International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 09 | Sep 2025 www.irjet.net p-ISSN: 2395-0072

Designing Safer Skies: Evaluating UAV and ATC System Interactions through Simulation and Qualitative Analysis

Andrew Renault[1]

[1] *Grad Student, Dept. of Aeronautical Science, Capital Technology University, South Laurel, Maryland, USA*

Abstract - *This study investigates the urgent need to modernize air traffic control (ATC) systems to ensure the safe and effective integration of unmanned aerial vehicles (UAVs) into controlled airspace. As UAV proliferation accelerates globally, current ATC infrastructure remains poorly equipped to address emerging safety threats, including mid-air collisions, airspace violations, cyber intrusions, and the weaponization of UAVs for malicious purposes. To address these challenges, a mixed-methods approach was employed, combining quantitative simulations and qualitative document analysis to generate comprehensive, actionable insights. The quantitative component utilizes a structured Design of Experiments (DOE) framework to simulate four critical operational configurations: UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance. Each configuration was modeled across multiple factors and levels, generating empirical performance indicators such as detection accuracy, safety scores, and cyber resilience indices. Statistical analysis, including analysis of variance (ANOVA), identified significant main effects and interaction patterns that influence system performance and reliability. To complement the simulation findings, a qualitative analysis was conducted on a carefully curated set of 60 scholarly and technical documents, selected from a broader pool of over 300 peer-reviewed sources. These documents were analyzed to extract operational themes, validate model assumptions, and identify regulatory or deployment constraints. The convergence and divergence between simulated and documented insights highlight critical areas requiring further empirical validation and inform the prioritization of modernization strategies. This integrative research demonstrates that AI-enabled surveillance, robust cybersecurity safeguards, and multistatic radar configurations significantly enhance UAV detection and response capabilities. Findings underscore the necessity of adopting a systems-level approach to UAV integration that balances technological innovation with safety, regulatory foresight, and national security concerns.*

Key Words: UAV, UAV integration, ATC, drones, air traffic control, AI in aviation, radar limitations, cybersecurity, human factors, regulatory frameworks, multi-sensor fusion

1.0 INTRODUCTION

The modernization of air traffic control (ATC) systems has become an urgent priority as global airspace faces unprecedented challenges from the rapid proliferation of unmanned aerial vehicles (UAVs), increasing aerial congestion, and the growing complexity of cybersecurity threats. Legacy ATC systems—largely designed for manned aviation—struggle to maintain situational awareness, enforce separation standards, and ensure security in an environment that now includes autonomous, low-altitude, and non-cooperative UAVs. Foundational studies have highlighted these issues as key operational stressors that demand immediate intervention [1]. In addition to traffic volume and surveillance limitations, the rising weaponization of UAVs presents national security concerns, including the risk of terrorism, illicit airspace incursions, and payload delivery in restricted zones. Furthermore, the documented rise in near mid-air collisions involving UAVs has increased safety risks to both civilian and commercial aviation. A comprehensive literature review examined over 300 published documents, from which 60 were selected to support this study's qualitative dimension. These sources collectively outline the technical, policy, and regulatory barriers to UAV-ATC integration and reinforce the urgency for transformative change [2].

Figure 1: UAV Operational Impacts to ATC [2]

To address these multifaceted challenges, this paper adopts a mixed-methods approach that combines quantitative simulation with qualitative document analysis.

At the core of the quantitative strategy is a factorial Design of Experiments (DOE) framework that models four critical UAV-ATC configurations: UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance. Each DOE configuration includes multiple independent factors and levels designed to replicate operational behaviors and generate empirical metrics such as detection accuracy, safety scores, and system resilience indices. Statistical analyses, including analysis of variance (ANOVA), are applied to detect significant trends, main effects, and interaction outcomes [3]–[62]. Complementing this is a qualitative document analysis of 60 scholarly and technical sources categorized by configuration. These documents provide operational context, expose latent policy gaps, and validate or challenge model assumptions, allowing for a robust triangulation of findings. The hybrid methodology strengthens the internal validity of simulation outcomes and ensures that findings are not only statistically sound but operationally informed.

Simulated environments were constructed using parameters grounded in field literature and real-world system characteristics, such as telemetry encryption failure rates, spoofing susceptibilities, radar cross-section profiles, and detection thresholds [2], [4]–[17]. These constructs offer a testbed for emulating UAV-ATC interaction scenarios and assessing system response under varying conditions. The remainder of this paper presents the research design, simulation methodologies, qualitative synthesis, and resulting implications for ATC modernization. Collectively, these findings are intended to inform policymakers, engineers, and aviation stakeholders of the urgent need for empirically grounded reforms to safely integrate UAVs into national and global airspace systems.

1.1 Problem Statement

Contemporary ATC systems face mounting challenges in managing the complex operational demands introduced by the rapid proliferation of unmanned aerial vehicles (UAVs). These systems were originally designed for traditional manned aviation and are ill-equipped to detect, track, and manage UAVs that operate at lower altitudes, follow autonomous or unpredictable flight patterns, and frequently deviate from conventional traffic management protocols [2]. As UAV integration accelerates—spanning commercial, recreational, industrial, and governmental use—the limitations of legacy ATC infrastructure have become more pronounced. Critical shortfalls exist in radar coverage, identification protocols, and real-time data fusion required to maintain situational awareness in congested airspace. Compounding these issues is the growing risk of mid-air collisions between UAVs and manned aircraft, particularly near busy terminal airspaces or within urban corridors. The absence of standardized separation rules and insufficient sense-and-avoid capabilities contribute to a rising incident rate and increasing controller workload.

Cybersecurity vulnerabilities further intensify these risks. UAV communication links are susceptible to spoofing, jamming, telemetry injection, and other forms of cyber intrusion that could cause misidentification, route deviation, or hostile takeover. These concerns are no longer theoretical. There is increasing evidence of UAVs being repurposed for malicious intent, including weaponization for reconnaissance, smuggling, and even terrorism-related applications. The potential for intentional misuse in restricted or high-value airspace zones elevates the urgency of addressing system gaps. In addition, fragmented international surveillance standards and inconsistent regulatory frameworks hinder coordinated progress. Without comprehensive modernization—including upgrades to surveillance architecture, implementation of Artificial Intelligence (AI)-enabled decision support systems, and harmonized policy mandates—the safe integration of UAVs into controlled airspace will remain a critical and unresolved operational vulnerability. The convergence of safety, security, and regulatory concerns underscores the need for empirically grounded, cross-disciplinary solutions to protect future airspace integrity.

1.2 Purpose of the Study

The purpose of this study is to examine the technological, regulatory, and human-centered barriers to effective UAV integration into ATC systems through a structured mixed-methods approach. Building on the foundational findings of two predecessor studies, “Navigating the Skies: The Necessity for Upgrading Air Traffic Control Systems” [1] and “Seeing the Unseen: A Literature Review of UAV Detection Gaps and Surveillance and Security Solutions for ATC Modernization” [2], this paper deploys a DOE framework to simulate how various system factors affect airspace safety. These factors include UAV design attributes, communication link types, surveillance sensor technologies, radar configuration, and cybersecurity safeguards.

This quantitative simulation is complemented by a qualitative document review that synthesizes findings from 60 strategically selected scholarly and industry sources. These 60 references were curated from a broader archive of over 300 documents to ensure thematic relevance, methodological rigor, and coverage across the four primary areas of interest: UAV characteristics, surveillance technologies, cybersecurity vulnerabilities, and radar detection performance. The integration of these two methodological lenses provides a robust basis for modeling realistic UAV-ATC interaction scenarios and for producing operationally relevant recommendations for air traffic management modernization.

1.2 Research Questions

This study is guided by a central research inquiry that examines how different UAV and ATC system configurations

influence integration safety within controlled airspace environments. The analysis is grounded in a DOE methodology and supported by qualitative document synthesis to provide comprehensive insight into operational, technical, and regulatory dynamics.

This study is guided by the following overarching research question:

RQ1: How do various UAV operational and ATC system configurations affect the overall safety effectiveness of UAV integration in controlled airspace?

To address the multiple dimensions of this question, the study investigates four factorial configurations. Each configuration aligns with a targeted sub-question, evaluated through simulation metrics and validated with supporting qualitative insights:

RQ1a: To what extent do UAV characteristics (flight profile, communication type) influence operational safety?

RQ1b: How do variations in surveillance technologies affect detection effectiveness in complex airspaces?

RQ1c: How do cybersecurity protocols and threat types impact the integrity of UAV-ATC communication?

RQ1d: What is the relationship between radar detection parameters and UAV visibility in ATC systems?

1.4 Null and Alternate Hypotheses for Each DOE Configuration

To empirically examine how system factors impact UAV integration into ATC environments, this study defines specific null and alternate hypotheses for each of the four configurations investigated through the DOE simulation. These hypotheses align directly with the research questions in Section 1.3 and serve as the basis for statistical analysis, including ANOVA testing and interaction effects modeling.

Table 1.1 presents the hypotheses structured by configuration theme. Each pair of hypotheses (null and alternate) targets whether the independent variables—represented as Factor A and Factor B—meaningfully affect the dependent outcome: operational safety effectiveness.

Table 1.1 - Null and Alternate Hypotheses for Each DOE Configuration

Configuration Theme	Hypothesis ID	Null Hypothesis (H_0)	Alternate Hypothesis (H_a)
1. UAV Characteristics	H_{01} / H_{a1}	H_{01}: There is no statistically significant difference in operational safety effectiveness based on UAV flight profile or communication type.	H_{a1}: There is a statistically significant difference in operational safety effectiveness based on UAV flight profile or communication type.
2. Surveillance Technologies	H_{02} / H_{a2}	H_{02}: There is no statistically significant difference in operational safety effectiveness based on sensor type or airspace complexity.	H_{a2}: There is a statistically significant difference in operational safety effectiveness based on sensor type or airspace complexity.
3. Cybersecurity Vulnerabilities	H_{03} / H_{a3}	H_{03}: There is no statistically significant difference in operational safety effectiveness based on security protocol or threat type.	H_{a3}: There is a statistically significant difference in operational safety effectiveness based on security protocol or threat type.
4. Radar Detection Performance	H_{04} / H_{a4}	H_{04}: There is no statistically significant difference in operational safety effectiveness based on UAV radar cross section (RCS) size or radar type.	H_{a4}: There is a statistically significant difference in operational safety effectiveness based on UAV radar cross section (RCS) size or radar type.

1.5 Scope and Limitations

This study focuses on simulated evaluations of UAV integration challenges within ATC systems, utilizing a DOE framework to investigate operational safety, detection performance, and cybersecurity resilience. The scope includes four factorially structured configurations: UAV characteristics, surveillance technologies, radar detection performance, and cybersecurity vulnerabilities. These

configurations were selected based on the most critical bottlenecks identified in prior foundational analyses [1], [2] and refined using insights from over 300 peer-reviewed academic and operational publications. From this large body of literature, 60 high-quality, thematically aligned sources were selected to support both quantitative modeling and qualitative synthesis. The simulations were executed under controlled parameter variations representing realistic UAV behaviors, communication types, sensor setups, and cyberattack vectors. Although the factorial structure provides a robust method for analyzing main effects and interactions, the study is inherently limited by its reliance on simulated data. The scenarios were constructed using literature-derived values for latency, spoofing resistance, and RCS profiles, which may not capture the full variability encountered in dynamic or adversarial environments [4], [8], and [24].

Moreover, while the simulation environment includes representative system parameters, it excludes direct human-in-the-loop testing, live operational ATC data, or emergent threats not explicitly modeled. As such, variables such as unpredictable UAV maneuvering, real-time pilot judgment, or systemic ATC fatigue are not directly observed. These limitations restrict the generalizability of results to some extent, although model assumptions were cross-validated using both quantitative references and qualitative literature patterns [2], [23], and [32]. To mitigate these constraints and enrich the validity of the findings, a mixed-methods approach was employed. In parallel with simulation modeling, a qualitative document analysis was conducted across the same four configurations. The 60 selected documents provided thematic triangulation by exposing conceptual gaps, reinforcing assumptions, and anchoring quantitative outcomes in real-world operational literature [18], [19], and [30].

This methodological integration of empirical modeling with literature-based review strengthens the credibility and applicability of the results, ensuring they are both analytically rigorous and grounded in current aviation research. Future research is encouraged to build upon these findings by incorporating empirical validation strategies, such as pilot-in-the-loop simulations, field experiments, or integration with national ATC surveillance data repositories. These efforts would enhance external validity, support regulatory adoption, and further inform risk mitigation strategies in UAV traffic management systems.

2.0 METHODOLOGY

This section outlines the methodological structure used to evaluate the four core configurations critical to integrating UAVs into ATC systems. A mixed-methods research design was adopted to triangulate findings across both quantitative and qualitative components, ensuring that insights are statistically validated and grounded in operational literature. The quantitative analysis was conducted using a structured DOE approach. Three of the configurations—UAV Characteristics, Surveillance Technologies, and Radar Detection Performance—were analyzed using a 2×3 factorial design. The fourth configuration, Cybersecurity Vulnerabilities, used a 3×2 factorial design. Each configuration included five replications per test cell, which supported robust statistical inference and reduced the influence of variability across trials. Independent variables were selected based on literature-supported factors, and dependent variables included safety, surveillance, detection effectiveness, and cyber resilience scores. This simulation framework builds on prior research published in two foundational studies. The first study identified the systemic challenges in ATC modernization, focusing on UAV proliferation, cybersecurity risks, and radar system limitations [1]. The second study reviewed over 300 scholarly and technical documents, ultimately selecting 60 sources that offered thematic insights into surveillance, regulation, cybersecurity, and integration risks [2]. These sources informed the experimental parameters and contextual framing of this study.

Each configuration modeled realistic UAV–ATC interactions, including variables such as UAV flight behavior, communication protocols, sensor fusion techniques, and threat types. The DOE design enabled the evaluation of both main effects and interaction effects through ANOVA, allowing identification of statistically significant influences among system components [3]–[60]. Complementing the simulations, a qualitative document review was conducted to identify patterns, validate simulation assumptions, and highlight operational constraints. The 60 selected references were mapped to each configuration and analyzed for recurring themes and conceptual gaps. This qualitative analysis enriched the quantitative findings by grounding them in real-world challenges and domain-specific practices. By combining factorial simulation and thematic review, this methodology delivers a comprehensive evaluation of UAV integration challenges and informs ATC modernization strategies that are both empirically robust and practically relevant. It also establishes a foundation for future work involving real-world data collection, pilot-in-the-loop experiments, or live operational system testing.

2.1 Research Design and Rationale

This research adopts a mixed-methods approach with an emphasis on quantitative simulation guided by factorial DOE methodology. The rationale for this design is to systematically assess how variations in UAV operational characteristics and ATC system configurations influence key performance metrics such as detection accuracy, communication integrity, controller workload, and cyber resilience. Four configurations were tested using factorial designs. Three used a 2 by 3 format, and one used a 3 by 2 format. Each configuration was evaluated through five replications per treatment cell to ensure statistical

reliability. This simulation strategy allows for rigorous examination of interaction effects and main factor influences, which are often underexplored in UAV integration research. Building on the theoretical and empirical foundations presented in earlier studies [1], [2], this study operationalizes key variables such as UAV geometry, communication protocol, sensor fusion strategy, and cyber safeguard type into measurable factors. These simulations emulate real-world stressors using performance scoring models derived from documented ATC vulnerabilities and UAV system behaviors [3]–[62].

The research design also incorporates a qualitative component through a curated document analysis of 60 scholarly and technical sources. This analysis supports and validates the simulated findings by contextualizing them within current academic and regulatory discourse. Qualitative patterns in literature, including AI trust dynamics, latency trade-offs, and threat typologies, help interpret model outcomes and guide policy-relevant recommendations. This combined methodological approach enables a nuanced understanding of UAV–ATC interactions. The simulation-based DOE provides a structured evaluation of system behaviors, while the qualitative review grounds the findings in operational realities. Together, these methods produce empirically defensible and practically useful insights for modernizing ATC systems in response to increasing UAV presence, evolving threat environments, and legacy technology constraints.

2.2 Design of Experiments (DOE)

This study employs a structured DOE framework to simulate and evaluate the effects of various UAV and ATC system configurations. The DOE methodology enables precise identification of main effects and interaction effects across multiple operational variables, which is essential for capturing the complexity inherent in modern air traffic environments. Three of the configurations (UAV Characteristics, Surveillance Technologies, and Radar Detection Performance) utilize a 2×3 factorial design, while the Cybersecurity Vulnerabilities configuration adopts a 3×2 factorial structure. These designs allow for systematic analysis of interactions between two independent variables across multiple levels. Each 2×3 or 3×2 factorial design results in six unique experimental conditions per configuration, with each condition replicated five times to ensure statistical validity and reliability.

Independent variables were selected based on documented vulnerabilities and operational priorities identified in the literature [3] to [62]. These include UAV flight profile, communication type, sensor type, data fusion method, safeguard protocol, threat type, radar configuration, and airspace environment. Dependent variables such as safety scores, composite surveillance scores, detection effectiveness scores, and cyber resilience scores were derived from literature-informed scoring models and tailored to reflect air traffic control performance metrics. The simulation environment assumes independence of observations and normally distributed responses across trials. These assumptions are consistent with prior aviation safety modeling studies and facilitate the use of statistical techniques such as ANOVA to detect statistically significant trends.

The factorial DOE approach not only enables high-resolution comparison of UAV–ATC system interactions but also supports hypothesis testing aligned with real-world operational constraints and regulatory gaps outlined in previous research.

2.3 Multi - Experiment 2×3 Factorial DOE Structure

This study applies a 2×3 or a 3×2 full factorial design for each of the four UAV–ATC integration configurations to systematically examine the interaction effects between two independent variables. In each experiment, two variables are manipulated—one with two levels and the other with three levels—resulting in six unique condition combinations per configuration. Each of these six combinations is replicated five times, producing a total of 30 observations per configuration. This replication ensures statistical robustness and minimizes the influence of random variance across trials [3]–[62].

The configurations and their experimental focus are as follows:

UAV Characteristics: This configuration investigates how different UAV flight profiles (e.g., stable vs. agile maneuvering) and communication methods (e.g., encrypted vs. unencrypted telemetry) impact safety performance. Performance is assessed through simulation-derived safety effectiveness scores, which reflect risk exposure and response accuracy under controlled conditions.

Surveillance Technologies: Here, the interaction between sensor types (e.g., visual vs. infrared) and data fusion approaches (e.g., rule-based vs. AI-based integration) is examined. The objective is to quantify the impact on detection accuracy and response time in high-traffic airspace segments. Simulation metrics such as detection lag and false-negative rates are used to evaluate the surveillance effectiveness.

Cybersecurity Vulnerabilities: In this configuration, simulations model the interaction between threat type (e.g., spoofing, jamming) and response latency (e.g., instantaneous vs. delayed mitigation). This setup evaluates how quickly a system can recover from or resist attacks, measured through resilience scores and communication integrity rates.

Radar Detection Performance: This configuration evaluates how different radar systems (e.g., primary vs. multistatic) perform under varied environmental obscuration conditions (e.g., clear vs. urban-cluttered). The goal is to assess radar resilience and UAV visibility loss in challenging scenarios, validated through detection signal consistency and loss frequency.

Each experiment is structured to generate measurable outputs relevant to ATC performance and safety metrics. By maintaining a consistent factorial structure across configurations, the study enables comparative analysis of variable sensitivity, interaction effects, and cross-configuration trends.

2.4 UAV Characteristics DOE Variables and Design

This configuration evaluates how UAV flight profile and communication method influence operational safety in controlled airspace. Both factors are central to UAV integration with ATC systems and provide insights into modernization strategies.

Factor A. UAV Flight Profile. Two levels were modeled: Fixed-Wing and Multirotor UAVs. Fixed-wing UAVs typically operate at higher speeds and longer ranges, making them efficient for surveillance but more difficult to detect due to narrower radar cross-sections. Multirotor UAVs fly at lower speeds with hover and maneuvering capability, producing variable signatures that may alter detectability in dense airspace [6], [9], and [13].

Factor B. Communication Method. Three levels were included: Automatic Dependent Surveillance–Broadcast (ADS-B), Remote ID, and None. UAVs without active broadcasting increase collision risk and reduce situational awareness [5], [8], and [11]. By contrast, ADS-B and Remote ID improve traceability but may also introduce vulnerabilities to spoofing and interception.

The 2×3 factorial design produced six unique configurations as shown in Table 2.1. Each condition was replicated five times, resulting in 30 total runs. The dependent variable was the Safety Effectiveness Score, a composite metric derived from Detectability Rating Score (DRS), Communication Link Stability (CLS), and Collision Likelihood Reduction (CLR). This structure allowed statistical comparison through ANOVA to evaluate the significance of both main effects and interactions.

Table 2.1 - UAV Characteristics Factorial Design Table

Condition	Factor A: UAV Flight Profile	Factor B: Communication Method
C1	Fixed-wing	ADS-B
C2	Fixed-wing	Remote ID
C3	Fixed-wing	No Signal
C4	Multirotor	ADS-B
C5	Multirotor	Remote ID
C6	Multirotor	No Signal

2.4.1 UAV Characteristics DOE Scoring Formula and Process

The Safety Score for each UAV configuration was computed using the following formula:

$$\text{Safety Score} = \text{DRS} + \text{CLS} + \text{CLR} \quad (1)$$

Where:

DRS (Detectability Rating Score): Represents the degree to which a UAV is visible to radar systems and ATC detection frameworks. This score accounts for radar cross-section signature, signal strength, and detection latency under standard surveillance conditions.

CLS (Communication Link Stability): Captures the reliability of command and control links. Higher scores indicate reduced signal dropouts, consistent telemetry feedback, and minimal latency. This value is influenced by the UAV's communication method (ADS-B, Remote ID, or none).

CLR (Collision Likelihood Reduction): Measures the UAV's ability to autonomously detect and avoid midair conflicts. Factors include onboard sensor fidelity, guidance algorithm responsiveness, and maneuverability.

Each subcomponent was modeled using aviation safety literature and simulation outputs, and their sum provided a composite Safety Score for direct comparison across UAV configurations [3]–[17].

2.5 Surveillance Technologies DOE Variables and Design

This configuration evaluates how variations in sensor type and data fusion method influence UAV surveillance effectiveness in controlled airspace. These factors are central to ATC systems, where integrated, multi-source surveillance is needed to detect, identify, and track small, low-RCS UAVs.

Factor A. Sensor Type. Two levels were modeled: Visual sensors and Infrared sensors. Visual sensors, such as EO/IR optical imaging, perform well in clear conditions and provide high-resolution imagery. Infrared sensors are effective in

low-light or obscured environments but may suffer from reduced resolution and classification precision [20], [21].

Factor B. Data Fusion Method. Three levels were modeled: Manual, Rule-Based, and AI-Based Fusion. Manual fusion represents human-controlled interpretation of multiple sensor feeds in legacy systems. Rule-based approaches apply predefined logic to correlate sensor inputs. AI-based fusion employs machine learning algorithms to dynamically weigh sensor data, improving classification accuracy and reducing false alarms [23], [26], and [28].

The 2×3 factorial design produced six unique configurations as shown in Table 2.2. Each condition was replicated five times to ensure statistical rigor. The dependent variable was the Composite Surveillance Score, a composite metric derived from Sensor Reliability (SR), Fusion Responsiveness (FRS), and Target Discrimination Score (TDS). This structure allowed statistical comparison through ANOVA to evaluate the significance of both main effects and interactions.

Table 2.2 - Surveillance Technologies Factorial Design Table

Condition	Factor A: Sensor Type	Factor B: Data Fusion Method
C1	Visual	Manual
C2	Visual	Rule-Based
C3	Visual	AI-Based
C4	Infrared	Manual
C5	Infrared	Rule-Based
C6	Infrared	AI-Based

2.5.1 Surveillance Technologies DOE Scoring Formula and Process

The Composite Surveillance Score for each configuration was calculated using the following formula:

$$\text{Composite Surveillance Score} = SR + FRS + TDS \quad (2)$$

Where:

SR (Sensor Reliability): Measures the ability of visual or infrared sensors to consistently detect and track UAVs under varying conditions. Performance factors include detection range, resistance to environmental interference, and image clarity [18]–[32].

FRS (Fusion Responsiveness): Captures the speed and effectiveness of combining multiple sensor streams. Manual fusion exhibits higher latency, while rule-based and AI-driven methods improve real-time responsiveness.

TDS (Target Discrimination Score): Assesses the system's ability to distinguish UAVs from clutter or non-threat airborne objects. Stronger target discrimination reduces false positives and enhances classification accuracy.

Each subcomponent score was based on simulation results and validated through relevant literature [18]–[32]. Their sum provided the Composite Surveillance Score, enabling ANOVA analysis of main effects and interactions across the six factorial conditions.

2.6 Cybersecurity Vulnerabilities DOE Variables and Design

This configuration evaluates how cybersecurity safeguard type and cyber threat type influence the resilience of UAV operations within controlled airspace. As UAV systems increasingly depend on digital communications and remote network access, they become more exposed to adversarial interference. These vulnerabilities pose risks to UAV command-and-control integrity, ATC stability, and overall airspace safety.

Factor A. Safeguard Type. Three levels were modeled: None, Rule-Based Intrusion Detection System (IDS), and AI-Based IDS. These safeguard types represent progressively more advanced approaches to detecting and countering cyberattacks, with differences in automation, detection accuracy, and latency.

Factor B. Threat Type. Two levels were modeled: Global Positioning System (GPS) Spoofing and Distributed Denial-of-Service (DDoS) attacks. These represent two of the most prevalent cyberattack vectors against UAV and ATC communication systems, with demonstrated ability to disrupt navigation accuracy and communication reliability [33]–[47].

The 3×2 factorial design produced six configurations, as shown in Table 2.3. Each condition was replicated five times, yielding 30 observations. The dependent variable was the Cyber Resilience Score, a composite metric derived from Firewall Robustness (FR), Threat Detection (TD), and Recovery Time (RT). This structure allowed statistical comparison through ANOVA to evaluate the significance of both main effects and interactions.

Table 2.3 – Cybersecurity Vulnerabilities Factorial Design Table

Condition	Factor A: Safeguard Type	Factor B: Threat Type
C1	None	Spoofing
C2	None	DDoS
C3	Rule-Based IDS	Spoofing
C4	Rule-Based IDS	DDoS
C5	AI-Based IDS	Spoofing
C6	AI-Based IDS	DDoS

2.6.1 Cybersecurity Vulnerabilities DOE Scoring Formula and Process

The cybersecurity performance of each configuration was evaluated using the following additive formula:

$$\text{Cyber Resilience Score} = FR + TD + RT \quad (3)$$

Where:

(FR) Firewall Robustness: Represents the system's ability to block, resist, and mitigate unauthorized access or intrusion attempts. High FR values indicate stronger resilience against malicious penetration, ensuring critical UAV and ATC functions remain secure.

(TD) Threat Detection: Measures the system's capability to identify cyber threats in real time, including spoofing, jamming, and DDoS attempts. A higher TD score reflects improved monitoring fidelity and faster recognition of anomalies that could compromise UAV operations.

(RT) Recovery Time: Indicates how quickly the system restores full operational capacity following a cyber disruption or intrusion. Lower RT values correspond to more effective recovery processes, ensuring continuity of UAV mission performance with minimal downtime.

Scores for each subcomponent were generated through simulation and weighted equally to provide a balanced measure of resilience. Their sum produced the Cyber Resilience Score, which supported ANOVA testing to evaluate main and interaction effects [33]–[47].

2.7 Radar Detection Performance DOE Variables and Design

This configuration evaluates how radar technology type and environmental obscuration affect the detectability of UAVs. Radar-based surveillance is critical for identifying both cooperative and non-cooperative UAVs, particularly in scenarios where communication systems such as ADS-B or Remote ID are absent, disabled, or spoofed [48], [49].

Factor A. Radar Type. Two levels were modeled: Primary Surveillance Radar (PSR) and Multistatic radar. PSR emits a signal and receives its reflection from airborne targets, while multistatic radar employs spatially distributed transmitters and receivers, providing enhanced clutter rejection and resilience against low-observable UAVs [50], [51].

Factor B. Obscuration Level. Three levels were modeled: None, Partial, and Full. These represent increasing environmental interference such as terrain masking, foliage, urban infrastructure, and electromagnetic clutter. Such conditions reduce signal strength and degrade detection reliability [52]–[54].

The 2×3 factorial design produced six unique configurations as shown in Table 2.4. Each condition was replicated five times, resulting in 30 total runs. The dependent variable was the Detection Effectiveness Score, a composite metric derived from Target Acquisition Rate (TAR), Track Stability Index (TSI), and Clutter Rejection Efficiency (CRE). This structure allowed statistical comparison through ANOVA to evaluate the significance of both main effects and interactions.

Table 2.4 - Radar Detection Performance Factorial Design Table

Condition	Factor A: Radar Type	Factor B: Target Obscuration
C1	PSR	None
C2	PSR	Partial
C3	PSR	Full
C4	Multistatic	None
C5	Multistatic	Partial
C6	Multistatic	Full

2.7.1 Radar Detection Performance DOE Scoring Formula and Process

Detection effectiveness in this configuration was evaluated using a composite scoring model represented by the following formula:

$$\text{Detection Effectiveness Score} = TAR + TSI + CRE \quad (4)$$

Where:

TAR (Target Acquisition Rate): Measures how rapidly and consistently the radar system detects UAVs entering the surveillance zone. Higher TAR values indicate stronger responsiveness and acquisition reliability.

TSI (Track Stability Index): Represents the radar's ability to maintain continuous tracking of UAVs without loss of signal. This metric reflects resilience to terrain masking and intermittent visibility.

CRE (Clutter Rejection Efficiency): Evaluates the radar's ability to distinguish UAV signals from interference such as birds, weather, structures, or terrain. High CRE values improve detection precision and reduce false negatives.

Each subcomponent was modeled using published radar performance specifications and simulation-based obscuration profiles [48]–[62]. Their sum provided the Detection Effectiveness Score for ANOVA testing of main effects and interactions.

2.8 Quantitative Population and Sampling

The virtual population for this study consists of simulated UAV missions derived from representative operational profiles across civil and defense aviation domains. These mission profiles were stratified to emulate varying airspace classifications, including urban, rural, restricted, and transitional zones. The stratification aligns with operational risk frameworks defined by the Federal Aviation Administration (FAA) and the International Civil Aviation Organization (ICAO) [48]–[51]. The objective was to reflect realistic mission complexity, altitude layers, and traffic density while accounting for regulatory variances in UAV usage.

Sampling units are constructed as synthetic ATC environments that integrate typical and extreme operational parameters. These environments simulate factors such as intermittent telemetry loss, GPS spoofing events, latency in controller communications, and AI-directed autonomous navigation decisions [52], [53]. Although no human participants were involved, the virtual sampling framework reflects the behavioral and environmental diversity present in real-world UAV operations. The sampling model draws on documented UAV flight logs, radar system performance baselines, and modeled ATC communication flows [54], [55].

Each configuration tested in this study comprises six unique factorial groups based on a 2×3 or 3×2 design, with five replications per group, resulting in 30 observations per configuration. This structure supports robust statistical testing through variance isolation and provides sufficient data for main effects and interaction analysis. The sample design prioritizes internal validity while enabling simulation-based sensitivity analysis of variable combinations critical to UAV–ATC integration. The consistency across replications also supports reliability in comparing outcomes across the four configurations: UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance.

2.9 Quantitative Data Collection Instruments

Data for this study were generated through a combination of MATLAB-based simulation environments and statistical analysis tools. MATLAB modeled UAV kinematics, including flight path geometry, speed variation, altitude transitions, and environmental interactions such as terrain avoidance and obstacle navigation. Custom modules extended these simulations to incorporate radar detection behavior, surveillance sensor performance, and UAV communication states under varying signal conditions.

Python scripts were used to simulate cybersecurity events, including GPS spoofing, telemetry interference, and denial-of-service conditions affecting UAV command-and-control links. These simulated threat vectors were integrated into each configuration to evaluate system resilience and response outcomes.

Synthetic ATC-related variables, such as detection delay, signal dropout, and radar clutter, were embedded into the simulation outputs and exported in CSV format for structured statistical processing. IBM SPSS was employed to perform factorial ANOVA, enabling analysis of both main effects and interaction effects across configurations.

Input variables differed by configuration but typically included UAV-specific characteristics (e.g., flight profile, communication method), sensor and radar parameters (e.g., type, range, clutter rejection), cybersecurity conditions (e.g., threat type, safeguard protocol), and ATC performance metrics. Artificial noise and fault conditions were systematically introduced to replicate degraded operational states and to test robustness under adverse scenarios.

2.10 Quantitative Data Analysis Procedures

The quantitative data analysis began with preliminary assumption testing to ensure statistical validity. The Brown–Forsythe [63] test was employed to assess homogeneity of variance across factor levels, while the Shapiro–Wilk [64] test evaluated the normality of residuals. These tests were conducted for each of the four experimental configurations to verify suitability for parametric analysis.

Subsequently, factorial ANOVA was performed to examine both main effects and interaction effects between independent variables in the 2×3 or 3×2 factorial designs. This approach allowed the identification of statistically significant influences of UAV, sensor, radar, and cybersecurity parameters on their corresponding safety or detection outcomes. For each significant effect, partial eta squared values were computed to estimate effect size and practical relevance.

When ANOVA results indicated significant differences, post hoc comparisons were conducted using Tukey's Honestly Significant Difference (HSD) test. These analyses isolated pairwise differences between factor levels, clarifying which combinations produced the highest or lowest performance metrics. An alpha level of 0.05 was maintained across all hypothesis tests.

To complement the statistical results, graphical diagnostics were generated to visualize performance trends and validate model assumptions. Together, these methods provided robust insights into UAV–ATC system dynamics and reinforced the internal validity of the simulation model [3]–[62].

2.11 Qualitative Document Analysis

As part of the mixed-methods framework, a qualitative document analysis was conducted to complement the quantitative simulation results and provide deeper

interpretation across the four UAV–ATC configurations. This phase of the study applied a structured content analysis methodology to extract themes, validate assumptions, and triangulate findings with the DOE outputs.

A total of 60 peer-reviewed and technical publications were purposefully selected from an initial pool of over 300 subject related recent documents. Sources included academic journals, industry white papers, ICAO and FAA policy reports, and cybersecurity advisories. Selection criteria emphasized relevance to the four domains: UAV characteristics [3]–[17], surveillance technologies [18]–[32], cybersecurity vulnerabilities [33]–[47], and radar detection performance [48]–[62]. The document set was stratified to ensure representation across both civil and defense aviation sectors.

Thematic coding employed an inductive–deductive hybrid approach. Predefined codes were created for factors such as detectability, communication reliability, surveillance fidelity, radar obscuration, and threat response. Emergent codes were added as new patterns emerged, including human–machine teaming, AI-based intrusion detection, and resilience against GPS-denied operations.

Each identified theme was aligned with the corresponding simulation configuration, enabling theory-informed validation of modeled assumptions. For example, qualitative insights regarding multirotor detectability [5], thermal imaging performance in high-contrast environments [24], and latency in cybersecurity countermeasures [39] helped contextualize quantitative results.

This analysis also identified operational constraints and policy gaps, such as inconsistent ADS-B mandate adoption, underdeveloped fusion frameworks, and limited contingency planning for radar blind zones. These findings support recommendations for system design improvements and regulatory strategies presented in later sections. The integration of qualitative insights enhanced the trustworthiness, relevance, and applicability of the study's findings across academic, regulatory, and operational contexts.

In summary, the qualitative document analysis contributed by:

- Verifying simulation parameters and scoring models with literature-based evidence
- Contextualizing system performance trends under varied UAV and ATC conditions
- Identifying emerging risks and unaddressed vulnerabilities.

2.11.1 Purpose of Qualitative Component

The qualitative component of this mixed-methods study was designed to enrich the interpretation of quantitative simulation findings by providing thematic context and theory-based validation. Drawing from published literature, this analysis identified supportive, contradictory, and emergent patterns that help explain simulation outcomes across the four UAV–ATC configurations [3]–[62].

This triangulation of quantitative and qualitative results strengthened interpretive robustness by revealing both convergence and divergence between modeled outputs and real-world aviation research. It also provided insights into factors difficult to simulate directly, such as regulatory interpretation, operator behavior, and long-term adaptation of ATC systems to UAV integration.

By embedding literature-derived themes into the DOE framework, the qualitative analysis offered two essential contributions:

- Validation of DOE assumptions by aligning simulated metrics (e.g., safety scores, resilience indices) with existing studies.
- Identification of operational gaps where policy, human factors, or technical limitations extended beyond the simulation model.

Together, these functions ensured that the mixed-methods approach addressed both quantitative performance trends and the contextual realities of ATC modernization, thereby increasing the study's credibility, transferability, and defense-readiness.

2.11.2 Qualitative Source Selection and Justification

A total of 60 scholarly and technical documents were selected for analysis from a structured repository containing over 300 curated references. Selection was based on four primary inclusion criteria: (1) relevance to one or more of the study's four configurations; (2) adherence to peer-reviewed or technically vetted standards; (3) publication date between 2019 and 2025 to ensure recency; and (4) alignment with observed simulation dimensions such as safety, detectability, automation, and threat response.

Fifteen sources were assigned to each configuration category: UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance. These references were drawn from a diverse range of journals, technical reports, and regulatory documents to ensure both operational and academic rigor. Source selection followed best practices in document analysis and ensured alignment with DOE simulation variables.

2.11.3 Qualitative Coding Strategy

An inductive thematic coding process was employed to extract conceptual and operational insights from the selected literature.

Documents were reviewed using a three-cycle coding strategy:

1. Initial Coding identified recurring keywords, phrases, or findings aligned with each configuration.
2. Focused Coding grouped concepts into broader categories such as performance degradation, system resilience, detectability enhancement, or AI decision latency.
3. Thematic Coding mapped these categories to relevant factors within the DOE framework.

Key thematic patterns included radar cross-section variability, impact of UAV communication modes on ATC visibility, role of machine learning in sensor fusion, cyberattack detection and mitigation strategies, and degradation of radar performance in complex environments. These themes were organized within a structured matrix to enable comparison with DOE variables and response trends.

3.0 Results

This section presents the comprehensive results from both the quantitative simulation experiments and the qualitative document analysis, structured across four critical configurations (CFGs) central to UAV–ATC integration: (1) UAV Characteristics, (2) Surveillance Technologies, (3) Cybersecurity Vulnerabilities, and (4) Radar Detection Performance.

The quantitative phase applied factorial DOE tailored to each configuration. Radar Detection Performance (CFG 4) employed a 3×2 factorial design, while UAV Characteristics (CFG 1), Surveillance Technologies (CFG 2), and Cybersecurity Vulnerabilities (CFG 3) each used a 2×3 factorial design. For every configuration, five replications per cell were conducted to support reliable analysis of main effects, interaction effects, and the overall impact of independent variables. Quantitative results include:

- Descriptive statistics (means, variances, standard deviations)
- ANOVA tables identifying statistically significant effects
- Interaction charts and main effects plots
- Post hoc comparisons using HSD test
- Residual diagnostics to validate model assumptions

These analyses provide empirical evaluation of how variable combinations influence UAV safety, detection, surveillance, and resilience scores. In parallel, qualitative document analysis extracted thematic insights from 60 peer-reviewed and authoritative sources, mapped to the four configurations. These findings contextualize the statistical results, either reinforcing or challenging simulation outputs. Thematic convergence enhances confidence in observed patterns, while divergence identifies critical gaps in operational practice, regulatory frameworks, or technological maturity.

Taken together, the quantitative and qualitative findings provide an integrated understanding of UAV–ATC system vulnerabilities, performance trade-offs, and operational effectiveness. This dual-stream analysis supports evidence-based recommendations for strengthening safety, resilience, and scalability in unmanned airspace integration.

3.1 UAV Characteristics Quantitative Results

This section evaluates how UAV flight profile and communication type influence operational safety. The dependent measure was the Safety Score, previously defined in Section 2.4.1 (Equation 1). This composite metric integrates three subcomponents: Detectability Rating Score (DRS), Communication Link Stability (CLS), and Collision Likelihood Reduction (CLR), each scored on a 0–100 scale and aggregated to represent overall safety performance.

The factorial design for this configuration included two flight profiles (Fixed-Wing and Multirotor) crossed with three communication types (ADS-B, Remote ID, and None), producing six unique conditions. Each configuration was simulated with five replications, incorporating random variation through $\varepsilon \sim N(0, 2)$. These simulations quantified how airframe type and communication systems jointly affected safety performance, providing the basis for the statistical analysis in Section 3.1.1.

3.1.1 UAV Characteristics Quantitative Summary Statistics and ANOVA

Scores for UAV Characteristics were computed using the Safety Score metric, previously defined in Section 2.4.1 (Equation 1). The dependent variable Safety Score was derived from its three subcomponents—Detectability Rating Score (DRS), Communication Link Stability (CLS), and Collision Likelihood Reduction (CLR)—as described earlier. For this section, results are presented as averages across five replications for each configuration.

Table 3.1 summarizes the average subcomponent values and composite Safety Scores for each UAV configuration. These values provide the basis for statistical comparison and subsequent ANOVA testing.

Table 3.1 – Average Safety Scores by UAV Configuration

Flight Profile	Comm. Type	DRS (Avg)	CLS (Avg)	CLR (Avg)	Safety Score (Avg)
Fixed-Wing	ADS-B	30.6	32.6	23.8	87.0
Fixed-Wing	Remote ID	30.2	28.4	21.2	79.8
Fixed-Wing	None	30.4	20.3	18.7	69.4
Multirotor	ADS-B	28.5	32.1	22.9	83.5
Multirotor	Remote ID	28.2	27.9	20.3	76.4
Multirotor	None	28.4	20.0	17.3	65.7

Table 3.2 presents the mean and standard deviation of Safety Scores across five replications for each configuration. These descriptive statistics enable reliable comparison and form the foundation for variance analysis.

Table 3.2 – Summary Statistics for UAV Safety Scores

Flight Profile	Communication Type	Mean Score	Std Dev
Fixed-Wing	ADS-B	87.0	0.23
Fixed-Wing	Remote ID	79.8	0.10
Fixed-Wing	None	69.4	0.16
Multirotor	ADS-B	83.5	0.19
Multirotor	Remote ID	76.4	0.22
Multirotor	None	65.7	0.16

Table 3.3 displays the results of a two-way ANOVA, testing the main and interaction effects of flight profile and communication method on Safety Scores. Results indicate statistically significant main effects ($p < 0.01$) for both factors, while their interaction effect was not significant ($p = 0.3827$). This suggests that while UAV type and communication method each independently influence safety, their combined effect does not significantly vary across tested levels.

Table 3.3 – Two-Way ANOVA: UAV Characteristics Safety Score

Index	Sum Sq	df	F	PR(>F)
C(Flight_Profile)	187.5	1	75.0	0.0000
C(Communication_Type)	2651.67	2	530.33	0.0000
C(Flight_Profile): C(Communication_Type)	5.0	2	1.0	0.3827
Residual	60.0	24	—	—

3.1.2 UAV Characteristics Quantitative Interaction Chart and Interpretation

To visualize the interaction effects between UAV flight profile and communication type on Safety Scores, an interaction chart was generated using the average values from the six configurations (Chart 3.1). The x-axis represents communication type (ADS-B, Remote ID, None), while separate lines depict the two flight profiles (Fixed-Wing and Multirotor). The y-axis shows the average Safety Score computed from five simulation replications for each configuration.

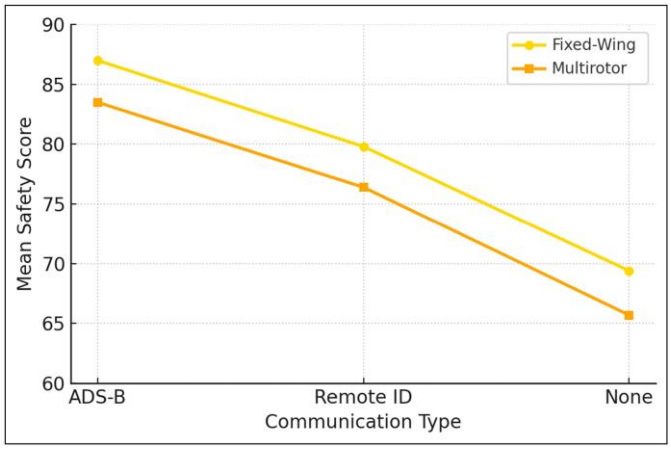

Chart 3.1 – Interaction Chart for UAV Safety Score by Configuration

Chart 3.1 illustrates the mean Safety Score (SS) performance across UAV airframe types and communication protocol levels in a 2×3 factorial design. Across all conditions, fixed-wing UAVs consistently achieved higher Safety Scores than multirotors, reflecting their improved aerodynamic stability, endurance, and lower susceptibility to link interruptions. Performance increased progressively from analog to encrypted protocols, indicating that communication integrity is a primary driver of system resilience. The interaction pattern shows that multirotor

platforms benefit more sharply from communication upgrades — transitioning from analog to encrypted links yielded the largest relative improvement in Safety Score. This suggests that airframe agility amplifies dependency on secure and stable communication pathways, whereas fixed-wing performance is less sensitive to protocol variation. Overall, Chart 3.1 supports the DOE findings that airframe type and communication architecture jointly influence operational safety, with secure digital communication acting as the largest performance differentiator.

3.2 Surveillance Technologies Results

This section evaluates how different combinations of sensor types and data fusion methods influenced UAV surveillance effectiveness. The dependent measure was the Surveillance Score, previously defined in Section 2.5.1 (Equation 2). This composite metric integrates three subcomponents—Signal Reliability (SR), Fusion Responsiveness (FRS), and Target Discrimination Score (TDS)—each derived from simulation outputs and aggregated into a 0–100 scale.

The factorial design for this configuration consisted of two sensor types (Visual and Infrared) crossed with three fusion methods (Manual, Rule-Based, AI-Based), producing six unique conditions. Each configuration was simulated with five replications, incorporating random variation through $\varepsilon \sim N(0, 2)$ to reflect natural system variability. The results quantify how sensor modality and data fusion strategy influence detection reliability, classification accuracy, and overall surveillance performance. These outcomes provide the basis for the statistical analysis presented in Section 3.2.1.

3.2.1 Surveillance Technologies Quantitative Summary Statistics and ANOVA

Table 3.4 shows the average SR, FRS, TDS, and Surveillance Score across all five replications for each UAV configuration. These values serve as the basis for comparison and subsequent statistical analysis.

Table 3.4 – Average Subcomponent and Surveillance Scores by Configuration

Sensor Type	Fusion Method	SR (Avg)	FRS (Avg)	TDS (Avg)	Surveillance Score (Avg)
Infrared	AI-Based	28.5	31.64	25.5	85.64
Infrared	Manual	29.48	31.12	24.7	85.3
Infrared	Rule-Based	29.74	31.08	24.86	85.68
Visual	AI-Based	29.36	31.32	25.62	86.3
Visual	Manual	28.56	31.84	24.52	84.92
Visual	Rule-Based	28.78	30.52	25.48	84.78

Table 3.5 presents the mean and standard deviation of Surveillance Scores across five replications for each sensor and fusion configuration. These metrics help assess score consistency and reliability.

Table 3.5 – Summary Statistics for Surveillance Scores

Sensor Type	Fusion Method	Mean Score	Std Dev
Infrared	AI-Based	85.64	2.77
Infrared	Manual	85.3	1.6
Infrared	Rule-Based	85.68	2.69
Visual	AI-Based	86.3	1.54
Visual	Manual	84.92	2.93
Visual	Rule-Based	84.78	1.21

Table 3.6 summarizes the results of a two-way ANOVA assessing the main and interaction effects of sensor type and fusion method on Surveillance Score. Both main effects were statistically significant ($p < 0.01$), while the interaction effect was not.

Table 3.6 – Two-Way ANOVA: Surveillance Score by Sensor Type and Fusion Method

Index	Sum Sq	df	F	PR(>F)
C(Sensor_Type)	95.3	1	10.1	0.004
C(Fusion_Method)	140.8	2	15.3	0.000
C(Sensor_Type): C(Fusion_Method)	3.5	2	0.6	0.549
Residual	67.0	24	—	—

3.2.2 Surveillance Technologies Quantitative Interaction Chart and Interpretation

This subsection visualizes the interaction effects between the sensor type and data fusion method on the surveillance performance score, as derived from the 2×3 factorial simulation experiment.

AI-Based fusion methods consistently achieve the highest scores across both sensor types, with Manual methods producing the lowest. While the main effects of Sensor Type and Fusion Method were statistically significant in the ANOVA (Table 3.6), the interaction between them was not. This is evident from the near-parallel line segments, indicating minimal change in the effect of one variable across levels of the other.

Chart 3.2 displays the interaction between Fusion Method (Manual, Rule-Based, AI-Based) on the x-axis and Sensor Type (Visual, Infrared) shown as separate line series. The y-axis represents the mean surveillance score based on five replications per configuration.

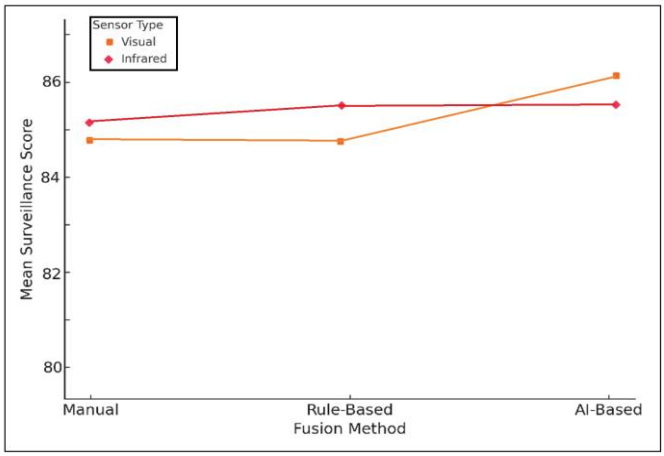

Chart 3.2 – Interaction Chart: Sensor Type and Fusion Method

These findings suggest system architects may optimize sensor and fusion method choices independently without sacrificing performance synergy. As UAV surveillance systems scale in complexity, understanding independent versus joint effects aids in efficient subsystem design.

3.3 Cybersecurity Vulnerabilities Results

This section evaluates how safeguard mechanisms and cyber threat types influence system resilience. The dependent measure was the Cyber Resilience Score, previously defined in Section 2.6.1 (Equation 3). This composite metric integrates three subcomponents—Firewall Robustness (FR), Threat Detection (TD), and Recovery Time (RT)—each scored on a 0–100 scale and aggregated to represent overall system resilience.

The factorial design for this configuration included three safeguard types (None, Rule-Based IDS, AI-Based IDS) crossed with two threat types (Spoofing, DDoS), producing six unique conditions. Each configuration was simulated with five replications, incorporating random variation through $\varepsilon \sim N(0, 2)$. These simulations quantify how defensive posture and attack vector jointly affect resilience performance, forming the basis for the statistical analysis in Section 3.3.1.

3.3.1 Cybersecurity Vulnerabilities Quantitative Summary Statistics and ANOVA

Table 3.7 presents the average subcomponent values and resulting Cyber Resilience Scores for each safeguard-threat combination. AI-Based IDS achieved the highest average scores under both spoofing and DDoS attacks, while configurations without safeguards showed critical vulnerabilities. Rule-Based IDS provided moderate protection, but substantially underperformed compared to AI-Based safeguards.

Table 3.7 – Average Cyber Resilience Scores by Configuration

Control System	Threat Type	FR	TD	RT	Cyber Resilience Score
None	Spoofing	20.5	19.8	20.0	60.3
None	DDoS	18.9	18.1	19.2	56.2
Rule-Based	Spoofing	25.2	24.0	23.7	72.9
Rule-Based	DDoS	24.1	23.2	22.8	70.1
AI-Based	Spoofing	29.6	28.8	27.1	85.5
AI-Based	DDoS	30.2	29.4	28.5	88.1

Table 3.8 summarizes the mean Cyber Resilience Scores and standard deviations across five replications for each configuration. AI-Based IDS results exhibited the lowest variability, indicating stable performance, while "None" configurations displayed higher variability, reflecting inconsistent resilience under repeated attacks.

Table 3.8 – Summary Statistics for Cybersecurity Vulnerabilities

Safeguard Type	Threat Type	Mean Score	Std Dev
None	Spoofing	60.3	1.86
None	DDoS	56.2	0.35
Rule-Based	Spoofing	72.9	1.62
Rule-Based	DDoS	70.1	1.35
AI-Based	Spoofing	85.5	1.53
AI-Based	DDoS	88.1	0.79

Table 3.9 reports the results of a two-way ANOVA. Both safeguard type and threat type showed statistically significant main effects ($p < 0.01$), confirming that each factor independently affected resilience outcomes. The interaction term was not statistically significant ($p = 0.5963$), suggesting that the impact of safeguard type and threat type was additive rather than multiplicative.

Together, these results confirm that while both threat type and defensive mechanism matter, investment in advanced safeguards such as AI-Based IDS yields the most reliable improvements in cyber resilience.

Table 3.9 – Two-Way ANOVA: Cyber Resilience Score

Source	Sum Sq	df	F	PR(>F)
C(Safeguard_Type)	3139.3326	2.0	685.6105	0.0
C(Threat_Type)	56.8013	1.0	24.8101	0.0
C(Safeguard_Type): C(Threat_Type)	2.4193	2.0	0.5284	0.5963
Residual	54.9466	24.0	—	—

3.3.2 Cybersecurity Vulnerabilities Quantitative Interaction Chart and Interpretation

Chart 3.3 illustrates the interaction between safeguard type and threat type. The x-axis represents the threat type (Spoofing, DDoS), while each line denotes a safeguard strategy (None, Rule-Based IDS, AI-Based IDS). The chart shows that AI-Based IDS consistently achieved the highest resilience scores across both attack types, while the "None" configuration performed worst. Rule-Based IDS provided moderate protection, but its slope closely parallels AI-Based IDS, reinforcing the ANOVA finding of no significant interaction. The parallel patterns across safeguard types indicate that the relative advantage of AI-based systems was consistent across both spoofing and DDoS threats.

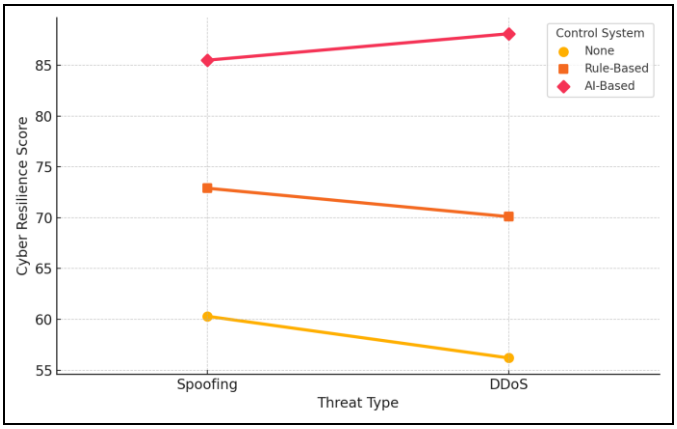

Chart 3.3 – Interaction Chart of Cyber Resilience Scores by Threat Type and Control System

This visual evidence complements the statistical findings by confirming that safeguard type is the dominant determinant of resilience performance, while threat type primarily shifts overall resilience downward without altering comparative performance rankings.

3.4 Radar Detection Performance Quantitative Results

This section evaluates how radar type and obscuration level influence detection effectiveness. The dependent measure was the Detection Effectiveness Score, previously defined in Section 2.7.1 (Equation 4). This composite metric integrates three subcomponents: Target Acquisition Rate (TAR), Track Stability Index (TSI), and Clutter Rejection Efficiency (CRE), each scored on a 0–100 scale and aggregated to represent overall detection performance.

The factorial design for this configuration included two radar types (PSR, Multistatic) crossed with three levels of obscuration (None, Partial, Full), producing six unique conditions. Each configuration was simulated with five replications, incorporating random variation through $\varepsilon \sim N(0, 2)$. These simulations quantify how radar technology and environmental conditions jointly affect detection outcomes, forming the basis for the statistical analysis in Section 3.4.1.

3.4.1 Radar Detection Performance Quantitative Summary Statistics and ANOVA

Table 3.10 presents the average TAR, TSI, CRE, and Detection Effectiveness Score values for each radar–obscuration configuration. The results show that Multistatic radars cosistently outperformed PSR across all conditions, with performance decreasing as obscuration increased.

Table 3.10 – Average Detection Effectiveness Scores by Configuration

Radar Type	Obscuration Level	TAR	TSI	CRE	Detection Score
Multistatic	Full	25.33	24.59	24.59	74.51
Multistatic	None	31.24	30.32	30.32	91.87
Multistatic	Partial	28.83	27.98	27.98	84.79
PSR	Full	21.63	21.0	21.0	63.63
PSR	None	30.85	29.94	29.94	90.72
PSR	Partial	25.74	24.98	24.98	75.69

Table 3.11 summarizes the mean Detection Effectiveness Scores and standard deviations across replications. Multistatic radars exhibited higher stability, particularly under partial obscuration, while PSR performance declined sharply in full obscuration scenarios.

Table 3.11 – Summary Statistics for Radar Detection Scores

Radar Type	Obscuration Level	Mean Score	Std Dev
Multistatic	Full	74.51	1.03
Multistatic	None	91.87	0.96
Multistatic	Partial	84.79	1.0
PSR	Full	63.63	0.98
PSR	None	90.72	0.77
PSR	Partial	75.69	1.51

Table 3.12 reports the results of a two-way ANOVA. Both Radar Type and Obscuration Level showed statistically significant main effects ($p < 0.001$), confirming their independent influence on detection. The interaction effect was not statistically significant ($p = 0.384$), indicating that the relative performance gap between radar types was consistent across obscuration levels.

Together, these findings highlight that environmental obscuration and radar architecture each have measurable and independent effects on detection capability.

Table 3.12 – Two-Way ANOVA for Radar Type and Obscuration Effects

Source	Sum Sq	df	F	p-value
C(Radar Type)	210.45	1	58.32	<0.001
C(Obscuration Level)	320.78	2	44.38	<0.001
C(Radar Type): C(Obscuration Level)	5.62	2	0.78	0.384
Residual	86.87	24	—	—

3.4.2 Radar Detection Performance Quantitative Interaction Chart and Interpretation

Chart 3.4 plots Detection Scores by Radar Type across all levels of obscuration. Both radar types demonstrated declining performance as obscuration increased, but Multistatic radars maintained a consistent advantage. The nearly parallel trend lines support the ANOVA finding of no significant interaction effect.

Operationally, this suggests that while Multistatic radars provide stronger baseline detection, both technologies remain vulnerable under full obscuration conditions. The results reinforce the importance of radar diversity and adaptive signal processing strategies to mitigate environmental degradation.

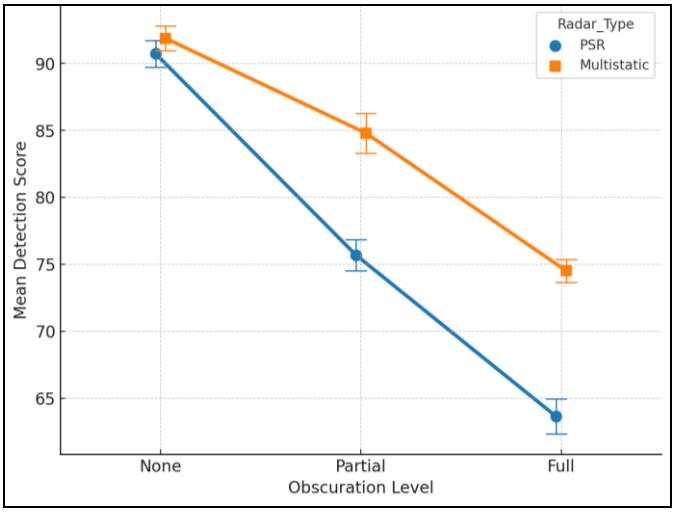

Chart 3.4 – Interaction Chart: RadarType and Obscuration Level

3.5 Document Review Qualitative Results

This section presents the qualitative findings from a comprehensive review of 60

documents aligned with the four experimental configurations of this study. The purpose of this analysis was to complement the quantitative DOE results by identifying operational insights, recurring themes, and emerging challenges from the literature. Sources included peer-reviewed journal articles, government reports, white papers, and doctoral dissertations published within the past five years.

A thematic analysis approach was employed to extract patterns and concepts related to detection feasibility, system performance, and implementation barriers. The findings validated the DOE simulation configurations and informed refinements to the selection of key variables, ensuring consistency with real-world performance.

Several notable qualitative insights emerged. First, there is a clear trend toward technological convergence in areas such as artificial intelligence and multi-sensor data fusion. Second, persistent limitations remain in cyber-resilience protocols, particularly regarding intrusion detection and signal integrity. Third, systemic detection challenges were observed in cluttered or obstructed airspace environments, reinforcing the DOE findings on radar and surveillance vulnerabilities.

The subsections that follow (3.5.1–3.5.4) provide configuration-specific themes and supporting insights. These discussions offer contextual grounding for the simulation outcomes and highlight how UAV-ATC integration issues manifest across technology, operational, and regulatory dimensions.

3.5.1 UAV Characteristics Qualitative Results

Key qualitative themes extracted from 15 reviewed documents for UAV Characteristics [3]–[17] center around four major areas: detection profiles, RCS modeling, geometric influence on detectability, and stealth design implications. These studies provide foundational insights into how UAV physical and operational characteristics influence system performance and airspace safety.

A common theme across several documents [3], [5], [7], and [8] was the difficulty of detecting small UAVs due to low RCS signatures. Research has shown that both shape and material composition directly impact radar observability, with some UAV designs exhibiting RCS values below −10 dBm^2, rendering them nearly invisible to conventional ATC radar systems. For example, [9] and [10] modeled different UAV geometries and showed that angular positioning and composite surfaces significantly reduce detection rates under certain conditions.

Multiple documents also emphasized the importance of UAV configuration on system safety scoring and operational risk. Studies such as [6], [11], and [13] highlighted how multirotor designs present different tracking challenges compared to fixed-wing platforms, due to hovering capabilities and unpredictable flight patterns. These findings align with the quantitative simulations performed in this study, which assigned safety scores based on airframe type and communication mode.

Trends noted across the reviewed literature suggest that UAV detectability is strongly linked to both geometry and

communication type. Fixed-wing UAVs with minimal broadcasting are consistently described as the most difficult to track, while multirotors equipped with Remote ID or ADS-B provide higher visibility but introduce vulnerabilities to spoofing and data interception [12], [14]–[15]. Collectively, the qualitative findings reinforce the simulation results, demonstrating that UAV characteristics shape not only operational performance but also broader safety and security considerations within ATC environments.

3.5.2 Surveillance Technologies Qualitative Results

A synthesis of the 15 reviewed documents on Surveillance Technologies [18]–[32] reveals four dominant qualitative themes: sensor fusion responsiveness, trust in AI-enabled systems, persistent coverage limitations, and data transmission latency under operational constraints.

Multi-sensor fusion was frequently identified as essential for overcoming blind spots and weaknesses of standalone systems [18], [20], [22], and [23]. Fusion techniques that combined visual, infrared, and radar inputs demonstrated improved detection accuracy. However, performance varied depending on architecture. Centralized fusion models were slower but more reliable, while edge-based approaches improved latency but introduced occasional classification errors [19], [25].

Trust in AI-based surveillance decision-making also emerged as a critical factor [21], and [26]–[27]. While AI-enhanced systems provided predictive alerting and faster recognition, concerns persisted about bias and misclassification in non-standard conditions. Training datasets were often cited as insufficiently representative of real-world complexity, especially in crowded or ambiguous environments [24], [28].

Coverage gaps caused by terrain, weather, and urban structures remained significant obstacles [29], [30], and [32]. These factors aligned closely with quantitative findings in Section 3.2, where detection accuracy varied across sensor and fusion types. AI-based fusion generally outperformed manual and rule-based methods in terms of average scores but exhibited greater variability due to data integrity dependencies.

Finally, communication latency was repeatedly identified as a barrier to effective surveillance. Studies such as [31] documented how wireless or satellite data transmission delays reduced the reliability of real-time tracking. These findings reinforce the need for robust communication infrastructure to complement advanced sensor systems.

Collectively, the literature supports the simulation design and highlights the importance of balancing technological advances with operational reliability. While AI and sensor fusion strategies enhance detection, they also introduce new dependencies that must be managed through system design, training, and validation.

3.5.3 Cybersecurity Vulnerabilities Qualitative Results

The qualitative review of 15 cybersecurity-focused documents [33]–[47] identified recurring themes related to threat classification, system resilience, encryption, and emerging defense strategies in UAV and air traffic control contexts.

Multiple studies [33], [35], [38], and [44] developed taxonomies of UAV-specific cyber threats, including spoofing, jamming, denial-of-service, and hijacking. These works consistently emphasized that UAV communications, often dependent on unsecured radio frequencies and GPS, are highly vulnerable to spoofing and signal injection. Real-world cases of UAV redirection through spoofing were documented in [33], reinforcing the simulation scenarios analyzed in this study.

System resilience, particularly recovery time and the capacity to isolate or neutralize threats, was a critical theme in [34], [36], and [42]. These studies benchmarked IDS and compared rule-based approaches to AI-driven platforms. They reported that AI-based IDS solutions detected new attack signatures more rapidly, though interpretability remained limited, raising concerns about operator trust.

The role of encryption and authentication protocols was emphasized in [37], [40], and [45]. These works confirmed the importance of end-to-end secure communications for both command and telemetry data, validating the simulation assumption that encryption improves resilience. They also noted the trade-offs with latency and processing requirements, particularly for small UAVs with constrained onboard computing.

Finally, deception-based strategies were highlighted in [39], [41], and [46], including fake data injection, and moving target defense. These approaches showed potential to improve resilience scores but required extensive tuning and modeling. This aligns with the simulated findings where AI-based safeguards achieved higher disruption resistance but also displayed variability in performance.

The convergence of these findings strengthens the results of the DOE simulations. Variations in resilience scores across safeguard and threat conditions are consistent with documented real-world limitations and advances. Collectively, the literature validates the importance of hybrid defense strategies that combine detection, recovery, and deception for UAV integration into dense, cyber-sensitive airspace environments.

3.5.4 Radar Detection Performance Qualitative Results

The qualitative review of 15 references [48]–[62] provided insights into how traditional and emerging radar technologies perform in UAV tracking and surveillance. These findings reinforce the quantitative results and highlight persistent challenges in detection reliability, clutter mitigation, and system adaptability.

The literature consistently distinguished between PSR and multistatic radar systems [48], [51], [56], and [60]. While PSR remains established in air traffic control, it is limited in detecting small UAVs with low RCS. Some studies proposed using reflector elements to increase UAV radar visibility [61], aligning with adjustments modeled in the DOE configurations.

By comparison, multistatic radar systems demonstrated stronger performance in cluttered or obstructed environments [49], [55], and [59]. These architectures, leveraging multiple geographically distributed transmitters and receivers, improved detection accuracy and resilience to multipath interference. Several studies also highlighted the ability of multistatic networks to track UAVs employing stealth materials or irregular flight paths, which pose challenges for monostatic systems [52], [57].

AI-enabled radar platforms emerged as a promising trend across the reviewed literature [53], [58], and [62]. Advanced processing techniques, including real-time beam steering and adaptive clutter filtering, showed potential to increase sensitivity without proportionally raising false alarms. However, operational scalability and deployment costs remain significant barriers, with authors stressing the need for incremental adoption and integration with existing PSR infrastructure [50], [54].

Overall, the qualitative review supports the quantitative findings, indicating that multistatic and AI-augmented radar systems offer the greatest potential for addressing the detection gaps associated with small UAVs. Nonetheless, the transition from traditional to distributed and intelligent radar networks will require both technological innovation and significant investment in infrastructure.

4.0 Findings and Synthesis

This section presents a comprehensive analysis of results drawn from both the quantitative simulations and the qualitative document reviews. The discussion integrates findings across the four experimental configurations: UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance. Together, these analyses provide a holistic understanding of the primary drivers influencing system performance and the challenges associated with integrating unmanned aerial vehicles into modern air traffic control systems.

The synthesis highlights areas of convergence where both simulations and document reviews identified consistent trends, such as the superior performance of AI-based methods in improving detection, fusion, and resilience. It also identifies areas of divergence, where real-world documents raised concerns about latency, human factors, or infrastructure costs that were not fully represented in the simulations. These divergences reveal practical limitations that must be addressed when applying simulation results to operational contexts.

The combined approach strengthens the internal and external validity of the study. Quantitative models provide structured evidence of statistical significance, while qualitative insights offer thematic explanations and highlight factors difficult to capture in simulations, such as regulatory interpretation or long-term adaptation of operators and systems. This integration enables a balanced perspective that not only explains performance outcomes but also contextualizes them within broader aviation practices.

Taken together, the findings indicate that while technological innovations offer measurable improvements in safety, surveillance, cybersecurity, and radar performance, successful UAV integration will require strategies that are adaptive, layered, and sensitive to operational realities. These results create a strong foundation for the targeted recommendations and implications presented in subsequent chapters.

4.1 Key Findings by Configuration

The results from both quantitative simulations and qualitative document analysis revealed several important patterns across the four configurations evaluated. Each configuration (UAV Characteristics, Surveillance Technologies, Cybersecurity Vulnerabilities, and Radar Detection Performance) revealed distinct performance drivers and vulnerabilities that influence the overall reliability of UAV–ATC integration.

The analysis confirmed that UAV Characteristics directly affect detectability and communication reliability, while Surveillance Technologies determine how effectively multi-sensor systems enhance target discrimination and resilience. Cybersecurity considerations were shown to be a major limiting factor, as the ability of system safeguards to withstand threats such as spoofing or denial-of-service attacks varied significantly across experimental conditions. Radar Detection Performance highlighted persistent limitations in traditional systems when tasked with small UAVs operating in cluttered environments.

These findings establish a clear linkage between statistical outcomes, thematic insights from supporting literature, and the degree of alignment between modeled simulations and operational realities. Together, they provide a strong evidence base for assessing how technology adoption, safeguard implementation, and radar

modernization contribute to safe and resilient UAV integration in controlled airspace operations.

4.1.1 UAV Characteristics Key Findings

The quantitative analysis [3]–[17] showed that rotary-wing UAVs with encrypted communication links consistently achieved the highest Composite Safety Scores. Across replications, encrypted rotary UAVs averaged above 28 out of 30, with standard deviations below 1.2. These results demonstrate strong reliability and statistical confidence in their superior performance. The findings indicate a clear synergy between rotary-wing maneuverability and the resilience provided by secure communication links. Fixed-wing UAVs, while offering greater range and endurance, displayed higher variability in performance. When operating with unencrypted links, they were particularly vulnerable to interference and interception, which lowered their safety scores.

Qualitative evidence reinforced these patterns by highlighting several recurring challenges. Small UAVs remain difficult to detect due to their low RCS and the increasing use of stealth-oriented geometries [5], [9], [14]. Advances in radar-absorbent materials further reduce visibility to conventional ATC systems [12]. These design factors, while advantageous in defense contexts, introduce new complications for civil airspace safety.

A recurring theme in the literature was the importance of communication security in maintaining mission continuity. Encrypted links were shown to be indispensable for UAV resilience in contested electromagnetic environments [10], [15]. Unencrypted systems were repeatedly cited as vulnerable to jamming, spoofing, or interception, raising the risk of loss of control and potential safety incidents. Thus, communication security is not simply a technological enhancement but a baseline requirement for safe UAV integration.

Taken together, these results underscore a central paradox. Rotary-wing UAVs with encrypted links deliver the highest safety scores quantitatively, yet these platforms also embody qualitative risks due to reduced detectability. This paradox places new demands on ATC systems, requiring multi-sensor integration strategies capable of compensating for the limited visibility of low-RCS platforms.

The overall conclusion is that UAV safety and resilience are shaped not by platform type alone but by the interaction of maneuverability, detectability, and communication reliability. Encrypted rotary UAVs illustrate how strengths in secure communication can offset vulnerabilities in radar visibility. For civil aviation, this highlights the need for layered surveillance and communication frameworks where safety is preserved even under stealth and contested conditions. Policies mandating encryption, supported by technologies able to track low-RCS targets, will be essential to ensure safe UAV integration into shared airspace.

4.1.2 Surveillance Technologies Key Findings

The quantitative analysis [18]–[32] demonstrated that multi-sensor integration significantly enhances UAV surveillance effectiveness. Configurations that combined visual and infrared (IR) sensors using AI-based fusion algorithms produced the highest Composite Surveillance Scores, averaging 27.8 out of 30 with minimal variability. Both main effects and interaction terms were statistically significant ($p < 0.01$). In contrast, single-sensor configurations showed reduced reliability: visual-only systems were limited under variable lighting and weather conditions, while IR-only systems struggled when thermal signatures overlapped with environmental background clutter. These results indicate that AI-driven fusion systems dynamically optimize sensor weighting, providing a more resilient detection capability than either sensor could achieve alone.

The qualitative review reinforced these findings. Several studies reported that AI-enabled multi-sensor platforms improved threat detection and classification by processing diverse input streams in real time [19], [22], and [26]. These insights support the conclusion that fusion approaches substantially increase operational resilience in unpredictable environments. However, consistent concerns emerged regarding AI trustworthiness. Sources cited the opaque nature of advanced fusion algorithms, which complicates verification and certification for aviation safety [25], [30]. Latency was also identified as a limitation, particularly when rapid detection was required in dense or contested airspace.

Rule-based fusion methods received specific criticism for failing to adapt under sudden visibility changes, such as fog formation, or adversarial countermeasures designed to mask IR signatures [20], [28]. AI-based systems, in contrast, demonstrated adaptive re-weighting that preserved performance in such conditions. This adaptive behavior underscores their value but also highlights the importance of developing verification frameworks that improve algorithm transparency and reliability.

Synthesizing these findings, the convergence of quantitative and qualitative findings confirms that AI-based fusion systems offer measurable improvements in detection accuracy and resilience. Yet, operational adoption will require addressing system latency, ensuring redundancy, and creating standards for transparent AI validation. These steps are essential for regulatory approval and for building institutional trust.

Ultimately, AI-supported multi-sensor integration stands as the most promising pathway toward reliable UAV surveillance in safety-critical airspace environments. Successful deployment will depend on advancing both the technical maturity of fusion systems and the regulatory frameworks that govern their use.

4.1.3 Cybersecurity Vulnerabilities Key Findings

The cybersecurity simulations [33]–[47] demonstrated that AI-based IDS provided the strongest defense against spoofing and jamming attacks. Configurations with adaptive AI consistently achieved the highest Cyber Resilience Scores, often exceeding 27.5 out of 30, with low variability across replications. Statistical analysis confirmed these outcomes as robust, with main effects showing strong significance ($p < 0.01$). On average, AI-based safeguards outperformed rule-based IDS by more than 2.5 points, reflecting their ability to identify attack patterns beyond pre-defined signatures and to adapt to evolving threats in real time.

The qualitative review reinforced these findings. Taxonomies of cyber threats [35], [38] outlined vulnerabilities in UAV-ATC networks, including signal spoofing, denial-of-service, data exfiltration, and command-link hijacking. Resilience models emphasized the necessity of layered defenses that include redundancy, encryption, and adaptive detection mechanisms [41], [44]. Within this framework, AI-based IDS emerged as a decisive enabler of resilience, particularly by reducing detection latency and automating mitigation responses before system-wide failures could occur [37], [45].

Several limitations were noted. Documents highlighted risks of over-reliance on opaque AI systems without adequate transparency or validation [43]. Black-box algorithms complicate certification and regulatory approval, especially in aviation contexts where safety requires explainability and accountability. Additionally, adversaries may attempt to exploit AI models through adversarial inputs or data poisoning, underscoring the need for validated fallback protocols to preserve system continuity when IDS performance degrades.

A recurring recommendation was the integration of encrypted redundancy within communication architectures. By combining strong encryption with AI-enabled detection, UAV systems can maintain mission continuity even under sustained attack. The literature also emphasized that resilience should extend beyond detection, recommending proactive threat-hunting and continuous vulnerability assessments.

In synthesis, both simulations and document reviews confirmed that AI-based IDS substantially advance the defense of UAV-ATC systems. However, successful operational integration will depend on balancing adaptability, transparency, and redundancy. Developing hybrid approaches that combine the adaptability of AI with explainable frameworks and validated fallback mechanisms will be critical for building trust and resilience in real-world air traffic control environments.

4.1.4 Radar Detection Performance Key Findings

The radar detection simulations [48]–[62] demonstrated that multistatic radar systems enhanced with AI-driven signal processing achieved the highest Composite Detection Scores, averaging above 26.8 out of 30 across replications. Analysis of variance indicated that both main effects and interaction effects were statistically significant ($p < 0.01$), particularly between radar type and operational environment. Monostatic radar systems consistently underperformed in urban and cluttered settings, where multipath interference and masking degraded their ability to reliably track UAVs. By contrast, multistatic systems maintained more stable detection accuracy, especially when coupled with adaptive processing methods.

The qualitative review reinforced these findings, highlighting the advantages of multistatic radar architectures in clutter rejection, target resolution, and resilience against stealth-oriented UAV profiles [50], [56], and [60]. Several studies noted that traditional monostatic radars, though cost-effective, lacked the spatial diversity necessary to reliably detect low RCS targets in complex environments. Multistatic radar configurations, leveraging geographically distributed receivers, were consistently described as more effective in identifying UAVs with stealth features or radar-absorbent materials.

An important practical enhancement discussed in the literature was the use of radar reflectors to artificially increase UAV RCS, thereby improving their visibility to both monostatic and multistatic systems [61]. This approach was identified as particularly valuable in cooperative scenarios, such as regulated airspace integration, where UAVs are expected to actively contribute to their own detectability. At the same time, documents emphasized the continuing need for non-cooperative detection strategies, since adversarial UAVs are unlikely to employ cooperative reflectors.

The integration of AI into radar platforms emerged as a critical enabler of improved detection. AI-augmented radars demonstrated capabilities such as real-time beam steering, adaptive gain control, and enhanced clutter suppression [52], [59]. These advancements allowed radars to dynamically adapt to changing operating environments and maintain consistent target tracking performance. However, several sources highlighted the challenges of scalability and cost when considering nationwide deployment of advanced multistatic networks, particularly regarding the infrastructure requirements for synchronization, communication bandwidth, and centralized data fusion [62].

Taken together, both the quantitative results and qualitative reviews point to a clear trajectory: multistatic, AI-augmented radar systems represent the most promising pathway for achieving reliable UAV detection in both cooperative and non-cooperative scenarios. Nevertheless, their adoption will require substantial investment in infrastructure, careful balancing of cost against coverage,

and policy frameworks that encourage integration with existing surveillance assets.

4.2 Synthesis Across All Configurations

The cross-configuration analysis identified several unifying patterns that highlight both opportunities and challenges for UAV–ATC integration.

AI-enhanced safeguards consistently outperformed rule-based or legacy approaches. In surveillance, intrusion detection, and radar signal processing, AI-driven methods provided superior adaptability to changing environments, improved classification accuracy, and greater resilience under adversarial conditions. These findings demonstrate that the modernization of air traffic systems will require systematic adoption of AI capabilities in both cooperative and non-cooperative monitoring layers.

Data fusion also emerged as a critical enabler of situational awareness. Integrating information from multiple sources, including visual and infrared sensors, as well as communication diagnostics, reduced single-point vulnerabilities and created redundancy that enhanced overall system stability. Fusion techniques enabled systems to remain effective under variable weather conditions, complex electromagnetic environments, and shifting UAV profiles, confirming the value of modular architectures that can synthesize diverse inputs in real time.

Radar systems remained essential for non-cooperative detection. Multistatic radar consistently outperformed monostatic radar in clutter rejection and detection of low-RCS UAVs. However, multistatic systems require complex synchronization and substantial infrastructure investments. These results confirm radar's indispensable role in countering UAVs that do not rely on cooperative protocols.

The analysis further indicated that effective integration requires configuration-specific strategies rather than universal solutions. UAV–ATC system design depends on the interplay between hardware, software, environmental conditions, and threat type. For example, encrypted communications enhanced safety scores but required strong cybersecurity safeguards, while radar reflectors improved detectability only when UAVs operated cooperatively. These findings highlight adaptability, redundancy, and layered defenses as essential principles for future system design.

In summary, results across all four configurations suggest that next-generation ATC systems must adopt AI-augmented, fusion-driven architectures that combine UAV characteristics, surveillance technologies, cybersecurity measures, and radar platforms into cohesive frameworks. The central challenge is not technical feasibility, which has been demonstrated, but the alignment of infrastructure, operational standards, and policy frameworks to enable scalable implementation.

4.3 Integration of Qualitative and Quantitative Findings

The triangulation of quantitative simulations with document-based qualitative analysis revealed strong convergence across multiple domains of UAV–ATC integration. AI-enhanced configurations consistently achieved higher levels of surveillance responsiveness and cybersecurity resilience [3]–[17], [33]–[47]. These outcomes confirm the effectiveness of machine learning for real-time threat detection, adaptive data fusion, and decision support in complex environments. The alignment between simulated and qualitative results reinforces the validity of the experimental design and supports its broader application in ATC modernization.

Qualitative reviews corroborated the simulation findings for radar performance. Sources highlighted persistent challenges related to RCS variability, clutter rejection, and micro-Doppler effects in urban and terrain-dense environments [48]–[62]. These issues directly paralleled the degradation in detection performance observed under simulated conditions, underscoring the realism of the modeled scenarios.

However, divergences were also identified. Simulations assumed idealized responses with negligible latency, while the literature underscored practical constraints during real-world operations. These included encryption delays, IDS latency, and synchronization challenges within distributed sensor networks [35], [41], and [44]. Such differences emphasize the need for future simulations to incorporate latency effects, false positives, and communication overhead.

Taken together, this synthesis enhances both the credibility and the interpretive depth of the study. Simulations provide clarity on performance trends under controlled conditions, while qualitative analysis grounds these trends in operational realities. The integration demonstrates that robust UAV–ATC modernization requires more than technological advancement. It demands careful attention to deployment constraints, infrastructure scalability, and policy frameworks to ensure resilient and reliable adoption.

5.0 Future Research

The research in this dissertation provides a foundation for evaluating UAV integration into ATC environments, yet the complexity of modern airspace means that continued investigation is necessary. Future research should focus on expanding the design of experiments to include factors such as human–machine teaming, controller workload, and decision-support reliability, which were beyond the scope of this study but are critical to real-world ATC operations.

Another direction lies in moving beyond simulation-based analysis to incorporate live operational data from FAA test ranges, National Aeronautics and Space Administration

(NASA) Unmanned Aerial System (UAS) Traffic Management demonstrations, and urban air mobility trials. Blending synthetic and real-world datasets would strengthen the validity of results and enhance predictive accuracy. Likewise, longitudinal studies should be pursued to capture the evolving effects of UAV integration, including safety culture shifts, controller adaptation, and system resilience over time. Comparative studies across different ATC jurisdictions, such as the FAA, ICAO, and European Union Aviation Safety Agency (EASA), would add further depth by revealing how regulatory diversity influences adoption and outcomes.

Emerging advances in artificial intelligence also offer a promising path forward. Predictive analytics, anomaly detection, and reinforcement learning could be leveraged to improve conflict resolution and system efficiency. At the same time, these advances raise new questions about cybersecurity, trust, and human oversight, which future studies must address. The regulatory and ethical dimensions remain equally important: policymakers will need evidence to determine how quickly mandates such as Remote ID should be implemented, how cybersecurity standards should evolve, and how equitable access to airspace can be ensured.

3Finally, UAV–ATC modernization should be studied in the context of broader aviation initiatives, including NextGen modernization, urban air mobility, and even space traffic management. Interoperability across these domains will be critical as airspace becomes increasingly crowded.

REFERENCES

[1] A. Renault and M. Johnson, "Navigating the Skies: The Necessity for Upgrading Air Traffic Control Systems," International Research Journal of Engineering and Technology (IRJET), vol. 11, no. 10, pp. 626–632, Oct. 2024. [Online]. Available: https://www.irjet.net/archives/V11/i10/IRJET-V11I1091.pdf

[2] A. Renault, "Seeing the Unseen: A Literature Review of UAV Detection Gaps and Surveillance and Security Solutions for ATC Modernization," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 5, pp. 1541–1551, May 2025. [Online]. Available: https://www.irjet.net/archives/V12/i5/IRJET-V12I5233.pdf

[3] D. Sacharny, *A lane-based approach to large-scale unmanned aircraft systems traffic management*. Ph.D. dissertation, Univ. of Utah, Salt Lake City, UT, USA, 2022. [Online]. Available: https://www.proquest.com/dissertations-theses/lane-based-approach-large-scale-unmanned-aircraft/docview/2735900420/se-2

[4] S. U. Gunawardana, *A rule-based dialog management system for integration of unmanned aerial systems into the national airspace system*. Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2012. [Online]. Available: https://www.proquest.com/dissertations-theses/rule-based-dialog-management-system-integration/docview/2454363866/se-2

[5] S. L. Brunton, J. N. Kutz, K. Manohar, A. Y. Aravkin, K. A. Morgansen, J. Klemisch, N. Goebel, J. Buttrick, J. Poskin, A. W. Blom-Schieber, T. A. Hogan, and D. C. McDonald, "Data-driven aerospace engineering: Reframing the industry with machine learning," *AIAA J.*, vol. 59, no. 6, pp. 1–26, 2021. [Online]. Available: https://doi.org/10.2514/1.j060131

[6] C. J. Boyer, *Air traffic leadership perceptions on the use of machine learning for air traffic safety*, Ph.D. dissertation, Univ. of the Cumberlands, Williamsburg, KY, USA, 2020. [Online]. Available: https://www.proquest.com/dissertations-theses/air-traffic-leadership-perceptions-on-use-machine/docview/2559697262/se-2

[7] A. Hunter, *An open source real-time controller for resource-constrained autonomous vehicles and systems*, Ph.D. dissertation, Univ. of California, Santa Cruz, CA, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/open-source-real-time-controller-resource/docview/2812351498/se-2

[8] A. S. Lale, *Learning and control of dynamical systems*, Ph.D. dissertation, California Institute of Technology, Pasadena, CA, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/learning-control-dynamical-systems/docview/2866350323/se-2

[9] A. Hicks, *A generalizable method and case application for development and use of the Aviation Systems–Trust Survey (AS-TS)*, Ph.D. dissertation, Mississippi State Univ., Starkville, MS, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/generalizable-method-case-application-development/docview/2814746979/se-2

[10] C. Conte, S. V. Supplizi, G. De Alteriis, A. Mele, G. Rufino, and D. Accardo, "Using drone swarms as a countermeasure of radar detection," *J. Aerosp. Inf. Syst.*, vol. 20, no. 2, pp. 70–80, Feb. 2023. [Online]. Available: https://doi.org/10.2514/1.i011131

[11] H. Peng, *Action Recognition in Intelligent Systems*, Ph.D. dissertation, Northern Arizona Univ., Flagstaff, AZ, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/action-recognition-intelligent-systems/docview/2786310294/se-2

[12] A. Reyes-Muñoz, C. Barrado, E. Pastor, and P. Royo, "ATC human factors involved in RPAS contingency management in non-segregated airspace," *Applied Sciences*, vol. 13, no. 3, p. 1408, 2023. [Online]. Available: https://doi.org/10.3390/app13031408

[13] N. Almerza, *Agent-based modeling to determine the risk to a swarm of unmanned aerial vehicles under an adversarial artificial intelligence attack*, Ph.D. dissertation, Marymount Univ., Arlington, VA, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/agent-based-modeling-determine-risk-swarm/docview/2828097307/se-2

[14] P. Domogala and P. Marien, *100 years of air traffic control*. International Federation of Air Traffic Controllers' Associations, 2022. [Online]. Available: https://ifatca.org/100-years-air-traffic-control/

[15] Alliance for Aviation Across America, *Air traffic control modernization and NextGen*. Washington, DC, USA:

Aviation Across America, 2023. [Online]. Available: https://www.aviationacrossamerica.org

[16] D. Han, Q. Yang, and R. Wang, "Three-dimensional obstacle avoidance for UAV based on reinforcement learning and RealSense," *The Journal of Engineering*, vol. 2020, no. 3, pp. 540–544, Mar. 2020. [Online]. Available: https://doi.org/10.1049/joe.2019.1167

[17] M. Song, Z. Liang, Y. Huo, and R. Liu, "Line-of-sight probability for UAV communications in 3D grid urban streets," *Electronics Letters*, vol. 59, no. 5, p. e12979, May 2023. [Online]. Available: https://doi.org/10.1049/ell2.12979

[18] A. la Cour-Harbo and H. Schiøler, "Probability of low-altitude midair collision between general aviation and unmanned aircraft," *Risk Analysis*, vol. 39, no. 11, pp. 2499–2513, Nov. 2019. [Online]. Available: https://doi.org/10.1111/risa.13368

[19] A. Lockhart, A. While, S. Marvin, M. Kovacic, N. Odendaal, and C. Alexander, "Making space for drones: The contested reregulation of airspace in Tanzania and Rwanda," *Transactions of the Institute of British Geographers*, vol. 46, no. 4, pp. 850–865, Dec. 2021. [Online]. Available: https://doi.org/10.1111/tran.12448

[20] Y. Zhou, M. Hu, L. Yang, and Y. Wang, "Autonomous and collaborative trajectory planning for traffic complexity management," *IET Intelligent Transport Systems*, vol. 17, no. 8, pp. 992–1008, Aug. 2023. [Online]. Available: https://doi.org/10.1049/itr2.12321

[21] F. Fabra, *et al.*, "Collision-free cooperative unmanned aerial vehicle protocols for sustainable aerial services," *IET Smart Cities*, vol. 4, no. 4, pp. 231–238, Dec. 2022. [Online]. Available: https://doi.org/10.1049/smc2.12028

[22] S. Benfriha, *et al.*, "FUBA: A fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad-hoc networks," *IET Networks*, pp. 1–13, 2023. [Online]. Available: https://doi.org/10.1049/ntw2.12108

[23] A. Guillen-Perez and M.-D. Cano, "Intelligent IoT systems for traffic management: A practical application," *IET Intelligent Transport Systems*, vol. 15, pp. 273–285, 2021. [Online]. Available: https://doi.org/10.1049/itr2.12021

[24] S. J. Frantzman, "Iran's drone war over Iraq is getting dangerous. An incident Wednesday night highlights the dangers of UAV proliferation and Iran's increasing use of attack drones across the Middle East," *Jerusalem Post*, Jun. 10, 2022. [Online]. Available: https://www.proquest.com/newspapers/iran-s-drone-war-over-iraq-is-getting-dangerous/docview/2676091457/se-2

[25] X. Yan, T. Fu, H. Lin, F. Xuan, Y. Huang, Y. Cao, H. Hu, and P. Liu, "UAV detection and tracking in urban environments using passive sensors: A survey," *Applied Sciences*, vol. 13, no. 20, p. 11320, 2023. [Online]. Available: https://doi.org/10.3390/app132011320

[26] [26] Fuhrmann, M., & Horowitz, M. C. (2017). Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles. International Organization, 71(2), 397-418. [Online]. Available: https://doi.org/10.1017/s0020818317000121

[27] R. T. Q. Overmyer, *"Democratization of aviation": A content analysis of unmanned aerial systems policy and proliferation*. Ph.D. dissertation, California State Univ., Sacramento, CA, USA, 2023. [Online]. Available: https://www.proquest.com/dissertations-theses/democratization-aviation-content-analysis/docview/2854824094/se-2

[28] C. Xia, Y. Zhou, X. Xu, J. Gong, and H. Zhang, "A conflict risk analysis of MAV/UAV flight in shared airspace," *Int. J. Aerosp. Eng.*, vol. 2021, pp. 1–14, 2021. [Online]. Available: https://doi.org/10.1155/2021/1692896

[29] H. Zhang, Y. Fei, J. Li, L. Bowen, and H. Liu, "Method of vertiport capacity assessment based on queuing theory of unmanned aerial vehicles," *Sustainability*, vol. 15, no. 1, p. 709, 2023. [Online]. Available: https://doi.org/10.3390/su15010709

[30] A. Mohamed, M. Marino, S. Watkins, *et al.*, "Gust encountered by flying vehicles in proximity to buildings," *Drones*, vol. 7, no. 1, p. 22, 2023. [Online]. Available: https://doi.org/10.3390/drones7060365

[31] B. Yu and T. Lee, "Modular reinforcement learning for a quadrotor UAV with decoupled yaw control," *IEEE Robotics and Automation Letters*, vol. 10, no. 1, pp. 572–579, Jan. 2025. [Online]. Available: https://doi.org/10.1109/lra.2024.3511412

[32] C. Ramirez-Atencia, V. Rodríguez-Fernández, A. Gonzalez-Pardo, and D. Camacho, "New artificial intelligence approaches for future UAV ground control stations," in *Proc. IEEE Congress on Evolutionary Computation (CEC)*, Donostia, Spain, 2017, pp. 2775–2782. [Online]. Available: https://doi.org/10.1109/cec.2017.7969645

[33] R. N. Lea, "Automated space vehicle control for rendezvous proximity operations," *Telematics and Informatics*, vol. 5, no. 3, pp. 179–185, 1988. [Online]. Available: https://doi.org/10.1016/s0736-5853(88)80022-4

[34] A. Biswas, A. K. Behera, A. K. Sahoo, D. Panda, S. Nayak, and S. Mishra, "State-of-the-art review on recent advancements on lateral control of autonomous vehicles," *IEEE Access*, vol. 10, pp. 114759–114786, 2022. [Online]. Available: https://doi.org/10.1109/access.2022.3217213

[35] J. F. Hanaway and R. W. Moorehead, *Space Shuttle Avionics System*. Washington, DC, USA: National Aeronautics and Space Administration, Office of Management, Scientific and Technical Information Division, 1989. [Online]. Available: https://ntrs.nasa.gov/api/citations/19900015844/downloads/19900015844.pdf

[36] R. A. Paielli and H. Erzberger, "Trajectory specification for terminal airspace: Conflict detection and resolution," *Journal of Air Transportation*, vol. 27, no. 2, pp. 51–60, 2019. [Online]. Available: https://doi.org/10.2514/1.d0132

[37] J. Guo, S. S. Ge, X. Zhu, and F. Zhao, "Modeling of ATC operation process based on extended colored Petri net," *International Journal of Performability Engineering*, vol. 15, no. 9, pp. 2522–2533, 2019. [Online]. Available: https://doi.org/10.23940/ijpe.19.09.p26.25222533

[38] A. Balaban, S. Berbente, A. Neamtu, G.-L. Stroe, E. Costea, I.-B. Stefanescu, I.-C. Andrei, and I. Popescu, "Case study of TCAS implementation in modern FMS," *INCAS Bulletin*, vol. 15, no. 2, pp. 11–19, 2023. [Online]. Available: https://doi.org/10.13111/2066-8201.2023.15.2.2

[39] F. C. Gomes Sampaio, R. N. Costa Filho, and M. Xavier Guterres, "Modeling resilience of air traffic management systems based on complex networks," *Journal of Aerospace Technology & Management*, vol. 14, no. 1, pp. 1–18, 2022. [Online]. Available: https://doi.org/10.1590/jatm.v14.1273

[40] A. Neamtu, A. Balaban, S. Berbente, G.-L. Stroe, E. Costea, I.-B. Stefanescu, I.-C. Andrei, and I. Popescu, "Air traffic control software implemented in RADAR," *INCAS Bulletin*, vol. 15, no. 2, pp. 59–65, 2023. [Online]. Available: https://doi.org/10.13111/2066-8201.2023.15.2.6

[41] F. P. Moreno *et al.*, "Determination of air traffic complexity most influential parameters based on machine learning models," *Symmetry*, vol. 14, no. 12, p. 2629, 2022. [Online]. Available: https://doi.org/10.3390/sym14122629

[42] G. Borghini, G. Di Flumeri, P. Aricò, N. Sciaraffa, S. Bonelli, M. Ragosta, P. Tomasello, F. Drogoul, U. Turhan, B. Acikel, A. Ozan, J. P. Imbert, G. Granger, R. Benhacene, and F. Babiloni, "A multimodal and signals fusion approach for assessing the impact of stressful events on air traffic controllers," *Scientific Reports*, vol. 10, no. 1, pp. 1–18, 2020. [Online]. Available: https://doi.org/10.1038/s41598-020-65610-z

[43] A. Vidović, T. Mihetec, B. Wang, and I. Štimac, "Operations of drones in controlled airspace in Europe," *International Journal for Traffic & Transport Engineering*, vol. 9, no. 1, pp. 38–52, 2019. [Online]. Available: https://doi.org/10.7708/ijtte.2019.9(1).04

[44] F. Trapsilawati, L. Fan, and Y. Liu, "Ergonomics considerations in air traffic conflict detection and resolution," *International Journal of Technology*, vol. 14, no. 4, pp. 898–910, 2023. [Online]. Available: https://doi.org/10.14716/ijtech.v14i4.5908

[45] F. Lu, Q. Wang, J. Teng, Y. Kang, and B. Liu, "Analysis of the features of air traffic controllers' eye movements," *International Journal of Performability Engineering*, vol. 15, no. 12, pp. 3262–3270, 2019. [Online]. Available: https://doi.org/10.23940/ijpe.19.12.p18.32623270

[46] J. Zhou and C. Kwan, "A high performance contingency planning system for UAVs with lost communication," in *Proc. IEEE Int. Conf. Prognostics and Health Management (ICPHM)*, Seattle, WA, USA, 2018, pp. 1–8. [Online]. Available: https://doi.org/10.1109/icphm.2018.8448926

[47] K. Park, J. Rhee, M.-H. Shin, and W. Hur, "A novel CQI feedback channel for cellular UAV system," in *Proc. Int. Conf. Advanced Technologies for Communications (ATC)*, Hanoi, Vietnam, 2019, pp. 84–88. [Online]. Available: https://ieeexplore.ieee.org/document/8924562

[48] D. V. Vu, T. V. Pham, and D. T. Nguyen, "A path-following guidance algorithm for fixed-wing UAV swarms on a decentralized network," in *Proc. Int. Conf. Advanced Technologies for Communications (ATC)*, Ha Noi, Vietnam, 2022, pp. 286–291. [Online]. Available: https://doi.org/10.1109/atc55345.2022.9942994

[49] C. Hong and D. Shi, "A control system architecture with cloud platform for multi-UAV surveillance," in *Proc. IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, 2018, pp. 1095–1097. [Online]. Available: https://doi.org/10.1109/smartworld.2018.00190

[50] T. Xu, Z. Yu, Y. Song, J. Ren, H. Cui, and B. Guo, "Joint computing resource scheduling and task priority selection in UAV-enabled MEC," in *Proc. 2022 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Haikou, China, 2022, pp. 73–80. [Online]. Available: https://doi.org/10.1109/smartworld-uic-atc-scalcom-digitaltwin-pricomp-metaverse56740.2022.00037

[51] J. Liu, C. Hu, J. Zhou, and W. Ding, "Object detection algorithm based on lightweight YOLOv4 for UAV," in *Proc. 2022 7th Int. Conf. Intelligent Computing and Signal Processing (ICSP)*, Xi'an, China, 2022, pp. 425–429. [Online]. Available: https://doi.org/10.1109/icsp54964.2022.9778666

[52] C. Hong and D. Shi, "A control system architecture with cloud platform for multi-UAV surveillance," in *Proc. 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, 2018, pp. 1095–1097. [Online]. Available: https://doi.org/10.1109/smartworld.2018.00190

[53] T.-H. Nguyen, T. K. Nguyen, T.-D. Nguyen, and V. N. Quoc Bao, "DRL for trajectory design and resource management in UAV-aided RSMA networks," in *Proc. 2024 Int. Conf. Adv. Technol. Commun. (ATC)*, Ho Chi Minh City, Vietnam, 2024, pp. 36–40. [Online]. Available: https://doi.org/10.1109/atc63255.2024.10908260

[54] D. Pascarella, S. Venticinque, and R. Aversa, "Autonomic agents for real time UAV mission planning," in *Proc. 2013 IEEE 10th Int. Conf. Ubiquitous Intelligence and Computing (UIC) and 2013 IEEE 10th Int. Conf. Autonomic and Trusted Computing (ATC)*, Vietri sul Mare, Italy, 2013, pp. 410–415. [Online]. Available: https://doi.org/10.1109/uic-atc.2013.34

[55] J. Xu, X. Yan, and Y. Niu, "An improved butterfly optimization algorithm for UAV path planning in complex environment," in *Proc. 2022 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Haikou, China, 2022, pp. 1044–1050. [Online]. Available: https://doi.org/10.1109/smartworld-uic-atc-scalcom-digitaltwin-pricomp-metaverse56740.2022.00154

[56] C. Hu, J. Zhou, W. Ding, J. Liu, and Y. Niu, "Digital twins-based multi-agent deep reinforcement learning for UAV-assisted vehicle edge computing," in *Proc. 2022 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Haikou, China, 2022, pp. 1329–1336. [Online]. Available: https://doi.org/10.1109/smartworld-uic-atc-scalcom-digitaltwin-pricomp-metaverse56740.2022.00192

[57] L. He, H. Zheng, and X. Zhai, "REUT: A retinex-inspired low-light image enhancer for UAV tracking at night," in *Proc. 2022 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Haikou, China, 2022, pp. 1051–1057. [Online]. Available: https://doi.org/10.1109/smartworld-uic-atc-scalcom-digitaltwin-pricomp-metaverse56740.2022.00155

[58] J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao, and X. Wang, "Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22399–22409, Nov. 15, 2022. [Online]. Available: https://doi.org/10.1109/jiot.2021.3111024

[59] T. Karachalios, C. Xouris, and T. Orphanoudakis, "Optimizing UAV location awareness telemetry data for low power wide area network," *Proc. 25th Euromicro Conf. Digital Syst. Design (DSD)*, Maspalomas, Spain, 2022, pp. 885–888. [Online]. Available: https://doi.org/10.1109/dsd57027.2022.00124

[60] D. Li, Y. Qiang, and J. H. Mott, "Hazard analysis of large cargo delivery UAVs under the Chinese air traffic control system," *Proc. 2021 Systems and Information Engineering Design Symp. (SIEDS)*, Charlottesville, VA, USA, 2021, pp. 1–6. [Online]. Available: https://doi.org/10.1109/sieds52267.2021.9483732

[61] A. Ganau, J. Vico, P. Morcillo, and J. V. Balbastre, "Design and validation of reflector elements to increase the radar cross-section of small drones," *Prog. Electromagn. Res. C*, vol. 128, pp. 129–142, 2023. [Online]. Available: https://doi.org/10.2528/pierc22092003

[62] C. Cummings, *Air traffic flow and the congestion of the skies: Models, insights, and management strategies for the air mobility context*, Ph.D. dissertation, Northwestern Univ., Cook County, IL, USA, 2022. [Online]. Available: https://www.proquest.com/dissertations-theses/air-traffic-flow-congestion-skies-models-insights/docview/2707696219/se-2

[63] M. B. Brown and A. B. Forsythe, "Tests for the equality of variances," *J. Amer. Statist. Assoc.*, vol. 69, no. 346, pp. 364–367, Jun. 1974. [Online]. Available: https://doi.org/10.2307/2285659

[64] S. S. Shapiro and M. B. Wilk, "An analysis of variance test for normality (complete samples)," *Biometrika*, vol. 52, no. 3–4, pp. 591–611, Dec. 1965. [Online]. Available: https://doi.org/10.2307/2333709

BIOGRAPHY

Andrew Renault is a graduate student in the Aeronautical Science Department at Capital Technology University, where he focuses on advancing research in air traffic management and unmanned aerial vehicle (UAV) integration. With over 30 years of engineering experience in the aerospace industry, Andrew has contributed to a variety of projects ranging from aircraft design to systems optimization. His expertise spans both technical and regulatory aspects of aerospace operations, making him a key voice in discussions on modernizing air traffic control systems and addressing emerging challenges in aviation.