**Sławomir Augustyn**[*]

# GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) FOR EFFICIENCY OF AIR TRANSPORT IN THE CYBERSECURITY DOMAIN

**Abstract:** This paper shows a Global Navigation Satellite System (GNSS) for the efficiency of air transport in the cybersecurity domain as a new development of space logistics, supported by safety engineering for the operational techniques and technologies in space. Moreover, this development of air transport is dedicated to a logistics supply chain supported by GNSS telecommunication. A new development is also significant for space technology because of its account improvement range and independence from most terrestrial network failures. The development of air transport is observable during the making of GNSS, which ensures wide-ranging continuous information for ensuring the safety and security of people and businesses when terrestrial network connections are disrupted. This publication's primary goal is to present an analysis and assessment of an industrial air transport enterprise which plays a significant role in supply chain cargo, e.g., transport of dangerous goods like medical supplies. The research problem was formulated as a question: What conditions made GNNS efficiency of air transport in the cybersecurity aspect? The publication adopted the following hypotheses:

1. The participation of GNNS in the efficiency of air transport depends on cybersecurity.
2. The Deep Space Network as support of air transport.
3. Cybersecurity of navigation systems supporting air transport.

The following research methods have been used in the publication: analysis and synthesis, comparison, search of normative acts and literature on the subject, abstraction, and inference. The author hopes the results obtained from the research and the presented considerations will constitute a starting point for further scientific research on the discussed subject.

**Keywords:** safety engineering, satellite system GNSS, space logistics, cybersecurity, innovation.

[*] Sławomir Augustyn - Military University of Technology, Warsaw, Poland.E-mail: slawomir.augustyn@wat.edu.pl, ORCID: 0000-0001-7711-5736

# 1. INTRODUCTION

Air transport has a significant role in the logistics management supply chain. Primarily when it is used in space cargo for the carriage of food, water and technological devices, e.g. electronic devices like digital, video cameras or dangerous goods, e.g., medical supplies etc., its role gains particular importance when the strategy of space logistics can be used for creating, storing or transmitting navigation and information in the form of electronic data in air operations. In response to the cybersecurity of human and natural environment in technical and economic aspects, the Global Navigation Satellite System (GNSS) has to support air transport.

Due to safety regulations in aviation and space law, rising freight prices and tightening of restrictions on travel, there is a perceived decline in air transporting interest in using different types of aircraft, space rackets or shuttle space, which is supported by navigation satellite systems.

The aviation and space logistics should be based on certain assumptions:

- A new development of physiological characteristics allows for the creating of a new approach to Global Navigation Satellite Systems for defining the concept of air transport.
- The quality of air transport design and maintenance value is achieved by making correct process decisions to ensure human safety and cargo security.
- The integrated support of high-quality air transport by developing technological service and space knowledge.

The international community must unite on how air transport issues are dealt with in the Global Navigation Satellite System. Currently, a selection of initiatives is being presented in the international community that attempts to deal with aviation and space security questions – some from the civil perspective, some from the disarmament perspective.

These benefits from new aviation transportation advances can be achieved by integrating satellite systems based on modern technologies and services into fully wired communities. These intellectual ventures are created by urban aviation supplying consumers with satellite services. Furthermore, these satellite services aspects recognize the opportunity for aviation transport support by building customized business models with risk assessment based on data collected from online activities of the Global Navigation Satellite System.

The air transport trends are very dynamic in innovative technologies, e.g., the Internet of Things (IoT), electronic devices and robotics, which influence the development of logistics management procedures and quality standards of society. It is becoming an inspiring benchmark for a new aviation and space industry strategy.

Cybersecurity has become increasingly important, with the international community witnessing several satellites in the Medium Earth Orbit – MEO. Satellite systems are vital to international security and underpin daily activities necessary for economies to function for the safety and security of humans and the natural environment. This GNSS service is threatened by the growth of irresponsible behaviour in space. That is why space activity creates a new way and new solutions in safety engineering, aviation transport and space logistics. These solutions include artificial intelligence (AI) and augmented reality (AR), which are improving the controlling and distribution of modern devices necessary for operations, satellite transmission, observation and global positioning of transport objects in safety and security domains.

This publication adopted the sources to build a holistic view of the future of air transport from different perspectives while supporting GNSS related to cybersecurity. Furthermore, a new business opportunity in logistics supply chain management and more sustainable space services should be driving new requirements for space handling.

## 2. ADVANCED SATELLITE COMMUNICATIONS FOR AIR TRANSPORT SAFETY

In the development of aviation and space technologies, the efficiency of air transport expansion is characterized by the dynamical rising performance design of avionics Global Navigation Satellite System (GNSS) and aviation augmentation reality systems used for an increasing number of commercial flight, which is essential for critical aviation and space tasks, e.g. comprehensive, safe and secure area navigation, communication, observation and precision approach of aircraft or shuttle spaces. GNSS augmentation reality can take many forms, with cybersecurity strategies sharing the same principle of providing supplementary important information related to the objects, improving the system security's performance and trustworthiness.

Global Navigation Satellite System augmentation benefits in air transport in the cybersecurity domain can be summarised as follows:

- increased runway access, route optimization and more direct en-route flight paths and new, better precision approach services for aviation and space logistics;
- reduced delays and simplified avionics equipment with better quality maintenance;
- potential elimination and support of ground-based navigation aids, e.g. VHF Omni-Directional Range (VOR), Instrument Landing System (ILS), etc., with reduced cost to Air Navigation Service Providers (ANSPs);
- secure of natural environmental, e.g. low quantity of $CO_2$, SO emissions and low level of noise;

- better safe airspace management, more capacity, fuel savings, aircraft health monitoring;
- better safety of flight and security of passengers and cargo.

However, GNSS for supporting aviation applications systems comprises space, control, and aviation segments (Figure 1). The space segment includes the navigation, communication and observation satellites required for safe global coverage.

The user segment includes many GNSS receivers developed for air, ground and marine navigation positioning applications. The control segment includes one or more Control and Processing Stations (CPSs) connected to several Ground Monitoring Stations (GMSs) and antennae located around the globe for Telemetry, Tracking and Command (TT&C) signals down and uplink and navigation message and integrity signals uplink to the satellites.

The Ground Monitoring Station antennae passively track each GNSS satellite in view and collect integrity-ranging signals from each satellite for retransmission data with GNSS time.

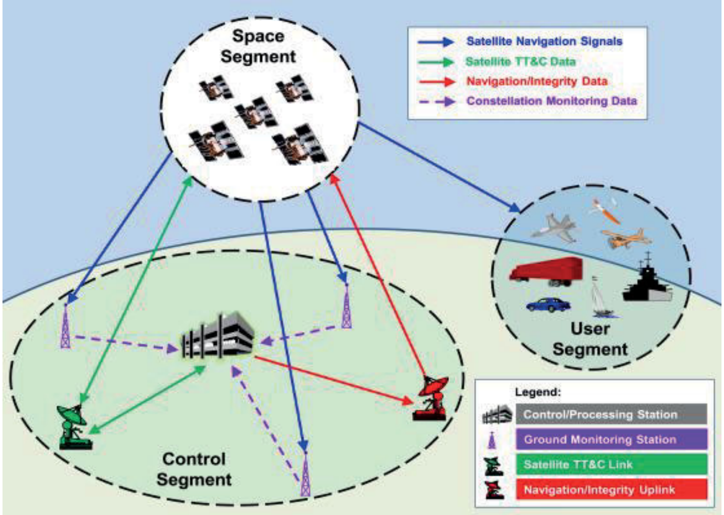

Space Segment
Satellite Navigation Signals
Satellite TT&C Data
Navigation/Integrity Data
Constellation Monitoring Data
User Segment
Control Segment
Legend:
Control/Processing Station
Ground Monitoring Station
Satellite TT&C Link
Navigation/Integrity Uplink

**Figure 1.** Global Navigation Satellite Systems (GNSS) segments
Source: Sabatini, R., Moore, T., Ramasamy, S.: *Global Navigation Satellite Systems performance analysis and augmentation strategies in aviation*, Progress in Aerospace Sciences, Volume 95, November 2017, Pages 45–98.

Air transport safety correlates with GNSS and critical infrastructure protection, civil security and border control in cybersecurity. Airspace is the most critical area all over the world. e.g. despite the heavy impact of the SARS-COV-2 and COVID-19 pandemic on the world economy in the aviation sector, the number of flights is still expected to reach the anticipated 50% forecast increase by 2050 in the social security aspect.

That is why air transport must be created by developing logistics management, new launching systems and innovation showing safety and security solutions for user communities in space. For example, an Iris Space Program creates innovative techniques within complete 4-D trajectory management over airspace across the globe to make aviation safer, greener and more efficient by developing a new satellite-based air-ground communication between controllers and cockpit pilots for Air Traffic Management (ATM). An Iris Program will also play an essential role in ATM modernization to achieve success in the European Green Deal target for carbon-neutral aviation by 2050.

The aviation sector is responsible for 3–5% of the European Union's total transport greenhouse emissions and more than 2–3% of global emissions. An Iris Program will contribute to the attainment of the net zero emission target of 2050 and the mid-term 2030 goal for 55% emissions concerning 2019 by enabling:

– more and more efficient and safe flight routes,
– create real-time important secure information sharing,
– optimized airline operations for cost savings.

Overall, an Iris Program represents a safe and secure, reliable cyber resilience to hackers' attacks and performance confidential requirements required to support the Air Traffic Service (ATS). These satellites in GNSS have the potential to become the best global service and support link-data-needed services.

A high-level diagram created by an Iris Program concerning an end-to-end system highlighting the highly secured Iris link, including authentication and message integrity features, is shown in Figure 2.

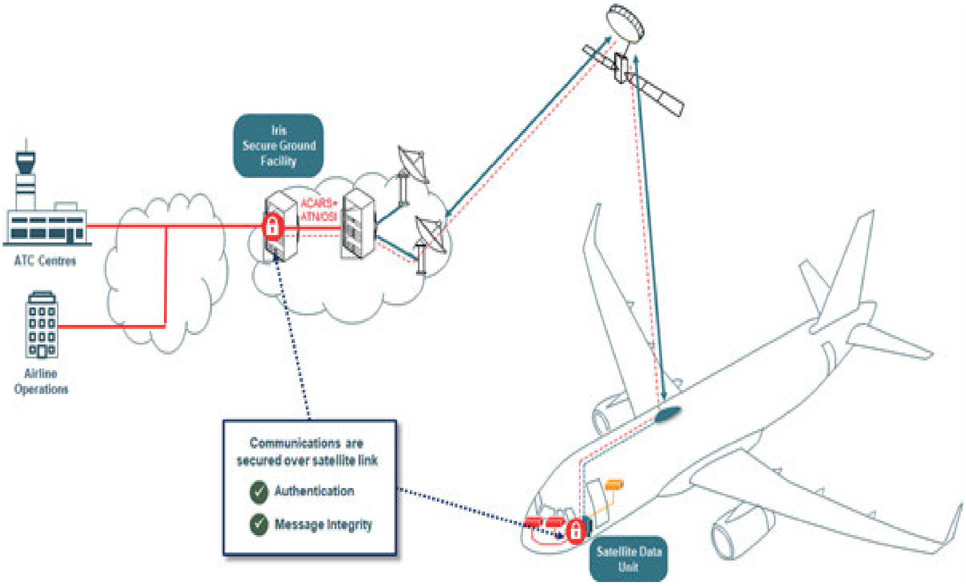


**Figure 2.** Integrated support of knowledge for air transport safety
Source: https://artes.esa.int/iris-satellite-communication-air-traffic-management

Moreover, an Iris Program is ready to interconnect with the Common European ATM infrastructure and systems' developments to enable compatibility with Aeronautical Telecommunications Network – Internet Protocol Suite (ATN-IPS) standards and technology communications.

From aviation standards and international security safety law regulations, an Iris Program technology is a crucial potential means of compliance with the Data Link Services Implementing Rule conditional to corresponding performance requirements for air transport safety supported by highly advanced satellite communications, e.g. GNSS.

## 3. CYBERSECURITY OF NAVIGATION SYSTEMS SUPPORTING AIR TRANSPORT

Navigation systems supporting air transport in globalization and the communication environment between humans and computerization with software development are factors which must be secured against cyber threats in the communications aviation sector. The cybersecurity of communication aviation is an essential domain of protection against cyber attacks.

These cyber-attacks are complicated by different threats that exist in systems' programs. A new trend in safety procedures, information technology experts give information about hacker attacks on sophisticated air navigation systems installed on aircraft, control and air communication systems to ground airport service systems.

Air transport is assessed as the safest means of the civil aviation ecosystem concerning not only the duty of the staff and crews but also all possibilities of counteracting cyber threats to preserve and even increase the efficiency for safety, security and resilience of travellers and cargo.

The requirements of interest in air transport must be taken the following aspects:

- The entire aviation ecosystem must be forced to introduce very stringent cyber-threat level checks,
- Each element of the aviation ecosystem should be tested regardless of the time of assembly,
- These systems regarding the safety of passengers and security of cargo must be isolated because they are susceptible to cyber attacks,
- All employees should have situational awareness related to cyber attack threats and the protection of systems procedures.

Air transport as a critical safe systems should be tested by independent external accessibility and integrity aviation companies with extensive experience in cybersecurity. Air transport systems have to have high-security priorities, such as satellites and aviation communication systems, which should ensure strong authentication and confidentiality in every flight situation. Along with the dynamic development of air transport, it is subject to a new growing type of threats, such as cyber-attacks, in the following aspects:

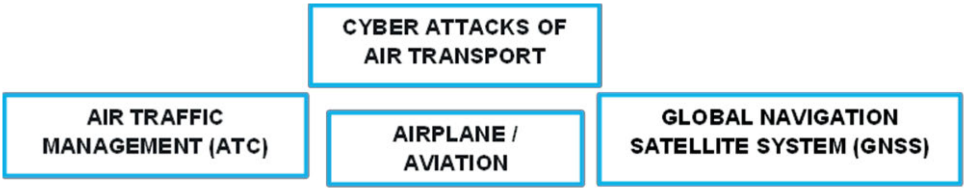
- the extensive data collection of information at airport power networks,
- specific action during handling and flight plan through cyber threats in technological relations,
- achieving specific financial profits by telecommunications, e.g. blackmail,
- weakening competition of staff and crew through malicious attacks,
- attack on individual civil aviation cells of air traffic control by computer viruses.

Such activities of hackers influence less, ensuring the security of the growing number of travellers and cargo. That is why cybersecurity experts must oversee the development of existing airports and introduce more complex modern ecosystems using modern information technology and advanced computer systems.

The development of existing airports should be done by the confidential cyber security strategy in increased interpersonal interaction and devices and services. Innovation and cost reduction due to the transformation of the aviation ecosystem create common goods. Moreover, sophisticated software is increasingly used to provide effective digital solutions for experienced aviation and space industry employees, e.g. supported by Artificial Intelligence (AI).

Analyzing threats from cyber-attacks to air transport should be divided (Figure 3) into the following aspects:

- Air Traffic Management,
- Global Navigation Satellite System,
- Airplane and airport infrastructure.



CYBER ATTACKS OF AIR TRANSPORT

AIR TRAFFIC MANAGEMENT (ATC)

AIRPLANE / AVIATION

GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS)

**Figure 3.** Threats of air transport during cyber attacks
Source: Leśnikowski W.: *Threats from cyberspace for civil aviation*, ASzWoj, Warsaw 2020

Furthermore, cyber threats are dangerous in the field of aviation security. Therefore, the Global Navigation Satellites System consists of the three following main areas:

1. Air Traffic Management (ATM) and Air Traffic Control (ATC) as controllers provide information in airspace controlled by operating aircraft and ground air traffic services to prevent collisions.
2. Airport and Airfield security control can be defined as actions to prevent cyber attacks in disrupting the operation of airports, mainly dedicated to

facilitating passengers, e.g. departure control, baggage handling, and cargo, e.g. dangerous goods, etc.

3. Aircraft cyber security of air carrier systems can be defined as cyberspace prevention to intentional actions in cybersecurity.

Moreover, a cyber attack is hazardous on aviation and space devices, especially on-board airport infrastructure such as two-way radios and Air Communication Addressing and Reporting Systems (ACARS) concerning sending messages or data information about aircraft. In such a technological and natural environment, hacker attacks on flight safety and security of passenger and cargo aircraft systems can cause severe problems with operational air tower control standards.

For instance, the hacker attack on the airport internet forced the US Federal Aviation Authority to close some of Alaska's air traffic control systems. The following example was the attack on the deactivation of passport control systems at departure terminals at the airport; it caused the delay of many flights. Finally, hacker attacks on navigation systems create similar situations to technical failure of aviation ecosystems.

According to cybersecurity experts, hackers can take control of the primary systems of the aircraft and all its avionics during the flight. Furthermore, cybersecurity specialists reword to the security of passengers and cargo inform about possibilities of breaking into aircraft system computers, e.g. navigation and turbine engine systems. In this situation, the security program, which diagnoses the weak element of the aircraft in order to protect airspace control, must be constantly unimproved against hacker attacks.

In hacker attacks, the security of passenger flights can be possible by the security of the GNSS communication system between the flight control tower and the aircraft. Also, attacking hackers can influence the pilot's decisions regarding false information about an aircraft's position in the sky or airport runway approaching. Moreover, hackers can take control of an aeroplane, even when the laptop restricts access to Wi-Fi or Bluetooth in the aeroplane. This situation requires a quick response from the carrier and the aircraft industry to ensure a unique interface providing access only to connect the so-called Electronic Flight Bag (EFB), electronic navigation aids and maintenance ground handling operations. The solution to this problem is entirely changing the outdated aviation ecosystems to protect them from cyber-attacks.

Currently, many aviation companies implement innovation programs that would counteract cyber attacks by particular signals to create a team of specialists responsible for timely software updates and constant monitoring of aircraft conditions, e.g., power turbine engines, avionics parameters, etc.

Air carriers' strategies must take these measures to combat cyber attacks on aircraft due to the severe activity of cyber threats in the civil aviation sector. Strategies for developing air transport in the cyber security domain are essential to prevent and eliminate dangerous effects.

These threats are explained by using more sophisticated air navigation systems on board aircraft and air communication systems, including flight information and ground security control at airports. On the other hand, hacker attacks on the civil aviation ecosystem make cybersecurity efforts and implement solutions by the International Civil Aviation Organization (ICAO), which activities of stakeholders relate to identifying these threats and risks as much as possible.

These activities implement a more significant number of rules and measures to prevent and protect against cyber attacks by the following tasks:

a) Airports implement modern measures to secure every IT system in the aviation ecosystem.
b) International Air Transport Association (IATA) has proposed annual audits to allow airlines to counteract cyber attacks.

Security specialists against unauthorized access to aircraft IT systems claim that aviation manufacturers have long known the situation of software shortcomings. Cyber attacks on aircraft IT systems require specialized knowledge and special equipment that the average person does not possess, which is why the opinion of specialists has not been treated as a standard security threat.

The aviation industry and air transport are currently facing a significant challenge, having links with other industry sectors from cyberspace, whose task is to look for a way to secure aircraft IT systems against cyber-attacks.

Nowadays, the safety of aircraft and the security of passenger and cargo can be much safer by using cybersecurity, whereas the implementation of innovative technologies is evolving very dynamically. Both are used in safe air transport and to perform cyber attacks by hackers.

## 4. CONCLUSIONS

In summary, a Global Navigation Satellite System (GNSS) for efficiency of air transport in the cybersecurity domain as a new reactive approach to innovative logistics technology in space is a period of dynamic global cooperation change, especially in space services segments. In addition, the structural changes of air transport security against hacker attacks in aviation intelligence ecosystems create interaction between quality services for modern safety airlines business models and customer security supported by, e.g. augmented reality in self-learning systems or big data analytics to digitalize airspace logistics.

The more fundamental issue in the future of air transport in global communication is GNSS between the interaction of human and intelligent aviation ecosystems. Intelligent aviation ecosystems will be able to make better human process decisions. Thus, an aviation business will be improved and secure, as well as more sustainable space logistics services in new requirements of airspace handling.

That is why transmission data and communication are vital issues for aviation cargo, especially during the air transport of dangerous goods. The GNSS improve aviation ecosystems to help aircraft travel around Earth. In summary, implementing practical applications in air transport supported by GNSS in cybersecurity domain based on, e.g. Artificial Intelligence will become interdisciplinary research and development of international programs related to economics and safety engineering systems covered by intellectual property frameworks.

## BIBLIOGRAPHY:

1. Augustyn, S., *Crew – spacecraft – environment anthropotechnical system in view of engineering systems*, Aviation Advances & Maintenance, ITWL, Warsaw 2018
2. Augustyn, S., *Earth observation & navigation law and technology. Space Situational Awareness, sensors - selected aspects*, IUS PUBLICUM Warsaw 2017
3. Augustyn, S., *The decision model of an aircraft crew in safety system. International Journal of Computer and Information Technology*, Vol. 2, Issue 2. 2013
4. Clarinox Technologies 2009 *Real Time Location Systems* at https://www.nottingham.ac.uk/grace/documents/resources/marketreports/realtimelocationsystems09.pdf accessed 19 Feb 2017 and at https://en.wikipedia.org/wiki/Real-time_locating_system accessed 19 Feb 2017
5. Coleman DJ., Rajabifad, A & Kolodziej, KW 2016 '*Expanding the SDI Environment: Comparing Current Spatial Data Infrastructure with Emerging Indoor Location-based Services*', International J. Digital Earth, Jan 2016
6. IATA, *Guidance for the transport of cargo and mail on aircraft configurated for the carriage of passengers*, Edition 3 – 04 May 2020
7. IATA Economics'*Freighters and Preighters – The Agility of Airline Cargo Operations.* Chart of the Week, 1 April 2021
8. IATA Economics', *The importance of 'preighters' seems to start to diminish*, Chart of the Week 15 April 2022
9. International Earth Rotation and Reference systems Service (IERS) 2016 at https://datacenter.iers.org/web/guest/eop/-/somos/5Rgv/latest/16 accessed 12 Jan 2017
10. Lee, J., et al. *Historical and future trends in aircraft performance, cost and emissions*, Annu Rev Energy Environ. 2001; 26:167–200.
11. Leśnikowski, W., *Threats from cyberspace for civil aviation*, ASzWoj, Warsaw 2020
12. Sabatini, R., Moore, T., Ramasamy, S.: *Global navigation satellite systems performance analysis and augmentation strategies in aviation*, Progress in Aerospace Sciences, Volume 95, November 2017, Pages 45–98.
13. Secure World Foundation Fact Sheet on UN COPUOS Working Group on Draft *International Code of Conduct for Outer Space Activities*, 2011.
14. https://artes.esa.int/iris-satellite-communication-air-traffic-management