Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 319-326, 3, 2025

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 9, pp. 319-326, 3, 2025

Research Article

Integration of drones and intelligent security systems

József Udvaros[*1,2]

[1]*Department of Mathematics and Computer Science, Trnava University, Slovakia*
[2]*Department of Business Information Technology, Budapest University of Economics and Business, Hungary*

[*]*(jozsef.udvaros@truni.sk) Email of the corresponding author*

(Received: 12 March 2025, Accepted: 16 March 2025)

(6th International Conference on Innovative Academic Studies ICIAS 2025, March 12-13, 2025)

ATIF/REFERENCE: Udvaros, J. (2025). Integration of drones and intelligent security systems. *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(3), 319-326.

Abstract – The integration of drone technology and intelligent security systems is one of the most important research areas of our time, which can significantly contribute to more efficient and autonomous security solutions. The aim of this article is to examine the possibilities of connecting these two technological areas within a theoretical framework, highlighting the potential benefits of integration and the challenges it entails. We review the application possibilities of drones, as well as key elements of intelligent security systems such as IoT-based sensor networks and the role of artificial intelligence. We examine the possible integration models that enable the event-driven, autonomous application of drones in the security infrastructure, with particular attention to the possibilities of data collection, analysis and automatic response. We highlight the technical obstacles to implementation, such as communication, energy efficiency and the regulatory background. We briefly discuss the role of education, which is crucial for understanding the technology, gaining social acceptance and successfully applying the integration. The results of the study indicate that the integration of drones and intelligent security systems is theoretically sound and holds significant potential for the future in the security industry. The article recommends further research, especially in the areas of artificial intelligence development and the development of interdisciplinary educational programs.

Keywords – Intelligent Security Systems, Drones, Drone Technology, Autonomous Security Solutions, Education.

I. INTRODUCTION

In recent years, the security sector has increasingly focused on the use of various advanced technologies, especially drones and intelligent systems based on artificial intelligence (AI) and the Internet of Things (IoT). These innovative solutions offer significant development potential, as they enable faster detection of dangerous situations, real-time data collection and analysis, and automatic or semi-automatic implementation of appropriate measures. Drone technology stands out primarily for its mobility, autonomy, rapid response capability, and flexible applicability. In contrast, the most important advantage of intelligent security systems is that they process complex data, predict security incidents, and provide effective decision support to users.

By combining the two technologies, integrated security systems can be created that are more efficient and automated than ever before. Such integration can enable real-time, autonomous security surveillance, rapid emergency response, and intelligent risk analysis, thereby significantly reducing the potential for human error while increasing the reliability of the system as a whole.

However, integration is not without challenges: technical difficulties arise, for example, in the areas of stable data connectivity, energy efficiency, autonomy, and communication standards between systems. In addition, serious social, legal, and ethical concerns are associated with the use of such systems, especially in the areas of data protection, privacy, and liability issues.

Taking all of this into account, the aim of this study is to discuss the opportunities, benefits, and challenges and obstacles related to the integration of drone technology and intelligent security systems from a theoretical perspective. The study also briefly mentions the role of education, as the transfer of appropriate professional knowledge, the development of competencies, and the shaping of user attitudes are key to the social acceptance and successful application of the technology.

In the following chapters, we first provide a detailed overview of drone technology and the theoretical foundations of intelligent security systems, and then present integration options, analyzing their future significance for the further development of the security industry.

II. DRONE TECHNOLOGY OVERVIEW

Drone technology has undergone explosive development over the past decade and now is increasingly used not only for military or hobbyist applications, but also in many civilian areas, such as agriculture, environmental protection, industrial inspection and especially security. These devices commonly referred to as Unmanned Aerial Vehicles (UAVs), play a prominent role in situations where rapid mobility, access to hard-to-reach places, or safe reconnaissance in dangerous environments are required.

Drones can generally be divided into three main categories based on their size, capabilities and application areas: micro drones, small and medium-sized drones, and long-range professional UAV systems. The most common type of drones in security applications are small, highly maneuverable, and equipped with multiple sensors (such as cameras, infrared sensors, LiDAR systems). These devices are capable of quickly and efficiently monitoring larger areas, and collecting and transmitting data in real time to security centers.

One of the most important features of drone technology is its level of autonomy, which is supported by the continuous development of on-board control systems and decision-support algorithms based on artificial intelligence. Recent developments allow drones to navigate independently, avoid obstacles, and be able to perform automatic missions without human intervention. With the development of communication technologies, they are now also capable of real-time, high-speed data transmission and remote control, making them an ideal platform as part of intelligent security systems [1].

However, it is important to emphasize that drone technology currently has limitations. The issue of power supply is particularly challenging, as limited battery capacity can significantly reduce the operating time and range of drones. In addition, the technological background necessary for the autonomous operation of drones, such as stable communication, adequate data security, and the regulatory environment, still requires significant development.

In the following, I will summarize the most important technological features and operational characteristics of drones, present the diverse application possibilities of drone technology in various industries, highlight the role of education in understanding and effectively utilizing drone technology, and describe the current challenges and future perspectives of the technology.

A. The most important technological features and functionalities of drones

Drones are unmanned aerial vehicles (UAVs) that are capable of operating autonomously or remotely. Their technological equipment includes, among others, sensor and control systems, obstacle avoidance technologies, and the use of cognitive radio technologies. Advanced technology allows them to reach difficult-to-reach areas with or without human intervention, making them widely used in military, commercial, personal, and future technological applications. An overview of drone technology highlights the versatility of their operation, from small, compact devices to long-range, highly advanced systems,

with a particular emphasis on the potential for autonomous operation through the integration of artificial intelligence and machine learning [2].

B. Application opportunities for drone technology in various industries

Drones can be widely used in many industries, such as environmental protection, disaster management, agricultural optimization, infrastructure analysis, military operations, sports and recreation, and firefighting and rescue tasks [3]. Industrial drone applications can revolutionize the operation of industries such as agriculture, healthcare, and military. In addition, drones are expected to play a key role in future communication technologies, especially in next-generation wireless networks [4].

C. The role of education in understanding and applying drone technology

Education is crucial for the effective understanding and dissemination of drone technology and the training of future professionals, especially in the fields of science, technology, engineering and mathematics (STEM). There is a growing need to integrate drones and related GIS technologies into the education system. Drones can be successfully used in the teaching of basic GIS and engineering skills from primary school to higher education, supporting a broad, structured understanding of the technology [5][6].

D. Current challenges and future opportunities for drone technology

The increasingly widespread industrial application of drone technology creates many new opportunities, but also raises significant challenges, such as security issues, the risk of cyberattacks, and the problem of malicious use. Future prospects for the technology include the exponential growth of the Asian market, the widespread use of drone technology in government and business, and the further development of AI and machine learning-based autonomous decision-making and adaptive operation [7][8].

The diversity of technical features of drone technology holds significant industrial and societal opportunities, to which education can contribute significantly. Despite security and cybersecurity challenges, the future development prospects of the technology are extremely promising, both in terms of market growth and technological advancement [9][10].

III. CHARACTERISTICS OF INTELLIGENT SECURITY SYSTEMS

A. Theoretical foundations and main components

Intelligent security systems are built on several theoretical foundations and technological components that enable the integration of advanced methods and technologies.

Basic elements

These systems usually consist of a central unit, subsystems and separate components that work together to manage security threats. The central element is typically a protected system that includes artificial intelligence (AI) elements and focuses primarily on managing security threats, significantly improving the functionality of the entire system [11].

Design principles

Common principles used in the design of intelligent security systems include decomposition, the use of neural networks, digital signal processing, and the incorporation of algorithms based on artificial intelligence. Other areas of emphasis include digital signal processing technologies, machine learning algorithms and various forms of artificial intelligence. The integration of these technologies enables real-time pattern recognition and automatic management of security threats [12].

Security analysis frameworks

For example, Negative Systems Theory is often used as an analytical framework for intelligent security systems, which emphasizes openness, inclusiveness, interactive connections between systems, and maintaining dynamic equilibrium. Negative Systems Theory is applied in systems, which helps identify potential security threats arising from open and interactive connections, and analyzes the stability of system subcomponents.

B. The role of education in the dissemination of smart technologies

Education can play a crucial role in the successful dissemination and effective use of smart technologies:

- STEM/STEAM education: Science, technology, engineering, arts, and mathematics (STEAM) education helps prepare the young generation for the technological challenges of the future. This multidisciplinary educational paradigm is key to fostering creativity, developing problem-solving skills, and improving the long-term quality of life [14][15].
- Education systems need to be renewed in order to integrate knowledge elements related to drones and intelligent security systems. It is particularly important to create safe, inclusive, and effective learning environments that provide students with the opportunity to understand the complexity of intelligent technologies and effectively apply them [16][17][18].

Intelligent security systems are built on the integration of several advanced technologies and theoretical concepts, and providing an appropriate, multidisciplinary educational background is a key factor in the successful application of which.

IV. THEORETICAL BACKGROUND FOR THE INTEGRATION OF DRONES AND INTELLIGENT SECURITY SYSTEMS

In the previous chapter, we reviewed the most important features and application possibilities of drone technology. In this chapter, we present the theoretical foundations of the operation of intelligent security systems, as well as the key technological components that enable the autonomous, adaptive and real-time operation of the systems. This overview provides the basis for a better understanding of the integration possibilities discussed later.

A. Possible models and conceptual frameworks for integration

Conceptual process models

One of the key theoretical foundations for the integration of drones into practice is the so-called conceptual process models. According to a proposed model, the connection of drones and intelligent security systems requires the definition of a central system (core) for managing basic risks, as well as the definition of related subsystems and components. These models enable the rapid and efficient management of security threats and incidents [19].

According to another theoretical approach, the basis for the application of drones for security purposes is the so-called Internet of Drones (IoD) concept, which uses trusted authority centres for secure and efficient communication. This ensures the reliability and security of communication channels while ensuring the portability of devices [20].

Theoretical frameworks

A comprehensive theoretical framework is essential for understanding the integration process, which allows for the systematization and categorization of different types of drones. Such a system supports a multifaceted understanding of drones and helps to map the relationships between different technological, functional and usage characteristics [21].

The integration of artificial intelligence (AI) into drones has brought significant progress in the field of autonomous operation and real-time decision-making, while simultaneously laying the foundation for a wide range of security applications for drones [22].

Security modeling frameworks

System models such as Negative Systems Theory, which provide a theoretical basis for security analyses related to integration, provide an open, interactive connection, and dynamic equilibrium. This approach supports the identification of security threats and the analysis of the stability of subsystems [23].

Other theoretical models exist to address security challenges, such as ethical hacking frameworks for testing the resilience of drones, which aim to examine and improve the resilience of drones to cyberattacks and malicious interference [24].

B. The role of education in disseminating professional and theoretical knowledge

Education plays a fundamental role in the effective understanding and application of smart security technologies. It is important to create training programs that prepare professionals and researchers using drones as measurement tools, taking into account measurement uncertainties and accuracy requirements [25].

The importance of practice-oriented education is also evident in the training of security professionals, for example during law enforcement training, where participants also learn the practical handling and control of UAV devices.

Methodological approaches used in education include the Educational Mechatronics Conceptual Framework (EMCF), which provides students with the opportunity to acquire knowledge and skills related to drones in realistic simulation environments, thereby developing their practical competencies [26][27].

According to the definition emphasizing the importance of STEM/STEAM integration in education, the use of drones can effectively develop students' interdisciplinary thinking and problem-solving skills, contributing to their effective preparation for the future labor market [28][29].

The integration of drones and intelligent security systems includes several theoretical models and conceptual frameworks that address various aspects of safety, autonomy, and practical applications. Educational initiatives are of paramount importance in disseminating professional knowledge and theoretical understanding, preparing future professionals through specialized training. Drone education, which fits into the STEM framework, also supports multidisciplinary learning, facilitating the development of students' competencies in order to effectively prepare them for the technological challenges of the future.

V. FUTURE RESEARCH DIRECTIONS

In the previous chapters, we presented the theoretical foundations, operational characteristics and application possibilities of the integration of drone technology and intelligent security systems. In this chapter, we focus on future research directions that can further increase the effectiveness and widespread acceptance of these technologies.

A. Technological development and new theoretical opportunities

The integration of drones and intelligent security systems is expected to undergo significant further development. One of the main directions of future research will be the development of artificial intelligence and machine learning capabilities, with particular attention to autonomous decision-making, real-time event detection, and increasing the accuracy of predictive analytics. Another important area of research could be increasing the energy efficiency of drones, for example by using alternative energy sources, new battery technologies, or even wireless power transfer.

In addition, innovations are expected in the field of communication technologies, especially in the field of 5G and future 6G networks, which will enable more stable, faster and more secure data connections between drones and intelligent systems. New theoretical models can also be developed, such as integrated frameworks that can more effectively handle complex security challenges, thereby improving the reliability and scalability of the entire system.

B. *Education as a way to support technological developments*

In parallel with technological developments, the role of education cannot be neglected. In short, it should be emphasized that educational institutions, especially higher education institutions, will play a key role in training future technology professionals. Integrating new technologies into curricula and transferring multidisciplinary knowledge can ensure that students are able to effectively utilize and further develop intelligent security systems and drone technology.

Combining theoretical and practical knowledge within STEM education can contribute to the next generation of professionals becoming responsible and safe users and developers of new technologies. To this end, future research should examine the educational methods and tools that can most effectively convey complex knowledge related to intelligent systems.

VI. DISCUSSION

Based on the theoretical approaches presented in this article, it is clear that the integration of drones and intelligent security systems offers significant opportunities for the security sector. The systems resulting from the integration can significantly outperform traditional security solutions in terms of autonomy, reaction speed, data collection capacity and event management efficiency. However, these technologies also face several challenges, such as limited energy resources, ensuring secure communication, or obstacles arising from the data protection and legal environment. These factors may currently hinder the wider spread and acceptance of the technology.

Another important question is how to increase social acceptance, which depends significantly on people's security awareness and how trustworthy they consider new technologies. In the case of drones, privacy protection may be a particularly sensitive area, which requires further research and regulatory steps.

The role of education in this process is of paramount importance: appropriate training and educational programs can provide the necessary theoretical knowledge and practical skills for professionals, and education can also be of fundamental importance in shaping broader social awareness.

The integration models and conceptual frameworks revealed during the research can provide a suitable basis for further empirical studies, which can help to more accurately identify real practical challenges and solution options.

VII. CONCLUSION

This study examined the possibilities of integrating drone technology and intelligent security systems within a theoretical framework. We demonstrated that the combination of the mobility, autonomous operation capability and real-time data collection capabilities of drones, and the advanced analytical, decision-support and autonomous action capabilities of intelligent security systems can create integrated systems that significantly increase the efficiency of security applications.

The analysis highlighted that although integration offers numerous technological advantages, it also faces various technical, legal and social challenges. The most prominent of these are the standardization of communication standards, the issue of energy supply, and the consideration of data protection and ethical aspects.

Future research should focus on further integrating artificial intelligence, developing autonomy and decision-making capabilities, and increasing the efficiency of education. Emphasizing the role of education is crucial, as the acquisition of multidisciplinary competencies required by future professionals is a fundamental condition for the successful application of technology.

It can be stated that the integration of drones and intelligent security systems offers promising opportunities, but at the same time requires careful preparation and conscious development in order for the technology to become widely applicable and socially accepted in the long term.

REFERENCES

[1] Kiss, G. and Berecz, É.C., 2019. Questions of security in the world of autonomous vehicles. In Proceedings of the 5th International Conference on e-Society, e-Learning and e-Technologies (pp. 109-115).

[2] Gholami, A., 2024. Exploring drone classifications and applications: a review. International Journal of Engineering and Geosciences, 9(3), pp.418-442.

[3] Baruah, R.L. and Dagar, S.B., 2023. Fire fighter drone with robotic gripper. Materials Today: Proceedings, 79, pp.334-337.

[4] Lucia, L.D. and Vegni, A.M., 2023. UAV main applications: From military to agriculture fields. In Internet of Unmanned Things (IoUT) and Mission-based Networking (pp. 1-23). Cham: Springer International Publishing.

[5] Joyce, K.E., Meiklejohn, N. and Mead, P.C.H., 2020. Using minidrones to teach geospatial technology fundamentals. Drones, 4 (3), 1–11 [online]

[6] Gabaľová, V., 2025. Teaching Robotics in Education 4.0. International Journal of Advanced Natural Sciences and Engineering Researches, 9(3), 191–202.

[7] Krichen, M., Adoni, W.Y.H., Mihoub, A., Alzahrani, M.Y. and Nahhal, T., 2022. Security challenges for drone communications: Possible threats, attacks and countermeasures. In 2022 2nd International conference of smart systems and emerging technologies (SMARTTECH) (pp. 184-189). IEEE.

[8] Granieri, F., 2024. Navigating the Skies: A cross-country exploration of drone policies in Europe, USA and China, unveiling privacy and cybersecurity challenges. JL, Mkt. & Innovation, p.156.

[9] Sivaraks, J., Malisuwan, S. and Kaewphanuekrungsi, W., 2021. Space Industry Development: Opportunities and Challenging in Thailand. International Journal of Science and Management Studies (IJSMS), 4(5), pp.64-71.

[10] Thai, H.D., Yoon, C.W. and Huh, J.H., 2024. Recent Development of Drone Technology Software Engineering: A Systematic Survey. IEEE Access.

[11] Korneev, N.V., 2020. Intelligent complex security management system FEC for the industry 5.0. In IOP Conference Series: Materials Science and Engineering (Vol. 950, No. 1, p. 012016). IOP Publishing.

[12] Amosov, O.S. and Baena, S.G., 2017. The hierarchical approach to designing the Intelligent Information and Telecommunication System for Higher Educational Institution Security. In 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM) (pp. 116-119). IEEE.

[13] Lixia, N.I.U., Xiaomeng, L.I. and Hongmei, W.A.N.G., 2024. Construction of intelligent system security analysis system under view of negative systematics in 5G era. China Safety Science Journal, 34(8), p.1.

[14] Nakata, H., Takamatsu, K., Bannaka, K., Kozaki, R., Murakami, K., Matsumoto, S., Kishida, A. and Nakata, Y., 2023. Proposal of Knowledge Network Model Education for STEM/STEAM Education. In International Congress on Information and Communication Technology (pp. 571-579). Singapore: Springer Nature Singapore

[15] Hyksova, H., Stoffová, V. and Gabaľová, V., 2022. Teaching robotics and online programming using a virtual robot. In INTED2022 Proceedings (pp. 7140-7147). IATED.

[16] Gonçalves, B.F., Patrício, M.R. and Comiche, A., 2024. The Challenges of Learning Assessment in the Age of Artificial Intelligence. In World Conference on Information Systems and Technologies (pp. 23-32). Cham: Springer Nature Switzerland.

[17] Yakovleva, O., Slyusar, V., Kushnir, O. and Sabovchyk, A., 2021. New trends in scientific and technological revolution (STR) and transformation of science and education systems in the paradigm of sustainable development. In E3S Web of Conferences (Vol. 277, p. 06006). EDP Sciences.

[18] Gabal'ová, V., Karpielová, M. and Stoffová, V., 2023. Beginners Online Programming Course for Making Games in Construct 2. In Proceedings of International Conference on Recent Innovations in Computing: ICRIC 2022, Volume 1 (pp. 547-558). Singapore: Springer Nature Singapore.

[19] Thangavelu, S., Janczewski, L., Peko, G. and Sundaram, D., 2020. A Dynamic security-dedicated approach to commercial drone vulnerabilities, threat vectors and their mitigation. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1054-1059). IEEE.

[20] El Hanine, M., El-Yahyaoui, A. and Es-Sadaoui, R., 2024. The Internet of Drones: Evolution, Applications and Security Solutions. In International Conference On Big Data and Internet of Things (pp. 955-965). Cham: Springer Nature Switzerland.

[21] Barros, J., Henriques, J., Reis, J., Rosado, D.P. and Melão, N., 2024. Unmanned aerial systems: a systematic literature review. In International Conference on Information Technology & Systems (pp. 82-93). Cham: Springer Nature Switzerland.

[22] Caballero-Martin, D., Lopez-Guede, J.M., Estevez, J. and Graña, M., 2024. Artificial intelligence applied to drone control: A state of the art. Drones, 8(7), p.296.

[23] Rimoli, G.P., Palmieri, F. and Ficco, M., 2024. Synthetic threat dataset generation by uav fleet simulation. In The 14th International Defense and Homeland Security Simulation Workshop (pp. 1-8).

[24] Baird, A., Pearce, H., Pinisetty, S. and Roop, P., 2022. Runtime interchange of enforcers for adaptive attacks: A security analysis framework for drones. In 2022 20th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE) (pp. 1-11). IEEE.

[25] Daponte, P., De Vito, L., Lamonaca, F., Picariello, F., Rapuano, S. and Riccio, M., 2017. Measurement science and education in the drone times. In 2017 IEEE international instrumentation and measurement technology conference (I2MTC) (pp. 1-6). IEEE.
[26] Luque-Vega, L.F., Lopez-Neri, E., Arellano-Muro, C.A., González-Jiménez, L.E., Ghommam, J., Saad, M., Carrasco-Navarro, R., Ruíz-Cruz, R. and Guerrero-Osuna, H.A., 2022. UAV-based smart educational mechatronics system using a MoCap laboratory and hardware-in-the-loop. Sensors, 22(15), p.5707.
[27] Sedláček, M., Mráz, E., Rajchl, M. and Rodina, J., 2023. Environment for UAV education. In International Conference on Robotics in Education (RiE) (pp. 257-269). Cham: Springer Nature Switzerland.
[28] Ahmed, H.O.K., 2021. Towards application of drone-based GeoSTEM education: Teacher educators readiness (attitudes, competencies, and obstacles). Education and Information Technologies, 26(4), pp.4379-4400.
[29] Joyce, K.E., Meiklejohn, N. and Mead, P.C., 2020. Using minidrones to teach geospatial technology fundamentals. Drones, 4(3), p.57.