Software Engineering Institute

Commercial Mobile Alert Service (CMAS) Alerting Pipeline Taxonomy

The WEA Project Team

March 2012

SPECIAL REPORT
CMU/SEI-2012-TR-019

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0000911

Table of Contents

List of Figures

List of Tables

Abstract

This report presents a taxonomy developed for the Commercial Mobile Alert Service (CMAS). The CMAS Alerting Pipeline Taxonomy is a hierarchical classification that encompasses four elements of the alerting pipeline: alert originator, Integrated Public Alert and Warning System aggregator, commercial mobile service provider infrastructure, and recipients. The taxonomy treats the alert-originator element in the most detail, identifying key features of alert-originator organizations and systems. It also identifies a limited number of features for the other three elements. The purpose of the CMAS taxonomy is to help stakeholders understand and reason about required operations. To this end, the report provides a representative scenario to ensure that the taxonomy defines the elements used in CMAS operations. The CMAS Alerting Pipeline Taxonomy will simplify some actions related to an organization's effort to integrate into CMAS. The taxonomy will simplify analysis by decomposing the CMAS Alerting Pipeline into features so that the interactions among pieces will be simpler to understand. And the taxonomy will simplify guidance by representing the domain in a manageable form for explaining a variety of situations.

1 Introduction

The Commercial Mobile Alert Service (CMAS) is one of the major components of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS). CMAS enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via commercial mobile service providers (CMSPs). CMAS is being developed and deployed via a collaborative partnership that includes the cellular industry, the Federal Communications Commission (FCC), and the Department of Homeland Security Science and Technology Directorate (DHS S&T). The Software Engineering Institute (SEI) is supporting the DHS S&T by developing an integration strategy and associated artifacts to support the successful deployment, operations, and sustainment of the CMAS capability, with a special focus on the needs of alert originators [FEMA 2011c].

The CMAS Alerting Pipeline Taxonomy introduced in this document is one of the first products of the SEI effort. The taxonomy is a classification scheme that encompasses the following four elements of the alerting pipeline: the alert originator, IPAWS Aggregator, CMSP infrastructure, and recipients. This first release of the taxonomy is most detailed in its treatment of the alert-originator element, identifying key features of alert-originator organizations and systems. It also identifies a limited number of features for the other three elements.

The goal of the taxonomy is to create a shared understanding of the major elements involved in originating, aggregating and routing, disseminating, and receiving CMAS messages. It also provides a common language for specifying, modeling, analyzing, and discussing key features of those elements. The SEI is using the taxonomy to develop scenarios, analyze cyber threats, develop security guidance, and deliver an integration strategy. In addition, other performers, for example, the RAND Corporation (tasked to develop a penetration strategy) and the Johns Hopkins University Applied Physics Lab (tasked to develop simulations) will be able to use the feature classifications to inform their work. The taxonomy will also be of interest to other members of the CMAS ecosystem—including the organizations that originate emergency alert messages; organizations that broadcast alerts; and organizations that supply, compete with, purchase from, and govern the alert notification community—who wish to understand the important facets of the domain. We describe the ecosystem in more detail later in this document.

1.1 Terminology Used in This Document

A taxonomy is a hierarchical classification that separates a set of elements into groups; elements in the same group share certain significant characteristics, or features. Through these groupings, a taxonomy defines concepts within a domain (such as emergency alerting) and creates a vocabulary consisting of element and feature names. Table 1 lists some terms key to understanding the taxonomy.

Table 1: Key Terms for the Taxonomy

Term	Definition
Taxonomy	Hierarchical classification of elements and features into related groups.
CMAS taxonomy	CMAS Alerting Pipeline Taxonomy, a classification of CMAS elements and features into related groups.

Element	Constituent part of the taxonomy at the top level. For CMAS, elements include the alert originator, IPAWS Aggregator, CMSP infrastructure, and recipient.
Feature	Characteristic of an element (e.g., the software or hardware used to originate alerts) or a lower level characteristic of a feature (e.g., a quality attribute of the software or hardware, such as reliability or security).
Feature tree	Tree structure, used to illustrate the taxonomy, consisting of a "parent" element (or major branch of the tree) and its "child" features (offshoots of the major branch). Features may, in turn, have their own "child" features. CMAS feature trees for each element appear in Section 3.
Ecosystem	System formed by the interaction of a community of organisms with their environment. In our case, the organisms are organizations working together to provide emergency alerts.
Ecosystem model	Abstract representation of the ecosystem formed by combining relationships native to the domain with data gathered from a number of sources, which can aid strategic decision making.

1.2 Approach to Taxonomy Development

To create the taxonomy, we followed the following four-step process, illustrated in Figure 1:

1. We developed a foundation for the taxonomy based on
   - an initial set of scenarios that describe the use of alert notification systems, which we analyzed to derive the key system elements and features.
   - an ecosystem model of the CMAS operational environment in which organizations originate and disseminate alerts. This ecosystem model is included in Appendix D. The ecosystem model illustrates, for example, suppliers of CMAS products and services as well as policies, regulations, and cyber threats that affect development and operations of CMAS capability.
2. We analyzed the top-level *elements* in the scenarios and ecosystem to derive detailed f*eature trees* that populate the CMAS Alerting Pipeline Taxonomy.

   The feature tree for each CMAS element provides a detailed view of the characteristics of that element. These feature details support efficient and effective reasoning about alerting organization characteristics, quality attributes such as interoperability and security, and integration risks and issues. Feature trees support analysis of the characteristics of organizations adopting CMAS, system modeling efforts, and development of a CMAS integration strategy.
3. To evaluate the CMAS taxonomy, we used a mission thread analysis, as illustrated in Section 4. A mission thread is a high-level scenario that runs through all of the steps from the initiation of a task to its completion. For CMAS, the mission thread begins with an event that requires alert generation and ends when targeted mobile devices receive the alert. The evaluation process involves mapping each step in the thread to relevant elements and features of the taxonomy. Ideally, this process develops scenarios sufficient to exercise every element in the taxonomy.
4. To refine the taxonomy, we will incorporate feedback provided as performers review the taxonomy and learn more about CMAS elements and features in the course of their work.

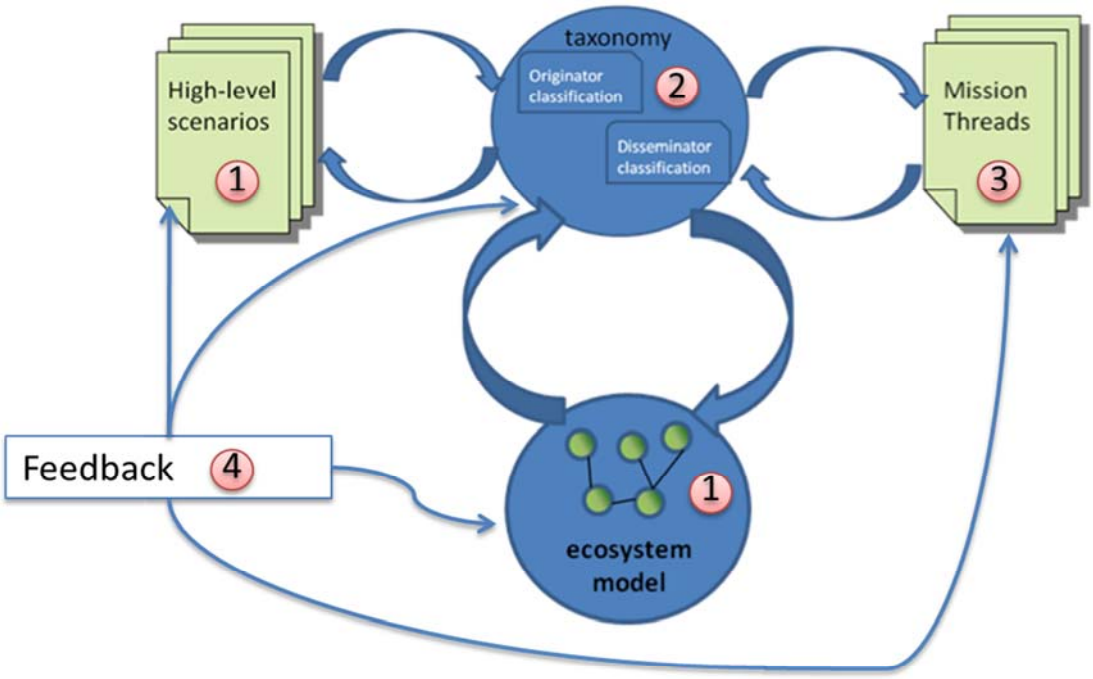

Figure 1: Taxonomy Development and Evaluation

The process of creating the CMAS Alerting Pipeline Taxonomy has identified many of the key features—that is, the attributes and behaviors—of the various actors and functions in the alerting pipeline. These features can be used to specify and analyze capability requirements and quality attribute requirements that are key to acquiring, developing, operating, and sustaining these systems.

1.3 Document Structure

The remainder of this document describes the CMAS Alerting Pipeline Taxonomy. Section 2 presents the scope of the taxonomy in the larger IPAWS context and identifies the top-level taxonomy elements. Section 3 contains the taxonomy itself, including element and feature classifications. For each element, we present a feature tree along with a table that briefly defines each feature. Section 4 describes the use of a mission thread to evaluate the taxonomy. Finally, Section 5 identifies future directions for taxonomy work. The document also contains four appendices, including a glossary (Appendix A), an acronym list (Appendix B), the initial CMAS scenarios (Appendix C), and the CMAS ecosystem model used in taxonomy development (Appendix D).

2 Taxonomy Scope and Context

Taxonomies can represent as much of a domain as the analyst deems appropriate and can contain as much detail as needed for the purpose at hand. This section sets the boundaries for the CMAS Alerting Pipeline Taxonomy in terms of the breadth of CMAS components and environmental factors the taxonomy will cover. We begin by locating CMAS in the context of IPAWS. Then, we identify CMAS Alerting Pipeline elements and link them to components in the *Commercial Mobile Alert System (CMAS) Concept of Operations (CONOPS)* [FEMA 2009].

2.1 CMAS in the IPAWS Context

CMAS is part of FEMA's IPAWS, as shown in Figure 2. IPAWS encompasses other alerting capabilities as well, including the Emergency Alert System (EAS), which is known to many of us. As IPAWS modernizes the nation's alert infrastructure and adds new ways to warn people of imminent threats, CMAS will deliver geographically targeted alerts to the public on all mobile devices. CMAS messages will include presidential alerts, imminent threat alerts, and America's Missing: Broadcast Emergency Response (AMBER) alerts. The CMAS Alerting Pipeline Taxonomy described in this document focuses on CMAS-specific elements of IPAWS, which we will introduce next.

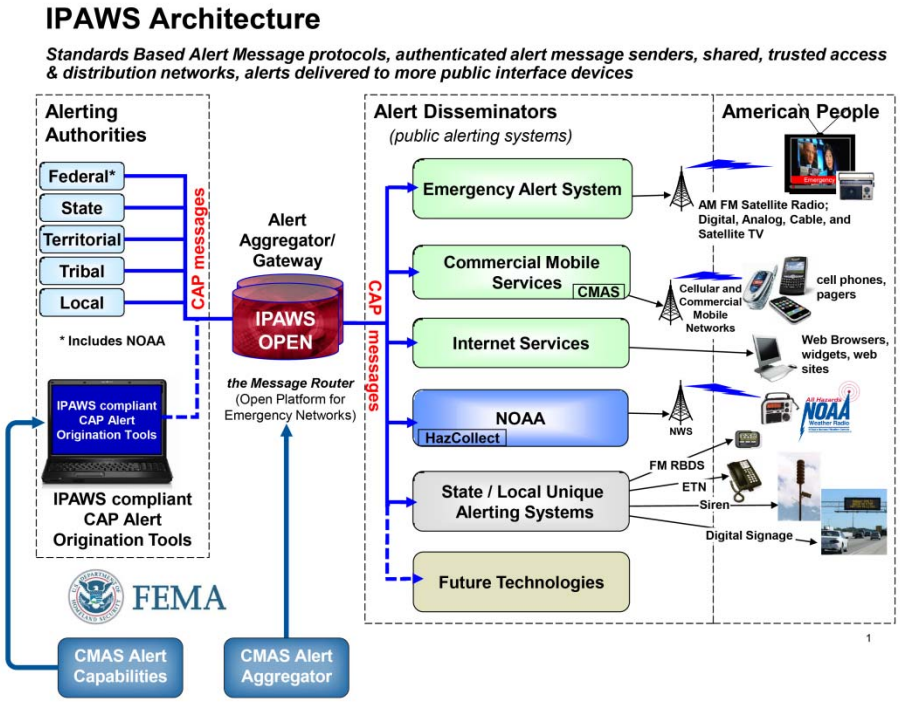

Figure 2: CMAS in the IPAWS Context [Modified from FEMA 2011b]
This figure is adapted to show CMAS components.

2.2 The CMAS Alerting Pipeline

CMAS provides a combination of administrative and operational functions focused on the alerting pipeline, which is designed to generate, send, and receive messages formatted according to the Common Alerting Protocol (CAP) [OASIS 2010]. Figure 3 shows the nominal flow of alerts (CAP-formatted messages) in the CMAS Alerting Pipeline, from authorized originators, to aggregators, to the mobile devices supported by a CMSP [FEMA 2009]. This figure also serves as a functional reference model for CMAS, illustrating six principal groupings of functionality in the pipeline:

1. CAP alert originator
2. CMAS Alert Aggregator
3. Federal Alert Gateway
4. CMSP Gateway
5. CMSP infrastructure
6. mobile devices

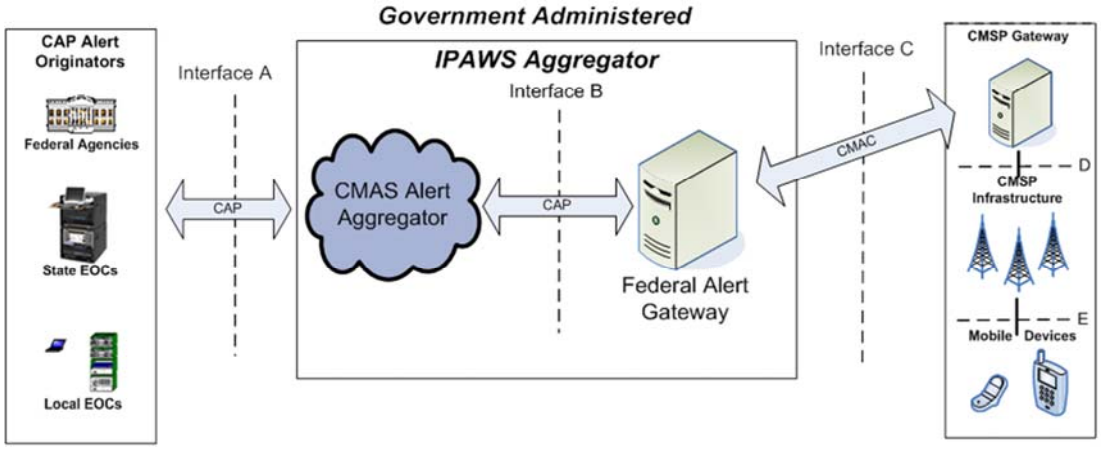

Figure 3: CMAS Functional Reference Model [FEMA 2009]

These six functionality groupings map to four CMAS Alerting Pipeline Taxonomy elements as shown in Table 2 and illustrated in Figure 4. The four elements shown in the pipeline form the basis for the classifications in the taxonomy presented in Section 3.

Table 2: Functionality Groupings and Taxonomy Elements

Functionality Groupings [FEMA 2009]	CMAS Alerting Pipeline Taxonomy Element
CAP alert originator	Alert originator
Alert Aggregator & Federal Alert gateways	IPAWS Aggregator
CMSP Gateway & CMSP infrastructure	CMSP infrastructure
Mobile devices	Recipient

In Figure 4, two-way arrows depict bidirectional information flow between the alert originator and IPAWS Aggregator, and between the IPAWS Aggregator and the CMSP infrastructure. This is because for these pairs of elements, the destination element can return error messages to the source element. However, the arrow between the CMSP infrastructure and the recipient is unidi-

rectional. This is because the CMSP infrastructure broadcasts alerts to recipients, so the recipients cannot return messages to the CMSP infrastructure.

We combined the Alert Aggregator and Federal Alert Gateway into one element, the IPAWS Aggregator, because we are not currently exploring the internal technical details of the Alert Aggregator and Federal Alert Gateway or the interface between them, due to the client direction scope at the systems-of-systems level. Similarly, we are not exploring the technical details of, or interfaces between, the CMSP Gateway and CMSP infrastructure, so we combined those two functional components into one element, the CMSP infrastructure.

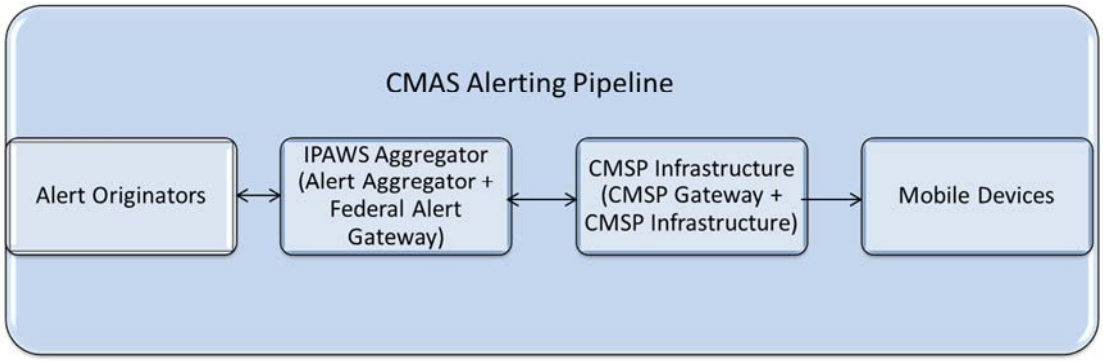

Figure 4: Top-Level Taxonomy Elements in the CMAS Alerting Pipeline

These four elements are the top-level elements in the CMAS Alerting Pipeline Taxonomy. In Section 3, we provide a detailed decomposition of these elements.

3 CMAS Alerting Pipeline Taxonomy

CMAS is a complex system of systems that has many different types of elements, including hardware, software, information, and people. The CMAS system has a *pipeline* architecture. The pipeline of alerts runs from an alert originator, through an infrastructure, to a network of disseminators, and finally arrives at individual recipients. Within the CMAS Alerting Pipeline, we provide a series of elements with views of the complete taxonomy. These elements are shown in Figure 5. Each element has a unifying theme and covers a few specific concepts.

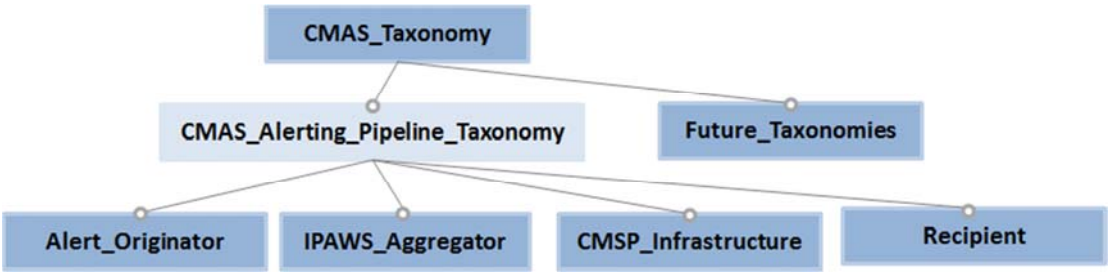

Figure 5: CMAS Alerting Pipeline

3.1 CMAS Alerting Pipeline

The basic CMAS Alerting Pipeline classifies four main elements in the taxonomy. Figure 6 shows a list of element features for origination systems and classifies different types of origination systems. Figure 7 shows a list of features of FEMA's aggregator that will influence how the aggregator is integrated with the originator systems. Figure 8 shows a list of features for the infrastructure through which the originator passes messages to the aggregator. Figure 9 classifies the recipients. Together these support defining combinations of factors to build scenarios that designers and testers can use to understand the interactions between the originator of an alert and the aggregator. We discuss each classification in more detail next.

3.1.1 Alert Originators

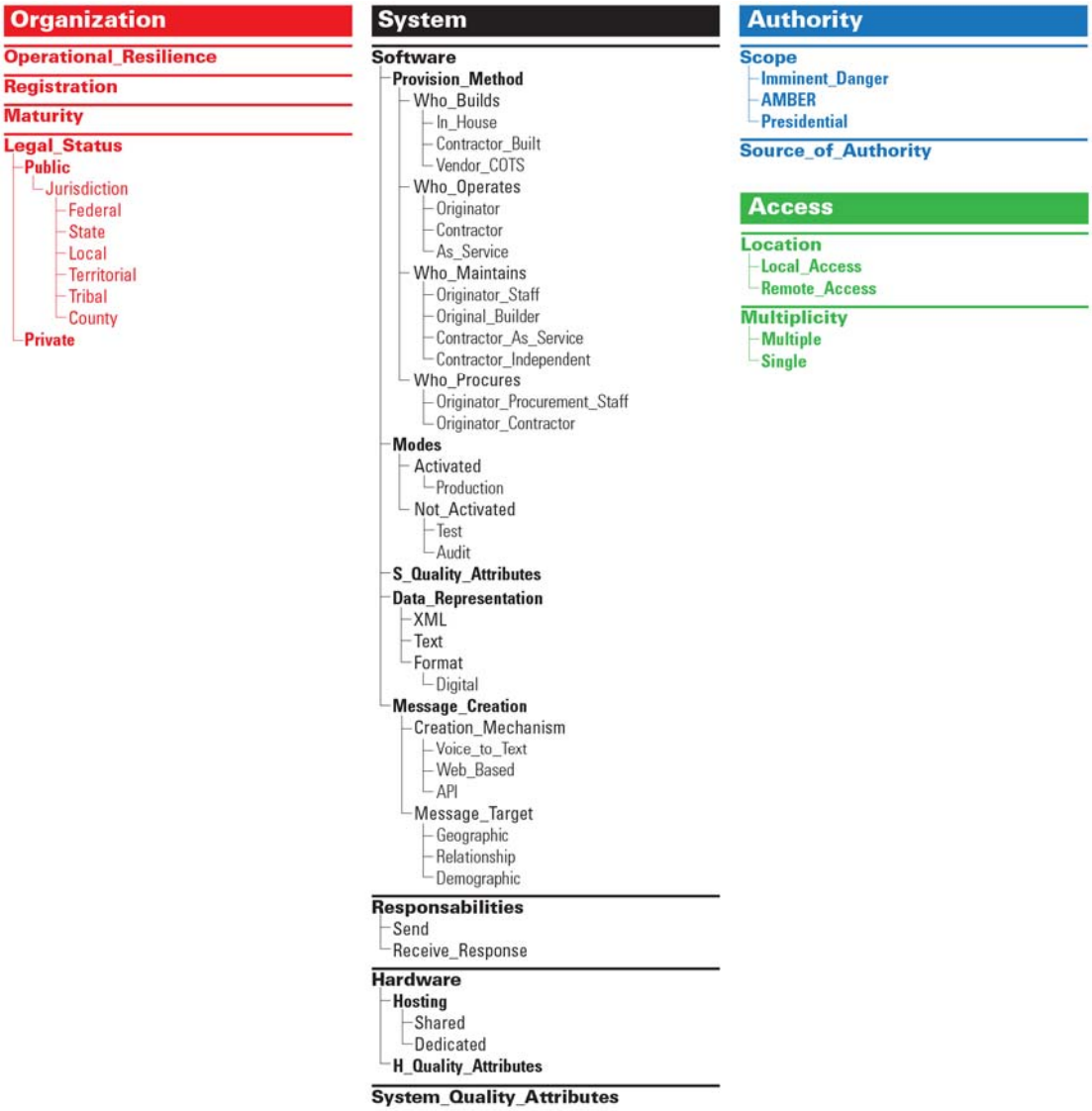

Figure 6: Alert Originator Features

Table 3: Descriptions of Alert Originator Features in Figure 6

Feature	Description	Comments
Organization	The legal entity responsible for actions such as originating alerts	
• Operational_Resilience	An organization's ability to adapt to risk that affects its core operational capacities	[Carelli 2010]
• Registration	Has the organization registered with an authorizing authority?	
• Maturity	The organization's experience and level of performance in similar activities	

• Legal_Status	The legal form that the organization takes	Corporation, partnership, federal agency, state government organization, local government or public safety organization, tribal government, territorial government, other public/ private sector organization
○ Public	A government agency of some level of government	Federal agency, state government organization, local government (e.g., city, county) or public safety organization (e.g., for a public university), tribal government, or territorial government
▪ Jurisdiction	Authority of a legal entity to originate certain types of alerts for certain geographic locations	Part of message validation in the aggregator will be whether the alert originator has the appropriate authority for the alert he or she has originated.
• Federal	The United States of America	
• State	Any of the 50 states	
• Local	Various forms of governmental units within a state	Township, village, city, and many other designations
• Territorial	Areas governed by the U.S. but not granted statehood	
• Tribal	Areas governed by Native American tribes	
• County	Specific subunit of a state	
○ Private	Not a government agency	
System	The software, hardware, data, procedures, and people needed to configure, operate, and sustain the alert origination capability	
• Software	The computer programs, procedures, rules, data, and associated documentation of the CMAS message origination system	[ISO/IEC/IEEE 2010]
○ Provision_Method	Method by which the capability is provided	Provisioning includes procuring, building, operating, and sustaining.
▪ Who_Builds	The original constructor of the software	
• In_House	The software is built by people employed by the organization that will use the software.	
• Contractor_Built	The software is custom built by an organization other than the one that will use it.	
• Vendor_COTS	The software was already built or is being built by a vendor who markets it to a wide range of organizations.	There is a growing ecosystem of companies and products. See the ecosystem model in Appendix D for more.
▪ Who_Operates	The organization that uses the software	

• Originator_Staff	The software is operated by the staff of the organization that originates the alert messages.	
• Original_Builder	The software is operated by the staff of the organization that built the software.	
• Contractor_as_Service	The software is operated by the staff of the organization that offers the software as a service.	
• Contractor_Independent	The software is operated by the staff of an organization that has no relationship to the organization that originates the alert messages.	
▪ Who_Maintains	The organization that keeps the software operational, performs minor modifications and updates, and manages the configuration (e.g., adding users or changing user privileges)	
• Originator	The software is maintained by staff of the organization that originates alerts.	
• Contractor	The software is maintained by staff separate from the organization that originates alerts.	
• As_Service	The software (alert origination capability) is hosted by a vendor or service provider and made available over a network.	
▪ Who_Procures	The entity that makes the business arrangements to receive the software	
• Originator_Procurement_Staff	The system is procured by in-house staff.	
• Originator_Contractor	The system is procured by a contractor on behalf of the originator.	
○ Modes	The state of the software with respect to originating alert messages	
▪ Activated	The system is ready to originate alert messages.	
• Production	The software is in the act of producing an alert message.	
▪ Not_Activated	The system is not ready to originate alert messages.	
• Test	The system is in a state in which an existing set of test actions can be performed.	
• Audit	The system is in a state in which it can be queried and can produce reports.	

▪ S_Quality_Attributes	The quality attributes of the software; nonfunctional attributes essential for the software to be usable for its intended purpose	A candidate list: Survivability Dependability Reliability Availability Security Supportability Maintainability Time to restore Modifiability Testability Performance Timeliness Throughput Latency
▪ Data_Representation	The mechanism used to structure the information	
• XML (eXtensible Markup Language)	A self-describing scheme for structuring data	
• Text	Characters represented by a character code, such as UTF-8 for Unicode	
• Format	The type of representation used for the message	
○ Digital	A binary representation of the data	
▪ Message_Creation	Information about creating messages	
• Creation_Mechanism	The mechanisms that are available for creating messages	
○ Voice_to_Text	A voice recognition application allows the user to speak the alert message and then translates it into proper format.	
○ Web_Based	The ability to issue alert messages through a web page	
○ API	Messages are created by another software program	
• Message_Target	The intended recipients of the message	
○ Geographic	The recipients are all people within a specified geographic area.	
○ Relationship	The recipients are all people with a specific association.	
○ Demographic	The recipients are all people with a specific characteristic.	
• Responsibilities	What the system is expected to do	
○ Send	A message is delivered to the aggregator.	
○ Receive_Response	An error in a message format will result in an error message being returned to the sender.	

• Hardware	Information about hardware	
○ Hosting	Conditions under which the system is managed	
▪ Shared	Software other than the alerting system is running on the same machine.	
▪ Dedicated	Only the alerting system is running on the machine.	
○ H_Quality_Attributes	The quality attributes of the hardware: nonfunctional attributes essential for the hardware to be usable for its intended purpose	A candidate list: Reliability Availability Maintainability
• System_Quality_Attributes	Those qualities that are important to the successful operation of the system as a whole	
Authority	In CMAS, individuals will have certain specified authorizations that define the bounds of their actions (e.g., ability to originate an alert).	
• Scope	Limitations on the alert messages that the organization can originate	
○ Imminent_Threat	An alert issued to warn recipients of any event that has or could occur that would threaten their safety	
○ AMBER	An alert issued to make the recipients aware of an abducted child	
○ Presidential	An alert issued by the president of the United States	
• Source_of_Authority	Entity that has provided the organization the ability to place an alert message in CMAS	
Access	Means by which originator accesses the capability to originate an alert message	
• Location	Location of originator of alert message with respect to the alert-origination system	
○ Local_Access	Whether alert messages can be originated only from a single hardware system that the originator must use in person	
○ Remote_Access	Whether alert messages can be generated when the originator is in a different physical location from the location of the system	
• Multiplicity	Number of systems available to originators in the organization	
○ Multiple	There are multiple systems capable of originating alert messages.	

○ Single	There is a single system instance used for originating alert messages.	

3.1.2 IPAWS Aggregator

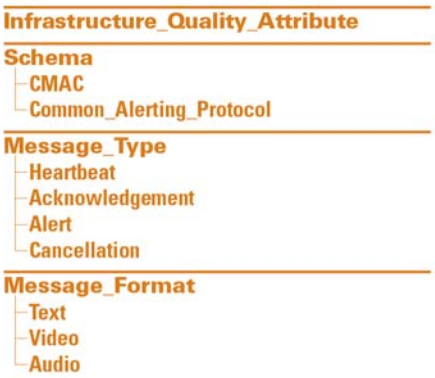

Figure 7: Aggregator Features

Table 4: Descriptions of Aggregator Features in Figure 7

Element	Description	Comments
• Infrastructure_Quality_Attribute	The properties required of the interaction of the hardware, software, and people	A candidate list: Throughput Reliable Available Secure
• Schema	Each alerting protocol has a schema from which valid messages will be created.	Common_Alerting_Protocol is the most important for CMAS, but others are possible, including CMAC, an intermediate protocol used in the infrastructure.
○ CMAC (Commercial Mobile Alert Reference Point C)	The format used for CAP messages as they are disseminated from the aggregator to the operators	
○ Common_Alerting_Protocol	The standard format for alerts at origination	
• Message_Type	Several basic types of messages are needed to fulfill the purpose of the system. Alerts are the content messages for which the system is designed. Acknowledgment messages allow an upstream entity to know that a message has been successfully received. Heartbeat messages simply test that system elements are functioning properly.	
○ Heartbeat	A message is dispatched periodically to determine that all required parts of the system are capable of doing their job.	
○ Acknowledgment	A message sent to inform of the arrival of a previous message	
○ Alert	A message sent to make the receiver aware of important infor-	

	mation	
○ Cancellation	A message sent to make the receiver aware of the cancellation of a previously sent alert	
• Message_Format	The medium and pattern in which the message is shaped	
○ Text	A message represented by human-readable characters	
○ Video	A message represented by images	CMAS does not deliver video but the IPAWS Aggregator does.
○ Audio	A message represented by sound	CMAS does not deliver video but the IPAWS Aggregator does.
• Actions	The actions taken by the infrastructure	
○ Authentication	CAP messages are checked for authorized initiator.	
○ Validation	CAP message is validated against the XML schema.	
○ Translation	CAP messages are translated to CMAC message format.	

3.1.3 CMSP Infrastructure

Figure 8: CMSP Infrastructure Features

Table 5: Descriptions of CMSP Infrastructure Features in Figure 8

Element	Description	Comments
• Message_Receipt	Actions taken upon receipt of a message	
○ Authentication	Ensures that the message comes from an authorized source	Does the person listed in the message as the originator have current credentials?
○ Validation	Ensures the message is in the correct form	Does the CMAS message comply with the CAP profile's XML schema?
• Profile_Management	The aggregator maintains multiple profiles to use in authenticating the senders and possibly the receivers of alerts.	
• Message_Dissemination	The gateway forwards to the appropriate dissemination channels.	

3.1.4 Recipients

Figure 9: Recipient Features

Table 6: Descriptions of Recipient Features in Figure 9

Element	Description	Comments
• Personal_Information	What a system uses to identify individual authorized users and originators	
• Location	The geographical location of the stakeholder's mobile device	May be provided in forms other than a traditional address
• Responsibility	The position held by the stakeholder will impose requirements to act under certain circumstances.	
• Authority	In CMAS, individuals will have certain specified authorizations that define the bounds of their actions.	
○ Issue_Alerts	The categories of alerts a particular stakeholder is authorized to issue	
• Actions	The decisions and activities people are permitted to take to fulfill their responsibilities	
• Disabilities	Any attribute of the stakeholders that requires adaptive devices or measures to allow them to participate in the system	
○ Physical	The requirement relates to a physical limitation.	
▪ Sight	The limitation relates to the ability to see.	CMAS documentation requires a vibration cadence; may need larger fonts or automated readers
▪ Hearing	The limitation relates to the ability to hear.	CMAS documentation requires a vibration cadence; may require headphones or visual presentation of all information
▪ Mobility	The limitation relates to the ability to move.	May require surrogate to bring items such as a cell phone within using distance
○ Mental	The limitation relates to mental ability.	May require lower levels of vocabulary or other adaptations to usual practice

4 Evaluating the Taxonomy

The value of the CMAS taxonomy is realized when we can use it to help understand and reason about required operations. In this section, we examine a representative scenario to ensure that the taxonomy defines the elements used in that scenario. We used the SEI's mission thread approach [SEI 2012] to analyze a number of scenarios. Here we present only one as a way of illustrating the usefulness of the taxonomy. Note that the example is only an illustration of an approach to evaluating the taxonomy and does not purport to be formal or comprehensive.

A terrorist attack has just taken place in the center of Philadelphia, Pennsylvania. Multiple bombs have exploded in the subway. A regional emergency operations center generates an alert and warning message to notify Philadelphia and its surrounding geographical areas to take action to avoid the subway. An individual at the Philadelphia emergency operations center, having the proper credentials and alert generation access rights for geo-targeting alerts in the Philadelphia area, generates an EAS alert and a CMAS message. The alert indicates that the subway area should be avoided until further notice. Message recipients, including mobile device end users, in the affected areas are directed to turn to the appropriate local media for further instructions as well as for guidance on evacuating or sheltering in place [FEMA 2009].

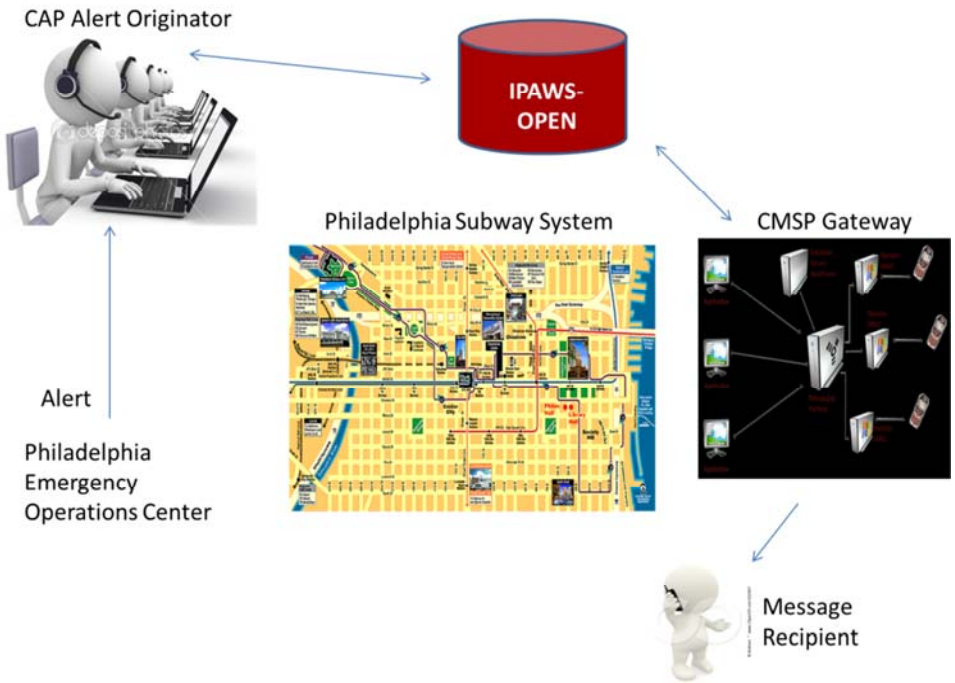

Figure 10: Environmental Context Diagram for the Philadelphia Subway Bombing Scenario

Table 7 shows the major elements in this scenario along with their location in the taxonomy.

Table 7: Mission Thread to the Ecosystem Model Map

Mission Step	Step Description	Taxonomy Elements
1	The Main Street train has just left the Spring Garden Center station.	
2	Multiple bombs explode in the Spring Garden Center station.	
3	The Philadelphia Transportation Authority control center notices loss of video and data communications with the Spring Garden station.	We begin outside the taxonomy but within the ecosystem Suppliers of originator information
4	The Philadelphia Transportation Authority contacts the Philadelphia emergency operations center that a problem has occurred and the subway station should be avoided.	Alert_Originator Organization Jurisdiction: Local Authority Scope Imminent_Threat System Software Provision_Method Who_Operates Originator
5	The Philadelphia Emergency Operations Center's CAP console operator sends the message to IPAWS.	Originator Suppliers of originator systems IPAWS Aggregator Schema Common_Alerting_Protocol
6	The message is verified by IPAWS and the CAP message is sent to the CMAS Alert Aggregator, which sends it to the Federal Alert Gateway, which, in turn, sends the CMAC-formatted message to the CMSP Gateway.	IPAWS_Infrastructure Schema Common_Alerting_Protocol CMSP_Infrastructure
7	The cell phone providers receive the CMAC message and then broadcast the message to appropriate territory based on the agreed level of support.	CMSP_Infrastructure Outside the taxonomy: suppliers of disseminator systems
8	The message is received by mobile device subscribers.	Recipient
9	The message is displayed on mobile devices.	Outside the taxonomy: mobile device supplier (and configurer)

Using the CMAS ecosystem model shown in Appendix D, we can get a measure of coverage, that is, the parts of the model exercised by the scenario as indicated by the line crossing the ovals in Figure 11.

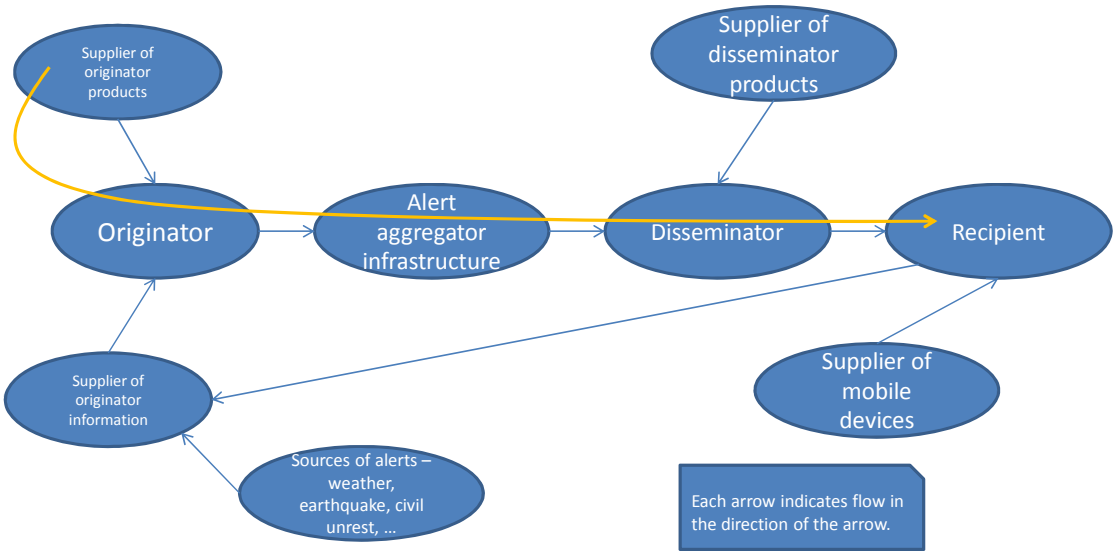

Figure 11: Map of Scenario

As an extension to the scenario, the Philadelphia Eagles are scheduled to play the New York Giants on the night of the attack. The NFL's Chief of Operations, in town for the game, receives the CMAS message on his phone. He is a federally authorized originator. He sends an alert to the New York area to reach those fans planning to travel to Philadelphia by train and alert them to seek alternative routes.

Table 8: Mission Thread Extension

Mission Step	Step Description	Taxonomy Elements
10	Original alert is received and prompts a new alert.	Recipient Outside of taxonomy: supplier of originator information Originator
11	The message is verified by IPAWS and the CAP message is sent to the CMAS Alert Aggregator, which sends it to the Federal Alert Gateway, which, in turn, sends the CMAC-formatted message to the CMSP Gateway.	IPAWS infrastructure CMSP infrastructure
12	The cell phone providers receive the CMAC message and then broadcast the message to appropriate territory based on the agreed level of support.	CMSP infrastructure Outside of taxonomy: suppliers of disseminator systems
13	The message is received by mobile device subscribers.	Recipient
14	The message is displayed on mobile devices.	Outside of taxonomy: mobile device supplier (and configurer)

The extension to the scenario increases the coverage of the pipeline as shown in Figure 12. The feed-forward loop shows how a CMAS message can be propagated through the pipeline multiple times if the recipient is also an authorized originator.

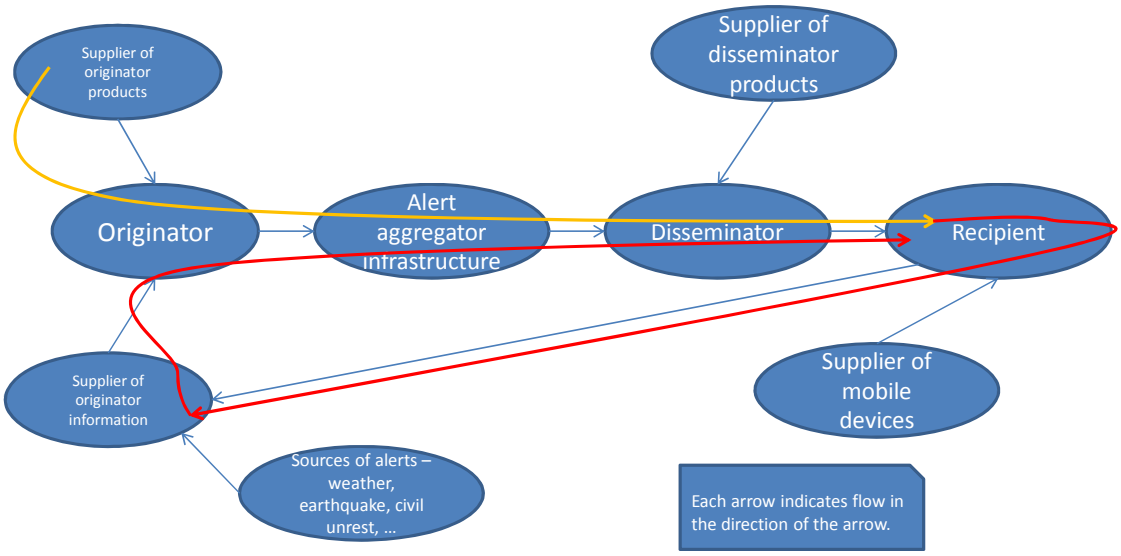

Figure 12: Extension to Include Secondary Alert

5 Using and Validating the Taxonomy

5.1 Using the Taxonomy

In considering CMAS adoption, challenges include integrating existing or new systems, user interfaces, and networks used by message originators and message disseminators. There are thousands of message originators who may initiate alerts. These include state, county, city, and tribal governments; local districts for fire protection, transit, and public utility services; and an ever-growing number of private-sector alert systems (e.g., for universities). The sheer number and diversity of these systems precludes an integration approach based on a case-by-case system examination or the application of a one-size-fits-all policy.

The CMAS Alerting Pipeline Taxonomy will simplify some actions related to an organization's effort to integrate into CMAS. Becoming CMAS compliant can require modifications to hardware, software, information, and people. The taxonomy will simplify both analysis and guidance:

- Analysis: By decomposing the CMAS Alerting Pipeline into features, the interactions among pieces will be simpler to understand.
- Guidance: The taxonomy represents the domain in a manageable form for explaining a variety of situations. Developers and testers will be able to define scenarios more quickly and easily by using the features in the taxonomy as building blocks.

Other performers in the DHS's CMAS program can use the features identified in the taxonomy to explain why an organization is successful at specific parts of CMAS operation. They can capture patterns for successful integrations and make them available as portions of the overall integration strategy. The salient features in the taxonomy can help shape the penetration strategy, which can detail techniques for getting more disseminator organizations to agree to join CMAS and handle CAP messages. These same features can provide valuable insights for building simulations of CMAS.

5.2 Validating the Taxonomy

Validating the taxonomy will proceed along two lines. Section 4 presented a high-level scenario using the mission thread approach. As the SEI CMAS team generates more of these threads, we will use each to exercise the taxonomy. We will investigate differences between the content of a mission thread and the taxonomy. Over time, this will validate the correctness and completeness of the taxonomy and identify areas where the taxonomy can be improved.

The SEI CMAS team will also continue to monitor the community for examples of successful integration. Collecting these examples has two purposes. Comparing an organization's successful experience with the guidance that we would give based on the taxonomy will allow for validation and evolution of the taxonomy. Over time, this will validate the correctness and continually redefine completeness.

6 Summary and Future Directions

This initial release of the CMAS Alerting Pipeline Taxonomy provides several points from which to approach CMAS. The CMAS ecosystem model adds the people at each end of the pipeline for completeness. The CMAS taxonomy then builds on this expanded model. The taxonomy presented here should provide a consistent context for other tasks.

The taxonomy will evolve as CMAS evolves and as understanding of the issues surrounding CMAS evolves. The ability to receive alerts from areas other than the person's current location and the ability to forward alerts to other devices are examples of possible future features. The IPAWS architecture positions FEMA and DHS to take advantage of emerging mobile devices.

The need for additional elements and features will emerge as we elaborate the CMAS Alerting Pipeline Taxonomy in future versions. Particularly likely to emerge are classifications based on risks related to the system-of-systems nature of CMAS and the security characteristics of the constituent systems. Both risk and security appear at multiple places in the current classifications and will evolve as we drill down into the existing classifications.

Appendix A Glossary

alert	*See alert message.*
alert acknowledgment	1. CMSP gateways are responsible for acknowledging message receipt. 2. A subscriber (end user of a mobile device) is responsible for acknowledging alerts.
Alert Aggregator	The link in the CMAS pipeline that collects alerts from various sources and sends them to the appropriate dissemination points.
alert area	The geographic region to which the alert applies.
alert class	*See alert type.*
alert message	A message formatted according to the CAP. Currently restricted to text only, with a maximum of 90 characters, and in the English language.
alert originator	An organization authorized to issue an alert. Alert origination occurs at the presidential, federal, state, local, and tribal government levels.
alert recipient	A mobile service subscriber.
alert status	An indication of whether an alert is active, updated, cancelled, etc.
alert type	A CMAS message can be one of three types: presidential, imminent threat, or AMBER.
attention signal	A unique vibration cadence or audio signal to indicate to a subscriber that a mobile device has received a CMAS message.
Commercial Mobile Alert Reference Point C (CMAC)	The format used for CAP messages as they are disseminated from the aggregator to the operators.
Commercial Mobile Service Provider (CMSP) Gateway	The CMSP function that receives, authenticates, and validates alert messages from the Federal Alert Gateway.
Common Alerting Protocol (CAP)	An open, nonproprietary digital message format for alert messages. The CAP is a standard produced by the Organization for the Advancement of Structured Information Standards (OASIS).
Federal Alert Gateway	The federal function that translates alert messages into the format required by CMSPs and sends the messages to the appropriate CMSP gateways.

geo-targeting	Translating the alert area indicated in the alert message into the associated set of cell sites or paging transceivers for the broadcast of the alert message.
message	An alert message or a test message.
message log	A record of all outgoing CAP-formatted messages from an alert originator.
message validation	A message is compared to the official schema for messages following the specified protocol.
profile	1. An agreed-upon subset and interpretation of the CAP specification (e.g., the IPAWS CAP profile constrains the CAP standard for use by IPAWS exchange partners). 2. Information about a CMSP that enables the federal aggregator and gateway functions to determine if the CMSP is a current CMAS participant, the alert area is covered by that CMSP, etc. (The Federal Alert Gateway maintains a catalog of CMSP profiles.)
provider	A CMSP that owns and operates the infrastructure capable of delivering alerts to mobile devices.
region	*See alert area.*
test message	A required monthly test (RMT) message or a periodic heartbeat message. These are CAP-formatted messages, like any other alert message.

Appendix B Acronyms

AMBER	America's Missing: Broadcast Emergency Response
API	application programming interface
CAP	Common Alerting Protocol
CMAC	Commercial Mobile Alert Reference Point C
CMAS	Commercial Mobile Alert Service
CMSP	commercial mobile service provider
COTS	commercial off-the-shelf
DHS S&T	Department of Homeland Security Science and Technology Directorate
EAS	Emergency Alert System
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GUI	graphical user interface
IPAWS	Integrated Public Alert and Warning System
OASIS	Organization for the Advancement of Structured Information Standards
OEM	office of emergency management
OPEN	Open Platform for Emergency Networks
RMT	required monthly test
SBIR	small business innovation research
XML	Extensible Markup Language

Appendix C Initial Scenarios

Active Shooter Operational Scenario

An active shooter has opened fire in a crowded area in front of the main entrance to the Mall of America (Bloomington, MN) and runs inside the mall. Multiple people have been killed and several others have been wounded. The Bloomington Police Department's Mall of America Unit personnel, located on the second floor of the east entrance to the mall, are the first to arrive at the scene. They establish an incident command center to coordinate efforts with the Minneapolis Emergency Preparedness Team. The incident commander has decided to issue a CMAS message for the entire Monroe County, to including Bloomington and the Minneapolis–St. Paul International Airport. The message will alert people inside the mall to take shelter in place and those outside to avoid the mall area and turn to other appropriate media for further instructions, where up-to-date information and instructions are provided on a regular basis.

Purpose	To generate and send a CMAS message to alert people about an active shooter inside the Mall of America and instruct those inside to shelter in place and those outside the mall to avoid the area
Event	Active shooter inside the mall
Originator	A Minneapolis Emergency Preparedness individual having the proper authority, training, credentials, and alert generation access rights for geo-targeting
Alert message	Message follows a predefined template and must convey the following: Specific hazard: a person shooting people at random Location: inside Mall of America Time frames: ongoing Source of warning: Minneapolis Emergency Preparedness Office Magnitude: life threatening Likelihood: observed Protective behavior: take shelter in place or stay away from mall area
Disseminator	Participating CMSPs within Monroe County
Technology	A map-based CMAS authoring tool used as cloud-based service through a secure internet connection Tool vendor connects directly to IPAWS Aggregator Cellular broadcast messaging technology
Recipient	90% of all turned-on mobile devices within Monroe County at the time the CMAS message is issued and which are subscribing to participating CMSPs or are roaming on the network of participating CMSPs
Response target	Message recipients who are inside the mall are instructed to take shelter, for instance, by securing doors, staying silent, avoiding sudden movement, silencing cell phones, etc. Message recipients who are outside the mall are instructed to avoid coming to mall area and to turn to other media where further information is assumed to be.

Tornado Warning Operation Scenario

The Denver/Boulder National Weather Service local office has spotted a tornado in the Denver area heading southwest across Jefferson Country (JeffCo), Colorado, at 30 mph. This information is shared with the JeffCo Office of Emergency Management (OEM). The designated emergency manager has decided to issue a Tornado Warning through a CMAS message within the entire JeffCo jurisdiction. The message will notify members of the public about the imminence of a radar-indicated tornado heading toward their area and instruct them to take shelter by moving indoors to a low level or interior space.

Purpose	To generate and send a CMAS message to alert members of the public about a radar-indicated tornado heading from Denver southwest across JeffCo and instruct them to take shelter
Event	An already-formed tornado
Originator	A JeffCo OEM individual having the proper authority, training, credentials, and alert generation access rights for geo-targeting
Alert message	Message follows a predefined template and must convey the following: Specific hazard: tornado Location: Jefferson County Time frames: imminent Source of warning: JeffCo OEM Magnitude: life threatening and potential property damage Likelihood: observed Protective behavior: take shelter immediately
Disseminator	Participating CMSPs within JeffCo
Technology	A map-based CMAS authoring tool used as a commercial off-the-shelf (COTS) product operated from JeffCo OEM COTS product is configured to connect directly to IPAWS Aggregator Cellular broadcast messaging technology
Recipient	90% of all turned-on mobile devices within JeffCo at the time the CMAS message is issued and which are subscribing to participating CMSPs or are roaming on the network of participating CMSPs
Response target	Message recipients are instructed to take shelter indoors in a lower level or interior space and to stay away from glass doors, windows, and walls until further notice

Daycare Raid Operational Scenario

A small day care in Christiansburg, Virginia, has been raided by two masked persons at around 7:00 a.m. A four-year-old girl has been abducted, put in a green Dodge minivan, and driven in the direction of US-460 West. A Christiansburg Police Department deputy officer arrives at the scene first and immediately sends the name, description, and photo of the abducted child along with descriptions of the two suspects and their vehicle to the dispatch center. The Christiansburg Police Department's chief has decided to issue an AMBER alert using CMAS within Montgomery and Giles counties to cover towns and cities connected by US-460. The CMAS message will alert the community about an abducted child and give critical information about the child and suspects, direct them to other sources for more information, and request help in alerting local authorities about information relevant to the case.

Purpose	To generate and send a CMAS message to galvanize the help of the public about a child abducted from a local day care
Event	Child abduction from day care
Originator	A Christiansburg Police Department individual having the proper authority, training, credentials, and alert generation access rights for geo-targeting
Alert message	Message follows a predefined template and must convey the following: Specific hazard: two suspects abducted a child from a day care Location: local Christiansburg day care Time frames: ongoing Source of warning: Christiansburg Police Department Magnitude: risk of serious bodily injury or death Likelihood: observed Protective behavior: send relevant information to law enforcement about the case
Disseminator	Participating CMSPs within Montgomery and Giles counties
Technology	A map-based CMAS authoring tool developed in-house as part of a dashboard application that connects to multi-notification systems. The tool integrates directly with the IPAWS Open Platform for Emergency Networks (OPEN) cellular broadcast messaging technology.
Recipient	90% of all turned-on mobile devices within Montgomery and Giles counties at the time the CMAS message is issued and which are subscribing to participating CMSPs or are roaming on the network of participating CMSPs
Response target	Message recipients are directed to other media to learn more information and are encouraged to send relevant information about the abduction to law enforcement

Appendix D CMAS Ecosystem Model

Introduction

Purpose

Every organization exists in a complex network of customers, suppliers, competitors, and collaborators. Just as in a natural ecosystem, an organization receives needed resources from some members of the network and must protect itself from other members. An ecosystem model is an abstract representation of the ecosystem formed by combining relationships native to the domain with data gathered from a number of sources, which can aid strategic decision makers. An ecosystem model for an organization supports strategic decision making by providing information about the interactions among the organizations that are sufficiently related that the actions of one organization affect others. An ecosystem model captures relationships over a broader scope than many managers think about on a day-to-day basis and can be used to set agendas for answering specific questions.

The CMAS ecosystem model allows strategic thinkers in the emergency-notification domain to consider relationships among the organizations, software products, and innovations for the future to determine how they can benefit. For example, emergency managers can benefit through improved alerting systems, and organizations supplying the CMAS community can benefit through improved profits. The model is only as good as the data that it represents. This model will evolve as we collect and incorporate more information into it.

Scope

The CMAS ecosystem includes organizations that originate emergency alert messages and organizations that broadcast alerts. It also includes organizations that receive requests for emergency assistance, such as OnStar, if they also have the capability to send emergency alerts to their customers.

Audience

The audience for an ecosystem model is strategic decision makers. For CMAS the audience includes government officials of various jurisdictions, such as FEMA and DHS officials who set policy and strategic directions; emergency managers; and executives in the provider organizations. The people charged with making strategic decisions regarding systems, business alliances, and innovations within the scope of the ecosystem can use this model to assess their choices. The model should alert them to dependencies within the ecosystem that affect the impact of their decisions.

Content Overview

The ecosystem model includes three views of the CMAS ecosystem. The business view uses Porter's Five Forces model to identify the members of the ecosystem and classify them based on one set of criteria [Porter 2008]. The software view is divided into the originator and disseminator roles of the CMAS architecture. The innovation view uses a classification from *Businessweek* to dissect the ecosystem from the perspective of how technological advances will affect the business and software views.

Figure 13 shows a notional ecosystem model that identifies the major categories of organizations and represents the major categories of software systems. Detailed figures of the business view identify many of these organizations. One limitation of the current version of the CMAS ecosystem model is that it lists suppliers of originators but does not follow the supply chains beyond that. Most supply chain issues occur in links subsequent to the original equipment manufacturer, that is, the focal organization. Future versions of the ecosystem model may be able to add more information about supply chains.

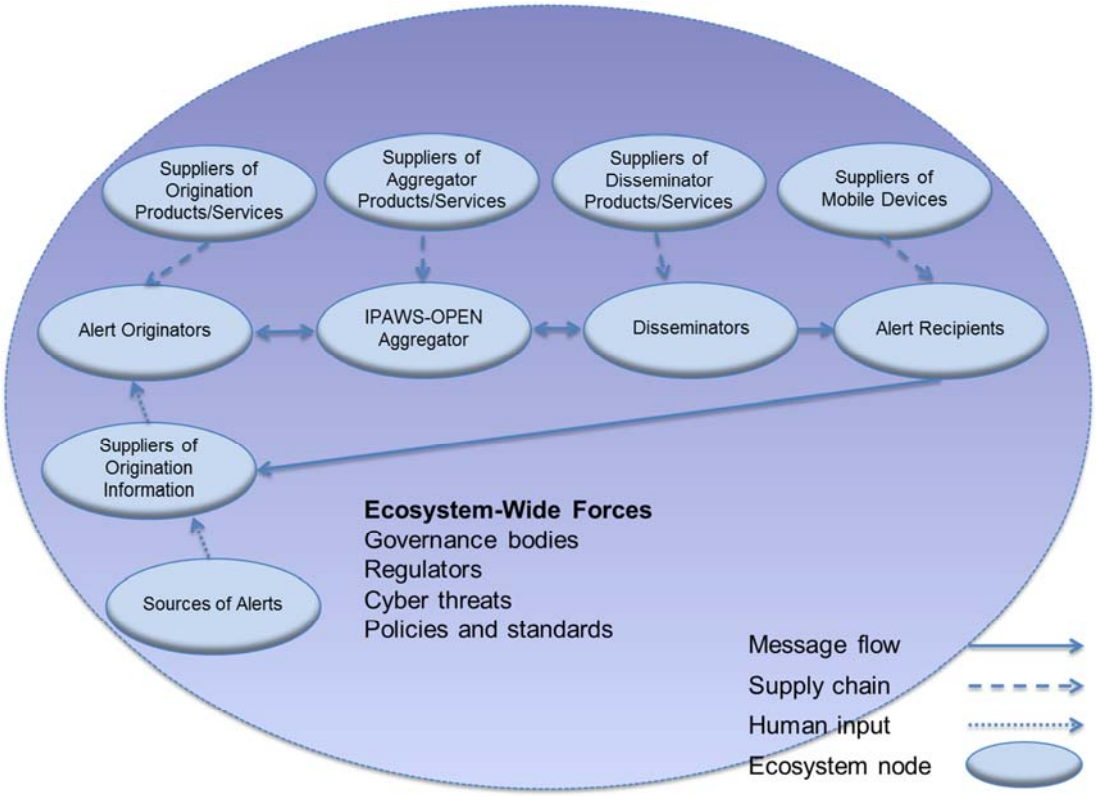

Figure 13: Notional Ecosystem Model

Business View

Strategy Development

Porter's Five Forces for business strategy development, shown in Figure 14, is a strategic development tool that uses the five external forces that act on a company to develop a strategic plan [Porter 2008]. The CMAS ecosystem is an interesting blend of commercial and governmental organizations, some of which collaborate within the emergency alerting system of systems and some of which compete in the marketplace to provide products and services. We will explore the five forces from this unusual perspective.

Since the CMAS project is a government-led initiative, there is access to much of the business and technical information about those portions of the system of systems that the government provides. Basic specifications in the original Congressional orders are available to all strategists [FCC 2011].

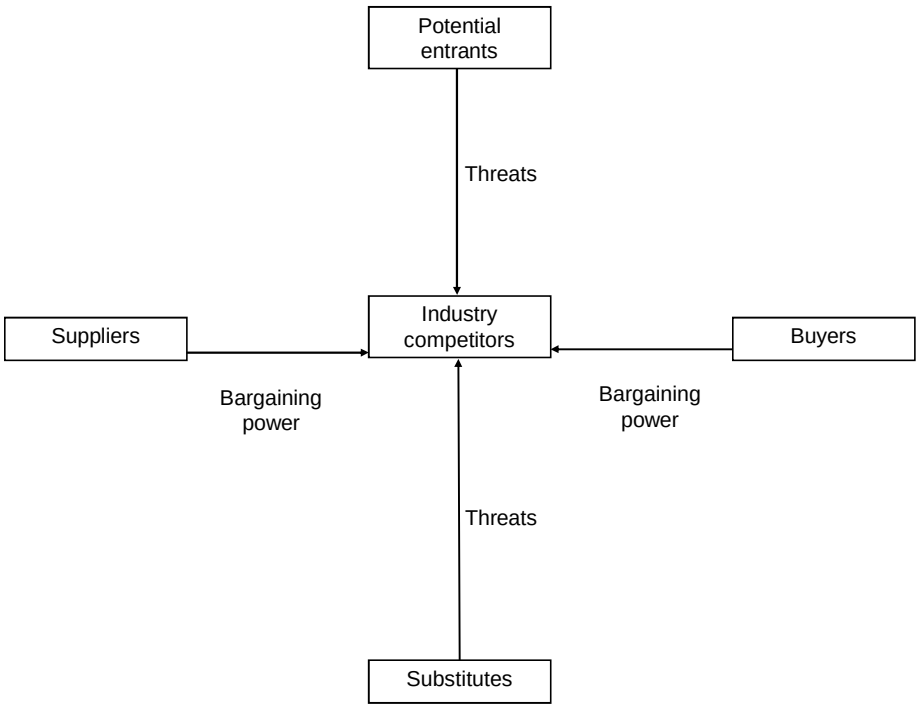

Figure 14: Porter's Five Forces Model [Porter 2008]

Competitors

Organizations within the CMAS system have disparate views of competition. From the perspective of FEMA and DHS, competition is not an issue. Communication of emergency alerts is a critical service that consumers should receive, and if others provide it, that is acceptable. From the disseminators' perspective, CMAS is a feature that may add value for the consumer at the moment but will soon become a commoditized, basic requirement. For example, as the baby boomers grow older, mobile services might advertise the cell phone as a safety net as part of a short-term marketing strategy. From the originators' perspective, a competitor represents a jurisdictional issue. For a given emergency and geographic region, multiple authorized originators may exist for each type of alert. They must resolve "competition" prior to the need to issue an alert to ensure that the originators issue only one alert per event. The DHS can assist by having a suggested authorization plan for city, county, and state governments. From the recipients' perspective, there is existing competition. Products like ELERTS (elerts.com), an app for iPhone and Android, claim to allow longer messages and two-way conversation.

Suppliers

The ecosystem model divides the "suppliers" category into three segments: FEMA, suppliers to the originators, and suppliers to the disseminators.

FEMA supplies the OPEN Aggregator as a central aggregator through which all emergency alerts will flow. More localized environments, such as university or corporate campuses, use other aggregators. CMAS performers should monitor the suppliers of these more localized aggregators to mine their features for new ideas. One particular issue for OPEN will be the ability to handle the messaging load during a widespread emergency.

A large number of software vendors supply alert originating systems. Figure 15 shows an initial graphic, and a list appears at the end of this appendix.

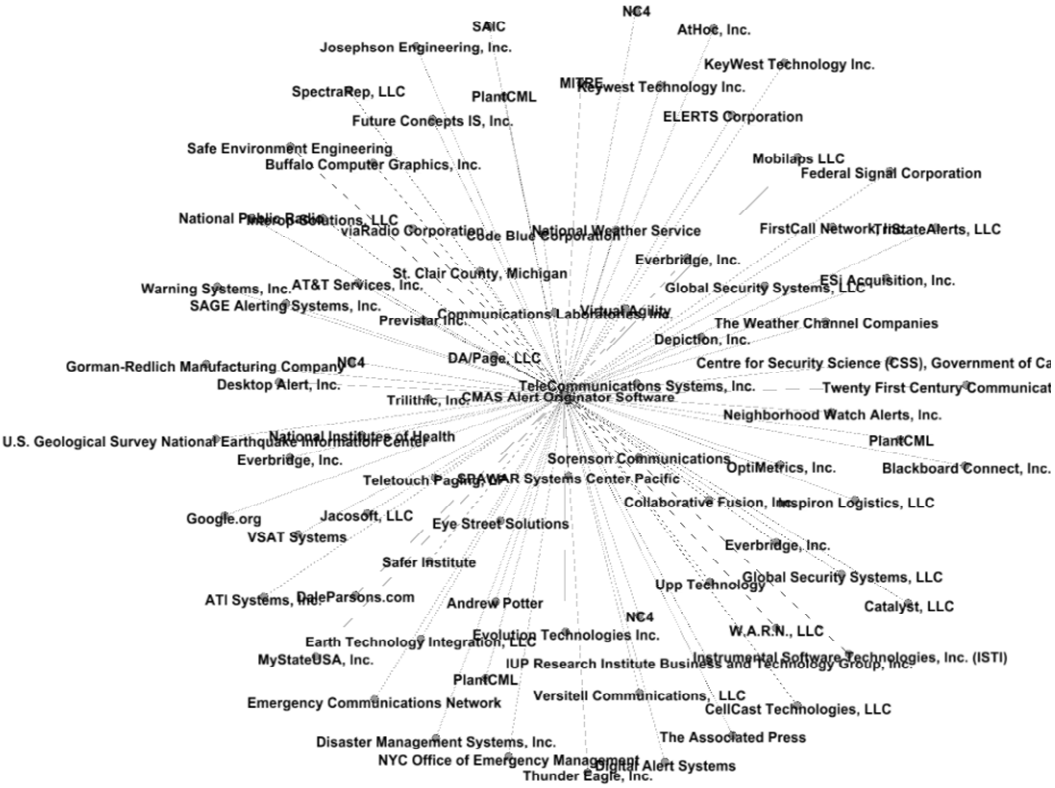

Figure 15: Suppliers of Origination Software

A smaller number of vendors supply the disseminators. One major hardware supplier is Alcatel-Lucent, but we have not seen a central software supplier. Ultimately, every carrier has to implement CMAS in their respective systems. Many of the disseminators have in-house software development organizations and will not use outside suppliers. The DHS can help grow this market through more participation in telecommunication organizations and by sponsoring workshops that bring together development organizations of the disseminators to share patterns and techniques.

Buyers (Users)

There are several types of buyers in the CMAS ecosystem. The goal of buyers of emergency alert systems, such as emergency management officials, is to reach as much of the targeted audience as possible as rapidly as possible. Buyers drive evolution of the alert systems as their communication patterns change and the audience migrates from one form of communication to another or from one service provider to another. Alert originators initially chose television and radio to broadcast emergency alerts since most people had access to those media. Now originators and disseminators are exploring areas such as social networks because the public uses social media widely, and it has changed the evolutionary trajectory. Consumers of emergency information initially relied on publicly available services, but the options have expanded to include paid versions of these services.

Potential Entrants

The greatest potential for new entrants into the CMAS ecosystem is as new suppliers of origination software. This is a competitive market; however, most of the suppliers seem to be relatively small, regional organizations. Emergency alert systems require a wide range of features. The features provided in the taxonomy illustrate the range of features in various alert systems. The DHS could stimulate this market with an initiative to grant awards for small business innovation research (SBIR) related to emergency management. The DHS might also stimulate the formation of open-source communities for emergency alert systems. The CAP message format is a simple XML-based format that is easy to work with. The cost of entry into this market is low. Wrapping an open-source XML editor with a few graphic user interface (GUI) widgets can produce an alerting tool, albeit one that is not integrated into the rest of the user's software toolset for emergency management.

Substitutes

The organizations shown in Figure 15 provide alternatives for acquiring emergency alert origination software. Acquisitions are getting competing bidders, but the market is quite diverse, making it difficult to know exactly which products are substitutes for each other. For some time, acquirers will have to hunt for the features they want or spend time developing a robust specification. An integration strategy, currently under development, will assist acquirers in gaining that information.

Constraints

The most important constraints in the CMAS environment are government regulations, policies, and standards. The *CMAS First Report and Order* provides a set of requirements and specifications that service providers must satisfy in order to participate in CMAS [FCC 2008]. In addition, the CAP is central to CMAS. All origination software must produce messages that are CAP compliant.

Software View

The notional CMAS software architecture, shown in Figure 16, provides the major elements that divide the software ecosystem into three categories. The organizations shown in Figure 15 produce products that fit mainly into the originator category. Much less information is available on the software for dissemination due to the competitive nature of many of those organizations. A later version of this model will include more information about disseminators' software.

Figure 16: CMAS Software Architecture

The originator and disseminator categories have little overlap due to the different nature of the tasks and the output. Origination software must be usable by individuals with little training while operating under crisis pressures. The software must be flexible, allowing operation from a variety of sources while maintaining security to ensure that any alert is properly authorized. The main output is well defined and standardized in the CAP message standard. The dissemination software takes the well-defined CAP messages as input and propagates the message to a variety of devices, all of which it has control over even if it does not own them. The disseminator must provide an

output that can be delivered to a large number of brands and models of devices. This software will see continual evolution as communication standards and technologies evolve.

Innovation View

Innovation in an ecosystem of software-intensive products usually involves both the business and the software; therefore, the innovation view of the ecosystem captures the interaction between the business and software views. *Businessweek* identified a classification of types of innovation. We use that classification to explore innovation in the CMAS ecosystem.

Innovation occurs in four main ways [Businessweek 2009]:

- **Product innovation:** Product innovation is occurring in each segment of the CMAS architecture. The OPEN Aggregator is a new concept and will require high reliability and availability to avoid becoming the single point of failure. Disseminators are exploring a unique means of delivering messages—cell broadcast—that must be delivered regardless of the state of the receiver. Originators are working on integrating CMAS with existing alerting systems to ensure that they reach the greatest number of their constituents.
- **Process innovation:** Originators are considering how to authorize a wider range of people to offer alerts and allow a wider variety of ways to physically create and issue alert messages. The issuing process also changes in that the originator has a wider range of ways to define the area to which the alert will be sent.
- **Customer experience innovation:** Disseminators are experimenting with the best ways to display an alert given the limitations of the lowest common denominator among the variety of cell phone devices. Everyone must be able to access the message, even those who use the phone only occasionally. CMAS also requires that disseminators support both vibration and audible signals to accommodate recipients with specific needs.
- **Business model innovation:** So far, there is little evidence of innovation in this area. One example is that cell carriers may be defining new ways to target portions of their users to receive messages. The most evident innovations are the new, open standards under construction. These standards can lead to new business models when new ways of providing services emerge.

Five factors of the business and software climate influence innovation [Businessweek 2009]:

- **Strategy:** One strategy that CMAS participants will use is to cover as many media outlets as possible. By adding cellular communication, the alert system will address a growing audience who no longer has landline service.
- **Process:** The DHS and FEMA are innovating by creating communication processes that engage a range of system stakeholders. The current CMAS effort will provide major opportunities for stakeholder involvement. By publishing standards, these organizations are changing the process of producing CAP-compliant products.
- **Climate:** The innovations in this ecosystem currently speak to the need for more narrowly targeted warnings and alerts. As advances in radar and other forecasting improvements allow meteorologists to more accurately identify the locations in danger, CMAS will provide more narrowly focused alerts.

- **Structure:** The aggregator architecture is structuring the alerting activities to provide a system-of-systems approach that will make extending the structure easier and more accurate. However, a system of systems brings risks. The requirement that an error message be sent back to the originator of a faulty message adds to the necessary structure.
- **Competency:** The research work funded by the DHS is helping a set of practitioners and researchers to increase their understanding of the concepts and actions surrounding warnings and alerts. The data collected by the SEI during stakeholder interviews also adds to our knowledge and our ability to strategize.

Ecosystem Analysis

Three fundamental measures of the health of an ecosystem are productivity, robustness, and niche creation. We evaluate the progress of CMAS according to these characteristics.

In terms of productivity, the larger ecosystem of all types of public emergency alerts is expanding as a result of the CMAS project. By offering new opportunities for alerting the public to emergencies, the value of the ecosystem to potential members, such as the cell carriers, has greatly increased. Meanwhile, the state of the world in terms of environmental climate and politics requires more attention to warnings and alerts. These concerns cut across political boundaries to include systems such as the Pacific Rim Tsunami Warning System. Much activity exists in this arena, with private companies and educational institutions installing systems, so the ecosystem is highly productive.

In terms of robustness, the ecosystem meets a fundamental need for the security and safety of the human population, so funding must be sufficient to stimulate research and development in the area of warnings and alerts. Wireless technology in particular requires attention to communication security, so the ecosystem needs more research in this area.

In terms of niche creation, the ecosystem continues to grow. With the planned deployment of CMAS to bring alerts and warnings to cellular phones, this program has created a new audience and in many senses a new niche in the larger communication ecosystem. It will likely create additional niches as new communication technologies gain acceptance.

Recommended Actions Derived from Building the Ecosystem Model

Previous sections of this report included several recommendations, and we summarize these here.

- DHS S&T can assist in resolving jurisdictional ambiguity by having a suggested authorization plan for city, county, and state governments.
- DHS S&T can help grow the segment of technology providers into a community by participating in telecommunication organizations and sponsoring workshops at national conferences and as stand-alone events to bring together development organizations of the disseminators to share patterns and techniques.
- The CMAS program should monitor suppliers to mine their features for new ideas.
- DHS S&T could stimulate this market with an SBIR related to emergency management. It might also stimulate the formation of open-source communities for emergency alert systems.

Elements of the CMAS Ecosystem

This is an initial list of CMAS components created early in the ecosystem study to get a flavor of the ecosystem. It is not a detailed inventory.

Originators

- Federal
- State
- Territorial
- Tribal
- Local
- Collaborative operating groups

Suppliers of Originator Software

- Andrew Potter
- Associated Press
- AT&T Services, Inc.
- AtHoc, Inc.
- ATI Systems, Inc.
- Blackboard Connect, Inc.
- Buffalo Computer Graphics, Inc.
- Burke Technologies
- Cadco Systems, Inc.
- Catalyst, LLC
- CellCast Technologies, LLC
- Centre for Security Science, Government of Canada
- CMAS Alerts Disseminator Software
- Code Blue Corporation
- Collaborative Fusion, Inc.
- Communications Laboratories, Inc.
- DaleParsons.com
- DAPage, LLC
- Depiction, Inc.
- Desktop Alert, Inc.
- Digital Alert Systems
- Disaster Management Systems, Inc.
- Earth Technology Integration, LLC
- ELERTS Corporation
- Emergency Communications Network
- ESi Acquisition, Inc.

- Everbridge, Inc.
- Evolution Technologies, Inc.
- Eye Street Solutions
- Federal Signal Corporation
- FirstCall Network, Inc.
- Future Concepts IS, Inc.
- Global Security Systems, LLC
- Google.org
- Gorman-Redlich Manufacturing Company
- HollyAnne Corp
- Inspiron Logistics, LLC
- Instrumental Software Technologies, Inc. (ISTI)
- Interop-Solutions, LLC
- IUP Research Institute Business and Technology Group, Inc.
- JacoSoft, LLC
- Josephson Engineering, Inc.
- KeyWest Technology, Inc.
- M&N Laboratories
- MITRE Corporation
- MobiLaps, LLC
- Multi-Technical Services, Inc.
- MyStateUSA, Inc.
- National Institutes of Health
- National Public Radio
- National Weather Service
- NC4
- Neighborhood Watch Alerts, Inc.
- New York City Office of Emergency Management
- Nixle
- OptiMetrics, Inc.
- PlantCML
- Previstar, Inc.
- Safe Environment Engineering
- Safer Institute
- SAGE Alerting Systems, Inc.
- SAIC
- Sorenson Communications

- SPAWAR Systems Center Pacific
- SpectraRep, LLC
- St. Clair County, Michigan
- TeleCommunications Systems, Inc.
- Teletouch Paging, LP
- TFT, Inc.
- Thunder Eagle, Inc.
- T-Mobile
- Trilithic, Inc.
- TriStateAlerts, LLC
- Twenty First Century Communications, Inc.
- U.S. Geological Survey National Earthquake Information Center
- Upp Technology
- Verizon
- Versitell Communications, LLC
- viaRadio Corporation
- Virtual Agility
- VSAT Systems
- WARN, LLC
- Warning Systems, Inc.
- Weather Channel Companies

Disseminators

- CMAS
- EAS
- Internet
- National Oceanic and Atmospheric Administration
- Unique local services

Disseminator Component Developers

One Way Out

- Broadcast Message Center/Alcatel-Lucent
- Everbridge (for companies, buildings, universities, etc.)
- National Emergency Alert Notification System

One Way In

- American Medical Alert
- American Senior Safety Agency
- Code Red
- LifeStation

- Medical Home Alert
- MedicalAlert/ConnectAmerica
- ParentREACH/Amfax Corporation

In/Out

- OnStar

References

URLs are valid as of the publication date of this document.

[Alberts 2008]
Alberts, C.; Smith, J., II; & Woody, C. *Multi-view Decision Making (MVDM) Workshop* (CMU/SEI-2008-SR-035). Software Engineering Institute, Carnegie Mellon University, 2008. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8507

[Barbacci 2003]
Barbacci, M. R.; Ellison, R.; Lattanze, A. J.; Stafford, J. A.; Weinstock, C. B.; & Wood, W. G. *Quality Attribute Workshops (QAWs), Third Edition* (CMU/SEI-2003-TR-016). Software Engineering Institute, Carnegie Mellon University, 2003. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6687

[Businessweek 2009]
Businessweek. *Fifty Most Innovative Companies*. http://www.businessweek.com/magazine/toc/10_17/B4175innovative_companies.htm (2009).

[Carelli 2010]
Carelli, R. A.; Allen, J. H.; & White, D. W. *CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational* Resilience. Addison-Wesley Professional, 2010.

[Cebula 2010]
Cebula, J. J. & Young, L. R. *A Taxonomy of Operational Cyber Security Risks* (CMU/SEI-2010-TN-028). Software Engineering Institute, Carnegie Mellon University, 2010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9395

[CMSAAC 2007]
Commercial Mobile Service Alert Advisory Committee. *PMG-0035 Commercial Mobile Alert Service Architecture and Requirements*. Federal Communications Commission, 2007.

[DHS 2011]
Department of Homeland Security & Touchstone Consulting Group. *The CMAS Alert Broadcast*. DHS, 2011.

[FCC 2008]
Federal Communications Commission. *CMAS First Report and Order* (PS Docket No. 07-287, FCC 08-99). FCC, 2008. http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-08-99A1.pdf

[FCC 2011]
Federal Communications Commission. *Commercial Mobile Telephone Alerts (CMAS)*. http://transition.fcc.gov/pshs/services/cmas.html (2011).

[FEMA 2009]
Federal Emergency Management Agency. *Commercial Mobile Alert System (CMAS) Concept of Operations (CONOPS)* (Version 1.0). FEMA, 2009.

[FEMA 2011a]
Federal Emergency Management Agency. *Integrated Public Alert and Warning System – Open Platform for Emergency Networks (IPAWS-OPEN) Common Alerting Protocol Message Construction Guide* (Version 0.4). FEMA, 2011.
http://www.fema.gov/pdf/emergency/ipaws/ipaws_cap_mg.pdf

[FEMA 2011b]
Federal Emergency Management Agency. *IPAWS Architecture Diagram*.
http://www.fema.gov/pdf/emergency/ipaws/architecture_diagram.pdf (2011).

[FEMA 2011c]
Federal Emergency Management Agency. *IPAWS Projects: Commercial Mobile Alert System*.
http://www.fema.gov/emergency/ipaws/projects.shtm#6 (2011).

[ISO/IEC/IEEE 2010]
International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. *ISO/IEC/IEEE 24765: 2010, Systems and Software Engineering – Vocabulary*. ISO, 2010.

[NAS 2011]
National Academy of Sciences. *Public Response to Alerts and Warnings on Mobile Devices*. National Academies Press, 2011.

[OASIS 2009]
Organization for the Advancement of Structured Information Standards. *Common Alerting Protocol, v1.2 USA Integrated Public Alert and Warning System Profile* (Version 1.0). OASIS, 2009.
http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf

[OASIS 2010]
Organization for the Advancement of Structured Information Standards. *Common Alerting Protocol* (Version 1.2). OASIS, 2010. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

[OUSD 2008]
Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems, and Software Engineering. *Systems Engineering Guide for Systems of Systems, Version 1.0*. OUSD (A&T)/SSE, 2008. http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf

[Porter 2008]
Porter, M. E. "The Five Competitive Forces That Shape Strategy." *Harvard Business Review 86*, 1 (January 2008): 78–93.

[SANS 2012]
SANS Institute. *Glossary of Security Terms*. SANS, 2012. http://www.sans.org/security-resources/glossary-of-terms

[SEI 2012]
Software Engineering Institute. *Mission Thread Workshop*. Software Engineering Institute, Carnegie Mellon University, 2012.
http://www.sei.cmu.edu/architecture/tools/establish/missionthread.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2012	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Commercial Mobile Alert Service (CMAS) Alerting Pipeline Taxonomy	FA8721-05-C-0003

6. AUTHOR(S)

The WEA Project Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2012-TR-019

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report presents a taxonomy developed for the Commercial Mobile Alert Service (CMAS). The CMAS Alerting Pipeline Taxonomy is a hierarchical classification that encompasses four elements of the alerting pipeline: alert originator, Integrated Public Alert and Warning System aggregator, commercial mobile service provider infrastructure, and recipients. The taxonomy treats the alert-originator element in the most detail, identifying key features of alert-originator organizations and systems. It also identifies a limited number of features for the other three elements. The purpose of the CMAS taxonomy is to help stakeholders understand and reason about required operations. To this end, the report provides a representative scenario to ensure that the taxonomy defines the elements used in CMAS operations. The CMAS Alerting Pipeline Taxonomy will simplify some actions related to an organization's effort to integrate into CMAS. The taxonomy will simplify analysis by decomposing the CMAS Alerting Pipeline into features so that the interactions among pieces will be simpler to understand. And the taxonomy will simplify guidance by representing the domain in a manageable form for explaining a variety of situations.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Commercial Mobile Alert Service, emergency alerting, IPAWS, software architecture, software acquisition, software integration, taxonomy	52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL