

Quantum-Safe Roads & Autonomous Mobility

Securing traffic control, connected and autonomous vehicles, and vertiports — where a spoofed sensor or jammed link becomes a public-safety event.

[← Aerospace & Transportation](#)

In this paper

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

1. Executive summary

Connected traffic control, autonomous road and marine fleets, and aerial taxis form a cyber-physical mesh in which a spoofed sensor or a jammed communications link is not just a data breach — it is a public-safety event. AI-driven traffic and mobility systems make the integrity of every sensor feed mission-critical.

iBlades secures mobility ecosystems with a hardware-anchored, post-quantum fabric that overlays existing infrastructure. It guarantees the provenance of sensor and AI data, isolates roadside and control-center systems, secures vehicle-to-infrastructure links, and counters AI-driven attacks by shrinking the exposed software surface.

2. The 2026 threat landscape

Cyber-physical and V2X attacks

Jamming and man-in-the-middle attacks on vehicle-to-everything (V2X) links can hijack or disrupt autonomous and aerial vehicles, while roadside controllers and intelligent-transport field equipment offer a physically exposed attack surface.

AI-accelerated attacks and data poisoning

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing exposed services, and moving laterally after a foothold. The defining mobility risk is **data poisoning**: spoofed sensor feeds push AI traffic and fleet systems toward dangerous decisions.

The real target is complexity. AI attacks feed on exposed interfaces, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Harvest Now, Decrypt Later (HNDL)

Mobility and passenger-movement data intercepted today can be decrypted once quantum computers mature, exposing sensitive patterns of life for years to come.

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM and ML-DSA/Dilithium; FIPS 203/204) with keys generated locally and rotated autonomously.

- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh; provides a cryptographic "chain of custody" for sensor and AI-training data and low-latency vehicle-to-infrastructure links without costly private networks.
- **GuardTron™** — plug-and-play hardware isolation for roadside traffic controllers and field equipment, and a secure gateway for vertiports and autonomous fleets.

- **ManoTron™** — hardware-secured mobile communications for operators and field teams.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement across the mobility network.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, EDR/XDR, SASE, and identity tools.

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric
UNECE R155	Vehicle cybersecurity management	Secure V2X links, data integrity, zero-trust access
ISO/SAE 21434	Road-vehicle cybersecurity engineering	Cryptographic data provenance, isolation
IEC 62443	Industrial / OT security	Hardware segmentation for roadside controllers
ISO 27001	Information security management	Zero-trust access, immutable audit trails

5. A low-risk pilot path

- **Select** a single intersection or roadside controller.

- **Deploy** the edge node inline to isolate the controller — no changes to signal timing or field equipment.
- **Validate** by injecting false sensor data in a test; poisoned data is rejected, latency is unaffected.
- **Demonstrate** post-quantum key rotation and audit evidence; reverse cleanly if desired.

Ready to secure your mobility 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@iblates.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

© 2026 iBlades.ai. All rights reserved. All trademarks and technologies are the property of their respective owners.