TTTP

DOI: 10.7251/JTTTP2302037R
UDC: 656.7:[005.591.45:004.62

REVIEW

Aviation cyber security

Boris Z. Ribarić
PhD candidate, Pan-European university Apeiron Banja Luka, Bosnia and Herzegovina, borisribaric87@hotmail.com

Dragan Vasiljević
vasiljevicdj68@gmail.com

Julijana Vasiljević
julija2921968@gmail.com

Boris R. Mikanović
PhD candidate, Pan-European university Apeiron Banja Luka, Bosnia and Herzegovina, boris.r.mikanovic@apeiron-edu.eu

Received: September 13, 2023
Accepted: September 29, 2023

Abstract: Information technology is increasingly prevalent in all branches of traffic. In aviation, a significant amount of data is processed by computerized systems and transmitted through communication networks. Within this digital environment, characterized by technology and a vast number of digital files, a security system is essential to ensure the proper functioning of the system. To achieve effective and efficient information security management, it is crucial to thoroughly examine the factors influencing information security and plan the necessary measures for implementation.

Keywords: information system, safety, cyber, aviation.

INTRODUCTION

“Cyber in aviation” refers to the application of cybersecurity or cyber technology in the aviation sector. This includes the protection of aircraft, flight systems, networks, and information from cyberattacks and threats. Aviation cybersecurity is crucial to ensure the safe and reliable operation of aircraft and aviation operations. Cyber space is an environment in which the cognitive world (sensory world) is created through intellectual action via information and communication systems. [1]

The use of different types of information ensures the functioning of segments and activities of many organizations. Business risk is permanently affected by information security. All information systems and networks must be provided for their operation [2]. When we talk about information security, we mean - preserving the confidentiality, integrity, and availability of information. Due to the risk of information security, significant attention must be paid to conducting business activities in the market [3].

These are just some of the basic steps that the aviation sector takes to protect against cyberattacks, but cybersecurity is a dynamic field that requires constant updating and adaptation to confront increasingly sophisticated threats. The protection of information security has been especially imposed by the development of computer technologies by networking computers that are becoming vulnerable in all branches of the economy and life, so we must approach the effective protection of the information we have.

Information properties:

- The information can only be accessed by confidential persons, organizations, or processes, and care must be taken to ensure that an unauthorized person cannot access it, which is – Confidentiality;
- Each piece of information must have completeness and the property of preservation and accuracy that it represents - Integrity of information;
- The information must be available to users who have the authority to access it - the availability of information.

The above properties of information will increase their security as well as business continuity and reduce the risk to the lowest possible acceptable level. Care must be taken in the processes of designing information systems through various technical solutions for both software and hardware. To achieve the required level of security, it’s necessary to consider factors that affect the security of information, as well as the analysis and implementation of the necessary measures. [4]

Digital information technologies, as well as large amounts of data that are processed through computerized systems, must be protected. In other words, access to sensitive data can only be had by authorized persons, and unauthorized persons should be denied access, with any such attempt being recorded and analyzed. To protect the system, effective and efficient protection of the information we have at our disposal is essential, regardless of the place and form in which it is stored and used. It must be taken into account that the security of information is also represented by the information carrier, the protection of objects, its storage, use, and storage. Applying the appropriate policy of processes, procedures, organizational culture, and software and hardware components ensures information security. By implementing a large number of processes of different types and levels of complexity that are provided through the appropriate number of resources, we call this information security management [5].

As the use of information is an important segment in the activities of organizations, it is given great importance through ISO standards, especially the ISO 27000 series - Information Security Management Systems (ISMS). Information is an interpreted message, reducing uncertainty and increasing knowledge. When we talk about data, we mean raw facts about the real world that are represented by information carriers. When we want to obtain quality information, we need to process a certain type of data to make their selection to obtain the essence. We use this information in our work, and when we apply it several times, it grows into knowledge. The development of information technologies, computer technologies, and their networking in computer networks requires attention to information security. Through increased production, computer prices are falling and becoming more affordable for everyone. The trend is to use wireless technologies. Mobility is one of the characteristics and intentions. Data is being distributed more and more, more and more people are mastering computer technology, and access to standards is open to anything that presents a chance for information security to be compromised. For this reason, new standards like ISO/IEC 27001 dealing with the business risk approach are being introduced [4].

There are more and more attempts at cyber attacks on digital computer network systems from an unknown source. There are a number of attacks - cyber attacks that an attacker can launch. They look for system vulnerabilities where an attack can be effectively implemented. We characterize all this as an illegal action that should be disabled and prevented.

CYBER SECURITY IN AVIATION

Information technologies are increasingly represented. Security issues we need to address: access to sensitive data and unauthorized persons who should be denied access. When talking about such security problems in the digital world, the term cybersecurity is used. There is a great attempt at cybercrime in various branches of industry. Currently, according to EASA data, about 1000 attacks per month are directed at the aviation sector in aviation. Certain technical failures (problems in the operation of the radar system and automated systems in aviation) are often presented in the media as possible cyber attacks. No cyber attack has been confirmed, the air community has begun to address a potential problem.

Cyber threats were mentioned in a 2011 update in ICAO Annex 17, Security. ICAO mentioned cyber security as a high-level obstacle to the implementation of the Global Air Navigation Plan. With the transition to technologically advanced systems comes the need to address technologically advanced threats. How the system evolves from a connected point-to-point structure to a networked network where node elements are connected by digital connections using IP (Internet Protocol). An Internet-like network structure requires security comparable to critical Internet services. When the system is set up, every step of implementation must be taken into account. And it doesn't stop when the system is broadcast online: it must remain a focal point throughout its life cycle, every working day at every level. Taking this attitude into account, the user is an essential component for maintaining and improving security.

Powerful algorithms are the domain of engineers as well as secure implementation, robust hardware and software and solid networks, but choosing a good password and refusing to give any relevant data to someone who may be an attacker using social engineering techniques remains in the domain of end users. As a consequence, end users must understand the basics of security and appropriate protocols and behaviors to avoid weakening the system, which means that training on the topic must be provided.

Potential aviation-specific threats

So far, there has been talk of attacks on networks in general. Attention should be drawn to potential attackers. Who might be interested in removing any element of the civil aviation system? There are at least four types of hazards: Amateur hackers: this is the first group when it comes to computer attacks. The challenge of finding a way to break into a protected system may be the reason for a computer-savvy individual with high skills and motivation, but most are unwilling to cause harm or face the legal consequences of breaking into a critical system. However, they cannot be ignored. Criminals: One person behind a computer can attack thousands of potential targets often thousands of miles away, in another country with a different legal system. This explains why scams, such as phishing or ransomware, are on the rise. This group is potentially more dangerous than the previous one because they have economic motivation. On the other hand, criminals try to maximize the benefits by attacking targets with minimal cost and effort to take defensive measures, but no extraordinary resources are needed as they will switch to less protected and most profitable targets if they find appropriate resistance.

Terrorists: While ordinary cybercriminals tend to have financial motivations and no reason to create unnecessary damage, the goal of terrorists is generally to cause as much damage as possible. High visibility of aviation events makes it an attractive target for such purposes. Individual aircraft were previously targeted, but computerized networks can allow an attack on multiple aircraft at once or cause widespread disruption of the ATM system. The will to maximize damage makes terrorists a dangerous threat and creates the need to use the most powerful forms of cyber defense for flight control, as well as for any other highly automated security-critical system.

Cyber war: when hostilities occur, the enemy's key infrastructure becomes the target: electricity, communication, food supply and of course flight control. As a result, target systems are automated and their malware infection is sometimes attributed to foreign agencies. It is accepted that malware is already ready to attack critical infrastructure and that such attacks can be launched as retaliation against other cyber attacks. It is almost impossible to protect the system against such opponents because they have huge resources at their disposal, as well as the necessary skills. [5]

What kind of attacks can aviation expect?

Ways of harming and disrupting the system are limited only by the human imagination. Any of the components of the CNS-ATM system would have its own vulnerabilities. Currently, the voice communication between the controller and the pilot seems to be compromised, and occasionally false messages are reported from someone pretending to be pilots using a simple radio transmitter. Cyberattacks on aircraft equipment represent a serious threat to passenger safety and the operational functionality of aircraft. Attackers may attempt to target various aircraft systems and components. Here are several potential scenarios and the impacts of cyberattacks on aircraft equipment:

1. Aircraft Systems: Attacks on aircraft systems, such as flight control, navigation, communication, and electrical systems, can lead to a loss of control over the aircraft or other critical flight issues;

2. Entertainment Systems: Cyberattacks on in-flight entertainment systems (IFE - In-Flight Entertainment) can enable attackers to access passenger devices or even cause discomfort to passengers;

3. Communication Systems: Attacks on aircraft communication systems can jeopardize the pilots' ability to communicate with air traffic control or other aircraft, leading to confusion and hazards in the air;

4. Navigation Systems: Manipulation of aircraft navigation systems can result in changes to the flight path or pilot disorientation;

5. Engines and Maintenance Systems: Cyberattacks on aircraft engines or maintenance systems can impact their reliability and safety.

A datalink controller-pilot (CPDLC) would require a higher technical skill level for an attacker to succeed in an attack. But because there is no "party line" effect, a successful attack will be harder to detect. A fake controller or a successful attack by a man in the environment that changes the appropriate approval can have a serious impact. Theoretically, it is possible to mention navigation systems, including conventional terrestrial systems, as well as satellite ones. But as the attacker should be close to the target, it seems that it will have a difficult effect on commercial aviation - unless the attacker is not on a plane or the attack takes place near the airport. Simply interfering with voice, data connection, or navigation, including satellite signals, is also a threat. Newer ATM concepts, some of which rely on (encrypted) networks, may be even more vulnerable.

Traffic at a remote controlled airport - Remote Control - can be interrupted by inserting false data in the communication between the sensors at the airport and

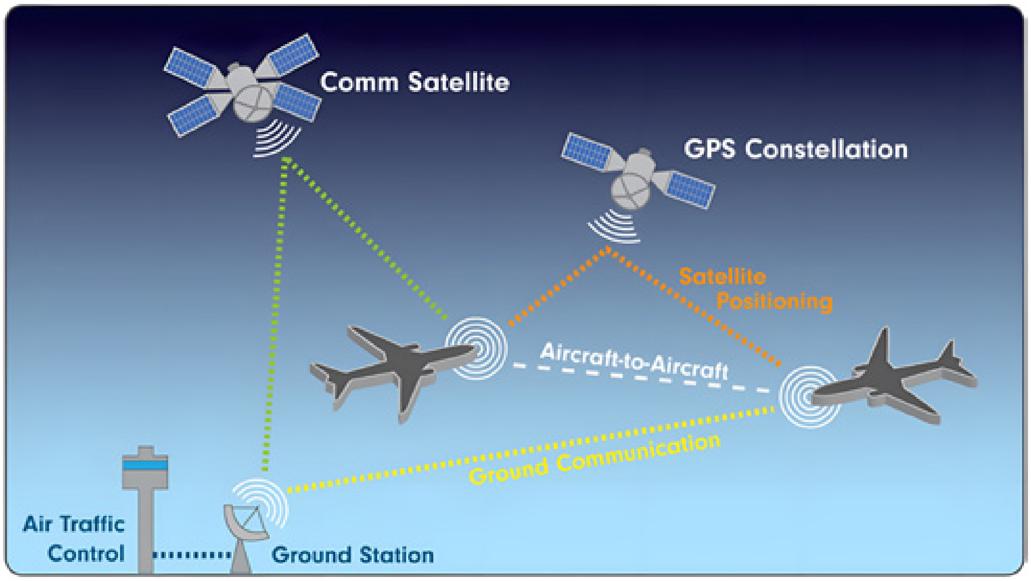

Figure 1. ADS-B system mode

the cameras and the remote tower. It is much easier to simply cut off communication via DDoS attacks that would make controllers blind, deaf and mute. The worst-case scenario is a DDoS attack on a single facility that controls several remote towers that would disrupt traffic at several single-action airports.

The use of - ADS-B

Automatic – the system works automatically, without pilot command,

Dependent – position obtained from GNSS*,

Surveillance – each station on the ground as well as the aircraft in the air which are equipped with a suitable receiver can perform surveillance.

The basis of the ADS idea is the fact that within the aircraft itself, there are data (aircraft identification, position, state vectors, short-term "intentions," description of maneuvers, aircraft type ...) that "only" should be delivered to interested users, whether they are on the ground (e.g., ATC *) or in the air (collision avoidance). ADS-B communication, not - encrypted - encrypted. To prevent the spread of "ghost planes" into the system, the ADS-B position was confirmed by calculating the Time Difference of Arrival (TDOA) signal to different ADS-B receivers. A concept such as SWIM (System Wide Information Management) may be a target for hackers. Best described as "ATM-only Internet" is a network in which all types of data are available exclusively to authorized users: meteorological data, flight trajectories, surveillance data, etc. This information is shared by all authorized users connected to the system, including individual aircraft. But the use of IP (Internet Protocol) means that the same types of attacks used on the Internet can be used against such a SWIM network, including DDoS, insertion of false data, theft of sensitive data, or ransomware. Extending the system to all types of users, from ATC to smaller parts of the general aviation structure and from airlines to meteorological services, means that there are many vulnerable entry points that could be used to compromise such a system [3]

FMS - Fligt Management System

It is a system of programmed optimal flight control that consists of the integration of various aircraft subsystems.

FMS enables the selection of automation levels for all phases of flight and provides information on appropriate indicators:

1. The main components of FMS are: FMC (Flight Management and Guidance Computer), calculates the 3D position of the aircraft, performance, and other parameters necessary for accurate and efficient flight according to a previously defined path, which are obtained based on manually entered or automatically entered data;

2. MCDU (Multipurpose Control and Display Unit), a multi-purpose control panel used for data entry and representing the connection between the pilot and the FMC;

3. FCU (Flight Control Unit), a device for controlling the horizontal and vertical flight profile of an aircraft;

4. Flight Management Source Selector, a device through which input sources are selected, used by FMC;

5. Display system, a system that displays data and information to the pilot.

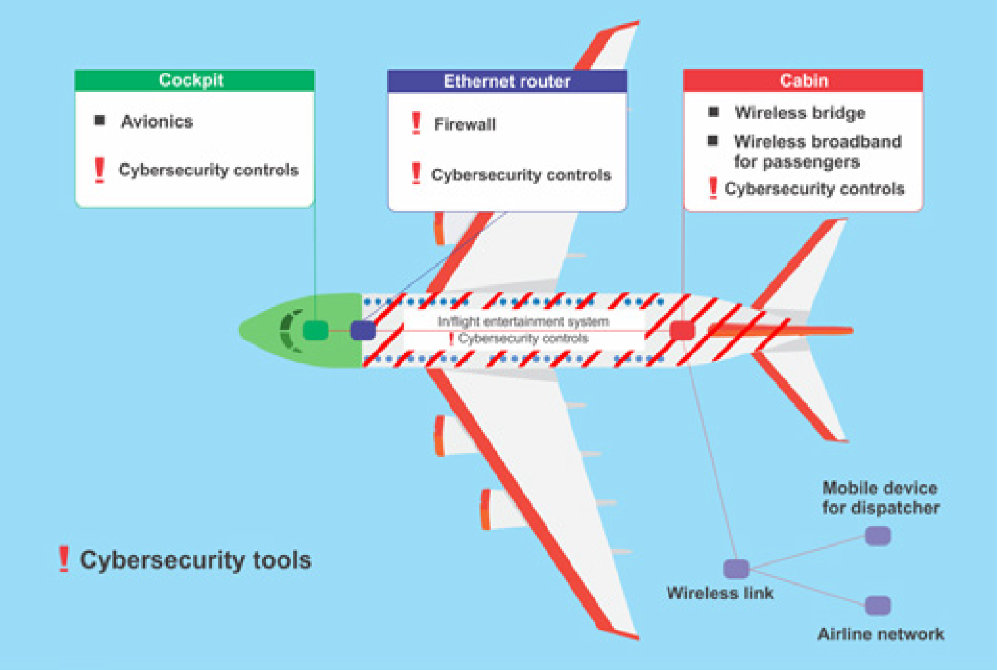

Figure 2. Illustration of active protection against cyber attacks in commercial passenger aircraft

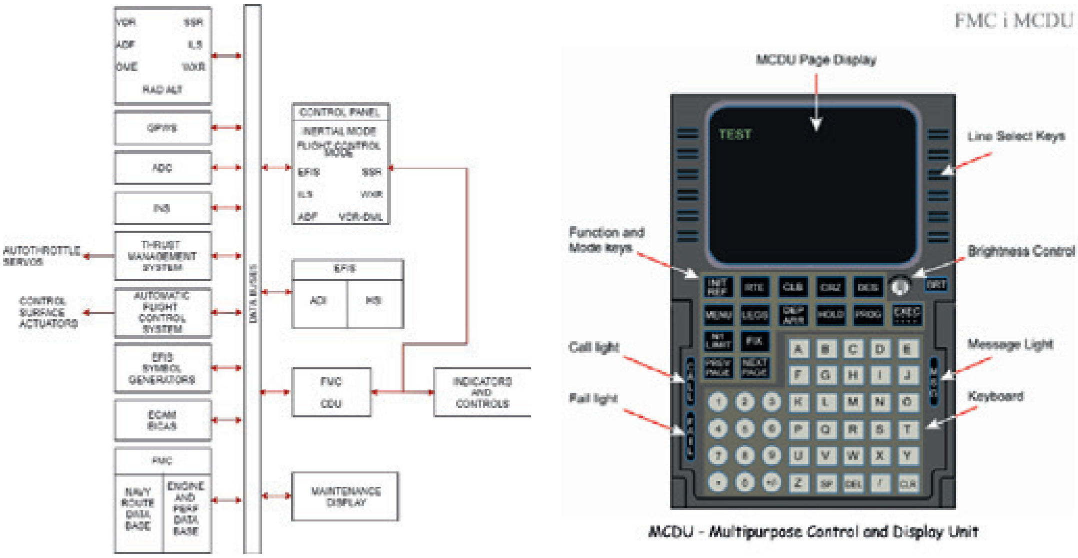

Figure 3. FMS scheme

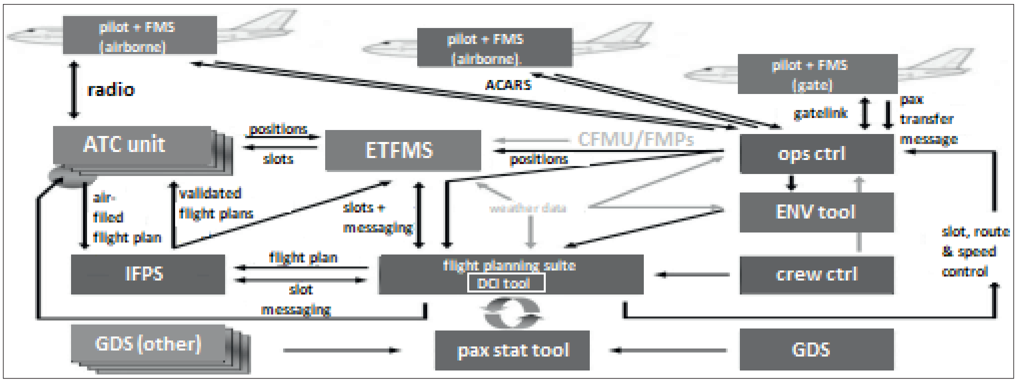

Figure 4. Data exchange mechanism

DATA EXCHANGE

The mechanism of data exchange includes meteorological data (weather data), aircraft positions, flight plans submitted from the air and confirmed flight plans (air-filed flight plan, validated flight plan), and the flow of information within this system. Coordination is provided by exchanging data on slots (a slot is a permit obtained by the airport to use its resources at a specific time) and flight plans with flight control (ATC unit) and its various services.

Communication between the aircraft and the company is provided by the system. For slots, speed, and route, data is transmitted via datalink and gatelink. Datalink as a means of digital data exchange should play a major role in practical application, as it can be used to change a flight plan or enter via FMS with the assistance of a pilot. In addition, it can be used as a means of dynamic flight monitoring, sending automatic downlink messages about the position and altitude of the aircraft and the remaining amount of fuel, in response to questionable uplink messages. Downlink messages are messages sent by an aircraft via the datalink to the ground (airline operations center), while uplink messages are messages sent from the ground to an aircraft [5].

CONCLUSION

Information, including process information support, information systems, and networks, is a critical business asset for any organization and is indispensable to its operations.

In a modern, highly complex, and interconnected business environment, information is increasingly exposed to a growing number of threats and vulnerabilities from various sources, including human activities, natural disasters, accidents, and more.

To protect against cyberattacks on aircraft equipment, aviation companies and aircraft manufacturers must implement a range of measures, including:

1. Strengthening Cybersecurity Systems: This involves implementing the latest security measures and technologies to preserve the security of aircraft systems.
2. Monitoring Network Activities: This includes regularly monitoring network activities to detect unusual or suspicious events.
3. Fundamental Information Protection: This involves classifying and encrypting sensitive data to prevent unauthorized access.

4. Staff Training: This is about educating pilots and technical personnel on cybersecurity and helping them recognize suspicious activities.
5. Regular System Updates: It is essential to keep avionics software and systems up-to-date to address vulnerabilities.

Cybersecurity in the aviation industry is paramount for ensuring passenger safety and the proper functioning of aircraft.

n many cases, information systems lack sufficient security measures during the design process. While certain technical means (software and hardware) for system protection are often applied, these measures are inadequate given the current conditions of system application. To achieve the required level of information system security, effective and efficient management is necessary, involving appropriate organizational and managerial solutions, procedures, and practices.

Although the Air Force has relatively few cybersecurity incidents, the increasing use of modern technology and network connectivity makes such events more likely. The International Civil Aviation Organization (ICAO) has recognized cybersecurity as a priority issue and called on states to commit to addressing it through a resolution. Various steps have been taken to enhance cybersecurity by organizations, including national regulators such as the FAA and EUROCONTROL. However, the aviation industry still has a long way to go to catch up with other industries in terms of adopting interconnected systems [5].

REFERENCE

[1] Vasiljević, D., Vasiljević, J., Đurić, A., “Cyberspace - definition and classification,” Proceedings of the National Conference on “Hybrid Warfare - The Dilemma of Contemporary Conflict Concepts” at the Institute for Strategic Research, University of Defense in Belgrade, Belgrade, 2018.

[2] Alkalaj, I., *The Rol of SNET (Safety Nets)*, Skyguide-Swiss Air Navigation Service Ltd., 2008.

[3] Babić, O., Netjasov, F., “Air Traffic Control, Faculty of Traffic Engineering, Belgrade, 2018.”

[4] Magazine - THE CONTROLLER - Journal of Air Traffic Control, july 2017, Volume 56 Issue 2, pp 12 - 15.

[5] Zoran B. Ribarić, “Doctoral dissertation, ‘Integration of Air and Ground Traffic Information in the Passenger Air Transport System,’ Paneuropean University APEIRON, Banja Luka, 2018.”

[6] International Civil Aviation Organization (ICAO): Enhancing safety and expanding capacity; implementation of ADS-B out in the Unated States, AFI Planing and implementation regional group, Twenty first meeting (APIRG/21), Nairobi, Kenya (09-11 October 2017).

[7] Aviation Cyber Security Strategy - Moving Britain Ahead (2018), The Department for Transport, London, UK.

[8] ENISA - The European Union Agency for Network and Information Security (decembar, 2016): Securing Smart Airports.

[9] Zekos, G., (2007). State cyberspace juristiction and personal cyberspace juristiction, International Journal of Law and Information Technology, Oxford University Press, London, Vol. 15 No. 1.

[10] Tipton, H., Krause, M., (2004). Information Security Management Handbook (fifth edition), CRC Press, New York.

[11] ICAO Doc – Security and Facilitation Strategic Objective, Aviation Cybersecurity Strategy, October, 2019.