Chapter 1

Land Mobile Radio

Land Mobile Radio: Ensuring Reliable Public-Safety Communications

Scott Neal
Senior Vice President, Wireless and Court Technology Services
Mission Critical Partners

Nick Falgiatore
PE, Senior Technology Specialist
Mission Critical Partners

The Importance of Modernizing Legacy LMR for Public Safety

Across the United States, legacy land mobile radio (LMR) systems remain essential for public-safety and mission-critical communication, yet many are nearing or past end of life. Equipment obsolescence, deteriorating infrastructure, rising operational demands, and limited lifecycle funding are converging to create significant risks for reliability, resilience, and interoperability. To ensure long-term viability, agencies must pursue coordinated modernization to strengthen LMR communications. This includes system replacement or regional integration, robust lifecycle funding, and structured preventive maintenance.

Challenges Facing Land Mobile Radio Systems Today

LMR systems and voice communications underpin daily operations for first responders, utilities, transportation, and other mission-critical sectors. However, most systems rely on aging infrastructure, unsupported firmware, and subscriber equipment that manufacturers no longer service. Environmental stress on tower sites, outdated shelters, and insufficient backhaul further degrade system performance and reliability.

Coverage challenges remain widespread. While mobile coverage is often adequate, portable and in-building performance is inconsistent due to dense construction, urban growth, and unregulated in-building system installations. The result is operational vulnerability in high-risk indoor environments.

Cost escalation is another defining challenge. Project 25 (P25) systems, while offering modern features, have become prohibitively expensive for many jurisdictions. Total cost of ownership continues rising based on maintenance contracts, proprietary interfaces, software updates, and cybersecurity needs. Subscriber equipment is subject to similar pressures, with standard P25 radios costing $6,000–$7,000 and hybrid LMR/cellular devices exceeding $10,000 before subscription fees.

Cybersecurity risk is increasing as attackers target public-safety infrastructure and LMR systems shift toward IP-based architectures. Many agencies operate with obsolete firmware, inconsistent software updates, limited monitoring, and no dedicated cybersecurity personnel. As devices roam across LMR, commercial cellular, Wi-Fi, and private 5G networks, the attack surface continues to expand.

Despite these challenges, the LMR landscape is entering a transformative period. Multi-network, software-defined communications — blending LMR, cellular, private 5G, and satellite — promise stronger coverage, enhanced resilience, and operational capabilities that bridge the industry to next-generation public-safety communications.

Opportunities for the Future: Transformative Advances in LMR Technology

Hybrid LMR–Cellular Integration for Seamless Coverage – The most impactful development is seamless systems integration between LMR and broadband, enabling radios to automatically switch among networks based on coverage, policy, and operational priorities. This strengthens reliability in buildings, basements, dense urban centers, and remote areas where LMR alone is insufficient. Broadband access also unlocks capabilities such as GPS, mapping, CAD data, images, and video exchange.

Hybrid devices such as Motorola SmartConnect and L3Harris BeOn® are already in the field. Over time, these devices will support intelligent roaming across LMR, commercial cellular, private 5G, Wi-Fi, and satellite networks. Key benefits include:

- Near-continuous coverage without investing heavily in new LMR sites.
- Resilience during disasters or infrastructure failures.
- Greater flexibility in future system design and funding strategies.

Hybrid integration is a foundational step toward next-generation communications.

Private 5G Networks as Cost-Effective Alternatives to P25 – Private 5G networks provide broadband network coverage at significantly lower cost than new P25 sites. A private 5G radio site can be built for 8–10 times less than a P25 trunked site, while supporting data-rich applications beyond LMR's capabilities. These networks integrate easily with hybrid radios and serve use cases such as tribal lands, university campuses, industrial facilities, business districts, and municipal centers.

LEO Satellite Integration for Remote Coverage – Low Earth Orbit (LEO) constellations such as Starlink and Lynk introduce possibilities for direct-to-device satellite connectivity. This technology could extend coverage into remote terrain, wilderness areas, and environments where tower construction is impractical.

Satellite-enabled devices could eventually autonomously prioritize LMR, cellular, Wi-Fi, or satellite signals based on real-time availability.

Challenges remain — including latency, capacity management, device integration, and ensuring continuous satellite availability — but progress is rapid.

Broadband-Enabled Smart Features for Radios – Broadband integration will transform radios from voice-centric devices to multifunction operational platforms. Capabilities include:

- High-speed GPS and mapping.
- CAD incident data pushed to the radio.
- Transmission of images, video, and situational updates.
- Enhanced integration with 911 centers and command staff.

These features improve situational awareness, reduce response times, and strengthen decision-making.

Advanced Features: Automated Drone Deployment – Emerging concepts propose that activating the radio's emergency button could automatically deploy a drone to the user's location. This would provide instant overhead imagery, enhance responder safety, and improve search-and-rescue outcomes. Although early in development, this capability represents a significant operational innovation.

Challenges Facing Land Mobile Radio Systems Modernization

Aging Infrastructure and Unsupported Equipment – Many LMR systems rely on discontinued components, unsupported firmware, and aging analog or early digital equipment. Even P25 trunked systems are reaching the 10-year mark when major upgrades and costly service agreements are required.

Notable issues:

- Inability to obtain replacement parts for older VHF/UHF systems.
- Deteriorating or inadequate shelters, grounding, antenna systems, and microwave backhaul.
- Environmental exposure often leads to catastrophic failures.

Persistent Coverage Gaps in Urban and Indoor Environments – Coverage gaps, especially for portable and in-building use, remain universal. Urban growth, new construction, and unregulated or poorly installed in-building systems degrade signal quality.

Notable issues:

- Conventional systems lack engineered, guaranteed coverage.
- In-building coverage remains inadequate despite National Fire Protection Agency (NFPA) requirements.
- Agencies lack the staff needed to regulate third-party in-building system installations.

Skyrocketing Costs and Vendor Lock-In – The LMR ecosystem has become increasingly expensive and consolidated, with agencies locked into proprietary interfaces and vendor-driven upgrade cycles.

Notable factors:

- P25 system costs are prohibitive for many small and medium agencies.
- Total cost of ownership is rising across maintenance, software, and cybersecurity.
- Vendor dominance (particularly Motorola) drives pricing power.
- Lack of open interfaces limits multi-vendor competition.

Cybersecurity Vulnerabilities in Public-Safety Communications – System reliability is threatened by absent redundancy, insufficient monitoring, and reactive, rather than preventive, maintenance.

Notable issues:

- Growing complexity of the communications network introduces new failure points.
- Maintenance, software, and cybersecurity costs are increasing.
- Few agencies maintain capital reserves or lifecycle funds for system refreshes.
- Vendor-driven obsolescence forces costly upgrades on fixed timelines.
- Workforce shortages limit engineering, technical, and cybersecurity proficiency.

Understanding P25 Interoperability Challenges – Despite P25's standardized air interface, practical interoperability remains limited due to variable compliance, legacy systems, proprietary features, and inconsistent governance.

Notable issues:

- Difficulty coordinating across regions and mutual-aid partners.
- Operational issues with multi-vendor subscriber fleets.
- Reliance on SOPs, governance, and training that often lag technological change.

Addressing Sustainability and Lifecycle Management for Public Safety Systems

Many agencies lack structured lifecycle management for infrastructure, subscriber units, and software agreements. Without proactive funding and planning, systems undergo emergency replacements rather than scheduled modernization.

Notable issues:

- No multi-year refresh plans for radios or infrastructure.
- Software update agreements vary widely and are inconsistently funded.
- Large capital costs arise after long-term service contracts expire.

Subscriber Equipment and Cost Challenges for Public Safety Agencies – Subscriber inventories contain large numbers of obsolete radios lacking encryption, GPS, broadband capability, or current firmware. Replacement costs continue to rise, and some vendors now charge subscription fees tied directly to radio functionality.

Examples:

- P25 radios: $6,000–$7,000
- Hybrid devices: $10,000 or more, plus recurring subscription charges

Criminal Justice Information Services (CJIS) Compliance and Encryption Requirements for LMR Systems – CJIS security requirements mandate that criminal justice information transmitted over LMR systems must be encrypted minimally to the 128-bit standard. Encryption to this standard requires additional costs.

Facilities and Environmental Risks Impacting Public Safety Networks – Tower sites and shelters vary dramatically in condition. Space limitations, inadequate grounding, and failing HVAC systems shorten equipment lifespan and harm system performance. Geographic challenges, especially in rural and mountainous regions, make comprehensive coverage expensive and difficult. Environmental risks include extreme heat/cold, lightning, flooding, hurricanes, wildfires, and tornados.

Cybersecurity Concerns for Public Safety Communications Systems – Risk of cyberattacks is now a major concern as public-safety networks become targets for ransomware and other attacks. Many LMR systems contain outdated software, unsupported firmware, and weak encryption. With limited cybersecurity personnel, agencies depend heavily on vendors.

Risks include:

- AI-driven cyberattacks are becoming more sophisticated.
- Large attack surfaces from end-of-life components.
- Vulnerabilities in IP-based system elements.
- No internal monitoring tools or mitigation capabilities.
- Expanded exposure as radios roam across commercial and private networks.

Emerging Trends in Public Safety Communications Technology

Adoption of Hybrid LMR–Cellular Systems offering seamless roaming and multi-network resilience.

Rise of Private 5G Networks as a cost-effective alternative to P25 expansion and a platform for advanced broadband applications.

Satellite Integration for Coverage Expansion enabling resilient coverage in remote regions and disaster zones.

Broadband-Enabled Smart Radios transforming radios into smart, data-rich platforms that enhance situational awareness and operational safety.