the GPS for GNC services and can operate in Extended Visual Line Of Sight (EVLOS) [14].

Autonomous

In autonomous mode, the on-board Autopilot is provided with a flight plan e.g., guided, auto and smart RTL modes of the Ardupilot. After this mode is activated the ground controller cannot (or is not required to) intervene for the control. The aircraft requires no user input and is solely dependent on the integrated guidance system including obstacle avoidance and course rerouting, in case of smart RTL mode. In a GPS guided drone, PVT solution is calculated for navigating course and execution of mission Beyond Visual Line Of Sight (BVLOS). Since the C2 link is never/rarely used in the autonomous operational mode, the threat vectors are restricted to GPS-based threats only [14].

3.2.2. Security Threats

The rapid development and success of UAV-related technologies have brought security issues to UAVs [13]. Next, we study the security threats of UAVs from three domains, as shown in Figure 2.

- In the physical domain, a major security problem is that destructive weapons may maliciously damage UAVs.
- In the cyber domain, the security problems (such as injection attacks, jamming attacks and hijacking attacks) are mainly caused by attacks on communication networks, which leads to data loss or jeopardizing UAV flight processes. Eventually, UAVs are out of control or even destroyed.

- In the cyber-physical domain, security issues are through cyber-attacks that impact physical environments or devices. The flight systems, data links, ground control stations and other support equipment may face various security threats.

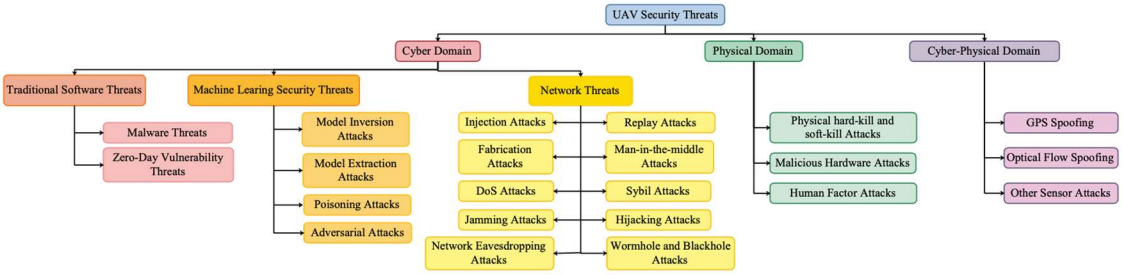


Figure 2 UAV Security Threats [13]

Security Threats in Physical Domain

In recent times, there has been a notable emergence of security threats posed by UAVs within the physical domain. While most UAV incidents involve cyber domain attacks, civilian UAVs are also susceptible to physical domain assaults.

Primarily, direct attacks manifest as physical hard-kill methods. UAVs traversing at low altitudes are vulnerable to being neutralized via projectile kinetic energy weapons or directed energy weapons. Mitigation against such attacks typically involves operators vigilantly monitoring UAV movements to thwart potential destruction by attackers.

Furthermore, UAVs may encounter physical soft-kill attacks, which exacerbate flight complexities through various means such as the deployment of solid clusters of objects like particles or dense foam. Moreover, human factor attacks pose a significant security risk to UAVs, encompassing actions aimed at destruction or theft. Among the defensive measures, the utilization of electronic anti-theft locks serves as a deterrent against theft.

UAVs Security Threats in Cyber Domain

Wireless communication renders UAVs susceptible to an array of cyber-attacks, presenting significant risks. Military UAVs, tasked predominantly with clandestine operations such as strike missions, rescue operations, and reconnaissance, face substantial jeopardy when targeted by cyber threats, potentially resulting in severe military setbacks. Similarly, civilian UAVs are prone to exploitation by hackers or adversaries. Thus, both military and civilian UAVs remain susceptible to cyber assaults, necessitating continuous vigilance. As delineated in Figure 2, cyber threats encompass traditional software vulnerabilities, machine learning security risks, and network vulnerabilities. For the present discussion, our focus will center solely on network threats.

Network Layer Attacks [15]

Comparable to other interconnected devices, UAVs encounter analogous threats within the network layer, as evidenced by previous research. The primary categories of network layer assaults encompass flooding attacks, de-authentication attacks, and routing attacks, delineated subsequently.

Flooding Attack: The conventional flooding attack, known as the Denial of Service (DoS) attack, entails a significant consumption of system resources aimed at rendering a network service inaccessible, thereby impeding legitimate users from accessing the service in a normal manner. Given their reliance on limited computing resources and power, UAVs are particularly susceptible to DoS attacks. Given their airborne nature, the ramifications of DoS attacks on UAVs can be severe. For instance, the inability to receive Ground Control Station (GCS) commands may result in loss of aerial control and depletion of battery power, potentially leading to hazardous incidents such as crashes. Certain researchers have utilized security tools to execute DoS attacks on UAVs, employing tactics such as inundating a UAV with a large volume of data packets to incapacitate it, ultimately resulting in a crash.

De-Authentication Attack: Many drones are outfitted with Wi-Fi capabilities for communication with Ground Control Stations (GCS) and reception of user commands. Nevertheless, the Wi-Fi module operating on the

802.11 protocol exhibits notable vulnerabilities. Due to the absence of encryption in its management frame, it becomes susceptible to exploitation by malicious actors. Such individuals can exploit this weakness by crafting deceptive de-authentication frames, thereby prompting disconnection between the GCS and the UAV. The attacker initiates the process by intercepting and identifying the Medium Access Control (MAC) addresses associated with both the UAV and its linked user. Subsequently, the attacker dispatches a falsified de-authentication frame packet to the user, effectively severing the communication link with the UAV. This action enables the attacker to establish control over the UAV.

Routing Attack: Another form of assault primarily targets multi-UAV networks or UAV swarms. The frequent turnover of nodes within UAV networks facilitates the potential for routing attacks, akin to those observed in wireless sensor networks. In such scenarios, attackers may introduce UAV nodes under their control into a UAV network, masquerading them as legitimate UAVs, or compromise existing UAVs within the network to instigate a routing attack. These nefarious nodes are camouflaged to appear as optimal routing agents with the aim of manipulating the entire routing infrastructure. Subsequently, other nodes may unwittingly select these malicious nodes to relay their packets. Routing attacks pose significant threats to multi-UAV networks, precipitating network-wide dysfunction by undermining their routing protocols. Common manifestations of routing attacks encompass black hole attacks, gray hole attacks, and wormhole attacks.

Physical Layer Attacks: Physical layer attacks of the network communication on UAVs pertain to incursions within wireless communication channels, alternatively known as physical link assaults. These attacks, contingent upon the adversary's conduct, delineate into two categories: passive eavesdropping and active eavesdropping.

Passive Eavesdropping Attack: In the context of passive eavesdropping attack, an entity with malicious intent covertly intercepts communication over a wireless channel, gathering transmitted data without engaging in any overt activities. This form of eavesdropping, characterized by its clandestine nature, does not disrupt the legitimate exchange of messages between users or UAVs, posing challenges for UAV operators in terms of detection and precise localization of the eavesdropper.

Active Eavesdropping Attack: In contrast to passive eavesdropping, the active eavesdropping attack presents a greater level of danger due to its encompassment of both eavesdropping and signal interference. An active eavesdropper possesses the capacity to employ jamming devices to maliciously transmit interference signals onto legitimate channels. This method effectively degrades the integrity of the legitimate channel, rendering a legitimate receiver incapable of receiving packets, thereby significantly impeding the ability of UAVs to execute tasks and transmit crucial information. Additionally, active eavesdroppers possess the capability to relocate to optimal eavesdropping positions or utilize sophisticated wireless devices, such as full-duplex eavesdroppers, to intercept wireless signals. This amplifies the potency of the attack, especially when coupled with collaboration with potential passive eavesdroppers, leading to extensive disruption of lawful UAV communications.

4. Spoofing attacks

Spoofing is a prominent threat in aviation and (civil) satellite cybersecurity, as unauthenticated and unencrypted communication protocols are in widespread use in real-world deployments. Although the threat is well-known and mitigation mechanisms have been proposed, current protocol versions do not implement them yet for economic reasons.

4.1. ADS-B

The Automatic Dependent Surveillance - Broadcast (ADS-B) represents a contemporary technological framework amalgamating extant solutions within the domains of telecommunications, navigation, and airspace surveillance. It constitutes a pivotal component of both the FAA's NextGen initiative[4] and Eurocontrol's CASCADE program[5], aimed at enhancing the safety, efficiency, automation, and environmental sustainability of the air traffic system. Signifying its significance, ADS-B technology is accorded a dedicated Category 21 ASTERIX protocol for aircraft information exchange.

The ADS-B system automatically delivers the necessary data to users (both on the ground and in the air). Its integral part is the GNSS, so that the ADS-B system depends on the accuracy of the positioning system. The ADS-B standard regulates the exchange of broadcast messages between aircraft and ATC ground stations. It can work as a transmitter (ADS-B Out) or a receiver (ADS-B In). The ADS-B In allows the aircraft to receive data which is displayed on the CDTI (Cockpit Display of Traffic Information) interfaces (most often, MFD and EFB devices), and which are emitted by other aircraft positioned in a relatively close environment. The same information is used for TCAS systems. Within the ADS-B Out system, the status information of the aircraft is handed over.

The ADS-B system consists of three interdependent components:

- ground infrastructure (GBT stations and antenna system),
- aircraft equipment (ADS-B specialized transponder, GPS, receiver, altimeter, CDTI6, etc.),
- operational procedures (regulatory basis for the implementation and use of the ADS-B system).

Communication within the ADS-B is realized by using the radio system according to standardized communication protocols, such as 1090 MHz extended squitter (1090-ES), 987 MHz Universal Access Transceiver (UAT) and VHF Datalink Mode 4 (VDL-M4), which will be used depends on the type of aircraft (in accordance with the FAA guidelines). Each ADS-B message contains an 8 µs preamble for synchronization and a 56-bit (short) or 112-bit (extended) data block. Thus, an extended ADS-B message has 112 bits which are transmitted using 1090 MHz (“extended squat”) data links (FAA, 2010). The ADS-B protocol format with a 112-bit message frames contain a preamble (8.0 ms), which is used to synchronize transmitters and receivers and 112-bit payload which consists of five segments. The first, 5-bit segment contains telecommunication transmission data and refers to the downlink format used to encode broadcast messages, the second, 3-bit segment is the field of choice, while the third, 24-bit segment contains a unique aircraft address. The next 56 bits (ADS-B data) refer to sub-segment data such as flight identification (call sign), position (latitude/longitude), position accuracy, barometric and geometric height, vertical velocity, trajectory angle, and ground speed (Ghose & Lazos, 2015). ADS-B messages are not encrypted: the last 24 bits include a parity check that detects and corrects transmission errors in the messages. ADS-B frames are modulated by pulse modulation with a pulse length of 1 ms. As the ADS-B protocol transmits data at a speed of 1 Mbit/s, the total duration of the ADS-B extended message is 120 ms (including the preamble) [8].

4.1.1. Cyber-attacks on ADS-B

The vulnerabilities inherent in the ADS-B system primarily stem from its utilization of RF waves for communication, whereby messages are transmitted as unencrypted text. This characteristic renders them susceptible to exploitation by malicious actors, who often target such unsecured transmissions [8]. Consequently, the security risks confronting the ADS-B pertain to the integrity of the communications between air traffic control (ATC) and aircraft. Inadequately secured connections may enable unauthorized interception or manipulation of ADS-B messages, particularly those containing sensitive data. Various forms of attacks on the ADS-B system, ranging in severity and impact on aircraft operations, include eavesdropping, jamming, message insertion, deletion, and modification (as shown in Table 2) [16].

[4] https://www.faa.gov/nextgen

[5] https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast

Table 2 Different types of attacks on the ADS-B system [16]

Attack type	Purpose of attack	Way of attack
Eavesdropping	Eavesdrop operating status information of aircraft (aircraft reconnaissance)	Obtain ADS-B data of the corresponding airspace through ADS-*B In*
Jamming	Jam the transmission of an ADS-B message in a specific airspace	By using an ADS-B transmitting device with sufficient high transmit power in the relevant frequency band
Message injection	Inject fake aircraft into a specific flight scenario, confusing ATC systems (aircraft target ghost injection/flooding)	By using a transmitting device with sufficient high transmit power in the relevant frequency band and capable of generating correct modulation and conforming to the ADS-B message format
Message deletion	Delete some or all of the information contained in a message (aircraft disapperance)	By implementation at the physical layer through constructive/destructive interference
Message modification	Modifify the information contained in a message (virtual trajectory modification)	Realized by overshadowing and bit-flipping at the physical layer of the system and can also be achieved by combining two attack methods

Hence, eavesdropping inflicts minimal harm as it lacks direct impact on the ATC system. Conversely, message deletion affects the aircraft surveillance system, causing temporary disappearance from the ATC map, albeit aircraft identification remains feasible through radar or multilateral systems. Message alteration exemplifies a typical "spoofing" maneuver and imposes significant repercussions on the ATC infrastructure. For instance, the "boiled frog" spoofing tactic [17] entails continuous but subtle alterations to aircraft position information within CSDP messages. This method poses challenges to surveillance technologies like radar systems and positioning, making it arduous to discern minor deviations falling within adjustment accuracies. Consequently, this leads to imprecise aircraft control by air traffic control and delayed system responses to avert mid-air collisions [8].

4.1.2. ADS-B spoofing

A spoofing attack targeting the ADS-B system involves the manipulation of ADS-B messages, accomplished by inserting counterfeit data. This form of attack can originate from both terrestrial and aerial sources. Figure 3 provides an elucidation of two distinct variants of spoofing assaults on the ADS-B: message insertion spoofing and ground station spoofing. In the former, attackers utilize cost-effective Software-Defined Radios (SDRs) to either rebroadcast previously captured messages (termed repeat attacks) or transmit newly generated, accurately modulated false messages (characterized as introducing ghost planes). The primary objective of such an attack is to fabricate the presence of non-existent entities, colloquially known as ghost aircraft, with the intention of disrupting Air Traffic Control (ATC) systems. In the latter variant, attackers manipulate the ICAO address within ADS-B messages by utilizing an ADS-B transponder airborne, masquerading as a recognized and trustworthy aircraft, thereby evading detection by surveillance mechanisms.

Thus, depending on the way the spoofed messages are generated, ADS-B spoofing attacks can be divided into three types:

- message or IQ data replay attack,
- ghost aircraft injection attack, and
- aircraft spoofing attack [8].

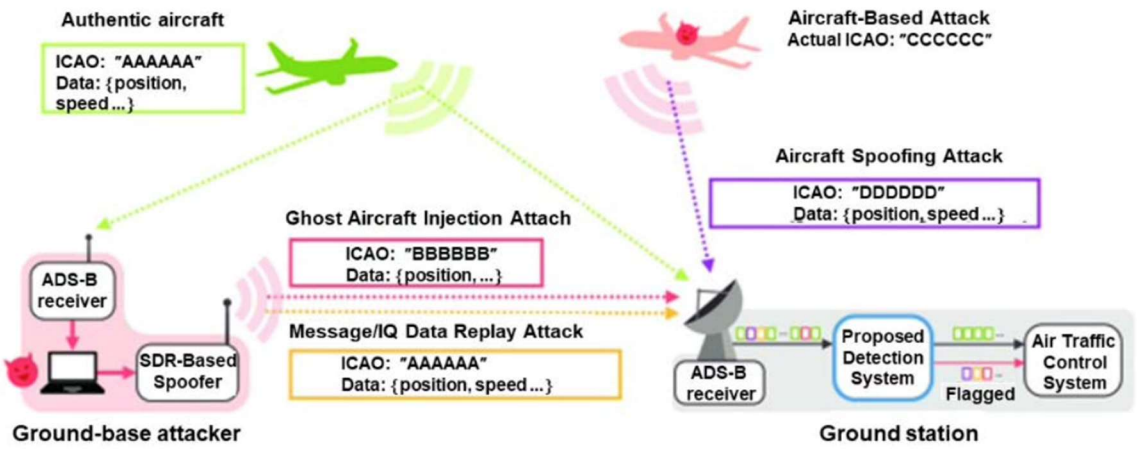


Figure 3 Illustration of two types of attacks on the ADS-B: the ground-based attack, using a SDR spoofer and an aircraft-based attack where the attacker uses an ADS-B transponder with a changed ICAO address [18]

In a scenario known as message/IQ data replay attack, an adversary stationed on the ground captures the contents of authentic ADS-B messages or IQ data utilizing a Software Defined Radio (SDR). Subsequently, the attacker retransmits these recorded messages at a later point without altering their original content. This form of attack exhibits a high level of sophistication owing to the wealth of information embedded within the captured IQ data, including details related to the Doppler effect, transmitter characteristics, and channel characteristics, making it arduous to replicate through conventional means.

Ghost aircraft injection attack involves a ground-based attacker utilizing an SDR device to transmit falsified ADS-B messages containing arbitrarily chosen content. Specifically, the attacker can fabricate trajectories for nonexistent aircraft ("ghosts") and craft corresponding ADS-B messages by meticulously selecting Doppler displacements. This manipulation renders these phantom aircraft visible to ground stations.

In an aircraft spoofing attack, a malicious aircraft endeavors to impersonate a recognized or trusted aircraft by spoofing its ICAO address while concealing its true identity. Given the physical presence of the deceptive aircraft, such masquerade attempts remain undetected even when a secondary radar surveillance system is deployed.

To detect spoofing, i.e. for the protection of wireless ADS-B communication, various security methods have been proposed, based on the existing cryptographic techniques. An alternative to this are non-cryptographic approaches which are based on signal separation (PHY-layer signal separation), time and position verification (such as TDoA-MLAT)[30], Doppler shift, etc. The most recently developed methods for ADS-B system spoofing detection are based on the predictions of mathematically set models and network analysis [8]. One of these is the method based on a SODA-DNN (Deep Neural Network) spoofing detector [18], whose application allows the detection of spoofing attacks with a very high probability and a very small proportion of false alarms, which is a significant improvement over other state-of-the-art detectors.

4.2. GNSS

The act of spoofing within the Global Navigation Satellite System (GNSS) context entails the dissemination of fabricated signals with the aim of deceiving recipient receivers into interpreting them as genuine signals. Consequently, these receivers may derive inaccurate position fixes, erroneous clock offsets, or both. A systematic dissemination of false position or timing fixes could potentially induce hazardous behavior in the recipient platform, which operates under the assumption of the validity of the received fixes. Noteworthy instances include instances where Global Positioning System (GPS) spoofing resulted in the inadvertent descent of a hovering drone and the deviation of a yacht from its intended course.

Efforts directed towards spoofing defense primarily revolve around the detection of such attacks to alert the recipient receiver regarding the unreliability of its navigation fix and clock offset. A secondary aim involves restoring a dependable navigation and timing solution.
Receivers equipped with receiver autonomous integrity monitoring (RAIM) mechanisms at the pseudorange level already possess a basic defense mechanism against spoofing. An incongruous set of five or more pseudoranges would enable the receiver to identify an unsophisticated spoofer who transmits one or more

false signals without striving to achieve a plausible consistency. In 2001, the Volpe report warned of the potential that a sophisticated, subtle form of spoofing might outflank this defense[6].

The potential threat posed by spoofing in the GNSS community garnered scant attention within open literature until the development and successful testing of a spoofer against a commercial off-the-shelf (COTS) receiver. This integrated receiver/spoofer leverages knowledge of authentic GNSS signals and its positional relationship with the target. Its modus operandi involves capturing each receiver channel by aligning spoofed signals with authentic ones from visible satellites. The spoofer initially emits signals at low power, gradually escalating until it seizes control of the receiver's tracking loops. Subsequently, it subtly veers the victim off course to a false position or timing fix, employing a drag-off strategy to elude detection by the receiver's tracking loops, which remain locked throughout the attack. Detection evasion also extends to rudimentary RAIM techniques, as the falsified signals consistently align with the spoofer's prescribed false fix.

Interest in GNSS spoofing surged following reports of real-world malevolent spoofing incidents. Notably, Iranian military forces purportedly intercepted a highly classified CIA drone in December 2011, allegedly employing spoofing to coerce it into landing in Iran under the guise of landing at its designated base in Afghanistan[7]. Speculation of spoofing activities has also arisen in the Korean peninsula. During the war in Ukraine GPS signals were widely disrupted to prevent strikes by Russian drones.[8] Despite these instances, confirmed instances of coordinated receiver/spoofer attacks remain elusive.

Live-signal spoofing experiments have been conducted under controlled conditions, exemplified by the drone interception and yacht spoofing experiments, aimed at assessing the threat landscape and potential countermeasures. Similar assessments have been conducted by the DLR in Germany[9].
Growing apprehension surrounding GNSS spoofing stems from the accessibility of inexpensive programmable signal simulators, facilitating potential attacks. Notably, a fully functional software-defined GPS signal simulator was publicly released on GitHub in June 2015, capable of running on various low-cost COTS RF generation platforms[10]. A researcher at the University of Bath in the U.K. verified its efficacy as a spoofer against standard civil GPS receivers. Such developments highlight the feasibility of developing spoofing capabilities for under $5k using COTS GNSS signal simulation and record-and-replay devices.

A plethora of potential targets exists for malicious spoofers, ranging from military assets like surveillance drones to civilian infrastructure reliant on GNSS for navigation or precise timing. Despite advancements in encryption technology rendering properly secured receivers impervious to typical spoofing attacks, vulnerabilities persist, with the potential for meaconing attacks against encrypted signals.

Despite heightened awareness of GNSS spoofing since 2008, no commercially available COTS civilian receivers offer robust defense against state-of-the-art attacks. While some manufacturers are exploring solutions, tangible defenses remain absent from the market. Nonetheless, numerous promising authentication techniques have emerged and been demonstrated in research literature.

The Federal Aviation Administration (FAA) has mandated all civil aircraft to be ADS-B Out equipped by January 1, 2020. The ADS-B Out broadcast sent to Air Traffic Control (ATC) consists of the aircraft’s position, velocity, and other aircraft-specific information, all of which being unencrypted, poses a serious integrity threat. With readily available ADS-B trackers[11], a spoofer can accurately track an aircraft to generate a spoofed trajectory that can go undetected.

GPS spoofing is a more challenging and technology-intensive operation as compared to brute-force jamming since a failed spoofing attempt can still yield the desired or unintentional jamming effects as its byproduct. In a basic spoofing attack type termed as ‘‘Meaconing’’, the attacker simply captures the authentic GPS signals and re-transmit them towards the target. Also, an attacker could orchestrate a more advanced attack by constructing a fake GPS signal containing malicious information. Such attacks are termed as ‘‘Fabrication’’ [14].

[6] https://rosap.ntl.bts.gov/view/dot/8435

[7] https://www.wired.com/2011/12/iran-drone-hack-gps

[8] https://www.newscientist.com/article/2415318-ukraine-will-spoof-gps-across-the-country-to-stop-russian-drones

[9] https://elib.dlr.de/188374/

[10] https://github.com/osqzss/gps-sdr-sim

[11] https://www.flightradar24.com/build-your-own

Humphreys et al. groups the GPS spoofing attacks into three categories as (a) Simplistic, (b) Intermediate and (c) Sophisticated, based upon the complexity of the attack and the used hardware [19].

- Simplistic GPS spoofing is broadcasting arbitrary spoofed GPS signal without catering for the state of the targeted receiver.
- An intermediate GPS spoofing attack is centered on pre-surveyed information about the target such as publicly available parameters of authentic GPS signal being received by the victim receiver at the time of the attack.
- Lastly, a sophisticated attack uses multiple coordinated phase-locked intermediate spoofers to evade spoofing detection protocols of the target receiver.

The absence of an authentication mechanism renders the GPS receiver incapable of discerning between genuine and malevolent signals. Furthermore, due to its unrestricted accessibility and the availability of technical parameters such as C/A code modulation in the public domain, the Civil GPS is susceptible to replication through signal simulation or inexpensive open-source equipment. In contrast, duplicating the authentic P(Y) code utilized by the US Department of Defense (DoD) is technically unfeasible owing to its classified signal structure and the limited disclosure of information regarding the encryption technique employed.

A GPS spoofing attack aims to manipulate the PVT (Position, Velocity, Time) calculations at the receiver's end, thereby potentially causing disruptions or deviations in time measurements and introducing errors in location measurements, as elaborated in subsequent sections.

4.2.1. Time spoofing

Spoofed GPS signal transmitted by an attacker can cause time-bias and abrupt changes in the victim's receiver clock [19]. In the case of a swarm of drones being controlled by a master drone, this type of attack will have catastrophic consequences as an alteration in the time of reference clock may induce errors in PVT calculations by the victim. Due to this clock offset, the master drone would be required to recalculate its position, which may lead it to a collision course with the slave drones within the swarm [14].

In addition to drones, the manipulation of time caused by GPS spoofing presents a significant risk to various time-dependent systems, including those utilized in the finance and banking sector, cellular communications, and energy distribution networks. CDMA-based communication systems' base stations rely on GPS-referenced time for inter-tower communications. A study conducted at the University of Texas showcased the susceptibility of CDMA-based cellular communications to GPS spoofing attacks, inducing a 10us drift within 30 minutes, resulting in communication disruptions. Similarly, researchers have illustrated the efficacy of GPS-based time spoofing attacks against GPS time-reference receivers employed by Power Measurement Units (PMUs) in smart grid systems. Through a meticulously designed spoofing attack, a 400us time drift was induced, surpassing the standard accuracy threshold for measured phased angles recorded by PMUs. Moreover, it has been demonstrated that a rudimentary spoofing attack utilizing a Software Defined Radio (SDR) can manipulate time in high-end smartwatches. Additionally, during DEFCON 25, researchers successfully showcased time manipulation through GPS spoofing attacks targeting Network Time Protocol (NTP) servers[12].

To summarize, time manipulation attacks utilizing GPS spoofing have the capacity to influence the perceived temporal data of GPS-enabled devices, thereby inducing inaccuracies in path computation and potential collisions among aerial platforms. Furthermore, such attacks may disrupt cellular communications and pose a risk of power distribution system failures, given their reliance on GPS-derived timing information, potentially leading to blackout scenarios.

4.2.2. Location spoofing

Fundamentally, a GPS spoofing attack entails the manipulation of the target's GPS-derived location calculations, leading to the generation of inaccurate position fixes. Drones heavily rely on GPS systems for navigation and positional awareness across various operational modes. This reliance renders them susceptible to exploitation through location spoofing attacks. The pervasive acceptance and integration of autonomous GPS-driven traffic management systems, exemplified by initiatives like the NEXT GENeration air

[12] https://www.youtube.com/watch?v=isiuTNh5P34

traffic system (NEXTGEN) in the USA[13], accentuates the realism and severity of GPS location spoofing threats, posing significant safety risks to such systems.

Recent research endeavors have effectively showcased the feasibility of GPS location spoofing against commercially available drones. For instance, within indoor environments, researchers successfully manipulated the location of a 3DR Solo drone utilizing an SDR device running an open-source script. Likewise, studies have demonstrated the vulnerability of sophisticated consumer drones from DJI to simplistic spoofing attacks, illustrating their susceptibility to manipulation in the absence of authentic GPS signals. The ramifications of spoofing a drone's location encompass deviations from intended flight paths, potential collisions, hijacking incidents, or even complete takeover, compelling the drone to land at a designated location chosen by the attacker [14]. Notably, autonomous drones can be enticed to deviate from their programmed routes through GPS course deviation attacks.

Beyond aerial platforms, GPS technology finds extensive application in diverse domains such as shipping, railway transport, freight trucks, and taxi services, facilitating tracking and location-based functionalities. In the realm of commercial trucking, GPS-based location spoofing can be leveraged to navigate unauthorized routes or facilitate fraudulent activities, including theft of cargo or the vehicle itself. Demonstrations of off-board attack scenarios have simulated the dissemination of falsified location data by cargo trucks. Additionally, in road navigation contexts, researchers have showcased the potential of SDR-based spoofing devices to generate spurious road routes in urban environments like Boston and Manhattan, USA, thereby posing risks of diversion, endangerment, or hijacking for victim vehicles [14].

4.2.3. End-goal

The spoofing attacks targeting moving objects, particularly UAVs, utilizing GPS can also be classified according to the goals pursued by the attacker. Various objectives may drive spoofing attempts, including diversion, destruction, endangerment, and interception of the target platform. The attainment of these objectives significantly relies on the capabilities of the spoofer in contrast to the anti-spoofing measures employed by the victim. A spoofer can target a GPS-guided aerial platform to accomplish the following objectives [14]:

- Diversion: Intentionally spoofing the location of the target to obstruct or delay its progression towards its intended destination.
- Destruction: Endangering the target by redirecting it towards a collision course, whether towards an aerial obstacle or the ground, by manipulating its altitude parameters.
- Hijacking: Temporarily gaining control of the target to seize control from the victim.
- Apprehension: Guiding the victim towards a predetermined location and compelling it to land safely within a secure zone for the purpose of capturing the drone or its cargo.

4.2.4. Attack Technique

The method utilized for GPS spoofing is contingent upon various factors, including the hardware capabilities of the spoofer, the sophistication of the algorithm employed, and the extent of information accessible to the spoofer regarding the victim's parameters, such as real-time location, velocity, antenna placement, and anti-spoofing features. Predicated on the specific attack technique employed, GPS spoofing attacks can be categorized into four distinct classifications [14].

Meaconing

Meaconing refers to the illicit practice of intercepting and rebroadcasting the original GPS signal to induce time-drift and confusion in GPS receivers. This phenomenon, also known as a "replay attack," constitutes a foundational form of spoofing. Meaconing is readily executable by attackers without the need to decrypt the encrypted P(Y) code, rendering it applicable to both civilian and military GPS signals. However, meaconing spoofer capabilities are confined to manipulating signal delay exclusively, lacking the ability to alter signal parameters [9].

Propagation Delay: Within this method of attack, the perpetrator fabricates a spoofed GPS signal featuring a customized signal propagation delay, transmitting it either prior to or following the genuine GPS signal while maintaining the authentic GPS timestamp. The spoofing entity can introduce either fixed or variable signal propagation delays for individual satellites within the counterfeit signal.

[13] https://www.faa.gov/nextgen

- Matching Delay: The attacker imposes a uniform delay value across all satellites comprising the spoofed signal.
- Non-matching Delay: By introducing varying delays independently for each satellite signal, the attacker disrupts signal propagation times, resulting in non-uniform delays within the spoofed signal.

Fabrication

A more sophisticated form of GPS spoofing entails the generation and transmission of synthetic GPS signals with the intention of misleading a GPS receiver, thereby compelling it to execute predetermined malicious commands, potentially leading to the acquisition of complete control over the system. In comparison to GPS jamming and meaconing, this represents a higher level of attack sophistication, involving the complete reconstruction of GPS signals. In such an attack scenario, a falsified GPS signal containing spoofed almanac and ephemeris data is emitted toward the GPS receiver with a power advantage, coercing it to synchronize with the fraudulent signal. Should the GPS receiver of the targeted UAV transition from the authentic GPS signal to the counterfeit one, the spoofer stands to potentially deceive the victim. An advanced GPS spoofing operation necessitates additional factors such as the attacker's ability to compute the spoofed location and the directional control of the spoofing signal for precise targeting [14].

Time alteration

The temporal integrity of the spoofed GPS signal can be compromised by an attacker through manipulation of either the GPS timestamp or the propagation time of the signal, or by altering both parameters concurrently.
GPS Timestamp Alteration: The attacker fabricates the spoofed GPS signal with a divergent GPS timestamp compared to the legitimate GPS signal, while maintaining the propagation time unchanged from that of the authentic signal. Modification of the GPS time-stamp results in distortion of the perceived time and location by the recipient receiver.
GPS Timestamp and Signal Propagation Manipulation: In this variant of attack, the perpetrator fabricates the spoofed GPS signal by simultaneously adjusting both the GPS timestamp and the signal propagation time.

Time and phase compensated attack

This represents an advanced category of attack wherein the attacker possesses comprehensive awareness of the target's geographical coordinates and the arrangement of its antennae. By meticulously assessing the orientation and placement of the target's antenna system, the spoofer formulates a spurious signal characterized by a methodical introduction of delay and manipulation of phase angles.

4.2.5. Open problems and future research directions

The Global Positioning System (GPS) has garnered significant attention from security researchers owing to its extensive utilization across various domains and its inherent susceptibilities [14]. This segment elucidates several unresolved issues concerning GPS spoofing and delineates potential avenues for future investigation to catalyze additional scholarly endeavors.

UAV Spoofing Using Follower Spoofers

Investigating the limitations of spoofing through the utilization of airborne follower/limpet spoofers presents a compelling avenue for research, as there exists a paucity of literature in this particular domain. Limpet spoofers are subject to stringent Size, Weight, Power, and Cost (SWaP-C) constraints. If successfully developed, they could be employed as adversarial follower drones or 'disloyal wingmen,' maintaining a consistent distance and angle relative to the target drone. While this strategy may streamline spoofing algorithms by removing variables related to range and angle fluctuations, it introduces novel research hurdles, such as orchestrating remote control of the follower UAV spoofer and reliably ensuring adherence to the follower trajectory without reliance on sensory or trajectory cues from the target UAV.

Spoofing Multi-GNSS Receivers

An ongoing research challenge involves investigating the feasibility of spoofing UAVs that utilize multi-GNSS (Global Navigation Satellite System) receivers. This endeavor entails employing multiple synchronized spoofers simultaneously, each directed at a distinct GNSS receiver. Spoofing parameters can be predetermined (fixed) or dynamically adapted to the targeted receiver. Noteworthy challenges in this pursuit encompass synchronization between spoofers, management of interference, power, and directivity.

SWaP-efficient DF for UAV Deployment

Outfitting the GPS navigation system of UAVs with Direction Finding (DF) capability holds promise for detecting and thwarting spoofing attacks. The ongoing challenge lies in the advancement and validation of SWaP-efficient DF systems, suitable for integration with GPS systems onboard lightweight aerial platforms, constituting an unresolved research endeavor.

Obfuscation-resilient spoofing algorithms

Methods for location obfuscation can be employed to counteract spoofing algorithms. An intriguing avenue for further research involves the creation of spoofing algorithms resilient to obfuscation, capable of deciphering obfuscation parameters and employing suitable spoofing techniques to counteract them. This field necessitates exploration of spoofing strategies adept at effectively spoofing UAVs despite inaccurate or incorrect location data.

5. Safety and Security: Interplay

5.1. Safety-Security Co-Design

From the safety aspect, the greatest challenge regarding safe urban airspace operations is the coordination of flight missions comprising both manned and unmanned aircraft. To this end, a complete single source picture of the sky is indispensable. With non-cooperative/malicious UAVs in urban airspace, we foresee the emergence of a UTM Service Provider (USP) which shall be able to obtain information from a drone detection and positioning systems (DDPS) and a ground-based traffic information system-broadcast (TISB). An implementation of DDPS is proposed to be based on a sensor-fusion system (e.g., radar and passive-RF) to detect and locate any type of UAVs including unauthorized ones, enabling blacklisting and whitelisting based on customer preferences.

From the security aspect, the proposed novel non-terrestrial network architecture, making use of heterogeneous links, comes with its own security requirements. On top of the inherent challenges in wireless security, we foresee that thwarting spoofing attacks will become a focus point of related security efforts. Such attacks could potentially cripple two major functionalities of the novel architecture utilizing unauthenticated communication protocols: i) advanced localization (via GNSS spoofing) and ii) the above-mentioned drone detection (via ADS-B spoofing). In addition, UAVs introduce an entirely new set of security challenges: they can be operated either by remote control or autonomously using onboard computers; accordingly, the UAV system is vulnerable to attacks that target either the cyber and/or physical elements, the interface between them, the wireless link, or even a combination of multiple components.

6G promises trustworthiness that translates to a holistic security architecture on the network level. While existing security solutions from 5G provide a solid foundation, the cyber-physical nature of 6G-connected aerial vehicles requires a thorough investigation. In addition to the traditional security attributes of confidentiality, integrity, and availability, access control and non-repudiation, we must consider that security threats may impact safety (and, thus, human lives) directly. Therefore, a security-safety co-analysis/co-design mindset is crucial [20].

Safety-security co-design is an approach that integrates safety and security considerations into the design and development of systems, products, or processes. It recognizes the interconnectedness of safety and security aspects and aims to address them in a holistic manner to ensure the overall reliability, resilience, and integrity of the system.
In safety-security co-design:

1. **Safety**: Safety focuses on the prevention of accidents, hazards, or failures that can lead to harm or damage to people, property, or the environment. It involves identifying and mitigating risks through measures such as redundancy, fail-safe mechanisms, and hazard analysis.
2. **Security**: Security, on the other hand, deals with protecting systems, data, and assets from unauthorized access, breaches, or malicious attacks. It involves implementing measures such as encryption, access controls, and intrusion detection to safeguard against threats and vulnerabilities.

The co-design aspect emphasizes the importance of addressing safety and security requirements together throughout the entire lifecycle of a system or product. This includes:

- **Early Integration**: Safety and security considerations are integrated into the initial design phase, ensuring that potential risks and vulnerabilities are identified and addressed from the outset.
- **Trade-off Analysis**: Trade-offs between safety and security requirements are carefully evaluated to find the optimal balance that minimizes risks without compromising functionality or usability.
- **Continuous Assessment**: Safety-security co-design involves continuous assessment and validation to ensure that safety and security measures remain effective as the system evolves and new threats emerge.

By adopting a safety-security co-design approach, organizations can create more robust and resilient systems that are better equipped to handle both accidental failures and intentional attacks, thereby enhancing overall safety, security, and reliability.

5.2. Background

Here, we briefly introduce some prominent safety and security analysis methods and adopt a safety-security co-evaluation method based on Systems Theoretic Process Analysis (STPA) [21].

5.2.1. Safety Analysis

Safety entails the absence of harm to equipment or individuals in the face of either random or systematic failures. Safety engineering encompasses the identification, evaluation, and reduction of potential risks to acceptable levels. A hazard denotes a possible event that could result in a safety breach, violating safety objectives. Risk quantifies the level of significance of a hazard, typically computed as a product of probability and severity, or occasionally with an additional factor reflecting the level of control [22].

During the conceptual phase, an initial hazard analysis is conducted to elucidate safety requirements. Subsequently, the preliminary product design undergoes assessment against safety objectives to unveil potential safety hazards. Once hazards are identified and prioritized, safety concepts are devised to mitigate these risks, refining into concrete safety requirements in subsequent phases.

In ISO 26262, the safety hazard analysis activity is termed Hazard Analysis and Risk Assessment (HARA), which remains agnostic to specific safety analysis techniques. Techniques like FTA, FMEA/FMECA, and STPA offer processes for hazard identification, linking hazardous events such as component failures to system-level safety. The Automotive Safety Integrity Level (ASIL) in ISO 26262 categorizes inherent safety risk in automotive systems or components. ASIL acts as a risk assessment model, determined by factors including severity of hazards, likelihood of exposure, and controllability by operators.

Traditional safety analysis techniques rely on probabilistic methods to estimate safety factors based on reliability, which refers to a system or component's ability to operate under specified conditions for a defined duration. These techniques typically assess the consequences of component failures and include methods like Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and Hazard and Operability Analysis (HAZOP), which have been utilized since the 1960s and are widely employed across industries.

In modern Cyber-Physical Systems (CPS), which integrate computation, networking, physical processes, and human interactions, safety hazards often arise from dynamic interactions between processes rather than individual component failures. Conventional safety analysis approaches, which primarily focus on component failure rates, may not adequately capture these hazards. To address this limitation, N. Leveson introduced Systems-Theoretic Process Analysis (STPA) as an alternative. STPA views safety as a dynamic control issue rather than solely relying on component failure, identifying various hazardous causes beyond failure scenarios. Its primary objective is to pinpoint inadequate control scenarios that could lead to accidents and develop detailed safety constraints to either eliminate or manage these unsafe conditions.

5.2.2. Security Analysis

Security entails safeguarding information or information services against intentional attacks or unintentional events. Security engineering involves identifying, assessing, and mitigating potential threats to acceptable levels. A threat refers to a possible event, deliberate or accidental, that may lead to a security breach, with intentional threats commonly termed cybersecurity attacks. Like safety risk, security risk is quantified by the probability and severity of a threat.

In the initial system design phase, security risk analysis aims to identify security requirements, enabling the design of mitigations in later engineering stages to prevent information compromise. This process typically begins with defining security goals, instantiated from overarching objectives like Confidentiality, Integrity, and Availability. By mapping threats to these security goals, risks are prioritized, allowing the formulation of countermeasures that translate into concrete security requirements and implemented as security functions to safeguard system assets.

Within the security standard SAE J3061, the security analysis activity is termed Threat Analysis and Risk Assessment (TARA), akin to the safety analysis activity HARA in ISO 26262 [23]. TARA identifies potential threats to system features and assesses associated risks. Unlike safety analysis, which focuses on functional safety items, security analysis covers a broader scope, as non-functional safety items may also be vulnerable to security risks. For example, infotainment systems like CD players or cellular devices in vehicles can serve as attack surfaces. Additionally, system security depends not only on individual component security but also on the security of their interconnections.

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives) is a method derived from ISO 27005, designed for analyzing, evaluating, and addressing risks associated with information systems [24]. It tailors a security policy to meet an organization's specific requirements, comprising five key steps: Circumstantial study - establishing the context; Identification of security requirements; Risk analysis; Identification of security objectives; and Determination of security requirements.

STRIDE is a widely used security analysis technique that encompasses both a threat model and a systematic approach to threat modeling [25]. It categorizes security threats into six types: Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, and Elevation of privilege. By providing a structured classification of threats, STRIDE facilitates comprehensive security analysis. Employing a software tool, the STRIDE threat modeling process commences with a functional description of the system depicted as a Data Flow Diagram (DFD), from which a set of threats is derived through the application of STRIDE threat categories.

5.3. A Practical Method for Safety-Security Co-Evaluation

To reconcile the divergent requirements of security and safety while mitigating potential conflicts, several methodologies have been introduced to integrate both facets of analysis. One such methodology is the Security-Aware Hazard and Risk Analysis (SAHARA), which amalgamates the principles of STRIDE and HARA methodologies [26]. SAHARA prescribes a sequential approach wherein security analysis precedes safety analysis: initially, security analysis is conducted utilizing the STRIDE framework to discern threats, followed by safety analysis employing HARA, wherein security threats influencing safety are treated as a specialized subset of safety hazards.

SAHARA represents a step towards harmonizing safety and security analyses. It offers a relatively accessible learning curve for engineers proficient in STRIDE and HARA methodologies. However, SAHARA adheres to the conventional HARA paradigm, characterized by an examination of system components to preclude failures or breaches, premised on a repository of knowledge concerning potential issues inherent in individual components. In contrast, the methodology proposed below, rooted in System-Theoretic Process Analysis (STPA), adopts a system-theoretic standpoint for safety-security co-analysis. Diverging from conventional approaches, this methodology facilitates a seamless integration of security and safety analyses into a unified framework, treating both safety and security as emergent properties resulting from system interactions with the environment. Instead of pinpointing hazards or threats to discrete components, the methodology scrutinizes the efficacy of the system's control structure to ensure predictable behavior. Such an approach suits the dynamic and complex nature of the envisioned combined ASN.

The EU ECSEL SECREDAS project proposed a STPA-based co-evaluation method to integrate the safety and security analysis for the domain of connected vehicles [1]; we adopt this methodology with minor modifications. This method provides insight into the interplay between safety and security through an initial cross-discipline analysis before the individual safety/security analysis. Revealing such interplay allows us to (1) assess the impact of security risks on safety, and vice versa, (2) disclose the cases where the two aspects have conflicting interests, e.g. a safety-enforcing technology may lead to security risks [21].

STPA, rooted in systems theory, diverges from traditional safety analyses, which predominantly attribute safety hazards to component failure rates. Instead, STPA identifies the intricate interactions between modern systems and their environments as the primary sources of safety hazards. Leveson underscores that accidents in complex systems may occur due to unforeseen interactions among the system's control software, sensors, and environment, even in the absence of component failures. Addressing such hazards, STPA frames safety as a dynamic control challenge rather than a consequence of individual component failures. Its overarching aim is to pinpoint deficient control scenarios that could precipitate accidents and devise detailed safety constraints to eliminate or manage these unsafe conditions.

In the realm of cybersecurity, conventional security analyses typically focus on threats to system assets, such as data or services. However, in modern Cyber-Physical Systems (CPS), security incidents can also pose safety hazards due to intricate interactions among cyber processes, physical processes, the environment, and human actors. For example, in the Jeep Cherokee case, white-hat attackers remotely manipulated a car's functions via its cellular connection. Acknowledging the unpredictability of real-world attacks, we draw inspiration from STPA to conceptualize cybersecurity as a dynamic control issue rather than merely a matter

of threat prevention. Adopting STPA's system-theoretic perspective, a security incident may arise when the system fails to detect inadequate scenarios. Consequently, safety-security analysis aims to identify and address such inadequate scenarios by enhancing control loops for monitoring system interactions. This viewpoint enables the mitigation of both safety and security incidents through observation, prevention, or detection of hazardous actions.

The STPA-based safety-security co-analysis method scrutinizes a system's process model, reflecting its initial design. Safety and security risks manifest as undesired scenarios resulting from complex interactions among the system's internal processes or between the system and its environment. This approach empowers designers to adopt a cross-disciplinary perspective, unveiling risks and devising mitigation strategies in the early stages of the conceptual phase.

STPA proceeds with the following steps: (A) Identifying safety accidents and hazards; (B) Defining actors and control actions; (C) Identifying hazardous control actions, and (D) Identifying scenarios.

5.3.1. Identifying safety accidents and hazards

STPA delineates a safety **accident** as "an undesired or unplanned event resulting in loss, encompassing human life or injury, property damage, environmental pollution, or mission loss," and defines a hazard as "a system state or set of conditions that, in conjunction with specific worst-case environmental conditions, will lead to an accident (loss)". These identified system accidents and hazards facilitate the tracing of lower-level analysis outcomes to their system-level ramifications. For instance, in the context of a connected car, a safety accident could entail "the vehicle collides with objects or individuals due to an inability to brake," potentially stemming from various safety hazards, such as a malfunctioning electronic or mechanical component within the braking system or a failure of an Electronic Control Unit (ECU) following an update with a tampered image.

Security extension. The co-evaluation method incorporates an extension to address security incidents concurrently with safety accidents and hazards. In the realm of connected cars, security incidents may serve as potential causes of safety accidents, and such cause-effect relationships are identified accordingly. Drawing inspiration from the security analysis methodology EBIOS, our approach identifies security incidents, referred to as "feared events" in EBIOS, as breaches of a primary asset's security criterion. Primary assets encompass system functions, hardware/software components, or data stored, processed, or transmitted within the system. Typical information security criteria include availability, integrity, and confidentiality, though additional criteria like Authenticity, Non-repudiation, and Authorization are left for future exploration. Depending on the functionality of impaired assets, a security incident may or may not precipitate safety accidents. For instance, a compromised ECU within the car's braking system constitutes both a security incident, due to the breach of ECU function integrity, and a safety hazard, potentially leading to a safety accident. Conversely, an unauthorized alteration to mileage data stored in a car constitutes a security incident without posing a safety hazard. This extension to STPA enables the identification of security incidents as potential contributors to safety accidents within the analytical framework.

5.3.2. Defining actors and control actions

In STPA, a system is characterized by its functional control structure, which comprises hierarchical control loops. Actors within these loops are classified into two categories: controllers, responsible for executing operational logic and making decisions based on specific conditions, and controlled processes, tasked with executing commands from controllers and providing feedback. It's noteworthy that a controlled process can be further decomposed into a control loop, consisting of a set of controllers and controlled processes. For instance, at the highest level, an integrated flight management system comprises several control loops (see Section 5.4). System functionality is realized through the execution of control actions by these actors, such as the UTM Service Provider communicating with authorized UAVs to coordinate their flight.

Security extension. The co-evaluation method extends control actions by incorporating parameters that represent data transmitted by these actions through specific communication channels. In the original STPA framework, control actions denote real-time control signals, like a driver applying brakes in a car, which are either executed as intended or not, depending on the action provider. However, in Information and Communication Technology (ICT) systems, control actions often involve data transmissions via

communication channels like the Internet and diverse wireless links. The successful execution of a control action hinges not only on the action provider but also on the reliability of the communication channel. By delineating between control actions and transmitted data, the proposed approach enables the differentiation of various instances of unexpected control action behavior, which could stem from improper action provision or the compromise of transmitted data.

5.3.3. Identifying hazardous control actions

Within the framework of STPA, erroneous interactions and flawed safety constraints are recognized as primary contributors to accidental scenarios. These issues are identified by pinpointing hazardous control actions—actions conducted improperly that may lead to safety hazards. STPA provides heuristic keywords for deriving hazardous control actions from regular actions, including "Not provided," "Provided (when not supposed)," "Provided too late/early," "Provided out of order," "Stopped too soon," or "Applied too long." Each hazardous control action is then linked to its consequences, which are among the safety hazards identified earlier.

Security extension (1). In ICT systems, where control actions often entail transmitted data over potentially compromised channels, it's crucial to expand the analysis beyond individual actions. The data can be compromised during transmission, even if the action itself is properly conducted. Hence, we introduce new keywords for deriving hazardous control actions:

- "Provided but not received": denoting a scenario where the control action is executed by the sender, but the transmitted data is not received by the intended recipient. This aligns with "Unavailability" in security terminology.
- "Provided but impaired": signifying a situation where the control action is executed, but the received data is compromised, corresponding to "non-integrity" in security terminology.
- "Provided but disclosed": highlighting a control action intended to be confidential but is disclosed.
-

Security extension (2). For safety-security co-analysis, it's imperative to understand the impact of hazardous control actions not only on system safety but also on security. Here, the method associates identified hazardous control actions with their resultant security incidents. For instance, if the UTM Service Provider sends a command to an authorized drone that is compromised during transmission, this hazardous control action can be identified using the keyword "Provided but impaired" for the control action "send(command)." Consequently, drones might get steered towards otherwise dangerous or restricted areas, constituting both a security incident and a safety hazard.

5.3.4. Identifying scenarios

The final stage of STPA delves into the causes of hazardous control actions within specific scenarios, typically arising from flaws in the process model due to inadequate feedback. Two types of scenarios are examined: (1) Why would hazardous control actions occur? (2) Why would a control action be improperly executed or not executed at all? From these scenarios, a set of safety requirements is derived to address such design flaws.

While the preceding steps considered the existence of control actions and feedback, they did not explore how feedback is measured or detected, or how control actions are executed. Scenarios pinpoint the precise causes of hazardous control and feedback, refining the control structure. Scenarios leading to hazardous actions may involve:

- Inadequate control algorithms: Flaws in the control algorithm or its implementation, such as assuming previous control actions were executed properly.
- Inadequate process model: Issues like delayed or absent feedback, incorrect feedback, misinterpretation, or disregarding of correct feedback by the controller.
- Unsafe control input from another controller.

The scenario analysis stage completes a causal-effect chain, identifying which scenarios lead to hazardous control actions, which in turn result in security incidents or safety hazards. In cases where security incidents also pose safety hazards, an unsecure scenario coincides with an unsafe one. For example, in a flight management system, if an intrusion into an authorized drone goes undetected, leading to the hazardous control action of sending a tampered message to the UTM Service Provider, the consequence—such as misguided flight management commands by the UTM—constitutes both a security and safety hazard.

It's noteworthy that the STPA-based co-analysis method offers a distinct perspective compared to conventional safety/security analysis techniques. Canonical techniques focus on identifying and preventing known failures/attacks to components—essentially, what should not happen. Conversely, STPA analysis aims to ensure the system always behaves correctly by monitoring its behavior via feedback. This forward-looking approach is particularly advantageous for security analysis, given the unpredictability of malicious attacks. As demonstrated in the subsequent case study, STPA analysis underscores the importance of incorporating feedback, often overlooked in security engineering.

5.4. Case study: detecting unauthorized drones in urban airspace

Despite attracting attention in diverse civil and commercial applications, Unmanned Air Vehicles (UAVs - also known as drones) undoubtedly pose several threats to airspace safety that may endanger people and property. While such threats can be highly diverse in terms of the attackers' intentions and sophistication, ranging from pilot unskillfulness to deliberate attacks, they all can produce severe disruption. Between 19 and 21 December 2018, hundreds of flights were cancelled at London Gatwick Airport following reports of visual UAV (drone) sightings. The London Gatwick incident and similar ones clearly illustrate that coordinating and authorizing flight missions of manned and unmanned aircraft is not sufficient to ensure safe urban airspace operations. Coming EASA and FAA regulations on geofenced no-fly zones and direct remote identification will prevent UAVs from flying unintentionally at locations where not allowed to, but those regulations will not stop non-compliant UAVs or malicious UAV activities. Detecting and locating UAVs not broadcasting their location (non-cooperative) is required to ensure a complete, single source picture of the sky in urban areas.

5.4.1. System model

To remedy the issue with non-cooperative UAVs in urban airspace, we propose that a UTM Service Provider (USP), shall be able to obtain information from a drone detection and positioning systems (DDPS) and a ground-based traffic information system-broadcast (TISB). An implementation of DDPS is proposed to be based on a sensor-fusion system (e.g. radar and passive-RF) to detect and locate any type of UAV. An implementation of GBAT is proposed to be based on a ground-based low-power ADS-B transmitter and an ADS-B receiver. GBAT is exchanging information in two directions. Firstly, the ground-based ADS-B transmitter of GBAT is used to broadcast the location of unauthorized/non-cooperative UAVs. A low-flying manned aircraft will then obtain the information directly in the aircraft's built-in ADS-B receiver. Secondly, there is information exchange in the opposite direction as well. A low-flying aircraft broadcasting its location using its built-in ADS-B transponder would be picked up by the ground-based ADS-B receiver of GBAT and then sent to authorized UAVs via USP.

Note that one can foresee a control mechanism for grounding unauthorized UAVs by force, effectively transforming the interaction between the DDPS and unauthorized UAVs a whole abstract control loop. We leave the design and analysis of such mechanism for future work.

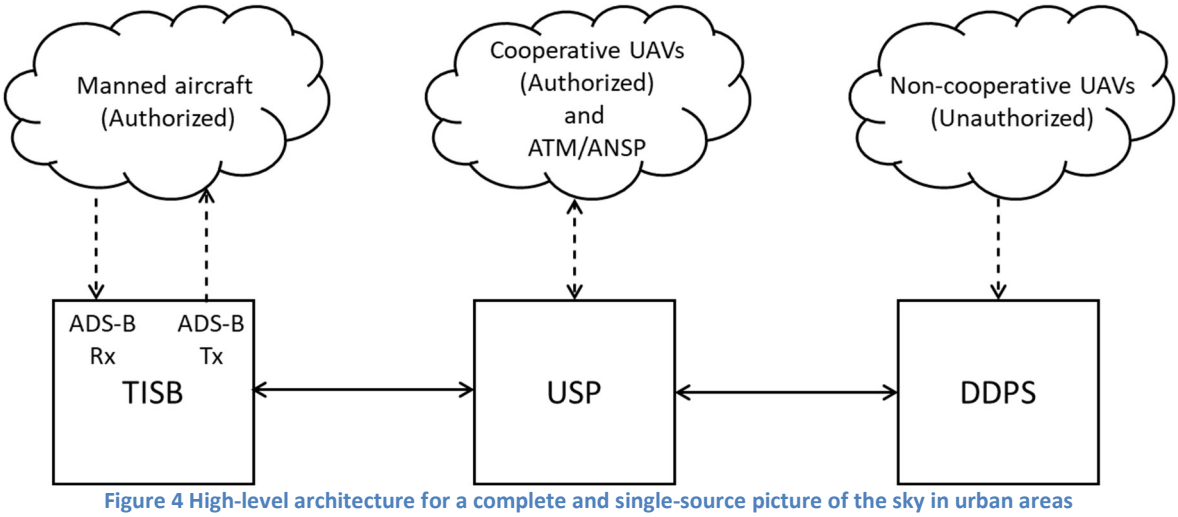


Figure 4 High-level architecture for a complete and single-source picture of the sky in urban areas

5.4.2. Preliminary safety-security co-evaluation

This section summarizes our case study on the drone detection system with the safety-security co-evaluation method going through the four steps presented above. We make several simplifications in the case study to keep the analysis tractable and meaningful at the same time.

Safety accidents and hazards

With flying UEs, the malfunction or unavailability of any of the ground-based control nodes such as the TISB or USP or, in fact, the malfunction of UEs themselves, may cause safety-related accidents. Data that has been tampered with, e.g., fake location updates, may also cause accidents. The malfunctions of the safety-critical subsystems, whether unavailability or abnormal behavior, may be caused by receiving and/or sending illegitimate data.

In this case study, we consider only accidents and hazards caused by the malfunctions of ICT subsystems which may be a consequence of compromised communication and subsequent decision-making potentially involving ground-based flight management entities. Other causes of safety accidents, e.g., failure of flying devices or power outages, are out of the scope of this preliminary analysis.

Table 3 Safety accidents of flying UEs

	Safety Accident
A-1	UAV collides with objects or people
A-2	Manned aircraft collides with UAV, objects, or people

Table 3 summarized the safety accidents of flying UEs that we identified, making a distinction based on the actual type of UE actively involved, as they are controlled by different ground-based subsystems.

Based on the accidents above, we identified four safety hazards connected to the two different UE types (see Table 4): i) the UE receiving invalid/falsified information on which it decides on its trajectory, and ii) the UE not receiving information in time.

Table 4 Safety Hazards of Flying UEs

	Safety Hazard	Safety Accident
H-1	UAV navigating abnormally due to receiving invalid information	**A-1**
H-2	Manned aircraft navigating abnormally due to receiving invalid information	**A-2**
H-3	UAV navigating abnormally due to not receiving information in time	**A-1**
H-4	Manned aircraft navigating abnormally due to not receiving information in time	**A-2**

Security incidents

In flying UEs, the assets include all data processed or stored in the UE, including system logs, map data, as well as all component functions, including sensors, actuators, internal communication networks, in-flight entertainment systems, etc. Generally speaking, the cybersecurity incidents of a flying UE include any security breach which may happen to any of these assets. Here, however, we concern ourselves only with the incidents as effects of unsecure communications and subsequent unsafe decision-making of UEs potentially involving ground-based flight management functions. Inside flying UEs, the major assets which may be impacted are the aircraft/UAV maneuvering function (with a human in the loop) through the communication subsystem.

Security incidents are derived by associating the violation of the well-known CIA (Confidentiality, Integrity, Availability) security criteria to the asset. Table 5 summarizes the identified cybersecurity incidents, and their potential impact on safety are given in the rightmost column. Observe that I-1, I-2, I-4, and I-5 are both security incidents and safety hazards, while I-3 and I-6 are only security incidents. Nevertheless, from the cybersecurity point of view, an incident should be identified and mitigated, irrespective of its safety impact.

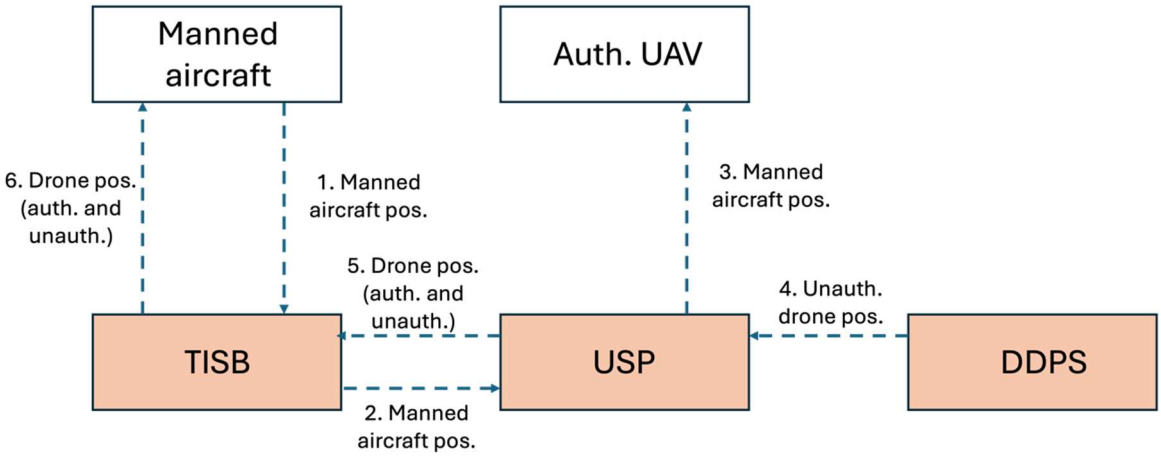
Table 5 Security Incidents of Flying UEs

	Security Incident	Safety Accident
I-1	(Availability) Manned aircraft communication subsystem shuts down (overload)	**A-2**
I-2	(Integrity Manned aircraft communication subsystem receives invalid information	**A-2**
I-3	(Confidentiality) Manned aircraft control command sequence exposed to eavesdropper	**None**
I-4	(Availability) UAV communication subsystem shuts down	**A-1**
I-5	(Integrity) UAV communication subsystem receives invalid information	**A-1**
I-6	(Confidentiality) UAV Control command sequence exposed to eavesdropper	**None**

Actors and control actions

The control diagram of the system under consideration is constructed in Figure 5. Note that we made several simplifications to focus on the most significant actions and subsystems. First, as regulated by the FAA[14], UAVs have no ADS-B Out (sending) capability, but the authorized drones have ADS-B In functionality, so they are able to receive updates on other flying endpoints from the USP. Second, we do not model the ATM/ANSP function separately, we assume it is integrated with the USP. Third, as unauthorized UAVs cannot be controlled at this time, we simply omit them from the control diagram; however, their presence and location are picked up and relayed by the DDPS. We also omit communication from USP to DDPS for similar reasons. Last, we assume that all wired communications (TISB-USP-DDPS) are secured and authenticated, as they do not have to depend on standard but unsecure communications protocols. The resulting simplified control diagram is depicted in Figure 5. Control actions are numbered starting from the information source, grouped by information type. Controllers (red boxes) and controlled processes (white boxes) could be further refined into control structures hierarchically, which facilitates multi-level analysis.

Figure 5 Control diagram



Next, we list the actions grouped by the actors in Table 6.

Table 6 Actors and Control Actions

	Control Action	
Manned aircraft	1. Send(aircraft.pos,TISB)	Broadcasts its own position (TISB receives)
TISB	2. Relay(aircraft.pos,USP) 6. Relay(drone.pos,MA)	Sends aircraft position to USP Broadcasts drone pos. (Manned aircraft receives)
USP	3. Relay(aircraft.pos,UAV) 5. Relay(drone.pos,TISB)	Broadcasts aircraft position (Auth. UAV receives) Sends unauth+auth drone pos. to TISB
Authorized UAV	-	-

[14] https://www.federalregister.gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft

DDPS	4. Relay(unauth.pos,USP)	Senses and sends unauth drone pos. to USP

Hazardous control actions

This step identifies hazardous control actions and their potential consequences as safety hazards or security incidents. Here we assume that the DDPS do not make errors in sensing unauthorized UAVs. We also assume that wireline relaying of data may be delayed but cannot be compromised or sent out of order. Note that security incidents that do not bear safety consequences are not represented. Observe that some hazardous control actions may cause a security incident, a safety hazard, both, or neither.

Controlled Process	Control Action	Not provided/not received	Provided when not supposed	Provided but impaired (invalid/tampered)
UAV	Send(aircraft.pos,TISB)	H-3 lack of aircraft info	I-4 UAV flooded with aircraft info	H-1 navigating on invalid aircraft info I-5 spoofed aircraft info
UAV	Relay(aircraft.pos,USP)	H-3 lack of aircraft info	-	-
UAV	Relay(aircraft.pos,UAV)	H-3 lack of aircraft info	I-4 UAV flooded with aircraft info	H-1 navigating on invalid aircraft info I-5 spoofed aircraft info
Manned aircraft	Relay(unauth.pos,USP)	H-3 lack of unauth. drone info	-	-
Manned aircraft	Relay(drone.pos,TISB)	H-4 lack of drone info	-	-
Manned aircraft	Relay(drone.pos,MA)	H-4 lack of drone info	I-1 aircraft flooded with drone info	H-2 navigating on invalid drone info I-2 spoofed drone info

Scenario analysis

In this step, we identify the scenarios where process model flaws cause hazardous control actions. Against the process model flaws, safety constraints and security countermeasures are identified and presented as requirements. Then, the security and safety requirements can be evaluated in the context of the control structure with respect to different scenarios, and then be refined. Table 7 summarizes the result of this step.

Table 7 Scenario analysis

Hazardous control actions	Safety hazards and security incidents	Process model flaws	Safety and security requirements
Not provided/not received	H-3 lack of aircraft info H-4 lack of drone info	aircraft, UAVs, and ground functions incorrectly believe that there is no new positioning data	R-1 ground functions should do periodic polls for information among themselves if nothing received
Provided when not supposed	I-1 aircraft flooded with drone info I-4 UAV flooded with aircraft info	aircraft and UAVs incorrectly believe that they have to process all ADS-B In messages	R-2 ADS-B messages in both directions should be authenticated
Provided but impaired	H-1 navigating on invalid aircraft info H-2 navigating on invalid drone info I-2 spoofed drone info I-5 spoofed aircraft info	aircraft, UAVs, and TISB incorrectly believe that all ADS-B In messages contain valid information	R-3 ADS-B messages in both directions should be integrity protected and authenticated

Note that R-3 contains R-2 as a subset. It is easy to see that, e.g., R-3 is both a security (mitigating I-2 and I-5) and safety requirement (mitigating H-1 and H-2). Through this simplified use case, we showed that the safety-security co-design/co-analysis approach is essential for building and operating trustworthy cyber-physical systems.

6. Safety and Security: Impact on Sustainability

The information and communications technologies (ICTs) industry plays a vital role for combating the world's climate change and sustainability challenges. The United Nation's introduction of its sustainable development goals (SDGs), which include a framework of the 17 areas that need to be addressed and that works as a guideline for reaching a sustainable world [31]. The ICTs are the backbone of today's digital economy and have enormous potential to accelerate the progress for reaching the SDGs and improve people's lives by enabling and providing worldwide mobile connectivity and global coverage [32]. ICT is crucial for achieving all the 17 SDG goals (displayed in Figure 6 below) and should be considered as a catalyst for accelerating the three pillars of sustainable development: economic growth, social inclusion, and environmental sustainability.

Figure 6 The UN's 17 Sustainable Development Goals

With more than half of the world's population already living in urban environments, and with the estimation that about 70% of the world's population will be living in urban areas by 2050, ICTs will be essential in offering innovative ways to managing cities more effectively through, for instance, smart buildings, intelligent transport systems, smart water and waste management, and effective energy consumption etc. The establishment of UAM will also play a vital role in the evolution of urban sustainability. Satellite-based communication systems do not only provide data for monitoring of weather, climate data etc. but can ultimately also complement the terrestrial communication networks by providing additional connectivity for rural and sparsely populated areas.

The 2030 Agenda for Sustainable Development highlights that the continuous development and the spread of information and communication technology has a great potential to bridge the digital divide [34]. In Europe, the SESAR ATM Masterplan predicts a growth of air traffic in the future [33]. But while the benefits of a continued growth in air traffic for European citizens are clear in terms of mobility, connectivity, and availability of new services (e.g., services that will be enabled by drones/UAV etc.), this growth also brings concerns about climate impacts. These concerns are prompting the aviation industry to accelerate its efforts to address air travel environmental sustainability.

The EU has a plan to cut greenhouse gas by at least 55% by 2030 and reach its carbon neutral goal by 2050 [35]. In support of this goal, the SESAR project has prioritized solutions that will gradually contribute to the elimination of environmental inefficiencies caused by the aviation infrastructure. This will be done by ensuring that it provides solutions that will exploit the potential offered by next generation aerial vehicles and aircraft. The main ambition of the SESAR project is working towards the digitalization of ATM and to support electrification of aerial vehicles, where the overall goal is to strive for a more climate neutral aviation industry. The challenges of global climate change and the need to reduce our carbon footprint makes it critical that the next generation 6G networks employ the most energy efficient available technologies, that will reduce the dependency on non-renewable

sources and use solely renewable energy sources. In addition to energy consumption and emissions, the ICT sector's overall environmental impact must also be considered, including the handling of water consumption, raw material sourcing, and waste handling etc. 6G is considered by many to be the sustainable "Green G" [36]. Use cases that will emerge related to 6G and also to 6G-SKY, including all key actors in the entire value chains, will need to embrace a strong focus on sustainability and work actively towards reducing any climate change impacts.

In terms of future spectrum strategy and regulations, these should be seen as an enabler for technology with an essential focus on sustainability and will also work towards spectrum being used as efficiently as possible. The ITU has stated that it strongly supports and encourages the efforts of countries to leverage technology to accelerate progress towards the SDGs and is also developing a framework for assessing the impact – both positive and negative – of digital technologies on the climate" [37]. The 6G sustainability study in [38] has shown for a city scenario that HAPS can reduce grid energy of a mobile network by 10% to 50% by switching off terrestrial base stations. Large part of rural terrestrial sites are deployed for providing coverage and not for capacity need. HAPS can replace such towers in wide sparsely populated areas. Furthermore, novel hydrogen based power solutions are promising carbon free network operation.

7. Conclusions

In this deliverable, the safety and cybersecurity aspects of the combined ASN concept proposed by the 6G-SKY project are put forward and analyzed. As these aspects could warrant a standalone project, we put the focus on pressing issues elicited by the key characteristics of the envisioned network architecture that distinguish it from other 6G proposals.

First, we identified the defining properties of the architecture: i) the cyber-physical nature of the proposed system, ii) the inherent integration of flying UEs into the networks, and iii) the prevalence of unauthenticated and unencrypted communication protocols in the non-terrestrial networking domain exposing these systems to the threat of spoofing. Second, we provided an overview on the state of cybersecurity in aviation. We established the state of the art both in relation with manned aircraft and UAVs, setting the stage for the more specific threat analysis in the later sections. Third, we surveyed the challenges and proposed solutions around the threat of spoofing. As protocols like ADS-B and GNSS are both critically important for the non-terrestrial domain and are in heavy use in real-world deployments, it is imperative that the project is up to date in this topic. With novel attacks still being rolled out, especially targeting GNSS, the 6G-SKY project must either i) adopt or develop mitigation mechanisms or ii) augment or partly replace GNSS-based operation with more autonomous localization and synchronization solutions.

Finally, invoked by the cyber-physical nature of the combined ASN architecture, we introduced the concept of safety-security co-design and co-analysis. We provided an overview of related concepts, a brief introduction to existing techniques, and a more detailed background study on the STPA-based co-evaluation method conceived by the EU ECSEL SECREDAS projected in the context of connected and autonomous vehicles. Since flying UEs are themselves connected and some of them are envisioned to progress towards completely autonomous operation, this method represented an adequate match for our use cases. As a use case we proposed an integrated UTM system complete with functionality to detect and localize unauthorized drones; implementing the 6G-specific joint sensing and communication concept, the DDPS itself is a safety enabler for the mission-critical networked aviation sector. Through carefully following the steps of the STPA-inspired safety-security co-evaluation methodology, we identified safety hazards and cybersecurity incidents pertaining the system under consideration and conducted a scenario analysis on its control structure which produced some joint safety-security requirements which could be satisfied with countermeasures from the cybersecurity domain, proving that the co-analysis approach is indeed essential. Moving forward, the insights garnered from this analysis will serve as a foundation for the development of robust safety and cybersecurity mechanisms, taking into account the interplay of safety hazards and cybersecurity threts, thereby facilitating the design and realization of a secure and dependable combined ASN.

8. References

[1] Project SECREDAS, "Deliverable D2.5, Safety Security Privacy Evaluation Framework," 2020.

[2] P. Porambage, G. Gur, D. Osorio, A. Gurtov, M. Liyanage and M. Yilanttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society,* vol. 2, pp. 1094-1122, 2021.

[3] Y. Siriwardhana, P. Pawani, L. Madhusanka and Y. Mika, "AI and 6G security: Opportunities and challenges," in *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit*, 2021.

[4] Y. Wu, "Ethically responsible and trustworthy autonomous systems for 6G," *IEEE Network,* vol. 36, no. 4, pp. 126-133, 2022.

[5] M. Ozger and a. et, "6G for Connected Sky: A Vision for Integrating Terrestrial and Non-Terrestrial Networks," in *oint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2023.

[6] R. Alguliyev, Y. Imamverdiyev and S. Lyudmila, "Cyber-physical systems and their security issues," *Computers in Industry,* no. 100, pp. 212-223, 2018.

[7] F. Rinaldi, M. Helka-Liina, T. Johan, P. Sara, A. Sergey, I. Antonio, K. Yevgeni and A. Giuseppe, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE access,* vol. 8, pp. 165178-165200.

[8] K. V. Dejan and Đ. Ž. Dragan , "Spoofing in aviation: Security threats on GPS and ADS-B systems," *Vojnotehnički glasnik,* 2021.

[9] C. Günther, "A Survey of Spoofing and Counter-Measures," *J Inst Navig,* 2014.

[10] E. Ukwandu, M. A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovic and X. Bellekens, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *information,* 2022.

[11] R. Akram, K. Markantonakis, K. Mayes, P. Bonnefoi, D. Sauveron and S. Chaumette, "Security and performance comparison of different secure channel protocols for Avionics Wireless Networks," in *Proceedings of the 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, Sacramento, USA, 2016.

[12] M. Smith, D. Moser, M. Strohmeier, V. Lenders and I. Martinovic, "Analyzing privacy breaches in the aircraft communications addressing and reporting system (acars)," in *arXiv*, 2017.

[13] Z. Yu, Z. Wang, J. Yu, D. Liu, H. Song and Z. Li, "Cybersecurity of Unmanned Aerial Vehicles: A Survey," *IEEE Aerospace and Electronic Systems Magazine.*

[14] S. Z. Khan, M. Mohsin and W. Iqbal, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science,* 2021.

[15] L. Wang, Y. Chen, P. Wang and Z. Yan, "Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications," *IEEE Communications Standards Magazine,* 2021.

[16] J. Wang, Y. Zou and J. Ding, "ADS-B spoofing attack detection method based on LSTM," *J Wireless Com Network,* 2020.

[17] E. Chan-Tin, V. Heorhiadi, N. Hopper and Y. Kim, "The frog-boiling attack: limitations of secure network coordinate systems," *ACM Transactions on information and system security (TISSEC).*

[18] X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell and R. Poovendran, "Detecting ADS-B spoofing attacks using deep neural networks," in *IEEE Conference on Communications and Network Security (CNS)*, Washington, 2019.

[19] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in *2008 ION GNSS Conference*, Savanna, GA, 2008.

[20] E. Lisova, Š. Irfan and A. Čaušević, "Safety and security co-analyses: A systematic literature review," *IEEE Systems Journal,* vol. 13, no. 3, pp. 2189-2200, 2018.

[21] T. Ishimatsu, N. G. Leveson, T. John, K. Masa, M. Yuko and N. Haruka, "Modeling and hazard analysis using STPA," in *Proceedings of the 4th IAASS Conference, Making Safety Matter*, 2010.

[22] C. Ericson, A. Hazard analysis techniques for system safety, John Wiley & Sons, 2015.

[23] G. Macher, E. Armengaud, E. Brenner and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," in *Computer Safety, Reliability, and Security: 35th International Conference, SAFECOMP 2016*, 2016.

[24] B. F. Zahra and A. Belmekki, "Risk analysis in Internet of Things using EBIOS," in *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017.

[25] R. M. K. Khan, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017.

[26] G. Macher, H. Sporer, R. Berlach, E. Armengaud and C. Kreiner, "SAHARA: a security-aware hazard and risk analysis method," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2015.

[27] [Online]. Available: https://www.celticnext.eu

[28] L. Krishna and R. R. Murphy, "A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles".

[29] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE,* 2016.

[30] Yaro, Abdulmalik & Sha'ameri, A.Z. & Yarima, Said. (2021). Direct and Indirect TDOA Estimation based Multilateration System Position Estimation Accuracy Comparison. ELEKTRIKA- Journal of Electrical Engineering. 20. 54-64. 10.11113/elektrika.v20n1.226.

[31] [Online]. Available: https://sdgs.un.org/goals

[32] [Online]. Available: https://www.itu.int/en/sustainable-world/Pages/default.aspx

[33] [Online]. Available: The European ATM Master plan: https://www.sesarju.eu/masterplan

[34] [Online]. Available: https://www.itu.int/en/sustainable-world/Pages/default.aspx

[35] [Online]. Available: https://www.un.org/development/desa/en/news/administration/achieving-sustdev-through-icts.html

[36] [Online]. Available: https://climate.ec.europa.eu/eu-action/european-green-deal/2030-climate-target-plan_en

[37] [Online]. Available: https://www.ericsson.com/en/blog/2022/1/rebound-effect-climate-impact-ict

[38] D. Renga and M. Meo, "Can High Altitude Platform Stations Make 6G Sustainable?," in *IEEE Communications Magazine*, vol. 60, no. 9, pp. 75-80, September 2022.