AVIATION
2009
13(4): 116–121

SECURITY ANALYSIS OF UAV RADIO COMMUNICATION SYSTEM

Darius Rudinskas[1], Zdobyslaw Goraj[2], Jonas Stankūnas[3]

[1,3]Antanas Gustaitis Aviation Institue, Rodunės kelias 30, LT–02187, Vilnius, Lithuania
[2] Warsaw University of technology, Airplane and Helicopter Department
E–mail: [1]darius.rudinskas@.vgtu.lt, [2]goraj@meil.pw.edu.pl, [3]jnst@vgtu.lt

Received 17 June 2009; accepted 18 November 2009

Darius RUDINSKAS, post–graduate student.
Education: 2006 master's degree in Electronic Engineering, Vilnius Gediminas Technical University, Faculty of Electronics.
Present position: post–graduate student at Antanas Gustaitis Aviation Institute.
Research interests: security analysis of radio communication systems, wireless sensors, integrated health management systems.

Zdobyslaw GORAJ, Prof Dr Habil
Education: MSc (Eng.) – 1972, PhD – 1977, D Sc – 1992, Prof – 2002.
Affiliations and functions: 1973–2002 – Warsaw University of Technology, lecturer of Flight Dynamics; 1982–1989 – PZL – Okecie light aircraft company, senior airplane designer; 1992–1999 – Institute of Aviation, head of flight dynamics group; 1993–1996 – Institute of Aeronautics and Applied Mechanics, deputy director; 1996–2002 – Faculty of Power and Aeronautical Engineering, vice dean for scientific affairs.
Experience: aircraft designer since 1982; flight dynamics researcher since 1977; main organizer of the international seminars entitled: Recent Research And Design Progress In Aeronautical Engineering And Its Influence On Education (1994–2000); member of the editorial boards of the following journals: (1) Aircraft Design (Holland), (2) Journal of Aerospace Engineering (United Kingdom), (3) Turbo And Jet Engines (Israel), and (4) Transactions of the Institute of Aviation – Scientific Quarterly (Poland); Polish coordinator and representative in European Fifth Framework Program devoted to unmanned aerial vehicles – coordinator of UAVNET And CAPECON projects.
Lectures in foreign institutions: 1997 – Kyushu University, Japan, long endurance high altitude unmanned aerial vehicles; 1998 – Bristol University, UK, panel methods in teaching of airplane design; 1999 – Saint–Cyr, France, panel methods – theory and practice; Old Dominion University, Virginia, USA, coupled flight dynamic / panel method tool for conceptual design and analysis of existing vehicles; 2000 – Boeing, Saint Louis, USA, coupled flight dynamic / panel method analysis; Israel Aircraft Industry, design and flight dynamics of a HALE UAV; 2001 – London, Kingston University, civil unmanned aerial vehicles (UAVs), "State of the Art And Challenges for the Future".
Teaching: mechanics of rigid bodies, flight mechanics, flight dynamics, airplane aerodynamics and airplane design.
Publications: Author of numerous journal and conference papers (more than 80).
Present position: head of Department of Airplane And Helicopter Design; course director for Aerospace Engineering Program in WUT.

Jonas STANKUNAS, Prof Dr Habil
Date and place of birth: 1949 in Pakene, Rokiškis District, Lithuania.
Education: 1970 – Krivoj Rog Civil Aviation School, Ukraine; 1976 – Faculty of Automation at Vilnius Institute of Civil Engineering; 1981 – post-graduate studies at Vilnius Institute of Civil Engineering.
Affiliations and Functions: 1970–1972 – aviation technician, Vilnius Joint Aviation Platoon; 1972–1975 – expert, Radio Apparatus Technology Dept.; 1975–1978 – senior engineer, Sector of Science Research; 1982–1987 – head of science laboratory of slow wave and deflecting systems, Vilnius Institute of Civil Engineering; 1988–1993 – assoc prof, Radio Apparatus Technology Department, Vilnius Technical University (formerly Vilnius Civil Eng. Institute) and Kaunas University of Technology (formerly Kaunas Polytechnic Institute). Since 1993 – director of Antanas Gustaitis Aviation Institute (AGAI) of Vilnius Gediminas Technical University; 1993–1995 – assoc prof; 1995 – habilitated doctor; 1995–1997 – prof, Air Traffic Control Department (AGAI); since 1997 – prof, Avionics Department (AGAI); vice chairman of Council of Lithuanian National Aeronautical Technology Platform; delegate of the Republic of Lithuanian at the Specific Program Committee "Cooperation", theme "Transport (including Aeronautics)"; member of Advisory Council for Aeronautics Research in Europe (ACARE).
Awards: laureate of Lithuanian State Award in Technological Sciences, 1997.
Publications: author or co–author of 143 scientific articles, 4 monographs, 31 reports, 97 scientific reports, and 9 educational methodological publications.
Inventions: author or co–author of 14 inventions.
Training: advancement training in Great Britain, Canada and Sweden.

ISSN1648-7788 print / ISSN 1822-4180 online DOI: 10.3846/1648-7788.2009.13.116-121
http://www.aviation.vgtu.lt

Abstract. This paper presents analyzed questions of the safety of the information transferred by the radio connection link of the Polish UAV project "Aircraft for monitoring" SAMONIT. This safety is especially important for the design and use of unmanned aerial vehicles (UAV). This paper also presents the structure of the SAMONIT communication system, security threats to the radio connection system, and possible measures to ensure secure information.

Keywords: UAV, security, communication system.

1. Introduction

An unmanned aerial vehicle (UAV) may be used for various purposes: military, monitoring, transportation, and radio communication (UAVNET… 2006). For UAV management, telemetry, and other data transmission, a radio communication link is used. It could inevitably be confronted with threats: loss of radio communication, transmitted information, or control or deliberate external intervention. To avoid these undesirable consequences, it is necessary to take information security measures (Rudinskas *et al.* 2008). In this paper, the radio-related problems, potential threats, and possible solutions of the UAV project "Aircraft for monitoring" SAMONIT in the framework of Institute of Aeronautics and Applied Mechanics at Warsaw University of Technology are analysed (Goraj 2007, Goraj 2008, Goraj *et al.* 2008).

2. System description

Various uses are being developed for unmanned aircraft. UAVs, depending on the purpose and the configuration, can be in touch with the ground at the station or with other UAVs and can also receive data from independent sources of information (GPS, meteorological stations, etc.) (Torun 1999). A summary the UAV communication scheme is presented in figure 1.

Main purpose of the SAMONIT is surveillance of the European Union's external borders in Poland. The ground to air aircraft communication system is used for communication between a ground control station and the UAV. These communication channels are used to transmit commands for the control of the UAV, telemetry data, or other information.

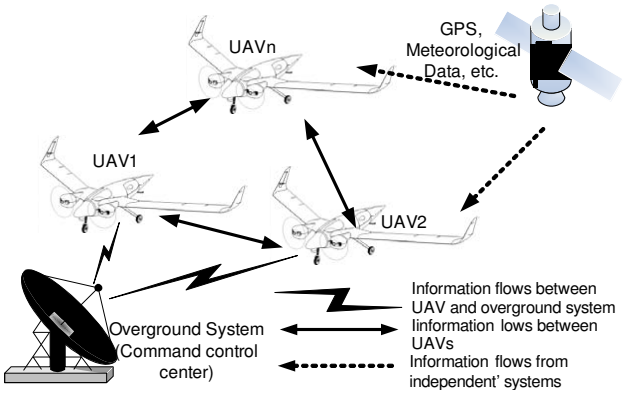

Fig 1. Review of information flows between different systems (Goraj 2007)

Communication systems are classified into two groups:

– information transfer system;
– information security system.

In the next chapters, we will discuss the methods and equipment of information security.

3. Security threats

For UAV management, telemetry, and other data transmission a radio communication link has been used. It is inevitably confronted with threats: loss of radio communication, transmitted information, or control or deliberate external intervention. The threats come in two types: those independent of humans, and those related to humans (Fig. 2).

To continue further we will detail the potential threats.

One of those types is independent of human threats-natural phenomena that have an effect on transmission quality but not on the security of the transferred data (Fig. 2).

Human-related threats include eavesdropping on the communication channel, changing or damaging information, and blocking the channel (Fig. 2).

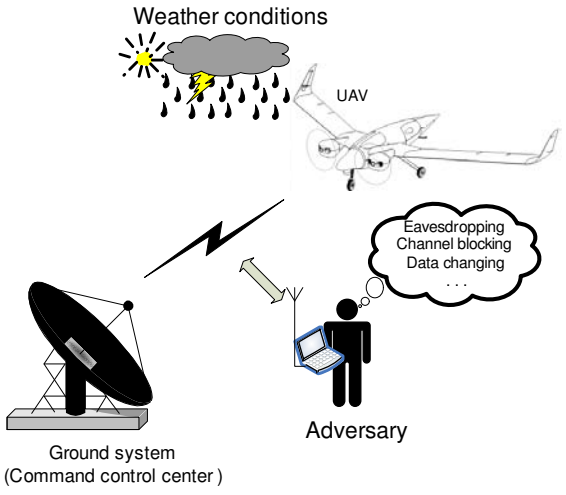

Fig 2. Potential threats

Regardless of the purpose of the UAV, strong information security measures are necessary. They are required because, as was previously mentioned, corrupted information may have a negative impact on the vehicle, or the information gathered may be used in other attacks against the UAV.

4. Measures of information security

An adversary may attempt to manipulate transferable data with the intention of hiding, modifying or delaying control commands. Such critical faults in the UAV influence mission success or flight hazards. The manipulation may be done by corrupting, replaying, or blocking the data during its collection or distribution. However, during real-time UAV operation integrated units generate alerts on the attacks. Furthermore, the adversary may passively eavesdrop on critical data to derive information that may be used for other attacks. Although the above two threats do not cause immediate hazards for flights, they may be exploited for the future attacks.

Physical protection and logical (software) security measures can be used for information security (Torun 1999). The physical security measures assign to technical safeguards (physical protection of information memory devices). Information coding, complex data transfer protocols and encryption algorithms, etc. All information security measures have to be integrated in the radio communication system (Fig. 3).

The default SAMONIT radio communication systems do not include security equipment to protect the transfer of information (Homziuk *et al.* 2009). Figure 3 shows the functional diagram of the SAMONIT radio communication system with integrated equipment for the information security (dotted line boxes "Encrypt/Decrypt"). We will discuss these boxes later.

In order to mitigate the aforementioned threats, we make the following security primitives and recommendations:

– Reliability of radio channel: Radio quality on aerial vehicles is influenced by various factors: the frequency band used, the distance, the weather conditions, the intensity of external noise, the position of the aircraft, etc. To ensure the quality and reliability of radio communication, it is necessary to use duplicating transmitters with perpendicular antennas. When there is a communication problem with the main device, automatically turns the second transmitter and continues to maintain the link. For the SAMONIT communication system several different frequencies (35 MHz, 2.4 GHz) are used (Goraj 2007, Goraj 2008, Homziuk *et al.* 2009). With the use of a very high frequency (GHz) transmitter, signal polarization is relevant, and therefore it is recommended to install duplicate transmitter antennas in different planes perpendicular to each other, thus ensuring the required polarization (Viero *et al.* 2007). The second most important factor is a material from which the aircraft body is made. For the SAMONIT body composite materials with carbon fibre are used. The carbon is a conductor and shields the electrical equipment that is inside of body. Hence, all

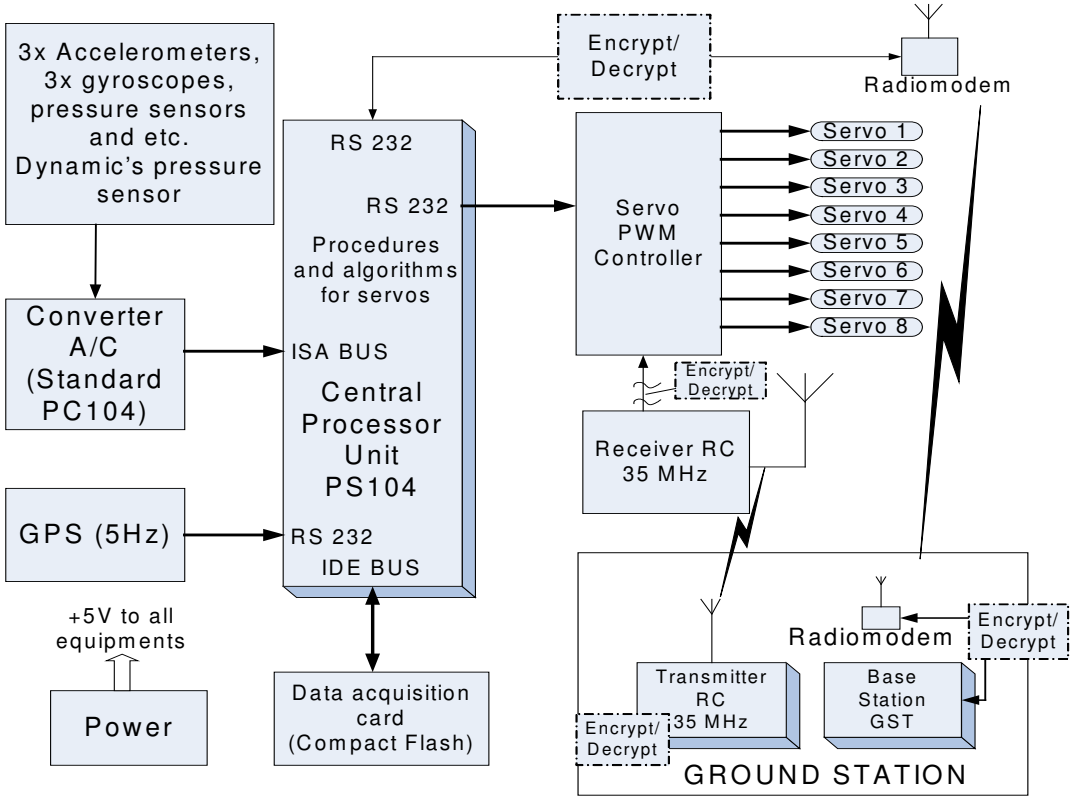

Fig 3. The functional diagram of SAMONIT radio communication system (Homziuk *et al.* 2009)

– Communications antennas must be mounted on the surface of the SAMONIT. If impossible to mount antennas on the surface, "windows" made from other materials (example – glass fibre) must be built–in on the body;

– Integrity: The SAMONIT communication channel must be protected from unauthorized modification of data by an adversary attempting to hide, for example, a change in controls commands or telemetry data. Hence, data received from the UAV must be identical to (or an aggregate of) data sent by the originating UAV (Robinson 2007a);

– Authenticity: Furthermore, the UAV must also be protected from the injection of misleading data sent by unauthorized ground stations. In order to prevent external adversarial attacks, when receiving data the UAV must be able to verify the validity of both the source and the message. For defending against compromised ground stations, the UAV can employ distributed solutions, such as a majority voting scheme that can jointly determine validity (Lazos *et al.* 2005);

– Confidentiality: Not all information, transferred to/from a UAV, are public: control commands, telemetry data, etc. The assurance of confidentiality will be discussed below;

– Mitigation of Channel Jamming: The adversary can, for example, employ jamming attacks to block or delay critical fault detection from propagating towards the ground station. Therefore, channel-jamming attacks must be detected as soon as possible and mitigated in the UAV. A potential solution was described by M. Li; there a UAV adjusts its transmission rate in order to contain jamming interference (Li *et al.* 2007);

– Secure Routing: The UAV and ground station need to route their readings timely and reliably even when under attack. The UAV and ground station routing protocol must be robust enough to withstand jamming attacks that induce long and energy–inefficient routes. The routing protocol must also be robust enough to resist attacks based on misleading routing messages. For example, if geographic routing is used, is capability to change location information (e.g. the wormhole attacks (Lazos *et al.* 2005));

– Early and Correct Detection of Manipulation: Any manipulation of transferred information must be detected as soon as possible, while false alarms must be avoided. For this threat, we can use the intrusion detection system. The SAMONIT onboard computer must also have the capability to create an archive for all events.

5. Confidentiality assurance

Communications in the UAV that contain proprietary data or sensitive data capable of aiding future attacks (e.g., engine fuel level, collected data) must be protected against passive eavesdropping on the wireless channels.

The simplest solution is to transfer data in plaintext format using simple data transfer protocol: *start*, *data*, *checksum* and *stop* bytes (Fig. 4).

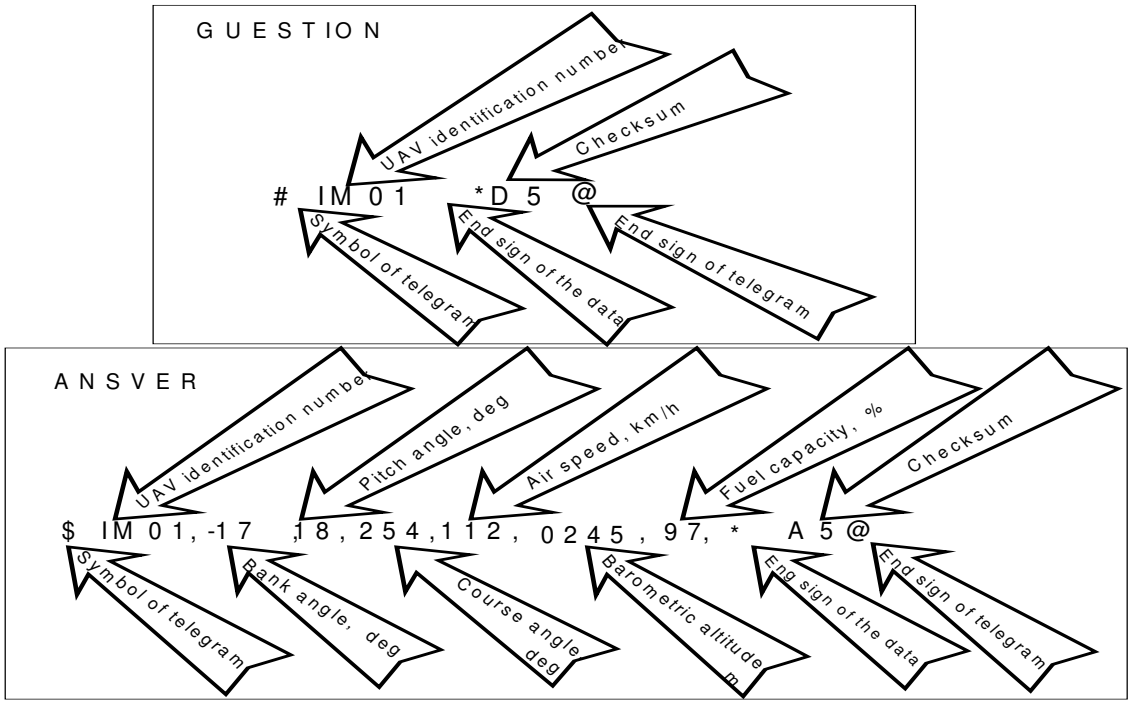

Fig 4. Structure of questioning message and answering message corresponding to the telemetry layout (Homziuk *et al.* 2009)

This data transfer method is simple but not secure. In addition, no radio modems used have integrated security measures (Homziuk *et al.* 2009, MaxStream… 2005). For providing integrity, authenticity and confidentiallity of UAV communications, cryptography can be used.

All cryptographic equipment can be integrated into the communication channel as hardware, as an embedded tool (Fig. 3, dotted boxes), or software tools integrated into the main computer of the SAMONIT can be used. There is simple integrate a hardware cipher tool into communication channel, but it challenge some problems. First, it is hardware and needs a power supply and it adds weight. Second, we lose time converting data from different protocols. Software tools do not have the weakness that hardware tools have, but ciphering time is directly dependent on the speed of the main processor (8, 16, 32, or more bits), capacity of the memory, and programs installed.

Since UAV's are limited in terms of battery (fuel) power, symmetric cryptography is preferred. Asymmetric cryptography has the drawback of being relatively computation and communication intensive. At the same time, to increase UAV's functions, asymmetric cryptography-based solutions such as digital signature can be used to communicate with other subsystems (Li *et al.* 2007, Robinson 2007b). Furthermore, solutions based on link layer cryptography, i.e. using a cryptographic key shared by two neighbours, are more suitable than solutions based on end-to-end cryptography, i.e. using a key that is shared by each originating UAV and the end destination, which can be an aggregator, a UAV, or the base station.

Standard ciphering tools such as those are used in wireless networks can be used to guarantee confidentiality. For example, one of the possible measures is the Advanced Encryption Standard (FIPS… 2001). The AES has different modes: AES Counter mode (AES–CTR), AES–CCM, and AES–CBC–MAC. The ciphering keys used cannot be less than 32 bits.

Cryptography solution can't be used only for transferred data including checksum securing in transfer protocol, or for data and service information (Fig. 5).

$IM01, -17, 18, 254, 112, 0245, 97, *, A5 @	- Plain Text Message
ОњGDц‹{Ьn·п)р:~ОИЄ—уѕщХhЮ†,	- Ciphered Message

Fig 5. Plain text message and AES128 encrypted message (Homziuk *et al.* 2009)

The ciphering process requires a lot more capacity for mathematical calculations, and sometimes that is difficult to achieve in the system. There now exist solutions, however that allow cryptographic capabilities to be integrated in small embedded systems. For example, ciphering solutions can be derived from from smart card technology (ZK–Crypt… 2009).

Most available radio communication systems have integrated security measures that are configured by default settings. To protect transferred information, exploring all available integrated security measures is recommended.

Conclusions

1. The security of transferred information is needed for safe UAV use.
2. The analysis of the radio communication system in the SAMONIT project demonstrates that security equipment for transferred data is insufficient, and an adversary could perform external intervention.
3. The minimum requirements for the security of transferred information it is advisable to use data ciphering methods.

References

FIPS PUB 197: Anouncing the Advanced Encryption Standard (AES) [online]. 2001. Available from Internet: <http://www.csrc.nist.gov/publications/fips/fips197/fips–197.pdf>.

Goraj, Z., 2007 UAV platforms designed in WUT for border surveillance. *AIAA paper,* 2965.

Goraj, Z., 2008. Mini UAV designed for surveillance long endurance mission. In *The 4th International Symposium on Innovative Aerial / Space Flyer System:* Proceedings of the 4th Int. Symposium. Jan. 14, 2008, Tokyo. 11–20, 14.

Goraj, Z.; Frydrychewicz, A.; Cisowski, J. *et al.* 2008. Progress in design and manufacturing of PW–141 – a long endurance MINI UAS. In *Proc. of the 8th International Conference on RRDPAE.* Brno, October 15–17, 2008.

Homziuk, A.; Hajduk, J. 2009. Opracowanie systemu akwizycji danych, telemetrii, autopilota I stacji bazowej BSP SAMONIT. In *Projekt BSP SAMONIT*. Warszawa.

Li, M.; Koutsopoulos, I.; Poovendran, R. 2007. Optimal jamming attacks and network defense policies in wireless sensor networks. In *IEEE INFOCOM*. 1307–1315.

Lazos, L.; Poovendran, R. 2005. SeRLoc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks,* 1(1): 73–100.

MaxStream, Inc. 2005. *Confidential & Proprietary. Xstream–PKG–R™ RS232/485 RF Modem – Product Manual* [online] 4.2B. Available from Internet:< www.maxstream.net >.

Robinson, R.; Li, M.; Sampigethaya, K. *et al*. 2007a. Impact of public key enabled applications on the operation and maintenance of commercial airplanes. *AIAA ATIO*.

Robinson, R.; Li, M.; Lintelman, S. *et al*. 2007b. Challenges for IT infrastructure iupporting iecure ietwork-enabled commercial airplane operations. In *AIAA Infotech@Aerospace Conference*.

Rudinskas, D.; Stankunas, J. 2008 Analysis of design problems of integrated health management systems in the small aircrafts. In *Proc. of the*

8th International Conference on RRDPAE. Brno, October 15–17, 2008.

Torun, E. 1999. UAV Requirements and design consideration. In *RTO SCI Symposium on "Warfare Automation: Procedures and Techniques for Unmanned Vehicles",* Ankara, Turkey, April 26–28, 1999.

UAVNET homepage [online], 2006. [cited 25 March 2009]. Available from Internet: < http://www.uavnet.com/ >.

Viero, T. ; Rounioja, K. ; Sipila, T. *et al.* 2007. Dual antenna receivers for high data rate terminals. *Wireless Personal Communications*. Springer Netherlands. 43(2). ISSN 0929–6212 (print) 1572–834X (online).

ZK–Crypt homepage [online], 2009. [cited 25 March 2009]. Available from Internet: <http:// www.fortressgb.com/apage/39649.php >.

BEPILOČIŲ ORLAIVIŲ RADIJO RYŠIO SISTEMOS ANALIZĖ

D. Rudinskas, Z. Goraj, J. Stankūnas

S a n t r a u k a

Straipsnyje nagrinėjami Lenkijos bepiločių orlaivių projekto SAMONIT (monitoringo lėktuvas) radijo ryšiu perduodamos informacijos saugumo klausimai. Ypač svarbi yra radijo ryšiu perduodamos informacijos apsauga kuriant bepiločius orlaivius (BO) ir kitas nuotolinio valdymo transporto priemones. Straipsnyje pateikiama SAMONIT ryšių sistemos struktūra, galimos grėsmės informacijos perdavimui, saugumui bei integralumui; taip pat radijo ryšio sistemos apsaugos būdai bei priemonės.

Reikšminiai žodžiai: bepilotis orlaivis, BO, saugumas, radijo ryšio sistema.