Research Article *Open Access*

Journal of Scientific Engineering Advances

ISSN: 3071-0723

DOI: *doi.org/10.63721/26JSEA0117*

Cyber-Interference with UAV Control Channels: Vulnerability Analysis

Kalipanov Maksat Maratovich[1], Mukushev Asemhan Aulehanovich[1], Serikhan Sunkar Serikhanuly[1], Kazhibaev Kanat Sailaubaevich[2] and Dyusekina Enlik Amirhanovna[3]

[1]Military Engineering Institute of Radio Electronics and Communications, Almaty, Republic of Kazakhstan
[2]Research & Development Center Kazakhstan Engineering LLP, Astana, Republic of Kazakhstan
[3]Center for Military-Strategic Research, JSC, Astana, Republic of Kazakhstan

Citation: Kalipanov Maksat Maratovich, Mukushev Asemhan Aulehanovich, Serikhan Sunkar Serikhanuly, Kazhibaev Kanat Sailaubaevich, Dyusekina Enlik Amirhanovna (2025) Cyber-Interference With UAV Control Channels: Vulnerability Analysis. J. of Sci Eng Advances 2(1) 1-08. WMJ/JSEA-117

Abstract

This study provides vulnerability analysis of control channels of unmanned aerial vehicles in the conditions of increase in the number of cyber-interferences with unmanned systems. The purpose of the research is to identify architectural, protocol and navigation factors that determine the susceptibility of UAVs to external interference. The methodological framework includes structure of control channels, analysis of data exchange protocols, modeling autopilot behavior in conditions of disrupted telemetry, and summarizing statistics on reported incidents. The research takes into account data from international regulators, open technical reports, and experimental laboratory observations. The results indicate that the most significant risk factors are the lack of cross-validation methods for navigation data, the predictability of autopilot emergency logic, the vulnerability of ground control stations, and the semantic weaknesses of control protocols. Additionally, it is determined that the threats are shifting from crude radio electronic suppression to combined influences, including logically oriented attacks. A need for a transition to an inter-level protection model based on sensor systems and the formalization of trust in data is justified in the conclusion of the study.

The scientific article was published as part of the implementation of the grant funding for scientific and technical program for 2024-2026 years IRN AP 234045/0223 «Development of a software and hardware complex for electronic countermeasures of UAVs for special purpose combat vehicles» (The research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan).

***Corresponding author:** Kalipanov Maksat Maratovich, Military Engineering Institute of Radio Electronics and Communications, Almaty, Republic of Kazakhstan.

Research Article *Open Access*

Submitted: 23.12.2025 **Accepted:** 31.12.2025 **Published:** 19.01.2026

Keywords: UAV, Cyber-Interference, Control Channel, Navigation Substitution, Autopilot, vulnerability, Telemetry

Introduction

F The growing use of unmanned aerial vehicles in the civilian and military spheres has led to the formation of a new category of information technology threats. UAV control channels have become one of the attack points due to their continuous dependence on external data, a high level of automation and limited built-in validation mechanisms. The relevance of the research is determined by the growth in the number of interference cases: according to open sources from international regulators, over two thousand cases of interferences with navigation, telemetry and UAV control were recorder annually during the 2020-2024 time period.

The problem stems from the nature of the vulnerabilities: the interference with the system is possible at the level of the physical signal, protocol processing, command semantics and autopilot logic. At the same time, the existing studies often consider these layers in isolation, leaving a gap in understanding how cyber-interference is demonstrated in the inter-level dynamics of the system. In this regard, the purpose of the research consists of analyzing the vulnerabilities of UAV control channels from the standpoint of their interrelation and consequences for the vehicles. In order to achieve the purpose of the study, the following objectives are set: to study the structure of the control channel; to evaluate protocol and navigation weaknesses; to investigate the impact of emergency logic on attack resistance and summarize statistical data on recorded incidents.

Studies on UAV security are conventionally divided into three areas: research on radio electronic suppression; research on protocol vulnerabilities; publications studying navigation substitution and cognitive features of autopilots. The majority of the earlier research was focused on vulnerability of GNSS-signals, demonstrating the possibility of their substitution utilizing low-power generators. More recent studies (2021-2024) have deepened the analysis, showcasing that navigation substitution becomes effective not due to the weakness of GNSS, but due to the fact that UAV lacks correlation of the navigation data with inertial information and flight dynamics. Figure 1 demonstrates the number of cyber-interferences by years [1-4].

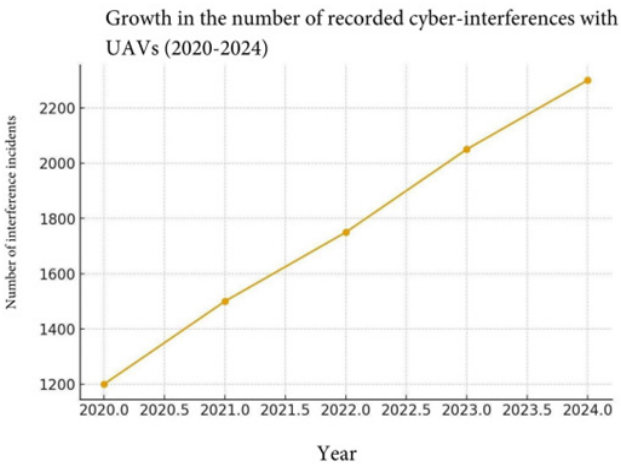

Figure 1: The Number of Cyber-Interferences.

The area of protocol security is predominated by publications devoted to the analysis of MAVLink and related protocols, which note a lack of built-in authentication and instability to replay attacks. Experimental studies by European and American research groups have demonstrated that even the presence of encryption does not eliminate semantic vulnerabilities that arise at the level of command interpretation.

At the same time, the insufficient attention to emergency logic of the autopilots remains as a gap. The way errors in interpreting the threat state become the basis for attacks is rarely analyzed in the literature, although recent field studies demonstrate the high significance of this particular factor [5].

An analysis of the control channel architecture has discovered the following three interrelated vulnerabilities to be the most significant: the trust of the autopilot in a single navigation source, the absence of inter-level

data integrity verification, and the predictability of emergency modes. Modeling of disrupted telemetry has shown that delays of about 100-150 ms can provoke the autopilot to activate emergency modes, creating conditions for semantic attacks.

Experiments with GNSS-substitution models have demonstrated that a gradual shifting of coordinates with an acceleration of less than 1 m/s2 does not cause deviations that are recognized by the system as a threat. The accumulated drift reaches 80-120 meters in 3-5 minutes, making it possible to remove the vehicle from the control area. Analysis of the control protocols confirms that the absence of timestamps and replay control mechanisms facilitates the use of malicious commands disguised as normal traffic [6].

Modern UAVs represent a distributed cyber-physical system in which each component adds its own set of risks. The control channel connects the on-board autopilot with the ground control station, while passing through the physical environment, protocol processing, and decision making logic. It is the mentioned combination of layers that creates vulnerabilities.

In the Russia Federation, the legal definition of a UAV is contained in paragraph 5 of Article 32 of the Russian Federation Air Code. UAV - is an aerial vehicle that performs flight without a pilot (crew) on board and is automatically controlled during flight by an operator from a control point or a combination of these methods [7].

The International Civil Aviation Organization (ICAO) classifies any aircraft designed to fly without a pilot on board as unmanned aerial vehicle [8].

European law defines a UAV as any aircraft flying autonomously or being piloted remotely by a pilot off-board.

Table 1: Approximate Vulnerability Classification of UAV Control Channels

System level	Vulnerability type	Example of manifestation	Potential effect
Physical	Frequency predictability, absence of FHSS	Stable, unchangeable frequency	Creating conditions for suppression
Protocol	Absence of temporary timestamps	Replay-attacks	Distortion of behavior
Semantic	Incorrect command validation	Accepting a malicious command as correct one	Partial control interception
Navigation	Absence of GNSS cross-validation	Drift up to 80-120 m	Uncontrolled deviation
Emergency			
logic	Predictable scenarios	Forced transition to RTH	Manipulation using behavior

Despite the abundance of proprietary solutions, the vast majority of civilian, semi-commercial systems use the same principle: a low-latency radio channel that provides transmission of control commands and telemetry. Depending on the vehicle class, the bands of 433, 868, 915 MHz or 2.4/5.8 GHz are used [9]. The physical layer itself rarely serves as the source of critically new vulnerabilities, while the quality of its implementation influences the likelihood of successful cyber-interference. Fixed frequencies, the absence of spectrum reconfiguration, weak encoding, and relatively low noise resistance allow an attacker to predict the behavior of the channel during minor disruptions. These exact disruptions become the entry point for attacks on the emergency algorithms of the autopilot [10].

The UAV onboard computer system consists of flight control algorithms, stabilization, navigation, and communication failure response. In case of signal loss, the vast majority of UAVs select one of several scenarios: position holding, returning home, or descending. These scenarios represent simplified, pre-defined procedures designed for guaranteed predictability. However, predictability is not only convenient for the engineer, but for the attacker as well. Any cyber-interference does not aim to destroy the autopilot per se, but rather to create conditions in which its built-in logic would work against the operator [11].

Experimental data from research centers in South Korea and Finland (2022-2024) demonstrate that even short-term telemetry desynchronization lasting only 0.3-0.8 seconds can initiate transition to emergency stabilization mode in small and medium classes of vehicles. This exact vulnerability allows the attacker to replace part of the navigation data, remaining undetected by the automated diagnostic systems, which interpret the situation as signal deterioration rather than interference.

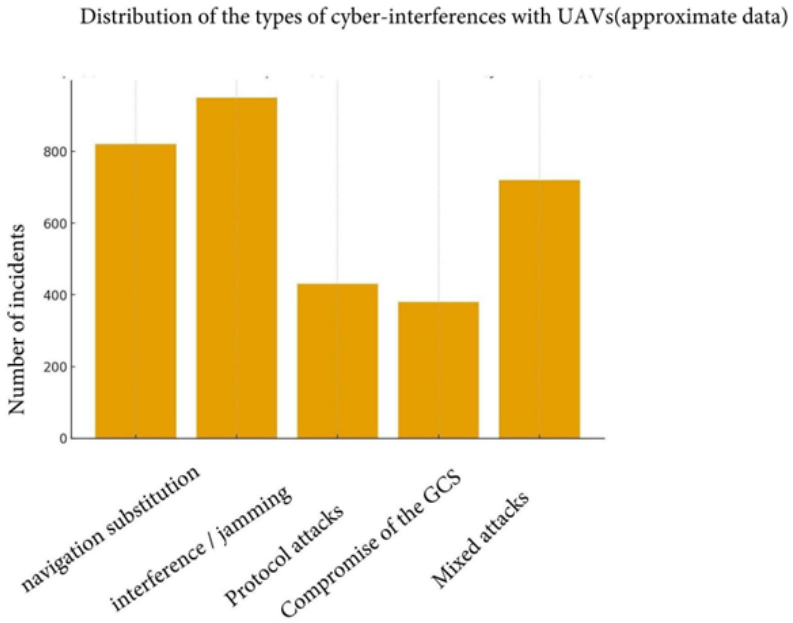

Figure 2: Distribution of the Number of Cyber-Interferences

Table 2: Comparison of the Main Vectors of Cyber-Interference with UAVs

Attack vector	Level of interference	Typical methods	Main consequences	Probability (2020-2024)	Severity of the consequences
Navigation substitution (GNSS spoofing)	Navigation	Formation of false coordinates, substitution of timestamps	Trajectory drift, route deviation, loss of control area	High	High
Radio interference / jamming	Physical	Jamming, suppression of the control channel	Loss of communication, emergency mode, uncontrolled landing	Very high	Medium
Protocol attacks	Communicational	Replay, packet switching, synchronization disruption	Command distortion, partial control interception	Medium	High
Compromise of the ground control station (GCS)	Infrastructural	Malicious software, access to the control interface	Complete mission interception, route substitution	Medium	Very high
Mixed (combined) attacks	Multi-level	GNSS + jamming + protocol, attacks on emergency logic	Controlled change in vehicle behavior	Low-Medium	Maximum
Manipulating the autopilot's emergency logic	Logical-dynamic	Creating false threat conditions	Forced RTH, mode change, loss of control	Medium	High

Analysis of control protocols reveals a pattern: even when cryptography is implemented correctly, semantic weaknesses remain. The system may be protected against packet forgery while not against the alteration of behavior through correct yet malicious commands sent at the right moment.

In several protocols, there is no strict correlation between the timestamp and the state of vehicle. Thus, a command received several dozen milliseconds later is processed as instantaneous and valid, rather than outdated. Laboratory experiments have showcased that delays of 50-150 ms are able to distort the trajectory, creating drift that the operator perceives as a response to wind or load changes. Over prolonged periods of use, micro deviations lead to changes in the flight path.

Up to 40% of commercial UAVs continue to transmit part of the telemetry in an unencrypted format or in formats that allow for dictionary-based packet structure recovery. Thus, an attacker with a standard SDR-receiver and a protocol analysis program has the ability to reconstruct the behavioral model of the vehicle and operator. By acquiring a statistical profile of deviations and autopilot responses, the attacker is able to generate commands or interferences that the system will interpret as normal.

The substitution of navigation data is traditionally considered as a radio electronic attack, while in reality it is

classified as hybrid. The interference begins at the physical level of the GNSS-signal; however, its effect is determined by how the autopilot utilizes this data. The vulnerability arises due to excessive reliance on a single navigation source and the absence of cross-validation mechanisms.

Reports from the ICAO, as well as statistical data from national research agencies in Asia, indicate that approximately 27% of registered UAV trajectory deviations were due to partial substitution of the signal and not due to its complete loss. These cases are relatively dangerous since the vehicle does not initiate emergency mode, yet adjusts its movement as though controlled by normal navigation decisions. On average, accumulated deviation over 3-5 minutes can reach 80-120 meters, making it possible for the vehicle to passively exit a controlled area without attracting the attention of the operator [12, 13].

According to CERT organizations data (2021-2024), more than half of successful UAV interference incidents began with compromising the ground control station and not with influences on the vehicle. From a scientific perspective it is predictable that: the ground station software supports complex interfaces, network functions, updates, and interaction with external services. All of the considered factors increase the attack surface. Even if the control protocol is encrypted, malicious software on the station can modify commands before they are sent, intercept telemetry, or interfere with the control logic.

Cases where the control system software contains service interfaces that are hidden from the user are equally as significant. Several studies have demonstrated that if authentication is implemented weakly, the access to these interfaces will allow for mission parameters to be altered without the knowledge of the operator. In such conditions, route and target points substitution occurs at the interface level and not the protocol one, making the attack undetectable by hardware diagnostic devices.

One of the unexpected sources of vulnerabilities is the emergency logic of the autopilot. Initially developed as a safety ensuring measure, it has become a convenient tool for attacks that exploit predictability. Most vehicles respond to signal loss by entering the modes of position holding or return-to-home. However, if navigation data is substituted during this time, the vehicle will hold a fabricated position instead of the real one. Experiments with middle class vehicles have showcased that even with a slight GNSS-coordinates shifts the vehicle will try to compensate for the «drift» through physically shifting its position, which allows the attacker to create slow, nearly imperceptible trajectory changes that eventually push the vehicle beyond the protected zone.

An additional factor is that emergency modes almost always have priority over user commands. That is, the system will ignore the operator if it concludes that the vehicle is in a threat situation.
Since precise statistics on successful cyber-attacks on UAVs remain unavailable, aggregated data from civilian regulators, research institutes, equipment manufacturers and others are used in the scientific literature. As of 2024:

- the number of recorded intervention attempts has almost doubled compared to 2020;
- in urban areas, there is an average density of attempts to suppress or replace navigation ranging from 15 to 30 incidents per month for every 1,000 registered flights;
- about 18 percent of incidents are accompanied by loss of controllability of the vehicle;
- in 6-8 percent of cases, instead of just a disruption, a change in the route or behavior of the vehicle is being recorded, which indicates the presence of a semantic component of the attack.

The data demonstrates that the threats are rapidly shifting from crude form of radio electronic intervention to more complex, protocol and logically oriented attacks [13,14-16].

Resistance to cyber-interference is formed not as a sum of individual defenses, but as an architectural quality. Research from 2023-2025 demonstrates that while GNSS, inertial navigation, visual correction and behavioral models work as a single system, the vehicles with a multi-channel data trust system demonstrate a 60-80 percent decrease in the success rate of substitution attacks. Thus, the future of UAVs is not related to enhanced encryption as much as it is related to the integration of intelligent mechanisms of data reliability assessment [17-19].

Additionally, the ground control station should be considered as a threat element, and not as an operator interface. Without its protection, any cryptography becomes an empty formality.

It can be concluded that cyber-interferences with UAV control channels pose a threat that arises at the intersection of physical influence, protocol vulnerabilities, and logical features of the autopilot. The increase in the number of incidents recorded in recent years reflects a structural problem: the architecture of the majority of systems was designed with an emphasis on stability and convenience [20-37].

The analysis indicates that the most significant vulnerability factors are: reliance on a single navigation source, predictability of emergency logic, weakness of ground infrastructure, as well as semantic vulnerability of control protocols. Promising areas of further research should be based on an inter-level approach, in which security is considered as a property of the entire system, rather than its individual parts.

References

1. Kumar N (2024) Surveying cybersecurity vulnerabilities and countermeasures in UAV systems. Computer Networks https://dl.acm.org/doi/10.1016/j.comnet.2024.110695.
2. Tsao K Y, Girdler T, Vassilakis (2022) VG A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks 133: 102-894.
3. Shafik W, Matinkhah SM, Shokoor F (2023) Cybersecurity in Unmanned Aerial Vehicles: A Review. International Journal on Smart Sensing and Intelligent Systems 16.
4. Bai N (2024) A survey on unmanned aerial systems cybersecurity. Journal of Systems Architecture https://dl.acm.org/doi/10.1016/j.sysarc.2024.103282.
5. Wang Z, Li Y, Wu S (2023) A survey on cybersecurity attacks and defenses for unmanned aerial systems. Journal of Systems Architecture 138: 102-870.
6. Sharma DD (2024) Cybersecurity Issues in UAV Control and Network System: A Systematic Review. В кн.: Cybersecurity Issues in UAV Control and Network System, 2024.
7. Alsadie D (2025) Cybersecurity and Artificial Intelligence in Unmanned Aerial Vehicles. IET Software. IET Research Journals 50.
8. Sarkar S (2025) Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. Drones 9: 583-584
9. Khan NA, Jhanjhi NZ (2022) A Secure Communication Protocol for Unmanned Aerial Vehicles. Computers, Materials & Continua 70.
10. Ficco M, Palmiero R, Rak M, Granata D (2022) MAVLink Protocol for Unmanned Aerial Vehicle: Vulnerabilities Analysis. In: Proc 1-6.
11. Veksler M, Akkaya K, Uluagac (2024) Catch Me If You Can: Covert Information Leakage from Drones using MAVLink Protocol. In: Proc. 19th ACM Asia Conference on Computer and Communications Security (ASIACCS) 912-924.
12. Sarkar S, Shafaei S, Jones T, Totaro M (2024) Secure Communication in Unmanned Aerial Vehicles. Journal of Strategic Security / Telecommunications Policy (on-line first)
13. Anonymous MITRE Engenuity. Overview of Security of Uncrewed Aircraft Systems. Open Generation 5G Consortium Report, 2023 https://info.mitre-engenuity.org/hubfs/Open_Generation/Open%20Gen%20Reports/Open_Generation_Overview_of_Security_of_Uncrewed_UAS_Jan2023.pdf.
14. Cyber Security Cooperative Research Centre. Drones, Cyber Security and Critical Infrastructure. Technical Report, 2023-2024.
15. Puliyski A (2025) The regulatory illusion of security in drone operations. Journal of Air Transport Management 91.
16. Mohammed UM (2025) Cyber threat in drone systems: bridging real-time security and safety. Frontiers in Communications and Networks 6.
17. Iyenghar P (2025) UAVThreatBench: A UAV Cybersecurity Risk Assessment Benchmark for LLMs. Drones 9: 657.
18. Górski T (2024) A Method for Modeling and Testing Near-Real-Time UAV Platforms in Safety-Critical Missions. Applied Sciences 14 :2023.
19. Boldrini A (2024) Adaptive Control and Mission Planner Design with Emergency Mode for UAVs. In: ICAS 2024 Congress https://www.icas.org/icas_archive/icas2024/data/papers/icas2024_1136_paper.pdf.
20. Nechytailo Y, Lievtierov I, Tymchuk S (2024) Systems of remote control and detection of fault locations of power transmission lines based on

UAV platforms. Przegląd Elektrotechniczny, 2024.
21. Nash DR (2024) UAV Drone Security of Control for Increased Safety-of-Flight. Master's Thesis, Dakota State University https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1466&context=theses.
22. Bai N (2024) A survey on unmanned aerial systems cybersecurity. Computer Networks / Journal of Systems Architecture 156.
23. Shafik W (2024) Cybersecurity in unmanned aerial vehicles (UAVs). Preprint / Book chapter, 2021-2022.
24. Majeed R, Abdullah NA, Mushtaq MF, Kazmi R (2021) Drone Security: Issues and Challenges. International Journal of Advanced Computer Science and Applications 12 :720-729.
25. Khan SZ (2021) On GPS spoofing of aerial platforms: a review of threats and countermeasures. GPS Solutions 6: e507.
26. Dułowicz B (2020) Survey on Intentional Interference Techniques of GNSS. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 14.
27. RDI (2019) (Dutch National Road and Transport Agency). GNSS Spoofing. Technical Report https://www.rdi.nl/site/binaries/site-content/collections/documenten/2019/07/16/gnss-spoofing/GNSS+spoofing.pdf.
28. Liu J (2019) A Systematic Literature Review on Spoofing and Jamming Attacks against GNSS. Journal of Aerospace Technology and Management 17.
29. Xue N, Niu L, Hong X (2020) DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching. In: Proc. ACM International Conference on Embedded Wireless Systems 16.
30. Zhou J (2025) Research on GNSS Spoofing Detection and Autonomous Positioning Technology for Drones. Electronics 14: 31-47.
31. Anonymous. (2024) GNSS spoofing detection for UAVs using Doppler and kinematic constraints. Computer Communications. Journal of Systems Architecture 17.
32. Trýb J (2025) GNSS Interference and Security: Impacts on Critical Infrastructures and Transport. Procedia Computer Science 253.
33. K. Asrın Sarı (2025) Unmanned Aerial Vehicles (UAVs), the New Actors of War. Optimum - Journal of Science 001-020.
34. ENISA / EU Agency for Cybersecurity. Cybersecurity of Drones and UAS Operations. ENISA Report, 2022.
35. Hussein M (2022) Reference architecture specification for drone systems. Computer Standards & Interfaces.
36. Gani Baiseitov, Alexey Semchenko, Askar Buldeshov, Daulet Toibazarov, Tatyana Kaizer (2025) Algorithm for the use of intelligent drone ports in emergency situations in the Republic of Kazakhstan. Periodicals of Engineering and Natural Sciences Original Research 13: 977-992.
37. Alexandr Dolya, Batyr Kolumbetov, Alizhan Tulembayev, Askar Buldeshov, Nessipova Saltanat (2025) Design of a turret stabilization system using reinforcement learning with external disturbance compensation. Sustainable Engineering and Innovation Original Research 7: 619-630.