ONDAS NETWORKS

Cybersecurity Benefits of Modernizing Legacy Narrowband Radio Train Networks

EXECUTIVE SUMMARY

Legacy narrowband (NB) radio systems in critical train operations were not designed to withstand modern cyber threats. Upgrading to the advanced wireless technology of IEEE 802.16t ("dot16") modernizes private networks to deliver transformational cybersecurity improvements which are critical for national security, public safety, and critical infrastructure.

KEY CYBERSECURITY BENEFITS OF UPGRADING TO dot16

1. End-to-End Encryption with Dynamic Key Management
Utilizes AES-256 and TLS 1.3 protocols for dynamic, ephemeral encryption keys. dot16 supports mutual authentication across endpoints, eliminating static key vulnerabilities common in legacy NB systems.

2. Zero Trust Architecture Compatibility
dot16 networks enable microsegmentation, identity-based access control, and policy enforcement at the network edge. Compliant with NIST Zero Trust and CMMC frameworks.

3. Edge Computing for Threat Detection and Response
Built-in edge compute capabilities allow for real-time anomaly detection and local incident response—without needing to backhaul data to a centralized system.

4. Secure Container-Based Software Management
dot16 supports Docker- and Kubernetes-based isolation of services, using cryptographically signed containers. This architecture enables rapid deployment and rollback in case of compromise.

5. Over-the-Air (OTA) Updates with Integrity Verification
Push signed firmware and updates directly to field-deployed radios securely—eliminating the risks and delays of manual updates.

6. Full Visibility and Auditability
dot16 enables continuous telemetry, SIEM integration, and full-stack logging—ensuring organizations can detect, investigate, and respond proactively.

7. Resilient, Self-Healing Network Architecture
In the event of a cyber incident, dot16's containerized services can auto-redeploy or restart. Edge nodes remain operational even when disconnected from central control.

ABOUT IEEE 802.6t

IEEE 802.16t is a next-generation wireless communication standard specifically designed for mission-critical industrial applications, including railroads and other critical infrastructure sectors. Ratified in 2025, it operates in sub-1 GHz spectrum bands and supports narrow and wide channel configurations while delivering high throughput, low latency, and robust cybersecurity protections.

The standard incorporates advanced encryption (AES-256), mutual authentication, software-defined networking, and quality-of-service (QoS) controls, making it well-suited for private broadband networks that require secure, resilient, and scalable communications.

As an open IEEE standard, 802.16t promotes vendor interoperability, rapid innovation, and long-term sustainability for modernizing industrial wireless systems.

dot16

LEGACY NARROWBAND SYSTEMS ARE AT RISK

As legacy narrowband systems struggle to keep pace with today's cybersecurity demands, organizations face increasing risk from sophisticated threats. IEEE 802.16t (dot16) was designed to meet this challenge by offering a secure, resilient alternative for private wireless networks. The comparison below highlights the critical differences between outdated infrastructure and a modernized dot16 deployment.

Vulnerability	Legacy NB Systems	Modernized with dot16
Encryption Agility	Static keys, outdated ciphers, no encryption	AES-256, TLS 1.3, ephemeral keys
Auth Control	Weak or pre-shared	PKI, MFA, RBAC
Software Updates	Manual, infrequent	Secure OTA, automated
Threat Detection	None or delayed	Real-time, edge-based
Supply Chain Risk	Hard to verify firmware	Verified container images
Audit & Logging	Minimal	Full-stack observability

STRATEGIC OUTCOMES – ADOPTING dot16 (OR IEEE 802.16t)

- **Strengthens cyber posture across communications infrastructure**
- **Enables compliance with DoD, DHS, and NIST cybersecurity mandates**
- **Secures critical rail safety applications and operations**
- **Protects against modern threats including ransomware, spoofing, and supply chain attacks**
- **Future-proofs network for AI/ML, autonomous operations, and integrated ISR**

Legacy Wireless Rail Networks	Critical Rail Network Use Cases
900 MHz **450 MHz** **220 MHz** **160 MHz**	MC-IOT . Vital Communication Links . Centralized Traffic Control Crossing Monitoring . Wayside Detectors . Positive Train Control Distributed Power . Remote Control Locomotive Operations Intelligent Crossings . Distributed Locomotive Power . Train Telemetry Head-of-Train (HOT) . End-of-Train (EOT)

Learn More:
To explore how IEEE 802.16t and Ondas Networks' technology can secure your communications infrastructure, contact us at:

networks-inquiries@ondas.com | www.ondasnetworks.com