An Advanced EAS Relay Network Using the Common Alerting Protocol (CAP)

by Art Botterell

The Emergency Alert System (EAS) is the nation's best-known public warning system, but recent studies have identified limits inherent in its design. Other systems augment EAS, but have many of the same limitations. A Common Alerting Protocol (CAP) has been developed through an international standards process. A design concept and non-proprietary architecture for a consolidated public warning network based on EAS and CAP is described. The approach described can provide enhanced security, improved warning system coordination, simplified operational procedures and reduced costs without disrupting existing EAS facilities or programs.

The Advanced EAS Relay Network

The Advanced EAS Relay Network (AERN) will improve EAS performance and security with a digital "overlay" system based the new Common Alerting Protocol (CAP) and digital audio formats. It will also improve the coordination of EAS with other alerting systems in delivering complete, consistent and coordinated warning messages to the public. AERN will combine the security and robustness of digital transmission with the flexibility and interoperability of a standards-based communications.

AERN is not a product; it is a non-proprietary architecture that can be implemented voluntarily by any agency, broadcaster or system integrator without licensing or patent restrictions, without disrupting existing EAS relay arrangements, and without any changes to existing government regulations or policies.

AERN will provide:

- A single secure mechanism for authorized officials to control and coordinate multiple warning systems, including but not limited to EAS;
- Simple user "console" software that aids alert originators in composing complete and effective EAS messages and encodes those messages as CAP data and digital audio;
- Automated interfaces that authenticate and select CAP-based EAS alerts and broadcast them, aurally and visually, via existing EAS encoders;
- Reliable private and public digital networks[1] in three operational modes to link originators to broadcasters and cable operators;
- State-of-the-art security to ensure message authenticity and integrity, even over public networks;
- Cost-effective implementations based on open, non-proprietary technical standards in stand-alone applications and within other emergency management and public safety information products; and,
- Full compatibility with existing EAS technologies, policies and regulations[2].

[1] Private and public data networks have proven remarkably resilient under disaster conditions, e.g., the 9/11/2001 terrorist attacks and the 2003 Northeast electrical blackouts: see National Research Council, "The Internet Under Crisis Conditions: Learning from September 11," (2003).

[2] The Federal Communications Commission's rules for EAS comprise Title 47, Part 11 of the Code of Federal Regulations.

The Challenge of Effective Public Warning

During emergencies effective public warnings can save lives, prevent injuries, reduce property losses and control fear. Effective public warning requires systems and procedures that:

- Reach everyone at risk in a timely fashion;
- Deliver understandable and useful warning messages;
- Maximize recipient confidence in, and thus response to, warning messages; and,
- Minimize the occurrence and impact of failures and false alarms.

Decades of academic research and practical experience regarding warning systems and public behavior when confronted with warnings have been compiled and summarized in recent reports by the National Science and Technology Council[3] and the national non-profit Partnership for Public Warning[4]. Among the findings of these studies, two are crucial:

- Effective warning delivery involves the coordinated and consistent use of multiple channels of communications; and,

- Effective warning messages have certain key components that frequently are missing from warnings issued using current procedures.

In addition to their immediate life-saving value, public warnings can have significance far beyond their target areas. Systematic monitoring of real-time data about warnings issued at the local level can provide valuable inputs to regional or national "situational awareness" programs.

The Emergency Alert System

The Emergency Alert System (EAS) is a national public warning and public information network based on the facilities of radio and television broadcasters and the cable television industry. (A comprehensive history and assessment of the EAS has recently been compiled by the Partnership for Public Warning.[5])

The primary purpose of EAS is to enable national authorities to communicate with the public in time of national emergency; it is for this purpose that EAS is mandated and maintained by federal regulation. Although fortunately it has yet to be called upon to perform its national security mission, EAS is used hundreds of times every year in an ancillary role of aiding local officials in alerting and informing local populations about various local threats including environmental, technological and man-made emergencies (e.g., AMBER Alerts regarding child abductions.)

From a functional point of view EAS has three basic components:

- **Originators** – Officials and agencies with public warning responsibilities that decide when to activate (or, in the local case, to request activation of) the EAS and provide message content;

- **Broadcasters and Cable Operators** – Owners and operators of the facilities for delivering EAS messages to the public; and,

- **Relay Networks** – The facilities by which EAS messages are transmitted from the originators to the broadcast and cable facilities.

[3] National Science and Technology Council, "Effective Disaster Warnings," (2000)
[4] Partnership for Public Warning, "A National Strategy for Integrated Public Warning Policy and Capability," (2003)
[5] Partnership for Public Warning, "The Emergency Alert System (EAS): An Assessment," (in final revisions at this writing)

In practice this pattern is complicated by the fact that broadcasters frequently provide major portions of the local relay network, and in some areas are even called upon to perform EAS message origination.

State and local authorities have come to rely heavily on EAS, both because of the extensive reach of broadcast media and cable television, and for the economies achieved though "dual use" of facilities already in place for the federal mission. These voluntary efforts by broadcasters, cable operators and state and local emergency planners have saved many lives and reduced losses on many occasions. However, the EAS technology has some inherent limitations that affect local users:

- EAS is an audio-based system. Although a data header that holds encoded targeting and categorizing information accompanies the EAS audio, the header information is extremely limited in detail. It cannot, for example, provide captioning of the complete alert message for deaf and hearing-impaired TV viewers. Nor can it be used to activate highway signs or other text-based alerting systems.

- Especially during severe emergencies, EAS audio messages often are composed "ad lib" by originators who lack the time or the experience to compose complete and effective warning messages "on the fly." Even where scripts have been prepared in advance, they frequently are unavailable when needed and may not always be suitable for an unexpected event. (In the worst case originators might actually defer issuing a warning for fear of doing it incorrectly.)

- EAS operates separately from other public warning systems. To achieve the audience reach, technical reliability and corroboration required for a public warning to be effective, the originator must execute not only the EAS activation procedure but also several other procedures to activate several other systems. This creates an additional workload on the originator just when the originator has the least time to spare. Frequently the result is that other systems are not used or their messages are not consistent in content and timing.

- Local EAS relay networks, particularly the links to originators, use various technologies and channels and may not always be adequately secured against interference or "spoofing" attacks.

- EAS relay networks are designed for "top-down" dissemination of messages from an authoritative source to the public. They do not provide a mechanism for tracking local warning activity at the state, regional or national levels.

NOAA Weather Radio and Local Warning Systems

The NOAA Weather Radio (NWR) system of VHF radio transmitters controlled from National Weather Service offices provides another large-scale public alerting capability. NWR signals cover the vast majority of the nation's population. Many NWR receivers can be activated automatically using the same data header codes used in the EAS. Although originally installed specifically for weather warnings, NWR has been used as an all-hazard warning system in a number of areas. It also serves as part of the EAS relay network in some parts of the country.

Supplementing these two national public warning systems are a wide variety of other technologies that have been deployed by local jurisdictions and private, including:

- Sirens and public-address systems;
- Telephone notification systems;
- Programmable highway signs and other public display systems;
- Travelers Information Service low-power radio transmitters;
- Wireless systems utilizing pagers, cell phones and other devices; and,
- Internet-based alerting systems using e-mail, instant messaging, web and other protocols.

Each of these systems has strengths and weaknesses and especially when used in tandem they can be highly effective. However, they all share a common set of limitations with EAS:

- **Limited reach** – No one technology can reach everyone under all circumstances;
- **Technical vulnerability** – Any single technology can be vulnerable to deliberate attack or unexpected technical failures;
- **Unique procedures** – Each system has its own unique activation tools and procedures; and,
- **Limited impact** – Members of the public tend not to act on the first warning message they receive. (After all, it might be a false alarm.) If a warning from one system is not confirmed by other sources, not only does research indicate that the particular warning message is likely to be ignored, but the credibility of that source may also be compromised for the future.

The key to effective public warning lies not in perfecting any one system or technology, but in using all available means of communication in a coordinated and efficient way.

The Common Alerting Protocol

The Common Alerting Protocol (CAP) is a simple data format for exchanging all-hazard emergency alerts among all kinds of networks and warning systems. By putting alerts from different sources into a single format CAP also facilitates the detection of patterns in local warning activity that might reveal an otherwise undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

In November 2000 the National Science and Technology Council (NSTC) issued a survey study and report on "Effective Disaster Warnings." It recommended that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems."

Acting on that recommendation, an international working group of more than 130 emergency managers and information technology and telecommunications experts convened in 2001. Beginning with specific recommendations from the NSTC report, the Common Alerting Protocol Working Group refined the CAP format through detailed reviews and a series of field trials and exercises. In 2003 the national non-profit Partnership for Public Warning sponsored the draft CAP standard into the OASIS standards process. In August 2003 the OASIS Emergency Management Technical Committee, representing leading providers of emergency management software, adopted the CAP 1.0 specification as a Committee Standard[6].

Based on the XML data exchange language, the non-proprietary CAP alert message format is compatible with new communications technologies such as Web Services, as well as with existing data formats including the Specific Area Message Encoding (SAME) used for EAS and NWR. It offers enhanced capabilities including:

- Much more complete and detailed information than earlier alert formats;
- Flexible geographic targeting using latitude/longitude shapes and other codes;
- Multilingual and multi-audience messaging;
- Phased effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- A facility for digital encryption and signature capability; and,
- A facility for including digital images and audio.

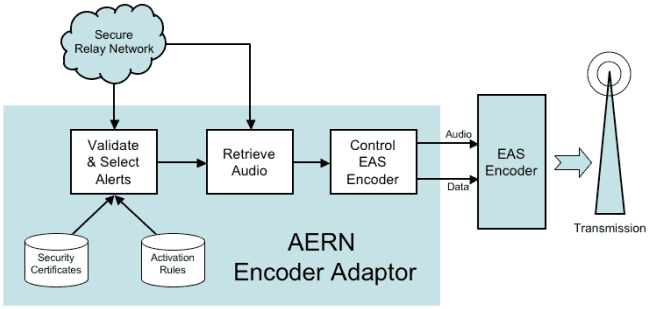
[6] Organization for the Advancement of Structured Information Standards (OASIS), Emergency Management Technical Committee; "Common Alerting Protocol v 1.0," (12 August 2003)

CAP can be used to reduce warning system costs and operational complexity by eliminating the need for multiple custom interfaces to the many sources and systems involved in all-hazard warning. The CAP message format can be converted to and from the internal data formats of sensor and alerting systems, providing a basis for a technology-independent national "warning internet."

The AERN EAS Encoder Adaptor

Broadcast and cable operators use a device called an "encoder" to format EAS broadcasts automatically. This device assembles the EAS data header, which includes codes for message category, target area, transmission and expiration time and source identifier, and then sequencing the broadcast of that header, designated attention tones, the audio message, and an end-of-message data signal.

To originate an EAS broadcast using current technology, an originator enters the header information either through controls on the encoder unit itself or via a remote control attached by a data link. Then the originator records the audio portion of the message and triggers the automatic broadcast sequence.

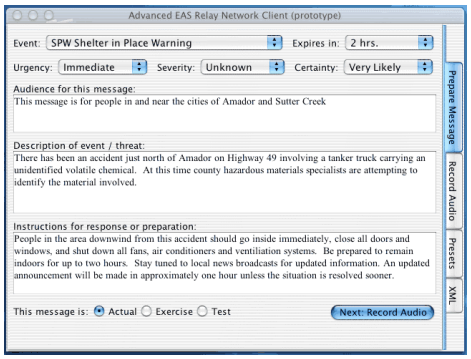


The AERN Encoder Adaptor connects to the encoder in the same way as an ordinary encoder control unit. It monitors the relay network for incoming AERN (CAP) messages, authenticates and selects received alerts by location and category, retrieves the recorded audio, and then extracts EAS header data from the CAP message and triggers the EAS encoder. Transmission can be automatic or it can require manual operator approval, as dictated by station/system policy.

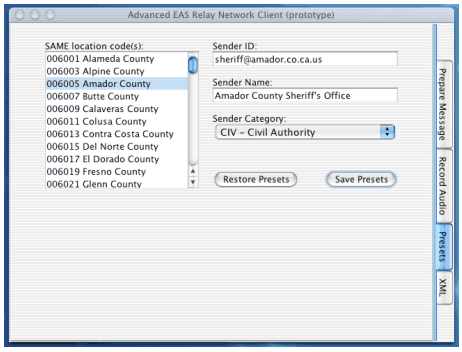
The AERN Encoder Adaptor can be implemented as an add-on device that attaches to existing EAS encoders. It also can be integrated within future models of the EAS encoders themselves. Similar adaptors can be deployed for other warning systems and devices (sirens, telephone notification systems, etc.) to provide coordinated activation using a single alerting message.

The AERN Origination Console

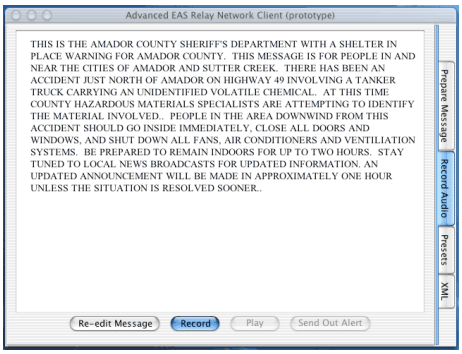
At the agency originating the EAS message, software on an ordinary networked computer provides a series of computer input screens to guide the operator through the steps of composing a complete and effective warning message. This "console" can be implemented either as a stand-alone application (as in the prototype screens shown here) or as a module within some other software package (e.g., a computer aided dispatch system or an emergency management software package.)



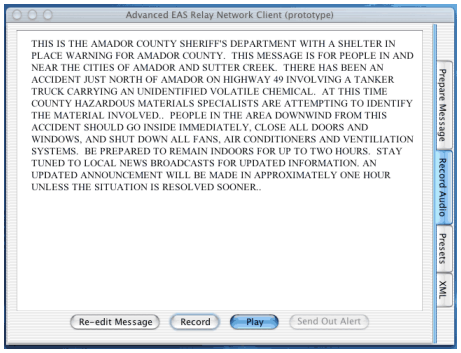
The main message entry screen prompts the originator to compose the elements of the EAS message. Additional parameters used in the CAP message format, such as the urgency, severity and certainty values, can be adjusted as necessary, although in most EAS applications the supplied default values will be correct.



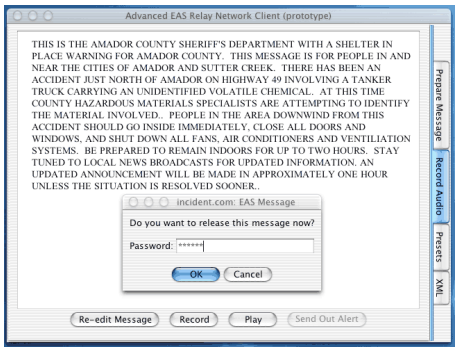
Default parameters can be set in advance and stored. These might include targeting code or codes for the originator's jurisdiction, as well as the originator's agency name, category and identification codes. These default values can be updated from time to time and overridden if necessary for a particular EAS alert.



The edited message is displayed in the form of a script, as in this simulated example. The originator reads this script into either the computer's built-in microphone or a separate microphone attached to the computer's audio input.



After recording the originator plays back the audio recording to make sure it is clear and conforms to the message text. The message may be re-recorded as necessary.



Once the originator is satisfied with the recorded version the alert is released to broadcasters and cable operators over the relay network.

This simple step-by-step process assists the originator in composing a clear and complete alert message that can also simultaneously activate other alerting systems. It also ensures that the recorded audio is accompanied by the complete text of the message in a form compatible with television captioning, text messaging and public display systems. In the future the message text might be input directly to text-to-speech synthesis systems like those used in the NOAA Weather Radio system.

The AERN Secure Relay Network

AERN supports three complementary modes of transmission from message originators to broadcast stations and cable system "head ends":

- **Direct circuit** – The originator's console establishes an encrypted data connection directly to each broadcast/cable outlet's Encoder Adapter, and transmits the CAP data and the digital audio directly to each unit. This is the most rapid mechanism, and allows constant monitoring of network status. However, it places the greatest demands on network capacity at the origination point. It can also be relatively complex to administer, especially in areas where there are numerous potential originators and numerous broadcast and cable outlets.

- **Secure server** – The console program "uploads" the CAP text and digital audio file to an off-site secure Web server. Each Encoder Adaptor "polls" the server several times a minute to retrieve any new alerts. Authentication of originators can be centralized at the server, and the same server can trigger non-EAS warning systems simultaneously. AERN servers can be established at the local, state, regional or national level, and alerts can be forwarded automatically from one server to another as required.

- **Data broadcast** – The CAP text and digital audio are forwarded to a secure "gateway" computer and from there are broadcast over a one-way circuit such as a satellite or digital TV transmission. The transmissions are repeated as long as the message remains in effect.

Each CAP message contains a unique message identifier, so these modes can be used in any combination without triggering duplicate EAS broadcasts.

The security provisions in AERN focus on ensuring:

- **Authenticity** – The message actually came from the ostensible source;
- **Authority** - The source is an authorized EAS originator; and,
- **Integrity** - The text and audio were received exactly as sent.

AERN applies two layers of security to achieve these goals:

- **Transport-layer encryption** – All network connections used to transmit EAS messages are secured using commercial-grade encryption.

- **Digital signatures** – Using standard public-key methods, each CAP message is "signed" with an encrypted data that can be used to verify that a) it came from the source claimed, and b) the text has not been modified. A separate "digest" code in the CAP message can be used to verify that the accompanying audio file also is authentic and unmodified.

In addition to authorization checks at AERN servers and data-broadcast gateways, each Encoder Adaptor can also verify received messages against a set of security certificates for authorized originators.

In addition to the modern Internet, which has proven surprisingly resilient during disasters[7], AERN also can utilize private data networks operated by government or industry. And while AERN will extend and improve officials' access to EAS and other warning systems, it will not interfere with existing (mostly analog) federal, state and local relay network arrangements. AERN will increase the technological diversity and reliability of EAS relay architectures as well as the quality of EAS messaging and integration with other warning systems.

[7] National Research Council, *op. cit.*

Implementing AERN

AERN is a low-cost, low-risk option for improving EAS and public warning in general. AERN will deploy in parallel with existing systems without disrupting them. No regulatory or policy changes will be required. The required infrastructure (computers, network connections, etc.) is widely available and generally already in place. And the additional technologies (CAP and streaming audio formats) have been developed, standardized and released for commercial implementation without licensing fees or restrictions.

Development and deployment of AERN can be achieved in three phases, beginning immediately:

1. Rapid initial development and technical testing in cooperation with EAS equipment vendors, broadcasters and emergency management / public safety personnel[8]. This process might be conducted under the auspices of a neutral non-profit organization representing government and industry;

2. Limited voluntary field trials and evaluations in parallel with existing EAS relay networks and other warning systems (especially NOAA Weather Radio);

3. "Productization" with the AERN functionality increasingly integrated into next-generation EAS equipment and emergency management / public safety systems.

Strategic Implications of AERN

AERN represents a fundamental redirection of the nation's strategy for public warning systems. Instead of a patchwork of separate warning systems, each devised for a particular hazard or region, AERN will drive the development of an integrated warning capability at the local, state, regional and national levels. It will leverage investments in warning technology and procedures across all hazards and all communities, resulting in:

- **Improved outcomes** – Coordinated use of multiple public and private warning systems, along with improved quality of warning messages, will yield improved reach and reliability, while increasing public compliance with individual warning messages and public support for public warning programs.

- **Increased flexibility** – Not all warnings issued using CAP will necessarily activate the broadcast and cable facilities of EAS. The flexible coding inherent in CAP allows flexible use of a wide range of dissemination options, with EAS activation itself used only in circumstances deemed appropriate under local, state and national EAS plans. Thus the deployment of AERN could result in increased public warning activity and yet fewer EAS activations.

- **Reduced costs** – The use of a common interface will reduce development and system integration costs for all kinds of public and private warning systems. Meanwhile, the coordinated use of multiple systems for warning delivery will reduce the need for builders of individual warning systems to overextend their technology or funding in an attempt to achieve coverage, reliability or effectiveness goals alone.

With AERN the Emergency Alert System can continue in its long-standing role as the backbone of the nation's public warning capability, enhancing it with the best features of 21st century technology while preserving what already works.

[8] A prototype implementation of AERN software has been developed by the author and a number of commercial software products are currently being enhanced with CAP interfaces that could be used to implement AERN.