Comments on the Australian Government Productivity Commission's Approach to Public Safety Mobile Broadband for PSA's

Date 28th October, 2015

Presented by:

Push2Talk
PO Box 110
Balgowlah 2093
1300 789 955
www.push2talk.com.au

Lee Shardlow

1. Executive Summary

The purpose of this document is to submit comments regarding the inclusion of cross-agency interoperability and collaboration as a fundamental capability of a Public Safety Mobile Broadband Network (PSMB).

A summary of the major points made in this document regarding this capability are:

1. The public *expects* and First Responders *need* a PSMB network to provide this capability.
2. This need goes beyond just voice/LMR/MCPTT interoperability – this cross agency need is also present for video sharing, text messaging, location sharing, and file/data sharing.
3. Agencies must be able to share their existing communication and data systems without requiring the buildout of new expensive systems.
4. Agencies must be able to interoperate without giving up control of their systems, i.e. maintain their sovereignty. Agencies will be less willing to participate in this PSMB - provided capability if it requires them to cede control of their systems.
5. This capability must be available even in disconnected operations and during regional disasters/outages.
6. This capability must be able to interoperate with non-PSMB agencies as well since incidents do not respect network boundaries. This capability should seamlessly bridge communications within agencies and between agencies regardless of whether those agencies are operating on the PSMB network or any other network.
7. Mutualink has developed and fielded a proven solution that meets all of these requirements. This system is operational worldwide including several American FirstNet Band14 BTOP deployments.

2. Introduction

Today, work is well underway on determining both the PSMB capabilities and a model for financial self-sustainability of the network. However, there does exist a substantial gap between the public's expectations of what a PSMB network will accomplish if and when it's rolled out and what might be currently being planned as deliverables. The public, as represented by the Australian Federal Government believes that a PSMB network is the antidote for the issue of first responder mission critical communications and interoperability. The Government believe that when first responders show up at an incident scene they should be able to communicate with disparate groups and have access to any additional data that would assist in resolving an issue. According to the Productivity Commissions Draft Report radio networks will be the predominate on-scene, mission-critical voice communication for the foreseeable future. This disconnect between the public's expectation of what the PSMB network will deliver into the foreseeable future will likely result in a disappointed and frustrated public, particularly with the billions of dollars being allocated to the network.

However, perhaps the reason that an expectation gap exists is because of the definition of interoperability that is being put forward by the Productivity Commissions Draft Documents:

1. *The ability for the capability to:*
   a. *be nationally interoperable, within and across agencies and jurisdictions*
   b. *operate in both metropolitan and regional Australia*
   c. *integrate voice communications that are traditionally carried on narrowband networks*
   d. *maintain integrity and security of communications*
   e. *ensure accessibility, priority and sufficient capacity for PSAs, particularly during periods of peak demand and during a localised incident*
   f. *be resilient and maintain continuity of service including under adverse operating circumstances*
   g. *consider the sustainability of arrangements in the context of rapidly changing technology and increased demand, including convergence of voice and data services*
   h. *be cost-effective, in terms of both capital and operating cost*
   i. *be nationally available by or before 2020, and*
   j. *be compatible with a variety of end-user devices*.

So, how do we fill the gap between public expectations and the current state of the proposed deliverable? Perhaps by slightly modifying the definition of interoperability that a PSMB network is trying to achieve in order to meet the public's expectation and easily close the gap.

Let's start by looking at some additional definitions of interoperability that are relevant to a PSMB network.

There exist many definitions of interoperability, but here are three relevant ones:

1. Network Interoperability, Regionalized networks communicate and allow for the flow of communications traffic among them through a centralized or regionalized core(s).
2. Device Interoperability, an enabled device (radio, smartphone, tablet PC, video surveillance systems) that works in one part of the country will work in other parts of the country.
3. Agency interoperability, Agencies can share multimedia enabled communications with other agencies both in and out of region and within LTE and on other wired and wireless networks such as existing mission critical radio networks and accessing other media types not provisioned on LTE networks (e.g. video enabled on terrestrial IP).

As we move forward the future of the PSMB network appears to be focused solely on how to deliver a PSMB network in the most cost efficient way. But will these decisions meet the public expectation of the PSMB network by facilitating interoperable communications among agencies on LTE and other networks inside and outside their regions.

If the PSMB network solution is to deliver agency interoperability, and not just device and network interoperability, then will it meet the core of public expectations?

If, for a moment, we contemplate the complexity of actually achieving broad-based, multimedia, national, agency interoperability that the public expects, shouldn't this capability be core to the architecture? How will an LTE device communicate with an LMR device within an agency? And still more complicated, how exactly will LTE users from different agencies communicate? What if those agencies also are using LMR? Simply placing devices within agencies on the same xxx MHz broadband network will not achieve agency interoperability. Look at all of the agencies on P25 systems that can't communicate, and this is only voice, what about video, data and telephony interoperability?

Furthermore if we uses definition of interoperability in the draft documents then the PSMB network could easily become a silo unto itself and do little to achieve the national policy goals; how will all of these complex inter-agency communications occur?

The government's goal of delivering a PSMB network may be slightly off the mark. Perhaps a goal of having first responders *actually adopting* a broadband network would get us closer to the desired end. First responders will not be compelled (forced) to join the network**;** the network must be competitive from all market perspectives including price and usability and capabilities.

However another critical attribute that must be present is trust. Will first responders trust the model chosen by government and the organization tasked with running such a network, not only from a reliability and resiliency perspective, but also from a sovereignty and security perspective? The complexities that emerge from a single silo security model and the credentialing and access that go along with that has yet to be successfully accomplished in the scale that would be necessary for an interoperable national broadband network deployment. An alternative multi-domain security scenario could greatly simplify cross agency credentialing with individual agencies only being credentialed for their resources. Agencies could then "push" those resources across the network to other agencies to accept versus the more cumbersome and burdensome pull model traditionally attempted.

There is a compelling argument for the existence of a gap between the public's expectation and PSMB network planned (as described in the draft documents and other publically available sources) capabilities.

Next we will provide some proven and elegant solutions to those gaps.

3. Silos and Security Domains

3.1 The Interoperability Problem

Every agency has private communications systems, data systems, etc. These systems are administered within the agency for security purposes, i.e. limiting access to internal personnel. In addition, these systems are necessarily isolated from similar systems in other agencies due to the very real need for securely controlling access to the systems and the data within. These isolated systems are called silos in some contexts.

Although silos are necessary constructs for maintaining agency sovereignty and control, they have a significant disadvantage when multiple agencies need to work together at incidents or events. This mutual response requires agencies to share information and communications to be effective in working together. It is in these situations where silos present an obstacle to the required collaboration.

Therefore this split personality of silos reduces to:

- Silos = Security Domains = Good for security.
- Silos = Communication Islands = Bad for interoperability.

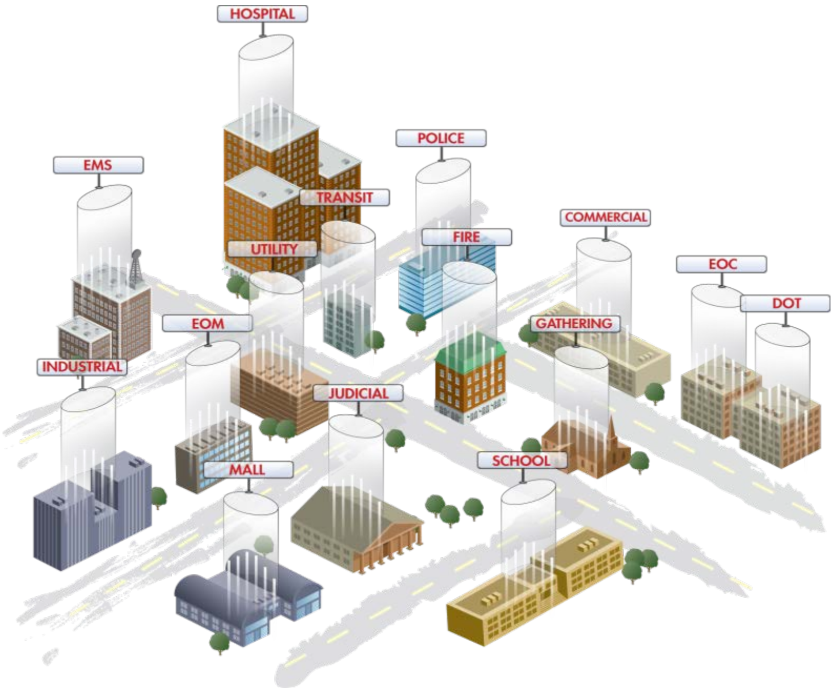


Figure 1 – Silos throughout a community

3.2 So Build a Bigger Silo?

Faced with the problem of such siloed systems needing to seamlessly interoperate, a common response is to build a bigger silo, hoping to eliminate the silo problem entirely. However, the problems with this approach are:

1. All silos have boundaries. Bigger silos may reduce the number of boundaries, but they do not eliminate the fundamental problem.
2. Silos are not all-encompassing. Even within a silo footprint, only certain agencies are included.
3. Once a silo transcends agency boundaries, agencies give up control of their resources to the silo owner.
4. Silos are expensive to build!

3.3 Goals for Ideal Solution

So if the answer is not to build a bigger silo, what then are some attributes of the ideal solution?

1. Recognize that silos will always exist, so don't fight against them – work with them.
2. Silos are not only LMR or voice - video, GIS, and data systems have the same problem, so need a media-agnostic solution.
3. Enable "selective" information flow between silos.
4. Ensure security with access control and encryption.
5. Maintain sovereignty of owning agencies.
6. Enable ad-hoc sharing under control of on-scene agency personnel.

3.4 A Distributed Approach to Bridging Silos

Given the above goals, one solution is to selectively and securely bridge existing silos together, as depicted in the following diagram.

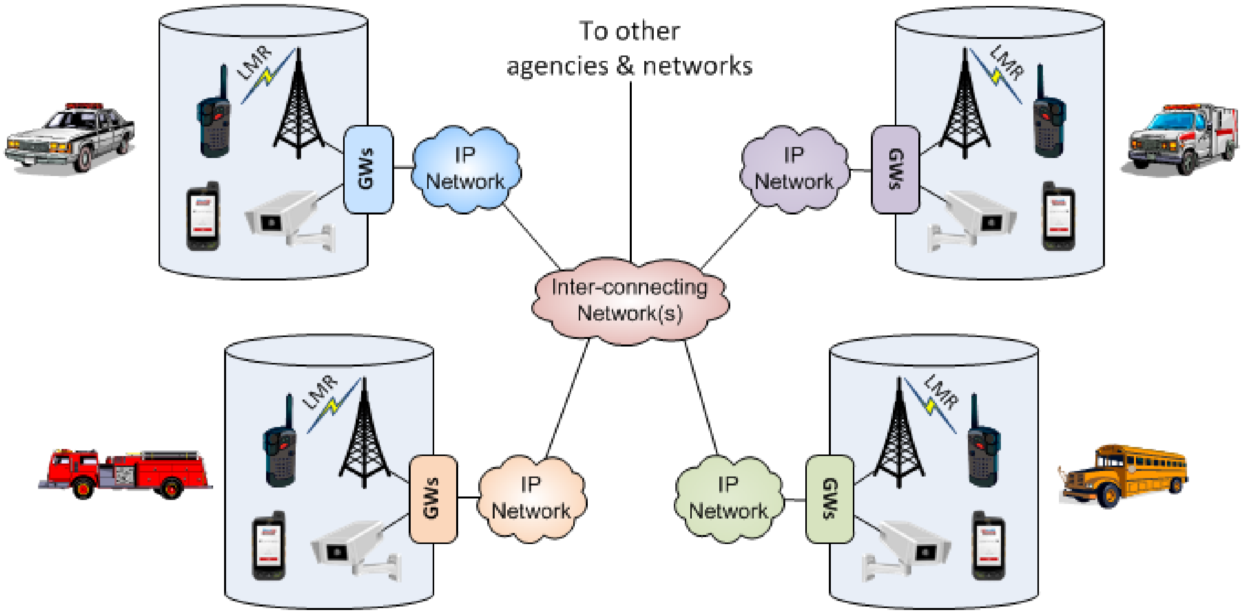


Figure 2 - Bridging Silos

Important aspects of this solution:

1. In each silo, gateways ("GWs") are connected to the communication and data systems that the owning agency wishes to share with other agencies. Types of gateways can include LMR, voice/telephony, video, GIS, and generic data gateways.
2. These gateways are then connected to one or more IP networks that allow the gateways to communicate with each other (either directly or through proxies).
3. The gateways may be controlled by authorized users whether they are within the owning silo or remote within the inter-connecting networks. These users direct what information from the gatewayed systems should be shared to which other gateways and users.
4. This is a distributed system in which the gateways may communicate directly with each other. No central servers or switches are required to enable this interoperability; such central control points would introduce undesired third-party control and therefore loss of sovereignty by the various agencies.

3.5 Recommendations

It is recommended that any PSMB network include a distributed silo bridging capability to enable cross-agency interoperability while maintaining the sovereignty of each agency.

4. Cross-Agency Sharing Models

4.1 Centralized Security Model

The PSMB network would have a specified a centralized enterprise architecture security model including a federated ICAM (Identity, Credential, & Access Management) system. This is appropriate for resources meant to be perpetually shared between many agencies (e.g. AFP data).

However, for agencies to share their private communication and data systems with other agencies to enable interoperability, this implies that they would need to connect those potentially sensitive systems to the PSMB network centralized security infrastructure. This would mean a loss of sovereignty by those agencies and most likely a significantly lowered (or absent) willingness to interoperate those systems on the PSMB.

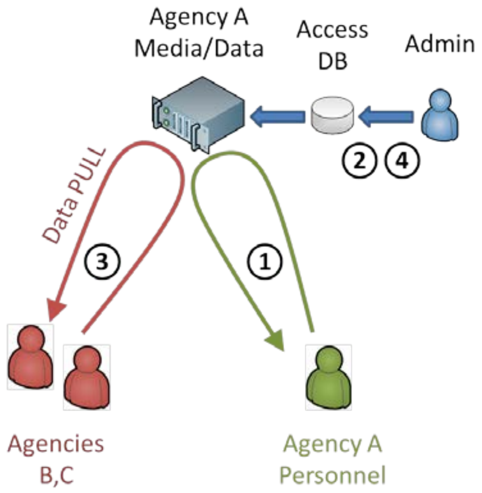
The sections below describe two different types of cross-agency sharing models.

4.2 The Centralized PULL Sharing Model

This model uses an access control database to control who can access particular communication systems and data systems within an agency. If someone from another agency requires access to a system, the access control database must be modified to allow this access so that they can directly access the system.

A sample workflow for sharing using the PULL model:

1. Agency A is accessing private media/data. They wish to share this with on-scene agencies B,C.
2. The agency admin adds the desired agency B,C members to the access control DB for the desired data.
3. The agency B,C members may then access (PULL) the data directly from the source system. This assumes a secured connection to the data is available and they have the appropriate application(s) installed.
4. When the sharing is no longer required, the admin must remove the members from the database.



Although this model is perfectly appropriate for a single security domain utilizing an enterprise security architecture, it has significant drawbacks when used for cross-agency sharing.

a. Other agencies now have direct access to private and potentially sensitive communication and data systems. Although access controls can generally determine which types of data these members may access, the appropriate level of granular access control is frequently provisioned incorrectly especially in times of urgent need.

b. It requires an administrator to re-provision the access database to grant access. This introduces an additional delay when seconds could count. Furthermore, an appropriate administrator may not be available when needed.

c. To access the private systems, other agencies would first need connectivity to those systems, presumably through a VPN to that agency. Additionally, if specific applications are required to access the private system, other agencies would need to have those applications installed.

d. For on-scene systems, someone with appropriate administrative training must be present to modify the access control database as needed.

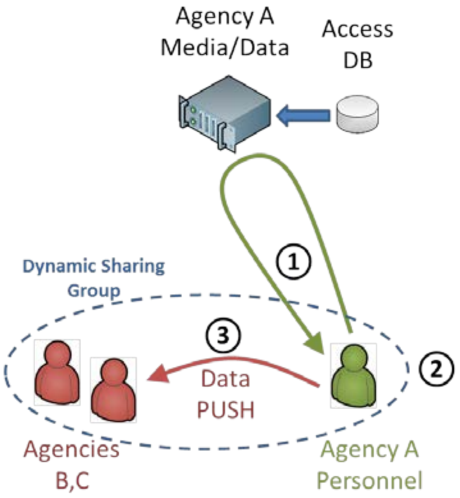
4.3 The Dynamic PUSH Sharing Model

This model uses a fundamentally different paradigm than the PULL model. The primary assertion of this model is that an agency member with access to private agency systems should be enabled to share selective information directly with other agencies as needed. In this way, agency members effectively act as “sharing gateways” to information or media from their private systems.

A sample workflow for sharing using the PUSH model:

1. Agency A is accessing private media/data. They wish to share this with other on-scene agencies B,C.
2. Agency A creates a Dynamic Sharing Group with the desired agencies B,C.
3. Agency A then shares (PUSHes) the desired media/data to agencies B,C.
4. When the sharing is no longer required, Agency A simply removes the media/data from the Dynamic Sharing Group.

Note that in this model, agencies B,C never have direct access to the data source, therefore agency A remains in complete control of their data at all times.



To fully meet the cross-agency sharing needs of first responders, these Dynamic Sharing Groups should have the following attributes:

a. Anyone can create a group and invite others into the group; others then accept or reject that invitation. No central administrative actions are required.

b. Groups can span multiple local and remote networks.

c. Groups can be ad-hoc (created on-demand) or long-term (exist until all members leave).

d. Groups do not require specific infrastructure to be present, i.e. the capability exists even in disconnected modes.

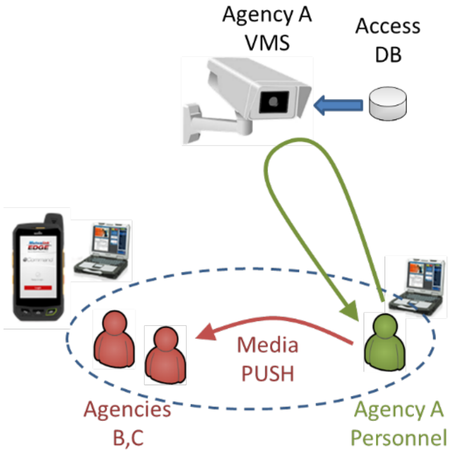
e. Each member can push any form of media/data to the group, each member then decides which media/data they wish to consume.

f. All media/data is end-to-end encrypted.

4.3.1 PUSH Model Examples

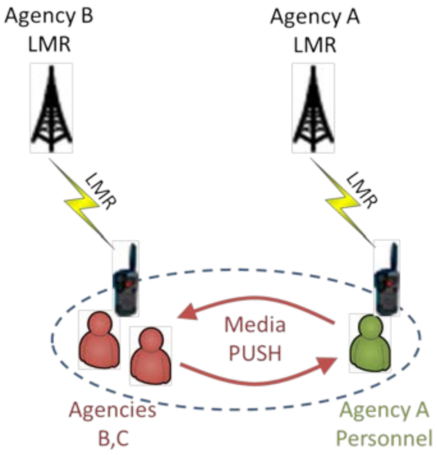
Shown here is an example of the PUSH model applied to a Video Management System (VMS). Since video feeds can be potentially sensitive information, it may not be desirable to give other agencies direct access to the VMS.

In this example, a member of Agency A determines which video feed(s) need to be shared with other agencies and pushes just those feeds to the appropriate agencies.



Shown here is an example of the PUSH model applied to LMR systems. In this example, multiple agencies are sharing their LMR systems to each other in the same Dynamic Sharing Group so this effectively creates a talk group patch.

In this example, the members of each agency determine which talk group needs to be shared with (patched to) other agencies and shares that talk group to the group.



4.4 Recommendations

It is recommended that the PSMB include a Dynamic Sharing Group capability to enable cross-agency interoperability while maintaining the sovereignty of each agency.

5. Network Connectivity Considerations

Given that multi-agency interoperability and collaboration are critical functions for first responders, it follows that this capability should ideally be available in all situations regardless of the wide-area network connectivity present.

5.1 Availability Goals

Goals for the availability of multi-agency interoperability in various network conditions include:

1. The capability should be available at incident scenes with little or no wide-area network connectivity.
    a. The capability should be included in MCUs and LTE deployables.
    b. The capability may be included in tactical kits brought to the scene by various agencies.
    c. If the capability is present in multiple components (e.g. tactical kits, MCUs, deployables) at an incident scene, the components should be able to seamlessly interoperate to provide an all-compassing capability across all components.
    d. The capability should be made available to devices that connect to on scene equipment using a wired network, WiFi, or LTE.

2. As wide-area connectivity becomes available, the on-scene capability should expand to make any newly-connected agencies available for interoperability as well.
3. The capability should be available to all agencies connected to the PSMB network.
4. The capability should also span agencies connected to networks other than the PSMB network such as commercial LTE, Public Safety Enterprise Networks (PSENs), and the Internet.
5. In cases of widespread network outages due to natural disasters, etc., the capability should have regional and/or local fallback if the PSMB network data centers are not reachable.

5.2 On-Scene Interoperability

The following diagram shows an example of how on-scene interoperability could be achieved to meet the above goals.

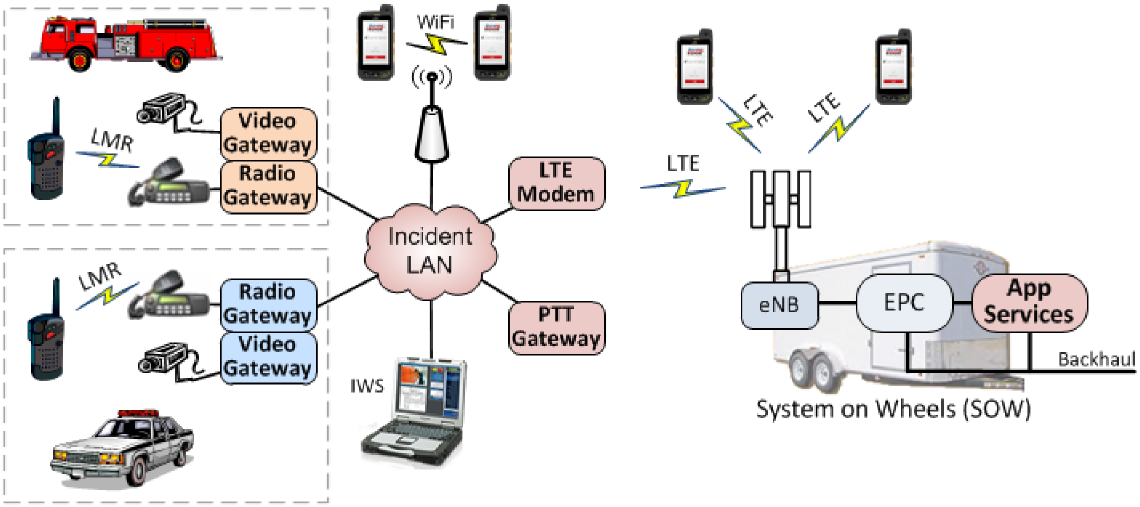
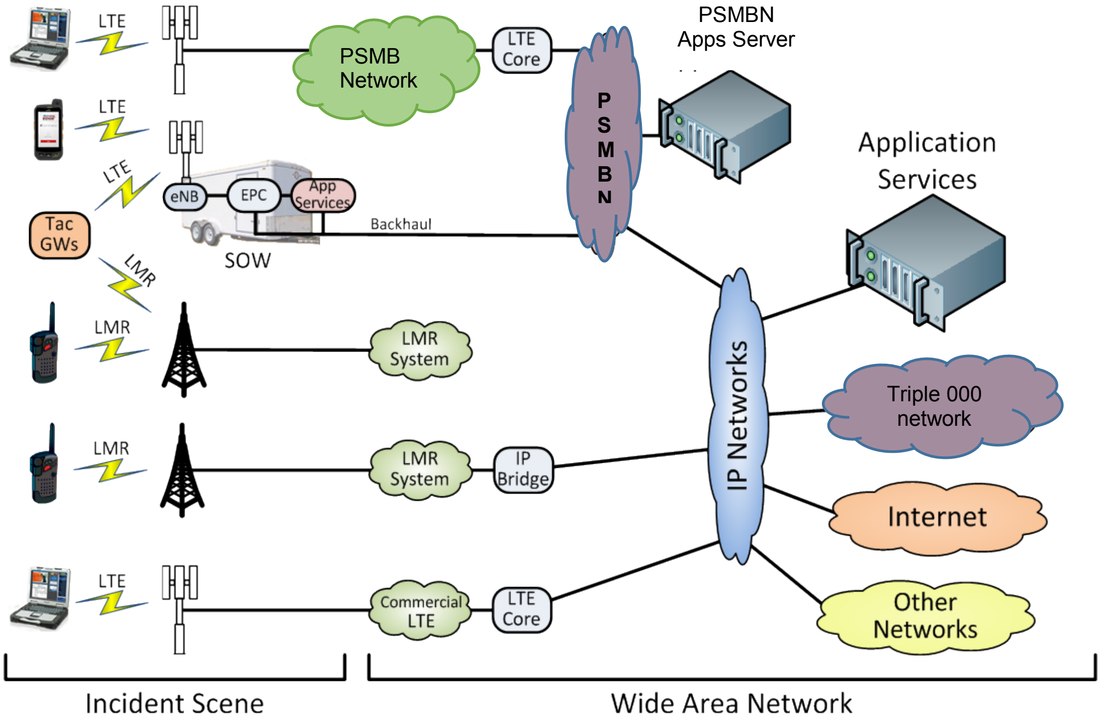


Figure 3 - On-Scene Interoperability

Note that in this diagram the SOW portion is optional; if not present the Incident LAN components continue to provide interoperability locally.

5.3 Full Scale Interoperability

The following diagram shows how interoperability between all components and networks could be achieved to meet the above goals.



5.4 Recommendations

It is recommended that the PSMB network include the capability of resilient cross-agency interoperability across a wide variety of network topologies and conditions.

6. Statement of Mutualink Capabilities

6.1 Current Production Status

The Mutualink solution is currently deployed live in hundreds of Federal, State and Local public safety and critical infrastructure agencies throughout the USA and overseas jurisdictions. It is being used operationally in day-to-day operations as well as local and regional incidents to interoperate and collaborate between many disparate agencies.

Mutualink has also deployed solutions incorporating Band14 in fixed sites, LTE deployables and tactical nodes (MCUs) which are currently operational in several BTOPs. (Click link here). Example deployment pictures are attached in Appendix A.

The capabilities described in this section are available in our current product; the specific mechanisms described are used in either our current production version or a pre-release version.

6.2 Fundamental Components

There are several types of fundamental operational components in the Mutualink system:

- **Gateways**. These devices connect to various communications & data systems that agencies wish to share or interoperate with other agencies.
- **User Applications**. These software applications are the primary user interface to the system and allow authorized users to control gateways as well as communicate directly with other users.
- **Thin-client Servers**. These server-side applications are used by thin-client user applications to gain the full functionality of thick-client user applications.
- **Network Functions**. These applications and devices help inter-connect and bridge between disparate IP networks and security domains.

6.2.1 Media and Resource Gateways

Gateways allow any communication or data system to be shared with and interoperate with other agencies. A gateway may be a physical device (e.g. when analog interfaces are required) or a logical software function (e.g. when only IP interfaces are required). Software gateway functions may reside on a small or large scale server platform (either hosted or on premise) or co-exist with a thick-client Mutualink user application on a laptop/desktop platform, etc.

Types of gateways available include:

- **Radio Gateway**. Interface to analog or digital LMR systems, intercoms, PAs, etc.
- **Video Gateway**. Interface to analog or digital video feeds/cameras/systems/wearables.
- **Telephony Gateway**. Interface to analog or digital telephony systems, PBXs, PSTN, SIP systems.
- **GIS Gateway**. Interface to enterprise GIS and AVL systems to provide location and geospatial data sharing.
- **Data Gateway**. Interface to arbitrary data systems to provide application-specific or opaque data connections.

In some contexts, gateways are also known as NICs (Network Interface Controllers).

6.2.2 User Applications

The user application ("Collaboration GUI") is the primary user interface to the full suite of Mutualink capabilities. Users of this application may communicate/collaborate directly with each other using voice, video, text messaging, file sharing, location and geospatial data sharing, and screen sharing. In addition, users may direct the operation of Mutualink Gateways that they are authorized to control.

There are two types of user applications available:

- **Thick Client**. This type of application runs on a laptop or desktop platform and has the full set of capabilities described above without requiring any server assist. Thick clients can communicate directly with other thick clients and gateways on the network in a peer-to-peer mode.
- **Thin Client**. This type of application runs on mobile platforms such as smartphones and tablets and requires a server-side component to achieve the same functionality as a thick client. For example, a thin client cannot directly control a gateway on the network, but it can do so indirectly by using a thin-client server.

One common type of thick client is an IWS (Interoperable Work Station) which is a dedicated secure appliance primarily for use as a Mutualink collaboration "terminal".

6.2.3 Thin-client Servers

These servers (“Edge Concentrators”) allow thin clients to achieve the same functionality as a thick client. Similar to software gateway functions, this server software may reside on a small or large scale server platform (either hosted or on premise), a laptop or desktop platform, or a compact embedded platform depending on the number of clients desired.

6.2.4 Network Functions

There are several network software functions that assist in inter-connecting and bridging disparate IP networks and security domains. These functions may run on a variety of hardware platforms, either coexisting with other Mutualink software functions (such as thin-client servers or thick clients) or on dedicated platforms.

The types of network functions available include:

- **Network Proxy**. This function allows Mutualink components on one IP network to communicate with Mutualink components on other IP networks (either local or remote) where IP routing between the networks is not available or desired, e.g. behind a NAT or wherever it’s desired to maintain network segregation. It achieves this by communicating with a similar Network Proxy function on the other networks.
- **Directory Service.** This function complements the Auto-Discovery feature (described below) to allow Mutualink components/users to publish their availability for other Mutualink components/users in situations where the Auto-Discovery feature is not active, e.g. across remote non-routable networks.

6.3 Distributed System Operation

A fundamental capability of the Mutualink system is that components can operate in a fully-distributed peer-to-peer mode. This allows Mutualink components on the same network to function together even in the absence of any additional infrastructure, servers, etc. The Mutualink components that are capable of direct peer-to-peer communication are gateways, thick clients, thin-client servers, network proxies, and directory services.

6.3.1 Auto-Discovery

The first step for components to communicate directly with each other is for each component to discover the presence of other directly-reachable components on the local network. The Mutualink Auto-Discovery feature uses IP multicast to perform this discovery function. Each component multicasts its availability and listens for those same announcements from other components; in short time all components will have discovered all other local components.

On the Collaboration GUI, all auto-discovered users and authorized gateways will be automatically displayed on the screen so the user may choose to directly communicate with them as desired.

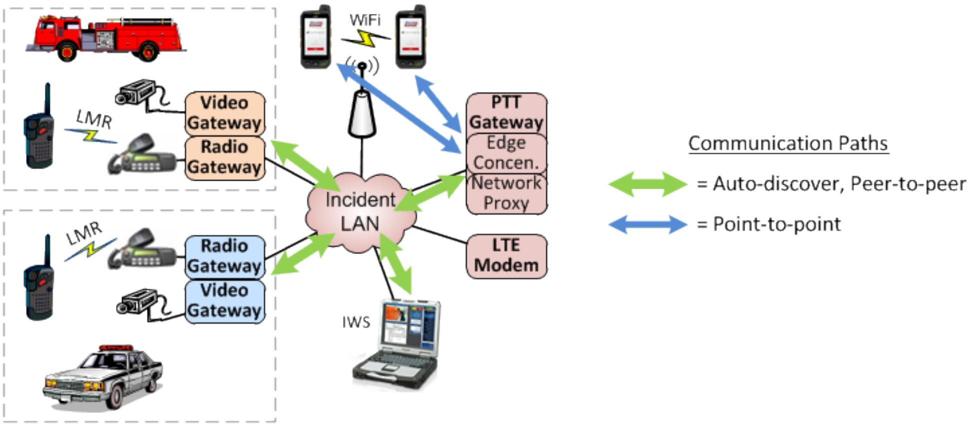
6.3.2 Direct Communication

When a user desires to communicate with another user or gateway shown on the screen, they create a Dynamic Sharing Group (described later) and simply drag-and-drop that user or gateway into the group. This causes an invitation message to be sent directly to the desired component via IP. If the invited component is another user, the user will be alerted and asked to accept or reject the invitation. If the invited component is a gateway, the gateway will validate the identity and authorization of the inviting user and decide whether to accept or reject the invitation accordingly.

Once an invitation is accepted, all communication (including media and data sharing) is similarly performed by direct communication between components. Wherever feasible, standard protocols such as SIP and RTP are used for real-time communication between components.

6.3.3 Example of On-scene Peer-to-peer Interoperability

Let’s revisit an earlier diagram to illustrate how this is implemented in the Mutualink System. Shown below is the example of an on-scene Incident LAN where multiple agencies have brought Mutualink gateways to the scene. The PTT Gateway is now expanded to show that included in that gateway is an Edge Concentrator thin-client server function as well as a Network Proxy function.

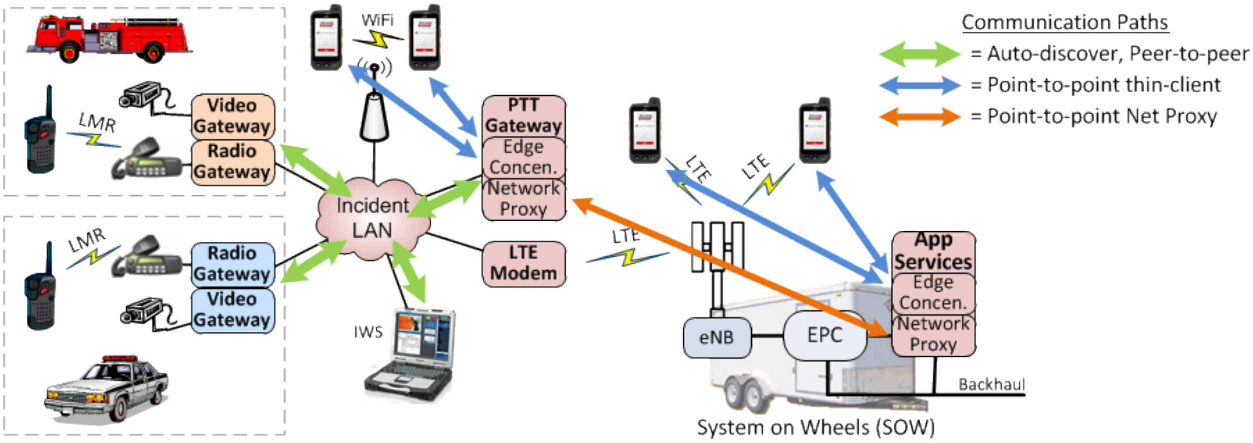


Note that the Radio & Video Gateways, the IWS thick client, and the PTT Gateway components will auto-discover each other and communicate directly as needed. Also shown are smartphone thin clients that connect to the Edge Concentrator and can then communicate with the other components.

This example also illustrates basic LTE<>LMR interoperability by virtue of the Mutualink PTT client in use on the smartphone coupled with the tactical radio gateways. If instead an infrastructure-based radio gateway was used to interface to a P25 ISSI, this would similarly demonstrate P25<>LTE interoperability.

6.3.4 Example of Inter-Network Interoperability

If we now connect that on-scene system via LTE to a SOW, we will illustrate how the distributed capability then expands to take advantage of the additional network.



Due to the new Network Proxy connection, the native LTE thin clients are now able to discover and communicate with the components in the Incident LAN. This process may then be repeated for any number of inter-connecting networks regardless of the transports used to connect the networks, e.g. wired, satellite, microwave, or LTE.

6.4 Dynamic Sharing Groups

A Dynamic Sharing Group is a fundamental Mutualink building block for sharing media & data among and between agencies; all sharing occurs within such a group.

When a user creates a new group, two things occur under the hood:

- A unique encryption key is dynamically generated for the group. All media and data for this group will be encrypted with this key.
- A local IP multicast address is reserved. Since group communications is inherently a many-to-many operation, IP multicast is used wherever the network allows for the most efficient communications and use of bandwidth.

In some contexts, Dynamic Sharing Groups are known as “Incidents” or “Missions”.

6.4.1 Group Invitations

Invitations to Dynamic Sharing Groups are sent using the standard SIP protocol. These invitations are sent as secure signed messages so that the identity of the sender can be authenticated and the contents of the invitation (including the initial group encryption key and the chosen multicast address) are encrypted so that only the intended recipient can decode the message.

6.4.2 Sharing Media and Data to a Group

Any member of a group may share arbitrary media & data resources to the group. This can be done either directly by the user (e.g. transmitting voice, sending webcam video, text messages, sharing files) or by the user directing a Mutualink gateway to share a specific resource from the system it is interfaced to (e.g. an LMR talk group or a video feed).

If the resource being shared is bandwidth-intensive (e.g. audio/video) then an additional local multicast address may be reserved similar to the original group address. This way, each member of a group may decide if they wish to use their bandwidth to consume media from that source and enable/disable that shared media at will.

6.4.3 Groups Involving Network Proxies

When members of a Dynamic Sharing Group span multiple non-routed networks (i.e. Network Proxies are in use), the remote Network Proxies may assign a different multicast address for their segment, or they may decide that unicast is more appropriate. These “local” address assignments are sent to local group members along with the original invitation as well as any subsequent messages.

6.5 Interoperability with P25, VoLTE, and Mission-Critical PTT

These capabilities are fundamentally made available simply by using the appropriate Mutualink gateway:

- **P25**. Although a P25 donor radio integration is certainly possible and may be the only solution for some tactical scenarios, a Mutualink digital radio gateway interfaced to a P25 ISSI offers superior quality and capability. When a user adds an ISSI gateway to a Dynamic Sharing Group, they are presented with a list of the available P25 talk groups available for interop use. The talk group they select will then be bridged to the desired sharing group.
- **VoLTE/MCV**. With the appropriate Mutualink digital telephony gateway, a VoLTE system could be integrated just as easily as a SIP PBX. Interoperability with other voice & video systems would then be achieved by adding a VoLTE “call” to the desired Dynamic Sharing Group.
- **Mission-Critical PTT (MCPTT).** Subject to final specification, this could be similar to a VoLTE integration if implemented in the IMS infrastructure. Additionally, if tactical MCPTT is implemented using a device-to-device ProSe or IOPS approach, the distributed nature of the Mutualink system is an ideal fit for interoperating MCPTT talk groups with other local & remote voice systems by using a tactical radio gateway at the incident scene.

6.6 Security

As this system is designed to share between multiple agencies, security is of utmost importance. To this end, the Mutualink system has been designed from the ground up with best-in-breed security features.

6.6.1 Identity Management

Identities are used for access control to gateways and for name identification to other users.

Mutualink’s identity management function uses a standard Public Key Infrastructure (PKI) with X.509 certificates. An important attribute of this PKI is that it does not require any cloud or centralized infrastructure to be present to operate; this makes the PKI ideal for a distributed system that must be able to be used in disconnected scenarios.

An identity certificate may be issued to an individual (using a “name” identifier) or to a device (perhaps using a “role” identifier). Each identity cert includes a human-readable identity including the agency affiliation and hierarchy.

Each Security Domain (silo) is authorized to issue credentials within their organizational name space.

- Domains may be authorized via Root CAs or Delegate CAs.
- Root CAs are added to the trust store with a list of namespaces that are authorized for that CA.
- Delegate CAs have their authorized namespaces included in their signed CA cert (via X.509 extension).

Security Domains may trust each other directly (e.g. Agency A trusts Agency B) or via trust inheritance from a larger domain (e.g. Agency A trusts everyone that the PSMBN domain trusts).

- These trust relationships can have their namespace scope constrained (e.g. I trust everyone that PSMBN does except for Agencies X & Y).
- These trust relationships can have their purpose scope constrained (e.g. I only trust my internal CA for gateway access, and other CAs for identification purposes only).

6.6.2 Encryption

All media & data within sharing groups is encrypted using dynamically-generated symmetric keys (AES-256 by default).

Encryption is performed end-to-end between all members of a sharing group; no infrastructure components can snoop on or modify media/data in transit.

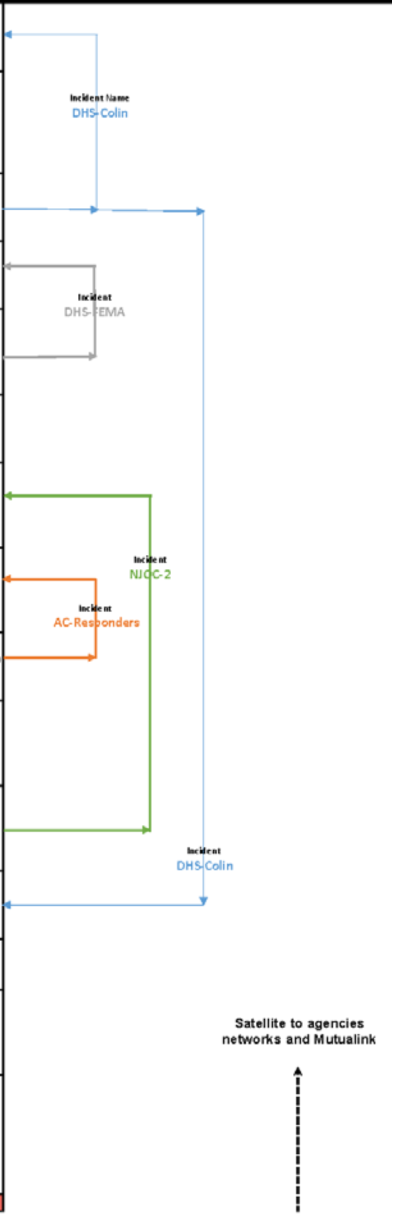
6.6.3 Approvals

The Mutualink system has been approved by JITC for use on DoD networks.

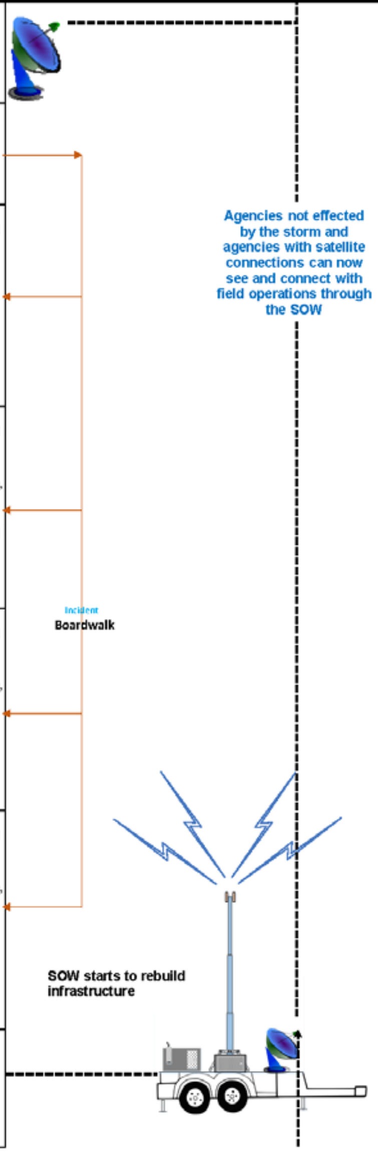
7. Example Use Cases

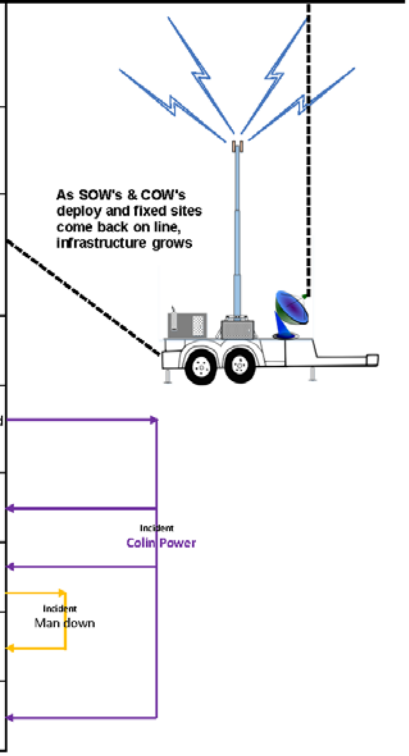
FirstNet, in appendix C-9 has asked for vendors capabilities to be evidenced through the demonstration of applicability in User Cases. Mutualink chose a large complicated Use Case (FEMA Type 1: National) and made it even more complicated, because that is how the world, and in fact national policy actually exist. What we attempt to show is representative example of some of the Agency interactions, Locations, Media Types, Transport methods (BC 14 and others) as a Hurricane hits the east coast. The storm will force communication interaction to build, climax with the destruction of infrastructure forcing the use of deployables, rebuild as the storm subsides and finally go into a recovery mode prior to the eventual end of the incident. As you will see Agencies, media types (radio video, data, location) span our entire society, yet they will be able communicate in a secure, ad hoc fashion.

Time	Conditions	Agency	Location	Media	Pipe	Who to interconnect with	Purpose	Mutualink Solution	Connections made through Mutualink
Day 1 1200 Hrs	Tropical Storm Colin becomes a category 1 hurricane reaching 75 MPH winds, just off the Cuban coast. No idea if it will hit the U.S. coast	DHS	DC	Voice intercom	Network / Internet	FEMA Albany, Trenton, Hartford	Initial Pre-Incident communications	DHS DC creates incident "**DHS-Colin**" invites & brings in 3 other DHS offices and FEMA in NJ to discuss plans between agencies	
Day 3 1000 Hrs	Hurricane Colin is off the coast of Florida still with 75 MPH winds turning up the U.S. coast. Hurricane Watch are issue from Virgina to Maine	DHS	DC	Voice intercom, File, Maps	Network / Internet	FEMA, Albany, Trenton, Hartford, Field Operations	Sharing coastal conditions and evacuation routs	DHS DC creates second incident "**Costal**" invites and brings in 3 other DHS offices and FEMA Field Operations in NJ to update on weather conditions and evacuation progress	
Day 3 1452 Hrs		DHS	Trenton	Files & Maps	Network / Internet	NJSP, ACPD & ACSO Field Operations	Review evacuation routs and procedures with the State Police, Police Department and Sherriff's Office	DHS invites and brings Highway Patrol into inciden "**DHS-Colin**" to update evacuation routs, procedures and progress	
Day 4 1230 Hrs	Superstorm Colin the largest Atlantic hurricane on record is 350 miles off the NJ coast, a category 2 hurricane with winds of 95 MPH heading for Atlantic City NJ. Hurricane Warning issued for NJ, NY, CT	DHS	DC, Albany, Trenton, Hartford	Voice telephone, Fixed Video,	Network / Internet, Cell Carrier	FEMA, NJ Command	Share evacuation status, beach video and open telephone connections	DHS creates new Incident "DHS-FEMA", invites and brings in FEMA NJ Command to share video and telephone	
Day 4 1535 Hrs		FEMA NJ Command	NJ	Voice, file, location & Video LTE	Cell Carrier, Band 14	On scene First Responders	Share conditions at multiple locations throughout the coast	FEMA invites and brings in on-scene First Responders with Mutualink EDGE smartphones and tablets into incident "DHS-FEMA" to provide real-time status of conditions at multiple locations	
Day 4 1900 Hrs		DOE	DC	Voice intercom, Files	Network / Internet	Nuclear power plant NJ **Oyster Creek**	Setup voice communications, review emergency procedures, monitor plant operations	DOE create incident (NJ**OC**) with Power Plant management to review emergency procedures	
Day 5 0200 Hrs		DOE	DC	Voice intercom, Video	Network / Internet, Cell Carrier	NJSP & Nuclear Power plant NJ Oyster Creek	Make connection to monitor evacuation progress from around the Oyster Creek plant	DOE creates second incident "NJOC-2", invites and brings in State Police to monitor power plant operations and review local area evacuation progress	
Day 5 1545 Hrs		FEMA	Trenton	Voice radio	Network / Internet, UHF, VHF	NJSP, ACPD, AC-EMS, ACSO	Connects agencies together with radio channel from each providing ground conditions from specific areas	FEMA creates incident "**AC-Responders**", invites and brings in NJ State Police, Atlantic City PD and EMS. Each agency brings their radio channel into the incident	
Day 5 2300 Hrs	Heavy rain, sustained winds 52 MPH, gusts 73 MPH, sporadic power outages, some coastal flooding	ACPD	Atlantic City	Voice radio, Video LTE, Location	Network / Internet, Cell Carrier	ACFD	PD & FD connect radio channel. FD provides video from smartphone in flooded areas	ACPD brings the AC Fire Department into the incident "AC-Responders"	
Day 6 0500		AC-EMS	Pulls up to accident scene	Voice radio, video LTE,	Cell Carrier, Band 14	AltantiCare Reg Med Center	EMS provides ER doctor patient info, vital's and video of patient	EMS creates incident, "**Patient-1**", using Mutualink EDGE from iPad on scene creates incident to discuss the patient with a doctor and share video from scene	
Day 6 0730		Nuclear Power plant NJ Oyster Creek	On-scene	Voice & Video LTE	Cell Carrier, Band 14	DHS, NJ-OHS&P	Plant operator providing update of conditions at the nuclear power plant	Power plant invites and brings 2 other agencies into incident "NJOC-2" to share information	
Day 6 0800		FEMA	DC	Voice intercom, Maps, Airport layout	Network / Internet	TSA Atlantic City International Airport	As conditions intensify FEMA monitors airport operations and security sharing this information with NJSP, ACPD & ACSO Field Operations within the incident	FEMA brings TSA into incident "DHS-Colin" with NJSP,ACPD & ACSO	
Day 6 1020		DHS	Albany, Trenton, Hartford	Voice intercom, file	Network / Internet,	Red Cross	Setting up shelters, sharing building layout files, personnel lists and supplies needed	DHS creates new Incident "**DHS-RC**", invites and brings in the Red Cross to discuss and share files for shelters	
Day 6 1330		NJ-OHS&P	Command Center	Voice radio, files, maps, video, location	Network / Internet, Band 14, VHF, UHF, P25	NJSP, ACPD & ACSO Field Operations	Coordinate final evacuation and emergency response	OSH&P creates incident "**OSHP-Colin**", invites and brings in State Police, local Police Department and field operations of the Sheriffs office	
Day 6 1600 Hrs	Superstorm Colin's eye is 10 miles offshore of Atlantic City, 92 MPH sustained winds, 140 MPH gusts, major power outages, Major flooding, fire starting on boardwalk, Cell carrier's are down or jammed, Public Safety Radio Comm's sporadic	NJ-OHS&P	Command Center	Voice radio, files, maps, video, location	Band 14, Wi-Fi, VHF, UHF, P25	Incident Command Post, Unified Coordination Group, Local EOC, State EOC	As communications is lost deployed Tactical Nodes placed pre-storm in strategic locations are brought on line providing local Voice, Video, Data coverage	Field commander's initialize a Tactical Node at each location. Download the Mutualink Android client to smartphones, setup a Wi-Fi bubble with the Tactical Node. Each commander creates an incident, invites and brings the smartphones into the incident.	
Communication infrastructure is down - All communication is lost - No Cell service, No radio, No Band 14									



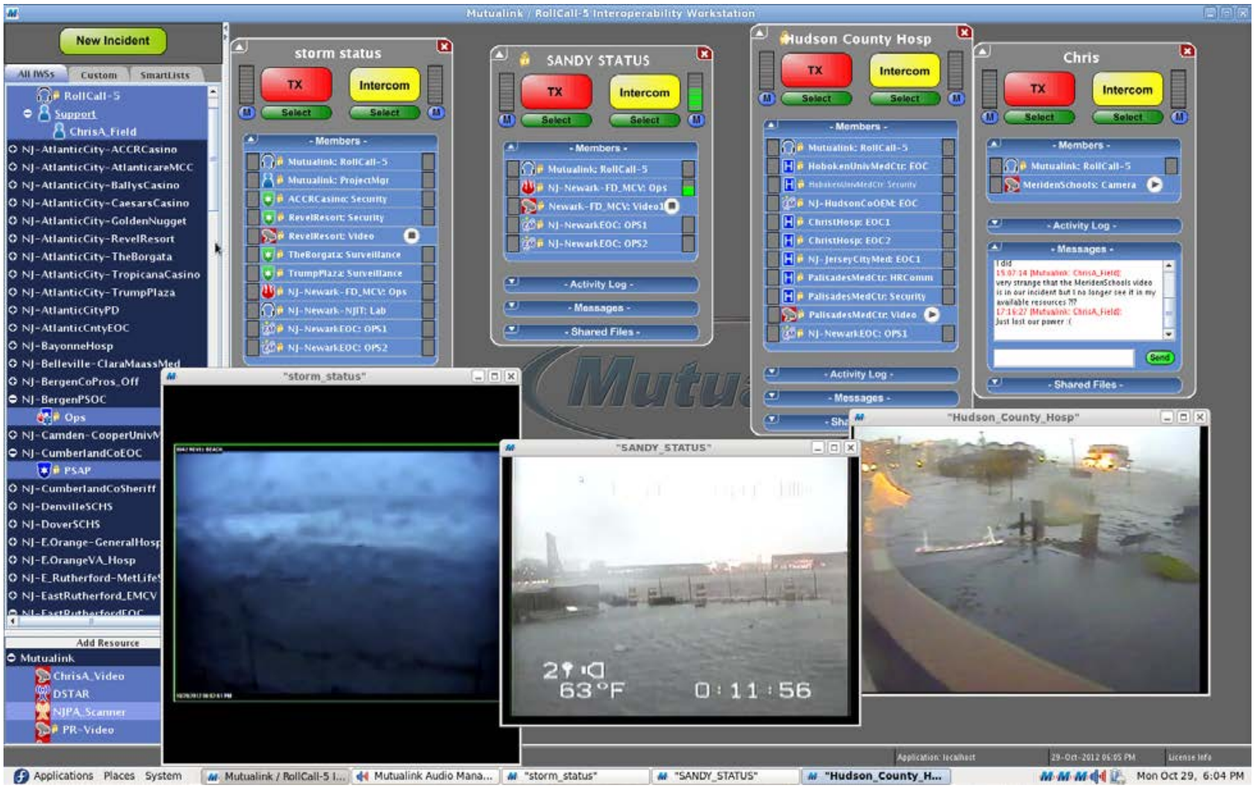
Satellite to agencies networks and Mutualink

Time	Conditions	Agency	Location	Media	Pipe	Who to interconnect with	Purpose	Mutualink Solution	Connections made through Mutualink
Day 6 2000 Hrs	Superstorm Colin comes ashore just north of Atlantic City NJ - high tide 20% above normal, 12" of rain, 32.5 foot waves, No First Responder communication exists, widespread power outages	FIMA National Operations Center	DC	Voice intercom, radio, files, photos, video	Network / Internet	FEMA NJ, CT, NY	Assessing damage as reports are received	FEMA creates incident **"FEMA-Colin"**, invites and brings in FEMA State offices in NJ, CT & NY. State offices are on backup generator and using satellite communications	 Agencies not effected by the storm and agencies with satellite connections can now see and connect with field operations through the SOW Incident Boardwalk SOW starts to rebuild infrastructure
Day 7 0930 Hrs	Wind & rain start to subside, no comm's infrastructure exists, Major fire on boardwalk and around Atlantic City	NJ-OS&P	Command Center	Voice radio, video smartphone & wearables, pictures, files, maps,	Wi-Fi	Incident Command Post Boardwalk	Tactical Nodes are deployed creating Wi-Fi bubble capable of receiving clients with voice communication and transmitting video from the scene	Field commander's initialize and sets up the Tactical Node and creates incident "**Boardwalk**".	
Day 7 1040 Hrs		ACFD	Pulls up to Incident Command Post	Video Smartphone, radio, Video wearable	Wi-Fi, VHF	Incident Command Post Boardwalk	Fireman (Atlantic City FD) pulls up to ICP to fight the fire and provide a VHF radio	Some Atlantic City FD download the Mutualink Android client from the Tactical Node to their smartphone. The field commander invites and brings them into the incident "**Boardwalk**" providing voice, video, data, file and location sharing though the Tactical Node. The field commander connects one of the Atlantic City FD VHF radios to the Tactical Node providing interoperability between VHF radio talk-around channel and the smartphones.	
Day 7 1150 Hrs		National Guard	Pulls up to Incident Command Post	Video Smartphone, radio, Video wearable	Wi-Fi, VHF, HF	Incident Command Post Boardwalk	National Guard pulls up to ICP to provide assistance and provide an HF radio	Some National Guard download the Mutualink Android client from the Tactical Node to their smartphone. The field commander invites and brings them into the incident "**Boardwalk**" providing voice, video, data, file and location sharing though the Tactical Node. The field commander connects one of the National Guards HF radios to the Tactical Node providing interoperability between HF, VHF radio talk-around channel and with the smartphones.	
Day 7 1205 Hrs		NJSP	Pulls up to Incident Command Post	Video Smartphone, radio	Wi-Fi, VHF, HF, UHF	Incident Command Post Boardwalk	Officer pulls up to ICP, downloads client to his smartphone, connects UHF radio to the Tactical Node	Some State Police download the Mutualink Android client from the Tactical Node to their smartphone. The field commander invites and brings them into the incident "**Boardwalk**" providing voice, video, data, file and location sharing though the Tactical Node. The field commander connects one of the State Police UHF radios to the Tactical Node providing interoperability between UHF, HF, VHF radio talk-around channel and with the smartphones.	
Day 7 1100 Hrs		ACPD	Pulls up to Incident Command Post	Video Smartphone, radio	Wi-Fi, VHF, UHF, 800 MHZ	Incident Command Post Boardwalk	Officer pulls up to ICP, downloads client to his smartphone, connects 800 MHz radio to the Tactical Node	Some Atlantic City PD download the Mutualink Android client from the Tactical Node to their smartphone. The field commander invites and brings them into the incident "**Boardwalk**" providing voice, video, data, file and location sharing though the Tactical Node. The field commander connects one of the Atlantic City PD800 MHZ radios to the Tactical Node providing interoperability between 800 MHz, UHF, HF, VHF radio talk-around channel and with the smartphones.	
Day 7 1830 Hrs		NJ-OHS&P SOW	Pulls up to Incident Command Post with SOW	Video Smartphone, radio, Video wearable	Wi-Fi, VHF, HF, UHF, 800 MHZ, Band 14, Satellite, Microwave	Incident Command Post Boardwalk	Provide Band 14 and Wi-Fi bubble and satellite backhaul	SOW deployable setup providing Band 14 bubble, Wi-Fi bubble and satellite connection to the agencies network, internet and Mutualink IRAPP Network. All Tactical Nodes within the Band 14 bubble will automatically connect to the SOW through Band 14	

Time	Conditions	Agency	Location	Media	Pipe	Who to interconnect with	Purpose	Mutualink Solution	Connections made through Mutualink
Day 7 2040 Hrs		Borgata Casino	Atlantic City	Voice radio, Video, File Sharing	Wi-Fi, VHF	SOW	The Casino is being used as a shelter and has Mutualink equipment. Through Mutualink IRAPP network the Casino connects to OSH&P and AltantiCare Regional Med Center	Casino creates an incident **"Shelter Borgata"**, invites and brings in OSH&P and the Hospital. They also bring in their in-house radio system. The building is running off backup power and satellite connection to IRAPP	 As SOW's & COW's deploy and fixed sites come back on line, infrastructure grows
Day 7 2350 Hrs		National Guard	Incident Command Post	Video Smartphone, radio, Video wearable	Wi-Fi, VHF, HF, UHF, 800 MHZ, Band 14	Incident Command Post	National Guard is deploying in surrounding areas using their HF radios back to the HF radio on the Tactical Node. They have full interoperability with every active through the SOW and Tactical Node	National Guard HF radio is already connected to the Tactical Node. Nothing needs to be done for the new team members to communication with people already on the ground.	
Day 8 0430 Hrs		NJ-OHS&P SOW & COW	Other Incident Command Post'	Video Smartphone, radio, Video wearable	Wi-Fi, VHF, HF, UHF, 800 MHZ, Band 14, Satellite, Microwave	Incident Command Post 's throughout area	Mor SOW's are deployed through the areas where no or little communication exista providing Band 14, Wi-Fi bubble and satellite backhaul connecting SOW's together with COWS increasing infrastructure	SOW deployable setup providing Band 14 bubble, Wi-Fi bubble and satellite connection to the agencies network, internet and Mutualink IRAPP Network. All Tactical Nodes within the Band 14 bubble will automatically connect to the SOW through Band 14	
Day 8 0600 Hrs		NY OHS&P	New York City	Voice intercom, File, Picture, Video	Network / Internet	NJ OHS&P. CT OSH&P	Assess damage---Both states have many Tactical Nodes, SOW's / COW's deployables in service providing infrastructure for a large percent of the effected area.	NY OHS&P creates incident "**Recovery from Colin"**, invites and brings in NJ OSH&P and CT OSH&P	
Day 8 0630 Hrs	Light rain with very low winds	NJ OSH&P	New Jersey	Voice intercom, File, Picture	Network / Internet	Jersey Central Power & Light	As roads are cleared for large power repair trucks OHS&P coordinates with power companies to get the most critical areas repaired first.	OHS&P creates an incident "**Colin Power"**, Foreman of line crews download the Mutualink client from the internet and are invited into incident Colin Power.	
Day 8 0640 Hrs		NJ OSH&P	New Jersey	Voice intercom, File, Picture, Video	Network / Internet, Band 14, Wi-Fi	Atlantic City Electric	OSH&P coordinating the rebuild of the power infrastructure	Foreman of line crews download the Mutualink client from the internet and are invited into incident **"Colin Power"**	
Day 8 0700 Hrs		Jersey Central Power & Light	New Jersey	Video & Voice Smartphone	Band 14, Wi-Fi, Cell Carrier	EMS, ACFD, ACPD	Accident with power lines, man down	The Power company foreman creates an new incident "**Man Down"**, invites and brings in EMT's, Police and Fire	
Day 8 0705	Weather back to normal	ACFD	Atlantic City, NJ	Voice & Video LTE, Voice Intercom	Cell Carrier, Band 14	OHS&P	The man down is a employee of the OHS&P	ACFD invites and brings in OSH&P	
Day 8 0645		NJ OSH&P	New Jersey	Voice intercom, File, Picture, Video	Network / Internet, Band 14, Wi-Fi	Orange Rock Electric	OSH&P coordinating the rebuild of the power infrastructure	Foreman of line crews download the Mutualink client from the internet and are invited into incident **"Colin Power"**	

As infrastructure is rebuilt and emergencies subside Mutualink incidence's are broken down and canceled

As you can see it is an almost infinitely complex environment, yet one we helped successfully manage during “Superstorm Sandy” below is a screen shot representing one participants view at one snapshot in time.



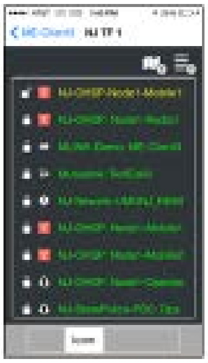
I did
15:07:14 [Mutualink: ChrisA_Field]:
very strange that the MeridenSchools video is in our incident but I no longer see it in my available resources ?!?
17:16:27 [Mutualink: ChrisA_Field]:
Just lost our power :(

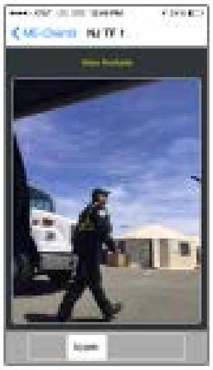
For a brief (12Min) primer on how all of this comes together, please click the link below
Mutualink Demo .

8. Conclusion

As described in this document, the issue of multi-media, multi-agency and multi network interoperability is one of extreme complexity. This fundamental issue needs to be addressed as a core capability of any options chosen for the PSMB network in order to meet the public’s expectations. The opportunity exists now to, at long last, put the nation’s interoperability issues behind us while we bring the nation’s first responders much needed broadband capabilities.

Appendix A
Mutualink in Action


ME-Client1
NJ TF 1
NJ-OHSP-Node1-Mobile1
NJ-OHSP-Node1-Radio1
MLINK-Demo-ME-Client1
Mutualink-TestCam
NJ-Network-UMSINJ_PIMM
NJ-OHSP-Node1-Mobile2
NJ-OHSP-Node1-Mobile3
NJ-OHSP-Node1-Operator
NJ-StatePolice-POC-Tips
Scan


ME-Client1
NJ TF 1
View Multiple
Scan

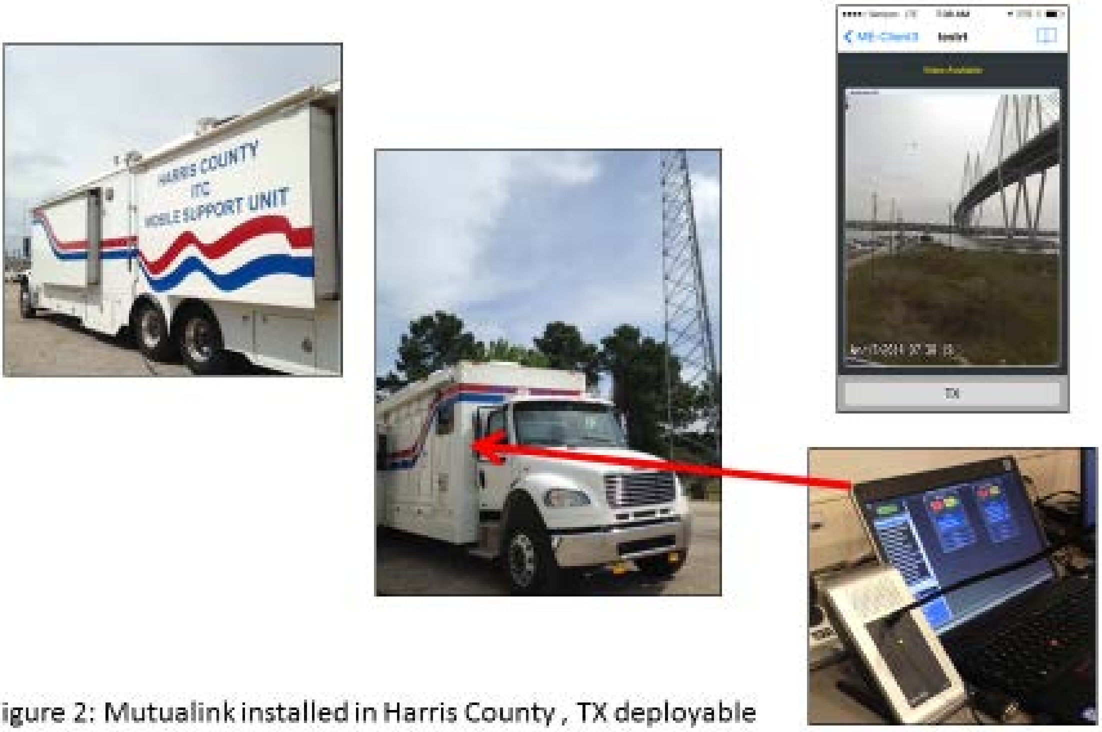


Figure 2: Mutualink installed in Harris County , TX deployable and on mobile clients for multimedia collaboration