Section 2

AIUAVS-DEVSECOPS METHODOLOGY AS SUPPORT UAV-BASED MINE CLEARANCE INFRASTRUCTURE

Bohdan Kosarevskyi
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser: Artem Tetskyi

Relevance. Ongoing warfare has left many regions contaminated with mines and unexploded ordnance, which hampers safe movement, infrastructure restoration, and the return to normal life. Unmanned aerial vehicles equipped with advanced sensors and tools have become essential in modern demining technology. These drones can detect mines and explosive devices from a safe distance, significantly reducing the risk to human operators. The integration of artificial intelligence further allows for real-time data analysis, facilitating informed decision-making and reducing operational costs.

Purpose. This study aims to review existing information technology methods and adaptations used in deploying unmanned intelligent systems for land demining, with a particular focus on information security. It covers security assessment methods, relevant metrics for demining support systems, and explains the AIUAVS-DevSecOps methodology, which integrates AI and DevSecOps principles.

Principal provisions. Several existing methodologies and frameworks are analyzed. The CVAIM method [1], an iterative process designed for business projects, can be adapted to deploy safe infrastructure for unmanned demining systems. The System Infrastructure Development Life Cycle adapts the SDLC specifically for infrastructure solutions, providing a seven-stage process - from requirements gathering to decommissioning - that integrates infrastructure-specific needs and security considerations at every step. The idea of dynamically distributing computations between local and remote resources to reduce processing time and maintain the compactness and energy efficiency of local resources by using larger computing capacities remotely [2]. Edge computing optimizes decision-making for offloading tasks, reducing latency and energy use, although data security remains a critical concern [3]. Optimal cloud infrastructure design focuses on security and scalability, addressing specific demining challenges. UAV swarms within networked control systems enhance productivity and efficiency but face resource and security constraints.

Securing UAV-based demining systems involves ensuring system reliability (measured by the Comprehensive Reliability Indicator), data integrity through encryption and authentication, robust cybersecurity measures like multi-factor authentication and intrusion detection, operational security via access control and risk management, and functional safety through testing and compliance with safety standards. The AIUAVS-DevSecOps methodology integrates AI and DevSecOps to rapidly develop and deploy secure infrastructure in critical systems, emphasizing continuous security monitoring, real-time management with anomaly detection, automated processes, and secure infrastructure management.

Conclusions. Modern IT methods are indispensable for creating and maintaining secure infrastructure for UAV-based demining systems. AI and AIUAVS-DevSecOps enhance system security, efficiency, and reliability. AI significantly improves the accuracy and speed of detecting explosives. As technology advances, unmanned systems are becoming more effective and safer, reducing the risk to human operators.

List of references

1. Banz A. Requirements Engineering Method for Infrastructure Automation and Cloud Projects. 2019 IEEE 27th International Requirements Engineering Conference (RE). 2019. Page 276-285. DOI: https://doi.org/10.1109/RE.2019.00037.
2. Callegaro D., Baidya S., Levorato M. Dynamic Distributed Computing for Infrastructure-Assisted Autonomous UAVs. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). 2020. Page 1-6. DOI: https://doi.org/10.1109/ICC40277.2020.9148986.
3. Callegaro D., Levorato M. Optimal Edge Computing for Infrastructure-Assisted UAV Systems. IEEE Transactions on Vehicular Technology. Volume 70(2). 2021. Page 1782-1792. DOI: https://doi.org/10.1109/TVT.2021.3051378.

Information about the authors

Bohdan Kosarevskyi, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», b.v.kosarevskyi@student.csn.khai.edu

Artem Tetskyi, PhD, Associate Professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», a.tetskiy@csn.khai.edu