IBLADES WHITEPAPER · AEROSPACE & TRANSPORTATION

The Quantum-Safe Transport Network

Securing aviation, rail, ports, and autonomous mobility against the converging threats of quantum decryption, AI-accelerated attacks, and an ageing operational-technology edge.

In this paper

1. Executive summary
2. The 2026 threat landscape
3. Sector deep-dives
4. The iBlades architecture
5. Regulatory & compliance mapping
6. A low-risk pilot path

1. Executive summary

The transportation sector — airlines and airports, railways and metros, seaports and shipping, and the emerging world of autonomous road and aerial mobility — is being rebuilt around hyper-connected, AI-driven, data-rich operations. That transformation delivers enormous efficiency, but it also stretches a security perimeter over decades-old operational technology (OT) that was never designed to be online.

Three forces now converge on this expanded attack surface: the **"Harvest Now, Decrypt Later"** quantum threat to long-lived sensitive data, **AI-accelerated attacks** that operate at machine speed, and a growing population of **unpatchable legacy and unmanned edge systems**. iBlades addresses all three with a single, hardware-anchored, post-quantum security fabric that overlays existing infrastructure — without ripping out or re-architecting the systems transport operators depend on.

2. The 2026 threat landscape

Harvest Now, Decrypt Later (HNDL)

Adversaries are intercepting and stockpiling encrypted data today — biometric identity records, passenger and loyalty data, cargo and trade documents, crew and maintenance communications — to decrypt once a cryptographically relevant quantum computer matures. Transportation is uniquely exposed: much of its data must remain confidential for decades, and biometric identifiers, unlike passwords, can never be reissued after a breach.

AI-accelerated attacks

Attacks that once required skilled human operators now run at machine speed. AI can discover vulnerabilities in minutes rather than weeks, probe thousands of systems, APIs, and exposed services simultaneously, exploit misconfigurations automatically, generate new malware variants that evade signature-based detection, and adapt continuously as defenses change. After gaining an initial foothold, AI maps trust relationships, credentials, and routes to move laterally through a network faster than any security team can respond.

AI also introduces a failure mode unique to connected transport: **data poisoning**, where spoofed sensor or telemetry feeds push AI-driven traffic, flight, rail, or logistics systems toward dangerous decisions. And it supercharges the "Harvest Now, Decrypt Later" threat — AI identifies and captures the highest-value encrypted traffic today for future quantum decryption.

> **The real target is complexity.** AI-powered attacks feed on the accumulated complexity of modern security stacks — every exposed API, admin console, endpoint agent, plug-in, integration, and remote-access path is a potential entry point. Reducing that exposed software surface does more to stop AI-driven attacks than adding yet another software layer on top.

The unpatchable legacy and unmanned edge

Signaling systems, baggage handlers, fuel controllers, port cranes, roadside traffic controllers, and runway equipment often run outdated software that cannot be patched without voiding warranties or halting operations. Meanwhile, unmanned and remote

assets — vertiports, environmental sensors, inspection drones — extend the attack surface into physically exposed locations.

> The pattern is consistent across every mode of transport. That is precisely why a single architecture — not a different point product per system — is the efficient answer.

---

3. Sector deep-dives

Aviation & airports

As airlines and airports adopt biometric "smart travel," AI-driven flight operations, and eVTOL vertiport networks, they concentrate irreplaceable biometric and AI-training data while still relying on legacy ground OT. iBlades encrypts biometric and AI data pipelines with post-quantum cryptography, isolates legacy baggage, fuel, and runway systems behind a hardware air-gap, secures crew mobile devices and electronic flight bags on any network, and protects remote, low-power vertiport infrastructure.

Read the full Aviation whitepaper →

Rail & metro

Rail signaling and train control demand zero-fail uptime, yet increasingly connect to corporate IT and remote maintenance — opening a ransomware path into safety-critical systems. iBlades applies "stealth-mode" hardware isolation to signaling and control rooms with no software agent (preserving vendor warranties), micro-segments operational networks from IT, and secures the command and video links used by track and tunnel inspection drones.

Read the full Rail & Metro whitepaper →

Ports & maritime

Hyper-automated terminals and digital trade platforms face a dual risk: kinetic attacks that can paralyze cranes and automated storage, and the harvesting of high-value trade-finance data. iBlades places crane, stacker, and PLC control systems inside a hardware "red zone" isolated from IT and the public internet, applies post-quantum encryption to

electronic bills of lading and trade documents, protects vessel navigation and satellite links, and cryptographically authenticates the sensor data feeding the port's digital twin.

Read the full Ports & Maritime whitepaper →

Roads & autonomous mobility

Connected traffic control, autonomous fleets, and aerial taxis form a cyber-physical mesh in which a spoofed sensor or jammed link becomes a public-safety event. iBlades provides a cryptographic "chain of custody" for sensor and AI-training data, a low-latency peer-to-peer mesh for vehicle-to-infrastructure communications, hardware isolation for roadside controllers, and secure gateways for vertiports and autonomous fleets.

Read the full Roads & Autonomous Mobility whitepaper →

---

4. The iBlades architecture

iBlades delivers one hardware-anchored, quantum-ready fabric that overlays existing infrastructure. It is built on NIST-standardized post-quantum cryptography (ML-KEM for key exchange and ML-DSA/Dilithium for digital signatures, FIPS 203/204), with keys generated locally and rotated autonomously.

- **NetTron™** — a software-defined, peer-to-peer quantum-safe mesh. Self-healing routing, autonomous key rotation, and cryptographic data provenance for sensor and AI pipelines.
- **GuardTron™** — a plug-and-play hardware edge node that isolates and encrypts legacy OT and unmanned assets. Agentless and warranty-safe, it makes protected systems invisible to attackers while allowing authorized traffic.
- **ManoTron™** — hardware-secured mobile communications for crews, field teams, and executives, routing traffic through a quantum-encrypted tunnel that isolates the device's radios.

AI-resilient by design

Because iBlades moves critical protection out of software and into a hardware-anchored layer, it counters AI-driven attacks at their source — complexity and exposure:

- **Reduced attack surface** — fewer exposed interfaces, consoles, and agents for AI to discover and probe.

- **Hardware-anchored trust** — trust lives in dedicated hardware that cannot be scanned or manipulated like an ordinary software service.
- **Cryptographic isolation** — even if one system is compromised, cryptographically controlled paths block AI-driven lateral movement; network access alone is not enough to spread.
- **Works alongside your stack** — deployed inline and transparently, it complements existing firewalls, EDR/XDR, SASE, and identity tools rather than replacing them.

---

5. Regulatory & compliance mapping

The iBlades fabric is designed to map cleanly onto the standards that govern transport security, and to provide the audit evidence regulators expect.

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric
ICAO / IATA (Aviation)	Aviation cybersecurity & data protection	PQC data-in-transit, OT isolation, audit logging
IMO MSC.428(98) / ISO 28000	Maritime & supply-chain cyber risk management	Vessel link encryption, OT red-zone, trade-document PQC
IEC 62443	Industrial / OT security	Hardware segmentation and boundary protection for OT
ISO 27001	Information security management	Zero-trust access, immutable audit trails

---

6. A low-risk pilot path

iBlades is designed to prove value without operational risk. A typical pilot follows four steps:

- **Select** one high-risk, non-critical asset or link (for example, a remote controller, a secondary system, or a single data path).
- **Deploy** the edge node inline in bridge mode — a fast install with no changes to the protected system, network, or workflow.
- **Validate** isolation and resilience with a red-team exercise, confirming legitimate traffic passes and attacks are blocked.
- **Demonstrate** post-quantum key rotation and audit evidence — and reverse the deployment cleanly if desired.

Ready to secure your transport network?

Request a briefing to see how a low-risk pilot would work in your environment.

Request a briefing

⬇ Download PDF

Back to overview

Prefer email? Reach us at hello@iblades.ai

Safe, effective, secure.

Next-generation cyber architecture making cybersecurity simple, reliable, and accessible for everyone.

hello@iblades.ai

Products

- NetTron™
- GuardTron™
- ManoTron™
- Pricing

Solutions

- Financial Institutions
- Healthcare
- Infrastructure
- Government & Military

Company

- About Us
- Partners
- Documentation
- Contact

Compliance

- NIST Approved
- SOC 2 Type II
- HIPAA Compliant
- ISO 27001
- FedRAMP Ready

HEADQUARTERS
127 Spring Street, Suite 120
Pleasanton, CA 94566

R&D CENTER
795 24th Street
Ogden, UT 84401