



Putting a CAP on Disparate Emergency Communication Systems

Monumental events – and a host of smaller-scale ones – point to the need for a more effective system to ensure that the general public, federal, state and local governments, and the private sector receive accurate and timely access to information in order to respond effectively to emergency situations.



■ *By Aviv Siegel*
AtHoc, Inc.

The single most important asset for decision makers and first responders is the ability to access information and communicate it to their teams and to the public.

Information is the antidote for an emergency. With the accurate and timely delivery of information, an emergency is defined and understood, enabling prompt reaction and effective countermeasures. Emergency management professionals call it “situational awareness.” Without information, emergencies grow in chaos and ambiguity, delaying a response and potentially increasing the exposure to and magnitude of any danger.

The terrorist attacks on September 11th, Hurricane Katrina and the shootings at Virginia Tech are a few of the high-profile events that illustrated this state of confusion for emergency personnel and the public.

On September 11th, the New York police and fire departments had to conduct massive and complex rescue operations with incompatible radio networks. The city's 9-1-1 system was overwhelmed with calls, and its operators did not have access to updates on the rapidly evolving situation, which resulted in the general public not getting good information or proper assistance. Many frustrated first responders reported that they received more information about what was happening from CNN than they did from their command structure.

Those tragedies revealed the consequences that result when communications and alerting systems are inadequate or compromised. Historically, emergency communications systems within the U.S. have been fragmented and isolated by technical and bureaucratic obstacles. No standardized alerting technology existed that could traverse federal agencies, much less interface with state and local agencies and the private sector.

Monumental events – and a host of smaller-scale ones – point to the need for a more effective system to ensure that the general public, federal, state and local governments, and the private sector receive accurate and timely access to information in order to respond effectively to emergency situations.

The urgent need to address this deficiency drove the proliferation of incompatible independent systems from government and private industry, with little to no thought about interoperability in protocol or technology. The predictable result was a landscape dotted with unconnected alerting systems with limited range, inadequate capability and questionable value. With the specter of severe consequences looming, action was urgently needed to correct the situation.

In November of 2000, the National Science and Technology Council (NSTC) produced a report entitled “Effective Disaster Warnings.” It contained the recommendation that a standard system should be developed to collect and automatically relay all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems.

In 2001, using the recommendations of the NSTC report, an independent group of emergency managers began developing what has become known as the Common Alerting Protocol, or CAP, an XML-based data format for exchanging public warnings between alerting technologies.

After field tests, in March of 2004 the first draft of the CAP 1.0 specifications was approved by the Organization for the Advancement of Structured Information Standards (OASIS), a not-for-profit, international consortium that oversees the development, convergence and adoption of e-business standards.

The adoption of the Common Alerting Protocol represented a quantum leap in the progression of multi-channel alerting systems with reliable interoperability across many domains. It provides a standardized way for existing and new emergency alerting technologies to communicate with each other, allowing technologies such as network-centric emergency alert systems to interoperate with traditional giant voice systems and with the National Emergency Alert System.

Last year, the International Telecommunications Unit (ITU) recognized CAP as an emerging global standard for alert and notification systems. The CAP structure offers a number of substantial benefits for all levels of government agencies, private industry and the public at large, including:

- Enhanced interoperability
- A single source interface for delivering alerts through multiple, disparate systems
- A national alerting infrastructure that can expand, upgrade or even replace, existing applications without disruption
- A real-time database of all warnings given at different levels to better coordinate utilization of assets

CAP is now being used as the foundation for the Integrated Public Alert and Warning System executive order, an all-hazard,

all-media, national warning architecture being developed by the Department of Homeland Security, the National Weather Service and the Federal Communications Commission.

In addition, OASIS continues to extend the architecture of standards for emergency situations. The consortium introduced the Emergency Data Exchange Language (EDXL) – a framework that provides better control over the flow of messages between systems during an emergency. EDXL itself is using the CAP standard as one of the possible conduits for emergency alerts.

Alerting systems will continue to evolve as the dynamic nature of a threat or crisis becomes more complex. The Common Alerting Protocol movement will continue to expand and evolve as new alerting technologies emerge within its structure. Ultimately, the goal of CAP is to provide a communication reliable infrastructure/standard for an effective warning system.

By standardizing protocols for emergency system operability, first responders and the public are much more likely to receive the timely and helpful information they need if and when an emergency situation confronts them.

Re-published with Permission

About the Author:

Aviv Siegel is the chief technology officer for AtHoc, a pioneer and leader in network-centric emergency notification systems. He is also a member of the OASIS Emergency Interoperability Committee working to promote the adoption of CAP to ensure interoperable emergency communications.

In an emergency, these people will rely on you.

YOU CAN RELY ON US.



Over 1,000,000 DoD personnel already rely on AtHoc.

AtHoc IWSAlerts™ reliably delivers emergency alerts to thousands of people via desktops, phones, BlackBerry devices, pagers and mass communication devices in a matter of seconds.

Transform your IP network into a unified mass notification system during an emergency for your entire organization.

AtHoc IWSAlerts — a proven enterprise-class emergency notification solution you can rely on.



To learn more, visit
www.athoc.com/relyonus