



MUTUALINK PROVIDES INTEROPERABILITY SOLUTION TO MEET NATIONAL SECURITY COMMUNICATIONS PRIORITIES

Comprehensive Emergency Communications Interoperability and Preparedness is a National Priority

This priority is illustrated by the new National Emergency Communications Plan (NECP) created by the Department of Homeland Security (DHS); the July 31, 2008 DHS press release states the NECP purpose as: "...to address gaps and determine solutions so that emergency response personnel at all levels of government and across all disciplines can communicate as needed, on demand, and as authorized." Homeland Security under Secretary Robert Jamison added: "This is a comprehensive plan designed to drive measurable and sustainable improvements to operable and interoperable emergency communications nationwide over the next three years. It emphasizes the human element and cross-jurisdictional cooperation, going beyond simply buying new equipment."

[Underlining added to note objectives fulfilled by the Mutualink solution.]

NECP's 3 GOALS

The NECP defines three (3) goals that establish a minimum level of interoperable communications and a deadline for federal, state, local and tribal authorities:

by 2010

90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) can demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

by 2011

75 percent of non-UASI jurisdictions can demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

by 2013

75 percent of all jurisdictions can demonstrate response-level emergency communications within three hours of a significant event, as outlined in the department's national planning scenarios.

Achieving National Objectives for Interoperability

Mutualink is a unique and innovative solution that, due to its low cost and unique capabilities, can serve as your scalable communication foundation for the implementation of community-wide preparedness and response. It unites federal, state and local first responders along with other critical community and private sector security organizations, such as schools, hospitals, malls, stadiums and executive protection forces. Mutualink incorporates NIMS compliant and intuitive call signs and protocols, which can be utilized by all members of a community to better handle incidents of all sizes and types. Mutualink enables access to these resources whenever assistance is quickly required from additional responders who were not previously connected to the incident.

By providing a robust and easy to use multimedia interoperable communications platform at a low cost, Mutualink is quickly adopted for use across entire communities and regions, while providing the scalability required for both day to day incidents and for large-scale emergency incidents.



OVERVIEW SOLUTION

Introduction to Mutualink

As an IP-based multimedia overlay network, Mutualink is designed to leverage the use of your existing radio equipment, including disparate systems, as well as next-generation communication technology. Mutualink's patent-pending architecture provides unmatched flexibility, reliability and control. Security and Public Safety agencies using Mutualink have the dual benefit of maintaining full control of their radio and related resources, while making them available for interoperable connection with other agencies' systems with the click of a mouse. Interconnection with the Mutualink network is achieved without impacting the operation of existing console and remote control equipment.

Mutualink is an "always on" system available around the clock. Mutualink blends IP and traditional radio networking technology with application software designed specifically to solve interoperability problems while delivering a solution affordable to everyone. Mutualink is highly scalable

supporting intra- and interagency interoperability scenarios across multiple disciplines and jurisdictions.

Mutualink, Inc. is a radio and wireless interoperability provider based in Wallingford, CT. The technology is based on Mutualink management's 16 years of experience in radio networks, public safety markets, wireless communications and advanced Voice & Radio-over-IP (VoIP & RoIP). Industry analysts have observed that Mutualink's design and affordability make it the first interoperability solution with the potential to reach wide scale acceptance and implementation.



Controllable, Intuitive & Affordable: Mutualink Delivers the Keys to Effective Interoperability

Controllable Solution: The "political" barriers to interoperability are resolved through: Mutualink is uniquely invitation-based, allowing users to maintain control of their respective resources by:

- Accepting or rejecting invitations to join incidents
- Dynamically contributing or removing communication assets as required
- Establishing or exiting incidents

Each agency has complete control over who is able to use their communication assets

There is no single agency or "trusted third party" controlling the system because no centralized switches or servers are required, unlike other interoperability solutions

Each agency purchases their own devices; they can then communicate directly with each other as desired over the peer-to-peer network

Mutualink users conduct dynamically configurable, real-time communications that are easily adapted to the stage, status and requirements of an incident.





OVERVIEW SOLUTION

Intuitive Ease of Use: Mutualink's user interface is quickly learned and easy to use:

- Icon-driven with Drag & Drop navigation to add radios, video or phones to an Incident
- Plain English naming conventions to enhance rapid communication and understanding
- Standard IM text format for messaging which mirrors cell phone and online texting
- Uncluttered workspace to create and manage up to eight concurrent incidents



Because of its utility for day-to-day usage, safety agency officials readily become familiar with usage protocols so that when a large crisis occurs they are prepared to use the system and respond quickly.

Affordable and Flexible: Mutualink's affordability allows many diverse organizations to improve emergency response through better incident management and interoperability:

- Multiple purchase options to eliminate capital barriers
- Budget process is shortened
- Facilitates incremental addition of endpoints
- Small investment provides access to the resources of the entire interoperability network



Mutualink is Interoperability for Radios, Phone, Text, Data & Beyond

- **LMR Radios:** Interconnect uniform and disparate systems
- **Telephony:** POTS landline, cellular, Wi-Fi and VoIP
- **Dispatch Collaboration:** Off-the-air conferencing between IWS dispatch centers
- **Files:** Blue prints, building floor plans, HAZMAT data
- **Video:** Live copter feeds, street/cruiser cams, building interiors
- **Text Messaging:** More effective than voice for informational content
- **PA System Interface:** Broadcast emergency messages

Mutualink Customer Examples

- Federal, State and Local Government
- Military Services
- Public Safety Agencies
- Schools and Universities
- Hospitals, Malls and Stadiums
- Airports, Transit and Ports
- Correctional Institutions
- Utilities, Public Works and Critical Infrastructure
- Corporate & Private Sector Security Forces

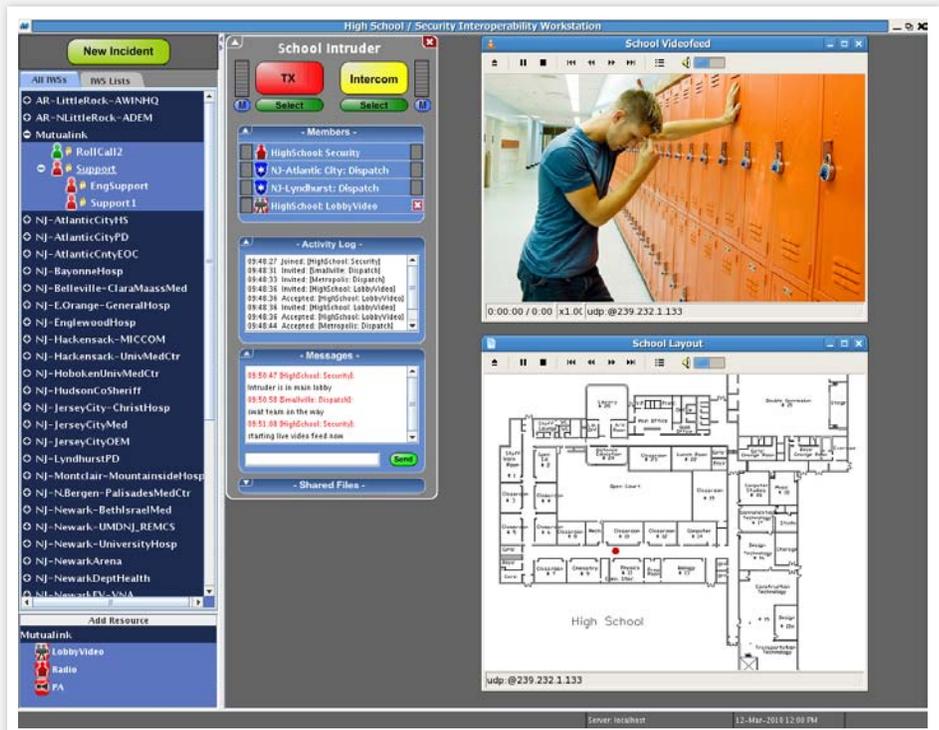


OVERVIEW SOLUTION

Typical Applications for Mutualink

- Improved Incident Command and Control
 - Incident network(s) can be established in seconds
 - Participants/resources can be dynamically managed from any authorized location (dispatch, remote, back-up, on-site)
 - Linking 2-way radios, telephone, video, etc. in Mobile Command Centers
- Dispatch-to-dispatch intercom
 - Voice, text, video and file sharing
 - Separate PTT/Intercom talk-paths enable Command & Control
- System disaster recovery/backup
- Access to incidents from remote locations
- COOP – Continuity of Operations during and following an incident.
- Connectivity for multiple locations
- System migration / transition support (patching new with old)
- Community-wide Interoperability:
 - PSAP to PSAP
 - PSAP to schools, universities, malls, stadiums, casinos, etc.
- On-site Incident Management Mutual aid response (e.g. fire, police and EMS agencies)
- Event Management: Coordination across multiple agencies

“Mutualink User Interface: Powerful Capabilities and **EASY** to Use.”





OVERVIEW SOLUTION

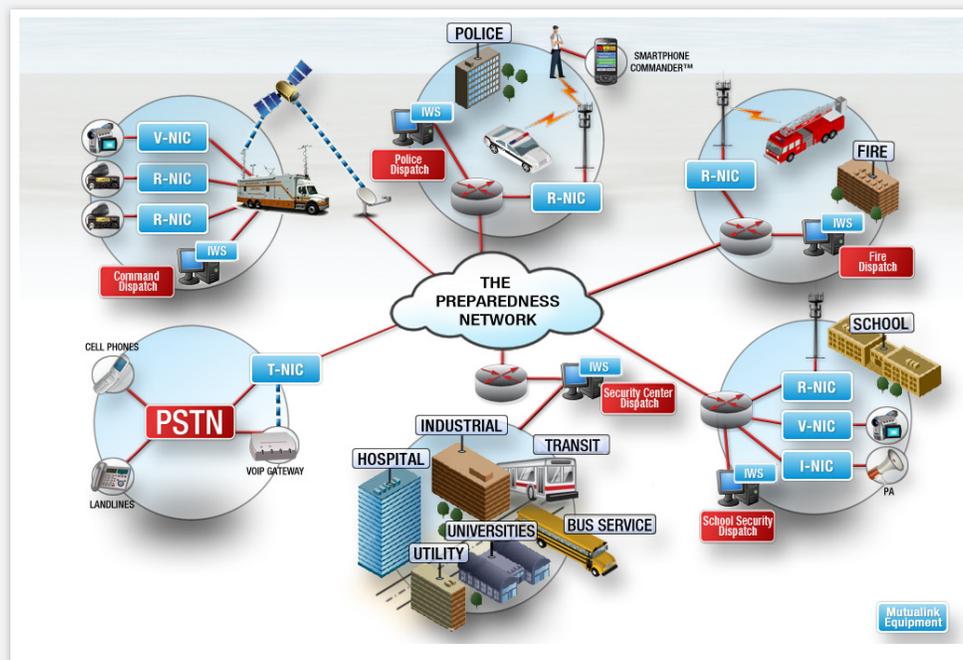
THE MUTUALINK COMMUNICATION AND INFORMATION SHARING NETWORK:

Technical Description

Mutualink is designed to be user-friendly, simple to operate and quick to learn. The simplicity of the Mutualink design makes installations and maintenance easy and inexpensive. With Mutualink, dispatchers from separate participating agencies can communicate using an IP connection such as a LAN with either voice or text messaging. Communication can be conducted behind the scenes or over the air to coordinate emergency incidents including fires, civil incidents, accidents, and special events, such as parades, concerts or political events. Mutualink provides the ability to link radio channels and other communication resources from one agency to the channels of another allowing communication between multiple agencies such as police, fire, DOT etc, at the click of a mouse.

System Overview

A Mutualink system (see diagram below) can consist of many different communication nodes (in blue) connected by a common IP network (called the Mutualink Interop Network). Interoperability between the various nodes is achieved through the Mutualink applications software that converts all communications and information input into IP packets then intelligently and securely routing them to the appropriate destination(s).



“ Mutualink Architecture Overview ”



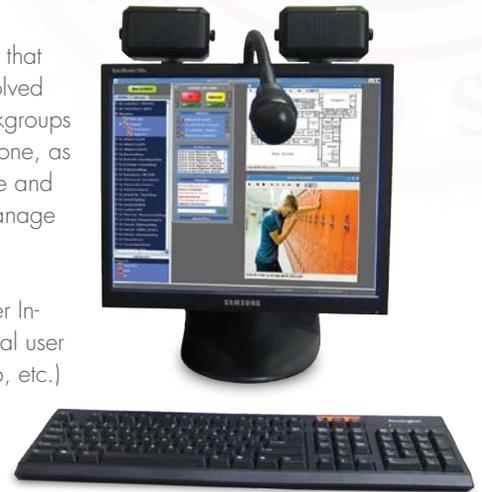
SYSTEM COMPONENTS

Mutualink Interoperability Workstation (IWS)

The Mutualink IWS provides an incident-based highly intuitive graphical user interface (GUI) that can be effectively used by a dispatcher or incident manager to communicate with other involved dispatch personnel as well as with units in the field. Interconnection of radio channels / talkgroups is facilitated using Mutualink's drag and drop interface. An IWS can be used either stand-alone, as a mini-console, or in combination with an existing console position. The IWS is simple to use and easy to maintain. In addition, the multi-featured and robust Mutualink software is easy to manage for System Administrators and other key personnel.

The IWS is a standard PC-based platform that provides the dispatcher with a Graphical User Interface (GUI) to control and operate the Mutualink system. The IWS is the primary operational user interface for the Mutualink system. It consists of a standard x86 PC platform (desktop, laptop, etc.) running the Mutualink real-time communications application on a Security Enhanced (SE) Linux operating system. The IWS allows the end user to:

- Control the interoperability of any authorized NICs
- Communicate with other IWSs and NICs via PTT voice, text messaging, public address and video display
- Share data files, such as floor plans and situational awareness data, with other IWS's



Network Interface Controllers for Radio (R-NIC), Video (V-NIC), Telephony (T-NIC), Intercom (T-NIC) and related Communications Interoperability

Mutualink's compact NIC devices provide an interface to existing LMR radio networks (P25, UHF, VHF, 700Mhz, Analog, Digital, etc.), as well as sources of video (cameras, video feeds, streaming video), voice communications (POTS landline, cellular, Nextel, Wi-Fi, VoIP, etc.) and public address systems. The NIC operates in a transparent mode, connecting with the network only when the associated radio channel or other resource is brought into an active incident. The NIC is a highly intelligent interface allowing a simple, effective and low-cost connection to legacy radio systems as well as next generation communications products.

Description of a NIC (R-NIC example): - The Radio Network Interface Controller (R-NIC) performs the function of routing audio control and status data from the IWS or other NICs in an incident to and from the transceiver it integrates into the network. As a gateway device, the R-NIC interconnects the Mutualink system to any existing conventional or trunked Land Mobile Radio systems. It consists of an embedded hardware device running a real-time SE Linux operating system and is available in either a desktop or rackmount configurations. Available methods of interconnecting to the LMR system include analog audio (PTT or VOX), digital audio (IP), and serial control. The R-NIC connects to the Mutualink system via a standard Ethernet connection.





MUTUALINK, CENTRAL STATION MONITORING AND VERIFIED RESPONSE

What is Verified Response?

Police departments across North America are continually challenged by the need to respond to all burglar alarms, particularly when a staggering 94% to 99% of alarms prove to be false. Despite extensive efforts to combat the problem, including call verification, permits, and fines, the cost for responding to false alarms continues to mount while the false alarm rate remains high and essentially unchanged.

Increasingly, police departments in North America are introducing Verified Response policies which require alarm companies to verify that a burglary has occurred or is occurring before police are dispatched through an eyewitness, monitored audio and/or video.

The following results are being realized by departments requiring verification:

- Significant time savings for police,
- The ability to re-deploy police officers to higher priority emergency calls,
- Concerns of skyrocketing burglary rates are proving unwarranted.

The definition of Verified Response has been expanded to include eye-witness reports, multiple-trip alarms, audio and video evidence, or known criminal activity in the area. The benefits of Verified Response include reducing the number of times that police officers are dispatched and increasing the ability to redirect police officers to more productive efforts.

Additionally, fears that Verified Response would lead to skyrocketing burglary rates appear to be unfounded as Verified Response often results in a reduction in burglary rates and increased arrests. Moreover, departments implementing Verified Response requirements are highly reluctant to go back to earlier methods for dealing with false alarms.

Negative public and/or alarm industry reaction for proposing Verified Response can be overcome and citizen acceptance achieved relatively quickly when accurate information is conveyed through public education via city-led task forces.

Mutualink's Role in Verified Response

Mutualink's multimedia communication resource sharing platform is uniquely suited for Response Verification at a central monitoring station. A security customer can now have video, audio or data files such as floor plans directly shared with first responders whether at dispatch or to an officer in route to the scene. Additionally, first responders can communicate directly to any people inside the facility via the facility's PA/intercom connection to the Mutualink system. This level of cooperation among central station monitoring firms and first responder agencies represents an unprecedented level of preparedness and response within the community.





TECHNICAL FEATURES AND FUNCTIONALITY

Technical Point: Peer-to-Peer

- The Mutualink system does not require servers for network nodes can communicate directly with each other in a peer-to-peer manner
- Nodes can function effectively in both ad-hoc

Technical Point: Auto Discovery

- Network nodes periodically announce themselves on a common multicast address that represents the particular network they belong to.
- This presence information is all that is needed make a node available for use in a peer-to-peer mode

Technical Point: Directory Services

- Mutualink Directory Nodes (MDNs) store node presence data for querying by other network nodes and/or Directory Nodes
- Directory Nodes operate in a hierarchal manner; they:
 - Gather information by auto-discovering network nodes in their vicinity as well as receiving reports from children and peers
 - Periodically report entry updates to parents and peers

Technical Point: Directory Queries

- When an IWS user desires to communicate with nodes not automatically discovered, the local MDN is queried
 - Queries can contain constraints on geographic location (e.g. within 50 miles) and/or services offered (e.g. dive team, bomb squad, search & rescue)
- If the local MDN does not contain the requested

and fixed-infrastructure deployments

- Nodes discover the presence of other nodes either through the Auto Discovery process or by querying a Mutualink Directory Node (MDN)

- All network nodes listen on this address and automatically discover the presence of other nodes belonging to their respective network that are currently active.

- Network nodes include: IWS, NIC, NMS, MDN

- Cache the results of queries as well as other MDN locations

- MDN topology can be both auto-discovered and provisioned
- Network Management Services (NMS) typically function as top-level MDNs
- Any IWS can act as a local or regional MDN* (either by configuration or by auto-election)

* The MDN is an extension of a standards-based LDAP server





OVERVIEW SOLUTION

Technical Point: Mutualink Security

- Control communications between all Mutualink nodes is encrypted and mutually authenticated using standards-based public-key cryptography.
- All media communications (voice, video, files, messages) are encrypted end-to-end using the highly-secure AES cipher (approved by the NSA for encryption of classified information), thereby preventing unauthorized access to any incident traffic
- Only external endpoints explicitly authorized may communicate with nodes within the Mutualink network
- Well-defined addresses, ports, and packet signatures make firewall configuration straightforward and secure
- Secure IPSEC tunnels may be used to place Mutualink nodes behind existing firewalls
- Suspicious network traffic is detected and can generate alerts to user-configurable locations
- Mutualink nodes may be segregated from existing LANs by using any combination of:
 - ⊙ Separate physical LANs or virtual LANs (VLANs)
 - ⊙ IPSEC/GRE tunnels between various locations

Technical Point: Reliability & Redundancy

- The Mutualink reliability design maxim:
 - ⊙ The failure of any one element shall not take more than one channel/interface out of service
- Since a peer-to-peer communication model is used (vs. a client-server model), the bulk of the reliability burden remains on the network.
 - ⊙ If any node fails, only that one node goes out of service.
- If a MDN fails (non-real-time failure, used only for searching for remote endpoints)
 - ⊙ Clients automatically query peer and/or parent MDNs
 - ⊙ Nodes and DSs cache previous query results
- If an NMS fails (non-operational failure)
 - ⊙ Nodes automatically report to secondary NMS

Technical Point: Standards Conformance

- Mutualink's approach is to use existing standards wherever feasible
- Standard protocols in use:
 - ⊙ SIP & RTP: Industry-standard VoIP protocols
 - ⊙ LDAP: Directory Service query/update protocol
 - ⊙ X.509: Common PKI certificate exchange format
 - ⊙ FTPS: File transfers between network elements
 - ⊙ HTTPS: Remote configuration and monitoring
 - ⊙ Proprietary protocols (when no suitable standards exist)
 - ⊙ Mutualink Control Channel (MCC): Used for auto-discovery and node status updates, etc.



OVERVIEW SOLUTION



REDEFINING INTEROPERABILITY

Controllable



Intuitive



Affordable



Mutualink, Inc.

Connecticut Office
1269 South Broad Street
Wallingford, CT 06492
(866) 957-5465

Research & Development Facility
238 Littleton Road
Westford, MA 01886
(978) 392-0040

Web: www.mutualink.net

E-Mail: info@mutualink.net