EENA Operations Document

Public Warning

Title:	Public Warning		
Version:	1.0		
Code:	2012_06_25_3.2.3_PW_v1.0.doc		
Revision Date:	25-06-2012		
Status of the document:	Draft	For comments	**Approved**

EENA asbl
info@eena.org - www.eena.org

Contributors to this document

This document was written by members of the EENA Operations Committee:

Members	Country / Organisation
Barnes, David	Civil Contingencies Secretariat, UK
Bruck, Charles	Rescue Services Agency Civil Protection Division, LU
Bruneteau, Frédéric	Ptolemus
Casse, Bertrand	Commscope
Dawson, Martin	Commscope
Domingo, Sohan	Intergraph
Gestoso, Luis	Murcia Region Emergency Services, ES
Gustavsen, Morten	UMS
Heen, Kjell	UMS
Jacquard, Claude	Information and Communication Centre Hainaut (Mons), BE
Lumbreras, Cristina	EENA
Marcusson, Hakan	Swedish Civil Contingencies Agency, SE
Muggerud, Tom	UMS
O'Brien, Tony	Commission for Communications Regulation, IE
Olsson, Lars	Swedish Civil Contingencies Agency, SE
Puertas, Francisco	Geoceler
Rahman, Naweed	Cassidian
Sanders, Peter	One2Many
Sembele, Viktorija	State Fire and Rescue Service, LV
Sen, Ayhan	Disaster and Emergency Management Presidency, TR
Strandberg, Ulf	SOSAlarm
Tiquet, Eric	Cap Gemini
Vainik, Feliks	eVigilo
van Alphen, Willem	KLPD Politie, NL
Veenendaal, David	Ministry of security and Justice, NL
Walter, Bruno	CellCast Corp.
Wood, Mark	CellCast Corp.

EENA asbl
info@eena.org - www.eena.org

Table of contents

EENA asbl
info@eena.org - www.eena.org

1 Introduction

Public Warning Systems are needed to protect the lives of people in case of major emergency by warning the public of impending disasters. Tornados, tsunamis, hurricanes, floods, natural volcanic, releases of deadly gas are dangerous situations where Public Warning Systems can safe lives. Chemical plants and nuclear facilities are required to have the ability to notify the surrounding public of an industrial accident.

There is no doubt that effective early warning systems have substantially reduced deaths and injuries from severe weather events.[1] Early warnings of flooding risks have been shown to be effective in reducing flood-related deaths (Malilay et al. 1997). For example, there is a difference between the 1992-1994 flooding along the Rhine and the Meuse rivers and the 1995 flooding along the same rivers (Estrela et al. 2001). The two floods had similar characteristics; both were caused by persistent heavy precipitation. Ten people lost their lives and over 900 million US$ in damages occurred during the first event, while the economic cost was reduced by almost a half no lives were lost during the 1995 flood due to awareness and behavioural changes.

Mortality in the United States declined significantly over the years because its early warning systems for recurring hazards such as lightning, floods, storms and heat waves are continually improving: mortality fell by 45 percent and injuries by 40 percent in 15.000 tornados from 1986 to 1999 thanks to more timely warnings that enabled people to take shelter (Teisberg and Weiher 2009).

In the last 50 years sirens have been the most widely used Public Warning System, together with radio broadcast. For public warning there is no single solution that fits all requirements to reach all citizens in case of an emergency. Therefore, multiple technologies need to be considered. This document investigates the various technologies that are available for public warning.

The 2011 amendment of section 22a of the Universal Service Directive calls on the Commission to present a report on the establishment of a "reverse 112 system", i.e. an EU-wide, universal, multilingual, accessible, simplified and efficient interconnected system for warning and alerting citizens in case of imminent or developing natural and/or man-made major emergencies and disasters of any type, considers that such a system should be implemented without hindering privacy and in combination with appropriate information and training campaigns for citizens.

Furthermore, section 22b calls on the Commission, in close cooperation with Member States, to assess and consider, as soon as possible, appropriate actions to extend the notion of the Universal Service to include the creation and maintenance of a pan-European, multilingual, accessible to all and efficient «reverse 112» i.e. an early warning system for citizens using telecommunications in case of imminent or developing major emergencies and disasters throughout the EU.

[1] Costs and Benefits of early Warning Systems (David Rogers and Vladimir Tsirkunov, 2010): http://www.preventionweb.net/english/hyogo/gar/2011/en/home/index.html

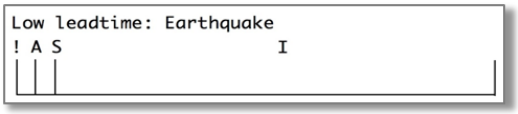
EENA asbl
info@eena.org - www.eena.org

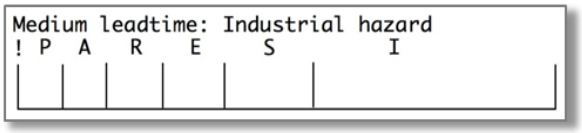
2 Event alert notification cycle time

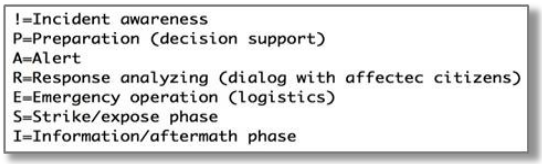
Public warning is the capability to bring to the immediate attention of all people who might be directly impacted following the onset, or predicted onset, of an emergency so that they can take action to mitigate the impact of this incident.

The time it takes to communicate critical information in an emergency can mean the difference between safety and catastrophe. The ability to accurately deliver the right information, to the right audience, at the right time is crucial to any emergency planning effort.

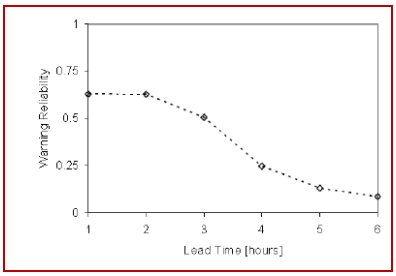
The time passed between an event occurrence and the reception of the warning message by the citizen is the "event alert notification time".
The "event alert notification time" will depend of the threats that each country or region faces. This could be anything from an earthquake to several less time critical incidents.



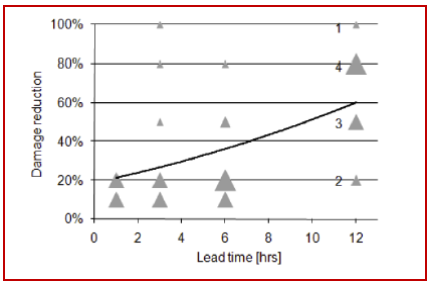




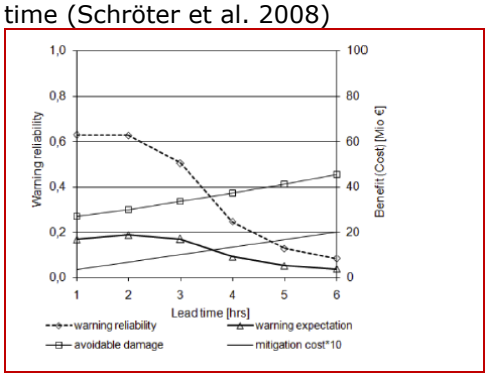
We can find very good examples in the "Costs and benefits of early warning systems" report (David Rogers and Vladimir Tsirkunov 2010) [2] about the relation between the public warning reliability, the lead time and as a consequence the cost-benefit of early warning systems.



Warning Reliability as a function of the lead time (Schröter et al. 2008)



Damage reduction as a function of lead time (Schröder et al. 2008)



Warning expectation as an indicator of optimal alert in the Besos basin (Schröter et al. 2008)

[2] Costs and Benefits of early Warning Systems (David Rogers and Vladimir Tsirkunov, 2010): http://www.preventionweb.net/english/hyogo/gar/2011/en/home/index.html

EENA asbl
info@eena.org - www.eena.org

3 Means of Public Warning

Requirements for communications from authorities and organizations to individuals, groups or the general public during emergencies have been published by ETSI in ETSI TS 102 182[3]. These requirements include the main means of public warning messages distribution:

- Mobile phones (Cell broadcast, Short Message Service - SMS, Multimedia Messaging System - MMS, Unstructured Supplementary Service Data - USSD, Instant Messages Service - IMS, Email, Push IP to Smartphones)
- Fixed phones
- Pagers
- TV, radio
- Sirens
- Billboards
- Internet (web, email, PC notification)

4 Public Warning Systems based on telephony

As described in ETSI TS 102 182, none of the technologies fulfils all requirements; however some technologies for mobile phones and fixed line phones will be considered in the present document.

4.1 Cell Broadcast description

Cell Broadcast (CB) is a technology that has a similar user experience as SMS has: text messages are displayed on the screen of the mobile device. However, the technology that is used to send the message to the mobile phone differs between both technologies. Where SMS is a point-to-point service, CB is a point-to-many service: a broadcast service.

With CB it is possible to send a text message to
- a large number of subscribers,
- including visitors from other countries,
- in near real-time,
- with location specific information,
- in their desired language,
- even when the network is congested.

Since CB is broadcast, it takes a single message to reach potentially all subscribers and roamers on the network, who have enabled the CB service on their mobile device, without the need to know the numbers of their mobile devices. To send a CB message to reach all subscribers (potentially millions) takes between seconds and a couple of minutes.
The message can be broadcasted in a single radio cell, in a group of cells or in the entire network, which makes the service location specific. Messages can be broadcasted in various languages and on the mobile phone only the message in the desired language will be displayed.

A big advantage compared for public warning use to other technologies is that in GSM a dedicated broadcast channel is always available, so CB messages can be broadcasted even when the voice and signalling channels are congested, which is bound to happen in cases of an emergency. In UMTS the CB technology has the highest priority for allocation of a channel.

CB is defined in 3GPP TS 23.041 for GSM, UMTS and LTE. CB includes the Earthquake and Tsunami Warning System (ETWS) which is in use in Japan and can deliver a notification within 4 seconds.

[3] www.etsi.org/deliver/etsi_ts/102100_102199/102182/01.04.01_60/ts_102182v010401p.pdf

EENA asbl
info@eena.org - www.eena.org

Specific use of CB for public warning in Europe is specified in ETSI TS 102 900 and this service is called EU-Alert. In the US the Commercial Mobile Alert Service (CMAS) via CB is specified in ATIS 0700006: CMAS in GSM and UMTS and in ATIS 0700010: CMAS in EPC.

EU-Alert and CMAS are compatible and mobile devices are appearing onto the market from 2011 onwards with a dedicated ring tone and vibration alert to distinguish warning messages from regular (CB and SMS) messages.

There is a label used in the US to mark all phones capable to receive alerts according to CMAS requirements:

4.2 SMS based system description

The use of SMS has long been criticized for use in critical situations due to congestion in the network. However the capacity in the networks have been largely increased the last years and used in the right way SMS will be a solid, reliable and efficient way to reach citizens in a matter of urgency.

One of the most obvious advantages of using SMS is that it works on any handset that can receive traditional SMS. This feature is quite important for the ability of reaching as many citizens as possible. No handset changes are required.

On the other hand traditional SMS is neither location based nor, due to network issues, suitable for alert purpose. ETSI TR 102 444 provides an overview of the functionality of the Short Message Service (SMS) and considers the relevance of certain service characteristics and certain specific functions to the use of SMS for Emergency messaging applications, and the Technical Report states the following:
"Whilst it is possible for SMS to be used for Authority initiated broadcast emergency messages certain criteria may limit the effectiveness of such a service. E.g. Difficulty in obtaining location information for specific MS's; SC or mobile network overload due to instantaneous demand to process large numbers of Short Messages which may result in delay or non delivery."

However ETSI TR 102 444 is dated in 2006 and a lot has changed in the mobile networks since then.

Two obstacles are, as said, the main reasons why traditional SMS is looked upon as not functioning for alerting the public; lack of geo-targeting messages and congestion in the network.

There are solutions today that enable the location-based capability besides utilizing the network in a more efficient way while still delivering the message to the handset as traditional SMS.

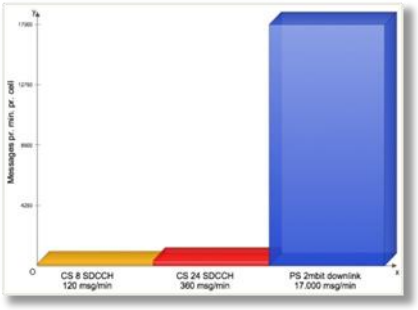
These solutions are mainly consisting of two different components:

- Geo-targeting is providing the localization capability, using probing technology to retrieve and store location updates from all users, including visitors, within the network. Geo-targeting may also make use of existing probes or other ways of retrieving location updates from the mobile phones. Certified components, not affecting existing mobile infrastructure, need to be installed in the operator's environment. It is quite common for mobile operators to install this kind of equipment due to the very fast growing commercial possibilities within location based services.

- An advanced SMSC is providing optimized use and protection of the mobile network. This is a special designed SMSC designed for alert purpose only, ensuring fast, efficient and secure message distribution with reduced network load. There is one major difference between regular mobile telephony and mobile alert telephony. While the normal messaging is all about being able to reach a particular person/phone located anywhere on the globe, mobile alert is about reaching an unknown set of people depending on their location (the area with the crisis).

Key capabilities of such a solution:

- Localizing of people within any given area
- Efficient message distribution (avoiding routing process)
- Avoiding load of HLR (reducing risk of congestion)
- Barring capability, protecting the mobile network during emergency situations
- Optimizing air traffic
- Designed to support packet switched network like 3G and LTE (not only 2G)
- Avoiding congestion
- Ease of implementation, do not affect the end user (no need for handset configuration)
- Cost efficient
- Will also reach visitors from other countries (as long as they can receive SMS)



The mobile technology is evolving fast and so is the deployment of it. The fast propagation of packet switched mobile technology will have the greatest impact on the air interface capacity. In a packet switched network the message capacity of an average cell configuration is approximately 150-200 messages per minute. In comparison the message capacity of a 2MB packet switched network (which is about to be quite common) will be about 17 000 short messages over a cell per minute. The figures are not exact, but is meant to visualize what the near future will bring.

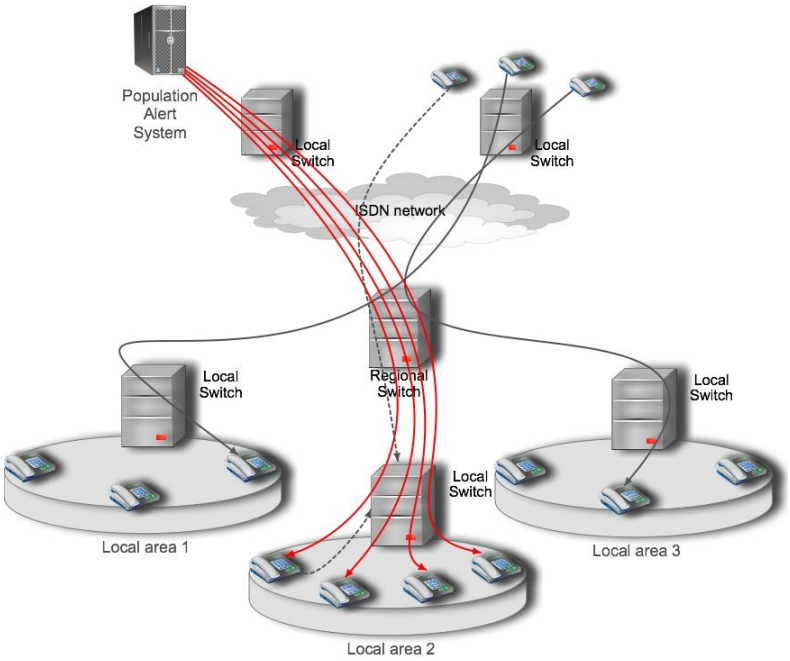
In other words, the capacity in the networks for sending SMS will in the very near future (already rolled out in several countries) not be an obstacle.

4.3 Systems for fixed telephones

There are some major challenges related to use of the fixed network for Geographic Alert. Geographic alert via the fixed phone network is different to traditional telephony and must be handled with care. Trying to reach as many as possible, in a certain geographic area in shortest possible time is close to the nature of spam and is a huge strain to the networks. Another challenge is scalability. In practice this means that the alert system may be used both for handling of alerts to civilians in rural areas with a small or old telecommunication infrastructure and for incidents in urban areas with high population density and modern high scale infrastructure. It is crucial that the alert system is intelligent and able to scale according to the area where it is going to be used. The phone network is scaled according to the population density of the area. If a system scaled for rural areas is going to be used for a major urban incident, it may take days to alert all the affected people. If a high-scaled system is used for alert of a minor rural area the consequences are even worse; the telephone infrastructure will most probably suffer from a major break down due to

congestion problems. Therefore automatic scaling and the ability to detect and protect the public telephone infrastructure from overload and congestion is crucial.

The figure is a simplified illustration of a typical structure of the PSTN (Public Switched Telephone Network), showing the difference between normal call flow and alert call flow.



The switches are scaled according to population density they are dedicated to cover. A normal infrastructure has large switches located on a regional level to distribute traffic to a number of local switches. Local switches are covering a specific local area. The local switches are scaled according to the number of people it covers.

If the number of telephone lines used simultaneously from the geographical alert system exceeds the number of available lines within the local telephone switch, an overload occurs. The consequences may be serious even when used for non-critical situation. Overload will not only slow the dissemination of alert messages, it will also cause problems with the outbound traffic from the area, like for instance emergency calls.

To summarise, following two capabilities should be evaluated as a requirement:

- Scalability to be able to use the system in different geographic areas (nation wide), always with optimized load
- Congestion control to avoid overload critical overload of the PSTN network

EENA asbl
info@eena.org - www.eena.org

5 Public Warning Systems based on TV and radio

There are 2 different possibilities to disseminate information over TV.

- Station broadcast

In this case the emergency notification platform is connected to a gateway located after the signal output from the relevant TV station adding a "super title" slide to the existing TV signal.

- Radio station broadcast uses the same principle.

With digital video broadcast (more precisely multi-cast) the information is being sent by the alert platform to the network service provider and from there to all the set-top-boxes in the specific area of the polygon.

6 Sirens

Sirens are an effective warning system for outdoor use especially in areas with special warning needs such as dams, chemical plants, harbours etc. Another advantage is that the system, if it is built up the right way, is able to work at least 4 – 5 days without external electric power. However costs for investments, maintenance and surveillance are rather high. Since they are a legacy of the Cold War, there is also a built-in resistance to the use of sirens among rescue people.

Furthermore, sirens can be used in a scalable way (from one siren to the whole area/country). The electronic sirens are also able to make spoken announcements.

EENA asbl
info@eena.org - www.eena.org

7 The use of social networks for public warning

Recent events have highlighted the growing importance of Social Networking for informing and mobilising masses of people. SMS and social networks such as Facebook and Twitter have become household names because of this, so it is a fact that they will evolve and grow from now on into a force which cannot be ignored.

The major issue with it is that it offers a platform for the spreading of unverified rumour which may cause confusion and panic. However official originators may also use social networks as a means of distribution of official messages, provided that the social community will accept it. How much it is accepted will depend on the group, and how responsibly such facilities are used by officials in the future.

Social networks are not designed for emergency situations, but they can provide important force multipliers if used wisely.

There are both good and bad aspects to the use of "Social Networking" technologies for public warning. As with all distribution technologies, it fills gaps in other distribution technologies and it itself has gaps which must be filled by other technologies. Therefore a total solution should include "Social Networking" technologies, while also respecting and covering for its weaknesses. This is one of the functions of a good gateway system.

There are three basic 'bearer service' technologies used for Social Networks.

- Pull
- Poll
- Push

The other two basic 'bearer services' are broadcast and multicast. They are not, at present, used in 'Social networking', but this may change.

'Social Networking' is very important and its importance will grow. But its dependency on underlying technologies which are not designed for the acute phase of an emergency may make it vulnerable. Gateways should include such services but as one part of a 'blended approach' to public warning.

7.1 Pull

'Pull' means that the end user has taken the initiative to go to, for example a Website, and get information. Typically a user uses a web browser to address a specific website by URL, and TCP/IP technology provides a session for the duration of the pull session.

Local Government Websites, government pages (i.e. 'Facebook' page) and broadcast media websites (i.e. BBC or others) are obvious places of interest, but online map sites also report very large spikes in accesses to geographical information about a place when that place gets in the news due to an on going disaster.

Because the initiative is taken by the user, the provider of the information has no control over which distribution channel the citizen chooses to go to, or when. The citizen cannot be warned of the problem over pull systems, because the citizen needs to be aware of a problem before he goes to look for information.

Websites, social network pages and other online services can be very rich and detailed sources of information. Users can browse specific levels of detail which are specific to their requirements, rather than having all of the detail dumped on all of them.

However, pull services of all sorts suffer from "Denial of Service" events caused by very large scale demands and intentional attacks. Websites and social network services have been known to "crash" when specific large scale events occur. The need to create separate TCP/IP

EENA asbl
info@eena.org - www.eena.org

sessions for each ongoing link to each subscriber means that events of a much greater scale than normal can cause exhaustion of the capacity of the servers, just at the moment when needed most. This is a well known phenomenon and the reason why pull services may not be relied upon during the acute phase of an emergency.

Alert messages can be copied to popular websites for onward transmission to its subscribers. This way, citizens can see a reassurance confirmation of the message from a source that they trust, maybe more than official channels.

Studies have shown that citizens seek at least three independent confirmations of an alert message before they believe it. Using their trusted Social Network is one way to reinforce the message.

Summary

Pull technologies depend on the user taking initiative, so cannot be regarded as a warning system, and often crash due to a tsunami of load at acute phase of the emergency.

This does not in any way diminish their power as information dissemination systems, which is a separate function, though one just as important in its own way. In addition it is dependant on the functioning of the internet in the area where the user is located. If the internet has failed, these options are generally not open.

The 'Gateway' systems can be configured to share information with websites and other data bases such as Google earth, provided the stakeholders agree.

7.2 Poll

'Poll' is special case of Pull. For example an RSS[4] feed client on a browser will periodically poll a source (by 'Pulling' from it) to see if there is an update of interest to the user.

Another method is to use a very short "Time to Live" for a website, so the browser keeps refreshing at regular short periods for as long as that website is up on the browser.

The problem is that if emergency messages are very rare, then the overwhelming majority of the traffic carried is polls to find out that there is nothing to report, for years and years.

Because of this fact, the polling interval is often set to be in the order of tens of minutes rather than seconds, so this introduces a long latency to the delivery of messages dependant on polling technologies.

In addition, if almost everyone is polling to test for an emergency message, this amounts to an un-scalable large order of magnitude of polls, which is a very large load on the network for no apparent point. This could produce an unsustainable burden on wireless access points, for example.

Summary

'Polling' allows periodic pulling but at the cost of high overhead both during the acute phase and even when the system is in idle mode. A poll would result in a large tsunami of pull events, causing problems for the servers.

[4] RSS (Really Simple Syndication) is used to publish frequently updated works such as blog entries, news headlines, audio, and video in a standardized format

EENA asbl
info@eena.org - www.eena.org

7.3 Push

'Push' technologies are when the system takes the initiative to reach the terminal of the user. Separate sessions are established with each terminal by using its address. Examples are telephone "Dial Down" systems, and SMS, IM, twitter and e-mail messaging systems such as Blackberry.

They broadly take three forms:

- One in which a database of opted-in subscribers is created and then parsed to find interested parties to a specific message.
- Or, a database of subscribers located in an area (a directory) is interrogated, and pushed to regardless of if they have subscribed or not.
- Or, some sort of location subsystem calculates the location of terminals in the area concerned, and sends data only to terminals in the area of interest.

The advantage of 'push' systems are that we eliminate the polling that poll systems need, and we get to alert the recipient to the matter of the emergency when we choose, not when they choose.

Because we are choosing the specific terminals one by one, we get to have very close control of exactly which terminals we address, so we can eliminate some and include others on the basis of both logical and geographical parameters.

Disadvantages include the need to create separate sessions with each terminal separately, which causes a loading issue on the network if the scale of the message is very large. Mobile systems such as mobile phone networks have the addition burden of 'Location', which means that a process of paging, access, and authentication needs to be done for each terminal separately, placing load on many of the networks mobility management elements such as the paging channel, HLR and VLR (unless special mitigation measures have been deployed).

Furthermore, if we are going to use 'Present Geographic Position' as one factor in the choice, we need to separately establish the position of terminals before the transmissions to those terminals can start. This may become a time consuming burden if done on a large scale.

Summary

Push technology puts the sender firmly in charge, but the need to establish separate sessions and process targets separately may cause loading issues in the case of very large scale message distributions.

8 Use of multiple technologies

The secret of success could be to blend the best attributes of all of the existing distribution methods. Each method has its own strengths and weaknesses, but blending them ensures that the weakness of each system is covered by the strength of another.

The problem is that the emergency manager may be faced with a complex mix of different technologies which makes it difficult to determine which technologies are best suited for any specific emergency situation.

For example, the city may decide to use sirens, TV crawlers, voice telephone dial-down, website feed, emails, FAX, social media, or any combination of technologies. There is no problem with doing so but obviously the technical protocols and methods used are very different from one to the other.

But to avoid confusion they must all tell the same tale, and must keep in step so that users do not become more confused the more versions of the message they see.

There are products that convert the proposed message to the format needed for each technology, and then signals it to the right network operations centre for the technology

EENA asbl
info@eena.org - www.eena.org

concerned. This may be a SMS gateway, a Cell Broadcast Centre, a pre arranged maps portal, phone bank, television station, or siren control system. It removes the technical detail of how things are done, from the emergency manager.

In ISO an International Standard – ISO 22322 Societal security and emergency management – is being developed. This standard provides principles and generic guidelines for developing, managing and implementing public warning, before, during and after incidents.

This International Standard is applicable to all organisations involved in preparation and issuing public warning on international, national, regional or local level.

The preparation and dissemination of public warning in this document is based on the two functions of hazard monitoring and warning dissemination. This approach excludes not other solutions.

This standard is under development (April 2012), in "working draft" status. It will go for a voting procedure (committee draft) in June 2012 to get comments from members outside the working group. Comments have to be worked into the standard, and two other voting procedures have to be completed, before it can be considered as a standard. This will take at least one year after.

9 Common Alert Protocol – CAP

The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

CAP may also be used as an integration between several components in an PWS such as sensors (or other Key Integrator Systems) being able to automatically trigger alerts based on threshold values. This opens for easy integration if both Key Indicators and outgoing warning channels both are CAP enabled.

Common Alert Protocol (CAP) is an open standard promulgated by OASIS, and can be found at:
http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

The ITU has adopted v1.1 of the CAP protocol and published this as an ITU recommendation in X.1303 (http://www.itu.int/rec/T-REC-X.1303/en).

Since CAP is a template, the actual interface standard on the use of various CAP parameters needs to be specified in a detailed specification. An example of such a specification is the CAP IPAWS Profile (see http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cs01/cap-v1.2-ipaws-profile-cs01.html). This specification is used in CMAS (see Annex).

CAP is somewhat US centric and therefore Canada has published its CAP-CP (Canadian Profile) variant (see http://capan.ca/index.php/en/cap-cp) and Australia is developing a CAP-AU-STD variant (see http://www.em.gov.au/CAP) which should also be useable in other Asia-Pacific regions.

An example of an implementation of CAP for CMAS IPAWS is given in the annex of this document.

A European example of CAP usage is the adoption of the "CAP Profile Fire" by the Italian National Fire Brigade in 2011 (see http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=4857).

EENA asbl
info@eena.org - www.eena.org

10 Operational aspects

10.1 Testing Public Warning Systems

Public Warning Systems are (hopefully) rarely used. They therefore spend most of their time "In maintenance".

We need to know if the system is going to work when needed. But the obvious way to do that is to set off the alerts. The issues are; that the public would become used to the alert tones to the point of becoming desensitised to it.

As the saying goes; "familiarity breeds contempt".

But this needs to be balanced against a conflicting need to constantly demonstrate the system in operation so that citizens can recognise it, and can be reassured that it will work, and how it will manifest itself, when needed.

There are the following needs for testing:

1. Testing (periodic test of PWS)
    - Public reassurance demonstration.
    - User training and exercise

2. Quality assurance of the system

10.1.1 Reassurance Demonstration test

'Public Reassurance' demonstrations may be scheduled on an annual basis, either on an annual disaster preparedness day (such as the anniversary of a notable disaster), or at the beginning of the season of maximum natural hazard.

Whenever possible, the PWS system should have some form of indication that a test is under way. In the case of a text system, the text should say "This is only a test", or a video caption should make it very clear that a test is occurring and not a real alert. Voice systems explain the nature of the test in a soft reassuring voice. Video presenters and avatars should have a relaxed, friendly, smiling countenance because in bars, for example, viewers can see the screen but not hear the audio from the program.

The whole management system should have means to indicate to all elements in the system that a reassurance test is under way, so that while public distribution occurs, an unambiguous method of identifying that there is no real emergency has occurred, should be factored in to the signalling.

Sweden:

Sweden tests the siren system at 1500 hours every third month at the first Monday in the month. Though it is a national test they have a public announcement in the national radio. The test has two purposes;

- To get the public aware of the siren system and
- That the public knows that it works in proper order and to train the operators of the system.

Government can also get feedback from the public if something is wrong with system or if something got wrong in the test.

The same day at 1900 hours they also test the Radio Data System (RDS) – this works not only at the indoor warning system, its works at all radios which have RDS features. When Sweden goes for EU-Alert they will probably test the system in the same manner.

This is important for the trust of the system as well as getting people aware that the system works

Sirens can often do multiple tones, but people tend to forget the meaning of the different tones.

Czech Republic:

The Czech Republic for example, formerly used about six different tones, but now they use only 1 because people forgot the meaning of the more obscure tones.

The Netherlands:

The Netherlands has a monthly siren test at noon on the first Monday of the month. Also this is advertised in the media each month, so Dutch people know that it is a test.

10.1.2 User Training and Exercise

"A plan is not a plan until it has been tested" is the mantra of the Business Continuity Planning profession, and with good reason. There are both technical and human aspects to complex situations, and so a method of exercising the humans with the technology without alarming the public is good.

For example, in Multicast technologies such as 'Cell Broadcast', it has been proposed that a separate range of Message Identifiers (Topic Numbers) can be assigned for use by participants in training exercises. This will be an authentic test of the technology but without alarming the public.

'Push' technologies such as SMS or twitter, should have an alternative distribution list which includes only participants in the exercise.

'Pull' technologies such as Facebook or websites, should have an alternative URL or number for the test, so that if anyone is seeking confirmation that the alarm is real, he will see only messages reassuring him that all is well. A further explanation that an exercise is underway may also be provided.

The Aggregator and Gateway technology needs be provided with means to differentiate exercises from real alerts, so that any actual public alert is suppressed, in order for human mistakes not to cause embarrassment.

The Netherlands:

The Netherlands broker system has a test mode. But some experts believe that it should be avoided that the system works when in test mode, but is never tested in live mode. Therefore public reassurance tests are also needed to provide a more 'real' end to end test.

Methods for this may include so called 'FOO' accounts (made-up 'Sending' authorities which have only exercise rights). The aggregator system would then assign such senders only limited access to exercise level sub distribution rather than full public distribution. Or, a signal which indicates that the message proposed to the system is in fact an exercise, may be added to the protocol signal departing the origination equipment.

Technical 'Outer loop' test

Sirens are silently tested from time to time by causing them to spin at a speed which is fast enough for shaft mounted tachometers to detect the spinning, but slow enough not to cause a noise. Other systems detect that the communications link from the command centre to the remote control unit is operational, and present an 'alarm' to the operator if a control unit fails to answer a periodic 'Hello' test, or if a line goes to the 'down' state.

The best way to test a system is to test that it is delivering its payload to the intended users, or second best, is offering its service to the users.

For example, Cell Broadcast systems may transmit periodic 'Heartbeat' messages from the system. This message is sent on a regular basis from am MI topic channel which is used for this purpose.

Receivers in the field then detect the arrival of the heartbeat message at the feedback receiver station, and report this to a monitoring system.

If the expected heartbeat message fails to arrive, then an alarm can be generated alerting administrators to the failure of the system.

As part of the troubleshooting process, the technical teams may need to send technical probe message to the system in order to confirm or allay their suspicions regarding overall system performance, and in order to generate log files for analysis.

Accordingly, it would be good to assign topic numbers for 'technical test' reasons.

Sweden:

In Sweden, "Quality assurance" tests of the system, which includes Technical 'outer loop tests' are done at least once a day automatically in the system. The QA of a system includes much more than just this part as can be described in this document – but it's a very important part.

Summary

Thousands of lives and Millions of Euros may be at stake if the alarm system fails at the moment it is needed, so a prompt and automatic testing system is clearly needed.

If a community is lucky enough never to use their investment in a warning system, they can still be reassured that it is functioning by regular public and silent tests. This way, transparency can show that the government is spending resources wisely.

It should also be noted that some technologies may be subject to overload or network congestion, and that is often not considered in the tests.

10.2 Procedures

There are strict national and regional laws about who can say what, where and how. Many of these are based on jurisdiction and boundaries which are territory based. For example a police chief of one city has no authority at all in another city.

In all cases there are detailed records kept for all ongoing and completed notifications

- Decision taking procedure
- Role of the PSAPs
- Use cases: successful cases where public warning has been used

EENA asbl
info@eena.org - www.eena.org

11 Examples of implementations and use of Public Warning Systems

This section contains descriptions of implementations in various countries.

11.1 Norway

Public warning for fixed phones

Major threats:
Due to a major accident in the small town of Lillestrøm in 2000 solutions were demanded for easier and faster ways of communicating with affected citizens. Norway faces threats like flooding, tsunamis, extreme weather and (after the 22nd of July 2011) also terror.

Decision and implementation period:
In 2003 the Directorate for Civil Protection and Emergency Planning launched the first large scale test towards fixed phones – with good results. Since then solutions covering fixed phones have not been used in large scale but on several occasions each year in local areas.

Technical solution:
The system corresponds with the description in section 5.3.

Public warning for mobile phones

Decision and implementation period:
To cover the areas in combination with sirens or areas where there are no traditional sirens and where the Civil Defence authorities don't have any plans for building such infrastructure for public warning.
In 2007 the first location based alert system for mobile phones was tested in an area where a tsunami due to a mountain slide in to a fjord is a major threat. In this case, several municipalities together with the Norwegian Water Resources and Energy Directorate and regional authorities joined forces to build a system based on electronic sirens and a simultaneous warning-message delivered as a SMS message on mobile phones.

Technical solution:
After some tests and agreements with all the mobile telephone companies the results from this were good. The SMS part of the system is based on the alerting system as described in section 5.2.

Public warning by mobile phones has been considered by national authorities in Norway, latest in a report to the Ministry of Justice in November 2011 and is described as a possible future resource together with the sirens that already exists, without taking any decision on what technology of warning to mobile phones that eventually will be preferred. However, the technology to distribute text-messages to mobile telephones has been used by local municipalities several times when smaller crisis has occurred, such as polluted air and water.

Additional information:

www.ums.no

11.2 The Netherlands

Decision and implementation period:

The Dutch government has done extensive testing with a CB based public warning system. The testing was evaluated by the Delft University and included tests with large groups of citizens to investigate technical aspects as well as acceptance by citizens. The reports can be found on the website of the Delft University (http://tudelft.nl).

In 2009 the Dutch government issued an RFP for a public warning system infrastructure. All three Dutch operators provide a CB service to the government which has become operational at the end of 2010. The next step is to inform the citizens about the NL-Alert service, which is to take place in 2012.

The funding of NL-Alert, including the infrastructure, is done by the Dutch government.

Technical solution:

The Dutch government decided to start NL-Alert with the support of legacy devices, and not wait till all mobile devices would support NL-Alert. The US has chosen a different approach and to wait for CMAS capable mobile devices to be available in 2012 before the service has gone live (see section 11.3).

Additional information:
http://www.eena.org/ressource/static/files/eena-riga-2012--aafkefinal-.pdf

11.3 Sweden

TV and radio Public Warning System:

The figures for Sweden, which may be valid for other parts of Europe as well, is that during day-time we reach approximately 30 % of the population by radio and during the evening approximately 30 % by TV. Night time, 22:00-06:30, radio and TV will reach just a few percent of the population.
Sweden also has a RDS (Radio Data System) based warning system in the areas around the Nuclear Power Plants with special warning receivers.
Radio and TV today are covering rather large areas; the effect on an announcement is that it reaches large areas which are not affected by the accident/event.

Sirens Public Warning System:
Warnings and information via radio and television is complemented with the system for outdoor warnings. Outdoor warnings can be given in practically all built-up areas with more than 1,000 inhabitants and in areas surrounding nuclear power stations. The system consists of around 4,500 sirens. In the event of danger, the "Important Public Announcement" (IPA) siren sounds, followed by information via radio or television. The equipment in the outdoor warning system is owned by the state, while the municipalities are the users and also responsible for operation and maintenance.

The system has gradually been modernized and is now computer and radio-based, which makes it possible to activate only the sirens that are needed at the time in question. The geographical delimitation means that persons who are not affected do not need to be worried by the warning. The system can also be used for sending spoken messages from sirens that are adapted for this. Reserve power is available to guarantee outdoor warnings also during power cuts. The system is tested four times a year through the sounding of the IPA siren. The channels of Sveriges Radio provide information both before and after the tests.

Warnings around nuclear power stations

In the inner preparedness zones around nuclear power stations, the inhabitants shall also be given warning indoors, as well as outdoor warning. This is done over the RDS system, and households are provided with special radio receivers intended for warnings.

Since 2002, the RDS receiver does not just warn about nuclear accidents, but is also activated during other serious accidents, such as accidents with hazardous substances. When an accident occurs, the display turns red and shows the text "IMPORTANT ANNOUNCEMENT", at the same time as sounding a piercing alarm signal. After this, the receiver switches automatically to Sveriges Radio P4 at high volume and gives information about the accident. The receiver will sound the alarm even if it is turned off. At an alarm, the clock stops, to make it possible to see when the alarm sounded. The receiver returns to the standard setting at the press of any button.

The common response to these accidents is to go indoors, close doors, windows and ventilation, and to listen to Sveriges Radio.

11.4 Spain

In Spain, the General Directorate for Civil Protection (Ministry of the Interior) and the Regions are responsible for implementation of public warning measures.

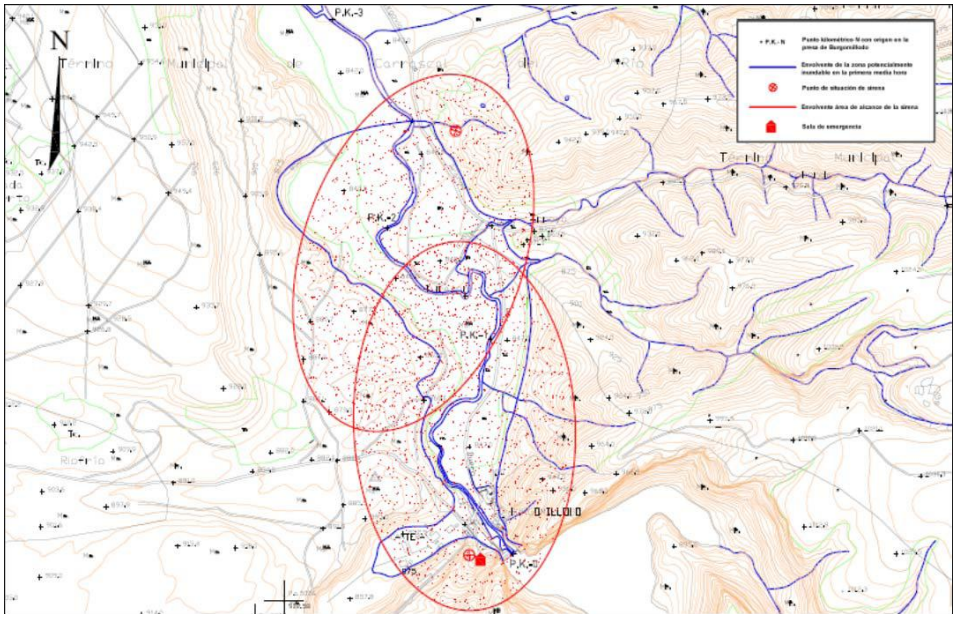
In the case of the regions, public warning measures vary widely from one region to another, from with siren-based warning, to mass messages being sent to fixed lines, faxes, sms or email.

The General Directorate of Civil Protection is in charge of all regulation concerning critical infrastructures, such as dams or nuclear plants, although at the moment each type has a specific national regulation to comply with (there is no single regulation that applies to all critical infrastructures).

For instance, the regulation concerning dams defines the minimum set of warning measures to be put in place, although it does not specifically indicate how often tests and user training exercises need to be carried out. The types of warning systems typically include:

- Acoustic warning based on sirens (Pneumatic/ Electronic) with specific signalling (i.e. french warning signal at frecuency200 Hz) to issue signals to the flooding area.

EENA asbl
info@eena.org - www.eena.org



- Simultaneous and automatic telephony based alert for subscribers in the flooding area, with information and detailed instructions provided using IVR systems.
- Alerting through media, and using the radio network, to provide instructions to be followed.

11.5 Japan

Major threats:
Earthquake is a common occurrence in Japan.

Decision and implementation period:
Area Mail is operational since 2007.

Technical solution:
Japan has an advanced infrastructure of seismic sensors in the ocean around Japan that detects earthquakes and which generates messages that are broadcasted to the citizens via the 'Area Mail' service. Area Mail is based on the Cell Broadcast bearer service. The 3GPP specified "Earthquake and Tsunami Warning System" (ETWS) uses both 'Area Mail' and additional Paging Channel bearers.

The ETWS detects the initial slight tremor of an earthquake, the Primary Wave and sends a warning message that an earthquake (Secondary Wave) is about to happen to the mobile devices in the affected area.

ETWS can deliver the first notification to mobile devices within four seconds using the 'Paging Channel' bearer. This Primary Notification only contains minimum information, such as "Earthquake" or "Tsunami". The mobile device will display a pre-set message.

The Secondary Notification uses the 'Area Mail' service (which is similar to the Cell Broadcast bearer service). This bearer contains more detailed information in text.

EENA asbl
info@eena.org - www.eena.org

11.6 Israel

Major threats:

Israel is in the focus of multi-fold challenges that are threatening the population's safety and security on a constant base. Besides being in the focal point of missile and rocket threats of the neighbouring countries, additional challenges are being imposed based on the fact that Israel is located on the Syrian-African Break of the respective tectonic plates.
As such Israel has to prepare itself for a devastating earthquake that might occur any minute. In addition to that, given the country's geographic circumstances and the fact that both the majority of the industry as well as the population are concentrated on 35% of the country's area, make the population also vulnerable to any kind of man made and natural disasters, something that has been proved once again during the devastating forest fires that took place beginning of December 2010 and caused the death of 41 people enforcing the evacuation of ten thousands of people.

Decision and implementation period.

According to the words of Zeev Tzuk Ram Head of NEMA (National Emergency Management Authority) *"My worst nightmare is that a strong earthquake will catch us unprepared with inability to warn the population and oversee & control the aftermath."*Following the aforementioned the Israeli Home Front Command and the National Emergency Management Authority "NEMA" came up with a new concept to deploy state of the art emergency alert and notification system based on new media age technologies. Unlike the efforts in the US and Europe where the authorities were looking for event alert notification *"Cycle Time"* of 10 and 3 minutes respectively the Israeli standard has set very harsh criteria where the *Cycle Time* has to be less than 20 seconds (on UMTS 3G networks) so that the entire Israeli population can be informed in time, reach protecting shelter and take respective measures. Recent measures show that the system's lead time is 7-8 seconds untilthe message arrives on the recipients' handsets.

Technical Solution:
After testing different solutions and providers, all of which have been dismissed lacking the mass media and timing requirement, beginning of 2009 eVigilo'ssolution based on the cell broadcast technologyhas been chosen to provide the core foundation for Israel's national alert and notification system. The system underwent harsh tests during Israel's 2009 Civil

Defense Drill "Turning Point 3" where the system has been tested which lead to the government decision to start with Cell broadcast as the first foundation of the national message project. The cell broadcast based solution is now expanded by existing means such as TV, radio, sirens and Internet. All of which is going to be operated from one central platform – the eVigilo IADC.

Different sensors and sensor fusion engines are also connected to the eVigilo system allowing additional input that is being sent automatically (in case of an earthquake or Tsunami) or via human interface. The protocol used for the communication is CAP v1.2

As for the human interface the input is being created by multiple institutions each responsible for different type of threats and coverage (national or regional)

As one of the first alert and notification solutions worldwide the eVigilo system provides one central solution that is used both by national authorities as well as municipalities for local alert and information purposes.

The uniqueness lies in the fact that itallows not only information flow from the municipalities to the population but allows also using the same platform for interactive information exchange where the citizens can send help requests and information to the authorities over the same central platform by using a dedicated Smartphone application with "Panic" button. The messages from the citizens contain a default help message, created text or even a photo taken at the incident's location.

This constellation provides the next step of evolution where the given alert and notification system is fully integrated into the 112 eco system.

Red – received help request from the citizen, text upon icon click
Green – Accomplished help request, case closed, text upon icon click
Blue – First responder nearby, text upon icon click

Additional information:
http://www.eena.org/ressource/static/files/national_message_-_april_2011_-_budapest.pdf

11.7 Chile

Decision and implementation period:
In February 2010, Chile has suffered from one of the worst earthquakes in its history. The event was even more tragic as the country has been hit also by a devastating tsunami right after the earthquake. Although the information was known and the US Pacific Tsunami Warning Center has delivered all necessary information in time, this precious information has not reached the public. Chile hasn't had an adequate emergency alert and notification system to alert the target population in time. This has lead to the fact that it suffered more casualties due to the Tsunami than through the earthquake itself. Newly elected President Sebastian Pineda decided to conduct a feasibility study.

The conclusion was that a new system should be put in place in order to be better prepared in the next emergency event.

Following the President's order the Chilean Sub Secretary of Telecommunications (Subtel) has issued in January 14th 2011 an official tender for deployment of Chile's next generation emergency alert and notification system.

The system's first phase based on cell broadcast technology has been handed over to operations in **October 2011**. It is now being expanded by further capabilities such as notification over TV, radio and Internet, incl push notifications to Smartphones that do not support the cell broadcast technology. The system in Chile wasthe first system of its kind in the Americas, advancing also the US American CMAS (PLAN / WEA) project.

EENA asbl
info@eena.org - www.eena.org

Technical solution:
The decision was to introduce a multi-channel alert and notification system using cell broadcast technology in the first phase to be completed then by further means of notification such as analogue and digital TV broadcast, radio, sirens and Internet. The Chilean project uses cell broadcast notification in its initial phase soon to be completed by further means of information as mentioned above. The system provides high availability and geo-site redundancy and stands up to the harshest security and reliability requirements. The system utilizes standard protocols based on OASIS CAP v1.2 (Common Alert Protocol), hence, ensures that any future technology could be seamlessly adopted and integrated.

11.8 Other initiatives

Other countries are investigating how to proceed with public warning. For example France, Lithuania, and Greece have issued an RFP for a public warning service based on cell broadcast. Korea has mandated a public warning service based on CMAS which shall go live by the end of 2012.

12 Recommendations

As explained in chapter 8, a Public Warning System should consist of a mixture of technologies that works best in a country. Most countries already have a warning system and the examples described in chapter 11 show that adding a technology in the mobile network is being done and is being considered in many countries today. The rationale behind this is that only since the last few years many citizens have a mobile phone which they carry with them most of the day. These citizens can be reached on their mobile phone for most of the day.

Therefore the recommendations in the present document are mostly focused in mobile networks technologies, which reflect the 2011 amendment of the Universal Service Directive.

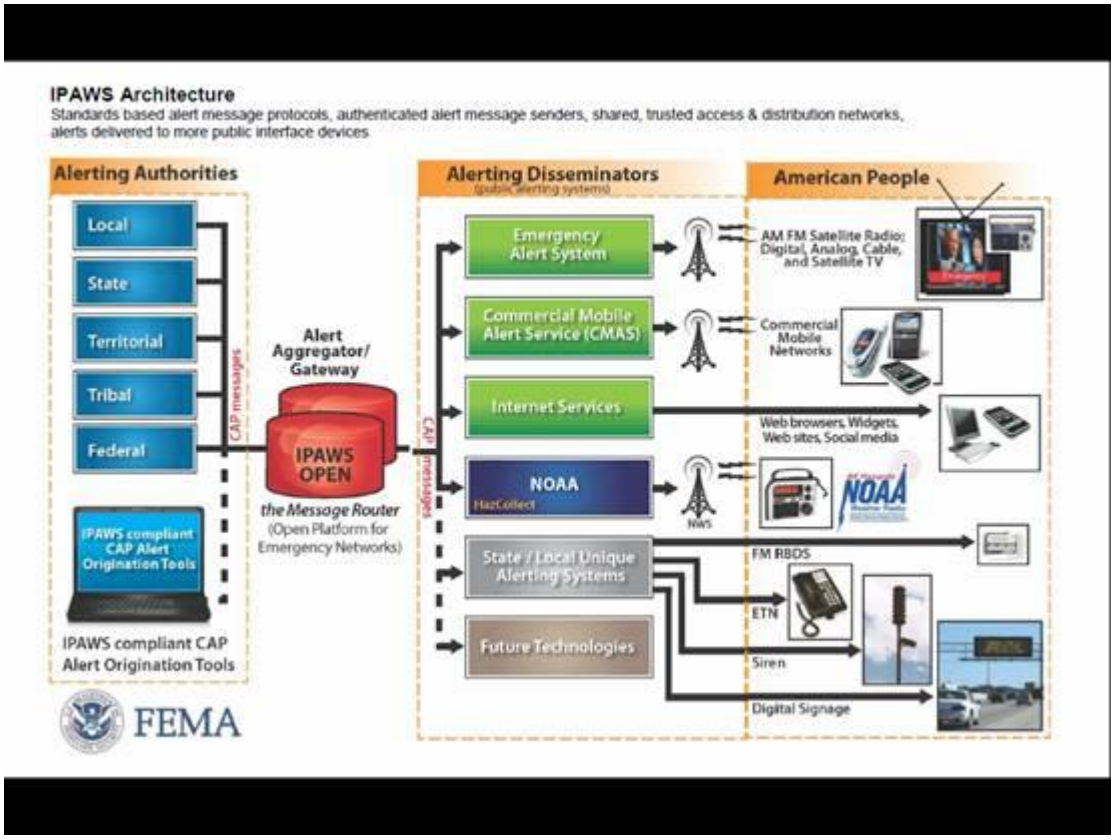
Stakeholders	Actions
European Authorities	Take appropriate actions to include the creation and maintenance of a pan-European, multilingual, accessible to all and efficient «reverse 112», as per 2011 amendment of the Universal Service Directive
National Government	Implement "reverse 112" to cover local, regional and national emergencies.
National / Regional Authorities	Create a clear Public Warning procedure with a clear description of responsibilities
Emergency services	Define situations and limits
National telecommunication regulator Network operators	To cooperate with National Government to facilitate the implementation of "reverse 112"

13 EENA Requirements

Requirements	
Definition of event alert notification cycle time for potential risks	Defined
Multilingual Public Warning System	Compulsory
Multi-technology Public Warning System	Compulsory

ANNEX A: example of an implementation of CAP in the United States of America

Executive Order 13407 states, "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people....and to ensure under all conditions the President can communicate with the American people." FEMA is designated within the Department of Homeland Security to implement the policy of the United States for a public alert and warning system and has established a program office to implement IPAWS. FEMA, as well as numerous public and private industry partners, are working together to transform the national alert and warning system to enable rapid dissemination of authenticated alert information over as many communications pathways as possible.



Public officials are granted the authority to alert the public of emergency situations through Federal, State, and local laws. Specific authorities may be designated in state Emergency Alert System, AMBER Alert, or other emergency operations plans. Generally, eligible organizations will be:

- Federal Agencies
- State Government Organizations
- Local Government or Public Safety Organizations
- Tribal Governments
- Territorial Governments

Prospective senders may group themselves in to a group called a "Collaborative Operating Group" (COG). This may be a single organisation or a group of organisations.

To request a COG, a group must;

EENA asbl
info@eena.org - www.eena.org

1 Select IPAWS compatible software which speaks 'Common Alert Protocol' (CAP).
2 Apply for Memorandum of Agreement (MoA) with FEMA.
3 Apply for 'Public Alerting Permissions' by getting approval from a 'Designated State official'.
4 Complete the web based training.

Common Alert Protocol (CAP) is an open standard promulgated by OASIS, can encapsulate parameters and also text, audio and video clips and other file formats for the use of participating networks in accord with their own technological capabilities and agreements.
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

Once the COG member has a valid MoA with FEMA, his message creating software is connected to the Federal "IPAWS OPEN" alert gateway via highly secure technology specified by the government.

This IPAWS OPEN gateway has the responsibility for Authenticating, Authorizing messages and then distribution of messages to participating distribution networks, such as mobile phone networks or digital signage operators. It accepts messages in CAP format.

'Participating Networks' may include text services, social networking, TV, Radio and Digital Signage operators. These may also accept messages in CAP format for further processing within their networks.

The Federal Communications Commission (FCC) recently issued their 5th Report and Order on EAS and this ruling makes CAP mandatory. FCC has adopted the EAS-CAP Industry Group (ECIG) Implementation Guide (I.G.) as the method to be followed for converting CAP messages to legacy EAS protocol. Recent changes include such things as more exact definition of file MIME types, such as the format for audio clips (e.g. MP3), and a facility for freeform text. Audio networks can either play the MP3 file as audio (a spoken message) or use a text to speech converter to create it. Special Attention Signals are also added to the audio.

http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

A 'Participating Commercial Mobile Service Provider' (e.g. a Mobile Phone Network) is a Commercial Mobile Service Provider that has voluntarily elected to transmit Alert Messages. Entry into Commercial Mobile Alert System (CMAS) for transmission over the Cell Broadcast bearer service is via a unit 'downstream' of IPAWS OPEN, called the Commercial Mobile Service Provider (CMSP) Gateway'. Alert messages are called 'Commercial Mobile Alert Messages' (CMAM). While 'Commercial Mobile Alert System (CMAS)' is a more technical name for the implementation of Cell Broadcast for public warning in the USA, FCC also refer to the Cell Broadcast based public safety system as 'Personal Localized Alerting Network' (PLAN). Some networks use the expression Wireless Emergency Alerts (WEA), while other states may also in the future use the expression CELL-ALERT, which more closely resembles the European EU-ALERT naming convention.

Communications between IPAWS OPEN and CMSP gateway over the C interface is defined in the standard ATIS/TIA J-STD-101.

CAP messages can include 'Freeform text' that will be used as the Cell Broadcast message in a parameter element (see below). If the COG has permission (from the network) to send freeform text, this information will be used when constructing the CMAM message. Otherwise the following algorithm is used by the IPAWS OPEN gateway before transmission to the CMSP gateway over the C interface;

There are four portions to the "generated CMAM Text" (see following CMAM Text table):

- "What is Happening" – based on CAP Alert <eventCode> element.

- "When the Alert Expires" – based on CAP Alert <expires> element.
- "What Action Should be Taken" – based on <eventCode> for two special cases and <responseType> elements for other allowed CMAS event codes.
- "Who is Sending the Alert" – based on CAP Alert <senderName> element.

The format for the CMAM Text is as follows:

[WHAT IS HAPPENING text string] " in this area " [WHEN EVENT EXPIRES text string] [WHAT ACTION SHOULD BE TAKEN text string] [WHO IS SENDING THE ALERT text string]

Or, the sender can create his own 'Freeform text' to describe the situation and name specific places. Here is the format for defining the freeform text.

```
<parameter>
    <valueName>CMAMtext</valueName>
    <value>freeform text</value>
</parameter>
```

FEMA guidelines have specified what sort of emergency is coded by the 'Specific Area Message Encoding' (SAME) codes. It's up to officials to correctly pick a SAME code for the event which most closely matches the situation, as this will affect the text that is eventually generated. FEMA offers training on interpreting and selecting SAME codes.

Categories include Take Shelter, Evacuate, Prepare, Avoid, Monitor.

For example the code for evacuate now is "EVI", whereas the code for take shelter is "SPW". The text on a mobile phone would read "Take Shelter in this area", but there is no ability to name any areas in plain language.

When selecting the area over which the message is to be sent, The IPAWS system uses one or more previously defined 'Federal Information Processing Standards' (FIPS) codes. Currently, standard (FIPS) 6-4 [Ref 6] is used, in which each FIPS is represented by a five digit number and is about the size of a County. CAP Messages sent to the IPAWS OPEN gateway must contain at least one FIPS code, so that this can be compared with the FIPS codes authorised for the COG. Also in the 5th Report and Order on EAS the FCC acknowledged that the Federal Information Processing Standard (FIPS) publication currently used to describe EAS Location Code numbering has been replaced by an American National Standards Institute (ANSI) publication Codes INCITS 31.200x (Formerly FIPS 6-4). So, the EAS location "FIPS Code" is now "ANSI Code.

Information on FIPS codes may be found in the following link; < http://www.itl.nist.gov/fipspubs/index.htm >.

Depending on network implementation, Senders may be limited to sending to whole FIPS codes, or group of FIPS codes.

The CAP protocol also allows the sender to send a freeform 'Polygon', which is then sent to the IPAWS OPEN gateway. Depending on the 'Memorandum of Agreement' with the individual participating distribution network, downstream systems, such as Cell Broadcast Centres (CBC) may alternatively use the 'Polygon' to determine which base stations have service within the Polygon, and transmit the message only to places inside the Polygon rather than the whole FIPS. However, a polygon can be smaller than a FIPS, bigger than a FIPS, or outside of any FIPS.

A CMSP gateway can reject a CMAM message if it does not fully conform to the agreed standard. So it's important that messages between the IPAWS OPEN gateway and the CMSP gateway are correctly and fully formatted. Listed below are some of the required parameters, only those messages with CMAS yes in brackets are transmitted by CMAS, though they may

be transmitted by other participating distribution networks. When a message is generated the sender must include the following fields;

Urgency, Severity, Certainty, Event Code and event Category. The codes on offer are;

Urgency
- Immediate (now) [CMAS yes, Imminent MI]
- Expected (within the next hour) [CMAS yes, Imminent MI]
- Future (more than an hour away).
- Past
- Unknown

Severity
- Extreme (extraordinary life or property damage) [CMAS, yes]
- Severe (Significant life or property damage) [CMAS, yes]
- Moderate possible loss
- Minor minimal or no losses
- Unknown

Certainty
- Observed (Have occurred or be on going) [CMAS, yes]
- Likely (>50% probability) [CMAS, yes]
- Possible (< 50% likely)
- Unlikely (Not Expected)
- Unknown

The event codes and event categories are according to the USA Federal Government 'Specific Area Message Encoding' (SAME) coding standard. A copy of the standard is listed below.

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-64A1.pdf

The contents of the SAME codes are also used to decide on the choice of Message identifier (MI) address used in the CMAS system.

In order to assure the system's operation, there is a periodic 'Silent Test' of the system. The SAME code for this is Required Monthly Test (RMT). On receiving a message bearing the RMT SAME, a different non-publicly advertised Message Identifier channel is used on Cell Broadcast, so that the public are not bothered by the required monthly test.

EENA asbl
info@eena.org - www.eena.org

ANNEX B: Features of Public Warning Systems

As all critical systems, the most important characteristic of Public Warning Systems is reliability. In addition to technical features, future Public Warning implementation also needs to take into consideration "what is the aim for a system". The following list suggests areas of importance:

Cost	
Cost related to infrastructure	Cost related to infrastructure includes hardware and infrastructure investments necessary for the service providers to establish the service
Cost related to implementation	Cost related to implementation includes processes and activities necessary for the end users (citizens) to take the alert service in use. This is covering both technical and non technical issues
Cost related to maintenance	Cost related to maintenance includes costs necessary for the service provider to run and maintain the alert channel

Network (For mobile network based Public Warning Systems)	
Theoretic capacity	The meaning of theoretic capacity is to identify which channel has the best theoretic capability to broadcast a large number of messages in a short period of time.
Practical capacity	The meaning of practical capacity is to identify which channels have the capability to reach citizens within a certain limit of time no matter the area size.
Congestion sensitive	Handling congestion is an evaluation of the alert channels capability to avoid or handle congestion in the mobile network.
Core network impact	Core network impact is an evaluation of to what extent the channel/bearer is loading the central core system like Visitor Location Register (VLR), Home Location Register (HLR), Mobile Switching Centre (MSC).
Air interface impact	Air interface impact is an evaluation of to what extend the channel/bearer is loading the radio interface and its channels like Single Dedicated Control Channel (SDCCH) which is crucial for the transmission of SMS.
Network protection feature	The capability for this channel/bearer to prevent traffic peaks from causing congestion during emergency situations. This is an add-on feature not part of the channel.
Authentication	Authentication of the message.
Capability to adapt to future generation networks	The capability for the mobile service to follow the mobile evolution, not being part of a proprietary path.
Security	The ability of the network to deny access to unauthorized users of the system

Functionality (For mobile network based Public Warning Systems)	
Localisation accuracy	Weather the channel has a localization feature, able to identify the handsets within an area and the level of accuracy of it
Logistics (National)	The capability to provide logistics/number of national handsets within an affected area
Logistics (visitors from abroad)	The capability to provide logistics/number of roamers from abroad within an affected area
Repeat	The capability to distribute the warning message in certain

EENA asbl
info@eena.org - www.eena.org

	given intervals. Content may have been changed or unchanged.
Response	The capability to handle response as a reply to the alert message from the end user, if required.
Multilingual	The capability to send multilingual warning message according to the different nationalities within the affected area.
Follow up (to certain respondents)	The capability to send a follow up message to affected people in similar situation/similar needs/responded equally.
Opt-in/opt-out (subscription)	The capability for the channel/bearer to handle opt-in/opt-out (subscription) in an easy and user friendly way.
Real time confirmation of messages sent	Real time status showing number of messages tried/sent during the alert process, if required.
Real time confirmation of messages delivered	Real time status showing number of messages successfully delivered during the alert process, if required.

Coverage/efficiency (For mobile network based Public Warning Systems)	
Alert of blind people	Capability to alert blind people without use of any proprietary handset or device.
Alert of people with disabilities	Capability to alert hearing disabled people without use of any proprietary handset or device.
Alert of visitors from abroad	Capability to alert visitors from abroad without use of any proprietary handset or device.
Alert of citizens abroad	Capability to alert travellers abroad without use of any proprietary handset or device.
Alert at night	Capability to alert at night without use of any proprietary handset or device.

Implementation (For mobile network based Public Warning Systems)	
Expected evolution year 1-3	Expected level of evolution during the first 3 years. Manual configuration of hand sets, opt-in requirements or any other activity required by the end user will have a severe impact on this topic.
Expected evolution year 4-6	Expected level of evolution during the next 3 years.
Depending on international evolution	Particularly related to the capability to alert visitors from other countries roaming to national service providers.
End user education required	Legislation differs from country to country and must be handled nationally, but nature of the different technologies may require different approaches.

Privacy issues
Effecting privacy legislation

Handset (For mobile network based Public Warning Systems)	
Supporting all 2G phones	Are all 2G phones supporting the channel/bearer?
Supporting all 3G phones	Are all 3G phones supporting the channel/bearer?
Supporting 4G/LTE entities	Is the system prepared to support phones and other devices using the upcoming 4G/LTE channel/bearer?
Handset changes required	Is the evolution of the service depending on changes on the handset which require changes in current standards?
Battery consumption affected	Will the battery consumption increase when enabling the service?
Consistent user interface	Do all cell phones present the alert message consistently, and does the user need to confirm having read the message

EENA asbl
info@eena.org - www.eena.org

	before other activities can be done on the phone, such as reading another text message or starting a voice call?
Manual config. Required	Does the end user need to perform any activity to activate the alert channel on the handset?
Alert notification	Does the phone support a PWS specific alert tone and vibrator cadence to distinguish the alert message from a regular message?

EENA asbl
info@eena.org - www.eena.org