Digital Alert Systems

White Paper

State/Local CAP EAS Systems

Challenges for Broadcasters Facing State, Local and Federal CAP EAS Systems & Interoperability requirements

Introduction: Looking for Federal, State and Local Networks

First of all, "don't panic." The right next-generation CAP EAS equipment choices can facilitate interoperability with a range of local, state and Federal CAP alerting networks. Equipment designed with the flexibility to handle a broad range of Federal, state and local system requirements will facilitate a relatively painless transition to the next generation CAP EAS environment.

This white paper addresses two basic questions: where CAP alerts will come from, and the practical implications for the radio and television broadcaster.

Much of the discussion and debate seems to have been focused on Federal efforts to deploy their own systems, principally the Federal Emergency Management Agency's "Integrated Public Alert and Warning System" (FEMA IPAWS), as well as the National Weather Service's own CAP initiatives. FEMA IPAWS appears to be headed towards operational status by mid to late 2011. The National Weather Service already has their own web-page of CAP alerts, with more developments to enable the two Federal agencies to interoperate.

Perhaps the more striking development, however, is the fact that there are a growing number of State and Local CAP EAS networks across the United States. These state and local areas are deploying their own advanced EAS capabilities using the same Common Alerting Protocol mandated at the Federal level. However, many of these networks are incorporating very different approaches to the relay of data than the Federal systems. Many of these data networks use satellites and/or the Internet, and some areas are even looking at alternative wireless ways of distributing CAP EAS.

What This Means for the Broadcaster

Bottom line, the proliferation of these various CAP networks will likely impact IT design strategies to accommodate these disparate systems, as well as the options broadcasters need to evaluate when considering CAP EAS encoder/decoders.

One way to look at this new generation of CAP EAS unit is that they are basically peripheral units placed at the edge of a network. Or in this case, at the edges of overlapping but distinct networks. Therefore, broadcasters should keep in mind that they will require CAP EAS encoder/decoders that are versatile

585-765-1155 | fax 585-765-9330
100 Housel Ave. | Lyndonville | NY | 14098
www.digitalalertsystems.com

enough to handle the demands of interoperating with a wide range of CAP-based systems – not just FEMA's Integrated Public Alert and Warning System (IPAWS), but the growing number of state and local CAP systems.

Moreover, broadcasters should take care to consider CAP EAS units that actually fit with systems the state already has in place -- or is planning. In some cases, this may require some conversations and coordination that quite frankly have not yet happened. In other cases, state agencies have already chosen systems for distribution of emergency messaging that not all cable broadcasters or broadcasters may even be aware of yet.

Where to Look for CAP Messages

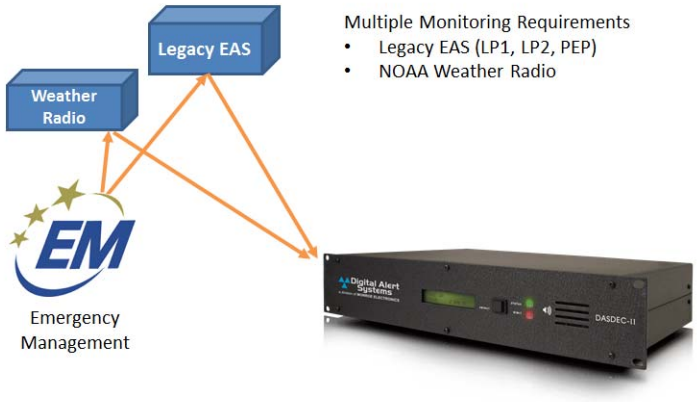
With the adoption of next generation CAP alerting capabilities, Federal, state and local agencies will be issuing EAS alerts via an expanded range of systems. These CAP messages will come from different governmental sources, over different transport media, with varying differences in how CAP EAS units must access those systems.

In addition, CAP EAS units must also be capable of monitoring the existing EAS system. As the FCC has made clear on numerous occasions, the existing EAS system is not going away even while the next generation CAP EAS is being deployed. The two capabilities will coexist, providing needed levels of redundancy.

A well designed and properly configured CAP EAS encoder/decoder can greatly facilitate making and managing the connections to these disparate CAP alerting sources. The CAP EAS unit should support the configurations to interface with any number of CAP sources, whether that means interfacing with Internet, satellite or wireless data transport networks, and whether that means supporting push or pull services. Optimally, support for these variations should be preconfigured in the CAP EAS encoder/decoder.

In Figure 1, we illustrate the current (or traditional) EAS monitoring scheme, based on radio relays. This legacy EAS system is not being shut down with the advent of CAP EAS systems. Rather, legacy EAS will run in parallel with next generation CAP EAS for some time to come. **Broadcasters will continue to require monitoring capabilities for legacy EAS, therefore requiring next-generation equipment to also be FCC certified.**

Figure 1: Traditional EAS Monitoring

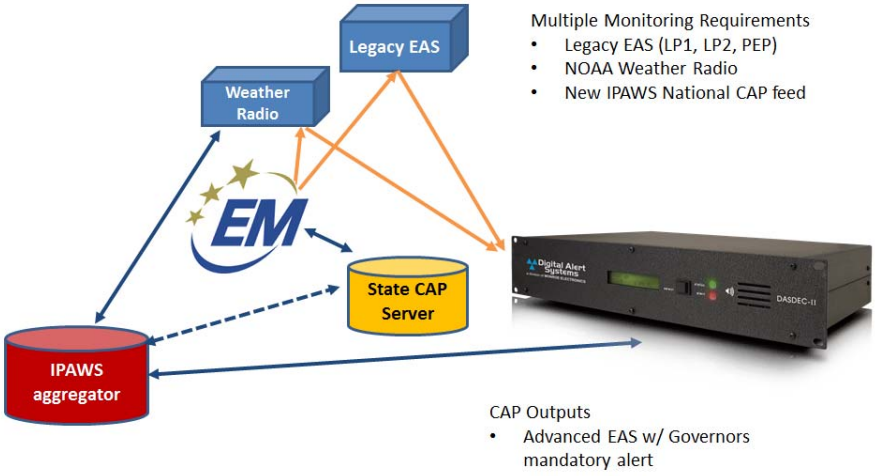


At the same time, a new layer of alert distribution in a very different format (data, rather than EAS tones) has come into play. One such network is FEMA's IPAWS system. IPAWS system will aggregate authenticated CAP alert messages from the National Weather Service, as well as state and local emergency management. The addition of the IPAWS distribution system is illustrated in Figure 2.

The reception of alerts from IPAWS must be performed by a equipment that is not only FCC-certified (Part 11), but has successfully completed IPAWS Conformance Assessment. Equipment that has passed the IPAWS conformance testing can demonstrate this with a Suppliers Declaration of Conformity (SDoC), that they must file with the government.

Figure 2: Expanded EAS CAP Monitoring

Legacy EAS + IPAWS CAP EAS



As depicted in Figure 2, State (and local) authorities will need to acquire some form of CAP origination capability (which may be a simple software package). However, just as with the EAS CAP encoder/decoder, that software must also complete the IPAWS Conformity Assessment process.

Importantly, the State CAP server – not the IPAWS server - will also act as the host for any EAS audio (voice) or multimedia that the emergency manager wishes to transmit. In operation, this means that the broadcaster's CAP EAS encoder/decoder will need to communicate with two distinct servers. The encoder/decoder will poll the IPAWS aggregator for the XML (text) portion of the alert. If there is an audio file present, the CAP EAS encoder/decoder will *also* need to interact with the state CAP server to seek out and insert the audio into the EAS message. Figure 2 shows the relationships and the interactions between a state CAP server and the IPAWS aggregator.

Now, let's go one step further. In addition to monitoring the IPAWS aggregator for alert messages, a significant number of states and localities have – or are planning – their own capabilities to transmit CAP EAS messaging. We add this layer of complexity in Figure 3. While a number of states may utilize IPAWS as a primary means of disseminating CAP messages, a very significant number of states will utilize their own systems as a primary means, and interface with IPAWS as a backup or secondary relay.

Figure 3: Expanded EAS CAP Monitoring
Legacy EAS + IPAWS + State/Local CAP EAS

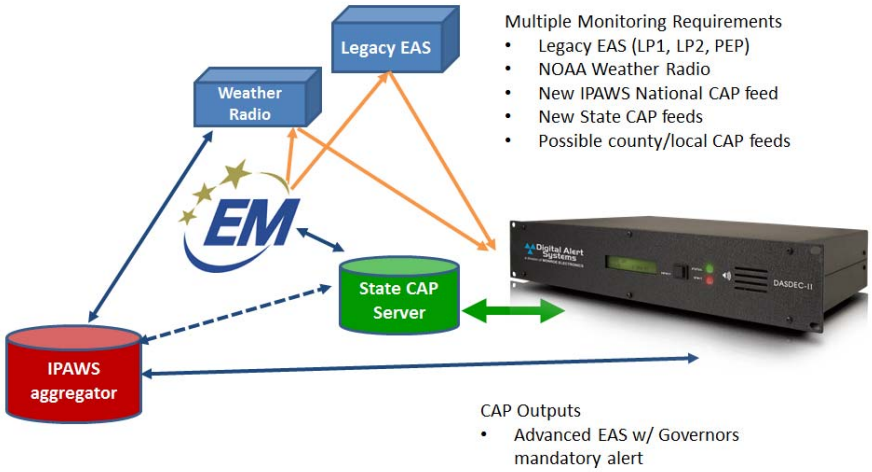
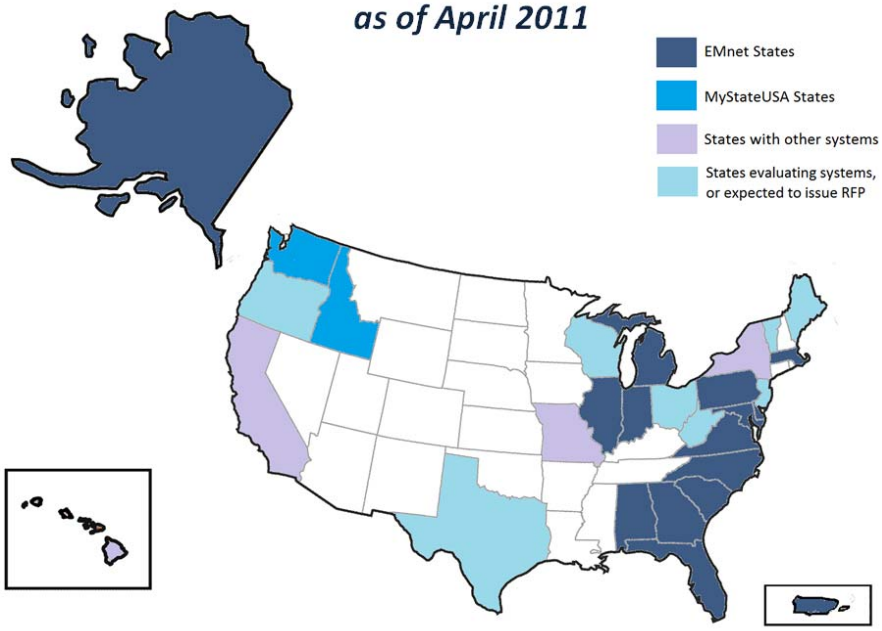


Figure 3 adds a direct link between the State CAP server and the broadcaster's encoder/decoder. This relationship adds a range of required capabilities for the CAP EAS encoder decoder. As discussed in the section below, there is already a considerable number of State (and local !) CAP systems in the field, using a diverse range of technologies and approaches to deliver CAP alerts.

State CAP EAS Systems

By mid-2011, broadcasters will be challenged with a hierarchy of CAP alert network sources in *at least 19 states*. The geographic reach of these 19 state systems is illustrated in Figure 4. In addition to these 19 states, at least 6 additional states are actively evaluating options for state and local CAP alert origination and distribution.

Figure 4: State CAP EAS Systems
as of April 2011



A summary table of the 19 known State CAP systems is detailed in Figure 5, breaking out transport methods and system providers. Notably, 14 of these states use a combination of satellite and Internet-based delivery, all sharing the same managed network provider. The remaining 5 states rely on the Internet for delivery, but even here there are key distinctions. Some Internet-based systems reply on Virtual Private Networks, requiring software and authorization for the CAP EAS unit to connect with the network. Some Internet based systems dedicate a special web page or resource to make alerts available. Some systems use push technologies. Others rely on pull methodologies.

Figure 5: State CAP EAS Systems
selected states as of April 2011

State	INTERNET	SATELLITE	PROVIDER
ALASKA	●	●	EMnet
CALIFORNIA	●		EDIS
DELAWARE	●	●	EMnet
DIST OF COLUMBIA	●	●	EMnet
FLORIDA	●	●	EMnet
GEORGIA	●	●	EMnet
HAWAII	●		IWSAlerts
IDAHO	●		MyState
ILLINOIS	●	●	EMnet
INDIANA	●	●	EMnet
MARYLAND	●	●	EMnet
MASSACHUSSETTS	●	●	EMnet
MICHIGAN	●	●	EMnet
NEW YORK	●		NY Alert
NORTH CAROLINA	●	●	EMnet
PENNSYLVANIA	●	●	EMnet
SOUTH CAROLINA	●	●	EMnet
VIRGINIA	●	●	EMnet
WASHINGTON	●		MyState

The satellite based system currently used in 14 of these states is called EMnet, provided by Comlabs. At least 2 to 3 additional states are expected to adopt EMnet by late 2011.

Additional EMnet states will be provided the same satellite and Internet access options. Some of the features of the EMnet system include encryption of messages and data feeds, remote acknowledgments, system monitoring, and assured message delivery. States currently using the EMnet system include Florida, Georgia, South Carolina, North Carolina, Virginia, Washington DC, Maryland, Delaware, Pennsylvania, Massachusetts, Michigan, Illinois, Indiana, and Alaska.

We will provide additional analysis of interface requirements with EMnet further below, because that system is the most frequently encountered state EAS CAP system.

Some other states have pursued a range of Internet based options. Washington and Idaho, for example, utilize a hosted web-based service called MyStateUSA. California and New York have opted to have CAP server capabilities custom built for their requirements. In these states, CAP EAS units poll their respective web servers at regular intervals for updates. However, the specific manner of the CAP data is made available differs somewhat from system to system.

These differences require CAP EAS units be able to handle each of these methods. In some cases, this will require the manufacturer to coordinate with the system provider on specific details.

State and Local Case Study: Comlabs EMnet

As a case study, the Comlabs EMnet system will be examined, both because it is the most prevalent State and Local CAP EAS network, but also because it poses a number of challenges to broadcasters by communicating via both Satellite and Internet. Again, the States in which EMnet is currently deployed include Alabama, Alaska, Delaware, District of Columbia, Florida, Georgia, Illinois, Indiana, Maryland, Massachusetts, Michigan, North Carolina, Pennsylvania, Puerto Rico, South Carolina, and Virginia – with two to three additional states expected to adopt the system in the near future.

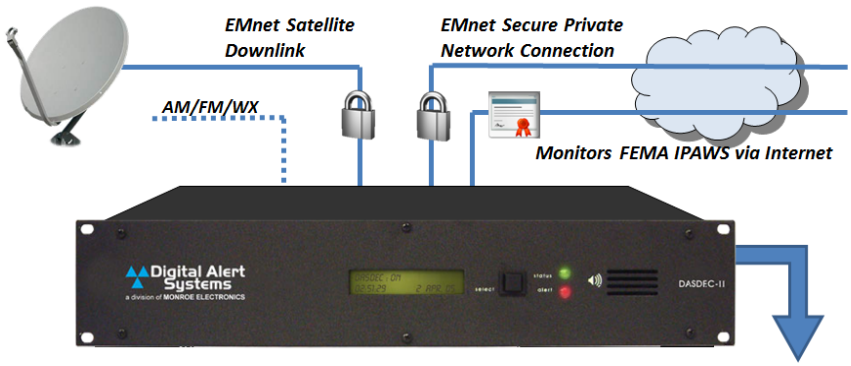
In some cases, EMnet has to date been deployed at key EAS sites (LP-1s and LP-2s) for example. In other states – notably Pennsylvania, Maryland and Florida – EMnet has been deployed widely across broadcast and cable TV sites. In either case, one can expect EMnet connections to extend out to the remaining cable TV and broadcast sites, with the adoption of the CAP mandate.

Broadcasters may be asked to monitor EMnet via satellite with an Internet return path or via the Internet only. The satellite equipment (1 meter dish, mount, cable, etc.) may, in many cases, be provided to the broadcasters under a government grant.

The satellite equipment will need to connect with one of two devices. Broadcasters can connect directly with EMnet with an enabled Digital Alert Systems DASDEC. Sites without a DASDEC can connect with an EMnet terminal – called the EM-Link.

Sites with an integrated DASDEC can enjoy a range of operational and cost efficiencies. As depicted in Figure 6, an EMnet enabled DASDEC contains the required EMnet satellite receiver and EMnet software to communicate with EMnet servers via both satellite and the Internet. This same single box solution is capable of monitoring the FEMA IPAWS aggregator, since it also possesses the required Declarations of Conformity. In addition, as an FCC-certified EAS encoder/decoder, the DASDEC provides the capability of including three radios within the single unit to monitor the legacy EAS.

Figure 6:
DASDEC-II fully integrated configuration for EMnet, EAS and FEMA IPAWS monitoring



As Figure 6 illustrates, the DASDEC is configured to receive the secure EMnet satellite communication, while also supporting secure communication with EMnet via Internet. These Internet communications include CAP alert delivery (for redundancy), as well as system monitoring, alert verification and acknowledgments, and other core EMnet management functions.

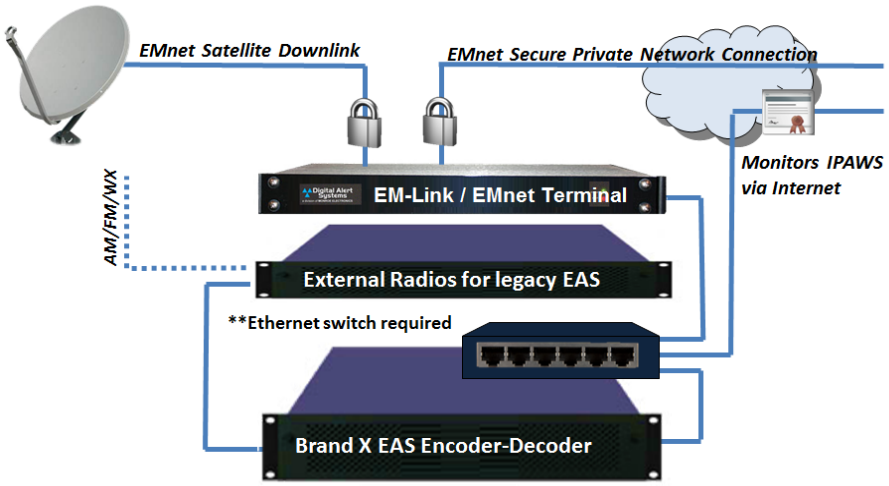
Because of its ability to integrate full EMnet functionality in an FCC-certified and IPAWS conformant device, the DASDEC has been adopted by EMnet as a device of choice for the cable TV and IPTV industry by Comlabs, the EMnet managed network provider. In a development that impacts at least 14 states, Digital Alert Systems and Comlabs launched a strategic alliance to extend the interoperability of the DASDEC CAP EAS products with the largest satellite and Internet CAP-based warning system in North America. The DASDEC is an authorized integrated CAP receiver and EAS encoder/decoder for the EMnet system, providing full support for both CAP and EMnet's advanced network monitoring and control capabilities.

Alternatively, broadcasters may elect to utilize other CAP EAS equipment in their plant. Let's examine how alternatives will need to address interoperability with EMnet, as well as the very CAP upgrade process itself.

Assuming the alternatives have passed the required FEMA IPAWS conformity testing, the expected digital connections for one brand of CAP encoder/decoder is depicted in Figure 7. This unit (Brand X) requires an external satellite receiver and management device (the EM-Link / EMnet Terminal) to perform the State and Local alert reception, acknowledgment, and system monitoring processes integrated into the single DASDEC unit above.

Because the unit illustrated below provides a single Ethernet LAN port, an additional Ethernet switch is required to manage separate Ethernet inputs. The unit illustrated below also requires external radios for monitoring legacy EAS.

Figure 7:
Brand X Configuration
for State EMnet and Federal IPAWS monitoring

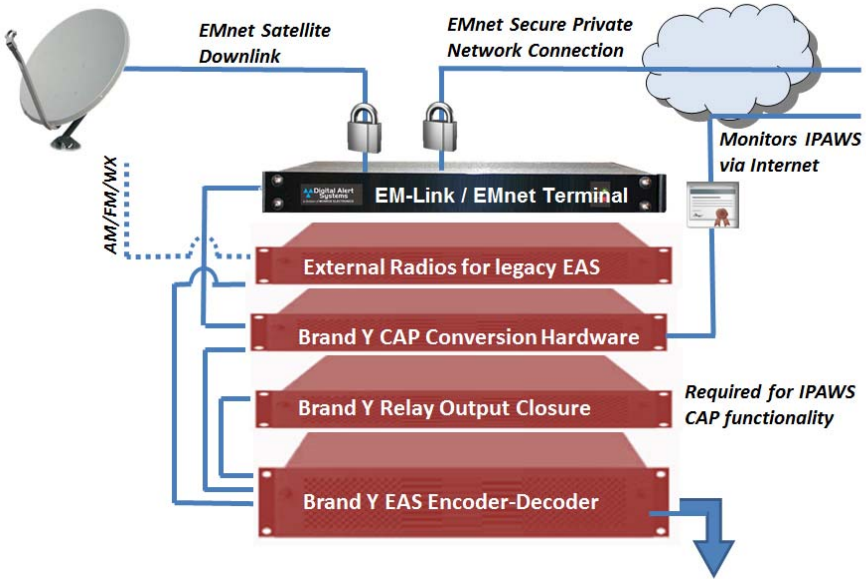


The CAP upgrade path for another model of EAS encoder/decoder is rather complex. Importantly, it is not known if this solution (Brand Y) has met the requirements of the IPAWS conformance tests. This solution necessitates several physical device additions to approach compliance with CAP data requirements.

As illustrated in Figure 8 below, this configuration requires at least two devices to support CAP compliance, including a CAP converter and a proprietary relay output device to force the legacy encoder-

decoder to respond to certain unique CAP capabilities. This will impact operational complexity, maintenance requirements, and costs.

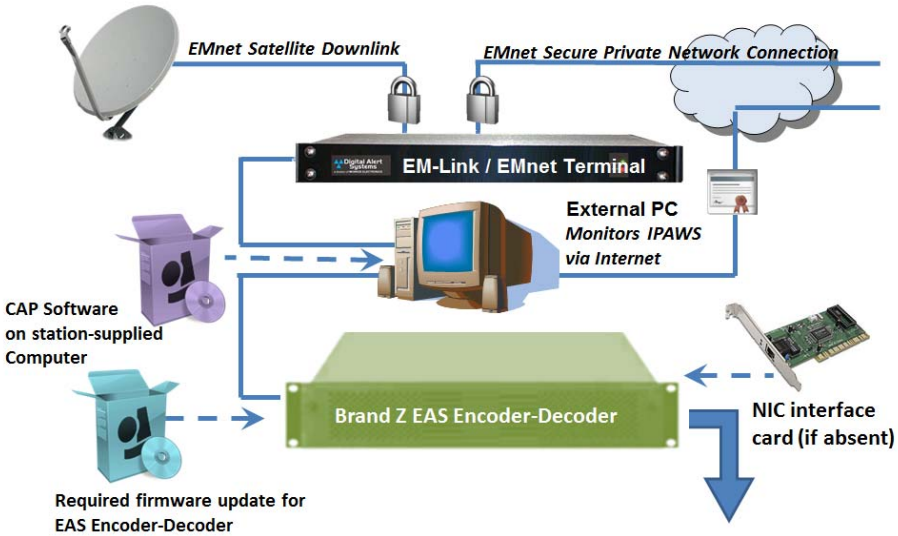
Figure 8: Brand Y configuration (with required add ons) for State EMnet and Federal IPAWS monitoring



Another encoder/decoder sometimes encountered in television operations requires external software and/or hardware as part of its CAP upgrade path. This Brand Z configuration is depicted below in Figure 9. CAP processing software would need to b acquired from the vendor, which would be hosted on a computer (likely Windows based) that is supplied and maintained by the broadcaster.

That computer would poll the EM-Link for alerts, as well as poll FEMA IPAWS (assuming the solution is conformant). The computer would then relay the processed alerts into the existing EAS encoder decoder. The existing EAS unit may itself require at least two updates, including a software update to be able to interface with the PC-based CAP software, and installation of a NIC interface card if one is not present.

Figure 9: Brand Z configuration (with software updates) for State EMnet and Federal IPAWS monitoring



Case Study: Other Internet-based Systems

One might assume that support for Internet-only systems may simplify matters, however, here again there are a range of challenges. As noted earlier, these Internet-based systems are using a variety of push and pull data delivery models, with varying levels of security and software required. A related question is the degree to which the CAP EAS encoder/decoder is pre-configured to support a State CAP source, and if not, the requirements to update that unit to add State CAP sources.

Figure 10:
DASDEC fully integrated configuration for
Web-based CAP *and* Federal IPAWS monitoring

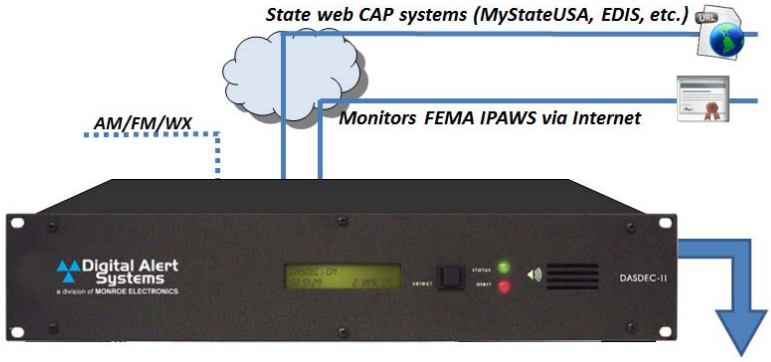


Figure 10 above again illustrates the Digital Alert Systems DASDEC. The DASDEC is currently configured to interface with and monitor sources including MyStateUSA (Washington State and Idaho), California's EDIS, and New York State's NY Alert. The DASDEC has also shown that it can support private network systems such as that deployed in Missouri, which entails proprietary VPN software.

The expected configuration requirements for alternative brands will require additional equipment, significantly so in at least one case. Also, broadcasters should be aware that in at least one state, an additional external computer or device may be required for management of the VPN connection.

These alternative units may also require CAP upgrades that include hardware and/or software elements to be added in line with the existing EAS encoder decoder, as well as required software updates to the legacy EAS unit, and installation of the NIC card. In addition, however, there is the question of whether such a solution is pre-configured to support various State CAP networks, and what costs there might be to add such support. Figure 11 illustrates the preconfigured CAP system support levels.

Figure 11: Comparison of Native Support for CAP EAS Systems

CAP System or Source	DASDEC CAP System Support	Brand X CAP Source Support	Brand Y CAP Source Support	Brand Y CAP Source Support
FEMA IPAWS	YES	YES	Unknown	Unknown
NOAA-NWS	YES	YES	Unknown	Unknown
Comlabs EMnet	YES	No (need EM-Link)	No (need EM-Link)	No (need EM-Link)
MyStateUSA	YES	YES	Unknown	Unknown
California EDIS	YES	YES	Unknown	Unknown
NY Alert	YES	YES	Unknown	Unknown
AlertManager	Yes	Unknown	Unknown	Unknown

As state and local CAP systems proliferate throughout the United States, broadcasters using the DASDEC can be assured of full interoperability with both the legacy EAS and next-generation CAP EAS, at the state, local and Federal levels.

Conclusions:

The proliferation of CAP networks, and likely increasing levels of usage by authorities, will place additional demands on broadcasters and vendors – not only at the initial installation of the solutions, but ongoing, as CAP systems evolve, requirements and standards change, and new states adopt additional systems. Broadcasters should evaluate their options carefully, not only on the basis of initial costs and requirements, but on the ability of their solution and vendors to accommodate a wide range of future changes and contingencies.