Semarak International Journal of Machine Learning

Journal homepage:
https://sijml.com/index.php/journal/index
ISSN: 3030-5241



AeroLink Intelligent Network System: Integrating AI and IoT for Enhanced Airport Cybernetics

Jeewah Arivarasan[1], Malenee Chandran[1,*], Safaa N Saud Al-Humairi[1]

[1] Department of Information Sciences and Engineering, Management and Science University, 40100 Shah Alam, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 28 June 2026
Received in revised form 25 July 2026
Accepted 10 August 2026
Available online 17 September 2026

Keywords:

Airport cybernetics; artificial intelligence; light fidelity; internet of things; radio frequency; LiDAR; cybersecurity

ABSTRACT

The aviation industry is undergoing a rapid digital transformation driven by integrated cyber-physical systems, yet modern airport cybernetics remains severely hindered by physical scalability constraints in traditional wired networks, communication disruptions, and escalating cybersecurity threats. Objective: While prior research has investigated these vulnerabilities in isolation, this study introduces the AeroLink Intelligent Network System, which integrates five core technologies to simultaneously enhance communication reliability, infrastructure scalability, and cybersecurity resilience. Method: Following the structured ADDIE development model, a hybrid physical prototype integrating Radio Frequency (RF), LiFi-inspired communication, Artificial Intelligence (AI), Internet of Things (IoT), and LiDAR-like detection was constructed and evaluated in a miniature airport diorama. Concurrently, a five-point Likert scale questionnaire was administered to airport stakeholders, yielding 544 valid responses for descriptive, reliability, correlation, and multiple regression analyses in SPSS. Results: Physical trials demonstrated that all technologies functioned successfully, with average response times of 2.00 seconds for RF, 2.26 seconds for LiDAR-like detection, 2.44 seconds for AI, 2.67 seconds for IoT, and 3.60 seconds for LiFi-inspired communication. The multiple linear regression model was highly significant, explaining 76.6 percent of the variance in airport cybernetics (R-squared = 0.766, $p < 0.001$), with cyberattack risk identified as the strongest predictor (Beta = 0.638, $p < 0.001$), followed by communication interference (Beta = 0.158, $p = 0.001$) and scalability limitations (Beta = 0.113, $p = 0.028$). Conclusion: These findings validate the AeroLink framework as an effective cohesive architecture capable of advancing intelligent airport operations by strengthening cybersecurity, network scalability, and communication reliability.

1. Introduction

1.1 Technological Context and Operational Significance

The global aviation sector is currently undergoing a rapid digital transformation characterized by the deep integration of advanced communication networks and cyber-physical systems. Modern airport infrastructures are increasingly dependent on the convergence of diverse information,

* *Corresponding author.*
E-mail address: malenee_chandran@msu.edu.my

communication, and sensor technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT), and high-speed wireless networks, to establish adaptive and intelligent cybernetic frameworks [1]. These integrated systems are critical for maintaining real-time situational awareness, optimizing resource management, and ensuring robust, collaborative decision-making across all airport stakeholders [2].

1.2 Problem Statement and Identified Research Gaps

Despite these technological advancements, contemporary airport operations are confronted with escalating systemic vulnerabilities that threaten operational continuity. Specifically, modern airport cybernetics is severely challenged by three interrelated bottlenecks: communication interference that disrupts critical data exchange between air traffic controllers and pilots, the scalability constraints of traditional wired physical networks that impede operational expansion, and a rapidly expanding attack surface for sophisticated cyberattacks [3,4]. Signal congestion and transmission overlap can severely compromise situational awareness [5], while the extensive cabling and cost of expanding physical wired infrastructures diminish operational flexibility and confound the integration of developing systems [6]. Furthermore, the increasing reliance on interconnected digital networks, cloud services, and IoT devices has heightened airport vulnerability to disruptive malware, ransomware, and unauthorized network intrusions [7].

A critical review of the literature reveals that while individual aspects of these challenges—such as isolated wireless congestion models or specific network security protocols—have been extensively investigated, traditional airport IT management continues to operate on fragmented, siloed platforms [8]. Traditional architectures frequently analyze and address cybersecurity vulnerabilities, network scalability, and communication interference in isolation, failing to consider their collective, feedback-driven impact on overall airport cybernetics. Furthermore, existing airport infrastructures typically lack a unified, cohesive framework that integrates diverse and emerging technologies—specifically the combination of AI, Light Fidelity (LiFi), Radio Frequency (RF), IoT, and Light Detection and Ranging (LiDAR)—to simultaneously mitigate these three bottlenecks. Recent research [9] underscores that while the deployment of heterogeneous smart devices accelerates operational automation, it drastically increases the network's attack surface, necessitating automated, multi-layered risk evaluation tools rather than isolated security patches.

1.3 Research Objectives and Outline of the Study

To address these integrated challenges, this study introduces the AeroLink Intelligent Network System, a comprehensive airport communication framework designed to improve airport cybernetics by enhancing communication reliability, infrastructure scalability, and cybersecurity resilience. Grounded in Cybernetic Theory, the proposed system employs a hybrid LiFi-RF-AI-IoT-LiDAR architecture to enable ongoing information exchange, adaptive decision-making, and intelligent control mechanisms. By integrating these five core technologies into a unified framework, AeroLink systematically reduces communication interference, physical scalability constraints, and cyberattack threats. Ultimately, this research seeks to advance intelligent airport ecosystems, enabling the implementation of smart, safe, and resilient airport operations.

The remainder of this manuscript is structured as follows: Section 2 establishes the theoretical foundation in Cybernetic Theory and reviews relevant literature on airport operational bottlenecks; Section 3 delineates the system architecture, hardware prototype development, and quantitative research methodology; Section 4 presents the experimental response-time findings and details the

statistical analysis of the questionnaire data; Section 5 discusses the significance of the findings, their contextualization within the literature, and the limitations of the study; and Section 6 synthesizes the conclusions and outlines future research pathways.

2. Literature Review and Related Work

2.1 Synthesis of Key Concepts and Foundations

A rigorous analysis of the system requirements for modern airport operations must build on established frameworks in wireless systems engineering, cybernetics, and cybersecurity. This study establishes a baseline by drawing on fifteen critical publications that define the operational, infrastructural, and methodological boundaries of the proposed research. Table 1 synthesizes these foundational studies, highlighting their core contributions and delineating their specific roles in guiding the conceptual development of the AeroLink Intelligent Network System.

The thematic review that follows expands on these foundational concepts to locate the specific research gaps addressed by the proposed system.

Table 1
Synthesis of the foundational concepts underpinning the AeroLink framework

Citation / Authors	Core Technology or Concept	Operational Role in AeroLink Framework
Basha [2]	Wireless network design in high-density airport operations	Anchors baseline for wireless deployment challenges in high-density areas
Alhammadi *et al*., [1]	Artificial Intelligence integration in 6G wireless networks	Grounds the AI-driven opportunities and processing capabilities
Ahmed [3]	ADS-B communication threats, risks, and security in ATM	Identifies specific vulnerabilities in Air Traffic Management data links
Skosana [10]	Evaluation of wireless technologies and infrastructure	Contextualizes traditional cellular networks and their limitations
Ukwandu [4]	Cybersecurity challenges and future trends in aviation	Establishes the baseline of rising threat vectors across aviation networks
Gallego García and Rodríguez [11]	Viable System Model (VSM) and conceptual modeling	Provides structural systems engineering and cybernetic framework
Kevadiya *et al*., [12]	Cybernetic perspective of AI and adaptive control systems	Links AI processing to adaptive feedback loops under Cybernetic Theory

Table 1 (***Continued***)

Citation / Authors	Core Technology or Concept	Operational Role in AeroLink Framework
Sabban and O. C. [13]	Innovations in Indoor Positioning Systems (IPS)	Informs the web-based Passenger Management navigation subsystem
Yang [5]	Communication errors in pilot-ATC interactions	Pinpoints voice and data communication interference as an operational hazard
Zhang and Q. D. [14]	Hierarchical networks for semantic pilot-ATC communication	Explores semantic understanding mechanisms to prevent transmission errors
Śliwa and D. P. [15]	Wireless communication advances in aviation and infrastructure	Details physical-layer performance and propagation barriers in aviation
Rossiter [7]	Smart airports and the evolving landscape of cyber threats	Validates the rising incidence of malware and ransomware in airport IT
Abuhassna *et al*., [16]	Technology integration within the ADDIE model for design	Outlines the structured development stages of the prototype
Moiso [17]	Application of instructional design models	Informs the structured implementation and evaluation phases
Sharma and Sharma [6]	Scalability of multi-airport systems in air transport	Highlights physical and financial constraints of wired infrastructures

2.2 Thematic Review of the Literature

2.2.1 Theme 1: Cybernetic theory and systems engineering in aviation operations

Cybernetic Theory provides the structural foundation required to analyze complex, adaptive, and goal-directed systems. In organizational modeling and system design, researchers such as Gallego García and Rodríguez [11] have demonstrated how the Viable System Model (VSM) helps complex networks achieve stability and self-regulation by balancing internal processes with dynamic environmental shifts. Similarly, Kevadiya *et al*., [12] have examined the cybernetic perspective of Artificial Intelligence, showing that integrating intelligent control mechanisms within feedback loops allows systems to monitor their own performance and adaptively respond to external perturbations.

The AeroLink Intelligent Network System operationalizes these cybernetic concepts. While existing literature primarily applies Cybernetic Theory conceptually to organizational structures or algorithmic control loops in isolation, AeroLink translates these feedback and control mechanisms into a physical, multi-layered airport communication framework. By coordinating real-time data flows between the Aircraft, ATC, Passenger, and Security subsystems, the AeroLink architecture

establishes a unified cybernetic loop where real-time performance indicators, such as transmission latencies and AI object detection events, feed directly into adaptive decision-making processes.

2.2.2 Theme 2: Optical wireless communication and hybrid networks in airports

As radio frequency spectrum congestion continues to escalate in congested transit hubs, Visible Light Communication (VLC) and Light Fidelity (LiFi) have emerged as essential technologies to supplement traditional wireless networks. In a comprehensive study, Khan [18] evaluated the scalability and security advantages of hybrid VLC-RF architectures, establishing that optical wireless networks provide significant physical-layer security and spectrum relief because light waves do not penetrate solid walls and are immune to electromagnetic interference. In the specific context of airport terminals, Vieira *et al*., [19] developed an indoor positioning system using tetrachromatic Light Emitting Diodes (LEDs) and Edge/Fog computing, demonstrating that modulated light signals can achieve precise passenger localization and wayfinding guidance without relying on saturated Global Positioning System (GPS) or Radio Frequency (RF) signals. This work was subsequently expanded by Vieira *et al*., [20], who integrated Deep Reinforcement Learning with VLC-enabled luminaires to optimize traffic flows and dynamically reroute Autonomous Guided Vehicles (AGVs) in busy terminal environments.

Although these advanced VLC architectures show significant potential, they are predominantly designed as isolated solutions focused strictly on pedestrian wayfinding or localized AGV routing. AeroLink directly addresses this limitation by integrating LiFi-inspired optical transmission with a robust RF backbone, AI-assisted edge processing, and IoT sensors into a cohesive, airport-wide operational platform. Rather than viewing VLC simply as an isolated localization utility, AeroLink implements it as a critical communication channel for ATC-to-aircraft coordination, securing data exchange against RF jamming while preserving standard RF channels for long-range, non-line-of-sight operations. This hybrid approach is validated empirically by AeroLink's technology response times, where the RF component achieved a rapid response of 2.00 seconds and the LiFi-inspired infrared module recorded a latency of 3.60 seconds, proving the operational viability of coexisting optical and radio transmission technologies.

2.2.3 Theme 3: Infrastructure scalability and wireless integration bottlenecks

The rapid expansion of digital offerings and passenger volumes in modern airports has exposed major scalability limits in traditional IT networks. Standard airport communications heavily rely on physical, wired network backbones. As Sharma and Sharma [6] observed, expanding these physical wired infrastructures to accommodate emerging systems requires extensive cabling, costly equipment upgrades, and substantial operational disruptions. This infrastructural bottleneck is further detailed in a dynamic analysis of airport development barriers by Hwilkowska-Kubala and Huderek-Glapska [21], which demonstrated that physical cabling constraints and high capital expenditures severely diminish an airport's operational flexibility and delay the adoption of modern, data-intensive digital services.

AeroLink directly addresses these scalability limitations by transitioning from high-maintenance, centralized wired networks to a decentralized, wireless, and optical mesh framework. By leveraging low-power, cost-effective microcontrollers such as the ESP32-S3 and Arduino Uno R3, the AeroLink system permits rapid, modular deployment of sensor nodes without the need for extensive physical cabling or structural modifications. The significance of this transition is supported by AeroLink's statistical analysis of 544 airport stakeholders, which revealed a strong positive correlation between

resolving scalability limitations and enhancing overall airport cybernetics ($r = 0.802$, $p < 0.01$). This empirical finding validates the transition from rigid wired systems to flexible, modular wireless architectures.

2.2.4 Theme 4: Cyber resilience and threat mitigation in airport ecosystems

The integration of cloud services, operational technology, and IoT devices has dramatically expanded the attack surface of contemporary airport networks, rendering them highly vulnerable to sophisticated cyberattacks. Lykou *et al*., [22] provided a seminal framework for smart airport cybersecurity, detailing threat vectors such as ransomware, malware, and unauthorized network intrusions, and emphasizing the critical need for multi-layered resilience controls that span both physical and digital assets. This systemic vulnerability was demonstrated in practice during major airport disruptions, which Rossiter [7] and industry reports [23] attribute to the vulnerability of shared, centralized passenger-processing and operational platforms to targeted ransomware. To mitigate these risks, Saura *et al*., [24] proposed automated anomaly detection frameworks utilizing Federated Learning to secure multi-tenant, smart cyber-physical systems at the network edge. Similarly, real-world trials conducted by Bianzino *et al*., [25] at Athens International Airport demonstrated that coordinating 5G-connected service robots, thermal imaging, and AI-powered analytics can enhance physical-layer security and operational monitoring in highly congested environments.

While these studies highlight the critical nature of airport cybersecurity, traditional airport management continues to implement security patches, wireless congestion models, and database protocols in isolation. AeroLink bridges this gap by introducing a multi-layered, cohesive security framework that combines hardware-level isolation (via hybrid RF-LiFi channels) and software-level intelligence (via edge-based AI camera surveillance). The necessity of this integrated approach is strongly reinforced by the regression analysis of AeroLink's survey data, which identified Cyber Attacks Risk as the most significant predictor of overall airport cybernetics performance (Beta = 0.638, $p < 0.001$), surpassing both communication interference (Beta = 0.158, $p = 0.001$) and scalability limitations (Beta = 0.113, $p = 0.028$). By proving that stakeholder perception of cybersecurity is the primary driver of cybernetic trust and efficiency, this research provides the empirical justification for AeroLink's unified, multi-technology defense architecture.

3. Methodology

3.1 Research Design and Systems Development Framework

A quantitative research approach, supported by a descriptive research design, was adopted to systematically evaluate the effectiveness of the AeroLink Intelligent Network System in enhancing airport cybernetics. The investigation focused on mitigating three critical operational vulnerabilities: communication interference, the reduced scalability of traditional wired infrastructure, and the risk of cyberattacks. Data were collected through a dual-method approach combining structured questionnaire administration and physical prototype evaluation.

The systems engineering lifecycle of the AeroLink Intelligent Network System was structured according to the ADDIE (Analysis, Design, Development, Implementation, and Evaluation) development model. The ADDIE framework is recognized as an effective, structured methodology for the design, deployment, and evaluation of technology-based systems [16,17,26]. The ADDIE model framework adopted in this study is illustrated in Fig. 1, and the operational phases of the model were executed as follows:

1. Analysis Phase: Contemporary airport operational challenges and stakeholder requirements were identified and analyzed.

2. Design Phase: The overall architectural design and functional specifications of the AeroLink network were developed.

3. Development Phase: The hardware configurations and integrated subsystems were constructed.

4. Implementation Phase: The physical prototype was deployed and integrated within a simulated operational environment.

5. Evaluation Phase: The hardware components were experimentally tested, and statistical analyses of stakeholder perceptions were performed to validate system efficacy.

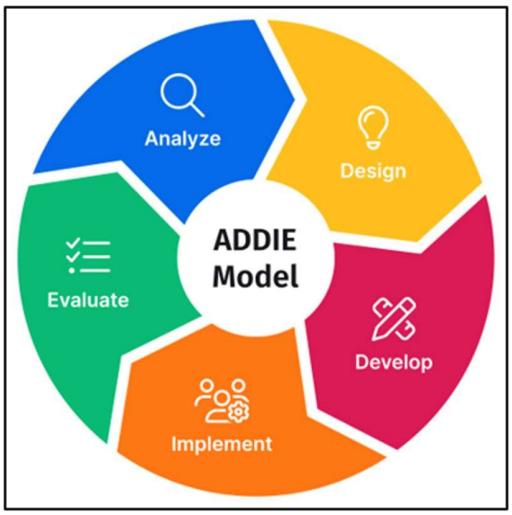


Fig. 1. ADDIE model framework [16]

3.2 System Architecture and Prototype Specifications

The AeroLink prototype was developed as an integrated, intelligent cybernetic framework consisting of four interconnected subsystems: Aircraft Management, Air Traffic Control, Passenger Management, and Security Management. The physical hardware and platform specifications for each subsystem were established as follows:

1. Aircraft Subsystem: This onboard module was constructed using an ESP32-S3 CAM, an Organic Light-Emitting Diode (OLED) display, an infrared receiver module, a TP4056 charging module, an XL6009 boost converter module, and a Lithium-Polymer (Li-Po) battery.

2. Air Traffic Control Subsystem: This ground station was designed around an Arduino Uno R3 microcontroller board, which was integrated with infrared communication transceivers and dedicated system monitoring components.

3. Passenger Management Subsystem: This component was developed as a web-based, interactive navigation platform to assist travelers.

4. Security Management Subsystem: This subsystem comprised a web-based control interface and a dedicated ESP32-CAM module deployed for continuous surveillance and security monitoring.

The schematic diagrams of the Aircraft and Air Traffic Control subsystems are presented in Fig. 2 and Fig. 3, respectively.

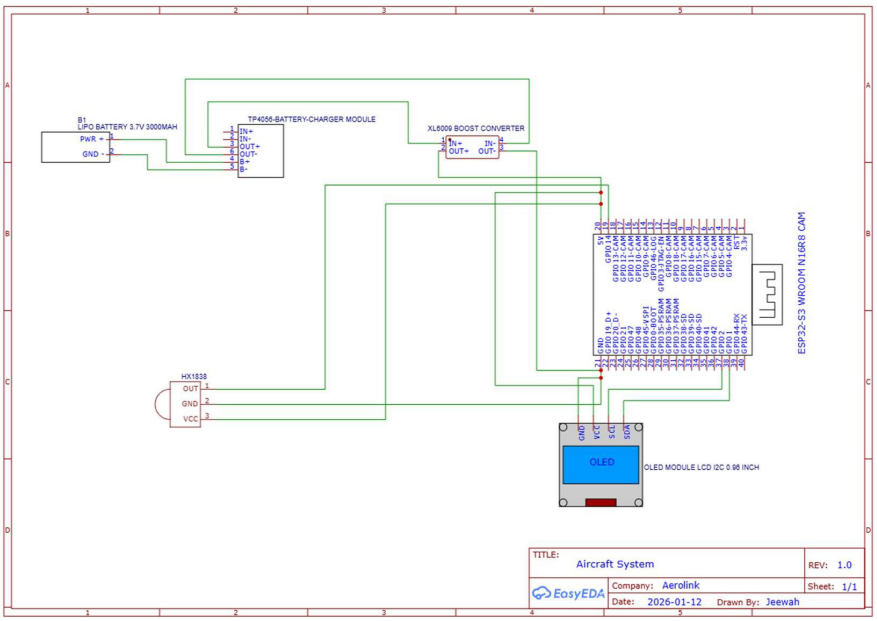


Fig. 2. Aircraft system schematic diagram

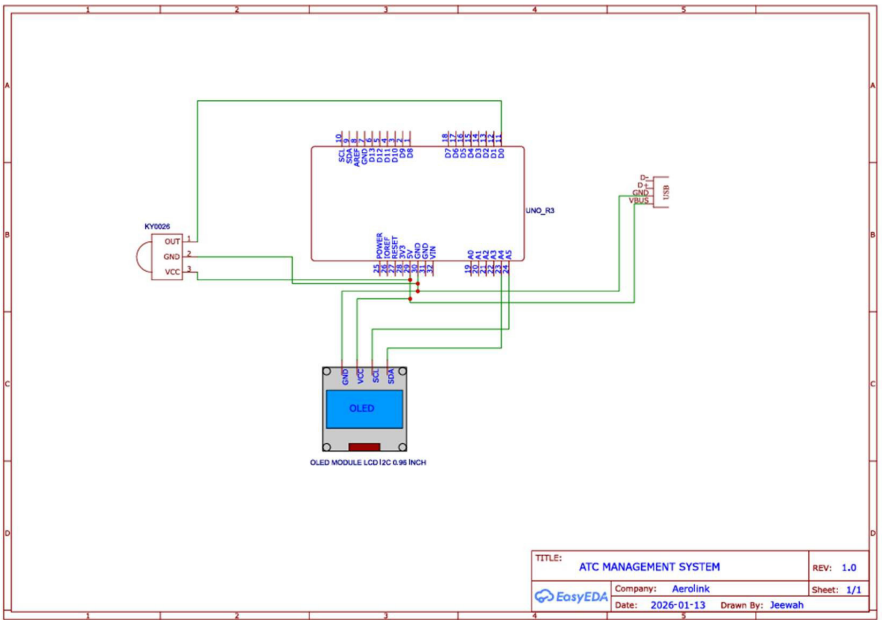


Fig. 3. ATC system schematic diagram

3.3 Experimental Setup and Prototype Testing Protocol

To evaluate the operational feasibility of the integrated technologies, a physical simulation environment was established. A miniature airport diorama was constructed, which featured a terminal structure, a runway, a taxiway, and an air traffic control tower, as shown in Fig. 4.



Fig. 4. Miniature airport diorama

The experimental testing of the AeroLink prototype was carried out according to the following protocols:

a. Communication and Sensing Integration: The ESP32-CAM and ESP32-S3 CAM modules were configured and deployed for Artificial Intelligence (AI) assisted monitoring and real-time object detection. Infrared communication links were established to simulate bidirectional Light Fidelity (LiFi) data transmission, aligning with standard wireless optical protocols [15,27].

b. Operational Performance Evaluation: Experimental testing focused on evaluating communication performance, real-time surveillance capabilities, web-based passenger navigation, obstacle detection, and the physical integration of all subsystems. Latency trials were conducted to measure the average response times of the five core technological components: Radio Frequency, LiDAR-like Detection (using the ESP32-S3 CAM), AI processing, IoT communication, and LiFi-inspired infrared communication.

3.4 Stakeholder Questionnaire and Data Collection Protocol

To gather primary, empirical data on stakeholder perceptions, a structured questionnaire was designed and distributed to airport users and operational personnel. The data collection was executed under the following protocol:

1. Measurement Scale: The questionnaire items were structured using a five-point Likert scale to systematically evaluate stakeholder perceptions across four core operational variables: the frequency/risk of security intrusions, scalability reduction in traditional wired networks, voice and data communication interference, and overall airport cybernetics.

2. Sample Population: A total of 544 valid, completed questionnaires were collected from the target stakeholders and compiled for subsequent statistical processing.

3.5 Statistical Data Analysis Methods

The collected questionnaire data were processed and analyzed using descriptive and inferential statistical methods. All quantitative calculations were executed using the Statistical Package for the Social Sciences (SPSS) software [28]. The analytical procedures consisted of:

1. Descriptive Analysis: Mean values and ranges were calculated to determine stakeholder agreement levels regarding airport cybernetics, communication interference, scalability limitations, and cyberattack risks.

2. Reliability Analysis: Cronbach's Alpha coefficient was calculated to assess the internal consistency and reliability of the measurement scales, adopting a standard minimum alpha threshold of 0.70 [29].

3. Correlation Analysis: Pearson's correlation coefficient (r) was computed to evaluate the strength and statistical significance of the linear relationships between the independent variables (scalability limitations, communication interference, and cyberattack risks) and the dependent variable (airport cybernetics).

4. Regression Analysis: Multiple linear regression analysis was performed to evaluate the combined predictive impact of the independent variables on the dependent variable, to determine the coefficient of determination (R-squared), and to evaluate model significance through the Analysis of Variance (ANOVA) F-test.

4. Results

4.1 Experimental Evaluation of AeroLink Prototype Subsystems

The performance and operational feasibility of the integrated AeroLink Intelligent Network System prototype were evaluated through simulated operations using a physical miniature airport diorama. This simulation environment featured a constructed terminal building, runway, taxiway, and air traffic control tower. The experimental evaluation measured the response times of the five core integrated technologies, which included Radio Frequency communication, Light Fidelity inspired communication, Artificial Intelligence, the Internet of Things, and LiDAR-like detection (utilizing the ESP32-S3 CAM module). The average response latencies recorded during these operational simulation trials are presented in Table 2.

Table 2
Average response time of AeroLink technology components

Technology Component	Average Response Time
Radio Frequency (RF)	2.00s
LiDAR-Like Detection (ESP32-S3 CAM)	2.26s
Artificial Intelligence (AI)	2.44s
Internet of Things (IoT)	2.67s
LiFi-Inspired Communication	3.60s

The experimental data indicate that all five technological components functioned successfully within the integrated prototype architecture. The Radio Frequency communication subsystem achieved the most rapid response time of 2.00 seconds, enabling immediate data exchange between the simulated aircraft and the Air Traffic Control ground station. The LiDAR-like detection module and the Artificial Intelligence processing module recorded average latencies of 2.26 seconds and 2.44 seconds, respectively, which demonstrated prompt obstacle identification and real-time computing at the network edge. The Internet of Things subsystem achieved an average latency of 2.67 seconds, successfully maintaining stable, real-time data flows between the physical diorama hardware and the web-based monitoring platform. The LiFi-inspired communication module, operating via an infrared transmission and receiver mechanism, recorded the longest response latency at 3.60 seconds. This delay was primarily attributed to the physical characteristics of the infrared transceiver and the

processing required for signal synchronization. Nevertheless, this response rate was sufficient to maintain reliable and uninterrupted data links within the prototype-scale airport environment.

4.2 Questionnaire Analysis Results

4.2.1 Descriptive analysis

The quantitative evaluation of stakeholder perceptions was based on 544 valid, completed questionnaires collected from airport users and operational personnel. The descriptive statistics revealed favorable and consistent stakeholder perceptions regarding the core study variables. The mean scores for each measurement scale were distributed as follows:

1. Airport Cybernetics: Mean values ranged from 3.81 to 3.94, indicating a high level of agreement regarding the necessity and effectiveness of integrated cybernetic control systems.
2. Risk of Cyber Attacks: Mean values ranged from 3.82 to 3.97, reflecting strong consensus among stakeholders regarding the critical threat of digital intrusions in modern aviation operations.
3. Scalability Limitations: Mean values ranged from 3.62 to 3.88, indicating widespread agreement that traditional wired infrastructures restrict operational expansion.
4. Communication Interference: Mean values ranged from 3.66 to 3.87, confirming that signal disruptions and overlapping transmissions remain highly prevalent operational hazards.

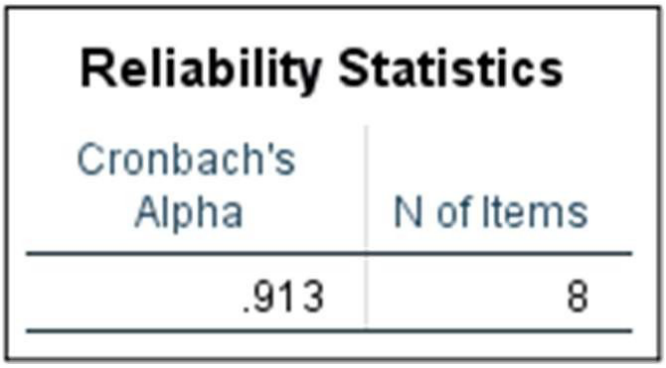
Overall, these descriptive statistics indicate that stakeholders consistently recognized the significance of these challenges and strongly concurred on the necessity of advancing airport cybernetics.

4.2.2 Reliability analysis

To assess the internal consistency and reliability of the survey scales, Cronbach's Alpha reliability coefficients were calculated for each variable. The analysis demonstrated high reliability across all measurement scales, with coefficients far exceeding the conventional academic threshold of 0.70. The reliability coefficients were recorded as follows:

1. Airport Cybernetics: Cronbach's Alpha was 0.913, demonstrating excellent internal consistency.
2. Risk of Cyber Attacks: Cronbach's Alpha was 0.907, confirming a highly reliable measurement scale.
3. Communication Interference: Cronbach's Alpha was 0.904, indicating very strong scale reliability.
4. Scalability Limitation: Cronbach's Alpha was 0.896, representing a robust and consistent measurement scale.

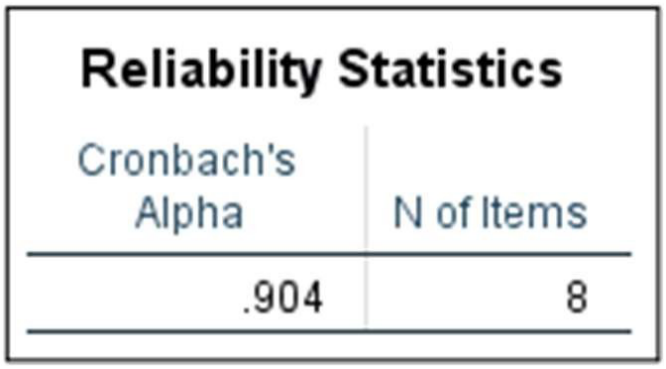
These exceptional alpha values confirmed the methodological rigor of the survey design and validated the data for subsequent inferential statistical analyses. The reliability analysis outputs for the four variables are presented in Fig. 5 to Fig. 8.



Reliability Statistics

Cronbach's Alpha	N of Items
.913	8

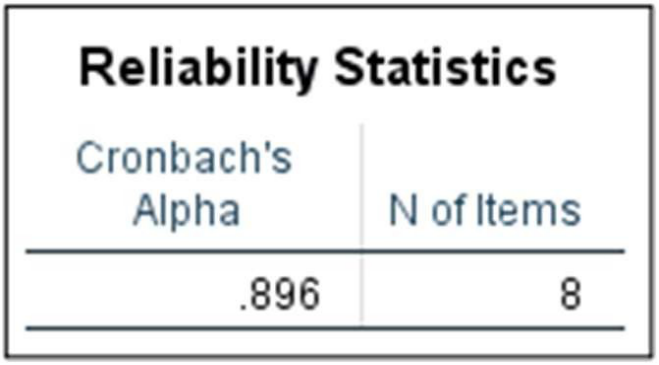
Fig. 5. Reliability analysis for airport cybernetics



Reliability Statistics

Cronbach's Alpha	N of Items
.904	8

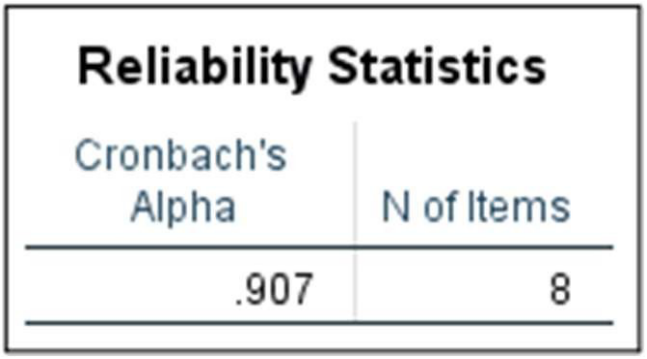
Fig. 6. Reliability analysis for communication interference



Reliability Statistics

Cronbach's Alpha	N of Items
.896	8

Fig. 7. Reliability analysis for scalability limitations



Reliability Statistics

Cronbach's Alpha	N of Items
.907	8

Fig. 8. Reliability analysis for cyber attacks

4.2.3 Bivariate correlation analysis

Pearson correlation analysis was executed to evaluate the strength and statistical significance of the linear relationships between the independent operational variables and the dependent variable, Airport Cybernetics. The analysis revealed statistically significant, strong positive correlations across all tested relationships ($p < 0.01$). The correlation coefficients were recorded as follows:

1. Cyber Attacks Risk and Airport Cybernetics: A very strong positive correlation was observed ($r = 0.865$, $p < 0.01$), establishing that stakeholder perceptions of cybernetic efficiency are most heavily tied to robust security measures.

2. Scalability Limitation and Airport Cybernetics: A robust positive correlation was identified ($r = 0.802$, $p < 0.01$), showing that resolving physical network bottlenecks is highly associated with improved system performance.

3. Communication Interference and Airport Cybernetics: A strong positive correlation was recorded ($r = 0.780$, $p < 0.01$), indicating that mitigating voice and data signal interference is significantly linked to overall operational coordination.

These bivariate findings confirm that improvements in infrastructure scalability, cybersecurity preparedness, and communication reliability are strongly and positively associated with the enhancement of overall airport cybernetics. The Pearson correlation analysis output is presented in Fig. 9.

Correlations

		AC	CI	SL	CAR
AC	Pearson Correlation	1	.780**	.802**	.865**
	Sig. (2-tailed)		.000	.000	.000
	N	544	544	544	544
CI	Pearson Correlation	.780**	1	.880**	.819**
	Sig. (2-tailed)	.000		.000	.000
	N	544	544	544	544
SL	Pearson Correlation	.802**	.880**	1	.861**
	Sig. (2-tailed)	.000	.000		.000
	N	544	544	544	544
CAR	Pearson Correlation	.865**	.819**	.861**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	544	544	544	544

**. Correlation is significant at the 0.01 level (2-tailed).

Fig. 9. Pearson correlation analysis for questionnaires

4.2.4 Multiple linear regression analysis

To evaluate the combined predictive impact of the three independent variables on the dependent variable, a multiple linear regression analysis was performed. The regression model proved to be highly statistically significant ($F = 588.474$, $p < 0.001$) and demonstrated high explanatory power, accounting for 76.6 percent of the total variance in Airport Cybernetics (R-squared = 0.766).

The individual standardized beta coefficients and their respective significance levels were recorded as follows:

1. Cyber Attacks Risk: This variable emerged as the strongest and most significant predictor of airport cybernetic performance (Standardized Beta = 0.638, $p < 0.001$).

2. Communication Interference: This variable was identified as the second most significant predictor (Standardized Beta = 0.158, p = 0.001).

3. Scalability Limitation: This variable also acted as a statistically significant predictor of the dependent variable (Standardized Beta = 0.113, p = 0.028).

These regression results establish that cybersecurity preparedness is the primary driver of successful airport cybernetics, supported by significant contributions from communication reliability and infrastructure scalability. The model summary, ANOVA test, and coefficient test outputs are presented in Fig. 10 to Fig. 12.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.875[a]	.766	.764	.42552	.766	588.474	3	540	.000

a. Predictors: (Constant), CAR, CI, SL

Fig. 10. Model summary for questionnaires

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	319.664	3	106.555	588.474	.000[b]
	Residual	97.777	540	.181		
	Total	417.441	543			

a. Dependent Variable: AC

b. Predictors: (Constant), CAR, CI, SL

Fig. 11. ANOVA test for questionnaires

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.372	.086		4.334	.000	.204	.541
	CI	.156	.045	.158	3.470	.001	.067	.244
	SL	.112	.051	.113	2.207	.028	.012	.212
	CAR	.645	.043	.638	15.075	.000	.561	.729

a. Dependent Variable: AC

Fig. 12. Coefficient test for questionnaires

5. Discussion

5.1 Restatement and Significance of Core Findings

The primary objective of this study was to design, develop, and evaluate the AeroLink Intelligent Network System, an integrated communication framework utilizing a hybrid Radio Frequency, Light Fidelity, Artificial Intelligence, Internet of Things, and LiDAR-like architecture to enhance overall

airport cybernetics. Specifically, the system was designed to simultaneously mitigate three major airport operational bottlenecks: communication interference, physical infrastructure scalability limitations, and cyberattack risks.

The experimental and statistical findings of this study demonstrate the successful attainment of these research objectives. At the physical hardware level, the prototype evaluation performed within a miniature airport diorama proved the operational feasibility of integrating these five diverse technologies into a cohesive, functional ecosystem. The recorded response times—ranging from the rapid 2.00 seconds achieved by the Radio Frequency module to the 3.60 seconds recorded by the LiFi-inspired infrared communication module—validated that all subsystems operated effectively within acceptable real-time processing latencies.

At the perceptual level, the statistical analysis of the questionnaire data collected from 544 airport stakeholders confirmed the theoretical and practical validity of the research framework. The multiple linear regression model demonstrated high explanatory power, accounting for 76.6 percent of the total variance in Airport Cybernetics (R-squared = 0.766, $F = 588.474$, $p < 0.001$). Within this model, Cyber Attacks Risk emerged as the most significant predictor of airport cybernetic performance (Beta = 0.638, $p < 0.001$), followed by Communication Interference (Beta = 0.158, $p = 0.001$) and Scalability Limitation (Beta = 0.113, $p = 0.028$). These findings are supported by exceptionally strong bivariate correlations, ranging from $r = 0.780$ to $r = 0.865$ ($p < 0.01$), and high scale reliability across all measured variables (Cronbach's Alphas > 0.89). Together, these results provide robust empirical proof that resolving scalability limitations, mitigating communication interference, and establishing proactive cyber defenses are critical, mutually reinforcing drivers of successful airport cybernetics.

5.2 Comparative Analysis and Contextualization in Literature

The empirical success of the AeroLink framework strongly reinforces and extends several established concepts in systems engineering and airport cybernetics. The high explanatory power of the regression model (R-squared = 0.766) provides robust validation for the application of Cybernetic Theory to airport operational systems, aligning with the foundational research of Gallego García and Rodríguez [11] and Kevadiya et al. [12]. While prior cybernetic studies have primarily applied feedback loops and self-regulation concepts conceptually to corporate management or isolated algorithmic controllers, this study successfully translates these theoretical parameters into a multi-layered physical communication framework that coordinates dynamic data flows between the Aircraft, ATC, Passenger, and Security subsystems.

The experimental performance of the hybrid communication subsystem directly addresses the radio frequency spectrum congestion detailed by Yang [5] and Zhang [14]. By successfully demonstrating the cohabitation of RF transmission (2.00s latency) and optical LiFi-inspired transmission (3.60s latency), the AeroLink prototype offers a practical method to bypass signal interference and transmission overlap in high-density areas. This approach extends the recent work of Vieira et al. [19], [20], who utilized Visible Light Communication (VLC) primarily for passenger wayfinding or localized Autonomous Guided Vehicle (AGV) routing. AeroLink expands on their research by demonstrating that wireless optical communication can serve as an active, integrated control channel for Air Traffic Control and security data transmission alongside standard RF backbones, thus providing a redundant and interference-resistant communication layer.

Furthermore, the robust correlation observed between Scalability Limitation and Airport Cybernetics ($r = 0.802$, $p < 0.01$) supports the assertions of Sharma and Sharma [6] and Hwilkowska-Kubala and Huderek-Glapska [21] that traditional, centralized wired infrastructures represent a

severe bottleneck to modern airport development. By transitioning from high-maintenance physical cabling to a decentralized wireless and optical mesh network using low-cost edge controllers (ESP32-S3 and Arduino Uno R3), the AeroLink framework demonstrates how airports can integrate advanced digital systems with minimal structural disruption and capital expenditure.

Finally, the preeminence of Cyber Attacks Risk as the strongest predictor of airport cybernetic performance in the regression model (Beta = 0.638, $p < 0.001$) validates the cybersecurity assessments of Lykou *et al*., [22] and Rossiter [7]. To contextualize this dominant finding, it is valuable to reference recent industry data. A recent report [30] indicates that 72 percent of airports worldwide are actively forecasting an increase in overall IT spend specifically targeting cybersecurity and biometric passenger-processing solutions to counter rising digital threat vectors. This global strategic focus mirrors the high consensus found among AeroLink's 544 respondents, who ranked the danger of cyberattacks as their foremost operational concern (Mean = 3.82 to 3.97). This finding also aligns with the automated multi-layered anomaly detection frameworks proposed by Saura *et al*., [24], confirming that security resilience is no longer an isolated technical requirement but the core foundation of contemporary cybernetic trust.

5.3 Explanatory Mechanisms and Technical Interpretations

The variation in response times recorded during the physical diorama testing can be explained by distinct hardware-level propagation and processing mechanisms. The Direct Radio Frequency module achieved the most rapid latency of 2.00 seconds because it operated via direct electromagnetic propagation with minimal signal-processing overhead and simple packet encapsulation. Conversely, the LiFi-inspired communication module recorded the longest response latency of 3.60 seconds. This delay was caused by the physical limitations of the infrared transceivers, including the slower rise and fall times of the emitting diodes, and the additional processing overhead required for optical signal modulation, demodulation, and receiver synchronization.

The relative predictive weights of the variables in the regression model also point to distinct perceptual mechanisms among airport stakeholders, which can be interpreted as follows:

1. Perceptual Dominance of Cybersecurity (Beta = 0.638): Stakeholders likely view cybersecurity as a fundamental baseline requirement for any digital system. If a system is perceived as vulnerable to malicious digital intrusion, ransomware, or unauthorized control, any operational benefits derived from real-time data integration, AI surveillance, or automated check-in are rendered void. Consequently, cybersecurity readiness is perceived as a critical gating factor, causing it to carry a disproportionately large weight in predicting overall cybernetic performance.

2. Moderate Weight of Communication Interference (Beta = 0.158): While voice and data disruptions are recognized as immediate operational hazards, stakeholders likely view these as localized, technical anomalies that can be mitigated through standard protocols, redundant channels, or voice read-back procedures. This lowers their perceived systemic threat level compared to cyberattacks.

3. Lower Weight of Scalability Limitations (Beta = 0.113): Although physical wired cabling constraints are strongly associated with airport cybernetics in bivariate analysis ($r = 0.802$), scalability is likely perceived by stakeholders as a long-term administrative, strategic, or capital-expenditure challenge rather than an active, daily threat to operational survival. Under multiple regression, where variables are evaluated simultaneously, the immediate operational urgency of cyberattacks and signal disruptions overshadows these long-term infrastructural challenges.

5.4 Methodological and Structural Limitations of the Study

While this research provides valuable empirical and experimental insights, several limitations must be acknowledged to contextualize the findings:

1. Correlational and Survey-Based Design: The survey component of this study relied on a cross-sectional correlational design. While the Pearson correlation and multiple regression analyses demonstrated highly significant predictive relationships, they cannot establish definitive causal links. The findings indicate strong associations and variance explanation in the model, but they do not prove that improving infrastructure scalability directly causes a quantitative enhancement in cybernetic efficiency.

2. Diorama-Scale Physical Prototype: The experimental testing of the AeroLink hardware was restricted to a prototype-scale, miniature airport diorama under controlled laboratory conditions. Physical propagation challenges that affect hybrid RF-LiFi architectures in large terminal buildings—such as beam divergence over long distances, signal scattering, line-of-sight blockages by heavy passenger volumes, atmospheric dispersion, and optical noise from fluctuating ambient lighting levels—were not fully evaluated at this scale.

3. Sample Profile and Geographic Generalizability: Although the sample size of 544 respondents was statistically robust, this study did not record the demographic profile of the participants, such as the ratio of passengers to operational staff, nor the geographic location of the regional hub where the data were collected. This lack of demographic specificity may limit the generalizability of the findings to different global airport networks with varying regulatory frameworks and technological baselines.

6. Conclusion

This study successfully developed and evaluated the AeroLink Intelligent Network System to optimize airport cybernetics by enhancing communication reliability, infrastructure scalability, and cybersecurity resilience. Physical prototype evaluation within a miniature airport diorama demonstrated the operational viability of integrating Radio Frequency, Light Fidelity, Artificial Intelligence, Internet of Things, and LiDAR-like technologies under a unified cybernetic architecture, with all components operating successfully within real-time response limits ranging from 2.00 to 3.60 seconds. Furthermore, statistical analysis of 544 stakeholders confirmed that these integrated technologies address critical operational bottlenecks, with multiple regression explaining 76.6 percent of the variance in airport cybernetics and identifying cyberattack risks as the most critical predictor. Theoretically, these outcomes validate the application of Cybernetic Theory to multi-layered airport systems through active feedback loops. Practically, the framework offers smart airports a scalable, wireless, and secure communication alternative to high-maintenance wired networks. Future research will focus on scaling the physical prototype to evaluate hybrid transmission performance within real-world terminal environments, specifically testing the effects of physical obstacles, ambient lighting noise, and line-of-sight blockages under dense passenger flows.

Acknowledgement
The authors gratefully acknowledge the support and facilities provided by Management and Science University (MSU).

References

[1] Alhammadi, Abdulraqeb, Ibraheem Shayea, Ayman A. El-Saleh, Marwan Hadri Azmi, Zool Hilmi Ismail, Lida Kouhalvandi, and Sawan Ali Saad. "Artificial intelligence in 6G wireless networks: Opportunities, applications, and challenges." *International Journal of Intelligent Systems* 2024, no. 1 (2024): 8845070. https://doi.org/10.1155/2024/8845070

[2] Basha, Aysha Siddhikha Husaini. "Architecting High-Density Wireless Networks for Mission-Critical Airport Operations." *Journal of Computer Science and Technology Studies* 7, no. 10 (2025): 31-41. https://doi.org/10.32996/jcsts.2025.7.10.4

[3] Ahmed, Waqas. "ADS-B communication in modern air traffic management: threats, risks and security solutions." *Science* 1 (2024): 100006. https://doi.org/10.70389/PJCS.100006

[4] Ukwandu, Elochukwu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, and Xavier Bellekens. "Cyber-security challenges in aviation industry: A review of current and future trends." *Information* 13, no. 3 (2022): 146. https://doi.org/10.3390/info13030146

[5] Yang, Hui-Hua, Yu-Hern Chang, and Yi-Hui Chou. "Subjective measures of communication errors between pilots and air traffic controllers." *Journal of Air Transport Management* 112 (2023): 102461. https://doi.org/10.1016/j.jairtraman.2023.102461

[6] Yang, Hui-Hua, Yu-Hern Chang, and Yi-Hui Chou. "Subjective measures of communication errors between pilots and air traffic controllers." *Journal of Air Transport Management* 112 (2023): 102461. https://www.doi.org/10.56726/IRJMETS43228

[7] Rossiter, Ash. "Smart airports and the evolving cyber threat." *Journal of Transportation Security* 18, no. 1 (2025): 26.https://doi.org/10.1007/s12198-025-00311-0

[8] Wavesight. (2025). Private Wireless Network Solutions for Digital Airport Operations: Resolving Fragmented Technologies and Scalability. Wavesight Whitepaper Series. https://wavesight.com/airline-and-airport-connectivity-solutions/

[9] Cyber Security Cooperative Research Centre. (2024). Smart Airports: Cyber Security Vulnerability and Mitigation Tool. CSCRC Research Report in partnership with TCS, AFP, and UNSW Canberra. https://cybersecuritycrc.org.au/smart-airports/

[10] Skosana, Siyabonga, Sibusiso Mlambo, Thabang Madiope, and Bonginkosi Thango. "Evaluating wireless network technologies (3G, 4G, 5G) and their infrastructure: A systematic review." *Available at SSRN 4992432* (2024). https://doi.org/10.20944/preprints202410.1331.v1

[11] García, Sergio Gallego, Rayco Rodríguez Reyes, and Manuel García García. "Design of a Conceptual Model for Improving Company Performance Based on Lean Management Applying the Viable System Model (VSM)." *European Journal of Formal Sciences & Engineering* 6, no. 2 (2023): 1 https://doi.org/10.2478/ejfe-2023-0011

[12] Kevadiya, T. Z., Kumar, P., Patel, S., and Sharma, A. (2024). The Cybernetics Perspective of Artificial Intelligence: Intelligent Control and Adaptive Systems. *Journal of Network Security*, 12, 26-30. https://doi.org/10.37591/JoNS.v12i01.138709

[13] Sabban, Albert, ed. *Innovations in Indoor Positioning Systems (IPS)*. BoD–Books on Demand, 2024.https://doi.org/10.5772/intechopen.111358

[14] Zhang, Xiaoxiao, D. E. N. G. Qihan, Yang Yang, Q. I. A. N. Shengsheng, H. U. I. Yi, Z. H. U. Yanbo, and C. A. I. Kaiquan. "Multi-task hierarchical network for semantic understanding of air traffic controller-pilot communication." *Chinese Journal of Aeronautics* (2025): 103812.https://doi.org/10.1016/j.cja.2025.103812

[15] Śliwa, Romana Ewa, Paweł Dymora, Mirosław Mazurek, Bartosz Kowal, Michał Jurek, Damian Kordos, Tomasz Rogalski et al. "The latest advances in wireless communication in aviation, wind turbines and bridges." *Inventions* 7, no. 1 (2022): 18. https://doi.org/10.3390/inventions7010018

[16] Abuhassna, Hassan, Samer Alnawajha, Fareed Awae, M. A. B. M. Adnan, and Bosede Iyiade Edwards. "Synthesizing technology integration within the Addie model for instructional design: A comprehensive systematic literature review." *Journal of Autonomous Intelligence* 7, no. 5 (2024): 1-28. https://doi.org/10.32629/jai.v7i5.1546

[17] Moiso, D. R. (2024). How to apply instructional design models to learning design. SessionLab. https://www.sessionlab.com/blog/instructional-design-models/

[18] Khan, L. U. (2021). Visible light communication: Applications, architecture, standardization, and research challenges. IEEE Communications Surveys & Tutorials, 23(2), 1398-1420.

[19] Vieira, Manuela, Manuel Augusto Vieira, Gonçalo Galvão, Paula Louro, Pedro Vieira, and Alessandro Fantoni. "Optimizing indoor airport navigation with advanced visible light communication systems." *Sensors* 24, no. 16 (2024): 5445.https://doi.org/10.3390/s24165445

[20] Vieira, Manuela, Manuel Augusto Vieira, Gonçalo Galvão, Paula Louro, Alessandro Fantoni, Pedro Vieira, and Mário Véstias. "Enhancing airport traffic flow: Intelligent system based on VLC, rerouting techniques, and adaptive reward learning." *Sensors* 25, no. 9 (2025): 2842. https://doi.org/10.3390/s25092842

[21] Hwilkowska-Kubala, A., and Huderek-Glapska, S. (2021). The sources of barriers to airport development: A dynamic approach. Journal of Air Transport Management, 90, 101959. https://doi.org/10.1016/j.jairtraman.2020.101959

[22] Lykou, Georgia, Argiro Anagnostopoulou, and Dimitris Gritzalis. "Smart airport cybersecurity: Threat mitigation and cyber resilience controls." *Sensors* 19, no. 1 (2018): 19. https://doi.org/10.3390/s19010019

[23] Polyswarm. (2026). Turbulence Ahead: Cyber Threats Targeting Aviation and Aerospace in 2026. Polyswarm Intelligence Report. https://blog.polyswarm.io/turbulence-ahead-cyber-threats-targeting-aviation-and-aerospace-in-2026

[24] Saura, Pablo Fernández, Jose Manuel Bernabé Murcia, Alejandro Molina Zarca, Jorge Bernal Bernabé, and Antonio Fernando Skarmeta Gomez. "Federated network intelligence orchestration for scalable and automated fl-based anomaly detection in b5g networks." In *2023 IEEE Future Networks World Forum (FNWF)*, pp. 1-6. IEEE, 2023.

[25] Bianzino, Aruna Prem, Andrea Basso, Giancarlo Caratti, Ciprian Comsa, Andrea Di Giglio, Carolina Garcia, Andreas Georgakopoulos et al. "Trials supported by smart networks beyond 5G: The TrialsNet approach." In *2023 IEEE Future Networks World Forum (FNWF)*, pp. 1-7. IEEE, 2023.

[26] Branson, R. K., Rayner, G. T., Cox, J. L., Furman, J. P., King, F. J., and Hannum, W. H. (1975). Interservice procedures for instructional systems development (vols. 1-5). Center for Educational Technology, Florida State University, Tallahassee, FL.

[27] IEEE Computer Society. (2023). IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 12: Light Communications (LiFi) (IEEE Std 802.11bb-2023). New York, NY: IEEE.

[28] IBM Corp. (2021). IBM SPSS Statistics for Windows, Version 28.0. Armonk, NY: IBM Corp.

[29] Cronbach, Lee J. "Coefficient alpha and the internal structure of tests." *psychometrika* 16, no. 3 (1951): 297-334. https://doi.org/10.1007/BF02310555

[30] SITA. (2024). Air Transport IT Insights 2024: Aviation Industry Ramps Up Focus on Cybersecurity Amid Record Investment. Geneva: SITA Publications. https://www.sita.aero/resources/blog/air-transport-it-insights-2024/