Journal of Industrial Engineering & Management Research

http://www.jiemar.org e-ISSN : 2722-8878

Vol. 7 No. 2 – April 2026

Layered CNS Interface Framework for Civil–Military Airspace Integration: A PRISMA-Based Systematic Review of Airspace Security Effectiveness

Budi Santoso

Universitas Pertahanan Republik Indonesia, (budi.santoso@doktoral.idu.ac.id)

Asep Adang Supriyadi

Universitas Pertahanan Republik Indonesia, (aadangsupriyadi@gmail.com)

Surachman Surjaatmadja

Universitas Pertahanan Republik Indonesia, (isur.atmadja@gmail.com)

Robby Mochammad Taufik

Universitas Pertahanan Republik Indonesia, (195dikreglx@gmail.com)

Afen Sena

Akademi Penerbang Indonesia, (afensena@mail.com)

Abstract

Airspace has evolved into a contested socio-technical domain in which civil aviation, military operations, and cyber infrastructures interact under increasing complexity yet remain structurally fragmented. Existing scholarship is dispersed across aviation safety, defense doctrine, and cybersecurity, limiting the development of integrative frameworks capable of explaining system-level security outcomes. While systems-of-systems (SoS) research predominantly emphasizes technical interoperability, the role of governance in structuring cross-domain integration remains insufficiently theorized.

This study addresses this gap through a PRISMA-based Systematic Literature Review (SLR) of 35 high-relevance sources indexed in Scopus, Web of Science, and ScienceDirect. Adopting a SoS perspective, it develops the Layered CNS Interface Framework (LCIF) as a governance-driven, multi-layer integration architecture linking policy, operational, technological, and cyber dimensions.

The synthesis suggests that airspace security effectiveness is shaped by three interdependent constructs—integration quality, interoperability, and adaptive capacity—within which civil–military air traffic management operates as a mediating mechanism translating structural integration into coordinated operational outcomes. These relationships are theoretically derived from cross-domain synthesis rather than empirically established.

The study contributes by extending SoS theory into the domain of security governance and by reconceptualizing interoperability as a multi-dimensional construct encompassing technical, institutional, and decision-making alignment. The LCIF model provides a theoretically grounded and empirically testable foundation, enabling future examination of multi-layer causal relationships through Structural Equation Modelling (SEM) in complex airspace systems.

Keywords

Airspace security; Civil–military integration; CNS systems; Air traffic management; Systems-of-systems; Cyber resilience

1. Introduction

Airspace has transitioned from a predominantly transportation-oriented domain into a contested strategic environment in which civil aviation, military defense systems, and digitally networked infrastructures interact under conditions of increasing operational complexity. This convergence intensifies coordination challenges, particularly in regions characterized by dense traffic flows and heightened geopolitical tensions, where airspace simultaneously underpins economic activity and national security imperatives (International Civil Aviation Organization (ICAO), 2016; North Atlantic Treaty Organization (NATO), 2016; Cui & Li, 2021; Zhang & Wang, 2020).

Despite growing policy attention, airspace governance remains structurally fragmented. In operational contexts with overlapping civil–military usage, misaligned coordination mechanisms generate tangible consequences, including degraded situational awareness, delayed response, and increased vulnerability to multi-domain disruptions (Australian Strategic Policy Institute [ASPI], 2021; Szayna et al., 2019). However, while such fragmentation is widely acknowledged, empirical and theoretical explanations of how it translates into system-level security inefficiencies remain limited.

This limitation is rooted in the disciplinary fragmentation of the literature. Aviation studies predominantly emphasize safety, efficiency, and regulatory compliance; defense scholarship focuses on command authority, threat detection, and operational readiness; while cybersecurity research highlights vulnerabilities such as GNSS spoofing and network intrusion. Although each domain demonstrates analytical depth, they remain weakly integrated, lacking cross-domain frameworks that systematically link governance mechanisms to measurable security outcomes (ICAO, 2016; NATO, 2016; European Union Agency for Cybersecurity [ENISA], 2023; Patriarca et al., 2022). As a result, airspace security is often examined through parallel analytical lenses rather than as an interdependent socio-technical system.

More critically, existing systems-of-systems (SoS) research—while conceptually suited to capturing interdependencies—remains predominantly oriented toward technical interoperability and system architecture. The governance dimension, particularly the role of institutional coordination in shaping system-level effectiveness, remains underdeveloped. Consequently, current studies seldom articulate causal mechanisms through which governance structures interact with technological and operational subsystems to produce observable security outcomes. This absence constrains the development of empirically testable and policy-relevant integration models (Levis & Athans, 1987; Rinaldi et al., 2001).

The research gap is therefore threefold: (1) persistent fragmentation across aviation, defense, and cybersecurity domains; (2) the absence of governance-integrated SoS frameworks capable of structuring cross-domain interactions; and (3) the lack of causal, operationalizable models linking integration mechanisms to airspace security effectiveness. These gaps are particularly salient in geopolitically sensitive regions such as the Indo-Pacific, where high-density civil aviation intersects with intensified military activity and evolving cyber threats, amplifying systemic vulnerabilities in the absence of coordinated governance architectures (ASPI, 2021; Szayna et al., 2019).

To address these limitations, this study proposes the Layered CNS Interface Framework (LCIF) as a governance-driven systems-of-systems integration model for civil–military airspace management. Moving beyond purely technical interoperability, LCIF conceptualizes integration as a multi-layer coordination mechanism encompassing policy, operational, technological, and cyber dimensions. By structuring controlled interaction across these layers, the framework seeks to enhance interoperability, enable coordinated decision-making, and support adaptive system resilience in complex multi-domain environments (MITRE, 2020; Christensen & Lægreid, 2007).

This study pursues three primary objectives: (1) to systematically identify and synthesize fragmentation patterns within the airspace security literature; (2) to develop a theoretically grounded conceptual model linking governance-driven integration to security outcomes; and (3) to formulate an analytically structured and empirically testable framework for future research.

The study contributes to the literature in three ways. First, it advances a theoretical contribution by extending systems-of-systems (SoS) theory into the domain of security governance, positioning governance not as a contextual variable but as a central mechanism shaping system-level effectiveness. Second, it offers a methodological contribution by integrating a PRISMA-based Systematic Literature Review (SLR) with theory-building and conceptual modelling, transforming fragmented interdisciplinary insights into a coherent analytical framework (Yin, 2018). Third, it provides a practical contribution by proposing a governance-oriented integration architecture that can inform policy design for civil–military coordination, CNS system alignment, and cyber resilience in complex airspace environments.

By reframing airspace as an integrated socio-technical and governance system, this study shifts the analytical focus from subsystem performance to the quality of cross-domain integration, thereby establishing a foundation for empirically testable models of airspace security effectiveness.

2. Literature Review and Hypothesis Development

2.1 Systems-of-Systems Security Governance

The systems-of-systems (SoS) perspective conceptualizes airspace as a heterogeneous architecture composed of civil aviation, military defense, and digital infrastructures operating under distributed control and partial autonomy (Alberts & Hayes, 2003; Jamshidi, 2009). Within this paradigm, system effectiveness is understood as an emergent property arising from interoperability, decentralized coordination, and dynamic interaction among subsystems (Levis & Athans, 1987; Rinaldi et al., 2001). However, the same characteristics that enable flexibility—modularity and autonomy—also introduce systemic fragility, particularly under conditions of tight coupling and high operational complexity (Perrow, 1999; Dekker, 2016; Dolgui et al., 2018).

A dominant strand within SoS research emphasizes technical architecture, interoperability standards, and engineering design. While this perspective has advanced understanding of system integration at the technological level, it remains insufficient in capturing governance dynamics—particularly the institutional arrangements, decision-making structures, and coordination mechanisms that regulate interactions among semi-autonomous subsystems. This reveals a persistent tension between decentralization and hierarchical control, where increased autonomy enhances flexibility but undermines coordinated response in high-stakes environments.

From a complex adaptive systems perspective, airspace exhibits non-linear interactions and feedback loops, where resilience depends on adaptive capacity and real-time coordination (Weick & Sutcliffe, 2007). Yet, governance remains under-theorized within SoS applications, limiting the ability to explain how institutional alignment shapes emergent system behavior.

Theoretical gap: Existing SoS literature lacks a governance-integrated framework capable of linking institutional coordination with system-level security outcomes.

Implication for LCIF: This gap necessitates extending SoS theory beyond technical integration toward a governance-driven architecture, forming the foundational logic of LCIF.

2.2 Civil–Military Integration in Airspace Management

Civil–military airspace integration is characterized by fundamentally divergent institutional logics: civil aviation prioritizes safety, efficiency, and regulatory compliance, whereas military systems emphasize security, control, and rapid threat response (NATO, 2016; Joint Chiefs of Staff, 2022). This divergence produces structural misalignment in operational protocols, decision hierarchies, and information-sharing practices, particularly under time-sensitive or contested conditions.

The dominant literature approaches this issue from two largely disconnected perspectives. Institutional studies emphasize coordination mechanisms and governance reforms, while technical studies focus on interoperability and system integration. However, neither perspective adequately captures the multi-layer interaction between governance structures and operational execution, resulting in partial and fragmented explanations of integration challenges.

This fragmentation reflects a deeper tension between safety-oriented stability and security-driven responsiveness, where efforts to optimize efficiency may inadvertently constrain adaptive response capabilities in adversarial scenarios. Moreover, existing models often assume coordination as a static condition rather than a dynamic process shaped by institutional alignment, situational awareness, and evolving threat environments.

Theoretical gap: There is no unified framework that integrates institutional, operational, and technological dimensions of civil–military coordination.

Implication for LCIF: Civil–military integration must be reconceptualized as a governance-mediated, multi-layer process, directly motivating the LCIF architecture.

2.3 CNS Systems and Air Traffic Management

Communication, Navigation, and Surveillance (CNS) systems form the technological backbone of air traffic management (ATM), enabling real-time coordination, safety assurance, and operational efficiency (ICAO, 2016; Cook et al., 2022; Cui & Li, 2021). The dominant perspective in this domain treats CNS as a safety-critical infrastructure, optimized for reliability, redundancy, and risk minimization.

However, this safety-centric orientation introduces limitations in contested or security-sensitive environments. CNS architectures are typically designed under assumptions of cooperative actors and stable operating conditions, which may not hold in scenarios involving adversarial interference, military operations, or cyber threats. As a result, CNS systems exhibit limited integration with defense infrastructures, creating vulnerabilities at the interface between civil and military domains.

This reflects a broader tension between technical interoperability and institutional interoperability. While systems may be technically compatible, the absence of aligned governance frameworks and decision protocols constrains their effective integration in practice.

Theoretical gap: CNS literature underestimates the role of governance in enabling cross-domain interoperability, treating integration primarily as a technical challenge.

Implication for LCIF: Effective integration requires embedding CNS within a governance-coordinated interface, a core principle operationalized in LCIF.

2.4 Cybersecurity and Airspace Vulnerabilities

The increasing digitalization of airspace has transformed it into a cyber-physical system exposed to evolving threats such as GNSS spoofing, signal jamming, and data manipulation (ENISA, 2023; European Commission, 2022; Zhang & Wang, 2020). The dominant cybersecurity perspective focuses on technical risk detection, mitigation, and system

hardening, often treating cyber threats as discrete and isolatable phenomena.

However, empirical evidence suggests that failures in complex systems rarely originate from isolated technical faults but instead emerge from latent systemic conditions, including weak coordination, fragmented governance, and misaligned institutional responses (Reason, 2000). Cyber risks, therefore, propagate across interconnected subsystems, affecting not only technical performance but also operational coordination and decision-making processes.

This reveals a critical tension between technical security solutions and systemic resilience. While cybersecurity measures may strengthen individual components, their effectiveness is limited without integration into broader governance frameworks that coordinate responses across domains.

Theoretical gap: Cybersecurity research remains weakly integrated with governance and airspace management literature, limiting its explanatory power in multi-domain environments.

Implication for LCIF: Cyber resilience must be embedded as a core governance layer, reinforcing the multi-layer integration logic of LCIF.

2.5 Hypothesis Development

Synthesizing insights across the reviewed domains, the PRISMA-based SLR indicates that airspace security effectiveness emerges from the interaction of governance integration, interoperability, and adaptive capacity within a complex SoS environment. These dimensions are not independent; rather, they operate through structured relationships linking institutional alignment to operational outcomes.

LCIF is therefore conceptualized as the primary integration mechanism, enabling coordinated interaction across policy, operational, technical, and cyber layers. Within this structure, Civil–Military Air Traffic Management (C-M ATM) functions as a mediating mechanism, translating structural integration into real-time coordination. Adaptive capacity—captured through Multi-Domain Threat Adaptability (MDTA) and Strategic Defense Posture (SDP)—enhances system responsiveness under dynamic threat conditions, while Political–Strategic Support (PS) conditions the strength of these relationships.

2.5.1 Direct Effects

H1: LCIF → C-M ATM (+)
H2: LCIF → ASE (+)
H3: SDP → C-M ATM (+)
H4: SDP → ASE (+)
H5: MDTA → C-M ATM (+)
H6: MDTA → ASE (+)
H7: C-M ATM → ASE (+)

2.5.1 Mediation Effects

H8: C-M ATM mediates LCIF → ASE
H9: C-M ATM mediates SDP → ASE
H10: C-M ATM mediates MDTA → ASE

2.5.3 Moderation Effects (Political–Strategic Support)

H11: PS moderates LCIF → C-M ATM
H12: PS moderates SDP → C-M ATM
H13: PS moderates MDTA → C-M ATM
H14: PS moderates C-M ATM → ASE

3. Methodology

3.1 Research Design and Review Protocol

This study adopts a Systematic Literature Review (SLR) guided by the PRISMA 2020 framework to ensure methodological transparency, replicability, and auditability (Page et al., 2021). Unlike narrative reviews, this approach follows a structured protocol comprising identification, screening, eligibility, and inclusion stages, enabling systematic reduction of bias and traceability of decisions.

The review is designed as an explanatory, theory-building inquiry, aiming to construct the Layered CNS Interface Framework (LCIF) within a systems-of-systems (SoS) governance paradigm. Consistent with theory-building logic, relationships among constructs are conceptually derived rather than empirically tested (Yin, 2018). The protocol specifies search strategy, selection criteria, quality thresholds, and coding procedures prior to analysis to ensure procedural consistency.

3.2 Data Sources and Search Strategy

3.2.1 Database Selection

Three major databases were selected to ensure comprehensive interdisciplinary coverage:

Scopus: broad indexing across engineering, aviation, and policy research;

Web of Science (WoS): high-impact, rigorously curated journals; and

ScienceDirect: domain-specific depth in aerospace, systems engineering, and transport

This combination minimizes publication bias while ensuring inclusion of peer-reviewed, high-impact studies relevant to airspace security, systems engineering, and governance.

3.2.2 Search Strings (Boolean Queries)

Search queries were constructed using Boolean operators, truncation, and field restrictions (TITLE-ABS-KEY), combining core constructs and related concepts:

("airspace security" OR "airspace management" OR "air traffic management")

AND

("civil-military integration" OR "civil military coordination" OR "joint airspace")

AND

("CNS systems" OR "communication navigation surveillance" OR "ATM systems")

AND

("systems of systems" OR "SoS" OR "integrated systems")

AND

("cybersecurity" OR "cyber resilience" OR "GNSS spoofing" OR "signal jamming")

AND

("command and control" OR "integrated air defense" OR "multi-domain operations")

3.2.3 Search Parameters

Fields searched: Title, Abstract, Keywords

Timeframe: 2000–2025

Language: English

Document type: Peer-reviewed journal articles

The search was conducted iteratively, with refinement of keywords to balance sensitivity (coverage) and specificity (relevance).

3.3 Inclusion, Exclusion, and Screening Procedure

3.2.1 Inclusion Criteria

Studies were included if they met all of the following: indexed in Scopus or Web of Science (Q1/Q2 journals), published between 2000–2025, written in English

Directly relevant to at least one core construct: Airspace security / ATM, Civil–military integration, CNS systems, Cybersecurity in aviation, and Systems-of-systems.

3.2.2 Exclusion Criteria

Studies were excluded if they: were non-peer-reviewed (reports, editorials, conference abstracts without full papers), lacked theoretical or methodological rigor, focused on unrelated domains (e.g., purely mechanical aviation engineering without system integration context), and were duplicates across databases

3.4 PRISMA Flow and Study Selection

The selection process followed PRISMA 2020 stages with explicit numerical tracking:

Identification: 135 records retrieved (Scopus = 62; WoS = 41; ScienceDirect = 32).

Duplicate removal: 25 duplicates removed → 110 records retained.

Screening (title/abstract review): 60 records excluded due to irrelevance → 50 records eligible.

Eligibility (full-text assessment): 15 articles excluded due to insufficient theoretical or methodological quality.

Final inclusion: 35 studies retained for synthesis, of which: 20 used for in-depth conceptual modelling, and 15 used for supporting thematic enrichment

This process ensures full transparency and replicability of study selection.

3.5 Quality Assessment Framework

To ensure analytical rigor, all included studies were evaluated using a five-criteria scoring system (scale: 1 = low, 5 = high):

Theoretical grounding (clarity and robustness of conceptual framework), methodological rigor (research design, data validity, analytical depth), relevance (alignment with core constructs), interdisciplinary integration (cross-domain applicability), citation impact (journal quality and scholarly influence), and studies scoring ≥3.5 (average) were retained. lower-scoring studies were excluded during eligibility screening.

3.6 Coding Procedure and Reliability

3.6.1 Coding Framework

A structured coding matrix was developed to extract and standardize information across studies: Bibliographic information, Domain classification (aviation, defense, cybersecurity), Theoretical framework (SoS, resilience, governance), Methodology, Key findings, and Identified gaps

Inter-Coder Reliability to ensure consistency: two independent coders analyzed the dataset, inter-coder agreement was assessed using Cohen's Kappa ($\kappa = 0.82$), indicating strong reliability, and Discrepancies were resolved through iterative discussion and consensus

This procedure enhances the objectivity and reproducibility of the synthesis process.

3.7 Data Analysis and Synthesis Strategy

The analysis integrates three complementary techniques:

Thematic synthesis: Identifies recurring patterns in governance, interoperability, and cyber resilience.

Conceptual mapping: Models interdependencies within SoS environments (Rinaldi et al., 2001).

Theory integration: Combines SoS, resilience, and governance theories into a unified analytical structure (Linkov et al., 2018).

This multi-method synthesis enables the transition from fragmented evidence to a coherent, theory-driven framework (LCIF).

3.8 Construct Operationalization

Concepts identified through synthesis were translated into analytically tractable constructs:

LCIF (integration mechanism)

C-M ATM (mediator: interoperability)

MDTA and SDP (adaptive capacity)

PS (moderator: political–strategic support)

ASE (dependent variable: system-level outcome)

Each construct is defined by dimensions and indicators grounded in the reviewed literature, ensuring construct validity and readiness for SEM-based empirical testing.

3.9 Methodological Contribution

This study advances SLR methodology in two ways:

From descriptive synthesis to theory-building model. Integrates PRISMA rigor with SoS-based conceptual modelling.

From domain fragmentation to governance integration. Produces a structured, multi-layer framework (LCIF) linking governance, operations, technology, and cyber dimensions

Accordingly, the methodology not only ensures transparency and replicability but also enables the development of an empirically testable, governance-driven integration model.

4. Results

4.1 Cross-Domain Fragmentation and Structural Gaps

The SLR reveals a structurally fragmented knowledge base reflecting core characteristics of systems-of-systems (SoS), including decentralized control, heterogeneous subsystems, and weak integrative governance (Maier, 1998; Jamshidi, 2009). Three dominant domains—aviation safety, defense, and cybersecurity—exhibit substantial internal sophistication but remain analytically and institutionally disconnected.

Aviation research, grounded in ICAO frameworks, prioritizes safety, efficiency, and CNS-enabled traffic management, yet largely treats airspace as a technical-operational environment with limited integration of security considerations (ICAO, 2016, 2018). In contrast, defense literature conceptualizes airspace as a contested battlespace, emphasizing command-and-control and integrated air defense architectures, while largely excluding civilian infrastructures (NATO, 2016). Cybersecurity studies identify escalating

vulnerabilities—such as GNSS spoofing, signal jamming, and data manipulation—associated with digitalized CNS/ATM systems, but typically isolate these risks from broader governance structures (ENISA, 2023).

This domain separation produces horizontal fragmentation, where safety, defense, and cyber logics evolve in parallel rather than as interdependent components of a unified socio-technical system. Such fragmentation constrains system-level understanding and limits the development of integrative frameworks capable of explaining airspace security effectiveness under conditions of interdependence and coordination complexity (Baxter & Sommerville, 2011; Rinaldi et al., 2001).

4.2 Thematic Convergence: Governance, Interoperability, and Cyber Risk

Across domains, four convergent patterns emerge.

First, a persistent governance gap is evident. Existing approaches—despite drawing on whole-of-government principles—remain institutionally bounded and insufficiently equipped to coordinate civil–military–cyber interactions in multi-domain environments (Christensen & Lægreid, 2007; Pierre & Peters, 2020; NATO, 2016; Joint Chiefs of Staff, 2022; Szayna et al., 2019). This limits synchronized response and integrated situational awareness.

Second, interoperability constraints are consistently identified as a critical bottleneck. Divergences in protocols, standards, and organizational cultures inhibit real-time coordination, particularly in high-tempo scenarios such as unauthorized incursions or grey-zone operations (ENISA, 2023; Zhang & Wang, 2020; Humayed et al., 2017; Kotenko & Saenko, 2022; Linkov et al., 2018). Interoperability thus emerges not merely as a technical issue, but as a combined technical–institutional challenge.

Third, cyber vulnerabilities are increasingly central. The expansion of digital CNS infrastructures amplifies systemic exposure to disruption, positioning cyber risk as a cross-domain threat affecting both operational continuity and coordination integrity (ENISA, 2023; Zhang & Wang, 2020; Humayed et al., 2017).

Fourth, the literature exhibits a deficit of causal and empirically testable models, with limited use of robust analytical frameworks such as Structural Equation Modelling (SEM) to link integration mechanisms with security outcomes (Hair et al., 2019; Kline, 2016). This constrains predictive capacity and policy relevance.

Collectively, these findings indicate that airspace security challenges are structurally rooted in fragmented governance, constrained interoperability, and systemic cyber exposure, necessitating an integrative analytical framework.

4.3 Construct Development and Synthesis

Building on these findings, the synthesis reconceptualizes Airspace Security Effectiveness (ASE) as an emergent system-level outcome arising from interdependent subsystems within an SoS architecture (Maier, 1998; Jamshidi, 2009). Three analytically linked dimensions are derived.

First, governance-driven integration addresses the identified coordination gap, capturing the extent to which institutional alignment enables cross-domain interaction (Pierre & Peters, 2020). This dimension is operationalized through the Layered CNS Interface Framework (LCIF).

Second, interoperability reflects the capacity for real-time coordinated action across heterogeneous systems. It is operationalized through Civil–Military Air Traffic Management (C-M ATM), conceptualized as a mediating mechanism translating structural integration into operational coordination (Rinaldi et al., 2001).

Third, adaptive capacity captures system resilience under dynamic and multi-domain threats, incorporating constructs such as Multi-Domain Threat Adaptability (MDTA) and Strategic Defense Posture (SDP) (Hollnagel, 2022; Weick & Sutcliffe, 2007).

These dimensions form a layered and interdependent structure, where governance integration enables interoperability, which in turn supports adaptive capacity. Importantly, contextual variables—such as political commitment and threat intensity—emerge as moderating conditions influencing the strength and consistency of these relationships (Buzan & Wæver, 2003; World Bank, 2021).

This synthesis transforms fragmented domain knowledge into a **coherent, multi-level construct model**, directly informing hypothesis development.

4.4 Structural Model Formulation

To operationalize these relationships, the synthesized constructs are formalized into a Structural Equation Model (SEM), enabling analysis of latent variables and multi-variable interactions (Hair et al., 2019).

Within this structure:

LCIF functions as the primary integration mechanism

C-M ATM operates as a mediator linking integration to outcomes

MDTA and SDP act as complementary predictors of system adaptability

Political–strategic factors serve as moderating variables

This model captures both direct and indirect pathways through which governance-driven integration may influence ASE, while accommodating contextual variability.

The SEM formulation provides a theoretically grounded and empirically testable architecture, enabling future validation using covariance-based or variance-based approaches.

5. Discussion

5.1 Fragmentation as a Systemic Condition, Not an Anomaly

The findings indicate that fragmentation in airspace security should not be interpreted as a series of isolated coordination failures, but as a systemic property of a loosely coupled systems-of-systems (SoS) architecture characterized by distributed authority and partial subsystem autonomy (Maier, 1998; Perrow, 1999). In such environments, aviation, defense, and cybersecurity domains evolve according to distinct institutional logics, generating persistent misalignment across governance, operational, and technical layers. Consequently, inefficiencies in interoperability and delayed coordination are structurally produced rather than contingently induced.

From this perspective, the absence of integrative governance mechanisms constrains the emergence of system-level effectiveness. The Layered CNS Interface Framework (LCIF) addresses this condition not by eliminating subsystem autonomy, but by structuring interdependencies through coordinated governance layers. However, this also introduces a critical tension: integration enhances coordination, yet excessive coupling may increase systemic fragility under conditions of failure propagation.

5.2 Extending SoS Theory into the Governance Domain

This study advances SoS theory by repositioning governance—not technology—as the primary coordinating mechanism of system effectiveness. While classical SoS literature emphasizes interoperability and architectural design, the findings suggest that governance

structures regulate how semi-autonomous subsystems interact, exchange information, and synchronize decisions.

LCIF operationalizes this shift through a multi-layer architecture (policy, operational, technical, cyber), reframing interoperability as a multi-dimensional construct encompassing institutional alignment and decision coherence alongside technical compatibility. This extension bridges systems engineering and public governance, but also exposes an inherent contradiction: SoS effectiveness requires decentralized adaptability, yet governance-driven integration introduces elements of hierarchical coordination. The resulting balance between flexibility and control becomes a defining condition of system performance.

5.3 Cross-Domain Contradictions and Trade-offs

The comparative synthesis reveals that each domain embodies a distinct—and partially incompatible—optimization logic. Aviation prioritizes safety, predictability, and efficiency within regulated environments (ICAO, 2016, 2018), whereas defense systems emphasize command authority, rapid response, and threat dominance (NATO, 2016). Cybersecurity, in turn, foregrounds system vulnerability, resilience, and adversarial disruption (ENISA, 2023).

These divergent priorities generate structural trade-offs. Safety-oriented standardization may limit operational flexibility in contested scenarios; military command hierarchies may conflict with civilian regulatory frameworks; and cybersecurity protocols may impose constraints on data sharing and system openness. The absence of integrative frameworks means that these trade-offs are managed implicitly rather than strategically. LCIF provides a conceptual mechanism to make these tensions explicit and governable, yet its effectiveness depends on the ability to reconcile competing institutional mandates without undermining domain-specific strengths.

5.4 Integration Paradox: Over-Integration vs Under-Coordination

A central insight emerging from the analysis is the integration paradox inherent in complex SoS environments. Under-coordination—characterized by fragmented governance and weak interoperability—produces blind spots in situational awareness and delays in response. Conversely, over-integration—through tightly coupled systems and centralized control—may amplify cascading failures and reduce adaptive flexibility.

LCIF navigates this paradox by proposing a layered coordination logic in which integration is selective, modular, and governance-driven. The policy layer defines boundaries and coordination rules; the operational layer enables real-time synchronization; the technical layer supports data interoperability (MITRE, 2020); and the cyber layer safeguards system resilience (Weick & Sutcliffe, 2007). Importantly, these layers interact non-linearly: misalignment at the governance level can propagate downward, while technological vulnerabilities can escalate upward into systemic risks. Thus, effectiveness depends not on maximal integration, but on calibrated alignment across layers.

5.5 Contextual Contingency and Boundary Conditions

The explanatory power of LCIF is inherently context-dependent. In geopolitically contested regions such as the Indo-Pacific, where high-density civil aviation intersects with military activity and evolving cyber threats, the costs of fragmentation are amplified and the demand for governance-driven integration becomes more acute (Buzan & Wæver, 2003). In contrast, in lower-risk environments, the marginal benefits of deep integration may not justify the institutional and operational costs.

This suggests that integration–security relationships are contingent upon political commitment, institutional capacity, and threat intensity. LCIF should therefore be interpreted as a conditional rather than universal model, whose applicability varies across geopolitical and operational contexts.

5.6 Implications for Theory and Empirical Research

Theoretically, this study shifts the analytical focus from subsystem optimization to governed interdependence as the primary driver of system-level outcomes. However, the proposed relationships remain conceptually derived. Empirical validation is required to assess the strength, direction, and potential non-linearity of these relationships.

Future research should employ Structural Equation Modelling (SEM) to test the hypothesized multi-layer interactions, complemented by comparative case studies to capture contextual variability. Multi-method approaches are particularly critical to bridge the gap between abstract modelling and operational realities in complex airspace environments.

5.7 Policy Implications: Integration as a Strategic Capability

The analysis suggests a clear policy implication: airspace security effectiveness depends less on enhancing individual subsystems than on governing their interaction. This requires institutionalizing civil–military coordination architectures, aligning technical interoperability with governance frameworks, and embedding cybersecurity as an integral layer of system design rather than a peripheral function.

Crucially, integration should be treated as a strategic capability rather than a purely technical objective. Over-centralization risks systemic brittleness, while persistent fragmentation sustains vulnerability. Effective policy must therefore calibrate integration—balancing coordination, autonomy, and resilience—within a multi-domain, dynamically evolving threat environment.

6. Conclusion

This study establishes that airspace security effectiveness is fundamentally a function of governed integration across civil, military, and cyber domains within a systems-of-systems (SoS) architecture. Rather than emerging from isolated subsystem performance, security outcomes are shaped by the quality of coordination, interoperability, and institutional alignment across interdependent components (Levis & Athans, 1987; Maier, 1998; Jamshidi, 2009). This reframing shifts the analytical focus from technical optimization to the governance structures that regulate interaction in complex, multi-domain environments.

The Layered CNS Interface Framework (LCIF) constitutes the study's central contribution. By integrating policy, operational, technical, and cyber layers into a unified architecture, LCIF advances a governance-driven model of airspace integration. In contrast to technology-centric approaches, it positions governance as the enabling condition for controlled information exchange, coordinated decision-making, and systemic resilience under conditions of uncertainty and threat (MITRE, 2020).

Theoretically, this study extends SoS scholarship into the domain of security governance by conceptualizing integration as a layered and interdependent mechanism through which governance alignment structures operational coordination and adaptive capacity. Within this perspective, fragmentation is not merely a technical deficiency but a structural governance condition that constrains system-level effectiveness.

However, the findings remain conceptually derived. As a PRISMA-based SLR, the study does not establish causal relationships empirically, and its conclusions are bounded by dataset selectivity and interdisciplinary scope. This limitation underscores the need for systematic empirical validation.

From a policy standpoint, the implications are decisive: effective airspace security requires institutionalized civil–military coordination, governance-aligned CNS integration, and the embedding of cybersecurity as a core architectural layer. Integration must therefore be

treated as a strategic capability, calibrated across governance and operational domains rather than pursued as a purely technical objective.

Future research should rigorously test the LCIF model using Structural Equation Modelling (SEM) and complementary mixed-method designs to evaluate causal pathways, non-linear effects, and contextual variability across geopolitical environments. Such efforts are essential to transition from conceptual synthesis to evidence-based governance models.

Overall, this study advances a paradigm shift from fragmented, domain-specific analyses toward an integrated, governance-centric model of airspace security, positioning governed integration as the primary determinant of effectiveness in complex systems-of-systems environments.

REFERENCES

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command and control in the information age*. CCRP Publication Series.

Australian Strategic Policy Institute. (2021). *Air and maritime power in the Indo-Pacific: Understanding regional security dynamics*. ASPI.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Buzan, B., & Wæver, O. (2003). *Regions and powers*. Cambridge University Press.

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. *Public Administration Review, 67*(6), 1059–1066. https://doi.org/10.1111/j.1540-6210.2007.00797.x

Choi, J., & Kim, K. (2023). Cyber threat intelligence-based risk assessment model for aviation systems. *Journal of Air Transport Management, 110*, 102413. https://doi.org/10.1016/j.jairtraman.2023.102413

Cook, A. J., Tanner, G., & Anderson, S. (2022). Evaluating the resilience of European air traffic management system under disruption. *Journal of Air Transport Management, 102*, 102226. https://doi.org/10.1016/j.jairtraman.2022.102226

Cui, Q., & Li, Y. (2021). Air traffic management efficiency and resilience: A data-driven analysis. *Transportation Research Part C: Emerging Technologies, 124*, 102962. https://doi.org/10.1016/j.trc.2020.102962

Dekker, S. (2016). Resilience engineering and safety management: A systemic approach. *Safety Science, 82*, 1–8. https://doi.org/10.1016/j.ssci.2015.08.003

Dolgui, A., Ivanov, D., & Sokolov, B. (2018). Ripple effect in the supply chain: An analysis and recent literature. *International Journal of Production Research, 56*(1–2), 414–430. https://doi.org/10.1080/00207543.2017.1387680

European Commission. (2022). *EU cybersecurity strategy for the digital decade*.

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape for the aviation sector*.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.

Hollnagel, E. (2022). Safety-II in practice: Developing the resilience potentials. *Safety Science, 147*, 105646. https://doi.org/10.1016/j.ssci.2021.105646

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

International Civil Aviation Organization. (2016). *Global air navigation plan* (Doc 9750, 5th ed.).

International Civil Aviation Organization. (2018). *Global air traffic management operational concept* (Doc 9854).

International Civil Aviation Organization. (2022). *ICAO aviation cybersecurity strategy*.

Ivanov, D., & Dolgui, A. (2022). A digital supply chain twin for managing disruption risks and resilience in the era of Industry 4.0. *International Journal of Production Research, 60*(5), 163–178. https://doi.org/10.1080/00207543.2021.1990020

Jamshidi, M. (2009). *Systems of systems engineering: Innovations for the 21st century*. Wiley.

Joint Chiefs of Staff. (2022). *Joint all-domain command and control (JADC2)*. U.S. Department of Defense.

Klein, G. (2008). Naturalistic decision making. *Human Factors, 50*(3), 456–460. https://doi.org/10.1518/001872008X288385

Kline, R. B. (2016). *Principles and practice of structural equation modelling* (4th ed.). Guilford Press.

Kotenko, I., & Saenko, I. (2022). Cyber resilience in aviation systems: Challenges and solutions. *Computers & Security, 114*, 102599. https://doi.org/10.1016/j.cose.2021.102599

Levis, A. H., & Athans, M. (1987). On the theory of command-and-control systems. *IEEE Transactions on Systems, Man, and Cybernetics, 17*(6), 1054–1067. https://doi.org/10.1109/TSMC.1987.4309068

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M.-V. (2018). Resilience metrics for cyber systems. *Environment Systems and Decisions, 38*(3), 1–10. https://doi.org/10.1007/s10669-018-9697-5

Maier, M. W. (1998). Architecting principles for systems-of-systems. *Systems Engineering, 1*(4), 267–284. https://doi.org/10.1002/sys.3890010404

MITRE Corporation. (2020). *Systems engineering guide for systems of systems (SoS)* (Report No. MITRE-ENG-2020-001).

National Aeronautics and Space Administration. (2018). *Air traffic flow management in the national airspace system* (NASA/TP-2018-219824).

North Atlantic Treaty Organization. (2016). *Allied joint doctrine for integrated air and missile defense (AJP-3.3)*.

Organization for Economic Co-operation and Development. (2011). *Together for better public services: Partnering with citizens and civil society*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Patriarca, R., Di Gravio, G., Costantino, F., & Tronci, M. (2022). The functional resonance analysis method for systemic risk assessment in complex socio-technical systems. *Safety Science, 147*, 105634. https://doi.org/10.1016/j.ssci.2021.105634

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Pierre, J., & Peters, B. G. (2020). *Governance, politics and the state* (2nd ed.). Macmillan.

Reason, J. (2000). Human error: Models and management. *BMJ, 320*(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25. https://doi.org/10.1109/37.969131

Stolzer, A. J., Halford, C. D., & Goglia, J. J. (2016). *Safety management systems in aviation*. Routledge.

Sun, X., Wandelt, S., & Zhang, A. (2022). Resilience of air transportation systems: A review and future research directions. *Transport Reviews, 42*(1), 1–30. https://doi.org/10.1080/01441647.2021.1977790

Szayna, T. S., Larson, E. V., O'Mahony, A., Robson, S., & Young, S. (2019). *Assessing the Army's multi-domain operations: Implications for future warfare* (RR-2787-A). RAND Corporation.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.

World Bank. (2021). *World development report 2021: Data for better lives*.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Zhang, J., & Wang, H. (2020). Cybersecurity risk assessment in aviation systems. *Journal of Air Transport Management, 87*, 101859. https://doi.org/10.1016/j.jairtraman.2020.101859

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137–150. https://doi.org/10.1016/j.ress.2016.02.009