IoT-AI 2025

ALEXANDER LAWALL

Cybersecurity in Civil Aviation –
Threat Landscape and Vulnerability Assessment of Attack Vectors

Venice, July 2025

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

PROF. DR. ALEXANDER LAWALL

Academic Roles

- Program Director, B.Sc. & M.Sc. Cyber Security and Cyber Security Management
- Professor in Cyber Security (Distance & On-site Learning)

Expertise

- System & Network Security
- Web Application & Cloud Security
- IoT and Industrial IT Security

Professional Affiliations

- Leadership Committee, "Management of Information Security" (Society for Informatics, GI)
- Professional Lead, "Security & GRC in IT" (Summit Leipzig)
- Member, Association of Cyber Forensics and Threat Investigators (ACFTI)
- Member, Zentrum Digitalisierung Bayern (ZD.B)
- Conference Committees Board Chair (IARIA)
- Steering Committee of the Conference SECURWARE & IoT-AI (IARIA)

Research & Publications

- Focus Areas: Cyber Security, Information Security, Industry 4.0/5.0, IoT, Rights Management
- Publications in national/international Journals and Conferences
- Keynote Speaker, Program Chair, Panel Expert of International Conferences

MOTIVATION AND RESEARCH DESIGN

Motivation & Problem Statement

- Aviation‘s fragility: past attacks (e.g., ransomware on airports, spoofed GNSS)
- Lack of encryption/authentication: many critical systems (e.g., ADS-B, ACARS)
- Regulation and legacy design: constraints for security upgrades

➢ Problem: Increase in digitized aviation → Raise of Cyber Risks

MOTIVATION AND RESEARCH DESIGN

Research Questions & Goal

RQ1: *Who are the relevant threat actors targeting civil aviation?*

RQ2: *What are the critical attack vectors exploited in this domain?*

RQ3: *How vulnerable are current aviation systems to these evolving threats?*

Goal: *Synthesize expert insights with literature for actionable findings*

MOTIVATION AND RESEARCH DESIGN

Methodology

- Qualitative Design: Semi-structured interviews with cybersecurity experts (aviation authorities, OEMs, consultants).
- Analysis: Inductive coding of themes: attack types, system weaknesses, feasibility
- Sources: Academic, regulatory, and technical documents support findings

THREAT ACTOR LANDSCAPE

Actor Type	Motivation	Capability
Nation-states	Espionage, sabotage	APTs, 0-days, stealth
Cybercriminals	Ransom, fraud	Malware, phishing
Hacktivists	Ideological disruption	DDoS, defacement
Insiders	Abuse of privileges	Deep access, hard to detect

- Insiders and nation-states pose the most critical safety risks

ATTACK SURFACE CATEGORIZATION

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Threat vectors were grouped across three domains:

- **Airborne Systems** (e.g., onboard avionics, satellite communication modules (SATCOM), flight management systems (e.g., ADS-B))
- **Ground Infrastructure** (e.g., airport IT, air traffic control (ATM) systems)
- **Communication Links** (e.g., ACARS, VHF radio, SWIM)

AIRBORNE SYSTEM VULNERABILITIES

Actor Vector	Likelihood	Impact
ADS-B spoofing	High	High
GNSS jamming/spoofing	High	High
SATCOM command injection	Medium	High
Legacy avionics exploitation	Medium	High

- ADS-B lacks encryption/authentication
- GNSS spoofing validated in real-world cases
- Legacy avionics resist patching due to certification limits

GROUND INFRASTRUCTURE RISKS

Actor Vector	Likelihood	Impact
Airport IT ransomware	High	Medium
ATM system compromise	Medium	High
Maintenance system manipulation	Medium	High

- Ground systems often use Commercial Off-The-Shelf (COTS) components with weak segmentation
- High exposure due to third-party access and legacy software

COMMUNICATION LINK THREATS

Actor Vector	Likelihood	Impact
ACARS interception	High	Medium
SWIM data injection	Medium	Medium-High
VHF/UHF spoofing	Low-Medium	Medium

- ACARS uses plaintext over VHF/SATCOM channels
- SWIM increases attack surface via IP-based APIs
- Threat affect flight planning and awareness

COMPARATIVE RISK OVERVIEW

System Category	Likelihood	Impact
Airborne Systems	Medium-High	High
Ground Infrastructure	Medium-High	Medium-High
Communication Links	Low-High	Medium-High

- Airborne systems: lower likelihood but highest impact
- Ground systems: high attackability, less direct safety impact

EXPERT INSIGHTS & DIVERGENCES

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Consensus

- ADS-B, ACARS, and legacy avionics = top risks
- Ground systems most accessible to attackers

Disagreements

- Severity of ACARS/VHF compromises
- Role of redundancy in mitigating communication failures

- *Need for scenario-based modeling to quantify cascading effects*

SECURITY GAPS IDENTIFIED

- **Outdated, unpatchable technologies (i.a. legacy systems)**: unpatched avionics and ATM software
- **Unsecured Protocols**: ADS-B, ACARS, VHF use plaintext
- **Poor Segmentation**: IT/OT boundaries are weak (lateral movement)
- **Limited detection and response capabilities**: Lacking real-time anomaly detection
- **Fragmented organizational accountability:** lack of rapid response and coordinated defense

ORGANIZATIONAL & POLICY CHALLENGES

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

- **Complex Ecosystem**: Airlines, airports, vendors, OEMs – fragmented accountability
- **Weak Governance**: Voluntary guidelines (e.g., ICAO, EASA) lack enforcement
- **Delayed Patching**: Responsibility unclear; updates slow

- *Call for harmonized regulations and minimum mandatory baselines*

STRATEGIC RECOMMENDATIONS

- Encrypt and authenticate all communication protocols (e.g., secure ADS-B, SWIM over TLS)
- Retrovit avionics with secure overlays, considering certification timelines
- Enforce network segmentation and AI-based anomaly detection
- Run joint cyber exercises and improve real-time treat intelligence sharing

CONCLUSION & FUTURE WORK

RQ1: *Who are the relevant threat actors targeting civil aviation?*

RQ2: *What are the critical attack vectors exploited in this domain?*

RQ3: *How vulnerable are current aviation systems to these evolving threats?*

Key Takeaways

- Aviation is highly exposed to cyber risks with severe safety implications
- Threats are technical and organizational in nature
- Security must be proactive, layered, and harmonized

Future Directions

- Scenario-based simulations for risk propagation
- Real-time ML for threat detection
- Policy research for better cross-national cyber security governance

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

How can we **enforce global cybersecurity standards** in civil aviation, when the **regulatory landscape is fragmented** and aircraft operate across **multiple jurisdictions** every day?

Given the **long life cycles and certification constraints** in aviation, **how** can we **design security systems** today that remain **resilient 20 or even 30 years** from now?

Prof. Dr. Alexander Lawall
alexander.lawall@iu.org