Best practices on Public Warning Systems for Climate-Induced Natural Hazards

Abstract: This study presents an overview of the Public Warning System, focusing on approaches, technical standards and communication systems related to the generation and the public sharing of early warnings. The analysis focuses on the definition of a set of best practices and guidelines to implement an effective public warning system that can be deployed at multiple geographic scales, from local communities up to the national and also transboundary level. Finally, a set of recommendations are provided to support decision makers in upgrading the national Public Warning System and to help policy makers in outlining future directives.

Authors: Claudio Rossi
Giacomo Falcone
Antonella Frisiello
Fabrizio Dominici

Version: 30 September 2018
Table of Contents

List of Figures.......................................................................................................................... 2
List of Tables.............................................................................................................................. 4
Acronyms................................................................................................................................. 4
Core Definitions ....................................................................................................................... 7
1. Introduction .......................................................................................................................... 10
   1.1 Motivations ................................................................................................................... 10
   1.2 Topics and goal of the study ....................................................................................... 12
2. Solutions and approaches on DRM .................................................................................... 14
   2.1 Crisis Communication ................................................................................................. 16
   2.2 Human Factors and Public Warning ........................................................................... 18
   2.3 UN guidelines .............................................................................................................. 20
3. Technical Standards ............................................................................................................. 23
   3.1 Standards and requirements for Public Warning systems implementation ............... 23
   3.2 The Common Alerting Protocol (CAP) ...................................................................... 28
4. Overview of selected Public Warning Systems ..................................................................... 33
   4.1 Macro level case studies ............................................................................................. 33
   4.1.1 USA ........................................................................................................................ 33
   4.1.2 European Union ...................................................................................................... 36
   4.2 European national and local case studies .................................................................... 39
   4.3 Use cases recap ............................................................................................................ 50
5. Recommendations ............................................................................................................... 52
   5.1 Organizational best practices ..................................................................................... 52
   5.2 System architecture ..................................................................................................... 54
   5.3 Use of technical standards .......................................................................................... 59
   5.4 Guidelines on styling for media adaptation ............................................................... 62
6. Future outlooks .................................................................................................................... 69
7. References ........................................................................................................................... 76
Annex I – Guidelines on technical specification for Public Warning Systems ......................... 79
Annex II – Script Interview on Future perspectives on PWS .................................................... 82

List of Figures

Figure 1 – European natural disaster loss from 2007 to 2017, summing up to 173 billion EUR. .... 10
Figure 2 – Recent Disaster (2005-2014) impacts considering the economic damage (USD), people affected and people killed (top), and top 10 countries worldwide by the number of disasters (bottom) ........................................ 11
Figure 3 - DRM Ecosystem ................................................................................................................ 15
Figure 4 - The four elements of systematic people-centred DRM ...................................................... 15
Figure 5 - Emergency Risk Communication Lifecycle ......................................................................... 16
Figure 6 – Effectiveness of warnings in reducing damages in function of the lead time (anticipation) ....................................................................................................................... 18
Figure 7 - The Sendai framework for DRR .......................................................................................... 21
Figure 8 - UNDP’s work in DRR ......................................................................................................... 22
Figure 9 - CAP v1.2 Document Object Model ..................................................................................... 29
Figure 10 – Example of CAP message ................................................................................................. 32
Figure 11 - IPAWS Architecture ......................................................................................................... 34
Figure 12 - Exploitation of the IPAWS infrastructure by Google Public Alerts system .................... 35
Figure 13 - Example of an IPAWS alert published by google and available through its tools ........ 35
Figure 14 - EFAS European flood archive prototype ......................................................................... 37
Figure 15 - Fire Weather Index from EFFIS on July 25, 2018 ............................................................. 38
Figure 16 - Colour-coded warnings in the European regions involved in Meteoalarm service ........ 39
Figure 17 - NL-Alert text message example ....................................................................................... 40
Figure 18 - Coverage area of a siren system for a flooding ............................................................... 41
Figure 19 – CeCAT Bulletin for avalanches ....................................................................................... 43
Figure 20 - Meteo-Hydrological warning bulletin issued by ARPA Piedmont .................................. 44
Figure 21 - Meteo-Hydrological CAP warning message issued by ARPA Piedmont ....................... 45
Figure 22 - Structure of the Modular Warning System (MoWaS) ....................................................... 46
Figure 23 - Snapshot of NINA mobile application ............................................................................ 47
Figure 24 - Flood Information Service homepage on 27th November 2017 .................................. 48
Figure 25 - 5-day flood risk bulletin, from 30th July 2018 to 3rd August 2018 .......................... 48
Figure 26 - Snapshot of the Flood Information System Dashboard .................................................. 49
Figure 27 – Suggested PWS approach ............................................................................................. 55
Figure 28: Comparison between CAPEX model (a) and OPEX model (b). ........................................ 55
Figure 29 - Suggested PWS architecture .......................................................................................... 56
Figure 30 - Suggested Public Warning Subsystem for sirens ............................................................ 57
Figure 31 – FAQ on the sirens ........................................................................................................... 64
Figure 32 – An SMS alert structure derived from CAP. Note that the temporal information is not included in this example. .......................................................... 65
Figure 33 – CAP warning message showed on a web platform. This example refers to a flood alert issued by the UK Environmental Agency and integrated in the I-REACT system

Figure 34 - Functions of social media in disasters

Figure 35 – Social media communication approaches in comparison

Figure 36 - WeSenseIT reporting example through mobile app and view through desktop

Figure 37- Snapshot of HydroNet software

Figure 38 - I-React reporting system

Figure 39 - Gamification in Cascais mobile application

Figure 40 - Original tweet vs labelled tweet through NLP techniques

Figure 41 - Burned area in Chieti, Italy

Figure 42 - Manual vs automatic computed shape of the burned area in Chieti, Italy

Figure 43 - Workflow of information and image retrieval from EFFIS and Copernicus Sentinel-2, and exploitation through AI and image processing techniques

List of Tables

Table 1 – Core concept and definitions in DRM

Table 2 - ETSI TS 102 182 (2010) Requirements vs Technologies - Broadcast (radio and TV)

Table 3- ETSI TS 102 182 (2010) Requirements vs Technologies - Mobile terminals

Table 4 - ETSI TS 102 182 (2010) Requirements vs Technologies - Other technologies

Table 5 - CAP segments overview

Table 6 - Warning thresholds of the Meteorological Service of Catalunya bulletin

Table 7 – Case Studies overview

Table 8 – People-centred PWS design and maintenance process

Table 9: Requirements vs Technologies – Mobile application, Social media and Chatbot with respect to the ETSI TS 102 182 requirements

Table 10 – Public Warning channel overview

Acronyms

AI  Artifical Intelligence
API  Application Programming Interface
ARPA  Agenzia Regionale per la Protezione Ambientale
BBK  Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
CAP  Common Alerting Protocol
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBRNE</td>
<td>Chemical, Biological, Radiological, Nuclear, and high yield Explosives</td>
</tr>
<tr>
<td>DG-ECHO</td>
<td>Directorate-General for European Civil Protection and Humanitarian Aid Operations</td>
</tr>
<tr>
<td>DRM</td>
<td>Disaster Risk Management</td>
</tr>
<tr>
<td>DRR</td>
<td>Disaster Risk Reduction</td>
</tr>
<tr>
<td>EAS</td>
<td>Emergency Alert System</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECMWF</td>
<td>European Centre for Medium-Range Weather Forecast</td>
</tr>
<tr>
<td>EENA</td>
<td>European Emergency Number Association</td>
</tr>
<tr>
<td>EFAS</td>
<td>European Flood Awareness System</td>
</tr>
<tr>
<td>EFFIS</td>
<td>European Forest Fire Information System</td>
</tr>
<tr>
<td>ERCC</td>
<td>Emergency Response Coordination Centre</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EWS</td>
<td>Early Warning System</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>FWI</td>
<td>Fire Weather Index</td>
</tr>
<tr>
<td>GPD</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>HCD</td>
<td>Human Centred Design</td>
</tr>
<tr>
<td>HFA</td>
<td>Hyogo Framework for Action</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IN-MHEWS</td>
<td>International Network for Multi-Hazard Early Warning Systems</td>
</tr>
<tr>
<td>IPAWS</td>
<td>Integrated Public Alert and Warning System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>JRC</td>
<td>Joint Research Centre</td>
</tr>
<tr>
<td>MODIS</td>
<td>Moderate Resolution Imaging Spectroradiometer</td>
</tr>
<tr>
<td>MoWaS</td>
<td>Modular Warning System</td>
</tr>
<tr>
<td>NLP</td>
<td>Natural Language Processing</td>
</tr>
<tr>
<td>NWR</td>
<td>NOAA Weather Radio</td>
</tr>
<tr>
<td>NWS</td>
<td>National Weather Service</td>
</tr>
<tr>
<td>OASIS</td>
<td>Advancing Open Standards for the Information Society</td>
</tr>
<tr>
<td>PWS</td>
<td>Public Warning System(s)</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>SatWaS</td>
<td>Satellite-based Warning System</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UNDP</td>
<td>United Nations Development Program</td>
</tr>
<tr>
<td>UNISDR</td>
<td>United Nations office for International Strategy for Disaster Reduction</td>
</tr>
<tr>
<td>URI</td>
<td>Universal Resource Identifier</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
<tr>
<td>WEA</td>
<td>Wireless Emergency Alert</td>
</tr>
<tr>
<td>WMO</td>
<td>World Meteorological Organization</td>
</tr>
<tr>
<td>WUI</td>
<td>Wild-Urban Interface</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Core Definitions

As in other research domains, when speaking about disaster risk management the terminology is very important to set a common language and ground discussions on consolidated and clearly defined concepts. In order to avoid ambiguity, throughout this document we refer to the terminology published by the UNISDR\(^1\), and we report in Table 1 the core concepts used in this study.

Yet the UNISDR definitions are not complete, e.g., it does not clarify the difference between the word Alert and Warning. These two terms sometimes are used interchangeably. According to the Cambridge dictionary:

- **Alert** [noun]: a warning to people to be prepared to deal with something dangerous: In the US, this difference is
- **Warning** [noun]: something that makes you understand there is a possible danger or problem, especially one in the future.

This does not help in delineating a clear difference in the context of emergency management. The US National Weather Service\(^2\) defines as warning something that has already happened, in contrast with the watch that is something related to an event that is predicted. However, some technical standards such as the Common Alerting Protocol (CAP) defines a general structure of an alerts, which can be both referred to a forecasted situation having a given likelihood (certainty) to happen in the future, either something that has been actually observed. The final clarification among these two words (i.e., alert and warning) in the context of emergency management is not in the scope of this work. Throughout this document, we interchangeably use the words warning, public warning, and alerts to refer to messages that are generated and propagated by the Public Warning System (PWS), which is the main focus of this study. Note that the PWS can be considered as a subsystem of the Early Warning System (EWS), which also includes hazard and risk monitoring and forecasting, among other functionalities.

**Table 1 – Core concept and definitions in DRM**

<table>
<thead>
<tr>
<th><strong>Disaster</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A serious disruption of the functioning of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability and capacity, leading to one or more of the following: human, material, economic and environmental losses and impacts.</td>
</tr>
</tbody>
</table>

Annotations: The effect of the disaster can be immediate and localized, but is often widespread and could last for a long period of time. The effect may test or exceed the capacity of a community or society to cope using its own resources, and therefore may require assistance from external sources, which could include neighbouring jurisdictions, or those at the national or international levels.

Emergency is sometimes used interchangeably with the term disaster, as, for example, in the context of biological and technological hazards or health emergencies, which, however, can also relate to hazardous events that do not result in the serious disruption of the functioning of a community or society.

---

1 https://www.unisdr.org/we/inform/terminology
2 https://www.weather.gov/lwx/WarningsDefined
**Disaster Risk:**
The potential loss of life, injury, or destroyed or damaged assets which could occur to a system, society or a community in a specific period of time, determined probabilistically as a function of hazard, exposure, vulnerability and capacity.

Annotation: The definition of disaster risk reflects the concept of hazardous events and disasters as the outcome of continuously present conditions of risk. Disaster risk comprises different types of potential losses which are often difficult to quantify. Nevertheless, with knowledge of the prevailing hazards and the patterns of population and socioeconomic development, disaster risks can be assessed and mapped, in broad terms at least.

It is important to consider the social and economic contexts in which disaster risks occur and that people do not necessarily share the same perceptions of risk and their underlying risk factors.

**Disaster Risk Management (DRM):**
Disaster risk management is the application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk and manage residual risk, contributing to the strengthening of resilience and reduction of disaster losses.

Annotation: Disaster risk management actions can be distinguished between prospective disaster risk management, corrective disaster risk management and compensatory disaster risk management, also called residual risk management.

**Early Warning System (EWS):**
An integrated system of hazard monitoring, forecasting and prediction, disaster risk assessment, communication and preparedness activities systems and processes that enables individuals, communities, governments, businesses and others to take timely action to reduce disaster risks in advance of hazardous events.

Annotations: Effective “end-to-end” and “people-centred” early warning systems may include four interrelated key elements: (1) disaster risk knowledge based on the systematic collection of data and disaster risk assessments; (2) detection, monitoring, analysis and forecasting of the hazards and possible consequences; (3) dissemination and communication, by an official source, of authoritative, timely, accurate and actionable warnings and associated information on likelihood and impact; and (4) preparedness at all levels to respond to the warnings received. These four interrelated components need to be coordinated within and across sectors and multiple levels for the system to work effectively and to include a feedback mechanism for continuous improvement. Failure in one component or a lack of coordination across them could lead to the failure of the whole system.

**Hazard:**
A process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation.

Annotations: Hazards may be natural, anthropogenic or socio-natural in origin. Natural hazards are predominantly associated with natural processes and phenomena. Anthropogenic hazards, or human-induced hazards, are induced entirely or predominantly by human activities and choices. This term does not include the occurrence or risk of armed conflicts and other situations of social instability or tension which are subject to international humanitarian law and national legislation. Several hazards are socio-
natural, in that they are associated with a combination of natural and anthropogenic factors, including environmental degradation and climate change.

Hazards may be single, sequential or combined in their origin and effects. Each hazard is characterized by its location, intensity or magnitude, frequency and probability. Biological hazards are also defined by their infectiousness or toxicity, or other characteristics of the pathogen such as dose-response, incubation period, case fatality rate and estimation of the pathogen for transmission.

**Resilience:**
The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions through risk management.
1. Introduction
1.1 Motivations

The European society is increasingly exposed to natural disasters as extreme weather events are becoming more frequent and more severe. The Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG-ECHO) highlights that the severity and the frequency of natural disasters has risen steadily over the past few decades in the EU, partly because of climate change, urbanization, population growth, and environmental degradation. Also, the European Environment Agency (EAA) reports that Europe is experiencing an increasing number of disasters, derived either from natural phenomena, technological accidents or human actions (Wehrli, 2010). These disasters affect EU citizens, the EU economy and environment every year (Echo). Over the period 1980-2016, the total reported losses caused by weather and climate-related extremes in the EEA member countries amounted to 436 billion EUR, while according to Munich Re between 2007 and 2017 there were 880 natural events (see Figure 1) accounting for 173 billion EUR. At the global scale, the UNISDR reports the impact of disasters happened between year 2005 and 2014 at 1.4 trillion losses, 1.7 billion affected people, and 0.7 million people killed. Figure 2 summarizes these numbers, giving the list of the top 10 countries by the number of disasters. The economic and societal impact will continue to escalate, as weather-related disasters alone could affect about two-thirds of the EU population annually by the year 2100, according to a recent data-driven forecast study (Forzieri, 2017).

Figure 1 – European natural disaster loss from 2007 to 2017, summing up to 173 billion EUR. (Source: http://natcatservice.munichre.com)

3 ECHO Factsheet – European Disaster Risk Management – January 2018
4 https://www.eea.europa.eu/
Figure 2 – Recent Disaster (2005-2014) impacts considering the economic damage (USD), people affected and people killed (top), and top 10 countries worldwide by the number of disasters (bottom) (Source: UNISDR 5)

5 https://www.unisdr.org/files/42862_economichumanimpact20052014unisdr.pdf
Climate change is expected to trigger more frequent and more intense extreme precipitation events. The frequency of occurrence of major hurricanes has already significantly increased in the last decades and it will likely continue to rise because of ocean warming. Coastal flooding events are more and more frequent, mainly due to sea-level rise; river floods, flash floods and landslide events are also increasing, in particular in alpine environments. Another expected effect of global warming is the increase in the frequency and the duration of regional heat waves and drought events. Higher spring and summer temperatures and earlier spring snowmelt typically cause soils to be drier for longer, increasing the likelihood of drought and the duration of the wildfire season. In 2017, a disastrous series of forest fires took place, during which over one million hectares of forest were destroyed (almost three times the five-year EU average) half of which was in Portugal alone, where more than 100 people were killed between June and October 2017. In July 2018, more than 90 people died in Greece during a devastating fire affecting a wild-urban interface (WUI). In both cases, people were trapped by fire when trying to escape from flames in spontaneous evacuations. These fires resulted in significant destruction of property and major impacts on the economy including network infrastructure, businesses (commercial and industrial), agricultural and forestry activities. The increased frequency of wildfires also induces an increase in the emissions of greenhouse gases, which in-turn contribute to global warming.

The human vulnerability to natural disasters is increasingly higher. Concurrently, global population and wealth are rising at a very fast pace, which in turn dramatically increase the exposure of humans and goods to natural and anthropogenic disasters. This calls for an unprecedented effort to improve the effectiveness of PWS to help society in becoming more resilient to disasters.

1.2 Topics and goal of the study

An effective PWS is of paramount importance in order to save lives and property and reduce the overall impact of emergency events. An effective PWS must be capable of delivering in a timely manner effective early warning, reaching all population, businesses while informing all the public authorities involved in the emergency management cycle, including those belonging to neighbouring countries in case of cross-border emergencies. In order to do so, both the technical and the organizational system must be designed so as to work together. At the same time, current PWS are not aware about the correct reception of an alert because the alerting process is designed to be unidirectional. For the same reason, if instructions are contained within the alert message, there is no way of knowing if such instructions have been followed or not, if and where there are people requiring the intervention of the authorities (e.g. rescue services).

The only structured way in which citizens can effectively contact authorities to request clarifications or issue new reports is through a specific telephone number (112 in Europe, 911 in the USA), which can get completely congested and unusable in case of large-scale emergencies. For example, when hurricane Harvey hit Houston in 2017, official emergency channels were overloaded, and so were the capacities of formal responders. For this reason, in large-scale emergencies in Europe authorities now urge the public to use social media to contact their families, to avoid overloading phone lines.6 Victims and affected citizens turn to social media to call for rescue and to request

---

6 "If you are ok, please inform your family using social networks to avoid the collapse of phone lines" (message on Twitter by Civil Protection of Catalonia, August 2017) https://twitter.com/emergenciescat/status/898209884474404868; "Don't call. Use texting or social media. Network is getting saturated" (message on Twitter by Belgium Crisis Center, March 2016) https://twitter.com/CrisiscenterBE/status/712207628571643905
assistance, as well as to coordinate and exchange information. Furthermore, during these situations social media facilitates the emergence of a diverse crowd of informal response groups, operating online as well as on the ground. In times of emergency, **people seek and share information using the platforms that are most familiar to them** (Potts, 2015), including popular websites, social media sites, and apps; however, these provide a Big Data stream in which important information can be missed and false information can propagate, potentially introducing additional difficulties in the disaster management cycle. An effective system is needed to fully exploit the tremendous potential of this stream of data, including geo-referenced content, as well as multimedia content such as audio, images, and videos, uploaded through personal mobile devices (smartphones, tablets) at an ever-growing rate. The user base of such devices is huge, with more than 6.8 billion mobile phone subscriptions in the world (International Telecommunication Union - ITU) (Sanou, 2013), a figure that is globally rising each year. Such technological innovations are significantly expanding the sensing power of communication networks, giving momentum to a massively distributed and user-driven data collection process known as “crowdsensing” or “crowdsourcing” (Purohit 2015). During emergencies, this new paradigm has been locally used to detect the occurrence of an event, detect sub-events, learn about urgent needs from the population, and determine affected areas, among other tasks, and in future it can be used also in the context of public warnings in case a response is required. However, the potential of crowdsensing for disaster management is far from being fully exploited.

The aim of this study is multi-fold. First, to **assess current approaches on disaster risk management** considering UN guidelines and with a focus on communication and human factors (Section 2). Second, to **review the key technical standards related to PWS** with a focus on the standardization of the content (Section 3). Third, to **present selected case studies to highlight practical approaches** currently in use both within the EU and also in the USA (Section 4). Fourth, to propose a **set of recommendations** as a set of take-aways that can be useful for decision-making with respect to future evolution of current PWS that can be deployed at multiple geographic scales, from local communities up to the national and work also at transboundary level (Section 5). Finally, ideas about future evolution of emergency management systems are also given (Section 6).
2. Solutions and approaches on DRM

Warning the population on incoming hazards and informing them on ongoing emergencies while suggesting countermeasures to adopt, are within the core aims of the EWS, which also includes hazard monitoring, forecasting, disaster risk assessment, timely and effective Public Warning to individuals, communities, businesses and others, so as to reduce disaster risks and prepare people for effective response. Each of these activities represents a core brick of the DRM, that even if well formalized, can vary according to the hazard type (e.g. natural, anthropogenic), geography of the affected regions and the socio-demography of the affected population.

The Public Warning is an institutional duty, as it has to come from official sources and provide authoritative, accurate and timely information to the population interested by risks and hazards at any level. As core component of the DRM cycle, the PWS includes and implements the sets of practices, tools and procedures that enable experts and authorities to transfer and share information on hazards and safe behaviours to the audience. In order to succeed in this aim, the UNISDR advises to implement a people-centred PWS. According to this perspective, the public is not an undefined group of people that passively receive information, warnings and intervention, but it represents a heterogeneous community with a range of characteristics to be addressed in order to guarantee that the warning contents will be received, understood and effectively followed. People centrality is also at the core of a slightly different approach, the Community Based DRM, that the UNISDR defines as a process that promotes the involvement of potentially affected communities in disaster risk management at the local level (UNISDR, 2017). The aim of this approach is to achieve a local strategy for disaster preparedness and risk reduction. In this view, the focus on people requires a detailed and site-specific knowledge of the population in terms of ethnography, age, vulnerabilities, education, religion, etc.

An articulated knowledge of the citizenship is the base to sustain and foster the community engagement, which is fundamental to make the warning communications effective and to actively involve people in DRM processes. The role of local authorities in promoting community-based disaster mitigation is very important to put the Community Based DRM in practice.

The progressive growth of the citizen role in DRM processes is also envisioned by the Situational Theory of Public (Grunig, 2005). In particular, the theory suggests different engagement and communication strategies based on the population segments. According to this view, these attitudes are context-dependent and are shaped by three core variables: the problem recognition, the constraint recognition and the level of involvement, which represent how much people connect themselves with the situation (e.g. hazard or crisis). According to the theory, a high-risk perception combined with a low constraints recognition results in complex behavioural patterns, such as more active information seeking and less effective information processing. The level of involvement in the crisis pushes people to continuously search for information. In such situations, people are more willing to actively communicate and cooperate with response organizations.

Crisis and disasters do reveal and make evident the need to review the traditional role assigned to citizens, especially given the socio-technical changes occurred in the last years. The public is no longer a passive recipient of messages generated according to safety policies but it can be considered as an active individual, who is able to directly and indirectly interact with information, who can be expected to play a role and even contribute to risk prevention and to emergency response. The acknowledge of the public as responding community is a step forward that drives the DRM to implement effective strategies to manage the increasingly complex hazards scenarios.
Inclusive and participatory DRM approaches reframe the traditional linear “warning chain” where the population is basically the end-point, opening the opportunity to re-design and integrate DRM ecosystem (see Figure 3) with innovative processes.

In comparison to the traditional approaches, the openness promoted by the novel approaches, stressing the relevance of new forms of dialogue with the population and among all the involved actors, implies deep changes that involve organizations, procedures, technology and skills of people.

An integrated DRM approach can tackle this complexity, including people in the process even though they are not part of any formal organization, that, on their side, can benefit of the voluntary contributions coming not only from active citizens, but also from the scientific community and – more recently – from organizations of digital volunteers. It is important to recognize that the effort in terms of coordination among organizations and actors is relevant, but fundamental to make the DRM a systemic, distributed and people centred ecosystems, grounding on 4 pillars, as shown in the Figure 4.

**Figure 3 - DRM Ecosystem**  
(Source: Nguyen et al., 2017)

**Figure 4 - The four elements of systematic people-centred DRM**  
(Source: Basher, 2006)
2.1 Crisis Communication

The crisis communication specifically supports the emergency management and reply to the need to inform and alert the public about an event. Educational purposes are accomplished by the risk communication, which is oriented to provide information on possible consequences (impacts) of hazards (CDC, 2012). The PWS specifically supports the Crisis Communication in providing emergency alerts that include crisis information, instructions and behavioural guidance. Nevertheless, the Crisis Communication works on a wider timespan and it is a dynamic process. An emergency is not a static event, but it evolves over time, and the communication must adapt to it, trying to anticipate as much as possible the necessary information.

The following schema (Figure 5) suggests the types of information that should be provided in the emergency phases, and highlights the key phases for a PWS (pre-crisis, initial).

![Emergency Risk Communication Lifecycle](Adapted from: CDC, 2012)

Information sharing and training on hazards, prevention measures and safe behaviours are essential in the emergency communication lifecycle. A solid and updated knowledge on risks and prevention measures increases the effectiveness of public alerts and the people safety during crises.

An articulated crisis communication strategy includes initiatives and resources to educate people and keep them informed about risks, safe behaviours and preventive measures for disaster risk reduction. These actions can help to keep a profitable dialogue between the population and the local authorities. This exchange has to be cared and kept living as a real conversation, making it interesting, valuable and tailored on the specific characteristics of people. The people centric
approach is the best framework to set up an engagement strategy able to include and speak with all population segments (young, workers, elderly, companies) by mean of multiple channels (online and offline) and to implement an effective crisis communication, which must be grounded on a solid PWS.

Literature investigates some gaps that limit the effectiveness of a PWS. Among them, the capability to **adequately reach the target people, the quality of the provided information, as well as the coherence of the messages conveyed by different organizations** represent important limitations of the current PWS (UNISDR, 2012; Kasperson, 2014). Official institutions, responders and population have very different needs, perspective and skills. To tackle these hindrances, the PWS shall be part of an alerting strategy focusing on the high complexity of all interplaying factors. Each single alert has to be designed as a communication act able to create trust, raise awareness, provide easy to understand information, motivate the public to act safely. Sometimes, alerts include technical data and forecasts that were primarily designed to address crisis and operation manager needs. Therefore, they should be adapted in order to better match the population needs.

Previous experiences and studies offer clear indications for an effective alert generation and delivery (Bean et al., 2015).

- **Hazard:** the alert has to describe the physical phenomenon and the risk it can pose. This information is crucial to harmonize subjective differences in the risk perception. In front of unclear or ambiguous messages, people tend to minimize the risk, incurring in unsafe behaviours.
- **Location:** geographical boundaries and environmental details about the area interested by the hazard has to be explicitly described. In addition, the nearest safe areas should be indicated. A particular care should be put when areas are visualized on maps, which are very useful if they do not show too many information types and if they provide a suitable complexity for the intended readers (Dransch et al., 2010). It is known that reading a map requires specific skills that might not be available in certain population segments.
- **Temporal validity:** the temporal validity of the alert must be specified a pair of date time objects, with clear reference to the time-zone (see ISO 8601:2004). The first date, which is often called “start date” or “effective date”, specifies when the alerts enters in force, while the second data, which is often called “end date” or expiration date”, states when the alert is no longer in valid. Whenever available, also the estimated temporal validity of the event to which the alert is referred should be specified.
- **Guidance:** effective alerts have to include clear instructions to stay safe. Literature shows that the more instructions the alert provides, the more likely people comply with them. This is especially important for risks for which people are less prepared to cope with, such as nuclear emergencies. Complete instructions should include the onset date, meaning the exact moment from which they have to be followed. This information is crucial to reinforce the urgency of the risk and to activate the response when needed.
- **Source:** the organization emitting the alert cannot be missed, otherwise it could not be trustable for receivers. Official sources are considered trustworthy, but note that they share the audience attention with informal resources, e.g. citizen generated content on social media platforms. The public at the same time receive and is used to search for multiple sources of information. The credibility of the source is crucial to set up an effective communication.
- **Anticipation or timeliness:** it is intuitive that the sooner the message is received, the better the citizens reply can be. As shown in Figure 6, a direct relationship between the warning (alert) lead time (anticipation) and the damage reduction has been observed, despite the warning (alert) reliability decreases with the lead time.
- **Style**: independently on the communication channel, alerts have to avoid redundancy. This fit with the psychophysiology of the human cognition because attentional and processing resources are limited. Moreover, the context can pose interferences and finally, the emotional reaction can decrease the effectiveness of the communication. Shortness helps to cope with these aspects and limit the ICT costs of transmission, e.g. in terms of bandwidth. Moreover, the communication style is very important to convey easily understandable messages, inspire credibility, and transmit the sense of severity and urgency. Therefore, the PWS has to guarantee a consistent information style that have to be designed to fit the different channels and audiences.

In general, alerts should not raise panic and negative emotional reactions and, at the same time, motivate people to correctly behave. Current approaches suggest to reorganize vertical communication strategies, i.e., the flow from the authority to the public. The Public Warning has to be based on a layered strategy, designed according to a deep knowledge of the target population. The specific characteristics of the target people in terms of needs, skills and habits, affect the capability to correctly interpret and follow alert instructions.

The adoption of technical standards related to the alert content and the channel used is of paramount importance, in order to implement a good strategy for the Public Warning process.

### 2.2 Human Factors and Public Warning

From the single **receiver perspective**, an alert message activates both cognitive and emotional factors, for the most part unconscious, that have been mapped to the following processes (Bean et al, 2015):

1. receiving the alert (hearing/reading);
2. understanding the alert message;
3. believing the reliability;
4. personalizing the alert;
5. confirming the alert is true;
6. and taking protective action.
We need time to process and assume information, especially if it contains critical messages. In order to facilitate and meet the various stages required to acquire an alert and act upon it, it is important to carefully design the alert, both in terms of content and transmission channel. The same message received many times on multiple channels results more effective. For instance, increasing the frequency of alerts rises the likelihood of evacuation.

**Repetition makes the communication more reliable and the reaction more urgent.** Recent literature (Lundgren and McMakin, 2009), suggests to communicate early, often, fully and to engage the audience throughout the whole DRM cycle, not only during the response phase.

How an alert is received by the audience is highly affected by **human and contextual factors**. Communication, including the Crisis communication, is not an objective science and it grounds on subjective and contextual factors that can create **biases and misinterpretation**. These may concern both receivers and emitters, so both Public and Authorities. Several studies investigating the contextual factors affecting the effectiveness of a PWS have found that there are relevant differences in how an alert is received and interpreted depending on the time of the day, on the channel used to transmit, and also on the socio-demographic characteristics of the audience. Commonly applied variables to segment the audience are the age, the economic status, the gender, the education level, physical or mental impairments. In addition to these, habits, family and professional roles should be kept into consideration because they can influence message interpretation and response. Moreover, **the experience of prior disasters might enhance the response** because the persons have learnt about protective actions and warning systems, but they can also hinder emotional reactions (Mayhorn & McLaughlin, 2014). According to Protective Action Decision Model (Lindell & Perry, 2012) also environmental conditions (such as dark, rain, sirens, smoke) and socio-cultural factors affect the risk perception and subsequently the individual recipient response upon the reception of alerts. Moreover, a key factor is the activity that the recipient is doing when the alerts is received, e.g. sleeping, working, walking.

**When delivering alerts, both human and contextual factors must be considered because they strongly affect the compliance with advices and instructions to be followed, especially in case of emergencies.**

Messages announcing a possible incoming hazard or suggesting how to behave during an ongoing crisis may trigger basic emotions such as fear and anger, that could be directed toward the alert or even to the emitter, decreasing the probabilities to activate safe behaviours. The range of emotional reactions includes hyper-activation, panic attack, apathy, resignation. The **trustworthiness** is an important cognitive and emotional modulator that can be leveraged to deliver effective alerts. In relation to risks and emergencies, people select and follow only reliable sources. In time of crisis, a range of communication aspects affect people trust, such as demonstration of empathy, commitment, competence, honesty and openness, responsibility, confidentiality, and equity. Additionally, the lack of consistency or disagreement among the messages delivered by official sources is perceived as a lack of coordination. Similarly, the lack of transparency or information disclosure are associated with not fulfilling risk management responsibilities.

**The Public Warning process should be managed by authoritative sources, who are perceived as trustworthy by the population.** Public alerts delivered by the different agencies operating in the DRM have to be coherent, open, and contain full information.
2.3 UN guidelines

Since the 1999, the UN is working for the implementation of the International Strategy for Disaster Reduction (ISDR), which promotes a global commitment in the risk assessment and management. Politic, scientific and economic institutions are involved to create synergy and facilitate the implementation of the measures at national and local level. Born in the 1960s, the office has been supporting several disasters and, in 2015, the UNISDR released the Sendai Framework, a worldwide agenda for Disaster Risk Reduction for the period 2015-2030. According to the UNISDR, over the decades, DRR has moved from a technical to a humanitarian discipline. The Sendai agenda is clearly articulated in goal, objectives and priority actions, as shown in Figure 7.

In continuity with previous resolutions, the Sendai Framework grounds on 3 main pillars:

- The shift of the focus from disasters to risks;
- The implementation of multi-risk perspective, including both small-scale and large-scale disasters, frequent and sudden events, natural and anthropogenic hazards related to environmental, technological and biological causes;
- Finally, the framework strongly encourages the application of people-centred DRM approaches.

The implementation guidelines explicitly refer to the priority of well-designed and impact oriented Early Warning Systems to address new risks and rapidly changing vulnerabilities (UNISDR EUR, 2016). Nowadays, Early Warning Systems work in many countries of the world, leveraging on scientific results and reliable ICT, often including low-cost technology (CODEV, 2018). As a result of the UNISDR International Conference on Multi-Hazard Early Warning Systems, the International Network for Multi-Hazard Early Warning Systems (IN-MHEWS) has been founded. It is a multi-stakeholder partnership for promoting and sharing best practices in multi-hazard early warning systems and services for DRR and resilience. As a strategic approach to early warning implementation, the IN-MHEWS suggests an approach based on the Standard Operating Procedures combined with impact-based forecasting and risk-based warnings (IN-MHEWS, 2016).
Chart of the Sendai Framework for Disaster Risk Reduction 2015-2030

Scope and purpose
The present framework will apply to the risk of small-scale and large-scale, frequent and infrequent, sudden and slow-onset disasters, caused by natural or manmade hazards as well as related environmental, technological and biological hazards and risks. It aims to guide the multi-hazard management of disaster risk in development at all levels as well as within and across all sectors.

Expected outcome
The substantial reduction of disaster risk and losses in lives, livelihoods and health and in the economic, physical, social, cultural and environmental assets of persons, businesses, communities and countries.

Goal
Prevent new and reduce existing disaster risk through the implementation of integrated and inclusive economic, structural, legal, social, health, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce hazard exposure and vulnerability to disaster, increase preparedness for response and recovery, and thus strengthen resilience.

Targets
<table>
<thead>
<tr>
<th>Substantially reduce global disaster mortality by 2030, aiming to lower average per 100,000 global mortality between 2020-2030 compared to 2005-2015</th>
<th>Substantially reduce the number of affected people globally by 2030, aiming to lower the average global figure per 100,000 between 2020-2030 compared to 2005-2015</th>
<th>Reduce direct disaster economic loss in relation to global gross domestic product (GDP) by 2030</th>
<th>Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030</th>
</tr>
</thead>
</table>

Substantially increase the number of countries with national and local disaster risk reduction strategies by 2020
Substantially enhance international cooperation to developing countries through adequate and sustainable support to complement their national actions for implementation of this framework by 2030
Substantially increase the availability of and access to multihazard early warning systems and disaster risk information and assessments to people by 2030

Priorities for Action
There is a need for focused action within and across sectors by States at local, national, regional and global levels in the following four priority areas.

- **Priority 1**: Understanding disaster risk
- **Priority 2**: Strengthening disaster risk governance to manage disaster risk
- **Priority 3**: Investing in disaster risk reduction for resilience
- **Priority 4**: Enhancing disaster preparedness for effective response, and to “Build Back Better” in recovery, rehabilitation and reconstruction

*Figure 7 - The Sendai framework for DRR*  
(Source: UNISDR, 2016)
At the same time, the United Nations Program Development (UNDP) is focusing on Priority 4 of the Sendai Framework. The UNDP is supporting 96 active early warning and preparedness projects, which focus on the improvement of DRM approaches, promoting multi-stakeholder participation through innovative technologies capable to better connect national and local Early Warning Systems with the most vulnerable communities. The UNDP reference strategy for DRR is shown in Figure 8, and it has been based on the Hyogo Framework for Action (HFA), a precursor of the Sendai Framework.

The outcomes of the supported project highlight that a better knowledge of risks strengthens the early warnings effectiveness and the risk mitigation actions. Early warning, besides saving lives, thanks to the mobile devices, bring impacts also on productive sectors, such as the agriculture and tourism. Moreover, it is demonstrated how it can be possible to go beyond early warning to provide advice on investments to decision-makers (UNDP, 2015). UNDP has published a very useful toolkit for supporting the communications strategies design, addressing effective issuance and packaging of early warnings and long-term communication actions on climate changes and related hazards (UNDP, 2016).
3. Technical Standards

The importance to adhere to a standard and to its application to the problem for which it has been designed, is not crucial only for the assurances that it normally offers in terms of uniqueness of the communication protocols and effectiveness of the procedures in it contained, but it allows besides a constructive comparison with other actors (i.e. countries) that adopts the same standard to face problems of similar entity. Such comparison can be therefore useful to assess the goodness of the techniques and of the adopted methodologies and to accelerate the process of the resiliency improvement with respect to the faced problem.

3.1 Standards and requirements for Public Warning systems implementation


ISO 22322:2015 – “Social security -- Emergency Management -- Guidelines for public warning” provides guidelines for developing, managing and implementing public warning before, during and after incidents. It is applicable to any organization responsible for public warning, from local up to international.

It identifies two main phases in the public warning system: the hazard monitoring and the warning dissemination. The monitoring is led by the risk assessment and should involve all the interested public authorities, which have to cooperate to enhance the public awareness. The dissemination includes all the activities that aim to identify the correct communication process (i.e. which is the most effective message, which communication channel to exploit, which groups of people to alert).

ETSI TS 102 182 (2010) - “Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies” gives an overview of the technical requirements for the communication from authorities to citizens in all types of emergencies. It defines the effectiveness of an emergency notification system in terms of objectives that it can achieve (e.g. detailed message that focus only on strategic information, fully accessibility of the information by the people) and feature to provide (i.e. requirements to satisfy).

The main features regard:

- **the delivering capability of the notifications**: people coverage should be at least 50% of the citizens in the relevant area within 3 minutes and 97% of the citizens in the immediately surrounding area of the relevant one within 5 minutes. Of course, in case of very rapid emergencies, such as earthquakes or tsunamis, the notification should be delivered to as many interested citizens as possible in the order of seconds (e.g. 10 seconds for an earthquake). For this reason, an emergency notification system should have a high availability and should offer geographic redundancy of the components and recovery plans for broken components;

- **the coverage capability of the notifications**: citizens need to have information that is specific to their location and the location of the emergency. An effective notification should cover an area of:
  - 1 km inside community boundaries
  - 5 km outside community boundaries
  - 30 km in rural areas
  - 60 km over sea of desert;
- **the delivering methods of the notifications**: multiple methods shall be supported, such as telephone voice, SMS, broadcast radio and TV, sirens, email, instant messaging service to mobile phones, mobile apps, web pages;
- **the message accessibility**: messages should be delivered even to people with special needs, such as hearing and vision impaired, and even in different languages (e.g. for visitors from other countries);
- **the security and data protection**: the emergency notification system should provide user authentication and should be sensitive with respect to the user data that it collects;
- **the recognizability of the emergency message**: an emergency notification system should be intrusive. This means that the reception of an emergency message should be enabled by default. Moreover, the message should be immediately recognizable and should be put in foreground as soon as it is possible.

To fulfil the high ambitions in terms of wide-ranging distribution of high effective messages and their delivery in the shortest possible time, ETSI TS 102 182 (2010) specifies clearly that none of the aforementioned technologies met all the necessary requirements, instead a combination of different methods would make it possible to achieve the goals. In the following tables, ETSI TS 102 182 (2010) summarises the necessary requirements to guarantee an efficient emergency notification system and the technologies able to meet them.

### Table 2 - ETSI TS 102 182 (2010) Requirements vs Technologies - Broadcast (radio and TV)
(Source: ETSI TS 102 182, 2010)

<table>
<thead>
<tr>
<th>Emergency notification systems shall</th>
<th>Analogue</th>
<th>RDS</th>
<th>DAB</th>
<th>DigTV</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>be able to reach citizens in their own dwelling</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens at their place of work</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach citizens in public venues</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach citizens on foot</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach citizens in a vehicle</td>
<td>V</td>
<td>V</td>
<td>some X</td>
<td>X</td>
<td>V = compliant X = non-compliant</td>
</tr>
<tr>
<td>be able to reach a citizen visiting another European country</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>provide sufficient instructions regarding actions to be taken</td>
<td>V</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V = compliant X = non-compliant</td>
</tr>
<tr>
<td>provide identification of the message/notification originator</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>deliver messages within a planned specified time</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>allow simultaneous delivery to targeted, large audiences or geographies</td>
<td>0</td>
<td>V</td>
<td>0</td>
<td>0</td>
<td>V = compliant 0 = non-compliant to geographies</td>
</tr>
</tbody>
</table>
Emergency notification systems shall | Analogue | RDS | DAB | DigTV | Legend
--- | --- | --- | --- | --- | ---
offer sufficient details of the emergency situation | V | 0 | V | V | V = compliant
       |       |       |       |       | 0 = message length inadequate
be able to retry delivery when the initial message delivery fails | 0 | 0 | 0 | 0 | 0 = messages can be repeated
support delivery of notification messages to those with special needs and unique devices, like terminals of hearing and speech impaired persons | 0 | 0 | 0 | 0 | 0 = broadcast is not specific for covering all specific needs
have the ability to deliver messages in multiple languages | V | 0 | V | V | V = compliant
       |       |       |       |       | 0 = message length inadequate
be capable of addressing congestion management across the various networks used | V | V | V | V | V = compliant

Table 3 - ETSI TS 102 182 (2010) Requirements vs Technologies - Mobile terminals
(Source: ETSI TS 102 182, 2010)

<table>
<thead>
<tr>
<th>Emergency notification system shall</th>
<th>Paging</th>
<th>CB</th>
<th>SMS</th>
<th>TV</th>
<th>MBMS</th>
<th>MMS</th>
<th>USSD</th>
<th>Email</th>
<th>IM Service</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>be able to reach citizens in their own dwelling</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens at their place of work</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens in public venues</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens on foot</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
</tbody>
</table>
| be able to reach citizens in a vehicle | V | V | V | X | X | V | V | V | V | V = compliant
       |       |       |       |       |       |       |       |       |       | X = watching video while driving a vehicle is not desired |
| be able to reach a citizen visiting another European country | V | 0 | V | V | 0 | V | V | V | V | V = compliant
       |       |       |       |       |       |       |       |       |       | 0 = compliant when phone is configured correctly |
| provide sufficient instructions regarding actions to be taken | V | V | V | V | V | V | V | V | V | V = compliant
<pre><code>   |       |       |       |       |       |       |       |       |       | X = non-compliant |
</code></pre>
<table>
<thead>
<tr>
<th>Emergency notification system shall</th>
<th>Paging</th>
<th>CB</th>
<th>SMS</th>
<th>TV</th>
<th>MBMS</th>
<th>MMS</th>
<th>USSD</th>
<th>Email</th>
<th>IM Service</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>provide identification of the message/notification originator</td>
<td>V</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>V = compliant, 0 = compliant, but no certainty. Could be a spoofed identity</td>
</tr>
<tr>
<td>deliver messages within a planned specified time</td>
<td>V</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>0</td>
<td>0</td>
<td>V</td>
<td>0</td>
<td>V = compliant, 0 = non-compliant for large audiences</td>
</tr>
<tr>
<td>allow simultaneous delivery to targeted, large audiences or geographies</td>
<td>V</td>
<td>V</td>
<td>X</td>
<td>0</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>0</td>
<td>X</td>
<td>V = compliant, 0 = non-compliant to geographies X = non-compliant</td>
</tr>
<tr>
<td>offer sufficient details of the emergency situation</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to retry delivery when the initial message delivery fails</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V = compliant, 0 = messages can be repeated</td>
</tr>
<tr>
<td>support delivery of notification messages to those with special needs and unique devices, like terminals of hearing and speech impaired persons</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>0</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant through terminal capability 0 = partly-compliant</td>
</tr>
<tr>
<td>have the ability to deliver messages in multiple languages</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be capable of addressing congestion management across the various network used</td>
<td>V</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>V = compliant, X = non-compliant</td>
</tr>
</tbody>
</table>
Table 4 - ETSI TS 102 182 (2010) Requirements vs Technologies - Other technologies
(Source: ETSI TS 102 182, 2010)

<table>
<thead>
<tr>
<th>Emergency notification systems shall</th>
<th>ETAS</th>
<th>Siren</th>
<th>Web</th>
<th>Email conventional PC based</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>be able to reach citizens in their own dwelling</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = siren not always heard</td>
</tr>
<tr>
<td>be able to reach citizens at their place of work</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = siren not always heard</td>
</tr>
<tr>
<td>be able to reach citizens in public venues</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach citizens on foot</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach citizens in a vehicle</td>
<td>X</td>
<td>0</td>
<td>X</td>
<td>X</td>
<td>0 = siren not always heard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to reach a citizen visiting another European country</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = not applicable</td>
</tr>
<tr>
<td>provide sufficient instructions regarding actions to be taken</td>
<td>V</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>provide identification of the message/notification originator</td>
<td>0</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = compliant, but no certainty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = possibly spoofed address</td>
</tr>
<tr>
<td>deliver messages within a planned specified time</td>
<td>0</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = non-compliant for large audiences</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = no guarantee</td>
</tr>
<tr>
<td>allow simultaneous delivery to targeted, large audiences or geographies</td>
<td>0</td>
<td>V</td>
<td>0</td>
<td>0</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = non-compliant to geographies</td>
</tr>
<tr>
<td>offer sufficient details of the emergency situation</td>
<td>V</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
<tr>
<td>be able to retry delivery when the initial message delivery fails</td>
<td>V</td>
<td>0</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 = messages can be repeated</td>
</tr>
<tr>
<td>support delivery of notification messages to those with special needs and unique devices, like terminals of hearing and speech impaired persons</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = not specific for covering all specific needs</td>
</tr>
<tr>
<td>have the ability to deliver messages in multiple languages</td>
<td>V</td>
<td>X</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X = non-compliant</td>
</tr>
</tbody>
</table>
Emergency notification systems shall be capable of addressing congestion management across the various networks used

<table>
<thead>
<tr>
<th>ETAS</th>
<th>Siren</th>
<th>Web</th>
<th>Email conventional PC based</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>V</td>
<td>X</td>
<td>X</td>
<td>V = compliant&lt;br&gt;X = non-compliant</td>
</tr>
</tbody>
</table>

To achieve the message recognisability and the ease with which it can be efficiently processed, it is necessary the adoption of a standard communication protocol that can be unambiguously parsed by the organization responsible for the message dissemination. In its standard, ETSI propose the Common Alerting Protocol (CAP) as notification message delivering protocol, which has been adopted also by the international Telecommunications Union (ITU) as defined in its Recommendation X.1303bis (ITU - Recommendation X.1303bis).

3.2 The Common Alerting Protocol (CAP)

The **CAP standard** (CAP, Common Alerting Protocol Version 1.2) is a digital message format for PWS notification promulgated by OASIS\(^7\). It follows the serialization rules of the XML standard, as specified in (Bray, 2008). The CAP is not related to any specific application or telecommunication method and can be easily used for any type of hazards.

It has been designed upon the concepts of:

- **Interoperability**: the CAP message provides a means for interoperable exchange of alter and notifications among different information systems;
- **Completeness**: the CAP message provides all the elements for generating an effective PWS message;
- **Simple implementation**: the CAP standard doesn’t place burdens of complexity on technical implementers;
- **Simple XML and portable structure**: the CAP message implementation is an XML document, but its format is sufficiently abstract to be adaptable to other coding schemes (e.g. JSON);
- **Multi-use format**: the message supports multiple types (e.g. alert, update, cancellation, acknowledgements, error message) and can be exploit in several applications (actual, exercise, test, system message);
- **Familiarity**: the data and the code values must be meaningful also to non-expert recipients;
- **Interdisciplinary and international utility**: the design allows a wide range of applications both in public safety and in emergency management and it is applicable worldwide.

A CAP message is composed by segments with different meaning. Its structure can be expressed with the Document Object Model (DOM) in Figure 9, which gives a tree representation of the message structure, as described in W3C (2002).

---

\(^7\) OASIS: Advancing open standards for the information society - https://www.oasis-open.org
There is a “base” segment that is the <alert>, which can contain one or more <info> segments, each of which including one or more <area> and/or <resource> segments. Each segment is composed by several elements that characterize the message, some of them are mandatory, others are not. The table below shows more in detail the segments meaning and their composition.

**Table 5 - CAP segments overview**

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
<th>Main sub-elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;alert&gt;</td>
<td>Provides information about the message, its purpose, its source and its status. It provides also a unique identifier of the message and links to other related &lt;info&gt; segment along with:</td>
<td>&lt;info&gt; segment along with:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &lt;identifier&gt;: unique identifier of the message;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &lt;sender&gt;: identifier of the message sender;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &lt;sent&gt;: time and date of the message origination;</td>
</tr>
<tr>
<td>Segment</td>
<td>Description</td>
<td>Main sub-elements</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>messages. An alert can Used alone for message acknowledgements, but most of the time it includes at least one <code>&lt;info&gt;</code> segment.</td>
<td></td>
<td><code>• &lt;status&gt;</code>: code denoting the appropriate message handling (i.e. Actual, Exercise, System, Test, Draft); <code>• &lt;msgType&gt;</code>: code denoting the message nature (i.e. Alert, Update, Cancel, Ack, Error); <code>• &lt;scope&gt;</code>: code denoting the intended distribution of the message (i.e. Public, Restricted, Private).</td>
</tr>
<tr>
<td><code>&lt;info&gt;</code></td>
<td>Describes an anticipated or an actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction). The urgency, severity and certainty elements distinguish less emphatic from more emphatic messages. The <code>&lt;info&gt;</code> segment may provide also instructions for appropriate response by message recipients and various other details (e.g. hazard duration, technical parameters, contact information, links to additional sources, etc).</td>
<td><code>&lt;resource&gt;</code> and/or <code>&lt;area&gt;</code> segments along with: <code>• &lt;language&gt;</code>: the (RFC 3066) code identifier denoting the language of <code>&lt;info&gt;</code> segment of the alert message; <code>• &lt;category&gt;</code>: code denoting the category of the subject event of the message (i.e. Geo, Met, Safety, Security, Rescue, Fire, Health, Env, Transport, Infra, CBRENE, Other); <code>• &lt;event&gt;</code>: text denoting the type of the subject event of the message; <code>• &lt;urgency&gt;</code>: code denoting the urgency of the subject event of the message (i.e. Immediate, Expected, Future, Past); <code>• &lt;severity&gt;</code>: code denoting the severity of the subject event of the message (i.e. Extreme, Severe, Moderate, Minor, Unknown); <code>• &lt;certainty&gt;</code>: code denoting the certainty of the subject event of the message (i.e. Observer, Likely, Possible, Unlikely, Unknown); <code>• &lt;audience&gt;</code>: text describing the intended audience of the alert message; <code>• &lt;effective&gt;</code>: effective date and time of the information of the alert message <code>• &lt;expires&gt;</code>: expiry date and time of the information of the alert message <code>• &lt;instructions&gt;</code>: text describing the recommended action to be taken by recipients of the alert message; <code>• &lt;parameter&gt;</code>: system-specific additional parameter associated with the alert message. An <code>&lt;info&gt;</code> segment can contain more than one <code>&lt;parameter&gt;</code> field.</td>
</tr>
<tr>
<td><code>&lt;resource&gt;</code></td>
<td>Provides external references with additional information such as text, image or audio file (a message can have more than one <code>&lt;resource&gt;</code>).</td>
<td><code>• &lt;resourceDesc&gt;</code>: human-readable text describing the type and content of the resource file (e.g. map, photo, etc); <code>• &lt;mimeType&gt;</code>: identifier of the MIME content type and sub-type of the resource file as described in (RFC2046); <code>• &lt;uri&gt;</code>: the Universal Resource Identifier (URI) of the hyperlink for the resource file. It is typically a Uniform Resource Locator (URL), used to retrieve the resource over the internet;</td>
</tr>
<tr>
<td>Segment</td>
<td>Description</td>
<td>Main sub-elements</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| <area>  | Describes the geographic area of the referred hazard by specifying geospatial shapes (polygons and circles) with their relative latitude, longitude and altitude values. A message can have more than one associated <area>. | • **<derefUri>:** it is the alternative of the URI and contains the base-64 encoded content of the resource file.  
• **<areaDesc>:** text describing the affected area of the message;  
• **<polygon>:** pairs of points defining a polygon that delineates the affected area of the message. The polygon is represented by a whitespace-delimited list of (WGS 84) coordinates pairs;  
• **<circle>:** paired values of a point and radius delineating the affected area of the message. The circular area is represented by a central point with (WGS 84) coordinate pair and a radius value in kilometres. |

The CAP template is simple but precise and allows its adoption to different scenarios. A single message can be manually forwarded to the linked warning systems, which convert it in the form suitable for their technologies (e.g. text caption on tv, voice on radio and telephone, triggering sirens), or can be also integrated in automatic procedures and triggered in turn by the warning systems (e.g. a wireless sensor device, collocated with a siren, triggers a CAP message that includes the location and the sensed data after the siren activation). We give below an example of a CAP alert message as part of the Homeland Security Advisory System Alert of the United States (Figure 10). More examples, including that one just mentioned, are available in (CAP, Common Alerting Protocol Version 1.2).
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>43b080713727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Security</category>
    <event>Homeland Security Advisory System Update</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <senderName>U.S. Government, Department of Homeland Security</senderName>
    <headline>Homeland Security Sets Code ORANGE</headline>
    <description>The Department of Homeland Security has elevated the Homeland Security Advisory System threat level to ORANGE / High in response to intelligence which may indicate a heightened threat of terrorism.</description>
    <instruction>A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider agency-specific Protective Measures in accordance with their existing plans.</instruction>
  </info>
  <parameter>
    <valueName>HSAS</valueName>
    <value>ORANGE</value>
  </parameter>
  <resource>
    <resourceDesc>Image file (GIF)</resourceDesc>
    <mimeType>image/gif</mimeType>
    <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
  </resource>
  <area>
    <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
  </area>
</alert>

Figure 10 – Example of CAP message
(Source: CAP, Common Alerting Protocol Version 1.2)
4. Overview of selected Public Warning Systems

Numerous public warning systems are used all over the world. They are mostly developed at national and local level, identifying procedures aimed at managing the communication during specific events and which better fit the background of each country/region. Generating well-defined management and communication procedures at a higher level, for example at a supranational level, is rather difficult. This difficulty arises on the one hand because of the specific needs of each country (e.g. more involved in certain types of hazards, preferred communication channels, etc.), on the other because the process of harmonization of the organizational infrastructure requires a very high effort in terms of management and control, both from the single countries and the supranational institutions who they belong. However, the support of higher-level organizations (and of their tools) can provide a better overview on the evolution of potential risks due to incoming hazards, allowing the implementation of communication strategies able to prevent efficiently the impact of the catastrophic event and to act in a timely manner during the manifestation of the event itself, in order to minimize the impacts as much as possible.

In the following paragraphs, we present some relevant cases of public warning system, analysing their functionalities, the technologies adopted and the impact that they have on people. We will first analyse systems that develop at a macro level (i.e. USA, EU), then shifting to relevant cases at national and local level, focusing on the area covered by the European Union. Important is the fact that none of the presented systems manage in such a way the people’s feedbacks, instead they all adopt a one-way communication method, from the professionals to the common people. This last point can represent a big challenge for the development of new types of PWS.

4.1 Macro level case studies

4.1.1 USA

In USA, the Federal Emergency Management Agency (FEMA\(^8\)) is in charge to support citizens and emergency personnel to build, sustain, and improve the nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. In 2006, in response to the disaster caused by Hurricane Katrina, the United States Department of Homeland Security, to which the FEMA belongs, was mandated to establish a new programme to modernize the existing population warning systems. For this reason, the FEMA designed and created an infrastructure able to integrate the pre-existing national systems into a single modern network, with the capabilities to exploit the emerging communication technologies. This network is called IPAWS\(^9\), Integrated Public Alert and Warning System, and today it represents the official US alert and warning infrastructure. The main mission of IPAWS is to provide integrated services and capabilities to local, state and federal authorities that enable them to alert and warn their respective communities via multiple communication methods. In fact, even pre-existing territorial and local government alert and warning systems have been able to integrate with the national infrastructure, providing a broader range of message options and communication pathways for the delivery of alert and warning information to the American people before, during and after a catastrophic event. Of course, due to its flexible but well-defined structure, even new alerting authorities or dissemination channels can be easily included in the infrastructure and this makes the IPAWS always ready to be extended with new emerging technologies.

---

8 https://www.fema.gov/
9 https://www.fema.gov/integrated-public-alert-warning-system
The IPAWS infrastructure identified two types of messages:

- alert message, that gives notice to the public that an event has occurred (e.g. a radio short sound, action or message);
- notification message, which includes more information than the notification and usually contains descriptions of the events and instructions for the public to try to protect them either from potential or ongoing hazards.

IPAWS in itself is not an alert and notification system but represents instead an input service to multiple alert and notification systems. It uses the CAP protocol to receive an alert and/or notification message from an alerting authority (left part of Figure 11), collects and validates the message through its open platform (IPAWS-OPEN) and distributes the message to multiple dissemination channels exploiting in turn the CAP protocol. Once the authority sends a message, the IPAWS-OPEN component performs some validation controls for ensuring that the source of the alert/notification is valid (i.e. certified), to make certain that the message is compliant with the CAP standard and to check if the authority has the permission to send this type of communication and to use the selected dissemination channel. If all these requirements are satisfied the message is forwarded to the correct dissemination channel, that is included in one of the following listed below:

- Emergency Alert System (EAS\textsuperscript{10}): the message dissemination pathway that sends warning via broadcast, cable, satellite and wireline services;
- Wireless Emergency Alert (WEA\textsuperscript{11}): the message dissemination pathway that broadcasts alert and warnings to cell phones and other mobile devices;

\textsuperscript{10} https://www.fema.gov/emergency-alert-system
\textsuperscript{11} https://www.fema.gov/frequently-asked-questions-wireless-emergency-alerts
• NOAA Weather Radio (NWR\textsuperscript{12}): a nationwide network of radio stations promulgated by the National Weather Service (NWS), that includes 1000 transmitters covering all 50 states, adjacent coastal waters, Puerto Rico, the U.S. Virgin Islands, and the U.S. Pacific Territories;
• Internet Systems\textsuperscript{13}: the All-Hazards Emergency Message Collection system (“HazCollect”), offered by NWS, automatically relays Non-weather Emergency Messages over the internet to subscribing software providers;
• Local Alerting Systems: the message dissemination pathway that sends warning and notification through specific communication technologies in all those areas subscribed for that kind of message.

![Diagram of IPAWS Alert, CAP feed, and Google Ecosystem]

*Figure 12 - Exploitation of the IPAWS infrastructure by Google Public Alerts system*

An example of dissemination channel included in the Internet Systems group is the Google Public Alerts\textsuperscript{14} tool, that reads the CAP messages from IPAWS-OPEN and make the IPAWS alert usable from its map service (through colour-coded layers) or from the search service (text and news feed).

![Example of an IPAWS alert published by google and available through its tools]

*Figure 13 - Example of an IPAWS alert published by google and available through its tools*

\textsuperscript{12} http://www.nws.noaa.gov/nwr/
\textsuperscript{13} https://www.fema.gov/media-library/assets/documents/113304
\textsuperscript{14} https://www.google.org/publicalerts
4.1.2 European Union
Under the umbrella of the Copernicus\textsuperscript{15} programme, the EU has created services and systems in order to support all Member States in improving emergency management. More precisely, within the public warning management systems, the Copernicus programme offers a service called Copernicus Emergency Management Service (Copernicus EMS).

Copernicus EMS provides information for disaster response management and supports recovery, disaster risk reduction, prevention, and preparedness activities. The service provides maps based on satellite imagery, addressing various emergency situations arising from natural or man-made disasters, as well as public warning services for flood and fire risks. It is composed by two main services:

- **the mapping component, which** provides map products and analysis in case of disasters. It addresses a wide range of emergency situations resulting from natural or man-made disasters, covering floods, earthquakes, tsunamis, landslides, severe storms, fires, industrial accidents, volcanic eruptions, and humanitarian crises;
- **the early warning component, which** delivers alerts and risk assessments of floods and forest fires.

For our purposes we focus the attention on the second component, the **Copernicus EMS early warning component**. It offers two services called European Flood Awareness System (EFAS\textsuperscript{16}) and European Forest Fire Information System (EFFIS\textsuperscript{17}).

**EFAS:** Fully operational since 2012, the EFAS is one of the longest running public warning flood systems in the world that covers such a diverse geographical area and boasts so many cooperating partners. It is also the first operational European system monitoring and forecasting floods across Europe. Today, this public warning system has the ability to begin providing warnings up to ten days in advance. This is made possible through the four operational centres executing the different parts of the service:

- **the EFAS Computational centre, where** the flood forecasts are produced and the EFAS information system platform is hosted;
- **the EFAS Dissemination centre, that** analyses the produced outputs and disseminates the information to the partners;
- **the EFAS Hydrological data collection centre, that** collects historic and real-time discharge and water level data across Europe;
- **the EFAS Meteorological data collection centre, that** collects historic and real-time meteorological data across Europe.

The service delivers the needed flood warning information to the partner National/Regional Hydrological Services and the European Response and Coordination Centre (ERCC\textsuperscript{18}). Technical leadership and development are provided by the JRC under the umbrella of the Copernicus emergency management service. EFAS service is currently not fully open to the public. Flood warnings are only made available to the partners and the ERCC. Currently the historical flood information access is being tested (Figure 14).

\textsuperscript{15} http://www.copernicus.eu/
\textsuperscript{16} https://www.efas.eu/
\textsuperscript{17} http://forest.jrc.ec.europa.eu/effis/
\textsuperscript{18} The Emergency Response Coordination Centre supports and coordinates a wide range of prevention and preparedness activities, from awareness-raising to field exercises simulating emergency response
EFFIS: Beside EFAS we have the EFFIS service. It provides the necessary information to prepare, mitigate and follow the forest fire hazards across Europe. This tool has been established by the European Commission (EC) together with the relevant fire services in the EU Member States and European countries. The goal of EFFIS is to provide harmonised information on forest fires and assess their effects in the pan-European region. For this purpose, a collaboration with EU Member States and neighbouring countries has been ongoing since 1998. EFFIS computes and spread across Europe fire related information, such as fire danger indices used to estimate the risk that a fire occurs in a given area. The fire danger forecast of EFFIS generates daily maps forecasting 1 to 10 days in advance and normally operates using meteorological forecast data received daily from the European Centre for Medium-Range Weather Forecast (ECMWF) and the French (MeteoFrance) meteorological services. Since 2007, EFFIS adopted the Canadian Forest Fire Weather Index (FWI) System as the method for the assessment of the fire danger level in a harmonized manner throughout Europe. For example, the layer presented in Figure 15 shows a fire danger forecast provided by ECMWF, computed with the FWI and having a spatial resolution of 16 kilometres. Each portion of the map is associated to a class which represents the danger level with respect to the risk of a fire. The classes are six and goes from very low danger (portion in green) to extreme danger (in the Figure 15, the portion in black).
EFFIS also provides information on fuel moisture and drought conditions. Active fires are detected using earth observation imagery: the MODIS\(^{19}\) and VIIRS\(^{20}\) sensors. Temperature differences between the areas that are actively burning with respect to neighbour areas allows the identification and the mapping of active fires. The spatial resolution of the active fire detection system is between 375 m (VIIRS) and 1 km (MODIS). All the geospatial layers can be accessed using a Web Map Service (WMS), such as Geoserver\(^{21}\), or requested using the web form.

**METEOALARM**: Meteoalarm\(^{22}\) is an initiative by EUMETNET, the public European weather services network within the World Meteorological Organization (WMO). It is a cooperative service that provides information to public and authorities about severe weather condition in 37 European countries. The warnings provided by Meteoalarm include: heavy rain with risk of flooding, severe thunderstorms, gale-force winds, heat waves, forest fires, fog, snow or extreme cold with blizzards, avalanches, severe coastal tides. The raw data are open and can be accessed through RSS\(^{23}\) feed, an XML-based web feed.

---

19 https://modis.gsfc.nasa.gov  
20 https://www.raytheon.com/capabilities/products/viirs/  
21 http://geoserver.org/  
22 https://www.meteoalarm.eu  
23 http://www.rssboard.org/rss-specification
The danger of a weather phenomenon and its impacts to society are described by colour-coded awareness levels. Colour coding is harmonized among the Meteoalarm member countries so that a specific colour indicates the same level disruption and potential danger caused by severe weather, no matter in which of the countries the event is happening. The selected colour coding for representing the awareness level is the following:

- Green, when no particular weather awareness is needed over land;
- Yellow, when the weather is potentially dangerous. It means that common meteorological phenomena have been forecast;
- Orange, when the weather is dangerous. It means that unusual meteorological phenomena have been forecast;
- Red, when the weather conditions are very dangerous. It means that exceptionally intense meteorological phenomena have been forecast.

4.2 European national and local case studies

In this section we report some examples of public warning system implementation in the countries of the European Union. In some cases, we will focus also on how those systems are managed at a regional point of view.
The information has been collected from public documentation available online. Some of the pilots have been then investigated further through in-dept interviews with representatives of national organizations. The interviews have focused in particular on the current PWS in use, technical standards and future perspectives (the script is included in Annex II – Script Interview on Future perspectives on PWS).

THE NETHERLANDS: the PWS in the Netherlands is based on a centralized national architecture that serves the forces in charge of the Early Warning and Response, at any level. The system is multi-hazard and multi-channel, and includes procedures to dispatch alert communication through the national siren system, the cell broadcasting technology and specific social media channels (Twitter, Facebook and Instagram). Since 2012, the Dutch government have provided to their citizens a system called NL-Alert24. NL-Alert is an alert system for emergencies that allows the authorities to inform people in the surrounding area of the event, by sending SMS to their cell phones. The message describes the situation and give instructions to the people for facing the emergency. All the cell phones in the relevant area will receive the messages automatically, given that the phone is switched-on and the telephone has reception25. The messages are not sent by texting but by means of cell broadcasting technology through all providers' transmission towers, as specified in ETSI TS 102 900 standard (2012).

All the messages start with the words "NL_Alert", followed by date, time and nature of the event. Instructions on how to proceed are usually included in the message. The figure above shows a NL-Alert message that reports the following information: "NL-Alert 22-06-2017 05:28 large fire in Eindhoven, Quinten Matsyslaan 35B. Stay out of smoke, close windows and doors, and turn off mechanical ventilation".

Concerning the future perspective, the Netherlands plans to dismiss the sirens within the next 5 years to rely more on the cell broadcasting, the social media and the mobile applications because considered more effective in reaching people. According to this direction, among the ongoing projects, it is interesting to highlight the development of a mobile application dedicated to enterprises, which can notify and share information and alerts on chemical hazards.

24 https://crisis.nl/nl-alert/
26 https://nltimes.nl/2017/07/03/national-cellphone-emergency-alert-test-scheduled-noon
SPAIN: in Spain, the responsibility for the implementation of public warning mechanism is in charge of the General Directorate for Civil Protection (Ministry of the Interior) and the Regions. As described in (EENA, 2015), the Operation Document for Public Warnings of the European Emergency Number Association (EENA), the General Directorate of Civil Protection is responsible for all regulation related to critical infrastructures, such as dams or nuclear plants, even if there is not a unique regulation for all the critical infrastructures, but each type has a specific national regulation. The types of warning systems typically include:

- Acoustic warning based on sirens (Pneumatic/ Electronic) with specific signalling (i.e. French warning signal at a frequency of 200 Hz) to issue signals to the flooding area. Figure 18 shows the connectivity between the sirens (green lines) and the colour-coded representation of the signal power (from – 107 dBm to -67 dBm);
- 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.

![Figure 18 - Coverage area of a siren system for a flooding](Source: EENA)

Regarding the regions, public warning measures vary widely from one region to another, from a siren-based warning, to mass messages being sent to fixed lines, faxes, SMS or email. For example, the Meteorological Service of Catalunya\(^27\), publish an online warning bulletin for the weather conditions. The bulletin is issued each time a weather event reaches one of the thresholds shown in Table 6 and it is updated twice a day until the end of the episode. In Figure 19 an example of an avalanche bulletin.

---

### Table 6 - Warning thresholds of the Meteorological Service of Catalunya bulletin

<table>
<thead>
<tr>
<th>Meteor</th>
<th>Low threshold</th>
<th>Threshold high</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intensity of rain</strong></td>
<td>Intensity &gt; 20 mm / 30 minutes</td>
<td>Intensity &gt; 40 mm / 30 minutes</td>
</tr>
<tr>
<td><strong>Accumulation of rain</strong></td>
<td>Accumulated &gt; 100 mm /24 hours</td>
<td>Accumulated &gt; 200 mm /24 hours</td>
</tr>
<tr>
<td><strong>Snow accumulated in 24 hours</strong></td>
<td>thickness ≥ 0 cm, altitude less than 300 meters</td>
<td>thickness &gt; 5 cm in height less than 300 meters</td>
</tr>
<tr>
<td></td>
<td>thickness &gt; 2 cm in altitude over 300 metres up to 600 metres</td>
<td>thickness &gt; 15 cm in altitude over 300 metres up to 600 metres</td>
</tr>
<tr>
<td></td>
<td>thickness &gt; 5 cm in altitude higher than 600 metres to 800 metres</td>
<td>thickness &gt; 20 cm in altitude higher than 600 metres to 800 metres</td>
</tr>
<tr>
<td></td>
<td>thickness &gt; 10 cm in altitude higher than 800 metres up to 1000 metres</td>
<td>thickness &gt; 30 cm in altitude higher than 800 metres up to 1000 metres</td>
</tr>
<tr>
<td></td>
<td>thickness &gt; 20 cm in heights above 1000 meters up to 1500 meters</td>
<td>thickness &gt; 50 cm in heights above 1000 meters up to 1500 meters</td>
</tr>
<tr>
<td><strong>Wind</strong></td>
<td>Highest streak &gt; 20 m/s to: Anoia, Alt Penedès, Bages, Baix Llobregat, Baix Penedès Barcelonès, Garraf, Gironès, Maresme, el Moianès, Vic, Pla d’urgell, Segarra, Segrià, Selva, Tarragona, Urgell, Vallès Occidental and Vallès Oriental</td>
<td>Highest streak &gt; 30 m/s to: Anoia, Alt Penedès, Bages, Baix Llobregat, Baix Penedès Barcelonès, Garraf, Gironès, Maresme, el Moianès, Vic, Pla d’urgell, Segarra, Segrià, Selva, Tarragona, Urgell, Vallès Occidental and Vallès Oriental</td>
</tr>
<tr>
<td></td>
<td>Highest streak &gt; 30 m/s Alt Empordà, Baix Ebre and Montsià</td>
<td>Highest streak &gt; 40 m/s region of Alt Empordà, Baix Ebre and Montsià</td>
</tr>
<tr>
<td><strong>State of the sea</strong></td>
<td>Waves &gt; 2.50 metres (heavy sea)</td>
<td>Waves &gt; 4.00 metres (mar brava)</td>
</tr>
<tr>
<td><strong>Cold</strong></td>
<td>Minimum extreme temperature: temperature lower than the percentile 2 of the minimum temperature daily</td>
<td>Wave of cold: temperature below the percentile 2 of the minimum temperature daily for three consecutive days or more</td>
</tr>
<tr>
<td><strong>Heat</strong></td>
<td>Maximum extreme temperature: a temperature higher than the percentile 98 of the daily max temperature</td>
<td>Heat wave: temperature above the percentile 98 maximum temperature daily for three consecutive days or more</td>
</tr>
</tbody>
</table>
ITALY (Piedmont): emergency managements systems in Italy are coordinated by the national Department of Civil Protection within the Functional Centres Network, having a Centre in each region and autonomous province of the country. As a representative example, we report here how the emergency system is managed in Piedmont region, in the north-west side of Italy. In Piedmont, the functional centre is the Regional Agency for Environmental Protection (ARPA), literally: “Agenzia Regionale per la Protezione Ambientale”\(^{28}\). Among other activities, ARPA operates a hydro-meteorological monitoring system that uses automatic tools to determine soil and atmospheric conditions. The interpretation of the data acquired and the results of data processing by modelling make it possible to carry out the continuous surveillance of the environment and the territory, to manage prediction, alerting and monitoring systems for situations requiring special attention, and to update on a continuous basis the climatological documentation for the usage in planning and programming activities. ARPA issues everyday a meteo-hydrological warning bulletin\(^{29}\) with a 36 hours validity.

---

\(^{28}\) [http://www.arpa.piemonte.it/](http://www.arpa.piemonte.it/)

The bulletin provides information on 11 homogeneous areas, pointed with letters from A to M. Besides the indicator of each area, possible critical situations are highlighted for weather events (in the case of Figure 20 no events are detected). In the right part of the bulletin, for each area, critical situations related to the effects of weather events are highlighted by a colour and eventually a description. The used colours are green, yellow, orange and red, indicating the criticality level of the event, from the absence of criticality (green) to the maximum criticality level (red). ARPA Piedmont is in charge to send the bulletin to the national civil protection, which is responsible eventually for activating the operating procedures, according to the alert range. Finally, the municipalities are responsible for alerting the population. There is no a unified procedure valid for all the municipalities, instead each of them acts according to internal rules (some municipalities use SMS service, some other use sirens and so on).

Interesting is the fact that all the bulletins are provided also in the form of a **CAP message**, as shown in the Figure 21.

---

**Figure 20 - Meteo-Hydrological warning bulletin issued by ARPA Piedmont**
(Source: ARPA Piedmont)

The bulletin provides information on 11 homogeneous areas, pointed with letters from A to M. Besides the indicator of each area, possible critical situations are highlighted for weather events (in the case of Figure 20 no events are detected). In the right part of the bulletin, for each area, critical situations related to the effects of weather events are highlighted by a colour and eventually a description. The used colours are green, yellow, orange and red, indicating the criticality level of the event, from the absence of criticality (green) to the maximum criticality level (red). ARPA Piedmont is in charge to send the bulletin to the national civil protection, which is responsible eventually for activating the operating procedures, according to the alert range. Finally, the municipalities are responsible for alerting the population. There is no a unified procedure valid for all the municipalities, instead each of them acts according to internal rules (some municipalities use SMS service, some other use sirens and so on).

Interesting is the fact that all the bulletins are provided also in the form of a **CAP message**, as shown in the Figure 21.
In this case the message has an <alert> block with some parameters inside of it (i.e. identifier, sender, sent, msgType, source, scope, note) and a sequence of 11 <info> blocks, one for each area of the region. The <info> block contains information on language, category, event responseType, urgency, severity, certainty, onset, expires, instruction and a set of parameters.
With the usage of the CAP standard, all the messages produced by ARPA can be included in automatic systems which can exploit them to activate the right communication channel or the most effective communication procedures.

**GERMANY**: since 1st July 2013, the German government has implemented its national Modular Warning System (MoWaS). The MoWas uses the government Satellite-based Warning System (SatWaS). Its creation is born of the necessity to extend the classical warning communication technologies (e.g. sirens) with the new ones (e.g. smartphones, drones, responsive internet application, etc). In this sense, MoWaS can be seen as a development stage of SatWaS, where the former goes beyond the limitations of power outages and loss of terrestrial transmission path of the latter, which often occur in certain areas during an ongoing catastrophic event. The MoWaS system is composed of three main blocks: trigger, transmission path and terminals.

**Figure 22 - Structure of the Modular Warning System (MoWaS)**
(Source: BBK)

The **trigger**, left side of Figure 22, includes the part of the decision makers and the controller using MoWaS stations in the situation centres of the Federal Government and the Federal States, as well as in the connected local control centres of the counties and independent towns. All transmission processes between the MoWaS and the MoWaS server are part of this sending part. After this, the **transmission path** aiming all warning multiplier starts. It includes all the elements from the MoWaS-server to the warning multipliers or the control systems of warning instruments (e.g. sirens). Warning multipliers can operate all kinds of end devices. Finally, the communication comes to the **terminal devices**, that include all warning media and instruments which are directly available to the population as end users. Addressees and devices which can transmit customised content, e.g. warning texts and recommendations for behaviour, are referred to as warning media. A wake-up call is generally included if the device has been prepared or set up accordingly (e.g. radio, television, internet, mobile app, etc). Devices which exclusively transmit a wake-up signal (e.g. sirens) or standardised text contents (e.g. some pager services) are referred to as warning instruments. All the

---

30 https://www.bbk.bund.de/EN/Topics/Crisis_management/Warning/MoWaS/MoWaS_node.html
31 https://www.bbk.bund.de/EN/Home/home_node.html
messages exchanged through the three blocks (i.e. trigger, transmission path and terminals) are formatted by following the CAP protocol.

As an example of a MoWaS terminal device we report here a mobile app called NINA\(^{32}\), which allows to disseminate the information to citizens via their mobile phones. The application is equipped with a built-in push-function which allows the citizens to be continually informed about the hazards. It offers also advices and event-related behaviour hints from experts, in order to improve the people capabilities in addressing the emergencies.

**UNITED KINGDOM**: another interest case study to present is the Flood Information Service\(^{33}\) provided by the Environment Agency of the UK. The service gives information on local flood risk warnings for England and Wales and publishes detailed descriptions on the potentially affected areas.

The information is accessible through the internet portal and a set of open APIs\(^{34}\). In addition, all the warning communications are also available as CAP messages.

---

32 [https://www.bbk.bund.de/DE/NINA/Warn-App_NINA_node.html](https://www.bbk.bund.de/DE/NINA/Warn-App_NINA_node.html)
33 [https://flood-warning-information.service.gov.uk/warnings](https://flood-warning-information.service.gov.uk/warnings)
The Flood Information Service offers also a 5-day flood risk bulletin which assess the severity of an event through colour-coded warning levels:

- Green (very low risk), which means that a flood event is very unlikely;
- Yellow (low risk), which means that a flooding is possible and people need to be aware;
- Orange (medium risk), which means that a flooding is expected and people need to be prepared;
- Red (high risk), which means that there are significant risks to life regardless the fact that a flood event is either already ongoing or not.
An interesting feature made available by the Flood Information Service is the so-called Dashboard\textsuperscript{35} which gives statistical information on the service usage and on additional measures such as the costs incurred by the government for providing and maintaining the service, the total numbers of users, the way the users access the service (i.e. mobile phones, pc, tablet).

![Figure 26 - Snapshot of the Flood Information System Dashboard](https://www.gov.uk/performance/flood-information-service)

**GREECE**: Greece is on the path to centralize the PWS infrastructure. From the organizational and procedural perspectives, it is already unified under the national Civil Protection organization. The current PWS infrastructure entails different connected subsystems including public displays. Other channel in use are press, radio, tv as well as web and social media. Sirens can be activated in case of for air attack and natural disasters, but the systems are under military control. Clear policies and continuous maintenance of guidelines and supporting material are considered core bricks of a more effective warning reception and response in case of hazard. In future, the cell broadcasting technology and dedicated mobile applications will be introduced, also to cope with the need to differentiate the touchpoints dedicated to the public, currently limited to the national emergency number. The recent natural disasters that Greece have suffered have put in evidence

\textsuperscript{35}https://www.gov.uk/performance/flood-information-service
the increasing complexity of the disaster scenarios. The priorities that will orient future innovation focus on **increasing prevention, increasing preparedness**, with a specific goal on the announcement tailoring and **improved collaboration among agencies**.

**FRANCE**: currently the PWS infrastructure in France consists of a mix of local and remotely connected systems. The main traditional communication channels are in use, even though the goal is to reduce the channel dispersion, conveying the greatest part of crisis communication on the same channel. Following this line, the future investments go towards the **maximization of the use of the social media, Twitter in particular**, as main touchpoint to alert the population. Beside their wide adoption and the technological stability, a very active support of the VOST and digital volunteers to maintain updated a range of twitter accounts, contributes to motivate this approach. The expressed need from French authorities is about a **European common system of public warning**, that would improve the cross-border cooperation among agencies and guarantying accessibility to the population on the base of a same communication strategy and implementation.

### 4.3 Use cases recap

We report here a recap table of the status quo for the various PWS of the analysed countries. The table highlights the actual features of each PWS use case and the observed trends for the near future when available.

#### Table 7 – Case Studies overview

<table>
<thead>
<tr>
<th>Country</th>
<th>PWS features</th>
<th>Delivery channels in use</th>
<th>Usage of CAP</th>
<th>Future outlooks</th>
</tr>
</thead>
</table>
| USA     | Centralised PWS (IPAWS) with an ICT infrastructure used by all the public warning national organizations | • SMS Broadcast  
• Radio, TV  
• Apps, web, digital signage  
• Social media  
• Mass notification systems  
• Sirens | Yes, at any level | NA |
| NL      | Centralised PWS infrastructure (crises.nl), but without a unique ICT architecture that can be used by all the public warning national organization | • SMS Broadcast  
• Radio, TV  
• Websites  
• Social media  
• Sirens | No, but they have their internal template for the NL-Alert System | They are planning to create a national mobile application for the public warning dissemination. They are also planning to dismiss their siren system within the next 5 years |
| SP      | Many non-unified systems at different levels | • SMS Broadcast  
• Radio, TV  
• Sirens | No | NA |
| IT      | Many non-unified systems at different levels | • Radio, TV  
• Websites  
• Sirens | No, but there are few individual attempts to use the CAP standard. However, it is not included in the | NA |
<table>
<thead>
<tr>
<th>Country</th>
<th>PWS features</th>
<th>Delivery channels in use</th>
<th>Usage of CAP</th>
<th>Future outlooks</th>
</tr>
</thead>
</table>
| DE      | Centralised PWS (MOWAS) with an ICT infrastructure used by all the public warning national organizations | • Broadcast SMS  
• Radio, TV  
• Apps (NINA)  
• Websites  
• Social media  
• Mass notification systems  
• Sirens  
• Paper | Yes, at any level | NA |
| UK      | Many non-unified systems at different levels. The flood environmental agency acts with a centralised ICT infrastructure with public APIs | • Websites  
• Social media | Yes, but only for flood | NA |
| GR      | Many systems at different levels | • Sirens  
• TV, Radio  
• Social Media | No | They are moving in the direction to implement a SMS broadcast system and a centralized mobile application |
| FR      | Many systems at different levels | • Sirens  
• TV, Radio  
• Social Media (Twitter) | No | They are moving in the direction of the improvement of their social media channels, especially Twitter |
5. Recommendations

In this section we provide a set of recommendations related to the implementation of an effective PWS, presenting them as key take-aways, and dividing them into three sections: organizational best practices, system architecture, technical standards, and guidelines on styling. The conclusions drawn in this section, together with the guidelines reported in Section 2, are meant to help decision makers in planning the evolutions of current PWS.

5.1 Organizational best practices

From the functional point of view, technical standards guarantee that the technological infrastructure and system work properly to reach and fully meet the goals of the PWS. Besides the technical capacity, non-technical requirements and capabilities are worth to be considered when implementing innovative solutions. The PWS is highly dynamic, where the content is subject to frequent changes and updates, and where different agents may need different contents and specific representations.

Organizational measures, meaning official procedures linking Early Warning and Response at different scale, from national to local level and vice versa, are mandatory to allow the PWS to be effective. However, the full potential of the PWS can be better exploited if ruled not only by emergency protocols, but also by an effective communication strategy, which is a crucial activity (EPR-Public Communication, 2012) that entails the design and the implementation of a decision tree that specifies what to communicate, when, how and to whom. The people-centred PWS is the right approach in order to address the aforementioned needs, and it can be outlined as follows (UNDP, 2016; Basher, 2006).

<table>
<thead>
<tr>
<th>Step</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CREATE A DEDICATED GROUP ON PUBLIC WARNING COMMUNICATION</td>
</tr>
<tr>
<td></td>
<td>It is important to dedicate human resources to the warning communication design and management. The suggestion is to create in advance, train and support a dedicated group of people in charge of design and assess the strategy and the operation of handling inbound and outbound information and warnings. The mission of the group is to guarantee to effectively convey and disseminate the proper information to the proper receivers through the most suitable channels and verify the impact of the communication strategy. It should also guarantee the accuracy of information, the harmonization of the messages provided by the official sources, and work with the local organizations to harmonize the communication and manage the interplay between authorities and citizens.</td>
</tr>
<tr>
<td></td>
<td>The Public Warning Communication Group should include some specific profiles, such as:</td>
</tr>
<tr>
<td></td>
<td>• Crisis communication manager, to lead and manage the information to be disseminated according to the communication strategy and to guarantee the Intra- and inter-organisational coordination and cooperation;</td>
</tr>
<tr>
<td></td>
<td>• User Experience and graphic specialist, to define the adaptation of the messages and their style for different targets and channels;</td>
</tr>
<tr>
<td></td>
<td>• Social media specialist, to manage the social networks, both with respect to data collection and communication with the population, institutions, other organizations;</td>
</tr>
<tr>
<td></td>
<td>• Communication Engineer, to implement the communication strategy and monitor the ICT infrastructure;</td>
</tr>
<tr>
<td>Step</td>
<td>Actions</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>•</td>
<td>Legal consultant, to ensure liability and regulations compliance.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td><strong>CONTINUOUSLY MAP THE COMMUNITY</strong>&lt;br&gt;The official maps provided by the competent authorities that monitor the expected risks should be complemented with specific maps of the local communities. This will help the decision-making process in each DRM phase, which have to be based on the real social structure, including the accurate knowledge of the human resources available on the territory. The community mapping shall monitor:&lt;br&gt;- Formal groups, e.g., associations and other emergency-related organizations active on the field;&lt;br&gt;- Local population meaningfully segmented including impaired and frail people, e.g., people with disabilities, such as speech and hearing impaired, non-local language speaking, elderly, children;&lt;br&gt;- Trained staff in social and health services (hospitals, rest homes, schools of every level, ...), whom could be helpful to support during emergency situations;&lt;br&gt;- Productive bodies, e.g., enterprises;&lt;br&gt;- Informal groups, e.g., support groups, leisure groups, etc.;&lt;br&gt;- Transitory people, e.g., visitors that usually don’t know the areas nor the specific risks;&lt;br&gt;- Communing people, namely people that are daily commuters due to work or other reasons;&lt;br&gt;- Local media;&lt;br&gt;- Other groups.&lt;br&gt;For each of the above groups, the reference persons and his/her preferred communication channels (e.g. phone, email, social media) have to be collected, kept updated, and used in the alerting strategy.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>DESIGN and KEEP UPDATED THE COMMUNICATION ASSETS</strong>&lt;br&gt;A good Public Warning communication strategy has to exploit the multi-channel capabilities of the PWS infrastructure according to the technical standards and the audience characteristics. The definition of such strategy has to be coordinated by the Public Warning Communication Group but it can also involve different stakeholders, agencies, local communities and group leaders, whom can help in the definition of:&lt;br&gt;- multi-hazard scenarios together with the associated target audience and the mapping with the systems and channels to be used in the identified cases;&lt;br&gt;- the main communication procedures to be followed;&lt;br&gt;After a consolidation of the above, communication experts and designers will then:&lt;br&gt;- design the informative resources needed to cover and serve all DRM phases and the different channels managed by the PWS, the population segments, incompliance with the standards;&lt;br&gt;- iteratively test the resources created with selected representatives of the audience groups, and integrate the feedbacks collected in order to optimize the initial designs;&lt;br&gt;- Prepare a dissemination plan according to all scenarios and media selected;&lt;br&gt;- Prepare and implement an impact assessment toolkit to be able to assess the communication strategy.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td><strong>IMPLEMENT THE PEOPLE CENTRED PWS</strong>&lt;br&gt;The implementation of new practices and systems has to be assessed over time. The following actions are key in order to create an effective PWS:&lt;br&gt;- Periodic training of the operators through practical exercises on the use of the PWS systems and on the evaluation techniques and tools;&lt;br&gt;- Educate the target audiences on the topics of risk awareness, prevention and on the possible ways to cooperate and support the official authorities in case of incoming or ongoing crisis;</td>
</tr>
<tr>
<td>Step</td>
<td>Actions</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>• Keep the channels alive with awareness information and knowledge tips, not only via the social media, but also via local TV, radio, and use paper materials to foster the communication with the local community;</td>
</tr>
<tr>
<td></td>
<td>• Involve the public in two-way communication, e.g. by creating a mobile application that allows citizens to provide selected information and feedbacks;</td>
</tr>
<tr>
<td></td>
<td>• Assess the timeliness, effectiveness and impact of the PWS and of the communication strategy introduced.</td>
</tr>
</tbody>
</table>

The standards selected in this document (Section 3) represent the core reference to **improve the procedural aspects of the Public Warning process**. Moreover, some international agencies provide ready-made toolkit for supporting the harmonization of the information according to populations segments and media characteristics (Section 2.3). The integration of these resources can improve the communication among all DRM stakeholders, including authorities at any level and the general public. Moreover, a standard-based approach can facilitate the **cross-border communication** among neighbouring countries.

Cross-border situations are common in meteorology. In fact, most European countries are relatively small in comparison with the scale of typical synoptic meteorological phenomena. Many important weather events, including windstorms, heavy rains, coastal surges or cold spells can affect large geographical areas containing several countries simultaneously; and these can occur within a very short timescale. This means that the need for effective exchange of warnings has existed in various European countries, and such exchanges have been developed for some time. The European Multi-Purpose Meteorological Awareness (EMMA) Programme (also known as Meteoalarm) is based on the concept of meteorological awareness and its general objective is to develop a graphical information system accessible by the general public for the provision of expected meteorological hazards within 24 hours. The system is intended to complement the existing national warning systems by providing a simple and efficient way of making users aware of possible meteorological risks. Note that the Meteoalarm system is mentioned only as a good example of integration, but it is only an information aggregator with a web interface, which is useful for supranational entities such as the EU to have some level of information. It is not a satisfy the requirements of a PWS and it cannot serve the needs of local, regional, and national authorities for the delivery of alerts to the population.

### 5.2 System architecture

As sketched in Figure 27, the PWS should be inclusive with respect to all DRM actors (i.e. agencies and authorities) involved in the emergency management procedures, supporting the delivery of alerts across multiple hazard and media using a common standard for alert exchange. The PWS must have API to share the alerts with other countries (e.g. border countries) and higher entities (e.g. EU). Therefore, the suggested approach is to build a **national centralized system, which integrates all alert messages sent by the authorities through the Internet, in a unique and secure gateway** to which multiple subsystems can be connected in order to read and spread the alert messages.

For the warning subsystems, a wireless infrastructure is preferable than a cabled once, both for cost saving purposes and for facilitating the connection between the system components. Moreover, the

---

36 [https://www.meteoalarm.eu/](https://www.meteoalarm.eu/)
usage pattern of a PWS can be subject to strong bursts when an emergency is expected or actually ongoing, and experience long periods of underutilization when no hazard is expected. This additional requirement suggests the usage of modern Cloud-based services that, according to the definition given by NIST\textsuperscript{37}, must feature broad network access and rapid elasticity. The latter is of paramount importance to keep OPEX aligned with the actual usage patterns, as show in Figure 28. However, these design choices have to be done in the early stages of the PWS design and should be included in the technical and functional specification document of the PWS system. In this regard, an example of content to include in a specification document is presented in Annex I – Guidelines on technical specification for Public Warning Systems.

\textbf{MULTI-AGENCIES}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{multi-agencies.png}
\caption{Suggested PWS approach}
\end{figure}

\textbf{Figure 27: Comparison between CAPEX model (a) and OPEX model (b).}

\textsuperscript{37}https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
As shown in Figure 29, the suggested architecture should consist of three main components:

- **ALERTING AUTHORITIES (AA):** This component is made up by the public authorities of a country. The authorities can belong to both the national, the regional and the local level, according to the internal regulation on the emergency management. All the authorities have to be certified and granted in order to be an active part of the system. Each authority of the AA component must be able also to send a message using a standard template that, as identified in Section 4.2, can be the CAP standard. The AA component should be extendable, allowing new certified authorities to be included in the system when their technology fits the architecture requirements. This customization feature is crucial, because gives the possibility to include also organizations that are external to the country. This is the case of transboundary authorities, whose public warning messages can be useful in case of cross-border disasters.

- **CENTRAL WARNING SYSTEM INFRASTRUCTURE (CWSI):** It represents the core of the entire system. It is made up by several sub-components that guarantee the communication between the authorities that create the warning message and the dissemination channels. The CWSI contains the **Warning System Main Server** that is the collector and dispatcher of the warning messages. To collect the messages, the Main Server exposes an **Application Programming Interface (API)**, a set of software procedures that allow the authorities of the AA component to send the CAP warning message. The set of APIs is reachable by internet and should be usable only by the authorized organizations. For this reason, the CWSI must contain also mechanisms of user authentication and authorization. When a communication comes to the Main Server, it collects the message in the internal **Warning System Storage** (i.e. a single database or a set of linked databases) to allow future inspections of the messages for several purposes (e.g. internal statistics, etc.) and then it forwards the message to the dissemination subsystems. If permitted,
the Warning System Storage content can be also be made open to third-party users or subsystems that are not part of the PWS infrastructure, and that can use the storage as an “open database of warning system”, usable through API exposed on the internet.

The CWSI must include also a Backup Server, which acts as the Main Server when this last is under maintenance.

After the Main Server have stored the data, it **sends in broadcast the CAP message on the internet through multiple channels** to which the dissemination subsystems are linked. Each linked subsystem should have a dedicated channel that they can “listen” for new incoming messages. All the channels are based on specific rules dependant on the values of the CAP message fields, which allow or deny the message transfer depending on whether specific conditions are matched. The conditions can be based for example on the hazard (the CAP \(<\textit{category}>\) field), the severity (the CAP \(<\textit{severity}>\) field) or the geolocation (the CAP \(<\textit{polygon}>\) field) of the event. In this way the dissemination subsystems can be activated only if a certain severity level is reached or if they are within a certain region of the country.

- **PUBLIC WARNING SUBSYSTEMS (PWS\textit{sub}):** it contains all the subsystems aiming to disseminate the CAP warning message. Each subsystem should have an \textit{Adapter}, a software component that listen to the dedicated channel for new warnings. When the Adapter detects a message on its channel, it reads the communication, parses the CAP message in order to filter only the fields that are needed for the technologies to which it is linked, and spreads the message through the network infrastructure for reaching the correct recipient. The PWS\textit{sub} must be customizable and extendable, allowing the subsystems that will be aligned to the requested technology, to be easily integrated in the system infrastructure. There can be also more than one subsystem using the same type of technology endpoint, for example subsystems with the radio and TV as endpoint that acts at different levels, either national, regional or local. Also, the social media subsystem must keep track and classify all the available channels/pages created by the different agencies (e.g., environmental monitoring, civil protection, fire fighters, red cross, etc.) according to the hazards and the geographical area they cover, so as to automatically post the adapted content on all appropriate pages.

In a view of giving a practical example of a PWS\textit{sub}, we detail a national siren system, which can be effectively used to alert the population in extreme cases requiring immediate reactions. As shown in Figure 30, this system is composed by an adapter, which parses and filters the CAP message, a communication channel and the receiver technology, which is precisely the siren. The Adapter can receive the CAP message both from the CWSI, as previously described, and directly from the authority, in case the CWSI infrastructure is not available yet or it is under maintenance and the backup server is not available.

\[\text{Figure 30 - Suggested Public Warning Subsystem for sirens}\]
Once the Adapter receives the message, it is filtered and translated to be reproduced by the siren. The siren should be multi-tone and should be able to play also voice-recorded messages. The multi-tone feature can be based either on the hazard or on the severity of the message and in this case, the Adapter should check respectively the CAP fields `<category>` or `<severity>`. The voice-recorded feature can instead reproduce a standard message depending on the hazard or on the severity of the warning communication, and in this case the Adapter should check the CAP fields `<category>` or `<severity>` and in addition one of the fields `<uri>` (i.e. the link to the resource voice-recorded message to reproduce) and `<derefUri>` (i.e. the base-64 encoded content of the resource file). All the unnecessary fields must be discarded by the adapter, for minimizing the size of the message sent to the network infrastructure.

The network infrastructure should be constituted by a primary secure (i.e. with encrypted messages) channel, which can be based either on 3G/4G cellular technology or on SATCOM technology, and by a secondary backup channel to be used only if the primary channel is not available. The backup channel can be based either on the TETRA\(^{38}\) standard, which guarantees message encryption, or on the UHF channel, which is commonly used for the television broadcasting and for this reason needs to be secured through an encryption key exchange process on an auxiliary channel. Finally, after the message goes through the channel, it is reproduced by the siren.

To summarize, the national PWS should be designed so as to:

- **be used by all agencies involved in DRM** across all administrative units (e.g. commune, region/department/prefecture, national). The PWS must be able to be configured and map users according to the organization structure of such agencies, associate them with the geographical area under their responsibility, and implement in a configurable rule-based manner the alerting procedures (e.g., escalation to higher level);
- **be used for all kind for alerts**, meaning for all kind of hazards and across all DRM phases;
- **receive standard alerts** from monitoring systems (e.g. sensors) as well as agencies (e.g. operators of environmental agencies, police, etc.) and broker them to public warning subsystems. The CAP standard is the suggested one in order to structure the alert content. The brokerage should be done according to the publish and subscribed pattern\(^{39}\) in order to allow the subsystems to subscribe to the topic of their interest (e.g. if a siren system is used only for nuclear alerting, it will not subscribe to topics related to natural hazards) and according to the area they cover;
- **publicly publish every alert generated** at a given URL containing complete information. This URL, eventually shortened, should be always disseminated despite the content adaptation required to propagate the alert on the selected distribution channels. Note that there are special cases in which this may not be feasible, e.g., in case of tonal sirens. In such cases the population must know a priori how to find the full alert information;
- **feature a reliable deployment** that can guarantee availability, reliability, and fault tolerance, according to clearly defined service level agreement. A Cloud-based deployment (private, public, or hybrid) is suggested in order to comply this these requirements;
- **allow Public Warning subsystems to be interfaced with the national PWS** and capable of adapting the content to the media they use.

---

38 https://www.etsi.org/technologies-clusters/technologies/tetra  
39 https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern
• support **standard data exchange with other (external) systems** through secured API and open
the message broker to PWS of neighbouring countries and supranational entities (e.g. EU) In this
way, the alerting in cross-border emergencies will become manageable;

5.3 Use of technical standards

As previously described in the document, we **recommend the use of the CAP standard to structure**
the alert content and the ETSI standard for the requirements that the technologies involved in a
PWS should satisfy. However, both these two standards show some gaps and are not always up-to-
date with respect to the new emerging technologies.

The CAP protocol for example, due to its flexibility and customizability features, considers many
important fields as optional, but for an effective warning message generation some of them should
be always included in a communication. Below we report a short list of consideration regarding the
CAP fields that are not mandatory for the protocol but that in our opinion must be always present:

• The `<polygon>` field, which is a list of (WGS 84) coordinates pairs, is considered as optional, but
it has a crucial importance for the generation of effective warning messages. For generating the
best communication as possible, is in fact necessary to geolocate the interested groups of people
according to the severity of the disaster effects in their surroundings. In order to warn people
on the move, who may reach the estimated affected area within the alert temporal span, it is
strongly suggested to extend the alert area and create a bigger communication area, e.g., taking
the bounding box that inscribes the alert polygon and extend it according to the average travel
speed and the temporal validity of the alert. Alternatively, and/or in parallel, the same alert can
be repeated over time with a periodicity that should be computed according to the alert severity
and certainty. The **alert should be automatically disseminated to all subsystems/agencies with**
**coverage/responsibility on areas having a non-null interception with the computed**
**communication area**;

• In a multicultural society, the `<language>` field, that indicates the language of the warning
message, is very important. A CAP message can include, in fact, more `<info>` segments with the
same information (`<severity>`, `<urgency>`, `<certainty>`, `<category>`, etc.) but with the textual or
media fields (`<instruction>`, `<event>` description, `<derefUri>` for the media attachment) in
different languages, in this way the communication endpoint such as television, radio or even
sirens, can reach the larger audience as possible, including even ethnic minorities. It is important
also that the values of the `<language>` field belong to a defined standard one of which can be,
for example, the RFC3066\(^{40}\) of the Internet Engineering Task Force\(^{41}\);

• The `<uri>` and `<derefUri>` fields indicate respectively the full absolute URI of a resource (typically
an URL over the internet) and the base-64 encoded data content of the resource (in this case
the media content is directly attached to the CAP message). For the CAP protocol both are
optional, but at least one of them should be always included in the message. If the `<uri>` is
included, then the message have a lower size, but the endpoint needs to be connected over the
internet to download and show the media content, on the other hand if the `<derefUri>` is
specified, no internet connection is requested to the endpoint for downloading the resource,
but the message size can increase a bit;

\(^{40}\)https://tools.ietf.org/html/rfc3066
\(^{41}\)https://www.ietf.org/
• The `<audience>` field, which is optional in the CAP standard, is not crucial for the message effectiveness but can be helpful to distinguish the recipients’ target. It can be used for instance as discriminator by the subsystems of the aforementioned PUWSub for disseminating messages to specific target of people (either professionals or citizens, people with special needs, etc.);

• The `<effective>` and `<expires>` fields indicate respectively the effective time of the information of the alert message and the expiry time of the information of the alert message. Either of them is not mandatory but it is very important to include this information in all the CAP messages. In addition, also the `<onset>` field, which indicates the expected time of the beginning of the event of the alert message, can be important to provide additional information about the context of the alert communication. All these date and time field values should be used in a standard way, such as `2018-09-30T10:49:00-01:00` for 30 September 2018 at 10:49 CET. Finally, we notice the absence of a field indicating the end of the hazardous event, and we think this can represent an important lack of the CAP protocol;

• The `<parameter>` field can be very useful for adding information that cannot be mapped by the other CAP fields, for example for information that has been set out within the organization. However, it is important to avoid the abuse of such a field and try to map as much information as possible with the corresponding CAP fields.

Moving now the attention to the ETSI standard presented in Chapter 3, we notice that it doesn’t include any reference to the technologies that nowadays are commonly used by all the people in their daily life, such as mobile applications, social networks (e.g. Facebook, Twitter, Instagram, etc.) and chatbots (e.g. as services built upon WhatsApp). For this reason, following the ETSI requirements listed in Table 2, Table 3 and Table 4, we have tried to map and check how the aforementioned three technologies fulfil the requirements. The result is shown in Table 9, and reports that many of the necessary requirements for an effective PWS are met by the mobile applications, the social network and the chatbot, but with limitations principally depending on the users must be aware of the existence of the specific systems and maybe after following registration procedures.

<table>
<thead>
<tr>
<th>Emergency notification systems shall</th>
<th>Mobile Applications</th>
<th>Social Media</th>
<th>Chatbot</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>be able to reach citizens in their own dwelling</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>Emergency notification systems shall</td>
<td>Mobile Applications</td>
<td>Social Media</td>
<td>Chatbot</td>
<td>Legend</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>be able to reach citizens at their place of work</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = in certain place of work the access to some applications or social media can be blocked</td>
</tr>
<tr>
<td>be able to reach citizens in public venues</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens on foot</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be able to reach citizens in a vehicle</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = not compatible with driving safety</td>
</tr>
<tr>
<td>be able to reach a citizen visiting another European country</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>provide sufficient instructions regarding actions to be taken</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>provide identification of the message/notification originator</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = compliant, but no certainty</td>
</tr>
<tr>
<td>deliver messages within a planned specified time</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = compliant, but no certainty</td>
</tr>
<tr>
<td>allow simultaneous delivery to targeted, large audiences or geographies</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>offer sufficient details of the emergency situation</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = compliant, but no certainty</td>
</tr>
<tr>
<td>be able to retry delivery when the initial message delivery fails</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = message can be repeated</td>
</tr>
<tr>
<td>support delivery of notification messages to those with special needs and unique devices, like terminals of hearing and speech impaired persons</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = compliant but coverage for all the specific needs is not guaranteed (e.g. people with blindness problems)</td>
</tr>
<tr>
<td>have the ability to deliver messages in multiple languages</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V = compliant</td>
</tr>
<tr>
<td>be capable of addressing congestion management across the various networks used</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 = compliant, but no certainty</td>
</tr>
</tbody>
</table>

Moreover, we notice the absence of a recognized standard that provides guidelines on how to present the warning message to the user, especially with the social media and mobile application technologies. This is often translated in a lack of useful information and in an ineffective communication, which frequently includes non-meaningful details for a common citizen. For this reason, next we address this problem and to provide a set of guidelines aiming to the creation of more effective warning messages and contents.
A final consideration regards the fact that there is not any EU policy that establish a list of certified standard to follow for the implementation of PWS. Furthermore, these standard documents are not regularly updated and so they often do not reflect the arising needs of the society and the opportunities provided by the most recent and emerging technologies.

5.4 Guidelines on styling for media adaptation

The plethora of channels and media available has to be managed in order to provide reliable, clear and effective messages considering that also human factors and the context of the situation highly influence the communication flow, both in emission and in reception. In addition, each channel shows specific features that require to be correctly addressed, because the same message cannot effectively work on any channel.

Every media has its own strength and weaknesses and no existing media can guarantee the timely delivery of alerts in all situations reaching the 100% of the population. For example, the cell broadcasting technology, which is one of the most modern and effective alerting technologies, can reach with an SMS all people with an active mobile phone, despite the carrier provider. However, at night almost all phones are in “not disturb” mode, and the reception of an SMS could not be effective. Therefore, usually a mix of multiple medias with different characteristics is used in order to maximize the alert reach. Table 10 recaps the main channel used in the context of Public Warning, describing their key strength (pros) and weaknesses (cons) with respect to key technical characteristics.

<table>
<thead>
<tr>
<th>Technology</th>
<th>DRM Phase</th>
<th>Pro</th>
<th>Cons</th>
<th>Notes on CAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sirens</td>
<td>• Early warning • Emergency Response</td>
<td>+ Volume regulation + Multi-tone + Customizable sounds (and voice messages) + Remotely controlled</td>
<td>- Do not provide instructions - Indoor coverage may be limited</td>
<td>Only few CAP fields can be used, mainly the category</td>
</tr>
<tr>
<td>Public displays</td>
<td>• Early warning • Emergency Response</td>
<td>+ Site specific + Remotely controlled</td>
<td>- Text only - Brevity</td>
<td>Only selected textual content can be visualized</td>
</tr>
<tr>
<td>Broadcast comm. (Radio, TV)</td>
<td>• Prevention • Early warning • Emergency Response</td>
<td>+ Wide audience + Plain language + Images allowed</td>
<td>- Text only - Brevity</td>
<td>Full content possible</td>
</tr>
<tr>
<td>Cellular com. (SMS)</td>
<td>• Early warning • Emergency Response</td>
<td>+ Geolocated distribution + Wide audience</td>
<td>- Text only - Brevity</td>
<td>Only selected textual content can be visualized</td>
</tr>
<tr>
<td>Mobile App</td>
<td>• All</td>
<td>+ Geolocated distribution + Data collection (Crowdsourcing) + Target specific + Bidirectional</td>
<td>- Internet connection dependent - Digital divide prone - Need to be downloaded by the user</td>
<td>Full content possible</td>
</tr>
<tr>
<td>Website</td>
<td>• All</td>
<td>+ Accessibility + Rich text and media allowed + Multi-hazards + Multilevel information</td>
<td>- Internet connection dependent - Digital divide prone</td>
<td>Full content possible</td>
</tr>
<tr>
<td>Technology</td>
<td>DRM Phase</td>
<td>Pro</td>
<td>Cons</td>
<td>Notes on CAP</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Social media</td>
<td>• All</td>
<td>+ Wide audience</td>
<td>- Internet connection dependent</td>
<td>Only selected textual content can be visualized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Rich text and media allowed</td>
<td>- Digital divide prone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Bidirectional</td>
<td>- Heavy coordination and control required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Need the registration to the page/channel</td>
<td></td>
</tr>
<tr>
<td>Chatbot</td>
<td>• All</td>
<td>+ Natural interface, natural language</td>
<td>- Internet connection dependent</td>
<td>Full content possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ In-app already in use</td>
<td>- Digital divide prone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Multimedia content allowed</td>
<td>- Need the registration to the channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Data collection (Crowdsourcing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Target specific</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Bidirectional</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

While using multiple media, we recommend to:

- **include the use of social media** in parallel with traditional media such as TV and radio, creating specific pages where to disseminate the alerts. Given the multitude of agencies and territorial segregations, we suggest that **every single agency** (e.g. water, environmental monitoring, responder) **should have its own social media page**, which should be known by the centralized PWS together with the page scope both in terms of hazard and territorial coverage. The alerts should be inserted by the agencies, also the local ones, using the client of the centralized PWS system according to the selected standard, so as to the brokered and automatically delivered in a coherent way to all media, agencies and social media pages after a proper adaptation.

- **Adapt the alert content to the media used.** Starting from a complete common standard that contains all the required information, develop automatic adapters in order to compose ad-hoc messages and styles according to the media on which the alert is propagated. For example, SMS cannot deliver multimedia content, only text is allowed, and long messages may be difficult to be read if split into multiple SMSs. Some social media (e.g. Twitter) have limitation on the content (e.g. 240 character, only one image/video per post)

- Build **templates for styles in a coherent way** across the different medias. Alerts should be always easily readable and understandable.

- Develop **multi-agency alerting plan and templates** for every possible hazard according to the severity level, so that when an emergency strikes the plan can be quickly applied. A single alert database containing pre-defined alert should be established, and shared among all entities involved in the emergency management both across different administrative areas and agencies.

- Alerts are effective only if understood. Plan **prevention campaign** to inform people about the risks they are exposed to, the situations that they may face, and explain the standard alert codes/colours and, in case of special media such as sirens, which are the tones used for the different hazard and define a clear behaviour, e.g. if you hear the siren, immediately go home

63
and turn on your TV or radio to get the instructions. Use easy to understand brochures or leaflets.\(^{42}\)

Next, we provide some reference example of alerts issued on selected channels, namely sirens, SMS, web, social media.

**SIRENS:** as outdoor warning system, the sirens are in use in most of the European countries. Mainly used in military context, they are also used to alert the population on very high-level hazards, such as critical storms. The message that sirens convey needs to be known a-priori to be correctly be decoded. The sequence of activation or the sounds – if many tones are supported - may have different meanings. In general, sirens are associated to a severe incoming threat and they suggest to immediately search for a shelter, or to go home and turn on the broadcasting technologies (TV, radio) to get more information. Indeed, the use of sirens needs to be complemented by clear instructions, that allow people to recognize them and to reply correctly to the warning.

Therefore, a dedicated section on Local Authorities websites or apps would be helpful to:

- Inform people about the existing siren systems and their location;
- Explain their use and the meaning of each tone;
- Provide instructions about what to do in case of sirens activation, covering different scenarios in which people can be (e.g. driving, at night, with children, for enterprises, ...);
- Allow to hear the alerting sounds with a sound preview;
- Provide contacts of the authority.

A friendly approach to present the aforementioned information is through the use of FAQ. A good example is given in the Figure 31.

![Frequently Asked Questions about Outdoor Warning Sirens](Figure 31 – FAQ on the sirens)

(Source: the US National Weather Service: https://www.weather.gov/dvn/sirenFAQ)

**SMS/CALL BROADCASTING:** the ETSI 102 900:2012 provides exhaustive guidelines to help PWS to pre-set a portfolio of messages to handle different levels of alert and types of communication. The NL Alert system is a useful example on how to effectively arrange an SMS communication (see Figure 17), while keeping the compliance with the CAP standards. Note that this example does not show any temporal information. This is a shortcoming because the temporal validity of the alert is a key information.

\(^{42}\) A good example of prevention content is available at http://iononrischio.protezionecivile.it/en/homepage/
In general, it is recommended to keep the message short, including the basic information highlighted in Section 2.1 and using only selected the CAP fields to compose the message. The incoming hazards, the interested area, the sender, the response type, the severity, the certainty, the urgency, are fundamental. It is also crucial to provide instruction to people, since the usage of the severity level could be not enough to provide the correct information and it does not explicitly suggest the safest actions to be taken. Finally, the URL (or URI) where to get the full message should be provided. Note that this approach can be effectively used also on social media.

WEB PLATFORM: nowadays a number of online platforms allow receiving map-based alerts on several hazards on a worldwide scale. They automatically aggregate data from multiple sources and present the warning communication to the general public. Among others, a good example of such a system is the Google Public Alert43. When showing an alert, a good visualization should focus on the key information, such as the affected area of the hazardous event and all the mandatory CAP data in a well-formatted way. Figure 33 shows how a message produced in compliance with the CAP standard by the UK Flood Environmental Agency can be presented in a web application to people and authorities alike. The communication should be reported on the map through its geographic coordinates and the click action on this localized warning on the map could trigger the opening of a pop-up (right side of the figure) with the detailed information regarding the alert.

43 https://google.org/publicalerts; https://www.google.org/publicalerts/alert?aid=7a0cdadf5a0adcbc&hl=en
Figure 33 – CAP warning message showed on a web platform. This example refers to a flood alert issued by the UK Environmental Agency and integrated in the I-REACT system (Source: I-REACT project)

SOCIAL MEDIA: social media adoption is very large and it is still growing. Such technology is widening the range of possible interactions among players and enabling powerful and effective Public Warning practices. During a crisis, people immediately start using mobile networks to communicate both among them and with Authorities, in a wide range of situations and information, as shown in Figure 34.

Social media play a prominent role in an undefined number of life and professional sectors. In terms of communication, they are a relevant channel that cannot be neglect, even in the DRM. Social media represent a digital environment where user generated contents and official sources of information co-exist. Authorities, volunteers, citizens can find there a space to cooperate and interact to promote prevention and safe behaviours, monitor expected or ongoing events and stay in contact during the response. Moreover, they are an excellent channel to offer a dynamic online presence on behalf of emergency organizations and Authorities at any level. According to EENA “warning systems shall consider social media in their concepts as additional means to reach-out to specific citizen groups”\textsuperscript{44}, due to the possibility to set-up a dynamic dialogue with connected people.

Over the institutional accounts, which can work as authoritative sources from where send out alerts on any kind of hazards, additional dedicated services/accounts can be very effective in creating communities, inform and train people on prevention and preparedness in more “quiet times”. A good example come from the I-REACT Project45, where a social media page has been created to actively manage a growing community on natural hazards events and disaster risk reduction46.

An effective social media use requires to transfer and adapt to the digital environment the best practices of the communication and coordination that already exist. It is important to know that the exploitation of social medias requires that organizations and institutions adopt suitable communication styles. Today, a social media strategy integrated with the PWS is essential, not only to communicate with the public, but also with other media and press, authorities and other organizations. Each social network has a specific environment and dynamics. Therefore, each of them requires specific adaptations, in consideration of technical constraints and different public they reach. Due to their interactive nature, a response protocol is highly recommended, but it is important to highlight that the social media communication requires to be managed by dedicated professionals. The risk of an automated approach is to fail in creating an engaging and relevant communication channel. The lack of effectiveness can affect the single messages as well as the profile as a whole. In Figure 35, two approaches of crisis communication on Twitter are compared.

---

45 www.i-react.eu (accessed on June 2018).
46 Against Disasters on Twitter: @AgainstDisaster (accessed on June 2018).
The left example provides more articulated and empathic messages, including videos, links to external sources and hashtag (#), while the right example shows a text-only approach, which appears less rich and captivating.

Figure 35 – Social media communication approaches in comparison

Considering the role that digital technology plays in crisis communication, even though the number of people connected is growing every day, few or small segments of population that have no access to digital channels still exist, as well as people that are not familiar with digital contents and interaction. It has been shown that ICT effectively reduces fatalities only in the presence of higher levels of educational attainment and digital literacy. The best practice and the state of the art of PWS focuses on the combination of different channels working in parallel, possibly managed by a centralized system allowing to harmonize the messages on the base of the audience and the media. This allows to tune communication according the phase of the risk or hazards and reach different audiences in different locations and situations.

68
We recommend to dedicate skilled personnel to the communications strategies and the design and management of warning messages and supportive communications products for several channels. This will allow to establish and take care of the bilateral communication with citizenship according to a people-centric approach.

6. Future outlooks

As already highlighted, best practices in Public Warning have to focus to a people-centric approach with a well-designed and updated communication scheme, passing through a continuous updating of the community mapping and a dedicated organisational infrastructure who is in charge of an effective message dissemination. The people-centric approach is just as ambitious as crucial for the PWS improvements and, in this sense, the new information and communication technologies (ICT) can make a very important contribution.

A growing collaborative paradigm that is becoming closer to be integrated in the DRM, is the **crowdsourcing**. The willingness to provide real-time and geo-localized information from the field, spread out and disseminate warnings and advices, as well as requests of help and assistance is massive (Schulze, 2015). This phenomenon is the base of the crowdsourcing, consisting in the collection and sharing of geospatial information from people with reference to a common context via internet-enabled mobile devices (Goodchild, 2007). This type of cooperative process is very powerful to establish a bi-directional channel of communication with the public. The fact that people tend to produce and share information, allows both to collect data that can support the situational awareness of the authorities and responders and to better disseminate official information and alerts. Thanks to the mobile technology, citizens can become digital volunteers, self-engaged and contributing to a participatory form of surveillance (Albrechtslund, 2008) based on the cooperative collection of peer-generated data. Data collected from the field represent a tangible resource able to meaningfully affect the emergency management. The dynamic data can support more detailed action plans at a control room level and can improve the situation awareness of the in-field agents, promoting an optimal resources allocation (Whittaker et al., 2015). Moreover, crowdsourcing can contribute to raise the individuals’ cognitive alertness, stimulating them to learn and improve their proactive attitude towards the collective safety (population, environment, common goods) (Tallacchini, 2014).

One of the most known crowdsourcing platforms is Ushahidi¹. Originally created for monitoring the Kenya election, afterwards it has been used for gathering reports by voluntary groups during natural disasters. Initially it was based on SMS by which citizens reported any kind of information or resource on the territory, enabling also the possibility to provide feedback on requests and instructions. Raised to the global attention during the Haiti Earthquake in 2010, Ushahidi effectively shows how such platforms of crisis mapping work for DRM organization and for the public at the same time. The collaborative mapping is one of the possible information channels in Public Warning that effectively works for both active citizens and receivers. From there on, the services to map and alert on every kind of hazardous event and accessible with the mobile technology have multiplied. Among the interesting examples, we have Crisis Mappers Net¹ that is founded on mobile platforms, computational linguistics, geospatial technologies and visual analytics to power rapid crisis response and Mobile4D¹, which is a crowdsourced disaster reporting and alerting service that in I See Change¹ are published as a Community Climate & Weather Journal.

Crowdsourcing can integrate traditional monitoring systems such as video-cameras, sensors, satellites and other sources, augmenting the informative potential (Manovich, 2006) and the public
**reporting** is one of the more recent examples of the crowdsourcing applied in DRM. It leverages on the massive availability of mobile Internet and on the human attitude to share information. The combination of available contextual factors enables the possibility to enhance the data collection and monitoring of natural events, as a valuable source of information for scientists and authorities. The major benefits are the enhanced territory monitoring and a raising population awareness towards hazards, risks and safer behaviours. The challenge is the integration of public data, so as to make them valuable, relevant and interoperable within the DRM ecosystem.

Nevertheless, to integrate them in the current processes, some constraints have to be considered:

- **The quantity of the information collected** is crucial, since the crowdsourcing needs a huge amount of data to be reliable. Moreover, these resulting data need to be pre-processed for being presented in a control room and also filtered to avoid the production of an information overflow that might negatively affect decisions and operations (Meier, 2013). From the operators’ perspective, new sources and data types widen the range of action: the physical space monitored by traditional surveillance tools becomes a **data-space** thanks to the digital asset provided by locative media and user-generated contents. Innovation technology and new channels of communication provide authorities additional resources, but they also change the work, introducing complexity. Automatic data filtering procedures based on machine learning techniques support the human agents to cope with the quantity, velocity and variety of data being collected, and help decision maker to focus on actionable data while excluding uninformative or misleading contents. The validation of data is mandatory and the possible management approach range from automatic systems to the human verification. Again, the crowdsourcing platforms can help, supporting the peer-validation and by integrating techniques such as social tagging and reputation systems (Pennacchiotti et al. 2013).

- Over the quantity, the crowdsourcing for the DRM needs for high **quality** information. **Accuracy and reliability of data** are crucial to avoid to introduce biases into the action planning and execution (Park, 2015). “Crowdsourcers” can suffer from disinformation, false judgments and social biases (Guo, et al., 2014). Moreover, their expertise can influence the accuracy of the collected data and their further use (De Longueville et al., 2010). In addition, the self-generated communication exchanged via social media is extremely fast, informal, and subjective. The way in which the messages are collected and composed may affect the processes of the information, both made by human and by automated agents (Yin et al. 2012).

In every phase of a crises, a huge amount of data is generated and exchanged, messages are almost always complemented even not based on pictures and videos. The capability to manage and use all the digital channels allow to better disseminate alerts and warning, increasing the number of people that can get the message and activate protective measures for them, their relatives, their neighbours. The impact for Civil Protections and responders can results in a better action, as a study on 120 countries on a time-rage from 1980 to 2013 shows: the availability of **connected devices** does [offer new ways to share disaster warning information](http://www.wesenseit.com/), to communicate in the aftermath of disasters and to reduce disaster-induced losses (Toya and Skidmore, 2015).

Projects proposing the public reporting in DRM have been developed or are still in development at EU Level. An example is [WeSenseIT](http://www.wesenseit.com/), presented under the FP7 EU research program, which aims “Developing citizen observatories of water and flooding to facilitate citizen engagement in planning, decision making and governance”.

---

47 http://www.wesenseit.com/
48 https://ec.europa.eu/research/fp7/index_en.cfm
People can report with the offered mobile application picture information about the water behavior in their communities and the information can be viewed also on a free access internet website, in this way the people can be informed and be aware on what is happening in a specific venue. These crowd data are also included on a software called HydroNet, a professional control room which allows the decision makers to combine the data submitted by the people through the mobile app with other data sources (e.g. forecasting and nowcasting models, measurements, etc.).

Of course, this kind of approach can be adopted for all the types of hazard, and an example is I-REACT\(^49\) (Improving Resilience to Emergencies through Advanced Cyber Technologies), a project built within the H2020-EU.3.7. program on Secure Societies – Protecting freedom and security of Europe and its citizens. The framework, among the many other features, gives to the people the possibility to reports with pictures and associated measures the actual situation (either dangerous or not).

\(^{49}\) http://www.i-react.eu/
In I-REACT, emergency management professionals in the control room, through their desktop application, can either validate or reject the report in order to avoid the proliferation of fake information and to give a feedback to the people.

For enhancing the mechanisms of engagement and education, all the new systems can include the concept of **gamification** (i.e. *the application of game thinking in non-game contexts, with the aim to motivate desired behaviours* (Detering 2012)), thinking also on mechanisms of tips (i.e. hints) as introduced in paragraph 4.2 with the NINA application of the German BBK, or giving for example bonus and penalties on how the person acts (e.g. whether the provided report has been validated or not by professionals in the case of I-React).

For reaching the objectives of education and resilience improvement, the gamification can be applied also to purely informative mobile application, with the goal of increasing the people awareness and disseminating the best practices on the issue of emergencies. For example, in the 3rd Annual Seminar of the DRMKC in Sofia on April 2018, the municipality of Cascais, among its initiatives for citizens engagement, presented the possibility to use tools (i.e. mobile application) including the concept of gamification, as shown in Figure 39.

---

50 [https://www.bbk.bund.de/DE/NINA/Warn-App_NINA_node.html](https://www.bbk.bund.de/DE/NINA/Warn-App_NINA_node.html)
51 [https://drmkc.jrc.ec.europa.eu/Portals/0/Partnerships/Seminars/3_Scientific_Seminar_DRMKC/Presentations/session_3a/pdf/S_joao_dinis-engaging_citizens_potential_for_climate_change_and_city_innovation.pdf](https://drmkc.jrc.ec.europa.eu/Portals/0/Partnerships/Seminars/3_Scientific_Seminar_DRMKC/Presentations/session_3a/pdf/S_joao_dinis-engaging_citizens_potential_for_climate_change_and_city_innovation.pdf)
The capillary spread of mobile applications, can help also in finding new ways of alerts and warnings dissemination methods, either for the prevention of or for the preparedness to a hazardous event.

The ICT can give a boost to PWS systems by also helping professionals and ordinary citizens to distinguish the noisy and ineffective information from the relevant one in a specific situation. In this sense, the emerging Artificial Intelligence (AI) techniques can be applied in several context. An example is the application of an AI technique called Natural Language Processing (NLP) to the messages produced by people on social media platforms. Generally, the NLP refers to the computer processing of natural language (i.e. the common language that we use everyday) for whatever reason and, for the PWS purposes, the context can be circumscribed on the messages produced on Twitter\textsuperscript{52}, the well-known social media engine, due to its increasing function of communication channel for hazardous events (e.g. natural, terrorist, etc.).

\textsuperscript{52} https://twitter.com/
For example, Figure 40 shows a real example of NLP application on Twitter. The original tweet (left side) is informing about a warning for a fire in Pisa (Italy) with 700 people forced to leave their homes. The NLP techniques applied to the message generates the labelled information of the right side of the figure. The labels “Fire”, “Affected people”, etc., are automatically computed and give to a human a first snapshot of the information contained in the tweet even without reading the message text. By including this mechanism in a more comprehensive software, the NLP could compute and label hundreds of tweets belonging to a specified time frame and region, and show on the screen of a professional in the control room all the labelled tweets, that can be eventually filtered by location, date, hazard type, or other fields. This would allow the professional to improve the monitoring performance and eventually to trigger warning communications.

The monitoring activity can be enhanced also by exploiting others AI techniques applied to the image processing. An example can regard the detection of area affected by disasters like the one shown in Figure 41. The image is provided by a satellite put in operation within the Copernicus Sentinel-2 mission\(^{53}\) and represents a burned area in Chieti (Italy) after a fire event.

\[\text{Figure 41 - Burned area in Chieti, Italy} \]
\[(\text{Source: Copernicus Sentinel-2})\]

In this case, the AI can help in automatically detecting and shaping the burned area, otherwise the operation should be carried out manually and for each image. Figure 42 presents side by side both the manual and the automatic detection of the area. The shape on the left side has been produced starting from the data provided by EFFIS\(^{54}\), while the right-side image has been computed by using AI techniques for image processing.

\(^{53}\) https://sentinel.esa.int/web/sentinel/missions/sentinel-2
\(^{54}\) http://effis.jrc.ec.europa.eu/
Generally, the manual annotation (i.e. shaping) is expensive, for this reason this kind of detection can be put in a workflow (Figure 43) that exploits the data produced by EFFIS and the images produced by the Sentinel-2 satellite, in order to generate updated maps, with a negligible loss of detail with respect to the gained time in avoiding the manual annotation. However, it is important to notice that all the techniques related to AI are very helping but still need the human supervision.
References


ETSI TS 102 182 v1.4.1 (2010), European Telecommunications Standards Institute. Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies. https://www.etsi.org/deliver/etsi_ts/102100_102199/102182/01.04.01_60/ts_102182v010401p.pdf (accessed in May 2018).


Annex I – Guidelines on technical specification for Public Warning Systems

This Annex presents advices about the content of a technical specification for a centralized PWS architecture delivery. The specification must contain all the functional requirements and the hardware and software components for satisfying them. Moreover, it must contain the necessary documentation (e.g. manuals, certifications, warranty, etc.) and references to the support and delivery policies.

### GENERAL REQUIREMENTS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional requirements</td>
<td>Depending on the alerting system, specific functional requirements must be defined. Examples of functional requirements valid for every PWS can be:</td>
</tr>
<tr>
<td></td>
<td>• Receiving alerts from monitoring systems in a standard format such as CAP</td>
</tr>
<tr>
<td></td>
<td>• Dispatch alerts in a standard format to any subscriber</td>
</tr>
<tr>
<td></td>
<td>• Allow the subscription</td>
</tr>
<tr>
<td></td>
<td>• Allow the user management (authentication, authorization)</td>
</tr>
<tr>
<td></td>
<td>• Ensure secure communication (e.g. encrypted messages)</td>
</tr>
<tr>
<td></td>
<td>The functional requirements must be also technology-specific. For sirens we can have for example:</td>
</tr>
<tr>
<td></td>
<td>• Multi-tone to map different hazards</td>
</tr>
<tr>
<td></td>
<td>• Voice support for custom messages</td>
</tr>
<tr>
<td></td>
<td>• Sirens connected to a centralized system with at least two secure wireless channels</td>
</tr>
</tbody>
</table>

### SOFTWARE

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backend System</td>
<td>It includes all the software specification for the storage, the delivery and the logic of the system. Examples of requirements are:</td>
</tr>
<tr>
<td></td>
<td>• Presence of REST API for receive and deliver the warning communications;</td>
</tr>
<tr>
<td></td>
<td>• User authentication and Authorization management;</td>
</tr>
<tr>
<td></td>
<td>• Type of database infrastructure to store the data and the sent communications;</td>
</tr>
<tr>
<td></td>
<td>• Usage of cloud-based hosting or in-house hosting for the software resources;</td>
</tr>
<tr>
<td></td>
<td>• Adopted programming languages.</td>
</tr>
<tr>
<td>Frontend System</td>
<td>It includes all the software specification for the user interfaces of the system. Examples of requirements are:</td>
</tr>
</tbody>
</table>
- Login and Registration page;
- Possibility to create warnings with delivery options (e.g. area, duration, instructions, etc.);
- Reports for monitoring the status of the endpoint (e.g. monitor of the status of the sirens);
- Statistics on the warning sent;
- Client requirements, such as web application with browser compatibility, mobile application for different operating systems.

Security

It includes all the software specification to guarantee the security of the system and the data transmission, such as the implementation of security protocols for the data exchanging based on cryptographic algorithms. These algorithms can belong to the Symmetric Key family, such as AES, or the Asymmetric Key family of which the most famous algorithms is RSA.

<table>
<thead>
<tr>
<th>HARDWARE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Comment</td>
</tr>
</tbody>
</table>
| Technological requirements | It includes all the hardware requirements of the system, such as:  
- Mounting equipment both indoor and outdoor (e.g. equipment for public poles, for buildings, etc.)  
- Infrastructure features (e.g. channel for communication like TETRA or UHF, uninterrupted power supply to cope with outages, etc.)  
- Additional features (e.g. water-proof, omnidirectional endpoint, multi-tone siren, volume dimensioned according to the covered area etc.) |
| Certification | It is certification that states that the hardware is tested and compatible to cope with the problem for which it was chosen |
| Warranty policy | It often depends on the national policies. The suggested period is at least 5 years. |

<table>
<thead>
<tr>
<th>SERVICE REQUIREMENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Comment</td>
</tr>
<tr>
<td>ICT Components</td>
<td>It includes the requirements regarding the software availability, which must be 7/24, and the response measures (e.g. response time of the system for delivering a warning for a certain type of hazard, etc.)</td>
</tr>
<tr>
<td>Requirements for suppliers</td>
<td>It includes all the requirements that a supplier has to show up (e.g. certifications, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SYSTEM DOCUMENTATION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Comment</td>
</tr>
</tbody>
</table>
Manuals

**SUPPORT POLICY**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training sessions</td>
<td>It includes the plan and schedule of training sessions</td>
</tr>
<tr>
<td>Level of support</td>
<td>It includes the requirements for the support that have to be agreed with the supplier (e.g. 7/24 support, email and phone support, etc.)</td>
</tr>
</tbody>
</table>

**DELIVERY POLICY**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery plan and information</td>
<td>It includes all the information and requirements about the delivery of the system (e.g. time plan, key milestones, etc.) and the payment schedule</td>
</tr>
</tbody>
</table>
Annex II – Script Interview on Future perspectives on PWS

INTRODUCTION
- Researchers introduction
- Context of the study and goals of the interview

GENERAL QUESTIONS
- Profile of the responders
- Organization (type and country)

CURRENT PWS DESCRIPTION
1. Which is the architecture of the Public Warning System in your Country?
   - It is based on several not connected local systems
   - Is based on a mix of local and connected systems
   - It is based on one centralized system connected with different subsystems
   - Other. Please, specify.

2. Is the current PWS able to manage multi-hazards warnings?
   - Yes
   - Not yet but in the next future
   - No

3. Which warning delivery channels does the PWS currently include?
   - Sirens
   - Public displays
   - Broadcast communication (TV, radio)
   - Cellular communication (SMS)
   - Specific mobile application(s)
   - Web
   - Social media
   - Other. Please, specify.

4. If the PWS includes the sirens: Which are the next future plans for sirens?
   - To keep it as it is
   - To update it with new sirens
   - To progressively abandon it and switch to other channels
   Please, provide motivations.

5. Are any of the following external platforms used or planned to be used as source or recipient to get, aggregate, harmonize or deliver Public Warnings? In positive case, explain how.
   - Severe Weather Information Centre (SWIC)
   - Meteoalarm
   - Meteoalert
   - Alert Hub
   - Other. Please specify.

6. Does the PWS implement the Common Alert Protocol – CAP Standard?
7. Does the PWS of your Country comply with any International Standard?
   - No
   - Not yet but in the next future
   - Yes. Could you provide some detail about?
   - Don’t now

8. Does it implement one of the following two International Standards on PWS management?
   - ETSI TS 102 182 Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies
   - Other. Please specify.

9. Which are the most important strengths of the current PWS?

10. And the most relevant weaknesses?

FUTURE PERSPECTIVES

11. Which of the following feature the PWS of your Country need to enhance?
   - Multiple hazard
   - Multi-channel
   - Modular
   - Centralized
   - Distributed
   - Secure from cyber attack
   - Other. Please specify.

12. On which of the following goals are the next future investment on PWS focusing on?
   - Extensive territory coverage capability
   - Better population targeting
   - Wider the coverage of the PWS with the following media (select them the following list)
     - Broadcast
     - Sirens
     - Mobile (SMS, IM, Email, App)
     - Social media (FB, Twitter)
     - Other. Please specify.
   - Integration of the existing platforms (Google alert, Copernicus EMS)
   - Centralized control system
   - Better Warning content (awareness, accessibility, effectiveness, credibility)
   - Improved security (cryptography)
   - Advanced techniques of data analysis for hazards monitoring
   - Other. Please, Specify.
13. Could you please provide some additional information on improvements you are going to handle?

RECAP and THANK YOU.