White Paper

Public Safety Communications Innovations: Advancing Interoperability in the Era of Transformation

Sponsored by: Verizon

Alison Brooks, Ph.D. Denise Lund
July 2021

EXECUTIVE SUMMARY

Despite some misinformation circulating in the marketplace, public safety agencies have choices when it comes to selecting communications and networking vendors. Public safety communications that are designed to be open and interoperable, using proven technology, help ensure that critical information is available when and where needed. Optimal public safety communications need to function as an interoperable system, with best-in-class network design, coverage, reliability, priority, and preemption — this means a secure, robust, and technology-agnostic approach to network, device, and application interoperability. To that end, the following five key criteria can guide agency communications' decision making when choosing a network:

- **Open and interoperable solutions.** Open and interoperable solutions provide for seamless continuity of communications, regardless of network, device, application, platform, or solution. Public safety agencies can leverage existing information technology (IT) investments with these solutions. In addition, agencies will have the confidence that critical communications including IP voice, video, data, and public safety apps will be available across networks with these solutions.
- **Innovation.** Network technology innovations that, for example, enable dispatch connections or enhance real-time situational awareness with access to maps, data, and integrated communications and information sharing with community partners, are game changers for public safety agencies. Look for solutions that leverage innovative, agile, and secure future-looking technology, with capabilities that provide for expansion, flexibility, redundancy, and scalability. Practically speaking, with these technological innovations, public safety agencies may be able to work unimpeded by communications mishaps with best-in-class, secure communications that meet priority needs.
- **Network coverage and reliability.** The importance of network coverage and reliability cannot be overstated. As network technology becomes increasingly important to, and embedded in, daily operations, network coverage will continue to rise in importance with the emergence of new technologies underpinned by IoT. Increasing adoption of fifth-generation network technology (5G) will have dramatic implications for public safety agencies in terms of coverage, capacity, and capabilities. Network coverage and reliability provide critical information assurance in crisis situations.

- **Pervasive security.** Public safety agencies can leverage next-generation network technology today to protect critical data, such as videos from crisis scenes and other contextual information, regardless of the mobile device type or network used by the recipient. Security and flexibility in the management of apps and data guarantee the right information will be received where and when needed.
- **Proven technology.** Public agencies should seek out communications providers with a proven track record of highly reliable services. Providers also should have a demonstrated commitment to helping solve the critical interoperability communications needs of the public safety market.

THE IMPORTANCE OF INTEROPERABILITY AND COMMUNICATIONS CONTINUITY FOR PUBLIC SAFETY

Historical Communication Challenges

Emergency and disaster response requires a coalition of forces that often must converge on an area to react, rescue, and recover. System incompatibility, aging technology, lack of planning and collaboration, limited radio spectrum, and lack of device interoperability historically have been factors in communication failure and compromised response.

For example, during the 9/11 terrorist attack, siloed, disconnected, and proprietary communications systems were unable to reliably connect emergency responders and maintain situational awareness. Hurricane Katrina highlighted the challenges inherent in lacking communications infrastructure — a situation that led to an increased loss of life. During the Boston Marathon bombings, first responders struggled to communicate with public safety officials because they lacked priority and preemptive access to the communications network when it became overwhelmed with traffic from the general public.

Each of these incidents underscores the importance of interoperability and continuity of communications for the public safety community. Communications continuity — the ability of emergency responders to maintain communications in the event of damage to, or destruction of, the primary communications infrastructure — is critical for both *lead agencies*, spanning federal, state, local, and national security agencies, and *supporting agencies* involved in an incident such as hospitals, critical infrastructure providers, other community security partners, and humanitarian agencies like the Red Cross.

Today, the increasing frequency, impact, and complexity of man-made and natural disasters make the continuity and interoperability of public safety communications more important than ever.

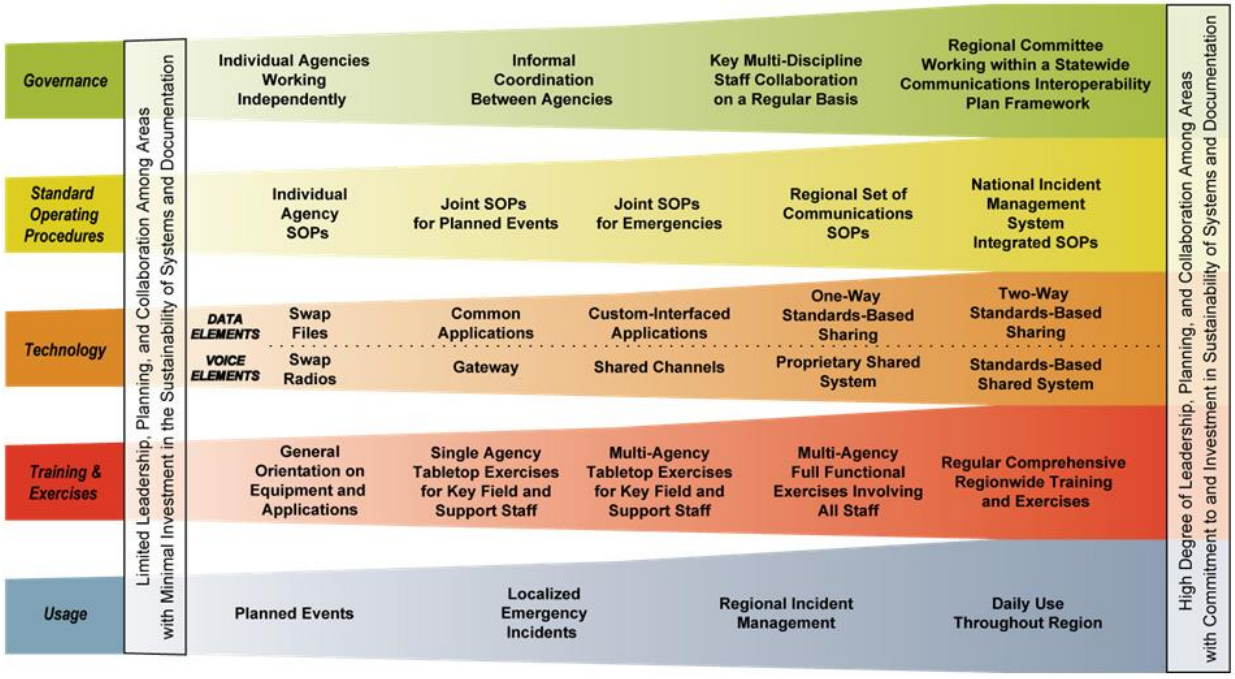
Interoperability: The What, Why, and How

What Is Interoperability?

In the context of public safety, interoperability is defined as the ability to exchange voice and data on demand, in real time, when needed, and as authorized without regard to network or device. In response to some of the communication challenges noted previously, the U.S. Department of Homeland Security (DHS), working with public safety stakeholders spanning North America, created the SAFECOM Interoperability Continuum, a five-pillar benchmark to help agencies establish interoperability within their organization and between adjacent stakeholders (see Figure 1).

FIGURE 1

SAFECOM Interoperability Continuum



Source: Department of Homeland Security, 2018

As illustrated in Figure 1, the technology pillar sits in the center of the continuum – a testament to its foundational significance.

The SAFECOM Interoperability Continuum's technology pillar seeks to move vendor solutions away from proprietary, walled-off, and disconnected solutions by encouraging open, standards-based information technology adoption. In particular, network scalability, capacity, and coverage issues have come into focus in recent years as the communications infrastructure has broken down or disappeared in times of greatest need, specifically because of shortcomings in technology interoperability.

The SAFECOM framework distinguishes between data and voice elements and identifies technology properties that fit into each stream on the continuum. Putting network capabilities in the cloud, manageable through software, is a clear way to address interoperability challenges today and as needs evolve into the future. Virtualization and software-defined networks (SDNs) facilitate priority routing between carrier networks.

Technological advances in the utilization of video, the proliferation of smartphones, and data communications raise questions about technology interoperability. The global proliferation of new, rich data sources – in particular the exponential growth in IoT and video sources (body-worn video, CCTV, in-car camera, citizen video, drone, etc.) – has refocused much of the discussion on interoperable solutions that allow public safety stakeholders to leverage digital assets and solutions.

Growth and variety in the types of devices further complicate the ability to communicate effectively. Today's devices include smartphones, wearables (panic buttons), radios, and video cameras with live streaming capabilities. Stated plainly, first responders using land mobile radios should have the ability to communicate with other first responders communicating via smartphones. Video from a camera, or data generated by a wearable sensor, should be visible in real time to all that need to know – first responders on their smartphones, the command post's dispatch console, and a big data system for deeper analysis.

Innovations in public safety–specific apps and services must also be interoperable. First responders and public safety stakeholders who have apps and services and the data that underpins them available on one network, but not on another, perpetuate interoperability issues and consequently diminish the overall effectiveness of technology solutions. An examination of fire services provides an excellent example of why this is important. Fire services respond to incidents by drawing resources from many different stations across broad geographies and jurisdictions and by accessing numerous telecommunications providers. Emergency responders need to leverage advanced tools on any network to coordinate their response with each other and other responders.

Why Is Interoperability Important?

Benefits and Opportunities

Interoperability enhances situational awareness; facilitates collaboration across an increasingly complex stakeholder ecosystem; enables faster, more effective response; allows agencies to leverage their existing IT investments; lays the groundwork for numerous additional efficiencies; and most importantly, can help save lives. Interoperable communications technology is critical for delivering intelligence in real time or near real time, and network capabilities and innovations like 5G will be pivotal for ensuring the real-time transfer of data and insights in an increasingly IoT-enabled environment. The following addresses each of these benefits in greater detail:

- **Enhanced situational awareness.** The ability of a first responder to know and understand the dynamics of the immediate environment, and how it will change over time, is critical. Technological interoperability enhances situational awareness by bringing information to public safety stakeholders that is more granular, timely, and rich and ultimately more actionable if that information is received when and where needed.
- **Better ecosystem collaboration.** Open, standards-based interoperable systems facilitate collaboration across a wide variety of public safety stakeholders as well as the wide variety of devices, applications, and networks they use.
- **Faster response times.** Interoperable solutions and network technology innovations can provide the public safety ecosystem with faster response times by leveraging common standards, and a common internet protocol, creating a common network that quickly integrates and unifies disparate data sources.
- **Ability to leverage existing IT investments.** Interoperable solutions help agencies harness online and mobile solutions, user interfaces, and back-end systems. Agencies can leverage their existing IT investments, and common, interoperable public safety communication networks allow public safety agencies to get away from hardware-intensive, purpose-built, or vendor-locked solutions. Investments on the back end allow agencies to choose what they want to purchase and connect whatever device, application, or endpoints are required.
- **Helping save lives.** The most important benefit of interoperability is increased human safety for both first responders and the citizens they serve.

How Is Interoperability Achieved?

To achieve interoperability in public safety communications, the application containing the critical information — whether it is video content from devices (including wearables) at the scene, location data, or other contextual or critical information — must be securely and successfully sent to members of the public safety ecosystem irrespective of the network, device type, or end-user applications used by an agency. Successful interoperability requires network availability as well as the use of standard, open technology design and collaboration between vendors in the ecosystem.

The key enablers of interoperability and continuity of communication are summarized in the sections that follow.

Availability, Coverage, and Redundancy

First and foremost, communications networks need to be available and redundant. Communications redundancy is achieved by ensuring that the information can travel along multiple routes. The PACE methodology, which stands for Primary, Alternative, Contingency, and Emergency communications, establishes the best four communications options in times of crises. For example, if an agency loses its primary connection (the best and intended method of communications), it can turn to the alternative (a common but less optimal communications avenue), then to the contingency method (capable of connecting but slower, more complicated, or more expensive), and finally, to its emergency communications infrastructure, which is a method of last resort as it has significant delays, costs, and negative impacts.

Networks built with redundant connections across geographies — with switchovers available in cases of a specific location's network challenges — serve as the foundation for interoperable communications. Deployables that serve as temporary cell sites must also be available to move into emergency locations.

Why It Matters

Rapidly enhancing communications coverage in remote locations in a crisis and in locations that are experiencing rapidly degrading communications bandwidth on the network helps ensure that crisis response is minimally delayed or not delayed. Without a reliable network connection from the site of an emergency, prioritized information sharing out to the field is simply not possible.

Priority and Preemption

Federal, state, and local government entities responsible for emergency response command and control can take advantage of the DHS Office of Emergency Communications' Wireless Priority Service (WPS) designation, which ensures basic voice and message communications are sent with priority designation across networks in an emergency. WPS requires agency and device preapproval on a preapproved network provider. With ongoing technology developments, however, interoperability is only optimized when all mission-critical apps are designated as having priority and the designation can be carried across networks. Supplementing WPS-designated communications with open, software-driven, and priority designations applied to the balance of mission-critical apps, such as push-to-talk (PTT) and the growing list of first responder apps and wearable-generated rich media, is critical.

Virtualized networks can help maintain priority and preemption capabilities. With the ability to program through open software standards and API integrations, it is easier to assign and transfer priority and preemption designations, regardless of the content and data applications.

Why It Matters

Priority and preemption need to travel from one network to another and, most importantly, need to apply to all critical information and not be limited to just voice or text communications. The types of communications and rich media that the public safety ecosystem relies on in a crisis are ever expanding. Since WPS does not apply to this growing list of apps and rich media, public safety agencies must incorporate an open, standards-based approach that network operators agree on for the additional, mutually beneficial information to be sent with priority. Without the incorporation of this approach alongside of the WPS program, public safety agencies risk not having key information from the live emergency situation in their hands when making decisions about next steps for rescue and recovery.

Private Core

Dedicated network resources that establish trusted internet connections, the quality of service appropriate in emergencies, and communications that are isolated from noncritical communications on the network are essential to interoperability.

While both physical and virtualized private core options can be sectioned off to commit bandwidth to public safety, virtualized networks can assign customizations, security, prioritization, and continuity guarantees through the ease of software integrations and definitions that can be difficult to implement with strictly hardware-based networks.

Why It Matters

Public safety communications rely on the ability to share information in a multiagency ecosystem. In particular, the number, types, and volume of rich media data sources (i.e., video) continue to grow in the emergency response realm. Consequently, the ability of a software-based network to segment types of data and applications to run over designated network resources reserved for public safety is beneficial.

Scalability, Expansion, and Flexibility

The ability to scale up network bandwidth to handle changing public safety needs is critical in incidents involving adjacent geographies, jurisdictions, and agencies.

With core network radio access and broadband functions increasingly residing as virtualized network capabilities in the cloud, communications capacity can be scaled up and down by the network provider. Because the controls are software based, the carrier can easily access them according to public safety agency protocol. The controls are then defined, designed, and managed accordingly.

Why It Matters

For the most part, public safety communication needs are unpredictable; they arise suddenly and vary in terms of bandwidth needs on a case-by-case basis. Moreover, during times of crisis, public safety communications are expected to increasingly incorporate the IoT devices that enable automatic collection and dissemination of conditions at the emergency site. To send and receive such rich media and timely information, networks will have to easily scale.

TECHNOLOGY EVOLUTION AND INNOVATION

Emergencies will continue to be a fact of life, and public safety agencies must respond effectively. Fortunately, technology innovations within the communications market provide public safety with new capabilities and opportunities to address communication challenges that would not have been addressable using older technology. Network providers have recently implemented technologies in the network (i.e., 5G) and through partnership with application and deployables specialists that are changing the public safety communications network environment, bringing true innovation to the field. Further:

- **5G deployments.** 5G wireless communications with low latency, high bandwidth, ultrafast speeds, and reliability now offer critical services for voice, video, and data that exceed 4G capabilities. 5G is part of the network of the future that mobile carriers and the application ecosystem can leverage to achieve varied IoT use cases that arise in the context of public safety agencies and first responder networks. Early 5G opportunities include video-based solutions (i.e., real-time body-worn video camera monitoring), real-time applications (i.e., location-based services), or mission-critical solutions (i.e., remote control and connectivity for unmanned aerial vehicles – drones). 5G operates as an intelligent edge network, and this fosters the development of applications of the future, enhancing capabilities using augmented reality, holographic video, robotics, computer vision, and so forth.
- **App innovations.** As innovations in networking technology dramatically change public safety communications, workflow, and capabilities, there are ancillary market innovations in the public safety-specific apps and services that sit on top of the networks. A recent example of this is the Department of Homeland Security's Enhanced Dynamic Geo-Social Environment (EDGE), a virtual collaborative training environment for federal, state, local, and tribal first responders that allows agencies to practice coordinated response for a number of common scenarios (**https://www.dhs.gov/science-and-technology/EDGE**).

Innovations in IoT, data transfer, and very low-latency speeds will invariably give rise to next-generation, real-time apps and solutions that become critical tools for responders. The partner ecosystem that is driving the creation of apps for public safety stakeholders will rise in importance. It will become crucial that the ecosystem developing mission-critical apps and solutions use open architectures and APIs industrywide.

Furthermore, competition in the ecosystem will create the right circumstances for innovation, choice, and cost-effectiveness for the end user.

The Rising Importance of Video

Video is becoming an indispensable tool for situational awareness, but as the number and types of video sources grow exponentially, it is becoming difficult to manage the transfer, viewing, analysis, and distribution of video in a timely, actionable manner. This has led to considerable innovation in secure platforms that allow first responders to connect to and share video sources in real time. One vendor, Mutualink, provides interoperable critical communications solutions that allow first responders and related entities to securely connect their organization's networks to communicate and share real-time video, real-time voice, and critical information. The company's interoperability solutions are compatible with virtually any device and network, based on a software-centric model that removes hardware dependencies, allowing connections between smartphones, video cameras, and land mobile radios (LMRs).

Deployables

"Deployables" refer to mobile emergency communications capabilities that can be wheeled, flown, or carried into an incident to provide public safety agencies with reliable voice and data communications where cellular network connectivity is unavailable. These assets provide critical capabilities including voice communications between responding entities, location-based services, mission-critical push to talk, situational awareness, and the receipt and exchange of video feeds.

Deployables range in size and capacity from large mobile units and trailers to communications units that can be carried in backpacks or positioned in drones. In general, the larger systems deliver better capacity, while the smaller systems are useful given their portability. Deployables deliver real-time connectivity and data transfer, regardless of the agency or application involved, and they have proven invaluable in recent natural disasters like Hurricane Michael.

KEY TAKEAWAYS TO GUIDE BUYING DECISIONS

Wireless carriers' investments in their software-based agile network design have never been more aligned with the needs of public safety agencies in terms of communications priority, reliability, availability, and coverage. As public safety agencies and first responders look to the future of crisis response, they envision innovative solutions enriching communication via enhanced abilities at information collection, management, analysis, and dissemination. In this vein, wireless carriers' vision of 4G LTE and 5G networks will resonate with the public safety market in the future. Management of voice and data communications availability and coverage is naturally going to expand to include connectivity with devices at the network edge. Wireless carriers are investing in virtualization and SDN designs that will make usage of 5G network possible, and for public safety agencies and first responders, this makes IoT on high-speed networks an attractive and realistic vision of the future of crisis management.

There is considerable confusion in the marketplace regarding public safety communications options. As public safety agencies throughout the country make critical spending decisions about their network providers, the following key considerations should factor heavily into decision making:

- **Open and interoperable solutions.** Public agencies need seamless continuity of communications, regardless of the networks, devices, or applications they use. With open and interoperable solutions, critical communications will be available even as public safety agencies can leverage their existing IT investments.
- **Innovation.** Network technology innovations are truly game changers for public safety agencies. Virtualization and software-defined networks are among the agile technologies that enable public safety agencies to work without the disruption caused by communications mishaps. Secure and future-looking technology also ensures that public safety agencies have best-in-class, prioritized communications.
- **Network coverage and reliability.** There is nothing more important to the daily operations of public safety agencies than network technology. As IoT, 5G, and other emerging technologies become pervasive, network coverage and reliability are the key criteria to ensure that critical information is shared in crisis situations.
- **Pervasive security.** Videos from crisis scenes and other contextual information must be handled by the network securely. No matter which type of mobile device or network is in use, pervasive security guarantees that the right information will be received anywhere and at any time.

Since the original publication of this white paper, there has been further, industrywide recognition of the benefits delivered by interoperability across networks, devices, applications, platforms, and solutions. For example, iCert (an industry consortium of public safety technology vendors) is seeking to create a shared understanding of how the ecosystem's technology products need to work collectively to buoy the public safety industry. Specifically, it is seeking to catalyze the implementation of next-generation 911 by establishing interoperability across the technology stack. Further, with 5G offering much greater density and lower latency in communications, this could enable greater interoperability across far larger device, sensor, and data volumes.

More broadly speaking, the interoperability imperative is being buoyed by its critical role in emerging technologies such as blockchain and its pivotal role in the healthcare industry. In healthcare, it is recognized that silos of clinical, administrative, payer, pharmacy, provider, inpatient, and outpatient data as well as physical, mental, and substance abuse data sit unacceptably isolated. Interoperability has matured rapidly recently in healthcare, in part because of technological advances in networking, cloud platform adoption, and government mandates to integrate data silos.

The public safety communications imperative is not going away. With emergencies a fact of life, public safety agencies need more efficient communications that facilitate information sharing, prioritized traffic, and timely and reliable delivery of critical data. Today's communications carriers have responded with innovative, software-defined technologies designed to enhance interoperability, security, and flexibility. More than ever, public safety agencies have choices when selecting systems and vendors that meet their needs. Public safety agencies would do well to seek out those communications and networking vendors that have a proven track record of providing highly reliable services and a demonstrated commitment to ongoing innovation.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com