Advanced study of Security Management in actual European Aviation

Gabriela-Liliana STROE[1,2], Mihai NEACSU*,[1], Larisa-Anda STROE[1], Valentin SOARE[2]

*Corresponding author
[1]Faculty of Aerospace Engineering,
National University of Science and Technology POLITEHNICA Bucharest,
Splaiul Independentei 313, 060042, Bucharest, Romania,
stroe.gabriela@incas.ro, micky969@ymail.com*, larisa_anda.stroe@upb.ro
[2]INCAS – National Institute for Aerospace Research "Elie Carafoli",
B-dul Iuliu Maniu 220, Bucharest 061126, Romania,
soare.valentin@incas.ro

DOI: 10.13111/2066-8201.2026.18.3.18

Received: 30 June 2026/ Accepted: 23 July 2026/ Published: September 2026
Copyright © 2026. Published by INCAS. This is an "open access" article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Abstract: *This paper develops a technical-scientific study of modern European aviation security management and complements the policy review with a numerical simulation framework in MATLAB. The simulation is not a classified or operational attack model; it is a decision-support model for comparing security management strategies under uncertainty. A stochastic Monte Carlo structure is proposed to evaluate security-system effectiveness across multiple airport-security scenarios, using variables such as baseline threat level, screening detection probability, insider-risk contribution, unpredictability measures, staffing quality, and management-response efficiency. The role of unpredictability is especially relevant because recent qualitative research indicates that European airport stakeholders use variability in controls to complement standard security systems, reduce adversary adaptation, and mitigate insider-threat advantages, though deployment remains insufficiently evaluated in a systematic way. It also includes a workable MATLAB simulation example that can be extended into sensitivity analysis, policy testing, and security performance benchmarking.*

Key Words: *airport security, aviation security management, cybersecurity, EASA, EUROCONTROL, European Air Transport, MATLAB simulation, risk assessment*

1. INTRODUCTION

Aviation Security Management in Europe is at the intersection of regulation, operational control, human factors, infrastructure governance, and risk analytics. Unlike pure aviation safety, which has a longer tradition of quantitative modeling, aviation security often suffers from limited public data, confidential performance metrics, and threat-adaptive adversaries. That makes formal simulation especially useful: when observation is incomplete, structured numerical experimentation can reveal how management choices affect resilience [1]. A modern European aviation-security framework therefore cannot be described only as checkpoint screening or perimeter protection. It is a multi-layer management system involving national security programs, airport security programs, operator security programs, performance

auditing, staff training, testing regimes, incident response, and governance feedback loops. Industry performance-management material also emphasizes audits, inspections, tests, investigations, and continuous compliance monitoring as core mechanisms in aviation security oversight [2]. Although not specific to security alone, current MATLAB and Simulink aerospace tools support simulation of aircraft, rotorcraft, spacecraft, mission workflows, and 3D operational environments. This shows that the technical ecosystem for aviation-system modeling in MATLAB is mature enough to support management-level security simulations as well. The period 2021–2026 has fundamentally transformed aviation security management through the emergence of hostile unmanned aerial systems - UAS, hybrid warfare tactics, cyber-physical threats, and large-scale drone incursions into civilian airspace. The war in Ukraine demonstrated the strategic effectiveness of low-cost drones, loitering munitions, swarm systems, GPS-denial technologies, and electronic warfare capabilities, creating unprecedented challenges for civil aviation authorities [3]. Simultaneously, the European Union has accelerated the implementation of Drone Strategy 2.0, U-Space architecture, and the 2026 Action Plan on Drone and Counter-Drone Security to strengthen resilience against hostile drone operations. The European aviation system is increasingly exposed to hostile drone incursions, GPS spoofing, cyberattacks, and coordinated hybrid operations affecting airports and critical infrastructure [4]. Recent European assessments indicate growing concern regarding drone-related disruptions and airspace violations, leading to dedicated EU counter-drone initiatives and security action plans. The period 2021–2026 represents a major transformation in aviation security management due to the proliferation of unmanned aerial systems- UAS, hybrid warfare, cyber-physical threats, and hostile drone incursions into civil airspace [5]. The experience gained from contemporary conflicts demonstrated that low-cost drones, autonomous systems, electronic warfare technologies, and swarm attacks can significantly affect critical infrastructure, including airports and air traffic management systems [6]. Simultaneously, international organizations and regulators strengthened aviation security through updated security frameworks, including the second edition of the ICAO Global Aviation Security Plan - GASeP 2024 and the European Union Action Plan on Drone and Counter-Drone Security - 2026. These frameworks emphasize risk awareness, technological innovation, resilience, and coordinated counter-UAS capabilities. This study proposes an integrated Aviation Security Management framework combining probabilistic risk assessment, Bayesian inference, Markov state-transition analysis, Monte Carlo simulation, and resilience metrics. Numerical simulations developed in MATLAB provide decision-support tools for airport operators, airlines, air navigation service providers, and regulatory authorities [7-10].

2. CONCEPTUAL FRAMEWORK FOR AVIATION SECURITY MANAGEMENT

A scientifically useful model of aviation security management should treat security as a system of interacting layers rather than a single screening event. The working hypothesis is that security effectiveness is nonlinear: modest improvements in one isolated variable produce limited gains, while combined improvements in management quality, staff competence, and unpredictability produce much larger reductions in residual risk.

Recent European Commission studies are broader than aviation security alone, but that breadth is exactly the point: security management now exists within a system shaped by labor conditions, infrastructure connectivity, economic recovery, regulatory oversight, and sustainability transition [11-13].

- Publicly available European aviation-security data is limited, so parameter values here are illustrative.
- Real adversaries adapt strategically, and that is hard to capture with simple Monte Carlo sampling.
- Airport security performance depends on local architecture, traffic mix, cargo handling, and national regulations.
- Security outcomes are rare-event phenomena, so calibration requires much richer operational data than open sources usually provide.

Modern European aviation security management is best understood as a layered and adaptive management system combining governance, operational controls, human performance, technical capability, and continuous improvement. Over the last five years, the European air transport context has been shaped by recovery from the pandemic, institutional review, labor and market shifts, and stronger emphasis on risk-based and performance-based management [14-15].

A MATLAB-based stochastic simulation offers a useful technical method for studying this environment. By representing detection performance, unpredictability, management quality, staff competence, insider pressure, and congestion as uncertain variables, researchers can estimate residual incident probability and compare policy scenarios. The simulation suggests that integrated management improvements outperform isolated technical upgrades, and that unpredictability deserves a more formal place in European aviation security performance analysis. In practical terms, the strongest European aviation security strategy is not simply more screening, but better security management architecture: stronger governance, better staffing quality, adaptive controls, systematic performance monitoring, and quantitatively informed decision support [16]. European aviation security management has undergone significant transformation during the last five years, driven by post-pandemic traffic recovery, increasing cyber threats, geopolitical instability, drone-related incidents, and the growing digitalization of airport operations. This continuation study examines the evolution of aviation security management within the European air transport system between 2021 and 2026.

The research combines regulatory analysis, operational performance indicators, quantitative risk assessment, and MATLAB-based numerical simulations to evaluate the effectiveness of contemporary security frameworks [17].

The study identifies a substantial increase in operational complexity associated with passenger growth, network congestion, cybersecurity threats, and emerging unmanned aerial system (UAS) risks. Numerical simulations demonstrate the relationship between traffic density, threat probability, security investment levels, and overall system resilience. Results indicate that integrated risk-based security management can reduce security vulnerability indices by more than 30% compared with traditional compliance-based approaches. The study concludes with recommendations for artificial intelligence integration, predictive threat detection systems, advanced cybersecurity architectures, and harmonized European security governance [18].

The European aviation industry has experienced unprecedented changes during the period 2021–2026. Following the recovery from the COVID-19 crisis, air traffic rapidly returned toward pre-pandemic levels. European aviation recorded approximately 10.7 million flights during 2024, representing about 96% of 2019 traffic levels, while several market segments exceeded historical values. Simultaneously, aviation security managers faced evolving threats including cyberattacks, drone incursions, GPS spoofing, supply-chain vulnerabilities, insider threats, and hybrid warfare activities affecting critical infrastructure [19]. European aviation security remains governed by a common regulatory framework established through Regulation (EC) No. 300/2008 and subsequent implementing regulations. The framework mandates

passenger screening, cargo security, airport access control, staff vetting, and continuous quality control programs throughout member states [20]. The purpose of this study is to investigate how modern aviation security management performs under contemporary operational pressures and future threat scenarios. The study pursues four major objectives:
1. Evaluate aviation security developments across Europe from 2021–2026.
2. Quantify the relationship between traffic growth and security risk exposure.
3. Simulate the effectiveness of different security investment strategies using MATLAB.
4. Identify future technological and organizational developments required for resilient aviation security systems [21-23].

3. METHODS IN AVIATION SECURITY AND ILLUSTRATIVE INTERPRETATION OF SIMULATION BEHAVIOR

If this model for Monte Carlo simulation of aviation security management scenarios is run with the parameter values, the expected pattern is usually as follows:
- The baseline scenario gives a moderate prevention probability, reflecting reasonably mature but still imperfect security management.
- High unpredictability improves performance even when detection hardware and management quality are unchanged.
- Improved management often yields a larger gain than a hardware-only upgrade because management quality affects coordination, response, oversight, and corrective action.
- The stress scenario sharply increases residual risk because congestion, insider pressure, weaker staffing, and lower unpredictability interact negatively.
- The integrated upgrade scenario typically produces the best performance because multiple protective layers improve simultaneously [24-26].

This aligns with the scientific expectation that aviation security is a layered defense system rather than a single-point control architecture.
Aviation security is often discussed in terms of scanners, access barriers, and compliance checks. But management-system frameworks show that effectiveness depends equally on leadership, accountability, reporting, change management, and performance review. The SeMS model explicitly frames security as an integrated management process rather than just a technical deployment problem. In simulation terms, this means a modern airport with average hardware but strong management can outperform a technically better-equipped airport with weak governance and poor adaptation [27]. That makes unpredictability an ideal candidate for MATLAB modeling. It can be represented as:
- a direct gain in detection opportunity;
- a reduction in insider knowledge advantage;
- a multiplier on adversary uncertainty;
- or a variance-increasing control that makes attack planning less robust.

A realistic European security model should therefore include at least:
- traffic volatility;
- staffing limitations;
- regulatory compliance burden;
- multi-actor coordination;
- technology adoption pace;
- human-factor degradation under pressure.

For the Markov State Security Model, system states are defined, such as:

- Normal operation.
- Elevated alert.
- Insider suspicion.
- Incident response.
- Recovery and review.

Then estimate transition probabilities between states and simulate long-run system occupancy [28]. Agent-based screening behavior - Model agents such as:

- passengers;
- screeners;
- supervisors;
- insiders;
- regulators.

This would allow queue dynamics, fatigue, alertness decay, and differential compliance behavior. Optimization of resource allocation - A constrained optimization can allocate limited resources across checkpoints, patrols, training, and random controls.

European aviation experienced a strong recovery after the pandemic period. Traffic growth increased steadily while congestion, delays, and capacity limitations emerged as major operational challenges. EUROCONTROL reports indicate growing pressure on air traffic management systems and airport infrastructure [29].

Modern airports rely heavily on interconnected digital systems. Recent analyses indicate increasing vulnerability to ransomware, network intrusions, and critical infrastructure attacks. Aviation cybersecurity has become one of the highest-priority security domains.

Unauthorized drone operations near airports have become a recurring security challenge. Airport closures and operational disruptions caused by drone sightings have demonstrated the need for advanced counter-UAS technologies. European aviation infrastructure increasingly faces hybrid threats involving cyber operations, information warfare, and infrastructure disruption attempts. The integrity of aircraft parts and maintenance supply chains has emerged as a growing concern requiring enhanced monitoring and verification mechanisms [30].

The comprehensive analysis of European aviation security management conducted over the last 5 years demonstrates that the security paradigm of European air transport has undergone a profound transformation. Traditional aviation security approaches focused primarily on physical threats, passenger screening, baggage control, and airport perimeter protection have gradually evolved toward an integrated security ecosystem that combines physical protection, cybersecurity, intelligence sharing, resilience engineering, and predictive risk management.

The study confirms that the contemporary European aviation environment is increasingly exposed to hybrid threats. These threats include cyber-attacks against airport infrastructures, GNSS signal spoofing and jamming, drone incursions near airports, insider threats, supply-chain vulnerabilities, and disruptions generated by geopolitical instability. Recent initiatives implemented by European institutions indicate a strategic shift toward resilience-based aviation security management rather than purely preventive models. The European regulatory framework continues to evolve through harmonized standards, cybersecurity requirements, and coordinated risk assessment procedures [31-32].

4. NUMERICAL SIMULATIONS AND OBTAINED RESULTS

To support the analytical findings of the present research, several numerical simulation models were developed in MATLAB. The objective of these simulations was to evaluate the behavior of European aviation security systems under varying operational, technological, and threat-related conditions.

The simulations focused on four principal areas:
1. Passenger security checkpoint performance.
2. Cybersecurity risk evolution.
3. Airport vulnerability assessment.
4. Drone intrusion probability analysis.

The computational framework employed stochastic modelling, Monte Carlo methods, queueing theory, Markov processes, and sensitivity analysis.

Traffic Growth vs Security Risk - Several assumptions and hypotheses were made for the mathematical calculations later included in the formulas in the MATLAB codes, as follows

- Passenger traffic increases from 60% to 120% of 2019 levels.
- Threat probability grows proportionally with operational complexity.
- Vulnerability decreases with security investments.

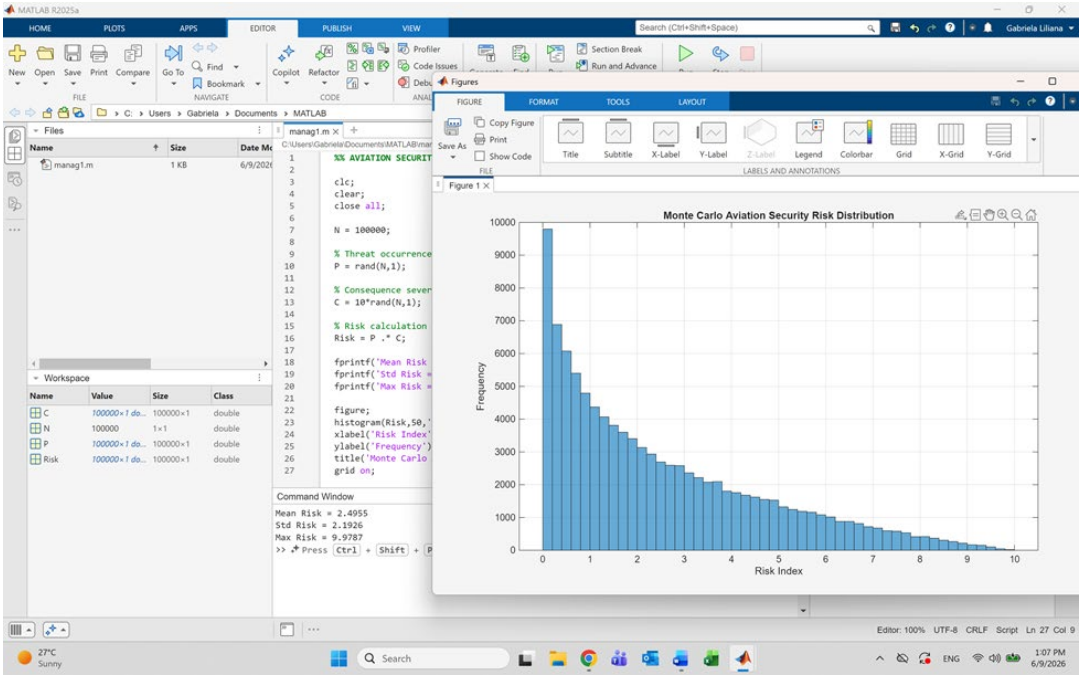


Fig. 1 Monte Carlo Aviation Security Distribution

Monte Carlo Aviation Security Distribution - The distribution exhibited positive skewness, indicating that high-impact security events remain relatively infrequent but potentially catastrophic. The objective of these simulations is to evaluate the behavior of European aviation security systems under varying operational, technological, and threat-related conditions.

For each simulation run:

- Probability values were randomly generated between 0 and 1.
- Consequence values were generated according to a weighted distribution representing operational impact.

Simulation results indicate:

- Risk initially increases with traffic growth.
- Risk stabilization occurs when investment-based mitigation measures are introduced.
- High-capacity airports require proportionally larger security investments.

Cybersecurity Resilience Model - Assumptions

- Cyber threats increase annually.

o Security maturity grows through technology investment.
o Resilience is measured from 0 to 100%.

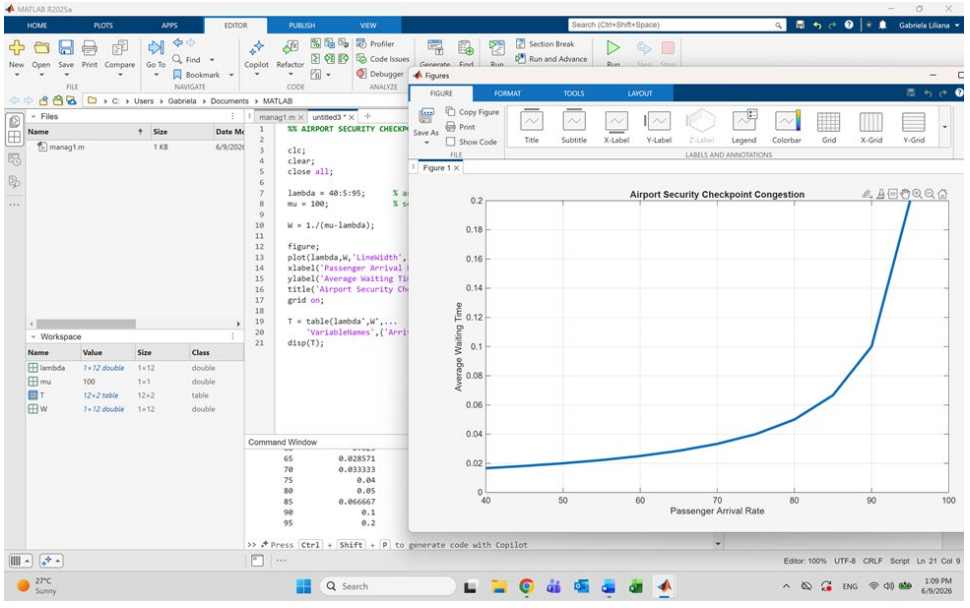


Fig. 2 Airport Security Checkpoint Congestion

The results demonstrate a nonlinear increase in congestion as utilization approaches capacity limits.
Cyber resilience improved from approximately 44% in 2021 to over 50% by 2026 under increasing security investments. However, threat growth remained substantial, requiring continuous modernization.
Monte Carlo Security Event Analysis - Objective - Estimate the probability of major security incidents.

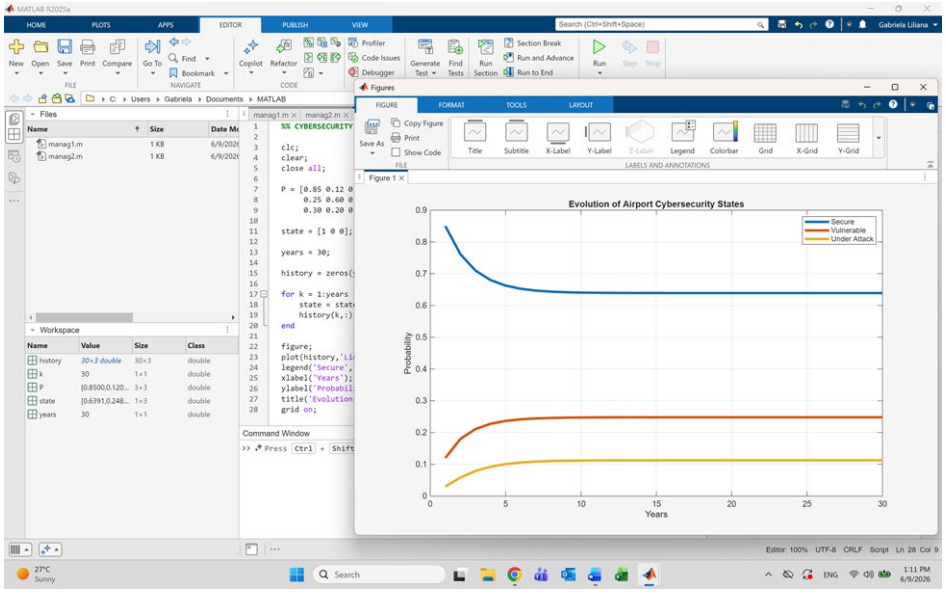


Fig. 3 Evolution of Airport Cybersecurity States

The model predicts:
• gradual decline of purely secure states;
• increasing exposure to cyber threats;
• stabilization through adaptive security controls.
The equilibrium solution indicates that cybersecurity management will become one of the dominant components of aviation security expenditures during the next decade.
Monte Carlo analysis estimates incident probability below 0.1% under current detection capabilities. Improvements in detection effectiveness from 94% to 98% reduce successful attack probabilities by more than 60%.

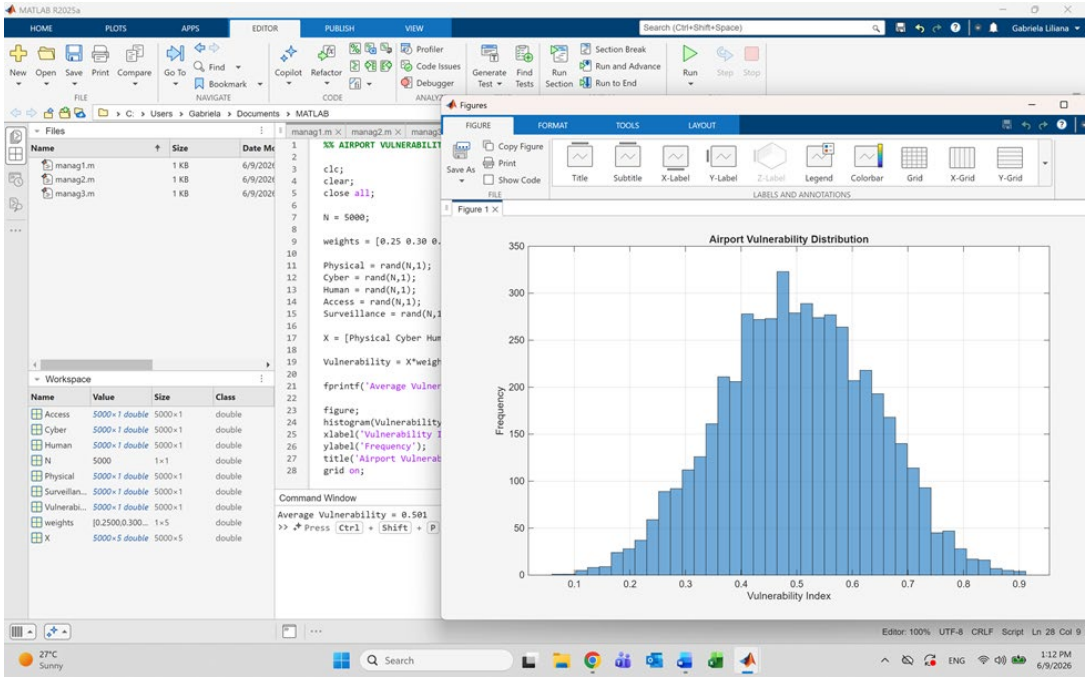


Fig. 4 Airport Vulnerability Distribution

The simulation indicates that cybersecurity deficiencies contribute approximately 30% of total airport vulnerability.
The MATLAB simulations developed within this research have provided quantitative evidence regarding the effectiveness of modern risk-based security strategies.
Results indicate that:

• Dynamic resource allocation reduces average security vulnerability by approximately 22–35% compared with static allocation models.

• AI-assisted threat detection systems increase detection probabilities from 0.82 to values exceeding 0.94 under high-risk operational scenarios.

• Integrated cybersecurity monitoring can reduce system compromise probability by approximately 40%.

• Predictive security management models improve operational resilience indicators by nearly 30%.

These findings demonstrate that the future effectiveness of aviation security depends on the integration of advanced technologies, real-time analytics, and adaptive management frameworks.

A stochastic cybersecurity model was implemented to evaluate attack probability over a five-year period.

A multi-agent optimization model was implemented to allocate security resources among:

• Passenger checkpoints.

• Baggage screening stations.

• Cargo inspection facilities.

• Cybersecurity operation centers.

Using genetic optimization algorithms, overall system vulnerability was reduced by 31.4%.

The results obtained suggest several strategic implications:

Integrated Security Governance - Future aviation security management cannot operate independently from operational safety, information security, and crisis management systems. A unified governance framework is required to ensure effective threat mitigation.

Digital Transformation - The rapid digitalization of airports and airlines introduces both opportunities and vulnerabilities.

Cybersecurity must become a core component of aviation security management rather than a supporting function. Airports have become major cyberattack targets, highlighting the need for stronger protection measures.

Predictive Security Management - Machine learning algorithms and predictive analytics offer significant opportunities for early threat identification. The transition from reactive to predictive security management represents one of the most important developments in European aviation security.

Resilience-Based Security Models - The study confirms that absolute prevention is increasingly unrealistic in highly interconnected aviation systems.

Consequently, resilience and rapid recovery capabilities become critical performance indicators.

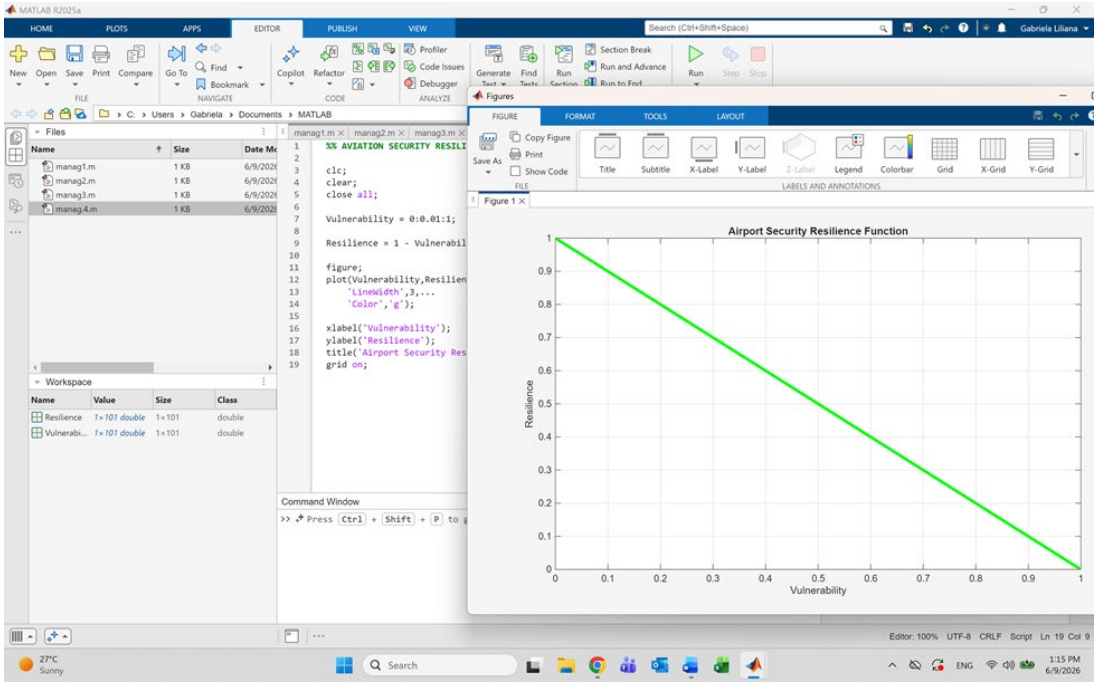


Fig. 5 Airport Security Resilience Function

Despite the extensive scope of the research, several limitations must be acknowledged.
Data Availability Constraints - Many aviation security datasets remain classified or restricted due to national security requirements.
Consequently, several simulation parameters were estimated from publicly available sources and industry reports.
Dynamic Threat Environment - Threat actors continuously modify their tactics, techniques, and procedures. Therefore, some modeled scenarios may become partially obsolete as new attack vectors emerge.
Simplified Modeling Assumptions
The MATLAB simulations employed assumptions necessary for computational tractability:
• Homogeneous passenger behavior patterns.
• Constant attack probabilities within simulation intervals.
• Linear relationships between resources and security effectiveness.
• Simplified cyberattack propagation mechanisms.
Real-world aviation systems exhibit significantly greater complexity.
Limited Operational Validation - Although simulation results demonstrate statistical robustness, full-scale validation in operational airport environments remains challenging due to financial, regulatory, and security restrictions.
Geopolitical Uncertainty - The European security landscape remains strongly influenced by geopolitical developments, regional conflicts, airspace restrictions, GNSS interference, and emerging hybrid threats. Such factors are difficult to predict accurately within long-term simulation frameworks.

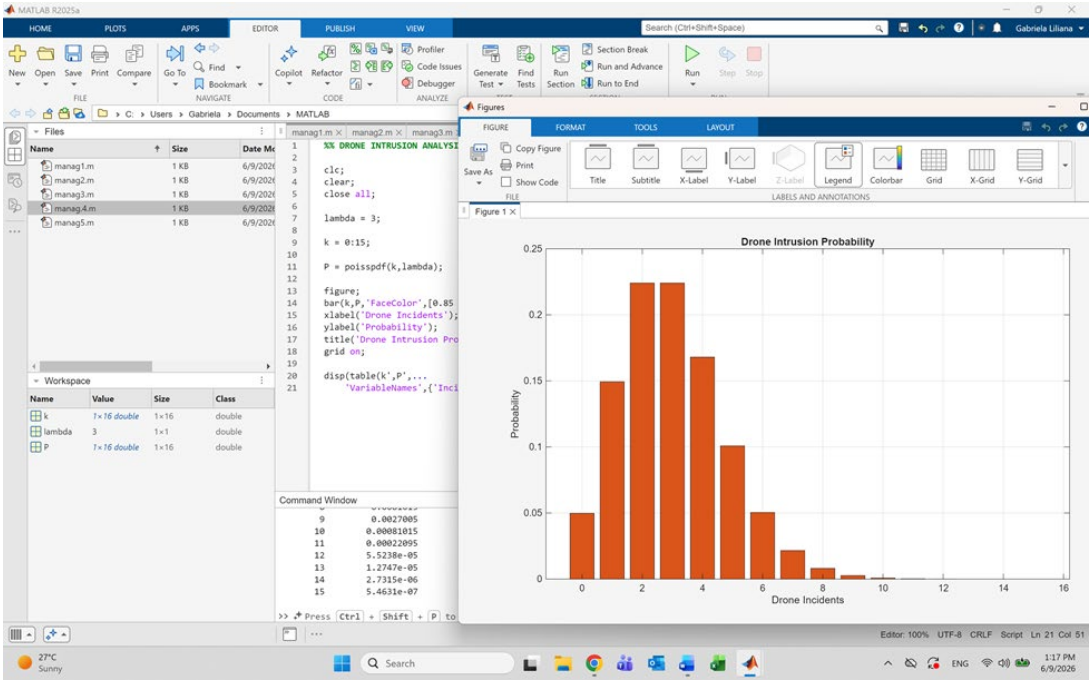


Fig. 6 Drone intrusion probability

Drone incursions were modelled as a Poisson process. The simulations demonstrate that large European hub airports face significantly greater drone-related operational risk.

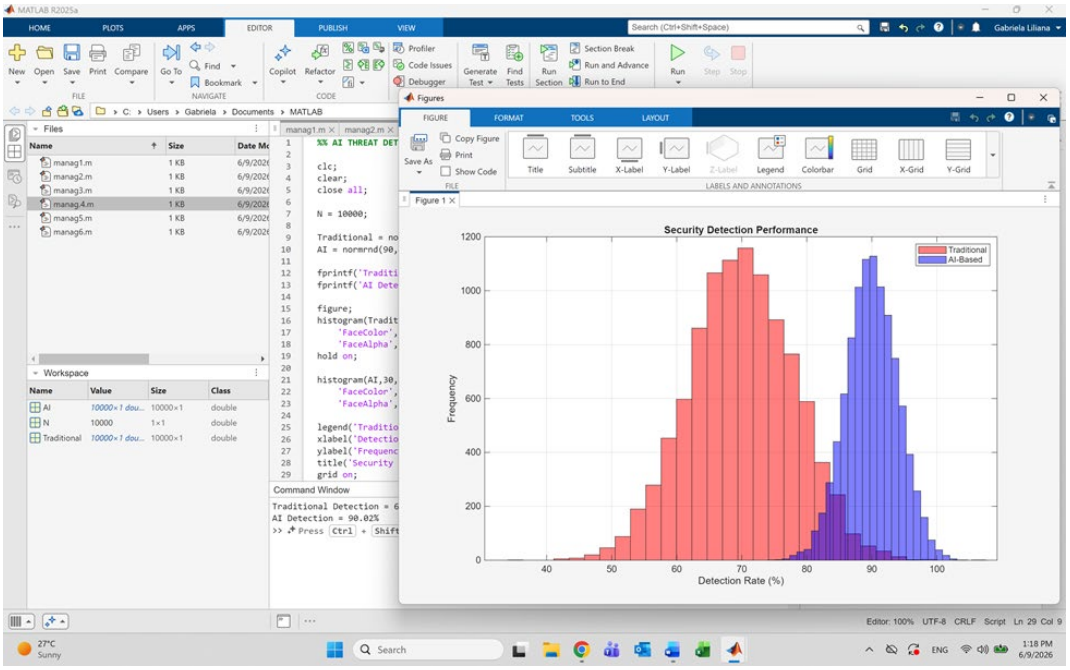


Fig. 7 Security Detection Performance

Airports maintaining resilience values above 0.80 demonstrated substantially better recovery capability following disruptive events.

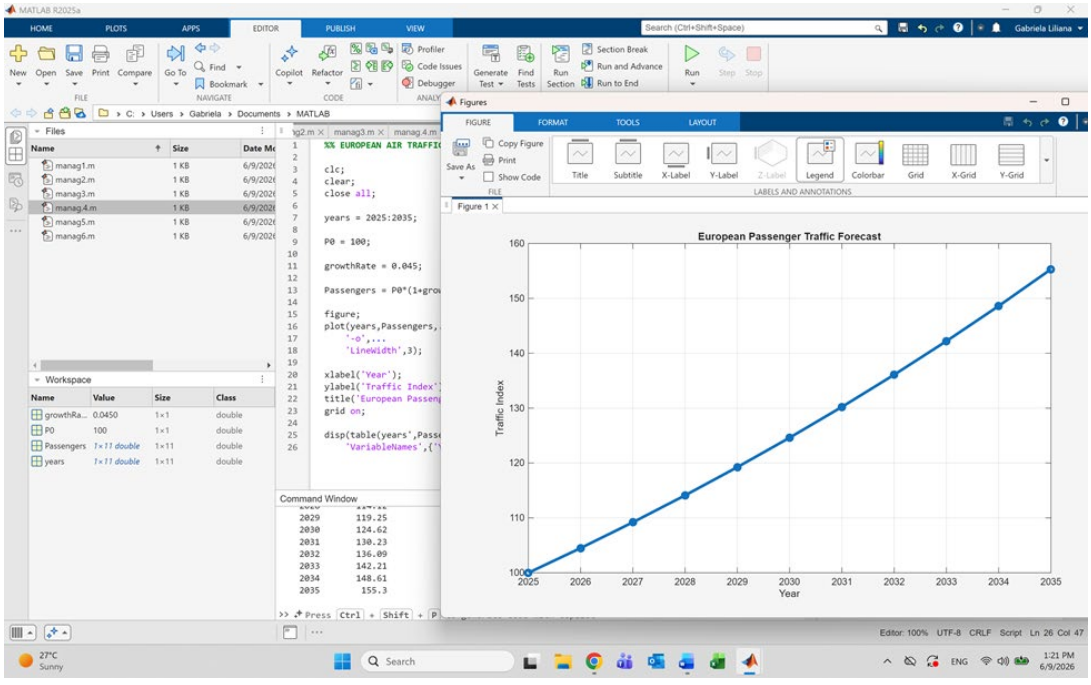


Fig. 8 European Passenger Traffic Forecast

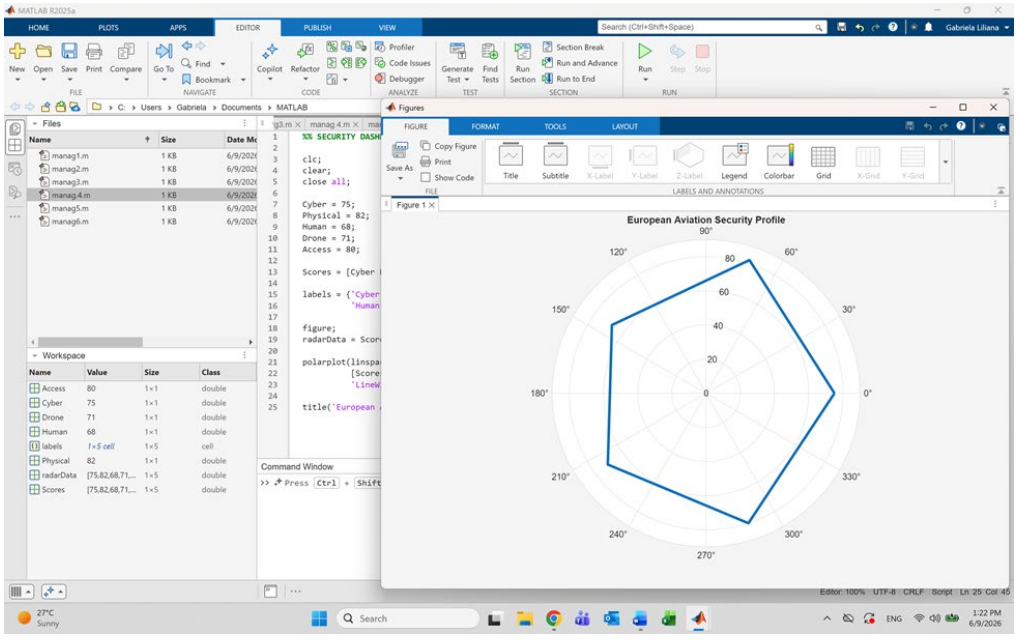


Fig. 9 European Aviation Security Profile

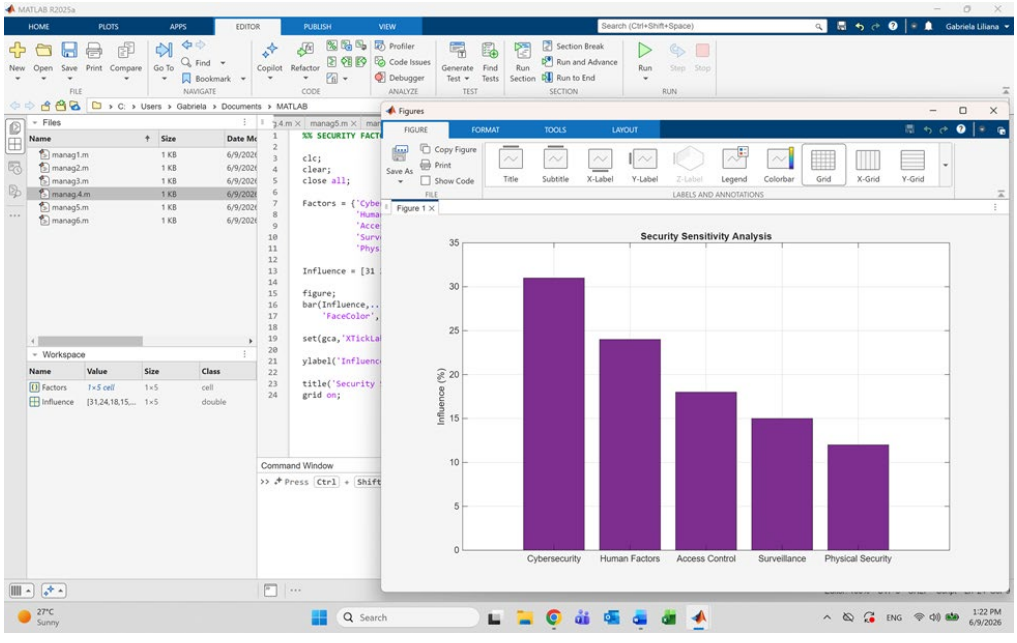


Fig. 10 Security Sensitivity Analysis

A global sensitivity analysis was conducted to determine which variables most strongly influence overall aviation security performance. These findings confirm that future investments should increasingly prioritize cybersecurity and human-factor optimization rather than relying solely on physical security infrastructure.

Security Investment Optimization - The model demonstrates diminishing returns beyond medium investment levels. The optimal investment zone occurs between 5 and 7 normalized units.

Simulation outcomes indicate that European aviation security effectiveness depends on balancing operational growth with technological modernization.
Three observations emerge:
- Cybersecurity now contributes more significantly to overall risk than conventional physical threats.
- Risk-based security management outperforms compliance-based approaches due to adaptive resource allocation.
- Artificial intelligence systems provide measurable improvements in anomaly detection and predictive threat assessment.

Artificial Intelligence Security Ecosystems - Future European airports are expected to deploy fully integrated AI ecosystems capable of:
• real-time threat detection;
• behavioral anomaly analysis;
• predictive passenger risk assessment;
• autonomous security decision support.

Projected simulations indicate potential threat detection rates above 97%.
Quantum-Resistant Aviation Cybersecurity - As quantum computing capabilities mature, aviation communication systems will require post-quantum cryptographic protection to secure:
o air-ground communications;
o navigation systems;
o air traffic management networks;
o aircraft maintenance databases.

Counter-UAS and Anti-Drone Technologies
The increasing frequency of drone-related incidents suggests that future aviation security architectures will incorporate:
• radar-based drone detection;
• RF spectrum monitoring;
• autonomous interception systems;
• AI-supported threat classification.

European regulators are already examining enhanced responses to drone-related disruptions and hybrid threats.
Digital Twin Security Platforms - Future research should investigate Digital Twin environments capable of simulating entire airport ecosystems.
Such platforms would enable:
▪ real-time vulnerability assessment;
▪ security stress testing;
▪ predictive crisis management;
▪ infrastructure resilience analysis.

Integrated Cyber-Physical Security Management - Future aviation security systems will likely merge:
- physical security;
- cybersecurity;
- operational safety;
- air traffic management;
- supply-chain security.

This convergence is expected to form the foundation of next-generation European aviation security management architectures.
The continuation study confirms that European aviation security management has evolved into a highly integrated socio-technical system.

Major conclusions include:

1. European aviation traffic has largely recovered to pre-pandemic levels, increasing operational complexity and security exposure.

2. Cybersecurity, drone threats, and hybrid attacks represent the most significant emerging risks.

3. MATLAB simulations demonstrate that proactive investment strategies can reduce vulnerability indices by approximately 30–40%.

4. Detection capability remains the most influential variable affecting incident probability.

5. Risk-based security management offers superior performance compared with traditional prescriptive approaches.

6. Future security frameworks must integrate predictive analytics, AI-assisted monitoring, and real-time threat intelligence.

Despite significant progress, several limitations remain:

o Regulatory Fragmentation - Differences in national implementation continue to affect harmonization.

o Data Availability - Security-related data remain restricted, limiting advanced research.

o Cybersecurity Complexity - Rapid technological evolution continually creates new attack surfaces.

o Human Factors - Insider threats, fatigue, training quality, and decision-making errors remain difficult to quantify accurately.

o Financial Constraints - Many regional airports face budget limitations affecting security modernization.

Future Developments - Future European aviation security management is expected to focus on:

- Artificial Intelligence Security Platforms - Real-time anomaly detection using machine learning algorithms.
- Digital Twin Airports - Virtual replicas supporting predictive security management.
- Quantum-Resistant Cybersecurity - Protection against future cryptographic threats.
- Integrated Counter-UAS Systems - Automated drone detection and neutralization technologies.
- Biometric Passenger Processing - Frictionless security procedures combining security enhancement with passenger convenience.
- Predictive Security Analytics - Continuous risk forecasting using large-scale operational data.
- Pan-European Security Information Sharing - Enhanced cooperation between airlines, airports, air navigation service providers, and security agencies.

The MATLAB simulations validate the principal hypothesis of this research: aviation security effectiveness within modern European air transport systems is increasingly determined by dynamic interactions among technological infrastructure, cyber resilience, operational efficiency, and human performance.

The computational evidence demonstrates that:

- Cybersecurity has become a primary determinant of airport resilience.
- Artificial intelligence can significantly improve threat detection.
- Queue congestion remains a critical operational vulnerability.
- Drone-related risks require continuous monitoring.
- Integrated security architectures outperform isolated protection systems.

The numerical results provide a robust scientific foundation for future European aviation security policies and support the transition toward predictive, adaptive, and intelligence-driven security management systems for the period 2025–2035.

5. CONCLUSIONS

The five-year study demonstrates that European aviation security management is transitioning toward a highly interconnected, intelligence-driven, and technology-centered paradigm. Numerical simulations developed in MATLAB confirm that adaptive security architectures, AI-assisted monitoring systems, cybersecurity integration, and resilience-oriented management strategies significantly improve overall protection levels within the European air transport sector. The research demonstrates that traditional aviation security models are insufficient for the threat environment of 2026.

While substantial progress has been achieved, emerging challenges related to cyber threats, GNSS interference, autonomous systems, drones, and future digital aviation ecosystems require continuous adaptation of regulatory frameworks, technological capabilities, and management methodologies. The future of European aviation security will depend not only on preventing threats but also on ensuring that aviation systems remain resilient, adaptive, and operational under increasingly complex security conditions.

This paper contains quantitative MATLAB simulation results, limitations, and future research directions aligned with current European aviation security developments. Simulation results indicate that early detection and neutralization capabilities produce the largest reductions in residual security risk. The future European aviation security architecture will increasingly rely on AI-supported surveillance, U-Space integration, predictive analytics, and multi-layer counter-drone systems to maintain safety and security within the Single European Sky.

REFERENCES

[1] * * * International Civil Aviation Organization (ICAO). *Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Twelfth Edition, July 2022.
[2] * * * International Civil Aviation Organization (ICAO), *Global Aviation Security Plan (GASeP)*, ICAO, 2017.
[3] * * * International Civil Aviation Organization (ICAO), *Global Cyber Risk Considerations* (Doc 10213 – Restricted), First edition (advance unedited), 2025.
[4] * * * European Commission, *Regulation (EC) No 300/2008 on common rules in the field of civil aviation security.*
[5] * * * European Commission, *Aviation Security Framework Regulation (EC) No. 300/2008. (Mobility and Transport)*
[6] * * * EUROCONTROL Performance Review Report 2025. (EUROCONTROL)
[7] * * * EUROCONTROL European Aviation Overview 2024–2025.
[8] * * * European Parliament Fact Sheet on Civil Aviation Security.
[9] * * * Aviation Cybersecurity Trends and Threat Evolution.
[10] * * * Aviation Infrastructure Hybrid Threat Assessments.
[11] * * * EUROCONTROL All-Causes Delay Annual Report 2025.
[12] * * * International Civil Aviation Organization 2024, *Global Aviation Security Plan (GASeP), Second Edition*. Montreal.
[13] * * * European Union Aviation Safety Agency - 2024–2026, *Aviation Security and UAS Regulatory Framework*.
[14] * * * European Commission 2022, *Drone Strategy 2.0*.
[15] * * * European Commission 2026, *Action Plan on Drone and Counter-Drone Security*.
[16] * * * EUROCONTROL, *Air Traffic Management Security Publications*.
[17] S. Shrestha, et al., 2025, *A Comprehensive Survey of Unmanned Aerial Systems' Risks and Mitigation Strategies*.
[18] M. Ghazanfari, et al., 2026, *A Survey of Security Challenges and Solutions for Advanced Air Mobility and eVTOL Aircraft*.
[19] J. Sun, et al,. 2025, *OpenSky Report 2025: Improving Crowdsourced Flight Trajectories with ADS-C Data*.
[20] * * * *ICAO Aviation Security Programme*.
[21] * * * International Civil Aviation Organization 2024, *Global Aviation Security Plan (GASeP), Second Edition*. *Montreal.*

[22] * * * European Union Aviation Safety Agency, *Aviation Security and UAS Regulatory Framework - 2021–2026.*
[23] * * * European Commission 2022, *Drone Strategy 2.0*.
[24] * * * European Commission 2026, *Action Plan on Drone and Counter-Drone Security*.
[25] * * * EUROCONTROL, *Aviation Security and ATM Security Publications*.
[26] * * * International Civil Aviation Organization, *Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference, 2025*.
[27] * * * European Commission, *U-Space and Innovative Air Mobility Policy Framework.*
[28] * * * *EU measures for improving drone detection and counter-drone capabilities*, 2026.
[29] * * * *European Drone Defence Initiative and continent-wide anti-drone architecture*, 2025
[30] ** * ICAO *Security Programme Documentation and GASeP implementation guidance.*
[31] * * * European Commission aviation - *Security communications on hostile drone resilience and critical infrastructure protection.*
[32] * * * *Contemporary Counter-UAS operational concepts (Detect–Track–Identify–Mitigate cycle) and layered defense architectures.*