WHITEPAPER | ELITE EDITION v3.0

Resilient Runways: Deterministic Network Architecture for Air Traffic and Airport Systems

Fault-Tolerant Network Fabrics for Safety-Critical Aviation

TAXIWAY Framework

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

> *Aviation networks do not have the luxury of best-effort delivery. When ATC depends on deterministic latency, network architecture becomes a safety discipline.*

This whitepaper introduces the TAXIWAY Framework and Network Criticality Score (NCS) for classifying aviation systems by latency sensitivity, redundancy, and safety impact. It includes a complete latency validation methodology with jitter instrumentation and threshold breach response procedures.

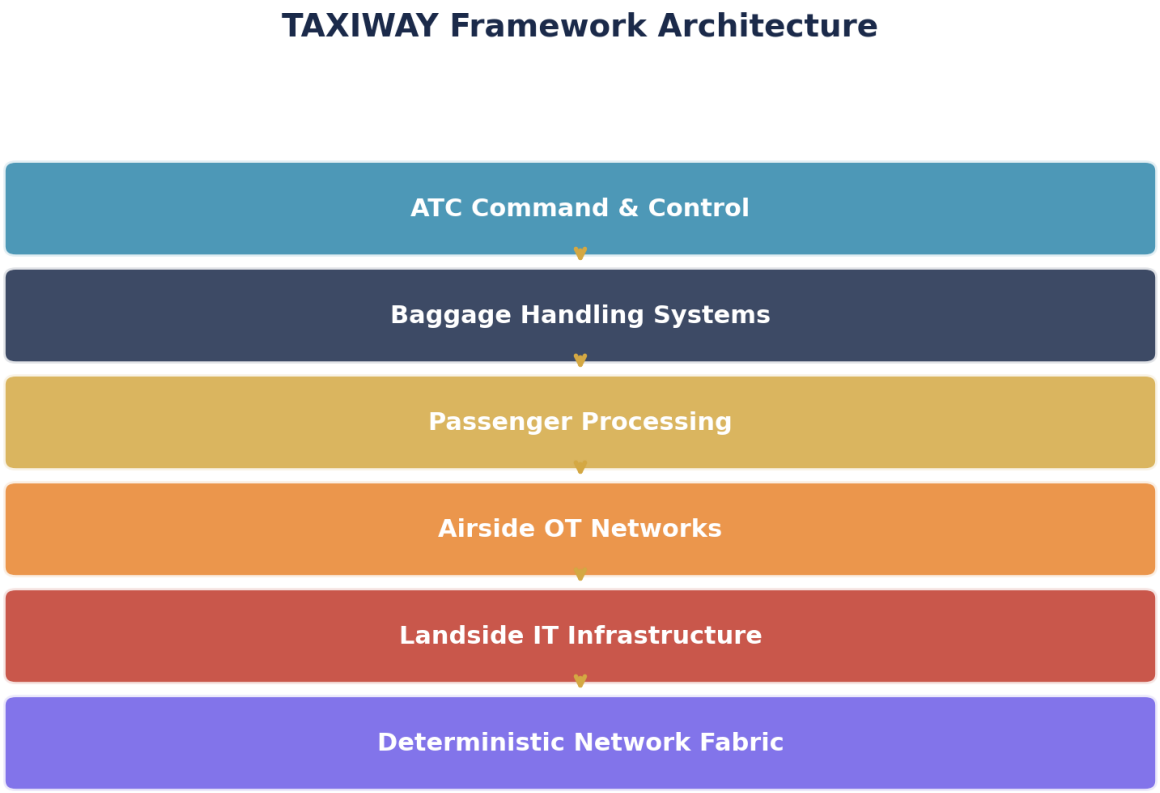

Figure 1: TAXIWAY Architecture

2. Deterministic Latency Requirements

System	Max Latency	Max Jitter	Packet Loss	Redundancy
ATC Voice/Data	< 150ms (ICAO)	< 5ms	0%	Active-Active, dual-path
ATC Surveillance	< 50ms	< 2ms	0%	Active-Active, air-gapped
Baggage Handling	< 500ms	< 20ms	< 0.01%	Active-Standby
Passenger Info	< 2s	< 100ms	< 0.1%	Load-balanced
Building Mgmt	< 5s	< 500ms	< 1%	Monitored

3. ATC Dependency Mapping

Primary System	Depends On	Failure Impact	Priority
Approach Radar	ASTERIX network, NTP, processing server	Cannot sequence landings	P0
Tower Radio	VoIP, frequency mgmt, recording	Pilot comms lost	P0
Departure Seq	A-CDM, airline feeds, gate mgmt	Departure delays cascade	P1

Primary System	Depends On	Failure Impact	Priority
Baggage Sort	PLC network, BHS server, DCS feed	Bags misrouted	P1
Check-In	CUTE/CUSS, DCS, payment gateway	Processing stops	P2

4. Latency Validation and Jitter Instrumentation

Deterministic latency claims must be continuously validated. The following instrumentation methodology provides ongoing assurance:

Instrumentation Architecture

```
# Continuous Latency Validation (deployed on dedicated probe hosts)
# Sends synthetic ASTERIX-like packets every 100ms and measures RTT + jitter

import time, socket, statistics

THRESHOLDS = {
'atc_surveillance': {'max_latency_ms': 50, 'max_jitter_ms': 2},
'atc_voice': {'max_latency_ms': 150, 'max_jitter_ms': 5},
'bhs': {'max_latency_ms': 500, 'max_jitter_ms': 20},
}

def measure_path(target, port, system_class, samples=100):
latencies = []
for _ in range(samples):
start = time.perf_counter_ns()
# Send probe packet and measure round-trip
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.settimeout(0.1)
sock.sendto(b'PROBE', (target, port))
try:
sock.recvfrom(64)
except socket.timeout:
latencies.append(float('inf'))
continue
rtt_ms = (time.perf_counter_ns() - start) / 1e6
latencies.append(rtt_ms)
time.sleep(0.1)

p99 = sorted(latencies)[int(len(latencies) * 0.99)]
jitter = statistics.stdev([l for l in latencies if l &lt; float('inf')])
threshold = THRESHOLDS[system_class]

if p99 &gt; threshold['max_latency_ms']:
```

```
trigger_alert('LATENCY_BREACH', system_class, p99)
if jitter &gt; threshold['max_jitter_ms']:
trigger_alert('JITTER_BREACH', system_class, jitter)

return {'p99_ms': p99, 'jitter_ms': jitter, 'loss_%': ...}
```

Listing 1: Continuous Latency Validation Probe

Threshold Breach Response Procedure

Breach Type	Severity	Immediate Action	Escalation	Resolution SLA
ATC latency > 50ms	P0 Safety	Alert ATC ops + network team + Safety Manager	CISO + Safety Manager	< 15 minutes
ATC jitter > 2ms	P0 Safety	Switch to backup path; investigate	Safety Manager	< 30 minutes
BHS latency > 500ms	P1 Operational	Alert BHS operations	Duty Manager	< 1 hour
FIDS latency > 2s	P2 Commercial	Log and investigate next business day	IT Support	< 24 hours

5. What Breaks This Design

AVIATION NETWORK FAILURE MODES:

- **STP Reconvergence:** Legacy L2 causes 30-50s outages during topology changes. Fix: VXLAN/EVPN fabric.
- **QoS Misconfiguration:** Priority queuing starves BHS during peak. Fix: dedicated QoS testing under peak-load.
- **NTP Drift:** 200ms clock drift causes ASTERIX message rejection. Fix: dual NTP with GPS reference.
- **Firmware Asymmetry:** Different firmware versions cause intermittent failures. Fix: strict standardisation.

6. Post-Mortem: Baggage System Grounded Flights

ILLUSTRATIVE SCENARIO: *Routine switch upgrade caused 47s STP reconvergence. ATC unaffected (separate VLAN). BHS PLC network lost connectivity. 340 bags misrouted. 12 flights departed without luggage. EUR 180K repatriation cost. Root cause: BHS not classified as flight-critical in dependency mapping.*

7. Network Criticality Score (NCS)

NCS = (0.50 x Safety) + (0.35 x Operational) + (0.15 x Commercial)
NCS > 7.0 = Active-Active mandatory | 4.0-7.0 = Active-Standby | < 4.0 = Monitored

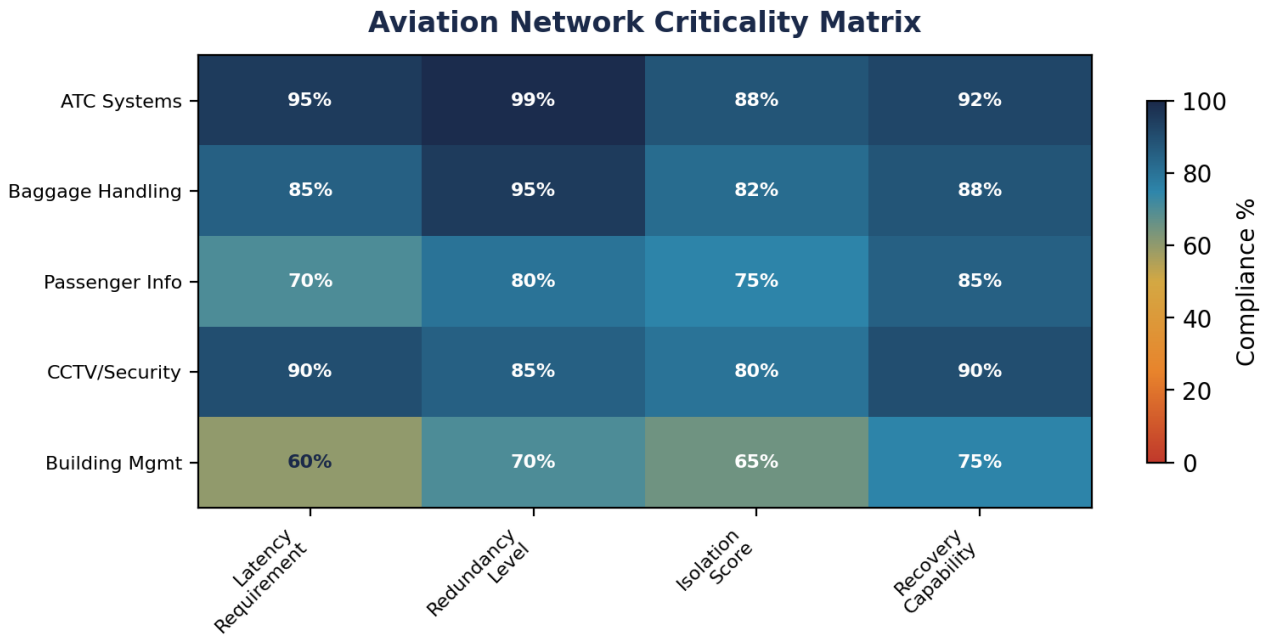

Figure 2: Aviation Network Criticality Matrix

8. Case Study

European hub: 45M pax/year, 4 terminals. TAXIWAY with VXLAN/EVPN. ATC availability: 99.9997%. NCS-driven investment reduced capex 22% while improving critical redundancy. Continuous latency probes deployed across all zones.

9. Limitations

- Latency thresholds based on ICAO standards; local CAA may impose stricter requirements.
- NCS weights reflect author experience; calibrate to airport risk profile.

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] EASA Part-IS
[12] ICAO Annex 17
[13] EUROCONTROL Cyber Strategy 2024-28