WHITE PAPER

# Introducing Unified Critical Communications

## for Public Safety

## EXECUTIVE SUMMARY

Public safety agencies already use a range of wireless communications networks, including Land Mobile Radio (LMR), public carriers like 3G and 4G, WiFi and satellite to connect back office and the field. The most basic form of communication that any agency uses is its LMR network, which is critical to emergency response. Increasingly, mobile data is being used to proactively and efficiently address public safety challenges. Dedicated public safety broadband networks are on the horizon. Each network type has its advantages for certain applications and tasks, but with that additional choice comes confusion.

By unifying their critical communications, agencies gain:

- more efficient operations and increased end user productivity,
- enhanced interoperability,
- increased cost savings,
- greater coverage,
- better resiliency.

## CONTENTS

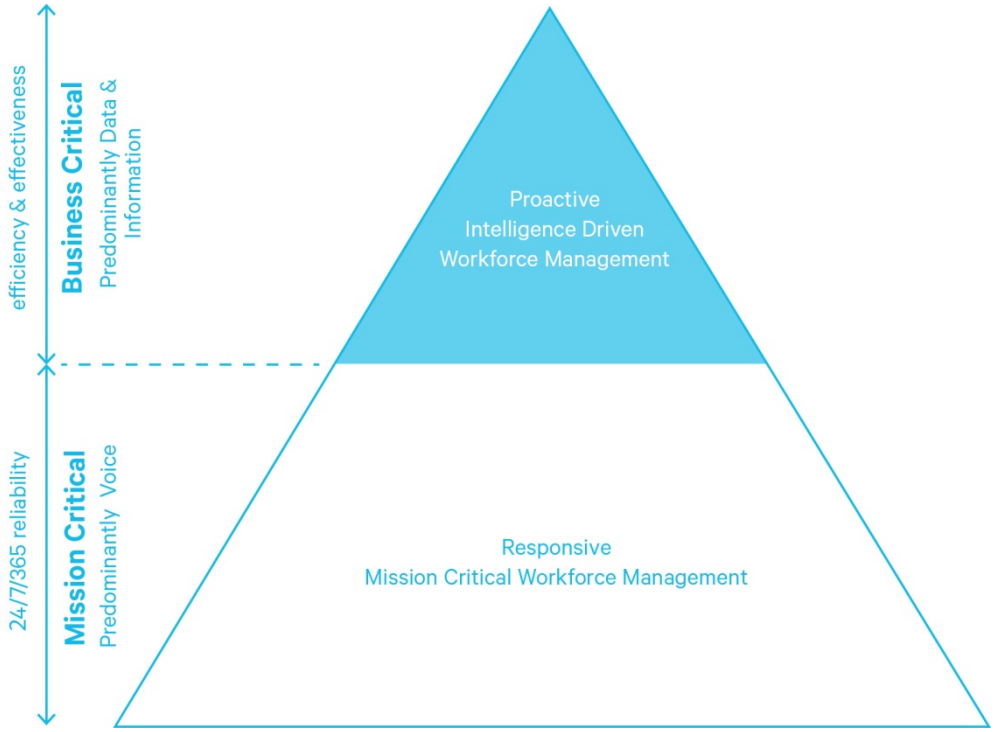

## CHALLENGING THE CURRENT MOBILITY PARADIGMS

A new generation of field workers, and greater ICT influence, demand the choice of durable, smart mobile devices to gain immediate access to this rich source of information. This brings with it a new set of challenges for agencies to deal with. The challenges include:

- the use of personal smartphones and tablets known as Bring Your Own Device (BYOD)
- policies to define and enforce mobile device use,
- vulnerabilities and security issues associated with mobile devices,
- finding, developing and using appropriate applications on mobile devices,
- managing data usage to avoid budget overruns,
- poor user adoption of agency applications.

The most basic application is effective voice communications required to meet mission critical objectives, but now mobile applications share information, video and text between the field and the back office, often simultaneously sharing different types of information with multiple operatives. The way these applications are used is reflected in the agency's standard operating procedures.

## THE HIERARCHY OF AGENCY NEEDS




***"…fragmented, disparate networks and systems inhibit effective and timely communications between staff, agencies and across jurisdictional lines."***

Historically, agencies have used public broadband networks to connect back-end systems to front-line staff. Service Level Agreements (SLAs) over private and public networks differ greatly, yet as the dependency on real-time predictive information increases, fragmented, disparate networks and systems inhibit effective and timely communications between staff, agencies and across jurisdictional lines.

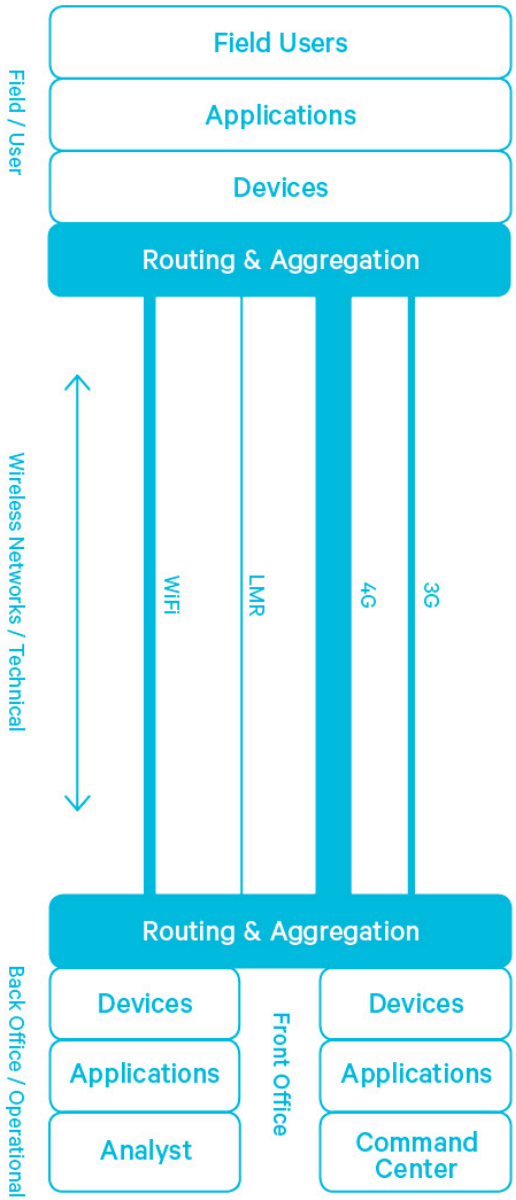
Increasingly, private broadband spectrum will be used to secure reliable access to communications, but it is not the only solution as the economics for deploying parallel networks will make it difficult to achieve necessary geographic coverage.

## UNIFYING YOUR CRITICAL COMMUNICATIONS

Unifying critical communications begins with the field officers and command centers who serve your community, who are often tasked with making effective decisions in extremely stressful situations.

However no single network can deliver all the information types required to achieve efficiency and effectiveness gains, particularly in the dynamic environment of modern public safety. This comes down to simple physics and economics. Integrating multiple communications bearers to create a single communications network will link the field to the back office.

The diagram illustrates unification as a solution.



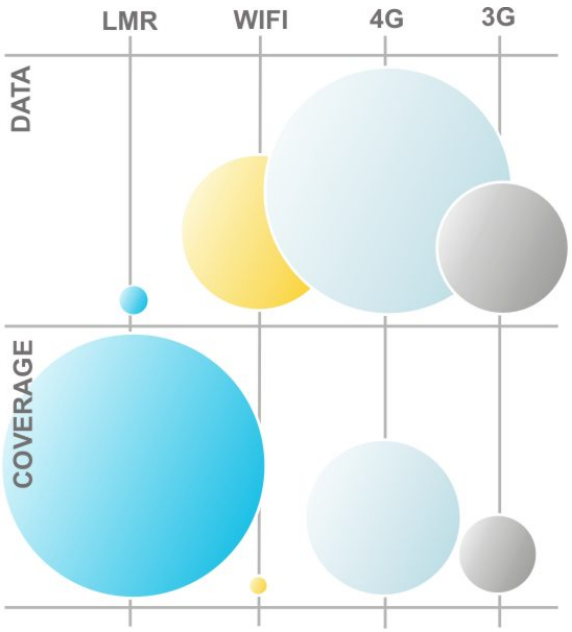

***… no single network can deliver all the information types required to achieve efficiency and effectiveness gains…***

## COMPARING TECHNOLOGIES

Wireless networks for connecting mobile staff, vehicles, users and applications include Land Mobile Radio (LMR), Public Cellular (3G and 4G LTE), WiFi, Satellite and Private LTE.

| | Advantages | Disadvantages |
|---|---|---|
| **LMR** | Wide area coverage, resilient, secured, rugged devices, greater coverage per site makes alternate power supplies more cost effective | Very low data rates, geared for predominantly voice, and some mission critical workforce management. |
| **3G Public** | Wide area coverage, inexpensive access | Moderate data rates, subject to commercial traffic congestion (with some ability to make a Quality of Service agreements), coverage follows population centers, smaller coverage per site increases costs of alternative power supplies |
| **4G LTE Public** | Highest data rates | Smaller coverage area currently, commercial service not geared to critical access priorities |
| **WiFi** | High data rates are possible, simple and cheap to deploy | Very small coverage area |
| **Satellite** | Available in all areas | Expensive user equipment and access |
| **Private 4G LTE** | High data rates, private control over access | Smaller coverage area, expensive to deploy duplicate infrastructure |

The diagrams that follow compare two critical network properties – coverage and data rates, succinctly illustrating why a single network can no longer meet complex agency requirements.




Simply by assessing the coverage and data capabilities of each technology, it becomes clear that no single network can serve the diverse needs of Public Safety agencies, so employing multiple networks becomes the reality. The requirements for unification of networks drive seamless use and roaming between them.

## MEETING AGENCY REQUIREMENTS

No single network can meet all the diverse requirements for their critical communications. This section summarizes their needs against the wireless network types.

### Mission Critical

People's lives and safety are dependent on network functioning and availability, where users have access to the network 24/7/365. There must also be a means of quickly communicating with large groups of people, setting up group communications with the push of a button, and prioritizing users depending on the situation. Networks must recognize the most important calls (distress/call for help) and pre-empt other communications, so that the most critical communications can go straight through.

### Business Critical

Business critical communications affect the productivity and efficiency of operations. They typically save time and money by reducing the resource required to complete necessary tasks. For example, in-field report filing for police officers reduces the need for them to return to base to submit reports, enabling them to spend more time on the street.

### Future-proof

As agency communication requirements change, agencies must adapt the communications network to meet identified needs. Networks built on open standards ensure a choice of vendors for network upgrades - proprietary networks can lock agencies into reliance on a single vendor.

### Control

Public Safety agencies must maintain autonomy over their communications network, and as importantly, certainty and control over their budget. Public network operators can change the rates, removing that budget certainty.

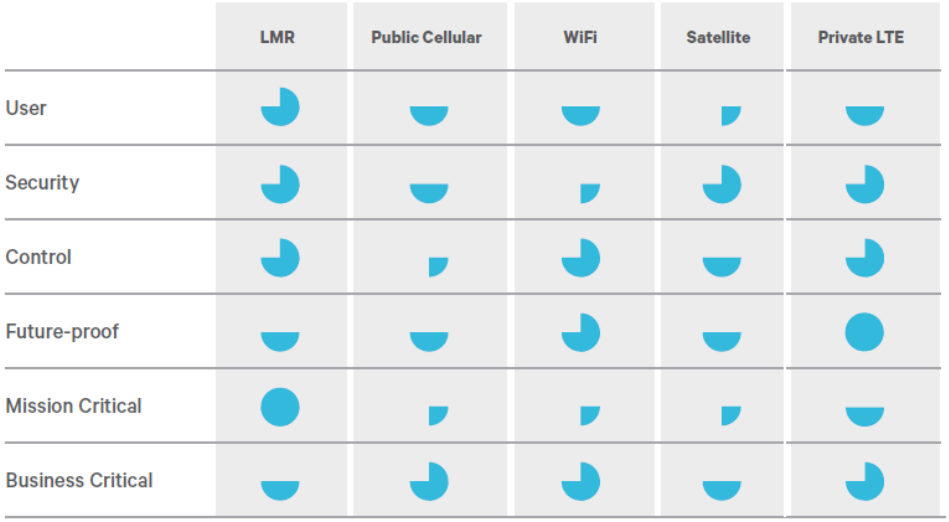
### Security

Security refers to both physical and electronic security, protecting against both intentional and unintentional attacks. Agencies must be able to control who has access to what information, and when, with checks and alarms to notify when security breaches occur. Various Mobile Device Management (MDM) tools can be implemented that allow applications and data to be managed and secured, across all mobile devices used on the network.

### Choice of User Access

Device interfaces must be simple enough that users can be quickly trained to use them with minimal re-training needed to retain this knowledge. Devices also need to be rugged to avoid damage in adverse conditions, have a long battery life and offer a wide range of useful functions.

***"agencies must be able to control who has access to what information, and when, with checks and alarms to notify when security breaches occur."***



## WHY UNIFY YOUR CRITICAL COMMUNICATIONS

Unified mission critical networks retain the total control necessary for mission critical users, but conceal the complexity of which bearer is used. Individual agency policy and needs drive the rules that frame how bearers are chosen, for each communication. Moving beyond this by looking at specific data flows can dramatically increase the performance and efficiency directly or by shaping traffic depending on need.

For example:

A police officer can received a 3G voice call on his smart phone. While he is taking the call, an application on the same smart phone monitors the group-mode LMR voice channels. At the same time, his sensor and GPS data is being sent over the private LTE network.

This is not only possible through this unified approach but is quickly becoming essential for proactive public safety operation. However if these networks remain entirely disparate, their major benefits cannot be realized. So the multiple benefits of unifying critical communications become apparent.

### Increased operational efficiency and effectiveness

The greatest benefit of unified critical communications is the increased efficiency and effectiveness that comes with integrated mission critical and business critical communications.

Unified critical communications provides agencies with solutions to the challenges of mobility and BYOD, driving BYOD policy. It allows your organization to augment the personal device with wireless access to other networks and have control over what applications use these other air interfaces when (i.e. offload information onto “free networks” or route information based on cost & criticality). This allows the organization to retain the cost leverage that BYOD provides, but at the same time optimize the air-time expenditure on other networks.

### Seamless communication

Central to unified critical communications is the “glue” that allows information to be shared and transported across a variety of applications and wireless systems. This includes Mobile Enterprise Application Platforms that binds back-office information to any device, and APIs (Application Programming Interfaces) that allow information to enter, or be extracted from the system, either in the field (eg sensor data) or back office. Applications can be developed for field users and then tied into the back-end systems. This coupled with change management and user training and mentoring practices will also increase the adoption rate among users.

### Redundancy

Communication can be sent out over multiple bearers. This means that:

- the most appropriate bearer for a message can be seamlessly selected,
- a message can be sent out over multiple bearers at the same time, to increase the chance it gets through.

All this is invisible to the user - they don’t need to manually select what network to use. They just communicate on their device. No changes to Standard Operating Procedures (SOPs) are required.

### Agency Interoperability

Unified solutions can be used by Public Safety agencies and critical infrastructure companies during emergencies. Interoperability enhances productivity, as critical information, tools and resources are readily accessible to all authorized users. Secured standards-based IP systems allow users to use a range of devices from mission-critical, highly rugged devices through to off-the-shelf smart phones running the latest O/S.

**Greater choice of vendors**

Standards-based platforms allow a range of vendor applications to be utilized. Open API approaches make it simple for vendors and agencies to quickly create value from the network data flows.

**Lower cost**

Unifying communications can include multiple providers of the same type of network. For instance, an agency can utilize different public 3G networks. A least-cost routing algorithm optimizes choice while maintaining mission critical safety.

**Better coverage**

The use of multiple networks extends the range of communications coverage for agencies. A mix of public and private systems can give significant improvements in coverage and the unified critical communications approach ensures that these are used optimally for mission-critical response.

***"…this is invisible to the user - they don't need to manually select what network to use. They just communicate on their device. No changes to Standard Operating Procedures (SOPs) are required."***

## CONCLUSION

The communications network options for Public Safety agencies have different characteristics and choosing between them can be confusing. The key to realizing the combined strengths of each network is a unified critical communications approach. This ensures seamless handling of bearer choices and greatly improves the efficiency of the over-all system.

The outcome is a solid communications solution that allows future proofed growth but can respond economically to dynamic changes, without compromising key mission critical objectives. You can maintain your choice of vendors for elements of the network and change your mind as you need to.