OPEN ACCESS

Int. Jr. of Contemp. Res. in Multi. *PEER-REVIEWED JOURNAL* *Volume 5 [Special Issue 1] Year 2026*

Research Article

Integration of Science and Technology in Interdisciplinary Research: A Systematic Literature Review with an Aviation Cybersecurity Lens

Ojaswini Malhotra [1*], Aparna Malhotra [2]

[1] Lecturer, Teaching Fellow, School of ICT, Griffith University, Australia

[2] Professor, Kaplan Business School, Griffith University, Australia

Corresponding Author: *Ojaswini Malhotra

DOI: https://doi.org/10.5281/zenodo.21354799

Abstract

Interdisciplinary research (IDR) is increasingly the default mode for addressing complex socio-technical problems, yet "integration" remains difficult because disciplines differ in epistemic norms, methods, and validation standards. Concurrently, research technologies, data infrastructures, workflow systems, modelling platforms, and AI-enabled tools are reshaping how integration occurs by mediating translation, standardisation, and coordination across disciplinary boundaries. Aviation cybersecurity provides a high-stakes exemplar: it is inherently interdisciplinary (safety engineering, avionics, human factors, software assurance, cryptography, governance) and constrained by stringent airworthiness and regulatory regimes (EASA, 2023; ICAO, 2021). Understanding the mechanisms by which science-and-technology integration enables (or distorts) interdisciplinary outcomes is therefore central to both knowledge production and safety-critical system stewardship.

Following PRISMA 2020 for systematic review reporting (Page *et al*., 2021) and PRISMA-S for search transparency (Rethlefsen *et al*., 2021), we conducted a structured search and thematic synthesis of peer-reviewed scholarship and authoritative standards/reports on interdisciplinary integration mechanisms and enabling research technologies. We used mixed-evidence appraisal guidance (e.g., MMAT) where applicable (Hong *et al*., 2018). Aviation cybersecurity literature and governance documents were included as a domain-specific lens, emphasizing airworthiness security process standards and sector-level cyber strategy and incident governance (EASA, 2023; ICAO, 2021; RTCA, n.d.; EUROCAE, 2014).

Evidence converges on five integration layers epistemic, methodological, infrastructure/data, socio-organizational, and governance and shows that technology functions as *boundary infrastructure* that actively shapes integrative possibilities (Star & Griesemer, 1989; Wilkinson *et al*., 2016). In aviation cybersecurity, integration is operationalized through lifecycle security processes and compliance structures (e.g., ED-202A/DO-326A family referenced by EASA guidance), alongside sector-level coordination pillars such as information sharing, incident management, and capacity building (EASA, 2023; ICAO, 2021). Reviews of aviation cyber threats highlight expanding attack surfaces across aircraft systems, aeronautical communications, ATM/airport ecosystems, and supply chains, amplifying the need for interdisciplinary

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 06-05-2026
- **Accepted:** 10-07-2026
- **Published:** 14-07-2026
- **IJCRM:**5(SP1); 2026: 141-145

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Malhotra O, Malhotra A. Integration of Science and Technology in Interdisciplinary Research: A Systematic Literature Review with an Aviation Cybersecurity Lens. Int J Contemp Res Multidiscip. 2026;5(SP1):141-145.

Access this Article Online

www.multiarticlesjournal.com

integration that is measurable and governable (EUROCONTROL, 2021; Mäurer, 2022; Ukwandu *et al*., 2022). We propose an integrative framework positioning science-and-technology integration as a coupled socio-technical process where platforms, standards, and workflows are not merely supportive tooling but constitutive elements of interdisciplinary knowledge integration. For safety-critical domains like aviation, integration must be treated as auditable lifecycle work with explicit governance, not an informal collaboration outcome.

KEYWORDS: Interdisciplinarity, convergence research, knowledge integration, boundary objects, FAIR data; research infrastructure, aviation cybersecurity, airworthiness security, cyber-physical systems, governance

1. INTRODUCTION

Interdisciplinary research is routinely invoked to confront complex challenges, but success hinges on integration, how heterogeneous concepts, data, methods, and accountability structures are aligned into coherent outcomes. Integration is not synonymous with collaboration; it is a multi-layered accomplishment requiring epistemic translation, methodological coupling, infrastructural interoperability, and governance legitimacy (Star & Griesemer, 1989; Stokols *et al*., 2008) [14, 15]. At the same time, science is becoming more team-based and increasingly mediated by shared technological systems (Wuchty *et al*., 2007) [18]. These systems repositories, workflow managers, modelling platforms, and standardization regimes shape what questions can be asked, what evidence is legible, and what forms of reuse are possible (Wilkinson *et al*., 2016) [17]. This is especially visible in convergence-oriented research agendas that explicitly target trans disciplinary integration for real-world impact (National Research Council, 2014) [9].

Aviation cybersecurity offers a sharp, slightly terrifying case study: aircraft and air traffic ecosystems are cyber-physical, globally networked, and intensely regulated. The domain demands integration between safety engineering, avionics architecture, secure communications, software assurance, operations, human factors, and policy. It also provides unusually explicit artefacts of integration airworthiness security process specifications and acceptable means of compliance illustrating how integration is institutionalized through standards and governance (EASA, 2023; EUROCAE, 2014; RTCA, n.d.) [1, 2, 13]. Sector-level strategy frameworks (e.g., ICAO's pillars) further show integration as a multi-stakeholder governance problem spanning information sharing, incident management, and capacity building (ICAO, 2021) [6].

Research Questions

- **RQ1:** How does the literature conceptualize and operationalize "integration" in interdisciplinary research?
- **RQ2:** What roles do research technologies (platforms, standards, workflows, AI-enabled tooling) play in enabling or constraining integration?
- **RQ3:** How is integration evaluated (indicators, outcomes, proxies), and what are the limits of current measurement approaches?
- **RQ4:** What does aviation cybersecurity reveal about integration in high-stakes, safety-critical interdisciplinary research?

2. METHODS

2.1 REVIEW DESIGN AND REPORTING

This review is reported using PRISMA 2020 guidance (Page *et al*., 2021) [10] and PRISMA-S recommendations for documenting search strategies (Rethlefsen *et al*., 2021) [12]. Given the topic's cross-field nature, we used a mixed-evidence synthesis approach: empirical studies, conceptual frameworks, and authoritative standards/reports were included when they directly addressed integration mechanisms and/or technology-mediated integration.

2.2 Eligibility Criteria

Inclusion:

- Explicit focus on interdisciplinary or transdisciplinary integration (mechanisms, theory, or evaluation).
- Explicit discussion of technology's role (data standards, infrastructures, cyberinfrastructure, workflows, AI tools) *or*integration mechanisms that are materially enacted via technical artifacts (e.g., boundary objects, ontologies, shared repositories).
- Aviation cybersecurity sources were included when they addressed integration across technical, organizational, and governance layers (e.g., airworthiness security processes; ATM cyber resilience governance; aeronautical communications security gaps).
- Peer-reviewed articles and high-authority institutional / standards documents.

Exclusion:

- Advocacy-only pieces lacking definable mechanisms or evaluable constructs.
- Purely technical papers without interdisciplinarity / integration relevance.

2.3 Information sources and search strategy

Searches were performed across multidisciplinary scholarly venues and high-authority institutional sources. A representative Boolean string was iteratively refined: ("interdisciplinary research" OR transdisciplinary OR "team science" OR convergence) AND (integration OR "knowledge integration" OR "boundary object*" OR interoperability OR "translation") AND (technology OR infrastructure OR platform* OR FAIR OR workflow OR "research software")
PLUS aviation lens terms (aviation OR avionics OR "air traffic management" OR ADS-B OR ACARS OR "airworthiness security" OR DO-326A OR ED-202A).

Search transparency was maintained in line with PRISMA-S (Rethlefsen *et al*., 2021) [12].

2.4 Study selection, extraction, and appraisal

Records were screened for relevance and extracted into a synthesis matrix (definition of integration; integration level; technology role; evaluation approach; barriers/enablers; domain context). For mixed-study bodies of evidence, appraisal guidance such as MMAT was used to support structured judgement rather than a single quality score (Hong *et al*., 2018) [5].

2.5 Synthesis approach

We conducted a thematic synthesis organized around integration *layers* and the role of technology as a mediating structure. Aviation cybersecurity findings were mapped onto the same integration layers to test the framework against a safety-critical, standards-heavy domain.

3. Results: What "Integration" Looks Like in the Literature

3.1 Integration is multi-layered (and frequently mis-measured)

Across the literature, integration is presented as alignment across heterogeneous knowledge systems often achieved through shared representations and negotiated practices rather than total consensus (Star & Griesemer, 1989) [14]. Team science research emphasizes that increasing scale and specialization require deliberate structures to coordinate work and evaluate outcomes (Stokols *et al*., 2008; Wuchty *et al*., 2007) [15, 18].

Measurement approaches frequently rely on bibliometric proxies (e.g., diversity and network-based indicators), which can capture disciplinary mixing but not necessarily *successful integration* (Leydesdorff & Rafols, 2011; Porter & Rafols, 2009) [7, 11]. This creates a persistent evaluation gap: interdisciplinary "variety" is easier to count than interdisciplinary "coherence."

3.2 Five integration layers

We synthesize the literature into five interlocking layers that recur across conceptual and empirical work:

1. **Epistemic integration:** Shared problem framings, agreed validity criteria, and negotiated meanings.
2. **Methodological integration:** Hybrid methods and model coupling; aligning inference logics (e.g., statistical, engineering, qualitative).
3. **Infrastructure/data integration:** Interoperability of data, software, workflows, and metadata; reproducibility and reuse as operational integration outcomes (Wilkinson *et al*., 2016) [17].
4. **Socio-organizational integration:** Team structures, roles, incentives, and coordination practices that support sustained integration (Stokols *et al*., 2008) [15].
5. **Governance integration-** accountability, compliance, ethics, incident response, and cross-stakeholder legitimacy.

3.3 Technology as boundary infrastructure

Boundary-object theory explains how heterogeneous groups coordinate via artifacts that are adaptable locally but stable enough to maintain shared identity (Star & Griesemer, 1989) [14]. In contemporary IDR, technology frequently becomes not a single boundary object but *boundary infrastructure*: standards, repositories, workflow systems, APIs, and platform ecosystems that mediate what gets integrated and how.

FAIR principles exemplify this shift by emphasizing machine-actionability and reuse, making interoperability an explicit integration target rather than an incidental byproduct (Wilkinson *et al*., 2016) [17].

4. Aviation Cybersecurity as a High-Stakes Integration Lens

Aviation cybersecurity illustrates the full stack of integration layers because it is simultaneously: (a) cyber-physical and safety-critical, (b) distributed across airlines / airports / ATM / manufacturers/regulators, and (c) constrained by certification and continuing airworthiness regimes.

4.1 Governance integration: ICAO pillars as sector-level integration scaffolding

ICAO's Cybersecurity Action Plan articulates seven pillars international cooperation, governance, legislation/regulations, cybersecurity policy, information sharing, incident management / emergency planning, and capacity building/culture explicitly positioning aviation cybersecurity as multi-stakeholder, multi-domain integration work (ICAO, 2021) [6]. This framing aligns directly with the "governance integration" layer and makes integration measurable through preparedness, coordination channels, and shared baselines.

4.2 Infrastructure and compliance integration: airworthiness security process standards

Aviation is unusual in how explicitly it codifies cybersecurity integration into lifecycle processes. EASA guidance (AMC) references the use of EUROCAE ED-202A/ED-203A/ED-204 (and equivalent RTCA DO documents) across initial and continued airworthiness contexts (EASA, 2023) [1]. RTCA identifies DO-326A as an airworthiness security process specification intended to augment certification guidance for handling information security threats to aircraft safety (RTCA, n.d.) [13]. EUROCAE's ED-202A similarly formalizes an airworthiness security process specification (EUROCAE, 2014) [2].

These artifacts function as boundary infrastructure: they coordinate multiple disciplines (systems engineering, security engineering, safety assurance, certification) via shared lifecycle steps, documentation expectations, and compliance narratives.

4.3 Method and epistemic integration: communications, aircraft systems, and threat models

Empirical reviews underscore that aviation cybersecurity spans heterogeneous attack surfaces and epistemic cultures. A major review maps threats and vulnerabilities across aviation infrastructures over decades, highlighting how digitization shifts risk into interconnected systems (Ukwandu *et al*., 2022) [16].

Work on aeronautical communications identifies gaps where standards historically under-specified cybersecurity properties, motivating interdisciplinary solutions spanning protocol design, operations, and governance (Mäurer, 2022) [8].

At the aircraft-systems level, reviews/taxonomies emphasize internal networks, component interdependencies, and cyber impacts on safety-critical functions, reinforcing the need for methodological integration between safety analysis and adversarial threat modeling (Habler *et al*., 2022) [4].

4.4 Socio-organizational integration: ATM cyber resilience as collaborative governance

EUROCONTROL frames ATM as a complex global infrastructure evolving alongside digitization and emphasizes stakeholder coordination to maintain cyber resilience (Eurocontrol, 2021) [3].

This aligns with team science insights: large-scale, distributed systems require institutionalized coordination mechanisms rather than ad hoc collaboration (Stokols *et al*., 2008) [15].

5. Proposed Framework: Science Technology Interdisciplinary Integration

We propose the Science Technology Interdisciplinary Integration Framework, which links integration layers to the roles of technology and to evaluable outputs. The framework treats technology as *co-constitutive* of integration: it shapes what can be shared, validated, reused, and governed.

Aviation mapping- how the lens "stress-tests" STII

- **Governance layer** is strongly formalized via ICAO pillars and regional regulatory guidance (ICAO, 2021; EASA, 2023) [6, 1].
- **Infrastructure layer** is unusually explicit via airworthiness security process specifications and continuing airworthiness guidance ecosystems (EUROCAE, 2014; RTCA, n.d.; EASA, 2023) [2, 1, 13].
- **Method/epistemic layers** remain challenging due to differences between safety assurance logic and adversarial security logic; the literature repeatedly flags this gap (Habler *et al*., 2022; Mäurer, 2022; Ukwandu *et al*., 2022) [4, 8, 16].

Table 1: STII Framework

Integration layer	Integration output	Technology role	Example evaluation signals
Epistemic	Shared framing & validity criteria	Shared conceptual artifacts; structured vocabularies	Stable cross-domain definitions; explicit assumptions
Methodological	Coupled methods/models	Workflow tooling; simulation/analysis platforms	Demonstrated coupling; triangulated evidence
Integration layer	Integration output	Technology role	Example evaluation signals
Infrastructure/data	Interoperable reusable objects	FAIR-aligned repositories; versioned pipelines	Cross-team reuse; reproducibility outcomes (Wilkinson *et al*., 2016) [17]
Socio-organizational	Coordinated teams & roles	Collaboration platforms; traceable decisions	Team process measures; coordination effectiveness
Governance	Accountable, compliant practice	Auditability; standards; incident processes	Compliance evidence; incident readiness (ICAO, 2021; EASA, 2023) [6,]

6. DISCUSSION

Core claim: integration is an engineered socio-technical outcome

The synthesis suggests that interdisciplinary integration should be treated less like a "team virtue" and more like an engineered outcome with technical and governance architectures. FAIR principles make this visible by turning interoperability and reuse into explicit design goals (Wilkinson *et al*., 2016) [17]. Aviation cybersecurity makes it unavoidable: integration failures are not just academic inefficiencies; they can translate into certification gaps, incident response fragmentation, and systemic risk propagation across globally coupled infrastructures (ICAO, 2021; EUROCONTROL, 2021) [6, 3].

Why bibliometric proxies aren't enough

Indicators of interdisciplinarity can quantify diversity and network positions, but they cannot certify integrative coherence or lifecycle assurance (Leydesdorff & Rafols, 2011; Porter & Rafols, 2009) [7, 11]. For safety-critical interdisciplinary domains, evaluation must include operational indicators: demonstrable reuse, traceable decision rationales, audit-ready compliance evidence, and incident preparedness maturity.

Implications for aviation cybersecurity research and governance

Treat cybersecurity integration as lifecycle assurance: Align threat modeling, safety analysis, verification, and continuing airworthiness practices into traceable end-to-end narratives (EASA, 2023; RTCA, n.d.) [1, 13].

Invest in boundary infrastructure: interoperable data models, testbeds, and red-team/blue-team evidence pipelines that connect research outputs to certification and operational contexts (Wilkinson *et al*., 2016; ICAO, 2021) [17, 6].

Institutionalize information sharing and incident readiness: consistent with ICAO pillars, integration requires shared baselines and practiced coordination, not just documents (ICAO, 2021) [6].

Research Agenda

1. **Operational measures of integration quality:** Go beyond "mixing" metrics toward validated coherence indicators (e.g., cross-domain reuse success, auditability, coupled-model performance under adversarial assumptions).
2. **Secure-by-design research infrastructures:** Expand FAIR-aligned ecosystems to include security properties and provenance guarantees for research workflows (Wilkinson *et al*., 2016) [17].

3. **Bridging safety and security epistemologies:** Develop shared formalism linking hazard analysis and adversarial threat analysis, with evidence standards acceptable to regulators and engineers (EASA, 2023; Habler *et al*., 2022) [1, 4].
4. **ATM and airport ecosystem resilience studies:** Focus on governance mechanisms for inter-organizational cyber resilience in distributed infrastructures (EUROCONTROL, 2021; ICAO, 2021) [3, 6].

7. LIMITATIONS

This SLR synthesizes a broad mixed-evidence literature across multiple domains with heterogeneous study designs and definitional variance. Access constraints and database coverage differences can affect exhaustiveness; therefore, results should be interpreted as a structured synthesis rather than a claim of complete enumeration. Future work should preregister a protocol, execute database-native queries across Scopus/Web of Science/IEEE/ACM with full screening counts, and publish the full extraction matrix per PRISMA 2020 checklists (Page *et al*., 2021; Rethlefsen *et al*., 2021) [10, 12].

8. CONCLUSION

Interdisciplinary integration is best understood as a multi-layered socio-technical process spanning epistemic alignment, methodological coupling, infrastructure/data interoperability, socio-organizational coordination, and governance legitimacy. Technology is not merely supportive; it frequently operates as boundary infrastructure that shapes what integration is possible and what outcomes become stable and reusable (Star & Griesemer, 1989; Wilkinson *et al*., 2016). Aviation cybersecurity demonstrates how integration must be institutionalized through lifecycle processes, compliance frameworks, and sector-level coordination pillars, offering a concrete model for “auditable interdisciplinarity” in safety-critical domains (EASA, 2023; ICAO, 2021; RTCA, n.d.).

REFERENCES

1. European Union Aviation Safety Agency. AMC 20-42: Airworthiness Information Security Risk Assessment (Easy Access Rules for AMC-20). Cologne: European Union Aviation Safety Agency; 2023 Jun 23.
2. EUROCAE. ED-202A: Airworthiness Security Process Specification. Saint-Denis: EUROCAE; 2014.
3. EUROCONTROL. Air Traffic Management: A Cybersecurity Challenge. Brussels: EUROCONTROL; 2021.
4. Habler E, *et al*. Evaluating the security of aircraft systems. arXiv. 2022;arXiv:2209.04028.
5. Hong QN, Gonzalez-Reyes A, Pluye P. Mixed Methods Appraisal Tool (MMAT), Version 2018: User Guide. Montreal: McGill University; 2018.
6. International Civil Aviation Organization. Cybersecurity Action Plan. 2nd ed. Montreal: International Civil Aviation Organization; 2021.
7. Leydesdorff L, Rafols I. Indicators of the interdisciplinarity of journals: diversity, centrality, and citations. Journal of Informetrics. 2011;5(1):87-100. doi:10.1016/j.joi.2010.09.002.
8. Mäurer N. Security in digital aeronautical communications: a comprehensive gap analysis. International Journal of Critical Infrastructure Protection. 2022;38:100549.
9. National Research Council. Convergence: Facilitating Transdisciplinary Integration of Life Sciences, Physical Sciences, Engineering, and Beyond. Washington (DC): The National Academies Press; 2014.
10. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, *et al*. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71.
11. Porter AL, Rafols I. Is science becoming more interdisciplinary? Measuring and mapping six research fields over time. Scientometrics. 2009;81(3):719-745. doi:10.1007/s11192-008-2197-2.
12. Rethlefsen ML, Kirtley S, Waffenschmidt S, Ayala AP, Moher D, Page MJ, *et al*. PRISMA-S: an extension to the PRISMA statement for reporting literature searches in systematic reviews. Journal of the Medical Library Association. 2021;109(2):174-200. doi:10.5195/jmla.2021.962.
13. RTCA. Security Standards (Including DO-326A Airworthiness Security Process Specification). Washington (DC): RTCA; n.d.
14. Star SL, Griesemer JR. Institutional ecology, "translations" and boundary objects: amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-1939. Social Studies of Science. 1989;19(3):387-420. doi:10.1177/030631289019003001.
15. Stokols D, Hall KL, Taylor BK, Moser RP. The science of team science: overview of the field and introduction to the supplement. American Journal of Preventive Medicine. 2008;35(2 Suppl):S77-S89.
16. Ukwandu E, *et al*. Cyber-security challenges in aviation industry: a review of threats, solutions and future directions. Information. 2022;13(3):146.
17. Wilkinson MD, Dumontier M, Aalbersberg IJ, *et al*. The FAIR guiding principles for scientific data management and stewardship. Scientific Data. 2016;3:160018. doi:10.1038/sdata.2016.18.
18. Wuchty S, Jones BF, Uzzi B. The increasing dominance of teams in the production of knowledge. Science. 2007;316(5827):1036-1039. doi:10.1126/science.1136099.