ETSI TR 103 273 V1.1.1 (2016-12)

TECHNICAL REPORT

Emergency Communications (EMTEL); Recommendations for public warning making use of pre-defined libraries

Reference

DTR/EMTEL-00032

Keywords

broadcasting, design for all

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes the rules and procedures to implement public warning making use of pre-defined libraries that enable simple and systematic multi-language and multi-mode presentation of warning messages in any European country. This includes the definition of dictionaries for public warning, syntax rules and procedures to formulate warning messages, as well as rules and procedures to extend dictionaries when required.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] UNISDR Terminology on Disaster Risk Reduction (2009).

NOTE: Available at www.unisdr.org/eng/terminology/terminology-2009-eng.html.

[i.2] D. S. Mileti and J. H. Sorensen: "Communication of emergency public warning, A social science perspective and state-of-the-art assessment", August 1990.

[i.3] Centers for Disease Control and Prevention, Crisis and Emergency Risk Communications: Best Practices, 2009.

[i.4] D. S. Mileti: "Warning messages and public response", Social science research findings & applications for practice, August 2009.

[i.5] Partnership for Public Warning, Protecting Americas Communities, An introduction to public alert & warning, 2004.

[i.6] W.T. Coombs: "Ongoing Crisis Communication: Planning Managing and Responding", 3rd edition, Thousand Oaks: SAGE, 2011.

[i.7] Australian Government, Emergency management Australia Evacuation planning, 2005.

[i.8] California Emergency Management Agency, Alert and Warning, Report to the California State Legislature, 2008.

[i.9] D. S. Mileti: "Factors related to flood warning response", U.S. Italy Research Workshop on the Hydrometeorology, Impacts, and Management of Extreme Floods, Italy, 1995.

[i.10] Working Group on Natural Disaster Information Systems, Subcommittee on Natural Disaster Reduction, Effective Disaster Warnings, 2000.

[i.11] C. Fitzpatrick and D. S. Mileti: "Motivating public evacuation". International Journal of Mass Emergencies and Disasters, August 1991.

[i.12] CAP V1.2: "Common Alerting Protocol Version 1.2".

[i.13] J-STD-101: "Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification".

[i.14] ISO 22322-2015: "Emergency Management - Guideline for Public Warning Systems".

[i.15] International Federation of Red Cross and Red Crescent Societies: "Community early warning systems: guiding principles".

NOTE: Available at www.ifrc.org.

[i.16] ISO EN 22300-2014: "Teminology".

[i.17] Recommendation ITU-T X.680 / ISO/IEC 8824-1: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.18] T. De Cola, J. M. Chaves, C. Parraga: "Designing an efficient communications protocol to deliver alert messages to the population during crisis through GNSS" in Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC), 2012 6th volume, no. pp.152-159, 5-7 September 2012, Baiona, Spain.

[i.19] Alert4All (A4A), EU-FP7 SEC-2010.4,3-1 funded project, 2011-2014.

NOTE: Available at http://alert4all.eu/.

[i.20] US National Weather Service.

NOTE: Available at http://www.weather.gov/.

[i.21] ETSI TR 103 335: "Emergency Communications (EMTEL); Guidelines for alert message content accessibility".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

alert decision maker: authority entitled to decide whether to warn the population or not based on the warning information gathered from the warning author

alert message: Equivalent to the term warning message in ISO 22322 [i.14].

alert message issuer: authority (or authorities) entitled to formulate alert messages, based on the information gathered from the warning author, and to send the alert message(s) to the population at risk in a direct manner or by means of one or several intermediaries

alert message recipient: citizen(s) at risk that should receive alert messages disseminated by the alert message issuer

NOTE: The citizen could either be present in a residential, business or recreation environment during the incident.

area of authority: area in which the alert message issuer is entitled to warn/alert the population

early warning system: set of capacities needed to generate and disseminate timely and meaningful warning information to enable individuals, communities and organizations threatened by an incident to prepare and to act appropriately and in sufficient time to reduce the possibility of harm or loss, as defined in ISO 22322 [i.14]

NOTE: This definition has been established by the United Nations International Strategy for Disaster Reduction in [i.1].

incident: This term is defined in the ISO EN 22300-2014 "Terminology" [i.16].

intermediary: service provider or operator that distributes the alert message provided by the alert message issuer over its communication infrastructure

warning author: agency that implements the hazard monitoring function and provides warning information to the alert decision maker and the alert message issuer

NOTE: Examples of the warning author are agencies that monitor and provide information on meteorology, hydrology, health information, etc., and evaluate the related risks.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Approval Committee
ASN	Abstract Syntax Notation
AVW	Avalanche Warning
BZW	Blizzard Warning
CAE	Amber Alert
CAP	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CC	Certification Committee
CDW	Civil Danger Warning
CEM	Civil EMergency
CEN	Comité Européen de Normalization
CET	Central European Time
CFW	Coastal Flood Warning
CMAS	Commercial Mobile Alert Service/System
DSW	Dust Storm Warning
EAN	President has issued an alert
EQW	EarthQuake Warning
EVI	EVacuate now
EWS	Early Warning System
FFW	Flash Flood Warning
FLW	FLood Warning
FRW	FiRe Warning
HMW	HazMat Warning
HUW	HUrricane Warning
HWW	High Wind Warning
ISO	International Standards Organization
LAE	Local Area Emergency
LEW	Police Warning
LME	Library Management Entity
NUW	Nuclear Power plant Warning
OEZ	Olympia EinkaufsZentrum
PDT	Pacific Daylight Time
PSAP	Public Safety Answering Point
PWS	Pubic Warning System
QCC	Quality Control Committee
RHW	Radiological Hazard Warning
SMW	Special Marine Warning
SPW	Take Shelter Now
SVR	SeVeRe storm warning
TC	Technical Committee
TOR	TORnado warning
TRW	TRopical storm Warning
TSW	TSunami Warning
UNISDR	United Nations International Strategy for Disaster Reduction
US	United States
UTC	Coordinated Universal Time (literally Universel Temps Coordonné)
VOW	VOlcano Warning
WEA	Wireless Emergency Alert
WSW	Winter Storm Warning
XML	eXtensible Markup Language

4 Public Warning Paradigm

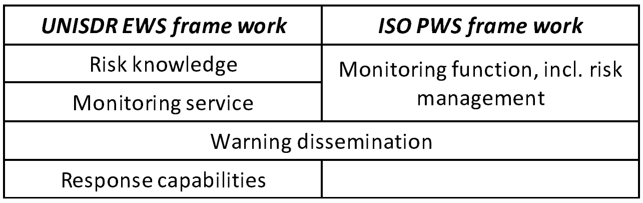
4.1 General

Public Warning is aiming to support the public audience with information about incidents/crisis and recommendation on remediating measures during incidents/crisis situations, incidents which could disrupt the safety and security of lives and/or assets.

Public warning is one important part of the entire emergency communication within the emergency and/or crisis management process. The complementary part of the emergency communication during such incidents/crisis is the information provision to the emergency management staff in the field enforcing the efficient implementation of effective response actions, thus limiting harm/damages to lives and assets.

Enabler for the emergency communication is well established risk knowledge/risk management functions, a monitoring function as well as response capabilities. These three functions outline/define content to the messages, which have to be disseminated either to the public or the emergency management staff.

The emergency communication should be capable of supporting man made as well as natural disasters based incidents/crisis situation. In this respect the most prominent global references UNISDR [i.1] and ISO technical committee "Security and Resilience" [i.14] are supplying two well-funded frame works (see figure 1), which are both covering the main area addressed in the present document, i.e. dissemination of public warning.



UNISDR EWS frame work	*ISO PWS frame work*
Risk knowledge	Monitoring function, incl. risk management
Monitoring service	
Warning dissemination	
Response capabilities	

Figure 1: UNISDR and ISO frameworks: functions

According to the UNISDR mandate the EWS frame work is only targeting natural disasters (meteorological, geological, biological, etc.) while the ISO PWS framework also addresses manmade disasters (incidents/crisis situations, e.g. 9/11, Oslo bombing, etc.) and also aims to cover the information provision to emergency management staff (first responders, volunteers, etc.) in the field (see figure 2).

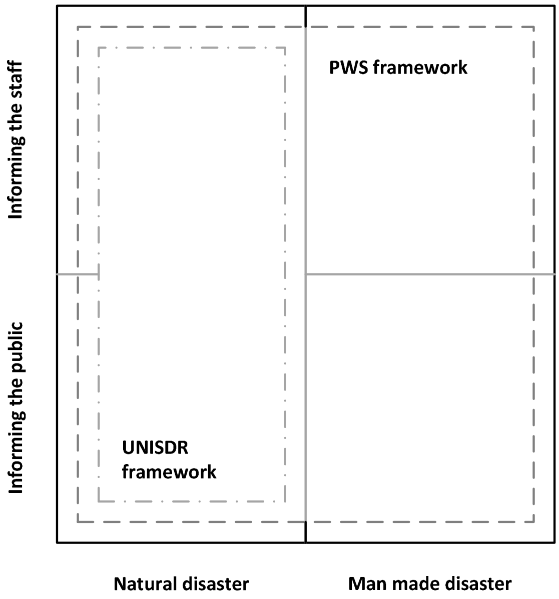


Figure 2: UNISDR and ISO frameworks: scope

Referring to both frameworks, the functions are characterized as follows:

- **Risk knowledge.** This term refers to prior knowledge of risks being faced by communities, for example by means of risk assessment, mapping of incidents and vulnerabilities, their patterns and trends.

- **Monitoring and warning function.** This term refers to the solid scientific basis for risk prediction and detection of incidents, as well as to the consequent decision process to disseminate warning messages to affected communities.

- **Dissemination and communication.** This term refers to the process of formulating and disseminating messages to affected communities upon detection or prediction of a risk situation.

- **Response capability.** This term refers to communities understanding their risks and reacting upon reception of warning messages.

This clause refers to best practices on the dissemination and communication process that yield best results inactionable warning and information, i.e. providing timely messages that reach, are understood and are acted upon by the population at risk [i.15].

In the dissemination and communication process, four main actors are involved, see figure 3:

- The warning author: agency that implements the hazard monitoring function and provides warning information to the alert decision maker and the alert message issuer. Examples of the warning author are agencies that monitor and provide information on meteorology, hydrology, health information, etc. and evaluate the related risks.

- The alert decision maker: authority entitled to decide whether to warn the population or not based on the information gathered from the warning author. Depending on the civil protection organization of a specific region, this role is typically covered by the Mayor, authorized personnel at civil protection agencies, or similar.

- The alert message issuer: authority entitled to (i) formulate alert messages, based on the information gathered from the warning author, and (ii) send these alert messages to the population at risk in a direct manner or by means of one or several intermediaries. This role is typically covered by civil protection agencies (or entities having similar functions) or specific responders, such as fire brigades. The actors model in [i.15] refers to the "alert message issuer" as "mediator", as its major role is to shape the alert message to be understandable by the community at risk, avoiding jargon and technical language, which can be expected from the warning author (agencies involved in the monitoring function), who has typically a scientific background.

- The intermediary: a service provider that distributes the alert message over its communication infrastructure for delivery to the alert message recipient. The intermediary may adapt the format of the alert message to make it compatible with the technology that will be used for delivery. Examples of intermediaries are telecommunication operators or radio or TV broadcasters.

- The alert message recipient: the citizen(s) at risk that should receive (read and understand) alert messages.

It is worth noting that this actors' model represents generic roles in the communication process for public warning that can be mapped into agencies and authorities in different manners, depending on the civil protection organization of each region or country. Several warning authors can provide warning information to a single or several alert decision makers and alert message issuers. The alert decision maker and alert message issuer may make use of information systems to aggregate the information from several warning authors to build a comprehensive risk situation awareness. Also PSAPs can be understood as warning authors when a risk situation is identified by means of citizens calling the emergency number. The roles of alert decision maker and alert message issuer may be fulfilled by the same authority, even by the same physical person in a specific context.

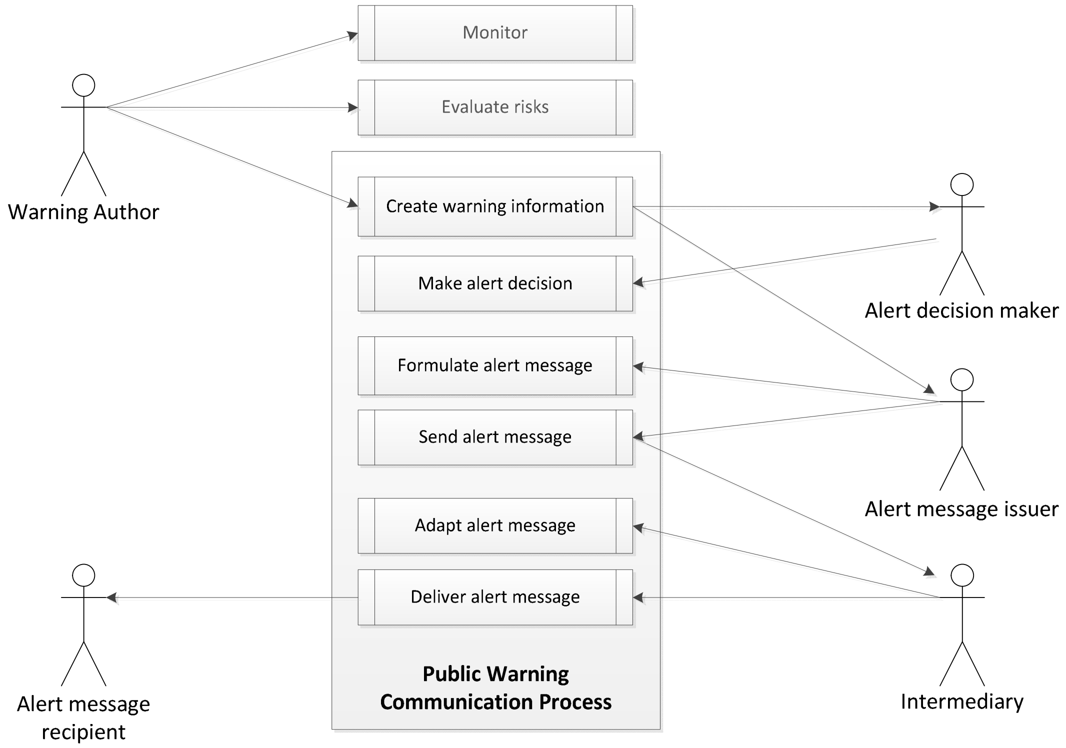


Figure 3: Communication process in public warning

The process depicted in figure 3 shows the actors and functions involved in the communication process in public warning. It should be noted that the monitoring and evaluation functions are functions that the warning author fulfil, but are considered previous to the communication process.

The purpose of this process is to create awareness about the occurring risk during an incident and to trigger a specific reaction or action plan at the alert message recipient site.

In this process, the warning author monitors hazards and evaluates the related risks to create warning information. This warning information is taken as input by the alert decision maker to decide whether to warn. The alert message issuer acts upon the decision formulating the alert message based on the input warning information and sends the alert message through the intermediary. The intermediary adapts the alert message to make it compatible with the technology or technologies that will be used to deliver the alert message and finally delivers it to the alert message recipient.

The alert message recipient will make a decision about his/her reaction/action plan as a result of an own risk evaluation in consideration of the alert message received, the own perception of the situation/environment and the available response capacity.

The perception of the situation by the alert message recipient is influenced by a number of factors; some of those factors may be autogenic (including cognition and physical abilities), others may be caused by a social and environmental context, others may be caused by the own perception of the situation by means of other information sources. Therefore, the dissemination and communication process should be managed by the alert message issuer in a manner that maximizes the probability that the alert message recipient understands and acts upon alert message reception in the intended manner.

4.2 Best Practices in Public Warning

4.2.0 Overview

There is a number of variables that the alert message issuer can steer to foster that the alert message recipient receives, understands and acts upon alert message reception in the intended manner:

- The alert message content and style.

- The channels used to disseminate the alert message.
- The frequency with which the alert message is repeated and updated.

This clause compiles best practices in the terms of the three variables listed above. Such best practices are a collection of standards and guidelines built from past experiences.

4.2.1 Criteria in the Public Warning Decision Process

The warning decision process encloses several decisions as listed below:

Whether to warn

The decision whether to warn is commonly supported by available emergency plans derived from past experiences or risk analysis of expected incidents in/for the area of authority. The decision has to consider a number of factors, e.g.:

- certainty of the available information;
- expected warning impact;
- long term trust in warning messages;
- costs.

The impact of false alarms can be negative (especially in the long term). On the one hand, emergency communication services can get overloaded (e.g. by significantly increased calls to PSAPs); on the other hand, several false alarms can yield the alert message recipient to dismiss other warning messages. Nevertheless, there is evidence that if the reasons that triggered false alarms are explained with a valid and rational explanation, the public is more tolerant to them. Hence, most authors recommend to warn in case of doubt, see Communication of emergency public warning, A social science perspective and state-of-the-art assessment [i.2]. Furthermore, the citizens at risk are exposed to additional information sources that can spread rumours. It is preferable to warn and state the certainty of the information than remaining silent and letting rumours spread, see Crisis and Emergency Risk Communications: Best Practices [i.3].

When to warn

The decision when to warn is related to the decision whether to warn. Once the risk is quantified and the warning need is identified and the action requested from the affected citizens has been determined, the alert message should be issued as soon as possible. However, low certainty of the available information may cause that the alert issuer waits for more data to increase the certainty of the warning decision. Furthermore, if the warning is issued too early, the available information may not be sufficient to provide accurate recommendations for protective actions. Further update messages should be issued including more details as they become available, see Communication of emergency public warning, A social science perspective and state-of-the-art assessment [i.2], and Warning messages and public response, Social science research findings & applications for practice [i.4].

Where and who to warn

An alert message should be addressed to all people at risk with regard to an occurred or expected incident within the area of authority. This means all people located at a geographical area that is or may be affected by the incident. The definition of the risk area boundaries may depend on the type of incident, existing emergency plans and additional information (e.g. weather forecast). Nevertheless, the public should not be understood as a whole group, but as a set of groups and the alert messages should address all of them. One solution is to issue different messages addressing each group. However, a more efficient solution is to shape the alert messages in a manner that they address all groups with a single message, unless different actions are recommended to different groups.

Consideration should be given to the fact that the area where the alert message is going to be distributed is partly determined by the technology that is used (e.g. radio propagation does not stop at boundaries).

Updating information

After having sent the first alert message, it is important to maintain the communication with the public, updating information when it becomes available until there is sufficient evidence to consider the situation "all clear". As soon as the risk situation is "all clear", a message should be disseminated stating the end of the risk situation to return to normality [i.5] and [i.6]. The frequency to provide update messages should be adapted to the time dynamics of the concrete incident [i.2].

Repeating information

Repeating the alert message through different channels has proven to improve the response efficiency [i.3], [i.5], [i.7] and [i.8]. This is mainly due to two aspects: on the one hand, the repetition through different media reinforces the authenticity of the information; on the other hand, the probability that an individual receives and notices the alert message increases. However, too frequent repetitions (in each channel) may relax the attention of the warning recipient [i.9]. This is especially risky when updated information is disseminated.

4.2.2 The Alert Message

4.2.2.0 Introduction

The content and style of the alert message influence significantly the response capability [i.2]. Optimal alert message style and content are recommended in the following.

4.2.2.1 Alert Message Style

The aspects listed below contribute to the best practice style of alert messages:

Specificity

The incident should be described in a precise, non-ambiguous manner and avoiding information omission [i.10].

Consistency

The alert message should be consistent in its own content and with other alert messages (e.g. with regard to updated information) [i.2] and [i.11].

Accuracy

The alert message should be accurate in the spelling and description of information. The latter aspect refers to formulating open statements with regard to the accuracy of available information [i.11].

Clarity

The alert message should be intelligible by the warning recipients [i.2]. This implies that clear and simple words as well as standard terminology should be applied, whereas technical language, codes, acronyms or jargon should be avoided [i.10].

Credibility

As stated in [i.11], upon warning message reception, the public belief can be strongly affected by the message style. For instance, the credibility of warning messages distributed over radio or video can be differently perceived, depending on the language, the voice tone, and the body language being used.

Therefore, the reliability of the alert message content is always requested by final recipients, so that they can trust the warning information therein provided and take the actions described in the related instructions and assess the risk involved when not taking the described action.

4.2.2.2 Alert Message Content

Each alert message should be tailored to the situation. However, there are general elements that should be part of the information contained in the alert message. Furthermore, the alert message content should include important information in the first place, starting with standardized headlines that summarize the content [i.10] followed by the full message. The way headlines are encoded should be such to avoid overly long messages, so as to keep the overall delivery latency under reasonable threshold and then allow prompt response from the final recipients. The following general elements should be contained in the full alert message to maximize the response capability.

Incident information

This includes a brief **description of the incident event**, its **intensity** level and **likelihood** of the incident event. In particular, intensity refers to the severity of the described incident, in order to inform the recipient about the impact that specific incident might have. Example of intensity scales are those used to classify earthquakes, hurricanes, tornados, and other related severe weather events. As far as likelihood is concerned, it refers to the certainty level of a disaster event occurrence, hence triggering the population to take the adequate measures, as advised by the public authorities. For instance, the certainty of flooding for the population not in close proximity to rivers can be assessed as 'unlikely', whereas it should be classified as 'very likely' for the citizens residing next to the river.

Target Location

The alert message should specify the location that is or could be at risk. This is essential for the warning recipients to understand if they are in or out of the risk area. The target location should be described in terms of geographic areas, recognizable landmarks (e.g. transportation routes, jurisdictional boundaries or recognizable geographical features).

Time information related to the incident

Expected incident impact time and time extent should be included in the alert message. Furthermore, a statement should be included with regard to the relevant time to take protective actions.

Guidance and protective actions

The alert message should include protective actions information, recommendations and guidance to the alert message recipients. The goal of the alert message is to maximize the response capability of the citizens at risk and therefore the incident information alone is not sufficient.

Alert message source (the alert message issuer)

Mentioning the source of the alert message is essential for the credibility of the message and trust of the alert message recipients. This has therefore a high impact on the alert message recipient actionability. The source of the alert message should be a competent authority and it is recommendable that several authorities endorse the message.

Further information sources

Disseminating an alert message could yield an overload of the PSAPs, as the alert message recipients might try to validate the alert message through contact with the authorities. To mitigate this undesired effect, it is recommendable to include sources of further information in the alert message.

However, it is not advised that such information is accessible over the service provider's network, since a huge concurrent access may cause congestion in the service provider's network or on the server where the information is made available.

Sequence

A crisis situation after a hazard onset evolves with time. Several alert messages should be disseminated over time with regard to the same incident. It is therefore important that means are provided to correctly reconstruct the sequence of alert messages corresponding to the same incident to allow the alert message recipients sorting the information appropriately.

4.2.2.3 Size and information quantity

In case of disasters alert messages might need to be distributed with very limited capabilities of the communication lines. Therefore alert messages should be as short as possible, still containing the information elements listed in clause 4.2.2.2 and obeying the style guidelines stated in clause 4.2.2.1.

4.2.2.4 Use of templates for alert messages

The use of templates helps preventing errors and issuing complete alert messages. They may also help in easing multi-language aspects. However, templates should remain sufficiently flexible to accommodate any possible incident.

4.3 Warning Message Recommendation

4.3.1 Conditions to Maximize Actionability Upon Alert Message Reception

Along with the discussion in clause 4.2, the dissemination and communication process maximizes the actionability in the alert message recipient under the condition that the targeted recipients:

- Receive the alert message.
- Notice that there is an alert message.
- Understand the alert message and
- Trust the alert message

Several factors involved in the dissemination and communication function can influence the fulfilment of the conditions above as indicated in figure 4 and further developed below.

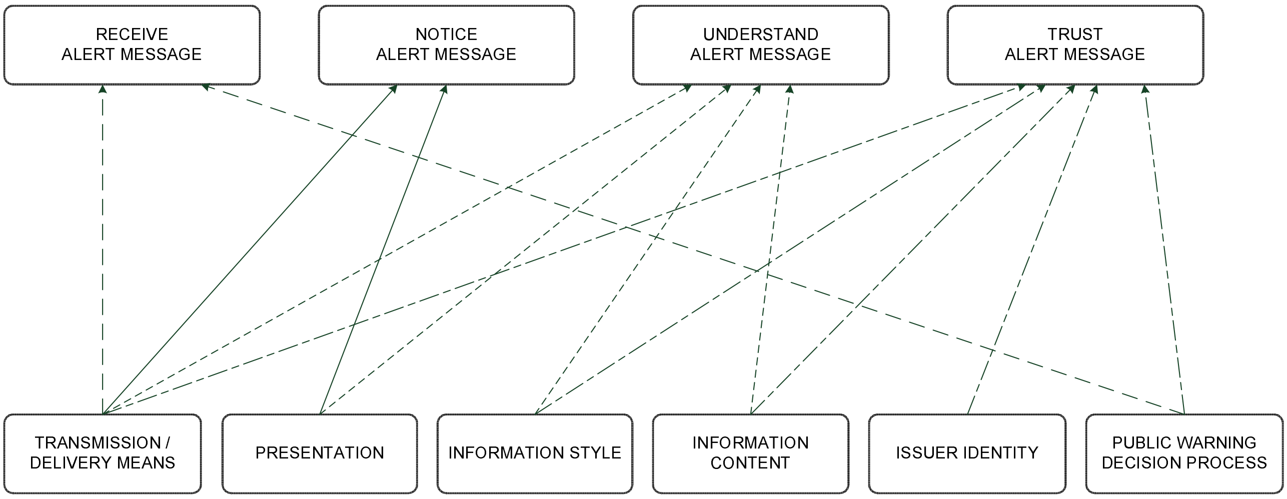


Figure 4: Factors of public warning influencing the response capability

Receive Alert Message

The condition that the targeted recipients actually receive the alert message depends on the use and availability of transmission and/or delivery means and the public warning decision process.

Once the decision whether to warn and when to warn has been made, authorities will make use of means to deliver alert messages to the targeted recipients. These may include any kind of media, sirens, pagers, public screens, alarm systems, communication or entertainment devices (for public and/or private use), etc. The means used may also differ in different regions and countries or even in areas with specific risks, such as chemical, biological, radioactive, nuclear or explosive processing and even earthquakes.

The objective is that the maximum people at risk is able to receive the warning information independently of their context (at home, at work, outdoors, on the move, during day or night) and their habits in the use of communication and entertainment devices. Hence, the use of multiple means to disseminate alert messages has been identified as the most suitable solution to maximize the number of targeted recipients that will actually receive the alert message [i.18], what has been called **Multi-Channel Public Warning.**

Notice Alert Message

The condition that the targeted recipients actually notice that there is an alert message they should pay attention to depends on two main factors. Firstly, the alert message should have been actually received through transmission or delivery means. Secondly, the used transmission or delivery means should be capable of calling the attention of the recipient when an alert message has been received; indicating uniquely that the message is an alert message.

In this context, the multi-channel public warning approach provides additional benefits, since the capabilities of different devices can be combined to increase the probability that the recipient will notice the alert message [i.18].

Understand Alert Message

The correct style and content of the alert message are paramount to achieve that the maximum number of recipients will understand the message, as already mentioned in clause 4.2.2. However, the manner in which the alert message is presented to various recipients is of high importance to address people with special needs. This includes different demographic/socio-economic segments and cognitive capabilities and/or impairments. Hence, human factors should be considered to avoid excluding part of the potentially affected population.

Furthermore, the recipients may receive alert messages through different channels (different, public and/or personal devices). Inconsistencies and/or contradictions in the content and style of the alert message received through different channels will yield confusion. Hence, it is required that alert messages received through different channels are at least consistent. Where possible, they should be identical.

In summary it is expected that the user interface of the device through which alert messages are received is tailored to the specific capabilities. Illustration of possible user interfaces and guidelines to their definition is actually out of the scope of the present document; the interested reader can refer instead to ETSI TR 103 335 [i.21].

Trust Alert Message

Trust is a highly subjective matter. Nevertheless, the alert message issuer can apply best practices to provide adequate trustworthiness to alert messages. Several aspects in the warning decision process and the alert message content and style that contribute to the trust of recipients on the alert message have been discussed in clause 4.2. In terms of warning decision process, adequate decisions in terms of whether to warn (minimize false alarms) and when to warn, as well as adequate repetition of alert messages contribute in the long term to the trust of citizens in alert messages. In the short term, content and style matters are more relevant, i.e. specificity, consistency, accuracy, certainty and clarity of the message, as well as the inclusion of a trustworthy authorized alert message issuer identity, as part of the alert message. The latter refers to an authorized institution, not a specific person.

Alert messages are however issued by specific authorized persons in practice, with the exception of automatized warnings in specific contexts. In the general case, it can be expected that a public warning official will issue alert messages at most in few occasions with long periods of inactivity. Furthermore, the formulation of alert messages by different officials may differ significantly in style (length, order of information items) and even contain errors, ambiguities or miss relevant information items, especially if they are formulated under stress. These shortcomings related to the human factor at the issuer side can negatively influence the trust of recipients in the alert message. Fully standardized alert message style can significantly help minimizing this negative effect, so that it can be guaranteed that alert messages are formulated according to best practice and in a harmonised manner.

Receiving consistent (where possible identical) alert messages through different channels known by the citizens and used by authorities for public warning purposes also boosts trust.

4.3.2 Alert Message Recommendations

Along with the discussion under clause 4.2 and clause 4.3.1, the following minimum recommendations apply to maximize the positive impact of alert messages in the response capability of people at risk [i.3]:

- Alert messages should be delivered through several different channels.
- Alert messages received through different channels should be consistent. The reception of inconsistent alert messages through different channels lead to uncertainty and to mistrust at the recipient side.
- In case the procedures and communication channels used for disseminating alert messages allow for it, the alert messages received through different channels should be identical.
- Alert messages should contain sufficient information about the reported incident. This includes the set of information transported in relevant fields of the Common Alerting Protocol (CAP) [i.12].
- Reference to previous messages related to the same incident.
- The content of the warning message should be formulated in a pre-defined and understandable style, avoiding jargon, complex words and ambiguities.
- The content and style of the alert message should be independent of the officials in charge of warning at a specific point of time, their origin, language skills, age, gender, social crowd, or any other personal and private circumstances.

- The alert message should be presented in appropriate manner to make the information accessible.
- The alert message should be delivered in multiple languages.

4.4 Alerting Library Concept

4.4.0 Introduction

The recommendations listed in clause 4.3.2 can be achieved by the combination of three factors:

- The establishment of standardized procedures to formulate alert messages that contain rules for semantics and syntax, i.e. content and style (information).
- The dissemination of the same (or at least coherent) alert messages through several channels, taking into account the transmission capability of each channel.
- The presentation of alert messages in the language that the recipients understand best and in a mode that the recipient can interpret.

More details about how alert message could be presented to people by means of a user interface can be found in ETSI TR 103 335 [i.21].

4.4.1 Alert message content

Clause 4.3.2 identifies the information items that should be present in the alert message. It is not scalable to create databases with all possible alert messages that could be created in any possible situation and in all languages. However, it appears reasonable to conceive alert messages as a set of coherently formulated information items as identified in clause 4.3.2. From this perspective, it is possible and scalable to create limited dictionaries for each information item identified in clause 4.3.2. The terms included in such limited dictionaries can be then combined in a suitable manner to each specific emergency situation based on minimal and factual input from the warning officials. Combining the limited dictionaries with the official's inputs and additional semantics intelligence, it is possible to create any alert message that is compliant with the targeted standard in any language, provided that the dictionary and semantic rules are available in the wished language.

Table 1: Alert message content

Information Item	Description	Examples	
Hazard Type	A hazard is a potential source of danger or risk. The relevant information to be included in the alert message is the hazard type, i.e. a term that identifies the situation with a single word or a closed expression.		EARTHQUAKE TSUNAMI FOREST FIRE CHEMICAL EXPLOSION, FLASH FLOOD, etc.
Target Location	The location at risk refers to the geographical area in which the alert message is valid. The location at risk can be referred to in different levels of granularity and using different approaches, e.g.: • Administrative area codes. • GPS coordinates to indicate a closed area. • Places of interest.	Administrative encoding: GPS coordinates: Places of interest (encoded):	NUTS (indicating country, region and locality) Centre and radius Polygon Public buildings, etc.
Time	This refers to the time of expected hazard onset. Further time information, such as time of validity/expiration of the alert message and time of warning issuing can be also delivered. The time can be easily encoded using date and time variables for very accurate message. Furthermore, general terms can be used when the available information is not accurate enough.	Date/Time encoding: General terms:	dd/mm/yyyy hh/mm/ss IMMINENTLY, SOON, IN THE NEXT HOUR, TODAY, TOMORROW…
Severity	The severity indicates the level of risk or potential impact. Some intensity scales are widely known for specific types of hazards (e.g. Richter scale for earthquakes). The intensity dictionary can include the applicable intensity levels to specific hazard types if they exist and also incorporate general terms to indicate intensity.	Specific intensity scales: General terms:	Richter, other SEVERE MODERATE LIGHT MINOR…
Certainty	Certainty indicates the level of knowledge that the issuing authority has about the emergency situation. Certainty can be expressed in levels of likelihood, or tagged as "observed" in case of already observed hazard onset.	General terms:	OBSERVED VERY LIKELY LIKELY POSSIBLE UNLIKELY
Protective Action	Response plans can contain pre-established protective actions that are applicable to specific hazards. More complex protective actions can be expressed by combinations of single protective actions.		STAY IN CLOSE WINDOWS GO TO SHELTER
Source	Citizens should know who sent them the message (mayor, chief fire brigade or chief of police); could also be for example EU-Alert if citizens are aware that EU-Alert is a government service.		

The specification of the alerting library should contain all keywords, terms and codes that should be applied to describe any emergency situation. Furthermore, each keyword, term and code should be encoded in a universal manner in order to keep the alerting library 'language-agnostic'. The recommendations for the alerting libraries are provided in clause 5.

4.4.2 Using alerting libraries

An alerting library is defined as a set of limited (but extendable) dictionaries, each of them covering a specific alert message information item as indicated in clause 4.4.1, i.e. containing the keywords and codes applicable to that information item, as shown in the example depicted in figure 5. The concept of using alerting libraries is based on the idea that given an emergency situation, the warning official will select the suitable keywords, terms or codes (where applicable) from the libraries to best describe the emergency situation. Additional intelligence (alert message processing) can be applied to compile a readable and comprehensive alert message from this keyword selection. This can be done in any language provided that the relevant syntax rules are encompassed in or available to the alert message processing function. Moreover, libraries can include information items to be presented in different modes apart from text in order to allow multi-modal presentation of the alert messages. Additional modes could include speech versions of the information items as well as, for instance, videos with the information items expressed in sign language. This would improve social inclusion by allowing people with special needs to receive and understand the message.

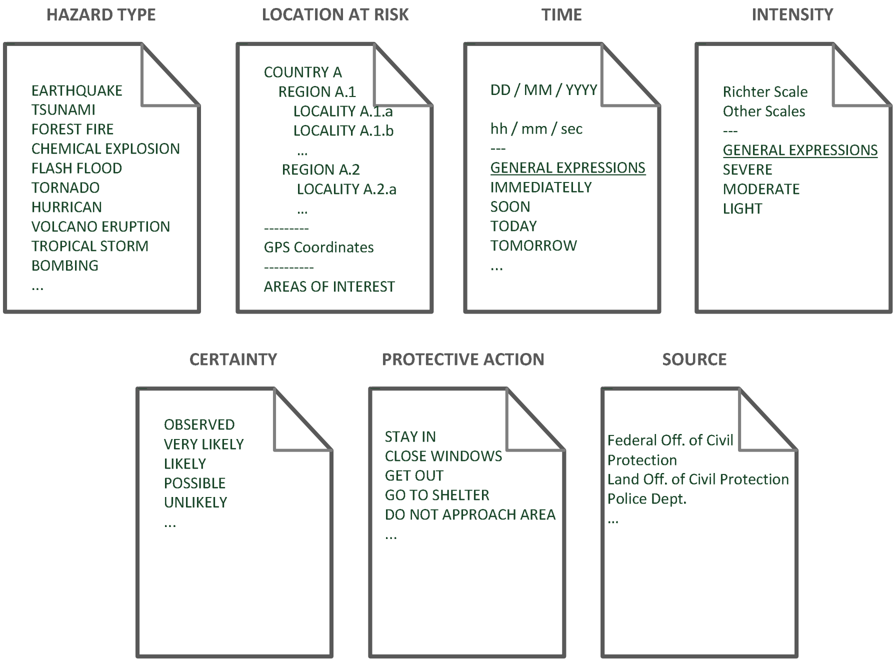


Figure 5: Alerting library structure

4.4.3 Updating alerting libraries

Based on the lessons learnt gathered in incidents/crisis situations and the agreed best practices, alerting libraries can be subject to updates or extensions. The aim of these updates is to improve the syntax and the used terms in order to minimize ambiguity or misinterpretation of the content conveyed in alert messages. Moreover, alerting libraries could be enhanced to fix existing errors or to enrich the currently available language dictionaries. Such operations belong to the class of change management, which is introduced in clause 8, where the indication of the main actors and the related functions is provided.

5 Alerting Libraries Description

5.1 Alerting Libraries Architecture

This clause defines the recommended architecture, structure and reference content of alerting libraries.

Alerting libraries are limited, but extendable dictionaries composed by:

- lists of categorized terms that provide the reference to describe completely the scope and details of an emergency situation in a keyword fashion, under consideration of the recommendations in clause 4;

- a set of sufficient rules that enable the assembly of comprehensive alert messages out of a set of selected terms and metadata.

This architecture is shown in figure 6.

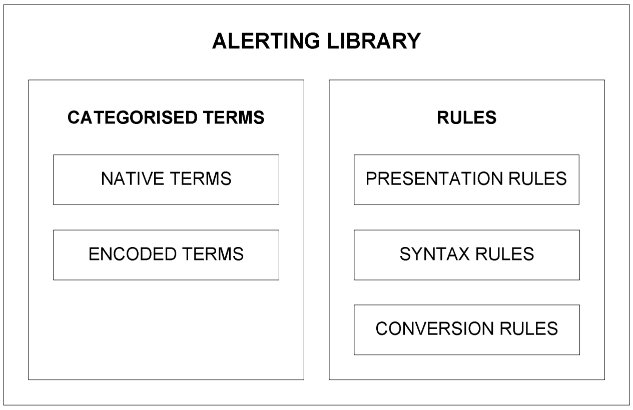


Figure 6: Alerting libraries architecture

The terms in the categorized lists should be universal. For that purpose, it is recommended to assign a unique code to each (native) term. In this manner, a library in a specific language would contain the list of encoded terms (i.e. the list of codes assigned to each term), that is universal, and the corresponding translation of each term in the specific language (i.e. native terms). The recommended reference structure for these categorized lists is provided in clauses 5.2 and 5.3.

Once an emergency situation is fully described by a selection of terms, a message can be formulated by means of syntax and presentation rules. Syntax rules will serve the formulation of clear closed sentences that describe the emergency situation, and the protective action to be taken. Presentation rules will serve the recommendation to present the important information first by means of headlines, followed by a more detailed description. Conversion rules are required to support time and location information, as discussed in clauses 5.4 and 5.5.

In this manner, the dictionary is composed by a language-agnostic and universal reference categorized, the encoded terms, and language-specific details, the native terms and rules. This is suited for scalability aspects, since the minimum required data both at the alert issuer side and at the alert recipient side to communicate with each other is limited to:

- the encoded terms, which are common to both as indicated in figure 7 by the grey colour, and
- the language-specific terms of the preferred language, which are different for each language package, as shown in figure 7 by the different backgrounds.

The rules to interpret alert messages based on alerting libraries are developed in clause 6.

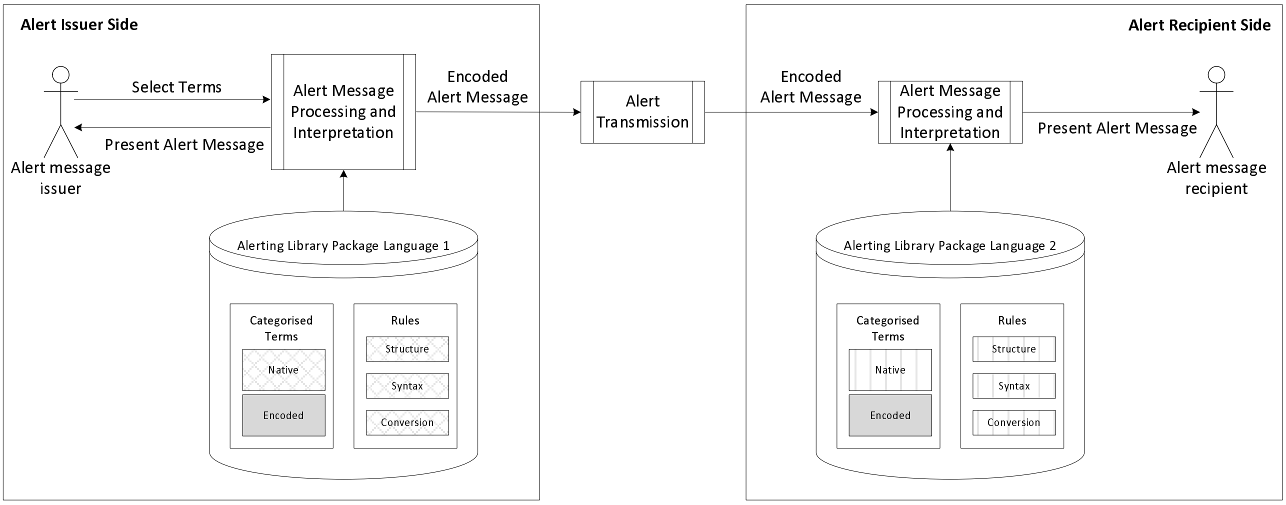


Figure 7: Illustration of alert message creation and presentation at alert issuer and alert recipient sides

The process depicted in figure 7 contains the following steps:

- the alert issuer selects the terms that describe the emergency situation;
- the alert message processing function makes use of the alerting library package to:
  - formulate an alert message that contains the selected terms and is compliant with the presentation, syntax and conversion rules; this message is presented to the alert issuer for validation purposes;
  - create an encoded message that contains the universal (language-agnostic) encoded terms and relevant metadata; this encoded message is transmitted over one or several communication systems after confirmation by the responsible alert issuer;
- at the recipient side, the encoded message is received and interpreted making use of the locally available alerting library package:
  - the encoded message is parsed to identify and translate the terms that describe the emergency situation in the locally available language, i.e. into the native terms;
  - the native terms and the presentation, syntax and conversion rules are applied to formulate a message that is then presented to the alert recipient.

5.2 Alerting Libraries Structure

What follows is a description of the information items that should compose the alert messages and the fields which should be included in the dictionaries. The information items to be included in the dictionaries will be encoded in compression-friendly manner in the language-agnostic library. The language-specific libraries will contain the language-specific terms.

The information items identified in clause 4.4.1 should be processed by the Alert Message Processing and Interpretation module, according to the content included in the alerting libraries to enable the generation of complete and best-practice compliant alert messages based on these libraries. In addition to the information fields that are relevant to the recipient of the alert message, from which a sub-set can be encoded in the alerting library, the alerting library should encompass metadata as well, enabling basic interoperability aspects between warning systems, as shown in table 2.

Table 2: Universal encoded library reference architecture

Information Category	Field	Description	Encoded in library
Hazard information	Hazard type	Term that describes the hazard unequivocally.	Yes
	Category	Classification of hazard in type of impact.	Yes
	Severity	Level of risk.	Yes
	Certainty	Level of knowledge on the hazard information.	Yes
Time	Onset time	Observed or expected time in which the hazard hits the location.	No
	Issuing time	Time at which the alert message was issued.	No
	Expiring time	Time at which the validity or relevance of the warning message expires.	No
Location	Administrative area	Universal unequivocal descriptor of a limited area.	Yes
	Generic area	Area described by coordinates in a geo-referenced mode, e.g. polygon of longitude, latitude points or circle characterized by coordinates of the centre and the radius.	No
Protective Action	Action	Term that describes the action recommended by the issuing authority to be implemented by the recipients.	Yes
	Urgency	Indication of time in which the 'Action' should be implemented.	Yes
Issuer	Authority identity	Universal unequivocal identifier describing a public authority entitled to issue warning messages to the population.	Yes
	Further information	Universal unequivocal identifier of web pages and/or PSAPs where the recipients of warning messages can gather further information about the situation.	No
Metadata	Message identifier	Unequivocal identifier of an alert message.	No
	Incident identifier	Unequivocal identifier of a specific event (defined by hazard type, location and onset time).	No
	Message type	Descriptor to differentiate messages related to the same event.	Yes
	Scope	Targeted audience for a warning message.	Yes
	Status	Descriptor for final purpose of the message (e.g. exercise, real warning, system test, etc.).	Yes
	Sequence number	Message counter within an incident identifier.	No
	Expiration time	Time when distribution of the message should cease.	No
	Administrative distribution area	Universal unequivocal descriptor of a limited area where the message needs to be distributed.	Yes
	Generic distribution area	Area described by coordinates in a geo-referenced mode, e.g. polygon of longitude, latitude points or circle characterized by coordinates of the centre and the radius where the message needs to be distributed.	No

5.3 Alerting Libraries

This clause provides examples and recommendations for the definition of alerting libraries reference content for an exemplary language-specific library (English UK) in table 3.

Table 3: Alerting libraries reference content

Information Category	Field	Content
Hazard information	Hazard type	Earthquake Heavy rain Flash flood Explosion Storm surgens Forest fire Toxic cloud Tsunami Heatwave etc.
	Category	See 'Category' field of the CAP protocol
	Severity	Extreme Severe Moderate Minor Unknown
Metadata	Message type	Warning Alert Information Update Cancel All clear
	Scope	Public Restricted Private
	Status	Actual Exercise System test

Information Category	Field	Content
Location	Administrative area	Name of administrative areas hierarchically organized from municipality to EU level
	Area description	Name of the landmark (if any), 'your area', etc.
Protective Action	Action	Shelter Evacuate Execute Monitor Assess None
	Urgency	Encoding of time frame in minutes hours or days
Issuer	Authority Identifier	List of public warning authorities

5.4 Support of Time Information

The support of time information should be unequivocal in the encoded library. However, the common manner to sort and indicate time information in different countries (using a specific language) might be different. The delivery of alert messages should present the time information according to the standards of the specific language selected by the recipient.

Additionally, time information should be provided using a unique format (for instance, UTC), so that the alert message time information can be related to the local time of the recipient. In order to do this, the Conversion Rules define how to convert time information to the local time in order to present the alert message in the way which is more useful and understandable for the user.

5.5 Support of Location Information

The support of location information, both for identifying the area where the message should be distributed as well as the affected area to be displayed in the alert message, should be unequivocal. However, the common manner to indicate distances in different countries (using a specific language) has an influence when presenting the message to the recipient. The delivery of alert messages should present the location information according to the standards of the specific language selected by the recipient and therefore, this fact is specified in the Conversion Rules to be applied.

5.6 Support of Unique Authority Identification

The support of authority identification information should be unequivocal in the encoded library. For that purpose, the authorities making use of alerting libraries should acquire a unique identifier. A central governance entity for the maintenance of the alerting libraries should deliver such unique identifiers after a registration, authentication and verification process.

The language-specific libraries should contain the legal name of the registered entities and a translation of those in the language of this language-specific library.

5.7 Common Alerting Protocol Compliance

5.7.1 Alerting libraries fields correspondence with CAP fields

The alerting libraries are information data bases to describe alert messages in a compression-friendly manner, so that alert messages can be efficiently abstracted and encoded at the sender side and decoded and assembled at the recipient side. Hence, it is beneficial to pre-define values of each identified field as far as this is possible. The scope of the alerting libraries is therefore partly overlapping with but not completely identical to that of the Common Alerting Protocol. Nevertheless, compliance or compatibility with the CAP protocol is beneficial, so that CAP-based messages can be accommodated in alerting libraries in an easy manner.

The alerting libraries structure described in clause 5.2 (table 2) complies with the Common Alerting Protocol as described in table 4.

Table 4: CAP compliance of the universal message reference content

Information Category	Field	Correspondence with CAP field
Hazard information	Hazard type	<info> <event>
	Category	<info> <category>
	Severity	<info> <severity>
	Certainty	<info> <certainty>
Time	Onset time	<info> <onset>
	Issuing time	<alert> <sent>
	Expiring time	<info> <expires>
Location	Area description	<area><areaDesc>
	Administrative area	<area> <geocode>
	Generic area	<area> <polygon> and <area> <circle>
Protective Action	Action	<info> <responseType>
	Instruction	<info> <instruction>
	Urgency	<info> <urgency>
Issuer	Authority identity	<alert> <sender>
	Further information	<info> <web> and <info> <contact>
Metadata	Message identifier	<alert> <identifier>
	Incident identifier	<info> <incidents>
	Message type	<alert> <msgType>
	Scope	<alert> <scope>
	Status	<alert> <status>
	Sequence number	See clause 5.6.2
	Expiration time	probably <info> <expires>
	Distribution area	probably <area> <polygon> and <area> <circle>

5.7.2 Special cases

It should be noted that the values of specific fields in the alerting libraries proposed in clause 5.2 do not correspond one to one with values in the CAP specification [i.12]. These special cases are described below.

Hazard type

CAP does not foresee a predefined list of hazard types within the field <info> <event>. However, the Alerting libraries should contain a list of potential hazards so that such information can be efficiently encoded.

Message type

The alerting libraries are defined for the sole purpose of sending alert messages to a target audience, not to acknowledge the correct reception or delivery of an alert message in the backward direction. Therefore, the Message type field in the alerting libraries does not include values such as "Ack" and "Error". Compared to the *<alert> <msgType> field in CAP, a*dditional values such as "Warning" and "Information" could be included in the list of potential values to the Message type field to further differentiate the intention of the alert message, for example to be added in the headline of the alert message. The value "All clear" denotes the end of an alert situation.

Sequence number

The intention of a sequence number is that alert messages that correspond to the same event (initial message, several updates, all clear, cancel) can be correctly sorted at the recipient side. The provisions of CAP to enable this feature is to identify each alert message by the triplet:{ *<alert> <sender>; <alert> <identifier>; <alert> <sent>}.* The sequence number could be automatically created by the "Alert Message Processing and Interpretation" module at the recipient side by sorting the alert messages with identical pair { *<alert> <sender>; <alert> <identifier>}* according to the value of the field *<alert> <sent>*.

6 Application of Alert Libraries

6.1 Alert4All Project Approach

In the course of the Alert4All project (A4A) [i.19], the use of alerting libraries has been exploited in order to have a more efficient implementation of alerting message distribution, especially for what concerns the content processing and the translation into the corresponding CAP messages (or any other equivalent alerting message protocol). To this end, two approaches have been considered to make use of alerting libraries: a transparent and an advanced approach.

Transparent approach

The simplest process for composing an alert message by using alert libraries is depicted in figure 8. The process consists of the following steps:

- The warning official (alert message issuer) selects the applicable keyword, term or code for each information item out of the alert libraries.
- The selection is provided as input to the alert message processing function.
- The alert message processing function generates an alert message with the correct syntax in a specific language out of the selected codes and keywords.
- The composed message is then transmitted through different channels and delivered.

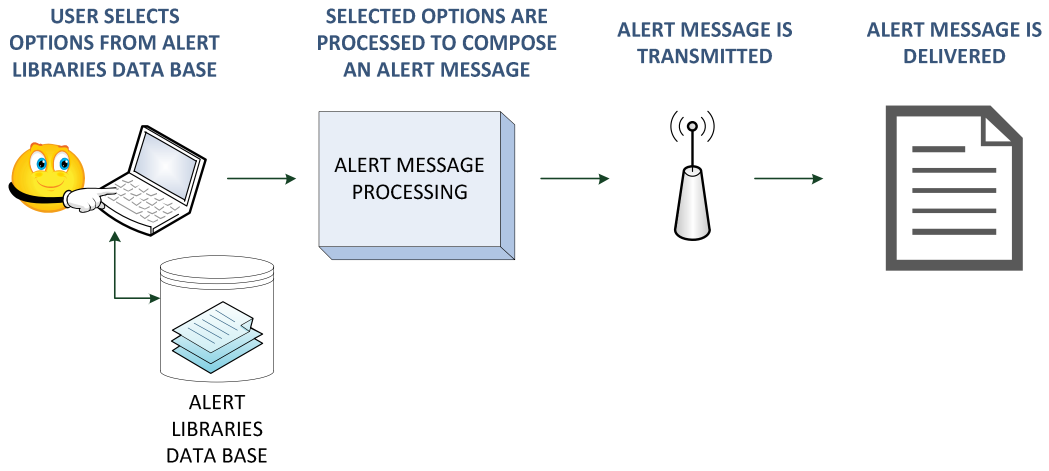

USER SELECTS OPTIONS FROM ALERT LIBRARIES DATA BASE
SELECTED OPTIONS ARE PROCESSED TO COMPOSE AN ALERT MESSAGE
ALERT MESSAGE IS TRANSMITTED
ALERT MESSAGE IS DELIVERED
ALERT MESSAGE PROCESSING
ALERT LIBRARIES DATA BASE

Figure 8: Composing an alert message making use of alerting libraries - Transparent approach

The transparent approach has the following consequences:

- The alert message resulting from the alert message processing function is a readable and comprehensive text (that could be transformed into speech, video, or other media and complemented by icons) in a specific language or languages.
- The languages and media mode delivered by the alert message processing function can be determined in advance or made selectable, so that the alert message issuer can manage it.
- The message outputted by the alert message processing function is transmitted transparently through suitable channels. Hence, the message is delivered to the recipient in the language and media form as outputted by the alert message processing function in case the alert channel can support the delivered media in the receiving devices.

Advanced approach

The use of alert libraries has further potential advantages if more intelligence is built also at the receiving devices. By using smartly the encoding of alerting libraries, the communications channels capacity required to transmit an alert message can be significantly reduced, provided that a suitable communication protocol can support the libraries.

Alert messages are typically described using the Common Alerting Protocol (CAP) [i.12], i.e. into XML "documents". This is very easy to implement but requires significant capacity for the transmission of a message, which can become an issue if the technology to transport the alert message is slow or has low capacity. ASN.1 [i.17] encoding can be applied to compress the CAP messages. However, further compression gains can be achieved by using a protocol that supports inherently the light encoding of libraries. Furthermore, very high flexibility in the presentation of alert messages can be achieved if the intelligence to interpret the alert message is decentralized to the receiving devices [i.18]. This is achievable given the high storage and processing capabilities of state-of-the-art receiving devices that are expected to even increase in future.

Concretely, the advanced approach to make use of alerting libraries is based on the idea that the alert message is only transmitted as a highly compressed code that contains the keyword selection made by the alert message issuer making use of a suitable communication protocol. The receiving devices can parse the coded message and interpret it making use of a locally installed alert message composition function and alerting libraries, both tailored to the preferred language as selected by the user.

The procedure is described in the following and depicted in figure 9:

- The alert message issuer selects the applicable keyword, term or code for each information item out of the alerting libraries.
- The selection is provided as input to the alert message processing function.
- The alert message processing function generates an encoded and highly compressed message out of the selected codes and keywords and embeds it into a suitable communication protocol.
- The encoded message is transmitted over several communication channels.
- The encoded message is received by receiving devices that contain local alerting libraries and a local alert message composition engine tailored to the selected language by the user.
- The encoded message is given as input to the local alert message composition function.
- The alert message composition function parses the protocol to extract and decode the information items of the alert message.
- The alert message composition function formulates a readable and coherent message out of the extracted information items.
- The alert message composition function provides means to present the alert message in a suitable manner to the recipient.

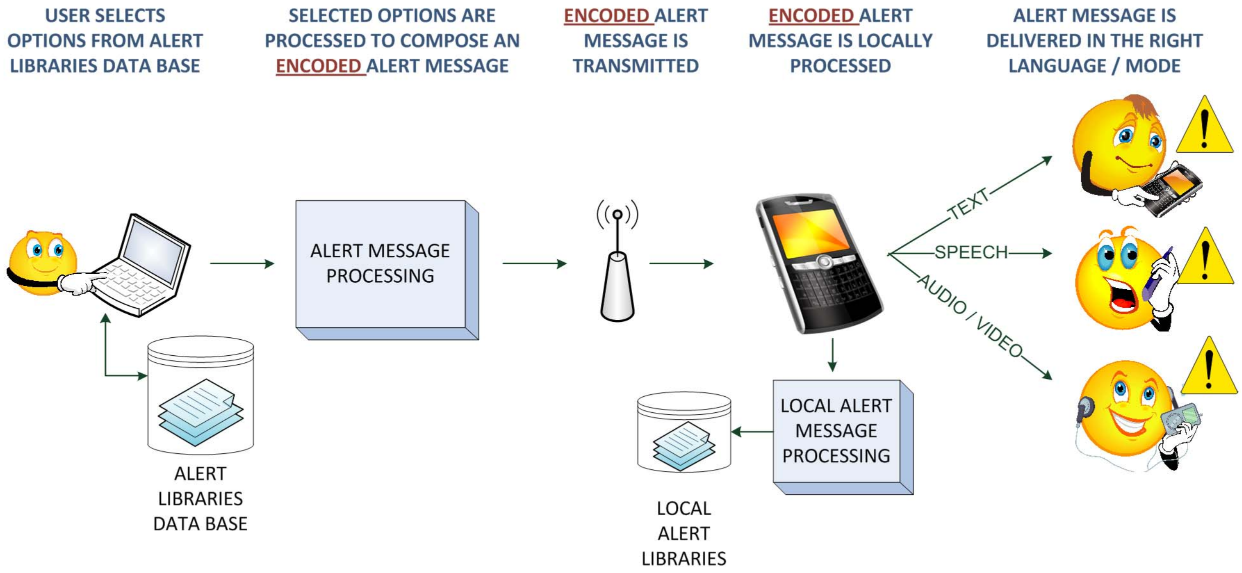

USER SELECTS OPTIONS FROM ALERT LIBRARIES DATA BASE
SELECTED OPTIONS ARE PROCESSED TO COMPOSE AN ENCODED ALERT MESSAGE
ENCODED ALERT MESSAGE IS TRANSMITTED
ENCODED ALERT MESSAGE IS LOCALLY PROCESSED
ALERT MESSAGE IS DELIVERED IN THE RIGHT LANGUAGE / MODE
ALERT MESSAGE PROCESSING
TEXT
SPEECH
AUDIO / VIDEO
ALERT LIBRARIES DATA BASE
LOCAL ALERT MESSAGE PROCESSING
LOCAL ALERT LIBRARIES

Figure 9: Composing an alert message making use of alerting libraries - Advanced approach

6.2 Examples of message translation

6.2.1 CMAS approach

This clause describes the generation of the CMAS text message based upon received CAP parameters as described in annex A of J-STD-101 [i.13].

The Federal Alert Gateway aggregates CAP messages received from alert message issuer, converts those messages to CMAS messages and transmits them to the mobile network operators. If a free form text message is not provided as part of the CAP message, then the Federal Alert Gateway "constructs" a text message automatically.

Automatically generated CMAS text messages using CAP fields may not provide the accuracy that alert message issuers are looking for or may not even result in meaningful messages. Two years after CMAS, now called Wireless Emergency Alert (WEA), went life most of the CMAS text messages are written by alert message issuers and not "constructed" by the Federal Alert Gateway.

A text message is constructed along the following format:

- What is happening.
- What area is affected.
- When the alert expires.
- What action should be taken.
- Who is sending the alert.

In case of weather related events the optional eventCode CAP element should be populated with a value to identify the type of weather alert. That value will be used to determine the text that describes the event. For example, FLW will be translated into "A flood warning". All other event codes can be found on the website of the US National Weather Service [i.20].

If the eventCode element is not populated the text that will be transmitted will be derived from the category element. For example the category element value Fire will be translated into "A fire warning". All other category element values can be found in CAP v1.2 [i.12].

The description of the area where the event occurs is provided in the CAP message as a textual description of unrestricted length in the areaDesc element. For CMAS use the affected area should be described with the text: "in this area", because the message is broadcast in the affected area.

The expiration time will be determined from the optional expires CAP element. If this element is not populated, the expiry time should be set to 24 hours from the onset in a 12 hour/Time zone format (i.e. "until 7:00AM PDT").

The response description should be taken from the optional responseType CAP element. For example the responseType element value Shelter should be translated into "Take shelter now". All other responseType element values can be found in CAP v1.2 [i.12]. If this element is not populated, the text alert message should contain a standard phrase such as "Check local media for info".

The sender should be added at the end of a CMAS message and is determined by the Federal Alert Gateway from the CAP element sender.

CMAS messages can be provided in English and in Spanish. The conversion from CAP elements to messages in either English text or Spanish text is performed as shown in tables 5 to 9.

Table 5: Event description

CAP element	Value	English Text	Spanish Text
category	Met	Severe Weather Warning	Advertencia meteorológica severa
	Safety	Public Safety Warning	Advertencia de seguridad pública
	Fire	Fire Warning	Advertencia de fuego
	Geo	Geologic Warning	Advertencia geológica
	Security	Security Warning	Advertencia de seguridad
	Rescue	Rescue Alert	Alarma de rescate
	Health	Health Warning	Advertencia de salud
	Env	Environmental Warning	Advertencia ambiental
	Transport	Transport Alert	Alarma de transporte
	Infra	Infrastructure outage	Apagón de infraestructura
	CBRNE	Hazardous Threat	Amenaza peligrosa
	Other	An alert has been issued	Un alerta ha sido emitida
eventCode	TOR	Tornado Warning	Aviso de tornado
	VOW	Volcano Warning	Aviso de actividad volcánica
	SVR	Severe Storm Warning	Aviso de tronada severa
	EQW	Earthquake Warning	Aviso de terremoto
	TSW	Tsunami Warning	Aviso de tsunami
	BZW	Blizzard Warning	Aviso de ventisca
	DSW	Dust Storm Warning	Aviso de vendava
	FFW	Flash Flood Warning	Aviso de inundaciones repentinas
	HWW	High Wind Warning	Aviso de vientos fuertes
	HUW	Hurricane Warning	Aviso de huracán
	TRW	Tropical Storm Warning	Aviso de tormenta tropical
	WSW	Winter Storm Warning	Aviso de tormenta de nieve
	CFW	Coastal Flood Warning	Aviso de inundaciones costeras
	FLW	Flood Warning	Aviso de inundación
	FRW	Fire Warning	Aviso de fuego
	SMW	Special Marine Warning	Aviso marítimo especial
	AVW	Avalanche Warning	Aviso de avalancha
	CDW	Civil Danger Warning	Aviso de peligro civil
	CEM	Civil Emergency	Mensaje de emergencia civil
	HMW	HazMat Warning	Aviso de materiales peligrosos
	LEW	Police Warning	Aviso de las autoridades de la ley
	CAE	AMBER Alert	Emergencia de rapto de menores
	NUW	Nuclear Power Plant Warning	Aviso de riesgo nuclear
	RHW	Radiological Hazard Warning	Aviso de peligro radiológico
	LAE	Local Area Emergency	Emergencia del área local
	EAN	President has issued an alert	El president ha emitido un alerta

Table 6: Affected Area

CAP element	Value	English Text	Spanish Text
N/A	N/A	in this area	Esta área es afectada

Table 7: Alert expiration

CAP element	Value	English Text	Spanish Text
expires	Text string which provides the expiration time of the information of the alert message in [dateTime] format	Translated to an event expires time in a 12 hour format (i.e. Until 7:00AM PDT)	Translated to an event expires time in a 24 hour format (i.e. hasta 7:00AM PDT)

Table 8: Actions to be taken

CAP element	Value	English Text	Spanish Text
eventCode	SPW	Take Shelter Now	Aviso de refugio
	EVI	Evacuate Now	Evacuación inmediata
responseType	Shelter	Take Shelter Now	Aviso de refugio
	Evacuate	Evacuate Now	Evacuación inmediata
	Prepare	Prepare for Action	Prepárese para la acción
	Execute	Execute Action	Realice la acción
	Monitor	Monitor Radio or TV	Compruebe nedios de noticias para información
	Avoid	Avoid hazard	Evite peligro

Table 9: Alert sender/originator

CAP element	Value	English Text	Spanish Text
CMAC_sender_name	Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g. may be based on an Internet domain name - could also come from the sender's name in the trust model.	Translated to an acronym or short abbreviation picked by the sender. See note 1.	Same as English version. See note 2.
NOTE 1: URLs, phone numbers, and email addresses are not sent to the mobile device. NOTE 2: URLs, phone numbers, and email addresses are not sent to the mobile device.			

6.2.2 Munich shooting on 22.06.2016

On Friday the 23rd of June 2016, a shooting took place in the shopping mall Olympia Einkauf Zentrum (OEZ) in Munich, resulting with 10 victims (including the murderer who committed suicide after the attack) and another 36 were injured. In the hours following the attack, the federal police distributed warning messages to the population in the form of posts in different social networks, which appeared in different languages in order to reach as many citizens as possible also taking into account the multi-national composition of Munich's population.

The summary of the original delivered messages is reported in table 10, subdivided per language:

Table 10: Warning messages,
Original heading: 'Polizei München @PolizeiMuenchen 22. Juli'

# Message/ Language	German	English	French	Turkish
1	+++ACHTUNG+++ Meiden Sie die Umgebung um das #OEZ - Bleiben Sie in Ihren Wohnungen. Verlassen Sie die Straße!+++	There has been gunfire - the Situation is unclear. we will keep you informed #munich #west #moosach	S'il vous plait restez a la maison a munich, pas dans les rues! #münchen, #oez, #schießerei	Silahli catisma ile yeni bilgeri size aktariyoruz.
2	Lage am #OEZ mit #Schießerei ist aktuell noch unübersichtlich. Es gab mehrere Verletzte. Sobald wir mehr haben gibt es weitere Infos.	There is Police Action at the Olympiaeinkaufszentrum #oez #munich #west #gunfire	On va écrire quand nous avons plus d'informations! #Schießerei, #münchen, #oez	Münich Hanauerstraße, Olympia Alisverismerkezinde Silahli saldiri gerceklesti
3	Meiden Sie öffentliche Plätze in #München. Die Lage ist noch unübersichtlich. #oez #Schießerei	The suspects are still on the run. Please avoid public places. #munich #oez #gunfire	S'il vous plait évitez le public pour le moment a Munich. #München, #oez, #schießerei	Su ana kadar bilinmedik sayida yaralilarimiz var
4		Please avoid public areas in #Munich right now. #gunfire		Saldiri dolaysiyla 6 kisi malesef hayatini kaybetdi
5				Saldirganlar halen yakalanamadi, lütfen evlerinizi terk etmeyin. Kalabalik yerlerden uzak durunuz

According to the information contained in the various messages, it is possible to make use of alerting libraries, on the basis of the following template.

Table 11: Alert library example

Hazard type:	GUNFIRE
Target location:	Munich, Munich-Moosach
Time:	22 July; 17:45
Severity:	SEVERE
Certainty:	OBSERVED
Protective action:	Please leave the streets, stay inside and avoid public places.
Source:	Police Department Munich

In this way a more synthetic representation of the message can be obtained, hence simplifying the generation of the message and the eventual distribution. In particular, the main advantage of using alerting libraries in this case would consist in mapping each field content to a given bit-string that can definitely reduce the size of transmitted messages. Moreover, each message can be easily translated in the recipient's language, provided that a proper translation engine is available in the recipient's device.

More details about the parsing operations and the related translation functions are implementation specific and therefore beyond the scope of the present document.

7 Recommendations for Alert Message Assembly Rules

7.1 Introduction

The process depicted in figure 7 (clause 5) includes the function to interpret the alert message. Inputs to this function are:

- an encoded alert message, in compliance with the recommendations made in clauses 4 to 5;
- the alerting library package of at least one language.

The function to interpret the alert message will make use of the structure, syntax and conversion rules contained in the alerting library package to formulate a human-readable alert message out of the input encoded alert message.

This clause provides recommendations to define structure, syntax and conversion rules that can be applied to enable the implementation of an alert message interpretation function. Furthermore, a guideline in an example language (English) is provided as well.

For the avoidance of doubt, the structure rules addressed in the present document relate to the formulation of alert messages. Recommendations for multi-modal presentation of alert messages, as well as the use of pictograms to guarantee accessibility are addressed in ETSI TR 103 335 [i.21].

7.2 Principles of Alert Message Assembly

7.2.0 Overview

The formulation of an alert message based on the input encoded message and the alerting library package should be kept as simple as possible. However, for an alert message to be actionable, it is also recommended to include sufficient information as described in clause 4.2.2.2 and to apply the style recommendations described in clause 4.2.2.1.

A simple, but effective approach to address these recommendations is the use of templates that enable sufficient flexibility to accommodate any kind of emergency situation. Furthermore, in accordance with the recommendation made in clause 4.2.2.2, the alert message should contain the most important information first, in the form of a headline, followed by the details. Accordingly, it is recommended to organize the rules for the alert message formulation in a hierarchical manner as shown in figure 10. This hierarchy starts from very high level information organization rules (structure rules), goes through syntax rules to formulate specific sentences and completes the picture with detailed rules that avoid ambiguities (conversion rules).

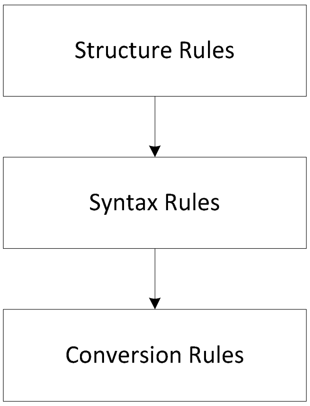


Figure 10: Structure of alert message assembly rules

7.2.1 Structure Rules

Structure rules define the number of sentences, their scope and their order of presentation to formulate a complete alert message in a generic manner, i.e. regardless of the type of hazard, its severity, likelihood, etc.

Example structure rules are provided in clause 7.3 for English.

7.2.2 Syntax rules

For the sentences required by the structure rules, the syntax rules define the procedure to formulate each specific sentence according to the input terms and available metadata.

Example syntax rules are provided in clause 7.4 for English.

7.2.3 Conversion rules

The information that should be contained in an alert message includes references to time and location, where the latter could be also formulated including distances. As stated in clauses 5.3 and 5.4, the presentation of these information items should be facilitated taking into account the relevant standards in the local language of the alert message recipient. Conversion rules serve exactly this purpose, i.e. they should define the format to correctly formulate time and location information in the language contained in the library.

Example syntax rules are provided in clause 7.5 for English.

7.3 Example Structure Rules for Text in English

An example alert message structure for a first alert message or update alert message could be as follows:

<Headline>

<Event description>

<Protective action>

<End line>

The scope of each element is listed below:

- <Headline> is the title of the message, containing only the basic information.
- <Event description> contains the information about the emergency event.
- <Protective action> contains the information about the recommended protective action.
- <End line> is a standard sentence containing a reference to the web site where more information can be found.

The syntax that should be applied to each of these building blocks is described in clause 7.4.

For release messages, i.e. messages indicating that the emergency situation has been released, the message structure can be simplified as follows:

<Release Headline >

<Release Body>

<End line>

The syntax that should be applied to each of these building blocks is described in clause 7.4.For cancel messages, i.e. messages indicating the cancellation of a previously sent message, the following structure could be applied:

<Cancel Headline >

<Cancel Body>

<End line>

7.4 Example Syntax Rules for Text in English

7.4.1 Syntax of First and Update Messages

The example basic syntax for each building block of first and update alert messages is described in table 12.

The syntax description makes use of fields that should be fixed depending on the input data to the alert message processing and interpretation function:

- <Label>
- <Hazard type>
- <Date>
- <Location>
- <Authority>
- <Verb>
- <Certainty>
- <Time>
- <Action>
- <Urgency>
- <Severity>
- <Additional info>
- <Web>

Table 12: Basic syntax of first and update alert messages

Field	Message Sequence	Condition	Syntax	Comment
<Headline>	First message	-	*<Label>. <Hazard type> <Date> in <Location>.*	The <Headline> syntax is described in table 5.
	Update message	-	*(Update) <Label>. <Hazard type> <Date> in <Location>.*	

<Event description>	First message	If {
		..Certainty field = "Observed"
		}
			The <Authority> <Verb> about <Hazard type> observed in <Location> <Date> at <Time>, approx. Intensity: <Severity>.	The <Event Description> is described in table 6.
				Specific fields that only appear in update messages are described in table 7.
				The <Verb> applied in the sentence will depend on the type of message (alarm, warning or information) and the <Certainty> is formulated according to the input certainty value.
				The formulation of the <Date> field is decided upon comparison of the date with the current date to formulate the message in friendlier manner.

		Otherwise	*The <Authority> <Verb> about <Certainty> of <Hazard type> in <Location> from about <Date> at <Time>, approx. Expected intensity: <Severity>.*	

	Update message	If {
		..Certainty field = "Observed"
		}
			The <Authority> <Verb> that the risk of <Hazard type> in <Location> <Certainty description> <Date> at <Time>, approx. <Severity description>.	

		Otherwise	*The <Authority> <Verb> about <Event type> observed in <Location> <Date> at <Time>, approx. <Severity description>.*	
<Protective action >	First message	-	*Please, <Action> <Urgency>.*	The <Protective Action> syntax is described in table 8.
	Update message	-		
<End line>	First message	-	*More info at <Web>.*	The <End line> syntax is described in table 9.
	Update message	-		

Table 13: <Headline> fields description

Field	Description	Relevant Reference	Condition	Assigned Value

<Label>	This field can take one of the following values:
	• Alarm
	• Warning
	• Information
	The assignment of the right value depends on the values of the input "Certainty" and "Severity" as stated in the "Condition" cell of this table.
		"Certainty" And "Severity"	If {
			Certainty = "Likely"
			OR
			Certainty = "Observed"
			OR
			Severity = "Extreme"
			OR
			Severity = "Severe"
			}
				"Alarm"

			If {
			Certainty = "Unlikely"
			AND
			Severity = "Minor"
			}
				"Information"

			Otherwise	"Warning"
<Hazard type>	This field should be filled with the hazard type input.	"Hazard type"	-	Value of Hazard type
<Date>	This field should be filled with the input onset date.	"Onset"	-	Value of "Onset"
<Location>	This field should be filled with the input location description.	"Location"	-	"Location"

Table 14: <Event Description> fields description for first and update messages

Field	Description	Relevant Reference	Condition	Assigned Value
<Authority>	Name of the corresponding authority corresponding to the authority identifier in table 3.	"Authority identifier"	N/A	N/A
<Verb>	A value should be assigned to this field that depends on the value of the "Label" field of the <Headline>.	"Label" field in <Headline>	If {Label = "*Alarm*"}	"alerts"
			If {Label = "*Warning*" }	"warns"
			If {Label = "*Information*" }	"informs"
<Certainty>	A value should be assigned to this field that depends on input "certainty".	"Certainty"	If {Certainty = "*Observed*"	"Observed"
			If {Certainty = "*Likely*"}	"High risk"
			If {Certainty = "*Possible*"}	"Medium risk"
			If {Certainty = "*Unlikely*"}	"Minor risk"
			If {Certainty = "*Unknown*"}	"Risk"
			If {Certainty = *Free Text*}	Free Text
<Hazard type>:	Input hazard type.	Hazard type	-	Value of "Hazard type"
<Location>	This field should be filled with the input location description.	Location	-	Value of "Location"
<Date>	Date included in the input "onset" time.	Date in "onset time"	If { "onset" is the same as the current date}	"today (dd/mm/yyyy)" See note.
			If {"onset" coincides with the day after the current date}	"tomorrow (dd/mm/yyyy)" See note.
			Otherwise	"dd/mm/yyyy"
<Time>	Time included in the input "onset". The time zone should not be included. Time is always supposed to be local time.	"onset"	-	"hh:mm" See note.
<Severity>	Severity description in the input "severity"	"Severity"		Value of "Severity"
NOTE: The format depends on the relevant conversion rules.				

Table 15: Additional <Event Description> fields specification for update message

Field	Description	Relevant Reference	Condition	Assigned Value
<Certainty description>	The alert message interpretation function should check if the "certainty" value has changed with respect to the previously received alert message. The message will specify in the text if the certainty continues to be the same or has varied.	"Certainty"	If the value of "Certainty" did not change with respect to previous message	"*Certainty continues to be*: <value of certainty field>"
			If the value of "Certainty" changed with respect to previous message	"*Certainty has changed to:* <value of certainty field>"
<Severity description>	The alert message interpretation function should check if the "severity" value has changed with respect to the previously received message. The message will specify in the text if the severity continues to be the same or has varied.	"Severity"	If the value of "Severity" did not change with respect to previous message	*"Intensity continues to be*: <value of severity field>"
			If the value of "Severity" changed with respect to previous message	*"Intensity has changed to*: <value of severity field>"

Table 16: <Protective Action> fields specification

Field	Description	Relevant Reference	Condition	Assigned Value
<Action>	The formulation of <Action> depends on the input value of "Protective action" in table 3.	"Protective action"	If { Protective Action = "*Shelter*"}	*"Take shelter"*
			If {Protective Action = "*Evacuate*"}	*"Evacuate"*
			If {Protective Action = "*Prepare*"}	*"Get prepared"*
			If { Protective Action = "*Execute*"}	*"Follow instructions"*
			If { Protective Action = "*Monitor*"}	*"Monitor"*
			If { Protective Action = "*None*"}	*"No action required"*
			If { Protective Action = *Free text*}	*Free text*
<Urgency>	The formulation of <Urgency> depends on the input value of the "urgency" in table 3.	"urgency" field in CAP	If { urgency = "*Immediate*"}	*"Immediately"*
			If { urgency = "*Expected*"}	*"Within next hour"*
			If { urgency = "*Future*"}	*"Within next 1 to 10 hours"*
			If { urgency = "*Unknown*"}	-
			If { urgency = *Free text}*	*Free text*

Table 17: <End line> fields specification

Field	Description	Relevant Reference	Condition	Assigned Value
<Web>	link hyperlink for the web site where more information can be found, as can be found in the "Issuer; Further information" field in table 3.	"Issuer; Further information"	-	Value of "Issuer; Further information"

7.4.2 Syntax of Release Messages

Table 18: Release message syntax description

Field	Syntax	Comment
<Release Headline>	*Released* <Headline>.	It refers to the <Headline> of the corresponding general message as described in table 5.
<Release Body>	*The* <Authority> *informs that the alert situation started on* <Date> *in* <Location> *is now released.*	<Authority>, <Date> and <Location> refer to the same fields of the corresponding general message as described in table 6.
<End Line>	*More info at* <web>.	<web> is as described in table 9.

7.4.3 Syntax of Cancel Messages

Table 19: Cancel message syntax description

Field	Condition	Syntax	Comment
<Cancel Headline>	-	*"Cancellation Message".*	-
<Cancel Body>	If one message is cancelled	*The* <Authority> *informs that the alert message with ID: <ID> has been cancelled.*	<Authority> is as described in table 6. <ID> and <List of IDs> correspond to the combination of <incident identifier> and <sequence number> metadata.
	If a list of messages are cancelled at once	*The* <Authority> *informs that the alert messages with ID: <List of IDs> have been cancelled.*	
<End Line>	-	*More info at* <web>.	<web> is as described in table 9.

7.5 Example Conversion Rules for Text in English

The conversion rules will provide the format in which time and location information should be presented. Some examples follow.

Example rules for the presentation date information:

- [mm-dd-yy]
- [mm-dd-yyyy]
- [dd-mm-yyyy]
- [dd/mm/yy]
- [mm-dd]
- [dd-mm]
- [dd/mm]
- etc.

Example rules for the presentation of time information:

- [hh:mm:ss]
- [hh:mm]
- [hh:mm:ss] CET +/- (local time use)
- etc.

Examples for the presentation of location information in terms of distances:

- Meters
- Kilometers
- Miles
- etc.

For distance and time information, it is also recommended that the universal encoded terms include a universal reference system for distance and time information. The conversion rules should then include the needed information to implement conversion calculations

8 Change Management

The libraries can be enriched with time extending them with additional language packages, new relevant terms, etc. Additionally, corrections might be applied to terms and rules (structure, syntax, conversion or presentation) when errors, unintended behaviour or any shortcomings are identified so as to guarantee the effectiveness of public warning.

To this end, it is recommended to define (i) a unique entity that is entitled to manage, maintain and update alerting libraries (e.g. a Library Management Entity (LME)) and (ii) a change management process including relevant actors and procedures that enable the management, maintenance and updating of alerting libraries so that official alerting library updates can be issued when required. Furthermore any changes to alerting libraries that may be requested need to be carefully assessed and only approved under favourable circumstances and in the positive case, the change implementation needs to be checked according to quality criteria. Only approved and quality-checked changes might be incorporated in an updated alerting libraries' issue. These steps should therefore be part of the change management process and may involve several actors.

Exemplary actors involved in a change management procedure are listed in table 20, where also the main functions are illustrated.

Table 20: Actors in the Change Management Process

Actor	Short name	Description	Functions
User Community	-	Involves all actors that have an interaction with the alerting libraries, either as consumer (user) or as part of the LME.	-
User	-	A member of the user community that issues a change request.	Propose a change request.
LME Point of Contact	LME PoC	Interface of the LME towards the user.	Receive change requests. Start the change request process in the LME.
LME Technical Committee	LME TC	Set of experts with sufficient knowledge to assess the feasibility, need, risks and impact of a change request from the technical perspective and to develop and implement change proposals.	Assess feasibility, need, risks and impact of a change request (technical perspective). Develop change proposals. Implement change proposals. Update change proposals in response to shortcomings report from the LME QCC.
LME Approval Committee	LME AC	Formal entity in the LME with the competence to approve the change process, under consideration of the recommendation from the LME TC.	Evaluate change requests from a global perspective. Approve or reject change requests.
LME Quality Control Committee	LME QCC	Set of experts with sufficient knowledge to assess the coherence and quality of draft updated libraries.	Review draft updated libraries in consideration of overall coherence and quality. Approve draft updated libraries. Provide shortcoming reports to the LME TC.
LME Certification Committee	LME CC	Entity in the LME to complete the formal process of certification and publishing of new libraries.	Formal step to assign the "certified" status to approved new libraries. Publishing of new libraries towards the user community.

The specification of the interfaces between the different actors involved in these operations is outside the scope of the present document.

History

Document history		
V1.1.1	December 2016	Publication