Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 130 **2026**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2026.130.17

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Zieliński, T. AI-enabled defense-in-depth: a multi-layered framework for countering UAS threats in smart airports. *Scientific Journal of Silesian University of Technology. Series Transport*. 2026, **130**, 299-323. ISSN: 0209-3324.
DOI: https://doi.org/10.20858/sjsutst.2026.130.17

Tadeusz ZIELIŃSKI[1]

AI-ENABLED DEFENSE-IN-DEPTH: A MULTI-LAYERED FRAMEWORK FOR COUNTERING UAS THREATS IN SMART AIRPORTS

Summary. Smart airports increasingly rely on interconnected cyber-physical systems, data-driven operations, and automation, which expands the attack surface for incidents involving unmanned aircraft systems (UAS). This article develops an AI-enabled defense-in-depth (DiD) conceptual framework for countering UAS threats in smart airports, addressing both kinetic and cyber-physical vectors while respecting the constraints of safety-critical aviation operations. The AI-based Intrusion Risk Intervention (AIRI) framework is central to the proposed approach. AIRI specifies a five-stage decision loop (detect–classify–assess–intervene–learn) integrating multimodal sensing, AI-assisted risk scoring, and human-in-the-loop decision support. The framework is positioned against representative airport-oriented UAS incident-management guidance and counter-UAS frameworks, and a compact validation is provided through (a) a cross-walk between AIRI stages and established incident-management steps and (b) a scenario exercise illustrating decision thresholds and intervention options. The paper further discusses regulatory, ethical, and operational requirements for deploying AI-enabled counter-UAS capabilities in European aviation, emphasizing traceability, logging, robustness, information-security management, and accountability. Claims are therefore limited to conceptual and design contributions

[1] Military Faculty, War Studies University, al. gen. A. Chruściela „Montera” 103, 00-910 Warszawa, Poland. Email: t-zielinski@akademia.mil.pl. ORCID: https://orcid.org/0000-0003-0605-7684

supported by the compact validation; the paper concludes by outlining the data, metrics, and governance artifacts required for future empirical evaluation in operational airport environments.

Keywords: smart airports, unmanned aircraft systems (UAS), artificial intelligence (AI) in aviation, counter-UAS (C-UAS), airport security frameworks

1. INTRODUCTION

The emergence of smart airports signifies a transformative moment in the evolution of global civil aviation. Situated at the crossroads of advanced digitalization, artificial intelligence (AI), and interconnected sensor technologies, smart airports reflect a paradigm shift from static transport nodes to intelligent, self-regulating ecosystems. These airports are crafted not only as gateways for air traffic but as dynamic operational environments that seamlessly integrate data from passengers, aircraft, logistics systems, and infrastructure components into real-time workflows. From biometric boarding and AI-enabled queue management to predictive maintenance and autonomous ground vehicles, the modern smart airport harnesses a wide range of cyber-physical technologies to enhance efficiency, sustainability, and user experience. However, this convergence of digital and physical layers also creates a broader, increasingly vulnerable threat landscape, especially given the emerging aerial threats posed by unmanned aircraft systems (UAS).

The rise of UAS – commonly called drones – has introduced new asymmetries and uncertainties into airport security. Originally developed for military reconnaissance and later adapted for commercial and recreational use, drones have transformed into modular, affordable, and highly maneuverable platforms capable of carrying sensors, payloads, or cyberattack vectors. The exponential growth in drone ownership, combined with the increasing autonomy of these systems, has made traditional perimeter-based security architectures irrelevant. Recent high-profile incidents – especially the extended disruption at London Gatwick Airport in 2018, which grounded over 1,000 flights – highlight how easily a single unauthorized drone can disrupt airport operations. These events have exposed critical vulnerabilities in current detection and mitigation capabilities and have raised concerns about the readiness of even technologically advanced airports to address low-cost, high-impact aerial incursions.

In this paper, unmanned aircraft system (UAS) is used as the primary term because airport protection and counter-UAS measures concern not only the aerial platform but the entire system (aircraft, command-and-control link, control station, payload, and supporting elements). The term unmanned aerial vehicle (UAV) denotes the aerial vehicle alone and is therefore avoided in the main narrative except when reproducing terminology used in cited sources or publication titles. The word drone is treated as a common, non-technical synonym used for readability at first mention and in selected illustrative passages; otherwise, the paper uses UAS consistently. Accordingly, counter-UAS (C-UAS) refers to the set of detection, tracking, identification, decision-support, and mitigation measures against unauthorized UAS activity in safety-critical airport environments.

Smart airports, because of their digital interdependence, are particularly vulnerable to these risks. Their reliance on Internet of Things (IoT) devices, wireless communication protocols, cloud-based data integration, and AI-driven decision systems has created a new operational paradigm that is highly efficient yet potentially fragile when faced with coordinated or intelligent threats. Today, a rogue drone is no longer just a nuisance in physical airspace; it can operate autonomously, capable of jamming radar signals, intercepting data packets, interfering

with navigation systems, or triggering false responses from AI surveillance tools. The complexity of managing such multi-domain threats, especially under real-time constraints, has far exceeded the capabilities of conventional counter-UAS (C-UAS) systems, which are typically reactive, siloed, and technologically outdated.

In this context, there is an urgent need for an integrated, adaptive, and intelligent framework capable of securing smart airports against UAS threats that reflects the complexity of their technological architecture. This paper addresses this need by introducing a defense-in-depth strategy tailored to smart airport environments, underpinned by a novel AI-based methodology called the AIRI model (AI-based Intrusion Risk Intervention). The defense-in-depth approach conceptualizes airport security as a multi-layered construct comprising physical detection and mitigation tools, digital safeguards against cyber-physical manipulation, and cognitive AI systems capable of interpreting threat behavior and supporting decision-making. Rather than relying on static defenses or isolated mitigation technologies, the framework envisions a resilient security ecosystem that perceives, reasons, and learns.

Central to this approach is the AIRI model, which operationalizes the defense-in-depth paradigm by integrating sensor fusion, AI-based classification, dynamic risk assessment, and escalation protocols into a coherent, continuously learning cycle. By incorporating explainable AI, federated learning, and human-in-the-loop governance, AIRI ensures that its interventions are timely, effective, and legally and ethically sound. This is especially crucial in the regulated domain of civil aviation, where the margin for error is minimal and where disproportionate responses can pose systemic risks.

This research also situates its proposed solution within the broader regulatory and policy context of European and international aviation security. As highlighted by recent frameworks such as the EU Drone Strategy 2.0, EASA's AI Roadmap, and ICAO's Annex 17, the governance of drone threats and the certification of AI in safety-critical infrastructure have become top-tier priorities for aviation authorities. These documents collectively call for a new generation of AI systems that are technically robust, ethically grounded, auditable, and aligned with human oversight. The AIRI model is developed in accordance with these expectations, offering a practical contribution to the evolving landscape of AI assurance in aviation.

This paper makes three principal contributions. First, it redefines the smart airport's security architecture to account for contemporary UAS threat dynamics. Second, it proposes a technologically and ethically viable model for integrating AI into real-time risk mitigation. Third, it provides a foundation for harmonizing AI-enabled security tools with emerging regulatory regimes and operational norms in civil aviation.

The study adopts a design-oriented conceptual research approach combining (a) a targeted review of peer-reviewed literature on counter-UAS and smart-airport security, (b) analysis of official and quasi-official aviation security guidance (e.g., EASA, ICAO, FAA, IATA) to extract operational and governance requirements, and (iii) design of the AIRI artefact (process model) followed by a compact validation via a framework cross-walk and scenario exercise. This positioning clarifies that the contribution is an integrative, prescriptive framework rather than an empirical performance evaluation.

The remainder of the paper is organized as follows: Section 2 presents a literature review. Section 3 analyzes the evolving threat landscape of drones concerning smart airport vulnerabilities. Section 4 develops the defense-in-depth concept, integrating physical, digital, and cognitive layers. Section 5 presents the AIRI methodology as a practical AI-enabled drone intrusion response model. Section 6 explores the regulatory, ethical, and operational implications of implementing such a system. Finally, Section 7 offers concluding reflections

and strategic recommendations for future research, policy design, and airport-level implementation.

2. LITERATURE REVIEW

Smart airports represent a paradigm shift in aviation, leveraging advanced technologies to enhance operational efficiency, passenger experiences, and security [1]. These airports integrate numerous systems, including sophisticated surveillance, data analytics, and automation, to optimize baggage handling and air traffic control processes [2]. The foundation of a smart airport lies in its ability to collect and process vast amounts of data from various sources, such as sensors, cameras, and passenger information systems [3]. This data-driven approach facilitates real-time decision-making, predictive maintenance, and personalized services, thus improving airport performance. Artificial intelligence plays a pivotal role in smart airports, enabling advanced functionalities such as automated security screening, predictive maintenance of airport infrastructure, and intelligent resource allocation [2]. AI algorithms can analyze passenger flow patterns to optimize gate assignments, reduce congestion, and enhance the overall passenger experience while providing proactive security measures by predicting and preventing potential threats [4]. Moreover, AI-powered systems can monitor and manage energy consumption, contributing to the airport's sustainability goals [5]. The integration of AI in air traffic control, for instance, can enhance safety and efficiency by predicting potential collisions and optimizing flight paths [6]. The complexity of smart airports necessitates robust cybersecurity measures to protect sensitive data and critical infrastructure from possible threats. The evolution of smart airports is closely linked to the development and deployment of advanced technologies such as the Internet of Things, cloud computing, and big data analytics, which collectively provide the infrastructure for intelligent airport operations. Engineering professionals and aviation construction experts acknowledge the transformative potential of AI to revolutionize project management processes in the aviation sector, thereby improving decision-making capabilities and overall efficiency [7].

The increasing prevalence of unmanned aircraft systems, or drones, poses a significant threat to airport operations and security [8]. UAS can be employed for various malicious purposes, including surveillance, smuggling, and even terrorist attacks. The potential for UAS to disrupt air traffic, damage aircraft, or harm individuals on the ground is a serious concern for airport authorities and security agencies [5]. The relatively low cost and easy access to drones make them an attractive tool for malicious actors. The growing sophistication of drone technology, including advanced navigation systems, extended flight ranges, and payload capacities, further amplifies the risk. The integration of AI in military applications underscores the potential for autonomous drones to conduct coordinated attacks, thereby making detection and interception even more challenging [5]. Airports must develop comprehensive counter-UAS strategies to mitigate these risks and safeguard their airspace and infrastructure. The susceptibility of drone technology to cyberattacks introduces another layer of complexity, as malicious actors can take control of drones and exploit them for nefarious purposes [9]. The use of commercial drones for illicit activities such as drug trafficking or unauthorized surveillance near airports has become an increasing concern for law enforcement agencies [5]. AI systems are vulnerable to manipulation through “deep fakes,” which could lead to misinformation and increased global instability [5]. The convergence of AI and drone technology necessitates ongoing monitoring and adaptation of security measures to counter potential threats.

Effective drone detection and risk mitigation are critical components of a comprehensive counter-UAS framework for smart airports. These countermeasures typically involve a multi-layered approach that integrates various technologies and strategies to detect, track, identify, and neutralize unauthorized drones. Radar systems, acoustic sensors, and optical cameras are commonly used to detect drones in airport airspace. These technologies can provide early warning of potential threats, allowing security personnel to act appropriately [10]. Radio frequency scanners can detect and analyze the communication signals between drones and their operators, aiding in identifying and tracking unauthorized UAS [11]. AI-powered video analytics can automatically detect and classify drones in real time, reducing the workload on human operators and improving threat-detection accuracy. Moreover, machine learning algorithms can be trained to identify anomalous drone behavior, such as unusual flight patterns or proximity to restricted areas, further enhancing situational awareness. Integrating these detection systems with risk assessment models can help prioritize threats and allocate resources effectively. Predictive analytics, driven by AI, can forecast potential drone incursions based on historical data, weather patterns, and other relevant factors, enabling proactive security measures. Real-time data analytics and integration of AI techniques can enhance automated incident management and overall transportation efficiency [12].

Neutralization techniques are used to disable or remove unauthorized drones from airport airspace, preventing them from causing harm or disruption. These methods range from non-kinetic measures, such as jamming and spoofing, to kinetic options, such as drone interceptors. Jamming disrupts communication between the drone and its operator, causing it to lose control or crash. Conversely, spoofing sends false GPS signals to the drone, redirecting it away from the airport or prompting it to land in a safe area. Drone interceptors, usually other drones equipped with nets or capture devices, can physically remove unauthorized drones from the airspace. These defensive systems aim to address challenges and reduce risks posed by hostile UAS incursions. Deploying such systems requires careful consideration of legal and regulatory implications and potential safety risks. Utilizing AI in autonomous weapon systems raises ethical concerns and questions about accountability. It's important to recognize that some neutralization techniques may interfere with legitimate drone operations or other airport systems. Careful planning and coordination are vital to minimize collateral effects.

AI-enabled defense-in-depth strategies are increasingly discussed as a way to counter UAS threats in smart airports by improving detection, classification, and risk-informed response. In safety-critical civil aviation, the role of AI is primarily decision support: fusing multi-modal sensor data (e.g., radar, RF, acoustic, EO/IR) and prioritizing events for human review, rather than replacing operational decision-makers. Machine learning can improve classification under cluttered conditions and support anomaly detection for cyber-physical interference and spoofing attempts [14-16].

Important ethical and legal issues arise when using AI systems in smart airports. The operational context of AI systems is crucial, as the risk of miscalculation increases when the context deviates from the training data [17]. It is crucial to remember that AI-driven systems are vulnerable to adversarial attacks, wherein malicious actors strategically manipulate input data to cause the AI to make incorrect decisions.

To identify the specific features of AIRI, Table 1 compares it with representative airport-oriented UAS incident-management guidance and critical-infrastructure counter-UAS frameworks. Existing guidance typically specifies governance and operational steps (detection–assessment–response–recovery) but remains intentionally technology-agnostic, with limited treatment of AI-enabled sensor fusion, real-time risk scoring, and post-incident learning loops. AIRI contributes an explicit, auditable AI-enabled decision loop that integrates these process

requirements with human oversight and continuous learning, making it suitable for safety-critical smart-airport environments.

Tab. 1

Positioning of AIRI against representative airport-oriented UAS incident-management guidance and counter-UAS frameworks

Framework (source)	Primary scope	Core process / phases	AI-specific content	Learning / feedback	Gap addressed by AIRI
EASA Drone Incident Management at Aerodromes [34]	Aerodrome ops & ANSP response	Report-assess-decide-respond-recover	Limited (tech-agnostic)	After-action lessons (procedural)	Adds AI-enabled risk scoring + auditable thresholds
ICAO infrastructure protection guidance [42]	Civil aviation infrastructure security	Preparedness-detection-response-recovery	Limited (tech-agnostic)	Post-event reporting (high level)	Adds learning loop linked to model/SOP updates
JRC five-phase approach [31]	Critical infrastructure protection	Prepare-prevent-detect-respond-recover	Mentions tech options	Continuous improvement emphasized	Operationalizes phases as AI decision loop + playbooks
FAA airport UAS detection/response work [46]	US airport UAS governance	Detection-coordination-response planning	Focus on legal/operational constraints	Iterative trials recommended	Integrates safety/legal constraints into interventions
IATA guidance on unauthorized UAS [54]	Airport/ANSP/operator coordination	Detection-response-recovery taxonomy	None (process focus)	Reporting & improvement	Provides AI-enabled prioritization + decision support
Standardized evaluation approaches (e.g., CWA 18150) [57]	Testing & evaluation	Scenario-based tests and metrics	Metrics for multi-sensor performance	Validation & comparability	Links evaluation metrics to AIRI outputs
AIRI (this paper)	Smart airports (cyber-physical)	Detect-classify-assess-intervene-learn	Explicit (fusion, risk scoring, Human-in-the-Loop)	Explicit (model + SOP update loop)	–

3. UAS THREAT LANDSCAPE IN THE ERA OF SMART AIRPORTS

Compartmentalized operations, paper-based procedures, and limited communication between systems have long characterized traditional airports. While functional, these infrastructures are increasingly strained by rising passenger volumes, growing security demands, and the necessity for environmental responsibility. In contrast, smart airports emerge as integrated digital environments that adapt to operational and passenger-related variables in real time. The shift is not purely technological but systemic, involving the convergence of data-driven decision-making with automated and autonomous processes that optimize every aspect of airport functioning [18].

At the heart of the smart airport is a network of interconnected technologies that work together to enhance efficiency, safety, and user experience. Infrastructure equipped with IoT devices allows for continuous monitoring of baggage, vehicles, environmental conditions, and passenger flow. Artificial intelligence enables predictive management of traffic patterns, resource allocation, and maintenance needs. Biometric identity verification speeds up passenger processing while enhancing security and minimizing physical contact. These components are supported by cloud-based platforms that facilitate real-time coordination among airport authorities, airlines, and service providers, ensuring a comprehensive and synchronized approach to operations [19].

One of the most striking differences between smart and traditional airports is the transformation of the passenger experience. In a conventional airport, travelers face manual check-in processes, physical document verification, and limited real-time information. In contrast, a smart airport enables passengers to navigate their journey using mobile applications, biometric authentication, and AI-guided assistance, often without interacting with airport staff. Baggage is tracked using RFID tags and routed by predictive logistics systems, minimizing delays and mishandling. On the airside, aircraft movements are directed by algorithms that calculate optimal taxiing routes, reducing fuel consumption and turnaround time. Once reliant on scheduled inspections, facility maintenance is now guided by sensor data that indicates when intervention is needed, enhancing safety and reducing operational downtime [20].

The operational transformation introduced by smart airports also extends to strategic areas. Enhanced automation and predictive analytics lower operational costs and reduce the likelihood of human error, while boosting service speed and reliability. Security is fortified through real-time surveillance, behavior analysis, and integrated threat detection systems. Environmental performance benefits from smart grids, optimized energy use, and waste monitoring, aligning with global sustainability goals [21]. However, this reliance on interconnected systems poses challenges in data protection and cybersecurity as the airport's digital footprint expands.

Smart airports are also redefining the role of aviation hubs in the broader transport ecosystem. As digital platforms enable harmonization of schedules, services, and passenger data across modes of transport, airports become nodes of intermodal mobility – connecting air, rail, and road systems in a seamless continuum [22]. This creates new opportunities for urban development, economic growth, and public-private innovation, but it also necessitates robust regulatory frameworks to ensure the ethical and secure use of emerging technologies.

The emergence and rapid proliferation of unmanned aircraft systems (UAS), more commonly referred to as drones, have introduced a new and complex dimension to the security environment of civil aviation. While initially developed and deployed for military applications, drones have since evolved into versatile platforms widely accessible to consumers, commercial actors, and public institutions. Their utility in aerial photography, infrastructure inspection, logistics, and agriculture has positioned them as a cornerstone of modern airspace

innovation [23]. However, the ubiquity of these systems has simultaneously generated a range of unanticipated risks, often inadequately mitigated, particularly for airport infrastructure, which now stands at the intersection of digital transformation and increased operational vulnerability. The evolution toward smart airports, characterized by the extensive integration of artificial intelligence, interconnected sensors, IoT networks, and data-driven automation, further amplifies critical aviation nodes' exposure to kinetic and non-kinetic drone threats. The result is a security ecosystem in which technological sophistication is paralleled, if not outpaced, by the growing complexity of threat vectors originating from or enabled by rogue drone activities [24].

The accelerating pace of drone adoption across Europe and beyond has dramatically altered the structure of low-altitude airspace. Forecasts by aviation regulators such as EASA suggest that by the early 2030s, millions of drones will operate across European skies, many of them in or near urban centers and airport control zones [25]. This trend has been catalyzed by a range of enabling factors, including declining hardware costs, the widespread availability of commercial off-the-shelf systems, and the relative ease with which basic piloting skills can be acquired. Simultaneously, the capabilities of these platforms have advanced significantly. Contemporary drones are often equipped with high-resolution optical systems, GPS navigation, autonomous flight software, swarming algorithms, and in some cases, the capacity to carry and deploy physical payloads. Notably, these systems are often modular and dual-use, which means that platforms initially intended for benign civilian purposes can be readily repurposed for malicious activities [23]. The implications of this dual-use character are profound, as it complicates both regulatory classification and detection protocols. The same drone used for real-time infrastructure monitoring may be reconfigured for signal jamming, illicit surveillance, or even physical sabotage of critical airport assets.

Empirical evidence of drones' disruptive capacity in airport environments has steadily accumulated over the past decade, with several high-profile incidents underscoring both the severity of the threat and the institutional unpreparedness to address it effectively. Perhaps the most emblematic case occurred in December 2018 at London Gatwick Airport, where repeated sightings of unauthorized drones led to the cancellation or diversion of over one thousand flights, directly impacting more than 140,000 passengers and resulting in an estimated financial loss exceeding £50 million [26]. Despite deploying advanced military-grade detection systems and extensive coordination between law enforcement and aviation authorities, no individual or group was conclusively identified or apprehended in connection with the incident. The episode revealed critical weaknesses in the capacity to neutralize a drone once detected and in the fundamental processes of attribution, forensic reconstruction, and incident response. More importantly, it demonstrated that the operational disruption caused by drones does not necessarily depend on direct physical collisions with aircraft or infrastructure [27]. A drone's confirmed presence or credible suspicion within controlled airspace is sufficient to activate emergency protocols that can paralyze airport operations.

This vulnerability is not unique to Gatwick. Comparable incidents have been recorded in Frankfurt, Dubai, Madrid, and Warsaw, among others, where unauthorized drone activity near runways and approach paths has resulted in temporary airspace closures, delays, and emergency procedural adaptations. These cases collectively illustrate that the threat posed by drones is geographically diffuse and functionally diverse. Drones can be deployed to harass aircraft, film secure areas, smuggle contraband into airport perimeters, or test the response latency of security systems – all without the need for advanced military capabilities [28]. Furthermore, as smart airports increasingly rely on complex, interoperable digital ecosystems to manage everything from airside logistics to passenger flow, they become vulnerable to a new class of drone-

enabled attacks that exploit both the physical and cyber domains. Drones can carry payloads capable of intercepting wireless signals, GPS spoofing, or conducting denial-of-service attacks targeting Wi-Fi infrastructure and sensor networks. They can hover within the electromagnetic perimeter of an airport terminal and collect data passively, or they can actively disrupt operations by flooding network ports, jamming control channels, or delivering malicious code to connected devices [29]. The convergence of cyber and physical capabilities within a single aerial platform creates an asymmetric threat environment in which traditional perimeter defense models are mainly rendered obsolete.

The evolving architecture of smart airports further compounds these challenges. By design, smart airports are constructed as layered ecosystems of interdependent subsystems, each relying on continuous data exchange, real-time analytics, and adaptive AI decision-making. These systems include automated baggage handling, intelligent lighting, HVAC control (Heating, Ventilation, and Air Conditioning), facial recognition for access and boarding, predictive maintenance for ground equipment, and even AI-optimized air traffic flow management [30]. While these innovations yield considerable efficiencies and sustainability benefits, they also create numerous potential points of failure and exploitation. A compromised drone could, for instance, manipulate the camera feeds used in perimeter security, interfere with RFID signals used for baggage tracking, or feed false data into AI systems tasked with queue management, thereby triggering incorrect responses. In the worst-case scenario, a coordinated drone attack could synchronize kinetic distraction (e.g., visual interference or low-altitude loitering) with a cyber intrusion, effectively overwhelming human operators and automated systems [31].

Moreover, the situational ambiguity surrounding many drone incidents complicates the decision-making environment for airport authorities and air traffic controllers. Drones are often difficult to detect using conventional radar due to their small size, low radar cross-section, and non-metallic construction. Acoustic and optical sensors may offer enhanced detection capabilities but are limited by environmental noise and line-of-sight constraints. Additionally, many counter-drone technologies, such as RF jamming or kinetic interception, are legally restricted in civilian contexts or operationally risky within dense passenger areas [11]. As a result, even when drones are identified, response options are constrained, and the default institutional reaction is often to ground flights as a precautionary measure. This reactive posture, while prudent, is inherently unsustainable in the face of increasing drone density and sophistication.

Adding to this complexity is the emerging phenomenon of drone swarms, which poses a qualitatively different threat profile. Swarms may consist of dozens or even hundreds of semi-autonomous drones capable of decentralized coordination and adaptive behavior. Such systems can saturate detection networks, exploit blind spots, and simultaneously mount distributed denial-of-service attacks against both physical and digital targets. The implications for airport security are particularly grave, as current C-UAS systems are primarily designed to neutralize single or low-multiplicity threats, not coordinated mass incursions [32]. Furthermore, as drone software becomes increasingly open-source and modular, the barrier to entry for developing swarm capabilities continues to diminish, raising the specter of asymmetric actors – including organized criminal groups or terrorist cells – employing coordinated aerial campaigns against airport infrastructure.

Beyond swarms, recent threat evolution includes higher levels of autonomy and deception. Low-cost platforms increasingly combine autonomous navigation (pre-programmed routes, terrain following, GPS/INS redundancy) with adaptive behaviors that can complicate attribution and intent assessment. At the same time, adversaries can exploit cyber-physical seams through GNSS spoofing, RF protocol manipulation, or coordinated cyberattacks

targeting airport networks and surveillance feeds. These trends reinforce the need for behavioral classification and risk-informed escalation logic (rather than purely signature-based detection), and they justify AIRI's explicit separation of classification, risk assessment, and intervention selection under human oversight [31,34,42].

Finally, the regulatory landscape surrounding drone use remains fragmented and reactive, especially near critical infrastructure. While the European Union has made significant progress in harmonizing drone regulations, particularly through the EASA framework and the Drone Strategy 2.0, enforcement mechanisms and technological implementation remain uneven across Member States [33]. National variations in airspace classification, remote ID requirements, and C-UAS deployment authorizations create a patchwork environment where both compliant and malicious drone operators may exploit legal ambiguities. This regulatory gap is particularly consequential for airports near national borders or high-density urban regions with limited jurisdictional coordination.

In sum, the threat landscape posed by UAS in the context of smart airports is characterized by multiplicity, ambiguity, and acceleration. The convergence of advanced drone technologies, expanding operational domains, and digital airport infrastructure has produced a security paradigm in which traditional risk-mitigation approaches are increasingly insufficient. Airports must contend with the kinetic risks of mid-air collisions and the strategic vulnerabilities of interconnected systems exposed to surveillance, interference, and cyber-physical exploitation. Addressing this challenge requires fundamentally rethinking defense postures, operational protocols, and technological architectures – shifting from linear, reactive systems to adaptive, AI-driven frameworks that can respond to an evolving, intelligent adversary.

4. DEFENSE-IN-DEPTH STRATEGY: INTEGRATING PHYSICAL, DIGITAL, AND COGNITIVE SECURITY LAYERS

In response to the accelerating threat posed by UAS to the integrity, safety, and continuity of civil aviation operations – especially in the context of digitally augmented, smart airport ecosystems – there is a growing consensus among scholars, regulators, and practitioners that traditional airport security models are no longer sufficient. The increasing frequency, complexity, and unpredictability of drone-related incidents have revealed the inadequacy of perimeter-based, single-layered defense systems that were designed primarily to address human intrusions or conventional criminal threats. This emergent security context demands a paradigmatic shift toward a layered, integrated, and adaptive approach that can dynamically detect, assess, and respond to aerial intrusions across multiple domains of airport operation [34]. The defense-in-depth (DiD) concept, long familiar in military and cybersecurity doctrine, offers a compelling architectural logic for this purpose (Figure 1). By deploying mutually reinforcing layers of defense across the physical, digital, and cognitive spectra, the DiD strategy aims not to guarantee perfect impermeability – an impossible goal in modern threat environments – but rather to create an anticipatory, responsive, and resilient security posture.

At its most basic level, a DiD framework begins with the physical layer, which comprises the sensory and kinetic components designed to detect and, where necessary, physically neutralize intruding drones. In the airport environment, this entails deploying a wide array of sensor types – radars, RF detectors, electro-optical and infrared cameras, acoustic arrays, and LIDAR systems – all positioned to maximize coverage of vulnerable zones such as runway approaches, terminal roofs, perimeters, and airside logistics corridors [22]. These sensors vary in range, resolution, and detection principles. Still, when integrated through sensor fusion

platforms – especially those enhanced by AI – they provide a high-resolution, real-time common operational picture. For instance, while radar systems excel at long-range detection of larger UAS, they often struggle with the low radar cross-sections of commercial drones. Acoustic arrays, conversely, can detect the distinctive harmonic signatures of drone propellers at close range but are vulnerable to environmental noise and directional ambiguity. EO/IR cameras offer visual confirmation but suffer weather-related degradation [11]. It is precisely in this multidimensionality that the DiD approach finds its strength: by aggregating and cross-validating inputs across sensor modalities, false positives can be minimized, detection certainty increased, and the risk of sensor saturation distributed.

Characteristic	Physical Layer	Digital Layer	Cognitive Layer
Focus	Detect and neutralize intruding drones	Address cyber-physical vulnerability	Adaptability, prediction, strategic depth
Methods	Sensors (radar, RF, EO/IR, acoustic, LIDAR)	Intrusion detection, anomaly detection, network analytics	AI models trained on drone behavior
Examples	ASPRID system at Milan Malpensa Airport	EASA AI Roadmap 2.0	AI-based drone intent classifiers
Mitigation	Sensor fusion, cross-validation	Blockchain data authentication	Adaptive learning, shared threat intelligence
Vulnerability	Weather-related degradation	Cyber-enabled disruption	Ethical and regulatory constraints

Fig. 1. Defense-in-Depth Layers for UAS Protection

The operationalization of this multi-sensor architecture has already been demonstrated in modular experimental platforms such as the ASPRID (Airport System Protection against Intruding Drones) system, which was piloted at Milan Malpensa Airport. ASPRID is a multi-layered drone detection and response system integrating radar, EO/IR, and RF-based sensing with a centralized AI-enabled decision-support module [35]. Notably, the system is designed for full interoperability with existing airport security platforms and flight management systems, allowing alerts to be cross-checked with scheduled UAS operations or geofenced airspace corridors. ASPRID's modular design also enables seamless integration of new components as technologies evolve. For instance, detection modules can be recalibrated with updated AI algorithms based on incident feedback. At the same time, mitigation tools, such as RF jammers or net capture drones, can be added or substituted depending on legal and environmental constraints. This adaptability is critical in civilian airport contexts, where legal frameworks may prohibit specific countermeasures, and where the safety of uninvolved passengers and infrastructure must be weighed against the urgency of response [35].

In parallel to physical detection and interception capabilities, the digital layer of the DiD framework addresses the less visible but equally consequential domain of cyber-physical vulnerability. As smart airports increasingly rely on interconnected systems to manage core functions – from baggage routing and biometric boarding to airside fleet management and predictive maintenance – their exposure to cyber-enabled disruption grows proportionally. Drones may act as mobile cyber weapons by deploying signal jammers, intercepting unencrypted Wi-Fi or Bluetooth communications, launching man-in-the-middle attacks, or injecting malicious code into IoT infrastructure [36]. The convergence of these threats with physical incursion risk creates a compounded attack surface, in which the drone serves as both sensor and saboteur. Within the digital layer, mitigation is achieved through AI-enabled intrusion detection systems, anomaly detection engines, and network behavior analytics that can flag irregular access patterns, unauthorized drone command frequencies, or synthetic GPS signals indicative of spoofing attempts [37].

One example of proactive digital security integration is the EASA AI Roadmap 2.0, which outlines a framework for AI trustworthiness, assurance, and lifecycle monitoring in aviation environments. According to the roadmap, AI components in safety-critical applications must undergo continuous validation through human-in-the-loop monitoring, explainable decision-making modules, and secure learning environments [38]. Applying these principles to drone mitigation, an airport's digital DiD layer would include an AI analytics engine that monitors digital infrastructure for anomalies and correlates these with external drone-related sensor feeds. For instance, a sudden loss of signal in a baggage system, coinciding with an unidentified drone hovering over the baggage handling area, would trigger an AI-generated alert flagging a likely coordinated intrusion. EASA's focus on human-centered AI also ensures that such alerts are interpretable and actionable by human operators, thus enhancing autonomous systems' legitimacy and operational coherence within high-stakes environments such as civil aviation hubs.

A further refinement of the digital layer involves implementing blockchain-based data authentication protocols to ensure the integrity of real-time communications among sensors, control towers, and AI analytics platforms. Such measures prevent adversaries from executing spoofing attacks that could manipulate sensor input or alter automated response thresholds. Moreover, digital twins of airport systems – virtual replicas that mirror the operational state of physical infrastructure – can be employed to simulate the impact of drone incursions and test mitigation responses under various threat scenarios [39]. These simulations, powered by real-time data feeds and AI-driven forecast models, allow for preemptive optimization of security protocols before an incident occurs.

While the physical and digital layers provide the structural foundation of the DiD architecture, the cognitive layer, enabled primarily through artificial intelligence, imbues the system with adaptability, predictive capability, and strategic depth. This layer's core is a suite of AI models trained on vast datasets of drone behavior, intrusion incidents, environmental variables, and airport operational patterns. These models, often built using deep learning techniques such as convolutional neural networks, long short-term memory networks, and reinforcement learning agents, can identify not just the presence of a UAS but its probable trajectory, intent, and operational risk level [40].

For instance, if an unidentified drone is detected entering restricted airspace, the cognitive layer does not merely log its presence – it analyzes its speed, altitude, maneuverability, deviation from commercial flight corridors, and proximity to sensitive infrastructure. If the drone's behavior aligns with patterns associated with reconnaissance missions or previous hostile incursions, the AI may assign a higher threat score and trigger a priority response.

The cognitive layer is also designed to function within an ethical and regulatory envelope: mitigation suggestions (e.g., jamming, interception, or passive tracking) are filtered through risk evaluation matrices that account for air traffic density, civilian proximity, and applicable legal constraints [41]. Thus, AI does not replace human decision-makers but augments their judgment with data-rich insights and predictive foresight.

Real-world implementations of cognitive-layer defense capabilities are still emerging, but testbeds such as ASPRID and components developed under the EU Horizon 2020 research framework have demonstrated promising outcomes. In particular, experimental deployments of AI-based drone intent classifiers – systems capable of inferring likely objectives from observed behaviors and context – have demonstrated utility in reducing false alarms and enabling proportionate responses. These classifiers are especially valuable in dense airspace environments where hobbyist drones, delivery UAS, and autonomous inspection drones coexist, and indiscriminate countermeasures could disrupt legitimate operations or lead to regulatory violations [7].

Moreover, the cognitive layer facilitates adaptive learning, enabling AI systems to be continuously retrained using data from past incidents, incident reports, and red-teaming exercises. This dynamic updating process ensures that the DiD framework evolves alongside the threat landscape, maintaining its relevance and efficacy. It also supports the development of shared threat intelligence across airports and aviation authorities through federated learning architectures. AI models trained at different sites can share insights without compromising sensitive data – a critical consideration for transnational aviation operations governed by heterogeneous privacy laws [42].

In its entirety, the defense-in-depth architecture for smart airport UAS protection is not merely a sum of its technical components but a systemic logic for managing uncertainty, complexity, and asymmetry in a rapidly evolving security environment. It recognizes that drones do not operate in isolation but as part of socio-technical systems shaped by global supply chains, evolving legislation, adversarial innovation, and technological convergence. Integrating physical, digital, and cognitive defense layers – each empowered by artificial intelligence and reinforced by modular, interoperable platforms – the DiD framework offers a scalable, ethically grounded, and operationally resilient approach to the next decade's most pressing aviation security challenge.

5. METHODOLOGICAL FRAMEWORK: THE AIRI MODEL (AI-BASED INTRUSION RISK INTERVENTION)

Building on the conceptual foundation established by the defense-in-depth architecture, the AIRI model – AI-based Intrusion Risk Intervention – proposes a structured, scalable methodology for detecting, classifying, and mitigating drone incursions in smart airport environments (Figure 2). Conceived as both an operational and analytical framework, AIRI integrates artificial intelligence at every stage of the UAS threat response cycle: from early detection and behavioral inference to escalation protocols, real-time intervention, and post-event learning. Unlike reactive models that rely on isolated detection technologies or human judgment subject to cognitive fatigue, AIRI is designed to function as a continuous, closed-loop system, linking sensor fusion, predictive analytics, human-in-the-loop oversight, and adaptive post-incident correction into a cohesive cycle of decision-making and action.

The first stage of AIRI is centered on pre-intrusion detection, where the emphasis is on identifying a drone's presence with sufficient lead time to enable downstream interventions. This is achieved through multi-modal sensor integration (e.g., radar, RF detection, acoustic sensors, EO/IR cameras, and, where available, LIDAR). AIRI further assumes AI-assisted sensor fusion, wherein inputs from disparate modalities are aggregated and analyzed using probabilistic models (e.g., Bayesian networks or ensemble classifiers) to reduce uncertainty and improve discrimination between drones, birds, and benign objects [43]. Project evidence such as ASPRID supports the qualitative value of multi-sensor fusion and centralized processing for situational awareness, although performance outcomes are highly context-dependent and must be validated per airport environment [35]. Fusion algorithms also allow AIRI to operate under suboptimal conditions (poor weather, RF interference, or urban clutter) by dynamically recalibrating sensor weights based on environmental context.

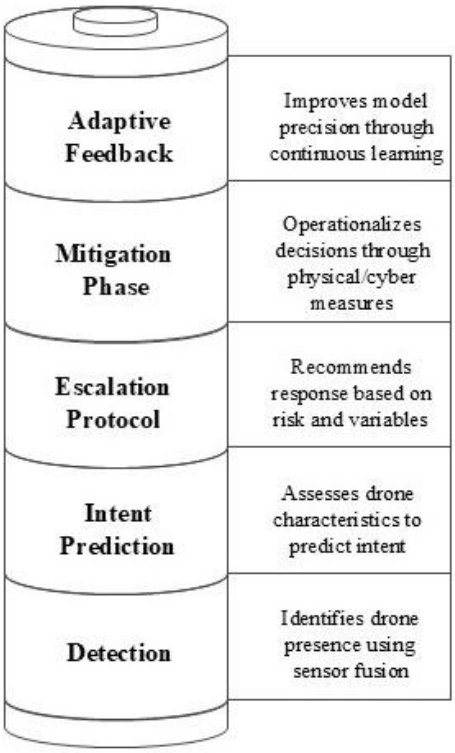

Fig. 2. AIRI Stages

The second stage of the AIRI methodology involves classification and intent prediction, a domain in which AI offers transformative potential. Once a drone is detected, the system must rapidly assess its characteristics – flight pattern, trajectory, speed, altitude, and loitering behavior – and compare them to known profiles stored in a threat behavior library. Using supervised and unsupervised machine learning techniques, including convolutional and recurrent neural networks, the system generates a risk score that estimates the drone's likely function: recreational, commercial, negligent, or hostile [44]. A drone that maintains a steady altitude and trajectory within a known geofenced delivery corridor may be classified as benign, while a UAS exhibiting erratic patterns, hovering near critical infrastructure, or exhibiting command-and-control signal anomalies may be flagged for elevated response. This form of intent inference, still in its infancy, is a growing area of research; projects under the EU's H2020

program and the EASA AI Roadmap emphasize the need for reliable models that can distinguish intent not merely on the basis of origin or proximity, but on nuanced temporal and behavioral patterns [38]. Opposing arguments exist – critics point to the challenge of ensuring accuracy without infringing on operational autonomy or making incorrect assumptions based on incomplete data – but the field is moving toward hybrid models combining machine reasoning with operator validation to offset these risks.

The third stage, escalation protocol and decision-loop execution, activates once a drone is classified as suspicious or hostile. AIRI connects real-time classification data with a pre-defined decision tree encoded in an AI decision support system. The decision tree weighs multiple variables: risk score, proximity to flight operations, current air traffic density, applicable legal restrictions, availability of mitigation tools, and situational awareness inputs from human operators. Based on these variables, AIRI recommends an appropriate response – monitoring, alerting, jamming, physical interception, or coordination with external agencies – and presents these recommendations in an interpretable format to a human-in-the-loop decision-maker [45]. The goal is not to fully automate kinetic response (which remains legally and ethically contentious in most jurisdictions), but to support human authority with rapid, explainable analytics. Such frameworks have already been explored in ICAO's Universal Security Audit Program (USAP-CMA), where risk-informed escalation mechanisms are essential for real-time UAS threat response planning.

Critics of this semi-autonomous escalation logic warn against excessive reliance on algorithmic outputs, particularly when legal responsibility for action (e.g., jamming or intercepting a drone) remains with human actors. There is also concern that AI decision-support systems might be gamed through adversarial tactics, in which a drone mimics benign behavior until the last possible moment to delay the activation of a response. AIRI includes a redundant validation layer to mitigate these vulnerabilities, requiring alerts with a threat score above a specified threshold to be confirmed by at least 2 independent AI classifiers and approved by human control personnel before active mitigation is deployed. This reduces the probability of false escalation while preserving response integrity.

The fourth stage of the AIRI model is the intervention and mitigation phase, where the system operationalizes its decisions through graded operational, physical, or cyber measures. In airport environments, most guidance emphasizes coordination among aerodrome operations, ATC/ANSP, law enforcement, and (where applicable) national security authorities, and it prioritizes safety and legality over rapid neutralization [34]. Accordingly, AIRI treats intervention as a constrained decision problem: response options are selected from pre-approved playbooks (e.g., communication warnings, temporary runway restrictions, security perimeter actions, or controlled escalation to specialist counter-UAS units) and require explicit human authorization for any active mitigation near aircraft or people. This design aligns with airport UAS response planning principles and supports auditable accountability [46].

The final stage of the AIRI cycle is post-event learning and adaptive feedback integration. Regardless of whether escalation occurs, every drone detection event is logged and subjected to retrospective analysis. AI systems extract features from event sensor performance, classification accuracy, decision latency, and false-positive rates, and feed them back into the training datasets. Over time, this continuous learning process improves model precision, updates threat classification profiles, and refines escalation criteria. Moreover, aggregated data from multiple AIRI-equipped airports can be shared (in compliance with privacy regulations) through federated learning protocols, enabling decentralized knowledge accumulation without compromising sensitive data. This feature is significant in transnational EU contexts, where shared learning on emerging threats, such as drone swarms or AI-enabled UAS,

can significantly enhance collective resilience. The Joint Research Centre (JRC) and EUROCONTROL's FLY AI action plan stress the importance of such real-time, evidence-based governance systems for drone risk management across critical infrastructure sectors [47].

Despite its promise, AIRI is not without limitations. First, its successful deployment depends on substantial infrastructure investment in sensor hardware and high-performance computing resources required for real-time AI inference. Second, its operational effectiveness hinges on cross-sector collaboration: airport authorities, air navigation service providers, law enforcement, cybersecurity experts, and AI vendors must work together, often across jurisdictional and organizational boundaries. Finally, AI model validation remains an open challenge. EASA rightly notes that developing certification standards for AI in aviation is still underway, particularly for safety-critical and real-time decision-making systems. Without a shared regulatory standard for AI behavior in counter-UAS applications, there is a risk of inconsistent implementation and uneven stakeholder trust.

Nonetheless, AIRI represents a vital step toward operationalizing artificial intelligence as a core component of airport security in the drone era. It embodies a technical solution and a shift in institutional thinking – from reactive defense to anticipatory risk governance; from human-centric bottlenecks to human-machine synergy; and from isolated interventions to integrated, learning-enabled ecosystems. As smart airports evolve into intelligent infrastructures capable of perceiving, reasoning, and responding in real time, the AIRI model offers a framework that is not only technologically sophisticated but normatively grounded, ethically aware, and strategically aligned with the emerging challenges of 21st-century airspace security.

Although this study is conceptual, a minimal validation is provided to justify the framework's scope and to constrain claims. First, Table 2 maps the AIRI stages to incident-management phases in established airport and critical-infrastructure guidance, demonstrating functional coverage and compatibility. Second, Table 3 illustrates AIRI decision logic in three representative airport scenarios, specifying observable cues, human decision points, and auditable outputs. This validation is not a substitute for field trials; rather, it establishes internal coherence and an evaluation blueprint for future empirical work.

Tab. 2

Cross-walk between AIRI stages and incident-management phases in selected guidance (illustrative mapping)

AIRI stage	EASA DIM (aerodromes) [34]	ICAO infrastructure protection [42]	JRC five-phase [31]	FAA airport UAS guidance [46]	Implementation note (smart airports)
Detect	Detection & reporting triggers	Detection / awareness	Detect	Detection capability & reporting	Multi-sensor fusion; logging of sensor context
Classify	Assessment (identify type/intent)	Assessment	Detect/Respond boundary	Identification & coordination	AI-assisted classification with human review
Assess	Risk evaluation & decision criteria	Risk-based response selection	Respond (decision)	Response planning	Risk score + uncertainty; safety constraints

Intervene	Response actions & coordination	Response / mitigation	Respond	Coordination and authorized mitigation	Playbooks; human authorization; deconfliction with ATC
Learn	Post-incident review	Recovery & improvement	Recover	After-action improvement	Model update governance; SOP refinement; audit trail

Tab. 3

Scenario exercise illustrating AIRI decision logic and human decision points (compact validation)

Scenario (airport context)	Observable cues (multi-sensor)	AIRI classification output	AIRI assessment (risk + uncertainty)	Intervention playbook (examples)	Human decision points / audit artifacts
S1: Recreational drone near final approach	RF signature; EO/IR visual; track crossing approach corridor	Recreational / negligent (low intent confidence)	Medium risk due to proximity; high uncertainty tolerated	Alert ATC + ops; temporary runway restriction; locate operator	Authorize airside measures; log thresholds, comms timeline, and operator ID
S2: Suspicious drone near cargo perimeter at night	Thermal hotspot; low RF; hovering near fence; repeated passes	Suspicious / surveillance (moderate intent confidence)	High risk to perimeter; moderate uncertainty; escalation trigger	Security response; perimeter lockdown; coordinate law enforcement	Authorize escalation; preserve evidence; record rationale and chain-of-custody
S3: Multi-UAS coordinated incursion + cyber anomaly	Multiple tracks; RF diversity; GNSS anomalies; CCTV feed disruptions	Coordinated hostile (high intent confidence)	Very high risk; rapid escalation; require multi-agency coordination	Activate major incident plan; airspace restrictions; specialist C-UAS unit	Incident commander decision; document deconfliction with ATC; post-incident model review

6. REGULATORY, ETHICAL, AND OPERATIONAL CONSIDERATIONS

Implementing artificial intelligence-driven counter-UAS within the complex operational environment of smart airports presents technical and logistical challenges, as well as a constellation of regulatory, ethical, and operational dilemmas. These challenges are particularly salient in contexts where civil aviation intersects with evolving norms of data governance, personal privacy, and the legitimate use of force or coercive technologies in non-military domains. As systems such as the AIRI model gain traction as viable frameworks for threat

mitigation, their deployment cannot occur in a normative vacuum. Instead, they must be embedded within a transparent, harmonized, and forward-looking regulatory ecosystem that balances technological innovation with the foundational principles of civil liberty, proportionality, and public trust [41].

From a regulatory standpoint, deploying AI-enhanced C-UAS systems at airports raises fundamental questions regarding compliance with national airspace sovereignty, international aviation law, and data protection legislation. At the European level, efforts to address these concerns have been spearheaded by institutions such as EASA and the European Commission by adopting the U-Space Regulatory Package, the Drone Strategy 2.0, and most recently, the EASA AI Roadmap 2.0. These documents outline a risk-based, layered governance model for manned and unmanned aviation, stressing the need for trustworthy, human-centric, and certified AI applications in critical airspace management [48]. The AI Roadmap highlights the imperative to align AI functionality with regulatory oversight mechanisms, emphasizing human-in-the-loop control, auditability, traceability, and robustness against adversarial exploitation.

In the European context, AI-enabled counter-UAS components used to support security decisions in safety-critical airport environments may fall within the scope of the EU Artificial Intelligence Act, especially when deployed as part of critical-infrastructure protection or safety-related decision support. This implies documented risk management, data governance, logging, transparency, human oversight, and post-deployment monitoring obligations. Complementarily, EASA's information-security framework (Part-IS) requires organizations to manage information-security risks with potential impact on aviation safety through a structured management system, incident reporting, and continuous improvement. For operationalization, AIRI governance can be aligned with recognized AI and security management frameworks (e.g., NIST AI RMF and ISO/IEC 42001) so that assurance artifacts are auditable and comparable across airports [50,53,55,56].

In practical terms, every decision an AI system makes – especially involving kinetic intervention against a drone or initiating an airport lockdown – must be explainable, reversible, and reviewable. The AIRI model complies with this mandate by incorporating human authorization protocols at every escalation stage, ensuring that AI-generated threat assessments are presented in transparent formats with sufficient contextual metadata for human review. Furthermore, the model incorporates regulatory guardrails through embedded legal rulesets that vary according to national constraints – for instance, automatic disabling of jamming functions in jurisdictions where electronic countermeasures are restricted or prohibited. This modular approach facilitates regulatory interoperability across European airports while maintaining compliance with local laws [39].

At the international level, the International Civil Aviation Organization (ICAO) has also contributed significantly to the normative architecture underpinning C-UAS implementation through Annex 17 of the Chicago Convention, which obligates member states to safeguard civil aviation against acts of unlawful interference and to ensure rapid, proportionate responses to elevated threat levels. Annex 17's emphasis on security risk assessment, stakeholder information sharing, and rapid threat mitigation is operationalized through its Universal Security Audit Programme, which encourages national authorities to establish and regularly update policies on UAS threat response [49]. The AIRI model aligns with this logic by structuring its intervention thresholds around dynamic risk scoring and ensuring interoperability with airport-level incident response plans. Nonetheless, ICAO standards remain general by design and leave significant discretion to national regulators, leading to a patchwork

of implementation practices that could compromise cross-border coordination in the event of transnational UAS threats.

The ethical considerations surrounding AI-enabled counter-UAS systems are complex. Key concerns include potential surveillance overreach, opacity of algorithmic decision-making, and the risk of biased logic in machine-learning classifiers [12]. In airport environments, security analytics that incorporate personal or behavioral data can create disproportionate impacts if not strictly governed. AIRI therefore constrains classification and assessment to operational and aeronautical variables (e.g., trajectory, altitude, velocity, RF signature, geofencing status) and requires explicit data-governance controls, audit logging, and human oversight for any data sources that could be linked to individuals, consistent with EU governance expectations for high-risk AI systems [50].

Another ethical dilemma arises from the possibility of false positives and disproportionate responses. An overzealous AI system that misclassifies a hobby drone as a hostile incursion could trigger costly operational disruptions, erode passenger confidence, or even cause physical harm if kinetic mitigation is misapplied. The principle of proportionality, well established in both EU fundamental rights law and international humanitarian law, requires that security interventions be necessary, targeted, and minimally harmful. This principle is embedded in the AIRI framework through a tiered escalation protocol that restricts kinetic or electromagnetic responses to only those scenarios where all non-invasive measures (e.g., tracking, warning, geofencing override) have been exhausted or deemed ineffective [51]. Additionally, AI decision rationales are logged and reviewed post-incident to ensure accountability and continuous improvement, thus aligning with the ethics of responsibility and transparency advocated by the European Commission's High-Level Expert Group on AI.

Opposing views emphasize the dangers of normalizing automated security apparatuses in civilian contexts, arguing that such systems, once deployed, may become entrenched and expanded beyond their original mandate. Critics fear a gradual erosion of civil liberties under the guise of safety, especially if AI capabilities such as facial recognition or behavioral analytics are integrated without strict safeguards [52]. These concerns are valid and underscore the importance of legislative sunset clauses, independent oversight bodies, and civil society engagement in the deployment of any AI-enabled security infrastructure. Moreover, the governance of such systems should not be left solely to technocrats or private vendors. Still, it should involve participatory mechanisms allowing airport users, labor unions, and local communities to shape the contours of legitimate and proportionate security.

From an operational standpoint, successfully implementing systems like AIRI requires significant coordination across diverse institutional domains. Airport operators, national aviation authorities, air navigation service providers, local police forces, and counter-terrorism units must develop joint standard operating procedures that define roles, responsibilities, escalation thresholds, and post-incident communication protocols. The Joint Research Centre addresses this complexity in its five-phase C-UAS methodology, emphasizing stakeholder alignment across solution design, implementation, and long-term operation. In their 2023 handbook, the JRC emphasizes that a viable C-UAS system must be "less a technology and more a process" – a modular architecture that evolves through institutional learning, technical iteration, and social feedback [31].

Implementing AIRI requires coordination across airport operators, ANSP/ATC, law enforcement, and relevant national authorities. Established guidance for drone incidents at aerodromes emphasizes predefined roles, communication protocols, and joint exercises to ensure that detection alerts translate into timely, proportionate actions without compromising flight safety [34,54]. AIRI complements this guidance by structuring information flows

(classification outputs, risk scores, uncertainty estimates) and by linking them to response playbooks and audit artifacts that can be reviewed during training and after-action processes [46].

Finally, the economic dimension of C-UAS deployment cannot be overlooked. Systems like AIRI require substantial capital expenditure for sensor arrays, computing infrastructure, cybersecurity hardening, and personnel training. For smaller airports with limited traffic volumes, these costs may appear prohibitive. However, the economic costs of a significant drone-related disruption, as seen at Gatwick in 2018 or Dubai International Airport in 2016, can far exceed the investment required for preventive infrastructure. Therefore, public-private partnership models, supported by EU grants under programs such as the Connecting Europe Facility or Horizon Europe, should be explored to ensure financial sustainability and equitable access to high-grade security technologies.

In conclusion, deploying AI-based counter-UAS systems, such as AIRI, in smart airports must be guided by a multifaceted normative architecture. This architecture must harmonize regulatory compliance with operational flexibility, uphold ethical principles while enabling technological innovation, and support institutional coordination without compromising individual rights. If these imperatives are respected, AI can serve not as a threat to civil liberties or human oversight, but as a catalyst for more responsive, transparent, and accountable security in the age of aerial autonomy.

7. CONCLUSION

Smart airports increasingly rely on interconnected cyber-physical systems and automation, which improves efficiency but also introduces new security dependencies. In parallel, UAS activity in the vicinity of aerodromes poses safety and security risks, including airspace disruption, perimeter intrusion, and potential cyber-physical interference.

This paper contributes an AI-enabled defense-in-depth conceptual framework for countering UAS threats in smart airports and introduces the AIRI process model (detect-classify-assess-intervene-learn) as an auditable decision loop integrating multimodal sensing, risk scoring, and human oversight.

The proposed framework aligns with established practices for airport incident management and for countering threats to critical infrastructure. It incorporates recognized incident response steps, outlines clear decision-making criteria, and defines procedures for intervention and assurance that support effective and accountable operations.

The analysis also highlights constraints that shape real-world deployment: heterogeneous national rules on active mitigation, requirements for explainability and accountability, and the need to manage information-security risks and model updates in a safety-critical setting. Accordingly, empirical evaluation and operational trials remain necessary future work; the paper outlines the metrics, data, and governance artifacts required to move from conceptual design to validated capability.

References

1. Gohar Usman, Michael C. Hunter, Agnieszka Marczak-Czajka, Robyn R. Lutz, Myra B. Cohen, Jane Cleland-Huang. 2024. "Towards Engineering Fair and Equitable Software Systems for Managing Low-Altitude Airspace Authorizations". In: *Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Society*, 177-188. Lisbon Portugal: ACM. DOI: https://doi.org/10.1145/3639475.3640103.
2. Sadou Abderrahmane Moubarek, Eric Tchouamou Njoya. 2023. "Applications of Artificial Intelligence in the Air Transport Industry: A Bibliometric and Systematic Literature Review". *Journal of Aerospace Technology and Management* 15: e2223. DOI: https://doi.org/10.1590/jatm.v15.1312.
3. Mayer Michael. 2023. "Trusting machine intelligence: artificial intelligence and human-autonomy teaming in military operations". *Defense and Security Analysis* 39: 521-538. DOI: https://doi.org/10.1080/14751798.2023.2264070.
4. Roshanaei Maryam, Mahir R. Khan, Natalie N. Sylvester. 2024. "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions". *Journal of Information Security* 15: 320-339. DOI: https://doi.org/10.4236/jis.2024.153019.
5. Rashid Adib Bin, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, Mehedy Hassan Bappy. 2023. "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges". Edited by Yu-an Tan. *International Journal of Intelligent Systems* 8676366. DOI: https://doi.org/10.1155/2023/8676366.
6. Gosling, Geoffrey D. 1987. "Identification of artificial intelligence applications in air traffic control". *Transportation Research Part A: General* 21: 27-38. DOI: https://doi.org/10.1016/0191-2607(87)90021-5.
7. Alketbi Mariam Abdalla, Fikri Dweiri, and Doraid Dalalah. 2024. "The Role of Artificial Intelligence in Aviation Construction Projects in the United Arab Emirates: Insights from Construction Professionals". *Applied Sciences* 15: 110. DOI: https://doi.org/10.3390/app15010110.
8. Yigitcanlar Tan, Federico Cugurullo. 2020. "The Sustainability of Artificial Intelligence: An Urbanistic Viewpoint from the Lens of Smart and Sustainable Cities". *Sustainability* 12: 8548. DOI: https://doi.org/10.3390/su12208548.
9. Tychola Kyriaki A., Konstantinos Rantos. 2025. "Cyberthreats and Security Measures in Drone-Assisted Agriculture". *Electronics* 14: 149. DOI: https://doi.org/10.3390/electronics14010149.
10. Mekdad Yassine, Ahmet Aris, Leonardo Babun, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, A. Selcuk Uluagac. 2023. "A survey on security and privacy issues of UAVs". *Computer Networks* 224: 109626. DOI: https://doi.org/10.1016/j.comnet.2023.109626.
11. Jin Hengkang. 2019. "Design of UAV Detection Scheme Based on Passive Acoustic Detection". *IOP Conference Series: Materials Science and Engineering* 563: 042085. DOI: https://doi.org/10.1088/1757-899X/563/4/042085.
12. Mirindi Derrick. 2024. "A Review of the Advances in Artificial Intelligence in Transportation System Development". *Journal of Civil, Construction and Environmental Engineering* 9: 72-83. DOI: https://doi.org/10.11648/j.jccee.20240903.13.

13. Johnson James. 2022. “Delegating strategic decision-making to machines: Dr. Strangelove Redux?” *Journal of Strategic Studies* 45: 439-477. DOI: https://doi.org/10.1080/01402390.2020.1759038.
14. Velasco Cristos. 2022. “Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments”. *ERA Forum* 23: 109-126. DOI: https://doi.org/10.1007/s12027-022-00702-z.
15. Ajaz Aleena, Ayesha Salar, Tauseef Jamal, Asif Ullah Khan. 2022. “Small Object Detection using Deep Learning (version 1)”. *arXiv.* DOI: https://doi.org/10.48550/ARXIV.2201.03243.
16. Roshanaei Maryam, Mahir R. Khan, Natalie N. Sylvester. 2024. “Navigating AI Cybersecurity: Evolving Landscape and Challenges”. *Journal of Intelligent Learning Systems and Applications* 16: 155-174. DOI: https://doi.org/10.4236/jilsa.2024.163010.
17. Goldfarb Avi, Jon R. Lindsay. 2022. “Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War”. *International Security* 46: 7-50. DOI: https://doi.org/10.1162/isec_a_00425.
18. Smart Airports, the digital transformation of airports. 2022. *Nexus Integra EN*.
19. Gürsel Serap, Rafet Demir, Hakan Rodoplu. 2023. “The effect of digitalisation on sustainability and smart airport”. *International Journal of Sustainable Aviation* 9: 26. DOI: https://doi.org/10.1504/IJSA.2023.127488.
20. Dias Clara, Jorge Silva. 2024. “Unveiling the future: Smart airports - applications, advantages, strategies and technological challenges”. *Journal of Airline and Airport Management* 14: 38. DOI: https://doi.org/10.3926/jairm.419.
21. Cho Sung-Hwan, Sang Yong Park. 2023. “Reviewing the Utilization of Smart Airport Security - Case Study of Different Technology Utilization”. *Journal of the Korean Society for Aviation and Aeronautics* 31: 172-177. DOI: https://doi.org/10.12985/ksaa.2023.31.3.172.
22. Huang Hailong, Jinfu Zhu. 2021. “A Short Review of the Application of Machine Learning Methods in Smart Airports”. *Journal of Physics: Conference Series* 1769: 012010. DOI: https://doi.org/10.1088/1742-6596/1769/1/012010.
23. Pyrgies John. 2019. “The UAVs threat to airport security: risk analysis and mitigation”. *Journal of Airline and Airport Management* 9: 63. DOI: https://doi.org/10.3926/jairm.127.
24. Haji Amiri Misagh, Ali Osman Kuşakcı. 2024. “A Scoping Review of Artificial Intelligence Applications in Airports”. *Transactions of Industrial Engineering* 10: 1-12. DOI: https://doi.org/10.61186/crpase.10.2.2900.
25. A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe. 2022. European Commission.
26. Kotkova Barbora. 2022. “Airport defense systems against drones attacks”. In: *2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, 85-90. Crete, Greece: IEEE. DOI: https://doi.org/10.1109/cscc55931.2022.00025.
27. Krlos Vasilis, Martin Larcher. 2023. *Protection Against Unmanned Aircraf Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites.* JRC Technical Report. Luxembourg: Publications Office of the European Union.
28. Lykou Georgia, Dimitrios Moustakas, Dimitris Gritzalis. 2020. “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies”. *Sensors* 20: 3537. DOI: https://doi.org/10.3390/s20123537.

29. Kabashkin Igor, Boriss Misnevs, Olga Zervina. 2023. “Artificial Intelligence in Aviation: New Professionals for New Technologies”. *Applied Sciences* 13: 11660. DOI: https://doi.org/10.3390/app132111660.
30. Rane Nitin, Saurabh Choudhary, Jayesh Rane. 2024. “Artificial intelligence for enhancing resilience”. *Journal of Applied Artificial Intelligence* 5: 1-33. DOI: https://doi.org/10.48185/jaai.v5i2.1053.
31. Hansen Paul, Faria R. Pinto. 2023. *Protection Against Unmanned Aircraft Systems: Handbook on UAS Protection of Critical Infrastructure and Public Space : a Five Phase Approach for C-UAS Stakeholders*. JRC Technical Report. Luxembourg: Publications Office of the European Union.
32. González-Jorge Higinio, Luis Miguel González-deSantos, Enrique Aldao, Gabriel Fontenla-Carrera. 2024. “C-UAS in the Protection of Critical Infrastructures”. In *Applying Drones to Current Societal and Industrial Challenges*, ed. Diego Carou, Antonio Sartal, J. Paulo Davim, 131-153. Management and Industrial Engineering. Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-55571-8_5.
33. Scott Benjamyn I., Konstantinos Andritsos. 2023. “A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe”. *Air and Space Law* 48: 273-296. DOI: https://doi.org/10.54648/AILA2023041.
34. Drone Incident Management at Aerodromes. Part 1: The Challenge of Unauthorised Drones in the Surroundings of Aerodromes. 2021. European Union Aviation Safety Agency.
35. Pascarella D., P. Bieber, M. Cioffi, T. Dubot, M. Ippolito, F.J. Jiménez Roncero, E. Martinavarro Armengol, et al. 2024. “Drone intrusion management systems in airports: assessment of ASPRID solution”. *Journal of Physics: Conference Series* 2716: 012070. DOI: https://doi.org/10.1088/1742-6596/2716/1/012070.
36. Anghuwo John Shivute, Peter Imanuel, Sam Shimakeleni Nangolo. 2024. “Anti-unmanned aerial vehicle detection system for airports: aviation and national security perspective”. *Journal of Transportation Security* 17: 12. DOI: https://doi.org/10.1007/s12198-024-00280-w.
37. Vozella Angela, Francisco Muñoz Sanz, Mario Antonio Solazzo, Edgar Martinavarro Armengol, Pierre Bieber, Giancarlo Ferrara. 2020. “Solution Set-up for Airport Protection from Intruder Drones”. In: *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, 4469-4476. Research Publishing Services. DOI: https://doi.org/10.3850/978-981-14-8593-0_4189-cd.
38. Artificial Intelligence Roadmap 2.0: Human-Centric Approach to AI in Aviation. 2023. European Union Aviation Safety Agency.
39. Tafur Cristian Lozano, Rosa Gabriela Camero, Didier Aldana Rodríguez, Juan Carlos Daza Rincón, Edwin Rativa Saenz. 2025. “Applications of artificial intelligence in air operations: A systematic review”. *Results in Engineering* 25: 103742. DOI: https://doi.org/10.1016/j.rineng.2024.103742.
40. Jiang Yirui, Trung Hieu Tran, Leon Williams. 2023. “Machine learning and mixed reality for smart aviation: Applications and challenges”. *Journal of Air Transport Management* 111: 102437. DOI: https://doi.org/10.1016/j.jairtraman.2023.102437.
41. Kashyap Ramgopal. 2019. “Artificial Intelligence Systems in Aviation”. In: *Advances in Computer and Electrical Engineering*, ed. Tetiana Shmelova, Yuliya Sikirda, Nina Rizun, Dmytro Kucherov, 1-26. IGI Global. DOI: https://doi.org/10.4018/978-1-5225-7588-7.ch001.

42. *Protection of Civil Aviation Infrastructure Against Unmanned Aircraft*. 2023. International Civil Aviation Organization.
43. Kovács Béla, Fanni Vörös, Tímea Vas, Krisztián Károly, Máté Gajdos, Zsófia Varga. 2024. "Safety and Security-Specific Application of Multiple Drone Sensors at Movement Areas of an Aerodrome". *Drones* 8: 231. DOI: https://doi.org/10.3390/drones8060231.
44. Wu Jie, Jiaquan Ye, Jie Zou, Jing Gao, Kaitao Cui. 2023. "Research on the Influence of Drone Countermeasure Equipment on the Surveillance System Used in Civil Aviation". *IEEE Access* 11: 134191-134198. DOI: https://doi.org/10.1109/ACCESS.2023.3337089.
45. Nalin Alessandro, Paolo Tripodi. 2023. "Future Warfare and Responsibility Management in the AI-based Military Decision-making Process". *Journal of Advanced Military Studies* 14: 83-97. DOI: https://doi.org/10.21140/mcuj.20231401003.
46. Federal Aviation Administration (FAA). 2021. CertAlert 21-05: On-Airport Small Unmanned Aircraft Systems (sUAS) and UAS Response Planning (Office of Airports). Available at: https://www.faa.gov/airports/airport_safety/suas.
47. The FLY AI Report Demystifying and Accelerating AI in Aviation/ATM. 2020. European Organisation for the Safety of Air Navigation.
48. Jepsen Jes Hundevadt, Kristian Husum Laursen, Kjeld Jensen. 2024. "A survey of state-of-the-art U-space research". In: *2024 10th International Conference on Automation, Robotics and Applications (ICARA)*, 265-272. Athens, Greece: IEEE. DOI: https://doi.org/10.1109/icara60736.2024.10552989.
49. International Civil Aviation Organization (ICAO). Universal Security Audit Programme – Continuous Monitoring Approach (USAP-CMA): objective and overview. Available at: https://www.icao.int/USAP.
50. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R1689.
51. Chen Yingzi, Zhiqing Li, Longchuan Li, Shugen Ma, Fuchun Zhang, Chao Fan. 2022. "An anti-drone device based on capture technology". *Biomimetic Intelligence and Robotics* 2: 100060. DOI: https://doi.org/10.1016/j.birob.2022.100060.
52. Bieber Pierre, and Thomas Dubot. 2024. "Drone Intrusions in U-Space: Risk Analysis and Modeling of Cyber-Physical Attacks". In: *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, 334-339. Naples, Italy: IEEE. DOI: https://doi.org/10.1109/TechDefense63521.2024.10863471.
53. European Union Aviation Safety Agency (EASA). Easy Access Rules for Information Security (Part-IS). Available at: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-publishes-new-revision-easy-access-rules-information-security.
54. International Air Transport Association (IATA). 2022. Unauthorised Unmanned Aircraft in the Vicinity of Airports: Guidance. Available at: https://www.iata.org/contentassets/fb1df0e634454acc9207418a5d1d636b/unauthorized-ua-guidance-material.pdf.
55. National Institute of Standards and Technology (NIST). 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
56. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 2023. ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system. Available at: https://www.iso.org/standard/81230.html.

57. Cubber De Geert, Daniela Doroftei, Paraskevi Petsioti, Alexios Koniaris, Konrad Brewczyński, Marek Życzkowski, Razvan Roman, Silviu Sima, Ali Mohamoud, Johan van de Pol, Ivan Maza, Anibal Ollero, Christopher Church, Cristina Popa. 2025. "Standardized Evaluation of Counter-Drone Systems: Methods, Technologies, and Performance Metrics". *Drones* 9: 354. DOI: https://doi.org/10.3390/drones9050354.

Received 24.09.2025; accepted in revised form 23.02.2026