LILEE SYSTEMS

Solution Brief

Next Generation Communications Management Unit

Market challenges

- **Wireless security:** Current solutions do not support message authentication and integrity checking which makes them extremely vulnerable to various security attacks.
- **Interoperability:** The lack of interoperability between rail operators results in operational downtime when host and tenant railroads have to coordinate schedules to update security keys.
- **Compliance:** The cryptographic algorithms and key distribution technique have to comply with the National Institute of Standards & Technology (NIST) or a similar standards body approved by FRA.
- **220 MHz radio links:** The capacity and coverage of the 220 MHz radio spectrum is no longer sufficient and may cause train delays.
- **Legacy hardware:** Aging hardware may not provide enough computational capacities for security software upgrades.

LILEE Systems Next Generation Communications Management Unit (CMU)

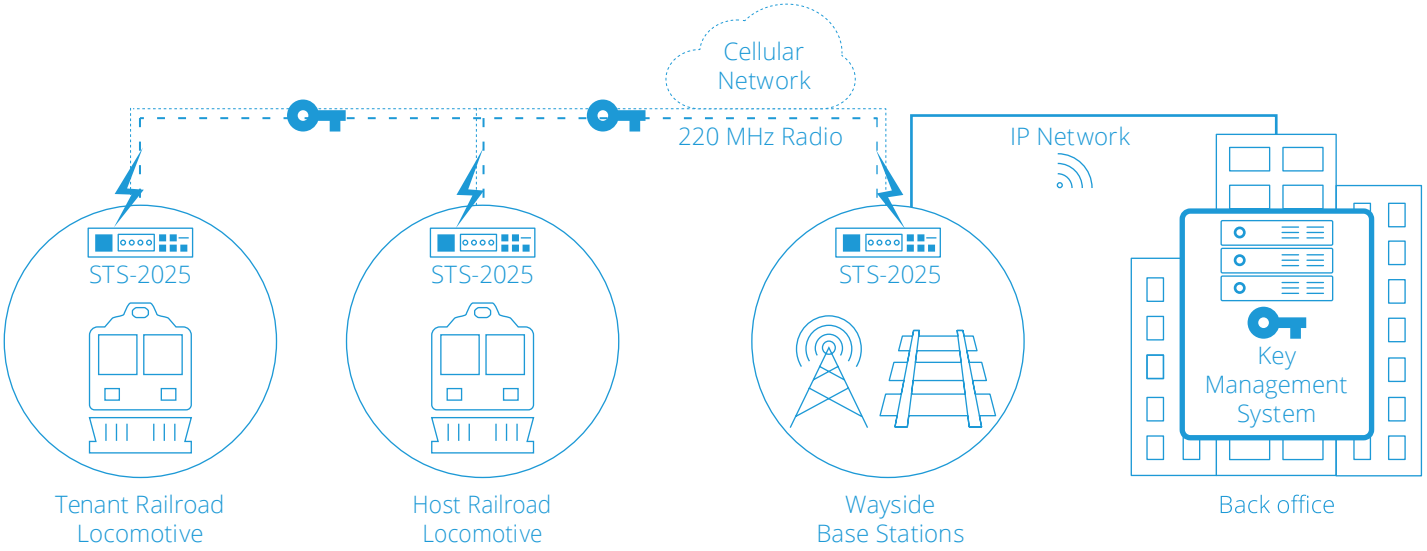
LILEE Systems offers the first and only 449 CFR § 236.1033-compliant solution on the market for wireless communications security and key management. The integrated solution consists of:

- **Key Management System (KMS):** Centrally manages cryptography-based keys among host and tenant railroads for interoperability and secure communications, and conducts key distributions and updates in the back office for remote systems
- **Wireless Security Software:** Enables authentication of messages between wayside systems and locomotive onboard computers on primary 220 MHz and on all alternate links
- **TransAir® STS-2025 Rugged Mobile Gateway**: Replaces existing, aging wayside and onboard communications units to deliver robust processing power for security software upgrades and to provide cellular backup links for PTC wireless communications

Federal Railroad Administration (FRA), as per the Code of Federal Regulations (CFR) Title 49, Section 236.1033, requires that all wireless communications between the office, wayside, and onboard components in a PTC system shall provide cryptographic message integrity and authentication.

Feature and Benefits

- **Meeting the PTC deadline:** As the market's first 449 CFR § 236.1033-compliant solution, LILEE CMU has successfully supported our customers to meet the secure wireless communications requirements before the PTC deadline.
- **Securing wireless communications:** Key Management System (KMS) provides unique cryptographic keys to ensure message integrity and authentication, addressing the security vulnerabilities.
- **Achieving interoperability:** With an inter-KMS interface that allows automatic key exchanges between different railroads, KMS solves the interoperability problems, minimizing downtime while boosting operational efficiency.
- **Proven technology:** The solution is field-tested for system reliability and security following FRA-approved specifications. It is fully compatible with the existing ACSES PTC systems.
- **New hardware:** The new STS-2025 rugged mobile gateway delivers robust wireless connectivty, edge computing capabilities and scalability to support thousands of security keys and software upgrades. A PPS output for the 220 MHz radio reduces system complexity by eliminating a dedicated GPS receiver. OTA (over-the-air) remote management of devices and applications further increases operational efficiency.
- **Communication Redundancy:** The IPCM software for the Back Office provides communication redundancy via cellular connectivity when 220 MHz radios are out of coverage or too congested.



The LILEE Systems Next Generation Communications Management Unit Solution

To learn more about how to implement the FRA-compliant solution for secure wireless communications and key management, please contact **info@lileesystems.com**.

LILEE Systems
2367 Bering Drive
San Jose, CA 95131
United States
www.lileesystems.com