Funding and Sustaining Land Mobile Radio (LMR) Trio
Part 1: Educating Decision-Makers on LMR Fundamentals

Introduction

Every day dedicated public safety responders risk their lives to make our communities safe and secure. Emergency responders at every level of government—federal, state, local, tribal, and territorial—must respond to and manage incidents of varying size and scope and assist communities with recovery efforts. This mission requires timely decision-making and coordination among law enforcement, fire, emergency medical services personnel, 911 staff, emergency managers, and medical professionals. As Figure 1 represents, multiple response agencies may be involved in a single incident. Communications is a mission-critical part of that response; a breakdown of communication at any one of these junctures could negatively affect response, risking life and property.

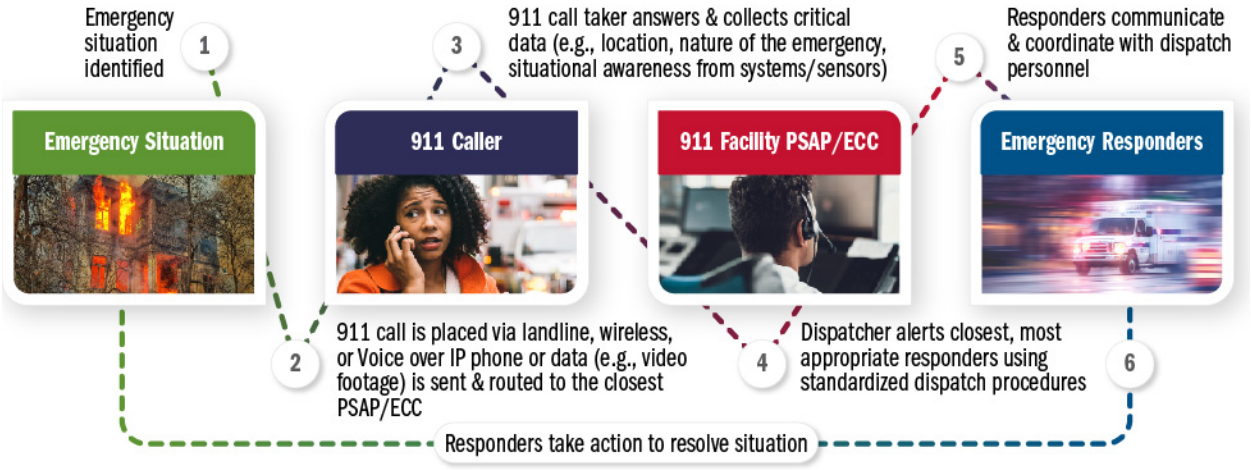

Figure 1: Mission-Critical Communications during Emergency Response

Public safety agencies rely on LMR systems as the primary means for transmitting mission-critical voice communications between emergency responders.

What Are LMR Systems?

LMR systems are terrestrially-based, wireless, narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works entities, and the military in tactical and non-tactical environments to support voice and low-speed data communications. LMR systems typically consist of handheld portable radios, mobile radios, base stations, a network, and repeaters.

- **Handheld portable radios** are carried by public safety personnel to provide immediate access and availability for mission-critical communications to Public Safety Answering Points (PSAPs)/Emergency Communications Centers (ECCs) and other public safety responders.
- **Mobile radios** are often located in vehicles and use the vehicle's power supply and a larger antenna to provide a greater transmission range than handheld portable radios.
- **Base station radios** are located in fixed positions, such as in PSAPs/ECCs.
- **A network** is required to connect the different base stations to the same communications system.
- **Repeaters** are used to increase the effective communications range of handheld portable radios, mobile radios, and base station radios by retransmitting received radio signals.

Figure 2 depicts a basic LMR system and shows the flow of communication between emergency responders using portable or mobile radios, which are connected to a network of base stations, towers, and repeaters.

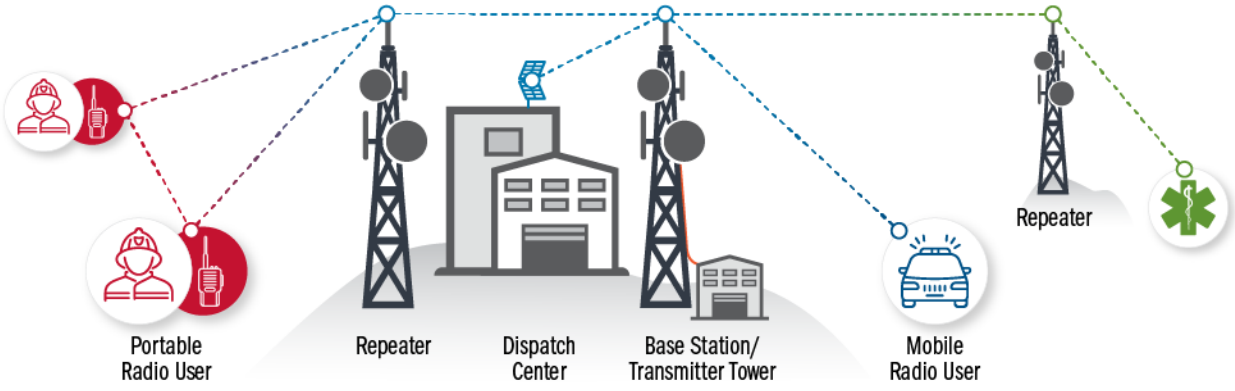

Figure 2: Basic Components of an LMR System

Since the 1930s, public safety officials have deployed LMR to support mission-critical voice communications. Over time, many public safety agencies have migrated from basic LMR systems to more advanced communications systems. Many agencies have transitioned from basic, **conventional** systems to more complex **trunked** systems. Conventional radio systems have dedicated frequencies and channels assigned to individual groups of users. When a user selects a channel and makes a call, other group members cannot use the channel until the transmission is complete. Trunked systems are computer-controlled and assign a pool of channels for use by multiple individuals, agencies, or departments. When users make a call on a trunked system, the system automatically selects an available channel, leaving the remaining channels open for others. While trunked systems are more complex and require more infrastructure than conventional systems, they allow a large group of users to share channels, increase capacity and interoperability, reduce congestion, and enable the more efficient use of communication channels.[1]

Some states, regions, and large urban areas have migrated their LMR systems supporting networks from basic systems to computer-based, or Internet Protocol (IP)-based systems, which has allowed agencies to increase capacity and connectivity (i.e., the number of users on a system), enhance capabilities, and improve interoperability. Figure 3 provides an example of a regional or statewide IP network.

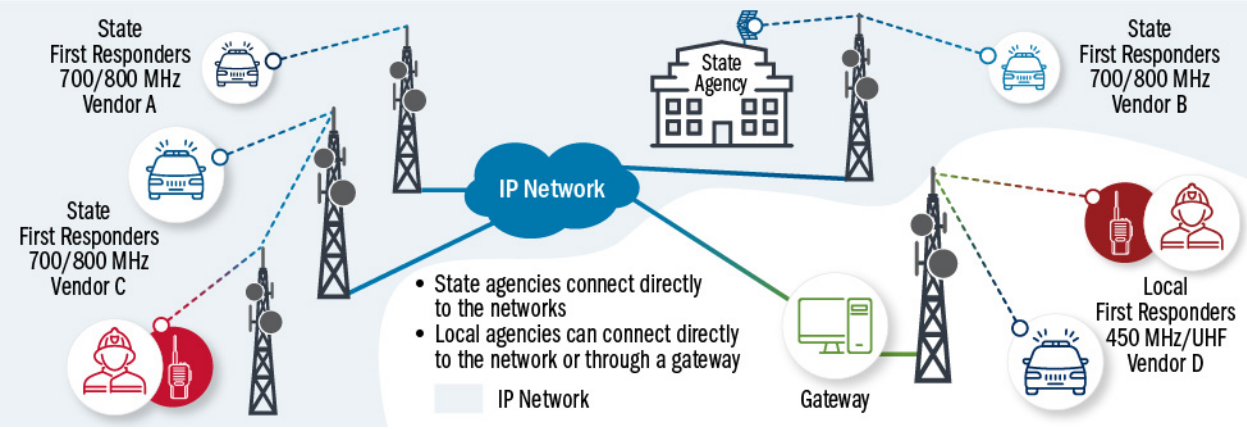

Figure 3: Example of a Regional or Statewide IP Network

[1] "First Responders: Much Work Remains to Improve Communications Interoperability." *GAO-07-301*: Published: April 2, 2007. gao.gov/products/GAO-07-301.

Why Are LMR Systems Important?

LMR systems are part of the multi-path approach to mission-critical communications. LMR systems continue to be the primary voice communications pathway for public safety personnel. Systems are designed and implemented to meet the unique needs of public safety, and deliver secure, reliable, mission-critical voice communications in a variety of environments, scenarios, and emergencies. Public safety personnel have used LMR technologies for many years as they provide the most reliable and highly available means of voice communications for public safety.

LMR technologies have been enhanced to provide mission-critical features. LMR technology has progressed over time from conventional analog voice service to complex systems incorporating digital protocols and trunking features that enable such features as rapid call-setup, group calling capabilities, high-quality audio, and tiered priority access to end-users. These enhancements have improved the interoperability, spectral efficiency, security, reliability, redundancy, and functionality of voice and low-speed data communications for public safety and public services personnel.

Public safety agencies are proficient in the use of LMR technologies. LMR technologies' features and functions have been integrated into response protocols and training curriculum and tested through planned exercises and real-world events. While new technologies are entering the market every day, emergency responders are most familiar with how LMR technologies work. This familiarity has helped public safety agencies plan for various scenarios and execute effective response operations using the unique features and functions of LMR.

Federal, state, local, tribal, and territorial agencies have invested billions of dollars in LMR infrastructure. The federal government has provided billions of dollars in grant funding coupled with state, local, tribal, and territorial government funds to install, expand, and enhance LMR systems. Individual states, localities, and regions have also devoted public funding to communications systems enhancements. Agencies and jurisdictions have worked together to leverage existing infrastructure, connect and expand LMR systems, and create networks of communications systems—a "systems of systems" environment. State, local, tribal, and territorial governments are continually upgrading these systems to improve interoperability, capabilities, coverage, and capacity while extending the return on investments. These systems are in place and provide proven, reliable, and redundant public safety communications support.

Current Challenges to Consider When Upgrading LMR Systems

Agencies have a variety of communications systems in place today as a result of LMR system and technological evolutions over the past several decades. Some agencies have basic LMR systems in place, while other agencies have implemented more advanced systems. Not all systems are compatible with each other, sometimes inhibiting public safety responders and officials' ability to talk to each other during routine and emergency incidents. Below are some of the challenges facing agencies and jurisdictions interested in upgrading public safety communications systems:

- **Agency-specific systems** have been designed to meet specific agency missions in defined geographic areas. Vendors historically offered customized and proprietary LMR systems and equipment designed to serve unique agency missions; vendors often built systems with proprietary features and functions and offered vendor-specific solutions that served single agency missions and needs, but may not have been compatible with surrounding systems. As a result, these siloed LMR systems may reduce communications interoperability with other agencies and neighboring jurisdictions.
- **Spectrum issues** can arise when agencies and jurisdictions secure licenses to operate their communications systems on the radio spectrum. The Federal Communications Commission assigns spectrum to public safety agencies according to their needs and use. Public safety communications systems operate on different spectrum frequencies (e.g., very high frequency [VHF], ultra-high frequency [UHF], 700 megahertz [MHz], 800 MHz). Systems that operate on different frequencies are not always interoperable. Agencies often invest in a combination of technologies that connect disparate systems to enable interoperability between systems, frequencies, and responders.

- **Non-standards-based systems** that are vendor-specific or customized, and therefore are incompatible with neighboring public safety LMR systems. Over the past 25 years, public safety agencies have embraced and are building accredited technical standards-based systems that are compliant with the Project 25 (P25) Suite of Standards.
- **Advanced technologies that may not be backward compatible** with current systems, including advanced LMR features, IP or computer-based systems, and broadband technologies that cannot interoperate with older LMR systems. This incompatibility results in proliferating interoperability issues until accredited technical standards are in place to facilitate connections between existing and new capabilities.
- **Lack of redundancy/backup communications solutions** that include commercial cellular voice and data networks as the primary or only backup source; these networks may be overwhelmed by system outages, congestion, and capacity issues during emergencies. As a result, emergency response may be hindered without call prioritization for responders or access to redundant communications systems.
- **Encrypted communications** that are proprietary or not standardized, prohibiting interoperability with radios that are not encrypted in the same manner; if encryption is used, it should be accredited, technical standards-based, and implemented inclusively among the collaborating agencies and jurisdictions to ensure existing interoperability is maintained.
- **Cybersecurity risks** continue to impact LMR systems through jamming, eavesdropping, and denial of service. While traditional systems have limited means of cyber entry, interconnection with IP-networks poses an exponentially increased risk. Public safety agencies must implement and maintain a robust cybersecurity posture.

Guidance for Agencies Interested in Upgrading LMR Systems

To overcome these challenges, the federal government provides grant funding and guidance to states, localities, tribes, and territories. The Cybersecurity and Infrastructure Security Agency (CISA) collaborates with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) to develop the annual *SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*. The *SAFECOM Guidance* provides recommendations, best practices, and resources to public safety agencies investing federal funds in emergency communications. **CISA encourages grant recipients to:**

- **Review the *National Emergency Communications Plan* (NECP) and *Statewide Communication Interoperability Plan* (SCIP)** to ensure that grant proposals support broader plans to improve communications operability and interoperability across all systems and users.
- **Coordinate with Statewide Interoperability Coordinators (SWICs)**, who serve as a single point of contact to implement statewide plans and coordinate regional projects.
- **Develop standard operating procedures** that provide mutually-approved processes to coordinate public safety agencies' resources during any operation.
- **Invest in training, exercises, and activities that enhance operational coordination** and prepare emergency responders to communicate across agencies.
- **Purchase standards-based equipment** (e.g., P25 for LMR, Long-Term Evolution for broadband technologies) to ensure public safety systems can interoperate.
- **Recognize cybersecurity risks** and continually invest in mitigation measures, including activities that encourage continuity and resilience.

State, local, tribal, and territorial governments should reference the *SAFECOM Guidance* when developing emergency communications projects and target federal funding toward the priorities above. In the event grant funding is unavailable, public safety agencies must identify alternative funding sources in their community. SAFECOM and NCSIWC developed the *Funding Mechanisms Guide for Public Safety Communications*, highlighting strengths, challenges, opportunities, and other considerations for funding sources to help agencies determine if certain mechanisms are suitable for their jurisdiction.

Conclusion

LMR technologies provide mission-critical voice communications tailored to public safety needs. While the community considers new and emerging technologies to supplement communications, public safety agencies must sustain current LMR capabilities until other technologies provide the reliability that LMR offers. Decision-makers should consider the impact of funding decisions on their agencies' ability to communicate during day-to-day incidents, emergencies, and natural and man-made disasters. The federal government and public safety agencies have spent billions building a vast LMR infrastructure and training users. Without continued investment to operate and maintain interoperable LMR systems, emergency communications could be compromised.

About SAFECOM/NCSWIC

SAFECOM includes more than 70 members representing federal, state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who aim to improve multi-jurisdictional and intergovernmental communications interoperability through collaboration with emergency responders and policymakers across federal, state, local, tribal, territorial, and international partners. SAFECOM members bring years of experience with emergency communications during day-to-day operations, emergencies, and natural and man-made disasters. They offer insight and lessons learned on governance, planning, training, exercises, and technologies, including knowledge of equipment standards, requirements, and use. SAFECOM members also provide input on the challenges, needs, and best practices of emergency communications, and work in coordination with the Department of Homeland Security to share best practices and lessons learned with others.

NCSWIC encompasses SWICs and their staff from the 56 states and territories. The council assists states and territories with promoting the critical importance of interoperable communications and sharing best practices to ensure the highest level of interoperable communications within and across states and with their international partners along the borders.

Additional Resources

Public safety agencies can reference the following additional materials for more information:

- SAFECOM Technology Resources: This webpage provides guidance and recommendations on communications technologies used in the public safety environment, including multiple LMR and P25 encryption resources such as the *Statement of P25 User Needs*, *Operational Best Practices for Encryption Key Management*, *P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Primer*, and *Best Practices for Planning and Implementation of P25 ISSI and CSSI*.
- P25 Suite of Standards: The Telecommunications Industry Association's website contains P25 standards development activities that address all technical matters for private radio communications systems and services, including definitions, interoperability, compatibility, and compliance requirements.
- Shared Communications Systems and Infrastructure (SCSI) Fact Sheet and SCSI Along the Southwest Border: This fact sheet and report inform the public safety community on the vision and benefits of SCSI. The materials outline the governance, risk management, resource sharing, and operations considerations that need to be addressed to ensure project success. Additionally, the report examines the opportunities, challenges, and actions required to create a SCSI project for federal, state, local, and tribal public safety organizations operating along the Southwest Border, serving as a case study for other regions.
- Emergency Communications System Value Analysis Guide: This guide is designed to help public safety agencies evaluate the cost-effectiveness of system components (e.g., infrastructure, fixed station equipment, devices, accessories, features, software, and data storage). It provides recommendations, best practices, and a Value Analysis Checklist to assist agencies in making these decisions. The accompanying brochure, *Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers*, provides key considerations and trade-offs between the cost and value of communications systems components when presenting plans to decision-makers.