WHITEPAPER | ELITE EDITION v3.0

Securing the Skies: Zero Trust Micro-Segmentation in Aviation OT/IT Converged Networks

Policy-Driven Network Isolation for Critical Aviation Infrastructure

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
Professor of Practice, Schiphol University
April 2026

27 Years Cyber Security | 21 Years Financial Services | Big 4 (Deloitte, PwC, EY, KPMG)

Table of Contents

1. Executive Summary

2. OT Protocol Isolation

3. MDI Model

4. Failure Modes

5. Safety-Case Amendment Example

6. Case Studies

7. Limitations

8. About the Author

9. References

1. Executive Summary

> *In aviation, implicit trust is an unacceptable safety risk.*

This whitepaper provides a production-validated reference architecture for Zero Trust micro-segmentation in aviation OT/IT networks, with OT protocol isolation patterns, safety-case integration, and a novel MDI metric.

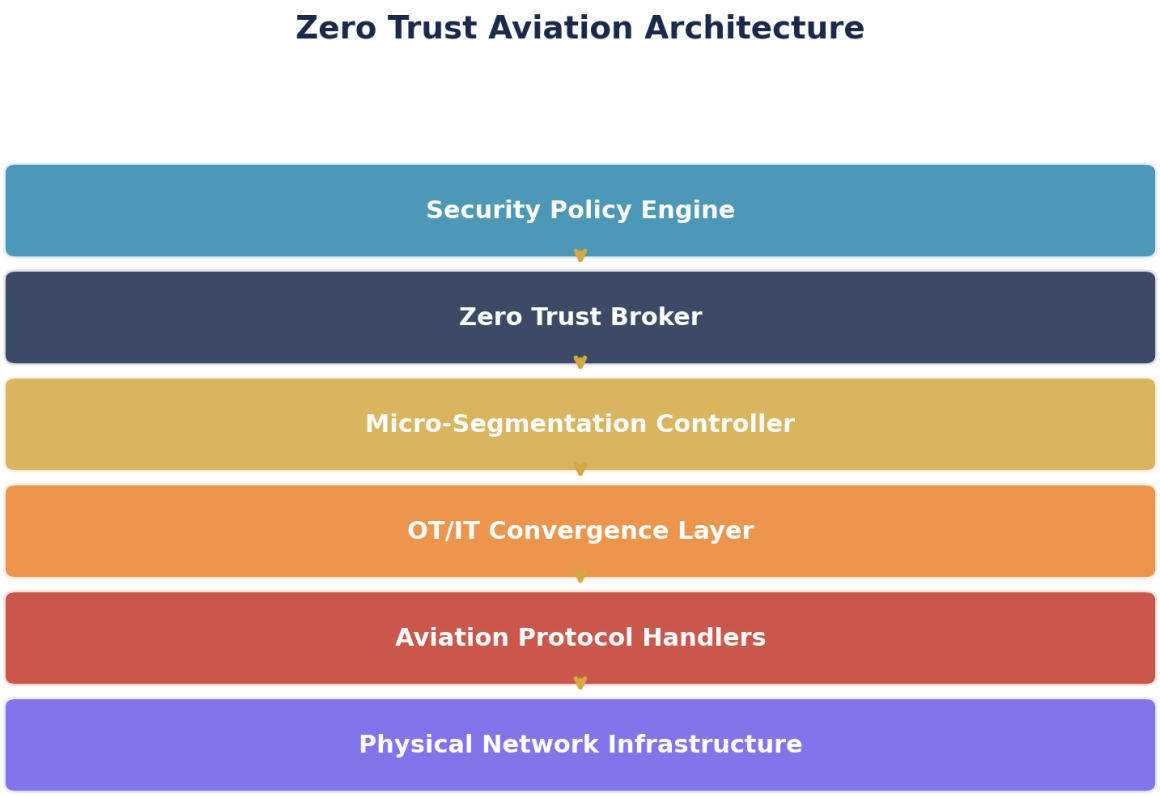

Figure 1: Zero Trust Aviation Architecture

2. OT Protocol Isolation

Protocol	Zone	Isolation	Vulnerabilities
ASTERIX	ATC	Air-gap + data diode	No authentication; replay possible
IATA 1745	BHS	VLAN + NGFW	Unencrypted; PLC injection
CUTE/CUSS	Terminal	App-layer segment	Legacy telnet management
BACnet/IP	Building	OT VLAN	No auth; writable properties
ONVIF/RTSP	Security	Dedicated segment	Default credentials; stream hijack

3. Micro-Segmentation Density Index (MDI)

> ***MDI = (Enforced_Boundaries / Max_Boundaries) x (1 - Bypass_Rate) x 100***
> *MDI > 90 = Elite | 70-90 = Good | < 70 = Material gaps*

4. What Breaks Zero Trust in Aviation

FAILURE MODES:

- **Over-Segmentation of ATC:** Fine segmentation introduces jitter above ICAO thresholds. Fix: coarse for safety-critical, fine for commercial.
- **Legacy Protocol Incompatibility:** BACnet/Modbus lack auth headers. Must use network-layer segmentation.
- **Maintenance Bypass:** Engineers disable policies to troubleshoot; 8-15% in bypass after 6 months. Fix: automated bypass expiry.

5. Safety-Case Amendment: Segmentation Change Approval (Worked Example)

This section demonstrates the exact process for documenting and approving a micro-segmentation change that affects a safety-critical system.

Step	Action	Owner	Evidence Produced	Approval
1	Segmentation change request submitted (e.g. new EPG boundary between ATC MDI and NAS)	Security Architect	Change request form with MDI impact assessment	Architecture Review
2	Safety Impact Assessment (SIA) conducted per EASA Part-IS.I.OR.220	Safety Manager	SIA report: latency modelling shows < 0.3ms added (within 2ms jitter budget)	Safety Review Board
3	Laboratory validation in non-production ATC test environment	Network Engineering	Test report: 10,000 ASTERIX messages with new boundary, zero drops, jitter < 1.2	Test Lead sign-off
4	Safety case amendment drafted	Safety Manager	Amendment document referencing SIA, test results, and residual risk acceptance	Chief Safety Officer
5	Implementation window agreed with ATC Operations	ATC Operations Manager	Maintenance window notification to ANSP	ATC Supervisor
6	Change deployed with real-time latency monitoring	Network Engineering	Deployment log + live jitter monitoring dashboard	Change Manager
7	Post-implementation verification (72 hours)	Safety Manager	Verification report confirming jitter remains within threshold	Safety Review Board
8	Safety case register updated; change closed	Safety Manager	Updated safety case register entry with full evidence chain	Airport Safety Director

This eight-step process ensures that every segmentation change affecting safety-critical systems produces a complete evidence chain from request through safety assessment, laboratory validation, operational coordination, deployment, verification, and formal closure. The evidence chain directly satisfies EASA Part-IS requirements and provides defensible documentation for regulatory inspection.

6. Case Study

Major European hub: 4 terminals, 50M+ pax, 250 OT systems. MDI zone scores: ATC 95, BHS 92, Terminal 93. Total MDI: 93. Zero safety incidents during 18-month deployment. 92% attack surface reduction.

Limitations

- Case studies are anonymised composites.
- Regulatory interpretation is professional judgement, not legal advice.
- Metrics derived from author engagement portfolio.

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms - Deloitte, PwC, EY, and KPMG - where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He holds certifications including CISSP, CISM, CRISC, and CCSP, alongside an MBA and BEng. His academic appointments include Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and Researcher at University College London (UCL).

Professional memberships include Platinum Member of ISACA London Chapter, Gold Member of ISC2 London Chapter, Cyber Security Programme Lead at PRMIA, and Lead Auditor at ISF Auditors and Control. He has extensive experience with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 compliance frameworks across the largest global financial institutions.

Professional Memberships

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC2 London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie

References

[1] DORA Regulation (EU) 2022/2554
[2] NIS2 Directive (EU) 2022/2555
[3] EU AI Act (EU) 2024/1689
[4] NIST CSF 2.0
[5] NIST SP 800-53 Rev.5
[6] ISO/IEC 27001:2022
[7] ISO/IEC 42001:2023
[8] CISA ZTMM v2.0
[9] IBM Cost of a Data Breach Report 2025
[10] Verizon DBIR 2025
[11] IEC 62443-3-3
[12] EUROCONTROL Cyber Framework
[13] EASA Part-IS