IBLADES WHITEPAPER · RAIL & METRO

Quantum-Safe Rail & Metro Networks

Protecting signaling and train control, separating operational networks from IT, and future-proofing passenger data — without voiding vendor warranties or interrupting service.

← Aerospace & Transportation

In this paper

1. Executive summary

Rail and metro operators demand zero-fail uptime, yet their signaling and train-control systems increasingly connect to corporate IT, remote maintenance, and vendor networks. That convergence opens a ransomware path into safety-critical operations, while long-lived passenger and movement data becomes a target for future quantum decryption.

iBlades secures rail networks with a hardware-anchored, post-quantum fabric that overlays existing systems. It isolates signaling and control from compromised IT, secures maintenance and inspection communications, and counters AI-driven attacks by shrinking the exposed software surface — all without modifying proprietary signaling systems or voiding vendor warranties.

2. The 2026 threat landscape

Ransomware into safety-critical signaling

As train-control and signaling systems connect to IT and remote maintenance, attackers gain a lateral path into networks that must never fail. A single ransomware event can halt an entire line, and legacy signaling software often cannot be patched without vendor recertification.

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing exposed services, generating evasive malware, and mapping trust relationships to move laterally after a foothold. **Data poisoning** of control or sensor feeds turns a data-integrity problem into a safety problem.

> **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)

Passenger, ticketing, and operational data intercepted today can be decrypted once quantum computers mature — a real risk for data that stays sensitive for years.

---

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.

- **GuardTron™** — "stealth-mode" hardware isolation for signaling and control rooms; agentless, so it protects proprietary systems without voiding vendor warranties, and micro-segments operational networks from IT.
- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh; secures maintenance links and future-proofs passenger and operational data.

- **ManoTron™** — hardware-secured mobile communications for field and maintenance teams, including secure links for track and tunnel inspection drones.

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 between IT and operational networks.
- **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
EN 50701	Railway cybersecurity	OT isolation, segmentation, secure communications
IEC 62443	Industrial / OT security	Hardware segmentation and boundary protection for signaling
ISO 27001	Information security management	Zero-trust access, immutable audit trails

---

5. A low-risk pilot path

- **Select** a single signaling or control link at one station or depot.
- **Deploy** the edge node inline in stealth mode — no changes to the signaling system or vendor certification.

- **Validate** isolation with an attack simulation; legitimate control traffic passes, unauthorized access is blocked.
- **Demonstrate** post-quantum key rotation and audit evidence; reverse cleanly if desired.

Ready to secure your rail 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